Journal of Advances in Mathematics and Computer Science

31(1): 1-6, 2019; Article no.JAMCS.46650

ISSN: 2456-9968

(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

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

Amrita Acharyya[1*] and Gerard Thompson[1]

[1] *Department of Mathematics, University of Toledo, Toledo, OH 43606, USA.*

Authors' contributions

This work was carried out in collaboration among both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JAMCS/2019/v31i130103

Editor(s):

(1) Dr. Rami Ahmad El-Nabulsi, Athens Institute for Education and Research, Mathematics and Physics Divisions, Greece.

(2) Dr. Thomas F. George, Chancellor / Professor, Department of Chemistry and Physics, University of Missouri-St. Louis, Boulevard St. Louis, USA.

Reviewers:

(1) Igor Bulyzhenkov, Moscow Institute of Physics and Technology, Russia.

(2) Dr. Mallikarjun Y. Kumbar, MASC College, Karnatka University, India.

(3) Francisco Frutos-Alfaro, University of Costa Rica, Costa Rica.

(4) Masato Nozawa, Kyoto University, Japan.

(5) Taxiarchis Papakostas, Technological Educational Institute of Crete, Greece.

Complete Peer review History: http://www.sdiarticle3.com/review-history/46650

Original Research Article

Received: 21 November 2018

Accepted: 25 January 2019

Published: 16 March 2019

Abstract

Quadratic forms in five variables over the field $\mathbb{Z}_2$ are classified by extending results previously obtained for four variables. It is shown that only one new form genuinely involving five variables appears.

Keywords: Quadratic form; field of two elements.

2010 Mathematics Subject Classification: $11E04, 11E25, 15A63$

**Corresponding author: E-mail: gerard.thompson@utoledo.edu*

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 five variables over the field $\mathbb{Z}_2$. In a recently published article [1] we have studied a similar problem for quadratic forms in four variables over the field $\mathbb{Z}_2$. The present article should be regarded as a sequel, so in the interest of efficiency we shall refer to [1] for many of the details.

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; see [2], [3], [4], [5] and [6].

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^tAx. Under a change of variables the matrix A changes according to P^tAP where P is non-singular. 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 non-zero 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 the situation is different, that is, if the matrix P is allowed to belong to $GL(n,)$ (the complex general linear group) rather than $GL(n,\mathbb{R})$ (the real general linear group), the distinction between positive and negative eigenvalues disappears and a quadratic form may always be reduced to diagonal form in which every non-zero 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 [7].

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. This issue as well material about forms in characteristic 2 is discussed in [8]. Another source for material about characteristic 2 is [9]. For further background material about quadratic forms we refer to [7] and a much more recent account with many references and many contemporary developments in [3]. In [4] the radical (maximal isotropic subspace) of a certain class of quadratic forms over fields of characteristic 2 is determined. In [5] among other things, the author studies the zeros of a quadratic form.

In this article we shall consider the equivalence of quadratic forms in five variables over the field $\mathbb{Z}_2$. We do so by extending our work on quadratic forms in four variables. The main conclusion is that just one new form appears in five variables: all other such forms are equivalent to forms in a fewer number of variables.

In terms of the literature on quadratic forms over finite fields, care must be taken to distinguish between results that apply to fields of characteristic p where p is an odd or even prime, whether the field is closed or perfect and so on. In the remainder of this article a "quadratic form" is always understood to be taken with coefficients in $\mathbb{Z}_2$. Our calculations have been facilitated by the symbolic manipulation program Maple.

2 A Result on Quadratic Forms in $4k+1$ Variables

Proposition 2.1. The quadratic form in n variables $\sum_{i<j\leq n} x^i x^j$ is equivalent to $\sum_{i<j\leq n-1} x^i x^j$ mod 2 if $n \equiv 1 \bmod 4$.

Proof. Starting from $Q = \sum_{i<j\leq n} x^i x^j$ define $x^i = X^i + X^n$ $(i < j < n)$ and $x^n = X^n$. Then replacing the x^i's by the X^i's gives

$$Q = \sum_{i<j<n} X^i X^j + X^n \sum_{i<j<n} (X^i + X^j) + \binom{n-1}{2}(X^n)^2 + X^n \sum_{i<n} X^i + (n-1)(X^n)^2$$

$$= \sum_{i<j<n} X^i X^j + (n-1)X^n \sum_{i<n} X^i + \frac{(n-1)(n+2)}{2}(X^n)^2.$$

If $n \equiv 1 \bmod 4$ then $n = 4k+1$ for some positive integer k. As such $n-1 \equiv 0 \bmod 2$ and $\frac{(n-1)(n+2)}{2} = 2k(4k+3) \equiv 0 \bmod 2$. □

3 The Zero Quadratic Form

We shall demonstrate in this Section that the zero quadratic form is equivalent only to itself. We write the quadratic form as

$$Q = \sum_i \alpha_i (x^i)^2 + \sum_{i<j} \beta_{ij} x^i x^j.$$

We make a change of variables called T corresponding to

$$x^i = A^i_j X^j$$

so that

$$Q = \sum_{i=1,j=1}^{n,n} \alpha_i (A^i_j X^j)^2 + \sum_{i<j,k=1,m=1}^{n,n} \beta_{ij} A^i_k A^j_m X^k X^j m.$$

Now put $Q = 0$ which entails that the coefficients of each of the $(X^i)^2$ and $X^i X^j$ where $i < j$ are zero. We obtain a homogeneous linear system in the variables α_i, β_{ij} where $i < j$. The matrix of coefficients has the following form:

$$\begin{bmatrix} AA & CC \\ 0 & BB \end{bmatrix}$$

where AA is $n \times n$, BB is $\binom{n}{2} \times \binom{n}{2}$ and CC is $n \times \binom{n}{2}$. Indeed the (i,j)th entry of AA is $(A^j_i)^2$; however, since we are working over the field $\mathbb{Z}_2$ each element $x \in \mathbb{Z}_2$ satisfies $x^2 = x$. In other words $AA = A^t$ and hence AA is a non-singular matrix. Concerning the matrix BB, we list the β_{ij} variables in the order $\beta_{12}, \beta_{13}, ..., \beta_{1n}, \beta_{23}, ..., \beta_{2n}, ..., \beta_{n-1,n}$. Then the corresponding entries in BB are given by $A^i_k A^j_m + A^i_m A^j_k$ where $1 \leq i < j \leq n, 1 \leq k < m \leq n$. Since we are working in $\mathbb{Z}_2$, the entries of BB consist of the 2×2 minors of A. However, as a consequence BB is the matrix of the transformation $\Lambda^2(T)$, that is, the second exterior power of T. The fact that we are working over $\mathbb{Z}_2$ causes no difficulty here. Again, since T is presumed to be invertible, so too is $\Lambda^2(T)$. As a result the entire matrix of coefficients is invertible. Thus:

Theorem 3.1. The zero quadratic form in n-variables with coefficients in $\mathbb{Z}_2$, is equivalent only to itself.

4 Equivalence of Quadratic Forms in Four Variables

We quote the following Theorem from [1]

Theorem 4.1. Every quadratic form in four variables x, y, z, t with coefficients in $\mathbb{Z}_2$ is equivalent to precisely one of $0, x^2, xy, xy + zt, xy + yz + zx, x^2 + xy + y^2, xy + yz + zx + xt + yt + zt$.

5 Classification of Quadratic Forms in Five Variables

Let us consider quadratic forms in *five* variables w, x, y, z, t with coefficients in $\mathbb{Z}_2$. We may write any such form as $ew^2 + w(ax + by + cz + dt) + Q(x, y, z, t)$ where $Q(x, y, z, t)$ is a quadratic form in *four* variables. Using Theorem 4.1 we have the following cases:

1. $ew^2 + w(ax + by + cz + dt)$
2. $ew^2 + w(ax + by + cz + dt) + x^2$
3. $ew^2 + w(ax + by + cz + dt) + xy$
4. $ew^2 + w(ax + by + cz + dt) + x^2 + xy + y^2$
5. $ew^2 + w(ax + by + cz + dt) + xy + zt$
6. $ew^2 + w(ax + by + cz + dt) + xy + yz + zx$
7. $ew^2 + w(ax + by + cz + dt) + xy + yz + zx + xt + yt + zt$

Now we consider each of these seven cases with regard to finding quadratic forms that genuinely contain five variables, that is, the quadratic form is not equivalent to a form in fewer than five variables. We shall write $p \sim q$ to mean that two quadratic forms are equivalent, that is, are related by a non-singular change of variables. If we do not give the transformation under which two forms are considered to be equivalent, such a transformation is considered to be obvious.

5.1

If $a = b = c = d = 0$ we have either 0 or w^2. Otherwise at least one of a, b, c, d is non-zero, say, d. Then putting $\bar{t} = ax + by + cz + t$ gives $ew^2 + wt$, dropping the bar. At all events we have a form in fewer than five variables.

5.2

Assuming that at least one of b, c, d is non-zero, say, d we put $\bar{t} = by + cz + t$ and obtain a form in three variables. If, however, $b = c = d = 0$, we obtain a form in two variables.

5.3

If one of c or d is non-zero, say d, then we may put $\bar{t} = ax + by + cz + t$ and obtain a form in four variables. If $c = d = 0$ we have a form in three variables.

5.4

If one of c or d is non-zero, say, d then we may put $\bar{t} = ax + by + cz + t$ and obtain a form in four variables. If $c = d = 0$ we have a form in three variables.

5.5

Based on symmetry we can reduce to the following eleven forms.

- $wx + xy + zt = x(w + y) + zt \sim xy + zt$
- $wx + wy + xy + zt$
- $wx + wz + xy + zt = x(w + y) + z(w + t) \sim xy + zt$
- $wx + wy + wz + xy + zt = xy + yw + wx + z(t + w) \sim wx + wy + xy + zt$
- $wx+wy+wz+wt+xy+zt \sim xy + zt$ $(X = x+w, Y = y+w, Z = z+w, T = t+w, W = w)$
- $w^2 + xy + zt \sim wx + wy + xy + zt$
- $w^2 + wx + xy + zt = w^2 + x(y + w) + zt \sim w^2 + xy + zt \sim wx + wy + xy + zt$
- $w^2 + wx + wy + xy + zt = (w + x)(w + y) + zt \sim xy + zt$
- $w^2 + wx + wz + xy + zt = w^2 + x(w + y) + z(w + t) \sim w^2 + xy + zt \sim wx + wy + xy + zt$
- $w^2 + wx + wy + wz + xy + zt = (w + x)(w + y) + z(t + w) \sim xy + zt$
- $w^2 + wx + wy + wz + wt + xy + zt \sim w^2 + xy + zt \sim wx + wy + xy + zt$

The conclusion is that for these eleven forms each one is equivalent to $xy+zt$ or $wx+wy+xy+zt$ and only the latter is a form in five variables.

5.6

If $d = 0$ we would have a quadratic form in four variables so $d = 1$. Based on symmetry we can reduce to the following eight forms.

- $wt + xy + yz + zx \sim wx + wy + xy + zt$
- $wx + wt + xy + yz + zx = w(x + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $wx + wy + wt + xy + yz + zx = w(x + y + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $wx + wy + wz + wt + xy + yz + zx = w(x + y + z + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $w^2 + wt + xy + yz + zx = w(w + t) + xy + yz + zx = wt + xy + yz + zx = \sim wx + wy + xy + zt$
- $w^2 + wx + wt + xy + yz + zx = w(w + x + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $w^2 + wx + wy + wt + xy + yz + zx = w(w + x + y + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $w^2 + wx + wy + wz + wt + xy + yz + zx = w(w + x + y + z + t) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$

5.7

- $wt + xy + yz + zx + xt + yt + zt = t(w + x + y + z) + xy + yz + zx \sim wt + xy + yz + zx \sim wx + wy + xy + zt$
- $wx + wy + xy + yz + zx + xt + yt + zt = (x + y)(w + z + t) + xy + zt \sim wx + wy + xy + zt$
- $wx + wy + wz + xy + yz + zx + xt + yt + zt = (w + t)(x + y + z) + xy + yz + zx \sim xy + yz + zx + xt + yt + zt$

- $wx + wy + wz + wt + xy + yz + zx + xt + yt + zt$ $(x = X + W, y = Y + W, z = Z + W, t = T + W, w = W) \sim xy + yz + zx + xt + yt + zt$
- $w^2 + wt + xy + yz + zx + xt + yt + zt$ $(x = X, y = Y, z = Z, t = T + W, w = W)$ $\sim wx + wy + wz + wt + xy + yz + zx + xt + yt + zt$
- $w^2 + wx + wy + xy + yz + zx + xt + yt + zt$ $(x = X, y = Y, z = T, t = Z + T, w = W) \sim w^2 + wt + xy + yz + zx + xt + yt + zt$
- $w^2 + wx + wy + wz + xy + yz + zx + xt + yt + zt$, $(x = Z, y = X + W, z = T, t = Y, w = W) \sim wx + wy + xy + yz + zx + xt + yt + zt$
- $w^2 + wx + wy + wz + wt + xy + yz + zx + xt + yt + zt$, $(x = Z, y = T + W, z = X, t = Y, w = W) \sim wt + xy + yz + zx + xt + yt + zt$

Hence:

Theorem 5.1. There is at most one quadratic form in five variables $xy + yz + zx + tw$ with coefficients in $\mathbb{Z}_2$, that is not equivalent to forms in four variables.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Acharyya A, Thompson G. Classifying quadratic forms over $\mathbb{Z}_2$ in four variables. British Journal of Mathematics and Computer Science. 2018;28(2):1-16.

[2] Lam TY. Introduction to quadratic forms over fields. AMS Publications; 2004.

[3] Elman R, Karpenko N, Merkurjev A. The algebra and geometry theory of quadratic forms. American Mathematical Society; 2004.

[4] Fitzgerald R. Highly degenerate quadratic forms over finite fields of characteristic 2. Finite Fields and their Applications. 2005;165-181.

[5] Hubenthal M. Maximal subspaces of zeros of quadratic forms over finite fields, preprint; 2006.

[6] Parimala R. A Hasse principle for rational quadratic forms over function fields. Bulletin of the American Mathematical Society. 2014;51(3):447-461.

[7] Cassels JWS. Rational quadratic forms. Academic Press; 1978.

[8] Albert AA. Symmetric and alternate matrices in an arbitrary field. Transactions of the American Mathematical Society. 1938;43(3): 386-436.

[9] Arf C. Untersuchungen über quadratische Formem in Körpern der Characteristic 2 (Teil I). J. Reine und Angewandte Mathematik. 1937;176:31-44.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://www.sdiarticle3.com/review-history/46650