

Computing in groups of Lie type with Lie algebras

Scott H. Murray

August 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 $GL_n(k)$ defined by polynomial equations

eg: $GL_n(k)$, $SL_n(k)$,

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

Jordan decomposition

semisimple matrix: has a basis of eigenvectors over \bar{k}
unipotent matrix: all eigenvalues 1

Also makes sense in a linear algebraic group
ie, independent of the embedding into GL

$$g \in G(k) \implies g = su \text{ uniquely with}$$

- s semisimple in $G(k)$
- u unipotent in $G(k)$
- $su = us$

Conjugating semisimple elements

G connected reductive linear algebraic group over k

T_0 standard maximal torus

Extend to the algebraic closure \bar{k}

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

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

Outline algorithm

- $L = L(G)$, $M = C_L(s)$
- H a Cartan subalgebra of M [de Graaf, Ivanyos, Rónyai]
- find Chevalley bases of L w.r.t. H and H_0
- we now have $a \in \text{Aut}(L)$ 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

- $L = L(G)$, $M = C_L(s)$
- 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 $a \in \text{Aut}(L)(k)$ s.t. $H^a = H_w$
- decompose $a = xb$ s.t. $x \in G(k)$ and $H_w^b = H_w$
- now $s^x \in T_w$

Computing a maximally split 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 as split as L
- recurse until M is a torus

Application: Conjugation

The conjugacy problem for semisimple elements needs

- conjugacy into a torus
- orbits of W on the torus

For unipotent elements:

Need to find a torus stabilising a given flag

Application: Sylow subgroups 1

$$(r, p) = 1$$

All r -Sylow subgroups in the normaliser of a rational torus

The normaliser of a rational torus is contained in the Weyl group,
so easy to deal with

Application: Sylow subgroups 2

Also need:

- to find a class of rational tori corresponding to each r [Broué & Malle]
- to ensure that we embed our Sylow in the right class
- r or p less than 5 [Bäärnhielm]

Stather has done the classical groups

Application: Lang's theorem

Given the orbits of $G(\bar{k})$ on $X(\bar{k})$,
Lang's Theorem lets you compute the orbits of $G(k)$ on $X(k)$

References

- de Graaf, Ivanyos, and Rónyai, *Computing Cartan subalgebras of Lie algebras*, Appl. Algebra Engrg. Comm. Comput. **7** (1996) 339–349
- Cohen, Murray, and Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), 1477–1498
- Broué and Malle, *Théorèmes de Sylow génériques pour les groupes réductifs sur les corps finis*, Math. Ann. **292** (1992), 241–262
- Cohen and Murray, *Algorithm for Lang’s Theorem*, www.win.tue.nl/~smurray