Computing in Sporadic Groups: An Application of Symmetric Generation

Ben Fairbairn

University of Birmingham

Groups St Andrews, University of Bath, August 2^{nd} 2009

Joint with RT Curtis

The Basic Idea

- A group G may contain a generating set $T \subset G$ that is symmetric

The Basic Idea

- A group G may contain a generating set $T \subset G$ that is symmetric i.e. $N_G(T)$ acts transitively on the elements of T giving a T a symmetric combinatorial structure.

The Basic Idea

- A group G may contain a generating set $T \subset G$ that is symmetric i.e. $N_G(T)$ acts transitively on the elements of T giving a T a symmetric combinatorial structure.
- Can turn this idea on its head

The Basic Idea

- A group G may contain a generating set $T \subset G$ that is symmetric i.e. $N_G(T)$ acts transitively on the elements of T giving a T a symmetric combinatorial structure.
- Can turn this idea on its head i.e. prescribe a symmetric combinatorial structure for T and ask "What does G look like?"

The Basic Idea

- A group G may contain a generating set $T \subset G$ that is symmetric i.e. $N_G(T)$ acts transitively on the elements of T giving a T a symmetric combinatorial structure.
- Can turn this idea on its head i.e. prescribe a symmetric combinatorial structure for T and ask "What does G look like?"
- Can be useful for representing elements of G succinctly as a word in the elements of T.

Symmetric Generation - ya wha'?

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2.

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.
Fix a transitive permutation group $N \leq Sym(n)$.

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.
Fix a transitive permutation group $N \leq Sym(n)$. We can define an action of N on $2^{\star n}$ thusly -

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.
Fix a transitive permutation group $N \leq Sym(n)$. We can define an action of N on $2^{\star n}$ thusly - for $\pi \in N$ set

$$t_i^{\pi} := t_{\pi(i)}.$$

Symmetric Generation - ya wha'?

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.
Fix a transitive permutation group $N \leq Sym(n)$. We can define an action of N on $2^{\star n}$ thusly - for $\pi \in N$ set

$$t_i^{\pi} := t_{\pi(i)}.$$

Using the above action we can define the semi-direct product

$$P := 2^{\star n} : N.$$

We write $2^{\star n}$ for a free product of n copies of C_2, the cyclic group of order 2. We write t_i for the involution generating the i^{th} copy of C_2.
Fix a transitive permutation group $N \leq Sym(n)$. We can define an action of N on $2^{\star n}$ thusly - for $\pi \in N$ set

$$t_i^\pi := t_{\pi(i)}.$$

Using the above action we can define the semi-direct product

$$P := 2^{\star n} : N.$$

We can P a **progenitor**.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the t_is.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the t_is.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the t_is.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$. We express this as

$$\frac{2^{\star n} : N}{\pi w} := G.$$

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the t_is.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$. We express this as

$$\frac{2^{\star n} : N}{\pi w} := G.$$

We call this a **symmetric presentation** of G.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the $t_i s$.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$. We express this as

$$\frac{2^{\star n} : N}{\pi w} := G.$$

We call this a **symmetric presentation** of G.
We call N the **control group** of G.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the $t_i s$.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$. We express this as

$$\frac{2^{\star n} : N}{\pi w} := G.$$

We call this a **symmetric presentation** of G.
We call N the **control group** of G.
We call the t_is the **symmetric generators** of G.

Symmetric Generation - ya wha'?

Any element of $P = 2^{\star n} : N$ may be expressed as πw where $\pi \in N$ and $w \in 2^{\star n}$, a word in the $t_i s$.
Given an element $\pi w \in P$ we may factor P by the subgroup $\langle \pi w \rangle^P$. We express this as

$$\frac{2^{\star n} : N}{\pi w} := G.$$

We call this a **symmetric presentation** of G.
We call N the **control group** of G.
We call the t_is the **symmetric generators** of G.
(Modulo notational abuse.)

Good Things Come in Small Packages

To establish if G is finite we enumerate the double cosets $NgN \subset G$.

Good Things Come in Small Packages

To establish if G is finite we enumerate the double cosets $NgN \subset G$. Since $g = \pi w$ for some $\pi \in N$ and $w \in 2^{\star n}$ we have

Good Things Come in Small Packages

To establish if G is finite we enumerate the double cosets $NgN \subset G$. Since $g = \pi w$ for some $\pi \in N$ and $w \in 2^{\star n}$ we have

$$NgN = N\pi wN = NwN.$$

Good Things Come in Small Packages

To establish if G is finite we enumerate the double cosets $NgN \subset G$. Since $g = \pi w$ for some $\pi \in N$ and $w \in 2^{\star n}$ we have

$$NgN = N\pi wN = NwN.$$

An adaptation of the celebrated Todd-Coxeter algorithm can be used to enumerate these and John Bray's coset enumeration program is extremely good at at running this procedure.

Good Things Come in Small Packages

To establish if G is finite we enumerate the double cosets $NgN \subset G$. Since $g = \pi w$ for some $\pi \in N$ and $w \in 2^{\star n}$ we have

$$NgN = N\pi wN = NwN.$$

An adaptation of the celebrated Todd-Coxeter algorithm can be used to enumerate these and John Bray's coset enumeration program is extremely good at at running this procedure.

JN Bray and RT Curtis "Double coset enumeration of symmetrically generated groups" J. Group Theory **7** *(2004) 167-185*

$2 \times 2 = ?$

If G is finite then there is a maximum length for w.

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if

$2 \times 2 =?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ has minimal length.

$2 \times 2 = ?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ has minimal length.
If $g := \pi_1 w_1$ and $h := \pi_2 w_2$ then $g, h \in G$.

$2 \times 2 =?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ $\underline{\text{has minimal length}}$.
If $g := \pi_1 w_1$ and $h := \pi_2 w_2$ then $g, h \in G$.

What is gh?

$2 \times 2 = ?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ has minimal length.
If $g := \pi_1 w_1$ and $h := \pi_2 w_2$ then $g, h \in G$.

What is gh?
What is g^{-1}?

$2 \times 2 =?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ has minimal length.
If $g := \pi_1 w_1$ and $h := \pi_2 w_2$ then $g, h \in G$.

What is gh?
What is g^{-1}?
Do we have $g = h$?

$2 \times 2 = ?$

If G is finite then there is a maximum length for w. We say $g \in G$ is **symmetrically represented** if it is expressed as $g = \pi w$ with $\pi \in N$ and $w \in 2^{\star n}$ has minimal length.
If $g := \pi_1 w_1$ and $h := \pi_2 w_2$ then $g, h \in G$.

What is gh?
What is g^{-1}?
Do we have $g = h$?

Use knowledge from the coset enumeration to answer these questions!

Example: the Janko group J_1

$|J_1|$=175 560

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

Example: the Janko group J_1

$|J_1| = 175\ 560$

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$.

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

266

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$266 > 7^2 = 49$$

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$266 > 7^2 = 49 > 11 + 4 = 15$$

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$266 > 7^2 = 49 > 11 + 4 = 15 (> 10 + 3 = 13).$$

Example: the Janko group J_1

$|J_1|$=175 560

$$\frac{2^{\star 11} : L_2(11)}{(\pi t_1)^5} \cong J_1$$

So every element can be symmetrically represented as πw with $\pi \in L_2(11) \leq Sym(11)$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$266 > 7^2 = 49 > 11 + 4 = 15 (> 10 + 3 = 13).$$

RT Curtis and Z Hasan "Symmetric Representation of the Elements of the Janko Group J_1" J. Symbolic Computation **22** *(1996), 201-214*

Example: the Janko group $J_3{:}2$

$|J_3 : 2| = 100\ 465\ 920$

Example: the Janko group $J_3{:}2$

$|J_3 : 2| = 100\ 465\ 920$

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

Example: the Janko group J_3:2

$|J_3 : 2| = 100\ 465\ 920$

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$.

Example: the Janko group J_3:2

$|J_3 : 2| = 100\ 465\ 920$

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

Example: the Janko group J_3:2

$|J_3 : 2|$=100 465 920

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

6156

Example: the Janko group J_3:2

$|J_3 : 2| = 100\ 465\ 920$

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

$$6156 > 9^2 = 81$$

Example: the Janko group J_3:2

$|J_3 : 2|$=100 465 920

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

$$6156 > 9^2 = 81 > (2^2 + 1) + 3 = 8$$

Example: the Janko group J_3:2

$|J_3 : 2| = 100\ 465\ 920$

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

$$6156 > 9^2 = 81 > (2^2 + 1) + 3 = 8 (> (2^2 + 1) + 2 = 7).$$

Example: the Janko group $J_3{:}2$

$|J_3 : 2|$=100 465 920

$$\frac{2^{\star 120} : (L_2(16) : 4)}{(\pi t_1)^5} \cong J_3 : 2$$

So every element can be symmetrically represented as πw with $\pi \in L_2(16) : 4$ and $l(w) \leq 3$. Compare this with the more 'traditional' representations:

$$6156 > 9^2 = 81 > (2^2 + 1) + 3 = 8 (> (2^2 + 1) + 2 = 7).$$

JD Bradley "Symmetric presentations of two sporadic simple groups" PhD thesis, University of Birmingham (2005)

Example: the conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0| = 8\ 315\ 553\ 613\ 086\ 720\ 000$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

JN Bray and RT Curtis "The Leech lattice Λ and the Conway group ·0 revisited" accepted by the transactions of the AMS

$$\frac{2^{\star\binom{24}{4}} : M_{24}}{(\pi t)^3} \cong \cdot 0$$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

> *JN Bray and RT Curtis "The Leech lattice Λ and the Conway group ·0 revisited" accepted by the transactions of the AMS*

$$\frac{2^{\star\binom{24}{4}} : M_{24}}{(\pi t)^3} \cong \cdot 0$$

Problem:

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

JN Bray and RT Curtis "The Leech lattice Λ and the Conway group ·0 revisited" accepted by the transactions of the AMS

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

Problem: $|\cdot 0 : \mathrm{M}_{24}|$ is a bit big!

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

JN Bray and RT Curtis "The Leech lattice Λ and the Conway group ·0 revisited" accepted by the transactions of the AMS

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

Problem: $|\cdot 0 : \mathrm{M}_{24}|$ is a bit big!
Too big in fact for us to enumerate the double cosets $\mathrm{M}_{24} w \mathrm{M}_{24}$.

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

JN Bray and RT Curtis "The Leech lattice Λ and the Conway group ·0 revisited" accepted by the transactions of the AMS

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

Problem: $|\cdot 0 : \mathrm{M}_{24}|$ is a bit big!
Too big in fact for us to enumerate the double cosets $\mathrm{M}_{24} w \mathrm{M}_{24}$.

!

Big is Beautiful

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

Big is Beautiful

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.

Big is Beautiful

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.

Big is Beautiful

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O\Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.
Indeed every element of $\cdot 0$ may written in the form $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$,

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.
Indeed every element of $\cdot 0$ may written in the form $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$

Big is Beautiful

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O\Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.
Indeed every element of $\cdot 0$ may written in the form $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$.

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.
Indeed every element of $\cdot 0$ may written in the form $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$.
Problem:

$$\frac{2^{\star 759} : \mathrm{M}_{24}}{\epsilon_O \epsilon_U \epsilon_{O \Delta U} = 1} \cong 2^{12} : \mathrm{M}_{24}$$

If we set $H := 2^{12} : \mathrm{M}_{24}$ then we can try and enumerate the double cosets $Hw\mathrm{M}_{24}$ inside $\cdot 0$ since $|\cdot 0 : H|$ is much smaller than $|\cdot 0 : \mathrm{M}_{24}|$.
John Bray's program can do this revealing that there are 19 double cosets of the form $Hw\mathrm{M}_{24}$ inside $\cdot 0$.
Indeed every element of $\cdot 0$ may written in the form $\pi \epsilon_C w$ where $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$.
Problem: can no longer multiply symmetrically represented elements together.

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin.

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

The subgroup $2^{12} : M_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross**

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

The subgroup $2^{12} : M_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?
The subgroup $2^{12} : \mathrm{M}_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.
Each double coset $Hw\mathrm{M}_{24}$ corresponds to an orbit of crosses under the action of M_{24} thus:

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

The subgroup $2^{12} : \mathrm{M}_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.

Each double coset $Hw\mathrm{M}_{24}$ corresponds to an orbit of crosses under the action of M_{24} thus:

$$\{\pm 8e_i\}$$

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?
The subgroup $2^{12}:\mathrm{M}_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.
Each double coset $Hw\mathrm{M}_{24}$ corresponds to an orbit of crosses under the action of M_{24} thus:

$$\{\pm 8e_i\} \xrightarrow{H} \{\pm 8e_i\}$$

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

The subgroup $2^{12} : \mathrm{M}_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.

Each double coset $Hw\mathrm{M}_{24}$ corresponds to an orbit of crosses under the action of M_{24} thus:

$$\{\pm 8e_i\} \xrightarrow{H} \{\pm 8e_i\} \xrightarrow{w} \Celtcross$$

Some Crosses to Bear

The group $\cdot 0$ is the group of automorphisms of the celebrated **Leech lattice** Λ that fix the origin. Can we use the geometry of this lattice to help us?

The subgroup $2^{12} : \mathrm{M}_{24} \leq \cdot 0$ is the stabilizer of a certain configuration of vectors in Λ called a **cross** - the 'standard cross' being the set of vectors $\{\pm 8e_i\}$, the other crosses being the images of this cross under the action of our symmetric generators.

Each double coset $Hw\mathrm{M}_{24}$ corresponds to an orbit of crosses under the action of M_{24} thus:

$$\{\pm 8e_i\} \xrightarrow{H} \{\pm 8e_i\} \xrightarrow{w} \boldsymbol{\Phi} \xrightarrow{\pi} \boldsymbol{\Phi}'$$

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1 \epsilon_{C_1} w_1$ and $\pi_2 \epsilon_{C_2} w_2$ in the form $\pi_3 \epsilon_{C_3} w_3$ with $l(w) \leq 4$.

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1\epsilon_{C_1}w_1$ and $\pi_2\epsilon_{C_2}w_2$ in the form $\pi_3\epsilon_{C_3}w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1\epsilon_{C_1}w_1$. Call this ⌖.

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1\epsilon_{C_1}w_1$ and $\pi_2\epsilon_{C_2}w_2$ in the form $\pi_3\epsilon_{C_3}w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1\epsilon_{C_1}w_1$. Call this ⌖.
2. Find the image of ⌖under the action of $\pi_2\epsilon_{C_2}w_2$. Call this ⌖′.

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1 \epsilon_{C_1} w_1$ and $\pi_2 \epsilon_{C_2} w_2$ in the form $\pi_3 \epsilon_{C_3} w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1 \epsilon_{C_1} w_1$. Call this Φ.
2. Find the image of Φunder the action of $\pi_2 \epsilon_{C_2} w_2$. Call this Φ'.
3. Find which M_{24} orbit Φ' belongs to (by inspection).

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1 \epsilon_{C_1} w_1$ and $\pi_2 \epsilon_{C_2} w_2$ in the form $\pi_3 \epsilon_{C_3} w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1 \epsilon_{C_1} w_1$. Call this Φ.
2. Find the image of Φunder the action of $\pi_2 \epsilon_{C_2} w_2$. Call this Φ'.
3. Find which M_{24} orbit Φ' belongs to (by inspection).
4. Look-up short word of symmetric generators w_3^{-1} that sends Φ' back to $\{\pm 8e_i\}$.

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1 \epsilon_{C_1} w_1$ and $\pi_2 \epsilon_{C_2} w_2$ in the form $\pi_3 \epsilon_{C_3} w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1 \epsilon_{C_1} w_1$. Call this Φ.
2. Find the image of Φunder the action of $\pi_2 \epsilon_{C_2} w_2$. Call this Φ'.
3. Find which M_{24} orbit Φ' belongs to (by inspection).
4. Look-up short word of symmetric generators w_3^{-1} that sends Φ' back to $\{\pm 8e_i\}$.
5. Find the Golay codeword ϵ_{C_3} by computing the image of $(2^{24}) \in \Lambda$ under the action of $(\pi_1 \epsilon_{C_1} w_1)(\pi_2 \epsilon_{C_2} w_2) w_3^{-1}$

Turning the Crank

We have identified what each of the 19 orbits of crosses under the action of M_{24} and found shortest possible words in the symmetric generators sending the standard cross to each of them. This suggests an algorithm for expressing the product of two elements $\pi_1\epsilon_{C_1}w_1$ and $\pi_2\epsilon_{C_2}w_2$ in the form $\pi_3\epsilon_{C_3}w_3$ with $l(w) \leq 4$.

1. Find the image of the standard cross $\{\pm 8e_i\}$ under the action of $\pi_1\epsilon_{C_1}w_1$. Call this 🕈.
2. Find the image of 🕈under the action of $\pi_2\epsilon_{C_2}w_2$. Call this 🕈′.
3. Find which M_{24} orbit 🕈′ belongs to (by inspection).
4. Look-up short word of symmetric generators w_3^{-1} that sends 🕈′ back to $\{\pm 8e_i\}$.
5. Find the Golay codeword ϵ_{C_3} by computing the image of $(2^{24}) \in \Lambda$ under the action of $(\pi_1\epsilon_{C_1}w_1)(\pi_2\epsilon_{C_2}w_2)w_3^{-1}$
6. Find the M_{24} element π_3 by finding the images of enough vectors of the form $8e_i$ under the action of $(\pi_1\epsilon_{C_1}w_1)(\pi_2\epsilon_{C_2}w_2)w_3^{-1}\epsilon_{c_3}$.

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi\epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$.

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi\epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi\epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

196560

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi \epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$196560 > 24^2 = 576$$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}\mathrm{Co}_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi\epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$196560 > 24^2 = 576 > 24 + 24 + 4 \times 4 = 64$$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0| = 8\ 315\ 553\ 613\ 086\ 720\ 000$

$$\frac{2^{\star\binom{24}{4}} : M_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi \epsilon_C w$ with $\pi \in M_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$196560 > 24^2 = 576 > 24 + 24 + 4 \times 4 = 64 (> 23 + 12 + 3 \times 4 = 47).$$

Example: the Conway group $\cdot 0 \cong 2^{\cdot}Co_1$

$|\cdot 0|$=8 315 553 613 086 720 000

$$\frac{2^{\star\binom{24}{4}} : \mathrm{M}_{24}}{(\pi t)^3} \cong \cdot 0$$

So every element can be symmetrically represented as $\pi\epsilon_C w$ with $\pi \in \mathrm{M}_{24}$, $\epsilon_C \in 2^{12}$ and $l(w) \leq 4$. Compare this with the more 'traditional' representations:

$$196560 > 24^2 = 576 > 24 + 24 + 4 \times 4 = 64(> 23 + 12 + 3 \times 4 = 47).$$

RT Curtis and BT Fairbairn "Symmetric Representation of the Elements of the Conway Group ·0" J. Symbolic Computation **44** *(2009), 1044-1067*

If you liked this...

fairbaib@maths.bham.ac.uk

If you liked this...

fairbaib@maths.bham.ac.uk

Slides are available at:
http://bham.academia.edu/BenFairbairn/Talks

If you liked this...

fairbaib@maths.bham.ac.uk

Slides are available at:
http://bham.academia.edu/BenFairbairn/Talks

PLEASE GIVE ME A JOB!

Thank you for listening