Journal of Advances in Mathematics and Computer Science

28(2): 1-16, 2018; Article no.JAMCS.42882
ISSN: 2456-9968
(Past name: British Journal of Mathematics & Computer Science, Past ISSN: 2231-0851)

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

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

[1] *Department of Mathematics, University of Toledo Toledo, OH 43606, U.S.A.*

Author's Contribution

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

Article Information

DOI: 10.9734/JAMCS/2018/42882
Editor(s):
(1) Raducanu Razvan, Assistant Professor, Department of Applied Mathematics, Al. I. Cuza University, Romania.
Reviewers:
(1) Piyush Shroff, Texas State University, USA.
(2) Tao Xie, Hubei Normal University, China.
(3) Naresh Kumar, Mewar University, India.
Complete Peer review History: http://www.sciencedomain.org/review-history/25717

Original Research Article

Received: 20th May 2018
Accepted: 19th July 2018
Published: 27th July 2018

Abstract

Quadratic forms in four variables over the field $\mathbb{Z}_2$ are sorted first of all with respect to permutation symmetry. Thereafter it is shown that any such form is equivalent to one of seven such canonical forms. The orthogonal group of each one of these seven forms is obtained. The paper closes with some remarks about quadratic forms in three variables.

Keywords: Quadratic form; field of two elements; orthogonal group.

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 four variables over the field $\mathbb{Z}_2$. As our references suggest,

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

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

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 [1], [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 [2]. 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. Yet another direction [3] concerns pencils of quadratic forms over finite fields.

Our calculations have been facilitated by the symbolic manipulation program Maple. Our method is elementary, if not to say naive; however, it has the advantage of being self-contained and accessible to non-experts. 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. Undoubtedly similar results exist in the literature but we did not find them anywhere organized in quite the same form and may require some sophisticated algebraic techniques. Finally, for us the group D_{2n} denotes the dihedral group of order $2n$. In a forthcoming paper we hope to be able to report on how to generalize some of our results to quadratic forms with five or more variables.

2 Preliminary Reduction

There are, in principle, $2^{10} = 1024$ quadratic forms but some are equivalent by transformations from the symmetric group S_4. Two such quadratic forms will be considered to be equivalent by an element of $GL(4,\mathbb{Z}_2)$, which is a finite simple group of order 20160. There are 64 forms that have no square terms.

2.1 Equivalence of quadratic forms

We shall write a general quadratic form Q in the form

$$\alpha x^2 + \beta xy + \delta xz + \epsilon y^2 + \lambda tx + \mu ty + \nu tz + \phi yz + \rho z^2 + \sigma t^2. \tag{1}$$

Working over $\mathbb{Z}_2$, it is not possible to associate to Q a symmetric matrix otherwise all cross terms would vanish. In fact one needs to exercise a great deal of care when working with $\mathbb{Z}_2$ because almost all the standard results of linear algebra no longer remain valid. Nonetheless, one may use instead an upper triangular matrix, $A = \begin{bmatrix} \alpha & \beta & \delta & \lambda \\ 0 & \epsilon & \phi & \mu \\ 0 & 0 & \rho & \nu \\ 0 & 0 & 0 & \sigma \end{bmatrix}$. See [8] for further details.

We shall make a change of variables P as

$$\begin{aligned} x &= aX + bY + cZ + dT \\ y &= eX + fY + gZ + hT \\ z &= iX + jY + kZ + mT \\ t &= nX + pY + qZ + rT. \end{aligned} \tag{2}$$

As such Q is transformed into

$$\begin{aligned} &\left(\alpha\, a^2 + \beta\, ae + \delta\, ai + \lambda\, na + \epsilon\, e^2 + \phi\, ei + \mu\, ne + \rho\, i^2 + \nu\, ni + \sigma\, n^2\right) X^2 + (\beta\, af + \\ &\delta\, aj + \lambda\, pa + \beta\, be + \delta\, bi + \lambda\, nb + \phi\, ej + \mu\, pe + \phi\, fi + \mu\, nf + \nu\, pi + \nu\, nj)XY \\ &+(\beta\, ag + \delta\, ak + \lambda\, qa + \beta\, ce + \delta\, ci + \lambda\, nc + \phi\, ek + \mu\, qe + \phi\, gi + \mu\, ng + \nu\, qi \\ &+\nu\, nk)XZ + (a\beta\, h + a\delta\, m + a\lambda\, r + \beta\, de + d\delta\, i + d\lambda\, n + em\phi + e\mu\, r + hi\phi \\ &+h\mu\, n + i\nu\, r + mn\nu)TX + (\alpha\, b^2 + \beta\, bf + \delta\, bj + \lambda\, pb + \epsilon\, f^2 + \phi\, fj + \mu\, pf + \rho\, j^2 \\ &+\nu\, pj + \sigma\, p^2)Y^2 + (\beta\, bg + \delta\, bk + \lambda\, qb + \beta\, cf + \delta\, cj + \lambda\, pc + \phi\, fk + \mu\, qf + \phi\, gj \\ &+g\mu\, p + j\nu\, q + k\nu\, p)YZ + (b\beta\, h + b\delta\, m + b\lambda\, r + \beta\, df + d\delta\, j + d\lambda\, p + fm\phi \\ &+f\mu\, r \ + hj\phi + h\mu\, p + nu\, r + m\nu\, p)TY + (\alpha\, c^2 + \beta\, cg + c\delta\, k + c\lambda\, q + \epsilon\, g^2 \\ &+gk\phi + g\mu\, q + k^2\rho)Z^2 + (k\nu\, q + q^2\sigma(\beta\, ch + \beta\, dg + c\delta\, m + c\lambda\, r + d\delta\, k + d\lambda\, q \\ &+gm\phi + g\mu\, r + hk\phi + h\mu\, q + k\nu\, r + m\nu\, q)TZ + \\ &\left(\alpha\, d^2 + \beta\, dh + d\delta\, m + d\lambda\, r + \epsilon\, h^2 + hm\phi + h\mu\, r + m^2\rho + m\nu\, r + r^2\sigma\right) T^2 \end{aligned} \tag{3}$$

and A transforms by P^tAP. However, there is no general reason to suppose that P^tAP should be upper triangular. Of course it is possible to replace P^tAP by an upper triangular matrix that is equivalent in the sense that it engenders the quadratic form X^tP^tAPX. In the next subsection we shall show that a sum of squares over $\mathbb{Z}_2$ is equivalent to just one square. Even if one starts with a strictly upper triangular matrix and obtains an equivalent strictly upper triangular matrix there is no guarantee that the two matrices will have the same rank. We consider two examples:

- $xy + zt$. Make the change

  $$x = X + Z + T, y = Y, z = Z, t = T. \tag{4}$$

  Then the form is transformed into $XY + YZ + YT + ZT$. The associated strictly upper triangular matrices are

  $$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

  respectively.

- $xy + zt$. Make the change

$$x = Y + Z, y = X + T, z = Y, t = Z + T. \tag{5}$$

Then the form is transformed into $XY + YZ + ZX + ZT$. The associated strictly upper triangular matrices are

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

respectively.

2.2 The zero quadratic form

Now we enquire about when a quadratic form can be transformed into zero. As such each of the ten coefficients of $X^2, XY, ..., T^2, TX$ must be zero. We regard $\alpha, \beta, \delta, \lambda, \epsilon, \phi, \mu, \rho, \nu, \sigma$ as unknowns and write out the matrix of coefficients as a 10×10 matrix:

$$M = \begin{bmatrix} a^2 & ae & ai & an & e^2 & ei & en & i^2 & in & n^2 \\ b^2 & bf & bj & bp & f^2 & fj & fp & j^2 & jp & p^2 \\ c^2 & cg & ck & cq & g^2 & gk & gq & k^2 & kq & q^2 \\ d^2 & dh & dm & dr & h^2 & hm & hr & m^2 & mr & r^2 \\ 0 & af+be & aj+bi & ap+bn & 0 & ej+fi & ep+fn & 0 & ip+jn & 0 \\ 0 & ag+ce & ak+ci & aq+cn & 0 & ek+gi & eq+gn & 0 & iq+kn & 0 \\ 0 & ah+de & am+di & ar+dn & 0 & em+hi & er+hn & 0 & ir+mn & 0 \\ 0 & bg+cf & bk+cj & bq+cp & 0 & fk+gj & fq+gp & 0 & jq+kp & 0 \\ 0 & bh+df & bm+dj & br+dp & 0 & fm+hj & fr+hp & 0 & jr+mp & 0 \\ 0 & ch+dg & cm+dk & cr+dq & 0 & gm+hk & gr+hq & 0 & kr+mq & 0 \end{bmatrix}.$$

Now we shall work "mod 2"; as such it turns out according to Maple that the determinant of M mod 2 is given by Δ^5 where Δ is the determinant of the transformation P. We require P to be non-singular. It follows that:

Proposition 2.1. *The zero quadratic form is equivalent only to itself.*

2.3 Forms that are sums of squares

In a space of dimension n any non-zero form that is a sum of squares is equivalent to x_1^2.

Proof. Consider the form $x_1^2 + x_2^2 ... + x_k^2$ where $k \leq n$. Make the transformation $x_1 = X_1 + X_2, x_2 = X_2 + X_3, x_3 = X_3 + X_4, ..., x_p = X_p + X_{p+1}, ...x_{k-1} = X_{k-1} + X_k, x_k = X_k, x_{k+1} = X_{k+1}, ..., x_n = X_n$. The transformation is invertible since the associated matrix consists of the identity plus an upper triangular matrix and reduces the given form to X_1^2 as required. □

As a result of the Lemma a square term can be transformed only into a sum of squares.

2.4 Forms that are square-free

- zero
- six monomials : xy, xz, xt, yz, yt, zt
- fifteen forms with two terms: three forms with no common factor $xy + zt, xz + yt, xt + yz$ and twelve forms with a common factor: $x(y + z), x(y + t), x(z + t), y(x + z), y(x + t), y(z + t), z(x + y), z(x + t), z(y + t), t(x + y), t(x + z), t(y + z)$
- twenty forms with three terms: four forms with a common factor $x(y + z + t), y(x + z + t), z(x + y + t), t(x + y + z)$, four forms in which one variable is absent $xy + yz + zx, xy + yt + tx, xz + zt + tx, yz + zt + ty$, and twelve forms in which two variables appear twice and each of the remaining variables appear once $xy + zt + xz, xy + zt + xt, xy + zt + yz, xy + zt + yt, xz + yt + xy, xz + yt + xt, xz + yt + zy, xz + yt + zt, xt + yz + xy, xt + yz + xz, xt + yz + ty, xt + yz + tz$
- fifteen forms with four terms: three forms in which the "missing" terms are $xy + zt, xz + yt, xt + yz$ and twelve in which the "missing" terms have a common factor such as $x(y + z)$
- six forms with five terms such as $xz + xt + yz + yt + zt$
- one form with six terms: $xy + xz + xt + yz + yt + zt$

Next we consider forms that contain, $0, 1, 2, 3$ and 4 squares, respectively, and use symmetry to compile a list of quadratic forms; an arbitrary quadratic form is equivalent to one of the forms in the list via a permutation.

2.5 Reduced square-free forms

- (1) 0
- (2) xy
- (3) $xy + zt$
- (4) $xy + xz = x(y + z)$
- (5) $xy + xz + xt = x(y + z + t)$
- (6) $xy + yz + zx$
- (7) $xy + zt + xz$
- (8) $xy + xz + yt + zt = (x + t)(y + z)$
- (9) $xy + xz + xt + zt = x(y + z + t) + zt$
- (10) $xy + xz + xt + yz + yt$
- (11) $xy + xz + xt + yz + yt + zt$

2.6 Reduced forms that contain one square

- (12) x^2
- (13) $x^2 + xy = x(x + y)$
- (14) $x^2 + yz$
- (15) $x^2 + xy + zt$
- (16) $x^2 + xy + xz = x(x + y + z)$
- (17) $x^2 + xy + yz = x^2 + y(x + z)$
- (18) $x^2 + yz + yt = x^2 + y(z + t)$
- (19) $x^2 + xy + xz + xt = x(x + y + z + t)$

- (20) $x^2 + xy + yz + yt = x^2 + y(x + z + t)$
- (21) $x^2 + xy + yz + zx = (x + y)(x + z)$
- (22) $x^2 + yz + zt + ty$
- (23) $x^2 + xy + zt + xz = x(x + y + z) + zt$
- (24) $x^2 + xy + zt + yz \equiv x(x + y + z) + z(x + y + t) \bmod 2$
- (25) $x^2 + xz + xt + yz + yt = x^2 + (x + y)(z + t)$
- (26) $x^2 + xt + yz + yt + zt$
- (27) $x^2 + xy + xz + xt + yz = x^2 + yz + x(y + z + t)$
- (28) $x^2 + xy + xz + yz + yt$
- (29) $x^2 + xz + xt + yz + yt + zt$
- (30) $x^2 + xy + xz + xt + yz + yt$
- (31) $x^2 + xy + xz + xt + yz + yt + zt$.

2.7 Reduced forms that contain two squares

- (32) $x^2 + y^2 + xy$
- (33) $x^2 + y^2 + xz$
- (34) $x^2 + y^2 + zt$
- (35) $x^2 + y^2 + xy + zt$
- (36) $x^2 + y^2 + xz + yt$
- (37) $x^2 + y^2 + xy + xz$
- (38) $x^2 + y^2 + xz + xt$
- (39) $x^2 + y^2 + xz + yz$
- (40) $x^2 + y^2 + xz + zt$
- (41) $x^2 + y^2 + xy + xz + xt = x^2 + y^2 + x(y + z + t)$
- (42) $x^2 + y^2 + xt + yt + zt) = x^2 + y^2 + t(x + y + z)$
- (43) $x^2 + y^2 + xy + yz + zx$
- (44) $x^2 + y^2 + xz + zt + tx$
- (45) $x^2 + y^2 + xy + zt + xz$
- (46) $x^2 + y^2 + xz + yt + xy$
- (47) $x^2 + y^2 + xz + yt + xt$
- (48) $x^2 + y^2 + xz + yt + yz$
- (49) $x^2 + y^2 + xz + yt + zt$
- (50) $x^2 + y^2 + xz + xt + yz + yt$
- (51) $x^2 + y^2 + xy + xt + yz + yt$
- (52) $x^2 + y^2 + xt + yz + yt + zt$
- (53) $x^2 + y^2 + xy + xz + xt + zt$
- (54) $x^2 + y^2 + xy + xt + yt + zt$
- (55) $x^2 + y^2 + xy + xt + yz + zt$
- (56) $x^2 + y^2 + xz + xt + yz + yt + zt$
- (57) $x^2 + y^2 + xy + xt + yz + yt + zt$
- (58) $x^2 + y^2 + xy + xz + xt + yz + yt$
- (59) $x^2 + y^2 + xy + xz + xt + yz + yt + zt$.
- (60) $x^2 + y^2 + xy + xz + xt + yt$

2.8 Reduced forms that contain three squares

- (61) $y^2 + z^2 + t^2 + xy$
- (62) $y^2 + z^2 + t^2 + yz$
- (63) $y^2 + z^2 + t^2 + xy + zt$
- (64) $y^2 + z^2 + t^2 + xy + xz = y^2 + z^2 + t^2 + x(y + z)$
- (65) $y^2 + z^2 + t^2 + xy + yz = y^2 + z^2 + t^2 + y(x + z)$
- (66) $y^2 + z^2 + t^2 + yz + yt = y^2 + z^2 + t^2 + y(z + t)$
- (67) $y^2 + z^2 + t^2 + xy + xz + xt = y^2 + z^2 + t^2 + x(y + z + t)$
- (68) $y^2 + z^2 + t^2 + xy + yz + yt = y^2 + z^2 + t^2 + y(x + z + t)$
- (69) $y^2 + z^2 + t^2 + xy + yz + zx$
- (70) $y^2 + z^2 + t^2 + yz + zt + ty$
- (71) $y^2 + z^2 + t^2 + xy + zt + xz$
- (72) $y^2 + z^2 + t^2 + xy + zt + yz$
- (73) $y^2 + z^2 + t^2 + xz + xt + yz + yt = y^2 + z^2 + t^2 + (x + y)(z + t)$
- (74) $y^2 + z^2 + t^2 + xt + yz + yt + zt$
- (75) $y^2 + z^2 + t^2 + xy + xz + xt + yz = y^2 + z^2 + t^2 + yz + x(y + z + t)$
- (76) $y^2 + z^2 + t^2 + xy + xz + yz + yt$
- (77) $y^2 + z^2 + t^2 + xz + xt + yz + yt + zt$
- (78) $y^2 + z^2 + t^2 + xy + xz + xt + yz + yt$
- (79) $y^2 + z^2 + t^2 + xy + xz + xt + yz + yt + zt$.

2.9 Reduced forms that contain four squares

- (80) $x^2 + y^2 + z^2 + t^2$
- (81) $x^2 + y^2 + z^2 + t^2 + xy$
- (82) $x^2 + y^2 + z^2 + t^2 + xy + zt$
- (83) $x^2 + y^2 + z^2 + t^2 + x(y + z)$
- (84) $x^2 + y^2 + z^2 + t^2 + x(y + z + t)$
- (85) $x^2 + y^2 + z^2 + t^2 + xy + yz + zx$
- (86) $x^2 + y^2 + z^2 + t^2 + xy + zt + xz$
- (87) $x^2 + y^2 + z^2 + t^2 + xy + xz + yt + zt$
- (88) $x^2 + y^2 + z^2 + t^2 + xy + xz + xt + yz$
- (89) $x^2 + y^2 + z^2 + t^2 + xy + xz + xt + yz + yt$
- (90) $x^2 + y^2 + z^2 + t^2 + xy + xz + xt + yz + yt + zt$

As result of the previous investigations we have succeeded in reducing the number of quadratic forms from the original 1024 down to 90. We claim that the list of 90 quadratic forms that have been reduced purely on grounds of symmetry may be further reduced to just seven:

$$0, x^2, xy, xy + zt, xy + yz + zx, x^2 + xy + y^2, xy + yz + zx + xt + yt + zt.$$

In the next Section we give explicit transformations that change each of the ninety forms into these seven.

3 Explicit Equivalences

In this Section we shall further refine the list of 90 forms found in Section 2 using the transformation P that changed 2 into 3. Equivalence of two forms is denoted by $\sim$ and the numbers of the forms pertain to Section 2. The letters $a, b, c, ..., r$ are the entries of the matrix P introduced in Section 3.

3.1 Forms equivalent to xy

1. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 1, g = 1, h = 0, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 \implies 2 \sim 4.$
2. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 \implies 2 \sim 5.$
3. $a = 1, b = 0, c = 0, d = 1, e = 0, f = 1, g = 1, h = 0, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1.\ xy + xz + yt + zt \sim xy \implies 2 \sim 8$
4. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 0, h = 0, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1.\ x^2 + xy \sim xy : \implies 2 \sim 13$
5. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 1, h = 0, i = 0, j = 0, k = 1, m = 1, n = 0, p = 0, q = 1, r = 0 : x^2 + xy + xz \sim xy \implies 2 \sim 16$
6. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 1, h = 1, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 : \implies 2 \sim 19$
7. $a = 1, b = 0, c = 1, d = 0, e = 1, f = 1, g = 0, h = 0, i = 0, j = 0, k = 1, m = 1, n = 0, p = 0, q = 0, r = 1 : \implies 2 \sim 21$
8. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 0, g = 1, h = 1, i = 0, j = 0, k = 1, m = 1, n = 1, p = 0, q = 1, r = 0 : \implies 2 \sim 30$
9. $a = 1, b = 1, c = 1, d = 0, e = 1, f = 1, g = 0, h = 0, i = 0, j = 1, k = 1, m = 0, n = 1, p = 1, q = 0, r = 1 : \implies 2 \sim 39$
10. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 1, g = 1, h = 1, i = 0, j = 0, k = 0, m = 1, n = 0, p = 1, q = 0, r = 0 : \implies 2 \sim 50$
11. $a = 1, b = 1, c = 0, d = 1, e = 1, f = 1, g = 1, h = 0, i = 0, j = 1, k = 0, m = 1, n = 0, p = 1, q = 0, r = 0 : \implies 2 \sim 56$
12. $a = 1, b = 1, c = 1, d = 1, e = 0, f = 1, g = 1, h = 1, i = 1, j = 0, k = 0, m = 1, n = 0, p = 1, q = 0, r = 1 : \implies 2 \sim 67$

3.2 Forms equivalent to $xy + zt$

1. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 0, j = 0, k = 0, m = 1, n = 0, p = 0, q = 1, r = 0 : \implies 3 \sim 7$
2. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 : \implies 3 \sim 9$
3. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 0, h = 0, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 : \implies 3 \sim 15$
4. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 1, h = 0, i = 0, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 : \implies 3 \sim 23$
5. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 1, h = 0, i = 0, j = 0, k = 1, m = 0, n = 1, p = 1, q = 0, r = 1 : \implies 3 \sim 24$
6. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 0, g = 0, h = 1, i = 1, j = 1, k = 0, m = 0, n = 1, p = 0, q = 1, r = 0 : \implies 3 \sim 27$

7. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 0, g = 0, h = 1, i = 1, j = 1, k = 0, m = 0, n = 1, p = 0, q = 1, r = 1 : \Longrightarrow\ 3 \sim 28$
8. $a = 1, b = 1, c = 0, d = 1, e = 1, f = 1, g = 1, h = 0, i = 1, j = 1, k = 0, m = 0, n = 0, p = 1, q = 0, r = 0 : \Longrightarrow\ 3 \sim 31$
9. $a = 1, b = 1, c = 0, d = 0, e = 0, f = 1, g = 0, h = 1, i = 1, j = 0, k = 0, m = 0, n = 1, p = 1, q = 1, r = 1 : \Longrightarrow\ 3 \sim 36$
10. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 1, g = 1, h = 0, i = 0, j = 1, k = 0, m = 0, n = 1, p = 0, q = 1, r = 1 : \Longrightarrow\ 3 \sim 46$
11. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 0, g = 1, h = 0, i = 1, j = 1, k = 0, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 3 \sim 47$
12. $a = 1, b = 1, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 1, j = 0, k = 0, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 3 \sim 48$
13. $a = 1, b = 1, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 1, j = 0, k = 0, m = 0, n = 1, p = 0, q = 1, r = 0 : \Longrightarrow\ 3 \sim 51$
14. $a = 0, b = 1, c = 0, d = 1, e = 1, f = 1, g = 1, h = 0, i = 1, j = 0, k = 0, m = 0, n = 1, p = 1, q = 0, r = 0 : \Longrightarrow\ 3 \sim 52$
15. $a = 1, b = 0, c = 1, d = 1, e = 1, f = 0, g = 0, h = 1, i = 1, j = 1, k = 0, m = 1, n = 0, p = 1, q = 0, r = 1 : \Longrightarrow\ 3 \sim 53$
16. $a = 0, b = 1, c = 0, d = 0, e = 1, f = 0, g = 0, h = 0, i = 1, j = 1, k = 1, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 3 \sim 59$
17. $a = 0, b = 1, c = 1, d = 0, e = 0, f = 1, g = 0, h = 1, i = 1, j = 0, k = 1, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 3 \sim 60$
18. $a = 1, b = 1, c = 1, d = 0, e = 0, f = 1, g = 1, h = 1, i = 1, j = 1, k = 0, m = 1, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 3 \sim 71$
19. $a = 0, b = 1, c = 0, d = 1, e = 0, f = 1, g = 0, h = 0, i = 0, j = 1, k = 1, m = 1, n = 1, p = 0, q = 1, r = 1 : \Longrightarrow\ 3 \sim 75$
20. $a = 1, b = 1, c = 1, d = 1, e = 1, f = 0, g = 1, h = 1, i = 0, j = 1, k = 0, m = 1, n = 0, p = 1, q = 1, r = 0 : \Longrightarrow\ 3 \sim 82$

3.3 Forms equivalent to $xy + yz + zx$

1. $a = 0, b = 0, c = 1, d = 1, e = 1, f = 0, g = 0, h = 0, i = 0, j = 1, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 10$
2. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 0, g = 1, h = 0, i = 1, j = 1, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 14$
3. $a = 0, b = 0, c = 1, d = 0, e = 1, f = 1, g = 0, h = 0, i = 1, j = 0, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 17$
4. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 0, g = 1, h = 1, i = 1, j = 1, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 18$
5. $a = 1, b = 0, c = 0, d = 0, e = 1, f = 1, g = 0, h = 0, i = 0, j = 0, k = 1, m = 1, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 20$
6. $a = 1, b = 0, c = 0, d = 1, e = 1, f = 1, g = 0, h = 0, i = 1, j = 0, k = 1, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 22$
7. $a = 1, b = 0, c = 1, d = 1, e = 1, f = 0, g = 0, h = 0, i = 0, j = 1, k = 0, m = 0, n = 1, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 25$

8. $a = 1, b = 0, c = 0, d = 1, e = 1, f = 0, g = 1, h = 0, i = 0, j = 1, k = 0, m = 0, n = 0, p = 1, q = 0, r = 1 : \Longrightarrow\ 6 \sim 29$
9. $a = 1, b = 1, c = 1, d = 0, e = 0, f = 1, g = 0, h = 0, i = 1, j = 1, k = 0, m = 0, n = 0, p = 0, q = 1, r = 1 : \Longrightarrow\ 6 \sim 33$
10. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 1, g = 0, h = 1, i = 1, j = 1, k = 1, m = 0, n = 0, p = 1, q = 0, r = 0 : \Longrightarrow\ 6 \sim 34$
11. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 0, g = 1, h = 0, i = 0, j = 1, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 37$
12. $a = 1, b = 1, c = 1, d = 1, e = 0, f = 1, g = 0, h = 0, i = 1, j = 1, k = 0, m = 0, n = 1, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 38$
13. $a = 1, b = 1, c = 0, d = 0, e = 1, f = 1, g = 1, h = 0, i = 0, j = 1, k = 0, m = 1, n = 0, p = 1, q = 0, r = 0 : \Longrightarrow\ 6 \sim 40$
14. $a = 1, b = 1, c = 0, d = 0, e = 0, f = 1, g = 0, h = 0, i = 1, j = 0, k = 1, m = 1, n = 1, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 41$
15. $a = 1, b = 1, c = 0, d = 0, e = 0, f = 0, g = 1, h = 0, i = 1, j = 1, k = 0, m = 1, n = 0, p = 1, q = 0, r = 0 : \Longrightarrow\ 6 \sim 42$
16. $a = 0, b = 1, c = 0, d = 0, e = 1, f = 0, g = 0, h = 0, i = 1, j = 1, k = 1, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 6 \sim 43$
17. $a = 1, b = 1, c = 0, d = 1, e = 1, f = 1, g = 1, h = 0, i = 0, j = 1, k = 0, m = 0, n = 0, p = 1, q = 0, r = 1 : \Longrightarrow\ 6 \sim 44$
18. $a = 1, b = 0, c = 0, d = 1, e = 0, f = 1, g = 1, h = 0, i = 1, j = 1, k = 0, m = 0, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 6 \sim 55$
19. $a = 1, b = 0, c = 0, d = 0, e = 0, f = 1, g = 1, h = 0, i = 1, j = 1, k = 0, m = 1, n = 0, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 57$
20. $a = 1, b = 1, c = 1, d = 0, e = 0, f = 0, g = 1, h = 0, i = 1, j = 0, k = 0, m = 1, n = 1, p = 0, q = 0, r = 0 : \Longrightarrow\ 6 \sim 58$
21. $a = 0, b = 1, c = 1, d = 1, e = 0, f = 0, g = 1, h = 1, i = 1, j = 1, k = 1, m = 1, n = 0, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 61$
22. $a = 0, b = 1, c = 0, d = 1, e = 0, f = 0, g = 1, h = 1, i = 0, j = 1, k = 1, m = 1, n = 1, p = 1, q = 0, r = 0 : \Longrightarrow\ 6 \sim 62$
23. $a = 1, b = 1, c = 1, d = 1, e = 0, f = 0, g = 0, h = 1, i = 0, j = 1, k = 1, m = 1, n = 1, p = 1, q = 0, r = 1 : \Longrightarrow\ 6 \sim 64$
24. $a = 0, b = 1, c = 1, d = 1, e = 0, f = 0, g = 1, h = 1, i = 1, j = 1, k = 0, m = 1, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 65$
25. $a = 0, b = 1, c = 1, d = 1, e = 1, f = 1, g = 0, h = 0, i = 0, j = 0, k = 1, m = 1, n = 1, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 68$
26. $a = 0, b = 0, c = 1, d = 1, e = 1, f = 1, g = 1, h = 1, i = 0, j = 1, k = 0, m = 1, n = 0, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 69$
27. $a = 0, b = 1, c = 0, d = 0, e = 0, f = 1, g = 1, h = 1, i = 1, j = 0, k = 1, m = 1, n = 1, p = 1, q = 1, r = 0 : \Longrightarrow\ 6 \sim 73$
28. $a = 0, b = 1, c = 1, d = 0, e = 0, f = 1, g = 0, h = 1, i = 1, j = 0, k = 1, m = 1, n = 1, p = 0, q = 1, r = 0 : \Longrightarrow\ 6 \sim 77$
29. $a = 0, b = 0, c = 1, d = 1, e = 1, f = 1, g = 1, h = 1, i = 0, j = 1, k = 0, m = 0, n = 0, p = 0, q = 0, r = 1 : \Longrightarrow\ 6 \sim 78$

30. $a=1,b=1,c=1,d=1,e=1,f=0,g=1,h=1,i=1,j=0,k=1,m=0,n=1,p=1,q=0,r=1:\Longrightarrow\ 6\sim 81$
31. $a=0,b=1,c=1,d=1,e=1,f=0,g=0,h=1,i=1,j=1,k=1,m=1,n=1,p=1,q=0,r=0:\Longrightarrow\ 6\sim 83$
32. $a=0,b=1,c=1,d=1,e=1,f=1,g=0,h=1,i=1,j=0,k=1,m=1,n=1,p=0,q=0,r=0:\Longrightarrow\ 6\sim 85$

3.4 Forms equivalent to $xy+yz+zx+xt+yt+zt$

1. $a=1,b=1,c=0,d=1,e=1,f=1,g=0,h=0,i=0,j=1,k=1,m=0,n=0,p=1,q=0,r:=0:\Longrightarrow\ 11\sim 26$
2. $a=1,b=1,c=0,d=0,e=0,f=1,g=1,h=0,i=0,j=1,k=0,m=1,n=1,p=0,q=0,r=0:\Longrightarrow\ 11\sim 35$
3. $a=1,b=1,c=0,d=0,e=0,f=1,g=1,h=0,i=1,j=1,k=0,m=1,n=1,p=0,q=0,r=0:\Longrightarrow\ 11\sim 45$
4. $a=0,b=1,c=0,d=1,e=1,f=0,g=1,h=0,i=0,j=1,k=0,m=0,n=1,p=0,q=0,r=0:\Longrightarrow\ 11\sim 49$
5. $a=1,b=0,c=0,d=0,e=0,f=1,g=0,h=1,i=1,j=0,k=1,m=0,n=1,p=1,q=0,r=0\ \Longrightarrow\ 11\sim 54$
6. $a=1,b=1,c=1,d=0,e=0,f=1,g=1,h=0,i=0,j=0,k=1,m=1,n=0,p=0,q=0,r=1:\Longrightarrow\ 11\sim 63$
7. $a=1,b=1,c=0,d=0,e=0,f=1,g=1,h=0,i=0,j=0,k=1,m=1,n=0,p=0,q=0,r=1:\Longrightarrow\ 11\sim 72$
8. $a=1,b=1,c=1,d=0,e=1,f=0,g=1,h=1,i=1,j=1,k=0,m=1,n=1,p=0,q=0,r=1:\Longrightarrow\ 11\sim 74$
9. $a=0,b=1,c=0,d=1,e=0,f=0,g=0,h=1,i=0,j=0,k=1,m=0,n=1,p=1,q=1,r=0:\Longrightarrow\ 11\sim 76$
10. $a=0,b=0,c=1,d=0,e=1,f=1,g=1,h=1,i=0,j=1,k=0,m=0,n=0,p=0,q=0,r=1:\Longrightarrow\ 11\sim 79$
11. $a=1,b=0,c=1,d=1,e=1,f=1,g=0,h=1,i=0,j=0,k=1,m=0,n=0,p=1,q=0,r=1:\Longrightarrow\ 11\sim 86$
12. $a=0,b=1,c=0,d=1,e=1,f=1,g=0,h=1,i=0,j=1,k=1,m=0,n=1,p=0,q=1,r=0:\Longrightarrow\ 11\sim 88$
13. $a=0,b=1,c=0,d=1,e=1,f=0,g=0,h=1,i=0,j=0,k=1,m=1,n=1,p=1,q=1,r=0\ \Longrightarrow\ 11\sim 90$

3.5 Forms equivalent to x^2+xy+y^2

1. $a=0,b=0,c=1,d=1,e=0,f=1,g=0,h=0,i=1,j=0,k=0,m=0,n=0,p=0,q=0,r=1:\Longrightarrow\ 32\sim 66$
2. $a=0,b=1,c=1,d=0,e=0,f=0,g=1,h=1,i=1,j=1,k=0,m=0,n=0,p=0,q=0,r=1:\Longrightarrow\ 32\sim 70$
3. $a=1,b=1,c=1,d=1,e=0,f=1,g=1,h=1,i=0,j=0,k=1,m=1,n=0,p=0,q=0,r=1:\Longrightarrow\ 32\sim 84$
4. $a=1,b=1,c=1,d=0,e=1,f=0,g=0,h=1,i=0,j=1,k=0,m=1,n=0,p=0,q=0,r=1:\Longrightarrow\ 32\sim 87$
5. $a=1,b=1,c=0,d=0,e=1,f=0,g=1,h=1,i=0,j=0,k=1,m=1,n=0,p=0,q=0,r=1:\Longrightarrow\ 32\sim 89$

4 Orthogonal Groups

A transformation P of a quadratic form will be said to be *orthogonal* if it is unchanged under P. In this Section we shall find the orthogonal groups of each of the seven canonical quadratic forms.

4.1 $x^2 + xy + y^2$

We shall begin by understanding why the quadratic form $x^2 + xy + y^2$ is not equivalent to a form that has one square or square-free form. In this regard under the transformation P of eq.(2), the quadratic form changes into

$$(a^2 + ae + e^2)X^2 + (b^2 + bf + f^2)Y^2 + (c^2 + cg + g^2)Z^2 + (d^2 + dh + h^2)T^2 + crossterms \quad (6)$$

If $c^2 + cg + g^2 = 0$ we can only have $c = g = 0$. If three square terms are zero we can assume WLOG that $b^2 + bf + f^2 = c^2 + cg + g^2 = d^2 + dh + h^2 = 0$ and hence $b = c = d = f = g = h = 0$. However, in that case, the determinant of P is zero and P becomes singular. Thus, any form equivalent to $x^2 + xy + y^2$ has at least two squares.

Now we shall determine the orthogonal group. Referring to the matrix P of eq.(2), we have to find the subgroup of all such P that preserves $x^2 + xy + y^2$ and it is advantageous to think of P as consisting of four 2×2 blocks. It follows from the analysis above that if P is orthogonal $c = d = g = h = 0$. The quadratic form changes now to

$$(a^2 + ae + e^2)X^2 + (af + be)XY + (b^2 + bf + f^2)Y^2. \quad (7)$$

Furthermore $\det P$ is given by $(af + be)(kr + mq)$. The matrices $\begin{bmatrix} a & e \\ b & f \end{bmatrix}$ must have determinant 1. The space of such matrices is of order six and itself determines a group isomorphic to S_3: generators are given by $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, for example. Precisely the same situation holds for the matrix $\begin{bmatrix} k & m \\ q & r \end{bmatrix}$, which produces another copy of S_3. Finally, the entries $\begin{bmatrix} i & j \\ n & p \end{bmatrix}$ are arbitrary in $\mathbb{Z}_2$ and the corresponding 4×4 matrices with the identity in the upper left 2×2 block, engenders the direct product of four copies of the group $\mathbb{Z}_2$. Altogether, the orthogonal group of $x^2 + xy + y^2$ is the semi-direct product $(S_3 \times S_3) \triangleleft (\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2)$ and has order $36 \times 16 = 576$.

4.2 0

The orthogonal group is a simple group $GL(4, \mathbb{Z}_2)$ of order 20160.

4.3 x^2

The orthogonal group is a subgroup of $GL(4, \mathbb{Z}_2)$ and consists of matrices of the form $\begin{bmatrix} 1 & 0 & 0 & 0 \\ a & b & c & d \\ e & f & g & h \\ i & j & k & m \end{bmatrix}$ where $bgm + bhk + cfm + chj + dfk + dgj = 1$; it is a semi-direct product of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the simple group of order 168. The order of the group is $8 \times 168 = 1344$.

4.4 xy

The orthogonal group is a subgroup of $GL(4, \mathbb{Z}_2)$ and consists of matrices of the form $\begin{bmatrix} a & 1+a & 0 & 0 \\ 1+a & a & 0 & 0 \\ i & j & k & m \\ n & p & q & r \end{bmatrix}$ where $kr + qm = 1$. The group is a semi-direct product $(\mathbb{Z}_2 \times S_3) \triangleleft 4\mathbb{Z}_2$. Its order is 192.

4.5 $xy + yz + zx$

Under the transformation P the form $xy + yz + zx$ changes according to

$$\begin{aligned}&(ae + ai + ei)\,X^2 + (af + aj + be + bi + ej + fi)\,XY + (ag + ak + ce + ci\\&+ek + gi)XZ + (ah + am + de + di + em + hi)\,TX + (bf + bj + fj)\,Y^2\\&+(bg + bk + cf + cj + fk + gj)YZ + (bh + bm + df + dj + fm + hj)\,TY + (cg\\&+ck + gk)Z^2 + (ch + cm + dg + dk + gm + hk)\,TZ + (dh + dm + hm)\,T^2\end{aligned} \tag{8}$$

The only way that the coefficient of X^2 can be zero is either to have $a = e = i = 0$, in which case the term in XY would be absent, or to have one of a, e, i being 1 and the other two zero. In fact one finds that the upper 3×3 block is a permutation of the columns of the identity. Then in order for the coefficients of XT, YT, ZT we will require that $d = h = m$ but then the coefficient of T^2 gives $d = h = m = 0$. The determinant of P is now found to be r and so we must have $r = 1$ and $n, p, q \in \mathbb{Z}_2$ are arbitrary. We find that the orthogonal group is a semi-direct product $S^3 \triangleleft (\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2)$ and its order is 48.

4.6 $xy + zt$

Under the transformation P the form $xy + zt$ changes according to

$$\begin{aligned}&(ae + in)\,X^2 + (af + be + ip + jn)\,XY + (ag + ce + iq + kn)\,XZ + (ah + de\\&+ir + mn)TX + (bf + jp)\,Y^2 + (bg + cf + jq + kp)\,YZ + (bh + df + jr + mp)\,TY\\&+ (cg + kq)\,Z^2 + (ch + dg + kr + mq)\,TZ + (dh + mr)\,T^2.\end{aligned} \tag{9}$$

If P is orthogonal the coefficient of X^2 is zero which gives $ae + in = 0$. There are only ten possible solutions:

- $a = e = i = n = 0$
- $a = e = i = n = 1$
- three of a, e, i, n equal to 0 and the remaining entry equal to 1
- $[a, e, i, n] = [1, 0, 1, 0], [a, e, i, n] = [1, 0, 0, 1], [a, e, i, n] = [0, 1, 1, 0]$ and $[a, e, i, n] = [1, 0, 0, 1]$.

Of these solutions, the first is untenable or else P will be singular. The same conditions apply to the remaining three columns of P. As such there are, in principle, $9 \times 8 \times 7 \times 6 = 3024$ matrices that have to be considered. However, if we consider eq(4.6), we see that under a permutation, the coefficients of $X^2, Y^2, ..., T^2$ are unchanged although they will be reassigned to different monomials. As such the order of the columns is relatively immaterial as concerns finding an orthogonal transformation. This observation enables us to reduce the number of possible matrices to $\binom{9}{4} = 126$. What is required then, is to sift through this list of 126 matrices and identify the ones that are non-singular and for which precisely two of the cross terms are non-zero. It is then possible to change the quadratic form to $xy + zt$ by applying a suitable permutation. We find that the following set of "P"-matrices eq.((2) satisfy the two conditions:

$$\begin{aligned}A &= \begin{bmatrix}1&0&1&0\\0&1&0&0\\0&1&0&1\\0&0&1&0\end{bmatrix} \quad B = \begin{bmatrix}1&0&1&0\\0&1&0&0\\0&0&1&0\\0&1&0&1\end{bmatrix} \quad C = \begin{bmatrix}1&1&1&1\\0&1&0&0\\0&1&0&1\\0&1&1&0\end{bmatrix} \quad E = \begin{bmatrix}0&1&0&0\\1&0&0&1\\0&1&1&0\\0&0&0&1\end{bmatrix}\\ F &= \begin{bmatrix}0&1&0&0\\1&0&0&1\\0&0&0&1\\0&1&1&0\end{bmatrix} \quad G = \begin{bmatrix}0&1&0&0\\1&1&1&1\\0&1&0&1\\0&1&1&0\end{bmatrix} \quad H = \begin{bmatrix}0&1&0&1\\0&1&1&0\\1&1&1&1\\0&1&0&0\end{bmatrix} \quad J = \begin{bmatrix}0&1&0&1\\0&1&1&0\\0&1&0&0\\1&1&1&1\end{bmatrix}.\end{aligned} \tag{10}$$

We should note also that the subgroup of *permutations* that preserves $xy + zt$ is isomorphic to D_8, the dihedral group of order 8 that is generated by $R = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix}$ and $S = \begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 0&1&0&0 \\ 1&0&0&0 \end{bmatrix}$. They do not arise as separate solutions because they are permutations of the identity matrix.

Let us note that $A = S^2FS^2R, B = RFS^2R, C = SF^3RFR, E = RS^2F, G = S^3RF^3RFR, H = RF^3RFRF, J = RS^2RF^3RFRF, S = F^3R$ where, of course, all products are calculated "mod 2" . It follows that the orthogonal group is generated by F and R only, subject to the relations $R^2 = F^6 = I$ and $RF^3RF^3 = F^3RF^3R$, the latter relation following from $S^3R = RS$ after eliminating S. In fact it is also true that $RF^2RF^2 = F^2RF^2R$ and $RF^4RF^4 = F^4RF^4R$.

It turns out that the group generated by R and F has order 72. The Sylow 3-subgroup is a unique and therefore normal and of course abelian since it has order 9. Its elements consist of

$$\{I, F^2, F^4, RF^2R, RF^4R, F^2RF^2R, F^4RF^4R, F^4RF^2R, F^2RF^4R\} :$$

the fact that this subgroup is abelian of order nine implies the various relations between F and R mentioned above. One of the Sylow 3-subgroups is the group D_8 alluded to above and in terms of F and R it may be written as

$$\{I, F^3R, F^3RF^3R, RF^3, R, F^3, F^3RF^3, RF^3R.\}$$

However, it is not normal; for example, $F^{-1}F^3RF = F^2RF = \begin{bmatrix} 1&1&1&1 \\ 0&0&0&1 \\ 0&1&0&1 \\ 1&0&0&1 \end{bmatrix}$ whereas all the matrices in D_8 are permutations. The conclusion is that the orthogonal group is a semi-direct product $D_8 \triangleleft (\mathbb{Z}_3 \oplus \mathbb{Z}_3)$.

4.7 $xy + yz + zx + xt + yt + zt$

In this case under the transformation P the quadratic form is changed into

$$\begin{aligned} &(ae + ai + an + ei + en + in)\, X^2 + (af + aj + ap + be + bi + bn + ej + ep \\ &+fi + fn + ip + jn)XY + (ag + ak + aq + ce + ci + cn + ek + eq + gi + gn \\ &+iq + kn)XZ + (ah + am + ar + de + di + dn + em + er + hi + hn + ir + mn) \\ &TX + (bf + bj + bp + fj + fp + jp)\, Y^2 + (bg + bk + bq + cf + cj + cp + fk \\ &+fq + gj + gp + jq + kp)YZ + (bh + bm + br + df + dj + dp + fm + fr + hj \\ &+hp + jr + mp)TY + (cg + ck + cq + gk + gq + kq)\, Z^2 + (ch + cm + cr + dg \\ &+dk + dq + gm + gr + hk + hq + kr + mq)TZ + (dh + dm + dr + hm + hr \\ &+mr)T^2. \end{aligned} \tag{11}$$

If P is orthogonal we need to have $ae + ai + an + ei + en + in = 0$ and likewise for the other columns. The only way to satisfy such an equation, apart form having $a = e = i = n = 0$, is to have just one of a, e, i, n equal to one or to have $a = e = i = n = 1$. Thus the orthogonal group can be described as follows. Every column has either one 1 and three 0's or there is one column with four 1's. Those non-singular matrices each of which have four columns that have one 1 and three 0's are permutations and S_4 is a subgroup of the orthogonal group with order 24. For the other elements, pick any column and assigns it four 1's (four such choices); next, pick one of the remaining columns and put a 1 in any of the four entries (four such choices); now go to one of the remaining two columns and put a 1 in a row that is different from the 1 assigned to the previous

column (three such choices); finally go to the last column and put a 1 in either of the rows which do not already contain two 1's (two such choices). Altogether we obtain $4 \times 4 \times 3 \times 2 = 96$. Together with the permutations we have a group of order 120 which is in fact S_5. To understand why we obtain S_5 we begin by taking the matrices such as $M_{12} = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix}$ to define the transpositions of the subgroup S_4. For the remaining four transpositions of S_5 we define

$$M_{15} = \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \end{bmatrix} \; M_{25} = \begin{bmatrix} 1&1&0&0 \\ 0&1&0&0 \\ 0&1&1&0 \\ 0&1&0&1 \end{bmatrix} \; M_{35} = \begin{bmatrix} 1&0&1&0 \\ 0&1&1&0 \\ 0&0&1&0 \\ 0&0&1&1 \end{bmatrix} \; M_{45} = \begin{bmatrix} 1&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&0&0&1 \end{bmatrix}.$$

Then $M_{12}, M_{13}, ..., M_{45}$, or in fact just of four of them, will generate the orthogonal group. For example $M_{15}M_{25}M_{35}M_{45}$ is the matrix $M_{12345} = \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 1&0&0&0 \end{bmatrix}$ which is a 5-cycle.

5 Equivalence of quadratic Forms

Now we shall take up the issue of showing that the seven canonical forms are mutually inequivalent. We know in the first place that 0 and x^2 are not equivalent to each other nor to any of the other five forms. For the other forms we note that if two forms are equivalent then they must have isomorphic orthogonal groups; for, an equivalence will induce an isomorphism of orthogonal groups and an orthogonal group is nothing but the set of self-equivalences. Thus:

Theorem 5.1. *Every quadratic form in four variables x, y, z, t with coefficients in $\mathbb{Z}_2$ is equivalent to precisely one of $0, x^2, xy, xy + zt, xy + yz + zx, x^2 + xy + y^2, xy + yz + zx + xt + yt + zt$.*

6 Quadratic Forms in Three Variables

The equivalence of quadratic forms in three variables was considered in [10]. Now we shall revisit the issue in light of the conclusions made in this paper. Thus every form in three variables is equivalent to one of $\{0, x^2, xy, xy + xz + yz, x^2 + xy + y^2\}$. Explicit equivalences to these forms can be read off from Section 5 by considering forms and their isomorphs that only involve three variables. For, example $x^2 + xy + y^2$ is equivalent only to $x^2 + y^2 + z^2 + xy + xz$ and $x^2 + y^2 + z^2 + xy + xz + yz$. We note also that the orthogonal groups of $0, x^2, xy, xy + xz + yz, x^2 + xy + y^2$ are, respectively, $GL(3, \mathbb{Z}_2), S_3 \lhd (\mathbb{Z}_2 \oplus \mathbb{Z}_2), D_8, S_3, S_3 \lhd (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

7 Conclusion

In this article we have extended the study of quadratic forms in three variables [10] to four variables. At the end we discern a list of precisely seven such inequivalent forms. We have also studied the orthogonal group of each such form. In the future we hope to be able to extend our work so as to include quadratic forms with more than four variables. It is clear, however, that some new techniques will be needed since the problem is of a completely different magnitude.

Acknowledgements

The authors thank Akaki Tikaradze and Charles Odenthal for helpful discussions.

Competing Interests

The Authors declared that they have no competing interests. The material in this article has not been, nor is currently under consideration for publication in any other journal or in any other publishing format.

References

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

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

[3] Fitzgerald RW, Yucas JL. Pencils of quadratic forms over finite fields. Discrete Mathematics. 2004;283:71-79.

[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.

[10] Thompson G. Classifying quadratic forms over $\mathbb{Z}_2$ in three variables. Hindawi Journal of Mathematics. 2016;8(3):740-763

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.sciencedomain.org/review-history/25717