# Counting Ovoids in the Triality Quadric

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

RMAC Seminar 12 April 2013

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

**Example ($p = 5$, $|\mathcal{S}| = 5^2 + 1 = 26$)**

$\mathcal{S}$ contains 6 vectors of shape $(5, 1, 1, 1, 1, 1)$;
20 vectors of shape $(-3, -3, -3, 1, 1, 1)$.

**Example ($p = 13$, $|\mathcal{S}| = 13^2 + 1 = 170$)**

$\mathcal{S}$ contains 20 vectors of shape $(5, 5, 5, 1, 1, 1)$;
30 vectors of shape $(-7, -5, 1, 1, 1, 1)$;
60 vectors of shape $(5, 5, -3, -3, -3, 1)$;
60 vectors of shape $(-7, -3, -3, -3, 1, 1)$.

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

**Example** ($p = 5$, $|\mathcal{S}| = 5^2 + 1 = 26$)

$\mathcal{S}$ contains 6 vectors of shape $(5, 1, 1, 1, 1, 1)$;
20 vectors of shape $(-3, -3, -3, 1, 1, 1)$.

**Example** ($p = 13$, $|\mathcal{S}| = 13^2 + 1 = 170$)

$\mathcal{S}$ contains 20 vectors of shape $(5, 5, 5, 1, 1, 1)$;
30 vectors of shape $(-7, -5, 1, 1, 1, 1)$;
60 vectors of shape $(5, 5, -3, -3, -3, 1)$;
60 vectors of shape $(-7, -3, -3, -3, 1, 1)$.

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

**Example ($p = 5$, $|\mathcal{S}| = 5^2 + 1 = 26$)**

$\mathcal{S}$ contains 6 vectors of shape $(5, 1, 1, 1, 1, 1)$;
20 vectors of shape $(-3, -3, -3, 1, 1, 1)$.

**Example ($p = 13$, $|\mathcal{S}| = 13^2 + 1 = 170$)**

$\mathcal{S}$ contains 20 vectors of shape $(5, 5, 5, 1, 1, 1)$;
30 vectors of shape $(-7, -5, 1, 1, 1, 1)$;
60 vectors of shape $(5, 5, -3, -3, -3, 1)$;
60 vectors of shape $(-7, -3, -3, -3, 1, 1)$.

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

**Example ($p = 5$, $|\mathcal{S}| = 5^2 + 1 = 26$)**

$\mathcal{S}$ contains 6 vectors of shape $(5, 1, 1, 1, 1, 1)$;
20 vectors of shape $(-3, -3, -3, 1, 1, 1)$.

**Example ($p = 13$, $|\mathcal{S}| = 13^2 + 1 = 170$)**

$\mathcal{S}$ contains 20 vectors of shape $(5, 5, 5, 1, 1, 1)$;
30 vectors of shape $(-7, -5, 1, 1, 1, 1)$;
60 vectors of shape $(5, 5, -3, -3, -3, 1)$;
60 vectors of shape $(-7, -3, -3, -3, 1, 1)$.

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

Let $V = \mathbb{F}_p^6$ and consider the quadratic form $Q : V \to \mathbb{F}_p$ defined by $Q(v) = \sum_i v_i^2$. A point $\langle v \rangle$ (i.e. one-dimensional subspace) is *singular* if $Q(v) = 0$. The *quadric* associated to $Q$ is the set of singular points. This is the *Klein quadric* over $\mathbb{F}_p$.

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $\mathbb{Z}^6 \to \mathbb{F}_p^6$ denoted by

$$x \mapsto \overline{x} = (\overline{x}_1, \ldots, \overline{x}_6).$$

The points $\langle \overline{v} \rangle$ for $v \in \mathcal{S}$ as above, gives an *ovoid* $\mathcal{O}$ in the Klein quadric: $p^2 + 1$ points of the quadric forming a coclique in the collinearity graph of the quadric.

# Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $\mathcal{S}$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \bmod 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|\mathcal{S}| = p^2 + 1$; and for all $x \neq y$ in $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

Let $V = \mathbb{F}_p^6$ and consider the quadratic form $Q : V \to \mathbb{F}_p$ defined by $Q(v) = \sum_i v_i^2$. A point $\langle v \rangle$ (i.e. one-dimensional subspace) is *singular* if $Q(v) = 0$. The *quadric* associated to $Q$ is the set of singular points. This is the *Klein quadric* over $\mathbb{F}_p$.

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $\mathbb{Z}^6 \to \mathbb{F}_p^6$ denoted by

$$x \mapsto \overline{x} = (\overline{x}_1, \ldots, \overline{x}_6).$$

The points $\langle \overline{v} \rangle$ for $v \in \mathcal{S}$ as above, gives an *ovoid* $\mathcal{O}$ in the Klein quadric: $p^2 + 1$ points of the quadric forming a coclique in the collinearity graph of the quadric.

# The $O_8^+(p)$ quadric (triality quadric)

Let $V$ be an 8-dimensional vector space over $\mathbb{F}_p$, with hyperbolic quadratic form $Q : V \to \mathbb{F}_p$. (For $p$ odd, we may take $Q(v) = \sum_i v_i^2$.) The nondegenerate bilinear form associated to $Q$ is

$$v \cdot w = Q(v + w) - Q(v) - Q(w).$$

A point $\langle v \rangle$ (i.e. one-dimensional subspace) is *singular* if $Q(v) = 0$. The *quadric* associated to $Q$ is the set of singular points. This is the *triality quadric* over $\mathbb{F}_p$. Two points $\langle v \rangle, \langle w \rangle$ of the quadric lie on a line of the quadric iff $v \cdot w = 0$.

An *ovoid* is a set of $p^3 + 1$ points in the quadric forming a coclique in the collinearity graph of the quadric. These exist for all $p$ (Conway et al. (1988)).

# The $O_8^+(p)$ quadric (triality quadric)

Let $V$ be an 8-dimensional vector space over $\mathbb{F}_p$, with hyperbolic quadratic form $Q : V \to \mathbb{F}_p$. (For $p$ odd, we may take $Q(v) = \sum_i v_i^2$.) The nondegenerate bilinear form associated to $Q$ is

$$v \cdot w = Q(v+w) - Q(v) - Q(w).$$

A point $\langle v \rangle$ (i.e. one-dimensional subspace) is *singular* if $Q(v) = 0$. The *quadric* associated to $Q$ is the set of singular points. This is the *triality quadric* over $\mathbb{F}_p$. Two points $\langle v \rangle, \langle w \rangle$ of the quadric lie on a line of the quadric iff $v \cdot w = 0$.

An *ovoid* is a set of $p^3 + 1$ points in the quadric forming a coclique in the collinearity graph of the quadric. These exist for all $p$ (Conway et al. (1988)).

# The $O_8^+(p)$ quadric (triality quadric)

Let $V$ be an 8-dimensional vector space over $\mathbb{F}_p$, with hyperbolic quadratic form $Q : V \to \mathbb{F}_p$. (For $p$ odd, we may take $Q(v) = \sum_i v_i^2$.) The nondegenerate bilinear form associated to $Q$ is

$$v \cdot w = Q(v + w) - Q(v) - Q(w).$$

A point $\langle v \rangle$ (i.e. one-dimensional subspace) is *singular* if $Q(v) = 0$. The *quadric* associated to $Q$ is the set of singular points. This is the *triality quadric* over $\mathbb{F}_p$. Two points $\langle v \rangle, \langle w \rangle$ of the quadric lie on a line of the quadric iff $v \cdot w = 0$.

An *ovoid* is a set of $p^3 + 1$ points in the quadric forming a coclique in the collinearity graph of the quadric. These exist for all $p$ (Conway et al. (1988)).

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

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

$E$ has 240 *root vectors* (vectors $x \in E$ with minimum $\|x\|^2 = 2$):
112 vectors of shape $(\pm1, \pm1, 0, 0, 0, 0, 0, 0)$;
128 vectors of shape $\frac{1}{2}(\pm1, \pm1, \ldots, \pm1)$ (an even number of '$-$' signs).

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $E \to V = E/pE$ denoted by $\bar{\ }$. Since $\frac{1}{2}\|x\|^2 \in \mathbb{Z}$ for all $x \in E$, we have a quadratic form

$$Q : V \to \mathbb{F}_p, \quad Q(\overline{x}) = \overline{\tfrac{1}{2}\|x\|^2}.$$

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

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

$E$ has 240 *root vectors* (vectors $x \in E$ with minimum $\|x\|^2 = 2$):

- 112 vectors of shape $(\pm1, \pm1, 0, 0, 0, 0, 0, 0)$;
- 128 vectors of shape $\frac{1}{2}\big(\pm1, \pm1, \ldots, \pm1\big)$ (an even number of '$-$' signs).

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $E \to V = E/pE$ denoted by $\overline{\phantom{x}}$. Since $\frac{1}{2}\|x\|^2 \in \mathbb{Z}$ for all $x \in E$, we have a quadratic form

$$Q : V \to \mathbb{F}_p, \quad Q(\overline{x}) = \overline{\tfrac{1}{2}\|x\|^2}.$$

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

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

$E$ has 240 *root vectors* (vectors $x \in E$ with minimum $\|x\|^2 = 2$):

112 vectors of shape $(\pm1, \pm1, 0, 0, 0, 0, 0, 0)$;

128 vectors of shape $\frac{1}{2}\left(\pm1, \pm1, \ldots, \pm1\right)$ (an even number of '$-$' signs).

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $E \to V = E/pE$ denoted by $\overline{\phantom{x}}$. Since $\frac{1}{2}\|x\|^2 \in \mathbb{Z}$ for all $x \in E$, we have a quadratic form

$$Q : V \to \mathbb{F}_p, \qquad Q(\overline{x}) = \overline{\tfrac{1}{2}\|x\|^2}\,.$$

# Conway's binary ovoids

Let $p$ be an odd prime. Fix a root, say

$$e = \tfrac{1}{2}(1,1,1,1,1,1,1,1) \in E\,.$$

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}e + 2E \subset E$ such that $\frac{1}{2}\|x\|^2 = p$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$.

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{2,p,e} = \left\{ \langle \overline{x} \rangle \;:\; \pm x \in \mathcal{S} \right\},$$

an ovoid in $E/pE \simeq O_8^+(p)$ (the *binary ovoid*).

# Conway's binary ovoids

Let $p$ be an odd prime. Fix a root, say

$$e = \tfrac{1}{2}\big(1,1,1,1,1,1,1,1\big) \in E\,.$$

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}e + 2E \subset E$ such that $\frac{1}{2}\|x\|^2 = p$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$.

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{2,p,e} = \big\{\langle \overline{x}\rangle \,:\, \pm x \in \mathcal{S}\big\},$$

an ovoid in $E/pE \simeq O_8^+(p)$ (the *binary ovoid*).

# Conway's binary ovoids

Let $p$ be an odd prime. Fix a root, say

$$e = \tfrac{1}{2}\big(1,1,1,1,1,1,1,1\big) \in E\,.$$

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}e + 2E \subset E$ such that $\frac{1}{2}\|x\|^2 = p$. Then $|\mathcal{S}| = 2(p^3{+}1)$ and $\mathcal{S}$ consists of $p^3 + 1$ pairs $\pm x$.

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{2,p,e} = \big\{\langle\overline{x}\rangle \,:\, \pm x \in \mathcal{S}\big\},$$

an ovoid in $E/pE \simeq O_8^+(p)$ (the *binary ovoid*).

# Conway's binary ovoids

Let $p$ be an odd prime. Fix a root, say

$$e = \tfrac{1}{2}(1,1,1,1,1,1,1,1) \in E\,.$$

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}e + 2E \subset E$ such that $\frac{1}{2}\|x\|^2 = p$. Then $|\mathcal{S}| = 2(p^3{+}1)$ and $\mathcal{S}$ consists of $p^3{+}1$ pairs $\pm x$.

**Example ($p = 3$, $|\mathcal{O}| = 3^3 + 1 = 28$)**

$\mathcal{S}$ contains 28 vector pairs of shape $\pm\frac{1}{2}(-3,-3,1,1,1,1,1,1)$.

**Example ($p = 5$, $|\mathcal{O}| = 5^3 + 1 = 126$)**

$\mathcal{S}$ contains 70 vector pairs of shape $\pm\frac{1}{2}(-3,-3,-3,-3,1,1,1,1)$;
56 vector pairs of shape $\pm\frac{1}{2}(5,-3,1,1,1,1,1,1)$.

# Conway's binary ovoids

Let $p$ be an odd prime. Fix a root, say

$$e = \tfrac{1}{2}(1,1,1,1,1,1,1,1) \in E\,.$$

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}e + 2E \subset E$ such that $\frac{1}{2}\|x\|^2 = p$. Then $|\mathcal{S}| = 2(p^3{+}1)$ and $\mathcal{S}$ consists of $p^3{+}1$ pairs $\pm x$.

**Example ($p = 3$, $|\mathcal{O}| = 3^3 + 1 = 28$)**

$\mathcal{S}$ contains 28 vector pairs of shape $\pm\frac{1}{2}(-3,-3,1,1,1,1,1,1)$.

**Example ($p = 5$, $|\mathcal{O}| = 5^3 + 1 = 126$)**

$\mathcal{S}$ contains 70 vector pairs of shape $\pm\frac{1}{2}(-3,-3,-3,-3,1,1,1,1)$;
56 vector pairs of shape $\pm\frac{1}{2}(5,-3,1,1,1,1,1,1)$.

Let $r \neq p$ be odd primes. Fix $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}u + rE \subset E$ such that $\frac{1}{2}\|x\|^2 = k(r-k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$. (Some degenerate cases occur for $r > p$.)

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{r,p,u} = \left\{\langle \overline{x} \rangle \,:\, \pm x \in \mathcal{S}\right\},$$

an ovoid in $E/pE \simeq O_8^+(p)$.

Ovoids isomorphic to $\mathcal{O}_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the *$r$-ary ovoids of type $E_8$* in $O_8^+(p)$.

Let $r \neq p$ be odd primes. Fix $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}u + rE \subset E$ such that $\frac{1}{2}\|x\|^2 = k(r-k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$. (Some degenerate cases occur for $r > p$.)

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{r,p,u} = \left\{ \langle \overline{x} \rangle \ : \ \pm x \in \mathcal{S} \right\},$$

an ovoid in $E/pE \simeq O_8^+(p)$.

Ovoids isomorphic to $\mathcal{O}_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the *$r$-ary ovoids of type $E_8$* in $O_8^+(p)$.

# The $r$-ary ovoids in $O_8^+(p)$

Let $r \neq p$ be odd primes. Fix $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}u + rE \subset E$ such that $\frac{1}{2}\|x\|^2 = k(r-k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$. (Some degenerate cases occur for $r > p$.)

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{r,p,u} = \left\{\langle \overline{x} \rangle \,:\, \pm x \in \mathcal{S}\right\},$$

an ovoid in $E/pE \simeq O_8^+(p)$.

Ovoids isomorphic to $\mathcal{O}_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the *$r$-ary ovoids of type $E_8$* in $O_8^+(p)$.

# The $r$-ary ovoids in $O_8^+(p)$

Let $r \neq p$ be odd primes. Fix $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Let $\mathcal{S}$ be the set of vectors $x \in \mathbb{Z}u + rE \subset E$ such that $\frac{1}{2}\|x\|^2 = k(r-k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of $p^3+1$ pairs $\pm x$. (Some degenerate cases occur for $r > p$.)

Reducing these vectors mod $pE$ gives

$$\mathcal{O} = \mathcal{O}_{r,p,u} = \left\{\langle\overline{x}\rangle \;:\; \pm x \in \mathcal{S}\right\},$$

an ovoid in $E/pE \simeq O_8^+(p)$.

Ovoids isomorphic to $\mathcal{O}_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the *$r$-ary ovoids of type $E_8$* in $O_8^+(p)$.

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^i$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^i$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^i$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^j$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^j$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $\mathcal{O}_{r,p,u}$ but only finitely many ovoids in $O_8^+(p)$. How many? How do we know when we have found them all?
2. Let $w(p)$ be the number of isomorphism classes of ovoids of type $E_8$ in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geqslant 1$.)
3. $r, p$ don't really have to be primes. Does anything comparable work in $O_8^+(q)$?
4. Ovoids in $O_8^+(q)$ which lie in an $O_7(q)$ hyperplane, are known only for $q = 3^i$. Why? Is the ovoid in $O_7(3)$ the unique $E_8$-type ovoid in $O_7(p)$?
5. Most $E_8$-type ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$, but no rigid ovoids in $O_8^+(q)$ have been found.
6. What is really going on in the construction of $E_8$-type ovoids?

# Conjectured number of $E_8$-type ovoids

Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_w$ be representatives for the isomorphism types of $E_8$-type ovoids in $O_8^+(p)$, under $G = PGO_8^+(p)$. The number of ovoids isomorphic to $\mathcal{O}_i$ is $[G : G_{\mathcal{O}_i}]$; note that

$$|G| = |PGO_8^+(p)| = \frac{2}{d}p^{12}(p^6-1)(p^4-1)^2(p^2-1)$$

where $d = \gcd(p-1, 2)$.

The subgroup $W(E_8)/\{\pm I\} \cong PGO_8^+(2) \leqslant G$ has order

$$|PGO_8^+(2)| = 348{,}364{,}800.$$

# Conjectured number of $E_8$-type ovoids

Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_w$ be representatives for the isomorphism types of $E_8$-type ovoids in $O_8^+(p)$, under $G = PGO_8^+(p)$. The number of ovoids isomorphic to $\mathcal{O}_i$ is $[G : G_{\mathcal{O}_i}]$; note that

$$|G| = |PGO_8^+(p)| = \frac{2}{d} p^{12}(p^6 - 1)(p^4 - 1)^2(p^2 - 1)$$

where $d = \gcd(p-1, 2)$.

The subgroup $W(E_8)/\{\pm I\} \cong PGO_8^+(2) \leqslant G$ has order

$$|PGO_8^+(2)| = 348{,}364{,}800.$$

# Conjectured number of $E_8$-type ovoids

## Conjectured Mass Formula

For $p \geqslant 5$,

$$\sum_{i=1}^{w(p)} [G : G_{\mathcal{O}_i}] = \frac{|G|(p^4+239)}{4|PGO_8^+(2)|};$$

i.e.

$$\frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_1}|} + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_w}|} = \frac{p^4+239}{4}.$$

The stabilizers $G_{\mathcal{O}_i}$ are not necessarily subgroups of $PGO_8^+(2)$. I am not claiming that the terms in this sum are always integers (but in every known case they are).

The cases $p = 2, 3$ are genuine exceptions. (When $p = 3$ the $E_8$-type ovoids lie in hyperplanes.)

# Conjectured number of $E_8$-type ovoids

## Conjectured Mass Formula

For $p \geqslant 5$,

$$\sum_{i=1}^{w(p)} [G : G_{\mathcal{O}_i}] = \frac{|G|(p^4+239)}{4|PGO_8^+(2)|};$$

i.e.

$$\frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_1}|} + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_w}|} = \frac{p^4+239}{4}.$$

The stabilizers $G_{\mathcal{O}_i}$ are not necessarily subgroups of $PGO_8^+(2)$. I am not claiming that the terms in this sum are always integers (but in every known case they are).

The cases $p = 2, 3$ are genuine exceptions. (When $p = 3$ the $E_8$-type ovoids lie in hyperplanes.)

# Conjectured number of $E_8$-type ovoids

## Conjectured Mass Formula

For $p \geqslant 5$,

$$\sum_{i=1}^{w(p)} [G : G_{\mathcal{O}_i}] = \frac{|G|(p^4 + 239)}{4|PGO_8^+(2)|};$$

i.e.

$$\frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_1}|} + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{\mathcal{O}_w}|} = \frac{p^4 + 239}{4}.$$

The stabilizers $G_{\mathcal{O}_i}$ are not necessarily subgroups of $PGO_8^+(2)$. I am not claiming that the terms in this sum are always integers (but in every known case they are).

The cases $p = 2, 3$ are genuine exceptions. (When $p = 3$ the $E_8$-type ovoids lie in hyperplanes.)

# The abundance of ovoids

**Corollary**

*Let $n(p)$ be the number of isomorphism types of ovoids in $O_8^+(p)$. If the Mass Formula holds, then for some absolute constant $C > 0$, $n(p) \geqslant Cp^4 \to \infty$ as $p \to \infty$.*

Currently it is known that $n(p) \geqslant 1$ (Conway et al., 1988).

# Verifying the Mass Formula for small $p$

| $p$ | $w(p)$ | Mass Formula |
|---|---|---|
| 5 | 2 | $96+120 = 216 = \frac{5^4+239}{4}$ |
| 7 | 2 | $120+540 = 660 = \frac{7^4+239}{4}$ |
| 11 | 4 | $120+120+960+2520 = 3720 = \frac{11^4+239}{4}$ |
| 13 | 4 | $120+1080+1680+4320 = 7200 = \frac{13^4+239}{4}$ |
| 17 | 7 | $120+120+540+960+3360+4320+11520 = 20940 = \frac{17^4+239}{4}$ |
| 19 | 6 | $120+120+1080+7560+8640+15120 = 32640 = \frac{19^4+239}{4}$ |
| 23 | 10 | $120+120+120+540+960+2520+3360 +7560+20160+34560 = 70020 = \frac{23^4+239}{4}$ |

Strictly speaking, these terms are *lower bounds* found by enumerating $r$-ary ovoids in $O_8^+(p)$ for small $r$ and testing for isomorphism. To compute $\mathrm{Aut}(\mathcal{O})$, use `nauty` to determine $\mathrm{Aut}(\Delta(\mathcal{O}))$ where $\Delta(\mathcal{O})$ is the associated two-graph. In general $\mathrm{Aut}(\mathcal{O}) \subseteq \mathrm{Aut}(\Delta(\mathcal{O}))$, and we check that equality holds in all cases.

# Verifying the Mass Formula for small $p$

| $p$ | $w(p)$ | Mass Formula |
|---|---|---|
| 5 | 2 | $96+120 = 216 = \frac{5^4+239}{4}$ |
| 7 | 2 | $120+540 = 660 = \frac{7^4+239}{4}$ |
| 11 | 4 | $120+120+960+2520 = 3720 = \frac{11^4+239}{4}$ |
| 13 | 4 | $120+1080+1680+4320 = 7200 = \frac{13^4+239}{4}$ |
| 17 | 7 | $120+120+540+960+3360+4320+11520 = 20940 = \frac{17^4+239}{4}$ |
| 19 | 6 | $120+120+1080+7560+8640+15120 = 32640 = \frac{19^4+239}{4}$ |
| 23 | 10 | $120+120+120+540+960+2520+3360 +7560+20160+34560 = 70020 = \frac{23^4+239}{4}$ |

Strictly speaking, these terms are *lower bounds* found by enumerating $r$-ary ovoids in $O_8^+(p)$ for small $r$ and testing for isomorphism. To compute $\mathrm{Aut}(\mathcal{O})$, use `nauty` to determine $\mathrm{Aut}(\Delta(\mathcal{O}))$ where $\Delta(\mathcal{O})$ is the associated two-graph. In general $\mathrm{Aut}(\mathcal{O}) \subseteq \mathrm{Aut}(\Delta(\mathcal{O}))$, and we check that equality holds in all cases.

# The Integral Octaves

We may regard $E$ as a nonassociative ring with identity. (There are 28800 ways to do this.) The 240 root vectors become the group $E^\times$ of units in this ring.

We call $E$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes_{\mathbb{Z}} E$.

There is an anti-automorphism $x \mapsto x^*$ satisfying

$$(x+y)^* = x^* + y^*; \qquad (xy)^* = y^* x^*; \qquad xx^* = x^* x = \tfrac{1}{2}\|x\|^2.$$

In particular, $\frac{1}{2}\|xy\|^2 = \frac{1}{2}\|x\|^2 \cdot \frac{1}{2}\|y\|^2$.

If $\frac{1}{2}\|x\|^2 = mn$ where $\gcd(m,n) = 1$, then $x = yz$ for some $y, z \in E$ with $\frac{1}{2}\|y\|^2 = m$, $\frac{1}{2}\|z\|^2 = n$. There are exactly 240 such pairs $(y, z)$.

We may regard $E$ as a nonassociative ring with identity. (There are 28800 ways to do this.) The 240 root vectors become the group $E^\times$ of units in this ring.

We call $E$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes_{\mathbb{Z}} E$.

There is an anti-automorphism $x \mapsto x^*$ satisfying

$$(x+y)^* = x^* + y^*; \qquad (xy)^* = y^* x^*; \qquad xx^* = x^* x = \tfrac{1}{2}\|x\|^2.$$

In particular, $\frac{1}{2}\|xy\|^2 = \frac{1}{2}\|x\|^2 \cdot \frac{1}{2}\|y\|^2$.

If $\frac{1}{2}\|x\|^2 = mn$ where $\gcd(m,n) = 1$, then $x = yz$ for some $y, z \in E$ with $\frac{1}{2}\|y\|^2 = m$, $\frac{1}{2}\|z\|^2 = n$. There are exactly 240 such pairs $(y, z)$.

# The Integral Octaves

We may regard $E$ as a nonassociative ring with identity. (There are 28800 ways to do this.) The 240 root vectors become the group $E^\times$ of units in this ring.

We call $E$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes_{\mathbb{Z}} E$.

There is an anti-automorphism $x \mapsto x^*$ satisfying

$$(x+y)^* = x^* + y^*; \qquad (xy)^* = y^* x^*; \qquad xx^* = x^*x = \tfrac{1}{2}\|x\|^2.$$

In particular, $\frac{1}{2}\|xy\|^2 = \frac{1}{2}\|x\|^2 \cdot \frac{1}{2}\|y\|^2$.

If $\frac{1}{2}\|x\|^2 = mn$ where $\gcd(m,n) = 1$, then $x = yz$ for some $y, z \in E$ with $\frac{1}{2}\|y\|^2 = m$, $\frac{1}{2}\|z\|^2 = n$. There are exactly 240 such pairs $(y, z)$.

# The Integral Octaves

We may regard $E$ as a nonassociative ring with identity. (There are 28800 ways to do this.) The 240 root vectors become the group $E^\times$ of units in this ring.

We call $E$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes_{\mathbb{Z}} E$.

There is an anti-automorphism $x \mapsto x^*$ satisfying

$$(x+y)^* = x^* + y^*; \qquad (xy)^* = y^* x^*; \qquad xx^* = x^* x = \tfrac{1}{2}\|x\|^2.$$

In particular, $\frac{1}{2}\|xy\|^2 = \frac{1}{2}\|x\|^2 \cdot \frac{1}{2}\|y\|^2$.

If $\frac{1}{2}\|x\|^2 = mn$ where $\gcd(m,n) = 1$, then $x = yz$ for some $y, z \in E$ with $\frac{1}{2}\|y\|^2 = m$, $\frac{1}{2}\|z\|^2 = n$. There are exactly 240 such pairs $(y, z)$.

# The Integral Octaves

We may regard $E$ as a nonassociative ring with identity. (There are 28800 ways to do this.) The 240 root vectors become the group $E^\times$ of units in this ring.

We call $E$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes_{\mathbb{Z}} E$.

There is an anti-automorphism $x \mapsto x^*$ satisfying

$$(x+y)^* = x^* + y^*; \qquad (xy)^* = y^* x^*; \qquad xx^* = x^* x = \tfrac{1}{2}\|x\|^2.$$

In particular, $\frac{1}{2}\|xy\|^2 = \frac{1}{2}\|x\|^2 \cdot \frac{1}{2}\|y\|^2$.

If $\frac{1}{2}\|x\|^2 = mn$ where $\gcd(m,n) = 1$, then $x = yz$ for some $y, z \in E$ with $\frac{1}{2}\|y\|^2 = m$, $\frac{1}{2}\|z\|^2 = n$. There are exactly 240 such pairs $(y, z)$.

# Canonical bijections between $E_8$-type ovoids in $O_8^+(p)$

Fix odd primes $r \neq p$ and $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Denote the binary ovoid

$$\mathcal{O}_{2,p,1} = \left\{\langle\overline{x}\rangle \;:\; \pm x \in \mathbb{Z} + 2E,\; \tfrac{1}{2}\|x\|^2 = p\right\}.$$

An alternative construction of the $r$-ary ovoid $\mathcal{O}_{r,p,u}$ is via the canonical bijection

$$f : \mathcal{O}_{r,p,u} \to \mathcal{O}_{2,p,1}$$

constructed as follows. Given $w \in \mathbb{Z}u + rE$ with $\frac{1}{2}\|x\|^2 = k(r-k)p$, $1 \leqslant k \leqslant \frac{r-1}{2}$, we have

$$w = xy$$

for some $x, y \in E$ such that $\frac{1}{2}\|x\|^2 = p$ and $\frac{1}{2}\|y\|^2 = k(r-k)$. If we also require $x \in \mathbb{Z} + 2E$, then this factorization is unique up to a $\pm 1$ factor and our bijection is

$$f : \langle\overline{w}\rangle \to \langle\overline{x}\rangle.$$

Fix odd primes $r \neq p$ and $u \in E$ such that $\left(\frac{-\frac{p}{2}\|u\|^2}{r}\right) = +1$.

Denote the binary ovoid

$$\mathcal{O}_{2,p,1} = \left\{\langle\overline{x}\rangle : \pm x \in \mathbb{Z} + 2E,\ \tfrac{1}{2}\|x\|^2 = p\right\}.$$

An alternative construction of the $r$-ary ovoid $\mathcal{O}_{r,p,u}$ is via the canonical bijection

$$f : \mathcal{O}_{r,p,u} \to \mathcal{O}_{2,p,1}$$

constructed as follows. Given $w \in \mathbb{Z}u + rE$ with $\frac{1}{2}\|x\|^2 = k(r-k)p$, $1 \leqslant k \leqslant \frac{r-1}{2}$, we have

$$w = xy$$

for some $x, y \in E$ such that $\frac{1}{2}\|x\|^2 = p$ and $\frac{1}{2}\|y\|^2 = k(r-k)$. If we also require $x \in \mathbb{Z} + 2E$, then this factorization is unique up to a $\pm 1$ factor and our bijection is

$$f : \langle\overline{w}\rangle \to \langle\overline{x}\rangle.$$

# Binary ovoids in an $O_7(p)$-hyperplane

When does $\mathcal{O}_{r,p,u}$ lie in an $O_7(p)$-hyperplane?

The binary ovoid $\mathcal{O} = \mathcal{O}_{2,p,e}$ lies in an $O_7(p)$-hyperplane iff $p = 3$.
But even this case is rather tricky.

# Binary ovoids in an $O_7(p)$-hyperplane

When does $\mathcal{O}_{r,p,u}$ lie in an $O_7(p)$-hyperplane?

The binary ovoid $\mathcal{O} = \mathcal{O}_{2,p,e}$ lies in an $O_7(p)$-hyperplane iff $p = 3$.
But even this case is rather tricky.

# Thank You!

# Questions?