Bases for algebraic groups

Tim Burness

University of Southampton

Joint work with Bob Guralnick and Jan Saxl

Groups and Geometries Workshop
Banff International Research Station
September 5th 2012

Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group.

A subset B of Ω is a **base** if the pointwise stabilizer of B in G is trivial.

The **base size** of G, denoted $b(G)$, is the minimal size of a base for G.

Equivalently, if G is transitive with point stabilizer $H = G_\alpha$ then $b(G)$ is the minimal size of a subset X of G such that

$$\bigcap_{g \in X} g^{-1}Hg = 1$$

Examples

- G has a regular orbit on $\Omega \iff b(G) = 1$
- $G = S_n,\ \Omega = \{1, \ldots, n\} = [n] \implies b(G) = n - 1$
- $G = \mathrm{GL}(V),\ \Omega = V \implies b(G) = \dim V$

Finite permutation groups

A transitive group G is **primitive** if G_α is a maximal subgroup of G.

Suppose G is primitive and $|\Omega| = n$.

- **Bochert, 1889** If $G \neq S_n$ or A_n then $b(G) \leqslant n/2$
- **Liebeck, 1984** If $G \neq S_n$ or A_n then there exists an absolute constant c such that $b(G) \leqslant c\sqrt{n}$
- **Seress, 1996** If G is soluble then $b(G) \leqslant 4$

Theorem. If G is almost simple and **non-standard** then $b(G) \leqslant 7$, with equality if and only if $G = \mathrm{M}_{24}$ and $n = 24$.

Here G is **standard** if $G_0 = A_n$ and Ω is an orbit of subsets or partitions of $[n]$, or $G_0 = \mathrm{Cl}(V)$ is classical and Ω is an orbit of subspaces of V.

Algebraic groups

Let G be an affine algebraic group over $\overline{K} = K$, $\operatorname{char} K = p \geqslant 0$. Let Ω be a faithful G-variety.

We define three base-related measures for the action of G on Ω:

$b(G)$: **exact base size:** Minimal c such that there exist c points in Ω with trivial pointwise stabilizer

$b^0(G)$: **connected base size:** Minimal c such that there exist c points in Ω with finite pointwise stabilizer

$b^1(G)$: **generic base size:** Minimal c such that there exists an open subvariety Λ of Ω^c and the pointwise stabilizer of any c-tuple in Λ is trivial

Clearly $b^0(G) \leqslant b(G) \leqslant b^1(G)$.

An example

Suppose $G = \mathrm{GL}_n(K) = \mathrm{GL}(V)$ and $\Omega = V$. Then

$$b^0(G) = b(G) = b^1(G) = n$$

- $b(G) = n$: $B \subseteq V$ is a base if and only if it contains a basis of V
- $b^0(G) = n$: The pointwise stabilizer of any $d < n$ vectors contains a copy of $\mathrm{GL}_{n-d}(K)$
- Fix a basis $\{e_1, \ldots, e_n\}$ for V. An n-tuple

$$\Big(\sum_j a_{1j} e_j, \ldots, \sum_j a_{nj} e_j\Big) \in V^n \cong K^{n^2}$$

  is a base if and only if $\det(a_{ij}) \neq 0$, so the set of such tuples is open in the Zariski topology on V^n. Therefore $b^1(G) = n$.

Simple algebraic groups

Let G be a simple algebraic group, let $H \leqslant G$ be a closed subgroup and set $\Omega = G/H$. The following hold:

- $\dim G/\dim\Omega \leqslant b^0(G) \leqslant \dim H + 1$
- $b^0(G) \leqslant b^1(G) \leqslant b^0(G) + 1$
- If $H \neq 1$ is finite then $b^0(G) = 1$ and $b(G) = b^1(G) = 2$

Set $b^0(G) = c$ and $\Gamma = \Omega^c$, say $\bigcap_i G_{\alpha_i}$ is finite for $(\alpha_1, \ldots, \alpha_c) \in \Gamma$.

Define a morphism $\phi : G \to \Gamma$, $\phi(g) = (g\alpha_1, \ldots, g\alpha_c)$, so $\phi : G \to \overline{\phi(G)}$ is a dominant morphism of irreducible varieties. For $y \in \phi(G)$,

$$0 = \dim\phi^{-1}(y) \geqslant \dim G - \dim\overline{\phi(G)} \geqslant \dim G - \dim\Gamma$$

so $\dim G/\dim\Omega \leqslant b^0(G)$.

Let $G = \mathrm{Cl}(V)$ be a simple classical algebraic group and set $\Omega = G/H$, where H is a maximal closed subgroup of G. Assume $\dim H > 0$ and H acts irreducibly on V. Then either $b^0(G) = b(G) = b^1(G) = 2$, or

G	Type of H	Conditions	$b^0(G)$	$b(G)$	$b^1(G)$
SL_n	$\mathrm{GL}_{n/2} \wr S_2$		3	3	3
	Sp_n	$n = 6$	4	4	4
	Sp_n	$n \geqslant 8$	3	3	3
	SO_n	$p \neq 2$	2	2	3
Sp_n	$\mathrm{Sp}_{n/2} \wr S_2$	$n \geqslant 8$	3	3	3
	$\mathrm{Sp}_{n/3} \wr S_3$	$n = 6$	3	3	3
	$\mathrm{GL}_{n/2}$	$p \neq 2$	2	2	3
	G_2	$(n,p) = (6,2)$	4	4	4
SO_n	$\mathrm{O}_{n/2} \wr S_2$	$n \geqslant 8,\ p \neq 2$	2	2	3
		$n \geqslant 8,\ p = 2$	2	?	3
	$\mathrm{GL}_{n/2}$	$n \geqslant 10$	3	3	3
	G_2	$n = 7,\ p \neq 2$	4	4	4

Let $G = \mathrm{Cl}(V) = \mathrm{Cl}_n$ and set $\Omega = G/H$, where $H = G_U$ is the stabilizer of a d-space U, $d \leqslant n/2$. Assume H is maximal and set $k = \lceil n/d \rceil$.

- If $G = \mathrm{Sp}_n$ then one of the following holds:
  - $b^0(G) = b(G) = b^1(G) = k$
  - $(n, d) = (6, 2)$ and $b^0(G) = b(G) = b^1(G) = 4$
  - U is t.i., $d = n/2$ and $b^0(G) = b(G) = 4$, $b^1(G) = 5 - \delta_{2,p}$
- The case $G = \mathrm{SO}_n$ is similar.
- If $G = \mathrm{SL}_n$ and d divides n then

$$b^0(G) = b(G) = b^1(G) = \begin{cases} k+3 & \text{if } 1 < d = n/2 \\ k+2 & \text{if } 1 < d < n/2 \\ k+1 & \text{if } d = 1 \end{cases}$$

  Otherwise, if $d \nmid n$ then

$$k + 1 \leqslant b^0(G) = b(G) = b^1(G) \leqslant k + 2 + \delta_{3,k}$$

Let G be a simple exceptional algebraic group and set $\Omega = G/H$, where H is a maximal closed subgroup of G. Assume H is non-parabolic, $p \neq 2$ and $\dim H > 0$. Then either $b^0(G) = b(G) = b^1(G) = 2$, or

G	H^0	$b^0(G) = b(G)$	$b^1(G)$
E_8	A_1E_7	3	3
	D_8	2	3
E_7	A_1D_6	3	3
	T_1E_6	3	3
	A_7	2	3
E_6	F_4	4	4
	D_5T_1	3	3
	C_4	2	3
	A_1A_5	3	3
F_4	B_4	4	4
	D_4	3	3
	A_1C_3	2	3
G_2	A_2	3	3
	A_1A_1	2	3

Let G be a simple exceptional algebraic group and set $\Omega = G/H$, where $H = P_i$ is a maximal parabolic subgroup of G.

Then

$$c - 1 \leqslant b^0(G) \leqslant b^1(G) \leqslant c,$$

where c is defined in the table and an asterisk indicates that

$$b^0(G) = b(G) = b^1(G) = c$$

	$H = P_1$	P_2	P_3	P_4	P_5	P_6	P_7	P_8
$G = E_8$	4^*	3^*	3^*	3^*	3^*	3^*	4	5^*
E_7	5^*	4^*	4	3^*	3^*	4^*	6^*	
E_6	6^*	5	4^*	4	4^*	6^*		
F_4	5	4	4	5				
G_2	4	4						

Some corollaries

Let G be a simple algebraic group over $\overline{K} = K$, $\operatorname{char} K = p \geqslant 0$. Let Ω be a primitive G-variety with point stabilizer H.

Assume G is not a classical group in a subspace action. Then $b^1(G) \leqslant 6$, with equality if and only if

$$(G, H) = (E_7, P_7),\ (E_6, P_1) \text{ or } (E_6, P_6)$$

Let G be a classical group in a non-subspace action. Then $b^1(G) \leqslant 4$, with equality if and only if

$$(G, H) = (\mathrm{SL}_6, \mathrm{Sp}_6),\ (\mathrm{SO}_7, G_2)\ (p \neq 2) \text{ or } (\mathrm{Sp}_6, G_2)\ (p = 2)$$

There are infinitely many non-standard finite almost simple primitive permutation groups G with $b(G) = 6$.

A key lemma

Let G be a simple algebraic group and set $\Omega = G/H$ with H^0 reductive. Then $b^1(G) \leqslant c$ if
$$\dim x^H < (1 - c^{-1}) \dim x^G$$
for all $x \in H$ of prime order.

- We need H^0 reductive since the proof requires $x^G \cap H$ to be a finite union of H-classes.
- To check the condition $\dim x^H < (1 - c^{-1}) \dim x^G$ we need information on the fusion of H-classes in G:

  G **classical:** B. (2004) on non-subspace actions: Roughly speaking, $\dim x^H \lesssim \frac{1}{2} \dim x^G$ in most cases.

  G **exceptional:** Lawther (2008) on unipotent classes; Lawther, Liebeck, Seitz (2002) in general.

Involution-type subgroups

Suppose $p \neq 2$. A maximal subgroup H of G is an **involution-type** subgroup if $H = C_G(\tau)$ for some involution $\tau \in \mathrm{Aut}(G)$.

e.g. if $G = \mathrm{SL}_{2n}$ then H is of type $\mathrm{SL}_n \wr S_2$, Sp_{2n} or SO_{2n}
e.g. if $G = E_8$ then $H = A_1 E_7$ or D_8

Set $\Omega = G/H$, $H = C_G(\tau)$ an involution-type subgroup. Then

$$b(G) = 2 \iff \exists\, g \in G \text{ such that } C_G(\tau\tau^g) \text{ is inverted by } \tau \text{ and contains no involutions}$$

Lemma. There is a unique G-class C of involutions in $\mathrm{Aut}(G)$ that invert a maximal torus of G. Moreover, $G = C^2$.

In particular, if $\tau \in C$ then $u = \tau\tau^g$ is regular unipotent for some $g \in G$. Furthermore, τ inverts $C_G(u)$ and thus $b(G) = 2$.

Theorem. Assume $p \neq 2$ and set $\Omega = G/H$, where $H = C_G(\tau)$ is an involution-type subgroup.

If τ inverts a maximal torus of G then

- H has a (unique) regular orbit on Ω, so $b^0(G) = b(G) = 2$; and
- the generic 2-point stabilizer has order 2^r, where $r = \mathrm{rank}(G)$, so $b^1(G) = 3$.

If τ does not invert a maximal torus then $b^0(G) \geqslant 3$.

e.g. if $(G, H) = (E_7, A_7.2)$ and $p \neq 2$ then $b^0(G) = b(G) = 2$, $b^1(G) = 3$.

Alternative methods are required when $p = 2$:

If $(G, H) = (E_8, D_8)$ then $\dim x^H < \frac{1}{2} \dim x^G$ for all $x \in H$ of prime order, so $b^1(G) = 2$. However, if $(G, H) = (E_7, A_7.2)$ then $\dim x^H = \frac{1}{2} \dim x^G$ for certain involutions; the best we can do is $2 \leqslant b^0(G) \leqslant b^1(G) \leqslant 3$.

Finite groups of Lie type

Suppose G is simple, $K = \overline{\mathbb{F}}_p$ and H is σ-stable, where σ is a **Frobenius morphism** of G. Then $G_\sigma = \{g \in G \mid g\sigma = g\}$ is a finite group of Lie type over $\mathbb{F}_q$ for some p-power q, and G_σ acts on G_σ/H_σ.

Let $\mathbb{P}(G_\sigma, c)$ be the probability that a randomly chosen c-tuple in G_σ/H_σ is a base for G_σ. Two related base measures:

$b(G_\sigma)$: **exact base size** of G_σ on G_σ/H_σ

$b^\infty(G_\sigma)$: **asymptotic base size:** Minimal c s.t. $\mathbb{P}(G_\sigma, c) \to 1$ as $q \to \infty$

Our earlier work applies. For example:

- $b^1(G) = b^\infty(G_\sigma)$
- If $q > 2$ then $b^0(G) \leqslant b(G_\sigma)$
- If $q >> 2$ then $b(G_\sigma) \leqslant b^1(G)$