Octonionic Ovoids

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

Third Mile High Conference on Nonassociative Mathematics
15 August 2013
Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

Consider a prime $p \equiv 1 \bmod 4$. Let $S$ 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 $|S| = p^2 + 1$; and for all $x \neq y$ in $S$, $x \cdot y \neq 0 \bmod p$.

Example ($p = 5$, $|S| = 5^2 + 1 = 26$)

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

Example ($p = 13$, $|S| = 13^2 + 1 = 170$)

$S$ 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 $(-7, -3, -3, -3, 1, 1)$.
Consider a prime $p \equiv 1 \text{ mod } 4$. Let $S$ be the set of all $x = (x_1, \ldots, x_6) \in \mathbb{Z}^6$ such that

1. $x_i \equiv 1 \text{ mod } 4$; and
2. $\sum_i x_i^2 = 6p$.

Then $|S| = p^2 + 1$; and for all $x \neq y$ in $S$, $x \cdot y \neq 0 \text{ mod } p$.

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

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

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

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

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

Then $|S| = p^2 + 1$; and for all $x \neq y$ in $S$, $x \cdot y \neq 0 \mod p$.

Example ($p = 5$, $|S| = 5^2 + 1 = 26$)

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

Example ($p = 13$, $|S| = 13^2 + 1 = 170$)

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

G. Eric Moorhouse  Octonionic Ovoids
Some ovoids in the $O_6^+(p)$ quadric (Klein quadric)

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

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

Then $|S| = p^2 + 1$; and for all $x \neq y$ in $S$, $x \cdot y \neq 0 \mod p$.

Example ($p = 5$, $|S| = 5^2 + 1 = 26$)

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

Example ($p = 13$, $|S| = 13^2 + 1 = 170$)

$S$ 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 $(-7, -3, -3, -3, 1, 1)$. 
Ovoids in $O^+_{2n}(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \rightarrow \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O^+_4(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O^+_6(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O^+_6(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse 
Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \rightarrow \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{4}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$. 
Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \to \mathbb{F}_q$.

(Projection) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{2n}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse

Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \rightarrow \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \subseteq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{4}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$.  

G. Eric Moorhouse  
Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \rightarrow \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle \subset V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{4}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse  Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \to \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{4}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse

Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \to \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{4n}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{6n}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6n}^+(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse

Octonionic Ovoids
Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \to \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \subseteq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

The $O_{2n}^+(q)$ quadric is a $(q + 1) \times (q + 1)$ grid; ovoids are transversals of the grid. Ovoids in the $O_{2n}^+(q)$ quadric exist for all $q$. The lattice construction of ovoids in $O_{6}^+(p)$ (above) can be generalized to all primes $p$. 

G. Eric Moorhouse

Octonionic Ovoids
Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \rightarrow \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle < V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $O$ of points of the quadric, meeting each generator exactly once. Equivalently, $O$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

Ovoids in $O_{2n}^+(q)$ are known for some values of $q$, including all $q = p$ prime (Conway et al., 1988). No o voids in $O_{2n}^+(q)$ are known in dimension $2n \geq 10$. 

G. Eric Moorhouse

Octonionic Ovoids
Ovoids in $O_{2n}^+(q)$ quadrics

Let $V$ be a $2n$-dimensional vector space over $\mathbb{F}_q$ with nondegenerate quadratic form $Q : V \to \mathbb{F}_q$.

(Projective) points are 1-dimensional subspaces $\langle v \rangle \subset V$; such a point is singular if $Q(v) = 0$. The associated quadric is the set of all singular points. A subspace $U \leq V$ is totally singular if it lies entirely in the quadric, i.e. each of its points is singular. A generator is a maximal totally singular subspace. All generators have dimension $n$, if $Q$ is chosen appropriately.

An ovoid is a set $\mathcal{O}$ of points of the quadric, meeting each generator exactly once. Equivalently, $\mathcal{O}$ is a set of $q^{n-1} + 1$ singular points, no two perpendicular.

Ovoids in $O_8^+(q)$ are known for some values of $q$, including all $q = p$ prime (Conway et al., 1988). No ovoids in $O_{2n}^+(q)$ are known in dimension $2n \geq 10$. 
Denote by $O$ the *ring of integral octaves*. The octonion algebra is $\mathbb{O} = \mathbb{R} \otimes \mathbb{Z} \cdot O$ and $O$ is isometric to a root lattice of type $E_8$ in $\mathbb{O}$.

The set of units $\mathbb{O}^\times$ is a Moufang loop of order 240, consisting of all elements of norm 1 in $O$.

For all $n \geq 1$, the number of elements $v \in O$ of norm $|v|^2 = n$ is

$$240\sigma_3(n) = 240 \sum_{1 \leq d | n} d^3.$$

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $O \to V := O/pO$ denoted by $\overline{-}$. Equipped with the quadratic form

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

$V$ is an orthogonal space of type $O_8^+(p)$. 

---

G. Eric Moorhouse

Octonionic Ovoids
Denote by $O$ the \textit{ring of integral octaves}. The octonion algebra is $O = \mathbb{R} \otimes \mathbb{Z} O$ and $O$ is isometric to a root lattice of type $E_8$ in $O$.

The set of units $O^\times$ is a Moufang loop of order 240, consisting of all elements of norm 1 in $O$.

For all $n \geq 1$, the number of elements $v \in O$ of norm $|v|^2 = n$ is

$$240 \sigma_3(n) = 240 \sum_{1 \leq d | n} d^3.$$

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $O \to V := O/pO$ denoted by $\bar{}$. Equipped with the quadratic form $Q : V \to \mathbb{F}_p$, $Q(\bar{x}) = |\bar{x}|^2$,

$V$ is an orthogonal space of type $O_8^+(p)$. 

G. Eric Moorhouse

Octonionic Ovoids
Denote by $O$ the *ring of integral octaves*. The octonion algebra is $O = \mathbb{R} \otimes \mathbb{Z} O$ and $O$ is isometric to a root lattice of type $E_8$ in $O$.

The set of units $O^\times$ is a Moufang loop of order 240, consisting of all elements of norm 1 in $O$.

For all $n \geq 1$, the number of elements $v \in O$ of *norm* $|v|^2 = n$ is

$$240\sigma_3(n) = 240 \sum_{1 \leq d | n} d^3.$$

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $O \to V := O/pO$ denoted by $\bar{\cdot}$. Equipped with the quadratic form

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

$V$ is an orthogonal space of type $O_8^+(p)$. 
Denote by $O$ the *ring of integral octaves*. The octonion algebra is $O = \mathbb{R} \otimes \mathbb{Z}$ and $O$ is isometric to a root lattice of type $E_8$ in $O$.

The set of units $O^\times$ is a Moufang loop of order 240, consisting of all elements of norm 1 in $O$.

For all $n \geq 1$, the number of elements $v \in O$ of *norm* $|v|^2 = n$ is

$$240\sigma_3(n) = 240 \sum_{1 \leq d | n} d^3.$$ 

Reduction mod $p$ gives maps $\mathbb{Z} \to \mathbb{F}_p$ and $O \to V := O/pO$ denoted by $\bar{\cdot}$. Equipped with the quadratic form

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

$V$ is an orthogonal space of type $O_8^+(p)$. 

G. Eric Moorhouse

Octonionic Ovoids
The ‘binary’ ovoids

**Theorem (Conway, Kleidman & Wilson, 1988)**

Let $p$ be an odd prime. Fix a unit $u \in O^\times$. Let $S$ be the set of vectors $x \in \mathbb{Z}u + 2O \subset O$ such that $|x|^2 = p$. Then $|S| = 2(p^3 + 1)$ and $S$ consists of $p^3 + 1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

$$O = O_{2,p,u} = \{ \langle x \rangle : \pm x \in S \},$$

an ovoid in $O/pO \simeq O_8^+(p)$.

The proof uses the most basic facts about the $E_8$ root lattice. Conway et al. also gave a construction of ‘ternary’ ovoids (replacing the prime 2 by 3 above).
The ‘binary’ ovoids

**Theorem (Conway, Kleidman & Wilson, 1988)**

Let $p$ be an odd prime. Fix a unit $u \in O^\times$. Let $S$ be the set of vectors $x \in \mathbb{Z}u + 2O \subset O$ such that $|x|^2 = p$. Then $|S| = 2(p^3 + 1)$ and $S$ consists of $p^3 + 1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

$$O = O_{2,p,u} = \{ \langle \bar{x} \rangle : \pm x \in S \},$$

an ovoid in $O/pO \simeq O_8^+(p)$.

The proof uses the most basic facts about the $E_8$ root lattice. Conway et al. also gave a construction of ‘ternary’ ovoids (replacing the prime 2 by 3 above).
The ‘binary’ ovoids

Theorem (Conway, Kleidman & Wilson, 1988)

Let $p$ be an odd prime. Fix a unit $u \in O^\times$. Let $S$ be the set of vectors $x \in \mathbb{Z}u + 2O \subset O$ such that $|x|^2 = p$. Then $|S| = 2(p^3 + 1)$ and $S$ consists of $p^3 + 1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

$$O = O_{2,p,u} = \{ \langle \overline{x} \rangle : \pm x \in S \},$$

an ovoid in $O/pO \simeq O_8^+(p)$.

The proof uses the most basic facts about the $E_8$ root lattice. Conway et al. also gave a construction of ‘ternary’ ovoids (replacing the prime 2 by 3 above).
Theorem (M., 1993)

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

Let $S$ be the set of vectors $x \in \mathbb{Z}u + rO \subset O$ such that $|x|^2 = k(r - k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|S| = 2(p^3 + 1)$ and $S$ consists of $p^3 + 1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

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

an ovoid in $O/pO \cong O_8^+(p)$. (Some degenerate cases occur for $r > p$.)

The proof uses facts about $E_8$ and the fact that $E_8 \oplus E_8$ has $480\sigma_7(n)$ elements of norm $n \geq 1$. (Or $O$ and theorems on factorization in $O$). Ovoids isomorphic to $O_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the $r$-ary ovoids of octonionic type in $O_8^+(p)$. 

G. Eric Moorhouse

Octonionic Ovoids
Theorem (M., 1993)

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

Let $S$ be the set of vectors $x \in \mathbb{Z}u + rO \subset O$ such that $|x|^2 = k(r - k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|S| = 2(p^3 + 1)$ and $S$ consists of $p^3 + 1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

$$O = O_{r,p,u} = \{ \langle x \rangle : \pm x \in S \},$$

an ovoid in $O/pO \cong O_8^+(p)$. (Some degenerate cases occur for $r > p$.)

The proof uses facts about $E_8$ and the fact that $E_8 \oplus E_8$ has $480\sigma_7(n)$ elements of norm $n \geq 1$. (Or $O$ and theorems on factorization in $O$). Ovoids isomorphic to $O_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the $r$-ary ovoids of octonionic type in $O_8^+(p)$. 

G. Eric Moorhouse

Octonionic Ovoids
Theorem (M., 1993)

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

Let \( S \) be the set of vectors \( x \in \mathbb{Z}u + rO \subset O \) such that

\[
|x|^2 = k(r - k)p \quad \text{for some } k \in \{1, 2, \ldots, \frac{r-1}{2}\}.
\]

Then \( |S| = 2(p^3 + 1) \) and \( S \) consists of \( p^3 + 1 \) pairs \( \pm x \). Reducing these vectors mod \( pO \) gives

\[
\mathcal{O} = \mathcal{O}_{r,p,u} = \{ \langle \bar{x} \rangle : \pm x \in S \},
\]

an ovoid in \( O/pO \cong O_8^+(p) \). (Some degenerate cases occur for \( r > p \).)

The proof uses facts about \( E_8 \) and the fact that \( E_8 \oplus E_8 \) has \( 480\sigma_7(n) \) elements of norm \( n \geq 1 \). (Or \( O \) and theorems on factorization in \( O \)). Ovoids isomorphic to \( \mathcal{O}_{r,p,u} \) (for primes \( r \neq p \), including \( r = 2 \)) are the \( r \)-ary ovoids of octonionic type in \( O_8^+(p) \).
Theorem (M., 1993)

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

Let \( S \) be the set of vectors \( x \in \mathbb{Z}u + rO \subset O \) such that \( |x|^2 = k(r - k)p \) for some \( k \in \{1, 2, \ldots, \frac{r-1}{2}\} \). Then \( |S| = 2(p^3+1) \) and \( S \) consists of \( p^3+1 \) pairs \( \pm x \). Reducing these vectors mod \( pO \) gives

\[ \mathcal{O} = \mathcal{O}_{r,p,u} = \{ \langle \bar{x} \rangle : \pm x \in S \}, \]

an ovoid in \( O/pO \cong O_8^+(p) \). (Some degenerate cases occur for \( r > p \).)

The proof uses facts about \( E_8 \) and the fact that \( E_8 \oplus E_8 \) has \( 480\sigma_7(n) \) elements of norm \( n \geq 1 \). (Or \( O \) and theorems on factorization in \( O \)). Ovoids isomorphic to \( \mathcal{O}_{r,p,u} \) (for primes \( r \neq p \), including \( r = 2 \)) are the \( r \)-ary ovoids of octonionic type in \( O_8^+(p) \).
Theorem (M., 1993)

Let $r \neq p$ be odd primes. Fix $u \in O$ such that \((-p|u|^2)_r = +1$. Let $S$ be the set of vectors $x \in \mathbb{Z}u + rO \subset O$ such that $|x|^2 = k(r - k)p$ for some $k \in \{1, 2, \ldots, \frac{r-1}{2}\}$. Then $|S| = 2(p^3+1)$ and $S$ consists of $p^3+1$ pairs $\pm x$. Reducing these vectors mod $pO$ gives

$$O = O_{r,p,u} = \{\langle x \rangle : \pm x \in S\},$$

an ovoid in $O/pO \cong O_8^+(p)$. (Some degenerate cases occur for $r > p$.)

The proof uses facts about $E_8$ and the fact that $E_8 \oplus E_8$ has $480\sigma_7(n)$ elements of norm $n \geq 1$. (Or $O$ and theorems on factorization in $O$). Ovoids isomorphic to $O_{r,p,u}$ (for primes $r \neq p$, including $r = 2$) are the $r$-ary ovoids of octonionic type in $O_8^+(p)$. 

G. Eric Moorhouse

Octonionic Ovoids
Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $O_{r,p,u}$ 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 octonionic ovoids in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geq 1$.)

3. $r, p$ don’t really have to be primes. Does anything comparable work in $O_8^+(q)$?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$; but no rigid ovoids in $O_8^+(q)$ have been found.

5. What is really going on in the construction of octonionic ovoids?
1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $O_{r,p,u}$ 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 octonionic ovoids in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geq 1$.)

3. $r, p$ don’t really have to be primes. Does anything comparable work in $O_8^+(q)$?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$; but no rigid ovoids in $O_8^+(q)$ have been found.

5. What is really going on in the construction of octonionic ovoids?
Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $O_{r,p,u}$ 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 octonionic ovoids in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geq 1$.)

3. $r, p$ don’t really have to be primes. Does anything comparable work in $O_8^+(q)$?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$; but no rigid ovoids in $O_8^+(q)$ have been found.

5. What is really going on in the construction of octonionic ovoids?
Open Questions

1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $O_{r,p,u}$ 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 octonionic ovoids in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geq 1$.)

3. $r, p$ don’t really have to be primes. Does anything comparable work in $O_8^+(q)$?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$; but no rigid ovoids in $O_8^+(q)$ have been found.

5. What is really going on in the construction of octonionic ovoids?
Open Questions

1. For each \( p \), there are infinitely many choices of \( r, u \) to choose in constructing \( O_{r,p,u} \) 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 octonionic ovoids in \( O_8^+(p) \). Does \( w(p) \to \infty \) as \( p \to \infty \)? (By Conway et al. (1988), \( w(p) \geq 1 \).)

3. \( r, p \) don’t really have to be primes. Does anything comparable work in \( O_8^+(q) \)?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in \( PGO_8^+(p) \); but no rigid ovoids in \( O_8^+(q) \) have been found.

5. What is really going on in the construction of octonionic ovoids?
1. For each $p$, there are infinitely many choices of $r, u$ to choose in constructing $O_{r,p,u}$ 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 octonionic ovoids in $O_8^+(p)$. Does $w(p) \to \infty$ as $p \to \infty$? (By Conway et al. (1988), $w(p) \geq 1$.)

3. $r, p$ don’t really have to be primes. Does anything comparable work in $O_8^+(q)$?

4. Most octonionic ovoids should be rigid, i.e. having trivial stabilizer in $PGO_8^+(p)$; but no rigid ovoids in $O_8^+(q)$ have been found.

5. What is really going on in the construction of octonionic ovoids?
Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_w$ be representatives for the isomorphism types of octonionic 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 $W(E_8)/\{\pm I\} \cong PGO_8^+(2) \leq G$ has order

$$|PGO_8^+(2)| = 348,364,800.$$
Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_w$ be representatives for the isomorphism types of octonionic 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 $W(E_8)/\{\pm I\} \cong PGO_8^+(2) \leq G$ has order

$$|PGO_8^+(2)| = 348,364,800.$$
Conjectured number of octonionic ovoids

Conjectured Mass Formula

For $p \geq 5$,

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

i.e.

$$\frac{|PGO_8^+(2)|}{|G_{O_1}|} + \frac{|PGO_8^+(2)|}{|G_{O_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{O_w}|} = \frac{p^4 + 239}{4}.$$

The stabilizers $G_{O_i}$ 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 octonionic ovoids lie in hyperplanes.)
Conjectured number of octonionic ovoids

Conjectured Mass Formula

For \( p \geq 5 \),

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

i.e.

\[
\frac{|PGO_8^+(2)|}{|G_{O_1}|} + \frac{|PGO_8^+(2)|}{|G_{O_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{O_w}|} = \frac{p^4 + 239}{4}.
\]

The stabilizers \( G_{O_i} \) 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 octonionic ovoids lie in hyperplanes.)
Conjectured number of octonionic ovoids

Conjectured Mass Formula

For $p \geq 5$,\

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

i.e.

$$\frac{|PGO_8^+(2)|}{|G_{O_1}|} + \frac{|PGO_8^+(2)|}{|G_{O_2}|} + \cdots + \frac{|PGO_8^+(2)|}{|G_{O_w}|} = \frac{p^4 + 239}{4}.$$

The stabilizers $G_{O_i}$ 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 octonionic 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 \( C > 0 \), \( n(p) \geq Cp^4 \to \infty \) as \( p \to \infty \).

Currently it is known that \( n(p) \geq 1 \) (Conway et al., 1988).
Verifying the Mass Formula for small $p$

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

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 $\text{Aut}(\mathcal{O})$, use *nauty* to determine $\text{Aut}(\Delta(\mathcal{O}))$ where $\Delta(\mathcal{O})$ is the associated two-graph. In general $\text{Aut}(\mathcal{O}) \subseteq \text{Aut}(\Delta(\mathcal{O}))$, and we check that equality holds in all cases.
Verifying the Mass Formula for small $p$

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

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 $\text{Aut}(\mathcal{O})$, use *nauty* to determine $\text{Aut}(\Delta(\mathcal{O}))$ where $\Delta(\mathcal{O})$ is the associated two-graph. In general $\text{Aut}(\mathcal{O}) \subseteq \text{Aut}(\Delta(\mathcal{O}))$, and we check that equality holds in all cases.
Canonical bijections between octonionic ovoids in $O_8^+(p)$

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

Denote the binary ovoid

$$O_{2,p,1} = \{ \langle x \rangle : \pm x \in \mathbb{Z} + 2O, \ |x|^2 = p \}.$$

An alternative construction of the $r$-ary ovoid $O_{r,p,u}$ is via the canonical bijection

$$f : O_{r,p,u} \to O_{2,p,1}$$

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

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

$$f : \langle w \rangle \mapsto \langle x \rangle.$$
Canonical bijections between octonionic ovoids in $O_8^+(p)$

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

Denote the binary ovoid

$$O_{2,p,1} = \{ \langle x \rangle : \pm x \in \mathbb{Z} + 2O, \ |x|^2 = p \}.$$ 

An alternative construction of the $r$-ary ovoid $O_{r,p,u}$ is via the canonical bijection

$$f : O_{r,p,u} \to O_{2,p,1}$$

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

$$w = xy$$

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

$$f : \langle w \rangle \mapsto \langle x \rangle.$$
Thank You!

Questions?