Research Article

Classifying Quadratic Forms Over $\mathbb{Z}_2$ in Three Variables

Gerard Thompson

Department of Mathematics, University of Toledo, Toledo, OH 43606, USA

Correspondence should be addressed to Gerard Thompson; gerard.thompson@utoledo.edu

Received 30 June 2016; Accepted 14 November 2016

Academic Editor: Fernando Torres

Copyright © 2016 Gerard Thompson. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The quadratic forms in three variables over the field $\mathbb{Z}_2$ are classified. Some remarks are made about the group of equivalences $GL(3, \mathbb{Z}_2)$ of the quadratic forms.

1. Introduction

By a *quadratic form*, we understand a homogeneous quadratic polynomial in n variables $\sum_{i,j} a_{ij}x^i x^j$ where the a_{ij} belong to a field or at least a commutative ring. In this article, we shall consider the equivalence of quadratic forms in three variables over the field $\mathbb{Z}_2$. As our references suggest, the study of quadratic forms over finite fields lies at the nexus of several areas of mathematics, combinatorics, cryptography, and the theory of algebraic curves, to name but three of them.

The standard approach to classifying quadratic forms over $\mathbb{R}$ associates to each quadratic form a symmetric matrix A so that the quadratic form is $x^t A x$. Under a change of variables, the matrix A changes according to $P^t A P$ where P is nonsingular. Such a change does not preserve the eigenvalues of A . The only invariants are the *signs* of the eigenvalues; as such, every matrix A may be reduced to a diagonal matrix in which every entry is 1, -1 , or 0. The number of nonzero diagonal entries is the *rank* of the quadratic form; one can also sensibly define the *signature* of the quadratic form to be the difference between the number of positive and number of negative entries when A has been diagonalized. Conventions vary in these definitions. Another approach is simply to repeatedly “complete the square” so as to reduce the quadratic form to diagonal form. Over $\mathbb{C}$, the situation is different; that is, if the matrix P is allowed to belong to $GL(n, \mathbb{C})$ rather than $GL(n, \mathbb{R})$, the distinction between positive and negative eigenvalues disappears and a quadratic form may always be reduced to diagonal form in which every nonzero entry is $+1$. Finally, if the matrix P is orthogonal then the eigenvalues of A

are preserved and one obtains the finite-dimensional spectral theorem: for further details see [1].

It is not possible to associate a symmetric matrix to a quadratic form when the field is $\mathbb{Z}_2$ since the cross terms would be all be zero. Instead, one could work simply with an upper triangular matrix. For background material about quadratic forms, we refer to [1, 2] and a much more recent account in [3]. For more theoretical considerations, we refer to [4] and references therein. In [5], the radical (maximal isotropic subspace) of a certain class of quadratic forms over fields of characteristic 2 is determined. In [6], among other things, the author studies the zeros of a quadratic form. Yet another direction [7] concerns pencils of quadratic forms over finite fields.

2. Group of Equivalences

The group of equivalences under which a quadratic form can be changed is $GL(3, \mathbb{Z}_2)$. It is a group of order 168: the first row is arbitrary except that it must not consist of all zeros giving seven choices; there are six possibilities for the second row and four for the third since it cannot be a sum modulo 2 of the first two rows. It is easy to see that every element $g \in GL(3, \mathbb{Z}_2)$ satisfies $g^7 = I$; where I is the 3×3 identity matrix by using the Hamilton-Cayley theorem: in fact, there are only four inequivalent characteristic polynomials. A Sylow 7-group is generated by the matrix $T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ but the subgroup is not normal. Hence, by Sylow's Theorem there must be 8 Sylow 7-groups and 48 elements of order 7.

The “Heisenberg” upper triangular unipotent matrices form a Sylow 2-subgroup of order 8 as do the corresponding lower triangular unipotent matrices; hence, neither is normal and the number of Sylow 2-subgroups k_2 can be either 3, 7, or 21. Each of these subgroups is not abelian and has at least two elements of order 2 and therefore the Sylow 2-subgroups must each be isomorphic to the dihedral group D_8 of order 8.

The sets of matrices of the form $\begin{bmatrix} 1 & 0 & 0 \\ x & 1 & y \\ z & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & x & z \\ 0 & 1 & 0 \\ 0 & y & 1 \end{bmatrix}$ comprise two more Sylow 2-subgroups and so $k_2 = 7$ or 21. In fact, it may be shown that $k_2 = 21$. For many more details, we refer to [8] which is, in effect, an entire course about the simple group of order 168 and is based almost entirely on the Sylow Theorem.

As regards the Sylow 3-subgroups we must have $k_3 = 1, 4, 7$, or 28. The group generated by $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ generates a non-normal subgroup of order three so $k_3 \neq 1$. In fact it turns out that $k_3 = 28$.

Actually, group $GL(3, \mathbb{Z}_2)$ is isomorphic to the unique simple group of order 168, the smallest order simple group after A_5 apart from the cyclic groups of prime order.

The 3×3 orthogonal group over $\mathbb{Z}_2$ is the trivial group since if the first row of a matrix P consists of 1's the other diagonal entries of PP^t will be zero.

3. Preliminary Reduction

There are, in principle, 64 quadratic forms but some are equivalent by transformations from the symmetric group S_3 . There are 8 forms that have no square terms so by symmetry such forms can be reduced to

$$xy, xy + xz, xy + xz + zx. \quad (1)$$

Similarly there are 8 forms that contain $x^2 + y^2 + z^2$ and they can be reduced to

$$\begin{aligned} x^2 + y^2 + z^2, x^2 + y^2 + z^2 + xy, x^2 + y^2 + z^2 + xy \\ + xz, x^2 + y^2 + z^2 + xy + xz + zx. \end{aligned} \quad (2)$$

There are 24 forms that contain one square and another 24 that contain two squares and these forms may be reduced to

$$\begin{aligned} x^2, x^2 + xy, x^2 + xz, x^2 + yz, x^2 + xy + xz, x^2 + xy \\ + yz, x^2 + xz + yz, x^2 + xy + yz + zx, \end{aligned} \quad (3)$$

$$\begin{aligned} x^2 + y^2, x^2 + y^2 + xz, x^2 + y^2 + yz, x^2 + y^2 + xy, x^2 \\ + y^2 + xy + xz, x^2 + y^2 + xy + yz, x^2 + y^2 + xz \\ + yz, x^2 + y^2 + xy + yz + zx, \end{aligned} \quad (4)$$

respectively. We note further that in (3) the second and third forms and the sixth and seventh are equivalent, respectively, by interchanging y and z , whereas in (4) the second and third and fifth and sixth forms are equivalent, respectively, by interchanging x and y . As such we have now reduced the original list of 64 forms to the following 20:

$$\begin{aligned} x^2 + y^2 + z^2, x^2 + y^2 + z^2 + xy, x^2 + y^2 + z^2 + xy + \\ xz, x^2 + y^2 + z^2 + xy + xz + zx \\ x^2 + y^2, x^2 + y^2 + xz, x^2 + y^2 + xy, x^2 + y^2 + xy + \\ xz, x^2 + y^2 + xz + yz, x^2 + y^2 + xy + yz + zx \\ x^2, x^2 + xy, x^2 + yz, x^2 + xy + xz, x^2 + xy + yz, x^2 + \\ xy + yz + zx \\ 0, xy, xy + xz, xy + xz + zx. \end{aligned}$$

4. Reduction to Canonical Form

Now we shall explain how the 20 forms given at the end of the previous section may be further reduced to just five canonical forms. We shall denote equivalence of forms by $\sim$ and in each case we give the accompanying transformation unless it is merely a permutation:

- (1) $x^2 + y^2 + z^2 \sim x^2 (x = X + Y, y = Y + Z, z = Z)$
- (2) $x^2 + y^2 + z^2 + xy \sim xy + z^2 (x = X, y = X + Y, z = X + Y + Z) \sim x^2 + yz$
- (3) $x^2 + y^2 + z^2 + xy + xz \sim x^2 + xz + z^2 (x = X, y = X + Y, z = X + Y + Z) \sim x^2 + xy + y^2$
- (4) $x^2 + y^2 + z^2 + xy + xy + xz \sim y^2 + yz + z^2 (x = X, y = X + Y, z = X + Y + Z) \sim x^2 + xy + y^2$
- (5) $x^2 + y^2 \sim x^2 (x = X + Y + Z, y = Y + Z, z = Z)$
- (6) $x^2 + y^2 + xz \sim y^2 + xz (x = X, y = X + Y, z = Z) z \sim x^2 + yz$
- (7) $x^2 + y^2 + xy$ canonical form
- (8) $x^2 + y^2 + xy + xz \sim y^2 + xz (x = Z, y = Y + Z, z = X + Y + Z) \sim x^2 + yz$
- (9) $x^2 + y^2 + xz + yz \sim xy (x = Z, y = Y + Z, z = X + Y)$
- (10) $x^2 + y^2 + xy + yz + zx \sim xy + z^2 (x = Z, y = Y + Z, z = X + Y + Z)$
- (11) x^2 canonical form
- (12) $x^2 + xy \sim yz (x = Z, y = Y + Z, z = X + Y + Z) \sim xy$
- (13) $x^2 + yz$ canonical form
- (14) $x^2 + xy + xz \sim xz (x = Z, y = Y + Z, z = X + Y) \sim xy$
- (15) $x^2 + xy + yz \sim x^2 + yz (x = X + Z, y = Y + Z, z = X)$
- (16) $x^2 + xy + yz + zx \sim xy (x = Z, y = Y + Z, z = X + Z)$
- (17) 0 canonical form
- (18) xy canonical form
- (19) $xy + xz \sim xy (x = Y, y = Y + Z, z = X + Y + Z)$
- (20) $xy + xz + zx \sim xy + z^2 (x = X + Z, y = Y + Z, z = Z) \sim x^2 + yz$.

5. The Canonical Forms

In this section, we shall justify the fact that the five canonical forms are mutually inequivalent. Clearly 0 is only equivalent to itself. Next, under a general transformation x^2 can change

only to $ax^2 + by^2 + cz^2$ and so it can only be equivalent to $x^2 + y^2$ and $x^2 + y^2 + z^2$, allowing for symmetry.

Next, we consider xy . Under a general nonsingular transformation

$$\begin{aligned}x &= aX + bY + cZ, \\y &= dX + eY + fZ, \\z &= gX + hY + iZ,\end{aligned}\tag{5}$$

xy is transformed to

$$\begin{aligned}adX^2 + (bd + ae)XY + (cd + af)ZX + beY^2 \\+ (bf + ce)ZY + cfZ^2.\end{aligned}\tag{6}$$

If xy were equivalent to $x^2 + yz$ then we would have $ad = 1$ and hence $a = d = 1$. Since the terms in zx and z^2 are absent we can only have $c = f = 0$ but then the coefficient of yz must be zero and hence xy is not equivalent to $x^2 + yz$.

Next we suppose that xy is equivalent to $x^2 + xy + y^2$. This time we find that $ad = bd + ae = be = 1$; however, these conditions are self-contradictory since we would have that $a = b = d = e = 1$ so that $bd + ae = 0$. Thus, xy is not equivalent to any of the other canonical forms.

Finally, we show that $x^2 + yz$ is not equivalent to $x^2 + xy + y^2$. In fact, under (5) the form $x^2 + yz$ transforms to

$$\begin{aligned}(a^2 + dg)X^2 + (eg + dh)XY + (fg + di)ZX \\+ (eh + b^2)Y^2 + (fh + ei)ZY + (c^2 + fi)Z^2.\end{aligned}\tag{7}$$

We consider a number of cases. Suppose first of all that $b = e = 1$. Then, $h = 0$, $g = 1$, $i = 0$, and $c = f = 0$ so that the transformation is singular. In the second case, suppose that $b = h = 1$. Then, we must have that $c = e = f = 0$ and $d = 1$; however, it then follows that $i = 0$ and again the transformation is singular. The last possibility starting from the Y^2 term in (7) is that $b = 0$ and $e = h = 1$. Then, we must have that $e = g = 1$ and $c = f = i = 0$ and again the transformation is singular.

Theorem 1. Over $\mathbb{Z}_2$ every quadratic form in three variables is equivalent to precisely one of $0, xy, x^2, x^2 + yz, x^2 + y^2 + xy$.

Competing Interests

The author hereby declares that there is no financial or other conflict of interests with regard to the dissemination of this paper.

Acknowledgments

The author thanks Akaki Tikaradze for helpful discussions.

References

- [1] J. W. Cassels, *Rational Quadratic Forms*, vol. 13 of *London Mathematical Society Monographs*, Academic Press, London, UK, 1978.

- [2] P. J. Cameron and J. J. Seidel, "Quadratic forms over $GL(2)$," *Indagationes Mathematicae*, vol. 76, no. 1, pp. 1–8, 1973.
- [3] T. Y. Lam, *Introduction to Quadratic Forms Over Fields*, AMS Publications, 2004.
- [4] R. Parimala, "A Hasse principle for quadratic forms over function fields," *American Mathematical Society. Bulletin. New Series*, vol. 51, no. 3, pp. 447–461, 2014.
- [5] R. W. Fitzgerald, "Highly degenerate quadratic forms over finite fields of characteristic 2," *Finite Fields and Their Applications*, vol. 11, no. 2, pp. 165–181, 2005.
- [6] M. Hubenthal, "Maximal subspaces of zeros of quadratic forms over finite fields," 2006.
- [7] R. W. Fitzgerald and J. L. Yucas, "Pencils of quadratic forms over finite fields," *Discrete Mathematics*, vol. 283, no. 1–3, pp. 71–79, 2004.
- [8] T. Vis, *The Existence and Uniqueness of a Simple Group of Order 168*, University of Denver, Denver, Colo, USA, 2007.

Hindawi

Submit your manuscripts at
<http://www.hindawi.com>