Ovoids over $\mathbb{Z}/m\mathbb{Z}$

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

26 Sept 2008 / RMAC Seminar

Projective n-space over $\mathbb{Z}/m\mathbb{Z}$

Let $R = \mathbb{Z}/m\mathbb{Z}$.

Projective n-space over R is the incidence system $PG(n, R)$ formed by the free R-submodules of R^{n+1} under inclusion.

Objects: submodules $U \leqslant R^{n+1}$ of rank $k = 1, 2, \ldots, n$ (so $U \cong R^k$)

$k = 1$: points
$k = 2$: lines
general k: 'subspace' of projective dimension $k-1$

Projective n-space over $\mathbb{Z}/m\mathbb{Z}$

$m = rs$

Suppose $\gcd(r, s) = 1$. The isomorphism

$$\mathbb{Z}/rs\mathbb{Z} \;\cong\; \mathbb{Z}/r\mathbb{Z} \;\oplus\; \mathbb{Z}/s\mathbb{Z}$$

induces

$$PG(n, \mathbb{Z}/rs\mathbb{Z}) \;\cong\; PG(n, \mathbb{Z}/r\mathbb{Z}) \;\times\; PG(n, \mathbb{Z}/s\mathbb{Z})$$

$$GL(n{+}1, \mathbb{Z}/rs\mathbb{Z}) \;\cong\; GL(n{+}1, \mathbb{Z}/r\mathbb{Z}) \;\times\; GL(n{+}1, \mathbb{Z}/s\mathbb{Z})$$
$$PGL(n{+}1, \mathbb{Z}/rs\mathbb{Z}) \;\cong\; PGL(n{+}1, \mathbb{Z}/r\mathbb{Z}) \;\times\; PGL(n{+}1, \mathbb{Z}/s\mathbb{Z})$$

Projective n-space over $\mathbb{Z}/q\mathbb{Z}$

$q = p^\nu$, $\nu \geqslant 1$

Reduction mod p gives a $\frac{q}{p}$-to-one map

$$\mathbb{Z}/q\mathbb{Z} \;\rightarrow\; \mathbb{Z}/p\mathbb{Z}$$

and a map

$$PG(n, \mathbb{Z}/q\mathbb{Z}) \;\rightarrow\; PG(n, \mathbb{Z}/p\mathbb{Z})$$

which is $\left(\frac{q}{p}\right)^n$-to-one on points.

So $PG(n, \mathbb{Z}/q\mathbb{Z})$ has

$$(p^n + p^{n-1} + \cdots + p + 1)\left(\frac{q}{p}\right)^n$$

points.

Projective n-space over a local ring R

More generally, let R be a ring with unique maximal ideal $M \subset R$ and residue field $F = R/M$.

$PG(n, R)$ is formed by the free R-submodules of R^{n+1} of rank $k = 1, 2, \ldots, n$ with inclusion relation.

The reduction mod M:

$$R \to F$$

induces a map

$$PG(n, R) \;\to\; PG(n, F)$$

which is $|M|^n$-to-one on points.

Examples

- $R = \mathbb{Z}/p^\nu\mathbb{Z}, \;\; M = pR, \; F = \mathbb{F}_p$
- R a Galois ring, $\;F$ its residual Galois field
- $R = \mathbb{Z}_p = \{p\text{-adic integers}\}, \;\; F = \mathbb{F}_p$

Quadratic Forms over R

A *quadratic form* on $V = R^{n+1}$ is a homogeneous polynomial of degree 2:

$$Q : R^{n+1} \to R$$

$$Q(x) = \sum_{0 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j$$

Its associated bilinear form is

$$B(x, y) = Q(x + y) - Q(x) - Q(y) = \sum_{0 \leqslant i \leqslant j \leqslant n} a_{ij}(x_i y_j + x_j y_i)$$

For a submodule $U \subseteq R^{n+1}$,

$$U^\perp = \{x \in R^{n+1} \,:\, B(x, u) = 0 \text{ for all } u \in U\}.$$

Assume B is *nondegenerate*, i.e. $V^\perp = 0$.

Quadrics over R

Let $U \subset R^{n+1}$ be a free R-submodule of rank k.

U is *totally singular* if $Q(u) = 0$ for all $u \in U$.
(This implies that $U \subseteq U^{\perp}$.)

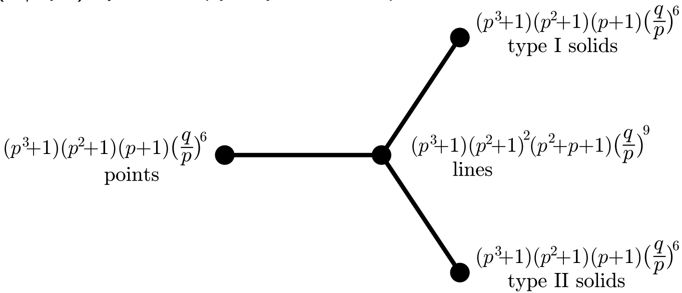
(For $k = 1$, we speak simply of a *singular point*).
The *quadric* corresponding to Q is the set of singular points in $PG(n, R)$.

Hyperbolic Quadrics over R

A quadratic form on R^{2k} is *hyperbolic* (i.e. of type $O^+_{2k}(R)$) if it is equivalent under $GL(2k, R)$ to

$$x_0x_1 + x_2x_3 + \cdots + x_{2k-2}x_{2k-1}\ .$$

The $O^+_8(\mathbb{Z}/q\mathbb{Z})$ quadric ($q = p^\nu,\ \nu \geqslant 1$) has



Ovoids in $O_8^+(R)$

An *ovoid* in $O_8^+(R)$ is a set $\mathcal{O}$ of singular points, such that every totally singular solid contains a unique point of $\mathcal{O}$.

A set $\mathcal{O}$ consisting of singular points in $O_8^+(\mathbb{Z}/q\mathbb{Z})$, $q = p^\nu$, $\nu \geqslant 1$, no two of which are perpendicular, satisfies

$$|\mathcal{O}| \leqslant \frac{(p^3+1)(p^2+1)(p+1)\left(\frac{q}{p}\right)^6}{(p^2+1)(p+1)\left(\frac{q}{p}\right)^3} = (p^3+1)\left(\frac{q}{p}\right)^3$$

and equality holds iff $\mathcal{O}$ is an ovoid.

The E_8 Root Lattice

Define the lattice $E_8 \subset \mathbb{R}^8$ by

$$E_8 = \left\{ \tfrac{1}{2}(x_1, x_2, \ldots, x_8) \;:\; x_i \in \mathbb{Z},\;\; x_1 \equiv x_2 \equiv \cdots \equiv x_8 \bmod 2,\; \textstyle\sum x_i \equiv 0 \bmod 4 \right\}.$$

Every vector $v \in E_8$ has *norm* $\|v\|^2 \in \{0, 2, 4, 6, \ldots\}$, and the number of vectors of norm $2k \geqslant 2$ is

$$240\sigma_3(k), \qquad \sigma_3(k) = \sum_{1 \leqslant d \,|\, k} d^3.$$

For each $m \geqslant 2$, $E_8/mE_8 \cong R^8$ where $R = \mathbb{Z}/m\mathbb{Z}$.
The quadratic form $Q : R^8 \to R$ defined by

$$Q(x) = \tfrac{1}{2}\|x\|^2 \mod m$$

is of type $O_8^+(R)$.

Conway's ovoids

A vector $v \in E_8$ is *primitive* if for all $k \geqslant 2$ we have $v \notin kE_8$.

Let $R = \mathbb{Z}/m\mathbb{Z}$, $m \geqslant 2$. Let $e \in E_8$ of norm 2 (a *root vector*, e.g. $e = \frac{1}{2}(1,1,1,1,1,1,1,1)$).

Theorem

Let $m \geqslant 3$ be odd. The set

$$\mathcal{S}_m = \{v \in e + 2E_8 \ : \ v \text{ primitive of norm } 2m\}$$

gives an ovoid in $E_8/mE_8 \cong O_8^+(\mathbb{Z}/m\mathbb{Z})$.

Due to Conway et. al. (1988) in the case m is an odd prime.

Example: Conway's ovoid in $O_8^+(\mathbb{Z}/9\mathbb{Z})$

Let $m = 9$. Ovoids in $O_8^+(\mathbb{Z}/9\mathbb{Z})$ have size $(3^3+1)\cdot 3^3 = 756$. The set

$$\mathcal{S}_9 = \{v \in e + 2E_8 \ : \ v \text{ primitive of norm } 18\}$$

consists of

$\pm\frac{1}{2}(5^2, -3^2, 1^4)$	(420 such pairs)
$\pm\frac{1}{2}(-7, -3^2, 1^5)$	(168 such pairs)
$\pm\frac{1}{2}(5, -3^5, 1^2)$	(168 such pairs)
total	756 pairs

$\mathcal{O}$ consists of 756 singular points $\langle(5^2, 6^2, 1^4)\rangle$, $\langle(2, 6^2, 1^5)\rangle$, $\langle(5, 6^5, 1^2)\rangle$ in $O_8^+(\mathbb{Z}/9\mathbb{Z})$. Under the reduction mod 3

$$O_8^+(\mathbb{Z}/9\mathbb{Z}) \to O_8^+(\mathbb{Z}/3\mathbb{Z})$$

we obtain *nothing like an ovoid* (28 singular points in $O_8^+(3)$, mutually nonperpendicular).

Example: Conway's ovoid in $O_8^+(\mathbb{Z}/15\mathbb{Z})$

Let $m = 15$. Ovoids in $O_8^+(\mathbb{Z}/15\mathbb{Z})$ have size $(3^3+1)(5^3+1) = 3528$. The set

$$\mathcal{S}_{15} = \{v \in e + 2E_8 \; : \; v \text{ primitive of norm } 30\}$$

consists of

$\pm\frac{1}{2}(9,-3^4,1^3)$	(280 such pairs)
$\pm\frac{1}{2}(9,5,-3,1^5)$	(336 such pairs)
$\pm\frac{1}{2}(-7^2,-3^2,1^4)$	(420 such pairs)
$\pm\frac{1}{2}(-7,5^2,-3^2,1^3)$	(1680 such pairs)
$\pm\frac{1}{2}(-7,5,-3^5,1)$	(336 such pairs)
$\pm\frac{1}{2}(5^4,-3^2,1^2)$	(420 such pairs)
$\pm\frac{1}{2}(5^3,-3^5)$	(56 such pairs)
total	3528 pairs

Example: Conway's ovoid in $O_8^+(\mathbb{Z}/15\mathbb{Z})$

The isomorphism

$$\mathbb{Z}/15\mathbb{Z} \;\cong\; \mathbb{Z}/3\mathbb{Z} \,\oplus\, \mathbb{Z}/5\mathbb{Z}$$

induces

$$O_8^+(\mathbb{Z}/15\mathbb{Z}) \;\cong\; O_8^+(\mathbb{Z}/3\mathbb{Z}) \;\times\; O_8^+(\mathbb{Z}/5\mathbb{Z})$$

Ovoids $\mathcal{O}_3$ in $O_8^+(\mathbb{Z}/3\mathbb{Z})$ and $\mathcal{O}_5$ in $O_8^+(\mathbb{Z}/5\mathbb{Z})$ give rise to an ovoid

$$\mathcal{O}_3 \times \mathcal{O}_5 \;\text{ in }\; O_8^+(\mathbb{Z}/15\mathbb{Z}).$$

But Conway's ovoid does not arise in this way! (its projections mod 3 and mod 5 do not give ovoids in $O_8^+(3)$ or $O_8^+(5)$).

Proof when m is an odd prime power $q = p^\nu$

Let $q = p^\nu$, p odd, and fix a root vector $e = \frac{1}{2}(1^8) \in E_8$.

Lemma

Let $u, v \in e + 2E_8$ of norm $2q$. Then $u \cdot v \equiv 0 \mod q$ iff $v = \pm u$.

Proof.

If $v = \pm u$ then $u \cdot v = \pm 2q \equiv 0 \mod q$. Conversely, suppose $u \cdot v \equiv 0 \mod q$. Then

$$\|u - v\|^2 = \|u\|^2 + \|v\|^2 - 2u \cdot v \equiv 0 \mod q.$$

Also $u - v \in 2E_8$ so $\|u - v\|^2 \equiv 0 \mod 8q$. But

$$\|u - v\|^2 \leqslant (\|u\| + \|v\|)^2 = (\sqrt{2q} + \sqrt{2q})^2 = 8q$$

so $\|u - v\|^2 \in \{0, 8q\}$. If $\|u - v\| = 0$ then $v = u$. Otherwise $v \in \langle u \rangle$ by Cauchy-Schwartz and $v = -u$. □

Proof when m is an odd prime power $q = p^\nu$

$$\mathcal{S}_q = \{v \in e + 2E_8 \;:\; v \text{ primitive of norm } 2q\}$$

gives a set of singular points $\mathcal{O}$ in $O_8^+(\mathbb{Z}/q\mathbb{Z})$. By the Lemma, no two points of $\mathcal{O}$ are perpendicular. It remains to be shown that $|\mathcal{O}| = (p^3+1)\left(\frac{q}{p}\right)^3 = q^3 + \left(\frac{q}{p}\right)^3$.

Proof when m is an odd prime power $q = p^\nu$

E_8 has

$$240\sigma_3(q) = 240(p^{3\nu} + p^{3(\nu-1)} + p^{3(\nu-2)} + \cdots + p^3 + 1)$$

vectors of norm $2q$, partitioned into 120 cosets mod $2E_8$. The number of pairs $\{\pm v\}$ of norm $2q$ in $e + 2E_8$ is

$$\sigma_3(p^\nu) = p^{3\nu} + p^{3(\nu-1)} + p^{3(\nu-2)} + \cdots + p^3 + 1.$$

How many of these are imprimitive? They have the form pv where $v \in e + 2E_8$ has norm $2\frac{q}{p^2} = 2p^{\nu-2}$; there are

$$\sigma_3(p^{\nu-2}) = p^{3(\nu-2)} + p^{3(\nu-3)} + \cdots + p^3 + 1$$

such pairs $\{\pm v\}$. Thus E_8 has

$$\sigma_3(p^\nu) - \sigma_3(p^{\nu-2}) = p^{3\nu} + p^{3(\nu-1)} = q^3 + \left(\frac{q}{p}\right)^3$$

antipodal pairs $\{\pm v\}$ of *primitive* vectors of norm $2q$ as required.

Conway's ovoids generalized yet again

In the previous construction, $e + 2E_8$ can be replaced by appropriate cosets of rE_8.

$r = 2$, p odd prime: *binary* ovoids in $O_8^+(\mathbb{F}_p)$ (Conway, 1988)
$r = 3$, $p \neq 3$ prime: *ternary* ovoids in $O_8^+(\mathbb{F}_p)$ (Conway, 1988)
general primes $r \neq p$: *r-ary* ovoids in $O_8^+(\mathbb{F}_p)$ (M., 1993)

In these constructions, we don't really need r and p to be prime! We only require $\gcd(r, p) = 1$.

Galois rings

Consider a prime power q and $\nu \geq 1$. The *Galois ring* $R = GR(q^\nu)$ of order q^ν has a unique maximal ideal $M \subset R$ and residue field $R/M \cong GF(p^\nu) = \mathbb{F}_{p^\nu}$.

An *ovoid* in $O_8^+(R)$ consists of

$$(p^{3\nu}+1)|M|^3 = (p^{3\nu}+1)\left(\tfrac{q}{p}\right)^{3\nu} = q^{3\nu} + \left(\tfrac{q}{p}\right)^{3\nu}$$

mutually non-perpendicular singular points.

Examples?