Ovoids in the Triality Quadric

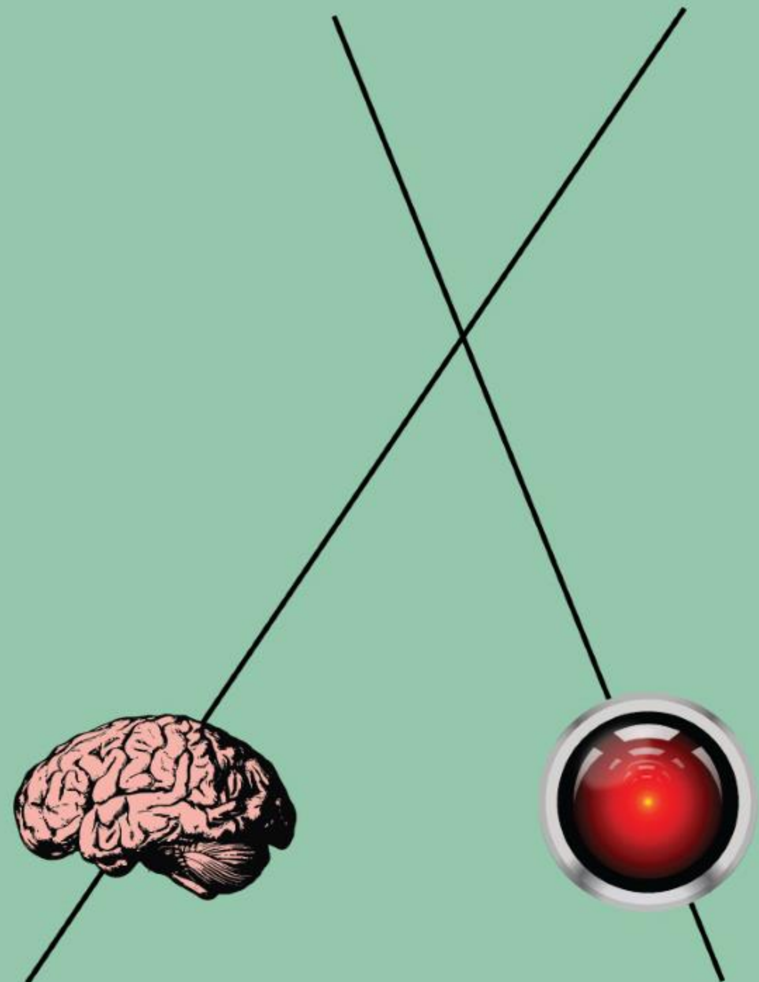
G. Eric Moorhouse

Department of Mathematics
University of Wyoming

FGEC 2019

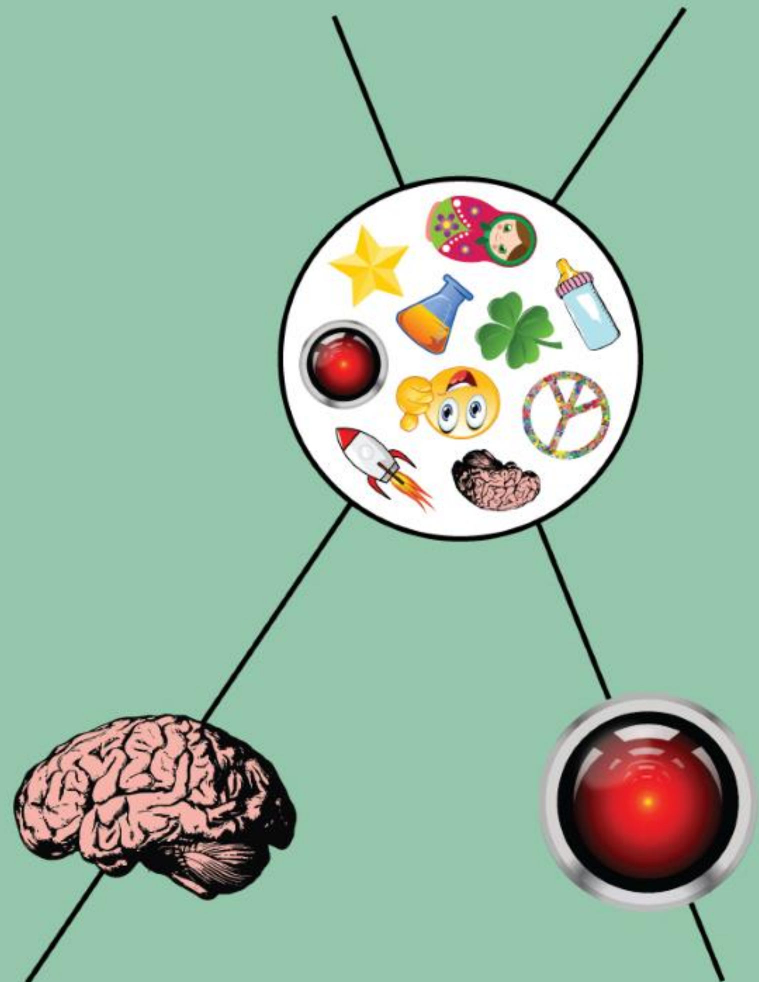
Axiom 1

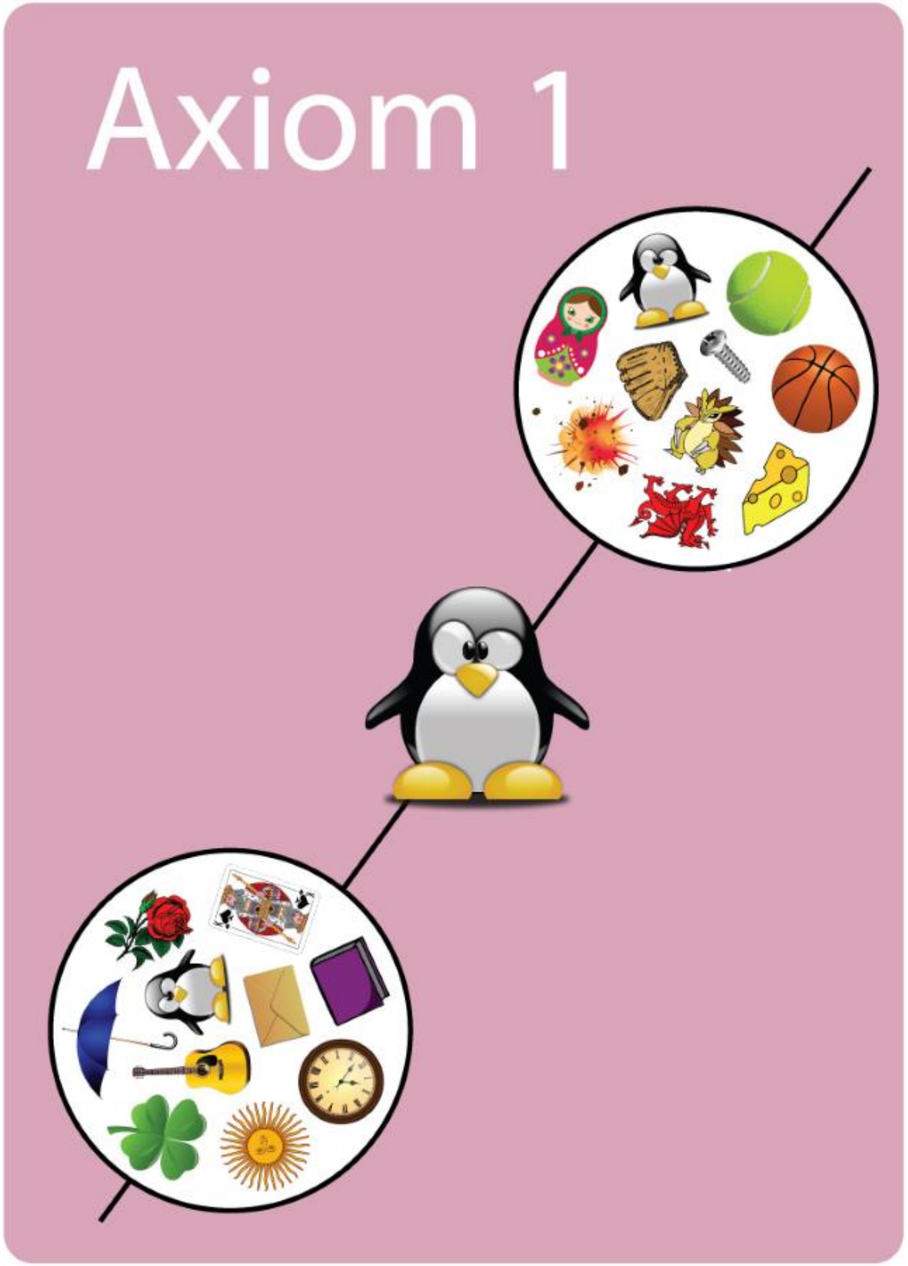
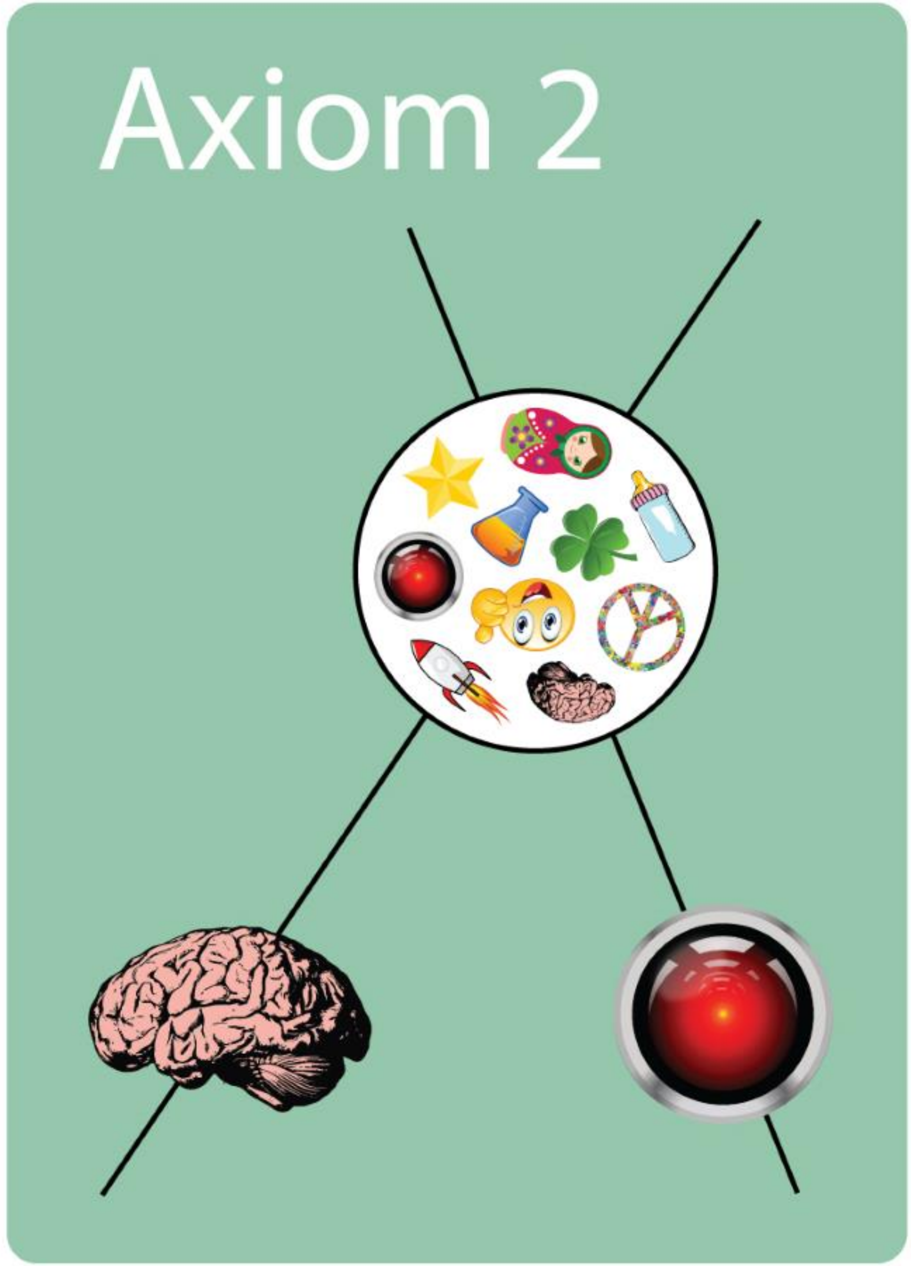
Axiom 2

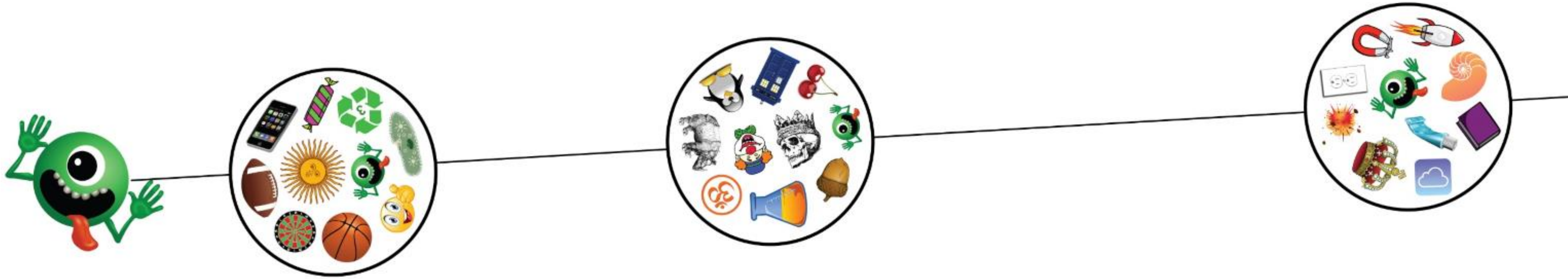


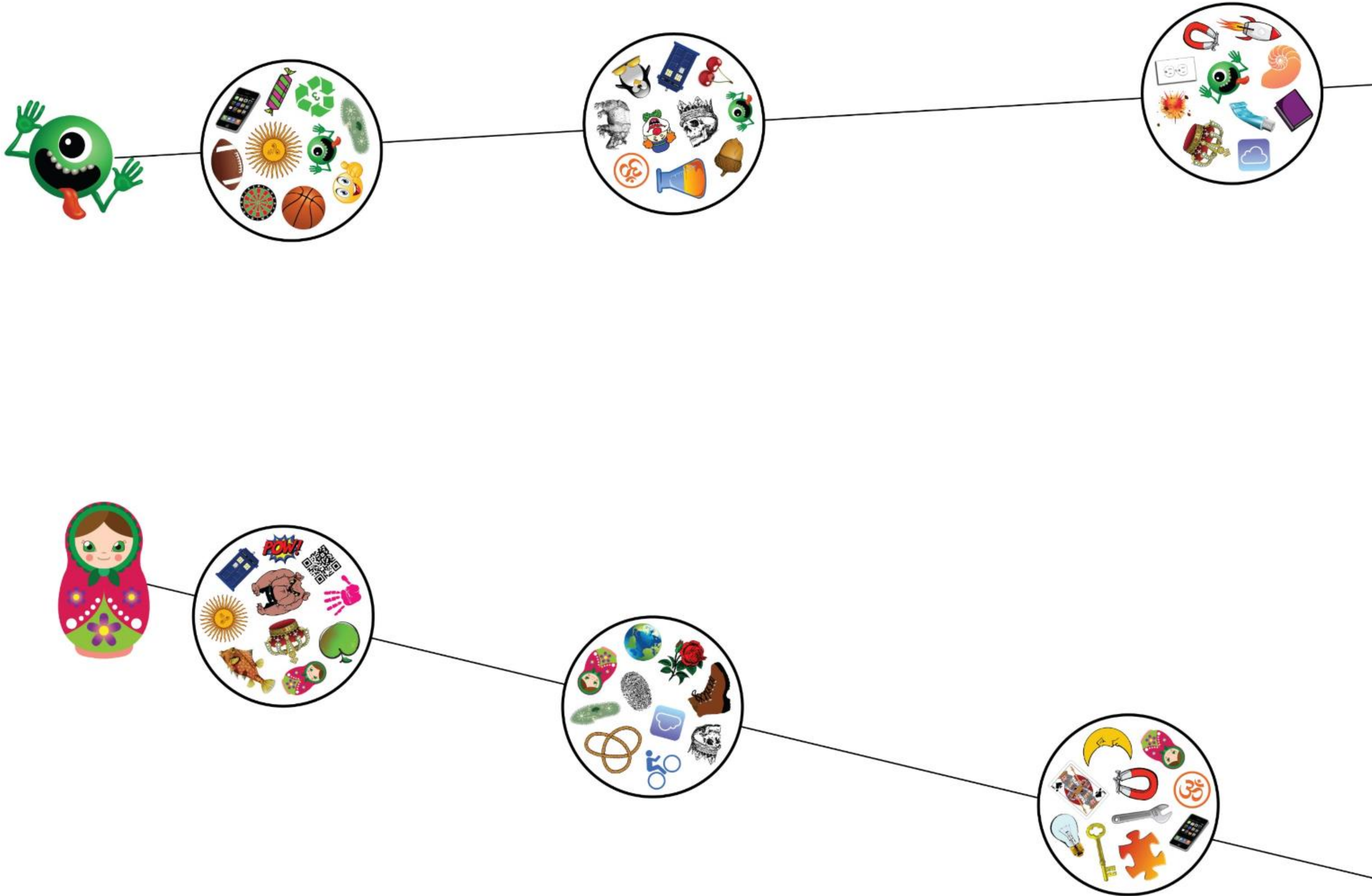
Axiom 1

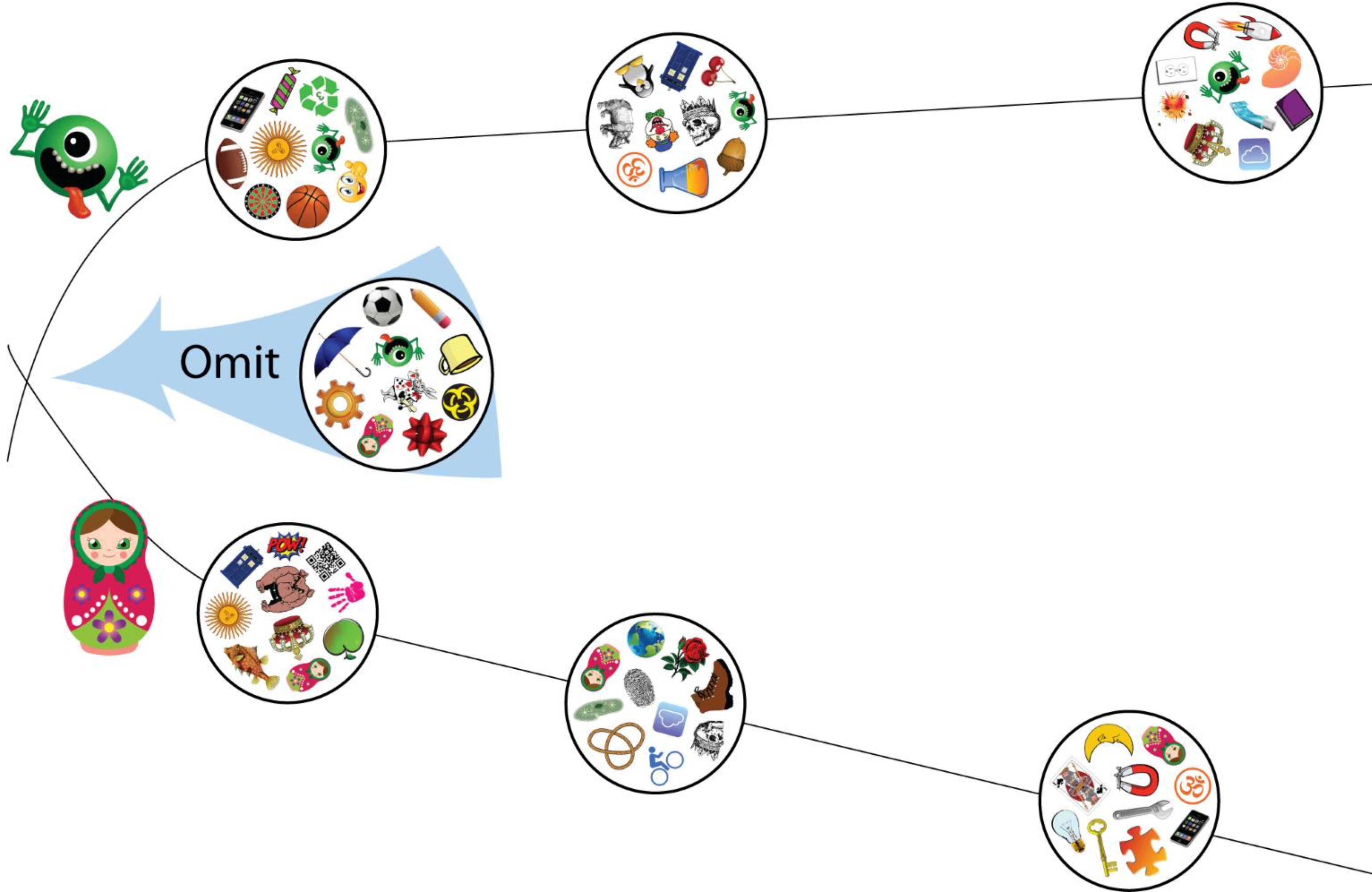
Axiom 2

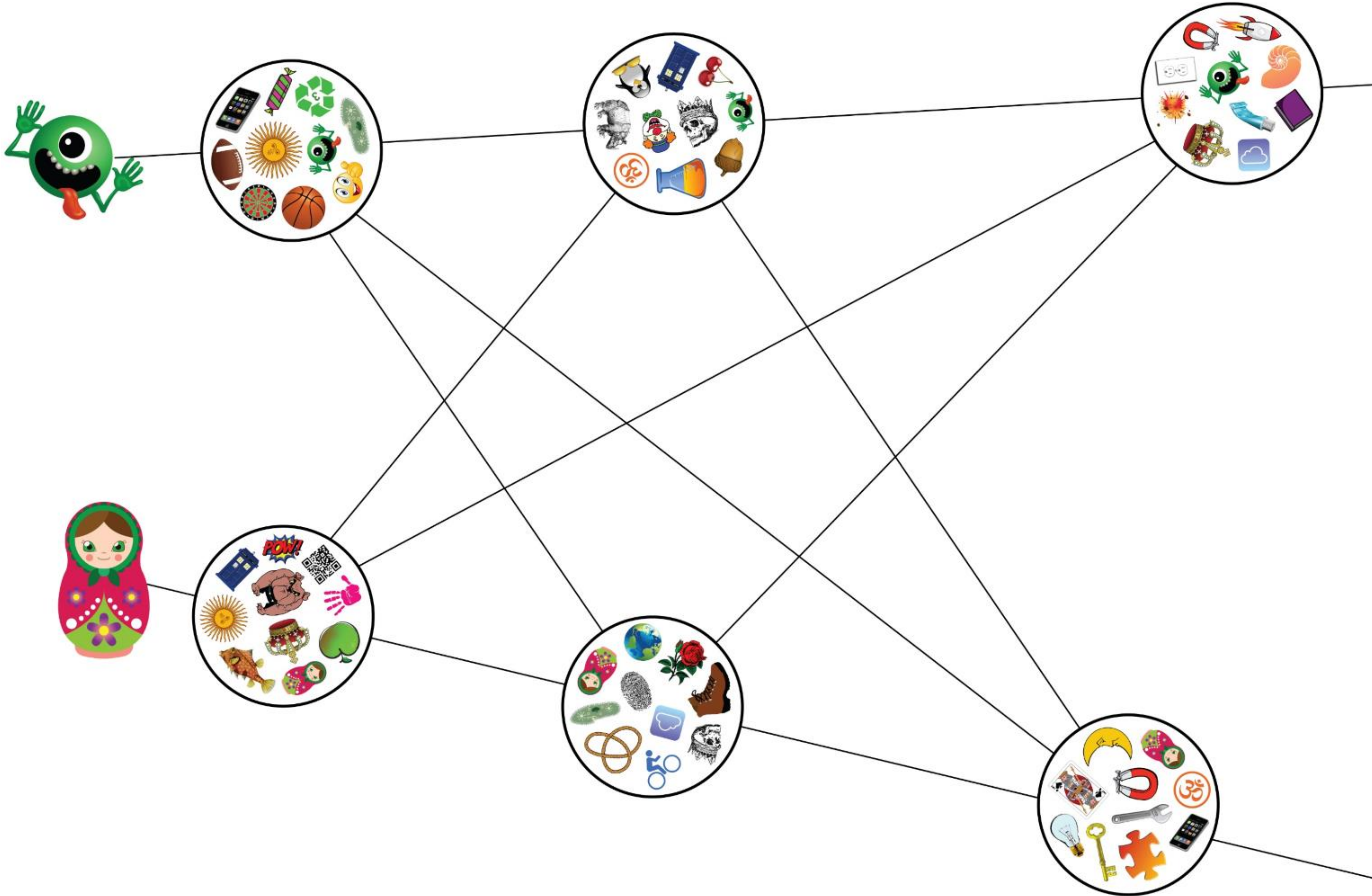



Axiom 1

Axiom 2




POW!


Omit


POW!


POW!


POW!


POW!


UNIVERSITY OF WYOMING
LEAVE NO DOUBT
icicle
goblin
slope 2
slope 1
dog
cactus
x
y

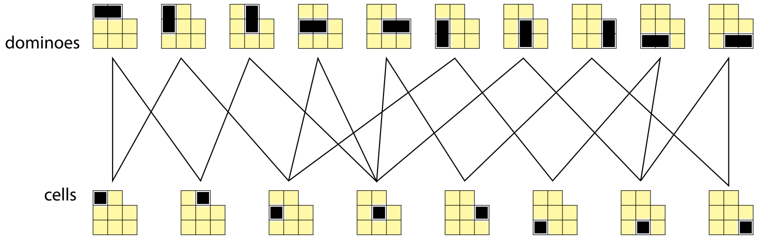
Ovoids in the Triality Quadric

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

FGEC 2019

Consider a bipartite graph representing incidences between *points* and *blocks*.

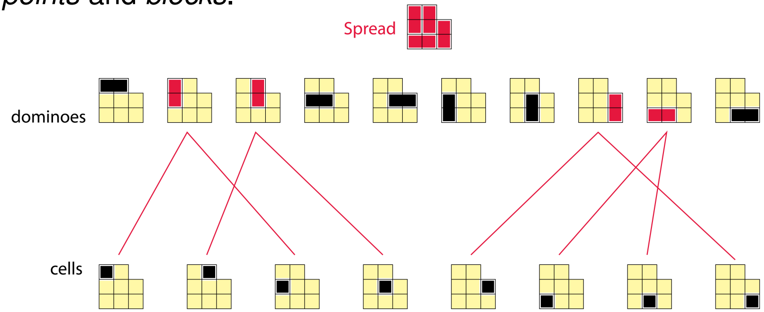


A spread is a set of blocks partitioning the points.

Dually, an ovoid is a set of points partitioning the blocks.

Ovoids and Spreads

Consider a bipartite graph representing incidences between *points* and *blocks*.

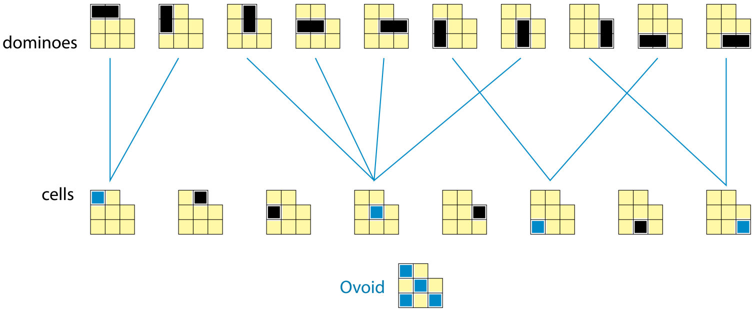


A spread is a set of blocks partitioning the points.

Dually, an ovoid is a set of points partitioning the blocks.

Ovoids and Spreads

Consider a bipartite graph representing incidences between *points* and *blocks*.

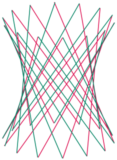


A spread is a set of blocks partitioning the points.

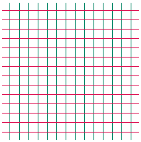
Dually, an ovoid is a set of points partitioning the blocks.

The $O_4^+(q)$ quadric (hyperbolic quadric in projective 3-space) is a $(q+1) \times (q+1)$ grid.

- q+1 lines
- q+1 lines

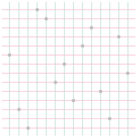


$=$



$(q+1)^2$ points;
$2(q+1)$ lines

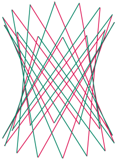
It has $(q+1)!$ ovoids (and 2 spreads). Each ovoid is a 'transversal' of the grid, having $q+1$ points.



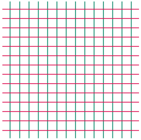
Ovoids in $O_4^+(q)$

The $O_4^+(q)$ quadric (hyperbolic quadric in projective 3-space) is a $(q+1) \times (q+1)$ grid.

- $q+1$ lines
- $q+1$ lines

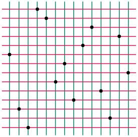


$=$



$(q+1)^2$ points;
$2(q+1)$ lines

It has $(q+1)!$ ovoids (and 2 spreads). Each ovoid is a 'transversal' of the grid, having $q+1$ points.



Ovoids in $O_6^+(q)$ (Klein Quadric)

The $O_6^+(q)$ quadric (Klein quadric) has

$(q^2+q+1)(q^2+1)$ points

$(q^2+1)(q+1)$ type I planes

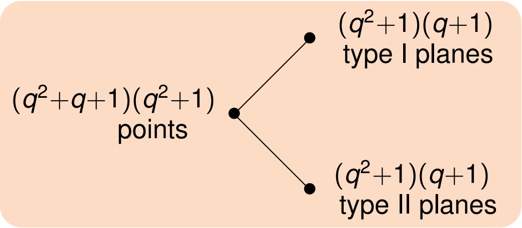
$(q^2+1)(q+1)$ type II planes

Each ovoid has size $|\mathcal{O}| = q^2+1$ (same as a set of q^2+1 points of the quadric, no two perpendicular).

Ovoids in $O_6^+(q)$ are known to exist in great abundance.

Ovoids in $O_6^+(q)$ (Klein Quadric)

The $O_6^+(q)$ quadric (Klein quadric) has



Each ovoid has size $|\mathcal{O}| = q^2 + 1$ (same as a set of $q^2 + 1$ points of the quadric, no two perpendicular).

Ovoids in $O_6^+(q)$ are known to exist in great abundance.

Ovoids in $O_6^+(q)$ (Klein Quadric)

The $O_6^+(q)$ quadric (Klein quadric) has

$(q^2{+}1)(q{+}1)$
type I planes

$(q^2{+}q{+}1)(q^2{+}1)$
points

$(q^2{+}1)(q{+}1)$
type II planes

Each ovoid has size $|\mathcal{O}| = q^2 + 1$ (same as a set of $q^2 + 1$ points of the quadric, no two perpendicular).

Ovoids in $O_6^+(q)$ are known to exist in great abundance.

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

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 Klein quadric $O_6^+(p)$

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 Klein quadric $O_6^+(p)$

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 Klein quadric $O_6^+(p)$

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 $\mathcal{S}$, $x \cdot y \not\equiv 0 \bmod p$.

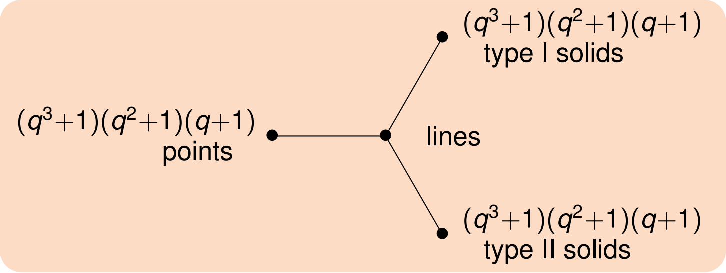
Example ($p = 5$, $|\mathcal{S}| = 5^2 + 1 = 26$)

$\mathcal{S}$ 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 $(-7, -3, -3, -3, 1, 1)$.

The $O_8^+(q)$ quadric (triality quadric) has



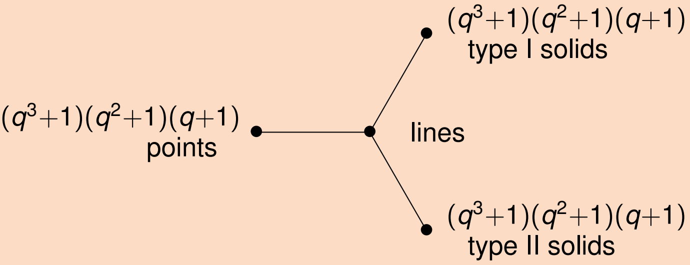
Each ovoid has size $|\mathcal{O}| = q^3 + 1$ (same as a set of $q^3 + 1$ points of the quadric, no two perpendicular).

Ovoids are equivalent to spreads (via triality).

When do they exist?

Ovoids in $O_8^+(q)$ (the Triality Quadric)

The $O_8^+(q)$ quadric (triality quadric) has



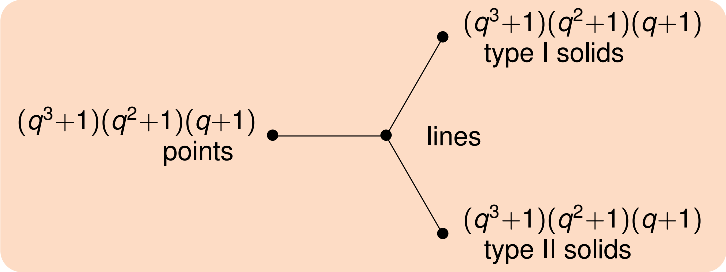
Each ovoid has size $|\mathcal{O}| = q^3 + 1$ (same as a set of $q^3 + 1$ points of the quadric, no two perpendicular).

Ovoids are equivalent to spreads (via triality).

When do they exist?

Ovoids in $O_8^+(q)$ (the Triality Quadric)

The $O_8^+(q)$ quadric (triality quadric) has



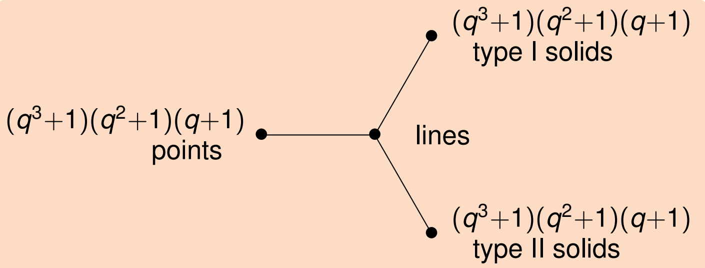
Each ovoid has size $|\mathcal{O}| = q^3 + 1$ (same as a set of $q^3 + 1$ points of the quadric, no two perpendicular).

Ovoids are equivalent to spreads (via triality).

When do they exist?

Ovoids in $O_8^+(q)$ (the Triality Quadric)

The $O_8^+(q)$ quadric (triality quadric) has



Each ovoid has size $|\mathcal{O}| = q^3 + 1$ (same as a set of $q^3 + 1$ points of the quadric, no two perpendicular).

Ovoids are equivalent to spreads (via triality).

When do they exist?

The E_8 Root Lattice

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and} \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

The E_8 Root Lattice

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

Let E be the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

This is the E_8 root lattice. It is

- a lattice (i.e. discrete additive subgroup of $\mathbb{R}^8$);
- integral ($x \cdot y \in \mathbb{Z}$ for all $x, y \in E$);
- unimodular (its density is 1, i.e. it has one point per unit volume on average);
- it has minimum distance $\sqrt{2}$ (so for any $x \neq y$ in E, $\|y - x\| \geqslant \sqrt{2}$); and
- it is unique with these properties. Any subset of $\mathbb{R}^8$ of density 1 has minimum distance at most $\sqrt{2}$; and up to isometry, E is the unique subset attaining this optimum.

The E_8 Root Lattice

E is the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

E has 240 shortest vectors ($e \in E$, $\|e\|^2 = e \cdot e = 2$) called root vectors:

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

For an odd prime p, there are $240(p^3+1)$ vectors $x \in E$ with $\|x\|^2 = 2p$.

The E_8 Root Lattice

E is the set of all vectors $\frac{1}{2}(x_1, x_2, \ldots, x_8) \in \mathbb{Q}^8$ such that

$$x_i \in \mathbb{Z}, \quad x_1 \equiv x_2 \equiv \cdots \equiv x_8 \mod 2, \quad \text{and } \sum_i x_i \equiv 0 \mod 4.$$

E has 240 shortest vectors ($e \in E$, $\|e\|^2 = e \cdot e = 2$) called root vectors:

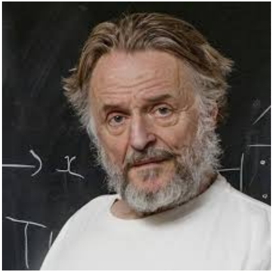
- $(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0)$ and permutations thereof (112 vectors of this shape); and
- $\frac{1}{2}(\pm 1, \pm 1, \ldots, \pm 1)$ with an even number of '$-$' signs (128 vectors of this shape).

For an odd prime p, there are $240(p^3+1)$ vectors $x \in E$ with $\|x\|^2 = 2p$.

Theorem (Conway et al., 1988)

For every prime p, there is an ovoid in the $O_8^+(p)$ triality quadric.

Take p to be an *odd* prime (the case $p = 2$ was previously solved). Fix a root vector $e \in E$. Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v \in e + 2E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. □



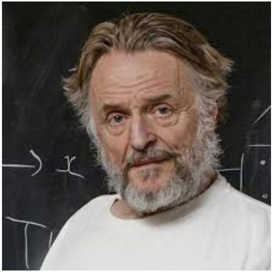
John H. Conway

Ovoids of Conway, Kleidman and Wilson (1988)

Theorem (Conway et al., 1988)

For every prime p, there is an ovoid in the $O_8^+(p)$ triality quadric.

Take p to be an *odd* prime (the case $p = 2$ was previously solved). Fix a root vector $e \in E$. Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v \in e + 2E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. □



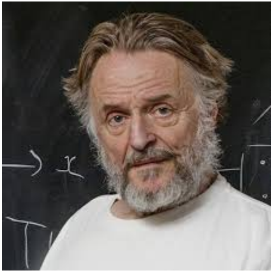
John H. Conway

Ovoids of Conway, Kleidman and Wilson (1988)

Theorem (Conway et al., 1988)

For every prime p, there is an ovoid in the $O_8^+(p)$ triality quadric.

Take p to be an *odd* prime (the case $p = 2$ was previously solved). Fix a root vector $e \in E$. Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v \in e + 2E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. $\square$



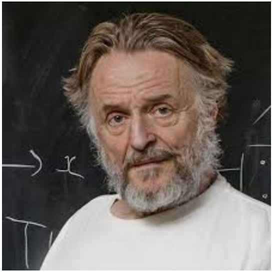
John H. Conway

Ovoids of Conway, Kleidman and Wilson (1988)

Theorem (Conway et al., 1988)

For every prime p, there is an ovoid in the $O_8^+(p)$ triality quadric.

Take p to be an *odd* prime (the case $p = 2$ was previously solved). Fix a root vector $e \in E$. Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v \in e + 2E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. □

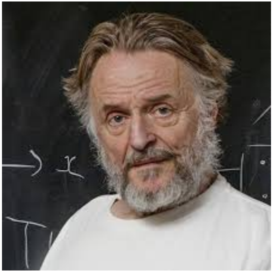


John H. Conway

Theorem (Conway et al., 1988)

For every prime p, there is an ovoid in the $O_8^+(p)$ triality quadric.

Take p to be an *odd* prime (the case $p = 2$ was previously solved). Fix a root vector $e \in E$. Let $\mathcal{S}$ be the set of all $v \in E$ such that $\|v\|^2 = 2p$ and $v \in e + 2E$. We easily conclude that $|\mathcal{S}| = 2(p^3+1)$ and $\mathcal{S}$ consists of p^3+1 pairs $\pm v$ which reduce (mod p) to give an ovoid in the triality quadric. $\square$



John H. Conway

More E_8-type ovoids in $O_8^+(p)$

We generalized Conway's construction (M., 1993) to a larger class of ovoids in $O_8^+(p)$, denoted

$$\mathcal{O}_{r,p}(u)$$

where $r \neq p$ are primes, $u \in E$ such that $\left(\dfrac{-p\|u\|^2/2}{r}\right) = +1$.

(The cases $r = 2, 3$ are in the original Conway paper.)

$\mathcal{O}_{r,p}(u)$ is formed using vectors $x \in \mathbb{Z}u + rE \subset E$ of norm $\|x\|^2 = 2k(r-k)p,\ \ 1 \leqslant k \leqslant \lfloor \frac{r-1}{2} \rfloor$.

We generalized Conway's construction (M., 1993) to a larger class of ovoids in $O_8^+(p)$, denoted

$$\mathcal{O}_{r,p}(u)$$

where $r \neq p$ are primes, $u \in E$ such that $\left(\frac{-p\|u\|^2/2}{r}\right) = +1$.
(The cases $r = 2, 3$ are in the original Conway paper.)

$\mathcal{O}_{r,p}(u)$ is formed using vectors $x \in \mathbb{Z}u + rE \subset E$ of norm $\|x\|^2 = 2k(r-k)p, \; 1 \leqslant k \leqslant \lfloor\frac{r-1}{2}\rfloor$.

We generalized Conway's construction (M., 1993) to a larger class of ovoids in $O_8^+(p)$, denoted

$$\mathcal{O}_{r,p}(u)$$

where $r \neq p$ are primes, $u \in E$ such that $\left(\frac{-p\|u\|^2/2}{r}\right) = +1$. (The cases $r = 2, 3$ are in the original Conway paper.)

$\mathcal{O}_{r,p}(u)$ is formed using vectors $x \in \mathbb{Z}u + rE \subset E$ of norm $\|x\|^2 = 2k(r-k)p, \;\; 1 \leqslant k \leqslant \lfloor \frac{r-1}{2} \rfloor$.

How many E_8-type ovoids are there?

Denote by n_p the number of equivalence types of ovoids (up to isometry and similarity) arising from our construction.

We conjectured that $n_p \to \infty$ as $p \to \infty$:

p	2	3	5	7	11	13	17	19	23
n_p	1	1	2	2	4	4	7	6	10

How many E_8-type ovoids are there?

Denote by n_p the number of equivalence types of ovoids (up to isometry and similarity) arising from our construction.

We conjectured that $n_p \to \infty$ as $p \to \infty$:

p	2	3	5	7	11	13	17	19	23
n_p	1	1	2	2	4	4	7	6	10

Counting Ovoids

So instead we count the *total* number of ovoids

$$N_p = \sum_{i=1}^{n_p} [G : G_{\mathcal{O}_i}]$$

where $\mathcal{O}_i$ are representatives of the n_p equivalence types under G, the full group of isometries and similarities.

Conjecture

For $p > 3$, $N_p = [G : W]\frac{p^4-1}{2}$.

Here $|G| = 2p^{12}(p^6-1)(p^4-1)^2(p^2-1)$, $W = W(E_8)/\{\pm I\}$, $|W| = 348{,}364{,}800$. This formula may be rewritten in the more convenient form

$$\sum_{i=1}^{n_p} \frac{|W|}{|G_{\mathcal{O}_i}|} = \sum_{i=1}^{n_p} \frac{[W : W_{\mathcal{O}_i}]}{[G_{\mathcal{O}_i} : W_{\mathcal{O}_i}]} = \frac{p^4-1}{2}$$

which we refer to as the Conjectured Mass Formula.

Counting Ovoids

So instead we count the *total* number of ovoids

$$N_p = \sum_{i=1}^{n_p} [G : G_{\mathcal{O}_i}]$$

where $\mathcal{O}_i$ are representatives of the n_p equivalence types under G, the full group of isometries and similarities.

Conjecture

For $p > 3$, $N_p = [G : W]\frac{p^4-1}{2}$.

Here $|G| = 2p^{12}(p^6-1)(p^4-1)^2(p^2-1)$, $\quad W = W(E_8)/\{\pm I\}$, $|W| = 348{,}364{,}800$. This formula may be rewritten in the more convenient form

$$\sum_{i=1}^{n_p} \frac{|W|}{|G_{\mathcal{O}_i}|} = \sum_{i=1}^{n_p} \frac{[W : W_{\mathcal{O}_i}]}{[G_{\mathcal{O}_i} : W_{\mathcal{O}_i}]} = \frac{p^4-1}{2}$$

which we refer to as the Conjectured Mass Formula.

Counting Ovoids

So instead we count the *total* number of ovoids

$$N_p = \sum_{i=1}^{n_p} [G : G_{\mathcal{O}_i}]$$

where $\mathcal{O}_i$ are representatives of the n_p equivalence types under G, the full group of isometries and similarities.

Conjecture

For $p > 3$, $N_p = [G : W]\frac{p^4-1}{2}$.

Here $|G| = 2p^{12}(p^6-1)(p^4-1)^2(p^2-1)$, $\quad W = W(E_8)/\{\pm I\}$, $|W| = 348{,}364{,}800$. This formula may be rewritten in the more convenient form

$$\sum_{i=1}^{n_p} \frac{|W|}{|G_{\mathcal{O}_i}|} = \sum_{i=1}^{n_p} \frac{[W : W_{\mathcal{O}_i}]}{[G_{\mathcal{O}_i} : W_{\mathcal{O}_i}]} = \frac{p^4-1}{2}$$

which we refer to as the Conjectured Mass Formula.

Counting Ovoids

The conjectured mass formula

$$\sum_{i=1}^{n_p} \frac{|W|}{|G_{\mathcal{O}_i}|} = \sum_{i=1}^{n_p} \frac{[W : W_{\mathcal{O}_i}]}{[G_{\mathcal{O}_i} : W_{\mathcal{O}_i}]} = \frac{p^4 - 1}{2}$$

is strongly supported by the following table of values:

p	n_p	Mass Formula
5	2	$120+192 = 312 = \frac{5^4-1}{2}$
7	2	$120+1080 = 1200 = \frac{7^4-1}{2}$
11	4	$120+240+1920+5040 = 7320 = \frac{11^4-1}{2}$
13	4	$120+2160+3360+8640 = 14280 = \frac{13^4-1}{2}$
17	7	$120+240+1080+1920+6720+8640+23040 = 41760 = \frac{17^4-1}{2}$
19	6	$120+240+2160+15120+17280+30240 = 65160 = \frac{19^4-1}{2}$
23	10	$120+240+240+1080+1920+5040+6720$ $+15120+40320+69120 = 139920 = \frac{23^4-1}{2}$

The exceptional case $p = 3$

Our conjectured mass formula fails when $p = 3$ since in this case alone, the ovoids lie in an $O_7(p)$ hyperplane.

See Ball, Govaerts and Storme (2006).

Lower bounds for n_p

If the Conjectured Mass Formula holds, then trivially

$$[G:W]^{\frac{p^4-1}{2}} = N_p = \sum_{i=1}^{n_p} [G:G_{\mathcal{O}_i}] \leqslant n_p|G| \quad \Rightarrow \quad n_p \geqslant Cp^4$$

as $p \to \infty$. This estimate is conservative since *most* of the E_8-type ovoids have $|G_{\mathcal{O}}| \ll |G|$.

Exercise: Find an ovoid with $G_{\mathcal{O}} = 1$.

Show that $G_{\mathcal{O}} = 1$ for most E_8-type ovoids.

What are reasonable *upper* bounds for $|G_{\mathcal{O}}|$?

Lower bounds for n_p

If the Conjectured Mass Formula holds, then trivially

$$[G:W]\frac{p^4-1}{2} = N_p = \sum_{i=1}^{n_p} [G:G_{\mathcal{O}_i}] \leqslant n_p|G| \quad \Rightarrow \quad n_p \geqslant Cp^4$$

as $p \to \infty$. This estimate is conservative since *most* of the E_8-type ovoids have $|G_{\mathcal{O}}| \ll |G|$.

Exercise: Find an ovoid with $G_{\mathcal{O}} = 1$.

Show that $G_{\mathcal{O}} = 1$ for most E_8-type ovoids.

What are reasonable *upper* bounds for $|G_{\mathcal{O}}|$?

Lower bounds for n_p

If the Conjectured Mass Formula holds, then trivially

$$[G:W]^{\frac{p^4-1}{2}} = N_p = \sum_{i=1}^{n_p} [G:G_{\mathcal{O}_i}] \leqslant n_p|G| \quad \Rightarrow \quad n_p \geqslant Cp^4$$

as $p \to \infty$. This estimate is conservative since *most* of the E_8-type ovoids have $|G_{\mathcal{O}}| \ll |G|$.

Exercise: Find an ovoid with $G_{\mathcal{O}} = 1$.

Show that $G_{\mathcal{O}} = 1$ for most E_8-type ovoids.

What are reasonable *upper* bounds for $|G_{\mathcal{O}}|$?

Lower bounds for n_p

If the Conjectured Mass Formula holds, then trivially

$$[G:W]\frac{p^4-1}{2} = N_p = \sum_{i=1}^{n_p}[G:G_{\mathcal{O}_i}] \leqslant n_p|G| \quad \Rightarrow \quad n_p \geqslant Cp^4$$

as $p \to \infty$. This estimate is conservative since *most* of the E_8-type ovoids have $|G_{\mathcal{O}}| \ll |G|$.

Exercise: Find an ovoid with $G_{\mathcal{O}} = 1$.

Show that $G_{\mathcal{O}} = 1$ for most E_8-type ovoids.

What are reasonable *upper* bounds for $|G_{\mathcal{O}}|$?

Lower bounds for n_p

If the Conjectured Mass Formula holds, then trivially

$$[G:W]\frac{p^4-1}{2} = N_p = \sum_{i=1}^{n_p}[G:G_{\mathcal{O}_i}] \leqslant n_p|G| \quad \Rightarrow \quad n_p \geqslant Cp^4$$

as $p \to \infty$. This estimate is conservative since *most* of the E_8-type ovoids have $|G_{\mathcal{O}}| \ll |G|$.

Exercise: Find an ovoid with $G_{\mathcal{O}} = 1$.

Show that $G_{\mathcal{O}} = 1$ for most E_8-type ovoids.

What are reasonable *upper* bounds for $|G_{\mathcal{O}}|$?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

The problem for general q

This construction fails for $q = p^r$, $r > 1$. Why?

It is natural to extend $\mathbb{Z} \subset A$, the ring of integers in a number field, such that $A/pA \cong \mathbb{F}_q$.

Also $E \subset \widehat{E} = E \otimes_{\mathbb{Z}} A$, $\widehat{E}/p\widehat{E} \cong \mathbb{F}_q^8$.

However, counting vectors of fixed norm in $\widehat{E}$ does not produce the necessary numbers for ovoids in $O_8^+(q)$.

Bigger problem: ovoids with the right automorphism groups apparently do not exist unless $q = p$. Why is this?

Compare: Our S_6-invariant ovoids in $O_6^+(q)$ apparently do not exist unless $q = p$. Why is this?

Adding Structure to $(\mathbb{F}_p^8, Q)$

$$
\begin{tikzcd}
\text{E_8 root lattice} & E \arrow[d, "\text{mod } p"'] & O \arrow[l, "\text{forget multiplication}"'] \arrow[d, "\text{mod } p"] & \text{ring of integral octaves} \\
\text{orthogonal space} & (\mathbb{F}_p^8, Q) & \mathfrak{C}_p \arrow[l, "\text{forget multiplication}"] & \text{Cayley algebra}
\end{tikzcd}
$$

There are are essentially $[G : W] = O(p^{28})$ choices of 'E_8 structure' that can be imposed on the orthogonal space $(\mathbb{F}_p^8, Q)$, but $p^6(p^4-1)^2 = O(p^{14})$ choices of Cayley algebra structure.

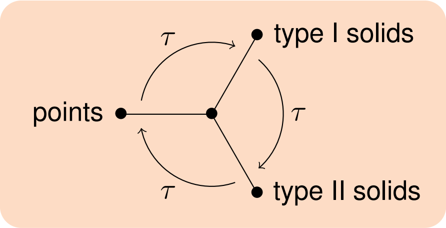
Adding Structure to $(\mathbb{F}_p^8, Q)$

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\text{E_8 root lattice} & E \arrow[d, "\text{mod } p"'] & O \arrow[l, "\text{forget multiplication}"'] \arrow[d, "\text{mod } p"] & \text{ring of integral octaves} \\
\text{orthogonal space} & (\mathbb{F}_p^8, Q) & \mathfrak{C}_p \arrow[l, "\text{forget multiplication}"] & \text{Cayley algebra}
\end{tikzcd}$$

There are are essentially $[G : W] = O(p^{28})$ choices of 'E_8 structure' that can be imposed on the orthogonal space $(\mathbb{F}_p^8, Q)$, but $p^6(p^4 - 1)^2 = O(p^{14})$ choices of Cayley algebra structure.

Triality automorphisms via the Cayley algebra $\mathfrak{C}_q$

$\langle x \rangle$



$$\begin{aligned}\langle x \rangle^{\tau} &= \mathfrak{C}_q x \\ &= \{y \in \mathfrak{C}_q \;:\; yx^* = 0\}\end{aligned}$$

$$\begin{aligned}\langle x \rangle^{\tau^2} &= x\mathfrak{C}_q \\ &= \{y \in \mathfrak{C}_q \;:\; x^* y = 0\}\end{aligned}$$

The role of nonassociative algebra

An alternative description of Conway's 'binary' ovoids $\mathcal{O} = \mathcal{O}_{2,p}(u)$, $p > 2$, $u \in O^{\times} = \{\text{roots of } E\}$:

In the ring O of integral octaves, the element $p \in O$ has $240(p^3 + 1)$ factorizations into irreducibles as $p = x^*x$, $x \in O$.

If we restrict $x \in e + 2O$ then there are $p^3 + 1$ pairs $\{\pm x\}$ of irreducibles. These give an ovoid in $O/pO \simeq \mathbb{F}_p^8$.

This is Conway's binary ovoid ($\mathcal{O} = \mathcal{O}_{2,p}(e)$ in my notation).

An alternative description of Conway's 'binary' ovoids $\mathcal{O} = \mathcal{O}_{2,p}(u)$, $p > 2$, $u \in O^\times = \{\text{roots of } E\}$:

In the ring O of integral octaves, the element $p \in O$ has $240(p^3+1)$ factorizations into irreducibles as $p = x^*x$, $x \in O$.

If we restrict $x \in e + 2O$ then there are p^3+1 pairs $\{\pm x\}$ of irreducibles. These give an ovoid in $O/pO \simeq \mathbb{F}_p^8$.

This is Conway's binary ovoid ($\mathcal{O} = \mathcal{O}_{2,p}(e)$ in my notation).

The role of nonassociative algebra

An alternative description of Conway's 'binary' ovoids $\mathcal{O} = \mathcal{O}_{2,p}(u)$, $p > 2$, $u \in O^\times = \{\text{roots of } E\}$:

In the ring O of integral octaves, the element $p \in O$ has $240(p^3+1)$ factorizations into irreducibles as $p = x^*x$, $x \in O$.

If we restrict $x \in e + 2O$ then there are p^3+1 pairs $\{\pm x\}$ of irreducibles. These give an ovoid in $O/pO \simeq \mathbb{F}_p^8$.

This is Conway's binary ovoid ($\mathcal{O} = \mathcal{O}_{2,p}(e)$ in my notation).

An alternative description of Conway's 'binary' ovoids $\mathcal{O} = \mathcal{O}_{2,p}(u)$, $p > 2$, $u \in O^\times = \{\text{roots of } E\}$:

In the ring O of integral octaves, the element $p \in O$ has $240(p^3+1)$ factorizations into irreducibles as $p = x^*x$, $x \in O$.

If we restrict $x \in e + 2O$ then there are p^3+1 pairs $\{\pm x\}$ of irreducibles. These give an ovoid in $O/pO \simeq \mathbb{F}_p^8$.

This is Conway's binary ovoid ($\mathcal{O} = \mathcal{O}_{2,p}(e)$ in my notation).

Other ovoid constructions from E_8

In our 1993 construction, the sublattice $rE \subset E$ can be replaced by $wO \subset O$ where $w \in O$.

Unfortunately (?) the resulting ovoids are not new.

The sublattice $wO \subset O$ is not an ideal of O due to nonassociativity (i.e. wO it is not a right O-module). Indeed, every right or left ideal of O is a two-sided ideal rO where $r \in \mathbb{Z}$.

Other ovoid constructions from E_8

In our 1993 construction, the sublattice $rE \subset E$ can be replaced by $wO \subset O$ where $w \in O$.

Unfortunately (?) the resulting ovoids are not new.

The sublattice $wO \subset O$ is not an ideal of O due to nonassociativity (i.e. wO it is not a right O-module). Indeed, every right or left ideal of O is a two-sided ideal rO where $r \in \mathbb{Z}$.

Other ovoid constructions from E_8

In our 1993 construction, the sublattice $rE \subset E$ can be replaced by $wO \subset O$ where $w \in O$.

Unfortunately (?) the resulting ovoids are not new.

The sublattice $wO \subset O$ is not an ideal of O due to nonassociativity (i.e. wO it is not a right O-module). Indeed, every right or left ideal of O is a two-sided ideal rO where $r \in \mathbb{Z}$.

Let q be an arbitrary prime power, and $\mathfrak{C}_q$ the Cayley algebra of order q.

So $\mathfrak{C}_q$ is a (nonassociative) alternative algebra of dimension 8 over $\mathbb{F}_q$. The units of $\mathfrak{C}_q$ form a Moufang loop $\mathfrak{C}_q^\times$ of order $q^3(q^4-1)(q-1)$.

Fix your favourite ovoid $\mathcal{O}$ in $O_8^+(q)$. We view $\mathcal{O}$ as a set of q^3+1 zero divisors in $\mathfrak{C}_q$, no two perpendicular.

Every ovoid $\mathcal{O}'$ is naturally in one-to-one correspondence with $\mathcal{O}$. This bijection is unique, given the Cayley algebra structure:

$$\mathcal{O}' = \{f(x)x \,:\, x \in \mathcal{O}\}$$

for some map $f : \mathcal{O} \to \mathfrak{C}_q$.

These bijections appear (but perhaps not so explicitly) in my ovoid construction. But . . .

What does this say about ovoids for general q?

Bijections between ovoids

Let q be an arbitrary prime power, and $\mathfrak{C}_q$ the Cayley algebra of order q.

So $\mathfrak{C}_q$ is a (nonassociative) alternative algebra of dimension 8 over $\mathbb{F}_q$. The units of $\mathfrak{C}_q$ form a Moufang loop $\mathfrak{C}_q^\times$ of order $q^3(q^4-1)(q-1)$.

Fix your favourite ovoid $\mathcal{O}$ in $O_8^+(q)$. We view $\mathcal{O}$ as a set of q^3+1 zero divisors in $\mathfrak{C}_q$, no two perpendicular.

Every ovoid $\mathcal{O}'$ is naturally in one-to-one correspondence with $\mathcal{O}$. This bijection is unique, given the Cayley algebra structure:

$$\mathcal{O}' = \{f(x)x \,:\, x \in \mathcal{O}\}$$

for some map $f : \mathcal{O} \to \mathfrak{C}_q$.

These bijections appear (but perhaps not so explicitly) in my ovoid construction. But …

What does this say about ovoids for general q?

Bijections between ovoids

Let q be an arbitrary prime power, and $\mathfrak{C}_q$ the Cayley algebra of order q.

So $\mathfrak{C}_q$ is a (nonassociative) alternative algebra of dimension 8 over $\mathbb{F}_q$. The units of $\mathfrak{C}_q$ form a Moufang loop $\mathfrak{C}_q^\times$ of order $q^3(q^4-1)(q-1)$.

Fix your favourite ovoid $\mathcal{O}$ in $O_8^+(q)$. We view $\mathcal{O}$ as a set of q^3+1 zero divisors in $\mathfrak{C}_q$, no two perpendicular.

Every ovoid $\mathcal{O}'$ is naturally in one-to-one correspondence with $\mathcal{O}$. This bijection is unique, given the Cayley algebra structure:

$$\mathcal{O}' = \{f(x)x \,:\, x \in \mathcal{O}\}$$

for some map $f : \mathcal{O} \to \mathfrak{C}_q$.

These bijections appear (but perhaps not so explicitly) in my ovoid construction. But . . .

What does this say about ovoids for general q?

Bijections between ovoids

Let q be an arbitrary prime power, and $\mathfrak{C}_q$ the Cayley algebra of order q.

So $\mathfrak{C}_q$ is a (nonassociative) alternative algebra of dimension 8 over $\mathbb{F}_q$. The units of $\mathfrak{C}_q$ form a Moufang loop $\mathfrak{C}_q^\times$ of order $q^3(q^4-1)(q-1)$.

Fix your favourite ovoid $\mathcal{O}$ in $O_8^+(q)$. We view $\mathcal{O}$ as a set of q^3+1 zero divisors in $\mathfrak{C}_q$, no two perpendicular.

Every ovoid $\mathcal{O}'$ is naturally in one-to-one correspondence with $\mathcal{O}$. This bijection is unique, given the Cayley algebra structure:

$$\mathcal{O}' = \{f(x)x \,:\, x \in \mathcal{O}\}$$

for some map $f : \mathcal{O} \to \mathfrak{C}_q$.

These bijections appear (but perhaps not so explicitly) in my ovoid construction. But . . .

What does this say about ovoids for general q?

Let q be an arbitrary prime power, and $\mathfrak{C}_q$ the Cayley algebra of order q.

So $\mathfrak{C}_q$ is a (nonassociative) alternative algebra of dimension 8 over $\mathbb{F}_q$. The units of $\mathfrak{C}_q$ form a Moufang loop $\mathfrak{C}_q^\times$ of order $q^3(q^4-1)(q-1)$.

Fix your favourite ovoid $\mathcal{O}$ in $O_8^+(q)$. We view $\mathcal{O}$ as a set of q^3+1 zero divisors in $\mathfrak{C}_q$, no two perpendicular.

Every ovoid $\mathcal{O}'$ is naturally in one-to-one correspondence with $\mathcal{O}$. This bijection is unique, given the Cayley algebra structure:

$$\mathcal{O}' = \{f(x)x \;:\; x \in \mathcal{O}\}$$

for some map $f : \mathcal{O} \to \mathfrak{C}_q$.

These bijections appear (but perhaps not so explicitly) in my ovoid construction. But ...

What does this say about ovoids for general q?

Connections to the Cayley plane

It is possible to make some sense of the E_8-type construction by embedding these ovoids as objects in the Cayley plane: vectors in O of norm $k(r-k)$ are factorizable as xy where $x^*x = r$ and $y^*y = r-k$. Such pairs $(x,y) \in O^2$ arise naturally in the rational Cayley plane from intersections of lines with certain 'conics'. Details?

This suggests a bigger (possibly related) question:

We know that there cannot be quadrics in $O_{24}^{+}(q)$, at least for any reasonably small q.

But what are the right geometric objects of interest in L/pL where L is the Leech lattice?

Connections to the Cayley plane

It is possible to make some sense of the E_8-type construction by embedding these ovoids as objects in the Cayley plane: vectors in O of norm $k(r-k)$ are factorizable as xy where $x^*x = r$ and $y^*y = r-k$. Such pairs $(x,y) \in O^2$ arise naturally in the rational Cayley plane from intersections of lines with certain 'conics'. Details?

This suggests a bigger (possibly related) question:

We know that there cannot be quadrics in $O^+_{24}(q)$, at least for any reasonably small q.

But what are the right geometric objects of interest in L/pL where L is the Leech lattice?

There exist ovoids in quadrics (including Klein and triality quadrics) over other rings such as $\mathbb{Z}/m\mathbb{Z}$. Some are constructible from E_8.

What do we make of these?

How about ovoids over Galois rings?

Ovoids over other rings

There exist ovoids in quadrics (including Klein and triality quadrics) over other rings such as $\mathbb{Z}/m\mathbb{Z}$. Some are constructible from E_8.

What do we make of these?

How about ovoids over Galois rings?

Ovoids over other rings

There exist ovoids in quadrics (including Klein and triality quadrics) over other rings such as $\mathbb{Z}/m\mathbb{Z}$. Some are constructible from E_8.

What do we make of these?

How about ovoids over Galois rings?

Thank You!

Questions?