

**EFFICIENT COMPUTATION
IN BLACK BOX CLASSICAL GROUPS**

Peter Brooksbank

The Ohio State University

Constructive Recognition

$G = \langle X \rangle$ given by a set X of generators

$H =$ “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 $g \in G$.

PROBLEM:

Given G , an image of a known quasisimple group H .

CONSTRUCT:

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

$\mathcal{C} =$ a family of quasisimple groups
(e.g. the special linear groups)

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

Finding composition series for matrix groups

Finding Sylow subgroups of permutation groups

Representation of G

standard copy of classical $H =$ subgroup of $GL(d, p^e)$

NATURAL REPRESENTATION

elements of $G = \langle X \rangle$ are $d \times d$ matrices over $GF(p^e)$

BLACK BOX

elements of G are binary strings of length N

group ops performed by an oracle (the “black box”):

GREY BOX

elements of G are $n \times n$ matrices over $\text{GF}(p^f)$

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.

Brief History

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

polynomial time with “discrete log” oracle...

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

polynomial time with $\text{SL}(2, q)$ oracle...

'99	Brooksbank Kantor	$H = \begin{cases} \text{SL}(d, p^e) \\ \text{Sp}(d, p^e) \end{cases}$	black box
-----	----------------------	--	-----------

Main Objectives

- (I) Black box algorithms having:
 - (a) improved timing over existing algorithms; and
 - (b) polynomial timing assuming an $SL(2, q)$ -oracle.
- (II) Practical implementations of those algorithms.

Main Obstacles

- (I) Avoiding recursion.
- (II) Dealing with low dimensional groups.
[notably $SU(3, p^e)$ and $SU(4, p^e)$]
- (III) Constructing root elements and root groups.
- (IV) Listing large elementary abelian subgroups.

Point Stabilisers

$$H = Cl(d, p^e)$$

$$V = GF(p^e)^d$$

$x \neq y =$ singular points of V

$$Q(x) = O_p(H_x)$$

Then

$$H_x = Q(x) \rtimes H_{x,y}$$

Facts

If $Z(Q(x)) \geq T(x)$ (transvection group) then $\overline{Q}(x) := Q(x)/T(x)$.

Otherwise $\overline{Q}(x) := Q(x)$.

1 $Q(x)^h = Q(x^h)$ for any $h \in H$.

2 $(H_{x,y})' \cong Cl(d-2, p^e); \quad \overline{Q}(x) \cong \langle x, y \rangle^\perp$.

3 $Q(x)$ acts regularly on $\{\text{singular } z \mid z \notin x^\perp\}$

Recent Developments

Black box constructive recognition algorithms for

$$H = \text{SU}(d, q) \quad [\text{B}, 2002]$$

$$H = \Omega^\epsilon(d, q) \quad [\text{B}, \text{Kantor}, 2003+]$$

which:

- (I) do not use recursion; and
- (II) run in polynomial time assuming oracles to handle $\text{SL}(2, q)$ subgroups and to compute discrete logs in cyclic groups of order $q \pm 1$.

Implementation

GROUP	BOX	ALGORITHM	SYSTEM
$SL(d, q)$	white	Celler L-Green	IN GAP3
$SL(2, q)$	grey	Conder L-Green O'Brien	Magma
$SL(d, q)$	white	L-Green +	Magma
other classical groups	white	B	GAP
$SL(d, q)$	black	Kantor Seress	GAP
$SL(d, q)$	black	Bratus +	GAP
$Sp(d, q)$ q odd	black	Kantor Seress	GAP
$SU(d, q)$ $q > 16$	black	B	GAP