

Algorithm for Lang's theorem

Scott H. Murray

December 15, 2004

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

Examples: $GL_n(k)$, $SL_n(k)$,
classical groups,
group of lower triangular matrices,
group of lower unitriangular matrices

This is a generalisation of a Lie group

Rationality

G a linear algebraic group

If the polynomial equations have coefficients in k ,
 G is defined over k

For K/k , define $G(K)$ to be the solutions in K
These are called rational points

Example

$$k = \mathbb{R}$$

$$U_1 = \{x \mid x = \bar{x}^{-1}\}$$

$$U_1(\mathbb{R}) = \{x \in \mathbb{C} \mid |x| = 1\}$$

$$U_1(\mathbb{C}) = \mathbb{C}^\times$$

$$GL_1 = \{x \mid x = \bar{x}\}$$

$$GL_1(\mathbb{R}) = \{x \in \mathbb{R} \mid x \neq 0\}$$

$$GL_1(\mathbb{C}) = \mathbb{C}^\times$$

Reductive groups

No closed normal unipotent subgroups

Classified by Dynkin diagrams and associated lattices

Type A: $GL_n(k)$, $SL_n(k)$, etc

Type C: symplectic groups $Sp_{2n}(k)$

Types B and D: orthogonal groups

Types E, F, G: exceptional groups

Type G_2 includes automorphisms of the Octonians

Row reduction in $GL_n(k)$

$$\begin{pmatrix} -6 & 4 & -2 & 2 \\ -6 & 11 & -4 & 4 \\ 28 & 5 & 1 & -2 \\ -29 & 26 & -8 & 10 \end{pmatrix}$$

Row reduction in $GL_n(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -1 & & 1 & \\ 5 & & & 1 \end{pmatrix} \begin{pmatrix} -6 & 4 & -2 & 2 \\ 6 & 3 & 0 & \\ 22 & 9 & -1 & \\ 1 & 6 & 2 & \end{pmatrix}$$

Row reduction in $GL_n(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -1 & & 1 & \\ 5 & & & 1 \end{pmatrix} \begin{pmatrix} & & & 2 \\ 6 & 3 & 0 & \\ 22 & 9 & -1 & \\ 1 & 6 & 2 & \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ -3 & 2 & -1 & 1 \end{pmatrix}$$

Row reduction in $GL_n(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -1 & 3 & 1 & \\ 5 & 2 & & 1 \end{pmatrix} \begin{pmatrix} & & & 2 \\ & 3 & & \\ 4 & & -1 & \\ -11 & & 2 & \end{pmatrix} \begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ & & & 1 \\ -3 & 2 & -1 & 1 \end{pmatrix}$$

Row reduction in $GL_n(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -1 & 3 & 1 & \\ 5 & 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} & & 2 & \\ & 3 & & \\ & & -1 & \\ -3 & & & \end{pmatrix} \begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -4 & & 1 & \\ -3 & 2 & -1 & 1 \end{pmatrix}$$

Row reduction in $GL_n(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -1 & 3 & 1 & \\ 5 & 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & & & \\ 3 & & & \\ & -1 & & \\ & & -3 & \end{pmatrix} \begin{pmatrix} & & 1 & \\ & 1 & & \\ & & 1 & \\ 1 & & & \end{pmatrix} \begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ -4 & & 1 & \\ -3 & 2 & -1 & 1 \end{pmatrix}$$

Lower unitriangular matrices

Define $x_{ij}(a) = I_n + aE_{ij}$ and $X_{ij} = \{x_{ij}(a) \mid a \in k\}$

Then

$$u = \prod_{0 \leq j < i \leq n} x_{ij}(t_\alpha)$$

$$\begin{pmatrix} 1 & & & & \\ 2 & 1 & & & \\ -4 & & 1 & & \\ -3 & 2 & -1 & 1 & \end{pmatrix} = x_{21}(2) x_{31}(-4) x_{41}(-3) x_{42}(2) x_{43}(-1)$$

Bruhat decomposition

$$\mathrm{GL}_n(k) = \bigcup_{w \in S_n} UH\dot{w}U_w$$

where

H = diagonal matrices

\dot{w} = permutation matrix of w

$$U = \prod_{j < i} X_{ij}$$

$$U_w = \prod_{\substack{j < i \\ jw > iw}} X_{ij}$$

Bruhat decomposition II

This generalises to every reductive group

$$G = \bigcup_{w \in W} UHwU_w$$

We have generalised row and column reduction to every group of Lie type with every highest weight representation

Rows/columns correspond to the weight vectors

Example: The symplectic group $\mathrm{Sp}_4(k)$

$$\mathrm{Sp}_4(k) = \{A \mid AJA^t = J\}$$

where

$$J = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{pmatrix}$$

Rows/columns are labelled $1, 2, \bar{2}, \bar{1}$

Root subgroups of $\mathrm{Sp}_4(k)$

$$x_{21}(a) = \begin{pmatrix} 1 & & & \\ a & 1 & & \\ & & 1 & \\ & & -a & 1 \end{pmatrix}$$

$$x_{\bar{2}1}(a) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ a & & 1 & \\ & a & & 1 \end{pmatrix}$$

$$x_{\bar{1}1}(a) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ a & & & 1 \end{pmatrix}$$

$$x_{\bar{2}2}(a) = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & a & 1 & \\ & & & 1 \end{pmatrix}$$

Row reduction in $\mathrm{Sp}_4(k)$

$$\begin{pmatrix} -2 & -2 & -1 & -1 \\ -5 & -3 & -2 & -2 \\ -3 & -7 & -2 & -3 \\ 14 & 27 & 9 & 11 \end{pmatrix}$$

Row reduction in $\mathrm{Sp}_4(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ 3 & & 1 & \\ -11 & 3 & -2 & 1 \end{pmatrix} \begin{pmatrix} -2 & -2 & -1 & -1 \\ -1 & 1 & 0 & \\ 3 & -1 & 1 & \\ 1 & & & \end{pmatrix}$$

Row reduction in $\mathrm{Sp}_4(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ 3 & & 1 & \\ -11 & 3 & -2 & 1 \end{pmatrix} \begin{pmatrix} & & -1 & \\ & 1 & 0 & \\ & -1 & 1 & \\ 1 & & & \end{pmatrix} \begin{pmatrix} 1 & & & \\ -1 & 1 & & \\ 2 & & 1 & \\ 2 & 2 & 1 & 1 \end{pmatrix}$$

Row reduction in $\mathrm{Sp}_4(k)$

$$\begin{pmatrix} 1 & & & \\ 2 & 1 & & \\ 3 & -1 & 1 & \\ -11 & 5 & -2 & 1 \end{pmatrix} \begin{pmatrix} & & -1 & \\ & 1 & & \\ & & 1 & \\ 1 & & & \end{pmatrix} \begin{pmatrix} 1 & & & \\ -1 & 1 & & \\ 2 & & 1 & \\ 2 & 2 & 1 & 1 \end{pmatrix}$$

Finite groups of Lie type

k a finite field

\bar{k} its algebraic closure

$G = G(\bar{k})$ a reductive group defined over k

$G(k)$ is a finite group of Lie type

This includes most finite simple groups

Finite fields

q a prime power

k the unique field of size q

k_r the unique extension of degree r in \bar{k}

$F : x \mapsto x^q$ is an automorphism of k_r

F has order r on k_r and generates the Galois group

Extend F coordinatewise to vectors, matrices, etc

$G(k)$ consists of the fixed points of F

$G(k_r)$ consists of the fixed points of F^r

Example: Conjugacy

$$\begin{aligned} g \in G(k) & \Leftrightarrow g = g^F \\ a^{-1}ga \in G(k) & \Leftrightarrow a^{-1}ga = (a^{-1}ga)^F \end{aligned}$$

Hence

$$a^{-1}ga = a^{-F}ga^F \quad \text{ie, } (a^F a^{-1})g = g(a^F a^{-1})$$

and so $a^F a^{-1}$ is in the centraliser of g

Lang's theorem

If G is a connected algebraic group over k , then

$$G \rightarrow G, \quad a \mapsto a^F a^{-1}$$

is onto

The F -conjugate of c by a is $a^{-F} c a$

Lang \iff every element is F -conjugate to the identity.

Minimum field degree

The *minimum field degree* of $g \in G(\bar{k})$ is the smallest r such that $g \in G(k_r)$

Suppose:

$c \in G$ has minimum field degree r

$c^{F^{r-1}} \cdots c^F c$ has order s

$c = a^{-F} a$ for some $a \in G$

Then a has minimum field degree rs

$$\left(c^{F^{r-1}} \cdots c^F c \right)^u = c^{F^{ru-1}} \cdots c^F c = a^{-F^{ru}} a^{F^{ru-1}} \cdots a^{-F^2} a^F a^{-F} a = a^{-F^{ru}} a.$$

General linear group: randomised

$$c \in \text{GL}_d(k_r)$$

Take

$$a = x + x^F c + x^{F^2} c^F c + \cdots + x^{F^{rs-1}} c^{F^{rs-2}} \cdots c^F c$$

for x a $d \times d$ matrix over k_{rs}

Then

$$a^F c = x^F c + x^{F^2} c^F c + \cdots + x^{F^{rs}} c^{F^{rs-1}} \cdots c^F c = a$$

General linear group: deterministic

$$c \in \text{GL}_d(k_r)$$

$$V(k) = k^d, \quad V(k_{rs}) = V(k) \otimes k_{rs}$$

$$E(k) = \{v \in V(k_{rs}) \mid v^F c = v\}$$

$$c = a^{-F} a \quad \iff \quad V(k)a = E(k)$$

choose bases for $V(k)$ and $E(k)$

write down a

General method

$$c \in G(k_r)$$

V a G -module defined over k

$$E(k) = \{v \in V(k_{rs}) \mid v^F c = v\}$$

$$c = a^{-F} a \quad \iff \quad V(k)a = E(k)$$

choose bases for $V(k)$ and $E(k)$

Problem 1: How do we find a

Problem 2: a may not exist!

Chevalley bases

V the adjoint representation, ie $V(k_{r,s})$ a $k_{r,s}$ -Lie algebra

Then $V(k)$ and $E(k)$ are isomorphic k -Lie subalgebras

The Chevalley bases are conjugate under $G(k_{r,s})$

This is constructive recognition for Lie algebras

Modular Lie algebras

Classification (Strade 98):

- Classical type
- Cartan type
- Melikian type (characteristic 3)
- ... (characteristic 2)