A THEOREM ON QUADRATIC FORMS OVER THE RING OF 2-ADIC INTEGERS

BURTON W. JONES AND WILLIAM H. DURFEE

1. Introduction. The theory of the equivalence of quadratic forms over the ring of 2-adic integers is considerably more difficult than the corresponding theory for forms over the \( p \)-adic integers, \( p \) an odd prime, and has only recently been worked out to a comparable degree. A problem still not completely solved is Witt's cancellation theorem: namely, if \( f, g \) and \( h \) are forms such that \( g \) and \( h \) have no variables in common with \( f \), then \( f + g \) equivalent to \( f + h \) implies \( g \) equivalent to \( h \). This theorem, though true for \( p \)-adic integers when \( p \) is odd, does not always hold when \( p \) is even. We give here a case when it does hold (see theorem below). While this theorem follows almost immediately from results in a paper by Jones [1, Theorems 2 and 6] it seems worthwhile in view of the rather long arguments of the theorems there to give an independent proof, especially since it in turn can be used to shorten some of the proofs of that paper.

2. Proof of the theorem. We denote by capital italic letters matrices over \( \mathbb{R}(2) \), the ring of 2-adic integers, while small italic letters with the exception of \( f, g \) and \( h \) will stand for numbers in \( \mathbb{R}(2) \). We shall consider only forms whose symmetric matrices have elements in \( \mathbb{R}(2) \). A matrix is unimodular if its elements are in \( \mathbb{R}(2) \) and its determinant a unit of \( \mathbb{R}(2) \). A form is called unimodular if its symmetric matrix is unimodular.

**Theorem.** Let \( f_1 \) and \( f_2 \) be two equivalent unimodular forms over \( \mathbb{R}(2) \) in \( x_1, x_2, \ldots, x_n \), \( g \) a nonsingular form over \( \mathbb{R}(2) \) in \( x_{n+1}, x_{n+2}, \ldots, x_{n+s} \) and \( h \) a nonsingular form over \( \mathbb{R}(2) \) in \( x_{n+1}, x_{n+2}, \ldots, x_{n+t} \). If there is a matrix over \( \mathbb{R}(2) \) taking \( f_1 + 2g \) into \( f_2 + 2h \), then there is one over \( \mathbb{R}(2) \) taking \( g \) into \( h \); if \( s = t \) and the former matrix is unimodular, then so is the latter.

**Proof.** Since \( f_1 \) and \( f_2 \) are equivalent we may take \( f_1 + 2g \) into \( f_2 + 2g \) by a unimodular transformation and thus we set \( f_1 = f_2 = f \). By [1, Lemma 1] \( f \) is equivalent to either a diagonal form or a sum of binary forms. If the latter is the case, then \( x^2 + f \) will be equivalent to...
a diagonal form and since \( x^2 + f + 2g \) is equivalent to \( x^2 + f + 2h \) we shall assume that \( f \) is a unimodular diagonal form. Let \( f, g \) and \( h \) have respectively \( F, G \) and \( H \) as their symmetric matrices over \( R(2) \) and let \( Q \) be the \( n+s \) by \( n+t \) matrix taking \( F+2G \) into \( F+2H \), where \( + \) denotes direct sum, that is,

\[
F + 2G = \begin{pmatrix} F & 0 \\ 0 & 2G \end{pmatrix}.
\]

Set

\[
Q = \begin{pmatrix} T & S_2 \\ S_3 & S_4 \end{pmatrix},
\]

where \( T \) is an \( n \) by \( n \) matrix, \( S_2 \) is \( n \) by \( t \), \( S_3 \) is \( s \) by \( n \) and \( S_4 \) is \( s \) by \( t \). Then \( Q'(F+2G)Q = F+2H \) yields the following equations:

\[
\begin{align*}
(1) & \quad T'FT + S_2'2GS_2 = F, \\
(2) & \quad T'FS_2 + S_4'2GS_4 = 0, \\
(3) & \quad S_2'FS_2 + S_4'2GS_4 = 2H.
\end{align*}
\]

We show in the following lemma that, since equation (1) implies \( T'FT \equiv F \) (mod 2), there is an automorph \( D \) of \( F \) over \( R(2) \) such that \( 2(T+D)^{-1} \) is in \( R(2) \). (An automorph of \( F \) is a matrix \( D \) such that \( D'FD = F \).) Furthermore equation (2) and the fact that \( T'F \) is a unit implies that \( S_2 \equiv 0 \) (mod 2) and hence that

\[
S = S_4 - S_3(T + D)^{-1}S_2
\]

has its elements in \( R(2) \). We shall show that \( S'2GS = 2H \). Now

\[
S'2GS = [S_4' - S_3' (T + D)^{-1}S_2']2G[S_4 - S_3(T + D)^{-1}S_2]
= S_4'2GS_4 - S_3' (T + D)^{-1}S_2' 2GS_4 - S_4'2GS_3(T + D)^{-1}S_2
+ S_4' (T + D)^{-1}S_4' 2GS_3(T + D)^{-1}S_2.
\]

Using (1) we have

\[
S_4' (T + D)^{-1}S_4' 2GS_3(T + D)^{-1}S_2
= S_4' (T + D)^{-1}[F - T'FT](T + D)^{-1}S_2.
\]

Since \( F - T'FT = (D+T)'F(D+T) - T'F(D+T) - (T+D)'FT \), the right side of (4) equals

\[
S_4'FS_2 - S_3' (T + D)^{-1}T'FS_2 - S_4'FT(T + D)^{-1}S_2,
\]

which, using (2), becomes

\[
S_4'FS_2 + S_3' (T + D)^{-1}S_4' 2GS_4 + S_4'2GS_3(T + D)^{-1}S_2.
\]
Hence \( S'2GS = S'_i2GS_i + S'_jFS_j = 2H \) from equation (3).

If \( s = t \) and \( Q \) is unimodular, we have not only \( S'GS = H \), but also by symmetry \( S^*HS^* = G \) for some \( s \) by \( s \) matrix \( S^* \) over \( R(2) \). By substitution we see that, since \( |G| \) is not zero, \( |S| \) is a unit and \( S \) is unimodular. The condition that \( g \) and \( h \) be nonsingular is not essential, as it can be shown with little difficulty that the theorem is still true without this restriction.

We now prove the basic lemma.

**Lemma.** If \( F \) is a unimodular diagonal matrix over \( R(2) \) and \( T \) a matrix over \( R(2) \) such that \( T'T^F \equiv F \) (mod 2), then there is an automorph \( D \) of \( F \) over \( R(2) \) such that \( 2(T + D)^{-1} \) is in \( R(2) \).

**Proof.** Let \( T = (t_{ij}), i, j = 1, 2, \ldots, n \) and \( F = a_1 + a_2 + \cdots + a_n \). Since permuting the rows and the same columns of \( T \) and \( F \) does not alter the properties we desire, we shall do this at will. Note that \( T'T \equiv I \) (mod 2).

First, suppose that \( t_{ii} \) is a non-unit for some \( i \). Permute rows and columns, if necessary, to make \( t_{ii} \) a non-unit, choose \( D = 1 + D_1 \) and set \( u = t_{ii} + 1 \), which will be a unit. If we set

\[
P = \begin{pmatrix} 1 & -u^{-1}T_2 \\ 0 & I \end{pmatrix}
\quad \text{and} \quad T = \begin{pmatrix} t_{11} & T_2 \\ T_3 & T_4 \end{pmatrix},
\]

where \( T_2 \) is a 1 by \( n - 1 \) matrix, \( T_3 \) is \( n - 1 \) by 1 and \( T_4 \) is \( n - 1 \) by \( n - 1 \), we have

\[
(T + D)P = \begin{pmatrix} t_{11} + 1 & 0 \\ T_3 & T_1 + D_1 \end{pmatrix},
\]

where \( T_1 = T_4 - T_3u^{-1}T_2 \) and \( D_1 \) is to be chosen an automorph of \( F_1 = a_2 + a_3 + \cdots + a_n \). By adding appropriate multiples of the first row of (5) to the later rows we can replace \( T_3 \) by 0 without altering \( T_1 + D_1 \). Referring now to the proof of the theorem and there replacing \( T, S_2, S_3, S_4 \) by \( t_{ii}, T_2, T_3, T_4 \), respectively, we see that \( T'T \equiv I \) (mod 2) implies that \( T'_1T'_3 \equiv I \) (mod 2).

Secondly, suppose that \( t_{ii} \) is a unit for every \( i \) and \( t_{ij} \) is a unit for some \( i \) and \( j \), \( i \neq j \). Permute rows and columns, if necessary, to make \( t_{ii} \) a unit, and choose \( D = I_2 + D_2 \), where \( I_2 \) is the 2 by 2 identity matrix. Then

\[
U = \begin{pmatrix} t_{11} + 1 & t_{12} \\ t_{21} & t_{22} + 1 \end{pmatrix}
\]
is unimodular and if we set
\[ P = \begin{pmatrix} I_2 & -U^{-1}T_2 \\ 0 & I \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} T_0 & T_2 \\ T_3 & T_4 \end{pmatrix}, \]
where \( T_0 \) is a 2 by 2 matrix, \( T_2 \) is 2 by \( n-2 \), and so on, we have
\[ (T + D)P = \begin{pmatrix} T_0 + I_2 & 0 \\ T_3 & T_1 + D_2 \end{pmatrix}, \]
where \( T_1 = T_4 - T_3 U^{-1}T_2 \) and \( D_2 \) is to be chosen an automorph of \( F_2 = \alpha_3 + \alpha_4 + \cdots + \alpha_n \). As in the preceding case we can replace \( T_3 \) by 0 and have \( T_1' T_1 \equiv I \pmod{2} \).

Thirdly, suppose \( T \) has the property that \( t_{ii} \) is a unit for every \( i \), \( t_{ij} \) is a unit for some \( i \neq j \) and \( t_{ij} t_{ij} \) is a non-unit for every \( i \neq j \). Now \( T' T \equiv I \pmod{2} \) implies that each row and column of \( T \) contains an odd number of units and that for each \( i \) and \( j, i \neq j \), there is an even number of values of \( k \) such that \( t_{ik} t_{jk} \equiv 1 \pmod{2} \). Thus by a permutation of rows and columns we may assume the leading 3 by 3 minor of \( T \) to be congruent (mod 2) to
\[ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \]

Furthermore, two of the first three diagonal elements of \( F \) are congruent (mod 4) and by a permutation of rows and columns of \( F \) and \( T \) we may assume that \( \alpha_1 \) and \( \alpha_2 \) are congruent (mod 4), that \( t_{11} t_{12} t_{22} \) is a unit and \( t_{21} \) a non-unit. We can complete the proof along the lines of the previous case if we can find an automorph \( D_0 \) of \( \alpha_1 x_1^2 + \alpha_2 x_2^2 \), where
\[ D_0 \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2}, \]

since then
\[ U = D_0 + \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \]
will be unimodular. Suitable matrices \( D_0 \) are
\[ \begin{pmatrix} 0 & \sigma^{-1} \\ \sigma & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 3 \sigma^{-1} \\ \sigma & 2 \end{pmatrix}. \]
according as \( \alpha_1 \equiv \alpha_2 \) (mod 8) or \(-3\alpha_1 \equiv \alpha_2 \) (mod 8), where \( \sigma \) and \( \tau \) are \( p \)-adic units satisfying the equations \( \alpha_1 = \alpha_2 \sigma^2 \), \(-3\alpha_1 = \alpha_2 \tau^2 \).

Finally, suppose \( T \equiv I \) (mod 2). Choose \( \lambda_1 = \pm 1 \) so that \( t_{11} + \lambda_1 \) is twice a unit and set \( D = \lambda_1 + D_1 \). By adding appropriate multiples of the first column of \( T + D \) to the other columns and then similarly for rows we can reduce the first row and column of \( T + D \) to \( (t_{11} + \lambda_1, 0, \cdots, 0) \). The remaining elements still will have the property that those on the diagonal are units and the non-diagonal elements are non-units.

By continuing the above reductive process we can reduce \( T + D \) to a direct sum of matrices \( T_i + D_i \), where each \( T_i + D_i \) is one of three types: a unit, twice a unit, or a 2 by 2 unimodular matrix. Hence \( 2(T + D)^{-1} \) will be in \( R(2) \).

BIBLIOGRAPHY


CORNELL UNIVERSITY AND
DARTMOUTH COLLEGE