Enumerating Cylotomic Hecke Algebras

Götz Pfeiffer

School of Mathematics, Statistics and Applied Mathematics
NUI, Galway

CoGrAl 2015
Friedrich-Schiller-Universität Jena

Overview

- Cosets of **parabolic subgroups** in **complex reflection groups** are particularly **easy to enumerate**.
- The Todd-Coxeter algorithm for **coset enumeration** in groups is a form of **Breadth First Search**.
- A **linear** Todd-Coxeter algorithm might compute a faithful matrix representation of the **cyclotomic Hecke algebra** H of a **complex reflection group** W.

Conjecture (Broué–Malle–Rouquier, 1998)

H *is a free of rank* $|W|$.

Theorem (Marin–Pf. 2014)

$W = \mathrm{G}_{12}, \mathrm{G}_{22}, \mathrm{G}_{24}, \mathrm{G}_{27}, \mathrm{G}_{29}, \mathrm{G}_{31}, \mathrm{G}_{33}$ *satisfy this conjecture.*

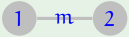
Coxeter Groups.

- A **Coxeter group** is a group W given by a presentation of the form
$$W = \langle S \mid (st)^{m_{st}} = 1;\ s, t \in S\rangle,$$
where $m_{ss} = 1$ and $m_{st} = m_{ts} \in \{2, 3, 4, \dots, \infty\}$ if $s \neq t$.

Examples

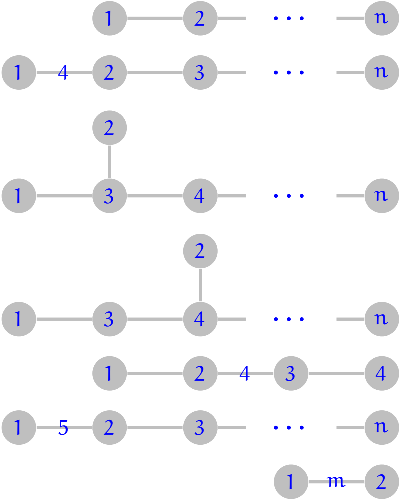
- $S_{n+1} = \langle (i, i+1) : 1 \leq i \leq n\rangle$.

- $D_{2m} = \langle s, t \mid s^2 = t^2 = (st)^m = 1\rangle$.



- W acts as **reflection group** on $\mathbb{R}^n$, where $n = |S|$.
- **Length function:** $\ell(ws) = \ell(w) \pm 1$, $w \in W$, $s \in S$.
- **Matsumoto's Theorem:** any two **reduced expressions** for $w \in W$ differ only by **braid relations** $sts \cdots = tst \cdots$
- W is a direct products of **irreducible** components.

Irreducible Finite Coxeter Groups



A_n $(n \geq 0)$.

B_n $(n \geq 2)$.

D_n $(n \geq 4)$.

E_n $(n \in \{6, 7, 8\})$.

F_4.

H_n $(n \in \{2, 3, 4\})$.

$I_2(m)$ $(m \geq 6)$.

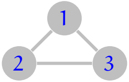
Parabolic Subgroups

- For each subset $J \subseteq S$, the **parabolic subgroup** $W_J = \langle J \rangle$ of W is itself a Coxeter group, with Coxeter generators J.
- The set $X_J = \{x \in W : \ell(wx) > \ell(x) \text{ for all } w \in W_J\}$ is a **transversal** of the right cosets of W_J in W.
- The factorization of $w \in W$ as $w = u \cdot x$ for unique $u \in W_J$ and $x \in X_J$ is **reduced**: $\ell(w) = \ell(u) + \ell(x)$.
- **Deodhar's Lemma:** Let $x \in X_J$ and $s \in S$. Then either $x.s \in X_J$ or $x.s = t \cdot x$ for some $t \in J$.
- The cosets of W_J in W can be enumerated without ever defining redundant cosets ...

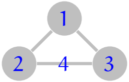
Complex Reflection Groups.

- Let $V = \mathbb{C}^n$.
- A **complex reflection** is an element of $GL_n(V)$ that fixes a hyperplane pointwise.
- A **complex reflection group** is a finite subgroup of $GL_n(V)$ generated by complex reflections.
- **Classification** (Shepard and Todd, 1954)**:** an irreducible complex reflection group is either a **monomial group** $G(m, p, n)$, or one of 34 **exceptions** called $G_4, \dots, G_{37}$ (including the finite Coxeter groups).
- Complex reflection groups are **like Coxeter groups** ...
- There is a notion of braid groups ... Coxeter-like presentations and diagrams ... a deformation of the group algebra ...
- Enumeration of the cosets of parabolic subgroups needs only a few redundant cosets if any ...

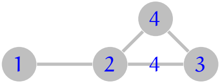
Some Exceptional Complex Reflection Groups



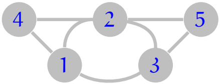
G_{12}: $1231 = 2312 = 3123$;
G_{22}: $12312 = 23123 = 31231$.



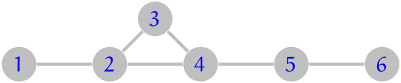
G_{24}: $231231231 = 323123123$;
G_{27}: $323123123123 = 231231231232$.



G_{29}: $432432 = 324324$.



G_{31}: $123 = 231 = 312$.



G_{33}, G_{34}: $423423 = 342342 = 234234$.

Breadth First Search.

Input. A (simple) **graph** $\Gamma = (V, E)$ and a vertex $x_0 \in V$.

Output. All vertices $x \in V$ that can be reached from x_0.

1. **initialize** a **queue** Q and a **list** L
2. **while** $Q \neq \varnothing$: pop a vertex x off Q and **process** x
3. **return** L

- For $x \in V$, set $E(x) = \{y \in V : \{x, y\} \in E\}$.

initialize Q and L

- Set $Q \leftarrow \varnothing$ and $L \leftarrow \varnothing$ and push x_0 onto L and Q.

process x

- **for each** $y \in E(x)$:
  if $y \notin L$: push y onto Q and L

Orbit Algorithm.

Input. A set S of permutations of a set X and a vertex $x_0 \in X$.

Output. The **orbit** of x_0 under the action of the group $G = \langle S \rangle$.

1. **initialize** a **queue** Q and a **list** L
2. **while** $Q \neq \varnothing$: pop a vertex x off Q and **process** x
3. **return** L

initialize Q and L

- Set $Q \leftarrow \varnothing$ and $L \leftarrow \varnothing$ and push x_0 onto L and Q.

process x

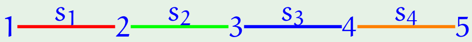
- **for each** $s \in S$:
  set $y \leftarrow x.s$
  if $y \notin L$: push y onto Q and L

Group Actions as Graphs.

- The Orbit Algorithm searches action graph $\Gamma(X, S)$ with given vertex set X, and implicit edges given by S.
- Suppose a finite group $G = \langle S \rangle$ acts on a finite set X.
- The **action graph** $\Gamma(X, S)$ has:
  vertex set X
  and **edges** $x \xrightarrow{s} x.s$, for $x \in X$, $s \in S$, if $x.s \neq x$.

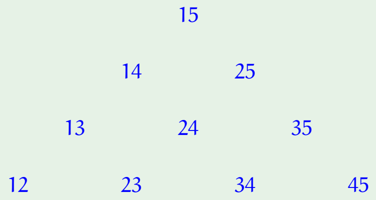
Example: S_5.

$X = \{1, 2, 3, 4, 5\}$;
$s_i = (i, i+1)$;
$S = \{s_1, s_2, s_3, s_4\}$;
$S_5 = \langle S \rangle$.



For example S_5 acting on $\binom{X}{2}$.

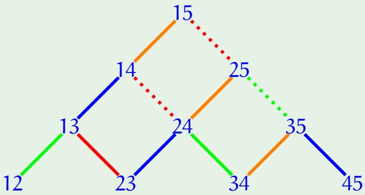
x	$x.s_1$	$x.s_2$	$x.s_3$	$x.s_4$
12				
13				
23				
14				
24				
15				
34				
25				
35				
45				



- The action of G on the orbit of x_0 is equivalent to an action on the cosets of a subgroup of G: the stabilizer of x_0.

For example S_5 acting on $\binom{X}{2}$.

x	$x.s_1$	$x.s_2$	$x.s_3$	$x.s_4$
12	12	<u>13</u>	12	12
13	<u>23</u>	12	<u>14</u>	13
23	13	23	<u>24</u>	23
14	24	14	13	<u>15</u>
24	14	<u>34</u>	23	<u>25</u>
15	25	15	15	14
34	34	24	34	<u>35</u>
25	15	35	25	24
35	35	25	<u>45</u>	34
45	45	45	35	45



$s_1 \mapsto (13, 23)(14, 24)(15, 25)$, $s_2 \mapsto (12, 13)(24, 34)(25, 35)$,
$s_3 \mapsto (13, 14)(23, 24)(35, 45)$, $s_4 \mapsto (14, 15)(24, 25)(34, 35)$.

- The action of G on the orbit of x_0 is equivalent to an action on the cosets of a subgroup of G: the stabilizer of x_0.

Coset Enumeration.

- The group G is given by a **presentation** $G = \langle S \mid R \rangle$ on a set S of abstract **generators**, with a set R of **relations**.
- A subgroup H is given by a set U of generating words in S.
- **Coset enumeration** searches the action graph $\Gamma(G/H, S)$, with both vertices and edges implicit.
- Grow a set X of **smart vertices** as needed, but be prepared to merge redundant vertices later . . .
- Each $x \in X$ has
  - a unique ID x.id, ($x.\text{id} = n \iff x = x_n$)
  - an associated word $x.\text{word} \in S^*$, (spanning tree)
  - images $x.s \in X \cup \{\perp\}$ for each $s \in S$, (coset table)
  - and a reference $x.\text{flat} \in X \cup \{\perp\}$ to the vertex it has possibly been replaced by.
- Eventually $x.s \in X$ for all $x \in X$, $s \in S$.

Coset Enumeration.

- Each $x \in X$ has a basic image $x^\flat$ defined recursively as

$$x^\flat = \begin{cases} x, & \text{if } x.\text{flat} = \bot \\ (x.\text{flat})^\flat & \text{else} \end{cases}$$

- Reserve notation $x.s$ for information stored with x.
- Denote by

$$x{:}w$$

  the image of $x \in X$ under the **partial action** of $w \in W$, which may return $\bot$ if an image is not yet known.
- Denote by

$$x!w$$

  the image of $x \in X$ under the **defining action** of $w \in W$, which if necessary enlarges X.

Coset Enumeration.

- Assume $S = S^{-1}$.
- For each $s \in S$ set

$$R_s = \{u^{-1}v^{-1} : usv = 1 \text{ in } R\} \cup \{vu : us^{-1}v = 1 \text{ in } R\},$$

the set of all words that a generator s can be replaced by due to a relation.

Example: $W = S_4$

- $W = \langle s_1, s_2, s_3 \mid$  $\rangle$

- $R_1 = \{s_2 s_1 s_2 s_1 s_2, \quad s_3 s_1 s_3\}$;
- $R_2 = \{s_1 s_2 s_1 s_2 s_1, \quad s_3 s_2 s_3 s_2 s_3\}$;
- $R_3 = \{s_1 s_3 s_1, \quad s_2 s_3 s_2 s_3 s_2\}$;

Coset Enumeration.

Input: A presentation $G = \langle S, R \rangle$ and a subgroup $H = \langle U \rangle \leq G$.

Output: The (right) cosets of H in G.

1. **initialize** a **queue** Q and a **list** L
2. **while** $Q \neq \varnothing$: pop a vertex x off Q and **process** x
3. **return** L

initialize Q and L

- set $Q \leftarrow \varnothing$ and $L \leftarrow \varnothing$
- set $x_0 \leftarrow$ **new Vertex**$(\varnothing)$
- **for each** $u \in U$: **trace** x_0 through $u = 1$.

- How to **process** x depends on the chosen **strategy**. This can be **relation driven** or **generator driven** or ...

Coset Enumeration

new Vertex(w)

- $x \leftarrow \{\text{id} : \#L, \quad \text{word} : w, \quad \text{flat} : \bot\}$
- **for each** $s \in S$: set $x.s \leftarrow \bot$
- push x onto Q and L

trace x through $ls = r$ (where $l, r \in S^*$, $s \in S$)

- **update edge** $x!l \xrightarrow{s} x!r$ (defining action)

update edge $x \xrightarrow{s} y$

- **try and set** $x.s$ to y
- **try and set** $y.s^{-1}$ to x (if s has an inverse)

Coset Enumeration

- Setting an already known image may cause a collision.

try and set $x.s$ to y

- **if** $x.s = \bot$:
  set $x.s \leftarrow y$
  else:
  if $(x.s)^\flat \neq y^\flat$: **merge** $(x.s)^\flat$ and $y^\flat$.

- A redundant vertex passes its images on and maintains a reference to the vertex it is replaced by.

merge x and y (assuming $x < y$)

- set y.flat $\leftarrow x$
- **for each** $s \in S$:
  if $y.s \neq \bot$: **update edge** $x \xrightarrow{s} y.s$

Coset Enumeration

$x{:}w$ (partial action)

1. set $y \leftarrow x$
2. **for each** letter s in w:
   set $y \leftarrow y.s$ (stored image)
   if $y = \perp$: **return** $\perp$
3. **return** y

$x!w$ (defining action)

1. set $y \leftarrow x$
2. **for each** letter s in w:
   set $y \leftarrow y!s$ (defining action)
3. **return** y

Coset Enumeration

$x!s$ (defining action)

- **return** $x.s \neq \perp$? $(x.s)^\flat$: x **sprout** s

- If an image is not known, a new vertex together with a joining edge are created. The vertex will automatically join the queue Q and the list L.

x sprout s

- set $y \leftarrow$ **new Vertex**$(x.\text{word}$ append $s)$
- **update edge** $x \xrightarrow{s} y$
- **return** y

Coset Enumeration

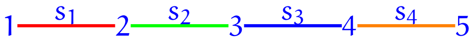
process x (relation driven)

- **for each** relation $l = r$ in R:
  if $x = x^\flat$: **trace** x through $l = r$.
- **for each** $s \in S$:
  if $x = x^\flat$: **trace** x through $s = s$.

process x (generator driven)

- **for each** $s \in S$:
  for each $w \in R_s$:
    if $x = x^\flat$:
      set $y \leftarrow x{:}w$ (partial action)
      if $y \neq \bot$: **update edge** $x \xrightarrow{s} y$
  if $x = x^\flat$: **trace** x through $s = s$.

Group Algebras.



x	$x.s_1$	$x.s_2$	$x.s_3$	$x.s_4$
$x_0 = \varnothing$	$s_1 \cdot x$	$s_2 \cdot x$	$s_3 \cdot x$	$\underline{x_1}$
$x_1 = s_4$	$s_1 \cdot x$	$s_2 \cdot x$	$\underline{x_2}$	x_0
$x_2 = s_4 s_3$	$s_1 \cdot x$	$\underline{x_3}$	x_1	$s_3 \cdot x$
$x_3 = s_4 s_3 s_2$	$\underline{x_4}$	x_2	$s_2 \cdot x$	$s_3 \cdot x$
$x_4 = s_4 s_3 s_2 s_1$	x_3	$s_1 \cdot x$	$s_2 \cdot x$	$s_3 \cdot x$

- Represents the group algebra $\mathbb{C}W$ as matrices over $\mathbb{C}H$:

$$s_1 \mapsto \begin{bmatrix} s_1 & 0 & 0 & 0 & 0 \\ 0 & s_1 & 0 & 0 & 0 \\ 0 & 0 & s_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \in (\mathbb{C}H)^{5\times 5}$$

$$s_2 \mapsto \cdots$$

Spinning: The $\mathbb{K}$-Linear Orbit Algorithm

Input. A set S of $n \times n$ **matrices** over K and a vector $x_0 \in K^n$.

Output. A K-basis for the A-**submodule** generated by x_0 under the action of the K-**algebra** $A = \langle S \rangle$.

1. **initialize** a **queue** Q and a **list** L
2. **while** $Q \neq \varnothing$: pop a vertex x off Q and **process** x
3. **return** L

initialize Q and L

- set $Q \leftarrow \varnothing$ and $L \leftarrow \varnothing$ and push x_0 onto L and Q.

process x

- **for each** $s \in S$:
  set $y \leftarrow x.s$
  if $y \notin \langle L \rangle_K$: push y onto Q and L

Vector Enumeration: $\mathbb{K}$-linear coset enumeration

Input. An $\mathbb{K}$-algebra presentation $H = \langle S \mid R \rangle$ and generators for an H-module V.

Output. An $\mathbb{K}$-basis for V in case $\dim_{\mathbb{K}} V$ is finite, and a matrix representation of H on V.

- The **relators** R are $\mathbb{K}$-combinations of words in S, corresponding to **relations** $\sum_w \alpha_w w = 0$.
- The **inverses** of the generators, if they exist, are $\mathbb{K}$-combinations of words in S.
- The basis 'points' constructed by the algorithm are still (just) words in S.
- Be prepared to identify a point with a $\mathbb{K}$-combination of other points.
- Apart from that: define new cosets, conclude images, and resolve coincidences, as before.

Iwahori–Hecke algebras

- Let $W = \langle S \rangle$ be a finite Coxeter group.
- Let $\mathcal{A} = \mathbb{Z}[q, q^{-1}]$, the ring of **Laurent polynomials** over $\mathbb{Z}$.
- The **Iwahori–Hecke algebra** H of W is the $\mathcal{A}$-algebra with generators $\{T_s \mid s \in S\}$ and relations

$$T_s^2 = qT_1 + (q-1)T_s,$$
$$T_sT_tT_s \cdots = T_tT_sT_t \cdots$$

  $s, t \in S$.
- By Matsumoto's Theorem, setting $T_w = T_{s_1}T_{s_2} \cdots T_{s_k}$ whenever $w = s_1s_2 \dots s_k$ and $\ell(w) = k$ is independent of the choice of reduced expression for w.
- H has a basis $\{T_w : w \in W\}$.
- $\mathbb{C} \otimes \mathrm{H}$ is a **deformation** of the group algebra $\mathbb{C}W$.
- Such algebras occur as endomorphism rings of certain modules for finite groups of Lie type (over $\mathbb{F}_q$).

Parabolic Subalgebras.

- Let $J \subseteq S$. The Iwahori–Hecke algebra H_J of the parabolic subgroup $W_J = \langle J \rangle$ is a subalgebra of H.
- H is a free (left) H_J module with basis $\{T_x \mid x \in X_J\}$:

$$H = \bigoplus_{x \in X_J} H_J \cdot T_x,$$

and the action of $s \in S$ is given by

$$T_x.T_s = \begin{cases} T_t \cdot T_x & \text{if } xs = tx \text{ for some } t \in J, \\ T_{xs} & \text{if } xs \in X_J \text{ and } \ell(xs) > \ell(x), \\ qT_{xs} + (q-1)T_x & \text{if } xs \in X_J \text{ and } \ell(xs) < \ell(x) \end{cases}$$

- This yields a representation of H by matrices over $K = H_J$.

$H = H(S_5)$ as H_J-module for $J = \{s_1, s_2, s_3\}$.

x	$x.T_1$	$x.T_2$	$x.T_3$	$x.T_4$
x_0	$T_1 \cdot x$	$T_2 \cdot x$	$T_3 \cdot x$	$\underline{x_1}$
x_1	$T_1 \cdot x$	$T_2 \cdot x$	$\underline{x_2}$	$qx_0 + \overline{(q-1)x}$
x_2	$T_1 \cdot x$	$\underline{x_3}$	$qx_1 + \overline{(q-1)x}$	$T_3 \cdot x$
x_3	$\underline{x_4}$	$qx_2 + \overline{(q-1)x}$	$T_2 \cdot x$	$T_3 \cdot x$
x_4	$qx_3 + \overline{(q-1)x}$	$T_1 \cdot x$	$T_2 \cdot x$	$T_3 \cdot x$

- Faithfully represents the algebra H by matrices over H_J:

$$T_1 \mapsto \begin{bmatrix} T_1 & 0 & 0 & 0 & 0 \\ 0 & T_1 & 0 & 0 & 0 \\ 0 & 0 & T_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & q & q-1 \end{bmatrix} \in H_J^{5\times 5}$$

$$T_2 \mapsto \cdots$$

Cyclotomic Hecke algebras

- The **cyclotomic Hecke algebra** H of a complex reflection group W generated by **conjugate involutions** $s \in S$ is the quotient of group algebra $\mathcal{A}\mathrm{B}$ of the braid group B of W with generators $\{\mathbf{s} : s \in S\}$ by the relations

$$\mathbf{s}^2 = \mathrm{q} + (\mathrm{q}-1)\mathbf{s}.$$

- Each of the complex reflection groups W under consideration has a maximal rank parabolic subgroup W_{J} which is a Coxeter group.
- Generator Driven Vector Enumeration applies, as algebra generators are invertible, relations are of the form $\mathrm{r} = 1$.

Results.

- Generator Driven Vector Enumeration constructs H as an H_J-module in the following cases:

W	$\|W\|$	W_J	$\|W/W_J\|$	time
G_{12}	48	A_1	24	0.5s
G_{22}	240	A_1	120	4.4s
G_{24}	336	B_2	42	0.6s
G_{27}	2160	B_2	270	17s
G_{29}	7680	B_3	160	15s
G_{31}	46080	A_3	1920	117m33s
G_{33}	51840	A_4	432	30s
G_{33}	51840	D_4	270	2m24s
G_{34}	39191040	A_5	54432	???
G_{34}	39191040	D_5	20412	???

- Together with known results, this proves the BMR freeness conjecture for all irreducible complex 2-reflection groups W, with the exception of $W = G_{34}$.

References.

- David Bessis and Jean Michel, **Explicit presentations for exceptional braid groups**, Experiment. Math. **13** (2004), no. 3, 257–266. MR 2103323 (2006b:20051)
- Mike Bostock, **D3 - Data-Driven Documents**, `www.d3js.org`.
- S. A. Linton, **On vector enumeration**, Linear Algebra Appl. **192** (1993), 235–248, Computational linear algebra in algebraic and related problems (Essen, 1992). MR 1236745 (94k:20022)
- I. Marin and G. Pfeiffer, **The BMR freeness conjecture for the 2-reflection groups**, arxiv:1411.4760.
- Götz Pfeiffer, **Coset Graphs of Complex Reflection Groups**, `schmidt.nuigalway.ie/goetz/cosets`.