Identity testing for radical expressions

Klara Nosan

Supervised by:
Mahsa Shirmohammadi, IRIF, Université de Paris
Nikhil Balaji, Indian Institute of Technology, Delhi
James Worrell, University of Oxford

August 2021

The general context

Identity testing is a fundamental problem in algorithmic algebra which asks to test equality of two given algebraic expressions. The identity testing problem has many versions according to the syntactic representation of expressions and the ring in which evaluation is carried out. For example, the \textit{Arithmetic Circuit Identity Testing} (ACIT) problem involves evaluating arithmetic circuits in the ring of integers. It is not known how to solve this problem in polynomial time: the difficulty being that the magnitude of an integer represented by a circuit can be doubly exponential in the circuit size. In fact, as shown in \cite{ABKPM06}, ACIT is polynomial-time equivalent to the \textit{Polynomial Identity Testing} (PIT) problem, which asks to test identity of circuits evaluated in the ring of multivariate polynomials over the integers. Both ACIT and PIT can be solved in randomised polynomial time and it is famously open whether there is a deterministic polynomial-time algorithm for these problems. Identity testing in number fields has been extensively studied in relation to solving systems of polynomial equations \cite{Ge93, Koi96}, polynomial identity testing \cite{CK00}, and decision problems on matrix groups and semigroups \cite{BBC+96, CLZ00}, among many other problems.

The research problem

In this project we study identity testing for circuits evaluated in rings of algebraic integers that are generated over \( \mathbb{Z} \) by real radicals. In more detail, we study the \textit{Radical Identity Testing} (RIT) problem: given an algebraic circuit \( C \) representing a multivariate polynomial \( f(x_1, \ldots, x_k) \in \mathbb{Z}[x] \), and a radical input \( \sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k} \) where the radicands \( a_i \), and exponents \( n_i \) are nonnegative integers, decide whether \( f(\sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k}) = 0 \). The most general version of the problem, where both the \( a_i \)'s and the \( n_i \)'s are given in binary, is known to be in the \textit{counting hierarchy}, which is in \textit{PSPACE}. This bound has been improved for the Bounded-RIT problem, a restricted version of the RIT problem where the input polynomial is represented by an algebraic formula rather than a circuit, showing that the restricted problem is in \textit{coRP} \cite{Bl98} when the radicands \( a_i \) are given in binary, and the exponents \( n_i \) in unary. The main challenge associated with the RIT problem is constructing efficient algorithms that would place the problem in the \textit{polynomial hierarchy}. Note that in RIT not only is the height of the output (which is an algebraic integer) doubly exponential in the circuit size, but also the degree of the output is exponential in the circuit size. This adds a second layer of difficulty and appears to prevent an easy reduction of RIT to ACIT.

Our contribution

Our main results concern several special cases of RIT. We consider the case, called 2-RIT, in which the inputs to the circuit are all square roots. We also consider the case, called 3-RIT, where the inputs are all cube roots. We show that 2-RIT lies in \textit{coRP} assuming the Generalised
Riemann Hypothesis (GRH), and in \textit{coNP} unconditionally. Our second main result is that 3-RIT lies in \textit{coNP} assuming GRH. Similar to the paper \cite{BPSW20} on identity testing for circuits with cyclotomic inputs (CIT), the basic idea of our algorithm is to evaluate the circuit in a finite field, that is, modulo a prime ideal. However, the generalisation of this approach to the RIT problem is not straightforward because repeated-radical field extensions are not as well-behaved as cyclotomic fields. The two main challenges are (i) to find a prime such that the finite field $\mathbb{F}_p$ is a quotient of the order $\mathcal{O}$ generated over $\mathbb{Z}$ by the collection of radicals labelling the input of the circuit (together with a suitable root of unity) and (ii) to verify in polynomial time that a non-deterministically chosen prime $p$ has the property described in (i), and $\mathbb{F}_p$ contains a representation of the input radicals.

To address (i) we show that we can find a prime $p$ of length polynomial in the circuit size, such that $\mathbb{F}_p$ corresponds to the aforementioned quotient, implying that the finite field computation can be done in time polynomial in the bit-length of the input. For this, we rely on standard number theoretical results on the splitting of primes in Galois fields, in particular, an effective version of the Chebotarev density theorem, which bounds the number of unramified primes in a given Galois field, as well as Dirichlet’s theorem on the density of primes in arithmetic progressions.

The need to address (ii) is the reason to restrict to quadratic and cubic roots. This restriction gives crucial information about the order $\mathcal{O}$, such as its dimension as a $\mathbb{Z}$-module.

Finally, we introduce a condition for tuples of algebraic numbers, which we call $k$-transitivity. As our third result we show that the RIT problem lies in \textit{coNP} assuming GRH whenever the input radicals (and their associated root of unity) are $k$-transitive or the Galois closure of the field generated by adjoining the input radicals to $\mathbb{Q}$ is monogenic.

**Arguments supporting its validity**

We prove the soundness of our algorithms using facts from algebraic number theory and Galois theory, leveraging results on how, given a number field $K$, the prime ideals of its ring of integers $\mathcal{O}_K$ factorise in $\mathcal{O}_K$. We show, in particular, that the finite field computation introduced in the CIT algorithm remains sound even when we take the computation to a finite field obtained by quotienting an order of the ring of integers $\mathcal{O}_K$, instead of $\mathcal{O}_K$ itself.

**Summary and future work**

In this work, we place the 3-RIT problem in \textit{coNP} assuming GRH, generalising this result to $K$-irreducible and monogenic number fields, and show that the 2-RIT problem is in \textit{coRP} assuming GRH and in \textit{coNP} unconditionally. We also note that the Bounded-RIT problem is in \textit{coRP} even when both the radicands $a_i$, as well as the exponents $d_i$, are given in binary.

Another case of Bounded-RIT that was previously known to be in the polynomial hierarchy is the case when the polynomial is given explicitly as opposed to with an algebraic circuit representation. Given such a (sparse) polynomial $f(x_1, \ldots, x_k) = \sum c_i x_i$, and a radical input $\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}$, the problem, again, asks, whether $f(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}) = 0$. This was first shown to be decidable in polynomial time over thirty years ago in \cite{Blo91}, and later in \cite{HBM10} shown to be in the circuit complexity class $\text{TC}^0$. However, both algorithms only work for the case when the radicands $a_i$ are given in binary, and the exponents $d_i$ in unary. Unlike the \textit{coRP} algorithm for the Bounded-RIT problem using the circuit representation, the two (conceptually) different algorithms for sparse input polynomials seem not to be easily adaptable for the case where the exponents of the radical input are given in binary. To the best of our knowledge, there are no intermediate complexity results for this slightly more general case, which is why we believe analysing it would be the best next step in the complexity analysis of the RIT problem and its subproblems.
1 Preliminaries

1.1 Ring theory

A ring is a set $R$ equipped with two binary operations, addition ($+$) and multiplication ($\cdot$), satisfying the following three sets of axioms, called the ring axioms: $R$ is an abelian group under addition, $R$ is a monoid under multiplication, and multiplication is distributive with respect to addition. We further assume the addition and multiplication to be commutative and with unity. The most familiar example of a ring is the ring $\mathbb{Z}$ of rational integers.

Given a ring $R$, a subset $I$ of $R$ is said to be an ideal if $I$ is an additive subgroup of the additive group of $R$ that absorbs multiplication by the elements of $R$. Given a rational prime $p \in \mathbb{Z}$, the additive group $p\mathbb{Z}$ is an ideal of $\mathbb{Z}$. Any ideal $I$ of $R$ that is not the whole of $R$ is said to be a proper ideal, that is, the underlying set of $I$ is a proper subset of the underlying set of $R$. A proper ideal $I$ is called a prime ideal if for any $a$ and $b$ in $R$, if $ab$ is in $I$, then at least one of $a$ and $b$ is in $I$.

An $R$-module over a ring $R$ is a generalisation of the notion of vector space over a field, wherein scalars are elements of a given ring with identity and an operation of multiplication (on the left and/or on the right), called scalar multiplication, defined between elements of the ring and elements of the module.

1.2 Algebraic number theory

A complex number $\alpha$ is algebraic if it is a root of a univariate polynomial with integer coefficients. The defining polynomial of $\alpha$, denoted $f_\alpha$, is the unique (up to multiplication by $\pm 1$) integer polynomial of least degree, whose coefficients have no common factor, that has $\alpha$ as a root. The degree of an algebraic number $\alpha$ is the degree of its minimal polynomial $f_\alpha$. If $f_\alpha$ is monic then we say that $\alpha$ is an algebraic integer. The sum, the difference, the product and the quotient of two algebraic numbers (except for division by zero) are algebraic numbers; this means that the set of all algebraic numbers is a field, commonly denoted by $\bar{\mathbb{Q}}$. The sum, the difference, and the product of two algebraic integers is again an algebraic integer; given an algebraic field $K$, the algebraic integers of $K$, form a ring denoted $O_K$, called the ring of integers.

A field $K$ is said to be a field extension, denoted $K/L$, of a field $L$, if $L$ is a subfield of $K$. Given a field extension $K/L$, the larger field $K$ is an $L$-vector space. The dimension of this vector space is called the degree of the extension and is denoted by $[K : L]$.

An algebraic number field (or simply number field) $K$ is a finite degree field extension of the field of rational numbers $\mathbb{Q}$. Thus $K$ is a field that contains $\mathbb{Q}$ and has finite dimension when considered as a vector space over $\mathbb{Q}$. It is well-known that each number field $K$ is a simple extension of $\mathbb{Q}$, i.e., $K$ can be represented as $K = \mathbb{Q}(\alpha)$, which is generated by the adjunction of a single element $\alpha \in K$, which is said to be the primitive element.

The Gaussian rationals $\mathbb{Q}(i)$ are the first nontrivial example of an algebraic number field, obtained by adjoining $i := \sqrt{-1}$ to $\mathbb{Q}$. All elements of $\mathbb{Q}(i)$ can be written as expressions of the form $a + bi$ with $a, b \in \mathbb{Q}$; hence $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Furthermore, $\mathcal{O}_{\mathbb{Q}(i)} := \mathbb{Z}[i]$.

An order $\mathcal{O}$ in a number field $K$ is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank $[K : \mathbb{Q}]$. Since $\mathcal{O}_K$ is also a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, it follows from the structure theorem for $\mathbb{Z}$-modules that the quotient $\mathcal{O}_K/\mathcal{O}$ is a finite abelian group. The order of this quotient, denoted $[\mathcal{O}_K : \mathcal{O}]$, is called the index of $\mathcal{O}$ in $\mathcal{O}_K$. It is known that $m\mathcal{O}_K \subset \mathcal{O}$ for $m = [\mathcal{O}_K : \mathcal{O}]$. For example, $\mathbb{Z}[2i] = \mathbb{Z} + 2\mathbb{Z}i$ is an order of the Gaussian integers of index 4, and $4\mathbb{Z}[i] \subset \mathbb{Z}[2i]$.

Let $p(x) \in K[x]$ be a polynomial. The splitting field of $p(x)$ over $K$ is the smallest extension of $K$ over which $p(x)$ can be decomposed into linear factors. The splitting field of $x^2 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$.

A root of unity is any complex number that yields 1 when raised to some positive integer power $n$, i.e., $\zeta$ such that $\zeta^n = 1$. If $\zeta_n$ is an $n$th root of unity and for each $k < n$, $\zeta^k \neq 1$, then $\zeta_n$ is a primitive $n$th root of unity.
then we call it a primitive \( n \)th root of unity. We can always choose a primitive \( n \)th root of unity by setting \( \zeta_n = e^{\frac{2\pi i}{n}} \) for \( k \) with \( k \in \mathbb{Z}_n^* \). The \( n \)th cyclotomic polynomial, for any positive integer \( n \), is the unique irreducible polynomial \( \Phi(x) \in \mathbb{Q}[x] \) with integer coefficients that is a divisor of \( x^n - 1 \) and is not a divisor of \( x^k - 1 \) for any \( k < n \). The \( n \)th cyclotomic polynomial \( \Phi_n \) is the minimal polynomial of a primitive \( n \)th root of unity, and its roots are all \( n \)th primitive roots of unity.

1.3 Galois theory

An algebraic field extension \( K/L \) is normal (in other words, \( K \) is normal over \( L \)) if every irreducible polynomial over \( L \) that has at least one root in \( K \) splits over \( K \). In other words, if \( \alpha \in K \), then all conjugates of \( \alpha \) over \( L \) (i.e., all roots of the minimal polynomial of \( \alpha \) over \( L \)) belong to \( K \). An algebraic field extension \( K/L \) is said to be a separable extension if for every \( \alpha \in K \), the minimal polynomial of \( \alpha \) over \( L \) is a separable polynomial. That is it has no repeated roots in any extension field. Every algebraic extension of a field of characteristic 0 is normal. A Galois extension is an algebraic field extension that is normal and separable. The following holds for separable extensions:

**Theorem 1** (Primitive Element Theorem). Let \( K/L \) a separable extension of finite degree. Then \( K = L(\alpha) \) for some \( \alpha \in K \); that is, the extension is simple and \( \alpha \) is a primitive element.

Given a Galois extension \( K/L \), the Galois group of \( K/L \), denoted by \( \text{Gal}(K/L) \) is the group of automorphisms of \( K \) that fix \( L \). That is, the group of all isomorphisms \( \sigma : K \rightarrow K \) such that \( \sigma(x) = x \) for all \( x \in L \). If \( K \) is a field with subfield \( L \subset K \), the Galois closure of \( K \) over \( L \) is the field generated by images of embeddings \( K \rightarrow K \) that are the identity map on \( L \).

Fix \( \alpha \) an algebraic number \( \alpha \) over a Galois extension \( K/L \). The image of \( \alpha \) under an automorphism \( \sigma \in \text{Gal}(K/L) \) is called a Galois conjugate of \( \alpha \). The Galois conjugates of \( \alpha \) are precisely the roots of the minimal polynomial \( f_\alpha \) of \( \alpha \). The Galois conjugates of a root of unity \( \zeta_n \) are its powers \( \zeta_n^k \) such that \( k \in \mathbb{Z}_n^* \); and \( \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \) includes all automorphisms \( \sigma \) defined by \( \sigma(\zeta_n) = \zeta_n^k \) for \( k \in \mathbb{Z}_n^* \).

The norm of \( \alpha \) is defined by

\[
N_{K/L}(\alpha) = \prod_{\sigma \in \text{Gal}(K/L)} \sigma(\alpha)
\]

For short, we may drop the subscript \( K/L \) if the underlying field is understood from the context. For \( \alpha = a + bi \in \mathbb{Z}[i] \) the only Galois conjugate is \( a - bi \), and thus its norm is the product \( N(\alpha) = (a + bi)(a - bi) = a^2 + b^2 \). Note that the norms of all Galois conjugate are equal, and the norm of an algebraic integer is always a rational integer itself.

The trace of \( \alpha \in K/L \) is defined by

\[
\text{Tr}_{K/L}(\alpha) = \sum_{\sigma \in \text{Gal}(K/L)} \sigma(\alpha)
\]

Again, we drop the subscript \( K/L \) if the underlying field can be understood from the context.

The ring of integers of \( K \), \( \mathcal{O}_K \), is a free abelian group of rank \( n \), and hence admits \( \mathbb{Z} \)-basis \( \{\alpha_1, \ldots, \alpha_n\} \). Given such a basis, we denote with \( \Delta_K \) the discriminant, and define it by

\[
\Delta_K = \det(\text{Tr}_{K/L}(\alpha_i \alpha_j))_{1 \leq i,j \leq n}
\]

Note that \( \Delta_K \) is always a non-zero integer.
1.4 $k$-Transitivity

Let $\alpha_1, \ldots, \alpha_k$ be algebraic integers with respective minimal polynomials $f_1(x), \ldots, f_k(x) \in \mathbb{Z}[x]$ over $\mathbb{Q}$. We say the tuple $(\alpha_1, \ldots, \alpha_k)$ is $k$-transitive if, for all $1 < i \leq k$, the polynomial $f_i(x)$ remains irreducible over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$.

Let $a_1, \ldots, a_k$ be $k$ be positive pairwise coprime integers, and $d \in \mathbb{N}$. By [Blo98], for all $1 < i \leq k$, we have that the minimal polynomial of $\sqrt[d]{a_i}$ over $\mathbb{Q}(\sqrt[d]{a_1}, \ldots, \sqrt[d]{a_{i-1}})$ is $x^{d_i} - c_i$ where $d_i$ is the smallest positive integer such that $\sqrt[d_i]{a} \in \mathbb{Q}$. Observe that $x^{d_i} - c_i$ is also the minimal polynomial of $\sqrt[d]{a_i}$ over $\mathbb{Q}$.

Fix $k$ positive pairwise coprime integers $a_1, \ldots, a_k$. Then by the above we have

**Remark 2.** The tuple $(\sqrt[a_1]{\cdot}, \ldots, \sqrt[a_k]{\cdot})$ is $k$-transitive.

We further prove that

**Lemma 3.** The tuples $(\sqrt[a_1]{\cdot}, \ldots, \sqrt[a_k]{\cdot}, \zeta_d)$ are $k$-transitive for $d = 3, 4, 6$.

**Proof.** The condition of $k$-transitivity holds for the tuple $(\sqrt[a_1]{\cdot}, \ldots, \sqrt[a_k]{\cdot})$ with $d \in \mathbb{N}$. It remains to prove that the cyclotomic polynomials $\Phi_d$ are irreducible over $\mathbb{Q}(\sqrt[a_1]{\cdot}, \ldots, \sqrt[a_k]{\cdot})$. Since the degrees of $\Phi_d$ are 2 for $d = 3, 4, 6$, if they factor over $K_d$, they completely split. But the $K_d$’s are real fields, and do not contain the respective $\zeta_d$’s.

1.5 Ramification theory

Let $K$ be a number field and let $p$ be a prime ideal of $\mathcal{O}_K$. Then $p \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, hence there must exist a rational prime $p$ such that $p \cap \mathbb{Z} = p\mathbb{Z}$. We say that $p$ is above $p$. We have

$$p \subset \mathcal{O}_K \subset K$$

$$p \subset \mathbb{Z} \subset \mathbb{Q}.$$

Given a number field $K$ with ring of integers $\mathcal{O}_K$, any ideal $I \subseteq \mathcal{O}_K$ admits a unique factorisation into prime ideals in $\mathcal{O}_K$. Let $p \in \mathbb{Z}$ be a rational prime. The ideal $p\mathcal{O}_K$ may not be prime in $\mathcal{O}_K$, but does factorise into prime ideals as follows

$$p\mathcal{O}_K = p_1^{e_1} \cdots p_t^{e_t}.$$

We say that $p$ is ramified if $e_i > 1$ for some $i$. Conversely, $p$ is non-ramified if $p\mathcal{O}_K = p_1 \cdots p_t$ where the $p_i$ are distinct. Using the vocabulary introduced above, we can observe that the prime ideals $p_i$ are all above $p$. Note that in the ring of integers of a number field, all prime ideals are maximal, hence all $p_i$ are also maximal ideals of $\mathcal{O}_K$.

For the Gaussian integers, the ideals $2\mathbb{Z}[i]$ and $5\mathbb{Z}[i]$ are not prime ideals and have respective factorisations $2\mathbb{Z}[i] = p^2$ and $5\mathbb{Z}[i] = p_1p_2$ where $p = (1 + i)\mathbb{Z}[i], p_1 = (2 + i)\mathbb{Z}[i], \text{ and } p_2 = (2 - i)\mathbb{Z}[i]$ are prime ideals. The prime 2 is the unique ramified prime in the Gaussian integers.

For more details and extended definitions from ramification theory, see Appendix A.

1.6 Models of algebraic computation

Let $X = \{x_1, \ldots, x_k\}$ be a set of commutative variables. An algebraic circuit $C$ over the variables $X$ is a directed, acyclic graph (DAG) with labelled vertices and edges. Vertices of in-degree zero (leaves) are labelled with variables in $X$, and $-1$; and the remaining vertices have labels in $\{+, \times\}$. Moreover, the incoming edges to $+$-vertices have labels in $\mathbb{Z}$, that is, the $+$-gates compute integer-weighted sums. There is a unique vertex of out-degree zero which determines the output of the circuit, a $k$-variate polynomial, in an obvious bottom-up manner.
Given an algebraic circuit, the parameters that will be of interest to us is its size, that is the number of gates (or wires) in the circuit; see Figure 1. The degree and the bit-length of the coefficients of a polynomial represented by a circuit is at most exponential in the size of the circuit.

An algebraic formula is an algebraic circuit where the underlying DAG is a tree. Essentially, this means intermediate computation cannot be reused – the output of any intermediate gate is fed into exactly one other gate (the fan-out of every node is exactly 1). Note that algebraic formulas are a strict subclass of algebraic circuits, as the condition on the underlying DAG ensures that the degree and bit-length of the coefficients of the represented polynomial are bounded by the size of the formula.

### 1.7 Computational complexity theory

In computational complexity theory, nondeterministic polynomial time (NP) is a complexity class used to classify decision problems. The class NP is the set of decision problems for which the problem instances where the answer is “yes” have proofs verifiable in polynomial time by a deterministic Turing machine, that is, only “yes”-instances have a polynomial-length certificate and there is a polynomial-time algorithm that can be used to verify any purported certificate. Alternatively, NP can be understood as the set of problems that can be solved in polynomial time by a nondeterministic Turing machine. The complexity class coNP is the class of problems whose complement is in NP. That is, a decision problem is in coNP precisely if only "no"-instances have a polynomial-length certificate and there is a polynomial-time algorithm that can be used to verify any purported certificate.

The complexity class randomised polynomial time (RP) is the class of problems for which a probabilistic Turing machine that runs in polynomial time in the input size, always returns "no" if the correct answer is "no", and, if the correct answer is "yes", returns "yes" with probability at least $\frac{1}{2}$ exists. Analogously, coRP is the class of problems whose complements are in RP. That is, problems for which a probabilistic Turing machine that runs in polynomial time in the input size, always returns "yes" if the correct answer is "yes", and, if the correct answer is "no", returns "no" with probability at least $\frac{1}{2}$ exists.

\[ p(x) = (1 - 2x)^{2^s} \]
2 The decision problem of radical identity testing

Given an algebraic circuit that computes a mathematical expression, a fundamental decision problem associated to it is checking whether the computed expression is identically zero. In this internship, we tackle this problem for the case when the input of the algebraic circuit are (positive) real unnested radicals, that is, algebraic numbers of the form $\sqrt[d]{a}$, with $d,a \in \mathbb{N}$. We formalise the problem as follows:

**Problem 4** (Radical Identity Testing). Let $C$ be an algebraic circuit representing a multivariate polynomial $f(x_1,\ldots,x_k)$ for some $k$, together with $k$ radicals $\sqrt[d_1]{a_{i_1}},\ldots,\sqrt[d_k]{a_{i_k}}$, where the radicands $a_{i_j}$ and the exponents $d_{i_j}$ are nonnegative integers, possibly written in binary. The Radical Identity Testing (RIT) problem asks whether

$$f(\sqrt[d_1]{a_{i_1}},\ldots,\sqrt[d_k]{a_{i_k}}) = 0.$$

Our aim, in particular, is to construct an efficient algorithm that decides the RIT problem, analyse its complexity and prove complexity bounds for the problem. We differentiate different variants of the problem depending on the possible representation of the $d_{i_j}$ (written in unary or binary) and the type of the circuit $C$.

Before we proceed, let us highlight that there is a polynomial-time reduction from the RIT problem to one of its variants where all radicands are pairwise coprime numbers. Given an algebraic circuit $C$ representing a $k$-variate polynomial $f(x_1,\ldots,x_k)$ together with $k$ input radicals $\sqrt[d_1]{a_{i_1}},\ldots,\sqrt[d_k]{a_{i_k}}$, we construct another algebraic circuit $C'$ representing an $\ell$-variate polynomial $f'(y_1,\ldots,y_{\ell})$ and input radicals $\sqrt[d_1]{m_{i_1}},\ldots,\sqrt[d_{\ell}]m_{i_{\ell}}$, with the $m_{i_j}$ pairwise coprime, and such that $f(\sqrt[d_1]{a_{i_1}},\ldots,\sqrt[d_k]{a_{i_k}}) = 0$ if and only if $f'(\sqrt[d_1]{m_{i_1}},\ldots,\sqrt[d_{\ell}]m_{i_{\ell}}) = 0$.

Given a set of integers $n_1,\ldots,n_k$, the factor-refinement algorithm [BDS93] computes a set $\{m_1,\ldots,m_{\ell}\}$ of (not necessarily prime) factors $m_j$ of the $n_i$’s such that $\gcd(m_j,m_k) = 1$ for all $1 \leq j < k \leq \ell$, and each $n_i$ can be written as a product of these factors, i.e., $n_i = \prod_{j=1}^{1} m_j^{e_{ij}}$ with the $e_{ij} \in \mathbb{N}$. If we denote by $n = \text{lcm}(n_1,\ldots,n_k)$, the factor-refinement algorithm runs in time $O(\log^2(n))$ (see also [Blö98, Lemma 3.1]), and the number $\ell$ of factors is bounded by $\sum_{i=1}^{k} \log(|n_i|)$. In order to reduce an instance of the RIT problem to a new instance with pairwise coprime radicands, we apply the factor-refinement algorithm to the $a_{i_j}$’s and compute a set of pairwise coprime factors $m_j$ as described. We then construct the algebraic circuit $C'$ from $C$ by replacing the leaves $x_i$, $i \in \{1,\ldots,k\}$, with a small circuit that computes $\prod_{j=1}^{\ell} y_{i_j}^{e_{ij}}$ when $a_i = \prod_{j=1}^{\ell} m_j^{e_{ij}}$; see Figure 2.

Henceforth, we assume that the input radicands to the RIT problem are pairwise coprime.

2.1 Variants of the decision problem

We now state two versions of the decision problem associated to identity testing of algebraic circuits evaluated on radicals. These variants give rise to different algorithms and different
In the RIT problem, we consider evaluating an algebraic circuit on radicals of the form \( \sqrt[\alpha]{a_i} \) when both the \( d_i \)'s and the \( a_i \)'s are written in binary. We provide an algorithm and a corresponding complexity bound for the problem when the Galois closure of the field generated by adjoining the input radicals to \( \mathbb{Q} \) is monogenic or the input radicals (and their associated root of unity) are \( k \)-transitive. We show that this is the case when the radicals are all cubic, quartic or sextic. We state these problems formally as follows:

**Problem 5** (**dth-Root Identity Testing**). Let \( C \) be an an algebraic circuit representing a multivariate polynomial \( f(x_1, \ldots, x_k) \) for some \( k \), together with \( k \) \( d \)th roots \( \sqrt[\alpha_1]{a_1}, \ldots, \sqrt[\alpha_k]{a_k} \), where the radicands \( a_i \) are rational primes, written in binary. The \( d \)th-Root Identity Testing (\( d \)-RIT) problem asks whether \( f(\sqrt[\alpha_1]{a_1}, \ldots, \sqrt[\alpha_k]{a_k}) = 0 \).

We also consider a different adjustment of the original problem and look at a subclass of algebraic circuits, namely algebraic formulas, which has previously been considered in [Blö98]. This particular subclass of algebraic circuits is interesting as the coefficients of the circuit, (which in the case of general algebraic circuits can have magnitude doubly exponential in the size of the circuit), stay exponential in the size of the circuits. Furthermore, due to their structure, algebraic formulas also have degree bounded by the size of the circuit. The problem has already been solved for the case where the \( a_i \)'s are given in unary, here we thus consider the more general version with both \( d_i \)'s and \( a_i \)'s given in binary:

**Problem 6** (**Bounded Radical Identity Testing**). Let \( C \) be an an algebraic formula representing a multivariate polynomial \( f(x_1, \ldots, x_k) \) for some \( k \), together with \( k \) radicals \( \sqrt[\alpha_1]{a_1}, \ldots, \sqrt[\alpha_k]{a_k} \), where the radicands \( a_i \) are nonnegative integers and exponents \( d_i \) are rational primes. The Bounded Radical Identity Testing (Bounded-RIT) problem asks whether \( f(\sqrt[\alpha_1]{a_1}, \ldots, \sqrt[\alpha_k]{a_k}) = 0 \).

Having stated the three main problems, the RIT, \( d \)-RIT and Bounded-RIT problems, we can now proceed with our approach to solving them.

### 3 Main results

A natural way to approach the RIT problem would be to use numerical approximation and compute an approximate value of the algebraic circuit evaluated on the radical input. In fact, this technique is used in [Blö98] to solve the Bounded-RIT problem with unary exponents. Actually, their algorithm does not compute an approximation of the actual algebraic integer computed by the formula, but rather one of its conjugates instead. Given an algebraic integer \( \alpha \), we have that either \( \alpha = 0 \) or \( \alpha \) and all of its conjugates \( \alpha' \) are non-zero. Instead of checking whether \( \alpha \neq 0 \), it thus suffices to check whether \( \alpha' \neq 0 \) for some conjugate \( \alpha' \) of \( \alpha \). The algorithm randomly chooses a large conjugate \( \alpha' \) of \( \alpha \) such that polynomially many bits suffice to separate the conjugate from 0. The probabilistic correctness of the algorithm relies on *separation bounds* for algebraic numbers, proved by [CK00] and [Blö98]. Intuitively speaking, since the bit-length of the coefficients and degree of polynomials computed by the formula is at most its size \( s \), given that all radicands are bounded by \( 2^s \) and exponents by \( s \), one can prove that \( |\alpha'| < 2^{2s} \) for all conjugates of \( \alpha \). The separation bound entails that whenever \( \alpha \) is non-zero, a random conjugate \( \alpha' \) of \( \alpha \) has absolute value larger than \( 2^{-4s} \) with probability at least \( \frac{2}{3} \).

The above numerical algorithm works well for algebraic formulas and radicals with unary exponents, providing a \( \text{coRP} \) upper bound. In general, the coefficients of an algebraic circuit could be doubly exponential in the size of the circuit, which would mean the algorithm would need exponentially many bits to numerically approximate (a random large conjugate of) the value computed by the circuit. This, in particular, would put this problem in the counting hierarchy (which lies between \( \text{coNP} \) and \( \text{PSPACE} \)), hence, a different approach is needed if we
want to improve the complexity upper bound of RIT. Note that the RIT problem is at least as hard as the Polynomial Identity Testing problem for circuits, which is in coRP and P-hard.

In a recent work by Balaji, Perifel, Shirmohammadi and Worrell [BPSW20], zeroness for algebraic circuits evaluated on roots of unity, namely the Cyclotomic Identity Testing (CIT) problem, has been studied. In that work a different approach to the identity testing of algebraic numbers has been introduced. The problem of large coefficients is avoided by taking the computation to a finite field and thus only computing with reduced coefficients. The finite field is chosen such that it is isomorphic to the quotient of the cyclotomic ring of integers by a suitable prime ideal. Given a single radical \( \sqrt[p]{a} \), the splitting field of \( x^{d} - a \) is abelian, and by the Kronecker—Weber theorem is contained in a cyclotomic field \( \mathbb{Q}(\zeta_{d}) \). However, for the RIT problem, in general, we have \( k \) radicals \( \sqrt[p]{a_{1}} \), and the above-mentioned fact need not hold for the splitting filed of \( \prod_{i=1}^{k} (x^{d_i} - a_{i}) \). We can thus view general radical field extensions as a generalisation of cyclotomic fields. In this regard, we aim to adjust the algorithm in [BPSW20] developed for the CIT problem, and extend it to the RIT problem.

Given \( d \in \mathbb{N} \), recall that the \( d \)th cyclotomic polynomial has degree \( \varphi(d) \), where \( \varphi \) is the Euler totient function. Given an algebraic circuit \( C \) and a \( d \)th root of unity \( \zeta_{d} \), with \( d \) written in binary, the algorithm in [BPSW20], in particular, chooses a prime \( p \) such that the finite field \( \mathbb{F}_{p} \) contains exactly \( \varphi(d) \) \( d \)th primitive roots of unity \( \omega_{d} \) (in other words, \( \varphi(d) \) elements \( \omega_{d} \) such that the smallest power \( i \) with \( (\omega_{d})^{i} \equiv 1 \pmod{p} \) is \( d \), one for each conjugates of \( \zeta_{d} \)). Once they find a prime \( p \) satisfying this condition, they show that, if \( p \) does not divide the norm of the value computed by the algebraic circuit evaluated on \( \zeta_{d} \), the underlying polynomial of the algebraic circuit vanishes on \( \zeta_{d} \) if and only if its reduction modulo \( p \) vanishes on \( \omega_{p} \) in \( \mathbb{F}_{p} \).

An important fact that ensures the soundness of the finite field reduction in the cyclotomic case is that given a root of unity \( \zeta_{d} \), the ring of integers of the cyclotomic field \( \mathbb{Q}(\zeta_{d}) \) is precisely \( \mathbb{Z}[\zeta_{d}] \). If we denote the cyclotomic field by \( K = \mathbb{Q}(\zeta_{d}) \), and its ring of integers by \( \mathcal{O}_{K} = \mathbb{Z}[\zeta_{d}] \), then given a prime \( p \), the way the ideal \( p\mathcal{O}_{K} \) factorises is directly related to the way the minimal polynomial of the primitive element \( \zeta_{d} \) of \( K \) splits in the finite field \( \mathbb{F}_{p} \). In particular, if \( \Phi_{d} \in \mathbb{Z}[x] \) is the \( d \)th cyclotomic polynomial, that is, the minimal polynomial of \( \zeta_{d} \), denote by \( \bar{\Phi}_{d} \) the reduction of \( \Phi_{d} \) modulo \( p \). If the factorisation of \( \Phi_{d} \) in \( \mathbb{F}_{p} \) is \( \Phi_{d}(x) = f_{1}(x)^{e_{1}} \cdots f_{t}(x)^{e_{t}} \), we have that the ideal \( p\mathcal{O}_{K} \) factorises into \( t \) prime ideals with powers corresponding to the respective degrees of the \( f_{i} \)’s. See Appendix A, Proposition 27 for the formal statement of this fact. By choosing the right prime \( p \), we thus can ensure that the minimal polynomial splits into linear factors in \( \mathbb{F}_{p} \), that is, that all the conjugates of the primitive element are distinct in \( \mathbb{F}_{p} \), which is what is done here.

However, given an arbitrary number field \( K = \mathbb{Q}(\theta) \), it is, in general, not the case that \( \mathcal{O}_{K} = \mathbb{Z}[\theta] \). While we always have \( \mathbb{Z}[\theta] \subset \mathcal{O}_{K} \), the equality need not hold. Let us look at an example

**Example 7.** Let \( K = \mathbb{Q}(\sqrt{5}) \). Then the ring of integers is \( \mathcal{O}_{K} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \). Note that \( \mathbb{Z}[\sqrt{5}] \subset \mathcal{O}_{K} \); in particular, \( \mathbb{Z}[\sqrt{5}] \) is an order of index 2 in \( \mathcal{O}_{K} \).

In the above example the primitive element of the number field fails to generate the ring of integers, however, we can still observe that the ring of integers can be obtained by adjoining one single element to \( \mathbb{Z} \). Note that this need not be the case in general, as the Primitive element theorem does not have an equivalent for the case of rings, hence a given ring could be generated by an arbitrary number of generators. In fact, this is a well-studied property in algebraic number theory. In particular, a number field \( K \) is said to be monogenic if \( \mathcal{O}_{K} = \mathbb{Z}[\alpha] \) for some \( \alpha \in K \), that is, if \( \mathcal{O}_{K} \) admits a power basis. Alongside cyclotomic fields, all quadratic fields are also monogenic, however, there are already examples of non-monogenic fields among cubic fields. Examples of such non-monogenic fields are the cubic field \( \mathbb{Q}(\sqrt[3]{198}) \), or the biquadratic field \( \mathbb{Q}(\sqrt{7}, \sqrt{10}) \).

Clearly, the reasoning behind the soundness of the identity testing algorithm for cyclotomic
fields cannot be directly reused for radical identity testing. Note especially that in our case, the input does not consist of a single number like a specific root of unity in the cyclotomic case, but rather several radicals, that is, we are dealing with a multivariate algebraic circuit. In the spirit of the original algorithm, we now need to ensure that all of the radicals and their conjugates are distinct in the chosen finite field. It is not difficult to show that in order for that to hold, it suffices to choose a prime $p$ such that the primitive element of the field and all of its conjugates are distinct in $\mathbb{F}_p$. Nonetheless, we still need to deal with the fact that the primitive element of a radical field extension does not generate the ring of integers.

Note that given a radical input $\sqrt[a_1]{a}, \ldots, \sqrt[a_k]{a}$, we always look at the Galois closure $K$ of the field generated by adjoining the input radicals to $\mathbb{Q}$. In the case where the field $K$ is monogenic, like in Example 7 above, even if the element $\alpha \in K$ that generates the ring of integers $\mathcal{O}_K$ is not necessarily equal to the primitive element of the field itself, the finite field computation introduced in the CIT algorithm can be proven sound.

We say that an instance of RIT is monogenic if the Galois closure of the field generated by the input radicals adjoined to $\mathbb{Q}$ is monogenic. By an adjustment of the idea behind the original algorithm, we show

**Theorem 8.** The RIT problem for monogenic instances is in coNP under GRH.

The case where the ring of integers $\mathcal{O}_K$ does not admit a power basis, on the other hand, requires more elaborate treatment. We observe that the Galois field $K$ described above can be constructed by adjoining $\sqrt[a_1]{a}, \ldots, \sqrt[a_k]{a}$, as well as a primitive $d$th root of unity $\zeta_d$ to $\mathbb{Q}$, where $d = \text{lcm}(d_1, \ldots, d_k)$. Then the ring $\mathcal{O} = \mathbb{Z}[\sqrt[a_1]{a}, \ldots, \sqrt[a_k]{a}, \zeta_d]$ is always an order of the ring of integers $\mathcal{O}_K$. Now given a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$ represented by an algebraic circuit $C$, we can observe that the algebraic integer $f(\sqrt[a_1]{a}, \ldots, \sqrt[a_k]{a})$ will always be in $\mathcal{O}$. Intuitively, since we know how to construct this order, we would like to replace the role that the ring of integers $\mathcal{O}_K$ plays in the original algorithm by $\mathcal{O}$. We observe this can be done for instances of RIT when the input radicals (and their associated root of unity) admit a specific property, which we call $k$-transitivity. In that case we construct the finite field used in our computation by taking a quotient of $\mathcal{O}$ by an appropriate prime ideal.

We say that an instance of RIT is $k$-transitive if the tuple $(\sqrt[a_1]{a}, \ldots, \sqrt[a_k]{a}, \zeta_d)$ is $k$-transitive, where the $\sqrt[a]{a}$’s are the input radicals and $d = \text{lcm}(d_1, \ldots, d_k)$. We prove that

**Theorem 9.** The RIT problem for $k$-transitive instances is in coNP under GRH.

Having understood the general approach to solving and pinpointing the complexity of the radical identity testing problem, let us highlight the main difficulty in the construction of the algorithm before proceeding to its formal statement. As indicated above, when choosing the prime $p$ for the finite field $\mathbb{F}_p$, in which we would like to do our computation, there are several conditions $p$ should meet. Moreover, we would like the prime to be relatively small (that is, of polynomial bit-length in the size of the input) in order for the finite field computation to be done in polynomial time. As it turns out, in the case of cyclotomic identity testing, where the conditions on the prime are weaker, it is possible to find such a “small enough” prime, which puts the CIT problem into the complexity class coNP. Moreover, when admitting the Generalised Riemann Hypothesis (GRH), the density of appropriate primes increases, and a randomised version of the algorithm, which puts the problem into BPP, is described in [BPSW20]. In what follows, we discuss how the additional conditions on the prime that are needed in the case of radical identity testing affect the density of appropriate primes, and state our algorithm, which places the RIT problem in coNP assuming GRH for monogenic and $k$-transitive instances. As a corollary of this, we show that

**Corollary 10.** The $d$-RIT problem is in coNP under GRH for $d = 3, 4, 6$. 


Note that the gap in the complexity classes of the CIT problem and the aforementioned versions of the RIT problem assuming GRH comes from the fact that when solving the RIT problem, we require a $d$th primitive root of unity, as well as all input radicals to have a distinct representation in $\mathbb{F}_p$, as opposed to the cyclotomic case, where only a $d$th primitive root of unity was required in $\mathbb{F}_p$, which decreases the density of appropriate primes. However, we manage to improve the complexity bound for one subclass of the class of radical identity testing problems, and show

**Theorem 11.** The 2-\textsc{RIT} problem is in $\text{coRP}$ assuming GRH and in $\text{coNP}$ unconditionally.

In the following section, we prove our four main results as stated above. Any missing proofs of the lemmas we use can be found in the appendix.

### 3.1 A \text{coNP} algorithm for RIT

In this section, we present a non-deterministic polynomial time algorithm for the RIT problem for monogenic and $k$-transitive instances. As discussed above, the idea is to work in a finite field obtained by quotienting the ring of integers $\mathcal{O}_K$, or one of its subrings, by a suitable prime ideal.

Below, we fix the radicals $\sqrt[d]{a_1}, \ldots, \sqrt[d]{a_k}$, where the radicands $a_i$ are pairwise coprime, and the $a_i$’s and the $d_i$’s are of magnitude at most $2^k$. Let $d = \text{lcm}(d_1, \ldots, d_k)$. We also fix $K$ to be the splitting field of $\prod_{i=1}^k(x^{d_i} - a_i)$; note that $K = \mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}, \zeta_d)$, that is, $K$ is obtained by adjoining the input radicals as well as a $d$th primitive root of unity $\zeta_d$ to $\mathbb{Q}$. In particular, since $K$ contains $\zeta_d$, the minimal polynomials of the radicals $f_i = x^{d_i} - a_i$ split into linear factors in $K$, that is, the extension $K/\mathbb{Q}$ is normal. Given a rational prime $p$ and a polynomial $g(x) \in \mathbb{Z}[x]$ we denote by $\bar{g} \in \mathbb{F}_p[x]$ the reduction of $g$ modulo $p$.

We now show that for an instance of the RIT problem, that is, an algebraic circuit $\mathcal{C}$ we denote by $\mathcal{C}$, the ring homomorphism $\mathcal{C}: \mathbb{Z}[\alpha] \rightarrow \mathbb{F}_p$ by $\mathcal{C}(\alpha) = \bar{\alpha}$. We define a homomorphism $\mathcal{C}': \mathbb{Z}[\alpha] \rightarrow \mathbb{F}_p$ by $\mathcal{C}'(\alpha) = \bar{\alpha}$. We define a homomorphism $\mathcal{C}': \mathbb{Z}[\alpha] \rightarrow \mathbb{F}_p$ by $\mathcal{C}'(\alpha) = \bar{\alpha}$ and argue that it is well-defined. Suppose that $g_1, g_2 \in \mathbb{Z}[x]$ are such that $g_1(\alpha) = g_2(\alpha)$. Then $(g_1 - g_2)(\alpha) = 0$ and $f | (g_1 - g_2)$ in $\mathbb{Z}[x]$, implying that $\mathcal{C}(f)$ divides $\mathcal{C}(g_1) - \mathcal{C}(g_2)$ in $\mathbb{F}_p$. Since $\mathcal{C}(f) = 0$, we have $\mathcal{C}(g_1) = \mathcal{C}(g_2)$. Hence $\mathcal{C}'(g_1(\alpha)) = \mathcal{C}'(g_2(\alpha))$ and so $\mathcal{C}'$ is well-defined. It follows that $\mathcal{C}$ factors through $\mathbb{Z}[\alpha]$ via $\mathcal{C}'$.

For Item 1, if $\mathcal{C}(\alpha) = 0$ then $\bar{\alpha} = \mathcal{C}'(\alpha) = 0$.

For Item 2, observe that the kernel of $\mathcal{C}'$ is a prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\alpha]$ satisfying $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{p}\mathbb{Z}$.

By definition $N_{L/\mathbb{Q}}(\mathcal{C}(\alpha))$ is the product of all Galois conjugates of $\mathcal{C}(\alpha)$, but all conjugates of $\mathcal{C}(\alpha)$ are in $\mathcal{O}_L$, hence $N_{L/\mathbb{Q}}(\mathcal{C}(\alpha)) \in \mathfrak{p}$. It follows that $\mathfrak{p} | N_{L/\mathbb{Q}}(\mathcal{C}(\alpha))$. 

**Lemma 12** suggests a natural test for the RIT problem when the Galois field $K$ is monogenic: evaluate the circuit in a finite field $\mathbb{F}_p$ that contains a distinct representation of the input
Example 13. Let \( L = \mathbb{Q}(\sqrt{7}, \sqrt{10}) \). Observe that \( \theta = \sqrt{7} + \sqrt{10} \) is a primitive element for \( L \), that is, \( L = \mathbb{Q}(\sqrt{7} + \sqrt{10}) \). The generators of \( L \) can be expressed in \( \theta \) as follows:

\[
\sqrt{7} = \frac{\theta^3 - 31\theta}{6} \quad \sqrt{10} = \frac{37\theta - \theta^3}{6}
\]

Now observe that \( \sqrt{7}, \sqrt{10} \notin \mathbb{Z}[\theta] \), but \( 6\mathcal{O}_L \subset \mathbb{Z}[\theta] \), and both \( 6\sqrt{7} \) and \( 6\sqrt{10} \) are in \( \mathbb{Z}[\theta] \).

It is known that for an order \( \mathcal{O} \) of \( \mathcal{O}_L \), \( m\mathcal{O}_L \subset \mathcal{O} \) for \( m = [\mathcal{O}_L : \mathcal{O}] \), and that \( m = 1 \) if and only if \( \mathcal{O} = \mathcal{O}_L \).

Note, however, that the algebraic integer computed by evaluating the algebraic circuit \( C \) on the input radicals \( \sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k} \), is always contained in the ring \( \mathbb{Z}[\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}] \), which is a subring of \( \mathcal{O}_K \). This property makes this subring a good candidate with which to replace \( \mathcal{O}_K \) in our soundness proof. But if we look at the proof of Lemma 12 carefully, we must also note we would need the ring to also be closed under Galois conjugation in order for the norm of the computed algebraic integer to be in contained in it. In order to ensure that, it suffices to also add the primitive \( d \)-th root of unity \( \zeta_d \) to this ring, and use \( \mathcal{O} = \mathbb{Z}[\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}, \zeta_d] \) in our computation, which in turn, is an order of \( \mathcal{O}_K \). Now, given a \( k \)-transitive instance of the RIT problem, we show that this idea does indeed ensure our finite field computation to be sound.

Lemma 14. Let \( (\alpha_1, \ldots, \alpha_k) \) be a \( k \)-transitive tuple of algebraic integers. Denote by \( f_i(x) \in \mathbb{Z}[x] \) the minimal polynomial of \( \alpha_i \) over \( \mathbb{Q} \), for all \( 1 \leq i \leq k \). Let \( p \) be a rational prime such that \( f_i(x) \) has respective roots \( \bar{\alpha}_1, \ldots, \bar{\alpha}_k \) in \( \mathbb{F}_p \). For all polynomials \( g(x) \in \mathbb{Z}[x_1, \ldots, x_k] \), we have

1. if \( g(\alpha_1, \ldots, \alpha_k) = 0 \) then \( \bar{g}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k) = 0 \), and
2. if \( \bar{g}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k) = 0 \) then \( p \mid N_{L/\mathbb{Q}}(g(\alpha_1, \ldots, \alpha_k)) \)

Proof. Define a ring homomorphism \( ev : \mathbb{Z}[x_1, \ldots, x_k] \rightarrow \mathbb{F}_p \) by \( ev(g) = \bar{g}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k) \). We define a homomorphism \( ev' : \mathbb{Z}[\alpha_1, \ldots, \alpha_k] \rightarrow \mathbb{F}_p \) by \( ev'(g(\alpha_1, \ldots, \alpha_k)) = ev(g) \) and argue that it is well-defined. We prove by induction on \( k \) that if \( g(\alpha_1, \ldots, \alpha_k) = 0 \) then \( ev'(g(\alpha_1, \ldots, \alpha_k)) = 0 \).

Let

\[
g(x_1, \ldots, x_k) = \sum_{i \in I} h_i(x_1, \ldots, x_{k-1})x_i^k
\]

for some polynomials \( h_i \in \mathbb{Z}[x_1, \ldots, x_{k-1}] \). We now consider two cases.
Case 1: $h_i(\alpha_1, \ldots, \alpha_{k-1}) = 0$ for all $i \in I$. Then, by the induction hypothesis, we have $\bar{h}_i(\alpha_1, \ldots, \alpha_{k-1}) = 0$ for all $i \in I$. It follows that

$$g(\alpha_1, \ldots, \alpha_k) = \sum_{i \in I} \bar{h}_i(\alpha_1, \ldots, \alpha_{k-1})\alpha_k^i = 0$$

Case 2: $h_i(\alpha_1, \ldots, \alpha_{k-1}) \neq 0$ for some $i \in I$. Define

$$h(x) = \sum_{i \in I} h_i(\alpha_1, \ldots, \alpha_{k-1})x^i$$

Then $h$ is a non-zero polynomial with $h(\alpha_k) = 0$ and hence by $k$-transitivity of $(\alpha_1, \ldots, \alpha_k)$, we have that $f_k(x) | h(x)$. In turn it follows that $\bar{h}(\alpha_k) = 0$. It follows that $\text{ev}',$ and $\text{ev}$ factors through $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ via $\text{ev}'$.

For Item 1, $g(\alpha_1, \ldots, \alpha_k) = 0$ then $\bar{g}(\alpha_1, \ldots, \alpha_k)) = \text{ev}'(g(\alpha_1, \ldots, \alpha_k)) = 0$.

For Item 2, observe that the kernel of $\text{ev}'$ is a prime ideal $p$ in $\mathcal{O} = \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ satisfying $p \cap \mathbb{Z} = p\mathbb{Z}$. Note that by virtue of $L$ being Galois, the ring $\mathcal{O}$ is an order of $L$ and thus closed under Galois conjugation. Let $\beta = g(\alpha_1, \ldots, \alpha_k) \in \mathcal{O}$. By definition $N_{L/Q}(\beta)$ is the product of all Galois conjugates of $\beta$; but all conjugates of $\beta$ are in $\mathcal{O}$, hence $N_{L/Q}(\beta) \in p$. It follows that $p \mid N_{L/Q}(\beta)$.

We have just shown that given an instance of the RIT problem that is either monogenic or $k$-transitive, the computation can be taken to a finite field $\mathbb{F}_p$ for some rational prime $p$. The final question that remains to be answered before stating the algorithm is how to choose an appropriate prime $p$ that satisfies the two conditions given in Lemma 12 or Lemma 14. Let us call the primes $p$ such that $\mathbb{F}_p$ contains a distinct representation of the input radicals and their associated primitive root of unity good primes, and the primes that do not divide the norm of the algebraic integer computed by the circuit eligible primes. We will first discuss how to choose eligible primes.

Given a rational prime $p$, we would like to ensure that $p \mid N(\alpha)$, where $\alpha$ is the algebraic integer computed by a circuit. Observe that an integer of magnitude at most $s$ has at most $\log s$ divisors, thus the norm $N(\alpha)$ has at most $\log |N(\alpha)|$ divisors. Intuitively, this means that if we have a set of $\log |N(\alpha)| + 1$ primes, at least one of them will be eligible. Now let us see how we can bound this value.

In order to bound the magnitude of the norm, we first need a preliminary result regarding primitive elements of the number field $K$.

**Lemma 15** (Bound on the primitive element). The field $K$ has a primitive element $\theta$, computed as the linear combination

$$\theta = c_0\zeta_d + \sum_{i=1}^k c_i \sqrt{\alpha_i}$$

with $c_i \leq 2^{4k^2} \in \mathbb{Z}$ and $\deg f_\theta \leq 2^{2k^2}$.

Henceforth, we fix a primitive element $\theta$ for our number field $K$, computed as in Lemma 15. Using the degree bound on $\theta$, we can bound the magnitude of the norm $N(\alpha)$ of the algebraic integer $\alpha$ computed by the circuit as follows:

**Lemma 16** (Bound on the norm). Given an algebraic circuit $C$ of size $k$, denote by $\alpha \in \mathcal{O}_K$ the algebraic integer computed by $C$ evaluated on the $\sqrt[k]{a_i}$. We have

$$|N(\alpha)| \leq 2^{2k^3}$$

for $k \geq 4$. 

13
In the context of our algorithm, this means that if we find $2^{k^3} + 1$ good primes, at least one of them will also be eligible, and hence our finite field computation will be sound. Let us now focus on how we can ensure to find enough good primes of polynomial bit-length in the size of the input to complete our reasoning. Recall we say a prime is good if the radicals $\sqrt{a_1}, \ldots, \sqrt{a_n}$ and the primitive $d$th root of unity $\zeta_d$ have distinct representations in $F_p$. In order to ensure that, it suffices for the primitive element $\theta$ of $K$ and all of its conjugates to be distinct in $F_p$. This is equivalent to saying that the reduction of the minimal polynomial $f_\theta$ of $\theta$ modulo $p$, i.e., $\bar{f}_\theta \in \mathbb{F}_p[x]$, to split into linear factors in $\mathbb{F}_p$. Let us denote by $\pi_{f_\theta}(x)$ the number of primes $p \leq x$ such that this happens in $\mathbb{F}_p$ and count them.

Denote by $W(p)$ the number of roots of $f_\theta$ in $\mathbb{F}_p$ for a given rational prime $p$. Explicitly, we can define it as

$$W(p) = |\{k \mid 0 \leq k < p, f_\theta(k) \equiv 0 \pmod{p}\}|$$

Note that in our case, since we are working with a Galois field, if $f_\theta$ has one root in $\mathbb{F}_p$, it will have all of them, that is, $W(p)$ will either be 0 or $n$, where $n$ is the degree of $f_\theta$. Note also that we are only interested in unramified primes, as we want the representations of our algebraic integers in $\mathbb{F}_p$ to be distinct, and in order for that to be the case, we require $p \nmid \Delta_K$.

If we now try to compute a bound on the sum of $W(p)$ for all primes $p \leq x$ such that $p \nmid \Delta_K$, we need to take the number of all rational primes $p \leq x$, denoted $\pi(x)$, subtract the number of primes that could divide the discriminant, i.e., $\log \Delta_K$, and following [AO83], the number of remaining primes for which $f_\theta$ would not split in $\mathbb{F}_p$ is in $O(x^{1/2} \log(\Delta_K x^{\deg f_\theta}))$. Note that this bound comes from an effective version of the Chebotarev density theorem, which, intuitively, gives a bound on the density of unramified primes for a given Galois field $K$. Finally, as $W(p)$ gives us the number of roots of $f_\theta$ in $\mathbb{F}_p$ in our case, we can see it as a characteristic function assigning 0 to $p$ if $\mathbb{F}_p$ does not have any roots in $\mathbb{F}_p$, and $n$ otherwise, in order to actually count the primes we are interested in, we need to divide the sum of all values $W(p)$ by $n$, which yields a bound on $\pi_{f_\theta}$ as follows

**Proposition 17** (Bound on $\pi_{f_\theta}(x)$). Assuming GRH,

$$\pi_{f_\theta}(x) \geq \frac{1}{\deg f_\theta} \left[ \pi(x) - \log \Delta_K - cx^{1/2} \log(\Delta_K x^{\deg f_\theta}) \right]$$

where $c$ is an effective constant.

The above proposition suggests we would need a bound on the discriminant $\Delta_K$ of the number field $K$. Recall the definition of the discriminant of a number field; given a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of the ring of integers $\mathcal{O}_L$ of a number field $L$, we compute the discriminant $\Delta_L$ as the determinant of the matrix of traces of $\alpha_i \alpha_j$ for all $i, j = 1, \ldots, n$. Furthermore, the notion of a discriminant is not unique to solely number fields; we can also compute the discriminant of an order. In fact, given a number field $L$, its discriminant $\Delta_L$ is equal to the discriminant $\text{Disc}(\mathcal{O}_L)$ of its ring of integers $\mathcal{O}_L$. Now given a ring $\mathbb{Z}[\alpha]$, the discriminant $\text{Disc}(\mathbb{Z}[\alpha])$ is equal to the discriminant of the minimal polynomial of $\alpha$, that is, $\text{Disc}(\mathbb{Z}[\alpha]) = \text{Disc}(f_\alpha)$. It is a well-known fact that the discriminant of a polynomial can be computed as the product of the differences of the roots.

However, recall that in the case of a radical field extension $L$, its ring of integers $\mathcal{O}_L$ is not necessarily of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in K$. Furthermore, computing the ring of integers is a non-trivial task. In order to avoid this computation, we try to bound the discriminant using the discriminant of the order $\mathbb{Z}[\theta]$ of $\mathcal{O}_K$, generated by the primitive element $\theta$ of our number field $K$ and relate the two values by the following proposition (the proof of which can be found in [Ste10, Proposition 6.2.6])

**Proposition 18.** Suppose $\mathcal{O}$ is an order in $\mathcal{O}_L$. Then

$$\text{Disc}(\mathcal{O}) = \text{Disc}(\mathcal{O}_L) \cdot [\mathcal{O}_L : \mathcal{O}]^2$$
Proof of Theorems 8 and 9. Figure 3 presents a nondeterministic polynomial time algorithm
\( k \) (Bound on the discriminant)

\[ \text{Lemma 19} \]

\[ \text{Disc}(f) \equiv 0 \]

for the RIT problem as follows.

whether the algorithm runs in polynomial time. It is clear Step 1 can be
done in polynomial time. In Step 2, after guessing candidates for
\( \alpha_1, \ldots, \alpha_k \) verifying whether \( \alpha_i^{d_i} \equiv a_i \pmod{P} \) can be done in polynomial time by the repeated-squaring method. Finally,
Step 3 can clearly be done in polynomial time as well.

Now let us show that the RIT problem is in coNP. First suppose \( f(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}) \neq 0 \) for the polynomial \( f(x_1, \ldots, x_k) \) computed by \( C \).

Step 1: Guess prime \( p \leq 2^{4k^3} \).

Step 2: Guess \( \alpha_1, \ldots, \alpha_k \in \mathbb{F}_p \) and verify that \( \alpha_i^{d_i} \equiv a_i \pmod{p} \).

Step 3: Output 'Zero' if \( \bar{\alpha}_i \equiv \sqrt[k]{\alpha_i} \pmod{p} \) and 'Non-zero' otherwise.

Putting everything together, the above proposition suggests that \( \Delta_K \leq \Delta_{f_\theta} \), where \( \Delta_{f_\theta} = \text{Disc}(\mathbb{Z}[\theta]) \), which we bound as follows

**Lemma 19 (Bound on the discriminant).** For the primitive element \( \theta \) of \( K \), computed as a linear combination of \( \sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k} \), and \( \zeta_d \), we have

\[ |\text{Disc}(\mathbb{Z}[\theta])| \leq 2^{2k^2} \]

for \( k \geq 4 \).

Recall that we would like to choose enough good primes \( p \) so that at least one of them will be eligible, i.e., at least one of them will not divide the norm of the computed algebraic integer.

In particular, we would like to find \( x \) such that \( \pi_{f_\theta}(x) \geq 2^{k^3} + 1 \). Using the above bound, we claim that this is the case for \( x \geq 2^{4k^3} \)

**Lemma 20. Assuming GRH,**

\[ \pi_{f_\theta}(2^{4k^3}) \geq 2^{k^3} + 1. \]

Having understood the intuition behind the construction of our algorithm, we can finally give the algorithm explicitly, see Figure 3 and show that the RIT problem is in coNP for monogenic and \( k \)-transitive instances:

**Proof of Theorems 8 and 9.** Figure 3 presents a nondeterministic polynomial time algorithm for the RIT problem as follows.

Given input radicals \( \sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k} \), let \( d = \text{lcm}(d_1, \ldots, d_k) \), \( \zeta_d \) be a primitive \( d \)th root of unity and \( K = \mathbb{Q}(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}, \zeta_d) \) be the splitting field of \( \prod_{i=1}^{k}(x^{d_i} - a_i) \). Further denote by \( \theta \) a primitive element of \( K \), computed as in Lemma 15.

Let us first argue that the algorithm runs in polynomial time. It is clear Step 1 can be done in polynomial time. In Step 2, after guessing candidates for \( \alpha_1, \ldots, \alpha_k \), verifying whether \( \alpha_i^{d_i} \equiv a_i \pmod{p} \) can be done in polynomial time by the repeated-squaring method. Finally, Step 3 can clearly be done in polynomial time as well.

Now let us show that the RIT problem is in coNP. First suppose \( f(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}) \neq 0 \). Under GRH, the lower bound in Lemma 20 shows that \( \pi_{f_\theta}(2^{4k^3}) \geq 2^{k^3} + 1 \). It follows that there exists a prime \( p \leq 2^{4k^3} \) such that

- \( p \nmid N(f(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k})) \), and
- the finite field \( \mathbb{F}_p \) contains a distinct representation of the input radicals \( \sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k} \).

The polynomial certificate of non-zeroness of \( f(\sqrt[k]{a_1}, \ldots, \sqrt[k]{a_k}) \) then comprises, the above prime \( p \), and the list of integers \( \alpha_1, \ldots, \alpha_k \in \mathbb{F}_p \) such that \( \alpha_i^{d_i} \equiv a_i \pmod{p} \). Following
Lemma 12, we then have that $f(\alpha_1, \ldots, \alpha_k) \neq 0$ if $K$ is monogenic. Analogously, following Lemma 14, $f(\alpha_1, \ldots, \alpha_k) \neq 0$ if the RIT instance is $k$-transitive.

On the other hand, as noted above, for any prime $p$ and the representation $\alpha_1, \ldots, \alpha_k$ of radicals $\sqrt[\nu]{a_1}, \ldots, \sqrt[\nu]{a_k}$ in $\mathbb{F}_p$, if $f(\sqrt[\nu]{a_1}, \ldots, \sqrt[\nu]{a_k}) = 0$, then $f(\alpha_1, \ldots, \alpha_k) = 0$, as shown in Lemma 12 and Lemma 14 which concludes the proof for Theorems 8 and 9 respectively. 

Now putting together Theorem 9 and Lemma 3 which shows that the input radicals (and their associated $d$th root of unity) are $k$-transitive when $d = 3, 4, 6$, we immediately get Corollary 10.

3.2 A coRP algorithm for 2-RIT

In order to improve the obtained coNP bound for the RIT problem, in monogenic and $K$-irreducible fields, a natural question is to check whether our RIT algorithm could randomly choose a good prime $p$ to be used in the finite field computation. Recall we require that the prime $p$ has polynomial bit-length in the size of the input, and that the congruences $x^{d_i} \equiv a_i \pmod{p}$ are solvable in $\mathbb{F}_p$. By Chebotarev’s density theorem, roughly speaking, the density of such good primes is $\frac{1}{D}$ where $D = \prod_{i=1}^k d_i$. Since $D$ is exponential in the size of the input, good primes do not have sufficient density in order to directly be chosen randomly. The density remains insufficient even if all exponents $d_i$ are prime numbers written in unary.

In what follows, we show that the 2-RIT problem can be solved in randomised polynomial time under GRH, and that it is in coNP unconditionally. Recall that the 2-RIT problem is the identity testing for an algebraic circuit $C$ evaluated on square-roots $\sqrt{a_1}, \ldots, \sqrt{a_k}$ for $k$ rational primes $a_1, \ldots, a_k$. By Remark 2, all instances of the 2-RIT problem are $k$-transitive. This ensures that the finite field computation in our algorithm is sound, what remains to be shown is how to choose a good prime $p$ and determine the solutions to the equations $x^2 \equiv a_i \pmod{p}$ in $\mathbb{F}_p$.

As noted above, the natural density of primes is not sufficient even for the 2-RIT problem, however, we show that there is an arithmetic progression with a good density of primes, and that all primes in this progression are good. This is precisely what was done in [BPSW20] to decide the CIT problem (identity testing in cyclotomic fields).

Below, we state known effective bounds on the density of primes in an arithmetic progression, in particular, the following estimates, which have been shown in [DM13, Chapter 20, page 125] and [IK04, Corollary 18.8], respectively:

**Theorem 21.** Given $a \in \mathbb{Z}_n^*$, write $\pi_{n,a}(x)$ for the number of primes less than $x$ that are congruent to a modulo $n$. Then under GRH, there is an absolute constant $c > 0$ such that

$$\pi_{n,a}(x) \geq \frac{x}{\varphi(n) \log x} - cx^{1/2} \log x.$$  

Unconditionally, there exist effective positive constants $c_1$ and $c_2$, such that for all $n < c_1 x^{c_1}$,

$$\pi_{n,a}(x) \geq \frac{c_2 x}{\varphi(n) x^{1/2} \log x}.$$  

What remains to be understood is how to construct an arithmetic progression such that for every prime $p$ appearing in it, $\mathbb{F}_p$ contains a representation $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_p$ of the square-root input $\sqrt{a_1}, \ldots, \sqrt{a_k}$. As it turns out, this only requires a few simple yet neat number theoretical facts, which we recall now.

Let $p$ be an odd prime number. An integer $a$ is said to be a quadratic residue modulo $p$ if it is congruent to a perfect square modulo $p$, i.e., if there exists an integer $x$ such that $x^2 \equiv a$
mod $p$. The Legendre symbol is a function of $a$ and $p$ taking values in \{1, -1, 0\}, that is
\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\
-1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\
0 & \text{if } a \equiv 0 \pmod{p}.
\end{cases}
\]

Its explicit definition is as follows:
\[
\left( \frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p}
\]

Furthermore, given odd primes $p$ and $q$, the Law of quadratic reciprocity states:
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.
\]

We observe that in the case where $p \in 4N + 1$, then
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = 1 \iff \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) = 1 \text{ or } \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right) = -1
\]

In other words, $p$ is a quadratic residue modulo $q$ if and only if $q$ is a quadratic residue modulo $p$, when either $p$ or $q \equiv 1 \pmod{4}$.

As seen in the algorithm for the general RIT problem, the main challenge in deciding the problem is finding the right prime number for the finite field computation to be sound. In what follows, we leverage the above fact in order to choose the right $F_p$ for deciding 2-RIT. Recall that intuitively, we are looking for a prime $p$ such that $x^2 - a_i$ has a solution in $F_p$ for all $i$, that is, the $a_i$ is a quadratic residue modulo $p$. Since we will be choosing $p$ from an arithmetic progression, we can easily make that progression to be of the shape $4N + 1$, that is, to ensure that $p \equiv 1 \pmod{4}$. In that case the $a_i$’s will be quadratic residues modulo $p$ if and only if $p$ is a quadratic residue modulo $a_i$ for all $i$. In order to ensure that, it suffices to choose $p$ such that $p \equiv 1 \pmod{a_i}$ for all $i$, as $1$ is a perfect square modulo $a_i$ for all $i$, and thus $p$ a quadratic residue modulo $a_i$.

We have just shown that if we choose $p$ such that it satisfies all the above-mentioned congruences, the radicals $\sqrt{a_1}, \ldots, \sqrt{a_k}$ all exist (and are distinct) in $F_p$. Following Pocklington’s algorithm, there is a deterministic way to solve the equations $x^2 - a_i$ if $p \equiv 5 \pmod{8}$. See Appendix [F] for details. Note that this congruence encompasses the above restriction on $p$ being congruent to $1$ modulo $4$.

We now show how to construct an arithmetic progression such that all primes $p$ in the progression satisfy the above congruences. Denote by $A = \prod_{i=1}^{k} a_{i, \neq 2} a_i$ the product of all input radicands $a_i$, with the exception of $a_i = 2$ if that is the case for some $i$. Note that $A$ will always be odd as the $a_i$ are distinct primes. Let us look at the arithmetic progression
\[
8AN + b + 1, \quad (1)
\]

where $b$ is a solution of the following system of equations
\[
b \equiv 4 \quad \pmod{8} \quad \text{ (2)}
\]
\[
b \equiv 0 \quad \pmod{a_i} \text{ for all } a_i \neq 2.
\]

Since all the modulos in the equations \[(2)\] are pairwise coprime, by the Chinese remainder theorem, the system has a solution. By the above construction, we have an arithmetic progression such that all primes $p$ in the progression are good primes; note that even though we exclude the congruence for the case if $a_i = 2$, the equation $b \equiv 4 \pmod{8}$ will ensure the equation
Radical Identity Testing for square root inputs

**Input:** Algebraic circuit $C$ of size $k$ with input radicals $\sqrt{a_1}, \ldots, \sqrt{a_k}$, where the $a_i$ are primes of magnitude at most $2^k$.

**Output:** Whether $f(\sqrt{a_1}, \ldots, \sqrt{a_k}) = 0$ for the polynomial $f(x_1, \ldots, x_k)$ computed by $C$.

**Step 1:** Compute $b$ such that $b + 1 \equiv 5 \pmod{8}$, and $b + 1 \equiv 1 \pmod{a_i}$ for all $i$ such that $a_i \neq 2$.

**Step 2:** Pick $p$ uniformly at random from the set $S(a_1, \ldots, a_k)$ defined in (3).

**Step 3:** Compute $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_p$ such that $\alpha_i^2 \equiv a_i \pmod{p}$ as described in Figure 5.

**Step 4:** Output ‘Zero’ if $\bar{f}(\alpha_1, \ldots, \alpha_k) = 0$, where $\bar{f}$ is the reduction of $f$ modulo $p$; and ‘Non-zero’ otherwise.

Figure 4: Our algorithm for the 2-RIT problem, which runs in randomised polynomial time.

$x^2 - 2$ has a solution in $\mathbb{F}_p$. We also ensure that $p$ is such that we can deterministically find the representations $\alpha_1, \ldots, \alpha_k$ of $\sqrt{a_1}, \ldots, \sqrt{a_k}$ in $\mathbb{F}_p$. Define by $S(a_1, \ldots, a_k)$ the following set

$$\{p \leq 2^{5k^3} | p \in 8AN + b + 1 \text{ where } A = \prod_{i=1, a_i \neq 2}^k a_i \text{ and } b \text{ is a solution of (2)}\}. \quad (3)$$

We claim the following:

**Proposition 22.** Given an algebraic circuit $C$ of size $k$, denote by $\alpha$ the algebraic integer computed by $C$ evaluated on the $\sqrt{a_i}$. Suppose that $p$ is chosen uniformly at random from the set $S(a_1, \ldots, a_k)$ defined in (3). Assuming GRH,

(i) $p$ is prime with probability at least $\frac{1}{667}$, and

(ii) given that $p$ is prime, the probability that it divides $N(\alpha)$ is at most $2^{-k^3}$.

With the above proposition in hand, we can state our coRP algorithm, see Figure 4 and prove its complexity.

**Proof of Theorem 11.** Figure 4 presents a randomised polynomial time algorithm for the 2-RIT problem as follows. It is clear that the algorithm runs in polynomial time. Let us now argue its correctness.

First, suppose that $f(\sqrt{a_1}, \ldots, \sqrt{a_k}) = 0$, then by Remark 2 and Lemma 14 we have $\bar{f}(\alpha_1, \ldots, \alpha_k) = 0$, and hence the output is ‘Zero’. Second, suppose that $f(\sqrt{a_1}, \ldots, \sqrt{a_k}) \neq 0$. Then the output will be ‘Non-Zero’ provided that $p$ does not divide $N(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$. By Proposition 22(ii), the probability that $p$ does not divide $N(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$ is at least $1 - 2^{-k^3}$. Thus, the probability that the algorithm gives the wrong output is $2^{-k^3}$.

It remains to show that the 2-RIT problem is in coNP unconditionally. The idea is to modify the algorithm in Figure 4 replacing randomisation with guessing. Theorem 21 shows that $\pi_{8AN+1}(2^{3k^3}) > 2^{k^3}$ for $k$ sufficiently large. It follows that there exists a prime $p \leq 2^{3k^3}$ that does not divide $N(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$. The rest of the argument follows as in the proof of Theorem 9.

18
Discussion and open problems

In this work, we have shown that the RIT problem is in coNP under GRH for monogenic and $k$-transitive instances. We also provided a randomised polynomial time algorithm for the 2-RIT problem, and showed it is in coNP unconditionally. Our algorithms all work by reducing the polynomials modulo some prime $p$, and taking the computation to the finite field $\mathbb{F}_p$. We opt for this approach as the coefficients of polynomials represented by algebraic circuits could be doubly exponential in the size of the circuit, which would require too much space to do numerical approximation in polynomial time. We did, however, note that the latter approach has been shown to work for deciding the Bounded-RIT problem when the exponents of the radical input are unary. In particular, [Blo98] gives an algorithm that decides the Bounded-RIT problem with unary exponents, which runs in randomised polynomial time in the bit-length of the input.

We observe that by slightly adjusting a few steps of the algorithm without changing its runtime, we can ensure it to decide the Bounded-RIT problem with binary exponents, and thus place the general version of the Bounded-RIT problem in coRP.

Recall that given an instance of the Bounded-RIT problem, comprised of an algebraic formula $C$, and a radical input $\sqrt[k_1]{a_1}, \ldots, \sqrt[k_k]{a_k}$, the algorithm works by computing an approximation of a random conjugate of the algebraic integer $\alpha$ computed by evaluating $C$ on the radical input. Then, following a result on separation bounds for algebraic numbers, whenever $\alpha$ is non-zero, a random conjugate $\alpha'$ of $\alpha$ has a large absolute value with probability at least $\frac{2}{3}$. The argument still holds for the case where the exponents $d_i$ are given in binary, the only part of the algorithm that needs to be adjusted is the way we sample a random conjugate of $\alpha$.

Denote by $K$ the Galois closure of the field we obtain by adjoining the input radicals to $\mathbb{Q}$. Given an element $\alpha \in K$ that can be computed as a polynomial expression in $\sqrt[k_1]{a_1}, \ldots, \sqrt[k_k]{a_k}$, its Galois conjugates are given by evaluating the same expression on the conjugates of the $\sqrt[k_i]{a_i}$'s, if the $a_i$'s are pairwise coprime. The idea presented in the original paper is thus to first compute pairwise coprime factors $m_1, \ldots, m_\ell$ of the input radicands $a_1, \ldots, a_k$, such that $\sqrt[k_i]{a_i} = \prod_{j=1}^\ell \sqrt[k_j]{m_j^{d_{ij}}}$. Then, if we compute the minimal $d_{ij} \in \mathbb{Z}$ such that $\sqrt[k_j]{m_j^{d_{ij}}} \in \mathbb{Z}$, given a primitive $d_{ij}$th root of unity $\zeta_{d_{ij}}$, the Galois conjugates conjugates of $\sqrt[k_j]{m_j}$ are given by $\sqrt[k_j]{m_j^{d_{ij}}} \zeta_{d_{ij}}, \ldots, \sqrt[k_j]{m_j^{d_{ij}}} \zeta_{d_{ij}}^{-1}$. In the paper, a clever way to randomly choose primitive $d_{ij}$th roots of unity is described, which, in combination with the factor refinement, gives an algorithm to sample conjugates of the $\sqrt[k_j]{m_j^{d_{ij}}}$, thus computing a conjugate of $\alpha$.

If we reuse the same exact approach for the Bounded-RIT problem with radical inputs with binary exponents, the algorithm no longer runs in polynomial time. The increase in complexity appears when trying to compute the minimal $d_{ij}$ such that $\sqrt[k_j]{m_j^{d_{ij}}} \in \mathbb{Z}$. However, instead of applying factor refinement to the input $a_1, \ldots, a_k$, we can start by computing the partial factorisation of each one of the $a_i$'s by going through all primes up to $\log A$, where $A = a_1 \cdots a_k$. This can be done in polynomial time. Furthermore, the factors $m_i$ we get by applying factor refinement to the partially factored $a_i$'s are also bounded by $\log A$, and the rest of the computation can be done in polynomial time.
References


A Ramification theory (extended definitions)

Here, we extend the definitions of the ramification theory notions introduced in the preliminaries. Recall we look at the factorisation of an ideal \( p\mathcal{O}_K \) in \( \mathcal{O}_K \):

\[
p\mathcal{O}_K = p_1^{e_1} \cdots p_t^{e_t} \tag{4}
\]

In general, given a commutative ring \( R \) and \( \mathfrak{m} \) is a maximal ideal of \( R \), the residue field is the quotient ring \( k = R/\mathfrak{m} \), which is a field. Intuitively, \( k \) can be thought of as the field of possible remainders. Now, given a maximal ideal \( \mathfrak{p} \) of \( \mathcal{O}_K \), \( \mathcal{O}_K/\mathfrak{p} \) is a \( \mathbb{F}_p \)-vector space of finite dimension. The residual class degree (inertial degree), denoted \( f_\mathfrak{p} \), is the dimension of the \( \mathbb{F}_p \)-vector space \( \mathcal{O}_K/\mathfrak{p} \), that is

\[
f_\mathfrak{p} = \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})
\]

Looking at the factorisation \( 4 \), we can define the residue class degree of each one of the \( p_i \)'s as follows:

\[
f_i = [\mathcal{O}_K/p_i : \mathcal{O}_L/p]
\]

Given a prime \( p \in \mathbb{Z} \) and the factorisation of \( p\mathcal{O}_K \) into prime ideals \( p_i \), the ramification index of \( p_i \), written \( e_i \), is the exact power of \( p_i \) which divides \( p\mathcal{O}_K \).

We say that a prime \( p \in \mathbb{Z} \) is inert if the ideal \( p\mathcal{O}_K \) is prime, in which case we have \( p\mathcal{O}_K = \mathfrak{p} \), that is \( t = 1 \), \( e = 1 \), and \( f = n \). A prime \( p \) is said to be ramified if \( e_i > 1 \) for some \( i \), and non-ramified otherwise. Whether or not a prime is ramified is directly related to the discriminant of the field.

**Theorem 23.** Let \( K \) be a number field. If \( p \) is ramified, then \( p \) divides the discriminant \( \Delta_K \).

A prime \( p \) is said to be totally ramified \( e = n \), \( t = 1 \), and \( f = 1 \). That is \( p\mathcal{O}_K = p^e \) for some \( p \). Finally, a prime is said to be split if \( e_1 = \ldots = e_t = 1 \).

We have the following relations among the number of factors of \( t \), their residual class degrees \( f_i \), and their ramification indices \( e_i \):

**Proposition 24.** Let \( K \) be a number field and \( \mathcal{O}_K \) its field of integers. Let \( p \in \mathbb{Z} \) and let

\[
p\mathcal{O} = p_1^{e_1} \cdots p_t^{e_t}
\]

be its factorisation in \( \mathcal{O}_K \). We have that

\[
n = [K : \mathbb{Q}] = \sum_{i=1}^{t} e_i f_i
\]

Furthermore, in the case of a Galois field, the above relation simplifies as follows:

**Proposition 25.** If the field extension \( K/L \) is Galois, then \( e_1 = \ldots = e_t = e \), \( f_1 = \ldots = f_t = f \) and

\[
eft = n.
\]

The example below shows that this need not be the case if \( K \) is not Galois.

**Example 26.** Let \( K = \mathbb{Q}(\sqrt{2}) \), then \( \mathcal{O}_K = \mathbb{Z}[\sqrt{2}] \). Observe that for \( p = 2 \), the factorisation of \( p\mathcal{O}_K \) is as follows

\[
2\mathcal{O}_K = (\sqrt{2})^3
\]

That is, \( e = 3 \), and \( f = g = 1 \).
Now let us look at the factorisation of $p\mathcal{O}_K$ for $p = 5$. The minimal polynomial $f(x) = x^3 - 2$ of \( \sqrt[3]{2} \) factorises as
\[
x^3 - 2 = (x + 2)(x^2 + 3x + 4) \in \mathbb{F}_5[x]
\]
with the quadratic factor irreducible modulo 5. Thus
\[
5\mathcal{O}_K = (5, 2\sqrt[3]{2} + 2) \cdot (5, \sqrt[3]{2}^2 + 3\sqrt[3]{2} + 4)
\]
Hence $p = 5$, we have $e_1 = e_2 = 1$, $f_1 = 1$, $f_2 = 2$, and $g = 2$.

A number field $K$ is said to be monogenic if its ring of integers is of the form $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$, that is $\mathcal{O}_K$ admits a power basis. Given a prime $p \in \mathbb{Z}$ in that case, there is a direct relation between the factorisation of the ideal $p\mathcal{O}_K$ and the factorisation of the minimal polynomial of $\alpha$ in the finite field $\mathbb{F}_p$.

**Proposition 27.** Let $K$ be a number field, with ring of integers $\mathcal{O}_K$, and let $p$ be a prime. Let us assume that there exists $\alpha$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and let $f$ be the minimal polynomial of $\alpha$, whose reduction modulo $p$ is denoted by $\bar{f}$. Let
\[
\bar{\bar{f}}(x) = \prod_{i=1}^{t} \bar{f}_i(x)^{e_i}
\]
be the factorisation of $f(x)$ in $\mathbb{F}_p(x)$, with $\bar{f}_i(x)$ coprime and irreducible. We set
\[
p_i = (p, f_i(\alpha)) = p\mathcal{O}_K + f_i(\alpha)\mathcal{O}_K
\]
where $f_i$ is any lift of $\bar{f}_i$ to $\mathbb{Z}[x]$, that is $\bar{f}_i = f_i \mod p$. Then
\[
p\mathcal{O}_K = p_1^{e_1} \cdot \cdots \cdot p_t^{e_t}
\]
if the factorisation of $p\mathcal{O}_K$ in $\mathcal{O}_K$.

For the precise statement and proof of the above proposition, see [Ogg10, Proposition 3.3]. While cyclotomic and quadratic fields are both always monogenic, there are already examples of cubic number fields, the ring of integers of which does not admit a power basis. Nonetheless, a very similar relation holds for general number fields. Given a number field $K$, let by $\theta$ be its primitive element. The ring $\mathbb{Z}[\theta]$ is an order in $\mathcal{O}_K$, and the following holds:

**Lemma 28.** Suppose the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is coprime to $p$. Then the primes $p_i$ in the factorisation of $p\mathbb{Z}[\alpha]$ do not decompose further going from $\mathbb{Z}[\alpha]$ to $\mathcal{O}_K$, so finding the prime ideals of $\mathbb{Z}[\alpha]$ that contain $p$ yields the primes that appear in the factorisation of $p\mathcal{O}_K$.

The proof of the lemma above can be found in [Ste10 Lemma 4.2.1], alongside the explicit statement of the factorisation of $p\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ for a given number field $K$ ([Ste10 Lemma 4.2.3]), which we recall here:

**Theorem 29.** Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$ over $\mathbb{Z}$. Suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is a prime. Let
\[
\bar{f} = \prod_{i=1}^{k} \bar{f}_i^{e_i} \in \mathbb{F}_p[x]
\]
where the $f_i$ are distinct monic irreducible polynomials. Let $p_i = (p, f_i(\alpha))$ where $f_i \in \mathbb{Z}[x]$ is a lift of $\bar{f}_i$ in $\mathbb{F}_p[x]$. Then
\[
p\mathcal{O}_K = \prod_{i=1}^{t} p_i^{e_i}
\]

22
B On the primitive element of a radical field extension

The aim of this section is to prove the bounds on the degree of the primitive element $\theta$ of our number field, and the size of the constants used in the linear combination of the field generators that we use to construct it.

Let us first recall the setting for our number field. Given $k$ radicals $\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}$, with the $a_i$ pairwise coprime, and the $d_i$ and $a_i$ of magnitude at most $2^k$. Let $d = \text{lcm}(d_1, \ldots, d_k)$, and denote by $\zeta_d$ a primitive $d$th root of unity. We would like to construct the primitive element $\theta$ for the number field $K = \mathbb{Q} \left[ \sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}, \zeta_d \right]$. Note that besides adjoining the radicals to $\mathbb{Q}$, we also make sure to add $\zeta_d$, which ensures our field extension $K$ is Galois.

The primitive element for number fields is as follows:

**Theorem 30.** Let $K = L[\alpha_1, \ldots, \alpha_k]$ be a finite extension of $L$, and assume that $\alpha_2, \ldots, \alpha_k$ are separable over $L$. Then there is an element $\theta \in K$ such that $K = L[\theta]$.

The proof of the above theorem is constructive (see [Mil21 Theorem 5.1]), and computes the primitive element $\theta$ as a linear combination of the generators $\alpha_1, \ldots, \alpha_k$, that is $\theta = \sum_{i=1}^k c_i \alpha_i$. The computation of $\theta$ is to be done inductively, constructing first a primitive element $\theta_2$ for $L[\alpha_1, \alpha_2]$, then $\theta_3$ for $L[\alpha_1, \alpha_2, \alpha_3]$, and so on until $\theta_k$. Furthermore, it is shown that only finitely many combinations of the constants $c_i$ fail to generate a primitive element for the field extension $K$. This gives rise to an effective version of the primitive element theorem for number fields that induces a bound on the degree of the algebraic number $\theta$, as well as on the size of the constants $c_i$. In particular, for a field generated by two algebraic numbers, the bounds are as follow (see [Kur06 Proposition 6.6]):

**Proposition 31.** Let $\alpha$ and $\beta$ be algebraic numbers of degree $m$ and $n$ respectively. There exists an integer $c \in \{1, \ldots, m^2n^2 + 1\}$ such that $\alpha + c\beta$ is a primitive element of $\mathbb{Q}[\alpha, \beta]$.

Note that in general, we could choose $c_i \in \mathbb{Q}$ with only finitely many combinations of the $c_i$’s not giving us a primitive element. Thus the primitive element need not be an algebraic integer in general. However, we make the choice to choose $c_i \in \mathbb{Z}$, therefore the minimal polynomial $f_\theta$ of $\theta$ is monic and $\theta$ an algebraic integer.

Now let us prove our claim on the bounds on our primitive element $\theta$:

**Lemma 15 (Bound on the primitive element).** The field $K$ has a primitive element $\theta$, computed as the linear combination

$$\theta = c_0 \zeta_d + \sum_{i=1}^k c_i \sqrt[n]{a_i}$$

with $c_i \leq 2^{4k^2} \in \mathbb{Z}$ and $\deg f_\theta \leq 2^{2k^2}$.

**Proof.** Note that given $d_1, \ldots, d_k \leq 2^k$, their least common multiple is at most of size $2^{k^2}$, hence we have:

$$\deg \zeta_d \leq 2^{k^2}.$$ 

In the spirit of the proof of the primitive element theorem, use Proposition 31 inductively as follows:

$$\theta_2 = \sqrt[n]{a_1} + c_2 \sqrt[n]{a_2} \quad \deg \theta_2 \leq 2^{2k} \quad c_2 \leq (2^k)^2 (2^k)^2 + 1 \leq 2^k$$

$$\theta_3 = \sqrt[n]{a_1} + c_2 \sqrt[n]{a_2} + c_3 \sqrt[n]{a_3} \quad \deg \theta_3 \leq 2^{3k} \quad c_3 \leq (2^{2k})^2 (2^k)^2 + 1 \leq 2^{6k}$$

$$\vdots$$
\[ \theta_k = \sqrt[p]{a_1} + c_2 \sqrt[p]{a_2} + \ldots + c_k \sqrt[p]{a_k} \quad \text{deg } \theta_k \leq 2^{k^2} \]

\[ \theta = \theta_k + c_0 \zeta_d \quad \text{deg } \theta_2 \leq 2^{k^2} \]

\[ c_k \leq \left(2^{(k-1)k}\right)^2 \left(2^{k}\right)^2 + 1 \leq 2^{2k^2} \]

The claimed bounds on the degree of \( \theta \) and the size of the constants \( c_i \) follow. \( \square \)

## C Bound on the norm

In this section, we prove our bound on the norm of the algebraic integer computed by an algebraic circuit \( C \) on a radical input \( \sqrt[p]{a_1}, \ldots, \sqrt[p]{a_k} \), with the \( a_i \) pairwise coprime, and the \( d_i \) and \( a_i \) of magnitude at most \( 2^k \), that is an instance of the RIT problem. Recall we denote by \( K = \mathbb{Q}[\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_k}, \zeta_d] \), where \( d = \text{lcm}(d_1, \ldots, d_k) \), \( \zeta_d \) is a primitive \( d \)th root of unity. We claim:

**Lemma 16** (Bound on the norm). *Given an algebraic circuit \( C \) of size \( k \), denote by \( \alpha \in \mathcal{O}_K \) the algebraic integer computed by \( C \) evaluated on the \( \sqrt[p]{a_i} \). We have

\[ |N(\alpha)| \leq 2^{2k^3} \]

for \( k \geq 4 \).

**Proof.** Write \( \alpha = \sum b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}} \) where \( e_{i_1} + \ldots + e_{i_k} \leq 2^k \), \( b_i \in \mathbb{Z} \) with \( b_i \leq 2^{2k} \), \( i \) ranges over all monomials of the shape \( x_1^{e_{i_1}} \cdots x_k^{e_{i_k}} \). Let us denote by \( M \) the number of all such monomials, and count how many of them we can construct. Denote by \( D = \max(d_1, \ldots, d_k) \), then

\[ M = \binom{k + D}{D} = \binom{k + 2^k}{k} \leq \left( \frac{k + 2^k}{k} \right) \leq 2^{k^2} \]

Denote by \( G = \text{Gal}(K/\mathbb{Q}) \). Following Lemma 15, note that given the size bounds on our input, \( |G| \leq 2^{2k^2} \). Observe that the action of all \( \sigma \in G \) is determined by their action on \( \zeta_d \), that is

\[ \sigma(\sqrt[p]{a_i}) = \sqrt[p]{a_i} \sigma(\zeta_d). \]

Then

\[ N(\alpha) = N\left( \sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}} \right) \]

\[ = \prod_{\sigma \in G} \sigma \left( \sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}} \right) \]

\[ = \prod_{\sigma \in G} \sum_{i=1}^{M} b_i \left( \max_{j=1}^{k} x_j \right)^{\#e_i} \sigma(\zeta_d)^{\#e_i} \text{ where } \#e_i = e_{i_1} + \ldots + e_{i_k} = \sum_{j=1}^{k} e_{i_j} \]

\[ = \prod_{\ell \in \mathbb{Z}[G]} \sum_{i=1}^{M} b_i \left( \max_{j=1}^{k} x_j \right)^{\#e_i} \left( \zeta_d^{l} \right)^{\#e_i} \]

Finally, putting together all of our bounds yields

\[ |N(\alpha)| \leq \prod_{l=1}^{2^{2k^2}} \left( \sum_{l=1}^{2^{2k}} (2^{k})^{2k} \right) \]
\[
\leq \prod_{l=1}^{2^k} \left( \sum_{i=1}^{2^k} 2^{2^k(k+1)} \right) \\
\leq 2^{2k} \prod_{l=1}^{2^k} \left( 2^{k^2} \cdot 2^{2^k(k+1)} \right) \\
\leq \left( 2^{k^2} \cdot 2^{2^k(k+1)} \right)^{2^{2k}} \\
\leq 2^{2^{2k^2}} (2^{k^2} + 2^k + k^3) \\
\leq 2^{2^{2k^2}} \text{ for } k \geq 4.
\]

\[\square\]

### D Bound on the discriminant

The aim of this section is to prove a bound on the discriminant of the minimal polynomial of the primitive element of our number field \(K\). Recall we denote by \(K = \mathbb{Q}[\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}, \zeta_d]\), where \(d = \text{lcm}(d_1, \ldots, d_k)\), and \(\zeta_d\) is a primitive \(d\)th root of unity, and compute \(\theta\) as a linear combination of \(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}, \zeta_d\). Note also that we assume the magnitude of the \(d_i\)'s and \(a_i\)'s to be at most \(2^k\).

Recall that given a polynomial \(f(x) = a_n x^n + \ldots + a_1 x + a_0\) with roots \(r_1, \ldots, r_n\), its discriminant can be computed as

\[
\Delta_f = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{i\neq j} (r_i - r_j) 
\]

(5)

Now let us see how we use it to prove our claim:

**Lemma 19** (Bound on the discriminant). *For the primitive element \(\theta\) of \(K\), computed as a linear combination of \(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}\), and \(\zeta_d\), we have

\[
|\text{Disc}(\mathbb{Z}[\theta])| \leq 2^{2^{2k^2}} 
\]

for \(k \geq 4\).

**Proof.** Denote by \(G = \text{Gal}(K/\mathbb{Q})\) the Galois group of \(K\). Recall we construct the primitive element \(\theta\) of our radical number field as a linear combination of the radicals \(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}\) and a primitive \(d\)th root of unity \(\zeta_d\) as follows:

\[
\theta = c_0 \zeta_d + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}.
\]

We choose the \(c_i \in \mathbb{Z}\), hence \(\theta\) is an algebraic integer. The minimal polynomial \(f_\theta\) of the primitive element \(\theta\) has roots \(\theta = \theta_1, \ldots, \theta_{|G|}\). Note that the roots of \(f_\theta\) are given by the elements of \(G\), that is, \(\theta_i = \sigma_i(\theta)\) for some \(\sigma_i \in G\). Recall also that the elements of the Galois group \(G\) act on conjugates of a given element of \(K\) by permuting the \(d\)th roots of unity, that is, given \(\alpha \in K\), \(\sigma_i(\alpha) = \alpha \zeta_d^{b_i}\) for some and \(\sigma_i \in G\).

Note that given \(d_1, \ldots, d_k \leq 2^k\), their least common multiple is at most of size \(2^{2k}\), hence we have:

\[
\deg \zeta_d \leq 2^{k^2}
\]

As stated in Lemma 13, the constants \(c_i\) in the computation of the primitive element can be bound by:

\[
c_i \leq 2^{4k^2}
\]

25
Now given \( \sigma_j \in G \), write

\[
\sigma_j(\theta) = \sigma_j \left( c_0 \zeta_d + \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \right) \\
= c_0 \sigma_j(\zeta_d) + \sum_{i=1}^{k} c_i \sigma_j \left( \sqrt[4]{a_i} \right) \\
= c_0 \zeta_d^{i+1} + \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \zeta_d^i
\]

Then for \( 1 \leq j, l \leq |G|, j \neq l \)

\[
\sigma_j(\theta) - \sigma_l(\theta) = \left( c_0 \zeta_d^{i+1} + \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \zeta_d^i \right) - \left( c_0 \zeta_d^{l+1} + \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \zeta_d^i \right) \\
= c_0 \left( \zeta_d^{i+1} - \zeta_d^{l+1} \right) + \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \left( \zeta_d^i - \zeta_d^l \right)
\]

Note that for any two \( d \)th roots of unity \( \zeta_d^j, \zeta_d^l \), we always have \( \zeta_d^j - \zeta_d^l \leq 2 \), hence

\[
\sigma_j(\theta) - \sigma_l(\theta) \leq 2c_0 + 2 \left( \sum_{i=1}^{k} c_i \sqrt[4]{a_i} \right) \\
\leq 2 \cdot 2^{4k^2} + 2 \left( \sum_{i=1}^{k} 2^{4k^2} \cdot 2^k \right) \\
\leq 2^{4k^2+1} + 2^{4k^2+k+1}k \\
\leq 2^{2k^3} \text{ for } k \geq 4.
\]

Thus

\[
|\Delta_{f_\theta}| = \prod_{j \neq l} |\sigma_j(\theta) - \sigma_l(\theta)| \\
\leq \left( 2^{2k^3} \right)^{|G|^2} \\
\leq \left( 2^{k^3} \right)^{2^{2k^2}} \\
\leq \left( 2^{k^3} \right)^{2^{4k^2}} \\
\leq 2^{2k^3 \cdot 2^{4k^2}} \\
\leq 2^{2^{5k^2}} \text{ for } k \geq 4.
\]

\[\square\]

**E  Bound on the number of primes \( p \) such that \( \mathbb{F}_p \) contains a representation of the input radicals**

The aim of this section is to prove the following proposition:

**Lemma 20.** Assuming GRH,

\[
\pi_{f_\theta}(2^{4k^3}) \geq 2^{k^3} + 1.
\]
Proof. Recall the bound on $\pi_{f_\theta}$ given in Proposition 17:

$$\pi_{f_\theta}(x) \geq \frac{1}{\deg f_\theta} \left[ \pi(x) - \log \Delta_{f_\theta} - cx^{1/2} \log(\Delta_{f_\theta} x^{\deg f_\theta}) \right]$$

Recall also that $\pi(x)$, that is, the number of primes $\leq x$, can be bound as

$$\pi(x) \geq \frac{x}{\log x}$$

Finally, following Lemma 15, note that $\deg f_\theta \leq 2^{2k^2}$.

Now compute

$$\pi_{f_\theta}(2^{4k^3}) \geq \frac{2^{4k^3}}{2^{2k^2} \cdot 4k^3} - 2^{3k^2} - c \cdot 2^{2k^3} \cdot 2^{3k^2} - c \cdot 2^{2k^3} \cdot 4k^3$$

$$\geq \frac{2^{4k^3}}{2k^2} - 2^{2k^3} - c \cdot 2^{2k^3} \cdot 2^{3k^2} - c \cdot 2^{2k^3} \cdot 4k^3 \quad \text{for } k \geq 4$$

$$\geq 2^{3k^3} - 2^{2k^3} (1 + c \cdot 2^{3k^2} + c \cdot 4k^3)$$

$$\geq 2^{2k^3} (2^{k^3} - c \cdot 2^{3k^2} + c \cdot 4k^3)$$

$$\geq 2^{2k^3} \text{ for a fixed constant } c \text{ and } k \geq \max(c, 5)$$

$$\geq 2^{k^3} + 1.$$  

\[\square\]

**F  A note on Pocklington’s algorithm**

Pocklington’s algorithm is a technique for solving congruences of the form $x^2 \equiv a \mod p$, where $x$ and $a$ are integers and $a$ is a quadratic residue modulo $p$. Given an integer $a$ and odd prime $p$ as input, the algorithm separates three cases for $p$, and then computes $x$ accordingly. We are interested in the case where $p = 8m + 5$ for some $m \in \mathbb{N}$, as we note that $x$ can be computed deterministically as follows:

<table>
<thead>
<tr>
<th><strong>Pocklington’s algorithm for $p = 8m + 5$</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Prime $p \equiv 5 \mod 8$ and integer $a$ that is a quadratic residue modulo $p$</td>
</tr>
<tr>
<td><strong>Output:</strong> Solution of the equation $x^2 \equiv a \mod p$</td>
</tr>
<tr>
<td><strong>Step 1:</strong> Write $p = 8m + 5$ with $m \in \mathbb{N}$</td>
</tr>
</tbody>
</table>
| **Step 2:** If $a^{2m+1} \equiv 1 \mod p$:
  - Return $x = \pm a^{m+1}$.
  - If $a^{2m+1} \equiv -1 \mod p$:
    - Write $y = \pm (4a)^{m+1}$ and return $x = \pm \frac{y}{2}$ if $y$ is even, and $x = \pm \frac{4a}{y} y$ if $y$ is odd. |

Figure 5: Procedure to solve the congruence $x^2 \equiv a \mod p$ for prime $p \equiv 5 \mod 8$.

Let us briefly elaborate on the correctness of the above procedure. Given $p = 8m + 5$ with $m \in \mathbb{N}$, following Fermat’s little theorem, we have $x^{8m+4} \equiv 1 \mod p$. Since $x^2 \equiv a \mod p$, we can rewrite it as $a^{4m+2} \equiv 1 \mod p$. Now, let us look at two separate cases for $a$:

1. $a^{2m+1} \equiv 1 \mod p$
   - Then $a^{2m+2} \equiv a \mod p$, that is $(a^{m+1})^2 \equiv a \mod p$, hence $x = \pm a^{m+1}$.  

27
2. \( a^{2m+1} \equiv -1 \mod p \)

Note that 2 is a quadratic non-residue, so \( 4^{2m+1} \equiv -1 \mod p \), hence \( 4^{2m+1} a^{2m+1} \equiv 1 \mod p \). That is \( (4a)^{2m+1} \equiv 1 \mod p \) and following the reasoning from the previous case \( y = \pm(4a)^{m+1} \) is a solution of \( y^2 = 4a \), hence \( x = \pm \frac{y}{2} \), or if \( y \) is odd, \( x = \pm \frac{p+y}{2} \).

G The probability of choosing a good prime \( p \)

The aim of this section is to prove a bound on the probability of randomly choosing a good prime \( p \) in the randomised polynomial time algorithm for the S-RIT problem.

**Proposition 22.** Given an algebraic circuit \( C \) of size \( k \), denote by \( \alpha \) the algebraic integer computed by \( C \) evaluated on the \( \sqrt{a_i} \). Suppose that \( p \) is chosen uniformly at random from the set \( S(a_1, \ldots, a_k) \) defined in \( [3] \). Assuming GRH,

(i) \( p \) is prime with probability at least \( \frac{1}{16} k^3 \), and

(ii) given that \( p \) is prime, the probability that it divides \( N(\alpha) \) is at most \( 2^{-k^3} \).

**Proof.** We follow the proof of [BPSW20, Proposition 9].

Recall that we set \( a_i \leq 2^k \), which implies \( A \leq 2^{k^2} \). For (i), we note that by Theorem 21, the probability that \( p \) is prime is at most

\[
\frac{\pi_{8A,b+1}(2^{5k^3})}{2^{5k^3}/8A} \geq \frac{8A}{\varphi(8A) \log 2^{5k^3}} - \frac{c \log 2^{5k^3} 8A}{(2^{5k^3})^{1/2}}
\]

\[
\geq \frac{1}{2k^3} - \frac{c 5k^3 2^{k^2+3}}{22k^3}
\]

\[
\geq \frac{1}{2k^3} - \frac{c 5k^3 2^{k^3}}{22k^3}
\]

where \( c \) is the absolute constant mentioned in the theorem. For \( k \) sufficiently large, the above is \( \frac{1}{6k} \), which proves the claim.

For (ii), by Lemma 16 the norm of \( \alpha \) has absolute value at most \( 2^{2k^3} \), and hence \( N(\alpha) \) has at most \( 2^{k^3} \) distinct prime factors. Then, for \( k \) sufficiently large, the probability that \( p \) divides \( N(\alpha) \) given that \( p \) is prime is at most

\[
\frac{6k^3 \cdot 8A \cdot 2^{k^3}}{2^{5k^3}} \leq 2^{-k^3}
\]

\( \square \)