MACHINE CALCULATION OF THE P-ADIC INVARIANTS OF INTEGRAL QUADRATIC FORMS

-- submitted in partial fulfillment
of the senior thesis requirement of the
Department of Mathematics, Princeton University
by M. H. Wigler, April 1970

ACKNOWLEDGEMENT

I wish to express my gratitude to Professor Hale Trotter, who suggested this problem to me, for his guidance and enlightening discussions. I am also indebted to David Lombardero, whose work in this area two years ago made this effort possible.

M. H. Wigler

TABLE OF CONTENTS

INTRODUCTION

From any regular projection of a tame knot K it is possible to construct a Seifert surface, a 2-dimensional, orientable surface which spans K [4].[1] Any Seifert surface may be deformed into a disc with handles, and from this structure one can construct the Seifert matrix of the Seifert surface, V, which gives some information as to how the handles are twisted and entwined. When V is nonsingular the symmetric matrix V + V', where V' is the transpose of V, represents a quadratic form whose genus is an invariant of the knot type of K [5]. V is now known to be equivalent to the Murasugi matrix M*.[2]

Lombardero programmed an effective procedure for calculating the Murasugi matrix M* of a knot or link [4]. In the present paper I develop some of the theory and background for a program that calculates numerical invariants of the genus of the quadratic form given by M* + M*' The program has been written in Fortran IV for the IBM 360 mod 90 computer, and is designed to interface with Lombardero's program. It should not be difficult to adapt the program to more general situations.

PRELIMINARY CONCEPTS

A quadratic form, f, in n variables over the ring R (assumed to be commutative with identity) is an homogenous polynomial of degree two that can be written in the form

$$(1) \qquad f = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j$$

where $a_{ij} = a_{ji} \in R$. A quadratic form is called unary, binary, ternary,

etc. according as it is in one, two, three, etc. variables.

Let g be another form given by

$$g = \sum_{i=1}^{m} \sum_{j=1}^{m} b_{ij} y_i y_j. \tag{2}$$

f and g are said to be <u>equivalent over R</u>, written $f \sim g$ over R, when a change of variables

$$x_i = \sum_{j=1}^{m} t_{ij} y_j \tag{3}$$

brings f to g and when (3) may be solved for the y_j in terms of the x_i. It is clearly necessary for m=n if $f \sim g$. If $f \sim g$ over R, f and g represent the same values.

The relation "$\sim$" is clearly an equivalence relation, being reflexive, symmetric and transitive.

If f is a form in n variables and g is a form in m distinct variables, as in (1) and (2), f and g are said to be <u>disjoint</u>. Their disjoint union, $f \dot{+} g$, is the form in n+m variables

$$h = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{m} \sum_{j=1}^{m} b_{ij} y_i y_j. \tag{4}$$

h is said to have the <u>decomposition</u> $h = f \dot{+} g$. If f_i, i=1,2,..,N is a sequence of disjoint forms, we use the covenient summation notation

$$\sum_{i=1}^{N} f_i \tag{5}$$

to denote the disjoint union of the f_i, and the context shall indicate when summation is to be taken to be disjoint.

There is a convenient translation of all these notions into the

algebra of matrices over R. To f we associate the n x n symmetric matrix

(6) $$A(f) = ((a_{ij}))$$

Henceforth we shall also refer to symmetric matrices over R as quadratic forms over R. If X denotes the row matrix $[x_1,\ldots,x_n]$ and X' its transpose, the formal product

(7) $$X'A(f)X = f.$$

A is equivalent to B, $A \sim B$, if there exists an invertible T such that

(8) $$TAT' = B.$$

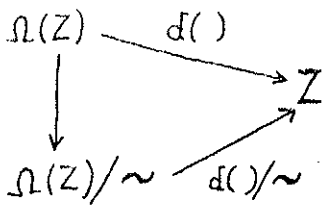
T is invertible if and only if det(T) is a unit in R.

If A is an n x n symmetric matrix and B an m x m symmetric matrix, we represent the direct sum

(9) $$A \dot{+} B = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

If our ground ring R is Z, the integers, d(f) = det(A(f)) is an <u>invariant</u> of f since T is invertible if and only if det(T) = $\pm$ 1. That is, d( ) is an effectively calculable function defined on the space of forms over the integers which attains identical values for equivalent forms. Pictorially,

(10)



is a commutative diagram, where $\Omega(Z)$ is the space of forms over Z. We say that d( ) <u>projects</u> to d( )/$\sim$ defined on the space of equivalence classes of forms $\Omega(Z)/\sim$.

RING HOMOMORPHISMS AND INDUCED MAPS

If $R \subseteq \tilde{R}$ and I is an ideal of R, we have the diagram

(11) $$\tilde{R} \overset{i}{\supseteq} R \xrightarrow{p} R/I$$

which induces the maps

(12) $$\Omega(\tilde{R}) \xleftarrow{i^*} \Omega(R) \xrightarrow{p^*} \Omega(R/I)$$

and

(13) $$\Omega(\tilde{R})/\sim \xleftarrow{\tilde{i}} \Omega(R)/\sim \xrightarrow{\tilde{p}} \Omega(R/I)/\sim .$$

In other words, if $f \sim g$ over R, $i^*(f) \sim i^*(g)$ over $\tilde{R}$ and $p^*(f) \sim p^*(g)$ over R/I.

When R = Z, we often wish to look at the case where $\tilde{R}$ is the field of real numbers, $\mathbb{R}$, and I = (m), the ideal generated by $m \in Z$. If f and g are two forms over Z,

(i) $f \sim g$ over $\mathbb{R}$, and

(ii) $f \sim g$ over $Z/(m)$ for every $m \in Z$,

then f and g are said to be of the same genus, or semiequivalent, which we write $f \vee g$.[3] Although equivalence over Z implies semi-equivalence, the converse does not hold.

It is a simple application of the Chinese remainder theorem that in order to establish (ii) we need only establish

(ii') $f \sim g$ over $Z/(p^w)$ for all prime p and all $w \geq 1$.[4]

We shall show in the sequel that it suffices to establish

(ii'') $f \sim g$ over $Z/(p_i^{w(i)})$ for $i=1,\ldots,N$ where

$$d(f) = \prod_{i=1}^{N} p_i^{w(i)-1}$$

and that a complete set of invariants exist for establishing equivalence

over the residue rings $Z/(p^w)$ when p is an odd prime.

We shall assume in the remainder of this paper that $d(f) \neq 0$. For if $d(f) = 0$ we can decompose f into a disjoint union of a nonsingular form with a zero form of the appropriate size.[5]

THE CONGRUENCE OF UNARY FORMS

As a first step towards developing a theory of the congruence of quadratic forms over the rings $Z/(p^w)$ we must investigate the congruence properties of ax^2 over $Z/(p)$. Now, $ax^2 \sim bx^2$ over $Z/(p)$ if and only if there is a $t \not\equiv 0 \pmod p$ such that $at^2 \equiv b \pmod p$. If such a t exists, a and b are said to belong to the same quadratic residue class modulo p. The Legendre symbol $(\frac{a}{p})$ will be of use here; it is defined for all odd primes on the multiplicative group $Z/(p)^+$ as follows:

$(\frac{a}{p}) = +1$ if $t^2 \equiv a \pmod p$ is solvable; that is, if a is a perfect square in $Z/(p)$; or, if a is in the same quadratic residue class as 1:

$(\frac{a}{p}) = -1$ otherwise.

We now list some properties of $Z/(p)$ for odd primes p that will be of use in the sequel:

p1. There are $(p-1)/2$ squares and $(p-1)/2$ nonsquares in the multiplicative group $Z/(p)^+$.

p2. $(\frac{a}{p}) = (\frac{b}{p})$ if and only if there is a t such that $at^2 \equiv b \pmod p$.

p3. $(\frac{\ }{p})$ is a homomorphism of the multiplicative

group $Z/(p)^+$ into the multiplicative group $\{1,-1\}$.

When p is an odd prime, the equation

(14) $$x^2 \equiv a \not\equiv 0 \pmod{p}$$

either has two nonidentical solutions, or it has none. Since every $x \in Z/(p)^+$ is a solution to an equation of the form (14), there are only (p-1)/2 equations of form (14) which have solutions. Hence p1.

If a and b are squares in Z/(p), so is there product. Let a be a nonsquare. If b is a nonzero square, ab must be a nonsquare. As b ranges over all (p-1)/2 possible values of nonzero squares, ab ranges over all (p-1)/2 possible values of nonsquares. From this it follows that if a and c are both nonsquares, there is some t such that $at^2 \equiv c \pmod{p}$. Hence, p2. It also follows that if c is a nonsquare, ac is a non zero square. Hence p3.

By p2 if $ba \not\equiv 0 \pmod{p}$ $ax^2 \sim bx^2$ if and only if $(\frac{a}{p}) = (\frac{b}{p})$.

THE DIAGONALIZATION OF FORMS OVER $Z/(p^W)$. WITT'S THEOREM FOR RINGS

In this section we introduce two powerful tools for reducing the problem of equivalence. The first result says that if we are working in one of the rings $Z/(p^W)$ where p is an odd prime, every form is equivalent to a diagonal form (i.e. a form whose matrix representation is diagonal). The second result, which is usually just proven for forms over a field, says that if we can decompose some form $h = f \dotplus g$ over one of the rings mentioned above, the equivalence class of h depends solely on the respective equivalence classes of f and g. In brief,

the space $\Omega(Z/(p^W))/\sim$ has an inherited structure of a semigroup under the operation induced by disjóint union.

The failure of these two results to hold for p = 2 accounts for some of the difficulty encountered in finding invariants for equivalence over the rings $Z/(2^W)$.

Now let us consider the algebra of n x n matrices over the ground ring R. Let I denote the identity matrix, and I_{ij} the matrix all of whose entries are zero except for the (i,j) entry which is the multiplicative identity of R. Let $S_{ij} = I + I_{ij}$. Then $S_{ij}' = S_{ji}$. If A is an n x n matrix, $S_{ij}A$ is the matrix obtained from A by adding the jth row of A to the ith. AS_{ji} is the matrix obtained from A by adding the jth column of A to the ith. Let $T_{ij} = (I + I_{ij} + I_{ji} - I_{ii} - I_{jj})$. $T_{ij}' = T_{ij}$. $T_{ij}A$ interchanges the ith and jth rows of A while AT_{ij} interchanges the columns.

Lemma If p^u divides each element of A, p^u divides each element of $S_{ij}A$, AS_{ji}, $T_{ij}A$, and AT_{ij}.

The proof is immediate.

THEOREM 1 Every form f is equivalent to a diagonal form over $Z/(p^W)$ provided p is an odd prime.

The proof consists of an algorithm, which we set forth straight away. Let $A=((a_{ij}))$ be the n x n matrix representation of some form f. We use the notation "$\leftarrow$" to mean "replace". For example, $a_{ii} \leftarrow a_{jj}$ means replace the value of a_{ii} with the value currently called a_{jj}.

(i) Let p^u be the highest power of p that divides all the a_{ij}.

(ii) If p^u is the highest power of p that divides a_{nn} (which we hereafter write as $p^u \| a_{nn}$) proceed to (vi).

(iii) If there is an a_{ii} such that $p^u \| a_{ii}$ proceed to (v).

(iv) Find a_{ij} such that $p^u \| a_{ij}$. $A \leftarrow S_{ij} A S_{ji}$. Then a_{ii} has been replaced with the value $a_{ii} + 2a_{ij}$ so that $p^u \| a_{ii}$.

(v) $A \leftarrow T_{in} A T_{in}$ so $p^u \| a_{nn}$.

(vi) It is still true that p^u is the highest power of p dividing each element of the matrix A. Hence we can solve for r_i the congruences

$$r_i a_{nn} + a_{ni} \equiv 0 \pmod{p^w}.$$

(vii) Let

$$T = I + \sum_{i=2}^{n} r_i I_{in}.$$

$A \leftarrow TAT'$ to obtain a matrix of the form

$$\begin{bmatrix} A^* & 0 \\ 0 & a_{nn} \end{bmatrix}$$

equivalent over $Z/(p^w)$ to A

(viii) If A^* has dimension greater than 1 x 1, repeat steps (i) through (viii) on A^*, otherwise, fin.

By this procedure we construct a diagonal matrix equivalent to A over $Z/(p^w)$.

The next theorem we state without proof since the proof is so similar.

THEOREM 2 If F is a field of characteristic not equal to 2, every form f is equivalent to a diagonal form over F.

THEOREM 3 If $f_i \sim g_i$ over R for i=1,...,N the disjoint sums

$$f = \sum_{i=1}^{N} f_i \sim \sum_{i=1}^{N} g_i = g \text{ over } R. \tag{15}$$

proof: If $T_i A(f_i) T_i' = A(g_i)$, let T be the disjoint sum $\sum_{i=1}^{N} T_i$. Then $TA(f)T' = A(g)$.

THEOREM 4 If $f^* \sim g^*$ over $Z/(p^W)$ and $f^* \dot{+} f \sim g^* \dot{+} g$ over $Z/(p^W)$, then $f \sim g$ over $Z/(p^W)$ provided that p is an odd prime.

proof: By the above theorem we can assume that $f^* = g^*$. By theorem 1 we can assume f^* is in diagonal form. Then the theorem will follow by induction on the number of variables in f^* provided that we can demonstrate its truth for $f^* = ax^2$. Now if $ax^2 \dot{+} f \sim ax^2 \dot{+} g$ we have the matrix equation

$$\begin{bmatrix} t & S \\ T & Q \end{bmatrix} \begin{bmatrix} a & 0 \\ 0' & A \end{bmatrix} \begin{bmatrix} t & T \\ S' & Q' \end{bmatrix} \doteq \begin{bmatrix} a & 0 \\ 0 & B \end{bmatrix} \pmod{p^W} \tag{16}$$

where A is the matrix representation of f, and B that of g. Hence

$$\begin{aligned} t^2a + SAS' &\equiv a \\ taT' + SAQ' &\equiv 0 \\ aTT' + QAQ' &\equiv B \end{aligned} \tag{17}$$

where 0 is the appropriate sized row matrix of zeros.

Let us look to $Y = Q + zTS$ for a solution, choosing an appropriate z, if possible, to suit our needs. Then

$$\begin{aligned} YAY' &\equiv (Q + zTS)A(Q' + zS'T') \equiv \\ &QAQ' + zQAS'T' + zTSAQ' + z^2TSAS'T' \equiv \\ &B - aTT' - ztaTT' - ztaTT' + z^2(a - t^2a)TT' \equiv \\ &B - aTT'(1 + 2zt - z^2 + z^2t^2) \equiv \\ &B - aTT'((zt + 1)^2 - z^2) \end{aligned} \tag{18}$$

The last term will be congruent to B (mod p^W) provided we can select

z so that $zt + 1 \equiv \pm z \pmod{p^w}$, or so that $z(t \pm 1) \equiv -1 \pmod{p^w}$. This can be accomplished if either $t + 1$ or $t - 1$ is a unit in $Z/(p^w)$, which is always the case when p is an odd prime. Hence $YAY' \equiv B$ and $f \sim g$ over $Z/(p^w)$ as we wished to show.

A similar proof yields

THEOREM 5 (Witt) If $f^* \sim g^*$ over a field F and $f^* \dot{+} f \sim g^* \dot{+} g$ over F, then $f \sim g$ over F, provided F is not a field of characteristic 2.

THE EQUIVALENCE OF FORMS OVER Z/(p)

Using theorems 1 and 3 and properties p1, p2 and p3 of the rings Z/(p) we will be able to find a complete set of invariants for the classification of forms over those rings when p is an odd prime.

Lemma $x^2 + y^2 \equiv a \not\equiv 0 \pmod{p}$ is always solvable in Z/(p) .

proof: When $p = 2$ the result is trivial. By p1 there are $(p-1)/2$ nonzero squares in $Z/(p)^+$ and hence $1+(p-1)/2$ squares in Z/(p). There are thus $1+(p-1)/2$ numbers of the form $a-x^2$ and at least one of them is a square.

Lemma Two binary forms $f = a_1x_1^2 + a_2x_2^2$ and $g = b_1y_1^2 + b_2y_2^2$ for which $d(f)d(g) \not\equiv 0 \pmod{p}$ are equivalent over Z/(p) provided p is an odd prime and

$$(19) \qquad \left(\frac{d(f)}{p}\right) = \left(\frac{d(g)}{p}\right)$$

proof: Case 1. $d(f) = -1$. Then $\left(\frac{a_1}{p}\right) = -\left(\frac{a_2}{p}\right)$ and similarly for the b_i. We can assume without loss of generality that $\left(\frac{a_1}{p}\right) = \left(\frac{b_1}{p}\right)$, for if not change the order of the y_i. By p2 we can find t_1 and t_2 such that $a_1t_1^2 \equiv b_1$ and $a_2t_2^2 \equiv b_2$. If

(20) $$T = \begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix}$$

then $TA(f)T' \equiv A(g) \pmod p$

Case 2. $d(f) = +1$. It will suffice to show that $f \sim x_1^2 + x_2^2$, for an identical argument would show $g \sim y_1^2 + y_2^2$. Since $(\frac{a_1}{p}) = (\frac{a_2}{p})$ we can find t such that $a_1 t^2 \equiv a_2$. Hence the change in variables $x_1 = ty_1$ and $x_2 = y_2$ yields $f \sim a_2(y_1^2 + y_2^2)$. By the previous lemma we can find t_1 and t_2 not both congruent to zero such that $a_2^{-1} \equiv t_1^2 + t_2^2$. Making the change of variables $2y_1 = t_1x_1 + t_2x_2$ and $2y_2 = t_1x_1 - t_2x_2$ yields $f \sim x_1^2 + x_2^2$.

THEOREM 6 Let f and g be two quadratic forms over $Z/(p)$ such that $d(f)d(g) \not\equiv 0 \pmod p$. If p is an odd prime, then $f \sim g$ if and only if both forms have the same number of variables and condition (19) holds.

proof: The necessity of the condition is immediate. For, if $TA(f)T' \equiv A(g)$, $(\det(T))^2 d(f) \equiv d(g)$ which, by p2 implies (19).

We use induction on the number of variables to show sufficiency. Again, there is no loss in generality if we assume f and g to be diagonal forms. If f and g are unary forms, the result follows from p2. If f and g are binary forms, use the previous lemma. If f and g are n-ary forms where $n \geq 3$, we can write $f = f_1 \dot{+} f_0$ and $g = g_1 \dot{+} g_0$ where f_0 and g_0 are equivalent binary forms. For, from among the diagonal coefficients of f there are at least two of the same quadratic residue class modulo p. Splitting these off to form f_0 we see that

(21) $$(\frac{d(f_0)}{p}) = +1.$$

Likewise we can find g_0 with the same relation holding. By the previous

lemma, $f_0 \sim g_0$. Since by the multiplicative property of the Legendre symbol, the conditions of the theorem still hold for f_1 and g_1, we may apply the inductive hypothesis to show that $f_1 \sim g_1$. It now follows as a consequence of theorem 3 that $f \sim g$.

According to the above theorem, the quadratic residue class of the determinant and the dimensionality of the form uniquely determine its equivalence class over the ring $Z/(p)$ when p is an odd prime and when also p does not divide the determinant of f.

The following theorem is also useful.

THEOREM 7 (The first lifting theorem) If $d(f)d(g) \not\equiv 0 \pmod{p}$ and $f \sim g$ over $Z/(p)$ where p is an odd prime, then $f \sim g$ over $Z/(p^w)$ for all $w \geq 1$.

proof: Assuming $f \sim g$ over $Z/(p^w)$ we shall prove $f \sim g$ over $Z/(p^{w+1})$. Let A and B be the matrix representations of f and g respectively. By the inductive hypothesis, the exists a matrix T invertible over $Z/(p^w)$ such that

$$TAT' \equiv B \pmod{p^w} \tag{22}$$

or,

$$TAT' \equiv B + p^w U \pmod{p^{w+1}} \tag{21}$$

where U is a symmetric matrix. Since $d(f) \not\equiv 0 \pmod{p}$, $\det A \not\equiv 0 \pmod{p}$. Hence A is invertible over $Z/(p^{w+1})$, and we denote its inverse in that ring by A^{-1}. Similarly, T is also invertible in $Z/(p^{w+1})$, and its inverse we also denote by T^{-1}.

Since p is an odd prime, 2 possesses an inverse. Let

$$S = T - \tfrac{1}{2}p^w U T'^{-1} A^{-1}. \tag{23}$$

Then

$$SAS' \equiv (T - \tfrac{1}{2} p^w UT'^{-1}A^{-1})A(T' - \tfrac{1}{2} p^w A^{-1}T^{-1}U \equiv \tag{24}$$
$$TAT' - \tfrac{1}{2} p^w UT'^{-1}A^{-1}AT' - \tfrac{1}{2}p^w TAA^{-1}T^{-1}U \equiv$$
$$TAT' - p^w U \equiv B \pmod{p^{w+1}}.$$

COMPLETE INVARIANTS FOR FORMS OVER $Z/(p^w)$

If f is a nonsingular diagonal form over $Z/(p^w)$ we can, by rearranging the variables of f, see that f is equivalent to the disjoint sum

$$\sum_{i=0}^{w-1} p^i f_i \tag{25}$$

where each of the f_i are diagonal forms, either null (that is, vacuous) forms, or with determinant prime to p. If a form f can be equivalenced to a form as in (25), we say that (25) is a proper decomposition of f over $Z/(p^w)$. The diagonalization theorem tells us that every nonsingular form f has a proper decomposition over $Z/(p^w)$ provided that p is an odd prime. Our next theorem tells us that this decomposition is essentially unique.

THEOREM 8 If f and h are two nonsingular forms over $Z/(p^w)$ where p is an odd prime, and they have the proper decompositions

$$f \sim \sum_{i=1}^{w-1} p^i f_i \quad \text{and} \quad h \sim \sum_{i=1}^{w-1} p^i h_i \quad \text{over } Z/(p^w) \tag{26}$$

then $f \sim g$ over $Z/(p^w)$ if and only if $f_i \sim h_i$ over $Z/(p)$ for every $i=0,1,\ldots,w-1$.

proof: The condition is sufficient. For, if $f_i \sim h_i$ over $Z/(p)$ are

nonsingular, the first lifting theorem tells us that $f_i \sim h_i$ over $Z/(p^w)$. Hence $p^i f_i \sim p^i h_i$ over $Z/(p^w)$, and this is also true if f_i and h_i are null forms. By theorem 3, $f \sim h$ over $Z/(p^w)$.

The condition is also necessary, and we shall show this by induction on w. For w=1, the theorem is true by the results obtained in the last section. Let us suppose the theorem tru for $1 \leq w < N$. Since $f \sim h$ over $Z/(p^N)$, $f \sim h$ over $Z/(p)$ and hence $f_0 \sim h_0$ over $Z/(p)$. By the lifting theorem, $f_0 \sim h_0$ over $Z/(p^N)$. By theorem 4, then,

$$(27) \qquad \sum_{i=1}^{N-1} p^i f_i \sim \sum_{i=1}^{N-1} p^i h_i \quad \text{over } Z/(p^N).$$

Rewriting, we find

$$(28) \qquad p \sum_{i=0}^{N-2} p^i f_{i+1} \sim p \sum_{i=0}^{N-2} p^i h_{i+1} \quad \text{over } Z/(p^N)$$

which implies

$$(29) \qquad \sum_{i=0}^{N-2} p^i f_{i+1} \sim \sum_{i=0}^{N-2} p^i h_{i+1} \quad \text{over } Z/(p^{N-1}).$$

Now both forms expressed in (29) are properly decomposed forms over $Z/(p^{N-1})$ and, applying the inductive hypothesis, we obtain

$$(30) \qquad f_i \sim h_i \quad \text{over } Z/(p) \text{ for } i=1,\ldots,N-1.$$

Since we have already shown $f_0 \sim h_0$ over $Z/(p)$ the theorem is true for all w. ¶ The next theorem is the second lifting theorem.

THEOREM 9 If $f \sim h$ over $Z/(p^u)$ where p^u does not divide d(f), and p is an odd prime, then $f \sim h$ over $Z/(p^w)$ for all $w \geq 1$.

proof: We need only consider $w > u$. Let

$$(31) \qquad f \sim f'' = \sum_{i=0}^{w-1} p^i f''_i, \text{ and } h \sim h'' = \sum_{i=0}^{w-1} p^i h''_i \text{ over } Z/(p^w)$$

where f'' and h'' are proper decompositions over $Z/(p^w)$. Now $d(f'') \equiv$

$t^2 d(f) \pmod{p^w}$ for some t prime to p. Thus p^u does not divide $d(f'')$ and hence all the f''_i for $i \geq u$ are null forms. Similarly for the h''_i, $i \geq u$. Hence,

$$(32) \qquad f \sim f' = \sum_{i=0}^{u-1} p^i f''_i \text{ , and } h \sim h' = \sum_{i=0}^{u-1} p^i h''_i \text{ over } Z/(p^w).$$

In particular, (32) also holds over the ring $Z/(p^u)$. But $f \sim h$ over $Z/(p^u)$. Hence $f''_i \sim h''_i$ over $Z/(p)$ for $i \leq u-1$ and also for $i \geq u$. By the previous theorem, $f \sim h$ over $Z/(p^w)$.

Combining results, we can state:

For any integral quadratic form f, let $c(f,i)$, $u(f,i)$, $r(f,i)$, and $w(f)$ $i=1,\ldots,N$ be numbers such that

d1 $f \sim \sum_{i=1}^{N} p^{u(f,i)} f_i$ over $Z/(p^w)$, $u(f,i) \neq u(f,j)$ only if $i=j$

d2 p^{w-1} is the highest power of p dividing $d(f) \neq 0$, and

d3 $r(f,i)$ is the rank of f_i, $c(f,i) = \left(\frac{d(f_i)}{p}\right)$ with $d(f_i) \not\equiv 0 \pmod{p}$.

Then

r1 such numbers exist for every nonsingular f,

r2 they are uniquely determined by the genus of f, and

r3 f v g only if $w(f) = w(g)$, $c(f,i) = c(g,i)$, $r(f,i) = r(g,i)$ and $u(f,i) = u(g,i)$ for $i=1,2,3, \ldots$

The above numbers are called the p-adic invariants of f. Note also that the numbers are explicitly calculable. Hence, the classification of nonsingular forms over the rings $Z/(p^u)$ for all odd primes p and all $u \geq 1$ is completely solved.

CONCLUSION

Two more theorems will round off our results.

THEOREM 10 If f v g, d(f) = d(g).

proof: If d(f) = 0 then d(g) = 0. For otherwise, we can find an integer m prime to d(g), and hence $f \sim g$ over Z/(m) which implies $t^2 d(f) \equiv d(g) \not\equiv 0 \pmod{m}$, a contradiction. We can now assume that d(f) and d(g) are both nonzero. Thus, $f \sim g$ over Z/(d(g)) and d(g) divides d(f). Similarly, d(f) divides d(g) and so d(f) = d(g).

We state without proof

THEOREM 11 If f v g, the signature of f equals the signature of g.

The signature of a form is defined as the number of positive terms minus the number of negative terms in the diagonal of any equivalent diagonal form. Two forms are equivalent over the reals if and only if their ranks and signatures agree. The proof is similar to the proofs of the previous section, and does not bear repeating.

DESCRIPTION OF PROGRAM

The design of the program is straight forward. The overall organization is as follows.

Operation begins in MAIN, which calls subroutine DATA. DATA reads the Murasugi matrix calculated in Lombardero's program [4], and returns its symmetrization in integer A and real*8 E. A call to subroutine MATEVL places the eigenvalues of E in its diagonal, from which MAIN computes the determinant and the signature of A. (MATEVL is a subroutine available in MATPAK, a matrix package, to users of the Princeton University computer center.) The integer matrix A, its rank N and de-

terminant D are passed to subroutine CALCUL, provided that A is neither singular nor unimodular. CALCUL calls subroutine FACTOR, which factors D into its prime divisors, stored in incresing order. For each odd prime divisor, p, of D, CALCUL reduces A to diagonal form (mod p^w) where p^{w-1} is the highest power of p dividing D. This it accomplishes through the auxilliary subroutines POWER, ADD, TRANS and function INV according to the algorithm outlined in THEOREM 1. ADD adds a given row and column to another row and column, while TRANS exchanges a given row and column for another. POWER finds the matrix element a_{ij} described in steps (ii) through (iv) and the power p^u of p described in step (i). The equation

(33) $$-ra_{nn} + a_{ni} \equiv 0 \pmod{p^w}$$

is solved as follows: Suppose p^u to be the highest power of p dividing a_{nn}. Then p^u divides a_{ni}. We solve

(34) $$-r(a_{nn}/p^u) + (a_{ni}/p^u) \equiv 0 \pmod{p^{w-u}}$$

by setting $r = (a_{ni}/p^u)(a_{nn}/p^u)^{-1}$ where the inverse is taken over the residue ring $Z/(p^{w-u})$. r solving (34) also solves (33). Function INV first calculates the inverse in the ring Z/(p) and then lifts to the ring $Z/(p^{w-u})$.

After A has been diagonalized, A, p, w, N and D are passed to subroutine INVAR which calculates the numbers c(f,i), u(f,i), r(f,i) and w(f) according to the scheme outlined in the section before the last. These are stored in matrix NUM. Subroutine CHAR(a,p) computes $(\frac{a}{p})$ using the formula

THEOREM 12 $a^{(p-1)/2} \equiv (\frac{a}{p}) \pmod{p}$.

proof: $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ since $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1$. If $a = t^2$, $a^{(p-1)/2} \equiv 1$, by the same reasoning. $x^{(p-1)/2} \equiv 1$ can have at most $(p-1)/2$ solution , which we have shown to be the $(p-1)/2$ squares. Hence if a is not a square, $a^{(p-1)/2} \equiv -1$.

After INVAR has computed the above p-adic invariants, control passes to subroutine CHECK whech tests for internal constraints on the invariants. They must satisfy the relations:

$$\text{(35)} \qquad \sum_{i=0}^{M} u(f,i)r(f,i) = w-1$$

$$\text{(36)} \qquad \sum_{i=0}^{M} r(f,i) = N$$

$$\text{(37)} \qquad \prod_{i=0}^{M} \left(\frac{d(f,i)}{p}\right) = \left(\frac{d(f)}{p}\right)$$

If these relations are not satisfied, an error message will be printed. If they do, control returns to MAIN via INVAR and CALCUL.

MAIN coordinates all the outputting.

FOOTNOTES

[1] A knot K is an embedding of S^1 in R^3. K and K' are said to be of the same type if there is an orientation preserving homoeomorphism of R^3 that maps R^3 - K into R^3 - K'. A link of m components is an embedding of m copies of S^1 into R^3.

[2] As reported to me by H. Trotter. The Murasugi matrix is defined in [4].

[3] This is not the usual definition of semiequivalence, but can be shown to be equivalent to any of the other definitions. In particular, we shall later show that condition (ii) implies d(f) = d(g).

[4] The Chinese remainder theorem states that if m_i, i=1,...,n are all relatively prime, $a_i \in Z$ for i=1,...,n arbitrary values, then the system of equations

$$x \equiv a_i \pmod{m_i} \quad i=1,\ldots,n$$

are simultaneously solvable for $x \in Z$. Thus to show that $f \sim g$ over Z/(m) we need only show $f \sim g$ over $Z/(p_i^{a(i)})$ where

$$m = \prod_{i=1}^{n} p_i^{a(i)}.$$

[5] A nice proof is found in [3].

BIBLIOGRAPHY

[1] R. H. Fox, Introduction to Knot Theory, New York, Blaisdell Publishing Company, 1963.

[2] B. W. Jones, The Arithmetic Theory of Quadratic Forms, Math. Assoc. Amer., 1967.

[3] R. H. Kyle,"Branched covering spaces and the quadratic forms of links," I, Ann. of Math., 59 (1954), 539-548.

[4] D. A. Lombardero, 'Machine calculation of the Murasugi matrix and related link invariants," Princeton University senior thesis, unpublished, 1968.

[5] H. F. Trotter, 'Homology of group systems with applications to knot theory," Ann. of Math., 76 (1962), 464-497.

[6] G. L. Watson, Integral Quadratic Forms, Cambridge, Cambridge University Press, 1960.

[7] G. H. Hardy, and E. M. Wright, An Introduction to the Theory of Numbers, Oxford, Clarendon Press, 1965.

A proposed measure of association

I Definition of the Uncertainty Function

Let A be a partition of the population P into n disjoint categories, A_i, i = 1, 2, . . ., n. Let $p_{A,i}$ denote the probability that a member of P will belong to the category A_i. Since A is a partition we require that:

$$(1) \qquad \sum_{i=1}^{n} p_{A,i} = 1 \quad .$$

Any finite-valued variable on P may be considered to be a partition of P into its disjoint value classes, and we will use the notion of a finite-valued variable interchangeably with with the notion of a finite partition.

For any partition A of a population P we may define the uncertainty of A in P by

$$(2) \qquad U(A,P) = - \sum_{i=1}^{n} p_{A,i} \log p_{A,i}$$

where the A_i and the $p_{A,i}$ are as before. From the definition it should be clear that the uncertainty of any partition is nonnegative. It can also be proven (by use of Lagrange multipliers) that the uncertainty of any n-partition (or n-valued variable) is greatest when all the categories are of equal probability, i.e.:

$$(3) \qquad p_{A,i} = 1/n \qquad \text{for all } i,$$

in which case the uncertainty will have the value log n. It can also be seen that the uncertainty has a value of zero, and hence a minimum, if the partition is a trivial partition, all the population belonging to one category.

II Joint Partitions and Joint Uncertainty

If B is another partition of P, into the disjoint categories B_j j = 1, 2, . . ., m and with associated probabilities $p_{B,j}$, then A and B together form a joint partition of P into n x m disjoint categories $A \times B_{i,j}$ i = 1, 2, . . ., n and j = 1, 2, . . ., m which we will denote by A x B. We can thus define the joint uncertainty of A and B by

$$(4) \qquad U(A \times B, P) = - \sum_{i=1}^{n} \sum_{j=1}^{m} p_{i,j} \log p_{i,j}$$

where $p_{i,j}$ is the probability associated with the category $A \times B_{i,j}$. If A and B are independent partitions, that is

(5) $$p_{i,j} = p_{A,i} \times p_{B,j} ,$$

then $U(A \times B, P) = U(A,P) + U(B,P)$. It is this property of the uncertainty function that justifies its definition. For, if the partitions A and B are independent then the sum of their uncertainties should just equal their joint uncertainty, seeing that knowledge of both A and B suffice to determine their joint outcome.

It can be shown analytically that given the constraints that A and B are fixed, the uncertainty $U(A \times B, P)$ is greatest when A and B are independent partitions.

III Conditional Uncertainty

We might ask what is the uncertainty in B if A is known, or, more precisely, what is the probable uncertainty in B if we know A. To answer this question requires knowledge of A x B and we define

(6) $$U(B/A,P) = \sum_{i=1}^{n} p_{A,i} \times U(B,A_i)$$

to be the conditional uncertainty of B given A. It corresponds to the probable uncertainty in B given the A category of some member of the population. (6) can be rewritten

(7) $$U(B/A,P) = \sum_{i=1}^{n} p_{A,i} \times \left(- \sum_{j=1}^{m} (p_{i,j}/p_{A,i}) \log (p_{i,j}/p_{A,i})\right)$$

from which it follows that

(8) $$U(B/A,P) = U(A \times B, P) - U(A,P) .$$

As we indicated earlier,

(9) $$U(A,P) + U(B,P) - U(A \times B, P) = 0$$

if and only if A and B are independent. Hence,

(10) $$U(B,P) - U(B/A,P) = 0$$

if and only if A and B are independent. Othertimes, the left hand side of (10) is positive. Moreover, $U(B/A,P) = U(B)$ if and only if knowledge of A completely specifies B. This suggests . . .

IV A Proposed Measure of Association

$\frac{U(A)+U(B)-U(M)}{U(B)}$

I propose

$$z = (U(B,P) - U(B/A,P)/U(B,P)$$

as a new measure of association between independent variable A and dependent variable B. It can be shown that z has the following properties:

(i) z is indeterminate iff* A is a trivial partition

(ii) the value of z lies between 0 and 1

(iii) z = 0 iff A and B are independent partitions

(iv) z = 1 iff A determines B

(v) z is order independent

Intuitive content of the z measure is this: it measures the extent knowledge of A helps in predicting determines B, or the extent that A fixes B. A high z value means that A has a high predictive value in relation to B.

V Some Additional Problems

It is clearly necessary to have some kind of measure of the significance of z, for even low z scores might be noteworthy if they are significantly larger than 0. Also, a significance level would indicate the reliability of predictions made from A.

A more mathematical problem is this: given the marginal partitions A and B what is the largest value of z possible among all possible distributions between A and B? I have suggested an algorithm for finding this value, but I won't describe it here. The result is this: If variable A has a similar distribution to B, there is a larger span of possible z values (a broader spectrum).

Michael Wigler

Michael Wigler

December 18, 1969

* 'iff' means 'if and only if'