Recognition of Classical Groups of Lie Type

Alice Niemeyer

UWA, RWTH Aachen

Linear groups

Let $q = p^a$ for some prime p and $\mathbb{F} = \mathbb{F}_q$ a field with q elements. Consider the vector space $\mathbb{F}_q^n$.

- $\mathrm{GL}(n, q)$: the group of all invertible $n \times n$ matrices with entries in $\mathbb{F}_q$. The general linear group.
- $\mathrm{SL}(n, q)$: the group of all invertible $n \times n$ matrices with entries in $\mathbb{F}_q$ and determinant 1. The special linear group.

Invariant Forms

Let $q = p^a$ for some prime p and $\mathbb{F} = \mathbb{F}_q$ a field with q elements. Consider the vector space $V = \mathbb{F}_q^n$. Let $G \leq \mathrm{GL}(n, q)$. Define a bilinear form $f = (.,.)$ on V.

Definition

f is invariant under G if $f(ug, vg) = f(u, v)$ for all $g \in G$.
f is invariant modulo scalars under G if for any $g \in G$ there exists $c_g \in \mathbb{F}_q^*$ with $f(ug, vg) = c_g f(u, v)$.
There is a matrix M_f such that $f(v, w) = vM_f w^T$.
f is invariant under G if $gM_f g^T = M_f$ for all $g \in G$.

The symplectic group

Let $q = p^a$ for some prime p and $\mathbb{F} = \mathbb{F}_q$ a field with q elements.
Consider the vector space $V = \mathbb{F}_q^n$.
Define a bilinear form $f = (.,.)$ on V.

- f is non-degenerate if $\forall w \in V \; f(v,w) = 0 \Rightarrow v = 0$
- f is alternating if $f(v,v) = 0$ for all $v \in V$.
- if f is alternating then $f(v,w) = -f(w,v)$, i.e. f skew-symmetric.
- if V has a non-deg., alternating bilinear form, then n even
- any two non-degenerate, alternating bilinear forms on V are equivalent up to a change of basis

The symplectic Group

Symplectic Group

Let f be a non-degenerate, alternating bilinear form on $V = \mathbb{F}_q^{2n}$.

- The symplectic group $\mathrm{Sp}(2n, q)$ is the group of all invertible $(2n) \times (2n)$ matrices with entries in $\mathbb{F}_q$ which leave f invariant.
- The general symplectic group $\mathrm{GSp}(2n, q)$ is the group of all invertible $(2n) \times (2n)$ matrices with entries in $\mathbb{F}_q$ which leave f invariant modulo scalars.

The symplectic group

Example

Let $q = p^a$ for some prime p and $\mathbb{F} = \mathbb{F}_q$. Let $V = \mathbb{F}_q^4$.
Let

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

Define $f : V \times V \to \mathbb{F}_q$ by $f(v, w) = vAw^T$. Then f is a non-degenerate, alternating bilinear form on V.

The symplectic group

Example

$$\mathrm{Sp}(4,17) = \left\langle \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 16 & 0 & 0 \end{pmatrix} \right\rangle.$$

Summary

Some of the finite classical groups of Lie type are:

- *linear groups:* $\mathrm{SL}(n, q)$.
- *symplectic groups:* $\mathrm{Sp}(n, q)$, n even.
- *orthogonal groups:* $\Omega^{\epsilon}(n, q)$,
  $$\epsilon = \begin{cases} \pm & n \text{ even} \\ \circ & n \text{ odd (and hence also } q) \end{cases}.$$
- *unitary groups:* $\mathrm{SU}(n, q)$.

The groups Ω and Δ

Name	Ω	Δ	Note
linear groups	$\mathrm{SL}(n, q)$	$\mathrm{GL}(n, q)$	
symplectic groups	$\mathrm{Sp}(n, q)$	$\mathrm{GSp}(n, q)$	n even
orthogonal groups	$\Omega^\epsilon(n, q)$	$\mathrm{GO}^\epsilon(n, q)$	$\epsilon = \begin{cases} \pm & n \text{ even} \\ \circ & n \text{ odd} \end{cases}.$
unitary groups	$\mathrm{SU}(n, q)$	$\mathrm{GU}(n, q)$	$V = \mathbb{F}_{q^2}^n$

formulas for the orders of Ω

Theorem

Let Ω be one of the groups of Lie type in characteristic p with $q = p^a$ given before and $n \geq 2$. Then

$$|\Omega| = \frac{1}{\ell} q^h P(q),$$

Ω	ℓ	h	$P(q)$
$SL(n,q)$		$\binom{n}{2}$	$\prod_{i=2}^{n}(q^i - 1)$
$Sp(2m,q)$		m^2	$\prod_{i=1}^{m}(q^{2i} - 1)$
$\Omega^\circ(2m+1,q)$	2	m^2	$\prod_{i=1}^{m}(q^{2i} - 1)$
$\Omega^+(2m,q)$	$(2, q-1)$	$m(m-1)$	$(q^m - 1)\prod_{i=1}^{m-1}(q^{2i} - 1)$
$\Omega^-(2m,q)$	$(2, q-1)$	$m(m-1)$	$(q^m + 1)\prod_{i=1}^{m-1}(q^{2i} - 1)$
$SU(n,q)$		$\binom{n}{2}$	$\prod_{i=2}^{n}(q^i - (-1)^i)$

Goal

Question

Neubüser asked in 1988: Given $G \leq \mathrm{GL}(n, q)$ give an algorithm to decide whether $\mathrm{SL}(n, q) \leq G$.

A first answer

Algorithm by Neumann and Praeger (1992). "A recognition algorithm for special linear groups." Proc. London Math. Soc. (3) 65 (1992), no. 3, 555-603.
Runtime: $O(n^4 \log(q))$.

Today's aim

Introduce an algorithm by N. and Praeger that answers the question whether a group $G \leq GL(n, q)$ acting absolutely irreducibly on the underlying vector space with knowledge about all preserved forms contains a corresponding classical group.

Background from Number Theory

Let a and m be positive integers. The least positive integer e with $a^e \equiv 1 \pmod{m}$ is called the order of a modulo m, denoted $\mathrm{ord}_m(a)$.

If $\gcd(a, m) = 1$ then $e = |\langle a \rangle|$ in $\mathbb{Z}_m^*$. In particular, $e \mid \varphi(m)$ and $e = \varphi(m)$ if and only if a is a primitive root modulo m.

Primitive Prime Divisor Elements

Let b and m be positive integers with $\gcd(b, m) = 1$ and $e = \mathrm{ord}_m(b)$.
Then $b^\ell \equiv 1 \pmod{m}$ if and only if $\ell = ce$ for some positive integer c.

s prime

$b^{s-1} \equiv 1 \pmod{s}$ thus e divides $s - 1$. In particular, $s = ce + 1$.

Definition

For positive integers b, e with $b > 1, e > 1$, a prime s is called a primitive prime divisor (or ppd) of $b^e - 1$, if $b^e - 1$ is divisible by s, but s does not divide $b^i - 1$ for $i < e$. A ppd s is called large if either

(a) $s \geq 2e + 1$, or
(b) $s = e + 1$ and s^2 divides $b^e - 1$.

Thus s is a ppd of b^e, if and only if $e = \mathrm{ord}_s(b)$.

Example

Consider $b = 7$. Then

$$\begin{aligned} 7^1 - 1 &= 2 \cdot 3 \\ 7^2 - 1 &= 2^4 \cdot 3 \\ 7^3 - 1 &= 2 \cdot 3^2 \cdot 19 \\ 7^4 - 1 &= 2^5 \cdot 3 \cdot 5^2 \\ 7^5 - 1 &= 2 \cdot 3 \cdot 2801 \\ 7^6 - 1 &= 2^4 \cdot 3^2 \cdot 19 \cdot 43 \end{aligned}$$

- 19 is a ppd of $b^3 - 1$ but 19 is not a ppd of $b^6 - 1$.
- 19 is a large ppd of $b^3 - 1$ because $19 > 2 * 3 + 1$.
- 5 is a ppd of $b^4 - 1$
- 5 is a large ppd of $b^4 - 1$ because, even though $5 = 4 + 1$, we have 5^2 divides $b^4 - 1$.

Definition

For a prime p and positive integers z, e with $z \geq 1, e > 1$, and $q = p^z$, a prime s is called a basic primitive prime divisor (or ppd) of $q^e - 1$, if $q^e - 1$ is divisible by s, but $p^i - 1$ is not divisible by s for $i < ze$.

Example

Let $q = 7^2$, so $p = 7$ and $z = 2$.

$$\begin{aligned}
7^1 - 1 &= 2 \cdot 3 & & \\
7^2 - 1 &= 2^4 \cdot 3 &= &\ 49 - 1 = q - 1 \\
7^3 - 1 &= 2 \cdot 3^2 \cdot 19 & & \\
7^4 - 1 &= 2^5 \cdot 3 \cdot 5^2 &= &\ 49^2 - 1 = q^2 - 1 \\
7^5 - 1 &= 2 \cdot 3 \cdot 2801 & & \\
7^6 - 1 &= 2^4 \cdot 3^2 \cdot 19 \cdot 43 &= &\ 49^3 - 1 = q^3 - 1
\end{aligned}$$

Thus 19 is a ppd of $49^3 - 1$ but 19 is not a basic ppd.

Existence of primitive prime divisors

Theorem (Zsigmondy 1892)

Let b, e be positive integers with $b \geq 2$, $e \geq 3$ and $(b, e) \neq (2, 6)$, then $b^e - 1$ has a primitive prime divisor.

Theorem (Hering and Feit (1974, 1988))

If $b \geq 2, e \geq 3$ then $b^e - 1$ has a large prime primitive divisor, except when

b	e
2	$4, 6, 10, 12, 18$
3	$4, 6$
5	6

ppd-elements

Definition

Let q be a prime power. Then $g \in \mathrm{GL}(n, q)$ is called a ppd(n,q;e)-element if $n/2 < e \leq n$ and $q^e - 1$ has a ppd s that divides $o(g)$.

Generic Parameters

Definition

We say that (X, n, q) are generic if $\Omega \leq X \leq \Delta$ and n and q are such that

- Ω contains a $\mathrm{ppd}(n, q; e_1)$ and a $\mathrm{ppd}(n, q; e_2)$-elements for some $n/2 < e_1 < e_2 \leq n$.
- Ω contains a basic $\mathrm{ppd}(n, q; e)$-element for some $n/2 < e \leq n$.
- Ω contains a large $\mathrm{ppd}(n, q; e)$-element for some $n/2 < e \leq n$.

Recognition Theorem

hypotheses

Let $G \leq \Delta(n, q)$ with $q = p^z$ and p prime, $n \geq 3$ and (Ω, n, q) generic.

- G acts absolutely irreducibly on $V = \mathbb{F}_q^n$
- G leaves invariant only the forms corresponding to $\Omega(n, q)$
- G contains $\mathrm{ppd}(n, q; e_1)$ and a $\mathrm{ppd}(n, q; e_2)$-element with $n/2 < e_1 < e_2 \leq n$
- there are e_3, e_4 with $n/2 < e_3, e_4 \leq d$ such that G contains a large $\mathrm{ppd}(n, q; e_3)$-element and a basic $\mathrm{ppd}(n, q; e_4)$-element.

Recognition Theorem

Theorem [N., Praeger [5]]

Suppose G satisfies the hypotheses. Then one of the following holds:

- [Classical Group]: G contains Ω
- [extension field example]: there is a prime divisor b of n and $G \sim H \leq \mathrm{GL}(n/b, q^b).b$.
- [nearly simple example]: $G' = \mathrm{PSL}(2, r)$, for a prime r with $n = \frac{r\pm1}{2}$, $e_1 = \frac{r-3}{2}$, $e_2 = \frac{r-1}{2}$ with ppds $s_1 = \frac{r-1}{2}$ and $s_2 = r$, or G' is one of the groups in Table 1.

Table 1

G'	n	e_1	e_2	r_1	r_2	$p = q$
$2 \cdot A_7$	4	3	4	7	5	$p \geq 23$
A_7	4	3	4	7	5	$p = 2$
M_{11}	5	4	5	7	11	$p = 3$
$2 \cdot M_{12}$	6	4	5	7	11	$p = 3$
M_{23}	11	10	11	11	23	$p = 2$
M_{24}	11	10	11	11	23	$p = 2$

The proof is based on:

Guralnick, Penttila, Praeger, Saxl. “Linear groups with orders having certain large prime divisors”. *J Proc. London Math. Soc.* (3) 78, 1999.

Properties of ppd-elements

Let g be a $\mathrm{ppd}(n, q; e)$-element in $\mathrm{GL}(n, q)$. Let $f(x)$ be its characteristic polynomial. Then

- $f(x)$ has an irreducible factor of degree e.
- V as $\langle g \rangle$-module has an irreducible $\langle g \rangle$-submodule W of dimension e.

Test whether a matrix is a ppd(n,q;e)-element

Algorithm 1: IsPPD

Input: q and $g \in \mathrm{GL}(n, q)$
Output: (e,large) or (e,not large) or false, $e > n/2$
if Char(g) *has no irr. fact. c of deg.* $e > n/2$ **then return** *false*;
$PPDs := q^e - 1$;
for $i = 1 \dots e - 1$ **do**
    $m :=$ Gcd($PPDs, q^i - 1$);
    $PPDs := PPDs/m$;
end
$PPDs$ contains all ppds with multiplicity; # M contains no pdds;
$M := (q^e - 1)/PPDs$; $y := x^M \pmod{c(x)}$;
if $y = 1$ **then return** *false*;
if $y^{(e+1)} \neq 1$ **then return** e, *large*;
return e, *not large* ;

Satz

The costs of ISPPD *are:*

1. $O(n^2 \log^2(q))$ *per* GCD *computation*
2. $O(n^3 \log^2(q))$ *for the loop for PPDs and M*
3. $O(n^3 \log(q))$ *for the characteristic polynomial*
4. $O(n^3 \log(q))$ *to factor the char. pol.*
5. $O(\log(M))$ *polynomial multiplications for* x^M*. As* $M \leq q^n - 1$ *these are at most* $O(n \log(q))$ *polynomial multiplications.*
6. $O(\log(n))$ *polynomial multiplications for* $y^{(e+1)}$*.*

As we work in $\mathbb{F}[x]/(c(x))$, polynomials have degree $e \leq n$. Polynomial multiplication and reduction modulo $c(x)$ costs $O(n^2 \log(q))$.

The costs of IsPPD are:

1. $O(n^2 \log^2(q))$ per GCD computation
2. $O(n^3 \log^2(q))$ for the loop for PPDs and M
3. $O(n^3 \log(q))$ for the characteristic polynomial
4. $O(n^3 \log(q))$ to factor the char. pol.
5. $O(\log(M))$ polynomial multiplications for x^M. As $M \leq q^n - 1$ these are at most $O(n \log(q))$ polynomial multiplications.
6. $O(\log(n))$ polynomial multiplications for $y^{(e+1)}$.

Total costs

$$O(n^3 \log(q)^2)$$

Proportion of $\mathrm{ppd}(n, q; e)$-elements

Theorem [N. & Praeger]

Let $n/2 < e \leq n$. Let $\Omega \leq G \leq \Delta$. The proportion $p_{\mathrm{ppd}(n,q;e)}$ of $\mathrm{ppd}(n, q; e)$-elements in G satisfies

$$\frac{1}{e+1} \leq p_{\mathrm{ppd}(n,q;e)} \leq \frac{1}{e}$$

Theorem

RECOGNISEΩ is a 1-sided Monte-Carlo algorithm with error probability ε. If the algorithm is called with $G \leq \Delta$ and ε and

- G fixes only the forms corresponding to Ω
- G acts absolutely irreducibly
- (Ω, n, q) are generic

and returns *true*, then $\Omega \leq G$. The probability that the algorithm returns false even though $\Omega \leq G$ is at most ε.

Complexity

The complexity of the algorithm is

$$O(\log(\varepsilon^{-1})(\xi + n^3 \log^2(q))),$$

where ξ is the cost for selecting a random element.

Black Box recognition of classical groups

A Monte-Carlo algorithm of Babai, Kantor, Pálfy and Seress [2] for:

Input: G and p.
G a Black-box group isomorphic to a finite, simple group of Lie type in characteristic p and N an upper bound for the length of the input.
Output: The name of G.

runtime: polynomial in the length the input.

generic version for classical groups

Definition

Let G be isomorphic to a finite simple classical group of Lie type. Let n be the natural dimension of the underlying vector space of characteristic p. Suppose p is known. We call G generic, if $p > 2$, $n > 12$, and if $G = \mathrm{SL}(n, q)$, then $q \geq 4$.

Problem

We cannot derive any information about a black-box group from the operation on the underlying vector space.

The groups

The finite, simple classical groups of Lie type are:

- *linear groups:* $\mathrm{PSL}(n, q)$.
- *symplectic groups:* $\mathrm{PSp}(n, q)$, n even.
- *orthogonal groups:* $\mathrm{P}\Omega^{\epsilon}(n, q)$,

$$\epsilon = \begin{cases} \pm & n \text{ even} \\ \circ & n \text{ odd (then also } q) \end{cases}.$$

- *unitary groups:* $PSU(n, q)$, over $\mathbb{F}_{q^2}$.

Idea:

Compute invariants of the groups, which assist in differentiating between the groups.

formulas for the orders of $P\Omega$

Theorem

Let $P\Omega$ be one of the finite simple classical groups of Lie type in characteristic p with $q = p^a$ given before and $n \geq 2$. Then

$$|P\Omega| = \frac{1}{\ell} q^h P(q),$$

$P\Omega$	ℓ	h	$P(q)$
$PSL(n,q)$	$(n, q-1)$	$\binom{n}{2}$	$\prod_{i=2}^{n}(q^i - 1)$
$PSp(2m,q)$	$(2, q-1)$	m^2	$\prod_{i=1}^{m}(q^{2i} - 1)$
$P\Omega^\circ(2m+1,q)$	$(2, q-1)$	m^2	$\prod_{i=1}^{m}(q^{2i} - 1)$
$P\Omega^+(2m,q)$	$(4, q^m-1)$	$m(m-1)$	$(q^m - 1)\prod_{i=1}^{m-1}(q^{2i} - 1)$
$P\Omega^-(2m,q)$	$(4, q^m-1)$	$m(m-1)$	$(q^m + 1)\prod_{i=1}^{m-1}(q^{2i} - 1)$
$PSU(n,q)$	$(n, q+1)$	$\binom{n}{2}$	$\prod_{i=2}^{n}(q^i - (-1)^i)$

Definition

A $\mathrm{ppd}(p, k)$-element in G is an element of order divisible by a primitive prime divisor r of $p^k - 1$.

The Invariants

$$|G| = \frac{1}{\ell} q^h P(q)$$

Then we define

- e_1 largest k, for which G has $\mathrm{ppd}(p,k)$-elements
- e_2 2. largest k, for which G has $\mathrm{ppd}(p,k)$-elements
- w $e_1/(e_1 - e_2)$

In particular, z divides all the e_i.

Invariants for $\mathrm{PSL}(n, q)$ and $\mathrm{PSp}(n, 2)$

group	e_1	e_2	e_3	w
$\mathrm{PSL}(n, q)$	n	$n-1$	$n-2$	n
$\mathrm{PSp}(n, q)$	n	$n-2$	$n-4$	$n/2$

Tabelle: Extract from Table 1 in [2], $q = p^z$

Proposition 3 in [2]

Proposition

There are at most 7 groups with the same invariants e_1 and e_2.

Hence except for $\mathrm{PSp}(2m, p^z)$ and $\mathrm{P}\Omega^{\circ}(2m+1, p^z)$ Babai et al. can distinguish all groups. For these two there exists an algorithm of Altseimer and Borovik.

Cost

The total cost is dominated by

- costs to compute e_1 and e_2
- cost to choose $N \log(\varepsilon^{-1})$ random elements which need to be tested for the ppd-property.

The cost to compute e_1 is

$$O(\sqrt{N} \log(\varepsilon^{-1})\xi + \sqrt{N}(N^2 \log(p) + Nz^2 \log(p))\mu).$$

μ is to cost of a Black-Box operation and ξ is the cost for selecting a random element.

Total Cost

is polynomial in $N, \log(p)$, $\log(\varepsilon^{-1})$ and μ.

Finding the characteristic

Liebeck & O'Brien [4] and Kantor & Seress [3] introduce algorithms which determine the characteristic of a finite, simple group G of Lie-type .
Let $\mathrm{ch}(G)$ the characteristic of G.

Finding the characteristic

Liebeck & O'Brien [4] prove that in a black box group G with input length N and an order oracle, the characteristic of G can be determined using $O(N)$ random elements. The order oracle is only sometimes required.

The three largest element orders

Now we present the idea of the algorithm in [3].
Let $m_1(G)$, $m_2(G)$ and $m_3(G)$ be the largest, second largest and third largest element orders in a finite, simple group G of Lie type. Then Kantor and Seress proved:

Theorem [Kantor and Seress [3]]

Let G and H be finite, simple groups of Lie type. If $m_i(G) = m_i(H)$ for $i = 1, 2, 3$, then $\mathrm{ch}(G) = \mathrm{ch}(H)$.

The algorithm of Kantor and Seress is a Monte Carlo algorithm which

- takes as input an absolutely irreducible subgroup G of $\mathrm{GL}(n, p^a)$ such that $G/Z(G)$ a finite simple group of Lie type
- returns a list of numbers containing the characteristic of G
- uses $O(\log^2(n)\log\log(n))$ random elements
- uses $O^{\sim}(n^3)$ field operations in $\mathbb{F}_{p^a}$
- supposes all primes at most $3n$ are known.

The list might have $O(n)$ elements. For $n < 3 \cdot 10^5$ it only has 1 entry.

Literature I

Christine Altseimer, Alexandre V. Borovik.
Probabilistic recognition of orthogonal and symplectic groups.
Groups and computation, III (Columbus, OH, 1999), 1–20, Ohio State Univ. Math. Res. Inst. Publ., 8, de Gruyter, Berlin, 2001.

L. Babai, W.M. Kantor, P.P. Pálfy, Á. Seress
Black-box recognition of finite simple groups of Lie type by statistics of element orders.
J. Group Theory 5 (2002), 383–401.

Literature II

William M. Kantor and Ákos Seress.
Large element orders and the characteristic of Lie-type simple groups.
Journal of Algebra 322 (2009), 802–832.

Martin W. Liebeck, E.A. O'Brien.
Finding the characteristic of a group of Lie type.
J. Lond. Math. Soc. (2) 75 (2007), no. 3, 741–754.

Alice C. Niemeyer, Cheryl E. Praeger.
A recognition algorithm for classical groups over finite fields.
Proc. London Math. Soc. (3) 77, 1998, 117–169.

C_6: Normalisers of extra special groups

Extra Special Groups

Let r be a prime. (Here r odd.)

Definition

Let R be an r-group. Then

- R is extra special if $Z(R) = \Phi(R) = R' \cong \mathbb{Z}_r$.
- R is of symplectic-type if all of its characteristic abelian subgroups are cyclic.

One can prove that $|G| = r^{2m+1}$ for some positive integer m.

Extra Special Groups of exponent r

Let r be a prime. (Here r odd.)

- There are (up to isomorphism) two extra-special groups of order r^3, namely one of exponent r and one of exponent r^2.
- Extra special groups of exponent r and order r^{2m+1} are central products of m extra special groups of order r^3 and exponent r.

C_6

The groups G we consider here are subgroups of $\mathrm{GL}(n, q)$ are normalisers of extra-special r groups R of symplectic-type of order r^{1+2m} (when r odd) with

- exponent of R is r
- R acts absolutely irreducibly on V, i.e. $n = r^m$
- G not conjugate to a subgroup defined over a smaller field

When r is odd, the groups are subgroups of $R.\mathrm{Sp}(2m, r)$

C_6

The case for $m = 1$ treated in [3].

- If $G \leq R.\mathrm{Sp}(2, r)$ use knowledge of all subgroups of $\mathrm{Sp}(2, r)$ to construct element $a \in R \backslash Z(R)$.
- Construct a generating set $\langle a, b \rangle$ for R using commutators of a with particularly chosen other elements.
- change basis of V
- test whether G normalises R
- complexity $O(\log(\varepsilon^{-1})(\xi + \log\log(r) + \log(q))\mu + \omega)$, where ξ cost of random element, μ group operation and ω finding r-th root in $\mathbb{F}_q$.

C_6

The case for $m > 1$ treated in [2].
It uses an idea by Babai & Beals [1] called Blind Descent

Blind Descent

Let G be a black box group. Goal: construct an element $g \in G$ which lies in a proper normal subgroup N of G but not in $Z(G)$.

Algorithm 2: BLINDDESCENT

Input: G Black Box Group
Output: $g \in G$
$c_0 := Random(G)$; (not in $Z(G)$);
for $i = 1$ *to* M **do**
    $g_i := Random(G)$;
    $c_i := [c_{i-1}, g_i]$;
    if $c_i \in Z(G)$ **then**
        Find random $x \in G$ such that $c_i := [c_{i-1}, g_i^x] \notin Z(G)$;
    end
end
return c_M;

Blind Descent

- if any g_i belongs to a proper normal subgroup, then so does the output of BLINDDESCENT.
- if the probability in G of finding an element in a proper normal subgroup is c then the algorithm succeeds in time $O(\log(\varepsilon^{-1})c^{-1})$.

C_6

- Las Vegas reduction algorithm in [2], i.e. the algorithm computes $\varphi : G \to H$ where here $H \leq G/Z(G)$.
- The case for $m > 1$ uses an adaption of BLINDDESCENT to find an element in R but not in $Z(R)$.
- Analysed when full symplectic group on top. Then
- Complexity $O(\log(\varepsilon^{-1})(\xi + n^4\rho_{\mathbb{F}}))$, where ξ cost of obtaining a random element and $\rho_{\mathbb{F}}$ the cost of a field operation.

For Further Reading I

Lásló Babai and Robert Beals
A polynomial-time theory of black box groups I
Groups St. Andrews, 1997 in Bath, Eds: Campbell, Robertson, Ruskuc and Smith, London Math. Soc. Lecture Notes Series 260.

Peter Brooksbank, Alice C. Niemeyer, Ákos Seress
A reduction algorithm for matrix groups with an extraspecial normal subgroup
Finite geometries, groups, and computation, 1–16, Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

For Further Reading II

Alice C. Niemeyer
Constructive recognition of normalizers of small extra-special matrix groups
Internat. J. Algebra Comput. 15 (2005), no. 2, 367–394.