Rewriting systems are useful for finite groups

Jack Schmidt

University of Kentucky

2008-12-02

Outline

- Motivating problem (Ch. 0)
- Examining available data types (Ch. 1)
- Application to the motivating problem (Ch. 2)
- Short rewriting systems for finite groups (Ch. 3)
- Future work

Ch. 0 Overview

- There was an interesting problem, "classify all finite groups"
- Gather finite groups into trees
- Find the children from a parent
- Find the leaves, including "infinite leaves"

From infinite to finite

- One infinite (**profinite**) group describes infinitely many finite groups
- Some have only very nice finite quotients
- We give three examples:
- A familiar 2-group, the *p*-group version, and a perfect group
- The last we want to understand, the first two we do

Old example

- The 2-adic dihedral group is the limit of the dihedral 2-groups:

$$G_\infty = \left\{ \begin{bmatrix} \zeta_2^i & v \\ 0 & 1 \end{bmatrix} : 0 \le i < 2, v \in \hat{\mathbb{Z}}_2 \right\} \le \mathrm{GL}(2, \hat{\mathbb{Z}}_2)$$

where $\zeta_2 = -1$

- This group has very few normal subgroups of finite index:
- 3 of index two (we ignore), and all others are the terms of its lower central series
- The quotients are precisely the dihedral groups of order 2^n, so all but the first lower central factor are simple G_∞ modules

Fancier example

- The p-adic "p"-hedral group is the limit of similar p-groups:

$$G_\infty = \left\{ \begin{bmatrix} \zeta_p^i & v \\ 0 & 1 \end{bmatrix} : 0 \leq i < p, v \in \hat{\mathbb{Z}}_p^{p-1} \right\} \leq \mathrm{GL}(p, \hat{\mathbb{Z}}_p)$$

where $\zeta_p \in \mathrm{GL}(p-1, \hat{\mathbb{Z}}_p)$ has minimal polynomial $\frac{x^p - 1}{x - 1}$

- This group has few normal subgroups of finite index:
- $p + 1$ of index p (we ignore), and all others are the terms of its lower cental series
- The quotients are groups of order p^n and nilpotency class $n - 1$ so all but the first lower central factor are simple G_∞ modules

Super example 6000

- The p-adic analytic Lie group is a limit of nice perfect groups:

$$G_\infty = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \hat{\mathbb{Z}}_p, ad - bc = 1 \right\} \leq \mathrm{GL}(2, \hat{\mathbb{Z}}_p)$$

where p is a "good" prime for the algebraic group SL_2 ($p \geq 5$)

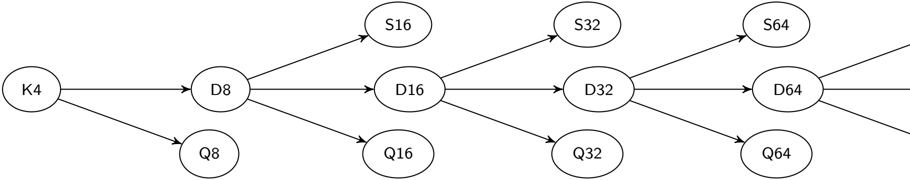
- This group has few normal subgroups of finite index:
- All are the terms of its p-core's lower central series
- The quotients are groups whose p-core's lower central factors are all simple G_∞-modules

From finite to infinite

- We can arrange groups into trees,
  $G/\gamma_n(O_p(G))$ is connected to $G/\gamma_{n+1}(O_p(G))$
  when the kernel is a simple G-module
- Here $\gamma_{n+1}(G) = [G, \gamma_n(G)]$ defines the lower central series
- Trees are easily understood for dihedral, 3-hedral
- 21st century work on 5-hedral, and more p-groups, but "OK"
- For the tree containing $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$
  there is exactly one infinite branch

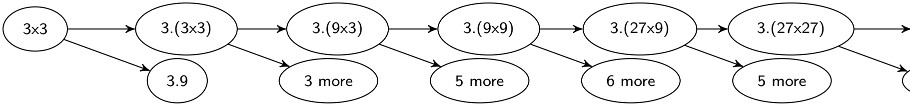
Old example

- G_∞ is 2-adic dihedral group (Folklore)
- Tree contains precisely those groups of order 2^n and nilpotency class $n-1$
- Not just dihedral, also quaternion and semi-dihedral
- Quotient of a quaternion or semi-dihedral by last term of lower central series is always dihedral
- Simple, regular picture (2 steps of burn-in, period 1):



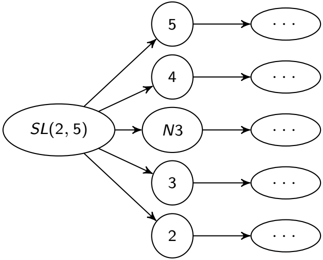
Fancier example

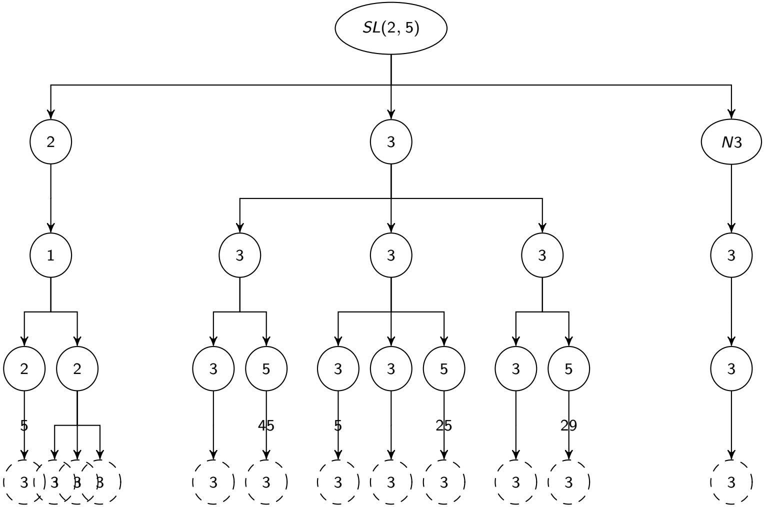
- G_∞ is 3-adic 3-hedral group (N. Blackburn, 1950s)
- Tree contains precisely those groups of order 3^n and nilpotency class $n-1$
- Not just 3-hedral, also five or six more
- Quotient of such by last term of lower central series is always a 3-hedral
- Bigger, still regular picture (3 steps of burn-in, period 2):



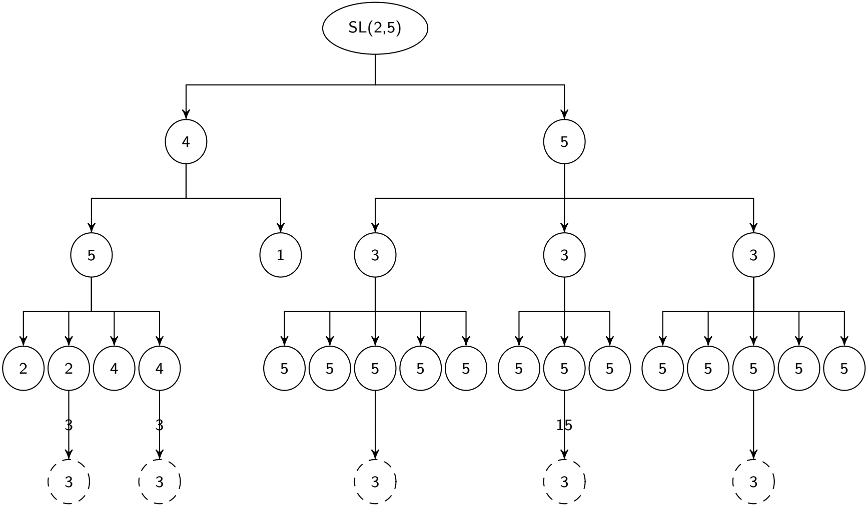
Super example 6000

- $G_\infty = SL(2, \hat{\mathbb{Z}}_5)$ (Still not understood)
- Tree contains precisely those groups G with $G/O_5(G) \cong SL(2,5)$ and with each lower central factor of the 5-core a simple SL(2,5)-module
- Unclear how many are missing
- Partial tree shows only slight regularity (JS 2006):





SL(2, 5)
2
3
N3
1
3
3
3
3
2
2
3
5
3
3
5
3
5
3
5
45
5
25
29
3
3
3
3
3
3
3
3
3
3
3
3
3


SL(2,5)
4
5
5
1
3
3
3
2
2
4
4
5
5
5
5
5
5
5
5
5
5
5
5
5
3
3
15
3
3
3
3
3

The general case

- For any p-group, at most finitely many infinite branches, each one defines a very nice p-adic matrix group
- For $SL(p, \mathbb{Z}/p\mathbb{Z})$, at least one infinite branch for $SL(p, \hat{\mathbb{Z}}_p)$ Could be more? May not be matrix groups?
- Infinite groups corresponding to p-groups are well understood
- Infinite groups corresponding to finite groups are not
- Other than the obvious nice examples, very few infinite branches known, all sporadic and small dimensional

Needed more examples

- In order to understand the infinite branches, might help to just draw longer branches
- Before my work, trees for not-p-groups were very partial (see handout)
- Figures on previous slides done with rewriting systems
- Can easily be continued
- However, hard to figure out which branches are "interesting"
- Why did so many software packages fail?
  Bad choice of data type!

Ch. 1 Choice of data type important

- Need to be able to compute with elements
- Need to be able to specify group extensions in the tree
- Permutation and matrix groups cannot handle the tree
- Finitely presented groups cannot compute with elements
- Rewriting systems can do it all!

Available datatypes cannot handle the tree

- Permutation and matrix groups are concrete
- However for $G_\infty = \hat{\mathbb{Z}}_p$, the quotient at depth n requires at least p^n space
- If G_∞ can be represented as a matrix group over $\hat{\mathbb{Z}}_p$, then depth n quotient has an element of order p^n
- If not matrix group, then current mathematics is so weak in this area that the infinite groups are useless

Reminder from intro

- Permutation groups do not work:
- A permutation group with an element of order p^n moves at least p^n points
- Proof by looking at cycle decomposition
- Matrix groups in characteristic p do not work:
- Such a group with an element of order p^n has dimension at least $p^{n-1} + 1$
- Proof by looking at minimal polynomial

Matrix groups in cross characteristic

- For a field of size q, where p does not divide q
- An element of order p^n has an irreducible minimal polynomial
- Degree d of polynomial is such that p^n divides $q^d - 1$
- Indeed d is the order of q mod p^n
- As n increases linearly, d increases exponentially

MG in CC: number theory

- If $v_p(\alpha - 1) = i \geq \gcd(p, 2)$, then the order of α modulo p^n is p^{n-i} for all $n \geq i$.
- Take $\alpha = q^k$ where k is the order of q modulo $p^{\gcd(p,2)}$.
- For p odd:
    - If $\alpha = 1 + p^i\beta$, then
    - $\alpha^p = (1 + p^i\beta)^p = 1 + p^{i+1}\beta + p^{2i+1}\frac{p-1}{2}\beta^2 + \cdots = 1 + p^{i+1}(\beta + p \cdot \gamma)$
    - $\alpha^{p^n} = (1 + p^i\beta)^{p^n} = 1 + p^{n+i}\beta + p^{2i+n}\frac{p^n-1}{2}\beta^2 + \cdots = 1 + p^{n+i}(\beta + p \cdot \gamma)$

Matrix groups in characteristic zero

- If $q > 2$, then any finite matrix group in characteristic zero is a matrix group in characteristic q
- Fancy proof given in references
- Simple proof of weaker result (abstract algebra exercise)
  Only prove for most q, field is the rationals
- Only finitely many numbers as matrix entries
- Only finitely many primes used in denominators
- Choose some other prime $q > 2$

MG in C0: binomial theorem

- If q doesn't divide b, then $\frac{a}{b}$ mod q makes sense
- Reduce the finite group mod q, what is the kernel?
- Nontrivial element is $I + q^n \cdot A$ where A is nonzero mod q
- Element has finite order, but look at its $k \cdot q^i$th power:

$$(I + q^n \cdot A)^{k \cdot q^i} = I + q^{n+i}(kA) + q^{2n+i}(\dots)$$

- This is not the identity mod q^{n+i+1} where q does not divide k
- Contradiction, so no nontrivial element in kernel

Rewriting systems for extensions

- Rewriting system with n generators, r rules, maximum normal form of length ℓ takes $O(r \cdot \ell \cdot \log(n))$ space.
- To get G by combining G/N with N, R_3 from R_1 and R_2:

$$\begin{aligned} n_3 &= n_1 + n_2 \\ r_3 &= r_1 + r_2 + n_1 \cdot n_2 \\ \ell_3 &= \ell_1 + \ell_2 \end{aligned}$$

- Compare this to group order (for Ch. 3)

$$|G| = |G/N| \cdot |N|$$

On the tree

- The root of the tree has some finite n_1, r_1, ℓ_1
- The N that can occur are only finitely many, so max values of $n_2 = M$, $r_2 \leq M^2$, $\ell_2 = Mp$
- So at depth k, one gets

$$\begin{aligned} n(k) &\leq n_1 + kM \\ r(k) &\leq r_1 + kM^2 + k^2 n_1 M \\ \ell(k) &\leq \ell_1 + kMp \end{aligned}$$

- All grow polynomially in k

Example

- Given the rewriting systems and actions:

$$G/N = \langle a, b : a^3 \mapsto 1, b^3 \mapsto 1, ba \mapsto ab\rangle$$
$$N = \langle c : c^3 \mapsto 1\rangle$$
$$c^a = c, c^b = c$$

- We can form several rewriting systems for possible "G":

$$\langle a, b, c : a^3 \mapsto 1, b^3 \mapsto 1, ba \mapsto ab, c^3 \mapsto 1, ca \mapsto ac, cb \mapsto bc\rangle$$
$$\langle a, b, c : a^3 \mapsto \mathbf{c}, b^3 \mapsto 1, ba \mapsto ab, c^3 \mapsto 1, ca \mapsto ac, cb \mapsto bc\rangle$$
$$\langle a, b, c : a^3 \mapsto 1, b^3 \mapsto 1, ba \mapsto ab\mathbf{c}, c^3 \mapsto 1, ca \mapsto ac, cb \mapsto bc\rangle$$
$$\langle a, b, c : a^3 \mapsto \mathbf{c}, b^3 \mapsto 1, ba \mapsto ab\mathbf{c}, c^3 \mapsto 1, ca \mapsto ac, cb \mapsto bc\rangle$$

Ch. 2 Rewriting systems work

- Important that the data-type is actually practical for tree problem
- Algorithm is natural, and published already in diverse contexts
- No theoretical result due to two troublesome steps
- Each is practical and well-studied, but only loose bounds proven

Always linear algebra

- Finding the children in any representation is mostly linear algebra, called "cohomology"
- Even doing the multiplciation table way (Schreier factor sets) is linear algebra in huge dimensions with very sparse matrices
- The rewriting way radically decreases dimension, but the matrices are now black box (need to multiply in p-group to get their action)
- Trouble in bounding the black box

Removing duplicates

- No matter what method is used to get the cohomology, then need to do orbit calculation to remove duplicates
- Cost is exponential in dimension of cohomology
- The dimension is mathematical property of the group
- No way to “optimize” it
- However, it is usually small (only once ≥ 6 in millions of examples tried)
- Best theoretical bound is polynomial growth of dimension

Example

- Here is a calculation of $H^2(G,V)$ for $G = 3 \times 3$ and $V = 3^1$:

$$
\begin{array}{rcl}
G &=& \langle a, b : a^3 \mapsto 1,\ b^3 \mapsto 1,\ ba \mapsto ab \rangle \\
C^2(G,V) &=& \langle z_1, z_2, z_3 \rangle \\
&\approx& \langle a, b, z_i : a^3 \mapsto z_1,\ b^3 \mapsto z_2,\ ba \mapsto abz_3 \\
&& \qquad z_i^3 \mapsto 1,\ z_i a \mapsto a z_i,\ z_i b \mapsto b z_i \\
&& \qquad z_2 z_1 \mapsto z_1 z_2,\ z_3 z_2 \mapsto z_2 z_3,\ z_3 z_1 \mapsto z_1 z_3 \rangle \\
B^2(G,V) &=& 0 \\
Z^2(G,V) &=& C^2(G,V)
\end{array}
$$

- Note the rewriting system method was optimal, nothing wasted below or above
- There are 4 orbits. Reps are (0,0,0), (1,0,0), (0,0,1), (1,0,1)

Grandchildren

- Now take G to be the child with $\zeta = (0, 0, 1)$,

$$\begin{aligned}
G &= \langle a, b, c : a^3 \mapsto 1,\ b^3 \mapsto 1,\ ba \mapsto abc, \\
&\qquad\qquad c^3 \mapsto 1,\ ca \mapsto ac,\ cb \mapsto bc \rangle \\
C^2(G, V) &= \langle z_1, z_2, z_3, z_4, z_5, z_6 \rangle \\
&\approx \langle a, b, c, z_i : a^3 \mapsto z_1,\ b^3 \mapsto z_2,\ ba \mapsto abcz_3, \\
&\qquad\qquad c^3 \mapsto z_4,\ ca \mapsto acz_5,\ cb \mapsto bcz_6, \\
&\qquad\qquad z_i^3 \mapsto 1,\ z_i a \mapsto az_i,\ z_i b \mapsto bz_i, \\
&\qquad\qquad z_i c \mapsto cz_i,\ z_j z_i \mapsto z_i z_{j (1 \leq i < j \leq 6)} \rangle \\
B^2(G, V) &= \langle z_3 \rangle \\
Z^2(G, V) &= \langle z_1, z_2, z_3, z_5, z_6 \rangle
\end{aligned}$$

- Now there is one dimension “wasted” above and below

GC: Detail for ∂^1

- $C^1(G, V) = V^3$ and one calculates columnwise to get:

$$\partial^1 : C^1 \to C^2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

  Here each row corresponds to a generator, and each column to a rule

- For instance the column corresponding to the rule $ba \mapsto abc$ is calculated by considering the rule for the generators (av_1, bv_2, cv_3) giving left hand side $bv_2av_1 = ba \cdot v_1v_2$ and right hand side $av_1bv_2cv_3 = abc \cdot v_1v_2v_3$, for a difference of $(1, 1, 1) - (1, 1, 0) = (0, 0, 1) = v_3$.

GC: Detail for ∂^2

- The map $\partial^2 : C^2 \to C^3$ is a bit larger, calculated columnwise.
- The column for $(ba, a^3, 1)$ corresponds to reducing $b \cdot a \cdot a^2$:

$$
\begin{aligned}
b(aaa) &\mapsto b\overline{z_1} \\
(ba)aa &\mapsto \overline{abc(z_3}aa) \mapsto ab(c\overline{a)a \cdot z_3} \\
&\mapsto ab\overline{ac(z_5}az_3) \mapsto aba(c\overline{a) \cdot z_3 z_5} \mapsto a(ba)\overline{ac} \cdot z_3 z_5^2 \\
&\mapsto a\overline{ab(c}a)c \cdot z_3^2 z_5^2 \mapsto aa(b\overline{a)c}c \cdot z_3^2 z_5^0 \\
&\mapsto (a\overline{aa)bc}cc \cdot z_3^0 z_5^0 \mapsto b(ccc) \cdot z_1 \mapsto b \cdot z_1 z_4
\end{aligned}
$$

so the column is
$(1, 0, 0, 1, 0, 0) - (1, 0, 0, 0, 0, 0) = (0, 0, 0, 1, 0, 0) = z_4$.

Complexity

- Notice the evaluation of ∂^1 was just linear algebra
- Cost was just the length of the left hand side plus the length of the right hand side mat-vecs and vector adds
- So $O(\ell \cdot n_2)$, where $n_2 \leq M$ and $\ell \leq \ell_1 + kMp$
- Each "$\mapsto$" step in the evaluation of ∂^2 was just linear algebra
- Cost of each was at most the length of the word mat-vecs and vector adds
- How many $\mapsto$ are required? How long can the "abc" word be?
- Best bound is subexponential (B.Höfling, unpublished, 2002) $O(\exp(C \cdot \log(n)^2))$
- In practice, often linear in k, the tree depth

Ch. 3 General results

- Rewriting system size scales with logarithm of group order if one stays on a tree
- What can we do in general? What about the root of the tree?
- Can always handle group by composition factors
- Can **uniformly** handle simple groups of Lie type
- Combining, all finite groups have rewriting system of size $O(\sqrt{|G|})$

Composition series

- **Notice:** $g_3 = g_1 + g_2$ generators and $r_3 = r_1 + r_2 + g_1 \cdot g_2$ rules
- Independent of the cohomology and the action
- Suffices to consider $G/N \times N$, the **direct product**
- Can break down entire composition series
- Suffices to consider **direct products of simple groups**

Reduction to simple groups

- The following groups have short rewriting systems:
  - All simple groups, except possibly some sporadics
  - $G \times H$, where G, H short and $|G|, |H| \geq 2^4$
  - G^k, where G nonabelian simple and $k \geq 4$
  - G, where G polycyclic, $|G| \geq 2^{14}$
  - $G \times H$, where G short, H polycyclic, $|G| \geq 2^4$
  - $G \times H$, where G short, $|G| \geq |H|^2$
  - G, where $|G| \geq \max(k^9, 2^{14}k^3)$, k the product of the orders of the simple exceptions

How to handle simple groups

- Groups with (B, N) pairs have a natural rewriting system
- If the (B, N) pair is split characteristic p satisfying the (weak) commutator relations, then the rewriting system is short
- Relies on having short Coxeter rewriting systems
- Alternating groups are nearly Coxeter groups
- Small sporadic groups have good enough “fake” split BN pairs, up to order 10^6 so far

How to handle groups of Lie type

- Groups of Lie type have a **Bruhat decomposition**:
  Each $g \in G$ has **unique** $(x, h, w, x') \in U \times T \times W \times U_w$:

$$g = x \cdot h \cdot \dot{w} \cdot x'$$

- Roughly $U = P$, $N_G(P) = T \ltimes P$, $N = N_G(T)$, $W = N/T$, $U_w = P \cap P^{\dot{w}}$

- In GL and PSL, U is the upper uni-triangular matrices, T is the diagonal, N are the monomial, W are the permutation matrices, and Bruhat is LU decomposition

- U, T are polycyclic, W is a finite Coxeter group,
  so we have **normal forms** for the parts of g

Bruhat decomposition as rewriting system

- The Bruhat decomposition is **natural** and easily **computable**
- Normal forms are not closed under contiguous subwords, so this is not **not a rewriting system**
- Easy to fix: use **simple roots** instead of positive roots
- Instead of $B\dot{w}_1\dot{w}_2U_{w_1w_2}$ use $B\dot{w}_1X_1\dot{w}_2X_2$, equal as sets.
- Is a rewriting system, as if G had normal subgroup B and quotient group W

The Bruhat rules

- The polycyclic rules of B using independent toral generators and positive root generators, **polynomial in the rank**
- The rules from the Weyl group, **polynomial in the rank**
- The rules $w_i x_i(v) x_j(1)$ for each simple root i, each "field element" v, and each simple root $j < i$
- Number of rules is now a polynomial in the rank and the **size of the field**
- Easily bounded by $|W||P| \leq \sqrt{|G|}$, but really $O(q^n) \ll O(\sqrt{|G|})$, q field size, n number of positive roots

Coxeter groups

- Number of rules is quadratic in rank, order is factorial
- Rules are simple, basically extended "exchange laws"
- For alternating groups:
  - Use generating system $(n-2, n, n-1), (1, 2)(n-1, n), \ldots, (n-3, n-2)(n-1)$
  - Consider the last $n-3$ generators as normal subgroup (Coxeter group Sym$(n-2)$)
  - Number of rules is quadratic in n, order is factorial
  - Rules divide into about 10 families

A few low rank families

Family	*Gens*	*Rules*	*Order*
A_1	$k+2$	$q+(\frac{1}{2}k^2+\frac{3}{2}k+2)$	q^3-q
A_2	$3k+4$	$q^2+(k+2)q$ $+(\frac{9}{2}k^2+\frac{21}{2}k+7)$	$q^8-q^6-q^5+q^3$
${}^2A_2$	$3k+3$	$q^3+(\frac{9}{2}k^2+\frac{15}{2}k+5)$	$q^8-q^6+q^5-q^3$
G_2	$6k+4$	$q^5+(9k+6)q$ $+(18k^2+16k+7)$	$q^{14}-O(q^{12})$
A_3	$6k+6$	$q^3+2q^2+(3k+4)q$ $+(18k^2+33k+15)$	$q^{15}-O(q^{13})$

Small simple groups

G	$\lvert G\rvert$	n	r	ϕ
$A(1,4)$	60	4	11	0.585
$= A(1,5)$		3	9	0.537
$= Alt(5)$		3	11	0.585
$= brute$		2	6	0.438
$A(1,7)$	168	3	11	0.468
$= A(2,2)$		5	19	0.575
$= brute$		2	11	0.468
$A(1,9)$	360	3	15	0.461
$= Alt(6)$		4	24	0.540
$= brute$		3	14	0.449
$A(1,8)$	504	5	19	0.474
$= brute$		3	17	0.456
$A(1,11)$	660	3	15	0.418
$= brute$		3	19	0.454
$A(1,13)$	1092	2	17	0.405
$= brute$		2	25	0.461
$A(1,17)$	2448	2	21	0.391
$= brute$		2	49	0.499
Alt(7)	2520	5	40	0.471
$= brute$		3	36	0.458

G	$\lvert G\rvert$	n	r	ϕ
$A(1,19)$	3420	3	23	0.386
$A(1,16)$	4080	6	32	0.417
$A(2,3)$	5616	7	40	0.428
$^2A(2,3)$	6048	6	44	0.435
$= brute$		3	49	0.447
$A(1,23)$	6072	3	27	0.379
$A(1,25)$	7800	4	32	0.387
M_{11}	7920	3	62	0.460
$A(1,27)$	9828	5	38	0.396
Alt(8)	20160	6	61	0.414
$= A_3(2)$		9	63	0.418
$A_2(4)$	20160	10	42	0.377
...				
M_{12}	95040	5	303	0.498
J_1	175560	5	192	0.436
Alt(9)	181440	7	86	0.367
M_{22}	443520	4	150	0.386
J_2	604800	6	219	0.405
Alt(10)	1814400	8	116	0.329

Future work: three main directions

- Find **all** terminating, confluent rewriting systems for a group
- Use algebraic variety ideas to compress rewriting systems of groups of Lie type
- Use theory to complete a few of the trees

FW: All rws

- Simple group of order 60 is alternating, sporadic (B,N), and several kinds of Lie group, but best rewriting system was found through brute force.
- Can we find **all** terminating, confluent rewriting systems for it?
- New technique uses directed spanning trees to find all confluent rewriting systems ($\approx 30,000$ on two generators)
- Current work: which ones are terminating?
- Hard problem in CS for **infinite** languages

FW: Algebraic rws

- Bruhat rewriting systems scale with field size
- Program to generate them has size polynomial in Lie rank
- Uses rational functions (algebraic variety morphisms) to specify rules
- Current work: can one do a confluence check directly from the morphism
- Can one execute chapter 2 in this context?
- Does the field of the group need to match/not-match the field of the module? The field of other composition factors in the group?

FW: Complete the trees

- Many trees partially calculated (all perfect p-roots of order up to 1000, all to depth at least 3, some to depth 8)
- A few trees seem well-behaved, but none were finite
- Need to apply more modern modular representation theory
- Actually only in last two years have small p-group p-roots been done, though problem was officially solved in the 1980s
- Techniques there may apply here, but with difficulty (periodic patterns in p-group trees due to infinite group being soluble, usually insoluble in my work)

THE END