Finite groups have short rewriting systems

Jack Schmidt

University of Kentucky

AMS Kalamazoo 2008-10-18

Rewriting systems are useful for finite groups if they have few rules. We show that all but finitely many finite groups have rewriting systems where the number of rules squared is less than the group order.

Outline

- What are rewriting systems and why do we want **short ones**?
- Rewriting systems refining a **composition series** are short
- Non-sporadic **simple group** rewriting systems are short
- **All but finitely many** finite groups are short

What are rewriting systems?

- Like a finitely presented group, but **without uncertainty**.
- Finitely presented group: $\langle a, b : a^2 = b^2 = (ab)^2 \rangle$
- Does $a^3 b^3 = ab$? Should you replace a^2 with b^2 or vice versa?
- Rewriting system: $\langle a, b : a^2 \mapsto b^2, b^4 \mapsto 1, ba \mapsto ab^3 \rangle$
- Easier to use because the relations have a **direction** and always **simplify**.
- Easy to put every element in form $a^i b^j$ with $0 \leq i < 2$ and $0 \leq j < 4$.

Why do we want to use them?

- **Polycyclic presentations** are a very successful special case, but are limited to soluble groups.

- **Finite presentations** are natural and flexible, but are difficult to compute within.

- **Permutation** and **matrix** representations are very concrete, but some "small" groups have no small degree representations.

- **Rewriting systems** form an effective datatype for these, but finding rewriting systems is harder.

How do we get them?

- Only has to handle **simple groups**, since extensions are easy
- Early method:
  - Choose a generating set, compute a finite presentation, then apply Knuth-Bendix with one of the standard orderings
  - **No bounds** on runtime or space of KB. Many generating sets, many orderings.
  - Had to hope to get **lucky**. Failed to handle some simple groups of interest.
- New method handles groups of Lie type **generically**

What does short mean?

- Several measures of efficiency:
  - Number of generators
  - Number of rules
  - Length of rules
  - Number of overlaps
  - Existence of a fast multiplier
- I chose to focus on the **number of rules**
- Multiplier important, but poorly understood even for *p*-groups

How short is short?

- Number of generators could be required to be logarithmic in group order (length no longer than longest chain of subgroups)
- **Short rewriting system** means fewer than $\sqrt{|G|}$ **rules**
- For fixed composition factors, the number of rules is **logarithmic** in the composition length
- But, for $PSL(2, p)$ the best one could do was $O(p)$
- Induction works smoothly with the above definitions

Quotient groups

- Use the generators and rules of G/N and N for G

- One has to modify the rules of G/N to take into account their new values in N ($xN \mapsto yN$ implies $x \mapsto yn$)

- One needs new rules to describe the action of the generators of G/N on N ($n \cdot q \mapsto q \cdot (n^q)$)

- **Total:** $g_3 = g_1 + g_2$ generators and $r_3 = r_1 + r_2 + g_1 \cdot g_2$ rules

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

- Simple groups of Lie type have a **Bruhat decomposition**: For every $g \in G$ there are unique $b \in B$, $w \in W$, $x \in U_w$:

$$g = b \cdot \dot{w} \cdot x$$

- Roughly $B = N_G(P) = T \ltimes P$, $N = N_G(T)$, $W = N/T$, $U_w = P \cap P^{\dot{w}}$
- In GL and PSL, B is the upper triangular matrices, T are the diagonal, P are the upper triangular with diagonal 1, W are the permutation matrices, Bruhat is LU
- B is polycyclic, W is a finite Coxeter group, and the double coset decomposition means we can combine them as if it was a quotient group

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

G	$\|G\|$	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
$= \mathit{brute}$		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
$\mathrm{Alt}(8)$	20160	6	61	0.414
$= A_3(2)$		9	63	0.418
$A_2(4)$	20160	10	42	0.377
$\ldots$				
M_{12}	95040	5	303	0.498
J_1	175560	5	192	0.436
$\mathrm{Alt}(9)$	181440	7	86	0.367
M_{22}	443520	4	150	0.386
J_2	604800	6	219	0.405
$\mathrm{Alt}(10)$	1814400	8	116	0.329

Conclusions and future work

- Rewriting systems of moderately short length exist for all finite groups
- They can be effectively written down given constructive recognition of the composition factors
- One needs to better understand why BN pairs have good rewriting systems in order to handle sporadic groups

The End