Orthogonal geometry over the field with two elements

J.I. Hall
Michigan State University
East Lansing, MI, 48824, USA

PJC60, Ambleside

I. Introduction
A. A nonexample

Nonexample (PJC and JIH 1984)

In a projective space $\mathcal{P}$ over $\mathbb{D}$ consider a chain of subspaces with union $\mathcal{P}$. Color the gaps between spaces alternately green and white. Then every line of $\mathcal{P}$ has either 0 or 1 points that are green or 0 or 1 points that are white.
Conversely, any green-white coloring of the points of $\mathcal{P}$ that has this property comes about in this way.

Two difficulties: (1) If $\mathcal{P}$ has uncountable rank we have to be careful about what we mean.

(2) What about $\mathbb{D} = \mathbb{F}_2$ where lines only have three points?

In the case $\mathbb{D} = \mathbb{F}_2$ we get the same result with the same proof provided we assume additionally:

In no projective plane of $\mathcal{P}$ are the green points or the white points exactly the three points of a triangle.

. . . that is:

No projective plane has an orthogonal geometry of type $\mathrm{O}_3(2)$ induced upon it by the coloring.

B. Definition(s)

An *orthogonal geometry* is a vector space V equipped with a quadratic form Q or the associated projective space $\mathbb{P}V$ equipped with the corresponding lattice of totally singular subspaces. Over $\mathbb{F}_2$ the distinction is small since $\mathbb{P}V$ is essentially $V \setminus \{0\}$.

Definition

Let V be a vector space over the field $\mathbb{F}$. A quadratic form is a map $Q\colon V \longrightarrow \mathbb{F}$ with:

- $Q(\,(x_1, \ldots, x_i, \ldots)\,) = \sum_{i \leq j} a_{i,j} x_i x_j$ for fixed $a_{i,j} \in \mathbb{F}$;
  OR
- $Q(ax) = a^2 Q(x)$, for all $a \in \mathbb{F}$ and $x \in V$; and

$$B(x, y) = Q(x + y) - Q(x) - Q(y)$$

is an $\mathbb{F}$-bilinear form.

Remarks.

- If $\mathbb{F}$ has characterisitic not 2, then Q can be reconstructed from the symmetric bilinear form B.
- If Char $\mathbb{F} = 2$, then B is alternating (that is, symplectic).
- If $\mathbb{F}$ is perfect of characteristic 2 then the bilinear form

  $$B(ax, by) = Q(ax + by) - a^2 Q(x) - b^2 Q(y)$$

  gauges the extent to which Q fails to be a semilinear transformation with respect to the Frobenius automorphism.
- If $\mathbb{F} = \mathbb{F}_2$ then Q is defined by $Q(0) = 0$ and the biadditive form

  $$B(x, y) = Q(x + y) + Q(x) + Q(y)$$

  which gauges how much Q fails to be a linear functional.

Rewrite the defining equation as

$$Q(ax+by) = B(ax,by) - a^2 Q(x) - b^2 Q(y)\,.$$

The form Q is therefore uniquely determined by the form B and the values of Q at any basis of V.

The radical of the form B is

$$\mathrm{Rad}(B) = \{\, v \in V \mid B(v,x) = 0,\ \text{all } x \,\}$$

The rank of the forms B and Q is the codimension of $\mathrm{Rad}(B)$ in V.

From now on we will assume our field is $\mathbb{F}_2$.

The restriction of Q to the radical $\mathrm{Rad}(B)$ is a linear functional. Its kernel is the singular radical

$$\mathrm{SRad}(Q) = \{\, v \in V \mid Q(v) = 0,\ B(v,x) = 0,\ \text{all } x \,\},$$

which therefore has codimension 0 or 1 in $\mathrm{Rad}(B)$.

We say that Q is nondegenerate if $\mathrm{Rad}(B) = 0$ and nonsingular if $\mathrm{SRad}(Q) = 0$.

The form Q induces a nonsingular quadratic form on $V/\,\mathrm{SRad}(V)$.

Example

Types of forms in low dimension.

1. $V = \{0, v\}$ of dimension 1 must have rank 0.
   (i) Singular: $Q(v) = 0$, $Q(0) = 0$.
   (ii) Nonsingular: $Q(v) = 1$, $Q(0) = 0$.
2. $V = \{0, v, w, v + w\}$ of dimension 2.
   (i) Rank 0, totally singular: $Q(v) = Q(w) = Q(v + w) = 0$.
   (ii) Rank 0, defective: $Q(v) = 0$, $Q(w) = Q(v + w) = 1$.
   (iii) Rank 2, totally nonsingular :
   $Q(v) = Q(w) = Q(v + w) = 1$.
   (iv) Rank 2, hyperbolic : $Q(v) = Q(w) = 0$, $Q(v + w) = 1$.
3. $V = \langle v, w, x\rangle$ of dimension 3.
   (i) Rank 0, totally singular: $Q(v) = Q(w) = Q(x) = 0$.
   (ii) Rank 0, defective: $Q(v) = Q(w) = 0$, $Q(x) = 1$.
   (iii) Rank 2, degenerate: $\{0, x\} = \mathrm{Rad}\, B$ with $Q(x) = 0$.
   (iv) Rank 2, nonsingular: $\{0, x\} = \mathrm{Rad}\, B$ with $Q(x) = 1$.

C. Some areas of application

Questions involving orthogonal geometry over $\mathbb{F}_2$ have come in varied contexts:

lie algebras
group cohomology
quantum error correction
pseudorandom sequences
Grassmann spaces
lattice theory
local graph theory
double Bruhat cells
vertex operator algebras

singularity theory
extraspecial groups
Moufang loops
coding theory
translation planes
mapping class groups
cluster algebras

II. Characterisations
A. Linear algebra

Call a function $F\colon V \longrightarrow \mathbb{F}_2$ *k*-even if on each k-subspace it takes the value 1 an even number of times. By inclusion-exclusion, if F is k-even, then it is m-even for all $m \geq k$.

Example

1. $k = 1$. On each 1-space $\{0, v\}$ we have have $F(0) = F(v)$. That is, F is a constant function.
2. $k = 2$. Assume $F(0) = 0$. Then always

   $$F(x + y) = F(x) + F(y)\,,$$

   and F is a linear functional.

Theorem

Let V be a vector space of $\mathbb{F}_2$ and $Q\colon V \longrightarrow \mathbb{F}_2$ with $Q(0) = 0$. Then Q is a quadratic form if and only if it is 3-even.

PROOF. As $Q(0) = 0$ by assumption, we must prove that $B(x, y) = Q(x) + Q(y) + Q(x + y)$ is biadditiive. Clearly $B(x, y) = B(y, x)$ and $B(x, x) = 0$.

Since Q is 3-even, $B(x + y, z) + B(x, z) + B(y, z)$ is a sum of an even number of 1's and so is 0.

B. Incidence geometry

Consider partial linear spaces (collections of points and lines with two lines meeting in at most one point) that mimic the set of totally singular lines and the set of totally nonsingular lines.

That is, for a fixed $\alpha = 0, 1$, consider a set of points $\mathcal{P}$ and set of lines $\mathcal{L}$ such that each line is a 3-subset of $\mathcal{P}$ and for each line ℓ and point $p \notin \ell$ we have

- $\alpha = 0$ and p is collinear with either 1 or 3 points of ℓ;
- $\alpha = 1$ and p is collinear with either 0 or 2 points of ℓ.

We hope to prove that there is a vector space V and quadratic form Q with $\mathcal{P}$ the nonzero vectors with $Q(v) = \alpha$.

Let $V_0 = {\mathbb{F}_2}^{\mathcal{P}}$, and define the quadratic from Q_0 on V_0 by

$$\begin{array}{rcl} Q_0(x) & = & \alpha\,,\ \text{for } x \in \mathcal{P}\,,\ \text{and} \\ B(x,y) & = & \alpha\,,\ \text{for } x, y \text{ collinear,} \\ & = & 1-\alpha\,,\ \text{for } x, y \text{ not collinear.} \end{array}$$

Lemma

If $\{x, y, z\}$ is a line of $\mathcal{L}$, then in V_0 we have $x + y + z \in \mathrm{SRad}(Q_0)$.

Therefore $V = V_0/\,\mathrm{SRad}(Q_0)$ equipped with the induced form Q gives a nonsingular space in which each line of $\mathcal{L}$ become a line (that is, a 2-space less 0) of the desired type.

A nondegeneracy condition gives injectivity on $\mathcal{P}$.

For $\alpha = 0$ it is now possible to show that every vector of V is the sum of at most three images of points, and we find

Shult's Triangle Theorem

For $\alpha = 0$ we have the singular points (1-spaces) and totally singular lines (2-spaces) of a nonsingular quadratic form.

For $\alpha = 1$ we are headed towards Shult's Cotriangle Theorem, but we cannot bound length. More examples than that of totally nonsingular points and lines do occur.

C. Group theory

Let the group G be generated by the conjugacy class D of involutions. Then G (more properly, (G, D)) is a 3-transposition group provided:

$$\text{for } d, e \in D,\ |de| = 1, 2,\ \text{or } 3\,.$$

The motivating example is given by the transposition class of the symmetric group.

3-transposition groups were introduced by Bernd Fischer, and three of the sporadic finite simple groups arise as examples.

The diagram of a set Δ of 3-transpositions is the graph with the set as vertices and two adjacent when their product has order 3.

Theorem

The following are equivalent:
(1) *A 3-transposition group* (G, D) *in which, for* $d, e, f \in D$, *we never have* $|\langle d, e, f \rangle|$ *equal to* 18 *or* 54*.*
(2) *A connected partial linear space* $(\mathcal{P}, \mathcal{L})$ *in which the subspace generated by a pair of intersecting lines is always dual affine of order* 2 *(a Pasch configuration).*

This result connects the present discussion with that of the previous section since the spaces of (2) are examples of cotriangular spaces—they satisfy the $\alpha = 1$ condition.

Proof.

(1) $\Longleftarrow$ (2): For each point $p \in \mathcal{P}$ let τ_p be the involutory permuation of $\mathcal{P}$ that fixes p and all points not collinear with p and switches the two remaining points on all lines on p. Then $D = \{ \tau_p \mid p \in \mathcal{P} \}$ is a class of 3-transpositions in $\mathrm{Aut}(\mathcal{P}, \mathcal{L})$.

(1) $\Longrightarrow$ (2): The point set $\mathcal{P}$ is D and a line of $\mathcal{L}$ consists of the three 3-transpositions in a subgroup $\mathrm{Sym}(3)$.

Three 3-transpositions have a diagram that either is a spherical Dynkin diagram or is affine of type $\tilde{A}_2$. The weird numerology implies that in that last case, the three must generate $\mathrm{Sym}(4)$ (or $\mathrm{Sym}(3)$).

The 3-transposition groups satisfying the condition (1) are usually called symplectic 3-transposition groups.

Remarks.

- The symmetric group satisfies the numerology. That is, the symmetric group is a symplectic 3-transposition group.
- $(\mathcal{P}, \mathcal{L})$ satisfies the earlier condition for $\alpha = 1$.

We now can state

Shult's Cotriangle Theorem

For $\alpha = 1$ we have the nonsingular points and totally nonsingular lines of a nonsingular quadratic form or we have the 2-subsets (points) and 3-subsets (lines) of a set.

Remember that we have an (unstated) nondegeneracy condition.

D. Groups generated by orthogonal transvections

Let x be a nonsingular vector for the quadratic form Q on the $\mathbb{F}_2$-vector space V. Then the linear transformation

$$\tau_x \colon v \mapsto v + B(v,x)x$$

is an orthogonal transvection. It is an isometry of Q in that

$$Q(v) = Q(v.\tau_x)$$

for all $v \in V$.

We write $\mathrm{O}_n^{\epsilon}(2)$ for the isometry group of a nonsingular form in dimension n with type ϵ. (If n is odd, then ϵ is not necessary.)

And the choice of notation is not a coincidence. The 3-transposition permutation τ_p that we saw earlier induces the appropriate orthogonal transvection on the space V constructed from the cotriangular space.

Indeed the class of orthogonal transvections in $\mathrm{O}_n^{\epsilon}(2)$ is a generating conjugacy class of 3-transpositions of symplectic type.

Conversely it can be shown that the symplectic 3-transposition groups and cotriangular spaces of the TFAE Theorem are precisely those associated with groups generated by orthogonal transvections.

The appropriate classification (now with no degeneracy restrictions) is then:

Theorem

Let Q be a quadratic form on the $\mathbb{F}_2$-space V. Let G be an isometry group of V generated by a G-conjugacy class of orthogonal reflections and having $[V, G] = V$. Then

- *$G = E \rtimes X$ with E an elementary abelian 2-group.*
- *X is isomorphic to $\mathrm{O}_n^{\epsilon}(2)$ or $\mathrm{Sym}(n+1)$.*
- *E is a direct sum of m copies of the natural n dimensional $\mathbb{F}_2$-module for X with $\dim_{\mathbb{F}_2} V = n + m$.*

Results of this type go back to McLaughlin.

Examples: $\mathrm{W}(A_n) = \mathrm{Sym}(n+1)$, $\mathrm{W}(D_n) = 2^{n-1} \rtimes \mathrm{Sym}(n)$, $\mathrm{W}(E_6) = \mathrm{O}_6^-(2)$.

III. Applications
A. Double Bruhat cells

Let G be an $\mathbb{R}$-split simply connected algebraic group with split torus H and Weyl group $W = N_G(H)/H$. Let B^+ and B^- be two opposite Borel subgroups with $B^+ \cap B^- = H$.

A double Bruhat cell is any one of the intersections

$$G^{(u,v)} = B^+ u B^+ \cap B^- v B^-$$

with (by slight abuse) $(u,v) \in W \times W$. Thus

$$G = \bigcup_{(u,v) \in W \times W} G^{(u,v)} .$$

The group H is regular on each double Bruhat cell with a natural section being given by the reduced double Bruhat cell

$$L^{(u,v)} = N^+ u N^+ \cap B^- v B^-$$

where N^+ is the unipotent radical of B^+. (more abuse)

It turns out (work of many) that the number of connected components of $L^{(u,v)}$ is equal to the number of orbits of a certain group generated by orthogonal transvections acting on $V = \mathbb{F}_2{}^{\ell(u)+\ell(v)}$.

The calculation is relevant for

- total positivity in semisimple groups
- symplectic leaves in semisimple groups
- classifying cluster algebras of finite/infinite type

A small gem that came up in this work:

Seven's Lemma

For a connected diagram Δ, the corresponding group generated by orthogonal transvections of Δ is of orthogonal (rather than symmetric) type if and only if Δ has a six vertex subdiagram Δ_0 whose transvections generate a subgroup $O_6^-(2)$.

B. Vertex operator algebras

Let $V = \bigoplus_{n \geq 0} V_{(n)}$ be a graded $\mathbb{C}$-space having a positive definite form and with $V_{(0)} = \mathbb{C}\mathbf{1}$ and $V_{(1)} = 0$.
We can (almost) give V the structure of a vertex operator algebra by defining a $\mathbb{C}$-algebra multiplication

$$V((z)) \otimes V((z)) \longrightarrow V((z))$$

with certain properties:

1. $z^i \cdot z^j = z^{i+j}$.
2. $\mathbf{1}$ "is" an identity element.
3. For $Y(A, z)$ the endomorphism of $V((z))$ given by fixing A of V, "we have" for sufficiently large N
$$(z - w)^N Y(A, z) Y(B, w) = (z - w)^N Y(B, w) Y(A, z)\,.$$
4. There are elements $e \in V_{(2)}$ that generate a Virasoro subalgebra acting on V.

Virasoro algebras are infinite dimension Lie algebras and have only three types of irreducible modules:

$$L(1/2,0), L(1/2,1/2), L(1/2,1/16)\,.$$

Consider the collection of all e as in the last axiom which in their action on V have no constituents $L(1/2,1/16)$. Define

$$\begin{aligned} \tau_e &= +id \text{ on each constituent } L(1/2,0) \\ \tau_e &= -id \text{ on each constituent } L(1/2,1/2). \end{aligned}$$

Then

Miyamoto, Matsuo

The collection of all such τ_e form a conjugacy class of 3-transpositions of symplectic type.