Automorphism Groups of Projective Planes with Arbitrarily Many Point and Line Orbits

G. Eric Moorhouse

Department of Mathematics
University of Wyoming

RMAC Seminar 14 Sept 2012

joint work with Tim Penttila

Projective Planes

A *projective plane* is a point-line incidence structure for which

- every pair of distinct points lies on a unique line;
- every pair of distinct lines meets in a unique point; and
- there exist four points with no three collinear.

Every point lies on $N+1$ lines, and every line has $N+1$ points, where N is the *order* of the plane (finite or infinite).

There are N^2+N+1 points and the same number of lines. In the infinite case, this number is simply N.

Projective Planes

A *projective plane* is a point-line incidence structure for which

- every pair of distinct points lies on a unique line;
- every pair of distinct lines meets in a unique point; and
- there exist four points with no three collinear.

Every point lies on $N+1$ lines, and every line has $N+1$ points, where N is the *order* of the plane (finite or infinite).

There are N^2+N+1 points and the same number of lines. In the infinite case, this number is simply N.

Projective Planes

A *projective plane* is a point-line incidence structure for which

- every pair of distinct points lies on a unique line;
- every pair of distinct lines meets in a unique point; and
- there exist four points with no three collinear.

Every point lies on $N+1$ lines, and every line has $N+1$ points, where N is the *order* of the plane (finite or infinite).

There are N^2+N+1 points and the same number of lines. In the infinite case, this number is simply N.

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Theorem (c. 1950's)

Let G be an automorphism group of a finite projective plane Π. Then G has equally many point and line orbits.

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Proof (Brauer, 1941).

Let Π be a finite projective plane with incidence matrix A, and let G be an automorphism group of Π. We have two permutation representations $\pi_i : G \mapsto GL_{N^2+N+1}(\mathbb{C})$ satisfying

$$\pi_1(g)^{-1} A \pi_2(g) = A \quad \text{for all } g \in G.$$

Here π_1, π_2 are the actions of G on points and lines respectively. Now

$$\pi_2(g) = A^{-1} \pi_1(g) A \quad \text{for all } g \in G$$

so

$$[\chi_1, 1_G] = [\chi_2, 1_G]$$

where $\chi_i(g) = tr\, \pi_i(g)$, i.e. the number of G-orbits on points equals the number of G-orbits on lines. □

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Proof (Brauer, 1941).

Let Π be a finite projective plane with incidence matrix A, and let G be an automorphism group of Π. We have two permutation representations $\pi_i : G \mapsto GL_{N^2+N+1}(\mathbb{C})$ satisfying

$$\pi_1(g)^{-1} A \pi_2(g) = A \quad \text{for all } g \in G.$$

Here π_1, π_2 are the actions of G on points and lines respectively. Now

$$\pi_2(g) = A^{-1} \pi_1(g) A \quad \text{for all } g \in G$$

so

$$[\chi_1, 1_G] = [\chi_2, 1_G]$$

where $\chi_i(g) = tr\, \pi_i(g)$, i.e. the number of G-orbits on points equals the number of G-orbits on lines. □

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Proof (Brauer, 1941).

Let Π be a finite projective plane with incidence matrix A, and let G be an automorphism group of Π. We have two permutation representations $\pi_i : G \mapsto GL_{N^2+N+1}(\mathbb{C})$ satisfying

$$\pi_1(g)^{-1}A\pi_2(g) = A \quad \text{for all } g \in G.$$

Here π_1, π_2 are the actions of G on points and lines respectively. Now

$$\pi_2(g) = A^{-1}\pi_1(g)A \quad \text{for all } g \in G$$

so

$$[\chi_1, 1_G] = [\chi_2, 1_G]$$

where $\chi_i(g) = tr\,\pi_i(g)$, i.e. the number of G-orbits on points equals the number of G-orbits on lines. □

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Proof (Brauer, 1941).

Let Π be a finite projective plane with incidence matrix A, and let G be an automorphism group of Π. We have two permutation representations $\pi_i : G \mapsto GL_{N^2+N+1}(\mathbb{C})$ satisfying

$$\pi_1(g)^{-1}A\pi_2(g) = A \quad \text{for all } g \in G.$$

Here π_1, π_2 are the actions of G on points and lines respectively. Now

$$\pi_2(g) = A^{-1}\pi_1(g)A \quad \text{for all } g \in G$$

so

$$[\chi_1, 1_G] = [\chi_2, 1_G]$$

where $\chi_i(g) = tr\,\pi_i(g)$, i.e. the number of G-orbits on points equals the number of G-orbits on lines. □

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Theorem (c. 1950's)

Let G be an automorphism group of a finite projective plane Π. Then G has equally many point and line orbits.

Does this hold in the infinite case?

Cameron (1984) seems to have been the first to put this question in print. Later (1991) he attributed the question to Kantor.

Dembowski-Hughes-Parker Theorem

a.k.a. Block's Lemma

Theorem (c. 1950's)

Let G be an automorphism group of a finite projective plane Π. Then G has equally many point and line orbits.

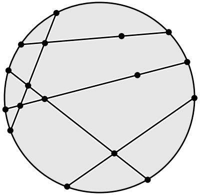
Does this hold in the infinite case?

Cameron (1984) seems to have been the first to put this question in print. Later (1991) he attributed the question to Kantor.

A *Near*-Example

Cameron mentions the following infinite design which comes close to what is required: Start with a closed disk D. Consider the 2-design

$\mathfrak{D}$: Points of D and Lines=Chords of D



Aut $\mathfrak{D}$ is transitive on lines (i.e. chords). It has two orbits on points (boundary points and interior points).

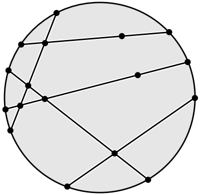
But $\mathfrak{D}$ is not a projective plane: two chords meet in 0 or 1 points.

Aut $\mathfrak{D} \cong PGL_2(\mathbb{R})$

A *Near*-Example

Cameron mentions the following infinite design which comes close to what is required: Start with a closed disk D. Consider the 2-design

$\mathfrak{D}$: Points of D and Lines=Chords of D



Aut $\mathfrak{D}$ is transitive on lines (i.e. chords). It has two orbits on points (boundary points and interior points).

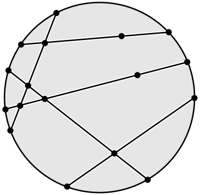
But $\mathfrak{D}$ is not a projective plane: two chords meet in 0 or 1 points.

Aut $\mathfrak{D} \cong PGL_2(\mathbb{R})$

A *Near*-Example

Cameron mentions the following infinite design which comes close to what is required: Start with a closed disk D. Consider the 2-design

$\mathfrak{D}$: Points of D and Lines=Chords of D



Aut $\mathfrak{D}$ is transitive on lines (i.e. chords). It has two orbits on points (boundary points and interior points).

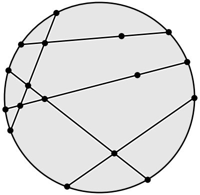
But $\mathfrak{D}$ is not a projective plane: two chords meet in 0 or 1 points.

Aut $\mathfrak{D} \cong PGL_2(\mathbb{R})$

A *Near*-Example

Cameron mentions the following infinite design which comes close to what is required: Start with a closed disk D. Consider the 2-design

$\mathfrak{D}$: Points of D and Lines=Chords of D



Aut $\mathfrak{D}$ is transitive on lines (i.e. chords). It has two orbits on points (boundary points and interior points).

But $\mathfrak{D}$ is not a projective plane: two chords meet in 0 or 1 points.

Aut $\mathfrak{D} \cong PGL_2(\mathbb{R})$

Theorem (M. and Penttila, 2012)

- *There exists a Desarguesian plane* Π *admitting a group* $G < \mathrm{Aut}\,\Pi$ *having two orbits on points, and more than two orbits on lines.*
- *Given any two nonempty sets* A *and* B*, there exists a projective plane* Π *admitting a group* $G \leqslant \mathrm{Aut}\,\Pi$ *having exactly* $|A|$ *orbits on points and* $|B|$ *orbits on lines.*

Skewfields
Artin's Problem

Consider an extension of skewfields $L \supseteq K$.

Artin (1946) asked whether it is possible for the left and right degrees of L over K to differ.

Cohn (1961) gave examples with one degree infinite and the other degree an arbitrary integer $n \geqslant 2$. Schofield (1985) gave examples where the left and right degrees are arbitrary integers $m, n \geqslant 2$.

For our construction, take left-degree > 2 and right-degree 2.

Skewfields

Artin's Problem

Consider an extension of skewfields $L \supseteq K$.

Artin (1946) asked whether it is possible for the left and right degrees of L over K to differ.

Cohn (1961) gave examples with one degree infinite and the other degree an arbitrary integer $n \geqslant 2$. Schofield (1985) gave examples where the left and right degrees are arbitrary integers $m, n \geqslant 2$.

For our construction, take left-degree > 2 and right-degree 2.

Skewfields

Artin's Problem

Consider an extension of skewfields $L \supseteq K$.

Artin (1946) asked whether it is possible for the left and right degrees of L over K to differ.

Cohn (1961) gave examples with one degree infinite and the other degree an arbitrary integer $n \geqslant 2$. Schofield (1985) gave examples where the left and right degrees are arbitrary integers $m, n \geqslant 2$.

For our construction, take left-degree > 2 and right-degree 2.

Desarguesian planes

An arbitrary Desarguesian plane $\Pi = PG(2, L)$ is coordinatized by a (possibly commutative) skewfield L. Points and lines correspond to left and right L-subspaces of L^3 of dimension 1, respectively:

Typical point: $P = L(a,\ b,\ c) = \{(\lambda a,\ \lambda b,\ \lambda c) : \lambda \in L\} \neq \{(0,0,0)\}$

$$\text{Typical line:}\quad \ell = \begin{pmatrix} d \\ e \\ f \end{pmatrix} L = \left\{ \begin{pmatrix} d\mu \\ e\mu \\ f\mu \end{pmatrix} : \mu \in L \right\} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\text{Incidence:}\quad P \in \ell \ \Leftrightarrow\ (a,\ b,\ c) \begin{pmatrix} d \\ e \\ f \end{pmatrix} = ad + be + cf = 0$$

$\mathrm{Aut}(\Pi) \cong PGL_3(L) = GL_3(L)/Z$ where $Z = \{\lambda I : 0 \neq \lambda \in Z(L)\}$

Desarguesian planes

An arbitrary Desarguesian plane $\Pi = PG(2, L)$ is coordinatized by a (possibly commutative) skewfield L. Points and lines correspond to left and right L-subspaces of L^3 of dimension 1, respectively:

Typical point: $P = L(a,\ b,\ c) = \{(\lambda a,\ \lambda b,\ \lambda c) : \lambda \in L\} \neq \{(0,0,0)\}$

$$\text{Typical line:} \quad \ell = \begin{pmatrix} d \\ e \\ f \end{pmatrix} L = \left\{ \begin{pmatrix} d\mu \\ e\mu \\ f\mu \end{pmatrix} : \mu \in L \right\} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\text{Incidence:} \quad P \in \ell \ \Leftrightarrow \ (a,\ b,\ c)\begin{pmatrix} d \\ e \\ f \end{pmatrix} = ad + be + cf = 0$$

$\mathrm{Aut}(\Pi) \cong PGL_3(L) = GL_3(L)/Z$ where $Z = \{\lambda I : 0 \neq \lambda \in Z(L)\}$

Desarguesian examples

Consider $G = PGL_3(K) < PGL_3(L)$ where $L \supseteq K$ has left-degree > 2 and right-degree 2.

Then G has 2 orbits on points of $\Pi = PG_2(L)$:

$$L(a,\ b,\ c) \in \begin{cases} (L(1,\ 0,\ 0))^G, & \text{if } a, b, c \text{ are right-linearly dependent over } K; \\ (L(1,\ \alpha,\ 0))^G, & \text{if } a, b, c \text{ are right-linearly independent over } K \end{cases}$$

where $\{1, \alpha\}$ is a basis for L as a right vector space over K. And *more than* 2 orbits on lines.

Desarguesian examples

Consider $G = PGL_3(K) < PGL_3(L)$ where $L \supseteq K$ has left-degree > 2 and right-degree 2.

Then G has 2 orbits on points of $\Pi = PG_2(L)$:

$$L(a,\ b,\ c) \in \begin{cases} \big(L(1,\ 0,\ 0)\big)^G, & \text{if } a, b, c \text{ are right-linearly dependent over } K; \\ \big(L(1,\ \alpha,\ 0)\big)^G, & \text{if } a, b, c \text{ are right-linearly independent over } K \end{cases}$$

where $\{1, \alpha\}$ is a basis for L as a right vector space over K. And *more than* 2 orbits on lines.

The Group G

Consider a multiplicative group G satisfying

(G1) G is infinite nonabelian;

(G2) Every conjugacy class in G other than $\{1\}$ has cardinality $|G|$; and

(G3) Every element of G has at most one square root in G.

For every infinite cardinal number C, there is such a group of cardinality C (e.g. a free group on C generators; in the countable case, 2 generators suffice).

The Group G

Consider a multiplicative group G satisfying

(G1) G is infinite nonabelian;

(G2) Every conjugacy class in G other than $\{1\}$ has cardinality $|G|$; and

(G3) Every element of G has at most one square root in G.

For every infinite cardinal number C, there is such a group of cardinality C (e.g. a free group on C generators; in the countable case, 2 generators suffice).

Plane Construction

Theorem

Let A and B be nonempty sets with $|A|, |B| \leqslant |G|$ where G satisfies (G1), (G2), (G3) above. Then there exists a projective plane Π of order $|G|$ with a group of collineations isomorphic to G, having exactly $|A|$ point orbits and $|B|$ line orbits.

Proof We require an indexed collection of subsets $D_{a,b} \subset G$ for $(a, b) \in A \times B$ satisfying certain conditions (see (D1), (D2) below).

$$\text{Points:} \quad (x, a) \in G \times A$$

$$\text{Lines:} \quad (y, b) \in G \times B$$

$$\text{Incidence:} \quad (x, a) \text{ lies on } (y, b) \Leftrightarrow xy^{-1} \in D_{a,b}$$

Plane Construction

Theorem

Let A and B be nonempty sets with $|A|, |B| \leqslant |G|$ where G satisfies (G1), (G2), (G3) above. Then there exists a projective plane Π of order $|G|$ with a group of collineations isomorphic to G, having exactly $|A|$ point orbits and $|B|$ line orbits.

Proof We require an indexed collection of subsets $D_{a,b} \subset G$ for $(a, b) \in A \times B$ satisfying certain conditions (see (D1), (D2) below).

$$\text{Points:} \quad (x, a) \in G \times A$$

$$\text{Lines:} \quad (y, b) \in G \times B$$

$$\text{Incidence:} \quad (x, a) \text{ lies on } (y, b) \Leftrightarrow xy^{-1} \in D_{a,b}$$

Plane Construction

The properties required of the subsets $D_{a,b} \subset G$ are:

(D1) For all $b_1, b_2 \in B$ and $g \in G$, there exists $a \in A$ and elements $d_i \in D_{a,b_i}$ such that $g = d_1^{-1}d_2$. The triple (a, d_1, d_2) is unique whenever $(b_1, g) \neq (b_2, 1)$.

(D2) For all $a_1, a_2 \in A$ and $g \in G$, there exists $b \in B$ and elements $d_i \in D_{a_i,b}$ such that $g = d_1 d_2^{-1}$. The triple (b, d_1, d_2) is unique whenever $(a_1, g) \neq (a_2, 1)$.

We construct the required subsets $D_{a,b} \subset G$ by transfinite recursion. When $|A| = |B| = 1$ just one subset $D \subset G$ is required, a *difference set* (Hughes, 1955).

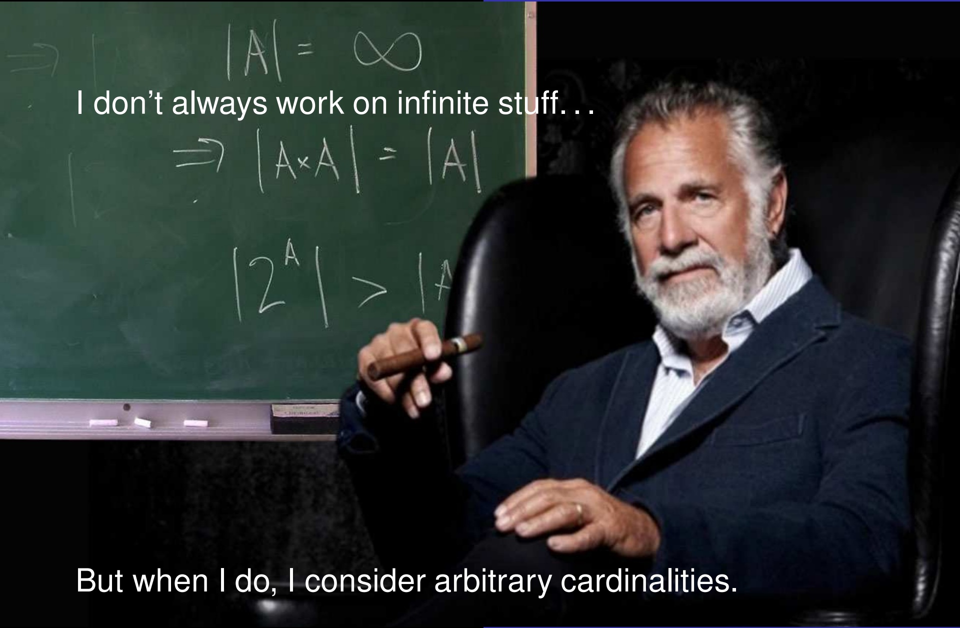
Plane Construction

The properties required of the subsets $D_{a,b} \subset G$ are:

(D1) For all $b_1, b_2 \in B$ and $g \in G$, there exists $a \in A$ and elements $d_i \in D_{a,b_i}$ such that $g = d_1^{-1}d_2$. The triple (a, d_1, d_2) is unique whenever $(b_1, g) \neq (b_2, 1)$.

(D2) For all $a_1, a_2 \in A$ and $g \in G$, there exists $b \in B$ and elements $d_i \in D_{a_i,b}$ such that $g = d_1 d_2^{-1}$. The triple (b, d_1, d_2) is unique whenever $(a_1, g) \neq (a_2, 1)$.

We construct the required subsets $D_{a,b} \subset G$ by transfinite recursion. When $|A| = |B| = 1$ just one subset $D \subset G$ is required, a *difference set* (Hughes, 1955).


I don't always work on infinite stuff. . .
$|A| = \infty$
$\Rightarrow |A \times A| = |A|$
But when I do, I consider arbitrary cardinalities.

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Let

$$\text{STEPS} = (A \times A \times G) \cup (B \times B \times G)$$

(here we assume $A \cap B = \varnothing$). Well-order the set of steps as

$$\text{STEPS} = \{\text{STEP}(\alpha) : \alpha < C\}$$

where $C = |\text{STEPS}| = |G|$. Recursively construct

$$D_{a,b} = \bigcup_{\alpha < C} D_{a,b}(\alpha).$$

Initially (i.e. at STEP(0)) all sets $D_{a,b}(0) = \varnothing$.

For every limit ordinal $\alpha < C$, set $D_{a,b}(\alpha) = \bigcup_{\beta<\alpha} D_{a,b}(\beta)$.

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Let

$$\text{STEPS} = (A \times A \times G) \cup (B \times B \times G)$$

(here we assume $A \cap B = \varnothing$). Well-order the set of steps as

$$\text{STEPS} = \{\text{STEP}(\alpha) : \alpha < C\}$$

where $C = |\text{STEPS}| = |G|$. Recursively construct

$$D_{a,b} = \bigcup_{\alpha < C} D_{a,b}(\alpha).$$

Initially (i.e. at STEP(0)) all sets $D_{a,b}(0) = \varnothing$.

For every limit ordinal $\alpha < C$, set $D_{a,b}(\alpha) = \bigcup_{\beta<\alpha} D_{a,b}(\beta)$.

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Let

$$\mathrm{STEPS} = (A \times A \times G) \cup (B \times B \times G)$$

(here we assume $A \cap B = \varnothing$). Well-order the set of steps as

$$\mathrm{STEPS} = \{\mathrm{STEP}(\alpha) : \alpha < C\}$$

where $C = |\mathrm{STEPS}| = |G|$. Recursively construct

$$D_{a,b} = \bigcup_{\alpha < C} D_{a,b}(\alpha).$$

Initially (i.e. at STEP(0)) all sets $D_{a,b}(0) = \varnothing$.

For every limit ordinal $\alpha < C$, set $D_{a,b}(\alpha) = \bigcup_{\beta<\alpha} D_{a,b}(\beta)$.

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Let

$$\text{STEPS} = (A \times A \times G) \cup (B \times B \times G)$$

(here we assume $A \cap B = \varnothing$). Well-order the set of steps as

$$\text{STEPS} = \{\text{STEP}(\alpha) : \alpha < C\}$$

where $C = |\text{STEPS}| = |G|$. Recursively construct

$$D_{a,b} = \bigcup_{\alpha < C} D_{a,b}(\alpha).$$

Initially (i.e. at STEP(0)) all sets $D_{a,b}(0) = \varnothing$.

For every limit ordinal $\alpha < C$, set $D_{a,b}(\alpha) = \bigcup_{\beta<\alpha} D_{a,b}(\beta)$.

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Now suppose $\alpha = \beta + 1 < C$. Form $D_{a,b}(\beta + 1) \supseteq D_{a,b}(\beta)$ by adjoining at most two elements of G, as follows. Consider only case STEP$(\alpha) = (b_1, b_2, g)$ (the other case STEP$(\alpha) = (a_1, a_2, g)$ is similar). *Three subcases:*

1. Suppose $g = d_1^{-1} d_2,\ d_i \in D_{a,b_i}(\beta),\ a \in A$. Then *add nothing*: $D_{a,b}(\alpha) = D_{a,b}(\beta)$ for all a, b.
2. If 1 fails, first choose $a_1 \in A$ arbitrarily. Form $D_{a,b}(\alpha) \supseteq D_{a,b}(\beta)$ by adding one or two new elements for $(a, b) \in \{(a_1, b_1), (a_1, b_2)\}$ and no new elements for other (a, b), such that $g = d_1^{-1} d_2,\ d_i \in D_{a_1,b_i}(\alpha)$. There are $|G| = C$ elements to choose from, and *fewer* than this many choices are excluded by (D1)–(D2).

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Now suppose $\alpha = \beta + 1 < C$. Form $D_{a,b}(\beta+1) \supseteq D_{a,b}(\beta)$ by adjoining at most two elements of G, as follows. Consider only case STEP$(\alpha) = (b_1, b_2, g)$ (the other case STEP$(\alpha) = (a_1, a_2, g)$ is similar). *Three subcases:*

1. Suppose $g = d_1^{-1}d_2,\ d_i \in D_{a,b_i}(\beta),\ a \in A$. Then *add nothing*: $D_{a,b}(\alpha) = D_{a,b}(\beta)$ for all a, b.
2. If 1 fails, first choose $a_1 \in A$ arbitrarily. Form $D_{a,b}(\alpha) \supseteq D_{a,b}(\beta)$ by adding one or two new elements for $(a,b) \in \{(a_1,b_1),(a_1,b_2)\}$ and no new elements for other (a,b), such that $g = d_1^{-1}d_2,\ d_i \in D_{a_1,b_i}(\alpha)$. There are $|G| = C$ elements to choose from, and *fewer* than this many choices are excluded by (D1)–(D2).

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Now suppose $\alpha = \beta + 1 < C$. Form $D_{a,b}(\beta + 1) \supseteq D_{a,b}(\beta)$ by adjoining at most two elements of G, as follows. Consider only case STEP$(\alpha) = (b_1, b_2, g)$ (the other case STEP$(\alpha) = (a_1, a_2, g)$ is similar). *Three subcases:*

1. Suppose $g = d_1^{-1} d_2,\ d_i \in D_{a,b_i}(\beta),\ a \in A$. Then *add nothing*: $D_{a,b}(\alpha) = D_{a,b}(\beta)$ for all a, b.
2. If 1 fails, first choose $a_1 \in A$ arbitrarily. Form $D_{a,b}(\alpha) \supseteq D_{a,b}(\beta)$ by adding one or two new elements for $(a, b) \in \{(a_1, b_1), (a_1, b_2)\}$ and no new elements for other (a, b), such that $g = d_1^{-1} d_2,\ d_i \in D_{a_1,b_i}(\alpha)$. There are $|G| = C$ elements to choose from, and *fewer* than this many choices are excluded by (D1)–(D2).

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Now suppose $\alpha = \beta + 1 < C$. Form $D_{a,b}(\beta + 1) \supseteq D_{a,b}(\beta)$ by adjoining at most two elements of G, as follows. Consider only case STEP$(\alpha) = (b_1, b_2, g)$ (the other case STEP$(\alpha) = (a_1, a_2, g)$ is similar). *Three subcases:*

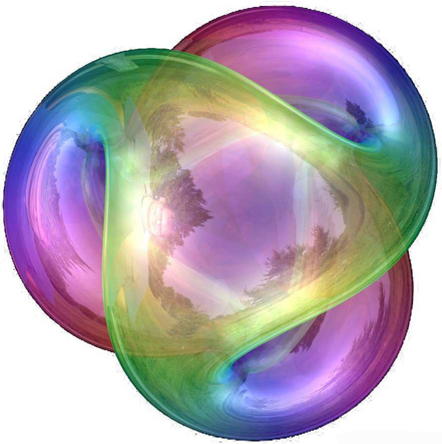
1. Suppose $g = d_1^{-1} d_2,\ d_i \in D_{a,b_i}(\beta),\ a \in A$. Then *add nothing*: $D_{a,b}(\alpha) = D_{a,b}(\beta)$ for all a, b.
2. If 1 fails, first choose $a_1 \in A$ arbitrarily. Form $D_{a,b}(\alpha) \supseteq D_{a,b}(\beta)$ by adding one or two new elements for $(a, b) \in \{(a_1, b_1), (a_1, b_2)\}$ and no new elements for other (a, b), such that $g = d_1^{-1} d_2,\ d_i \in D_{a_1,b_i}(\alpha)$. There are $|G| = C$ elements to choose from, and *fewer* than this many choices are excluded by (D1)–(D2).

Recursion on STEPS $= (A \times A \times G) \cup (B \times B \times G)$

Now suppose $\alpha = \beta + 1 < C$. Form $D_{a,b}(\beta+1) \supseteq D_{a,b}(\beta)$ by adjoining at most two elements of G, as follows. Consider only case STEP$(\alpha) = (b_1, b_2, g)$ (the other case STEP$(\alpha) = (a_1, a_2, g)$ is similar). *Three subcases:*

1. Suppose $g = d_1^{-1}d_2,\ d_i \in D_{a,b_i}(\beta),\ a \in A$. Then *add nothing*: $D_{a,b}(\alpha) = D_{a,b}(\beta)$ for all a, b.
2. If 1 fails, first choose $a_1 \in A$ arbitrarily. Form $D_{a,b}(\alpha) \supseteq D_{a,b}(\beta)$ by adding one or two new elements for $(a,b) \in \{(a_1,b_1),(a_1,b_2)\}$ and no new elements for other (a,b), such that $g = d_1^{-1}d_2,\ d_i \in D_{a_1,b_i}(\alpha)$. There are $|G| = C$ elements to choose from, and *fewer* than this many choices are excluded by (D1)–(D2).

Thank You!



Questions?