On the degrees of non-split extensions by an alternating group

László Babai*
University of Chicago
Draft: July 4, 2017

Abstract

Let $G \le S_n$ be a permutation group of degree n with a quotient isomorphic to A_k. We show that if $n < (1/2 - o(1))k^2$ then the extension splits. Motivated by this result, Guralnick and Liebeck have shown that the conclusion fails to hold if we allow n to be $n = 2k(k-1)$, establishing a tight quadratic growth rate for the smallest degree of a faithful permutation representation of a non-split extension by A_k.

1 Introduction

We study the following question. Given a positive integer k, what is the smallest value $n = n(k)$ such that there exists a non-split extension G of some group by the alternating group A_k with a faithful permutation representation of degree n. In other words, we are looking for a permutation group $G \le S_n$ such that G has an epimorphism onto the alternating group A_k that is a non-split extension. We are especially interested in the rate of growth of this function.

This question is completely answered in a pair of papers, showing that $n(k)$ grows at a quadratic rate. The lower bound is given in this paper, while the upper bound appears in a companion paper by Guralnick and Liebeck [GL].

In this note we show that the bound $n(k) \ge (1/2 - o(1))k^2$ is an immediate consequence of an old lemma and a recent one by the author (see Theorem 1.1 below).

Theorem 1.1. *Let $G \le S_n$ be a permutation group such that*

(a) the largest orbit of G has length n_0 ;

(b) G has a normal subgroup K such that $G/K \cong A_k$ where $k \ge 16$;

(c) $n_0 < k^2/4$.

Then the extension $1 \to K \to G \to A_k \to 1$ splits.

The same conclusion holds for every $\epsilon > 0$ and all sufficiently large $k > k(\epsilon)$ if we replace (c) by the condition

*Research partially supported by NSF Grant CCF 1423309

(c') $n_0 < (1/2 - \epsilon)k^2$.

Corollary 1.2. $n(k) \geq (1/2 - o(1))k^2$.

Answering the author's question proposed in a lecture in Jerusalem in November 2016, Guralnick and Liebeck [GL] proved that (contrary to the author's expectation) the quadratic rate of growth is optimal: $n(k) \leq 2k(k-1)$. This result, combined with Theorem 1.1 yields the tight quadratic growth rate for the $n(k)$ function:

$$n(k) = \Theta(k^2). \tag{1}$$

Guralnick and Liebeck [GL] also provide a separate proof of Cor. 1.2, by entirely different methods, and improve the constant by a factor of 2:

$$n(k) \geq (1 - o(1))k^2. \tag{2}$$

2 Notation and preliminaries

We write $\mathrm{Sym}(\Omega)$ to denote the symmetric group acting on the permutation domain Ω, and $\mathrm{Alt}(\Omega)$ for the alternating group. We denote the set $\{1, \ldots, k\}$ by $[k]$ and write $S_n = \mathrm{Sym}([n])$ and $A_n = \mathrm{Alt}([n])$. We also write S_n and A_n generically when we do not need to specify the permutation domain, only its cardinality.

We write operators in the exponent. Thus, for $x \in \Omega$ and $\sigma \in \mathrm{Sym}(\Omega)$ we write x^σ for the σ-image of x. We write x^G to denote the G-orbit of x. For a homomorphism $\varphi : G \to H$ we write G^φ to denote the image of G under φ.

A permutation group acting on Ω is a subgroup $G \leq \mathrm{Sym}(\Omega)$. The *support* of G is the set $\mathrm{supp}(G) = \{x \in \Omega \mid (\exists \sigma \in G)(x^\sigma \neq x)\}$. The support of a permutation σ is the support of the cyclic group generated by σ.

Let henceforth $G \leq \mathrm{Sym}(\Omega)$ and let $\mathfrak{B} = \{B_1, \ldots, B_k\}$ be a G-invariant partition of Ω. Let $\sigma \mapsto \overline{\sigma}$ denote the action $G \to \mathrm{Sym}(\mathfrak{B})$, so for $\sigma \in G$ we have $\overline{\sigma} \in \mathrm{Sym}(\mathfrak{B})$. We say that G is *clean* with respect to $\mathfrak{B}$ if for every $\sigma \in G$ we have $\mathrm{supp}(\sigma) = \bigcup \mathrm{supp}(\overline{\sigma})$, i. e., if $\sigma \in G$ fixes a block B_i setwise then σ fixes B_i pointwise. In other words, G is clean if and only if every orbit of G intersects each block B_i in at most one element.

A complement of a subgroup $K \leq G$ is a subgroup $L \leq G$ such that $KL = G$ and $K \cap L = \{1\}$. We say that K has a *clean complement* if K has a complement that is clean with respect to $\mathfrak{B}$.

For $x \in \Omega$ we denote the stabilizer of x in G by G_x, so $G_x = \{\sigma \in G \mid x^\sigma = x\}$. For a subset $\Psi \subseteq \Omega$ we write $G_{(\Psi)}$ to denote the pointwise stabilizer of Ψ and G_Ψ the setwise stabilizer of Ψ. We note that G is clean with respect to $\mathfrak{B}$ exactly if $G_B = G_{(B)}$ for each block $B \in \mathfrak{B}$.

For a set A and an integer $t \geq 0$ let $\binom{A}{t}$ denote the set of t-subsets of A; so $|\binom{A}{t}| = \binom{|A|}{t}$. Let $G^{(t)}$ denote the induced action of G on $\binom{\Omega}{t}$. We shall especially refer to the induced alternating groups $A_k^{(t)}$.

Let $\varphi : G \to A_k$ be an epimorphism. Following [Ba16], we say that $x \in \Omega$ is *affected* by φ if $(G_x)^\varphi \neq A_k$, and *unaffected* if $(G_x)^\varphi = A_k$. If x and y belong to the same G-orbit then G_x and G_y are conjugates, so if x is affected then so is y.

3 The old lemma

We start with a simple observation.

Proposition 3.1. *Let $G \leq \mathrm{Sym}(\Omega)$ and let $\mathfrak{B}$ be a G-invariant partition of Ω. Let L and M be clean subgroups of G such that $\mathrm{supp}(L) \cap \mathrm{supp}(M)$ consists of a single block $B \in \mathfrak{B}$. Then the subgroup $\langle L, M\rangle$ generated by L and M is clean.*

Proof. The nontrivial orbits of $\langle L, M\rangle$ are those nontrivial orbits of L and M that do not intersect B plus for each $x \in B$ the union of the orbits x^L and x^M. So each orbit of $\langle L, M\rangle$ intersects each bock of $\mathfrak{B}$ in at most one element. □

The following lemma appears in [Ba83].

Lemma 3.2. [Ba83, Lemma 21.13] *Let $G \leq \mathrm{Sym}(\Omega)$ and let $\mathfrak{B} = \{B_1, \ldots, B_k\}$ be a G-invariant partition of Ω. Suppose the image of the G-action $G \to \mathrm{Sym}(\mathfrak{B})$ is $\mathrm{Alt}(\mathfrak{B})$; let K be the kernel of this action. Assume further that $k > 2\sqrt{n}$ where $n = |\Omega|$. Then K has a clean complement.*

Proof. For $\tau \in G$ let $\overline{\tau}$ denote the action of τ on $[k] = \{1, \ldots, k\}$ corresponding to the action of τ on $\mathfrak{B}$. Let $b = n/k$; so $|B_i| = b$ for all i; and we have $k > 4b$. By Bertrand's postulate there is a prime p between $b + 1$ and $2b + 1$. Take $\pi \in G$ such that $\overline{\pi}$ is a p-cycle. As $b < p$, there is an m such that p does not divide m and π^m is clean. We may assume $m = 1$, and $\overline{\pi} = (1, 2, \ldots, p)$. Similarly, there exists a clean $\pi' \in G$ such that $\overline{\pi'} = (p, p + 1, \ldots, 2p - 1)$. By Prop. 3.1, the group $\langle \pi, \pi'\rangle$ is clean. Thus the commutator $\sigma := [\pi, \pi']$ is a clean permutation such that $\overline{\sigma}$ is a 3-cycle. Let σ_i be a conjugate of σ with $\overline{\sigma}_i = (i, i + 1, k)$. (Note that conjugates of clean elements are clean.) Again by Prop. 3.1, for k odd, the group generated by $\sigma_1, \sigma_3, \sigma_5, \ldots, \sigma_{k-2}$ is a clean complement to K. If k is even then let $\mathfrak{A}$ denote the stabilizer of the block B_k in the clean group $\langle \sigma_1, \sigma_3\rangle$. Clearly, $\mathfrak{A} \cong A_4$. Now $\mathfrak{A}, \sigma_4, \sigma_6, \ldots, \sigma_{k-2}$ generate a clean complement to K. □

Remark 3.3. We note that the result holds, without any change in the proof, if we replace the condition $k > 2\sqrt{n}$ by the condition $k > 2\sqrt{n_0}$ where n_0 is the length of the largest G-orbit.

The proof actually yields the following, asymptotically stronger bound.

Lemma 3.4. *Let $G \leq \mathrm{Sym}(\Omega)$ and let $\mathfrak{B} = \{B_1, \ldots, B_k\}$ be a G-invariant partition of Ω. Suppose the image of the G-action $G \to \mathrm{Sym}(\mathfrak{B})$ is $\mathrm{Alt}(\mathfrak{B})$; let K be the kernel of this action. Assume further that there exists a prime p such that $n_0/k < p \leq (k+1)/2$, where n_0 is the length of the largest G-orbit. Then K has a clean complement.*

Such a prime p exists for all $\epsilon > 0$ if $k > \max\{k(\epsilon), (\sqrt{2} + \epsilon)\sqrt{n_0}\}$ for a suitable function $k(\epsilon)$.

Remark 3.5. The author's D. Sc. dissertation (1983) where this lemma first appeared is in Hungarian and exists in a few copies only. The lemma first appeared in English in [BaKL] later in 1983. While the "extended abstract" [BaKL] is a joint paper by three authors, it states that it is in fact a simple merger of three independent contributions, and promises that each author would publish a detailed version of their respective contribution separately. Only one of us (Kantor) made good on that promise [Ka]. The present author included a detailed discussion of the above lemma in another joint paper [BaBT] in 1992. Finally in 2008 the author wrote up the promised detailed version of his contribution to [BaKL] in [Ba08]. That manuscript, giving an $\exp(O(\sqrt{n}\log n))$ bound on the complexity of the string isomorphism and coset intersection problems, was subsequently accepted for publication but the author procrastinated the final revisions until that paper was superseded by the recent quasipolynomial-time algorithm for the same problems [Ba16]. While this made the main results of [Ba08] obsolete, there may be continuing interest in the lemma above and the group theoretic structure theorem given in [Ba08] (see Section 6). We make these results accessible in the present note.

4 Permutation groups with an alternating quotient

The following result is a by-product of the author's recent work on the Graph Isomorphism problem [Ba16].

Theorem 4.1. *Let $G \le \mathrm{Sym}(\Omega)$ be a permutation group whose largest orbit has length n_0. Let $\varphi : G \to A_k$ be an epimorphism where $k \ge \max\{9, 2\log_2 n_0\}$. Then Ω has a subset Ψ with the following properties. Let $H = G_{(\Psi)}$ denote the pointwise stabilizer of Ψ in G.*

(i) Ψ is a union of some of the orbits of G. In particular, $H \triangleleft G$.

(ii) $H^\varphi = A_k$. In particular, $\Psi \ne \Omega$.

(iii) For each G-orbit $\Delta \subseteq \Omega \setminus \Psi$ there exists an integer $t_\Delta \ge 1$ and a system $\mathfrak{B}_\Delta$ of $|\mathfrak{B}_\Delta| = \binom{k}{t_\Delta}$ blocks of imprimitivity in Δ such that the G-action as well as the H-action on $\mathfrak{B}_\Delta$ is $A_k^{(t_\Delta)}$ and the kernel of the G-action on $\mathfrak{B}_\Delta$ is $\ker(\varphi)$.

Proof. Let Ψ be the union of the orbits unaffected by φ. Now item (i) is evident. Item (ii) is the content of the the "Unaffected Stabilizers Lemma" (Theorem 8.3.5 in [Ba16]. Item (iii) paraphrases item (e) of the "Main Structure Theorem" (Theorem 8.5.1) in [Ba16]. □

Corollary 4.2. *Let $G \le \mathrm{Sym}(\Omega)$ be a permutation group whose largest orbit has length n_0. Let $\varphi : G \to A_k$ be an epimorphism where $k \ge 16$ and $k(k-1) > 2n_0$. Then Ω has a subset Ψ with the following properties. Let $H = G_{(\Psi)}$ denote the pointwise stabilizer of Ψ in G.*

(i) Ψ *is a union of some of the orbits of* G*. In particular,* $H \triangleleft G$*.*

(ii) $H^\varphi = A_k$*. In particular,* $\Psi \neq \Omega$*.*

(iii) The set $\Omega \setminus \Psi$ *has a* G*-invariant partition* $\Omega \setminus \Psi = B_1 \sqcup \cdots \sqcup B_k$ *such that the kernel of the* G*-action on the set* $\mathfrak{B} = \{B_1, \ldots, B_k\}$ *is* $\ker(\varphi)$ *and* $G/\ker(\varphi) = A_k$ *acts in its natural action on* $\mathfrak{B}$*.*

Proof. First, one can verify that the conditions $k \geq 16$ and $k(k-1) > 2n_0$ imply $k \geq \max\{9, 2\log_2 n_0\}$. So the conclusion of Theorem 4.1 holds. But now $t_\Delta = 1$ for each affected G-orbit $\Delta \subseteq \Omega \setminus \Psi$ since otherwise we would have $|\Delta| \geq \binom{k}{2}$, contradicting the assumption $k(k-1) > 2n_0$. Finally, for $k \geq 7$, the group A_k has only one conjugacy class of subgroups of index k so we can match up the blocks in the various orbits Δ by their stabilizers in $G^\varphi = A_k$ to form the blocks B_i. □

5 Proof of the main result

Now the proof of Theorem 1.1 is a simple combination of Cor. 4.2 and Lemmas 3.2 and 3.4.

Indeed, let $G \leq \mathrm{Sym}(\Omega)$ satisfy conditions (a) and (b) of Theorem 1.1 along with condition (c) or (c'). From condition (c), which says $k^2 > 4n_0$, we infer that the condition $k(k-1) > 2n_0$ required by Cor. 4.2 holds. From condition (c'), which says $k^2 > 2n_0/(1-2\epsilon)$, we again infer $k(k-1) > 2n_0$ assuming $k > 1/(2\epsilon)$ which we may assume by resetting $k(\epsilon)$ to $\max\{k(\epsilon), 1/(2\epsilon)\}$.

Now Cor. 4.2 finds a subgroup $H \triangleleft G$ and a G-invariant partition $\mathfrak{B}$ of $\mathrm{supp}(H)$ such that $|\mathfrak{B}| = k$ and the H-action on $\mathfrak{B}$ is A_k. Therefore by Lemmas 3.2 and 3.4, the kernel L of the action $H \to \mathrm{Sym}(\mathfrak{B})$ has a clean complement $\mathfrak{A} \cong A_k$. Let K be the kernel of the $G \to \mathrm{Sym}(\mathfrak{B})$ action. Clearly $K \cdot \mathfrak{A} = G$. Moreover, given that $\mathfrak{A}$ is clean, it follows that $K \cap \mathfrak{A} = \{1\}$. So $\mathfrak{A}$ is a (clean) complement to K, hence the extension $1 \to K \to G \to A_k$ indeed splits. This completes the proof of Theorem 1.1.

6 Appendix: The structure of permutation modules under alternating action

TO BE ADDED

Acknowledgments

In November 2016 the author attended the 20th Midrasha Mathematicae, "60 Faces to Groups," in honor of Alex Lubotzky's 60th birthday, at the Israel Institute for Advanced Studies. The author wishes to express his gratitude to Alex and the organizers for the opportunity to speak there before an illustrious audience that included Bob Guralnick and Martin Liebeck. Their interest in the author's question prompted the present

write-up of Theorem 1.1 and yielded the satisfactory although (by this author) entirely unanticipated result [GL] that the quadratic lower bound in Cor. 1.2 was tight (up to a constant factor).

The author also wishes Alex Lubotzky many more productive years and happy anniversaries.

References

[Ba83] László Babai: *Permutation Groups, Coherent Configurations, and Graph Isomorphism.* D.Sc. Thesis (Hungarian), Hungarian Academy of Sciences, April 1983.

[Ba08] László Babai: Coset intersection in moderately exponential time. Manuscript, 2008. Slightly updated in 2013. Available on author's home page

[Ba16] László Babai: Graph Isomorphism in quasipolynomial time. E-print, 2016, arXiv:1512.03547. Version 2, January 2016.

[BaBT] László Babai, Robert Beals, and Pál Takácsi-Nagy: Symmetry and complexity. In: *Proc. 24th STOC*, ACM 1992, pp. 438–449.

[BaKL] László Babai, William M. Kantor, and Eugene M. Luks: Computational complexity and the classification of finite simple groups. In: *Proc. 24th FOCS*, IEEE Computer Society Press, 1983, pp. 162–171.

[BaL] László Babai and Eugene M. Luks: Canonical labeling of graphs. In: *Proc. 15th STOC*, ACM 1983, pp. 171–183.

[GL] Robert M. Guralnick and Martin W. Liebeck: Permutation representations of nonsplit extensions involving alternating groups. Manuscript. December 2016.

[Ka] William M. Kantor: Sylow's theorem in polynomial time. *J. Computer and System Sci.* **30** (1985), 359–394.

[Lu1] Eugene M. Luks: Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comp. Sys. Sci.* **25** (1982), 42–65.