Using modular Lie algebras to compute with algebraic groups

Scott H. Murray

July 24, 2005

Joint work with Don Taylor (University of Sydney),
Arjeh Cohen and Sergei Haller (Technical University of Eindhoven)

Linear algebraic groups

A subgroup of $\mathrm{GL}_n(k)$ defined by polynomial equations

eg: $\mathrm{GL}_n(k)$, $\mathrm{SL}_n(k)$,
group of lower triangular matrices,
group of lower unitriangular matrices

We are mostly interested in reductive groups, for now

Lie “correspondence”

Char 0: connected linear algebraic groups $\longleftrightarrow$ Lie algebras

This breaks down in characteristic p

The classification uses algebraic geometry and group theory
These are not very useful for computation

Conjugating semisimple elements

G connected reductive linear algebraic group over k
T_0 standard maximal torus

$s \in G(\bar{k})$ semisimple

Wish to find $\quad x \in G(\bar{k}) \quad$ s.t. $\quad s^x \in T_0$

Outline algorithm

- $L = L(G), \quad M = C_L(s)$
- H a Cartan subalgebra of M [de Graaf]
- find Chevalley bases of L w.r.t. H and H_0
- we now have $a \in \mathrm{Aut}(L)$ s.t. $H^a = H_0$
- decompose $a = xb$ s.t. $x \in G(\bar{k})$ and $H_0^b = H_0$
- now $s^x \in T_0$

Rational conjugation

Rational tori:
T_w for w a class representatives in the Weyl group W

$s \in G(k)$ semisimple

Wish to find $x \in G(k)$ and $w \in W$ s.t. $s^x \in T_w$

Outline algorithm

- $L = L(G), \quad M = C_L(s)$
- H a maximally split Cartan subalgebra of M
- find w corresponding to H
- find "standard" bases of L w.r.t. H and $H_w = L(T_w)$
- we now have $a \in \mathrm{Aut}(L)(k) \quad$ s.t. $\quad H^a = H_w$
- decompose $\ a = xb \quad$ s.t. $\quad x \in G(k)$ and $H_w^b = H_w$
- now $s^x \in T_w$

Computing a splitting Cartan subalgebra

k finite
$L = L(G)$ for some k-split connected reductive G

Outline algorithm

- repeatedly take random semisimple $s \in L$ until $M = C_M(s)$ is split
- recurse until M is a torus

First wish: restriction map

Efficient computation of the p-map

$[x^p, y] = (\mathrm{ad}\, x)^p y \quad \Longrightarrow \quad$ can compute $x^p + Z(L)$ in time $O(d^3 \log(p))$

the s_i involve at least $O(p)$ Lie multiplications

Second wish: recognition

- Statistical
- Name
- Constructive

Characteristics 2 and 3

Third wish: automorphisms

Find the automorphism group of a Lie algebra
Decompose automorphisms

References

- de Graaf, Ivanyos, and Rónyai,
  Computing Cartan subalgebras of Lie algebras,
  Appl. Algebra Engrg. Comm. Comput. **7**(5) 339–349
- Cohen and Murray,
  Algorithm for Lang's Theorem,
  `www.win.tue.nl/~smurray`