

EFFICIENT COMPUTATION WITH MATRIX GROUPS

Peter Brooksbank

The Ohio State University

Specifying Groups

Permutation Groups

X a set of permutations of a domain Ω

$G = \langle X \rangle$, a subgroup of $\text{Sym}(\Omega)$

Input Length: roughly $|X||\Omega|$

Matrix Groups

X a set of inv'ble matrices over a finite field

$G = \langle X \rangle$, a subgroup of $\text{GL}(d, q)$

Input Length: roughly $|X|d^2 \log q$

Matrix Groups as Permutation Groups?

Viewed naively as a subgroup of
 $\text{Sym}(\text{GF}(q)^d)$
subgroups of $\text{GL}(d, q)$ have degree q^d

- Degree is exponential in the input length
- Given matrix rep'n is far more concise

Matrix Group Recognition

BIG GOAL

Produce an efficient algorithm for the following problem

GIVEN: $G = \langle X \rangle \leq GL(d, q)$

FIND: A “composition tree” for G

- *Name* the composition factors
- Find a presentation for G

Effective Epimorphisms

Let G be a homomorphic image of concrete group H , where H is “standard copy” of a known group

An epimorphism $\psi: H \rightarrow G$ is **effective** if there are efficient procedures to find

- (a) the image $h\psi \in G$ of any given $h \in H$
- (b) a preimage $g\psi^{-1} \in H$ of any given $g \in G$

Constructive Recognition

PROBLEM:

Given G , image of known quasisimple group H

CONSTRUCT:

An effective epimorphism $\Psi: H \rightarrow G$

\mathcal{C} = a family of quasisimple groups

(e.g. the alternating groups A_n)

A **constructive recognition algorithm for \mathcal{C}** is one which solves this problem for all H in \mathcal{C}

**Constructive
Recognition
Algorithm**

**Preprocessing
Algorithm**

sets up a
data structure

**Application
Algorithm**

finds images
and preimages

Applications

Composition series for matrix groups

Sylow subgroups of permutation groups

Maximal subgroups of finite simple groups

Recognising groups of symplectic type

Classical Groups

Classical groups are groups of linear transformations of a vector space V which preserve some nondegenerate form \mathbf{f} on V

Generic quasisimple classical group denoted by $\text{cl}(V)$

FORM	NAME OF GROUP	$\text{cl}(V)$
alternating	symplectic	$\text{Sp}(V)$
hermitian	unitary	$\text{SU}(V)$
quadratic	orthogonal	$\Omega(V)$

Representation of G

WHITE BOX

(the natural representation)

- H = quasisimple classical group
- Standard copy of H = subgroup of $\mathrm{GL}(d, p^e)$
- Elements of G = $d \times d$ matrices over $\mathrm{GF}(p^e)$

Representation of G

BLACK BOX

(unnatural representations)

- $H =$ quasisimple classical group
- Standard copy of $H =$ subgroup of $GL(d, p^e)$
- Elements of $G =$ binary strings of length N
- Group operations performed by an “oracle”

g	\rightarrow	THE	\rightarrow	$g \cdot h$
		BLACK	\rightarrow	g^{-1}
h	\rightarrow	BOX	\rightarrow	$g = 1?$

Brief History

Date	Authors	Group(s)	Box
'95	Celler Leedham-Green	$H = \text{SL}(d, p^e)$	white
'95	Cooperman Finkelstein Linton	$H = \text{SL}(d, 2)$	black
'97+	Kantor Seress	ALL classical groups	black

polynomial time with “discrete log” oracle...

'99	Conder Leedham-Green	$H = \text{SL}(2, p^e)$	white
'01	Brooksbank	all classical groups	white
'02+	Leedham-Green O'Brien	$H = \text{SL}(2, p^e)$	“grey”

Theorem [Landazuri & Seitz, 1974]

Let H be a finite simple group of Lie type of characteristic p and let V be the natural module upon which H acts naturally. If H has a faithful representation of dimension n in characteristic $r \neq p$, then $|V| \leq n^c$ for some absolute constant c .

Interpretation

In a cross-characteristic representation, the field size p^e for the standard copy of H is polynomially related to the input length of G .

Consequence

The Kantor-Seress algorithm runs in polynomial time for input groups G given in cross-characteristic representations.

Representation of G

GREY BOX

(natural characteristic)

- $H =$ quasisimple classical group
- Standard copy of $H =$ subgroup of $\mathrm{GL}(d, p^e)$
- Elements of $G = n \times n$ matrices over $\mathrm{GF}(p^f)$

Brief History, continued...

Thesis: *To what extent can black box constructive recognition algorithms be improved if one hypothesises an oracle to handle $SL(2, q)$ subgroups?*

In 2000, Bill Kantor and I showed that the linear and symplectic cases of the Kantor-Seress algorithm can be modified to admit the use of such an oracle, giving rise to polynomial time procedures.

Main Objectives

- Black box algorithms for classical groups which have
 - (a) improved timing over existing algorithms
 - (b) polynomial timing assuming an $SL(2, q)$ -oracle
- Practical implementations of these algorithms

Main Obstacles

- Algorithms for low dimensional groups
[notably $SU(3, p^e)$ and $SU(4, p^e)$]
- Constructing root elements and root groups
- Listing large elementary abelian subgroups
- Avoiding recursion

Recent Developments

There are black box constructive recognition algorithms for classical groups H , naturally represented over a field of size q , which

1. do not use recursion
2. run in polynomial time assuming oracles to handle $SL(2, q)$ subgroups

for each of the following cases

- $H = SU(d, q)$ [B, 2002]
- $H = \Omega^\epsilon(d, q)$ [B & Kantor, 2003+]

Implementation

Group	Box	Algorithm	System
$SL(d, q)$	white	Celler L-Green	IN GAP3
$SL(2, q)$	grey	O'Brien L-Green	Magma
$SL(d, q)$	white/ grey	O'Brien L-Green	Magma
all classical	white	B	GAP
$SL(d, q)$	black	Kantor Seress	GAP & Magma
$SL(d, q)$	black	Bratus +	GAP
$Sp(d, q)$ q odd	black	Kantor Seress	GAP
$SU(d, q)$ prime $q > 16$	black	B	GAP

Future Directions

1. Exceptional Groups of Lie Type

Kantor & Magaard

2. New ideas for improved algorithms

a. Ryba

uniform treatment of grey box groups

b. Leedham-Green & O'Brien

improved algorithm for $SL(d, q)$

generalisations to other classical groups possible