Towards effective algorithms for linear groups

Eamonn O'Brien

University of Auckland

August 2009

Introduction

$G = \langle X \rangle \leq \mathrm{GL}(d, q)$

Can we answer the following?

- $|G|$
- Composition series or chief series for G
- Sylow p-subgroups
- Conjugacy classes of elements or subgroups of G
- Normaliser of $H \leq G$

Rarely

Challenge problems

Problem

Find the order of $H \leq \mathrm{GL}(6, 5^2)$.

... using either of GAP or Magma.

Problem

Given $g \in \mathrm{GL}(6, 5^2)$ *find its order.*

$\mathrm{GL}(d, q)$ has elements of order $q^d - 1$

Probably requires factorisation of $q^i - 1$, a hard problem.

Problem

Find the normaliser in $\mathrm{GL}(8, 3)$ *of a subgroup of moderate index.*

By contrast: if $G = \mathrm{Sym}(10^6)$, we can answer readily most questions about G, using "efficient" algorithms.

The "matrix recognition" project

Goal: efficient algorithms, both theoretically and practically.

One measure of algorithm performance:
in time polynomial in the size of the input

If f and g are real-valued functions, defined on all sufficiently large integers, then $f(n) = O(g(n))$ means $|f(n)| < C|g(n)|$ for some positive constant C and all sufficiently large n.

For $G = \langle X \rangle \leq \mathrm{GL}(d, q)$, $\log |G| < d^2 \log q$.
Input size is $|X| d^2 \log q$.

Desire: algorithms whose complexity involves $\log q$, not q.

Another measure: practical, implemented in GAP or MAGMA.

Outline of Lecture I

- Basic features
- Permutation group analogues
- Recognition strategies
- Simple groups: the tasks

Cost of matrix multiplication

Two $d \times d$ matrices A and B
Cost of $A \times B$ using conventional algorithm is $O(d^3)$.

Strassen: $O(d^{\log_2(7)})$

Coppersmith & Winograd (1990): $O(d^{2.37})$

Where do we notice improvements? Perhaps for $d \geq 100$.

Membership

Given $G \leq \mathrm{GL}(d, q)$ and $x \in \mathrm{GL}(d, q)$: is $x \in G$?

$|\mathrm{GL}(d, q)| = O(q^{d^2})$

Difficult even for ... 1×1 matrices over $\mathrm{GF(q)}$:

Example

$H := \langle [561], [520], [320] \rangle \leq \mathrm{GL}(1, 593)$.

Membership related to Discrete log problem

Problem

$F = \mathrm{GF}(q)$, $\omega \in F$ primitive.
Given $\alpha \in F^\times$, determine k so that $\alpha = \omega^k$.

No polynomial-time algorithm known.

Permutation groups

Sims (1970, 1971): base and strong generating set (BSGS).
G acts faithfully on $\Omega = \{1, \ldots, n\}$

Base: sequence of points $B = [\epsilon_1, \epsilon_2, \ldots, \epsilon_k]$ where $G_{\epsilon_1, \epsilon_2, \ldots, \epsilon_k} = 1$.

This determines chain of stabilisers

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(k-1)} \geq G^{(k)} = 1,$$

where $G^{(i)} = G_{\epsilon_1, \epsilon_2, \ldots, \epsilon_i}$.
S *strong generating set*: $G^{(i)} = \left\langle S \cap G^{(i)} \right\rangle$

Example

$G = \langle (1,5,2,6), (1,2)(3,4)(5,6) \rangle$
$B = [1,3]$
$G > G_1 > G_{1,3} = 1$
$S = \{(1,5,2,6), (1,2)(3,4)(5,6), (3,4)\}$

Central task: construct *basic orbits* – orbit B_i of the base point ϵ_{i+1} under $G^{(i)}$.

$$|G^{(i)} : G^{(i+1)}| = \#B_i$$

Schreier's Lemma gives generating set for each $G^{(i)}$.

Let U_i be transversal of $G^{(i+1)}$ in $G^{(i)}$.

Transversal provide normal form: every $g \in G$ has **unique** representation $g = u_k u_{k-1} \dots u_1$ where $u_i \in U_i$.

Sifting algorithm provides membership test for G.

Base image $B^g = [\epsilon_1^g, \ldots \epsilon_k^g]$ uniquely determines g:

if $B^g = B^h$ then $B^{gh^{-1}} = B$, so $gh^{-1} = 1$. Hence g can be represented as $|B|$-tuple.

For many interesting $G \leq S_n$, $|B|$ is small compared to n: *short base* groups.

Luks et al. (1980), Seress (2003): polynomial time.

Variations underpin both theoretical and practical approaches to permutation group algorithms.

Schreier-Sims for matrix groups

G acts faithfully on $V = F^d$: $v \cdot g$, for $v \in V$

Compute BSGS for G, viewed as permutation group on the vectors.

Base points: standard basis vectors for V.

Central problem: basic orbits B_i large. Usually $|B_1|$ is $|G|$.

Butler (1979): action of G on one-dimensional subspaces of V.

Murray & O'Brien (1995): heuristic algorithm to select base points.

Neunhöffer et al. (2000s): use "helper subgroups" to construct large orbits

Critical for success: **index of one stabiliser in its predecessor**.

$|S_n : S_{n-1}| = n$

"Optimal" subgroup chain for $\mathrm{GL}(d, q)$?

$$\mathrm{GL}(d, q) \geq q^{d-1}.\mathrm{GL}(d-1, q) \geq \mathrm{GL}(d-1, q) \geq \dots$$

Leading index: $q^d - 1$.

Example

Largest maximal subgroup $2^{11} : M_{24} \leq J_4$ index 173 067 389.

Randomness

$|\mathrm{GL}(d, q)| = O(q^{d^2})$

Many algorithms are **randomised**: use random search in G to find elements having prescribed property $\mathcal{P}$.

Example

- Characteristic polynomial having factor of degree $> d/2$.
- Order divisible by prescribed prime.

Common feature: algorithms depend on detailed analysis of **proportion** of elements of finite simple groups satisfying $\mathcal{P}$.

Classes of algorithms

Definition

A Monte Carlo algorithm is a randomised algorithm which may return an incorrect answer to a decision question, the probability of this event being less than some ϵ.

If one of the answers is always correct, then it is **one-sided**.

Definition

A Las Vegas algorithm is one which never returns an incorrect answer, but may report failure with probability less than ϵ.

Assume we determine a lower bound, say $1/k$, for proportion of elements in G satisfying Property $\mathcal{P}$.

To find element satisfying $\mathcal{P}$ by random search with a probability of failure less than given $\epsilon \in (0, 1)$: choose a sample of uniformly distributed random elements in G of size at least $\lceil -\log_e(\epsilon) \rceil k$.

Random elements of a finite group

Babai (1991): Monte Carlo algorithm to construct in polynomial time nearly uniformly distributed random elements.

Celler, Leedham-Green, Murray, Niemeyer, O'B (1995): *product replacement* algorithm

Pak (2000): polynomial time

GAP and MAGMA use latter.

Black-box groups

Babai & Szemerédi (1984)

Group elements represented by bit-strings of uniform length.

Operations: multiplication, inversion, and checking for equality with the identity element.

Representation-independent: model includes permutation groups and matrix groups defined over $\mathrm{GF}(q)$.

Definition

Black-box algorithm does not use specific features of the group representation, nor particulars of how group operations are performed; it uses only these operations.

The basic strategies

- Geometry following Aschbacher
- Characteristic structure

Both provide composition series (and more) for G.

Aschbacher (1984)

G maximal subgroup of $\mathrm{GL}(d, q)$, let V be underlying vector space

- G preserves some natural linear structure associated with the action of G on V, and has normal subgroup related to this structure,
- or G is almost simple modulo scalars: $T \leq G/Z \leq Aut(T)$ where T is simple.

Basic strategy

1. Determine (at least one of) its Aschbacher categories.
2. If $N \lhd G$ exists, recognise N and G/N recursively, ultimately obtaining a composition series for the group.

7 categories giving normal subgroup

Example

G acts imprimitively on V, preserving r blocks.

Then $\phi : G \to S_r$ where $r|d$ and $N = \ker \phi$.

Lecture II: Geometry after Aschbacher

CompositionTree: exploits geometry to produce composition series for G, factors are **leaves** of tree.

Base cases for Aschbacher strategy

Classical group in natural representation or other **almost simple modulo scalars**.

Liebeck (1985): almost all maximal non-classical subgroups of $\mathrm{GL}(d, q)$ have order at most q^{3d}.

Landazuri & Seitz (1974), Seitz & Zalesskii (1993): lower bounds for degrees of nonlinear irreducible projective representations of finite Chevalley groups. Faithful projective representations in cross characteristic have degree that is polynomial in the size of the defining characteristic.

Principal focus: *matrix representations in defining characteristic*.

Hiss & Malle (2001), Lübeck (2001): absolutely irreducible representations of degree ≤ 250 of quasisimple groups.

Can we name the group?

A prime r dividing $b^e - 1$ is a *primitive prime divisor* of $b^e - 1$ if r does not divide $b^i - 1$ for $1 \leq i < e$.

Zsigmondy (1892): $b^e - 1$ has ppd unless $(b, e) = (2, 6)$ or $e = 2, b = 2^n - 1$.

$$|\mathrm{GL}(d, q)| = q^{\binom{d}{2}} \prod_{i=1}^{d} (q^i - 1)$$

Hence ppds of $q^e - 1$ for various values of $e \leq d$ divide $|\mathrm{GL}(d, q)|$ and also orders of the various classical groups.

ppd-element: order a multiple of some ppd

Naming groups: Classical groups

Problem

Given $G = \langle X \rangle \leq \mathrm{GL}(d, q)$, *does* G *contain* $\mathrm{SX}(d, q)$*?*

Praeger & Neumann (1992), P & Niemeyer (1998): Monte Carlo polynomial-time algorithms to name classical group in natural repn.

Search for certain kinds of ppd-elements that occur with high probability in $\mathrm{SX}(d, q)$ and are in only a "small" number of other subgroups of $\mathrm{GL}(d, q)$.

Original motivation: Joachim Neubüser (1988) asked for analogue of algorithm to decide if $G \leq S_n$ contains A_n.

Naming groups of Lie type: Black box

Theorem (Babai, Kantor, Palfy, Seress, 2002)

Given a group G isomorphic to a simple group of Lie type of known characteristic, its standard name can be computed using a polynomial time Monte-Carlo algorithm.

Choose sample $\mathcal{L}$ of independent (nearly) uniformly distributed random elements of G.

Find the three largest integers $v_1 > v_2 > v_3$ such that a member of $\mathcal{L}$ has order divisible by a primitive prime divisor of one of $p^{v_i} - 1$.

Usually $\{v_1, v_2, v_3\}$ determines $|G|$ and name of G.

Altseimer & Borovik (2002): distinguish between $\mathrm{PSp}(2m, q)$ and $\Omega(2m+1, q)$, q odd and $m \geq 3$.

Finding the characteristic

BKPS and other algorithms assume that input G is a simple group of Lie type of known characteristic.

Problem

Given $G \leq \mathrm{GL}(d, q)$ where G is a group of Lie type in **unknown** *defining characteristic r. Can we determine r?*

Liebeck & O'B (2007):
Monte Carlo algorithm which proceeds recursively through centralisers of involutions to find $\mathrm{SL}(2, F_r)$. Now read off r.

Kantor & Seress (2009):
The three largest element orders determine the characteristic of Lie-type simple groups of odd characteristic.

Result: extremely powerful Monte Carlo algorithms to name group.

Constructive recognition

Given $H = \langle X \rangle$, a named (quasi)simple group.

1. Given $h \in H$, express $h = w(X)$.
   ("Constructive membership problem", "Word problem")

2. Given $G = \langle Y \rangle$ where G is faithful representation of H,
   - solve constructive membership problem for G;
   - construct "effective" isomorphisms
     $\phi : H \longmapsto G$
     $\tau : G \longmapsto H$.

Lecture III: Constructive recognition
Key concept: *standard generators*

Application I: Conjugacy classes of classical groups

Example: $H = \langle X \rangle = \mathrm{SX}(d, q)$
$G = \langle Y \rangle$ is symmetric cube.

Wall (1963): description of conjugacy classes and centralisers of elements of classical groups.

Murray & Haller (ongoing): algorithm, which given d and q, constructs classes for $\mathrm{SX}(d, q)$.

$\phi : H \longmapsto G$ now maps class reps and centralisers to G.

Example

Higman's (1961) count of p-groups of p-class 2.
Eick and O'B (1999): algorithm which, given d and p, counts precisely the number of d-generator p-groups of class 2.
Critical task: for each conjugacy class rep r in $G := \Lambda^2(\mathrm{GL}(d, p))$ use Cauchy-Frobenius theorem to count fixed points for r.

Application II: Maximal subgroups of classical groups

Kleidmann & Liebeck (1990): describe some maximal subgroups of classical groups where $d \geq 13$.

Bray, Holt & Roney-Dougal (ongoing): construct generating sets for geometric maximal subgroups, and all maximals for $d \leq 12$.

So obtain $M \leq H := \mathrm{SX}(d, q)$, classical group in natural representation.

Use $\phi : H \longmapsto G$ to construct image of M in arbitrary representation G.

Characteristic structure

G has characteristic series $\mathcal{C}$ of subgroups:

$$1 \leq O_\infty(G) \leq S^*(G) \leq P(G) \leq G$$

$O_\infty(G) =$ largest soluble normal subgroup of G, soluble radical

$S^*(G)/O_\infty(G) = \text{Socle}\,(G/O_\infty(G)) = T_1 \times \ldots \times T_k$ where T_i non-abelian simple

$\phi : G \longmapsto \mathrm{Sym}(k)$ is repn of G induced by conjugation on $\{T_1, \ldots, T_k\}$ and $P(G) = \ker \phi$

$P(G)/S^*(G) \leq \mathrm{Out}(T_1) \times \ldots \times \mathrm{Out}(T_k)$ and so is soluble

$G/P(G) \leq \mathrm{Sym}(k)$ where $k \leq \log|G|/\log 60$

Black-box model pioneered by Babai and Beals.

Babai, Beals, Seress (2009): can construct $\mathcal{C}$ directly in black-box groups in polynomial time (subject to Discrete Log solution and some other restrictions).

Ongoing work with Holt and Roney-Dougal: refine composition series obtained from "geometric model" to obtain chief series reflecting this characteristic structure.

Cannon & Holt: exploit this model in many algorithms e.g. automorphism group, conjugacy classes of subgroups.

Lecture IV: Towards effective computation