Pyber's base size conjecture

Attila Maróti

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences,
Budapest, Hungary

Workshop on Permutation Groups: Methods and Applications,
Bielefeld, January 12-14, 2017

We will speak about a submitted paper entitled

A proof of Pyber's base size conjecture

written by Hülya Duyan, Zoltán Halasi and AM.

One can find the pdf on `ArXiv`.

Bases

Let G be a finite permutation group acting on a finite set Ω.

A subset Δ of Ω is called a base for G if $\cap_{\delta \in \Delta} G_\delta = 1$.

Bases played a key role in the development of permutation group theoretic algorithms (see Seress (2003)). But bases of special kinds also appear in representation theory.

Bases for general permutation groups

The minimal size of a base for G (acting on Ω of size n) is denoted by $b(G)$. It is easy to see that $2^{b(G)} \leq |G| \leq n^{b(G)}$.

Blaha (1992) showed that the problem of finding $b(G)$ is NP-hard. But one may approximate $b(G)$ by a greedy heuristic. The size of such a base is $O(b(G) \log \log n)$ where $n = |\Omega|$ (Blaha (1992)).

Pyber (1993) showed that there exists a universal constant $c > 0$ such that almost all (a proportion tending to 1 as $n \to \infty$) subgroups G of $\mathrm{Sym}(n)$ satisfy $b(G) > cn$.

Bounding the orders of primitive permutation groups

Let G be a primitive permutation group of degree n and not containing $\mathrm{Alt}(n)$. There are several bounds for $|G|$ ($\leq n^{b(G)}$) in the literature whose proof use bounds for $b(G)$.

- $b(G) \leq n/2$ (Bochert (1889)).
- If G is uniprimitive, then $b(G) < 4\sqrt{n}\log n$ (Babai (1981)).
- If G is doubly transitive, then $b(G) < 2^{c\sqrt{\log n}}$ for a universal constant $c > 0$ (Babai (1982)).
- If G is doubly transitive, then $b(G) < c(\log n)^2$ where c is a universal constant (Pyber (1993)).
- Using CFSG, groups G with $b(G) \geq 9\log n$ were classified by Liebeck (1984).

Cameron's conjecture

An ingredient of Liebeck's proof was a result stating that an almost simple primitive permutation group of degree n in its, later called, non-standard action has order at most n^9. This bound was later improved by Liebeck and his result showed that the Mathieu group M_{24} in its action on 24 points is the worst case.

Cameron and Kantor conjectured that an almost simple primitive permutation group in its non-standard action has bounded minimal base size, perhaps 7 with equality holding for M_{24}.

The first part of this conjecture was established by Liebeck and Shalev (1999) and the second half was completed in a series of papers by Cameron, Kantor (1993), Liebeck, Shalev (2003 and 2005), James (2006 and 2006), Burness (2007), Burness, Liebeck, Shalev (2009), Burness, O'Brien, Wilson (2010), and Burness, Guralnick, Saxl (2011).

Babai's conjecture

Let d be a fixed positive integer. Let Γ_d be the class of finite groups G such that G does not have a composition factor isomorphic to an alternating group of degree greater than d and no classical composition factor of rank greater than d.

Babai, Cameron, Pálfy (1982) showed that if $G \in \Gamma_d$ is a primitive permutation group of degree n, then $|G| < n^{f(d)}$ for some function $f(d)$. Babai conjectured that there is a function $g(d)$ such that $b(G) < g(d)$ whenever G is a primitive permutation group in Γ_d.

Seress (1996) showed this for G a solvable primitive group. Babai's conjecture was proved by Gluck, Seress, Shalev (1998). Later Liebeck, Shalev (1999) showed that in Babai's conjecture the function $g(d)$ can be taken to be linear in d.

Pyber's conjecture

The previous three slides suggest that the order of a primitive permutation group is closely tied to its minimal base size.

On one hand we have the trivial bound $\log|G|/\log n \leq b(G)$ (holding for any permutation group G).

Pyber's conjecture (1993).

There exists a universal constant c such that for a primitive permutation group G of degree n we have $b(G) \leq c(\log|G|/\log n)$.

This bound fails if we drop the assumption that G is primitive.

Non-affine primitive permutation groups

Theorem (Liebeck, Shalev (1999); Burness et al (2007, 2009, 2010, 2011); Benbenishty (2005)).

If G is an almost simple primitive permutation group of degree n, then $b(G) < 15(\log|G|/\log n)$.

A formula for $b(G)$ when G is a primitive group of diagonal type has been obtained by Fawcett (2013) (and an upper bound was given by Gluck, Seress, Shalev (1998)). Primitive permutation groups of product type or of twisted wreath product type were treated by Burness and Seress (2015). After working out the constants we obtain the following.

Theorem.

If G is a primitive permutation group of degree n and not of affine type, then $b(G) < 45(\log|G|/\log n)$.

Affine primitive permutation groups

For the rest of the talk we will consider Pyber's base size conjecture for affine primitive permutation groups.

Let H be a finite (linear) group acting faithfully and irreducibly on a finite vector space V. Pyber's conjecture amounts to showing that there exist universal constants c_1 and c_2 such that

$$b(H) \leq c_1(\log |H| / \log |V|) + c_2.$$

This has been known for

- H solvable (Seress (1996));
- H acting coprimely on V (Gluck, Magaard (1998), see also Halasi, Podoski (2016));
- H a p-solvable group where p divides $|V|$ (Halasi, M (2016));
- H acting primitively on V (Liebeck, Shalev (2002 and 2014));
- certain groups H acting imprimitively on V (Fawcett, Praeger (2016)).

The distinguishing number

A closely related invariant to the minimal base size is the distinguishing number (in the sense of Albertson and Collins).

Let G be a finite permutation group acting on a finite set Ω of order n. The minimal number of colors needed to color all the points in Ω in such a way that the stabilizer in G of this coloring is trivial is denoted by $d(G)$ and is called the distinguishing number of G.

A trivial observation is that $|G| < d(G)^n$ when $n > 1$. This gives the lower bound $\sqrt[n]{|G|} < d(G)$.

We wish to find a similar upper bound. It is natural to assume that G is transitive.

Bounding the distinguishing number, I

An equivalent form of a result of Burness and Seress (2015) is that there exists a universal constant c such that if G is a transitive permutation group of degree n then $d(G) \leq |G|^{c/n}$. This was used in the non-affine case of Pyber's conjecture.

We aim to give a stronger and explicit bound and that will directly be applied. Moreover we need a different proof. The ideas of this new proof are implicitly used in the proof of the affine case of Pyber's conjecture.

Bounding the distinguishing number, II

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group. Put $n = |\Omega|$. Let $\Gamma = \{\Delta_1, \ldots, \Delta_k\}$ be a system of blocks of imprimitivity for G with $|\Delta_i| = m$ for $1 \leq i \leq k$. Let $H_i = N_G(\Delta_i)$ for each i with $1 \leq i \leq k$, and $N = \cap_{j=1}^{k} H_j$. Then $H_i / C_G(\Delta_i) \leq \mathrm{Sym}(\Delta_i)$. Furthermore, G acts on Γ with kernel N, so $K := G/N \leq \mathrm{Sym}(\Gamma)$.

Lemma

If H_j acts trivially on Δ_j (i.e. $H_j = C_G(\Delta_j)$) for every $1 \leq j \leq k$, then $d(G) \leq \lceil \sqrt[m]{d(K)} \rceil$.

Lemma

Assume that G is transitive. Suppose that $d(H_1) \leq c$ for some constant c. Then $d(G) \leq c \cdot \lceil \sqrt[m]{d(K)} \rceil$.

c is small when H_1 acts primitively on Δ_1 such that $H_1 / C_{H_1}(\Delta_1)$ does not contain $\mathrm{Alt}(\Delta_1)$. For in this case Seress (1997) and Dolfi (2000) showed that $d(H_1) \leq 4$.

Bounding the distinguishing number, III

The result of Seress (1997) and Dolfi (2000) carries over to quasi-primitive groups. In fact we have the following.

Theorem

Let $M \lhd G \leq \mathrm{Sym}(\Omega)$ be transitive permutation groups where M is a direct product of isomorphic simple groups. Then $d(G) \leq 12$ or $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$.

Assume that the action of H_1 is large (following Burness and Seress (2015)) with $N \neq 1$. Then the socle of N is a subdirect product of isomorphic alternating groups. We write $\mathrm{Alt}(m)^{k/t} \leq N \leq \mathrm{Sym}(m)^{k/t}$ and call t the linking factor of N.

Lemma

Let us assume that H_1 is large and $N \neq 1$ with linking factor t. Then $d(G) \leq 3 \cdot \lceil \sqrt[t]{m} \rceil \cdot \lceil \sqrt[m]{d(K)} \rceil$.

Bounding the distinguishing number, IV

Theorem

Let G be a transitive permutation group acting on a finite set of size $n > 1$. Then $\sqrt[n]{|G|} < d(G) \leq 48\sqrt[n]{|G|}$.

Sketch of proof. From the previous slide we may assume that there exists a minimal normal subgroup M in G which does not act transitively on Ω. Let an orbit of M on Ω be Δ_1, and let Γ be the set of orbits of M on Ω. Let the size of Γ be k and let H_1 be the stabilizer in G of Δ_1. Since $M \triangleleft H_1$, the previous theorem implies that $d_{\Delta_1}(H_1) \leq 12$ or $\mathrm{Alt}(\Delta_1) \leq H_1/C_{H_1}(\Delta_1) \leq \mathrm{Sym}(\Delta_1)$.

Case 1. $d_{\Delta_1}(H_1) \leq 12$. We skip this part.

Bounding the distinguishing number, V

Case 2. $\mathrm{Alt}(\Delta_1) \leq H_1/C_{H_1}(\Delta_1) \leq \mathrm{Sym}(\Delta_1)$ with $|\Delta_1| = m \geq 13$. In this case the action of H_1 on Δ_1 is large. Let the kernel of the action of G on Γ be N. Since $M \leq N$, we know that $N \neq 1$. Set $\epsilon = 1$ if $t = 1$ and $\epsilon = 2$ if $t \neq 1$. We have the following.

$$d(G) \leq 3\lceil \sqrt[t]{m} \rceil \lceil \sqrt[m]{d(K)} \rceil \leq 6\epsilon \sqrt[t]{m} \sqrt[m]{d(K)} = 6\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)}.$$

Set $c = 6 \cdot 2^{1/mt} \cdot 3^{1/t}$. By use of $\frac{1}{2}(m/3)^m < m!/2 = |\mathrm{Alt}(m)|$, we have that $d(G)$ is at most

$$6\epsilon \sqrt[mk]{m^{mk/t}} \sqrt[m]{d(K)} < 6\epsilon \sqrt[mk]{((m!/2) \cdot 2 \cdot 3^m)^{k/t}} \sqrt[m]{d(K)} \leq$$

$$\leq c \cdot \epsilon \sqrt[n]{(|\mathrm{Alt}(m)|)^{k/t}} \sqrt[m]{d(K)}.$$

We know that $\mathrm{Alt}(m)^{k/t} \leq N$. This gives the inequality $d(G) < c \cdot \epsilon \sqrt[n]{|N|} \sqrt[m]{d(K)}$. By the induction hypothesis, we have $d(K) \leq 48 \sqrt[k]{|K|}$. Thus

$$d(G) < c \cdot \epsilon \sqrt[m]{48} \sqrt[n]{|N|} \sqrt[n]{|K|} \leq 6 \cdot \epsilon \cdot 2^{1/13t} 3^{1/t} \sqrt[13]{48} \sqrt[n]{|G|} < 48 \sqrt[n]{|G|}.$$

Reducing to imprimitive linear groups

Let $H \leq GL(V)$ act irreducibly on V.

Liebeck, Shalev (2002 and 2014)

There exists a universal constant $c > 0$ such that if H acts primitively on V, then

$$b_V(H) \leq \max\{18\frac{\log|H|}{\log|V|} + 30\ ,\ c\}.$$

Therefore we may introduce the following notation. Let $V = \oplus_{i=1}^{t} V_i$ be a decomposition of V into a sum of subspaces V_i of V that is preserved by the action of H. For every i with $1 \leq i \leq t$, let $H_i = N_H(V_i)$ and let $K_i = H_i / C_{H_i}(V_i) \leq GL(V_i)$ be the image of the restriction of H_i to V_i. The group H acts on the set $\Pi = \{V_1, \ldots, V_t\}$ in a transitive way. Let N be the kernel of this action and let P be the image of H in $\mathrm{Sym}(\Pi)$. So $N = \cap_{i=1}^{t} H_i$ and $P \cong H/N$.

Reducing to the case when $b_{V_1}(K_1)$ is unbounded

Lemma

If $K_1 = 1$, then $b_V(H) = \lceil \log_{|V_1|} d_\Pi(P) \rceil$.

Theorem

Let us assume that $b_{V_1}(K_1) \leq b$ for some constant b. Then we have

$$b_V(H) \leq b + 1 + \log 48 + \frac{\log |P|}{\log |V|}.$$

Sketch of proof. By the previous lemma we have $b_V(H) \leq b + \lceil \log_{|V_1|} d_\Pi(P) \rceil$. Now apply $d_\Pi(P) \leq 48 \sqrt[t]{|P|}$.

Alternating-induced representations, I

Let $k \geq 5$ and let K be $\mathrm{Sym}(k)$ or $\mathrm{Alt}(k)$. Let U be the usual permutation module for K with permutation basis $\{e_1, \ldots, e_k\}$. Let U_0 be the submodule of such vectors whose augmentation is 0. This is irreducible if $p \nmid k$. When $p \mid k$, there is a 1-dimensional W such that U_0/W is irreducible.

We say that H is alternating-induced if $K_1 \cong K$ (with $k \geq 7$) and $V_1 \cong U_0$ (if $p \nmid k$) or $V_1 \cong U_0/W$ (if $p \mid k$).

The action of H on V may be described using the action of H on $U = \oplus_i U_i$ where U_i is a permutation module with basis $\{e_1^{(i)}, \ldots, e_k^{(i)}\}$.

Lemma

We have $b_V(H) \leq 2b_U(H) + 3$ for $k \geq 7$.

Alternating-induced representations, II

Theorem

If $H \leq GL(V)$ is an alternating-induced linear group, then

$$b_V(H) \leq 17 + 2(\log|H|)/(\log|V|).$$

Sketch of proof. Let H act on U by permuting (transitively) the basis $B = \{e_j^{(i)} \mid 1 \leq i \leq t,\ 1 \leq j \leq k\}$. Since any vector $u \in U$ can be seen as a coloring of this basis by using q (size of the field) colors, $b_U(H) \leq \lceil \log_q(d_B(H)) \rceil$. Apply the bound $d_B(H) \leq 48 \sqrt[kt]{|H|}$. Finally, apply the previous lemma.

(mod T)-representations, I

Definition

Let V be a finite vector space over $\mathbb{F}_q$ and $T \leq GL(V)$ any subgroup. We say that a map $X : H \to GL(V)$ is a $\pmod{T}$-representation of H if the following two properties hold:

(1) $X(g)$ normalizes T for every $g \in H$;

(2) $X(gh)T = X(g)X(h)T$ for every $g, h \in H$.

Linear representations and projective representations are examples of $\pmod{T}$-representations.

Definition

Let $T \leq GL(V)$ and $X_1, X_2 : H \to GL(V)$ be two $\pmod{T}$-representations of H. We say that X_1 and X_2 are $\pmod{T}$-equivalent if there is an $f \in N_{GL(V)}(T)$ such that $X_1(g)T = fX_2(g)f^{-1}T$ for all $g \in G$.

(mod T)-representations, II

We consider (mod T_V)-representations where $V = \oplus_{i=1}^t V_i$ and

$$T_V = \{g \in GL(V) \,|\, g(V_i) = V_i \text{ and } g|_{V_i} \in Z(GL(V_i)) \ \forall 1 \leq i \leq t\}.$$

This group is $\simeq (\mathbb{F}_q^\times)^t$.

If $X : H \to GL(V(p))$ is a (mod T_V)-representation, then the associated maps $X_i : H_i \to \Gamma L(V_i)$ are projective representations. Conversely, if $X_i : H_i \to \Gamma L(V_i)$ are equivalent projective representations, then the induced representation $X = \mathrm{Ind}_{H_1}^H(X_1) : H \to GL(V(p))$ (this can be uniquely defined up to (mod T_V)-equivalence) will be a (mod T_V)-representation of H transitively permuting the V_i, and it is easy to see that every (mod T_V)-representation of H transitively permuting the V_i can be obtained in this way.

Classical-induced representations without multiplicities, I

Let $X : H \to GL(V(p))$ be a $\pmod{T_V}$-representation of H. Notice that $X(H)T_V$ is a group. Assume that $X(H)T_V$ acts transitively on Π. We will consider its base size on V, denoted by $b_X(H)$.

Assume that X is classical-induced, i.e. the image K_i of the homomorphism $\mathfrak{X}_i : H_i \to P\Gamma L(V_i)$ is some classical group i.e. $S_i = \mathrm{soc}(K_i) \leq P\Gamma L(V_i)$ is isomorphic to some simple classical group $S = \mathrm{Cl}(k, q_0) \leq P\Gamma L(k, q)$ for $k \geq 9$ where $\mathbb{F}_{q_0}$ is some subfield of $\mathbb{F}_q$.

When $k \geq 9$ the group generated by all inner, diagonal and field automorphisms of S has index at most 2 in $\mathrm{Aut}(S)$.

Classical-induced representations without multiplicities, II

For any subset $\Delta \subseteq \Pi$ let $V_\Delta := \oplus_{V_i \in \Delta} V_i$, and $X_\Delta : N_H(\Delta) \to GL(V_\Delta(p))$ be the $\pmod{T_{V_\Delta}}$-representation of $N_H(\Delta)$ defined by taking the restriction of $X(h)$ to V_Δ for all $h \in N_H(\Delta)$. Furthermore, let the associated homomorphism $\mathfrak{X}_\Delta$ be $\mathfrak{X}_\Delta(h) := X_\Delta(h) T_{V_\Delta} / T_{V_\Delta}$. Define $S_\Delta := \mathrm{soc}(\mathfrak{X}_\Delta(C_H(\Delta)))$.

Multiplicity-free condition

If $\Delta \subseteq \Pi$ is an H-block such that $S_\Delta \simeq S$ and all $\mathfrak{X}_i : S_\Delta \to P\Gamma L(V_i)$ for $i \in \Delta$ are projectively equivalent, then $|\Delta| = 1$.

Proposition

Let X be classical-induced. Let $\Delta \subseteq \Pi$ be any H-block satisfying $S_\Delta \simeq S$. Suppose that the multiplicity-free condition holds. Then $|\Delta| \leq 2$.

Classical-induced representations without multiplicities, III

Theorem

There exists a universal constant $c > 0$ such that if $X : H \to GL(V)$ is a (mod T_V)-representation of H (with respect to a direct sum decomposition $V = \oplus_{i=1}^{t} V_i$), which is a classical-induced representation possessing the multiplicity-free condition, then $b_X(H) \leq 45(\log|H|)/(\log|V|) + c$.

A few words on the proof. There is an associated homomorphism $\mathfrak{X} : H \to N_{GL(V(p))}(T_V)/T_V$ defined by $\mathfrak{X}(h) := X(h)T_V/T_V$. There are two cases.

- $\mathfrak{X}(N) \neq 1$. Here $\mathrm{soc}(\mathfrak{X}(N))$ is a subdirect product of classical groups with linking factor at most 2. The previously mentioned result of Liebeck and Shalev (2002 and 2014) is used.
- $\mathfrak{X}(N) = 1$. In this case we use some ideas from the proof on the distinguishing number. We get a contradiction using the proposition on the previous slide.

Eliminating small tensor product factors, I

Recall that to prove Pyber's conjecture for affine primitive permutation groups, we may assume that H is induced from a primitive linear group H_1 having unbounded base size.

Theorem (Liebeck, Shalev (2002 and 2014))

Let $H \leq GL(U_k(p))$ be a primitive linear group of unbounded base size and $q = p^f$ be maximal such that $H \leq \Gamma L(U_{k/f}(q))$. Then there is a tensor product decomposition $U = U_1 \otimes U_2$ over $\mathbb{F}_q$ such that $1 \leq \dim(U_1) < \dim(U_2)$ and H preserves this tensor product decomposition. Let $H^0 = GL(U_{k/f}(q)) \cap H$ and let H_2^0 be the image of the projection of H^0 to $GL(U_2)$, that is,

$$H_2^0 := \{b \in GL(U_2) \,|\, \exists a \in GL(U_1) : \ a \otimes b \in H^0\}.$$

Then one of the following holds...

Eliminating small tensor product factors, II

Theorem (Liebeck, Shalev (2002 and 2014) continued)

... Then one of the following holds.

(1) $H_2^0 \simeq \mathrm{Sym}(m) \times \mathbb{F}_q^*$ or $\mathrm{Alt}(m) \times \mathbb{F}_q^*$ for some m such that U_2 is the unique non-trivial irreducible component of the natural m-dimensional permutation representation of $\mathrm{Sym}(m)$. In that case $\dim_{\mathbb{F}_q}(U_2) = m - 1$ unless $p \mid m$, when $\dim_{\mathbb{F}_q}(U_2) = m - 2$.

(2) H_2^0 is a classical group $\mathrm{Cl}(r, q_0) \leq GL(r, q)$ over some subfield $\mathbb{F}_{q_0} \leq \mathbb{F}_q$, where $r = \dim_{\mathbb{F}_q}(U_2)$.

Note that there is a similar characterization of primitive linear groups of large orders due to Jaikin-Zapirain and Pyber (2011).

Eliminating small tensor product factors, III

Theorem

There exists an absolute constant $c > 0$ such that if $X : H \to GL(V)$ is an irreducible linear representation over $\mathbb{F}_p$, then $b_X(H) \leq 45(\log|H|)/(\log|V|) + c$.

About the proof. A key tool is the following. Assume that the projective representation $X_1 : H_1 \to \Gamma L(V_1)$ preserves a tensor product decomposition $V_1 = U_1 \otimes W_1$ over $\mathbb{F}_q$ where U_1 and W_1 are $\mathbb{F}_q$ vector spaces and $\dim_{\mathbb{F}_q}(U_1) \leq \dim_{\mathbb{F}_q}(W_1)$. By taking the composition of X_i with the projection map to W_i, one can define new projective representations $Y_i : H_i \to \Gamma L(W_i)$. Let $Y : H \to GL(W(p))$ be the induced representation $Y = \mathrm{Ind}_{H_1}^{H}(Y_1)$, where W can be identified with $W_1 \oplus \ldots \oplus W_t$.

Lemma

We have $b_X(H) \leq \lceil b_Y(H)/\dim_{\mathbb{F}_q}(U_1)\rceil + 4$.

Eliminating small tensor product factors, IV

About the proof continued. This way we may pass from the representation X to Y. We get that Y is alternating-induced or classical-induced. We may use the previous results in case Y is alternating-induced or multiplicity-free classical-induced. Thus we must reduce to the case when Y is multiplicity-free classical-induced.

For this purpose let $\Delta \subseteq \Pi$ be a maximal H-block violating the multiplicity-free condition, i.e. $S_\Delta \simeq S$ and the representations $Y_i : S_\Delta \to \Gamma L(W_i)$ for $V_i \in \Delta$ are projectively equivalent. Let $Y_\Delta : N_H(\Delta) \to GL(W_\Delta(p))$ be the $\pmod{T_{W_\Delta}}$-representation defined by the restriction of Y. Then $Y = \mathrm{Ind}_{N_H(\Delta)}^H(Y_\Delta)$. Furthermore, by choosing a suitable basis, $Y_\Delta(N_H(\Delta))$ is included into the Kronecker product of a group of monomial matrices and a group of matrices isomorphic to some classical group. This means that we have a tensor product decomposition $W_\Delta = W_\Delta^{\mathrm{S}} \otimes W_\Delta^{\mathrm{C}}$ preserved by $Y_\Delta(N_H(\Delta))$. We apply the previous lemma once again.

Statement of the result

Theorem

There exists a universal constant $c > 0$ such that the minimal base size $b(G)$ of a primitive permutation group G of degree n satisfies

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

Remark. It is only a coincidence in the proof that the constant 45 appears both in the non-affine case and in the affine case.

Thank you for your attention.