UPPER BOUNDS ON POLYNOMIALS WITH SMALL GALOIS GROUP

ROBERT J. LEMKE OLIVER AND FRANK THORNE

Abstract. When monic integral polynomials of degree $n \geq 2$ are ordered by the maximum of the absolute value of their coefficients, the Hilbert irreducibility theorem implies that asymptotically 100% are irreducible and have Galois group isomorphic to S_n. In particular, amongst such polynomials whose coefficients are bounded by B in absolute value, asymptotically $(1+o(1))(2B+1)^n$ are irreducible and have Galois group S_n. When G is a proper transitive subgroup of S_n, however, the asymptotic count of polynomials with Galois group G has been determined only in very few cases.

Here, we show that if there are strong upper bounds on the number of degree n fields with Galois group G, then there are also strong bounds on the number of polynomials with Galois group G. For example, for any prime p, we show that there are at most $O(B^{3-\frac{2}{p}}(\log B)^{p-1})$ polynomials with Galois group C_p and coefficients bounded by B.

1. Introduction

Fix an integer $n \geq 2$ and let G be a subgroup of S_n. For any $B \geq 1$, let

$$P_n(B;G) := \#\{f \in \mathbb{Z}[x] \text{ monic, degree } n : \mathrm{ht}(f) \leq B, \mathrm{Gal}(f) \simeq G\},$$

where $\mathrm{ht}(f)$ is the maximum absolute value of the coefficients of f. The Hilbert irreducibility theorem implies that asymptotically 100% of such polynomials are irreducible and have Galois group S_n, so that $P_n(B;S_n) \sim (2B+1)^n$. There are very few other groups, however, for which the asymptotic order of $P_n(B;G)$ is known, even in small degrees; see [CD18] for recent results in degrees 3 and 4. Instead, one often must settle for placing upper bounds on $P_n(B;G)$.

There are two broad approaches in the literature to do so. The first uses the large sieve (often in conjunction with Serre's notion of thin sets) to bound from above the number of polynomials that avoid certain behavior modulo small primes; the record via this approach is due to Gallagher [Gal73], who shows that $P_n(B;G) \ll B^{n-\frac{1}{2}}(\log B)^{1-\gamma_n}$ with $\gamma_n > 0$ for all $G \not\simeq S_n$ simultaneously, and Zywina [Zyw10], who improves this to $P_n(B;G) \ll B^{n-\frac{1}{2}}$ for large n.

The other approach is to bound the number of polynomials such that some auxiliary Galois resolvent has an exceptional property; the pioneer of this approach and the overall record-holder is Dietmann [Die12, Die13], who shows that $P_n(B;G) \ll B^{n-1+\frac{1}{[S_n:G]}+\epsilon}$ for $G \neq A_n$ and that $P_n(B;A_n) \ll B^{n-2+\sqrt{2}+\epsilon}$.

Here, we introduce a third approach that has the potential to yield substantially stronger results but requires a hypothesis that is unproved in many cases. Before stating a general theorem, we begin with two unconditional results that are reflective of our method.

Theorem 1.1. *Let $p \geq 3$ be prime and let C_p denote the cyclic group of order p. Then $P_p(B;C_p) \ll B^{3-\frac{2}{p}}(\log B)^{p-1}$.*

More generally, for any $n \geq 2$, let $P_n^{\mathrm{gal}}(B)$ denote the number of monic, irreducible polynomials $f \in \mathbb{Z}[x]$ whose coefficients are bounded in absolute value by B, and for which the field $\mathbb{Q}(x)/f(x)$ is Galois.

Theorem 1.2. *If $n \geq 5$, then $P_n^{\mathrm{gal}}(B) \ll B^{\frac{3}{4}n+\frac{1}{4}+\epsilon}$.*

Our approach is as follows. When $G \subseteq S_n$ is transitive, any polynomial $f(x)$ counted by $P_n(B;G)$ cuts out a field $\mathbb{Q}(x)/f(x)$ whose normal closure has Galois group G and whose discriminant is $O_n(B^{2n-2})$. In Section 2, we bound from above the multiplicity with which a given field is cut out in this manner. It follows that if there are not too many fields with Galois group G, then there can also not be too many polynomials with Galois group G. To make this precise, let

$$\mathcal{F}_n(X;G) := \{K/\mathbb{Q} : [K:\mathbb{Q}] = n, \mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G, |\mathrm{Disc}(K)| \leq X\},$$

where $\widetilde{K}$ is the normal closure of $K/\mathbb{Q}$ and $\mathrm{Disc}(K)$ is the absolute discriminant of K, and set $N_n(X;G) := \#\mathcal{F}_n(X;G)$.

Theorem 1.3. *With notation as above, assume for some constant $e > \frac{1}{n^2-n}$ that the bound $N_n(X;G) \ll X^e$ holds for every sufficiently large X, with an implied constant depending at most on G and e. Then*

$$P_n(B;G) \ll B^{e(2n-2)+1}(\log B)^{n-1}.$$

If the group G is primitive, then this may be improved to $P_n(B;G) \ll B^{e(2n-2)+1-\frac{2}{n}}(\log B)^{n-1}$.

We recall that a permutation group G on n elements is said to be primitive if it preserves no nontrivial partition of the elements. For example, when p is prime, this hypothesis is satisfied for every transitive subgroup of S_p, so that Theorem 1.1 follows from Theorem 1.3 and the upper bound $N_p(X;C_p) \ll X^{\frac{1}{p-1}}$ [Mäk85, Wri89]. Theorem 1.2, on the other hand, follows from the first case of Theorem 1.3 and an upper bound of $O(X^{3/8+\epsilon})$ due to Ellenberg and Venkatesh [EV06, Proposition 1.3] on the number of Galois number fields. This result of Ellenberg and Venkatesh is not sharp, and correspondingly neither is Theorem 1.2. It could likely be improved substantially for any given n with modest effort.

Theorem 1.3 improves on the results provided by studying thin sets and Galois resolvents desribed above if for example its hypothesis holds with some $e \leq \frac{1}{2} - \frac{1}{2n-2}$; slightly weaker results suffice for any particular group G. Malle's conjecture [Mal04] predicts an asymptotic of the form $N_n(X;G) \sim c(G)X^{a(G)}(\log X)^{b(G)}$, where the constant $a(G)$ is the inverse of an integer and satisfies $\frac{1}{n-1} \leq a(G) \leq 1$. Thus, for $n \geq 5$, Theorem 1.3 conjecturally improves upon prior work whenever $a(G) \leq \frac{1}{3}$. This criterion is satisfied precisely when $G \subseteq S_n$ is such that for every $1 \neq g \in G$, the permutation action of g decomposes into at most $n-3$ orbits.

Acknowledgements

The authors would like to thank Sam Chow, Rainer Dietmann, Michael Filaseta, and Martin Widmer for helpful feedback.

RJLO was partially supported by NSF grant DMS-1601398. FT was partially supported by grants from the Simons Foundation (Nos. 563234 and 586594).

2. Multiplicities of polynomials cutting out fields

Given a number field K of degree n and signature (r_1, r_2), let

$$M_K(B) := \#\{f \in \mathbb{Z}[x] \text{ monic, degree } n : \mathrm{ht}(f) \leq B, \mathbb{Q}(x)/f \simeq K\}$$

be the multiplicity with which K is cut out amongst polynomials of height at most B.

The main result of this section is the following upper bound on $M_K(B)$.

Theorem 2.1. *Write*

$$\lambda = \min\{||\alpha|| : \alpha \in \mathcal{O}_K \setminus \mathbb{Z}\},$$

where for each $\alpha \in \mathcal{O}_K$ we write $||\alpha||$ for the maximum absolute value of α under the embeddings of K.

Then, we have

$$M_K(B) \ll \frac{B(\log B)^{r_1+r_2-1}}{\lambda}.$$

Loosely speaking, the idea of the proof of Theorem 2.1 is that most elements $\alpha \in \mathcal{O}_K$ should have minimal polynomials $f_\alpha(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ with coefficients scaling like $|a_i| \approx ||\alpha||^i$ rather than having all coefficients of roughly the same size. We show that the elements whose minimal polynomials are counted by $M_K(B)$ lie in a very restricted region inside Minkowski space, and then bound from above the number of elements inside that region.

To make this precise, we begin by recalling the definition of the *Mahler measure* of a polynomial. Given a monic polynomial $f \in \mathbb{C}[x]$, its Mahler measure $m(f)$ is defined to be

$$m(f) := \prod_{\theta : f(\theta)=0} \max\{1, |\theta|\},$$

where the product runs over the roots of f with multiplicity. A standard argument using Jensen's formula, which we learned about from [Ram15], establishes that if we write $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, then

$$m(f) \leq \sqrt{1 + a_1^2 + \cdots + a_n^2} \leq \sqrt{n+1} \cdot \mathrm{ht}(f). \tag{2.1}$$

Let $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} =: K_\infty$ be the standard embedding of K into Minkowski space. For any $x \in K_\infty$, we may analogously define its Mahler measure $m(x)$ by

$$m(x) := \prod_{\sigma} \max\{1, |x_\sigma|^{\deg \sigma}\}.$$

For any $Y \geq 1$, we let $\Omega_Y \subseteq K_\infty$ consist of those elements whose Mahler measure is at most Y. Then by (2.1) we have

$$M_K(B) \leq \#\{\Omega_{\sqrt{n+1}\cdot B} \cap (\mathcal{O}_K - \mathbb{Z})\}, \tag{2.2}$$

allowing us to proceed by bounding the right-hand side of (2.2). The volume of Ω_Y, or of its projection onto any subset of the coordinate axes, is easily computed to be $O_n(Y(\log Y)^{r_1+r_2-1})$. It therefore follows from *Davenport's lemma* [Dav51] that the simpler count $\#\{x \in \Omega_Y \cap \mathbb{Z}^n\}$ satisfies

$$\#\{x \in \Omega_Y \cap \mathbb{Z}^n\} \ll Y(\log Y)^{r_1+r_2-1}. \tag{2.3}$$

For the sake of motivation, we begin by proving a weaker result than Theorem 2.1 that recovers the bound in (2.3) but for $\#\{\Omega_{\sqrt{n+1}\cdot B} \cap (\mathcal{O}_K - \mathbb{Z})\}$.

Proposition 2.2. *With notation as above, $M_K(B) \ll B(\log B)^{r_1+r_2-1}$.*

Proof. Let $\mu \asymp_n 1$ be the shortest length of any nonzero vector in $\mathcal{O}_K$. Let $\eta > 0$ be an arbitrary small constant, write $\delta := \frac{\mu}{\sqrt{n}} - \eta$, and consider the dilation $\Lambda := \delta\mathbb{Z}^n$ of the integer lattice $\mathbb{Z}^n \subseteq K_\infty$. By construction, the box of side length δ centered at any point in $\delta\mathbb{Z}^n$ contains at most one point of $\mathcal{O}_K$. To each $\alpha \in \mathcal{O}_K$ we associate the nearest vector $v_\alpha \in \delta\mathbb{Z}^n$, choosing arbitrarily if there is more than one such. Then the map $\alpha \mapsto v_\alpha$ is injective and we write $\mathcal{S} := \{v_\alpha : \alpha \in \mathcal{O}_K\}$.

Let $Y = \sqrt{n+1}\cdot B$, so that $M_K(B) \le \#(\Omega_Y \cap \mathcal{O}_K)$. If $\alpha \in \Omega_Y \cap \mathcal{O}_K$, we have $\frac{1}{\delta}v_\alpha - x \in \frac{1}{\delta}\Omega_Y$ for some $x \in \mathrm{Box}(1)$, the unit box centered at the origin. Since $\delta \asymp 1$, we have

$$\begin{aligned}\#\{\Omega_Y \cap \mathcal{O}_K\} &\le \#\Big\{\frac{1}{\delta}\mathcal{S} \cap \Big(\frac{1}{\delta}\Omega_Y + \mathrm{Box}(1)\Big)\Big\} \\ &\le \#\Big\{\mathbb{Z}^n \cap \Big(\frac{1}{\delta}\Omega_Y + \mathrm{Box}(1)\Big)\Big\} \\ &\ll Y\log^{r_1+r_2-1}(Y),\end{aligned}$$

as desired, with the last inequality following from Davenport's lemma. □

Proof of Theorem 2.1. In the proof of Proposition 2.2, we still let $Y = \sqrt{n+1}\cdot B$ but now choose $\delta := \frac{\lambda}{\sqrt{n}} - \eta$ and define α and $\mathcal{S}$ as before. The map $\alpha \mapsto v_\alpha$ is no longer injective, but it has the property that $\alpha - \alpha' \in \mathbb{Z}$ whenever $v_\alpha = v_{\alpha'}$, and hence it has preimages of size $O(\lambda)$.

We now decompose the region Ω_Y as $\Omega_Y = \bigcup_{s_1,s_2} \Omega_{Y,s_1,s_2}$, where

$$\Omega_{Y,s_1,s_2} := \{x \in \Omega_Y \ : \ |x_\sigma| \ge \delta \text{ for exactly } s_1 \text{ real and } s_2 \text{ complex places } \delta\}.$$

For each Ω_{Y,s_1,s_2}, we now have that

$$\begin{aligned}\#\{\Omega_{Y,s_1,s_2} \cap \mathcal{O}_K\} &\le O(\lambda)\cdot\#\Big\{\frac{1}{\delta}\mathcal{S} \cap \Big(\frac{1}{\delta}\Omega_{Y,s_1,s_2} + \mathrm{Box}(1)\Big)\Big\} \\ &\le O(\lambda)\cdot\#\Big\{\mathbb{Z}^n \cap \Big(\frac{1}{\delta}\Omega_{Y,s_1,s_2} + \mathrm{Box}(1)\Big)\Big\} \\ &\ll \lambda\cdot\frac{Y(\log Y)^{r_1+r_2-1}}{\delta^{s_1+2s_2}} \\ &\ll \frac{Y(\log Y)^{r_1+r_2-1}}{\lambda^{s_1+2s_2-1}}.\end{aligned}$$

This bound is as desired when $s_1 + 2s_2 \ge 2$, leaving only the exceptional regions $\Omega_{Y,0,0}$ and $\Omega_{Y,1,0}$, the latter region being nonempty only if K has a real place.

The region $\Omega_{Y,0,0}$, if it is nonempty, is contained within a single box of length δ centered at the origin, and hence contains only rational integers that do not contribute to $M_K(B)$.

To bound $\#(\Omega_{Y,1,0} \cap \mathcal{O}_K)$, note that for each $\alpha \in \Omega_{Y,1,0}$, the corresponding v_α has exactly one nonzero coordinate. For each such v, the number of $\alpha \in \mathcal{O}_K \cap \Omega_{Y,1,0}$ with $v_\alpha = v$ is bounded above by the number of integers k with $m(v+k) \le Y$, which is $\ll \big(\frac{Y}{||v||}\big)^{\frac{1}{n-1}}$. We therefore have

$$\#(\Omega_{Y,1,0} \cap \mathcal{O}_K) \ll \sum_{1 \le j \le \frac{Y}{\delta}+1} \left(\frac{Y}{\delta j}\right)^{\frac{1}{n-1}} \ll \frac{Y\log Y}{\delta} \asymp \frac{Y\log Y}{\lambda},$$

the factor of $\log Y$ being extraneous unless $n = 2$, but harmless to include in all cases.

The theorem now follows by summing the above bounds over all s_1 and s_2. □

3. Proof of Theorem 1.3

We now turn to the proof of Theorem 1.3. If $f \in \mathbb{Z}[x]$ is monic of degree n and satisfies $\mathrm{ht}(f) \leq B$, then its discriminant satisfies $|\mathrm{Disc}(f)| \ll B^{2n-2}$. It follows that there is some positive constant c such that

$$P_n(B; G) \leq \sum_{K \in \mathcal{F}_n(cB^{2n-2}; G)} M_K(B).$$

Appealing to Proposition 2.2, we see that $M_K(B) \ll B(\log B)^{r_1+r_2-1} \leq B(\log B)^{n-1}$. By our hypothesis that $N_n(X; G) \ll X^e$ for every sufficiently large X, we conclude that

$$P_n(B; G) \ll B^{e(2n-2)+1}(\log B)^{n-1},$$

yielding the first case of the theorem.

For the second case, we require the following lemma of Ellenberg and Venkatesh.

Lemma 3.1. *Let $K/\mathbb{Q}$ be an extension of degree n. Then for any $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$, there holds $||\alpha|| \gg |\mathrm{Disc}(K)|^{\frac{1}{n(n-1)}}$.*

Proof. This is essentially [EV06, Lemma 3.1], but we recap the proof here because it is brief. The minimal polynomial f_α of such an α has discriminant bounded above by $O(||\alpha||^{n(n-1)})$. Since the discriminant of f_α is an upper bound on $\mathrm{Disc}(K)$, the result follows. □

If the group G is primitive, then any field $K \in \mathcal{F}_n(X; G)$ has no proper subextensions. By Lemma 3.1, it follows that for such fields, we may take $\lambda = |\mathrm{Disc}(K)|^{\frac{1}{n(n-1)}}$ in Theorem 2.1. So doing, we have

$$P_n(B; G) \ll \sum_{K \in \mathcal{F}_n(cB^{2n-2}; G)} \frac{B(\log B)^{n-1}}{|\mathrm{Disc}(K)|^{\frac{1}{n(n-1)}}} \ll B^{e(2n-2)+1-\frac{2}{n}}(\log B)^{n-1}$$

by partial summation and our assumption that $e > \frac{1}{n^2-n}$. This completes the proof.

4. Further examples

While obtaining upper bounds on $N_n(X; G)$ that are useful in Theorem 1.3 is difficult in general, there are some groups G for which strong results are available. For example Klüners and Malle [KM04] proved that for a nilpotent group $G \subseteq S_n$ of order n acting in its regular representation, we have $N_n(X; G) \ll X^e$ with $e = \frac{\ell}{n(\ell-1)} + \epsilon$, where ℓ is the smallest prime divisor of n. We therefore obtain:

Theorem 4.1. *Let G be a nilpotent group of order n, and let ℓ be the smallest prime divisor of $|G|$. Then for any $\epsilon > 0$,*

$$P_n(B; G) \ll_\epsilon B^{\frac{2\ell}{\ell-1}+1-\frac{2\ell}{(\ell-1)n}+\epsilon}.$$

We recall for the convenience of the reader that abelian groups are nilpotent, so Theorem 4.1 applies whenever G is abelian. Indeed, in the abelian case, Wright's earlier work [Wri89] implies that the factor of B^ϵ may be replaced by a power of $\log B$.

In fact, Malle's conjecture [Mal04] implies that the conclusion of Theorem 4.1 should hold for any group G of order n, not just nilpotent groups; this suggests for example that

$P_n^{\mathrm{gal}}(B) \ll B^{5-\frac{4}{n}+\epsilon}$ for every n. Additionally, recent work of Alberts [Alb18] establishes the weak Malle conjecture for nilpotent groups G in every representation, not just their regular representation; in many cases, this would yield strong upper bounds on $P_n(B;G)$ for nilpotent groups G with degree n representations.

References

[Alb18] Brandon Alberts. The Weak Form of Malle's Conjecture and Solvable Groups. *Preprint*, 2018. Available at `https://arxiv.org/abs/1804.11318`.

[CD18] Sam Chow and Rainer Dietmann. Enumerative Galois theory for cubics and quartics. *Preprint*, 2018. Available at `https://arxiv.org/abs/1807.05820`.

[Dav51] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.

[Die12] Rainer Dietmann. On the distribution of Galois groups. *Mathematika*, 58(1):35–44, 2012.

[Die13] Rainer Dietmann. Probabilistic Galois theory. *Bull. Lond. Math. Soc.*, 45(3):453–462, 2013.

[EV06] Jordan S. Ellenberg and Akshay Venkatesh. The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math. (2)*, 163(2):723–741, 2006.

[Gal73] P. X. Gallagher. The large sieve and probabilistic Galois theory. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 91–101. Amer. Math. Soc., Providence, R.I., 1973.

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. *J. Reine Angew. Math.*, 572:1–26, 2004.

[Mäk85] Sirpa Mäki. On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Ser. A I Math. Dissertationes*, (54):104, 1985.

[Mal04] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[Ram15] Ramya. Upper bound for Mahler's measure. *Blog post*, 2015. Available at `http://zerocollar.blogspot.com/2015/04/upper-bound-for-mahlers-measure.html`.

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58(1):17–50, 1989.

[Zyw10] David Zywina. Hilbert's irreducibility theorem and the larger sieve. *Preprint*, 2010. Available at `https://arxiv.org/abs/1011.6465`.

Department of Mathematics, Tufts University, 503 Boston Ave, Medford, MA 02155
E-mail address: `robert.lemke_oliver@tufts.edu`

Department of Mathematics, University of South Carolina, 1523 Greene St, Columbia, SC 29201
E-mail address: `thorne@math.sc.edu`