Electronic Colloquium on Computational Complexity, Report No. 64 (2003)

Upper Bounds on the Complexity of some Galois Theory Problems

V. Arvind and Piyush P Kurur
Institute of Mathematical Sciences, C.I.T Campus,
Chennai 600113, India
email: {arvind,ppk}@imsc.res.in

June 23, 2003

Abstract

Given a polynomial $f(X)$ with rational coefficients as input we study the problem of (a) finding the order of the Galois group of $f(X)$, and (b) determining the Galois group of $f(X)$ by finding a small generator set.

Assuming the generalized Riemann hypothesis, we prove the following complexity bounds.

(1) The order of the Galois group of an arbitrary polynomial $f(X) \in \mathbb{Z}[X]$ can be computed in $\mathrm{P}^{\#\mathrm{P}}$. Hence, the order can be approximated by a randomized polynomial-time algorithm with access to an NP oracle.

(2) For polynomials f with solvable Galois group we show that the order can be computed exactly by a randomized polynomial-time algorithm with access to an NP oracle.

(3) For all polynomials f with abelian Galois group we show that a generator set for the Galois group (as a permutation group acting on the roots of f) can be computed in randomized polynomial time.

These results also hold for polynomials $f \in K[X]$, where the field $K = \mathbb{Q}(\theta)$ is specified by giving the minimal polynomial of θ.

1 Introduction

A fundamental problem in computational algebraic number theory is to determine the Galois group of a polynomial $f(X) \in \mathbb{Q}[X]$. Formally, in this paper we study the computational complexity of the following problem:

{prob1}

Problem 1.1. *Given a nonzero polynomial $f(X)$ over the rationals $\mathbb{Q}$,*

(a) determine the Galois group of f over $\mathbb{Q}$.

ISSN 1433-8092

(b) determine the order of the Galois group of f over $\mathbb{Q}$.

Given two fields, $L \supseteq K$, the Galois group of the extension L/K (written as $Gal\,(L/K)$) is the set of all automorphisms of L that fixes K. Given a polynomial $f(X) \in K[X]$, the splitting field of $f(X)$ is the smallest field $L \supseteq K$ such that $f(X)$ factorizes into linear factors in L. We denote the splitting field of $f(X) \in K[X]$ by K_f. Given a polynomial $f(X) \in K[X]$ its Galois group G is completely determined by its action on the roots of f in K_f. We assume w.l.o.g throughout this paper that f is square-free. Otherwise, we can replace f by $f/gcd(f.f')$ which is square-free with the same Galois group. Thus, if we label the n distinct zeroes of f, we can consider G as a subgroup of the symmetric group S_n. Notice that this subgroup is determined only up to conjugacy (as the labeling of the zeroes of f is arbitrary). Since every subgroup of S_n has a generator set of size $n-1$ (c.f. [14] and [11]), we can specify the Galois group G in size polynomial in n. By computing the Galois group G of a polynomial f we mean finding a small generator set for G as a subgroup of S_n.

We first explain the size of a natural encoding of polynomials $f(X) \in \mathbb{Q}[X]$. Let size(a) denote the length of the binary encoding of an integer a. For a rational $r = p/q$ such that $gcd(p,q) = 1$, let $\text{size}(r) = \text{size}(p) + \text{size}(q)$. A polynomial is encoded as a list of its coefficients. For a polynomial $f(X) = \sum a_i X^i \in \mathbb{Q}[X]$ we define $\text{size}(f) = \sum \text{size}(a_i)$. Thus, for an algorithm taking a polynomial f as input, the input size is $size(f)$.

Given as input $f(X) \in \mathbb{Q}[X]$ there is a deterministic algorithm due to Landau [7] that computes the Galois group of f in time polynomial in the cardinality of the Galois group (also see [4]). However, this is not an efficient algorithm as the Galois group can be of cardinality exponential in n. It is still open if Problem 1.1(a), or even Problem 1.1(b), has a polynomial (in size(f)) time algorithm (c.f. the survey by Adleman and McCurley [1]). Neither is a better upper bound than the exponential-time algorithm mentioned above known, nor is any nontrivial hardness result known for the problem. Problem 1.1(b) is polynomial-time reducible to Problem 1.1(a).[1]

The Galois group of a polynomial is a fundamental object of study in algebraic number theory. We recall the celebrated result of Galois: a polynomial f over $\mathbb{Q}$ is said to be solvable by radicals if we can compute its zeroes from the coefficients by the standard arithmetic operations and taking rth roots, for any positive integer r. Galois theorem states that a polynomial $f \in \mathbb{Q}[X]$ is solvable by radicals if and only if its Galois group is a solvable group. Landau and Miller in [8] showed that the problem of testing whether the Galois group of a polynomial $f \in \mathbb{Q}[X]$ is solvable can be done in polynomial time. However, even when the Galois group is solvable, no polynomial-time algorithm is known for Problem 1.1(a) or Problem 1.1(b).

Summary of results

In this paper we prove the following new complexity upper bounds for some special cases of Problems 1.1(a) and (b), assuming the generalized Riemann hypothesis (henceforth GRH).

1. Given a polynomial $f \in \mathbb{Q}[X]$, the order of its Galois group can be computed by a polynomial time algorithm with one query to a #P oracle. This yields a *polynomial-space*

[1] Given a generator set for a subgroup G of S_n we can compute $|G|$ in time polynomial in n [11].

algorithm for Problem 1.1(b). In contrast, we observe here that Landau's algorithm [7] requires more than polynomial space.

2. If the Galois group of the polynomial is solvable then we get a randomized algorithm with NP oracle that *exactly* computes the order of its Galois group.

3. Assuming the GRH, we have a polynomial time randomized algorithm for computing the Galois group for a polynomial f with *abelian* Galois group. Previously, a polynomial-time algorithm was known only for the case when f is *irreducible* and has an abelian Galois group [7] (also see [4]), because in that case the Galois group has only $\deg(f)$ many elements.

Our main tool is an effective version of the Chebotarev density theorem, which holds assuming the GRH.

1.1 Galois theory background

We now recall some basic facts of Galois theory from [9, 16]. An *extension* of a field K is a field L that contains K. The extension is written as L/K. If L/K is a field extension then L is a vector space over K, its dimension is called the *degree* of the extension and is denoted by $[L : K]$. If $[L : K]$ is finite then L/K is a *finite* extension. If L/M and M/K are finite extensions then $[L : K] = [L : M].[M : K]$.

Let $K[X]$ denotes the ring of polynomials with indeterminate X and coefficients from the field K. $K[X]$ is a unique factorization domain. A polynomial $f(X) \in K[X]$ is *irreducible* if it has no nontrivial factor. If L/K is an extension, any polynomial in $K[X]$ is also a polynomial in $L[X]$. The *splitting field* of a polynomial $f(X) \in K[X]$ (denoted by K_f) is the smallest extension L of K such that f factorizes into linear factors in L. An extension L/K is *normal* if for any irreducible polynomial $f(X) \in K[X]$, f either splits in L or has no root in L. Any normal extension over K is the splitting field of a set of polynomials in $K[X]$. An extension L/K is *separable* if for all irreducible polynomials $f(X) \in K[X]$ there are no multiple roots in L. A normal and separable finite extension L/K is called a *Galois extension.*

An *automorphism* of a field L is a field isomorphism $\sigma : L \to L$. The *Galois group* of a field extension L/K (denoted by $Gal\,(L/K)$) is the subgroup of the group of automorphisms of L that leaves K fixed: i.e. for every $\sigma \in Gal\,(L/K)$, $\sigma(a) = a$ for all $a \in K$. By the Galois group of a polynomial $f \in K[X]$ we mean the Galois group $Gal\,(K_f/K)$. For a subgroup G of automorphisms of L, the *fixed field* L^G is the largest subfield of L fixed by G. We now state the fundamental theorem of Galois.

Theorem 1.2. [9, Theorem 1.1 Chapter VI] *Let L/K be a Galois extension with Galois group G. There is a one-to-one correspondence between subfields E of L containing K and subgroups H of G, given by $E \rightleftharpoons L^H$. The Galois group of $Gal\,(L/E)$ is H and E/K is a Galois extension if and only if H is a normal subgroup of G. If H is a normal subgroup of G and $E = L^H$ then the Galois group of $Gal\,(E/K)$ is G/H.* {funda:g

Roots of polynomials over $\mathbb{Q}$ are *algebraic numbers.* The *minimal polynomial* $T \in \mathbb{Q}[X]$ of an algebraic number α is the unique monic polynomial of least degree with α as a root. *Algebraic integers* are roots of monic polynomials in $\mathbb{Z}[X]$. A *number field* is a finite extension of $\mathbb{Q}$. We can consider number fields as subfields of $\mathbb{C}$, the field of complex numbers. For an algebraic number α, $\mathbb{Q}(\alpha)$ denotes the smallest number field that contains α. If $f(X)$ is the minimal polynomial of α then $\mathbb{Q}(\alpha)$ can be identified with the quotient $\mathbb{Q}[X]/(f(X)\mathbb{Q}[X])$. Every number field K has an element α such that $K = \mathbb{Q}(\alpha)$ (see [9, Theorem 4.6 Chapter V]). Such elements are called *primitive* elements of the field K.

Let $f \in \mathbb{Q}[X]$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Q}_f$. How do we obtain a primitive element for $\mathbb{Q}_f$? A well known lemma [16] states that $\mathbb{Q}_f$ has a primitive element of the form $\sum_{i=1}^n c_i\alpha_i$ for integers c_i. The proof actually yields a probabilistic version which states that $\sum_{i=1}^n c_i\alpha_i$ is primitive for most c_i.

{random:

Lemma 1.3. *Let $f \in \mathbb{Q}[X]$ be a degree n polynomial with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. For a random choice of integers $c_1, c_2, \ldots, c_n$ such that size$(c_i) \le n^2$ the algebraic integer*

$$\theta = \sum_{i=1}^{n} c_i\alpha_i$$

is such that $L = \mathbb{Q}(\theta)$ with probability $1 - \frac{1}{2^{O(n^2)}}$.

Let L be a number field and O_L be the ring of algebraic integers in L. We can write O_L as $O_L = \{\sum_{i=1}^N a_i\omega_i \mid a_i \in \mathbb{Z}\}$ where $\omega_1, \omega_2, \ldots, \omega_N$ is its $\mathbb{Z}$-basis. The *discriminant* d_L of the field L is defined as the determinant of the matrix $(\mathrm{Tr}(\omega_i\omega_j))_{i,j}$ where $\mathrm{Tr} : L \to \mathbb{Q}$ is the trace map. The discriminant d_L is always a nonzero integer. Let θ be an algebraic integer that is a primitive element of L and $T(X)$ be the minimal polynomial of θ, which is also of degree N. The discriminant $d(T)$ of the polynomial T is defined as $d(T) = \prod_{i\neq j}(\theta_i - \theta_j)$, where $\theta_1, \theta_2, \ldots, \theta_N$ are the N distinct roots of T (i.e. all the conjugates of θ). The following is important property that relates $d(T)$ and d_L.

Proposition 1.4. [3, Proposition 4.4.4] *Let L be a number field and T be the minimal polynomial of a primitive element θ of L. Then $d_L \mid d(T)$. More precisely, $d(T) = d_L \cdot t^2$, for an integer t.*

For any polynomial $g(X) = a_0 + a_1X + \ldots + a_nX^n$ with complex coefficients, let $|g|_2 = \sqrt{\sum |a_i|^2}$. Applying an inequality [6] which bounds every root η of g by $|g|_2$, we obtain the following.

{bound:c

Theorem 1.5. *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree n with splitting field L. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of f. Consider an element of the form $\theta = \sum c_i\alpha_i$, $c_i \in \mathbb{Z}$, and let T be the minimal polynomial of θ. If $N = deg(T)$ then $d(T) \le (2c|f|_2)^{N^2}$, where $c = \max\{|c_i| : 1 \le i \le n\}$. As a consequence, $d_L \le (2^{n^2}|f|_2)^{n!^2}$ and $\log d_L \le (n+1)!^2.\mathrm{size}(f)$.*

A polynomial $f(X) \in \mathbb{Q}[X]$ is said to be solvable by radicals if the roots of f can be expressed, starting with the coefficients of f, using only field operations and taking r^{th} roots for integer r. Galois showed that a polynomial is solvable by radicals if and only if its

Galois group is solvable. Implicit in his proof is an exponential-time algorithm to check if a polynomial is solvable by radicals. As already mentioned, Landau and Miller in [8] give a polynomial-time algorithm to check whether a given polynomial is solvable by radicals by avoiding the computation of the Galois group.

We now state Landau's result on computing the Galois group of a polynomial f. Its worst case running time is exponential in $\text{size}(f)$.

Theorem 1.6. [7] *Given a polynomial $f \in F[X]$, where the number field F is given as a vector space over $\mathbb{Q}$, the Galois group G of f over F can be computed in time polynomial in $|G|$ and $\text{size}(f)$.* {splitfi

1.2 Complexity Theory definitions

We briefly recall the definitions and notation for some standard complexity classes. Details can be found in a standard text, e.g. [2]. Let P denote the class of languages (decision problems) that are accepted by deterministic Turing machines in time bounded by a polynomial in input size, and NP denote the class of languages accepted by nondeterministic Turing machines in polynomial time. Likewise, we denote by BPP the class of decision problems that are accepted by polynomial-time bounded randomized Turing machines with error probability bounded by 1/3. By abuse of notation we also denote functions computable in deterministic polynomial time by P, and denote by BPP the class of functions computable by polynomial-time bounded randomized Turing machines with error probability bounded by 1/3.

A function $f : \{0,1\}^* \to \mathbb{N}$ is said to be in the counting class #P if there is a polynomial time nondeterministic Turing machine M such that $f(x)$ is the number of accepting paths of M on input x. We recall that #P functions can be computed in polynomial space.

A function f in the class P^A is computable by polynomial-time deterministic *oracle* Turing machine M which has access to oracle A: M can enter a special query state and query the membership of a string y in A. We can similarly define P^f for a function oracle f, and the classes BPP^A and BPP^f.

2 Chebotarev Density theorem

The main tool in the proofs of our complexity results is the Chebotarev density theorem. In this section we explain the theorem statement and also state it in a form that is suitable for our applications.

Let L be a number field and O_L be the ring of algebraic integers in L. Let $n = [L : \mathbb{Q}]$ be the degree of L. For any prime $p \in \mathbb{Q}$ consider the principal ideal pO_L generated by p (which we denote by p). Suppose the ideal p factorizes in O_L as $p = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_g^{e_g}$.

Then for each i, $O_L/\mathfrak{p}_i$ is a finite field of characteristic p with p^{f_i} elements for positive integers f_i such that $n = \sum_{i=1}^{g} e_i f_i$. Furthermore, if L is a Galois extension of $\mathbb{Q}$ then $e_1 = e_2 = \ldots = e_g = e$ and $f_1 = f_2 = \ldots = f_g = f$ for positive integers e and f, and thus $efg = n$. For the rest of this section we assume that $L/\mathbb{Q}$ is a Galois extension.

The prime p is said to be *ramified* in L if $e > 1$ and *unramified* otherwise. It is a basic fact about number fields that a prime p is ramified in L if and only if p divides the discriminant of L (see [13]).

For any unramified prime p if $\mathfrak{p}|p$ in O_L then there is an element $\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right) \in Gal\,(L/\mathbb{Q})$ known as the Frobenius element such that

$$\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right)\alpha = \alpha^p \pmod{\mathfrak{p}},\ \ \alpha \in O_L.$$

Furthermore, it is known that the set

$$\left[\frac{L/\mathbb{Q}}{p}\right] = \left\{\left(\frac{L/\mathbb{Q}}{\mathfrak{p}}\right) : \mathfrak{p}|p\right\}$$

is a conjugacy class in the Galois group G.

Now, for any conjugacy class C of G define the integer-valued function $\pi_C(x)$ as follows

$$\pi_C(x) = \left|\left\{p \leq x : p \text{ unramified prime and } \left[\frac{L/\mathbb{Q}}{p}\right] = C\right\}\right|.$$

We are now ready to state the Chebotarev density theorem.

{chebo}

Theorem 2.1 (Chebotarev density theorem). *Let $L/\mathbb{Q}$ be a Galois extension and $G = Gal\,(L/\mathbb{Q})$ be its Galois group. Then for every conjugacy class C of G, $\pi_C(x)$ converges to $\frac{|C|}{|G|}\cdot\frac{x}{\log x}$ as $x \to \infty$.*

In order to apply the above theorem in a complexity-theoretic context, we need the following effective version due to Lagarias and Odlyzko [5] proved assuming the GRH.

{eff:che

Theorem 2.2. *Let $L/\mathbb{Q}$ be a Galois extension and $G = Gal\,(L/\mathbb{Q})$ be its Galois group. If the GRH is true then there is an absolute constant x_0 such that for all $x > x_0$:*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\frac{x}{\log x}\right| \leq O\left(\frac{|C|}{|G|}x^{1/2}\log d_L + x^{1/2}\log x.|G|\right).$$

A useful special case is for the conjugacy class $C = \{1\}$, the identity element in G. A prime p such that $\left[\frac{L/\mathbb{Q}}{p}\right] = \{1\}$ is called a *split prime*. By definition, $\pi_1(x)$ denotes the number of split primes $p \leq x$.

{eff:spl

Corollary 2.3. *Let $G = Gal\,(L/\mathbb{Q})$ for a Galois extension $L/\mathbb{Q}$. If the GRH is true then there is an absolute constant x_0 such that for all $x > x_0$:*

$$\left|\pi_1(x) - \frac{1}{|G|}\frac{x}{\log x}\right| \leq O\left(\frac{1}{|G|}x^{1/2}\log d_L + x^{1/2}\log x.|G|\right).$$

3 Computing the order of Galois Groups

{orderse

Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree n without multiple roots and let L denote the splitting field of f. Suppose $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the set of roots of f. Let $d(f) \neq 0$ denote the discriminant of f.

The Galois group $G = Gal\,(L/\mathbb{Q})$ can be seen as a subgroup of S_n because each $\sigma \in G$ is completely determined by the way it permutes the n roots of f. Each $\sigma \in G$, when considered as a permutation in S_n, can be expressed as a product of disjoint cycles. Looking at the lengths of these cycles we get the *cycle pattern* $\langle m_1, m_2, \ldots, m_n\rangle$ of σ, where m_i is the number of cycles of length i, $1 \leq i \leq n$.

If p is a prime such that $p \nmid d(f)$, we can factorize $f = g_1 g_2 \ldots g_s$ into its distinct irreducible factors g_i over $\mathbb{F}_p$. Looking at the degrees of these irreducible factors we get the *decomposition pattern* $\langle m_1, m_2, \ldots, m_n\rangle$ of $f(\text{mod } p)$, where m_i is the number of irreducible factors of degree i.

We now state an interesting fact from Galois theory (see [16, page 198] and [9, Theorem 2.9, Chapter VII]).

{waerder

Theorem 3.1. *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree n such that $d(f) \neq 0$, and let L denote its splitting field. Let $G = Gal\,(L/\mathbb{Q})$. Let p be a prime such that $p \nmid d(f)$. Then there is a conjugacy class C of G such that for each $\sigma \in C$ the cycle pattern of σ is the same as the decomposition pattern of f factorized over $\mathbb{F}_p$. Furthermore, if $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are the n roots of f in its splitting field and if $\mathbb{F}_{p^m}$ is the extension of $\mathbb{F}_p$ where f (mod p) splits then there is an ordering of the roots $\{\alpha'_1, \alpha'_2, \ldots, \alpha'_n\}$ of f in $\mathbb{F}_{p^m}$ such that for all indices k and l, $\sigma(\alpha_k) = \alpha_l$ if and only if the Frobenius automorphism $x \mapsto x^p$ of $\mathbb{F}_{p^m}$ maps α'_k to α'_l.*

Now, given a degree-n polynomial f and $d(f) \neq 0$, for a partition $\overline{n} = \langle m_1, m_2, \ldots, m_n\rangle$ of n, let $\pi_{\overline{n}}(x) = \{p \text{ prime } \mid p \leq x, f \text{ has decomposition pattern } \overline{n} \text{ in } \mathbb{F}_p\}$. Let $G_{\overline{n}}$ be the set of all elements in G with $\overline{n}$ as cycle pattern. Since all elements of the Galois group G in the same conjugacy class have the same cycle pattern, combining Theorem 3.1 with the effective Chebotarev density theorem (Theorem 2.2) we get the following consequence.

{conjuga

Lemma 3.2. *Let f be a degree-n polynomial with $d(f) \neq 0$ and let $\overline{n} = \langle m_1, m_2, \ldots, m_n\rangle$ be a partition of n. If the GRH is true then*

$$\left|\pi_{\overline{n}}(x) - \frac{|G_{\overline{n}}|}{|G|}\frac{x}{\log x}\right| \leq O\left(\frac{|G_{\overline{n}}|}{|G|}x^{1/2}\log d_L + x^{1/2}\log x|G|^2\right),$$

where L is the splitting field of f.

The above theorem is easily proved by noting that $G_{\overline{n}}$ is a union of conjugacy classes of G, and by applying Theorem 2.2 for each conjugacy class contained in $G_{\overline{n}}$. When we add up the inequalities for each conjugacy class we obtain the theorem. Notice that we get $|G|^2$ in the second term as an upper bound for $|G||G_{\overline{n}}|$. We can now show that the prime factors of $|Gal\,(L/\mathbb{Q})\,|$ can be computed in polynomial time with access to an NP oracle given a monic $f \in \mathbb{Z}[X]$ as input.

{primes-

Theorem 3.3. *Assuming GRH, the following problem is in* NP*: Given a prime $p \leq n$, and a monic polynomial $f \in \mathbb{Z}[X]$ with $d(f) \neq 0$ as input, test if p divides the order of the Galois group of f. As a consequence, the set of prime factors of $|Gal\,(\mathbb{Q}_f/\mathbb{Q})\,|$ can be computed in* P^{NP}.

Proof. Let G denote the Galois group of f and s denote $size(f)$. Let X_p denote the set of elements of G of order p. Then X_p is non-empty if and only if p divides $|G|$. Furthermore, X_p is a union of conjugacy classes of G. Consider the set $Y_x = \{$prime $q \mid q \leq x$, and f factorizes in $\mathbb{F}_q$ into distinct irreducible factors of degrees 1 or p with at least one degree p factor $\}$, for any positive integer x. Applying Lemma 3.2, we can see that for $x \geq (n+1)!^6 s^4$ we have Y_x is non-empty if and only if X_p is nonempty. Now, to test if p divides $|G|$, the NP procedure can first guess a prime $q \leq (n+1)!^6 s^4$. To verify that $q \in Y_x$, the procedure next guesses and verifies the factorization of f in $\mathbb{F}_q$, and then checks that each irreducible factor is of degree 1 or p and there is at least one degree p factor.

Since all prime factors of $|G|$ are bounded by n, using the above NP procedure as oracle we can find all the prime factors of $|G|$ in polynomial time. □

We are ready to state the main result of this section: computing the order of the Galois group of a given $f \in \mathbb{Z}[X]$. Assuming GRH we show that it can be computed in $\mathrm{P}^{\#\mathrm{P}}$, which, to the best of our knowledge, gives the first polynomial-space bounded algorithm for the problem. The result is proved by a careful application of Corollary 2.3.

We require the following result on number fields, which we state from Cohen's book [3, Theorem 4.8.13].

{cohen}

Theorem 3.4. *Let $K = \mathbb{Q}(\theta)$ be a number field where θ is an algebraic integer with monic minimal polynomial $T(X)$. Let t be the index of θ, i.e. $t = [O_K : \mathbb{Z}[\theta]]$. Then for any prime p not dividing t if*

$$T(X) = \prod_{i=1}^{g} T_i(X)^{e_i} (\mathrm{mod}\ p),$$

then

$$p = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

in O_K, where, for each i, the finite field $O_K/\mathfrak{p}_i$ is $\mathbb{F}_{p^{f_i}}$ for $f_i = \deg T_i$.

{order}

Theorem 3.5. *Assuming GRH, the order of the Galois group of a monic polynomial $f \in \mathbb{Z}[X]$ can be computed in* $\mathrm{P}^{\#\mathrm{P}}$.

Proof. Let $K/\mathbb{Q}$ be a Galois extension of degree N. If p is a split prime over K then

$$p = \prod_{i=1}^{N} \mathfrak{p}_i,$$

for N distinct prime ideals $\mathfrak{p}_i$ (c.f. [13]). Let $G = Gal\,(K/\mathbb{Q})$. By Corollary 2.3 we have for all $x > x_0$:

$$\left|\pi_1(x) - \frac{1}{|G|}\frac{x}{\log x}\right| \leq \frac{1}{|G|}x^{1/2}\log d_K + x^{1/2}\log x.|G|.$$

If we can count the number $\pi_1(x)$ of split primes less that x, then using the above bounds we can estimate $\frac{1}{|G|}\frac{x}{\log x}$ well enough to find $|G|$. However, the difficulty is that we do not know how to test whether a prime p is a split prime or not in time polynomial in size(f) + size(p). Thus, instead of directly computing $\pi_1(x)$ we consider the following set A_x, for the given polynomial $f \in \mathbb{Z}[X]$: $A_x = \{p \text{ prime} \mid p \leq x, f \text{ splits in } \mathbb{F}_p\}$. Note that the language $L = \{(x, p, f) \mid p \text{ prime}, f \in \mathbb{Z}[X], p \leq x, \text{ and } p \in A_x\}$ is in P. For, in time polynomial in size(f) and size(p) we can check if all the factors of f in $\mathbb{F}_p$ are linear [17]. Thus the function $h(f, x) = |A_x|$ is in #P. We will now argue that $|A_x|$ approximates $\pi_1(x)$ closely enough for us to compute $|G|$ using the bounds of Corollary 2.3.

Let S_x denote the set of split primes bounded by x. We observe that $S_x \subseteq A_x$. To see this, let $p \in S_x$ and $\mathfrak{p}$ be any prime ideal that divides p. Then the field $O_L/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$ because p is a split prime. Now, notice that f splits in the field $O_L/\mathfrak{p}$: the roots of f in the field $O_L/\mathfrak{p}$ are $\alpha_i + \mathfrak{p}, 1 \leq i \leq n$. Thus, f also splits in $\mathbb{F}_p$, implying that $p \in A_x$.

Next, we argue that $|A_x \setminus S_x|$ is small relative to $|A_x|$. Consider a primitive element $\theta = \sum_{i=1}^{n} c_i\alpha_i$, $size(c_i) \leq n^2$, of $\mathbb{Q}_f$. Such an element is guaranteed to exist by Lemma 1.3. Notice that for every prime $p \in A_x$, the minimal polynomial $T(X)$ of θ also splits in $\mathbb{F}_p$. This is because, θ and its conjugates are all integer linear combinations of the roots of f and hence they all lie in $\mathbb{F}_p$. Thus, if $p \in A_x$ such that $p \nmid d(T)$ then, by Theorem 3.4, p is actually a split prime. Therefore, if a prime in A_x is not a split prime it must be a divisor of $d(T)$. More precisely, $A_x \setminus S_x$ is contained in the set of prime divisors of $d(T)$. From the bound in Theorem 1.5, it follows that $|A_x \setminus S_x| \leq \text{size}(f).((n+1)!)^2$. Hence, if we substitute $|A_x|$ for $\pi_1(x)$ in the inequality given by Corollary 2.3, the bound assumes the following form:

$$\left||A_x| - \frac{1}{|G|}\frac{x}{\log x}\right| \leq \frac{1}{|G|}x^{1/2}\log d_L + x^{1/2}\log x.|G| + \text{size}(f).((n+1)!)^2,$$

where the last term size$(f).((n+1)!)^2$ accounts for the discrepancy between $\pi_1(x)$ and $|A_x|$.

Let s denote size(f). The following claim, which is an easy consequence of the above inequality, shows that if we choose $x \geq (n+1)!^{10}s^2$, then $|A_x|$ approximates $\pi_1(x)$ closely enough to compute $|G|$ using the above inequality.

{claim-a

Claim 3.5.1.

1. *If* $x \geq (n+1)!^6(\log d_L)^2$ *then*

$$|A_x| \geq \left(1 - \frac{1}{(n+1)!}\right)\frac{1}{|G|}\frac{x}{\log x}.$$

2. *If* $x \geq (n+1)!^{10}s^2$ *then*

$$|G| - \frac{1}{(n+1)!} \leq \frac{1}{|A_x|}\frac{x}{\log x} \leq |G| + \frac{1}{(n+1)!}.$$

We are now ready to describe the $\mathrm{P}^{\#\mathrm{P}}$ procedure for computing the order of Galois groups. We first observe that the language $L = \{(x,p) \mid p \text{ prime and } p \leq x, p \in A_x\}$ is clearly in P. Thus, the function $h(x) = |A_x|$ is in #P. The $\mathrm{P}^{\#\mathrm{P}}$ procedure for computing $|G|$ is as follows: for $x = (n+1)!^{10}s^2$, compute $h(x) = |A_x|$ with one #P query. Finally, the procedure will compute (in polynomial time) the integer nearest to $\frac{1}{|A_x|}\frac{x}{\log x}$, which is the required value of $|G|$. This completes the proof. $\square$

Next we consider the approximate counting problem.

Definition 3.6. *A randomized algorithm $\mathcal{A}$ is an r-approximation algorithm for a #P function f with error probability $\delta < \frac{1}{2}$ if for all $x \in \{0,1\}^*$:*

$$Prob_y \left[|1 - \frac{\mathcal{A}(x,y)}{f(x)}| \leq r(|x|) \right] \geq 1 - \delta,$$

where y is a uniformly chosen random string used by the algorithm $\mathcal{A}$ on input x.

Stockmeyer [15] showed that for any #P function there is a $n^{-O(1)}$-approximation $\mathrm{BPP}^{\mathrm{NP}}$ algorithm. This immediately yields the following approximate counting algorithm for the order of the Galois group of $f(X) \in \mathbb{Z}[X]$.

{approx:

Theorem 3.7. *Let $f(X) \in \mathbb{Z}[X]$ be a degree n polynomial, G be its Galois group, and s denote size(f). For any constant $c > 0$ there is a $\mathrm{BPP}^{\mathrm{NP}}$ algorithm that computes an approximation A of $|G|$ such that*

$$\left(1 - \frac{1}{s^c}\right) A \leq |G| \leq \left(1 + \frac{1}{s^c}\right) A.$$

with probability greater than $\frac{2}{3}$.

We now derive a useful lemma as an immediate consequence of the above result.

{star}

Lemma 3.8. *Let f and g be monic polynomials in $\mathbb{Z}[X]$ with nonzero discriminant. Suppose the splitting field $\mathbb{Q}_g$ of g is contained in $\mathbb{Q}_f$ of f and $[\mathbb{Q}_f : \mathbb{Q}_g]$ is a prime power p^l. There is a $\mathrm{BPP}^{\mathrm{NP}}$ algorithm that computes $[\mathbb{Q}_f : \mathbb{Q}_g]$ exactly, assuming that $|Gal\,(\mathbb{Q}_g/\mathbb{Q})\,|$ is already computed.*

Proof. To see this it suffices to note that as $[\mathbb{Q}_f : \mathbb{Q}_g]$ is a prime power of a small prime $p \leq n = \deg f$, if we approximate $[\mathbb{Q}_f : \mathbb{Q}_g]$ using the $\mathrm{BPP}^{\mathrm{NP}}$ algorithm of Theorem 3.7 to within an inverse polynomial fraction, we will compute $[\mathbb{Q}_f : \mathbb{Q}_g]$ exactly. Such an approximation can be computed by first computing $[\mathbb{Q}_f : \mathbb{Q}]$ approximately and dividing it by $[\mathbb{Q}_g : \mathbb{Q}]$, which is already computed by assumption. $\square$

4 Computing the order of solvable Galois Groups

{sol:ord

In this section we show that if the Galois group G of $f \in \mathbb{Z}[X]$ is *solvable* then $|G|$ can be computed exactly in $\mathrm{BPP}^{\mathrm{NP}}$, assuming GRH. In fact, we show that for solvable Galois groups, finding $|G|$ is polynomial-time reducible to approximating $|G|$. In this section we rely heavily on the results from the seminal paper by Landau and Miller [8]. We begin by recalling some definitions.

A group G is said to be *solvable* if there is a *composition series* of G, $G = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ such that G_i/G_{i+1} is a cyclic group of prime order. Throughout this section by composition series we mean such a composition series.

A Galois extension K/F is said to be *solvable* if $Gal\,(K/F)$ is a solvable group. Let $G = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ be a composition series of G. We can find a corresponding tower of fields $F = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_t = K$ such that $Gal\,(K/E_i) = G_i$. Moreover if K/F is Galois then by the fundamental theorem of Galois (Theorem 1.2), since $G_i \rhd G_{i+1}$, the extension E_{i+1}/E_i is Galois.

At this point we recall some permutation group theory (c.f. [18]): Let G be a subgroup of S_n acting on a set $\Omega = \{1, 2, \ldots, n\}$ of n elements. G is said to be *transitive* if for every pair of distinct elements $i, j \in \Omega$, there is a $\sigma \in G$ such that σ maps i to j, written as $i^\sigma = j$. A *block* is a subset $B \subseteq \Omega$ such that for every $\sigma \in G$ either $B^\sigma = B$ or $B^\sigma \cap B = \emptyset$. If G is transitive then under G-action blocks are mapped to blocks, so that starting with a block $B_1 \subseteq \Omega$ we get a *complete block system* $\{B_1, B_2, \ldots, B_s\}$ which is a partition of Ω. Notice that singleton sets and Ω are blocks for any permutation group. These are the *trivial* blocks. A transitive group G is *primitive* if it has only trivial blocks. Otherwise it is called *imprimitive*. A *minimal block* of an imprimitive group is a nontrivial block of least cardinality. The corresponding block system is a *minimal block system*.

The following result about solvable primitive permutation groups [12] has been used to show polynomial time bounds for several permutation group algorithms [11]. In particular, it plays a crucial role in the Landau-Miller results [8].

Theorem 4.1 (Pálfy's bound). [12] *If $G < S_n$ is a solvable primitive group then $|G| \leq n^{3.25}$.*

Let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial and let G be the Galois group $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ which acts transitively on the set of roots $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of f. Let $\{B_1, B_2, \ldots, B_s\}$ be the minimal block system of Ω under the action of G and H be the subgroup of G that setwise stabilizes all the blocks: i.e. elements of H map B_i to B_i for each i. Let $B_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$, where $k = n/s$. Consider the polynomial $p(X) = \prod_{i=1}^{k}(X - \alpha_i) = \sum_{i=0}^{k} \delta_i X^i$.

In [8] it is shown that $p(X) \in \mathbb{Q}(\alpha_1)[X]$ and there is a polynomial time deterministic algorithm to find $p(X)$: the algorithm computes each coefficient δ_i as a polynomial $p_i(\alpha_1)$ with rational coefficients. In polynomial time we can compute a primitive element β_1 of $\mathbb{Q}(\delta_0, \delta_1, \ldots, \delta_k)$ [8] so that $\mathbb{Q}(\beta_1) = \mathbb{Q}(\delta_0, \delta_1, \ldots, \delta_k)$. Let $g(X) \in \mathbb{Z}[X]$ be the minimal polynomial of β_1. In the following theorem we recall some results from [8], suitably rephrased.

Theorem 4.2. {g:theor

1. *The degree of* $g(X)$ *is* s.

2. $H = Gal\,(\mathbb{Q}_f/\mathbb{Q}_g)$ *and* $Gal\,(\mathbb{Q}_g/\mathbb{Q}) = G/H$.

3. *The Galois group* $Gal\,(\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1))$ *acts primitively on* B_1.

Let $Gal\,(\mathbb{Q}(B_1)/\mathbb{Q}(\beta)) = G^{B_1} = G_0 \rhd G_1 \rhd \ldots \rhd G_t = 1$ be a composition series of the solvable group G^{B_1} and let $\mathbb{Q}(\beta_1) = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_t = \mathbb{Q}(B_1)$ be the corresponding tower of subfields of the extension $\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1)$. Since K_{i+1}/K_i is an extension of prime degree for each i we have the following proposition.

{minimal

Proposition 4.3. *For all* $0 \leq i < t$ *if* K' *be any field such that* $K_i \subseteq K' \subseteq K_{i+1}$ *then either* $K' = K_i$ *or* $K' = K_{i+1}$.

For each field K_j in the above tower, let θ_j be a primitive element, $0 \leq j \leq t$. I.e. $\mathbb{Q}(\theta_j) = K_j$ for each j. Let $h_j(X) \in K_{j-1}[X]$ be the minimal polynomial of θ_j over K_{j-1}. We can consider $h_j(X)$ as $h_j(X, \theta_{j-1})$, a polynomial over $\mathbb{Q}$ in the indeterminate X and the algebraic number θ_{j-1} as parameter. As before let $G = \cup_{i=1}^{s} H\sigma_i$. For each field K_j let K_{ij} be the conjugate field under the action of σ_i. More precisely, let $K_{ij} = K_j^{\sigma_i}$ and $\theta_{ij} = \theta_j^{\sigma_i}$. We have the following proposition which follows from the fact that σ_i is a field isomorphism which maps the extension $\mathbb{Q}(B_1)/\mathbb{Q}(\beta_1)$ to $\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i)$, for each i.

Proposition 4.4.

1. $K_{i0} \subseteq K_{i1} \subseteq \ldots \subseteq K_{it}$ *forms a tower of fields of the extension* $\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i)$ *corresponding to the composition series of* $Gal\,(\mathbb{Q}(B_i)/\mathbb{Q}(\beta_i))$.

2. $Gal\,(K_{it}/K_{ij}) = \sigma_i^{-1} G_j \sigma_i$.

3. $K_{ij} = \mathbb{Q}(\theta_{ij})$, *where* $\theta_{ij} = \theta_j^{\sigma_i}$.

4. *The minimal polynomial of* θ_{ij} *over the field* K_{ij-1} *is* $h_{ij}(X) = h_j(X, \theta_{ij-1})$.

For each i, let $\overline{h}_i(X)$ denote the minimal polynomial of θ_i over $\mathbb{Q}$ and let n_i be its degree. We have the following lemma about $\overline{h}_i$'s.

{hbar}

Lemma 4.5.

1. $n_0 = [\mathbb{Q}(\beta_1) : \mathbb{Q}]$ *and* $n_i = p_i n_{i-1}$, *where* $[K_i : K_{i-1}] = p_i$ *for each* i.

2. *If* C_i *be the set of all conjugates of* θ_i *then* $\overline{h}_{i+1}(X) = \prod_{\theta \in C_i} h_{i+1}(X, \theta)$.

Proof. Since $h_0 = g$, the minimal polynomial of $\theta_0 = \beta_1$ it follows that $n_0 = [\mathbb{Q}(\beta_1) : \mathbb{Q}]$. Furthermore, since $\mathbb{Q}(\theta_i) \cong \mathbb{Q}[X]/\overline{h}_i$ we have

$$n_i = [\mathbb{Q}(\theta_i) : \mathbb{Q}] = [\mathbb{Q}(\theta_i) : \mathbb{Q}(\theta_{i-1})].[\mathbb{Q}(\theta_{i-1}) : \mathbb{Q}] = p_i.n_{i-1}.$$

Notice that $n_i = n_0.\prod_{l=1}^{i} p_l$.

Let $h^*(X) = \prod_{\theta \in C_i} h_{i+1}(X, \theta)$. Since C_i is the set of all conjugates of θ_i, it follows that $h^*(X) \in \mathbb{Q}[X]$. Furthermore, since $h_{i+1}(X, \theta_i) \mid h^*(X)$ and since $h_{i+1}(X, \theta_i)$ is the minimal polynomial of θ_{i+1} over $\mathbb{Q}(\theta_i)$, θ_{i+1} is a root of h^*. Notice that $|C_i|$ is the number of conjugates of θ_i over $\mathbb{Q}$, which is $[\mathbb{Q}(\theta_i):\mathbb{Q}] = n_i$. Thus, the degree of h^* is $p_{i+1}.n_i = n_{i+1}$. It follows that h^* has to be the minimal polynomial $\overline{h}_{i+1}$ of θ_{i+1} over $\mathbb{Q}$.

□

We first recall a lemma from Lang [9, Theorem 1.12, Chapter VI]. {diamond

Lemma 4.6. *Let $K \supseteq k$ be number fields such that K/k is a Galois extension. Let F be an arbitrary finite extension of k then KF/F is Galois and $Gal\,(KF/F) \cong Gal\,(K/K\cap F)$.*

Let $E_i = \mathbb{Q}_{\overline{h}_i}$, $0 \le i \le t$, so that $E_0 \subseteq E_1 \subseteq \ldots E_t$ is a tower of field extensions, where $E_i/\mathbb{Q}$ is a Galois extension for each i. Notice that $\mathbb{Q}_f = E_t$ and $\mathbb{Q}_g = E_0$. We prove the following theorem on the structure of each of the Galois groups $Gal\,(E_{i+1}/E_i)$. {main:th

Theorem 4.7. *Let p_i be the order of G_i/G_{i-1}. For every i there is a l_i such that $Gal\,(E_i/E_{i-1})$ is an abelian group of order $p_i^{l_i}$. Furthermore $Gal\,(E_i/E_{i-1})$ is an elementary abelian p_i-group.*

Proof. To prove the theorem it suffices to show that there is a tower of field extensions $E_{i-1} = L_0 \subset L_1 \subset \ldots L_u = E_i$, such that L_j/L_{j-1} is of degree p_i.

We know that $\overline{h}_i = \prod_{\theta\in C_{i-1}} h_i(X,\theta)$, where C_{i-1} is the set of conjugates of θ_{i-1} (whose minimal polynomial over $\mathbb{Q}$ is $\overline{h}_{i-1}$).

In the sequel, let $u = n_i$ and $p = p_i$. Let $C_{i-1} = \{\xi_1, \xi_2, \ldots, \xi_u\}$ be the conjugates of $\theta_{i-1} = \xi_1$. Similarly, denote by η_1 the element θ_i. The minimal polynomial of η_1 (i.e. θ_i) over $\mathbb{Q}(\xi_1)$ is $h_i(X,\xi_1)$. For $1 \le j \le u$ consider the polynomial $h_i(X,\xi_j)$, choose and fix one of its p roots, and call it η_j. The following claim is immediate because $h_i(X,\xi_1)$ over $\mathbb{Q}(\xi_1)$ is a primitive polynomial.

Claim 4.7.1.

1. *$\mathbb{Q}(\eta_j)/\mathbb{Q}(\xi_j)$ is a cyclic Galois extension of degree p.*
2. *$E_i = \mathbb{Q}(\eta_1, \eta_2, \ldots, \eta_u)$.*

Now, for any j, $1 \le j \le u$, define the field $L_j = \mathbb{Q}(\eta_1, \eta_2, \ldots, \eta_j, \xi_{j+1} \ldots \xi_u)$. In Lemma 4.6, let $K = \mathbb{Q}(\eta_j)$, $k = \mathbb{Q}(\xi_j)$ and $F = \mathbb{Q}(\eta_1, \ldots, \eta_{j-1}, \xi_j, \ldots, \xi_u)$. Note that $KF = L_j$ and $F = L_{j-1}$. Using the Lemma 4.6 we have $Gal\,(L_j/L_{j-1}) \cong Gal\,(K/K\cap F)$. By Proposition 4.3 there is no subfield between K and k. Therefore, either $Gal\,(L_j/L_{j-1})$ is trivial or it is a cyclic group of order p. Hence

$$[E_{i+1}:E_i] = [L_u:L_{u-1}].[L_{u-1}:L_{u-2}]\ldots[L_1:L_0] = p^l$$

for some l. Consider the degree-p polynomial $h_i(X,\xi_j)$. We claim that $h_i(X,\xi_j)$ is either irreducible or splits over E_i. For, otherwise there will be some other prime smaller than p that divides $[E_{i+1}:E_i] = p^l$ which is not possible. It follows that the Galois group $Gal\,(E_{i+1}/E_i)$ is a subgroup of the product group $Gal\,(\mathbb{Q}(\eta_1)/\mathbb{Q}(\xi_1)) \times Gal\,(\mathbb{Q}(\eta_2)/\mathbb{Q}(\xi_2)) \times \ldots \times Gal\,(\mathbb{Q}(\eta_u)/\mathbb{Q}(\xi_u))$. Since each of $Gal\,(\mathbb{Q}(\eta_j)/\mathbb{Q}(\xi_j))$ is a cyclic group of order p, it follows that $Gal\,(E_{i+1}/E_i)$ is an elementary abelian p-group of order p^l. □

Before we prove the main result of this section we describe how the θ_i's and $\overline{h}_i$ can be computed in polynomial time.

4.1 Computing θ_i's and $\overline{h}_i$

{section

Before we describe the exact counting algorithm, we explain how we can efficiently compute the polynomials $\overline{h}_i$ and the elements θ_i described above. We repeatedly use Landau's algorithm (Theorem 1.6).

Recall that G^{B_1} is solvable permutation group whose action on B_1 is primitive. By Palfy's bound, we know that $|G^{B_1}| = O(n^{3.25})$. Therefore, by Theorem 1.6 we can find the splitting field $\mathbb{Q}(\alpha_1, \dots, \alpha_k)$ of $p(X)$, and thus we can explicitly find G^{B_1} which is the Galois group of $p(X)$ over $\mathbb{Q}(\beta_1)$.

Since $|G^{B_1}|$ is $O(n^{3.25})$, we can explicitly list the elements of G^{B_1} and hence find a composition series for it, all in time polynomial in n and $size(f)$. Let $G^{B_1} = G_0 \geq G_1 \geq \dots \geq G_t = 1$ be a composition series for G^{B_1}. Theorem 1.6 can also be used to compute in polynomial time a primitive element $\gamma \in \mathbb{Q}(\alpha_1, \dots, \alpha_k)$, where $\gamma = \sum_{i=1}^{k} c_i \alpha_i$ for some positive integers c_i. Thus, $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha_1, \dots, \alpha_k)$. Recall that the tower of fields corresponding to the computed composition series has the form $\mathbb{Q}(\beta_1) = K_0 \subset K_1 \subset \dots \subset K_t = \mathbb{Q}(\gamma)$. We find a primitive element $\theta_i = t_i(\gamma) \in \mathbb{Q}(\beta_1)[\gamma]$ for each K_i inductively for increasing values of i. Notice that t_i's are polynomials of degree bounded by $|G^{B_1}|$ which is $n^{O(1)}$. First, $\theta_0 = \beta_1$ is already computed. Suppose we have computed $\theta_1, \dots, \theta_{i-1}$. In order to compute θ_i consider the polynomial

$$r(X) = \prod_{\sigma \in G_i} (X - \sigma\gamma) = a_0 + a_1 X + \dots a_m X^m.$$

As $\sigma\gamma$, $\sigma \in G_i$ exhausts the conjugates of γ over K_i, it follows that r is the minimal polynomial of γ over K_i. Hence $\mathbb{Q}(a_0, a_1, \dots, a_m) = K_i$: $\mathbb{Q}(a_0, a_1, \dots, a_m) \subseteq K_i$ and r is also the minimal polynomial of γ over $\mathbb{Q}(a_0, a_1, \dots, a_m)$. Not all the coefficients of r can be in K_{i-1} otherwise r will also be the minimal polynomial of γ over K_{i-1} which leads to the contradiction $K_i = K_{i-1}$. Pick a coefficient $a_j \notin K_{i-1}$ of r. Now, $K_{i-1} = \mathbb{Q}(\theta_{i-1}) \subset \mathbb{Q}(a_j, \theta_{i-1}) \subset K_i$. However, since there is no field between K_i and K_{i-1} (Proposition 4.3), $\mathbb{Q}(\theta_{i-1}, a_j) = K_i$. As a result, by the primitive element Theorem [16], K_i has a primitive element of the form $\theta_{i-1} + c.a_j$ for a positive integer c, where $1 \leq c \leq |G^{B_1}|$. To find such a c, we can cycle over $1 \leq c \leq |G^{B_1}|$, compute the minimal polynomial M_i of $\theta_{i-1} + c.a_j$ over $\mathbb{Q}(\beta_1)$ and check if its degree is $[K_i : \mathbb{Q}(\beta_1)]$. Thus we can find $\theta_i = \theta_{i-1} + c.a_j$ as a polynomial $t_i(\gamma)$ with coefficients in $\mathbb{Q}(\beta_1)$.

Finally, to compute the minimal polynomial $\overline{h}_i$ of θ_i over $\mathbb{Q}$ we can use the following property of resultants.

Lemma 4.8. *Given two monic polynomials $f(X)$ and $g(X)$ over a unique factorization domain R*

$$Res(f, g) = \prod_{\beta \in Roots(g)} f(\beta).$$

For the unique factorization domain $\mathbb{Q}[X, Y]$ let $Res_X(f, g)$ be the resultant of f and g considered as polynomials in y over $\mathbb{Q}[X]$. If M_i is the minimal polynomial of θ_i over $\mathbb{Q}(\beta_1)$, we have

$$\overline{h}_i = \prod_{i=1}^{s} M_i(X, \beta_i) = Res_X(M_i, g),$$

where g is the minimal polynomial of β_1. Since the resultant can be computed in polynomial time [17], we obtain an efficient method to compute $\overline{h}_i$ for each i.

We now prove the main result of this section.

{second}

Theorem 4.9. *Assuming the GRH, there is a* $\mathrm{BPP}^{\mathrm{NP}}$ *procedure that takes as input a monic polynomial* $f \in \mathbb{Z}[X]$ *such that* $d(f) \neq 0$*, and computes* $|Gal\,(\mathbb{Q}_f/\mathbb{Q})\,|$ *exactly when* $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ *is solvable.*

Proof. We first consider the case when f is an irreducible polynomial. Applying the Landau-Miller algorithm [8], the procedure first checks in deterministic polynomial time if $G = Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is solvable. Next, as done in the Landau-Miller paper [8], the procedure computes a minimal block system $\{B_1, B_2, \ldots, B_s\}$ for G acting on the set $\{\alpha_1, \ldots, \alpha_n\}$ of roots of f. As before let $\prod_{\alpha_i \in B_1}(X - \alpha_i) = \sum \delta_i X^i$, and $\mathbb{Q}(\beta_1) = \mathbb{Q}(\delta_0, \delta_1, \ldots, \delta_k)$. Let $g(X)$ be the minimal polynomial of β_1. All this can be computed in polynomial time [8].

As explained before, we can compute the polynomials $\overline{h}_i, 0 \leq i \leq t$, where $\overline{h}_0 = g$ and we have a tower of fields:

$$\mathbb{Q}_{\overline{h}_0} \subset \mathbb{Q}_{\overline{h}_1} \subset \ldots \subset \mathbb{Q}_{\overline{h}_t},$$

where, by Theorem 4.7, $Gal\left(\mathbb{Q}_{\overline{h}_i}/\mathbb{Q}_{\overline{h}_{i-1}}\right)$ is of order p_i^l for some positive integer l.

The computation of $|Gal\,(\mathbb{Q}_f/\mathbb{Q})\,|$ is inductively done. Assume that the algorithm has already computed $|Gal\,(\mathbb{Q}_g/\mathbb{Q})\,|$. Furthermore, assume inductively that the procedure has already computed $|Gal\left(\mathbb{Q}_{\overline{h}_{i-1}}/\mathbb{Q}\right)|$ exactly. Now, by Lemma 3.8, there is a $\mathrm{BPP}^{\mathrm{NP}}$ computation that will exactly compute $|Gal\left(\mathbb{Q}_{\overline{h}_i}/\mathbb{Q}\right)|$. Proceeding thus, the $\mathrm{BPP}^{\mathrm{NP}}$ procedure can compute $|Gal\,(\mathbb{Q}_f/\mathbb{Q})\,|$, given $|Gal\,(\mathbb{Q}_g/\mathbb{Q})\,|$.

The task of computing $|Gal\,(\mathbb{Q}_g/\mathbb{Q})\,|$ by the procedure is recursively done: applying the Landau-Miller algorithm, we can first compute a chain of blocks $B_1 \subset B_1' \subset \ldots B_1^{(l)}$, where B_1' is the smallest block of G that properly contains B_1 and so on. Corresponding to each block $B_1^{(j)}$, we can obtain a polynomial $g^{(j)}$ (like $g(X)$ corresponds to B_1). Thus, in the recursive step, the roles of polynomials f and g is replaced by $g^{(j-1)}$ and $g^{(j)}$. This completes the description of the $\mathrm{BPP}^{\mathrm{NP}}$ procedure.

We now prove the general case (when f is not necessarily irreducible). Let $f = f_1 f_2 \ldots f_s$ be the factorization of f into irreducible factors $f_i \in \mathbb{Z}[X]$, all monic. This can be computed in polynomial time by the LLL algorithm [10]. Let K denote the splitting field of f and L denote the splitting field of $f_2 \ldots f_s$. We can write

$$|Gal\,(K/\mathbb{Q})\,| = |Gal\,(L/\mathbb{Q})\,|.|Gal\,(K/L)\,| = [K:L].[L:\mathbb{Q}].$$

Now the idea is to first compute $|Gal\,(L/\mathbb{Q})\,|$ and then compute $|Gal\,(K/L)\,|$ by applying Lemma 4.6 and reducing to the case of the irreducible polynomial f_1. Proceeding as for irreducible polynomials, we first compute polynomials $\overline{h}_i, 0 \leq i \leq t$, where $\overline{h}_0 = g$ and $\mathbb{Q}_{\overline{h}_t} = \mathbb{Q}_{f_1}$ such that the tower of fields $\mathbb{Q}_{\overline{h}_0} \subset \ldots \subset \mathbb{Q}_{\overline{h}_t}$ satisfies the condition that each extension $\mathbb{Q}_{\overline{h}_i}/\mathbb{Q}_{\overline{h}_{i-1}}$ is of order a power of a prime p_i. We can now write

$$|Gal\,(K/\mathbb{Q})\,| = [L\mathbb{Q}_{\overline{h}_t} : \mathbb{Q}] = [L\mathbb{Q}_{\overline{h}_0} : \mathbb{Q}].\prod_{i=1}^{t}[L\mathbb{Q}_{\overline{h}_i} : L\mathbb{Q}_{\overline{h}_{i-1}}].$$

Again, assume that the $\mathrm{BPP}^{\mathrm{NP}}$ procedure has recursively computed $|Gal\left(L\mathbb{Q}_{\overline{h}_0}/\mathbb{Q}\right)|$, which is $[L\mathbb{Q}_{\overline{h}_0} : \mathbb{Q}]$, exactly. It only remains to exactly compute $[L\mathbb{Q}_{\overline{h}_i} : L\mathbb{Q}_{\overline{h}_{i-1}}]$ for $0 \leq i \leq t$. Recursively, assume that the procedure has computed $[L\mathbb{Q}_{\overline{h}_{i-1}} : \mathbb{Q}]$. Now, by Lemma 4.6 we have

$$[L\mathbb{Q}_{\overline{h}_i} : L\mathbb{Q}_{\overline{h}_{i-1}}] = [\mathbb{Q}_{\overline{h}_i} : F],$$

where $F = \mathbb{Q}_{\overline{h}_i} \cap L\mathbb{Q}_{\overline{h}_{i-1}}$. But $\mathbb{Q}_{\overline{h}_{i-1}} \subseteq F \subseteq \mathbb{Q}_{\overline{h}_i}$. Thus $[\mathbb{Q}_{\overline{h}_i} : F]$ is also a power of p_i.

Now, by applying Lemma 3.8 we can compute $[L\mathbb{Q}_{\overline{h}_i} : L\mathbb{Q}_{\overline{h}_{i-1}}]$ exactly, as we have already computed $[L\mathbb{Q}_{\overline{h}_{i-1}} : \mathbb{Q}]$. The product of these two integers also gives $[L\mathbb{Q}_{\overline{h}_i} : \mathbb{Q}]$. This completes the description of the $\mathrm{BPP}^{\mathrm{NP}}$ procedure. The pseudo-code is given in the appendix. □

5 Finding the Galois group of an abelian extension

Let f be a polynomial over $\mathbb{Z}[X]$ such that $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian. In this section we give a polynomial-time randomized algorithm that computes the Galois group (as a set of generators) with constant success probability.

Suppose $f \in \mathbb{Z}[X]$ is monic, irreducible, degree n polynomial with Galois group G. Since G is a transitive subgroup of S_n, if G is abelian then $|G| = n$. Thus, given an irreducible $f \in \mathbb{Z}[X]$, the algorithm of Theorem 1.6 gives a $(\mathrm{size}(f))^{O(1)}$ algorithm for testing if its Galois group is abelian, and if so, finding the group explicitly. On the other hand, when f is reducible with abelian Galois group, no polynomial time algorithm is known for computing the Galois group (c.f. Lenstra [4]). However, for any polynomial f testing if its Galois group is abelian can be done in polynomial time: we only need to test if the Galois group of each irreducible factors of f is abelian.

Let f be a polynomial over $\mathbb{Z}[X]$ such that $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian. Let $f = f_1 f_2 \dots f_t$ be its factorization into irreducible factors f_i. Notice that if $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian then $Gal\,(\mathbb{Q}_{f_i}/\mathbb{Q})$ is abelian for each i. Consequently, each f_i is a primitive polynomial (i.e. f_i splits in any number field containing at least one root of f_i). Let $G = Gal\,(\mathbb{Q}_f/\mathbb{Q})$ and let $G_i = Gal\,(\mathbb{Q}_{f_i}/\mathbb{Q})$ for each i. Notice that $G \leq G_1 \times G_2 \times \dots G_t$.

Let n_i be the degree of f_i. Since each f_i is a primitive polynomial, $|G_i| = n_i$. Let θ_i be any root of f_i, $1 \leq i \leq t$. Then, $\mathbb{Q}_{f_i} = \mathbb{Q}(\theta_i)$ for each i. Factorizing f_i in $\mathbb{Q}(\theta_i)$, we can express the other roots of f_i as $A_{ij}(\theta_i)$, where $A_{ij}(X)$ are all polynomials of degree at most n_i, $1 \leq j \leq n_i$. We can efficiently find these polynomials $A_{ij}(X)$ for $1 \leq i \leq t$, $1 \leq j \leq n_i$. Thus we can write $f_i(X) = \prod_{j=1}^{n_i} (X - A_{ij}(\theta_i))$, where θ_i is one of the roots of f_i. We prove the following lemma which allows us to identify the polynomials A_{ij} with the elements of the group G_i in an unambiguous manner.

{abel}

Lemma 5.1. *Let θ be any root of f_i and let A_{ij} be polynomials of degree less than* $\deg(f_i)$ *such that $f_i(X) = \prod_{j=1}^{n_i}(X - A_{ij}(\theta))$. Then for $1 \leq j < deg(f_i)$, we have $A_{ij}(A_{ik}(\theta)) = A_{ik}(A_{ij}(\theta))$. Furthermore, for every $\sigma \in G_i$ there is an index $k, 1 \leq k \leq n_i$ such that for any root η of $f_i(X)$ we have $\sigma(\eta) = A_{ik}(\eta)$.*

Proof. All the roots of the polynomial f_i are given by $\theta_k = A_{ik}(\theta), 1 \leq k \leq n_i$. Since f_i is irreducible, for each k there is a element of G_i that maps θ to θ_k. Let σ_k be the element of G_i that maps θ to $\theta_k = A_{ik}(\theta)$. We have

$A_{ij}(A_{ik}(\theta)) = \sigma_k(A_{ij}(\theta)) = \sigma_k\sigma_j(\theta) = \sigma_j\sigma_k(\theta)$, because G_i is abelian. But, $\sigma_j\sigma_k(\theta) = A_{ik}(A_{ij}(\theta))$. Thus, $A_{ij}(A_{ik}(\theta)) = A_{ik}(A_{ij}(\theta))$.

Now, consider any root η of f_i. There is a j such that $\eta = \theta_j = A_{ij}(\theta)$. Applying the above identity, notice that σ_k maps η to $A_{ij}(A_{ik}(\theta)) = A_{ik}(A_{ij}(\theta)) = A_{ik}(\eta)$. □

From the above lemma it follows that for each $i, 1 \leq i \leq t$, the polynomials A_{ij}, $1 \leq j \leq n_i$ are independent of the choice of the root θ of f_i because the Galois group is abelian.

Now, let σ_{ij} denote the unique automorphism of $\mathbb{Q}_{f_i}$ that maps θ to $A_{ij}(\theta)$ for every root θ of f_i. Since $G \leq G_1 \times G_2 \times \ldots \times G_t$, any element $\sigma \in G$ is a t-tuple

$$\sigma = \langle \sigma_{1j_1}, \sigma_{2j_2}, \ldots, \sigma_{tj_t} \rangle,$$

for indices $j_1, j_2, \ldots, j_t$.

We will apply the Chebotarev density theorem to determine a generator set for G.

Let q be a prime such that $q \nmid d(f)$ and $\mathbb{F}_{q^m}$ be the extension of $\mathbb{F}_q$ where f splits. Observe that since G is abelian every conjugacy class of G is a singleton set. Let $\pi_g(x)$ denote the number $|\{p \leq x \mid p \text{ a prime and } \left[\frac{L/\mathbb{Q}}{p}\right] = \{g\}\}|$. By Theorem 2.1 $\pi_g(x)$ converges to $\frac{x}{(\log x)|G|}$. Assuming GRH we have, by Theorem 2.2, for every $g \in G$

$$\left|\pi_g(x) - \frac{x}{(\log x)|G|}\right| \leq \frac{x^{1/2}\log d_L}{|G|} + |G|.x^{1/2}.\log x. \qquad (1) \quad \{\texttt{sample}\}$$

Next, fix i and let $\{\alpha_1, \alpha_2, \ldots, \alpha_{n_i}\}$ be the roots of f_i. By Theorem 3.1, there is an ordering $\{\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_{n_i}\}$ of the roots of f_i in $\mathbb{F}_{q^m}$ such that the Frobenius automorphism $x \mapsto x^q$ maps $\overline{\alpha}_k$ to $\overline{\alpha}_l$ if and only if the element g (the unique Frobenius element corresponding to q) maps α_k to α_l. If the element $g = \langle \sigma_{1j_1}, \sigma_{2j_2}, \ldots, \sigma_{tj_t} \rangle$ we can determine σ_{ij_i} as follows: find the splitting field $\mathbb{F}_{q^k}$ of f_i. Since f_i is a primitive polynomial, $k \leq n_i$, thus $\mathbb{F}_{q^k}$ can be found efficiently.[2] Now, factorize f_i in $\mathbb{F}_{q^k}$. Pick any root $\overline{\theta} \in \mathbb{F}_{q^k}$ of f_i. Then $\overline{\theta}^q = A_{ij}(\overline{\theta})$ for exactly one polynomial A_{ij_i}, which can be found by trying all of them. This gives us σ_{ij_i}.

Thus, we can determine g as a t-tuple in polynomial time, in a manner independent of the choice of the root $\overline{\theta}$ of f_i in $\mathbb{F}_{q^k}$, which works correctly because of Lemma 5.1.

As a consequence of inequality 1, we have a nearly uniform polynomial-time sampling algorithm from the Galois group G. More precisely, if we choose $x \geq (n!)^{10}.\text{size}(f)^2$, then the algorithm samples $g \in G$ with probability in the range $(1/|G| - 1/x^{1/4}, 1/|G| + 1/x^{1/4})$.

The following claim shows that by picking a polynomial-sized sample using the sampling algorithm, we can find a generator set for G with high probability. We prove the claim for uniform sampling. The nearly uniform sampler from $G = Gal\,(\mathbb{Q}_f/\mathbb{Q})$ described above can only introduce an additive term that is inverse exponential.

[2] In fact $k|n_i$ because k is the order of the corresponding Frobenius element which is in the Galois group of f_i, and the order of the Galois group is n_i.

{uniform

Lemma 5.2. *Suppose we have a uniform sampling procedure $\mathcal{A}$ from a subgroup G of S_n. Then for every constant $c > 0$, there is a polynomial-time randomized algorithm with $\mathcal{A}$ as subroutine that outputs a generator set for G with error probability bounded by 2^{-n^c}.*

Proof. To see this, let $g_1, g_2, \ldots, g_m$ be a random sample drawn from G using $\mathcal{A}$, where $m = n^{O(1)}$ will be chosen later. To each g_i associate the 0/1 random variable X_i which takes the value 0 if either $\langle g_1, \ldots, g_{i-1} \rangle = G$ or $g_i \notin \langle g_1, \ldots, g_{i-1} \rangle$ and the value 1 otherwise. Let $p_i = \text{Prob}[\langle g_1, \ldots, g_{i-1} \rangle = G]$ and $q_i = \text{Prob}[g_i \notin \langle g_1, \ldots, g_{i-1} \rangle | \langle g_1, \ldots, g_{i-1} \rangle \neq G]$. Since G is a group and $\mathcal{A}$ is a uniform sampler from G, clearly $q_i \geq 1/2$. Thus, we have

$$\text{Prob}[X_i = 0] = p_i + (1 - p_i)q_i \geq 1/2 + p_i/2 \geq 1/2.$$

Let $X = \sum_i X_i$. Applying Markov's inequality we get that

$$\text{Prob}[X \leq 3m/4] \geq 1/3.$$

Hence, letting $m = 4(\log n!)$, the set $\{g_1, g_2, \ldots, g_m\}$ generates G with probability 1/3. The success probability can be boosted by suitably increasing the sample size. Notice that we can use the sifting algorithm for permutation groups (c.f [11]) to prune the generator set to $O(n^2)$ size. This completes the proof of the claim. ☐

We have thus proved the following theorem. The algorithm in pseudo-code for finding abelian Galois groups is given in the appendix.

{abel:th

Theorem 5.3. *There is a randomized polynomial time algorithm for computing a generator set for the Galois group of a polynomial $f \in \mathbb{Z}[X]$ if it is abelian.*

6 Galois group problems over arbitrary number fields

In this section we extend the complexity results of the previous sections to polynomials $f \in K[X]$, where K is an arbitrary number field. We assume that the field K is specified by giving the minimal polynomial $T(X) \in \mathbb{Q}[X]$ of a primitive element θ of K, so that $K = \mathbb{Q}(\theta) = \mathbb{Q}[X]/T(X)$.

W.l.o.g. we can assume that the polynomial $f \in K[X]$ is monic and we can write f as $f = \sum_{i=0}^{n} a_i(\theta)X^i$, where a_i's are polynomials in $\mathbb{Z}[X]$ of degree at most $m - 1$. By *size*(f) we mean $\sum_{i=0}^{n} size(a_i(X))$. Thus the input size is $size(f) + size(T)$.

Let $L = K_f$ and let $G = Gal\,(L/K)$. As in the previous sections, we will be applying the effective Chebotarev density theorem over K. For an ideal $\mathfrak{a}$ of O_K, let $N(\mathfrak{a})$ denote its *norm* over $\mathbb{Q}$ (which is the finite index of the additive subgroup $\mathfrak{a}$ of O_K). For a prime ideal $\mathfrak{p}$ of O_K let $\mathfrak{P}$ be a prime ideal of O_L that divides $\mathfrak{p}O_L$ (which we write as $\mathfrak{p}$). Then $O_L/\mathfrak{P}$ is a finite field extension of $O_K/\mathfrak{p}$. Since L/K is a Galois extension the ideal $\mathfrak{p}$ of O_L factorizes as

$$\mathfrak{p} = \mathfrak{P}_1^e \mathfrak{P}_2^e \ldots \mathfrak{P}_g^e.$$

As before $\mathfrak{p}$ is ramified in L if and only if $e > 1$. If $\mathfrak{p}$ is an unramified prime then for every $\mathfrak{P} \mid \mathfrak{p}$ there is a Frobenius $\left(\frac{L/K}{\mathfrak{P}}\right) \in Gal\,(L/K)$ such that

$$\left(\frac{L/K}{\mathfrak{P}}\right)\alpha = \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for all α in O_L. Similarly the subset $\left[\frac{L/K}{\mathfrak{p}}\right]$ of $Gal\,(L/K)$ defined by

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \left\{\left(\frac{L/K}{\mathfrak{P}}\right) : \mathfrak{P}|\mathfrak{p}\right\}$$

forms a conjugacy class of $Gal\,(L/K)$.

Let C be any conjugacy class of G and let $\pi_C(x)$ denote the function

$$\pi_C(x) = \left|\left\{\mathfrak{p} : \left[\frac{L/K}{\mathfrak{p}}\right] = C \text{ and } N(\mathfrak{p}) \leq x\right\}\right|.$$

We have by the effective version of the Chebotarev density theorem [5].

Theorem 6.1.

$$\left|\pi_C(x) - \frac{|C|}{|G|}\frac{x}{\log x}\right| \leq O\left(\sqrt{x}\log d_L + |C|\sqrt{x}\log x\right).$$

Throughout this section p, q etc. will denote primes in $\mathbb{Z}$, $\mathfrak{p}, \mathfrak{q}$ etc. will denote primes in O_K and $\mathfrak{P}, \mathfrak{Q}$ etc. will denote primes in O_L. For a prime p the $\mathfrak{p}_i$'s will denote its prime factors in O_K. Likewise for a prime $\mathfrak{p}$, $\mathfrak{P}_j$'s will denote its prime factors in O_L.

We first show, analogous to Theorem 3.5, that $[L : K]$ can be computed in polynomial time with a $\#P$ oracle. Observe that if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots of f then, by the primitive element theorem, there are integers $c_1, \ldots, c_n$, $size(c_i) \leq (mn)^2$ such that for $\gamma = \theta + \sum_{i=1}^n c_i\alpha_i$, $L = \mathbb{Q}(\gamma)$. Let $S(X)$ be the minimal polynomial of γ and $\gamma_1, \gamma_2, \ldots, \gamma_N$ be the conjugates of $\gamma = \gamma_1$.

Let $t = (size(f)size(T))^2$. Recall that for any polynomial with complex coefficients $g(X) = \sum_{i=1}^n a_i x^i$, we define $|g|_2 = \sqrt{\sum |a_i|^2}$, and every root η of g by $|g|_2$ [6]. Applying this bound we can easily see the following bound on the discriminant of S.

Lemma 6.2. *The discriminant of S, $d(S)$, is bounded by $C^{t.m.n!^2}$, and hence $\log d(S) = O\left(t.m.n!^2\right)$, where $C > 0$ is an absolute constant.*

We will now get a suitable estimate of $\pi_1(x)$, the number of split prime ideals $\mathfrak{p}$ of O_K with $N(\mathfrak{p}) \leq x$. Let A_x be the set of prime ideals $\mathfrak{p}$ of O_K satisfying the following conditions.

1. $N(\mathfrak{p}) \leq x$.

2. $f(X)$ splits in $O_K/\mathfrak{p}$.

3. If p is the prime such that $\mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z}$ then $p \nmid d(T)$.

We first show that $|A_x|$ is a #P-computable function of x. If p is a prime in $\mathbb{Q}$ such that $p \nmid d(T)$ then p is unramified in K. If T_i's are the irreducible factors of T in $\mathbb{F}_p$ then the prime ideals of O_K that divide p are $\mathfrak{p}_i = pO_K + T_i(\theta)O_K$. Also, implicit in the proof of Theorem 3.4 is the fact $O_K/\mathfrak{p}_i \cong \mathbb{Z}[\theta]/(p, T_i(\theta))$ (see [3]). Now, consider the language L consisting of tuples (x, p, g), where x and p are binary encodings of numbers and g is a suitable encoding of a polynomial in $\mathbb{F}_p$, satisfying the conditions:

- p is a prime such that $p \nmid d(T)$.
- $g(X)$ is a irreducible factor of T in $\mathbb{F}_p$.
- $p^{deg(g)} \leq x$.
- If $\eta = X \pmod{g(X)}$ in $\mathbb{F}_p[X]/g$ then $f(Y) = f(Y, \eta) \in \mathbb{F}_p(\eta)[Y]$ splits in $\mathbb{F}_p(\eta)$.

Clearly $|A_x| = |\{(p, g) : (x, p, g) \in L\}|$. Since $L \in \mathrm{P}$ it follows that $|A_x|$ is #P-computable.

Now we estimate how well $|A_x|$ approximates $\pi_1(x)$. We first state a lemma that will be useful in the proof.

{modlemm

Lemma 6.3. *Let L/K be a number field extension and let O_L and O_K be the corresponding ring of integers. Let $\mathfrak{p}$ be an ideal of O_K and $\mathfrak{P}$ be any one of the prime factors of $\mathfrak{p}O_L$ in O_L. Let $P(X) \in K[X]$ be any polynomial such that for some $\alpha \in O_K$, in the ring O_K we have $P(\alpha) \equiv 0$ (mod $\mathfrak{p}$). Then in O_L we have $P(\alpha) \equiv 0$ (mod $\mathfrak{P}$).*

Proof. $P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ is same as saying $P(\alpha) \in \mathfrak{p}$. Since $\mathfrak{p} = \mathfrak{p}O_K \subset \mathfrak{p}O_L \subset \mathfrak{P}$ we have $P(\alpha) \in \mathfrak{P}$. Hence $P(\alpha) \equiv 0 \pmod{\mathfrak{P}}$ in O_L. □

Lemma 6.4.

$$||A_x| - \pi_1(x)| \leq m(\log d(S) + \log d(T)).$$

Proof. Let S_x be the set of prime ideals of O_K that are split in O_L with $N(\mathfrak{p}) \leq x$. Notice that if $\mathfrak{p} \in S_x$ and if p is the corresponding prime in $\mathbb{Z}$ such that $p \nmid d(T)$ then $\mathfrak{p} \in A_x$. Since p can have 1 m factors in O_K $|S_x \setminus A_x| \leq m \log d(T)$.

Consider any prime $\mathfrak{p}$ in A_x and let p be the corresponding prime in $\mathbb{Z}$. Clearly $p \nmid d(T)$ and hence $\mathfrak{p} = pO_K + g(\theta)O_K$ for some irreducible factor $g(X)$ of $T(X) \pmod{p} \in \mathbb{F}_p[X]$. Also $O_K/\mathfrak{p} \cong \mathbb{Z}[\theta]/(p, g(\theta))$. If $p \nmid d(S)$ then any prime factor $\mathfrak{P}$ of $\mathfrak{p}$ over O_L is given by $\mathfrak{P} = pO_L + h(\gamma)O_L$ and $O_L/\mathfrak{P} \cong \mathbb{Z}[\gamma]/(p, h(\gamma))$, where $h(X)$ is some irreducible factor of $S(X)$ modulo p. We claim that in this case $\mathfrak{p}$ is split over O_L. To prove this we have to show that $[O_L/\mathfrak{P} : O_K/\mathfrak{p}] = 1$.

Observe that since f splits in $O_K/\mathfrak{p}$ we have elements $\eta_1, \eta_2, \ldots, \eta_n \in O_K$ such that $f(\eta_i) \equiv 0 \pmod{\mathfrak{p}}$. Using Lemma 6.3 we have $\eta_i \pmod{\mathfrak{P}}$, $1 \leq i \leq n$, are the roots of f in $O_L/\mathfrak{P}$. $O_L/\mathfrak{P}$ being a field and $\alpha_i \pmod{\mathfrak{P}}$ being roots of f in $O_L/\mathfrak{P}$ we can without lose of generality assume that $\alpha_i \equiv \eta_i \pmod{\mathfrak{P}}$.

If $k = [O_K/\mathfrak{p} : \mathbb{F}_p]$ then $\eta_i^{p^k} - \eta_i \equiv 0 \pmod{\mathfrak{p}}$. Hence we have

$$\alpha_i^{p^k} - \alpha_i \equiv \eta_i^{p^k} - \eta_i \equiv 0 \pmod{\mathfrak{P}}.$$

Also $\theta^{p^k} - \theta \equiv 0 \pmod{\mathfrak{P}}$. Since γ is a $\mathbb{Z}$ linear combination of θ and α_i's we have $\gamma^{p^k} - \gamma \equiv 0 \pmod{\mathfrak{P}}$. Hence $O_L/\mathfrak{P} \cong \mathbb{Z}[\gamma]/(p, h(\gamma)) \cong \mathbb{F}_{p^k} \cong O_K/\mathfrak{p}$ and therefore $\mathfrak{p}$ is a split prime over O_L. As a result for every prime $\mathfrak{p} \in A_x$, $\mathfrak{p} \in S_x$ if $p \nmid d(S)$. As there are at most m primes that divide p in O_K we have $|A_x \setminus S_x| \leq m \log d(S)$. Since $|A_x| - \pi_1(x) = |A_x \setminus S_x| - |S_x \setminus A_x|$, we have

$$||A_x| - \pi_1(x)| \leq m \log d(T) + m \log d(S)).$$

□

As in the proof of Theorem 3.5, we can compute $[L : K]$ by first computing $|A_x|$ for some suitably large x such that $size(x) = (size(f) + size(T))^{O(1)}$ using a single #P query and then computing the integer closest to $\frac{1}{A_x} \frac{x}{\log x}$. Hence we have the following theorem.

Theorem 6.5. *Let $K = \mathbb{Q}[X]/T(X)$ be a finite extension of $\mathbb{Q}$ and let $f(X) \in K[X]$. There is a polynomial time algorithm (polynomial in $size(T) + size(f)$) that makes one query to a* #P *oracle and computes $[K_f : K]$.*

Likewise, we can show the following lemma, analogous to Lemma 3.8.

{Kstar}

Lemma 6.6. *Let $K = \mathbb{Q}[X]/T(X)$ be a finite extension of $\mathbb{Q}$ and let f and g be monic polynomials in $K[X]$ with nonzero discriminant. Suppose the splitting field K_g of g is contained in K_f of f and $[K_f : K_g]$ is a prime power p^l. There is a* $\mathrm{BPP}^{\mathrm{NP}}$ *algorithm that computes $[K_f : K_g]$ exactly, assuming that $|Gal\,(K_g/K)\,|$ is already computed.*

Proceeding exactly as in Section 4 and applying Lemma 6.6, we can prove the following generalization of Theorem 4.9.

Theorem 6.7. *If K_f/K is a solvable extension then there is a randomized polynomial time algorithm with* NP *oracle that computes $[K_f : K]$.*

We now show that if the Galois group of a given $f \in K[X]$ is abelian then there is a randomized polynomial-time algorithm to find a small generator set for it. If $G = Gal\,(K_f/K)$ we show that there is a polynomial-time sampling algorithm for G, such that that for any $\sigma \in G$ the probability that the algorithm generates σ is in the range $\left(\frac{1}{m|G|} - \epsilon, \frac{1}{|G|} + \epsilon\right)$, where $m = [K : \mathbb{Q}]$ and ϵ is inverse exponential in the input size. Using this sampling 0, like in Lemma 5.2, we can easily get a polynomial-time randomized algorithm to compute G.

As before, $K = \mathbb{Q}(\theta)$ is given by the minimal polynomial of θ. More 0, $K = \mathbb{Q}(\theta) = \mathbb{Q}[X]/T$. Let $L = K_f$ and let $G = Gal\,(L/K)$. Pick a prime $p \in \mathbb{Z}$ such that $p \nmid d(T)$. Let T_i's be the factors of T over $\mathbb{F}_p$. The prime ideals of O_K that divides p are given by $\mathfrak{p}_i = pO_K + T_i(\theta)O_K$. Since G is abelian, all conjugacy classes are singleton sets, and hence for any two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ dividing $\mathfrak{p}$ in O_L we have

$$\left[\frac{L/K}{\mathfrak{p}}\right] = \left\{\left(\frac{L/K}{\mathfrak{P}_1}\right)\right\} = \left\{\left(\frac{L/K}{\mathfrak{P}_2}\right)\right\}.$$

Let $f \in K[X]$ be a polynomial such that $G = Gal\,(K_f/K)$ is abelian. Let $f = f_1 f_2 \ldots f_t$ be its factorization into irreducible factors f_i over K and let $G_i = Gal\,(K_{f_i}/K)$ for each

i. Then $G \leq G_1 \times G_2 \times \dots G_t$. Since each G_i is abelian, it follows that each f_i is a primitive polynomial. Thus, $|G_i| = \deg(f_i) = n_i$ and $K_{f_i} = K(\theta_i)$, where θ_i is any root of f_i. Factorizing f_i in $K(\theta_i)$, we can express the other roots of f_i as $A_{ij}(\theta_i)$, where $A_{ij}(X)$ are polynomials of degree at most n_i, $1 \leq j \leq n_i$. We can efficiently find these polynomials $A_{ij}(X)$ for $1 \leq i \leq t$, $1 \leq j \leq n_i$. Thus, $f_i(X) = \prod_{j=1}^{n_i}(X - A_{ij}(\theta_i))$, where θ_i is one of the roots of f_i. Exactly like Lemma 5.1 we can unambiguously identify the polynomials A_{ij} with the elements of the group G_i.

Thus, for any $\mathfrak{p}|p$ in O_K, if $f(X)$ has no multiple roots over $O_K/\mathfrak{p}$ then we can recover the action of the Frobenius $\left(\frac{L/K}{\mathfrak{P}}\right)$ on the roots of f for any $\mathfrak{P}|\mathfrak{p}$ in polynomial time.

We sketch the description of the almost uniform sampling algorithm for sampling prime ideals of O_K. The details are similar to Lemma 5.2. Let $f(X) = f(X, \theta)$ and let $\overline{f}(X) \in \mathbb{Q}[X]$ be $\overline{f}(X) = \prod_{\theta \in Roots(T)} f(X, \theta)$. In the sampling procedure we consider only those primes p that do not divide the discriminant of T and $\overline{f}$. Notice that we will miss out at most $\log d(T) + \log d(\overline{f})$ many primes. The polynomial $\overline{f}$ can be computed by computing $Res_X(f(X,Y), T(Y))$ as in section 4.1. The sampling algorithm is given below.

{algo

Input: Polynomials T and f and an integer x
Output: Prime ideal $\mathfrak{p}$ of O_K such that $N(\mathfrak{p}) \leq x$.
Pick a prime $p \nmid d(T)d(f)$ and $p \leq x$ randomly;
Factorize T over $\mathbb{F}_p$, let the factors be T_i's;
Pick a factor T_i randomly and return $(p, T_i(\theta))$;

Algorithm 1: Almost uniform sampler for prime ideals of O_K

For any $\sigma \in G$ let $\mathcal{P}_\sigma = \left\{\mathfrak{p} : \left[\frac{L/K}{\mathfrak{p}}\right] = \{\sigma\}\right\}$. Since any prime p has at most m prime factors, we can easily argue that the probability that the sampling algorithm 1 returns a prime $\mathfrak{p}$ in P_σ is in the range $\left(\frac{1}{m|G|} - \epsilon, \frac{1}{|G|} + \epsilon\right)$, where ϵ is inverse exponential in the input size. The fraction ϵ accounts for the primes missed out because of considering only those $p \nmid d(T)d(f)$. The above sampling procedure is such that for any $\sigma \in G$ the probability of picking σ is in the range $\left(\frac{1}{m|G|} - \epsilon, \frac{1}{|G|} + \epsilon\right)$. This probability range is good enough to prove the following result, similar to Theorem 5.3.

Theorem 6.8. *Let K be a number field given by $K = \mathbb{Q}(\theta) = \mathbb{Q}[X]/T$ for some monic irreducible $T(X) \in \mathbb{Z}[X]$. Let $f(X) \in \mathbb{Z}[\theta][X]$. If K_f/K is an abelian extension then there is a randomized polynomial time algorithm (polynomial in $size(T) + size(f)$) that computes the Galois group $Gal(K_f/K)$.*

7 Concluding Remarks

In this paper we have studied the problem of (a) computing the order of the Galois group of a given polynomial $f(X) \in \mathbb{Z}[X]$, and (b) determining the Galois group of $f(X) \in \mathbb{Z}[X]$ by finding a small generator set. Our approach is complexity theoretic, with the broad aim of classifying these problems in complexity classes. Assuming the GRH, we show that in general the order of the Galois group can be computed in $\mathrm{P}^{\#\mathrm{P}}$, and when the Galois group is solvable it can be computed in $\mathrm{BPP}^{\mathrm{NP}}$. Thus, we have a polynomial space-bounded algorithm for finding the order of the Galois group. In particular, when the group is solvable, finding the order is in the polynomial hierarchy. Our results suitably extend to the case when f is defined over an arbitrary number field.

In terms of computing the Galois group as a permutation group, for polynomials with *abelian* Galois group we show that this can be done in randomized polynomial time, assuming GRH. In the general case, no nontrivial upper bound for computing the Galois group other than exponential time is known even when the Galois group is solvable. On the other hand, the problem is not known to be even NP-hard. A challenging question is to precisely characterize the computational complexity of this important problem.

There are polynomial time algorithms for testing if the Galois group is abelian or solvable [7, 8]. However, no efficient algorithm for testing supersolvability or nilpotence of the Galois group is known. This is another intriguing open question.

References

[1] Leonard M. Adleman and Kevin S. McCurley. Open problems in number-theoretic complexity, II. In *Proceedings of ANTS-1*, volume 877 of *Lecture Notes in Computer Sciences*, pages 291–322, NY, 1994. Springer.

[2] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity I & II.* ETACS monographs on theoretical computer science. Springer-Verlag, Berlin, 1988 and 1990.

[3] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.

[4] Hendrik W. Lenstra Jr. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, April 1992.

[5] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields*, pages 409–464. Academic Press, London, 1977.

[6] E. Landau. Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques. *Bulletin de la Société de France*, 33:251–261, 1905.

[7] Susan Landau. Polynomial time algorithms for galois groups. In John Fitch, editor, *EUROSAM 84 Proceedings of International Symposium on Symbolic and Algebraic Computation*, volume 174 of *Lecture Notes in Computer Sciences*, pages 225–236, Cambridge, England, July 1984. EUROSAM, Springer.

[8] Susan Landau and Gary. L. Miller. Solvability by radicals is in polynomial time. *Journal of Computer and System Sciences*, 30:179–208, 1985.

[9] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Inc, third edition, 1999.

[10] Arjen K. Lenstra, Hendrik W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[11] Eugene M. Luks. Permutation groups and polynomial time computations. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 11:139–175, 1993.

[12] P. Pálfy. A polynomial bound for the orders of primitive solvable groups. *Journal of Algebra*, pages 127–137, July 1982.

[13] Paulo Ribenboim. *Classical theory of algebraic numbers*. Universitext. Springer, 1999.

[14] C C Sims. Computational methods in the study of permutation groups. *Computational problems in Abstract Algebra*, pages 169–183, 1970.

[15] L. Stockmeyer. On approximating algorithms for #P. *SIAM Journal of Computing*, 14:849–861, 1985.

[16] B. L. van der Waerden. *Algebra*, volume I. Springer-Verlag, seventh edition, 1991.

[17] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.

[18] Helmut Wielandt. *Finite Permutation Groups*. Academic Press, New York, 1964.

Appendix

{Galo

Function `Order`$(C(X) \in \mathbb{Z}[X])$
Input: $C(X) \in \mathbb{Z}[X]$ and C is solvable by radicals
Output: $[\mathbb{Q}_C : \mathbb{Q}]$
begin
    if *C is a constant polynomial or is of degree* 1 **then**
        return *1*
    end
    Let $C(X) = B(X)f(X)$ where f is an irreducible polynomial in $\mathbb{Z}[X]$;
    Let $\{B_1, B_2, \ldots, B_k\}$ be the minimal block system of $\Omega = \mathit{Roots}(f)$ under the action of $\mathit{Gal}\,(\mathbb{Q}_f/\mathbb{Q})$;
    (*
        If f is a primitive polynomial then we take $\{\Omega\}$ as the minimal block system.
    ***)**
    Compute $p(X) = \prod_{\alpha \in B_1}(X - \alpha) = \sum \delta_i X^i$;
    Compute the polynomial $g(X)$ such that $\mathbb{Q}[X]/g \cong \mathbb{Q}(\delta_1, \ldots, \delta_r)$;
    (*
        If f is a primitive polynomial, g can be taken as the constant polynomial 1
    ***)**
    Find polynomials $\overline{h}_0, \overline{h}_1, \ldots, \overline{h}_t$;
    Let $x_0 :=$ `Order`$(B(X)g(X))$;
    for $i := 1$ ***to*** t **do**
        Using the $\mathrm{BPP}^{\mathrm{NP}}$ algorithm compute a 0.1-approximate value of $[\mathbb{Q}_{Bh_i} : \mathbb{Q}]$. ;
        Let it be y_i. Find the unique l_i such that

$$0.9\frac{y_i}{x_{i-1}} \leq p_i^{l_i} \leq 1.1\frac{y_i}{x_{i-1}}.$$

        $x_i := x_{i-1}.p_i^{l_i}$;
    end
    return x_t ;
end

Algorithm 2: Computing the order of solvable Galois groups

{Galo

Input: $f(X) \in \mathbb{Z}[X]$ such that $Gal\,(\mathbb{Q}_f/\mathbb{Q})$ is abelian

Output: A generator set S for $Gal\,(\mathbb{Q}_f/\mathbb{Q})$

Let $B = (n+1)!^{10} size(f)^2$;
(*
By Claim 3.5.1.
*)
Let $f = \prod_{i=1}^{t} f_i$;
(*
f_i are its irreducible factors obtained using LLL.
*)
Let $n_i = \deg f_i$ and $M = \prod n_i$;
$S = \emptyset$;
for $i := 1$ ***to*** $T = 4 \log M$ **do**
  pick prime $q \leq B$ at random;
  if $q \nmid discr(f)$ **then**
    for $j := 1$ ***to*** t **do** $\tau_{ij} :=$ `Recover`(i, q) ;
    $\tau_i = \langle \tau_{ij_1}, \tau_{ij_2} \ldots, \tau_{ij_t} \rangle$;
    $S = S \cup \tau_i$;
  end
end

Function `Recover`(k, q)

Input: $q \nmid discr(f_k)$

Output: $\sigma \in Gal\,(\mathbb{Q}_{f_k}/\mathbb{Q})$ whose action on roots of f_k coincides with the action of $\left[\frac{\mathbb{Q}_{f_k}/\mathbb{Q}}{q}\right]$

Let $\overline{f}_k = f_k (\text{mod } q)$;
Let $\mathbb{F} \cong \mathbb{F}_{q^r}$ be the splitting field of $\overline{f}_k$ over $\mathbb{F}_q$;
Let $\overline{\theta} = x \pmod{\overline{f}_k(X)}$ in $\mathbb{F}$;
for $j := 1$ ***to*** n_k **do**
  if $\overline{\theta}^q = A_{kj}(\overline{\theta})$ **then** break
end
return σ_{kj}

Algorithm 3: Computing Galois group of Abelian extensions

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'