Bases, Pyber's conjecture and quasisimple groups

Joint work with Martin Liebeck

Melissa Lee

Imperial College London

8th August 2017

Definitions

Let G be a permutation group acting faithfully on a set Ω, with $|\Omega| = n$.

Definitions

Let G be a permutation group acting faithfully on a set Ω, with $|\Omega| = n$.

A base for G is a subset $B \subseteq \Omega$ such that $\bigcap_{b \in B} G_b$ is trivial.

Definitions

Let G be a permutation group acting faithfully on a set Ω, with $|\Omega| = n$.

A base for G is a subset $B \subseteq \Omega$ such that $\bigcap_{b \in B} G_b$ is trivial.

The size of the smallest possible base for G is called the base size of G, and is denoted $b(G)$.

Definitions

Let G be a permutation group acting faithfully on a set Ω, with $|\Omega| = n$.

A base for G is a subset $B \subseteq \Omega$ such that $\bigcap_{b \in B} G_b$ is trivial.

The size of the smallest possible base for G is called the base size of G, and is denoted $b(G)$.

Examples

- $G = S_n$, $b(G) = n - 1$
- $G = A_n$, $b(G) = n - 2$

In this talk, we will assume all of our groups have finite order, and that our actions are faithful.

A simple bound

Lemma

The base size $b(G)$ of the action of a permutation group G on a set Ω of size n satisfies

$$b(G) \geq \frac{\log |G|}{\log n}$$

A simple bound

Lemma

The base size $b(G)$ of the action of a permutation group G on a set Ω of size n satisfies

$$b(G) \geq \frac{\log |G|}{\log n}$$

Proof: Since the pointwise stabiliser of B is trivial, the action of each element $g \in G$ on Ω is determined by its action on the base B.

A simple bound

Lemma

The base size $b(G)$ of the action of a permutation group G on a set Ω of size n satisfies

$$b(G) \geq \frac{\log |G|}{\log n}$$

Proof: Since the pointwise stabiliser of B is trivial, the action of each element $g \in G$ on Ω is determined by its action on the base B. So for any base B,

$$|G| \leq n^{|B|} \Rightarrow |G| \leq n^{b(G)}$$

Therefore

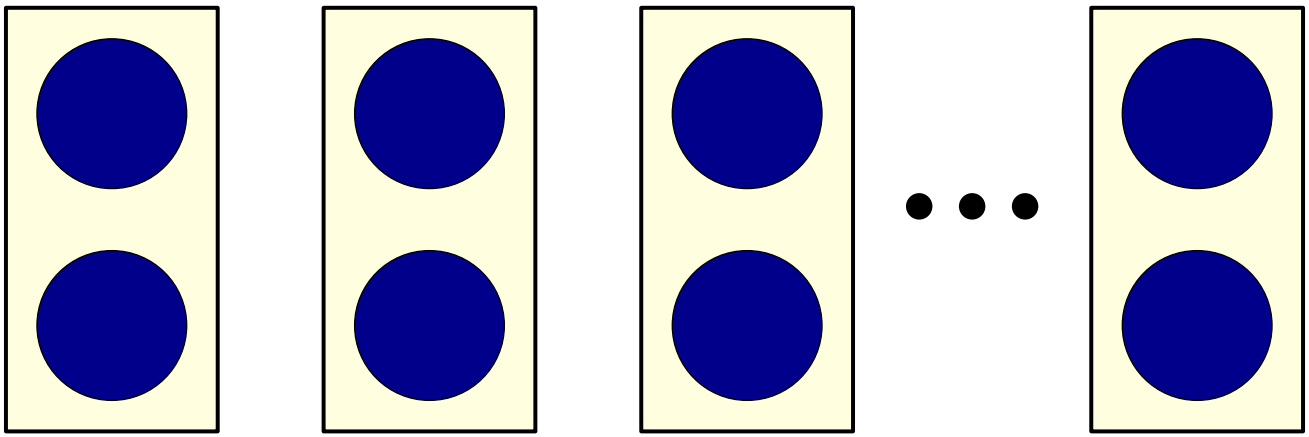
$$\frac{\log |G|}{\log n} \leq b(G).$$

Another example

$\mathbf{G = S_2 \wr C_k}$

- $b(G) = k$,

$$\frac{\log |G|}{\log n} = \frac{\log(2^k k)}{\log(2k)} = \frac{k + \log_2 k}{\log_2 k + 1}$$



Primitive groups

Suppose G is a finite permutation group acting transitively on Ω.

We say that G acts primitively on Ω if the only partitions of Ω preserved by G are $\{\Omega\}$ and $\{\{\omega\} \mid \omega \in \Omega\}$.

Primitive groups

Suppose G is a finite permutation group acting transitively on Ω.

We say that G acts primitively on Ω if the only partitions of Ω preserved by G are $\{\Omega\}$ and $\{\{\omega\} \mid \omega \in \Omega\}$.

Examples:

1. Primitive: S_k acting on t-sets from $\{1, \ldots, k\}$.
2. Imprimitive and transitive: $S_2 \wr S_k$ acting on k sets of size 2.
3. Imprimitive and intransitive: S_2^k acting on k sets of size 2.

Primitive groups

$\mathbf{G = S_k}$ acting on pairs of elements from $\{1, \ldots k\}$.

- Write $k = 3s + t$ with $0 \leq t \leq 2$

Primitive groups

$\mathbf{G = S_k}$ acting on pairs of elements from $\{1, \dots k\}$.

- Write $k = 3s + t$ with $0 \leq t \leq 2$
- $B = \{\{1, 2\}, \{2, 3\}, \{4, 5\}, \{5, 6\} \dots \{3s - 1, 3s\}\}$ (tack on $\{3s, 3s + 1\}$ if $t = 2$).
- $b(G) \leq \frac{2}{3}k + 1$

Primitive groups

$\mathbf{G = S_k}$ acting on pairs of elements from $\{1, \dots k\}$.

- Write $k = 3s + t$ with $0 \leq t \leq 2$
- $B = \{\{1, 2\}, \{2, 3\}, \{4, 5\}, \{5, 6\} \dots \{3s - 1, 3s\}\}$ (tack on $\{3s, 3s + 1\}$ if $t = 2$).
- $b(G) \leq \frac{2}{3}k + 1$
- **Halasi (2012):** If $k \geq 4$, then $b(G) = \lceil \frac{2k-2}{3} \rceil$

Primitive groups

$\mathbf{G = S_k}$ acting on pairs of elements from $\{1, \dots k\}$.

- Write $k = 3s + t$ with $0 \leq t \leq 2$
- $B = \{\{1,2\},\{2,3\},\{4,5\},\{5,6\} \dots \{3s-1, 3s\}\}$ (tack on $\{3s, 3s+1\}$ if $t = 2$).
- $b(G) \leq \frac{2}{3}k + 1$
- **Halasi (2012):** If $k \geq 4$, then $b(G) = \lceil \frac{2k-2}{3} \rceil$

$$\frac{\log |G|}{\log n} > \frac{\log(k!)}{\log(k^2)} \approx \frac{k}{2}$$

Affine groups

Let $V = V(d, q)$ be a d-dimensional vector space over $\mathrm{GF}(q)$.

- Both V and $\mathrm{GL}(V)$ act on V – define the general affine group $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$.

Affine groups

Let $V = V(d, q)$ be a d-dimensional vector space over $\mathrm{GF}(q)$.

- Both V and $\mathrm{GL}(V)$ act on V – define the general affine group $\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$.

Fact:

If $G = VG_0 \leq \mathrm{AGL}(V)$, with $G_0 \leq \mathrm{GL}(V)$, then G acts primitively on V if and only if G_0 acts irreducibly on V.

Such a group G is said to be primitive of affine type.

Some affine examples

Example 1

If $G = \mathrm{AGL}(V)$, then $b(G) = \dim V + 1$.

Some affine examples

Example 1

If $G = \mathrm{AGL}(V)$, then $b(G) = \dim V + 1$.

Example 2

$G = \mathrm{Sp}_{2k}(q)$, $V = V(2k, q)$.
Then $b(G) = 2k$,

$$\frac{\log |G|}{\log |V|} = \frac{\log(|\mathrm{Sp}_{2k}(q)|)}{2k \log q} \approx k$$

Uses for bases

Bases have been studied since the early days of permutation group theory.

Theorem (Bochert, 1889)

If G is a primitive permutation group of degree n which does not contain A_n, then $b(G) \leq n/2$.

Uses for bases

Bases have been studied since the early days of permutation group theory.

Theorem (Bochert, 1889)

If G is a primitive permutation group of degree n which does not contain A_n, then $b(G) \leq n/2$.

Theorem (Babai, 1981)

If G is a primitive permutation group of degree n which does not contain A_n, then $b(G) \leq 4\sqrt{n}\log n$.

Example: $G = S_k$ acting on pairs, $b(G) \approx 2k/3$, $n \approx k^2/2$

$$b(G) \leq k^2/4 \quad \text{vs.} \quad b(G) \leq 4\sqrt{2}k \log k$$

Uses for bases

Theorem (Babai, 1981)

If G is a primitive permutation group of degree n which does not contain A_n, then $b(G) \leq 4\sqrt{n}\log n$.

Recall that $|G| \leq n^{|B|}$:

Uses for bases

Theorem (Babai, 1981)

If G is a primitive permutation group of degree n which does not contain A_n, then $b(G) \leq 4\sqrt{n}\log n$.

Recall that $|G| \leq n^{|B|}$:

Corollary

If G is a primitive permutation group of degree n which does not contain A_n, then

$$|G| \leq n^{4\sqrt{n}\log n}$$

Uses for bases

- In recent times, bases have also been very useful in computational group theory.

- Knowing a base B for a permutation group G acting on a set Ω allows us to store each element of G as a $|B|$-tuple, rather than an $|\Omega|$-tuple.

Uses for bases

- In recent times, bases have also been very useful in computational group theory.

- Knowing a base B for a permutation group G acting on a set Ω allows us to store each element of G as a $|B|$-tuple, rather than an $|\Omega|$-tuple.

Theorem (Blaha, 1992)

Using a "greedy algorithm", we can find a base of a permutation group G of size $O(b(G)\log_2\log_2 n)$.

Uses for bases

- In recent times, bases have also been very useful in computational group theory.

- Knowing a base B for a permutation group G acting on a set Ω allows us to store each element of G as a $|B|$-tuple, rather than an $|\Omega|$-tuple.

Theorem (Blaha, 1992)

Using a "greedy algorithm", we can find a base of a permutation group G of size $O(b(G)\log_2\log_2 n)$.

Theorem (Blaha, 1992)

The problem of finding a base of minimal size for an arbitrary permutation group G is NP-hard.

Pyber's conjecture

From before:

$$n^{|B|} \geq |G| \Rightarrow \frac{\log |G|}{\log n} \leq b(G)$$

Pyber's conjecture

From before:

$$n^{|B|} \geq |G| \Rightarrow \frac{\log |G|}{\log n} \leq b(G)$$

Conjecture (Pyber 1993)

Let G be a primitive permutation group of degree n. Then there exists an absolute constant c such that

$$b(G) \leq c\frac{\log(|G|)}{\log n}$$

From the previous symplectic example, we see that we need $c \geq 2$.

Pyber's conjecture solved

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

The O'Nan-Scott Theorem

The O'Nan-Scott Theorem

A finite primitive permutation group G acting a set Ω falls into one of the following classes:

- Almost simple;
- Product type;
- Twisted wreath type;
- Diagonal type;
- Affine type.

The almost simple case

Suppose G is an almost simple group with socle G_0. A transitive action of G on a set Ω is standard if either:

1. G is a classical group acting on an orbit of subspaces of its natural module, or
2. $G_0 = A_n$ and Ω is an orbit of the set of k-subsets or partitions of $\{1, \ldots, n\}$.

The almost simple case

Suppose G is an almost simple group with socle G_0. A transitive action of G on a set Ω is standard if either:

1. G is a classical group acting on an orbit of subspaces of its natural module, or
2. $G_0 = A_n$ and Ω is an orbit of the set of k-subsets or partitions of $\{1, \ldots, n\}$.

Otherwise, the action is non-standard.

The Cameron-Kantor conjecture

Conjecture (Cameron, Kantor, 1993)

Suppose G is an almost simple primitive permutation group in a non-standard action. Then there exists a constant c such that $b(G) \leq c$.

The Cameron-Kantor conjecture

Conjecture (Cameron, Kantor, 1993)

Suppose G is an almost simple primitive permutation group in a non-standard action. Then there exists a constant c such that $b(G) \leq c$.

- The conjecture was established by Liebeck and Shalev in 1999
- Many authors contributed to determining c for various classes of almost simple groups.

The Cameron-Kantor conjecture

Theorem (Burness, O'Brien, Wilson, 2010; Burness, Liebeck, Shalev, 2009; Burness, 2007)

Suppose G is an almost simple group with socle G_0, and that G acts transitively on a set Ω.

1. If G_0 is sporadic or exceptional of Lie type, then $b(G) \leq 7$, with equality $\Leftrightarrow G = M_{24}$.
2. If G_0 is a classical group and the action of G is non-standard, then $b(G) \leq 5$.

Standard actions

Theorem (Benbenishty)

Pyber's conjecture holds for almost simple primitive permutation groups in standard actions.

S_k on pairs –revisited

$G = S_k$ acting on unordered 2-sets from $\{1, \dots k\}$.

$$b(G) = \lceil \frac{2k-2}{3} \rceil \leq \frac{4}{3} \frac{\log |G|}{\log n}$$

Back to Pyber's conjecture

Theorem (Duyan, Halasi, Maróti, 2016)

Let G be an almost simple primitive permutation group of degree n. Then

$$b(G) < 15\left(\frac{\log|G|}{\log n}\right)$$

Proving Pyber's conjecture

- **Product type:** Burness and Seress (2014): Pyber's conjecture holds. Duyan, Halasi and Maróti (2016):

$$b(G) \leq 9.16 \left(\frac{\log |G|}{\log n} \right) + 13 < (45/2) \left(\frac{\log |G|}{\log n} \right)$$

Proving Pyber's conjecture

- **Product type:** Burness and Seress (2014): Pyber's conjecture holds. Duyan, Halasi and Maróti (2016):

$$b(G) \leq 9.16 \left(\frac{\log |G|}{\log n} \right) + 13 < (45/2) \left(\frac{\log |G|}{\log n} \right)$$

- **Twisted Wreath type:** Burness and Seress (2014): Pyber's conjecture holds. Duyan, Halasi and Maróti (2016):

$$b(G) \leq 45 \left(\frac{\log |G|}{\log n} \right)$$

Proving Pyber's conjecture

- **Product type:** Burness and Seress (2014): Pyber's conjecture holds. Duyan, Halasi and Maróti (2016):

$$b(G) \leq 9.16 \left(\frac{\log |G|}{\log n} \right) + 13 < (45/2) \left(\frac{\log |G|}{\log n} \right)$$

- **Twisted Wreath type:** Burness and Seress (2014): Pyber's conjecture holds. Duyan, Halasi and Maróti (2016):

$$b(G) \leq 45 \left(\frac{\log |G|}{\log n} \right)$$

- **Diagonal type:** Fawcett (2013): Pyber's conjecture holds and

$$b(G) \leq \left\lceil \frac{\log |G|}{\log n} \right\rceil + 2 < 4 \left(\frac{\log |G|}{\log n} \right)$$

The affine case

Let $G = VG_0$ be a primitive group of affine type acting on V, and let $H = G_0 \leq \mathrm{GL}(V)$. Then G satisfies Pyber's conjecture if:

The affine case

Let $G = VG_0$ be a primitive group of affine type acting on V, and let $H = G_0 \leq \mathrm{GL}(V)$. Then G satisfies Pyber's conjecture if:

Seress (1996): H is soluble;

Gluck & Magaard (1998): The order of H is co-prime to the order of V;

Liebeck & Shalev (2002/2014): H has a primitive action on V;

Halasi & Maróti (2016): H is p-soluble;

The affine case

Let $G = VG_0$ be a primitive group of affine type acting on V, and let $H = G_0 \leq \mathrm{GL}(V)$. Then G satisfies Pyber's conjecture if:

Seress (1996): H is soluble;

Gluck & Magaard (1998): The order of H is co-prime to the order of V;

Liebeck & Shalev (2002/2014): H has a primitive action on V;

Halasi & Maróti (2016): H is p-soluble;

Theorem (Duyan, Halasi & Maróti (2016))

If G is a primitive permutation group of affine type of degree n, then

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

Improvements

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

Improvements

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

- Can we improve this coefficient of 45?

Improvements

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

- Can we improve this coefficient of 45?
- Down to 2?

Improvements

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

- Can we improve this coefficient of 45?
- Down to 2?
- Somewhere in between? And what is the constant c?

Improvements

Theorem (Duyan, Halasi & Maróti (2016))

There is a universal constant $c > 0$ such that $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 45\frac{\log|G|}{\log n} + c.$$

- Can we improve this coefficient of 45?
- Down to 2?
- Somewhere in between? And what is the constant c?
- To make improvements, we would need to improve the bounds in the product type, twisted wreath type and the affine type cases.
- Our focus is on the affine type groups.

A major case

G is quasisimple if it is perfect and $G/Z(G)$ is simple.

Examples: Simple groups, covers of sporadic or alternating groups

A major case

G is quasisimple if it is perfect and $G/Z(G)$ is simple.

Examples: Simple groups, covers of sporadic or alternating groups

$G = VG_0$ a primitive group of affine type, $G_0 \leq \mathrm{GL}(V) = \mathrm{GL}(n, q)$ with G_0 quasisimple and irreducible on V.

A major case

G is quasisimple if it is perfect and $G/Z(G)$ is simple.

Examples: Simple groups, covers of sporadic or alternating groups

$G = VG_0$ a primitive group of affine type, $G_0 \leq \mathrm{GL}(V) = \mathrm{GL}(n, q)$ with G_0 quasisimple and irreducible on V.

- We can find $b(G)$ by considering V as an $\mathbb{F}_q G_0$-module and finding $b(G_0)$.
- Then $b(G) = b(G_0) + 1$

Improvements

Theorem (M.L. & M.L. 2017)

Let $V = V(d, q)$, and $G \leq \mathrm{GL}(V)$ be quasisimple and act irreducible on V. Then one of the following holds:

1. $G = A_m$ and V is the natural A_m-module over $\mathbb{F}_q$ of dimension $d = m - \delta(p, m)$;
2. $G = Cl(d, q_0)$, a classical group with a d-dimensional natural module over a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$
3. $b(G) \leq 10$

Improvements

Theorem (M.L. & M.L. 2017)

Let $V = V(d, q)$, and $G \leq \mathrm{GL}(V)$ be quasisimple and act irreducible on V. Then one of the following holds:

1. $G = A_m$ and V is the natural A_m-module over $\mathbb{F}_q$ of dimension $d = m - \delta(p, m)$;
2. $G = Cl(d, q_0)$, a classical group with a d-dimensional natural module over a subfield $\mathbb{F}_{q_0}$ of $\mathbb{F}_q$
3. $b(G) \leq 10$

Theorem (Liebeck, Maróti, 2017)

Suppose V is a finite vector space, and let $H \leq \mathrm{GL}(V)$ be an irreducible, primitive linear group on V. Then

$$b(H) \leq 2\frac{\log|H|}{\log|V|} + 15$$

Improvements

Theorem (Halasi, Liebeck & Maróti (2017))

The base size $b(G)$ of a primitive permutation group G of degree n satisfies

$$b(G) < 2\frac{\log|G|}{\log n} + 20.$$

The multiplicative constant of 2 is optimal, from the symplectic example we had before.