On S-Equivalence of Seifert Matrices.

Trotter, H.F.

pp. 173 - 208

Inventiones math. 20, 173–207 (1973)

On S-Equivalence of Seifert Matrices

H.F. Trotter (Princeton)

Introduction

From the purely algebraic point of view taken in this paper, a *Seifert matrix* is simply a square matrix V of integers such that $\det(V+\varepsilon V')=\pm 1$, where ε is either $+1$ or -1 and V' is the transpose of V. The relation of *S-equivalence* is defined as follows [6]. W is (integrally) *congruent* to V if $W=PVP'$ for some integral matrix P with $\det(P)=\pm 1$. W is a *row enlargement* of V, and V is a *row reduction* of W, if W is obtained by bordering V with two additional rows and columns in such a way that

$$W=\begin{bmatrix} 0 & 0 & 0 \\ 1 & x & u' \\ 0 & v & V \end{bmatrix}. \tag{0.1}$$

(Here x is a number, v a column vector, and u' a row vector.) W is a *column enlargement* of V, and V a *column reduction* of W if W' is a row enlargement of V'. (The mnemonic idea behind the terminology is that row enlargement adds a row of zeros.) S-equivalence is then defined as the equivalence relation generated by congruence, enlargement, and reduction. It is easily checked that the class of Seifert matrices for a given value of ε is closed under S-equivalence. (Note that x and u' in the matrix (0.1) can be annihilated by a congruence transformation. Hence the meaning of S-equivalence is not altered if they are required to be 0, as in [6].)

The *Seifert form* determined by a Seifert matrix V is defined as a $(-\varepsilon)$-hermitian form on a certain torsion module A_V over the ring $\Lambda=Z[t,t^{-1},(1-t)^{-1}]$. The form takes values in F/Λ, where $F=Q(t)$ is the quotient field of Λ and "hermitian" refers to the conjugation which interchanges t and t^{-1}. The detailed definition is given in Section 1. The main result of this paper is the theorem that two matrices determine isometric forms if and only if they are S-equivalent.

Seifert matrices arise in the study of embeddings of an odd-dimensional sphere S^{2n-1} in S^{2n+1}. Any oriented $2n$-manifold M embedded in S^{2n+1} with $\partial M=S^{2n-1}$ is called a Seifert manifold for the given embedding. An integer-valued bilinear form θ is defined on $H_n(M)$ by setting $\theta(\alpha, \beta)$ equal to the linking number of a cycle representing α with a translate in the positive normal direction to M of a cycle representing β. (It is assumed that both S^{2n-1} and S^{2n+1} have given orientations.) The form θ vanishes on torsion elements and is therefore well-defined on the torsion-free part of $H_n(M)$, which is a finitely generated free Z-module. If $\{b_i\}$ is a basis for this module, the form is completely described by the matrix V with $v_{ij}=\theta(b_i, b_j)$, and it can be shown that any such V is a Seifert matrix, for $\varepsilon=(-1)^n$. A different choice of basis alters V by a congruence transformation, while adding an n-dimensional handle produces an enlargement of V, so one can not expect the embedding type of ∂M to determine more than an S-equivalence class of matrices.

These matrices, for $n=1$, the case of classical knot theory, were introduced by Seifert [14, 15], who showed that all the known knot-invariants depending on the homology of cyclic coverings could be computed from them. The notion of S-equivalence (under the name of h-equivalence) appeared in [16], but its significance was not then understood. Murasugi [11] actually used the relation (under the name of s-equivalence) applied to certain matrices defined directly in terms of the knot diagram, and showed that the S-equivalence class was invariant under Reidemeister moves, and hence well-determined by the knot type. A more general and direct proof, showing that surfaces embedded in a 3-manifold can have handles added to make them equivalent under isotopy if they have the same boundary, has been given by Rice [13]. Recent development of the subject, especially in the higher dimensions, is largely the work of Levine ([6, 7, 8] and further references to be found in these). The key fact that S-equivalence is *the* appropriate relation to study is established in [6]. More precisely, Levine showed (i) that all matrices associated with a given embedding are S-equivalent, and (ii) that S-equivalence is the strongest equivalence relation for which (i) holds. For $n>2$, he showed that simple embeddings (those with $\pi_i(S^{2n+1}-S^{2n-1})\approx\pi_i(S^1)$ for $i<n$) are precisely classified by S-equivalence of their associated matrices.

The Seifert form corresponding to the S-equivalence class of matrices associated with an embedding has a topological interpretation which should be mentioned, although it plays no explicit role in the results or proofs of this paper. Let (X, B) be the manifold with boundary which results from deleting a tubular neighborhood of S^{2n-1} from S^{2n+1}, and let $(\tilde{X}, \tilde{B})$ be its infinite cyclic covering space. Then Z acts as a group of covering transformations, and the homology groups of the pair $(\tilde{X}, \tilde{B})$ are modules over the group ring $\Lambda_0=Z(Z)=Z[t, t^{-1}]$. The module A_V of a Seifert form can of course be viewed as a Λ_0-module. It is then isomorphic to $H_n(\tilde{X})\approx H_n(\tilde{X}, \tilde{B})$ for any simple embedding [20]. (For the case $n=1$ this result goes back to Seifert's original paper [14].) Kearton

[20] has recently shown that the Blanchfield pairing [21] (which is defined using intersection numbers) leads to a $(-\varepsilon)$-hermitian form which essentially coincides with what we define as the Seifert form. Using a topological argument, he goes on to show that for $n \geqq 3$, the module structure of $H_n(\tilde{X})$ and the Blanchfield pairing precisely classify the simple embeddings. Combined with the work of Levine already cited, this yields an independent proof that S-equivalence of matrices is equivalent to isometry of the associated forms. Other references in which the relation of Seifert matrices to the homology of the infinite cyclic covering is discussed are [3, 7, 9], and [16].

We conclude the introduction with an outline of the contents of the paper. Parenthesized numbers such as (2.3) refer to definitions or theorems in the text.

Section 1 gives the basic definitions and notations, and contains the proof of the easy half of the main theorem (that S-equivalent matrices have isometric Seifert forms), as well as the fact that it is enough to consider non-singular matrices.

In Section 2 we observe that the module A_V underlying a Seifert form has no Z-torsion, and can therefore be viewed as a Λ-submodule of $QA_V = Q \otimes_Z A_V$. The latter is a module over $Q\Lambda = Q[t, t^{-1}, (1-t)^{-1}]$ and carries a $(-\varepsilon)$-hermitian form whose restriction to A_V is the original Seifert form. Define the following (2.2) for any non-singular Seifert matrix V:

$$S_V = (V + \varepsilon V')^{-1}$$

$$\Gamma_V = V S_V$$

$$T_V = -\varepsilon V' V^{-1}.$$

Then QA_V is a vector space over Q with dimension equal to the rank of V, and (with respect to a certain selected basis) the Λ-structure is given by identifying the action of t and $(1-t)^{-1}$ with multiplication by T_V and Γ_V respectively (2.5).

By methods similar to Milnor's [10] we obtain from the Seifert form a Q-valued ε-symmetric bilinear form on QA_V for which t is an isometry (2.8, 2.9). This *rational scalar form* has matrix S_V with respect to the selected basis. Isometry of QA_V and QA_W for non-singular V and W is equivalent to congruence of V and W over Q (2.11, 2.12). (Most of what we have described so far is a reformulation of known results to be found in [6] or [16].)

Just as with integral quadratic forms [12], integral congruence classes of Seifert matrices within a rational congruence class correspond to isometry classes of certain integral lattices in the vector space QA_V. These *admissible lattices* are characterized (2.13, 2.14) as those which are closed under multiplication by $(1-t)^{-1}$ and unimodular with respect to the scalar form. Such a lattice, corresponding to a matrix W, generates (over Λ) a Λ-module isometric to A_W. Two matrices have isometric Seifert forms if and only if there exist corresponding lattices which generate the same Λ-submodules (2.11).

Elementary calculations (2.15, 2.17) show that matrices which are S-equivalent via a single enlargement-reduction step correspond to lattices K, L such that $(K+L)/(K\cap L)$ is the direct sum of two cyclic groups and $(1-t)^{-1}K\subseteq L$ (or vice versa). The proof of the main theorem then reduces to showing that any two admissible lattices generating the same Λ-submodule can be joined by a chain of lattices in which each two in succession are related as just described.

In Section 3 we consider the p-adic completions, in which the integral lattices become modules over the p-adic integers Z_p embedded in a vector space over Q_p. It turns out (3.4) that in this context any admissible lattice L has a canonical direct sum decomposition $L_0+L_+ +L_-$ such that $\Lambda L=L_0+Q_pL_+ +Q_pL_-$, and that $\Lambda L=\Lambda K$ if and only if $L_0=K_0$. This analysis allows us to obtain the main theorem in the p-adic situation, and standard arguments suffice to complete the proof.

Section 4 contains a miscellany of results on the relation between S-equivalence and congruence, which come out as by-products of the main theorem. Among them are a proof that matrices of prime determinant are S-equivalent only if they are integrally congruent (4.7), and a sufficient condition (conjectured to be necessary) for an S-equivalence class to contain infinitely many congruence classes (4.13).

Section 5 presents some explicit examples illustrating various possibilities, including a matrix which is not S-equivalent to its transpose (5.2) and therefore comes from a non-invertible knot.

1. The Form Determined by a Seifert Matrix

We begin with some definitions and elementary generalities.

All rings will be assumed commutative. For a ring R, R^n denotes the free R-module of n-dimensional column vectors ($n\times 1$ matrices) over R. A square matrix is *unimodular* over R if it has entries in R and its determinant is a unit (invertible element) in R. A matrix over R is unimodular if and only if it has an inverse over R. If M is an $n\times n$ matrix then MR^n denotes the image of R^n under multiplication by M, i.e., the submodule of R^n generated by the columns of M. If R_0 is a subring of R, then R^n is considered as an R_0 module containing R_0^n as a submodule.

A *conjugation* on a ring R is an automorphism $r\mapsto\bar{r}$ whose square is the identity. A *symmetric module* C over a ring R with a conjugation is a module with an additive automorphism $c\mapsto\bar{c}$ such that $(rc)^-=\bar{r}\bar{c}$ for all $r\in R$, $c\in C$. A *hermitian (skew-hermitian) form* over R with coefficients in a symmetric module C consists of an R-module A and a bi-additive map $(a_1, a_2) \mapsto a_1 \cdot a_2$ from $A \times A$ to C such that

$$r a_1 \cdot a_2 = r(a_1 \cdot a_2)$$

and

$$a_2 \cdot a_1 = (a_1 \cdot a_2)^- \qquad \text{(hermitian)}$$

or

$$a_2 \cdot a_1 = -(a_1 \cdot a_2)^- \qquad \text{(skew-hermitian)}.$$

Two forms are *isometric* if there is an isomorphism between the underlying modules which preserves the dot-product. A square matrix M over a ring with conjugation is hermitian if $M' = \overline{M}$, where M' is the transpose of M. If M is hermitian then setting $a_1 \cdot a_2 = \bar{a}_2' M a_1$ for a_1, a_2 in R^n defines a hermitian form with coefficients in R. Similarly a matrix M such that $M' = -\overline{M}$ is called skew-hermitian and defines a skew-hermitian form.

Suppose R is an integral domain with a conjugation, with quotient field F, and M is an $n \times n$ non-singular hermitian (or skew-hermitian) matrix over R. The *quotient form determined by M* is a hermitian (skew-hermitian) form over R with values in the symmetric module F/R. Its associated module is by definition the quotient module R^n/MR^n, and for a_1, a_2 in R^n/MR^n, the product $a_1 \cdot a_2$ is defined as $\bar{b}_2' M^{-1} b_1$ (computed in F and reduced modulo R) where b_1 and b_2 are representatives in R^n of a_1 and a_2. The product is well-defined because if, for example, $a_1 = 0$ then b_1 is in MR^n, so $b_1 = M b_0$ for b_0 in R^n and $\bar{b}_2' M^{-1} b_1 = \bar{b}_2' b_0$ is in R. The same is true if a_2 is 0, in virtue of the assumed hermitian symmetry (skew-symmetry) of M.

Lemma 1.1. *If M_1 is hermitian (skew-hermitian) and P is unimodular then M_1 and $M_2 = P M_1 \bar{P}'$ determine isometric quotient forms.*

Proof. Verify that since P is unimodular (and hence so is $\bar{P}'$), multiplication by P gives an automorphism of R^n carrying $M_1 R^n$ onto $M_2 R^n$, and induces the required isometry of $R^n/M_1 R^n$ and $R^n/M_2 R^n$.

Lemma 1.2. *If U and M_1 are both hermitian (skew-hermitian) and U is unimodular then M_1 and*

$$M_2 = \begin{bmatrix} U & 0 \\ 0 & M_1 \end{bmatrix}$$

determine isometric quotient forms.

Proof. Suppose U is $k \times k$ and M_1 is $m \times m$. Because U is unimodular, $UR^k = R^k$, so the inclusion $R^m \to R^{k+m}$ induces an isomorphism of $R^m/M_1 R^m$ with $R^{k+m}/M_2 R^{k+m}$ (which is obviously an isometry).

Lemma 1.3. *Let A be the module R^n/MR^n, with M any $n\times n$ matrix. Then* $(\det M)\,a=0$ *for all a in A.*

Proof. For any b in R^n, Cramer's rule gives b_0 in R^n such that $(\det M)\,b=M\,b_0$ and so is in MR^n.

The following notations will be used for certain subrings of the field $F=Q(t)$, the field of rational functions in one variable over the rationals. F and these subrings are considered as rings with the conjugation characterized by $\bar{t}=t^{-1}$.

$$\Lambda_0=Z[t,t^{-1}]$$

is the subring generated by t and t^{-1}, and may be identified with the group ring of the infinite cyclic group generated by t,

$$\Lambda=\Lambda_0[(1-t)^{-1}]=Z[t,t^{-1},(1-t)^{-1}]$$

is the subring generated by t, t^{-1} and $(1-t)^{-1}$,

$$Q\Lambda_0=Q\otimes\Lambda_0=Q[t,t^{-1}],$$
$$Q\Lambda=Q\otimes\Lambda=Q[t,t^{-1},(1-t)^{-1}].$$

All these rings are integral domains having F as field of quotients. We introduce the notation

$$z=(1-t)^{-1}$$

and note the identities

$$\bar{z}=-tz=1-z$$

which show that Λ is closed under conjugation and is generated as a ring by z, z^{-1} and $\bar{z}^{-1}$.

We are now ready to introduce the forms defined by Seifert matrices. We assume that ε has been fixed as either $+1$ or -1 and that V is a $2h\times 2h$ matrix of integers such that $V+\varepsilon V'$ is unimodular over Z. (That the dimension of V must be even can be derived from the fact that $V+\varepsilon V'$, when viewed as a matrix over the field $Z/2Z$, is symmetric, non-singular, and zero on the diagonal.)

The *Seifert form determined by V* is a form over Λ (hermitian if $\varepsilon=-1$, skew-hermitian if $\varepsilon=+1$) with values in F/Λ, and is by definition the quotient form determined by the matrix

$$M_V=\bar{z}\,V-\varepsilon z\,V'=(t-1)^{-1}(t\,V+\varepsilon V')$$

which obviously satisfies the condition $M'_V=-\varepsilon\overline{M}_V$. We denote the module on which the form is defined by

$$A_V=\Lambda^{2h}/M_V\,\Lambda^{2h}$$

and refer to the form itself as $(A_V,\cdot)$.

Remark. The topological interpretation mentioned in the introduction suggests that one should work over Λ_0 and consider the Λ_0-module $B_V = \Lambda_0^{2h}/(tV + \varepsilon V')\Lambda_0^{2h}$ instead of A_V. As we shall see, using Λ instead of Λ_0 makes no real difference. It does, however, reflect a significantly different viewpoint. The definition of admissible lattices (2.13) and many of the subsequent propositions are more natural with Λ as coefficient ring, and the decomposition Theorem (3.4) depends on the factorization of t as $-\bar{z}z^{-1}$. The choice of rings makes no real difference because *multiplication by* $1-t$ *gives an automorphism of* B_V so that multiplication by $(1-t)^{-1}$ can be defined on it. In this way B_V becomes a Λ-module, which is easily seen to be isomorphic to A_V. To prove the italicized statement, let $D(t) = \det(tV + \varepsilon V')$ and note that $D(1) = \det(V + \varepsilon V') = \pm 1$. Now $1-t$ divides $D(t) - D(1)$; let $\varphi(t)$ be the quotient. Then for any $b \in B_V$, $\varphi(t)(1-t)b = D(t)b - D(1)b = -D(1)b = \pm b$ by Lemma 1.3, so an inverse to multiplication by $1-t$ is given by multiplication by either $\varphi(t)$ or $-\varphi(t)$, depending on the sign of $D(1)$.

Theorem. *The forms* $(A_V, \cdot)$ *and* $(A_W, \cdot)$ *determined by Seifert matrices* V *and* W *are isometric if and only if* V *and* W *are S-equivalent.*

The proof of the "if" part is almost immediate. If W is integrally congruent to V, so $W = PVP'$ with P unimodular over Z, then $M_W = PM_V P'$. Considered as a matrix over Λ, $P = \bar{P}$ and the isometry of $(A_V, \cdot)$ and $(A_W, \cdot)$ follows from Lemma 1.1. If W is a row enlargement of V, as given in Eq. (0.1) then

$$M_W = \begin{bmatrix} 0 & -\varepsilon z & 0 \\ \bar{z} & x\bar{z} - \varepsilon xz & -\varepsilon zv' + \bar{z}u' \\ 0 & \bar{z}v - \varepsilon zu & M_V \end{bmatrix}.$$

By Lemma 1.1 we may replace M_W by $PM_W\bar{P}'$ where

$$P = \begin{bmatrix} 1 & 0 & 0 \\ -x & 1 & 0 \\ \varepsilon\bar{z}z^{-1}v - u & 0 & 1 \end{bmatrix}.$$

Lemma 1.2 applies to the resulting matrix and gives the desired conclusion. The same argument obviously applies to column enlargements.

The proof of the converse will occupy the next two sections. We begin by taking care of a trivial case.

Lemma 1.4. $A_V = 0$ *if and only if every matrix S-equivalent to* V *is singular.*

Proof. Every enlarged matrix is obviously singular. Conversely, it is easy to show (see [16], p. 485 for details) that a singular Seifert matrix is integrally congruent to one of the form of W in (1.1). Successive reductions eventually yield either a non-singular matrix or one of the form $W=\begin{bmatrix}0 & 0\\ 1 & x\end{bmatrix}$ for which A_W is easily found to be 0. This proves the "if" part of the statement. The converse, which amounts to saying that if V is non-singular then $A_V \neq 0$ is a consequence of Proposition 2.5 in the next section.

2. The Seifert Form with Rational Coefficients

Given a Seifert form $(A, \cdot)$ we can construct a form $(QA, \cdot)$ over the ring QA with values in F/QA in an obvious way. We take the underlying module QA to be $Q \otimes A$ and define $(q_1 \otimes a_1) \cdot (q_2 \otimes a_2)$ to be $q_1 q_2 \psi(a_1 \cdot a_2)$ where $\psi: F/A \to F/QA$ is the quotient map. We call $(QA, \cdot)$ the *rational* Seifert form derived from $(A, \cdot)$. If the given form is $(A_V, \cdot)$ determined by a matrix V then (by right exactness of the tensor product functor), QA_V can be identified with $QA^{2h}/M_V QA^{2h}$ and it is easy to see that $(QA_V, \cdot)$ is in fact the reduced form over QA determined by M_V. Furthermore, the natural map $A_V \to QA_V$ which takes a into $1 \otimes a$ is induced by the natural inclusion $A^{2h} \to QA^{2h}$.

The next lemma shows that the rational form provides a framework for studying the integral form.

Lemma 2.1. *The map $A_V \to QA_V$ taking a into $1 \otimes a$ is a monomorphism.*

Proof. [1] We need to show that A_V is torsion-free as an abelian group, i.e., that if $ma = M_V b$ with $m \in Z$, a, $b \in A^{2h}$, then $a = M_V b_0$ for some $b_0 \in A^{2h}$. Let $\tilde{M}$ be the transposed matrix of cofactors of M_V. Then (Cramer's rule) $(\det M_V) b = \tilde{M} M_V b = m \tilde{M} a$, so m divides $(\det M_V) b = (1-t)^{-2h} \det(tV + \varepsilon V') b$. A is a unique factorization domain because A_0 is [2], so every $\lambda \in A$ has a unique representation as $(1-t)^n \lambda_0$ for some n (possibly zero or negative) and $\lambda_0 \in A_0$ and prime to $1-t$. Now m is obviously prime to $(1-t)^{-1}$ and is also prime to $\det(tV+\varepsilon V')$ because the latter takes the value ±1 when $t=1$. Hence m divides b, and $m^{-1} b$ is the required b_0.

For a *non-singular* Seifert matrix V we define the following rational matrices:

$$S_V = (V + \varepsilon V')^{-1}$$

$$T_V = -\varepsilon V' V^{-1} \tag{2.2}$$

$$\Gamma_V = V S_V.$$

Since V is a Seifert matrix, S_V is integral (and unimodular) and hence Γ_V is integral. The identity

$$\Gamma_V = (1 - T_V)^{-1} \tag{2.3}$$

follows from the observation that

$$(1-T_V)\Gamma_V=(1+\varepsilon V' V^{-1})VS_V=(V+\varepsilon V')S_V=1.$$

If V has rank $2h$ we define a $Q\Lambda$-structure on the vector space $Q\Lambda^{2h}$ by setting

$$f(t,t^{-1},z)v=f(T_V,T_V^{-1},\Gamma_V)v \tag{2.4}$$

where $f\in Q\Lambda$ is a polynomial in t,t^{-1} and z. (Consistency with the relation $z=(1-t)^{-1}$ follows from (2.3).)

The following proposition is essentially a rephrasing of results to be found in [6, 9, 16].

Proposition 2.5. *If V is a non-singular Seifert matrix of rank $2h$ then QA_V is a vector space of dimension $2h$ over Q. If it is identified with Q^{2h} by a suitable choice of basis, then*

(a) *the $Q\Lambda$-module structure is given by* (2.4) *so* $ta=T_V a$, $za=\Gamma_V a$.

(b) $a_1\cdot a_2=a_2' M_V^{-1} a_1 (\operatorname{mod} Q\Lambda)$.

(c) *A_V may be identified with the Λ-submodule generated over Λ by the chosen basis.*

Proof. Consider Q^{2h} as a $Q\Lambda$-module via (2.4). The standard basis of "unit vectors" freely generates $Q\Lambda^{2h}$ over $Q\Lambda$. Hence there is a unique $Q\Lambda$-homomorphism $\varphi\colon Q\Lambda^{2h}\to Q^{2h}$ taking the standard basis of $Q\Lambda^{2h}$ to the standard basis of Q^{2h}. The map φ is onto and trivial calculation shows that it carries anything in the submodule $M_V Q\Lambda^{2h}$ into zero. An inductive proof on the degree of $u\in Q\Lambda^{2h}$ (definable for these purposes as the maximum exponent of t, t^{-1} or z appearing in any component of u) can be used to show that $\varphi(u)=0$ implies $u\in M_V Q\Lambda^{2h}$. Hence $\ker(\varphi)=M_V Q\Lambda^{2h}$ and φ gives an isomorphism between QA_V and Q^{2h}. The "suitable basis" in QA_V is simply the image in QA_V of the standard basis in $Q\Lambda^{2h}$ and of course is mapped by φ onto the standard basis of Q^{2h}. The assertion (a) is immediate and (b) and (c) follow from the original definitions of the Seifert form. (In (c) we are identifying A_V with a Λ-submodule of QA_V as in Lemma 2.1.)

Milnor [10] has exhibited a close connection between certain hermitian forms and isometries of inner product spaces. To exploit this connection we introduce the function χ described in the next lemma, which plays the role taken by the trace homomorphism in [10]. The definition of χ is somewhat *ad hoc*, and was motivated by the desire to obtain the result of Proposition 2.10 below in the simple form given there.

By the elementary theory of partial fractions, any rational function has a unique decomposition as a sum of a polynomial and proper fractions (i.e., rational functions with numerator of lower degree than the denominator) with denominators which are powers of distinct irreducible polynomials. It follows readily that F splits over Q (not over QA) into the direct sum of QA (polynomials and proper fractions with denominators powers of t and $1-t$) and the subspace P, which we define to consist of 0 and all proper fractions with denominator prime to t and $1-t$. Then χ is defined as the Q-linear map such that

$$(2.6)\qquad \begin{aligned} \chi(f) &= f'(1), \quad && f \in P \\ &= 0, && f \in QA. \end{aligned}$$

(When f is in P, its denominator is prime to $1-t$, so its derivative f' can be evaluated at 1.) Since χ vanishes on QA we may and do consider it also as defined on F/QA.

Lemma 2.7. *If $f \in F$ has denominator prime to t and $1-t$ and numerator of degree less than or equal to the degree of its denominator, then $\chi(f) = f'(1)$.*

Proof. Let f satisfy the hypotheses with denominator of degree n with leading coefficient $q \neq 0$. Let p (which may be 0) be the coefficient of t^n in the numerator. Then $f = pq^{-1} + (f - pq^{-1})$ with $pq^{-1} \in QA$, $(f - pq^{-1}) \in P$, so $\chi(f) = (f - pq^{-1})'$ evaluated at 1, which is $f'(1)$.

Corollary 2.7a. $\chi(\bar{f}) = -\chi(f)$.

Proof. We may assume $f \in P$. Then $\bar{f}$ is in general not in P, but does satisfy the hypotheses of the lemma, and $\bar{f}(t) = f(t^{-1})$ has derivative $-t^{-2} f'(t^{-1})$. Evaluating at $t=1$ gives the result.

Corollary 2.7b. *For $f \in P$, $\chi((t-1)f) = f(1)$.*

Proof. The function $g(t) = (t-1) f(t)$ satisfies the hypotheses of the lemma, and $g'(1) = f(1)$.

Given a rational Seifert form we define the *scalar product* $[a_1, a_2] \in Q$ for $a_1, a_2 \in QA$ by

$$(2.8)\qquad [a_1, a_2] = \chi(a_1 \cdot a_2)$$

and speak of the *rational scalar form* $(QA, [\ \ ])$ or the *scalar form* $(A, [\ \ ])$ obtained by restriction to A viewed as a submodule of QA.

A module isomorphism that preserves dot-products obviously preserves scalar products. The converse is also true. It is not hard to show that if $\chi(\lambda a) = 0$ for all $\lambda \in A$ then $a \in QA$, so the value of $a_1 \cdot a_2$ in F/QA is determined by knowledge of $[\lambda a_1, a_2] = \chi(\lambda(a_1 \cdot a_2))$ for all λ. The observation that given a choice of basis, the module structure and scalar product determine the matrices Γ and S (see remarks preceding Proposition 2.11) and hence V and M_V, gives an alternative proof by direct computation. At any rate, isometry of Seifert forms implies isometry of scalar forms, and we shall be working with the latter for the rest of the proof.

The scalar product is obviously bilinear over Q, but is not Λ-linear. We have instead

Lemma 2.9. *The scalar product satisfies the identities*

(a) $[a_2, a_1] = \varepsilon [a_1, a_2]$.
(b) $[t a_1, t a_2] = [a_1, a_2]$.
(c) $[z a_1, a_2] = [a_1, \bar{z} a_2] = [a_1, (1-z) a_2]$.

Proof. Immediate from (2.7a) and the identities

$$a_2 \cdot a_1 = -\varepsilon (a_1 \cdot a_2)^{-},$$
$$t a_1 \cdot t a_2 = t\bar{t}(a_1 \cdot a_2) = a_1 \cdot a_2 \quad \text{and} \quad z a_1 \cdot a_2 = a_1 \cdot \bar{z} a_2.$$

Proposition 2.10. *With the hypotheses and notations of Proposition* 2.5, *and the same choice of basis,*

$$[a_1, a_2] = a_2' S a_1$$

for $a_1, a_2 \in QA$.

Proof. We have $[a_1, a_2] = \chi(a_1 \cdot a_2) = \chi(a_2' M_V^{-1} a_1)$ by (2.5b). Since the scalar product is bilinear over Q we need only show that $\chi(M_V^{-1}) = S$. Now $M_V^{-1} = (1-t)(tV + \varepsilon V')^{-1}$. Since V is non-singular, $D(t) = \det(tV + \varepsilon V')$ is a polynomial of degree $2h$ with non-zero constant term; since $D(1) = \pm 1$, $D(t)$ is prime to $1-t$. The entries of $(tV + \varepsilon V')^{-1}$ are rational functions with denominator $D(t)$ and degree at most $2h-1$. By (2.7b), $\chi(M_V^{-1})$ is given by evaluating $(tV + \varepsilon V')^{-1}$ at $t=1$, which gives S.

Given a rational scalar form $(QA, [\quad])$ and any basis $B = \{b_1, \ldots, b_{2h}\}$ for QA we can define matrices S_B, Γ_B by $s_{ij} = [b_j, b_i]$, $z b_j = \sum_i \gamma_{ij} b_i$ and then define $V_B = \Gamma_B S_B^{-1}$. Lemma 2.9 implies $S_B' = \varepsilon S_B$ and $S_B \Gamma_B = (1-\Gamma_B)' S_B$, from which it follows that $V_B' = \varepsilon S_B^{-1} \Gamma_B'$ and $S_B(V_B + \varepsilon V_B') = S_B \Gamma_B S_B^{-1} + \Gamma_B' = 1$. Hence S_B and Γ_B can be expressed in terms of V_B by formulas just like (2.2). If we also define T_B by $t b_j = \sum_i \tau_{ij} b_i$, then since $t = 1 - z^{-1}$, $T_B = 1 - \Gamma_B^{-1} = -\varepsilon V_B' V_B^{-1}$. These remarks, together with Propositions 2.5 and 2.10 give us

Proposition 2.11. *The rational scalar form $(QA_V, [\quad])$ determined by a non-singular Seifert matrix V is isometric to a given rational form $(QA, [\quad])$ if and only if there exists a basis B for QA with $V_B = V$. The scalar form $(A_V, [\quad])$ is isometric to $(A, [\quad])$ if and only if there exists a basis B for QA which generates A as a Λ-module and for which $V_B = V$.*

Given a basis B and a non-singular matrix P, the elements $\sum_i p_{ij} b_i$ form a new basis which we denote by BP. Elementary calculation gives

$$\Gamma_B = P\Gamma_{BP}P^{-1}, \qquad T_B = PT_{BP}P^{-1}$$

$$S_B = (P^{-1})' S_{BP} P^{-1}$$

$$V_B = PV_{BP}P'.$$

As an immediate corollary of the above and Proposition 2.11 we have

Proposition 2.12. *Two non-singular Seifert matrices determine isometric rational forms if and only if they are congruent over the rationals.*

(This result, for $\varepsilon = -1$, is more or less implicit in [16]. A satisfactory solution to the problem of classifying these rational forms is known. See [10] and references given there to earlier work.)

The matrix V_B is of course not a Seifert matrix for an arbitrary basis B. By the remarks following (2.2) it is necessary that S_B be integral unimodular and that Γ_B be integral. These conditions are also sufficient since they imply that $V_B = \Gamma_B S_B^{-1}$ is integral and $V_B + \varepsilon V_B = S_B^{-1}$ is unimodular. We can express these conditions in a coordinate-free way in terms of the free abelian group L_B generated by a basis B, which is a *lattice on* QA, in the terminology of [12]. Let us define a lattice L on $(QA, [\ \ ])$ to be *admissible* if

(2.13) (a) $zL \subseteq L$

(b) L is self-dual with respect to the scalar product $[\ \ ]$

where the self-duality condition means that for $a \in QA$, a is in L if and only if $[a, x] \in Z$ for all $x \in L$.

Lemma 2.14. *The matrix V_B associated with a basis B for the rational vector space QA is a Seifert matrix if and only if the lattice L_B spanned by B is admissible.*

Proof. Condition (2.13a) is obviously equivalent to the integrality of Γ_B. Equivalence of (2.13b) with unimodularity of S_B is also elementary; see [12], Section 82.

Since any two bases which generate the same admissible lattice are related by a unimodular matrix P, it follows as above that the associated Seifert matrices are integrally congruent and hence S-equivalent. The next lemma gives a condition on lattices under which the associated matrices are S-equivalent via an enlargement-reduction step, and is central to our proof of the main theorem. Extending the terminology of [12], p. 326, we say that two lattices K, L are *adjacent* (for some integer k) if all but two of the invariant factors of K in L are equal to 1 and the remaining two are k^{-1} and k, i.e. if K has an integral basis

$$\{b_1, b_2, b_3, \ldots, b_{2h}\}$$

such that $\{k^{-1}b_1, kb_2, b_3, \dots, b_{2h}\}$ is an integral basis for L. For K and L to be adjacent it is obviously necessary and sufficient that $K/(K\cap L)$ and $L/(K\cap L)$ both be isomorphic to Z/kZ for some k.

Lemma 2.15. *Let K and L be adjacent admissible lattices on the underlying space QA of the rational form $(QA, [\ \ ])$, and suppose $zK\subseteq L$. Then there are integral bases B for K and C for L such that a column enlargement of V_B is integrally congruent to a row enlargement of V_C, so V_B and V_C are S-equivalent.*

Proof. Let $B=\{b_1, \dots, b_{2h}\}$ and $C=\{c_1, \dots, c_{2h}\}$ be bases for K and L such that $c_1=k^{-1}b_1$, $c_2=kb_2$, $c_i=b_i$ for $i>2$. Such bases exist because K and L are adjacent. Since $b_i\in L$ for $i\neq 2$ we have $k^{-1}[b_1, b_i]=[c_1, b_i]\in Z$ for $i\neq 2$, so k divides every entry in the first row and column of S_B except for s_{12} and s_{21}. Since S_B is unimodular, s_{12} must be relatively prime to k. Let $U=S_B^{-1}$. Computation of the matrix of cofactors of S_B shows that the second row and column of U are divisible by k except for u_{12} and u_{21} which must be relatively prime to k. The condition $zK\subseteq L$, which implies $zK\subseteq K\cap L$ because K is admissible, implies that zb_i is an integral combination of $b_1, c_2, b_3, \dots, b_{2h}$. Hence the second row of Γ_B is divisible by k, and therefore so is the second row of $V_B=\Gamma_B U$. Because of the self-duality of L, $zK\subseteq L$ if and only if $[za, b]\in Z$ for all $a\in K$, $b\in L$. Since $[za, b]=[a, \bar{z}b]$ and K is self-dual the last condition is equivalent to $\bar{z}L\subseteq K$, and hence $\bar{z}L\subseteq K\cap L$. Hence $\bar{z}c_1=k^{-1}(1-z)b_1$ is an integral combination of $b_1, c_2, b_3, \dots, b_{2h}$, so the first column of $(1-\Gamma_B)$ is divisible by k and the entry in the first column, second row is divisible by k^2. The element v_{22} in V_B is equal to $\sum\limits_i \gamma_{2i}u_{i2}$. For $i>1$, k divides both γ_{2i} and u_{i2}, while k^2 divides γ_{21}. Therefore k^2 divides v_{22}. The element $v_{12}=\sum\limits_i \gamma_{1i}u_{i2}$. For $i>1$, k divides u_{i2} while $\gamma_{11}\equiv 1 \pmod k$ and u_{12} is relatively prime to k. Therefore $(v_{12}, k)=1$. For $j>1$, $v_{j2}=\sum \gamma_{ji}u_{i2}$ and k divides γ_{ji} for $i=1$ and u_{i2} for $i>1$, so k divides v_{j2}. Putting these facts together with the earlier observation that k divides the second row of V_B we see that there exist integers w, x, y, a with a relatively prime to k, and integer vectors p, q, r, s with $2h-2$ entries, and a $(2h-2)\times(2h-2)$ matrix V_0 such that

$$V_B=\begin{bmatrix} x & a & q' \\ kw & k^2y & ks' \\ p & kr & V_0 \end{bmatrix}.$$

By (2.12),

$$V_C=\begin{bmatrix} k^2x & a & kq' \\ kw & y & s' \\ kp & r & V_0 \end{bmatrix}.$$

Now take a column enlargement of V_B

$$W=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & y & w & ky & s' \\ 0 & 0 & x & a & q' \\ 0 & ky & kw & k^2y & ks' \\ 0 & r & p & kr & V_0 \end{bmatrix}.$$

Since a and k are relatively prime there exist integers g and h such that $ga-hk=1$. Let P be the matrix with

$$\begin{bmatrix} 0 & -k & 0 & 1 \\ h & 0 & g & 0 \\ a & 0 & k & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

in the upper left corner, the identity matrix of rank $2h-2$ in the lower right corner and zeros elsewhere. Then P is unimodular and

$$PWP'=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & g^2x & gkx & h & gq' \\ 0 & gkx & k^2x & a & kq' \\ 0 & gw & kw & y & s' \\ 0 & gp & kp & r & V_0 \end{bmatrix}$$

is a row enlargement of V_C.

The converse of Lemma 2.15 is also true, as we show below in 2.17. The converse is not needed in the proof of the main theorem, but clarifies the enlargement-reduction process, and is used to obtain several results in Section 4. The preliminary Lemma 2.16 is a special case of a result of Levine [8].

Lemma 2.16. *Let V be a non-singular Seifert matrix and W a row reduction of any matrix congruent to a row enlargement of V. Then W is congruent to V.*

Proof. Suppose QUQ' is a row enlargement of W, where U is a row enlargement of V and Q a unimodular matrix in the form

$$U=\begin{bmatrix} 0 & 0 & 0 \\ 1 & a & p' \\ 0 & q & V \end{bmatrix}, \quad Q=\begin{bmatrix} b & c & u' \\ d & e & v' \\ w & x & P \end{bmatrix}.$$

The first row of QUQ' must be zero, and multiplying by $(Q')^{-1}$ shows that the first row of QU is zero. In particular, $c=0$ and $cp'+u'V=0$, so the non-singularity of V implies $u=0$. The lower left entry in the partitioned form of QUQ' is then simply xb, and must be zero because QUQ' has the form of a row enlargement. Since Q is non-singular, $b \neq 0$, and so $x=0$. Then W, the lower right entry in the partitioned form of QUQ', is PVP'. Also $\det(Q)=(be)\det(P)$, so P must be unimodular, and W is congruent to V.

Lemma 2.16 can be restated as the assertion that a congruence class of singular matrices determines a unique congruence class of row reductions, provided the latter are non-singular. Of course it also determines a unique congruence class of column reductions. (Apply 2.16 to the transposed matrix.)

Proposition 2.17. *Let U and W be non-singular Seifert matrices such that a column enlargement of U is congruent to a row enlargement of W. Then there exist adjacent admissible lattices K and L on the space of a rational form $(QA, [\ \ ])$, such that $zK \subseteq L$, and K and L have respective bases B and C such that $U=V_B$ and $W=V_C$.*

Proof. The most general row enlargement of W has the form

$$Y_0=\begin{bmatrix} 0 & 0 & 0 \\ 1 & a & p' \\ 0 & q & W \end{bmatrix}$$

and an obvious congruence makes a and p zero. Since W is non-singular, there exists a unimodular P such that the first column of WP' is proportional to q, and the same is true for PWP' and Pq. By performing elementary column operations on PWP', not involving the first column, we can obtain $PWP'Q'$ with all elements of the first row zero except the first two, where Q' is the unimodular matrix expressing the elementary operations. Premultiplication by Q does not affect the zeros in the first row, and $QPWP'Q'$ has its first column proportional to QPq. Then

$$Y_1=\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & QPq & QPWQ'P' \end{bmatrix}$$

is congruent to Y_0 and has the partitioned form

$$Y_1=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & gb & kb & e & 0 \\ 0 & gc & kc & y & s' \\ 0 & gf & kf & r & W_0 \end{bmatrix}.$$

We may assume that the proportionality factors g and k are relatively prime, by letting b, c, f absorb any common factor. The greatest common divisor of k and e is easily seen to divide $\det(Y_1+\varepsilon Y_1)$ and must be 1. Therefore there exist integers m and x such that $me+b=kx$. Now add km times the fourth column of Y_1 to the third column and gm times the fourth column to the second, and also perform the corresponding row operations. Further operations adding multiples of the first row and column to others allow arbitrary modification in the second row (except in the first column) and we thus obtain a matrix congruent to Y_1 in the form

$$Y_2=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & g^2x & kgx & 0 & gq' \\ 0 & gkx & k^2x & a & kq' \\ 0 & gw & kw & y & s' \\ 0 & gp & kp & r & X \end{bmatrix}$$

where $w=c+my$, $p=f+mr$, $q'=ms'$, and $a=e+ky$ is relatively prime to k. Since g and a are relatively prime to k, so is ga, and there exist integers u and v such that $gau+kv=1$. Let R be the matrix which agrees with the identity except for having

$$\begin{bmatrix} 0 & k & -g & 0 \\ v & 0 & 0 & -u \\ 0 & au & v & 0 \\ ga & 0 & 0 & k \end{bmatrix}$$

for its upper left corner. Then

$$Y_3=RY_2R'=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & u^2y & -uw & -uky & -us' \\ 0 & 0 & x & a & q' \\ 0 & -uky & kw & k^2y & ks' \\ 0 & -ur & p & kr & X \end{bmatrix}$$

is congruent to Y_0.

Now W is a non-singular row reduction of a matrix congruent to Y_2, so by 2.16 it is congruent to

$$W_0=\begin{bmatrix} k^2x & a & kq' \\ kw & y & s' \\ kp & r & X \end{bmatrix},$$

while U is a non-singular column reduction of a matrix congruent to Y_3 and is therefore congruent to

$$U_0=\begin{bmatrix} x & a & q' \\ kw & k^2 y & ks' \\ p & kr & X \end{bmatrix}.$$

An easy reversal of the arguments in the proof of 2.15 gives the existence of lattices K and L with the required properties and bases B_0 and C_0 such that $U_0=V_{B_0}$ and $W_0=V_{C_0}$. Since U is congruent to U_0 and W to W_0, the same lattices have bases B and C with $U=V_B$ and $W=V_C$.

3. Localization

We can now reduce the proof of the main theorem to a question about lattices. By 2.11, two non-singular Seifert matrices that determine isometric forms will correspond to two admissible lattices K, L in the underlying space of the same rational scalar form which generate the same Λ-module, i.e. satisfy $\Lambda K=\Lambda L$. To show that the matrices are S-equivalent it is sufficient to find a chain of lattices $J_0=K, J_1, \ldots, J_r=L$ such that each pair J_{i-1}, J_i satisfies the hypotheses of 2.15. We shall prove the existence of such a chain by showing that if $K\neq L$ but $\Lambda K=\Lambda L$ then there exists a lattice $\bar{K}$ such that K, $\bar{K}$ satisfy the hypotheses of 2.15 and $\bar{K}$ is "closer" to L than K is. We measure the difference between K, L by the index of $K\cap L$ in $K+L$, which we denote by $d(K, L)$ and call the *discrepancy* between K and L. Obviously $d(K, L)=1$ if and only if $K=L$.

Throughout this section we assume that some fixed rational scalar form is given, and that all lattices are lattices on its underlying vector space.

Lemma 3.1. *For any admissible lattice K,*

$$\Lambda K=\bigcup_{m\geqq 0} z^{-m}\bar{z}^{-m}K.$$

Proof. Every element of Λ can be expressed as a polynomial in z times $(z\bar{z})^{-m}$ for some m, and $zK\subseteq K$.

We now turn to studying the problem over the p-adic rationals and integers (denoted as usual by Q_p and Z_p). With these coefficients, ΛK can be described very simply (Theorem 3.4 below) and we obtain a localized version of our theorem. Standard arguments are then used to show that the local result for all primes p implies the global result.

Obviously all the construction and discussion so far applies without change to the p-adic case. For the remainder of this section we suppose p to be a fixed rational prime; "integer" will mean "p-adic integer", "lattice" will mean lattice over Z_p, and so on. (Much of what follows generalizes immediately to any field complete under a discrete rank one valuation.)

We use $|\;|$ to denote the usual p-adic valuation. Recall that $|\alpha|\leqq 1$ if and only if α is an integer, $|\alpha|=1$ if and only if α is a unit of Z_p, and $|\alpha|<1$ if and only if α is divisible by p. A finite dimensional vector space V over Q_p has a unique compatible topology. If L is any lattice on V a non-archimedean norm giving the topology can be defined so that $|v|\leqq 1$ if and only if $v\in L$. To do so, choose a basis $\{x_i\}$ for L and define $|v|=\max_i |\alpha_i|$ where $v=\sum_i \alpha_i x_i$. For a linear operator A: $V\to V$ a norm $|A|$ can be defined as $\max_{ij} |\alpha_{ij}|$ where $[\alpha_{ij}]$ is the matrix of A with respect to $\{x_i\}$. Then $|Av|\leqq|A|\cdot|v|$ and $|A|\leqq 1$ if and only if $AL\subseteq L$. (For full discussion of this material see [12].)

The following lemma is simply the classical Hensel's lemma, stated in more explicit detail than is usual. The result is implicit in the usual proof. (See, for example, [12, p. 26].)

Lemma 3.2. *Let $\varphi(x)$ be a monic polynomial with p-adic integral coefficients, and suppose $\bar\varphi(x)=\bar\varphi_1(x)\,\bar\varphi_2(x)$ is a factorization of its reduction* mod p *into relatively prime factors over the field Z/pZ. Then there exist monic polynomials $\varphi_1, \varphi_2, \psi_1, \psi_2$ with p-adic integral coefficients such that $\varphi=\varphi_1\varphi_2$, $\varphi_1\psi_1+\varphi_2\psi_2=1$ and φ_1,φ_2 reduce to $\bar\varphi_1,\bar\varphi_2$*(mod p)*.*

Lemma 3.3. *Let X be an n-dimensional vector space over Q_p and U: $X\to X$ a linear map. If there exists a lattice L on X such that $UL\subseteq L$ then X is the direct sum of subspaces X', X'' invariant under U and such that*

(a) $\lim_{m\to\infty} U^m x=0$ *for all $x\in X''$;*

(b) *for any lattice L on X such that $UL\subseteq L$, L is the direct sum of $L'=L\cap X'$ and $L''=L\cap X''$;*

(c) *for L as in* (b), *$U|L'$ is an automorphism of L'.*

Proof. Let L be any lattice such that $UL\subseteq L$, and use it to define a norm as in the paragraph before 3.2. The matrix of U with respect to a basis of L has integral entries, so $\varphi(\lambda)=(-1)^n\det(U-\lambda)=\sum_{i=0}^{n} u_i\lambda^{n-i}$ is monic with integral coefficients. Let j be the greatest integer for which $|u_j|=1$. (We have $u_0=1$ so $j\geqq 0$.) Then reducing modulo p we have $\bar\varphi(\lambda)=\bar\varphi_1(\lambda)\,\bar\varphi_2(\lambda)$ where $\bar\varphi_1$ has degree j and non-zero constant term and $\bar\varphi_2(\lambda)=\lambda^{n-j}$. (The trivial cases $j=0$, $\bar\varphi_1=1$ and $j=n$, $\bar\varphi_2=1$ are possible.) Let $\varphi_1,\varphi_2,\psi_1,\psi_2$ be the polynomials whose existence is guaranteed by Lemma 3.1. Then φ_1 has degree j and its constant term is a unit, while φ_2 has degree $n-j$ and all its coefficients after the first are divisible by p. Define $P=\varphi_1(U)\,\psi_1(U)=1-\varphi_2(U)\,\psi_2(U)$. Since $\varphi_1(U)\,\varphi_2(U)=\varphi(U)=0$,

$P(1-P)=0$ and hence P is a projection commuting with U. Hence $X'=PX$ and $X''=(1-P)X$ give a direct sum splitting of X into invariant subspaces. (Note that X', X'' do not depend on L. The existence of L was used only to show that φ has integral coefficients.) The matrix of P with respect to a basis for L has integral entries; hence $PL \subseteq L \cap X' = L'$ and $(1-P)L \subseteq L \cap X'' = L''$. Since $PL+(1-P)L \supseteq L$ we have $L=L'+L''$. Hence there is no loss of generality in supposing the chosen basis for L to be the union of bases for L' and L''. Then $U|L'=U'$ and $U|L''=U''$ will have integral matrices. U' and U'' have φ_1 and φ_2 for their characteristic polynomials. The determinant of U' is (up to a sign) the constant term of φ_1 and therefore a unit. Hence U' is an automorphism of L'. The equation $\varphi_2(U'')=0$ gives $(U'')^{n-j} = -\sum_1^{n-j} v_i (U'')^{n-j-i}$ with all $|v_i|<1$. Hence $|(U'')^{n-j}|<1$ and $\lim_{m\to\infty}(U'')^m=0$.

Theorem 3.4. *Let V be the underlying space of a p-adic rational scalar form. Then V splits as a Λ-module into subspaces V_0, V_+, V_- such that*

(a) $\lim_{m\to\infty} z^m v=0$ *for* $v\in V_+$;

(b) $\lim_{m\to\infty} \bar{z}^m v=0$ *for* $v\in V_-$;

(c) *any admissible lattice L is the direct sum of $L_0=L\cap V_0$, $L_+=L\cap V_+$ and $L_-=L\cap V_-$;*

(d) *multiplication by z is an automorphism on L_0 and L_-;*

(e) *multiplication by $\bar{z}$ is an automorphism on L_0 and L_+;*

(f) $\Lambda L = L_0 + V_+ + V_-$.

Proof. Apply Lemma 3.3 twice with $X=V$ and U given by multiplication by z and $\bar{z}$, getting decompositions X_1', X_1'' and X_2', X_2'' respectively. Take $V_+=X_1''$, $V_-=X_2''$ and $V_0=X_1'\cap X_2'$. (It is easy to show that $V_+\cap V_-=0$, so V_0, V_+, V_- give a direct sum decomposition.) Then (a), (b), (c), (d), and (e) follow directly from the lemma. Part (f) follows from Lemma 3.1 since (a), (b), (d) and (e) imply that for any v in $V_+ + V_-$, $(z\bar{z})^m v$ will be in $L_+ + L_-$ for sufficiently large m, while $(z\bar{z})^{-m} L_0 = L_0$ for all m.

Corollary 3.4a. *If K and L are admissible p-adic lattices then $\Lambda K = \Lambda L$ if and only if $K_0 = L_0$.*

Lemma 3.5. *With the notation of* 3.4, *V_+ and V_- are isotropic and both are orthogonal to V_0.*

Proof. For any v, w we have $[v,w]=[\bar{z}^m v, z^{-m} w]$ for all m. For $v\in V_-$ and $w\in V_- + V_0$ we have $\bar{z}^m v \to 0$, while $z^{-m} w$ remains bounded as $m\to\infty$, so $[v,w]=0$. Hence V_- is isotropic and orthogonal to V_0. A similar argument applies to V_+.

Corollary 3.5a. *If L is an admissible lattice and $\{x_1, \ldots, x_k\}$ is a basis for L_+, then $\{\bar{x}_1, \ldots, \bar{x}_k\}$ is a basis for L_-, where $\bar{x}_i$ is the unique element of V_- such that $[x_j, \bar{x}_i] = \delta_{ij}$ for all j.*

Proof. Immediate from 3.5 and the unimodularity of L with respect to the scalar product.

Lemma 3.6. *Let K and L be admissible p-adic lattices. Then either $K_+ \subseteq L_+$ or there exists an admissible lattice K' adjacent to K such that $zK \subseteq K'$, $K_0 = K'_0$ and $d(K', L) < d(K, L)$.*

Proof. Let $\{x_1, \ldots, x_k\}$ be a basis for K_+ such that $\{p^{m_1} x_1, \ldots, p^{m_k} x_k\}$ is a basis for L_+ and $m_1 \geqq \cdots \geqq m_k$. Let r be the index such that $m_1 = \cdots = m_r > m_{r+1}$ and write m for the common value of $m_1, \ldots, m_r$. Let V_1, V_2 be the subspaces of V_+ spanned by $x_1, \ldots, x_r$ and $x_{r+1}, \ldots, x_k$ respectively. For $i = 1, 2$ write $K_i = K \cap V_i$, $L_i = L \cap V_i$, so $p^m K_1 = L_1$ and $p^{m-1} K_2 \subseteq L_2$. Let $B = pK_1 + K_2$ and note that K_+/B is a vector space over Z/pZ with a basis represented by $x_1, \ldots, x_r$. $B \subseteq p^{-m+1} L$ and since $zL \subseteq L$ we have $zB \subseteq p^{-m+1} L \subseteq pK_1 + V_2$. But $zB \subseteq zK_+ \subseteq K_+$, so $zB \subseteq (pK_1 + V_2) \cap (K_1 + K_2) = B$ and z induces $z_*: K_+/B \to K_+/B$. Since $z^n v \to 0$ for $v \in V_+$, z_* must be singular (in fact, nilpotent) and there exists a basis $\{\tilde{x}_1, \ldots, \tilde{x}_r\}$ for K_+/B such that $\operatorname{im}(z_*) \subseteq \operatorname{span}(\tilde{x}_2, \ldots, \tilde{x}_r)$. We can alter $x_1, \ldots, x_r$ by unimodular changes so that they represent $\tilde{x}_1, \ldots, \tilde{x}_r$ in K_+/B, and we suppose that this has been done.

Now define K'_+ as the lattice spanned by $px_1, x_2, \ldots, x_k$, that is, $K'_+ = B + \operatorname{span}(x_2, \ldots, x_k)$. By construction, $zK_+ \subseteq K'_+$ and *a fortiori*, $zK'_+ \subseteq K'_+$. Let $\{\bar{x}_1, \ldots, \bar{x}_k\}$ be the basis for L which is dual to $\{x_1, \ldots, x_k\}$ as in Corollary 3.5a, and define K'_- to have the basis $\{p^{-1} \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_k\}$, which is dual to the basis for K'_+. Then $zK'_- \subseteq K'_-$ by duality because $\bar{z} K'_+ \subseteq K'_+$, while $zK_- = K_- \subset K'_-$.

Finally take $K' = K_0 + K'_+ + K'_-$. We have shown that $zK \subseteq K'$ and $zK' \subseteq K'$. K' is obviously adjacent to K and the construction of K'_- makes K' unimodular. Comparing the bases for K and L (note that $\{p^{-m_1} \bar{x}_1, \ldots, p^{-m_k} \bar{x}_k\}$ is a basis for L_-) shows that if $m > 0$ then $d(K, L) = p^2 d(K', L) > d(K', L)$. But $m \leqq 0$ would imply $K_+ \subseteq L_+$, so the lemma is proved.

Proposition 3.7. *Let K and L be admissible p-adic lattices such that $\Lambda K = \Lambda L$. If $K \neq L$ then either there exists an admissible lattice K' adjacent to K with $\Lambda K' = \Lambda K$, $zK \subseteq K'$ and $d(K', L) < d(K, L)$ or there exists an admissible lattice L' adjacent to L with $\Lambda L' = \Lambda L$, $zL \subseteq L'$ and $d(K, L') < d(K, L)$.*

Proof. The condition $\Lambda K = \Lambda L$ is equivalent to $K_0 = L_0$. If $K_+ = L_+$ then by duality $K_- = L_-$ and $K = L$. Otherwise at least one of $K_+ \subseteq L_+$ or $L_+ \subseteq K_+$ is false, and Lemma 3.6 yields the result.

As indicated in the remarks at the beginning of this section, the proof of the main theorem will be complete if we can show that 3.7 holds for rational rather than p-adic lattices. The necessary arguments are well-known in the theory of quadratic forms. Given a rational scalar form with underlying vector space V, it extends to a p-adic form on $V_p = Q_p \otimes_Q V$. We consider V as imbedded in V_p, and for any lattice K on V define K_p as the Z_p-module it generates in V_p. K_p is of course a p-adic lattice on V_p. The following facts are obvious or easily obtained from propositions in [12, chap. 8]. Here K and L are any two lattices on V.

(3.8) (a) $(zK)_p = zK_p$ *for all* p.

(b) $K \subseteq L$ *if and only if* $K_p \subseteq L_p$ *for all* p.

(c) K *is unimodular if and only if* K_p *is unimodular for all* p.

(d) *If* $K \subseteq L$ *then* L_p/K_p *is isomorphic to the p-primary part of* L/K.

Lemma 3.9. *For any lattices* K, L *in the underlying space of a rational scalar form*

(a) $\Lambda K = \Lambda L$ *if and only if* $\Lambda K_p = \Lambda L_p$ *for all* p.

(b) K *is admissible if and only if* K_p *is admissible for all* p.

(c) K *is adjacent to* L *if and only if* K_p *is adjacent to* L_p *for all* p.

(d) $zK \subseteq L$ *if and only if* $zK_p \subseteq L_p$ *for all* p.

(e) $d(K, L) = \Pi d(K_p, L_p)$.

Proofs. (a) Lemma 3.1 and 3.8a.

(b) The Definition, 3.8a, 3.8b and 3.8c.

(c) The remark preceding Lemma 2.15 and 3.8d.

(d) 3.8a and 3.8b.

(e) 3.8d.

Now suppose we have rational lattices K, L with $\Lambda K = \Lambda L$ and $K \neq L$. By 3.9a and 3.8b there is some p for which K_p and L_p satisfy the hypotheses of Proposition 3.7. By interchanging K and L if necessary, we may assume there exists a K'_p satisfying the conclusions of 3.7. By Theorem 81:14 of [12], there exists a lattice K' such that $(K')_q = K_q$ for all $q \neq p$, while $(K')_p = K'_p$. By Lemma 3.9, this K' satisfies the conclusions of 3.7 and the proof of the main theorem is complete.

4. S-Equivalence and Congruence

In this section we develop a number of consequences of earlier propositions that shed some light on the relation between S-equivalence and integral congruence of matrices.

It will be convenient to introduce some more terminology and notational conventions which will tacitly apply throughout this section.

We assume a rational Seifert form given, with underlying vector space X. K and L (possibly with subscripts) will always denote admissible lattices on X, while M and N denote arbitrary lattices on X. U, V and W will denote *non-singular* Seifert matrices.

We write $[U]$ for the integral congruence class of U, and write $U \leftrightarrow K$ to indicate that $U = V_B$ (in the sense of Section 2) for some integral basis B of K.

A linear function σ: $X \to X$ is an *isometry* if $\sigma(zx) = z\sigma(x)$ and $[\sigma(x), \sigma(y)] = [x, y]$ for all x, y. If σ is an isometry and B a basis for K then $\sigma(B)$ is a basis for $\sigma(K)$, and obviously $V_{\sigma(B)} = V_B$. Conversely if B and C are bases of admissible lattices and $V_B = V_C$ then the unique linear function σ such that $\sigma(B) = C$ is an isometry. Thus the correspondence $U \leftrightarrow K$ induces a one-to-one correspondence between integral congruence classes of Seifert matrices (belonging to a given rational congruence class) and isometry classes of admissible lattices (on the space of a given form).

We call U a *row-neighbor* of W and W a *column-neighbor* of U, if for some $U_0 \in [U]$, U_0 is a column reduction of some matrix congruent to a row enlargement of W. A lattice K is a *row-neighbor* of L (and L a *column-neighbor* of K) if K and L are adjacent and $zK \subseteq L$. Note that since K and L are self-dual, they are adjacent if and only if $(K+L)/L$ is cyclic. Then Lemmas 2.15 and 2.17 amount to the statement that U is a row-neighbor of W if and only if $U \leftrightarrow K$ and $W \leftrightarrow L$ for some K and L such that K is a row-neighbor of L.

For any integer matrix P, let $C(P)$ denote the abelian group of integer column vectors modulo the subgroup generated by the columns of P. For a Seifert matrix U with $U \leftrightarrow K$, the quotient module K/zK is isomorphic to $C(\Gamma_U)$. Since $\Gamma_U = US_U$ and S_U is unimodular, $C(\Gamma_U) = C(U)$.

Levine [8] found a connection between the row-neighbors of a given U and the group $C(U)$. In fact he established a one-to-one correspondence between the congruence classes of row enlargements of U and the orbits of $C(U)$ under the action of a certain group. He could then conclude that the number of distinct congruence classes of row enlargements and *a fortiori* (in virtue of 2.16) the number of congruence classes of row-neighbors of U is bounded by $\text{order}(C(U)) = |\det(U)|$. The next lemmas lead to some refinements of this bound.

Lemma 4.1. *For each lattice M satisfying $zL \subseteq zM \subseteq L$, there is a unique admissible lattice K such that $M = K + L$ and $zK \subseteq L$, and conversely.*

Proof. The argument involves some calculations using dual lattices, so we begin by recalling the definition and some elementary facts. On any rational vector space with a symmetric or skew-symmetric non-singular inner product, the *dual* of a lattice M, denoted by $M^{\#}$, is defined as the set of all x such that $[x, y] \in Z$ whenever $y \in M$. (Note that a lattice on the space of a Seifert form is self-dual in the sense of 2.13 precisely if $L = L^{\#}$.) $M^{\#}$ is a lattice, and the following relations hold [12, p. 230].

(4.2) (a) $(M^{\#})^{\#} = M$,

(b) $M \subseteq N$ *if and only if* $N^{\#} \subseteq M^{\#}$,

(c) $(M \cap N)^{\#} = M^{\#} + N^{\#}$,

(d) $(M + N)^{\#} = M^{\#} \cap N^{\#}$.

For lattices on the space of a Seifert form we also have

(e) $zM \subseteq N$ *if and only if* $\bar{z} N^{\#} \subseteq M^{\#}$,

(f) $zM \subseteq M$ *if and only if* $zM^{\#} \subseteq M^{\#}$.

Here (e) is immediate from 2.9c and (f) follows because $zM = (1-\bar{z})M \subseteq M$ if and only if $\bar{z}M \subseteq M$.

We now claim that given M, the K satisfying the statement of the lemma is given by

$$\begin{aligned} K &= (M^{\#} + tL) \cap M \\ &= (M \cap tL) + M^{\#}. \end{aligned} \tag{4.3}$$

The equality of the two expressions follows from the modular law (that $(A+B) \cap C = (C \cap B) + A$ whenever $C \supseteq A$) and the fact that $M \supseteq L = L^{\#} \supseteq M^{\#}$. The two expressions are dual to each other by 4.2c and 4.2d, so $K = K^{\#}$. The hypothesis on M implies $L \subseteq M \subseteq z^{-1} L$, so $zM \subseteq L \subseteq M$ and hence $zM^{\#} \subseteq M^{\#}$. Since $z(tL) = t(zL) \subseteq tL$, each component of the right side of 4.3 is closed under z, so $zK \subseteq K$. Hence K is admissible. Obviously $K \subseteq M$ by construction and $L \subseteq M$ is given, so $K + L \subseteq M$. Now $M \subseteq z^{-1} L$ implies $\bar{z}M \subseteq tL$ and since $\bar{z}M = (1-z)M \subseteq M$ we have $\bar{z}M \subseteq K$. Then $M = zM + \bar{z}M \subseteq K + L$ so $M = K + L$. Since $zK \subseteq zM \subseteq L$, 4.3 defines a K with all the required properties.

Conversely, suppose K is given with $zK \subseteq L$, and $M = K + L$. The condition $zL \subseteq zM \subseteq L$ follows at once. To prove uniqueness we need to show that the right side of 4.3 does give K when $K + L$ is substituted for M. Note that $(K+L)^{\#} = K^{\#} \cap L^{\#} = K \cap L$, and let $K_0 = ((K \cap L) + tL) \cap (K + L)$. It is sufficient to show $K \subseteq K_0$ since then $K_0 = K_0^{\#} \subseteq K^{\#} = K$ and equality must hold. Since $zK \subseteq L$ we have $zK \subseteq K \cap L$ and $\bar{z}K \subseteq \bar{z}z^{-1} L = tL$. Hence $K = zK + \bar{z}K \subseteq (K \cap L) + tL$, so then $K \subseteq K_0$, as required.

Lemma 4.4. *If $W \leftrightarrow L$ then the row-neighbors of L are in one-to-one correspondence with the cyclic subgroups of $C(W)$, in such a way that the trivial subgroup corresponds to L and the whole group $C(W)$ corresponds to tL (which is a row-neighbor of L if and only if $C(W)$ is cyclic.)*

Proof. With each K satisfying $zK \subseteq L$, we associate the subgroup $zM/zL \subseteq L/zL \approx C(W)$ where $M = L + K$, which is a one-to-one correspondence by Lemma 4.1. The neighbors of L are precisely the K for which $(L+K)/L \approx zM/zL$ is cyclic. The trivial subgroup corresponds to $M = L$ and $K = L$ while the full group corresponds to $M = z^{-1}L$ and $K = tL$ (since $L + tL = z^{-1}(zL + \bar{z}L) = z^{-1}L$).

Remark. By examining the proofs of 2.17 and 4.1 it is easy to show that under the correspondence asserted in 4.4, the neighbor of W obtained by enlarging with the vector q (as in the definition of Y_0 in the proof of 2.17) and then reducing corresponds to the cyclic subgroup of $C(W)$ generated by q.

Lemma 4.5. *For any K and integer n, the lattices K and $t^n K$ are isometric.*

Proof. Multiplication by t is an isometry, by 2.9b.

Proposition 4.6. *The number of congruence classes distinct from the class of W that are represented by row-neighbors of W is less than or equal to the number of proper non-trivial cyclic subgroups of $C(W)$.*

Proof. If $W \leftrightarrow K$ then the number in question is equal to the number of isometry classes of lattices distinct from the class of K that are represented by row-neighbors of K, which does not exceed the number of row-neighbors of K distinct from K and tK. The result follows from 4.4.

Corollary 4.7. *If* $|\det W|$ *is* 1 *or a prime every non-singular matrix that is S-equivalent to W is congruent to W.*

If we work over the p-adic integers, all primes other than p become units, so 4.7 applies unless p^2 divides det W. Hence,

Corollary 4.7a. *If* det W *is square-free, every non-singular matrix S-equivalent to W is congruent to W over the p-adic integers, for every p.*

The neighbors of a matrix W are particularly easy to describe when $C(W)$ is itself cyclic, since then its cyclic subgroups correspond to the divisors of $\det(W)$. We shall call a form *cyclic* if $C(W)$ is cyclic for every non-singular W in the S-equivalence class of matrices representing it. (It is not true in general that if $C(W)$ is cyclic for one such W then it is cyclic for all. An explicit example is given in Section 5.) It turns out that cyclicity depends only on the rational class of the form, and in fact only on the Alexander polynomial. Let us call a form *p-cyclic* if the p-primary component of $C(W)$ is cyclic for all W representing the form. Obviously a form is cyclic if and only if it is p-cyclic for all p.

We are working with a fixed rational form on X, so Δ, the Alexander polynomial, and φ, the characteristic polynomial of Γ, are the same for all Seifert matrices V on X. We write d for the constant term of φ, which is also the leading coefficient of Δ and equal to $\det(V)$ for any V.

For any prime p we write X^p for the p-adic completion of X, and X^p_+, X^p_-, X^p_0 for the direct sum decomposition of X^p described in Section 3, with similar notation for the components of the completion K^p of a lattice K. We write φ_p for the characteristic polynomial of $\Gamma|X^p_+$ and δ_p for its degree, which equals the dimension of X^p_+ and X^p_-. Note that δ_p is the multiplicity with which 0 occurs as a root of φ, considered as a polynomial over Z/pZ. We write μ_p for the exponent of the highest power of p dividing d (which of course is the highest power dividing the constant term of φ_p).

Proposition 4.8. *A Seifert form is p-cyclic if and only if* $\min(\mu_p, \delta_p) \leqq 1$.

Proof. Recall that $C(W) \approx K/zK$ where $K \leftrightarrow W$, so the p-primary component of $C(W)$ is isomorphic to K^p/zK^p. This of course is trivial if $\mu_p = 0$ and isomorphic to Z/pZ if $\mu_p = 1$. In view of (3.4d), $K^p/zK^p \approx K^p_+/zK^p_+$. The quotient is cyclic if $\delta_p = 1$ since K^p_+ and zK^p_+ are then lattices on a one-dimensional space.

Conversely, suppose that $\mu_p = \mu > 1$ and $\delta_p > 1$. Let W be a representing matrix such that $C(W)$ is cyclic. W can be transformed by congruences so that its first column is divisible by p^μ and then, as in the proof of 2.17, further transformed to the form

$$W = \begin{bmatrix} p^{2\mu} x & b & p^\mu q' \\ p^\mu w & y & s' \\ p^\mu r & v & U \end{bmatrix}$$

with b relatively prime to p. Working over the field Z/pZ (in which b has an inverse) this is easily shown to be congruent to

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & s' \\ 0 & -\varepsilon s & U \end{bmatrix}$$

from which it follows that (modulo p) U is a Seifert matrix, and the characteristic polynomial of Γ_W is $\lambda(\lambda - 1)$ times the characteristic polynomial of Γ_U. Thus $\delta_p > 1$ implies that U is singular (mod p).

Now W is S-equivalent to

$$V = \begin{bmatrix} p^{2\mu-2} x & b & p^{\mu-1} q' \\ p^{\mu-1} w & p^2 y & p s' \\ p^{\mu-1} r & p v & U \end{bmatrix}$$

and since $\mu - 1 > 0$ and U is singular (mod p), the nullity of V(mod p) is at least two. Thus the p-primary component of $C(V)$ cannot be cyclic.

Remark. It is not difficult to show by a similar argument that if the p-primary component of $C(W)$ has a maximal cyclic subgroup of order p^k but is not cyclic, then W has a neighbor V such that $C(V)$ contains a cyclic subgroup of order p^{k+1}, while $C(V)$ and $C(W)$ have the same q-primary components for all $q \neq p$. It follows that every W is S-equivalent to some V with $C(V)$ cyclic. The fact seems curious but insignificant and we omit the proof.

Corollary 4.9. *A Seifert form is cyclic if and only if there is no prime p such that p^2 divides d and p divides the linear term of φ.*

Remark. The preceding condition is equivalent to requiring that there be no prime with p^2 dividing d and p dividing the second coefficient of the Alexander polynomial.

The criterion of Corollary 4.9 clearly depends only on the rational equivalence class of a form, so we may speak of a rational cyclic form as one with the property that some and hence all of its embedded integral forms are cyclic. Given a cyclic rational form on the space X, let G be the multiplicative group of positive rationals generated by the divisors of d. G is a free abelian group with the prime divisors of d as a basis. Let $\mathscr{L}$ be the set of all admissible lattices on X and S the set of equivalence classes on $\mathscr{L}$ under isometry. For $g \in G$, $L \in \mathscr{L}$, define $g \cdot L$ to be the unique admissible lattice K characterized by its p-adic completions as follows:

$$K^p = \begin{cases} L^p & \text{if } \delta_p = \mu_p = 0 \\ L^p_0 + p^k L^p_+ + p^{-k} L^p_- & \text{if } \delta_p = 1 \\ L^p_0 + z^k L^p_+ + \bar{z}^{-k} L^p_- = t^{-k} L^p & \text{if } \mu_p = 1 \end{cases}$$

where, in the last two cases, $k = k_p$ is the exponent of p in the prime-power decomposition of g. Note that the two formulas for K^p coincide if $\delta_p = \mu_p = 1$. $K = g \cdot L$ can alternatively be characterized as the unique admissible lattice such that $K^p_0 = L^p_0$ for all p, while, if k is the exponent of p in g, the index of K^p_+ in L^p_+ is p^k for $k \geqq 0$ and the index of L^p_+ in K^p_+ is $p^{|k|}$ for $k < 0$. It is obvious that we have defined an action of G on $\mathscr{L}$, i.e. $(gh) \cdot L = g \cdot (h \cdot L)$ for $g, h \in G$ and $L \in \mathscr{L}$. Furthermore $\sigma(g \cdot L) = g \cdot \sigma(L)$ for any isometry σ, so there is an induced action of G on S. The correspondence between congruence classes of matrices and isometry classes of lattices defines an action of G on the latter.

Proposition 4.10. *Let $\mathscr{M}$ be the set of integral congruence classes of matrices belonging to a rational congruence class that defines a cyclic Seifert form, and let G and its action on $\mathscr{M}$ be defined as above. Then the S-equivalence classes contained in the given rational congruence class are the orbits of $\mathscr{M}$ under G. The subgroup of G generated by d acts trivially.*

Proof. If two elements of $\mathcal{M}$ are in the same orbit there exist associated lattices K, L such that $K = g \cdot L$ for some g. From 3.4(f) and the definition of $g \cdot L$ it is clear that $\Lambda K = \Lambda L$ and hence that the given elements of $\mathcal{M}$ are S-equivalent. Conversely any two S-equivalent congruence classes correspond to lattices which can be joined by a chain of neighbors. By interpolating additional lattices in the chain if necessary, we may assume that for any pair of consecutive lattices K, L in the chain, K is of prime index p in $K+L$. Cyclicity implies that either $K = p \cdot L$ or $L = p \cdot K$, and hence the given lattices are related by an operation of G.

The subgroup generated by d acts trivially because $d \cdot L = t^{-1} L$ for any L, so $d \cdot L$ is isometric to L.

Corollary 4.11. *If* $\det(W) = \pm p^m$ *and W determines a cyclic form, then the number of integral congruence classes in the S-equivalence class of W is a divisor of m.*

Proof. $G/(d)$ is cyclic of order m, and acts transitively on the congruence classes within the S-equivalence class of W.

Corollary 4.12. *If W is the matrix of a cyclic Seifert form then the row-neighbors of W are the same as its column-neighbors.*

Proof. If $W \leftrightarrow L$ then U is a row-neighbor of W if and only if $U \leftrightarrow K$ with K adjacent to L and $zK \subseteq L$. Under the hypothesis of cyclicity this is equivalent to $L = g \cdot K$ for some integer g dividing d. But then K is isometric to $d \cdot K = (d/g) \cdot L$, so W is a row-neighbor of U, i.e. U is a column neighbor of W.

One might conjecture that the conclusion of (4.12) holds for all Seifert matrices, and the following proposition (which is a strengthening of Theorem 3 of [8]) tends to support this view. The conjecture is false, however, as shown by an example in Section 5.

Proposition 4.13. *If U and W are S-equivalent and non-singular then there is a chain* $U = V_0, V_1, \dots, V_n = W$ *with* V_i *a row-neighbor of* V_{i+1} *for each i.*

Proof. Let $U \leftrightarrow K$ and $W \leftrightarrow L$. Examining the construction given in (3.6) and (3.7) shows that it gives a chain of the required type if $L^p_+ \subseteq K^p_+$ for every p. For any p, K, and L, $t^{-m} L^p_+ = z^m L^p_+ \subseteq K^p_+$ for sufficiently large m, by 3.4(a). Since $L^p_+ = K^p_+$ for all but a finite number of p, we can take m sufficiently large to give the inclusion for all p. Since $t^{-m} L$ is isometric to L we have $W \leftrightarrow t^{-m} L$ and the conclusion follows.

Theorem 4.14. *If W is a Seifert matrix such that the minimal polynomial of* Γ_W *has a repeated factor whose constant term is divisible by a prime p, then the S-equivalence class of W contains representatives of* *infinitely many distinct congruence classes over the p-adic integers (and a fortiori, infinitely many integral congruence classes).*

Proof. Let $W \leftrightarrow L$. The conclusion of the theorem translates into a statement of the existence of infinitely many lattices K_k such that $\Lambda K_k = \Lambda L$ for all k, but K_k^p and K_j^p are not isometric (allowing isometries with coefficients in Q_p) unless $k=j$. We shall construct the p-adic completions K_k^p and define K_k by requiring $K_k^p = L^q$ for all $q \neq p$.

We write $X^p = X_+^p + X_-^p + X_0^p$ as usual, and let ψ be the minimal polynomial of $\Gamma | X_+^p$. Any factor of the minimal polynomial of Γ for which p divides the constant term must contain a p-adic factor that appears in ψ, so the hypothesis of the theorem implies that ψ contains a factor ψ_0^m with $m > 1$. We may further suppose that ψ_0 is irreducible (over Q_p) and that m is maximal, i.e. ψ_0^{m+1} does not divide ψ. By the elementary theory of canonical forms of matrices under similarity, X_+^p splits as a direct sum of Γ-invariant subspaces $Y + Y'$ such that $\Gamma | Y$ has ψ_0^m for both its characteristic and minimal polynomial. Furthermore, Y has dimension rm where r is the degree of ψ_0, and there exists $y \in Y$ such that the vectors $y_i = \Gamma^i y = z^i y$ for $i = 0, \ldots, rm-1$ form a basis for Y. Let M be the lattice generated by the y_i. The entries of the matrix of $z | Y$ with respect to the basis $\{y_i\}$ are all 0, 1 or coefficients in ψ_0^m and hence all in Z_p, so $zM \subseteq M$. Similarly a lattice N can be found on Y' with $zN \subseteq N$. By taking a dual basis as in (3.5a) we obtain a lattice $\overline{M} + \overline{N}$ on X_-^p such that $K^p = L_0^p + M + N + \overline{M} + \overline{N}$ is an admissible lattice on X^p and (by 3.4(f)), $\Lambda K^p = \Lambda L^p$. For any sequence M_k of lattices on Y satisfying $zM_k \subseteq M_k$, we can define K_k^p by the construction above (replacing M by M_k) and so obtain a sequence of admissible lattices with $\Lambda K_k = \Lambda L$ as required.

Since ψ_0 is monic, the vectors $x_{ij} = z^i \psi_0(z)^j y$ for $0 \leqq i < r$, $0 \leqq j < m$ also form a basis for M. We define M_k as the lattice generated by $p^k x_{i0}$ and x_{ij} for $0 \leqq i < r$, $1 \leqq j < m$. It is easily verified that $zM_k \subseteq M_k$.

To show that none of the K_k^p so constructed are isometric, we use the observation that for any polynomial f, the isomorphism class of $L/f(z)L$ depends only on the isometry class of L. We apply this, using $f = \psi_0^{m-1}$. Since $f(z) = z^{rm-r} \pmod{p}$, it acts unimodularly on X_0^p and X_-^p. Hence $K_k^p / f(z) K_k^p = M_k / f(z) M_k + N / f(z) N$. Now $f(z) x_{i0} = x_{i,m-1}$ and $f(z) x_{ij} = 0$ for $j > 0$, so $M_k / f(z) M_k$ is the direct sum of $rm - r$ copies of Z_p and r copies of $Z/p^k Z$, and distinct values of k give non-isomorphic Z_p-modules. Since $N/f(z)N$ is independent of k we conclude that distinct values of k give non-isometric lattices K_k^p, and hence that the matrices $W_k \leftrightarrow K_k$ are not congruent over Z_p.

I conjecture that the converse of Theorem 4.14 is also true. Levine [8] has obtained strong results (for the $\varepsilon = -1$ case) in this converse direction, and a more recent result of his (private communication) implies that the minimal polynomial of Γ_W must have some repeated factor if the S-equivalence class of W contains infinitely many integral congruence classes.

It was shown in [16], (for $\varepsilon = -1$, and with different terminology) that if U and W are non-singular and S-equivalent with determinant d then they are congruent over any extension of the integers in which d has an inverse. In particular they are congruent over $Z[d^{-1}]$, the subring of the rationals generated by d^{-1}. Levine gave an example in [6] to show that congruence over $Z[d^{-1}]$ does not in general imply S-equivalence. The following theorem gives a sufficient condition for the implication to hold. It is closely related to Theorem (3.1) in [1]. In fact the hypothesis is easily shown to be equivalent to Crowell's condition that every prime dividing the leading coefficient of Δ divide all but the central coefficient of Δ.

Theorem 4.15. *Let U and W be non-singular of rank $2h$ and belong to the same rational congruence class, with determinant d. If $\delta_p = h$ for every prime p dividing d then U and W are S-equivalent if and only if they are congruent over $Z[d^{-1}]$.*

Proof. S-equivalence of U and W implies that one can be converted to the other by congruence transformations using matrices which are either unimodular, or diagonal with entries k, k^{-1} and 1 on the diagonal, with k a divisor of d. Hence U and W are congruent over $Z[d^{-1}]$. Conversely, suppose U and W are congruent by a matrix P which is unimodular over $Z[d^{-1}]$, and let $U \leftrightarrow K$, $W \leftrightarrow L$. P is unimodular over Z_p for p not dividing d, so for all such p, $K_0^p = K^p = L^p = L_0^p$. But for p dividing d, the hypothesis implies $K_0^p = 0 = L_0^p$. Thus $K_0^p = L_0^p$ for all p, so by 3.4(a) and 3.9(a), $\Lambda K = \Lambda L$ and U and W are S-equivalent.

5. Examples

In computing examples, it is generally easier to use the technique implicit in the proofs of (2.15) and (2.17) than to carry out enlargement-reduction steps according to the basic definition. Suppose the i-th column of a Seifert matrix W is divisible by k, while the i-th row is divisible by k except for the entry w_{ij}, and w_{ii} is divisible by k^2. Let U be obtained from W by dividing the i-th row and column of W by k and multiplying the j-th row and column by k. We say that U is obtained from W by *transferring a factor of k from column i to row j.* In the proof of (2.17), U_0 is the matrix obtained from W_0 by transferring k from the first column to the second row, and the discussion there shows that U_0 is a row-neighbor of W_0. More generally, *the result of transferring a factor from a column to a row is a row-neighbor* of the original matrix. Of course we obtain column-neighbors by transferring factors from rows to columns.

Example 5.1. For any integers r, s with $r \neq 0$ let

$$W(r,s)=\begin{bmatrix}0 & 0 & -1 & 0\\ 1 & 0 & 0 & \varepsilon r\\ \varepsilon & 0 & 0 & 0\\ 0 & -r & 1 & s\end{bmatrix}, \quad U(r,s)=\begin{bmatrix}0 & 0 & -r & 0\\ 1 & 0 & 0 & \varepsilon\\ \varepsilon r & 0 & 0 & 0\\ 0 & -1 & 1 & s\end{bmatrix}.$$

Transferring r from column 2 to row 1 in $W(r,s)$ gives $U(r,s)$. Transferring r from row 3 to column 4 in $U(r,s)$ gives $W(r, s r^2)$. By induction, $W(r, s r^{2k})$ is S-equivalent to $W(r,s)$ for all $k \geqq 0$. By direct computation, the matrix $M = M(r,s) = \Gamma^2 - \Gamma - \varepsilon r I$, where $\Gamma = \Gamma_{W(r,s)}$, is zero except for $m_{13} = -\varepsilon s$ and $m_{42} = s$. If $W(r, s_1)$ and $W(r, s_2)$ are integrally congruent then $M(r, s_1)$ and $M(r, s_2)$ are integrally similar, which is possible only if $|s_1| = |s_2|$. Thus if $|r| > 1$ and $s \neq 0$, the matrices $W(r, s r^{2k})$ for $k = 0, 1, \ldots$ belong to distinct congruence classes, but are all S-equivalent. The minimal polynomial of $\Gamma_{W(r,s)}$ is $(x^2 - x - \varepsilon r)^2$ so we have here an illustration of Theorem 4.13. It is also easy to calculate that $C(W(r,s))$ is cyclic of order r^2 if s is relatively prime to r, while $C(U(r,s))$ is always isomorphic to $(Z/rZ)^2$, so these S-equivalent matrices have different C-groups.

It is sometimes feasible to check integral congruence for two given matrices U and W by elementary calculation. $W = PUP'$ if and only if $P' S_W P = S_U$ and $P\Gamma_U = \Gamma_W P$. The last condition is linear in P and the general solution for it is easily found. The first condition may then turn out to be tractable. This method was used by Rice for an example in [13]. We illustrate it with two examples (previously announced in [18]) of some interest in knot theory. In both examples, $\varepsilon = -1$.

Example 5.2. Let $U = \begin{bmatrix}5 & 2\\ 1 & 11\end{bmatrix}$ and $W = U'$. Then U and W are not S-equivalent.

Proof. Since $\det(U) = 53$ is a prime, it is sufficient, by (4.7), to show that U and W are not congruent. It is easily verified that the general solution of $P\Gamma_U = \Gamma_W P$ is $P = \begin{bmatrix}x - 2y & 2x + y\\ 5x + y & -x + 2y\end{bmatrix}$ and that $P' S_W P = S_U$ if and only if $\det(P) = -11x^2 - 3xy - 5y^2 = -1$. Writing $\det(P)$ as $-8x^2 - 2y^2 - 3(x^2 + xy + y^2) \leqq -8x^2 - 2y^2$ makes it obvious that the equation has no solution in integers.

This example of a matrix not S-equivalent to its transpose settles a question raised in [16]. A knot with such a matrix cannot be invertible. This example first appeared in [5].

Example 5.3. Let $U = \begin{bmatrix}1 & 1\\ 0 & -367\end{bmatrix}$ and $W = -U$. Then U and W are not S-equivalent.

Proof. Noting that 367 is prime and proceeding as in (5.2), we find that S-equivalence of U and W depends on the existence of P of the form $\begin{bmatrix} x+y & -y \\ -367y & x \end{bmatrix}$ with $\det(P)=x^2+xy-367y^2=-1$. Now

$$x^2+xy-367y^2$$

is the norm of the algebraic integer $x+y\omega$, where ω is a root of $z^2+z-367$ so that $Q(\omega)$ is the quadratic field with discriminant 1469. Thus P exists if and only if $Q(\omega)$ contains an integer of norm -1. The question can be settled by computing the fundamental unit of the field (an algorithm can be found in Chapter 7 of [19]), and the answer is no. (This example was in fact found by a computer search.) Alternatively one may note that $1469=(13)(113)$ and that $x=3$, $y=1$ is a solution of $13x^2-113y^2=4$, and apply the criterion given in [17].

The interest of this example lies in the fact that U and $-U$ are congruent over the rationals and over the p-adic integers for every p. Thus they cannot be distinguished by any of the "classical" invariants as given in [4]. To verify the assertion, note that $x=\frac{18}{5}$, $y=\frac{1}{5}$ is a rational solution of $x^2+xy-367y^2=-1$ and also a solution in Z_p for $p\neq 5$, while $x=\frac{2}{19}$, $y=\frac{1}{19}$ is a solution in Z_5.

Examples to illustrate some of the results in Section 4 can be given by matrices of rank 2. (Some results of systematic investigation of rank 2 matrices are reported in [8].) We first remark that rank 2 matrices are not very interesting when $\varepsilon=+1$. The only even unimodular symmetric form of rank 2 is represented by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, so any V is congruent to one such that $V+V'=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $V=\begin{bmatrix} 0 & 1-v \\ v & 0 \end{bmatrix}$ for some v. It is easy to show that two such matrices are congruent and hence S-equivalent if and only if they have the same determinant.

For $\varepsilon=-1$, any 2-by-2 Seifert matrix is congruent to one of the form $\begin{bmatrix} a & b+1 \\ b & c \end{bmatrix}$, which we abbreviate as $V(a,b,c)$. Note that the transpose of $V(a,b,c)$ is not in the proper form, but is congruent to $V(c,b,a)$. It is easy to check that PVP' continues to have this form only if $\det(P)=+1$. It is natural to associate the quadratic form $ax^2+(2b+1)xy+cy^2$ with $V(a,b,c)$; the correspondence is one-to-one, and congruence of matrices corresponds to proper equivalence of forms. The discriminant of the form is $D=1-4d$, where $d=ac-b(b+1)$ is the determinant of the matrix. We call $V(a,b,c)$ *positive* if a, c and d are all positive; these are exactly the conditions for the associated form to be positive definite. The classification of such forms is well-known (for example, see [19]), and translates into the following classification for positive matrices.

$V(a,b,c)$ is said to be *reduced* if $0<2b+1\leqq\min(a,c)$. Every positive V is congruent to one which is reduced. If $V(a,b,c)$ and $V(a',b',c')$ are both reduced and congruent then $b'=b$ and either $a'=a$, $c'=c$ or $2b+1=\min(a,c)$, $a'=c$, $c'=a$. $V(a,b,c)$ is congruent to its transpose if and only if it is congruent to $V(c,b,a)$; if it is reduced, the condition is equivalent to $a=c$ or $\min(a,c)=2b+1$.

Example 5.4. There are 10 distinct congruence classes of positive matrices of determinant 30, represented by the matrices $A=V(1,0,30)$, $B=V(2,0,15)$, $C=V(3,0,10)$, $D=V(5,0,6)$, $E=V(4,1,8)$, $F=V(6,2,6)$, B', C', D', and E'. (A' is congruent to A and F' is congruent to F.)

Proposition 4.10 applies. The group G is generated by 2, 3 and 5. The actions of 2 and 3 are identical and represented by the permutation cycles $(B'E'AEB)$ $(C'D'FDC)$ while the action of 5 is represented by $(E'BAB'E)$ $(D'CFC'D)$, that is, $2\cdot[B']=[E']$, $2\cdot[E']=[A]$, etc. Thus there are two S-equivalence classes consisting of 5 congruence classes each. The S-equivalence classes are included in distinct rational congruence classes, as may be shown by calculating the Hasse invariant [12] of the associated quadratic form at the prime 7.

The following example illustrates (4.11), with $p=2$, $m=6$.

Example 5.5. There are 12 congruence classes of positive matrices of determinant 64, represented by $A=V(1,0,64)$, $B=V(2,0,32)$, $C=V(4,0,16)$, $D=V(8,0,8)$, $E=V(3,1,22)$, $F=V(6,1,11)$, $G=V(5,2,14)$, $H=V(7,2,10)$, B', C', F' and H'. (A, D, E and G are congruent to their respective transposes.)

The action of 2 is described by the permutation (CAC') (DBB') (HEH') (FGF') so there are 4 S-equivalence classes, each containing 3 congruence classes. The Hasse invariants at 3 and 5 show that 4 distinct rational congruence classes are represented.

Finally, we exhibit a matrix of rank 6 which has a row-neighbor that is not a column-neighbor. There can be no such example of rank 2, because matrices of rank 2 define cyclic forms. I do not know whether there is an example of rank 4. We first give some definitions and a lemma that are needed to reduce the explicit computations to manageable size.

We introduce the notations

$$\operatorname{dg}(A,B)=\begin{bmatrix}A & 0\\ 0 & B\end{bmatrix} \quad\text{and}\quad \operatorname{sd}(A,B)=\begin{bmatrix}0 & A\\ B & 0\end{bmatrix}$$

where A and B are square matrices of the same size. (The notations "dg" and "sd" are meant to suggest "diagonal" and "skew-diagonal".) For any G, define $V(G)$ to be $\operatorname{sd}(\varepsilon G, I-G')$. Then $V(G)+\varepsilon V(G)'=\operatorname{sd}(\varepsilon I, I)$ so $V(G)$ is a Seifert matrix and $\Gamma_{V(G)}=\operatorname{dg}(G, I-G')$. Note that if $H=P^{-1}GP$ then $V(H)=RV(G)R'$ with $R=\operatorname{dg}(P^{-1},P')$, so $V(H)$ is integrally congruent to $V(G)$ if H is integrally similar to G. The following restricted converse is needed in discussing the example.

Lemma 5.6. *Suppose the characteristic polynomials of G and H are the same and have no common factor with that of $I-G'$. Then $V(H)$ and $V(G)$ are integrally congruent only if H and G are integrally similar.*

Proof. Suppose $V(H)=RV(G)R'$, where R partitions into $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$. Then $RS^{-1}R'=S^{-1}$, where $S^{-1}=V(G)+\varepsilon V(G)'=V(G)+\varepsilon V(H)'=\mathrm{sd}(\varepsilon I,I)$. It follows that $R\Gamma_{V(G)}=\Gamma_{V(H)}R$, so $AG=HA$ and $B(I-G')=HB$. Since the characteristic polynomials of $I-G'$ and H have no common factor, B must be zero. Hence $\det(R)=\det(A)\det(D)$ and A must be unimodular if R is. Then $H=A^{-1}GA$ and is integrally similar to G.

Example 5.7. Let

$$A=\begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 2 & 0 & 0 \end{bmatrix}, \quad B=\begin{bmatrix} 2 & 0 & 2 \\ 0 & -2 & 2 \\ 0 & -2 & 0 \end{bmatrix}, \quad C=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 4 & 0 & 0 \end{bmatrix},$$

$$D=\begin{bmatrix} 0 & 2 & 1 \\ -2 & 0 & 1 \\ 4 & 0 & 0 \end{bmatrix}.$$

Then $V(A)$, $V(B)$, $V(C)$, $V(C')$ and $V(D)$ represent distinct congruence classes. The row-neighbors of $V(A)$ are represented by $V(B)$, $V(C)$ and $V(D)$ while the column-neighbors are represented by $V(B)$, $V(C')$ and $V(D)$.

We first note that A and $I-A'$ have relatively prime characteristic polynomials, x^3-8 and $(x-1)^3+8$. The group $C(V(A))$ is isomorphic to $Z/7Z+(Z/2Z)^3$ and has proper cyclic subgroups of orders 2, 7 and 14. The subgroups of order 2 are generated by column vectors with 0 or 1 in the first three components and 0 in the last three. Given such a vector v, let u be the vector consisting of its first three components, and find a unimodular P such that the first column of AP is equal to $2u$. A congruence transformation by $\mathrm{dg}(P^{-1}, P')$ converts $V(A)$ to $V(G)$ where $G=P^{-1}AP$, and converts u to $P^{-1}u$. The fourth column of $V(G)$ is equal to 2 times the new bordering column. The fourth row of $V(G)$ is the first column of $I-G$ followed by zeros, and divisible by 2 except for the first entry. The result of the enlargement-reduction is then given by transferring a factor of 2 from the fourth column to the first row. The result has the form $V(H)$ with H rationally similar to G, so the conditions of (5.6) apply. Because A is invariant under cyclic permutation of rows and columns, the calculation need be done only for $u=(1, 1, 1)$, $u=(1, 0, 0)$

and $u=(1, 1, 0)$. The results turn out to be (congruent to) $V(B)$, $V(C)$ and $V(D)$ respectively.

The necessary checking of integral similarity is in practice easy. If $H=P^{-1}GP$ then $PH=GP$. For given G and H this is a system of linear equations for the entries of P, and the general solution in integers can be found. For the cases arising in this example it is then either obvious that $\det(P)$ is divisible by 2 or else a solution with $\det(P)=\pm 1$ is easily found by inspection. In this way it can be verified that no two of A, B, C, C' and D are similar, while A, B and D are similar to A', B' and D' respectively.

The same remarks apply, *mutatis mutandis*, to calculating the row-neighbor class corresponding to the unique subgroup of order 7. It turns out to be the class of $V(A)$ itself. Neighbors corresponding to subgroups of order 14 are neighbors of order 2 of neighbors of order 7, and so give nothing new. Thus the complete list of row-neighbor classes of $V(A)$ is represented by $V(B)$, $V(C)$ and $V(D)$.

Since A is similar to A', $[V(A)'] = [V(A')] = [V(A)]$ and it follows that $V(B')$, $V(C')$ and $V(D')$ represent the column-neighbors of $V(A)$.

This work was partially supported by the National Science Foundation under grant GP-34001.

References

1. Crowell, R.H.: The group G'/G'' of a knot group G. Duke Math. J. **30**, 349–354 (1963).
2. Crowell, R.H., Fox, R.H.: Introduction to Knot Theory. New York: Blaisdell 1963.
3. Erle, D.: Quadratische Formen als Invarianten von Einbettungen der Kodimension 2. Topology **8**, 99–114 (1969).
4. Fox, R.H.: The homology characters of the cyclic coverings of the knots of genus one. Ann. Math. **71**, 187–196 (1960).
5. Fox, R.H., Smythe, N.: An ideal class invariant of knots. Proc. Amer. Math. Soc. **15**, 707–709 (1964).
6. Levine, J.: An algebraic classification of some knots of codimension two. Comm. Math. Helv. **45**, 185–198 (1970).
7. Levine, J.: Polynomial invariants of knots of codimension two. Ann. Math. **84**, 537–554 (1966).
8. Levine, J.: Finite procedures in knot theory. (Mimeographed.) Brandeis University, 1972.
9. Milnor, J.: Infinite cyclic coverings. In: Conference on the Topology of Manifolds. Ed. J.G. Hocking. Boston: Prindle, Weber and Schmidt 1968.
10. Milnor, J.: On isometries of inner product spaces. Inventiones math. **8**, 83–97 (1969).
11. Murasugi, K.: On a certain numerical invariant of link types. Trans. Amer. Math. Soc. **117**, 387–422 (1965).
12. O'Meara, O.T.: Introduction to Quadratic Forms. New York: Academic Press 1963.
13. Rice, P.M.: Equivalence of Alexander Matrices. Math. Ann. **193**, 65–75 (1971).
14. Seifert, H.: Über das Geschlecht von Knoten. Math. Ann. **110**, 571–592 (1934).
15. Seifert, H.: Die Verschlingungsinvarianten der zyklischen Knotenüberlagerungen. Abh. Math. Sem. Hamburg Univ. **11**, 84–101 (1936).

16. Trotter, H. F.: Homology of group systems with applications to knot theory. Ann. Math. **76**, 464–498 (1962).
17. Trotter, H. F.: On the norms of units in quadratic fields. Proc. Amer. Math. Soc. **22**, 198–201 (1969).
18. Trotter, H. F.: On the algebraic classification of Seifert Matrices. Proceedings of the Georgia Topology Conference 1970, 92–103, University of Georgia, Athens, 1970 (mimeographed).
19. Dickson, L. E.: Introduction to the Theory of Numbers. Chicago: University of Chicago Press 1929.
20. Kearton, C.: Classification of simple knots by Blanchfield duality. Bull. Amer. Math. Soc. (to appear).
21. Blanchfield, R. C.: Intersection theory of manifolds with operators with applications to knot theory. Ann. Math. **65**, 340–356 (1957).

H. F. Trotter
Princeton University
Department of Mathematics
Box 37
Princeton, N. J. 08540
USA

(Received July 27, 1972)