Constructive recognition

Eamonn O'Brien

University of Auckland

August 2011

Constructive recognition: the main tasks

$H = \langle X \rangle \leq \mathrm{GL}(d, q)$ where H is (quasi)simple.

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

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

Key idea: standard generators.

Using standard generators

Define *standard generators* $\mathcal{S}$ for $H = \langle X \rangle$.

Need algorithms to:

- Construct $\mathcal{S}$ as *words* in X.
- For $h \in H$, express h as $w(\mathcal{S})$ and so as $w(X)$.

If $\langle Y \rangle = G \simeq H$ then:

- Find standard generators $\bar{\mathcal{S}}$ in G as words in Y.
- For $g \in G$, express g as $w(\bar{\mathcal{S}})$ and so as $w(Y)$.

Choose $\mathcal{S}$ so that solving for word in $\mathcal{S}$ is easy.

Now define isomorphism $\phi : H \longmapsto G$ from $\mathcal{S}$ to $\bar{\mathcal{S}}$

Effective: if $h = w(\mathcal{S})$ then $\phi(h) = w(\bar{\mathcal{S}})$.

Similarly $\tau : G \longmapsto H$.

Standard generators for $\mathrm{SL}(d, q)$

Leedham-Green & O'B (2009).
Natural module V for $H = \mathrm{SL}(d, q)$ with basis $\{e_1, \ldots, e_d\}$.
Define standard generators s, δ, u, v for H:

s, δ, u lie in copy of $\mathrm{SL}(2, q)$ and act on $\langle e_1, e_2 \rangle$ as:

$$s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \delta = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

cycle v maps

$$e_1 \mapsto e_d \mapsto -e_{d-1} \mapsto -e_{d-2} \mapsto -e_{d-3} \cdots \mapsto -e_1$$

Given $h \in H$, write $h = w(\mathcal{S})$ via echelonisation.

Simplest case: G and H *identical*.

Algorithm input $H = \langle X \rangle = \mathrm{SX}(d, q)$

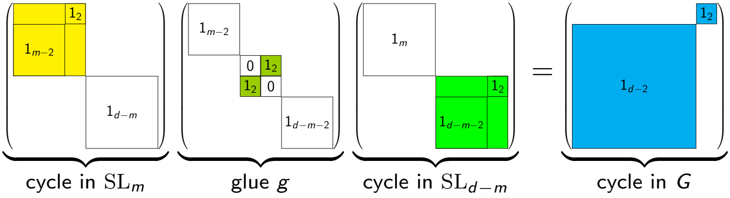
First task: construct $\mathcal{S}$ as *words* in X.

The basic algorithm

- Construct two subgroups H and K in G so

$$H = \begin{pmatrix} \mathrm{SX}_m & \\ & 1_{d-m} \end{pmatrix} \quad \text{and} \quad K = \begin{pmatrix} 1_m & \\ & \mathrm{SX}_{d-m} \end{pmatrix}$$

- Recursively construct standard generators $\mathcal{S}_H$ and $\mathcal{S}_K$ for H and K
- all but cycle from standard generators for G contained in $\mathcal{S}_H$
- cycle is constructed by glueing two cycles from $\mathcal{S}_H$ and $\mathcal{S}_K$. e.g. if $G = \mathrm{SL}(d, q)$ with even d and q, then



Odd characteristic

Theorem (Leedham-Green and O'B, 2009)

There is a Las Vegas algorithm that takes as input $G = \mathrm{SX}(d, q) = X$ of bounded cardinality of $\mathrm{GL}(d, q)$, and returns standard generators for G as SLPs of length $\mathrm{O}(\log^3 \mathrm{d})$ in X. The algorithm has complexity $O(d^4 \log q)$ measured in field operations.

t is involution in G, with eigenspaces E_+ and E_-

$C_G(t)$ is $(\mathrm{GL}(\mathrm{E}_+) \times \mathrm{GL}(\mathrm{E}_-)) \cap \mathrm{SL}(\mathrm{d}, \mathrm{q})$.

A *strong involution* in $\mathrm{SX}(d, q)$ has -1-eigenspace of dimension in range $(d/3, 2d/3]$.

$G = \mathrm{SX}(d, q)$ for q odd

1. Find and construct strong involution t having -1-eigenspace of dimension m.
2. Now construct $C_G(t)$. Construct the direct summands of the derived group to obtain $\mathrm{SX}(m, q)$ and $\mathrm{SX}(d - m, q)$ as *subgroups* of G.
3. Recursively construct standard generators for $\mathrm{SX}(m, q)$ and $\mathrm{SX}(d - m, q)$.
4. Construct centraliser C of involution

$$\begin{pmatrix} I_{m-2} & 0 & 0 \\ 0 & -I_4 & 0 \\ 0 & 0 & I_{d-m-2} \end{pmatrix}$$

5. Within C solve constructively for matrix g

$$\begin{pmatrix} I_{m-2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I_{d-m-2} \end{pmatrix}$$

6. Now m-cycle v_m and $(d-m)$-cycle v_{d-m} “glued” together by g to produce d-cycle $v_m g v_{d-m}$.

Cost of finding a strong involution

First step: search for an element of $\mathrm{SX}(d, q)$ of even order that has as a power a strong involution.

Theorem (Lübeck, Niemeyer, Praeger, 2009)

For an absolute constant c, the proportion of $g \in \mathrm{SX}(d, q)$ such that a power of g is a strong involution is $\geq c/\log d$.

Recursion to smaller cases requires additional results.

Theorem (Leedham-Green & O'B, 2009)

For some absolute constant c, the proportion of $g \in \mathrm{SX}(d, q)$ such that a power of g is a "suitable" involution is $\geq c/d$.

Constructing centralisers

Bray (2001): Monte Carlo algorithm to construct $C_G(t)$ for involution $t \in G$.

Algorithm exploits properties of dihedral group.

1. If $[t, g]$ has odd order $2m + 1$, then $g[t, g]^m$ commutes with t.
2. If $[t, g]$ has even order $2m$, both $[t, g]^m$ and $[t, g^{-1}]^m$ commute with t.

So convert random elements of G into elements of $C_G(t)$.

Elements not, in general, uniformly-distributed, but:

Lemma

If g is uniformly distributed among the elements of G for which $[t, g]$ has odd order, say $2n + 1$, then $g[t, g]^n$ is uniformly distributed among the elements of $C_G(t)$.

If odd order case occurs *sufficiently often*, we can construct nearly-uniformly distributed random elements of $C_G(t)$ in polynomial time.

Proportion of odd order elements

Theorem (Parker & Wilson, 2009)

Let G be a simple group of Lie type, of Lie rank r, defined over field of odd characteristic. The probability that $[t, g]$ has odd order, where t is a fixed involution and g is a random element of G, is at least c/r for some absolute constant c.

Example: lower bound for $\mathrm{PSL}_d(q)$ is $\frac{1}{12d}$.

Method: for each class of involutions, find a dihedral group of twice odd order generated by two involutions of this class, and show that a significant proportion of pairs of involutions in this class generate such a dihedral group.

Cost of construction of centraliser

Bray (2001)
Parker & Wilson (2010)
Holmes, Linton, O'B, Ryba, Wilson (2008)
Let μ, ξ and ρ denote the costs of a group operation, constructing a random element of G, and an order oracle respectively.

Theorem

Let H be a simple group of Lie rank r defined over a field of odd characteristic. The centraliser in H of an involution can be computed in time $O(r(\xi + \rho)\log(1/\epsilon) + \mu r^2)$ with probability of success at least $1 - \epsilon$, for $\epsilon > 0$.

This is a black-box Monte Carlo algorithm.

Even characteristic: Problems

- involutions cannot be found efficiently by a random search Guralnick & Lübeck (2001): proportion of elements in G of even order is $< 5/q$;
- groups for a recursion cannot be found in centraliser; Aschbacher & Seitz (1976): various types of involutions.

Theorem (Aschbacher & Seitz)

If $g \in G$ is a good involution, then, mod base change,

$$C_G(g) = \begin{pmatrix} \mathrm{GL_r} & * & * \\ & \mathrm{GL_{d-m}} & * \\ & & \mathrm{GL_r} \end{pmatrix} \cap G \quad \text{or} \quad C_G(g) = \begin{pmatrix} Sp_r & * & * \\ & \mathrm{SX}_{d-m} & * \\ & & Sp_r \end{pmatrix}$$

where $r = \mathrm{rank}(g-1)$, $m = 2r$, and SX_{d-m} same type as G.

Even characteristic – The general approach

- find $H = \mathrm{SX}(m,q) \leq G$ where $m \in [d/3, 2d/3]$ is even or $4|m$; if G is linear or unitary, then so is H, otherwise Ω^+;

$$\text{(via base change)} \quad H = \begin{pmatrix} \boxed{\mathrm{SX}_m} & \\ & \boxed{1_{d-m}} \end{pmatrix} \quad \text{and} \quad K = \begin{pmatrix} \boxed{1_m} & \\ & \boxed{\mathrm{SX}_{d-m}} \end{pmatrix}$$

- Recursion: construct standard generators of SX_m in H and a *good* involution $g \in H$ with $r = \mathrm{rank}(g-1) = m/2$
- in $C_G(g)$ find $K = \mathrm{SX}(d-m,q) \leq G$
- Recursion: construct standard generators of SX_{d-m} in K
- glue the cycles of SX_m and SX_{d-m}

Constructing $H \leq G = \langle X \rangle$

- Find $g \in G$ with 1-eigenspace of dimension $d/2 < e < 5d/6$; proportion of elements in G which power to such g is $O(1/d)$ (Lübeck, Niemeyer & Praeger, 2009)
- consider random conjugate $h = g^k$ in G; expect

$$S = \ker(g-1) \cap \ker(h-1) \quad \text{of dim. } 2e - d,$$
$$I = \mathrm{im}\,(g-1) + \mathrm{im}\,(h-1) \quad \text{of dim. } m = 2(d-e)$$

- choose basis through $V = I \oplus S$, so that

$$H = \begin{pmatrix} U & \\ & 1_{d-m} \end{pmatrix} \leq G$$

with $U = \langle a, b \rangle \leq \mathrm{SX}(m, q)$ of degree $m \in [d/2, 2d/3]$

Theorem (Praeger, Seress, Yalcinkaya)

$U = \langle a, b \rangle = \mathrm{SX}(m, q)$ *with probability at least* $1 - c/q$.

Constructing $K \leq G = \langle X \rangle$

- Recursion: construct standard generators of SX_m in H and good involution g of corank $r = m/2$; via base change

$$g \rightsquigarrow \begin{pmatrix} 1_r & 1_r & \\ & 1_r & \\ & & 1_{d-m} \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1_r & & 1_r \\ & 1_{d-m} & \\ & & 1_r \end{pmatrix}$$

- In centraliser $C_G(g)$ construct

$$C = \begin{pmatrix} \mathrm{SX}_r & * & * \\ & \mathrm{SX}_{d-m} & * \\ & & \mathrm{SX}_r \end{pmatrix} \leq C_G(g)$$

Bray (2000): random elements in centraliser
Kantor & Lubotzky (1990): random generation

Theorem (Babai, Palfy, Saxl (2010))

For every prime p the proportion of p-regular elements in $\mathrm{PSX}(d,q)$ is at least $1/(2d)$.

Lemma

Let $K = H \ltimes M$ where M is abelian and of exponent 2. Let $h \in H$ be of odd order and assume it acts fixed point freely on M. If $k = am \in K$ where $a \in C_H(h)$ and $m \in M$, then $a = hk(hh^k)^{(|h|-1)/2}$.

$$\begin{pmatrix} \mathrm{SX}_r & * & * \\ & \mathrm{SX}_{d-m} & * \\ & & \mathrm{SX}_r \end{pmatrix} \overset{(a)}{\rightsquigarrow} \begin{pmatrix} 1_r & * & * \\ & \mathrm{SX}_{d-m} & * \\ & & 1_r \end{pmatrix} \overset{(b)}{\rightsquigarrow} \begin{pmatrix} 1_r & & * \\ & \mathrm{SX}_{d-m} & \\ & & 1_r \end{pmatrix} \overset{?}{\rightsquigarrow}$$

$$\begin{pmatrix} 1_r & & \\ & \mathrm{SX}_{d-m} & \\ & & 1_r \end{pmatrix}$$

(a) N & P (1998), Babai et al. (2010): construct direct factor

(b) find random $f = \begin{pmatrix} u & & * \\ & 1_{d-m} & \\ & & u \end{pmatrix}$ of odd order k with u irreducible;

if $y = \begin{pmatrix} 1_r & * & * \\ & v & * \\ & & 1_r \end{pmatrix}$, then $fy(ff^y)^{(k-1)/2} = \begin{pmatrix} 1_r & & * \\ & v & \\ & & 1_r \end{pmatrix}$

(c) Guralnick & Lübeck (2001): squaring

Base cases for recursion

$\mathrm{SX}(d, q)$ where $d = 2, 3, 4$.

Conder, Leedham-Green, O'B (2006): $\mathrm{SL}_2(q)$.

Lübeck, Magaard and O'B (2006): $\mathrm{SL}_3(q)$.

Burns (2009): $\mathrm{SL}_4(q)$.

Results

Theorem (Dietrich, L-G, Lübeck, O'B)

Let $G = \langle X \rangle$ be a classical group in natural representation and even characteristic. There is a Las Vegas algorithm which constructs the standard generators for G as words in X. Subject to a discrete logarithm oracle, the algorithms needs

$$O(d^4 \log d \log^2 q)$$

field operations.

Easy modification: Las Vegas algorithm to construct involution in G as word in X

Writing elements as SLPs in classical groups

Elliot Costi (2009): algorithms to write element of G as SLP on our standard generators.

- $G = \mathrm{SX}(d, q)$: Complexity: $O(d^3 \log q)$
- $G \leq \mathrm{GL(n, q)}$ is defining char (projective) irreducible representation of $\mathrm{SX}(d, q)$. Complexity: $O(n^3 \log^3 q + n^4 \log q)$.

Schneider *et al.* (2011): arbitrary repn, our standard generators.

Black-box algorithms for classical groups

Theorem (Kantor & Seress, 2001)

There is a Las Vegas algorithm which when given a perfect group $G = \langle X \rangle \leq GL(V)$ where $G/Z(G)$ is isomorphic to a classical simple group of known characteristic produces a constructive isomorphism $G/Z \longmapsto C$.

Algorithm not polynomial in size of input:
factor of q in the running time.

Central difficulty?

Need to find elements of order p and they're hard to find!

$\rho(G)$ is proportion of p-singular elements in G.
Kantor, Isaacs, Spaltenstein (1995); Guralnick & Lübeck (2003)

Theorem

$\frac{2}{5q} < \rho(G) < \frac{5}{q}$ *where G is a group of Lie type defined over* $\mathrm{GF}(q)$.

So random search requires $O(q)$ random selections.

The obstacle

Brooksbank & Kantor (2001): algorithms can be made polynomial in $\log q$ given an *oracle* for constructive membership testing in $\langle X \rangle \cong \mathrm{SL}(2, q)$.

Critical task: find transvection as word in X.

Proportion is $O(1/q)$, can't search randomly.

B & K (2001-2006): Black-box algorithms for the classical families which run in polynomial time subject to existence of $\mathrm{SL}(2, q)$ *oracle*.

Constructive recognition for $\mathrm{SL}(2, q)$

Landazuri & Seitz (1974), Seitz & Zalesskii (1993): faithful projective representations in cross characteristic have degree that is **polynomial** in q, so critical focus is defining characteristic representation.

Let $\tau(d)$ denote the number of factors of d.

Theorem (Conder, Leedham-Green, O'B, 2006)

$G \leq \mathrm{GL(d, F)}$ for $d \geq 2$, where F has same characteristic as $\mathrm{GF(q)}$. Assume that G is isomorphic modulo scalars to $\mathrm{PSL}(2, q)$. Then, subject to a fixed number of calls to a Discrete Log Oracle, there exists a Las Vegas algorithm that constructs an epimorphism from G to $\mathrm{PSL}(2, q)$ at a cost of at most $O(d^5\tau(d))$ field operations.

Theorem (Brauer & Nesbitt, 1940)

Let F be an algebraically closed field of characteristic p, and let V be an irreducible $F[G]$-module for $G = \mathrm{SL}(2, q)$, where $q = p^e$. Then $V \simeq T_1 \otimes T_2 \otimes \cdots \otimes T_t \otimes_{\mathrm{GF(q)}} F$, where T_i is the s_i-fold symmetric power S_i of the natural $\mathrm{GF}(q)[G]$-module M twisted by the f_i th power of the Frobenius map, with $0 \leq f_1 < f_2 < \cdots < f_t < e$, and $1 \leq s_i < p$ for all i.

G absolutely irreducible representation of $\mathrm{SL}(2, q)$.
Three components to constructive recognition algorithm for G.

1. Decompose tensor product to obtain one symmetric power T_i.
2. Decompose T_i to obtain SL(2, q) in its natural representation.
3. Construct standard generators for SL(2, q).

Standard generators for SL(2, q) in natural repn

1. Find $A \in H$ of order $q-1$ and B a random conjugate of A.
2. Compute eigenvectors u and v of A, with corresponding eigenvalues a and a^{-1}.
3. Find a random element C of H and an i such that B^iC fixes $\langle u\rangle$, if such an i exists. If A and B^iC lie in $\mathrm{SL}(2,q)$ and have common eigenvector u, then $S = [A, B^iC]$ is a transvection fixing u.
4. Similarly, find a random element D of H and a j such that B^jD fixes $\langle v\rangle$ and $T = [A, B^jD]$ is not trivial. Now, T is a non-trivial transvection fixing v.
5. Write S, T, A with respect to the ordered basis (u, v) to obtain generating set for $\mathrm{SL}(2,q)$.

Step 3 critical: *i exists if and only if $\langle u \rangle C^{-1}$ lies in the orbit of $\langle u \rangle$ under $\langle B \rangle$.*

$B^i C$ fixes $\langle u \rangle$

Equivalently: $a^{2i} = \mu$ where $\mu \in \mathrm{GF(q)}$.

Its solution relies on *discrete log*.

Easy to find elements of order $q - 1$:
proportion is $\phi(q-1)/2(q-1) > 1/2 \log\log q$.

Now given $x \in \mathrm{SL}(2, q)$, use echelonisation to write x as word in S, T, A.

$\mathrm{SL}(3, q)$

Lübeck, Magaard, O'B (2007).
Exploit solution for $\mathrm{SL}(2, q)$ to find generators for set of six root subgroups in G which are normalised by single maximal torus.

Now parameterise root subgroups.

Also: algorithm to write $g \in G$ as word in images of standard generators.

Constructive recognition for the sporadics

Wilson (1996): standard generators for sporadic $G = \langle Y \rangle$

Bray and Wilson: black-box algorithms to find these (as words) in Y.

Two methods to solve constructive membership problem for G.

- Random Schreier works well for many – with careful choice of base points (O'B & Wilson, 2002).
- Reduction algorithm of Holmes et al. (2008): reduces constructive membership problem in G to three instances of the same problem for involution centralisers in G.

Constructive recognition for other families

- A_n: Bratus & Pak (2000), Holt; Beals et al. (2001-05). Black-box.
- Exceptional groups:
  - Henrik Bäärnhielm (2006-2009): Algorithms for matrix representations of Suzuki, large and small Ree groups.
  - Kantor & Magaard (2010): black-box algorithms.
- Small degree representations of $\mathrm{SL}(d, q)$ (Magaard, O'B, Seress, 2008).