Identity Testing for Radical Expressions

Nikhil Balaji
nbalaji@cse.iitd.ac.in
IIT Delhi
Delhi, India

Klara Nosan
nosan@irif.fr
Université Paris Cité, CNRS, IRIF
Paris, France

Mahsa Shirmohammadi
mahsa@irif.fr
Université Paris Cité, CNRS, IRIF
Paris, France

James Worrell
jbw@cs.ox.ac.uk
Department of Computer Science, University of Oxford
Oxford, UK

ABSTRACT

We study the *Radical Identity Testing* problem (RIT): Given an algebraic circuit over integers representing a multivariate polynomial $f(x_1, \ldots, x_k)$ and nonnegative integers $a_1, \ldots, a_k$ and $d_1, \ldots, d_k$, written in binary, test whether the polynomial vanishes at the *real radicals* $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, i.e., test whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. We place the problem in coNP assuming the Generalised Riemann Hypothesis (GRH), improving on the straightforward PSPACE upper bound obtained by reduction to the existential theory of reals. Next we consider a restricted version, called 2-RIT, where the radicals are square roots of prime numbers, written in binary. It was known since the work of Chen and Kao [16] that 2-RIT is at least as hard as the polynomial identity testing problem, however no better upper bound than PSPACE was known prior to our work. We show that 2-RIT is in coRP assuming GRH and in coNP unconditionally. Our proof relies on theorems from algebraic and analytic number theory, such as the Chebotarev density theorem and quadratic reciprocity.

CCS CONCEPTS

• **Mathematics of computing** → **Probabilistic algorithms**; • **Computing methodologies** → **Algebraic algorithms**; **Number theory algorithms**.

KEYWORDS

Algebraic Circuits, Computational Complexity, Number Fields, Polynomial Identity Testing, Randomised Algorithms

ACM Reference Format:
Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. 2022. Identity Testing for Radical Expressions. In *37th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) (LICS '22), August 2–5, 2022, Haifa, Israel.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3531130.3533331

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
LICS '22, August 2–5, 2022, Haifa, Israel
© 2022 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9351-5/22/08…$15.00
https://doi.org/10.1145/3531130.3533331

1 INTRODUCTION

Identity testing is a fundamental algorithmic question with numerous applications. In *algebraic* identity testing, the task is to determine the zeroness of an expression evaluated in a given ring. This problem has many different versions, depending on the syntax for giving the expression and the ring in which the evaluation is to be performed.

A basic instance of algebraic identity testing is the Arithmetic Circuit Identity Testing (ACIT) problem, which involves deciding the zeroness of an integer represented as an arithmetic circuit. The difficulty in this problem is that the integer may have bit length exponential in the size of the circuit. However, the problem admits a randomized polynomial-time algorithm: one evaluates the circuit modulo a prime that is randomly chosen in a certain range. The ACIT problem turns out to be polynomial-time interreducible with the problem of determining zeroness of an arithmetic circuit evaluated in the ring of multivariate polynomials: the so-called Polynomial Identity Testing (PIT) problem [4]. Over the years, PIT has found diverse applications in algorithm design; a few well-known examples are program testing [21], detecting perfect matchings [42], factoring polynomials [29], pattern matching in compressed texts [9, 35], primality testing [1, 2], equivalence and minimization of weighted automata [31, 32] and linear recurrence sequences [3, 17]. Whether PIT admits a deterministic polynomial-time algorithm is one of the central open questions in complexity theory.

The topic of this paper is *radical identity testing*, that is, testing zeroness of an expression in radicals, represented by an algebraic circuit. This generalizes the ACIT problem: the evaluation of the circuit occurs in the ring of integers of a number field, rather than the ring of integers of the rational numbers. Historically, expressions in radicals played a central role in solving polynomial equations. Such expressions also naturally arise in optimization problems on graphs embedded in Euclidean space, such as the Euclidean Minimal Spanning Tree and Traveling Salesperson problems [24]. Another source of radical expressions arises from an approach by Chen and Kao [16] to derandomizing PIT. Their idea was to test the zeroness of a multivariate polynomial by evaluating it on a certain randomly chosen radical expression. In their method, by construction, the radical expressions are such that the result of the evaluation is zero if and only if the polynomial is identically zero. The challenge then becomes to determine the zeroness of the resulting expression in radicals, for which Chen and Kao use numerical approximation.

This approach allowed to reduce the number of random bits required for the problem compared with previously known methods, such as those based on the Schwarz-Zippel lemma.

In this paper, we introduce a symbolic approach to the problem of identity testing algebraic integers in the number field generated over $\mathbb{Q}$ by *real radicals*; given an algebraic circuit representing a multivariate polynomial $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, and radical inputs $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ where the radicands a_i, and exponents d_i are nonnegative integers, the *Radical Identity Testing* (RIT) problem is to decide whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. The problem is easily seen to admit a PSPACE upper bound by a reduction to the existential theory of reals [14]: introduce a new formal variable for every gate of the circuit, add the equations $x_i^{d_i} - a_i = 0$ and $x_i > 0$ for every radical; RIT is now decided by checking if the resulting system of polynomial equations has a solution over the real numbers.

Our symbolic algorithm places RIT in coNP, assuming the generalised Riemann hypothesis (GRH). The main idea behind our algorithm is that if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \neq 0$ then there is a polynomial-length polynomial-time checkable witness of this fact — namely a prime p and $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$, satisfying $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$, such that $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k)$ is non-zero, where $\overline{f}$ is the reduction of f modulo p. Crucial to our approach is the fact of *joint transitivity*, which is the observation that the Galois group of the underlying real field acts jointly transitively on the roots of the various equations $x^{d_i} - a_i = 0$. This allows us to use any of the d_i conjugates α_i of $\sqrt[d_i]{a_i}$ over $\mathbb{F}_p$ in our symbolic algorithm to test whether $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$. In fact, joint transitivity alone can be used in conjunction with a result of Koiran [34] to place RIT in the polynomial hierarchy assuming GRH. Using Cheboratev's density theorem, and choosing a suitable prime, we improve this upper bound to show that RIT can be solved in coNP assuming GRH.

We next tackle a special case of RIT namely 2-RIT where the inputs to the circuit are square roots of distinct primes. The PIT algorithm in [16] gives a randomized numerical algorithm for the specific case of 2-RIT involving *bounded* algebraic circuits[1] at square roots of distinct prime numbers. However their method completely breaks down when the assumption of boundedness is dropped and the best known upper bound prior to our work was the same as that of the general RIT problem using Koiran's algorithm. We show that 2-RIT is in coRP assuming GRH and in coNP unconditionally. Our techniques are fundamentally different from those of [16]; we use quadratic reciprocity and Dirichlet's theorem on the density of primes in arithmetic progressions.

Related Work. Balaji et al. [7] studied the *cyclotomic identity testing* problem, where the goal is to determine if an algebraic integer in the cyclotomic number field $\mathbb{Q}(\zeta_n)$ computed by a given algebraic circuit is zero. They show that the problem lies in the complexity class BPP assuming the Generalised Riemann Hypothesis (GRH), and unconditionally in coNP. We further discuss the approach of [7] in relation to our work in Section 3.

Blömer [12] gave a randomized algorithm to test if a bounded algebraic circuit evaluated at low degree radicals evaluates to zero. Central to such identity questions on algebraic numbers is the knowledge of the Galois group of the extension where the numbers live in. Algorithmic complexity of computing with Galois groups is investigated in [5, 39, 46].

As in [12], our formulation of RIT does not permit nesting of radicals, that is, expressions such as $\sqrt{6 + 4\sqrt{2}}$. Computational problems associated with nested radicals are treated in [10, 11].

The Sum of Square Roots problem. Closely related to 2-RIT is the square root sum problem where the goal is to infer the sign of a given linear combination of square roots. This is a notorious open problem in numerical analysis and computational geometry. It is known to be decidable in the *Counting Hierarchy* [4], and the question of determining its precise computational complexity remains open since it was explicitly posed by Garey, Graham and Johnson [24] in 1976. Along with the related problem of determining the sign of an integer computed by a variable-free algebraic circuit, the square root sum problem is frequently used as a tool for proving hardness and obtaining upper bounds in quantitative verification [8, 22, 26, 33], algorithmic game theory [15, 23, 51], formal language theory and logic [27, 40]. We refer the interested reader to [20, 30] and the references therein for a discussion on the complexity status of the square root sum problem and related geometric questions.

The Elementary Constant problem. A related but harder identity testing problem that is a fundamental question at the intersection of transcendental number theory and model theory is the *Elementary Constant problem* [44]: given a complex number built from rationals using addition, multiplication and exponentiation determine if it is zero. Such numbers are called Elementary numbers, and they form an algebraically closed subfield of the complex numbers. While there is a decision procedure assuming Schanuel's conjecture [45] for the elementary constant problem, it is not known to be decidable unconditionally, and no significant complexity lower/upper bounds are known.

The Compressed Word problem. Arguably the earliest and most fundamental result on identity testing questions are word problems on finitely generated groups and semigroups [19]. There is a large body of work on the *Compressed Word problem* [41] which studies the computational complexity of word problems when the word is represented succinctly via a *straight line program*; see [7, 35] for relations between such word problems and arithmetic identity testing.

2 BACKGROUND AND OVERVIEW

In this section, we give a high-level overview of our main results and the main techniques used in our algorithms. We also introduce some of the definitions and notations along the way; we refer the reader to Appendix B and [49, 50] for more details.

Algebraic Circuits. Let $X = \{x_1, \ldots, x_k\}$ be a set of commutative variables. An *algebraic circuit* over X is a directed acyclic graph 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

[1] An algebraic circuit of size s computing a multivariate polynomial is called bounded if the degree and bit-length of the coefficients of the polynomials computed at every gate of the circuit is bounded by a polynomial function in s.

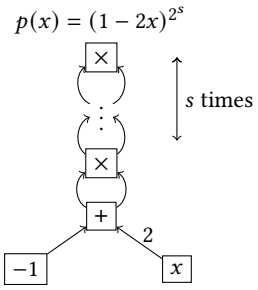

Figure 1: An algebraic circuit computing the polynomial $p(x) = (1-2x)^{2^s}$, with the highest degree monomial x^{2^s} and the coefficients double exponential 2^{2^s} in its size $s+3$.

the output of the circuit, a k-variate polynomial, computed in an obvious bottom-up manner. The *size* of a circuit is the number of its gates; see Figure 1. The *degree* of a circuit C is defined inductively as follows: input gates have degree 1, the degree of an addition gate is the maximum of the degrees of its inputs, the degree of a multiplication gate is the sum of the degrees of its inputs, and the degree of C is the degree of the output gate. Note that the degree of an algebraic circuit is an upper bound on the degree of its underlying polynomial. Thus the total 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.

2.1 Radical Identity testing

Let $f(x_1, \ldots, x_k)$ be a multivariate polynomial computed by an algebraic circuit, and $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ be k radicals, where the radicands $a_i \in \mathbb{N}$, and the exponents $d_i \in \mathbb{N}$ are nonnegative integers, written in binary. The *Radical Identity Testing* (RIT) problem asks whether

$$f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0.$$

We define the size of an RIT instance as the maximum of the size of the circuit, the number of input radicals k and the bit-length of the radicands a_i and exponents d_i.

The 2-RIT problem. This is a special case of RIT where all input radicals $\sqrt{a_1}, \ldots, \sqrt{a_k}$ are square roots and all radicands a_i are rational primes, written in binary.

The Bounded-RIT problem. This variant is defined exactly as the RIT problem, except that the input also includes an upper bound on the degree of the circuit that is given in unary. Thus in Bounded-RIT the degree of the circuit is at most the size of the instance.

2.2 Algebraic Number fields

Recall that $\alpha \in \mathbb{C}$ is *algebraic* if it is a root of a non-zero polynomial in $\mathbb{Q}[x]$. The minimal polynomial of α (over $\mathbb{Q}$) is the unique monic polynomial in $\mathbb{Q}[x]$ (that is a polynomial with the leading coefficient 1) having α as a root. The degree of an algebraic number α is defined to be the degree of its minimal polynomial, and denoted by $\deg \alpha$. If the minimal polynomial has integer coefficients then we say that α is an algebraic integer. Given $a, d \in \mathbb{N}$, the radical $\sqrt[d]{a}$ is an algebraic integer.

An *algebraic number field* (or simply number field) K is a finite degree field extension of $\mathbb{Q}$, that is, K is a field that contains $\mathbb{Q}$ and has finite dimension when considered as a vector space over $\mathbb{Q}$. The dimension of this vector space is called the degree of the extension and is denoted by $[K : \mathbb{Q}]$. We further denote by O_K the subring of K comprised by the algebraic integers in K. The ring O_K is a free abelian group and admits a $\mathbb{Z}$-basis; in other words, it can be generated over $\mathbb{Z}$ by adjoining a finite set of algebraic integers.

Given $n \in \mathbb{N}$, we write ζ_n for the primitive complex n-th root of unity $\zeta_n = e^{\frac{2\pi i}{n}}$. The n-th cyclotomic polynomial, denoted by Φ_n, is the minimal polynomial of ζ_n. The number field $\mathbb{Q}(\zeta_n)$ is an extension of $\mathbb{Q}$ obtained by adjoining ζ_n to it, where $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is equal to the degree of Φ_n. It is well known that the ring of integers of $\mathbb{Q}(\zeta_n)$ is the ring $\mathbb{Z}[\zeta_n]$ that is generated over $\mathbb{Z}$ by ζ_n.

Given a polynomial $f \in \mathbb{Q}[x]$, the splitting field K of f is the subfield of $\mathbb{C}$ generated by the roots of f. We say that a field extension $K/\mathbb{Q}$ is a Galois extension if K is the splitting field of some polynomial. The Galois group of K over $\mathbb{Q}$, denoted by $\mathrm{Gal}(K/\mathbb{Q})$, is comprised of all automorphisms of K that fix $\mathbb{Q}$ pointwise. The image of $\alpha \in K$ under an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is called a Galois conjugate of α, in other words, the Galois conjugates of α are precisely all the roots of its minimal polynomial. The Galois conjugates of ζ_n are all its powers ζ_n^k with $\gcd(k, n) = 1$. The norm of α over a Galois extension K is defined as the product of all the Galois conjugates of α:

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\alpha).$$

Note that the norms of all Galois conjugates are equal, and the norm of an algebraic integer is always a rational integer itself.

The minimal polynomial of the real radical $\sqrt[d]{a}$ over $\mathbb{Q}$ has the form $x^t - c$ where t is the smallest positive integer such that there exists an integer c with $\sqrt[d]{a} = \sqrt[t]{c}$. The conjugates of $\sqrt[d]{a}$ are then $\zeta_t^j \sqrt[t]{c}$ with $1 \le j \le t$. The splitting field K of $\prod_{i=1}^{k}(x^{d_i} - a_i)$ is $\mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}, \zeta_d)$, obtained by adjoining the radicals $\sqrt[d_i]{a_i}$ and a primitive root of unity ζ_d, with order $d = \mathrm{lcm}(d_1, \ldots, d_k)$, to $\mathbb{Q}$.

Given a number field K, the ring of integers O_K may not be a unique factorisation domain. However we do have unique factorisation of ideals into products of prime ideals in O_K. Recall here that an ideal $\mathfrak{p} \subset O_k$ is called a prime ideal if for all algebraic integers α and β, if $\alpha\beta \in \mathfrak{p}$, then at least one of α and β is in $\mathfrak{p}$. We say that a prime $p \in \mathbb{Z}$ splits completely in O_K if we can write pO_K as:

$$pO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

where the $\mathfrak{p}_i$ are distinct prime ideals of O_K and $n = [K : \mathbb{Q}]$. In the case when K is the splitting field of a polynomial $f \in \mathbb{Z}[X]$ over $\mathbb{Q}$, a sufficient condition for p to split completely over K is that f splits into distinct linear factors over the field $\mathbb{Q}_p$ of p-adic numbers.

2.3 Symbolic Algorithm

We will present a symbolic approach to identity testing of algebraic numbers that generalises the well-known fingerprinting procedure for solving ACIT which involves evaluating an algebraic circuit modulo a randomly chosen prime.

In the setting of ACIT, the computation occurs in the ring of integers $\mathbb{Z}$ of $\mathbb{Q}$. The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$, for (rational) primes

p. The algorithm takes the computation to a finite field $\mathbb{F}_p$ by a surjective homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}_p$ with kernel $p\mathbb{Z}$. The homomorphism φ is isomorphic to the quotient map of $\mathbb{Z}$ by the maximal ideal $p\mathbb{Z}$.

The soundness of the algorithm relies on the fact that if the value $z \in \mathbb{Z}$ computed by the circuit is non-zero, then one can randomly choose a prime p of size polynomial in the bit length of the input such that $\varphi(z)$ is non-zero.

A coNP procedure for RIT: Given input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ to RIT, we first reduce RIT to the case that the radicands a_i are pairwise coprime numbers and that the minimal polynomials of the input radicals $\sqrt[d_i]{a_i}$ are $x^{d_i} - a_i$ for all $i = 1, \ldots, k$. To do this we generalise the reduction in [12] and use the *factor refinement* algorithm [6] ; see Appendix A. Denote by K the splitting field of $\prod_{i=1}^{k}(x^{d_i} - a_i)$.

In Figure 2, we present a conceptually simple algorithm for deciding RIT and place this problem in coNP. Our coNP procedure is similar in spirit to the coRP procedure for the ACIT problem, alluded to above, inasmuch as it involves evaluating the circuit modulo a prime ideal. The proof of the correctness though is not as straightforward and relies on characteristics of the Galois group of K and concepts from number theory.

In the case of RIT we think of the evaluation as occurring in the ring of integers O_K. Specifically, the idea is to work modulo a prime ideal $\mathfrak{p}$ of O_K such that the quotient $O_K/\mathfrak{p}$ is a finite field $\mathbb{F}_p$ for some rational prime p. Note that the algorithm works directly with the finite field $\mathbb{F}_p$—the prime ideal $\mathfrak{p}$ is implicit in the choice of radicals in Line 1, and ideals in K only feature in the proof of correctness of the algorithm. Overall, the key idea is that if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \neq 0$ then there is a polynomial-length polynomial-time checkable witness of this fact — namely a prime p and $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$, satisfying $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$, such that $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k)$ is non-zero, where $\overline{f}$ is the reduction of f modulo p.

We first summarise the algorithm, see Figure 2, and then outline the correctness argument.

(1) We find a rational prime p such that each polynomial among $x^{d_1} - a_1, \ldots, x^{d_k} - a_k$ splits into distinct linear factors over $\mathbb{F}_p$. We can find such a prime p in non-deterministic polynomial time in the length of the problem instance by (i) choosing a prime p such that $p \equiv 1 \bmod d$, which ensures that $\mathbb{F}_p$ contains a primitive d-th root of unity, and (ii) guessing and checking $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ such that $\overline{\alpha}_i$ is any root in $\mathbb{F}_p$ of the polynomial $x^{d_i} - a_i$.

(2) We evaluate the polynomial $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k)$ in $\mathbb{F}_p$, where $\overline{f}(x_1, \ldots, x_k) \in \mathbb{F}_p[x_1, \ldots, x_k]$ is the reduction of f modulo p. If the result of this computation is zero then we report 'Zero'; otherwise we report 'Non-zero'.

Having summarised the algorithm we can now state our main result:

Theorem 1. *The RIT problem is in* coNP *under GRH.*

Below, we give a high-level idea of the correctness of Theorem 1. The first element of the correctness proof of the coNP algorithm is to argue that the prime p chosen in Item 1 completely splits in the ring of integers O_K. In this situation, for any prime-ideal factor $\mathfrak{p}$ of p, each quotient field $O_K/\mathfrak{p}$ is isomorphic to the finite field $\mathbb{F}_p$. By standard results in algebraic number theory we know that p completely splits in O_K if each polynomial $x^{d_1} - a_1, \ldots, x^{d_k} - a_k$ splits into linear factors over the field $\mathbb{Q}_p$ of p-adic numbers. But the latter requirement is guaranteed by Hensel's Lemma in tandem with Conditions 1(i) and 1(ii) that determine the choice of p in the algorithm. In more detail, Condition 1(i), that $p \equiv 1 \bmod d$, entails that $\mathbb{F}_p$ contains a primitive d-th root of unity. Indeed, since the powers of a root of unity are also all a root of unity themselves, and since the multiplicative group $\mathbb{F}_p^*$ is cyclic, it is clear that $\mathbb{F}_p^*$ contains a primitive d-th root of unity just in case $d \mid p - 1$. In combination with Condition 1(ii), that each of the polynomials $x^{d_1} - a_1, \ldots, x^{d_k} - a_k$, has a root in $\mathbb{F}_p$, we can conclude that each of the above polynomials in fact splits into distinct linear factors over $\mathbb{F}_p$. Then Hensel's Lemma allows us to lift this factorisation over $\mathbb{F}_p$ into a factorisation into distinct linear factors over $\mathbb{Q}_p$.

The second element of the correctness proof concerns the choice of $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$ in $\mathbb{F}_p$. In particular, we argue that the correctness of the algorithm does not rely, for $i = 1, \ldots, k$, on a specific choice of $\overline{\alpha}_i$ among the d_i roots of $x^{d_i} - a_i$ in $\mathbb{F}_p$. This argument is based on the fact that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set

$$\{(\alpha_1, \ldots, \alpha_k) \in K^k : \alpha_1^{d_1} = a_1 \wedge \cdots \wedge \alpha_k^{d_k} = a_k\}$$

That is, for any two k-tuples τ_1 and τ_2 in the set above, there exists an automorphism g in $\mathrm{Gal}(K/\mathbb{Q})$ such that $g(\tau_1) = \tau_2$. We will call this property joint transitivity; see Lemma 2.

Now for every prime ideal factor $\mathfrak{p}$ of pO_K there is a surjective homomorphism $\varphi : O_K \to \mathbb{F}_p$ with kernel $\mathfrak{p}$. For each choice of $\mathfrak{p}$ and for all $i = 1, \ldots, k$, the corresponding homomorphism φ maps α_i to some root $\overline{\alpha}_i$ of $x^{d_i} - a_i$ in $\mathbb{F}_p$. Conversely, using joint transitivity, we are able to show that every mapping $\alpha_1 \mapsto \overline{\alpha}_1, \ldots, \alpha_k \mapsto \overline{\alpha}_k$ where, for $i = 1, \ldots, k$, the $\overline{\alpha}_i$ is an arbitrary root of $x^{d_i} - a_i$ in $\mathbb{F}_p$, arises from the quotient map by some prime ideal factor of p. We conclude that the value $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k)$ in Item 2 is the image of $f(\alpha_1, \ldots, \alpha_k)$ under the quotient map $O_K \to O_K/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$.

It follows from the line immediately above that the algorithm has no false positives: if $f(\alpha_1, \ldots, \alpha_k) = 0$ in K then certainly $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$. We moreover show that for a suitable choice of prime p, namely such that p does not divide the norm of $f(\alpha_1, \ldots, \alpha_k)$ over $K/\mathbb{Q}$, the converse holds: if $f(\alpha_1, \ldots, \alpha_k) \neq 0$ in K then $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) \neq 0$ in $\mathbb{F}_p$. For more details, see Lemma 3.

A quantitative version of the Chebotarev density theorem guarantees we can find such a prime of polynomial bit size that splits. Informally speaking, Chebotarev's density theorem states that the set of rational primes p that split completely in O_K has density $\frac{1}{|\mathrm{Gal}(K/\mathbb{Q})|}$. The original statement of the theorem [48] is asymptotic, whereas for our algorithm we use its quantitative version in order to obtain a bound on the number of primes p of size polynomial in the bit length of the input such that pO_K completely splits, which requires GRH [38, 47]. We use the bound in combination with a bound on the norm of $f(\alpha_1, \ldots, \alpha_k)$ to ensure we can find at least one small prime that will not divide the norm and ensure our computation is sound.

Radical Identity Testing	
Input:	Algebraic circuit C of size at most s with input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, where $k \leq s$, the bit-length of the d_i and a_i is at most s, and the a_i are mutually coprime.
Output:	Whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ for the polynomial $f(x_1, \ldots, x_k)$ computed by C.
Line 1:	Guess a prime $p \leq 2^{4s^3}$ and $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ such that $p \equiv 1 \pmod{d}$ and $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$.
Line 2:	Output 'Zero' if $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$, where $\overline{f}$ is the reduction of f modulo p; and 'Non-zero' otherwise.

Figure 2: Our coNP algorithm for the RIT problem.

A coRP procedure for 2-RIT: We improve the obtained coNP bound for RIT in the case of 2-RIT, wherein all input radicals are square roots and all radicands a_i are rational primes (written in binary). We show that 2-RIT is in coRP under GRH, and that it is in coNP unconditionally. Our coRP algorithm chooses a suitable random prime to be used in the symbolic computation. As discussed above, the natural density of such suitable primes is $\frac{1}{|\operatorname{Gal}(K/\mathbb{Q})|}$, which is not sufficient even for 2-RIT. However, we show that there is an arithmetic progression with a good density of primes, and that all primes in this progression are suitable. To obtain this result, we rely on the law of quadratic reciprocity, as well as Dirichlet's theorem on the density of primes in arithmetic progressions.

We recall that a suitable prime p for our symbolic algorithm is such that the minimal polynomials of all input radicals split into linear factors over $\mathbb{F}_p$. In the setting of 2-RIT, the minimal polynomials of the inputs are in the form $x^2 - q_i$ where q_i is a rational prime. The above requires that the equations $x^2 \equiv q_i$ have solutions in $\mathbb{F}_p$, that is, q_i is a quadratic residue modulo p. But then by the law of quadratic reciprocity, p is a quadratic residue modulo prime q_i if and only if q_i is a quadratic residue modulo p, condition to $p \equiv 1 \pmod 4$. Roughly speaking, the latter holds if $p \equiv 1 \pmod{4q_i}$ (as 1 is a perfect square in $\mathbb{F}_p$).

By the Chinese remainder theorem and a more detailed argument similar to the above, we show that there is an arithmetic progression $A\mathbb{N} + b$ such that for all primes p in the progression, all polynomials $x^2 - q_i$, with $i \in \{1, \cdots, k\}$, split into linear factors over $\mathbb{F}_p$. We further impose another condition on A and b, based on Pocklington's algorithm, such that a root of each $x^2 - q_i$ can be computed in deterministic polynomial time in the length of the problem instance.

Finally, we use estimates on the density of primes in an arithmetic progression, see Theorem 3, to obtain the following result:

Theorem 2. *The 2-RIT problem is in* coRP *assuming GRH and in* coNP *unconditionally.*

3 THE RIT ALGORITHM

In this section, we present a co-nondeterministic polynomial time algorithm for the RIT problem. As discussed in Section 2, the idea is to work in a finite field obtained by quotienting the ring of integers of the splitting field of the input radicals by a suitable prime ideal.

Below, we fix an instance of the RIT problem given by an algebraic circuit C, and input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ with respective minimal polynomials $x^{d_i} - a_i$, where the radicands a_i are pairwise coprime; this assumption is without loss of generality as discussed in appendix A. We denote by s the size of our fixed RIT instance; that is, the size of the circuit is bounded by s, $k \leq s$, and the magnitude of the a_i and d_i to be at most 2^s. We further denote by K the splitting field of $\prod_{i=1}^{k}(x^{d_i} - a_i)$, which can be generated by adjoining to $\mathbb{Q}$ the radicals $\sqrt[d_i]{a_i}$ and a primitive d-th root of unity ζ_d, with $d = \operatorname{lcm}(d_1, \ldots, d_k)$. We denote by O_K the ring of integers of K.

In our construction, we evaluate the polynomial given by an algebraic circuit in a finite field $\mathbb{F}_p$ for some rational prime p that splits completely in O_K, that is, such that $pO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are distinct prime ideals of O_K, and n is the degree of the number field K.

In general, given a number field L and a rational prime q with prime ideal $\mathfrak{q}$ dividing qO_L, we say that $\mathfrak{q}$ lies above q in O_L. The residue field $O_L/\mathfrak{q}$ is isomorphic to an extension of the finite field $\mathbb{F}_q$, and we have that $\mathfrak{q} \cap \mathbb{Z} = q\mathbb{Z}$. However, in our special case of a completely split prime p in O_K, all residue fields $O_K/\mathfrak{p}_i$ are isomorphic to $\mathbb{F}_p$. This is crucial, as it ensures that the values in our finite field computation really will all be in $\mathbb{F}_p$ and not in one of its finite extensions (see the discussion in Section 5).

The following proposition asserts that a prime p completely splits in K if the minimal polynomials $x^{d_i} - a_i$ of our input radicals and the d-th cyclotomic polynomial (the minimal polynomial of ζ_d) split into distinct linear factors in $\mathbb{F}_p$.

Proposition 1. *Given a monic polynomial $g \in \mathbb{Z}[x]$ and its splitting field L, a prime $q \in \mathbb{Z}$ splits completely in L if g splits into distinct linear factors in $\mathbb{F}_q$.*

Proof sketch. Denote by $L_{\mathfrak{q}}$ the finite field extension of $\mathbb{Q}_q$ obtained by adjoining the roots of g to $\mathbb{Q}_q$. Let $\mathfrak{q}$ be a prime ideal lying above q in L. Recall that the decomposition group of a prime ideal $\mathfrak{q} \subset L$ is defined as the set of all automorphisms of $\operatorname{Gal}(L/\mathbb{Q})$ that fix $\mathfrak{q}$, i.e. $D_{\mathfrak{q}} = \{\sigma \in \operatorname{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Furthermore, since the field L is Galois, the following isomorphism holds:

$$D_{\mathfrak{q}} \cong \operatorname{Gal}(L_{\mathfrak{q}}/\mathbb{Q}_q) \tag{1}$$

Now given that g splits into distinct linear factors in $\mathbb{F}_q$, by virtue of L being Galois, it follows that all roots of g in $\mathbb{F}_q$ are non-zero.

Hence we can use Hensel's lemma to construct the solutions of g in $\mathbb{Q}_q$, that is, g splits completely in $\mathbb{Q}_q$. This, in turn, implies that $L_{\mathfrak{q}} = \mathbb{Q}_q$, that is, $\mathrm{Gal}(L_{\mathfrak{q}}/\mathbb{Q}_q)$ is trivial and (1) asserts that the same holds for $D_{\mathfrak{q}}$. This entails that the only automorphism that fixes the prime ideal $\mathfrak{q}$ is the identity, whereas for all non-trivial $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, which permute the conjugates of our input radicals, they will map elements of $\mathfrak{q}$ to elements of $O_L/\mathfrak{q} \cong \mathbb{F}_q$, i.e., $\mathbb{F}_q$ will indeed contain all roots of g. □

Example 1. *Let us look at an example instance of the RIT problem asking whether the polynomial $f(x) = x^2 - 10$ vanishes at the radical input $\sqrt{5}$. The computation occurs in the field $L = \mathbb{Q}(\sqrt{5})$, with ring of integers $O_L = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. We can observe that 11 is a completely split prime and note that the principal ideal of O_L generated by 11 factors as $11O_L = (4+\sqrt{5})(4-\sqrt{5})$. Since 11 totally splits in O_L, we have $O_L/\mathfrak{q} \cong \mathbb{F}_{11}$ for the prime ideal $\mathfrak{q} = (4+\sqrt{5})$ lying above 11. The polynomial $x^2 - 5$ completely splits to $(x-4)(x+4)$ in $\mathbb{F}_{11}$, and subsequently we have that $\mathbb{Q}_{11}(\sqrt{5}) = \mathbb{Q}_{11}$. The rational prime 5, however, is an example of the primes that we want to avoid as $5O_L = (\sqrt{5})^2$. In particular, the polynomial $x^2 - 5$ is irreducible in $\mathbb{F}_5$, implying that $L_{\mathfrak{q}} = \mathbb{Q}_q(\sqrt{5})$ and $[L_{\mathfrak{q}} : \mathbb{Q}_q] = 2$. If we evaluate f on the input $\sqrt{5}$ in $\mathbb{F}_{11}$, we get a true negative, as the computed value will be $6 \in \mathbb{F}_{11}$, whereas evaluating the polynomial in $\mathbb{F}_5$ would give us a false positive.*

3.1 Proof of correctness

Given a polynomial $g \in \mathbb{Z}[x]$ that is irreducible over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of the splitting field L of g acts transitively on the roots of g [50, Proposition 22.3] . We show that a stronger notion of transitivity holds for our real radicals $\sqrt[d_i]{a_i}$:

Lemma 2. *The group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set of k-tuples*

$$\mathcal{S} := \left\{(\alpha_1, \ldots, \alpha_k) \in K^k \mid \alpha_1^{d_1} = a_1 \wedge \cdots \wedge \alpha_k^{d_k} = a_k\right\}$$

Proof. Recall that $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ are real radicals with respective minimal polynomials $x^{d_i} - a_i$ and a_i mutually coprime.

Let $L_i := \mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_i]{a_i})$ for $i \in \{1, \ldots, k\}$. By virtue of the a_i being coprime and [12, Lemma 4.6], the polynomial $f_i := x^{d_i} - a_i$ stays irreducible over L_{i-1}, and thus is the minimal polynomial of $\sqrt[d_i]{a_i}$ over this field.

The proof follows by repeated use of the Isomorphism extension theorem, cf. [50, Theorem 5.12]. Note that L_i is a simple extension of L_{i-1} with $L_i = L_{i-1}(\alpha_i)$ where α_i is a solution of f_i. Denote by ψ_{i-1} an embedding of L_{i-1} into K. If α_i' is a root of $\psi_{i-1}(f_i)$ then there is a unique extension of ψ_{i-1} to a homomorphism $\psi_i : L_i \to K$ such that $\psi_i(\alpha_i) = \alpha_i'$. Applying the above inductively, we obtain a homomorphism $\psi_k : \mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \to K$, which by the Isomorphism extension theorem can again be extended to an automorphism of K acting jointly transitively on $\mathcal{S}$.

□

We now show that for an instance of the RIT problem, that is, an algebraic circuit with underlying polynomial f, and radical input with pairwise coprime radicands, the finite field computation is sound. 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.

Lemma 3. *Let p be a prime that completely splits in O_K, and let $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ be roots of the polynomials $x^{d_1} - a_1, \ldots, x^{d_k} - a_k$, respectively. Then for all $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, we have*

(1) if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ then $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$, and

(2) if $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$ then $p \mid N_{K/\mathbb{Q}}(f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}))$.

Proof. Recall that the radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ are such that their respective minimal polynomials are $x^{d_1} - a_1, \ldots, x^{d_k} - a_k$.

Consider a prime-ideal factor $\mathfrak{p}$ of pO_K. The quotient homomorphism $O_K \to \mathbb{F}_p$ with kernel $\mathfrak{p}$ maps the d_i distinct roots of each polynomial $x^{d_i} - a_i$ in O_K bijectively onto the roots of the same polynomial in $\mathbb{F}_p$. Then, by joint transitivity of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, established in Lemma 2, there is a homomorphism $\varphi : O_K \to \mathbb{F}_p$ such that $\varphi(\sqrt[d_i]{a_i}) = \overline{\alpha}_i$ for all $i \in \{1, \ldots, k\}$.

Item 1 follows from the fact that if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ then $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = \varphi(f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k})) = 0$. For Item 2, note that the kernel of φ is a prime ideal of O_K lying above p. Thus if $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$ then $p \mid N_{L/\mathbb{Q}}(f(\alpha_1, \ldots, \alpha_k))$. □

We have just shown that given an instance of the RIT problem, the computation can be taken to a finite field $\mathbb{F}_p$ for some rational prime p. In the following section, we discuss how to choose an appropriate prime p that satisfies the two conditions given in Lemma 3.

Lemma 2 plays an important role in the construction of our algorithm, and furthermore is one of the properties of the input to the RIT problem that makes our technique difficult to generalise to more general identity testing problems. In particular, joint transitivity ensures that in Lemma 3(1), no matter which representative of the $\sqrt[d_i]{a_i}$ we choose in $\mathbb{F}_p$, that is, no matter which solution of the equation $x^{d_i} - a_i$ we guess in $\mathbb{F}_p$, the computation remains sound. If we were, for instance, to generalise our identity testing problem to allow radical and cyclotomic inputs, joint transitivity may not hold anymore.

Example 2. *Consider the polynomial $f(x_1, x_2) = x_2^2 - x_1x_2 + 1$ with input $x_1 = \sqrt{2}$ and a primitive 8-th root of unity $x_2 = \zeta_8$. Note that the polynomial f vanishes at these values. The number field of the computation is $\mathbb{Q}(\sqrt{2}, \zeta_8)$, and we can choose the completely split prime 17 for our finite field computation. Indeed, the minimal polynomials of our input split as $x^2 - 2 = (x-6)(x+6)$ and $x^4 + 1 = (x+2)(x-2)(x+8)(x-8)$ in $\mathbb{F}_{17}$. However, since the Galois group of the field $\mathbb{Q}(\sqrt{2}, \zeta_8)$ does not act jointly-transitively on the input, we cannot choose the representatives of our two input numbers in $\mathbb{F}_{17}$ arbitrarily. In particular, by choosing 6 for $\sqrt{2}$ and 2 for ζ_8, and evaluating f in $\mathbb{F}_{17}$, the result would be 10, a clear false negative. This is due to the fact that the minimal polynomial $\Phi_8(x) = x^4 + 1$ of ζ_8 reduces in $\mathbb{Q}(\sqrt{2})$, hence, as soon as we choose 6 as a representative for $\sqrt{2}$, we cannot choose the representative for ζ_8 freely. In fact, if we replace x_1 by $\sqrt{2}$ and x_2 by x in the polynomial f, we obtain $(x^2 - \sqrt{2}x + 1)$, which is a factor of $\Phi_8(x)$ in $\mathbb{Q}(\sqrt{2})$. Indeed, $\Phi_8(x)$ factors as $(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ in $\mathbb{Q}(\sqrt{2})$, hence, as soon as we choose 6 as a representative for $\sqrt{2}$, we can only choose the roots of $(x^2 - 6x + 1)$ as representatives for ζ_8, whereas 2 is a root of the polynomial $(x^2 + 6x + 1)$ in $\mathbb{F}_{17}$.*

We note here that the underlying approach (working modulo prime ideals) is the same as in [7] and preceding works on versions of ACIT. However, as shown in Example 2, the transitivity condition given in Lemma 2 is crucial in our approach, whereas it has no equivalent in [7]. Furthermore, we have to allow for the fact that the ring of integers of the number field is no longer monogenic in the present case (e.g., Lemma 3 is analogous to Theorem 8 in [7], but the proof requires working in a certain order in the ring of integers). In relation to this, Example 2 explains some of the difficulties arising from attempting a common generalisation of [7] and the present paper.

3.2 Choice of the prime p

Let us call the primes p that completely split in O_K *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. Any missing proofs of the lemmas we use in this subsection can be found in Appendix C.

Given a rational prime p, we would like to ensure that $p \nmid N(\alpha)$, where α is the algebraic integer computed by a circuit. Observe that an integer of magnitude at most s has at most $\log s$ prime divisors, thus the norm $N(\alpha)$ has at most $\log |N(\alpha)|$ prime 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.

Recall that the norm of an algebraic number α in a Galois field can be computed as the product of its Galois conjugates. Thus, in order to bound the magnitude of the norm of our computed number, we need a bound on the magnitude of the conjugates of α, as well as the size of the Galois group, that is, the number of conjugates of α. The latter can be obtained using a bound on the degree of the number field K itself. Recall that the splitting field K of $\prod_{i=1}^{k}(x^{d_i} - a_i)$ is $\mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}, \zeta_d)$. Since the d_i are of magnitude at most 2^s, it follows that d is of magnitude at most 2^{s^2}, and the degree of K will be at most 2^{2s^2}. Using this bound, we show:

Lemma 4 (Bound on the norm). *Denote by $\alpha \in O_K$ the algebraic integer computed by C evaluated on the $\sqrt[d_i]{a_i}$. We have*

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

for $s \geq 4$.

In the context of our algorithm, this means that if we find $2^{s^3} + 1$ 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 be able to find enough good primes of polynomial bit-length in the size of the input to complete our reasoning.

To this aim, we use a quantitative version of the Chebotarev density theorem. Intuitively speaking, given a Galois extension L of $\mathbb{Q}$, the theorem gives a bound on the number of primes splitting in a certain pattern in O_L. The different classes of splitting patterns correspond to conjugacy classes of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of L. As it turns out, the primes splitting completely in L correspond to the conjugacy class $\{id\}$ containing solely the identity element id of $\mathrm{Gal}(L/\mathbb{Q})$. The asymptotic version of the theorem then asserts that the set of completely split primes has density $\frac{1}{|\mathrm{Gal}(L/\mathbb{Q})|}$. Denoting by $\pi(x)$ the number of all rational primes less or equal to x, and by $\pi_1(x)$ the number of completely split primes, the quantitative version of the theorem is as follows [38, 47]:

Proposition 5 (Bound on $\pi_1(x)$). *Assuming GRH,*

$$\pi_1(x) \geq \frac{1}{|\mathrm{Gal}(K/\mathbb{Q})|}\left[\pi(x) - \log \Delta_K - cx^{1/2}\log(\Delta_K x^{|\mathrm{Gal}(K/\mathbb{Q})|})\right]$$

where c is an effective constant.

To apply the above proposition we will need a bound on the discriminant Δ_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 O_L of a number field L, we compute the discriminant Δ_L as the determinant of the matrix $\mathrm{tr}(\alpha_i\alpha_j)$ for all $i, j = 1, \ldots, n$. However, in the case of a radical field extension L, computing a basis for its ring of integers O_L is a non-trivial task. In order to avoid this computation, we try to bound the discriminant using the discriminant of an order of our ring of integers O_K. Recall that an order O in a number field L is a free $\mathbb{Z}$-submodule of O_L of rank $[L : \mathbb{Q}]$. Looking again at the number field $L = \mathbb{Q}(\sqrt{5})$ with ring of integers $O_L = \mathbb{Z}[\frac{\sqrt{5}+1}{2}]$, note that $\mathbb{Z}[\sqrt{5}] \subset O_L$; in particular, $\mathbb{Z}[\sqrt{5}]$ is an order of index 2 in O_L. The following (see, e.g., [18, Proposition 4.4.4]) holds:

Proposition 6. *Suppose O is an order in O_L. Then*

$$\mathrm{Disc}(O) = \mathrm{Disc}(O_L) \cdot [O_L : O]^2$$

We construct an order O of O_K, the discriminant of which we can compute using a standard result in algebraic number theory. The Primitive element theorem states that any number field L can be generated by adjoining a single element θ, called the primitive element, to $\mathbb{Q}$, i.e., $L = \mathbb{Q}(\theta)$. Then the subring $\mathbb{Z}[\theta]$ of O_L is an order of O_L. Furthermore, the discriminant $\mathrm{Disc}(\mathbb{Z}[\theta])$ is equal to the discriminant of the minimal polynomial of θ. It is a well-known fact that the discriminant of a polynomial can be computed as the product of the differences of the roots.

We thus start with preliminary result regarding primitive elements of the number field K.

Lemma 7 (Bound on the primitive element). *The field K has a primitive element θ, computed as the linear combination*

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

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

Henceforth, we fix a primitive element θ for our number field K, computed as in Lemma 7. Now Proposition 6 suggests that $\Delta_K \leq \Delta_{f_\theta}$, where $\Delta_{f_\theta} = \mathrm{Disc}(\mathbb{Z}[\theta])$, which we bound as follows:

Lemma 8 (Bound on the discriminant). *We have*

$$|\mathrm{Disc}(\mathbb{Z}[\theta])| \leq 2^{2^{5s^2}}$$

for $s \geq 4$.

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 $\pi_1(x) \geq 2^{s^3} + 1$. Using the bound above, we claim that this is the case for $x \geq 2^{4s^3}$:

Lemma 9. *Assuming GRH,*

$$\pi_1(2^{4s^3}) \geq 2^{s^3} + 1.$$

3.3 Proof of Theorem 1

Proof of Theorem 1. Figure 2 presents a co-nondeterministic polynomial time algorithm for the RIT problem as follows.

Given input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, denote by K the splitting field of $\prod_{i=1}^{k}(x^{d_i} - a_i)$. Further denote by θ a primitive element of K, computed as in Lemma 7.

Let us first argue that the algorithm runs in polynomial time. In Step 1, after guessing candidates for p such that $p \equiv 1 \pmod{d}$ and $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$, verifying whether $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$ can be done in polynomial time by the repeated-squaring method. It is clear that Step 2 can be done in polynomial time.

Now let us show that the RIT problem is in coNP. First suppose $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \neq 0$. Under GRH, the lower bound in Lemma 9 shows that $\pi_1(2^{4s^3}) \geq 2^{s^3} + 1$. It follows that there exists a prime $p \leq 2^{4s^3}$ such that

- $p \nmid N(f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}))$, and
- p splits completely in K.

The polynomial certificate of non-zeroness of $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k})$ then comprises, the prime p above, as well as the list of integers $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ such that $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$. Following Lemma 3, we then have that $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) \neq 0$.

On the other hand, as we have noted above, for any prime p and the representation $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$ of radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ in $\mathbb{F}_p$, if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$, then $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$, as shown in Lemma 3, which concludes the proof. □

4 THE 2-RIT ALGORITHM

Our algorithm for RIT uses non-determinism to guess a "good" prime. It is natural to wonder whether such primes can instead be randomly sampled. 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 $\frac{1}{|\operatorname{Gal}(K/\mathbb{Q})|}$. Since the size of the Galois group of K over $\mathbb{Q}$ 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 the 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 problem for an algebraic circuit C evaluated on square-roots $\sqrt{a_1}, \ldots, \sqrt{a_k}$ for k rational primes $a_1, \ldots, a_k$. The proofs from Section 3.1 ensure that the finite field computation in our algorithm is sound; it remains to show how to choose a completely split 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.

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 [37, Chapter 20, page 125] and [28, Corollary 18.8], respectively:

Theorem 3. *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 $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ of the square-root input $\sqrt{a_1}, \ldots, \sqrt{a_k}$. As it turns out, this only requires some classical results on quadratic reciprocity, 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

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a non-quadratic residue mod } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

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 $p \in 4\mathbb{N} + 1$, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1 \quad \Leftrightarrow \quad \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \pm 1.$$

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 $q \equiv 1 \pmod{4}$.

In what follows, we apply the law of quadratic reciprocity in order to choose the right field $\mathbb{F}_p$ for deciding 2-RIT. Recall that intuitively, we are looking for a prime p such that $x^2 - a_i$ has a solution in $\mathbb{F}_p$ 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 $4\mathbb{N} + 1$, 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 polynomials $x^2 - a_i$ all split

Radical Identity Testing for square root inputs	
Input:	Algebraic circuit C of size at most s and a list of $k \leq s$ primes $a_1, \ldots, a_k$ of magnitude at most 2^s.
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 (5)
Step 3:	Compute $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$ such that $\overline{\alpha}_i^2 \equiv a_i \pmod p$ as described in Equation (2).
Step 4:	Output 'Zero' if $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$, where $\bar{f}$ is the reduction of f modulo p; and 'Non-zero' otherwise.

Figure 3: Our algorithm for the 2-RIT problem, which runs in randomised polynomial time (coRP).

and have non-zero roots in $\mathbb{F}_p$. Following Pocklington's algorithm, there is a deterministic way to solve the equations $x^2 - a_i$ if $p \equiv 5 \pmod 8$. In particular, writing $p = 8m + 5$, the solution of the equation $x^2 \equiv a \pmod p$ is given by the following function:

$$x = \begin{cases} \pm a^{m+1} & \text{if } a^{2m+1} \equiv 1 \pmod p, \\ \pm \frac{y}{2} & \text{if } a^{2m+1} \equiv -1 \pmod p \text{ and} \\ & y = \pm(4a)^{m+1} \text{ is even}, \\ \pm \frac{p+y}{2} & \text{if } a^{2m+1} \equiv -1 \pmod p \text{ and} \\ & y = \pm(4a)^{m+1} \text{ is odd}. \end{cases} \tag{2}$$

See Appendix D.1 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 $A = \prod_{i=1, a_i \neq 2}^{k} a_i$ 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

$$8A\mathbb{N} + b + 1, \tag{3}$$

where b is a solution of the following system of equations

$$\begin{aligned} b &\equiv 4 \pmod 8 \\ b &\equiv 0 \pmod{a_i} \text{ for all } a_i \neq 2. \end{aligned} \tag{4}$$

Since all the modulos in the equations (4) are pairwise coprime, by the Chinese remainder theorem, the system has a solution. By the construction above, 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 $x^2 - 2$ has a solution in $\mathbb{F}_p$. We also ensure that p is such that we can deterministically find the representations $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$ of $\sqrt{a_1}, \ldots, \sqrt{a_k}$ in $\mathbb{F}_p$. Define by $S(a_1, \ldots, a_k)$ the following set

$$\Big\{p \leq 2^{5k^3} \mid p \in 8A\mathbb{N} + b + 1 \text{ where } A = \prod_{i=1, a_i \neq 2}^{k} a_i \text{ and } b \text{ is a solution of (4)}\Big\}. \tag{5}$$

We claim the following:

Proposition 10. *Let C be an algebraic circuit of size at most s, and $a_1, \ldots, a_k$ primes of bit-length at most s, where $k \leq s$. Denote by α 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 (5). Then*

(i) p is prime with probability at least $\frac{1}{6s^3}$ assuming GRH, and
(ii) given that p is prime, the probability that it divides $N(\alpha)$ is at most 2^{-s^3} unconditionally.

With Proposition 10 in hand, we can state our coRP algorithm, see Figure 3, and prove its complexity.

Proof of Theorem 2. Figure 3 presents a coRP (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 Lemma 3, we have $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$, 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 10(ii), the probability that p does not divide $N(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$ is at least $1 - 2^{-s^3}$. Thus, the probability that the algorithm gives the wrong output is at mos 2^{-s^3}.

It remains to show that the 2-RIT problem is in coNP unconditionally. The idea is to modify the algorithm in Figure 3, replacing randomisation with guessing. Theorem 3 shows that $\pi_{8A,b+1}(2^{3s^3}) > 2^{s^3}$ for s sufficiently large. It follows that there exists a prime $p \leq 2^{3s^3}$ 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 1. □

Note that, in general, in the proof of the theorem above, GRH is required to obtain the coRP bound. This is because the unconditional lower bound on density of primes in arithmetic progressions is not strong enough for our purposes: The number of primes less than 2^{3s^3} which are favourable is just 2^{s^3}. This gives a probability of success at least 2^{-2s^3}, which is exponentially small in the instance size. In order to get a constant success probability, we have to repeatedly sample and run this algorithm 2^{2s^3} times, which yields an exponential time algorithm. However, under GRH, the bound is improved to $\frac{1}{6s^3}$ and polynomially many repetitions suffice for a constant success probability.

5 DISCUSSION

In this work, we have shown that the RIT problem is in coNP under GRH. We also provided a randomised polynomial time algorithm for the 2-RIT problem assuming GRH , and showed this problem in coNP unconditionally. Our algorithms work by reducing the polynomials modulo a "small" 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 presents problems for an approach via numerical approximation. We note though the latter approach has been shown to work for deciding the Bounded-RIT problem when the exponents d_i of the radical input $\sqrt[d_i]{a_i}$ are unary. In particular, [12] 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. 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 in Step 1 and 2 of the algorithm in [12], when trying to compute the minimal d_{ij} such that $\sqrt[d_i]{m_j}^{d_{ij}} \in \mathbb{Z}$). Recall our reduction of RIT to its variant where the minimal polynomials of the input radicals $\sqrt[d_i]{a_i}$ are $x^{d_i} - a_i$ and all radicands a_i are pairwise coprime numbers, presented in appendix A. Applying this reduction first would avoid the above-mentioned increase in complexity for the Bounded-RIT problem with binary exponents. It thus places the general version of the Bounded-RIT problem in coRP.

Working in extensions of finite fields. Our approach to RIT involves finding a prime p for which the required radicals exist in $\mathbb{F}_p$. Here it is tempting to consider working instead in a finite extension of $\mathbb{F}_p$. For example, it is well-known that every irreducible polynomial over $\mathbb{F}_p$ of degree d splits completely over $\mathbb{F}_{p^d}$. For solving RIT, a major problem with this approach is that if d is given in binary then representing an element of the field $\mathbb{F}_{p^d}$ requires space exponential in the bit length of d. Specialising to 2-RIT, we have that the required square roots all exist in $\mathbb{F}_{p^2}$, for any p. But working in $\mathbb{F}_{p^2}$ is only sound if the latter is a quotient of the number field K generated by the square roots, that is, if p has inertial degree 2 over K. Moreover, the asymptotic density of such primes is the same as for those that split over K.

REFERENCES

[1] M. Agrawal and S. Biswas. 2003. Primality and identity testing via chinese remaindering. *Journal of the ACM (JACM)* 50, 4 (2003), 429–443.

[2] M. Agrawal, N. Kayal, and N. Saxena. 2004. PRIMES is in P. *Annals of mathematics* (2004), 781–793.

[3] S. Akshay, N. Balaji, A. Murhekar, R. Varma, and N. Vyas. 2020. Near-Optimal Complexity Bounds for Fragments of the Skolem Problem. In *37th International Symposium on Theoretical Aspects of Computer Science (STACS 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

[4] E. Allender, P. Bürgisser, J. Kjeldgaard-Pedersen, and P. B. Miltersen. 2006. On the complexity of numerical analysis. In *CCC '06*. 331–339.

[5] V. Arvind and P. P. Kurur. 2003. Upper Bounds on the Complexity of Some Galois Theory Problems. In *Algorithms and Computation, 14th International Symposium, ISAAC 2003, Kyoto, Japan, December 15-17, 2003, Proceedings (Lecture Notes in Computer Science, Vol. 2906)*. Springer, 716–725.

[6] E. Bach, J. Driscoll, and J. Shallit. 1993. Factor Refinement. *Journal of Algorithms* 15, 2 (1993), 199–222.

[7] N. Balaji, S. Perifel, M. Shirmohammadi, and J. Worrell. 2021. Cyclotomic Identity Testing and Applications. In *ISSAC '21: International Symposium on Symbolic and Algebraic Computation, Virtual Event, Russia, July 18-23, 2021*. ACM, 35–42.

[8] M. Benedikt, R. Lenhardt, and J. Worrell. 2013. LTL model checking of interval Markov chains. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 32–46.

[9] P. Berman, M. Karpinski, L. Larmore, W. Plandowski, and W. Rytter. 2002. On the complexity of pattern matching for highly compressed two-dimensional texts. *J. Comput. System Sci.* 65, 2 (2002), 332–350.

[10] J. Blömer. 1992. How to Denest Ramanujan's Nested Radicals. In *33rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, 447–456.

[11] J. Blömer. 1997. Denesting by Bounded Degree Radicals. In *Algorithms - ESA '97, 5th Annual European Symposium, Proceedings (Lecture Notes in Computer Science, Vol. 1284)*, R. E. Burkard and G. J. Woeginger (Eds.). Springer, 53–63.

[12] J. Blömer. 1998. A Probabilistic Zero-Test for Expressions Involving Roots of Rational Numbers. In *Algorithms — ESA' 98*. 151–162.

[13] R. P. Brent. 2016. *Fast multiple-precision evaluation of elementary functions*. Springer International Publishing, 9–20.

[14] J. Canny. 1988. Some algebraic and geometric computations in PSPACE. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*. 460–467.

[15] K. Chatterjee and R. Ibsen-Jensen. 2014. The complexity of ergodic mean-payoff games. In *International Colloquium on Automata, Languages, and Programming*. Springer, 122–133.

[16] Z. Chen and M. Kao. 2000. Reducing randomness via irrational numbers. *SIAM J. Comput.* 29, 4 (2000), 1247–1256.

[17] V. Chonev, J. Ouaknine, and J. Worrell. 2016. On the complexity of the orbit problem. *Journal of the ACM (JACM)* 63, 3 (2016), 1–18.

[18] H. Cohen. 2013. *A Course in Computational Algebraic Number Theory*. Springer Berlin Heidelberg.

[19] Max Dehn. 1912. Transformation der Kurven auf zweiseitigen Flächen. *Math. Ann.* 72, 3 (1912), 413–421.

[20] E. D. Demaine, J. S. B. Mitchell, and J. O'Rourke. 2006. The open problems project: Problem 33.

[21] R. A. Demillo and R. J. Lipton. 1978. A probabilistic remark on algebraic program testing. *Inform. Process. Lett.* 7, 4 (1978), 193–195.

[22] J. Esparza, S. Kiefer, and M. Luttenberger. 2008. Solving monotone polynomial equations. In *Fifth Ifip International Conference On Theoretical Computer Science–Tcs 2008*. Springer, 285–298.

[23] K. Etessami and M. Yannakakis. 2010. On the Complexity of Nash Equilibria and Other Fixed Points. *SIAM J. Comput.* 39, 6 (2010), 2531–2597.

[24] M. R. Garey, R. L. Graham, and D. S. Johnson. 1976. Some NP-complete geometric problems. In *Proceedings of the eighth annual ACM symposium on Theory of computing*. ACM, 10–22.

[25] F. Gouvea. 2003. *p-adic Numbers: An Introduction*. Springer Berlin Heidelberg.

[26] C. Haase and S. Kiefer. 2015. The odds of staying on budget. In *International Colloquium on Automata, Languages, and Programming*. Springer, 234–246.

[27] C. Haase, S. Kiefer, and M. Lohrey. 2017. Counting problems for Parikh images. In *Leibniz International Proceedings in Informatics, LIPIcs*, Vol. 83. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 12.

[28] H. Iwaniec and E. Kowalski. 2004. *Analytic number theory*. Vol. 53. AMS.

[29] E. Kaltofen. 1989. Factorization of Polynomials Given by Straight-Line Programs. *Adv. Comput. Res.* 5 (1989), 375–412.

[30] N. Kayal and C. Saha. 2012. On the sum of square roots of polynomials and related problems. *ACM Transactions on Computation Theory (TOCT)* 4, 4 (2012), 1–15.

[31] S. Kiefer, I. Marusic, and J. Worrell. 2015. Minimisation of Multiplicity Tree Automata. *Foundations of Software Science and Computation Structures LNCS 9034* (2015), 297.

[32] S. Kiefer, A. Murawski, J. Ouaknine, B. Wachter, and J. Worrell. 2013. On the Complexity of Equivalence and Minimisation for Q-weighted Automata. *Logical Methods in Computer Science* 9 (2013).

[33] S. Kiefer and D. Wojtczak. 2011. On probabilistic parallel programs with process creation and synchronisation. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 296–310.

[34] P. Koiran. 1996. Hilbert's Nullstellensatz Is in the Polynomial Hierarchy. *Journal of Complexity* 12, 4 (1996), 273–286.

[35] D. König and M. Lohrey. 2018. Parallel identity testing for skew circuits with big powers and applications. *Int. J. Algebra Comput.* 28, 6 (2018), 979–1004.

[36] P. P. Kurur. 2006. *Complexity Upper Bounds using Permutation Group theory*. Ph. D. Dissertation. University of Madras, Chennai. https://piyush-kurur.github.io/research/publication/Thesis/2006-01-13-Thesis.pdf

[37] H. Davenport H. L. and Montgomery. 2013. *Multiplicative Number Theory*. Springer New York.

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

[39] S. Landau. 1984. Polynomial Time Algorithms for Galois Groups. In *EUROSAM 84, International Symposium on Symbolic and Algebraic Computation, Cambridge, England, UK, July 9-11, 1984, Proceedings (Lecture Notes in Computer Science, Vol. 174)*, J. P. Fitch (Ed.). Springer, 225–236.

[40] A. Lechner, J. Ouaknine, and J. Worrell. 2015. On the complexity of linear arithmetic with divisibility. In *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*. IEEE, 667–676.
[41] Markus Lohrey. 2014. *The compressed word problem for groups*. Springer.
[42] L. Lovász. 1979. On determinants, matchings, and random algorithms.. In *FCT*, Vol. 79. 565–574.
[43] J. S. Milne. 2021. Fields and Galois Theory. https://www.jmilne.org/math/CourseNotes/FT.pdf Lecture notes (version 5.0).
[44] D. Richardson. 1992. The elementary constant problem. In *Papers from the international symposium on Symbolic and algebraic computation*. 108–116.
[45] D. Richardson. 1997. How to recognize zero. *Journal of Symbolic Computation* 24, 6 (1997), 627–645.
[46] S. and G. L. Miller. 1983. Solvability by Radicals is in Polynomial Time. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*. ACM, 140–151.
[47] Jean-Pierre Serre. 1981. Quelques applications du théoreme de densité de Chebotarev. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 54, 1 (1981), 123–201.
[48] P. Stevenhagen, H. W. Lenstra, and Jr. 1995. Chebotarev and his density theorem.
[49] I. Stewart and D. Tall. 2001. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition*. Taylor & Francis.
[50] I. N. Stewart. 1973. *Galois theory*. Chapman and Hall.
[51] M. Ummels and D. Wojtczak. 2011. The complexity of Nash equilibria in limit-average games. In *International Conference on Concurrency Theory*. Springer, 482–496.

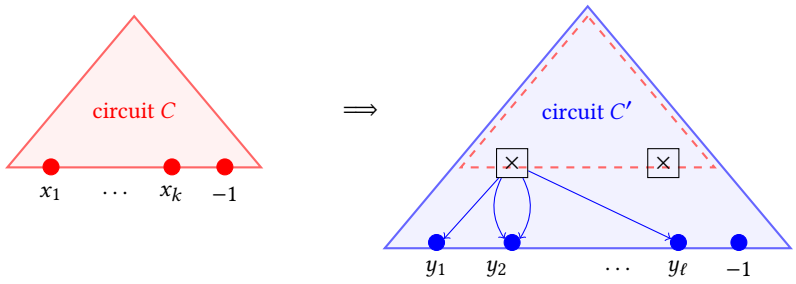

Figure 4: The scheme of the reduction from the RIT problem to its variant where the input radicands are pairwise coprime and the exponents are all equal. In this simple example, a_1 is factored to $m_1 m_2^2 m_\ell$.

A REDUCTION TO THE RIT PROBLEM WITH COPRIME RADICANDS

Given a set of integers $a_1, \ldots, a_k$, the *factor-refinement* algorithm [6] computes a set $\{m_1, \ldots, m_\ell\}$ of (not necessarily prime) factors m_j of the a_i's such that $gcd(m_j, m_k) = 1$ for all $1 \le j < k \le \ell$, and each a_i can be written as a product of these factors, i.e., $a_i = \prod_{j=1}^{l} m_j^{e_{ij}}$ with the $e_{ij} \in \mathbb{N}$. If we denote by $a = \mathrm{lcm}(a_1, \ldots, a_k)$, the factor-refinement algorithm runs in time $O(\log^2(a))$ (see also [12, Lemma 3.1]), and the number ℓ of factors is bounded by $\sum_{i=1}^{k} \log(|a_i|)$.

Reduction. Given an algebraic circuit C representing a k-variate polynomial $f(x_1, \ldots, x_k)$ together with k input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, we construct another algebraic circuit C' representing an ℓ-variate polynomial $f'(y_1, \ldots, y_\ell)$ and input radicals $\sqrt[t_1]{n_1}, \ldots, \sqrt[t_\ell]{n_\ell}$, with the n_j pairwise coprime and respective minimal polynomials $x^{t_j} - n_j$, such that $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ if and only if $f'(\sqrt[t_1]{n_1}, \ldots, \sqrt[t_\ell]{n_\ell}) = 0$.

We first compute the partial factorisation of each one of the a_i's by going through all primes up to $\log a$, which can clearly be done in $poly(\log a)$ time, where $a = \mathrm{lcm}(a_1, \ldots, a_k)$. We denote by $m_1, \ldots, m_r$, the primes p appearing in the factorisations of the a_i. We then apply the *factor-refinement* algorithm to the unfactored parts of the a_i's and compute a set of pairwise coprime factors $\{m_{r+1}, \ldots, m_\ell\}$ such that $a_i = \prod_{j=1}^{l} m_j^{e_{ij}}$. Then

$$f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0 \iff f\Big(\prod_{j=1}^{l} m_j^{\frac{e_{1j}}{d_1}}, \ldots, \prod_{j=1}^{l} m_j^{\frac{e_{kj}}{d_k}}\Big) = 0$$

To construct the new input radicals $\sqrt[t_i]{n_i}$ with respective minimal polynomials $x^{t_i} - n_i$, we compute for each $\sqrt[d_i]{m_j}$ the smallest d_{ij} such that $\sqrt[d_i]{m_j}^{d_{ij}} \in \mathbb{Z}$. Observe that in general $m_j = p_1^{f_{j1}} \ldots p_s^{f_{js}}$ with $p_1, \ldots, p_s$ rational primes, and we have

$$\sqrt[d_i]{m_j}^{d_{ij}} = \sqrt[d_i]{p_1^{f_{j1}} \cdots p_s^{f_{js}}}^{d_{ij}} = \left(p_1^{f_{j1}} \cdots p_s^{f_{js}}\right)^{\frac{d_{ij}}{d_i}}$$

which will be an integer if and only if $d_i \mid \gcd(f_{j1}, \ldots, f_{js}) \cdot d_{ij}$. Furthermore, observe that d_{ij} will be the smallest such power precisely when

$$d_i = \gcd(f_{j1}, \ldots, f_{js}) \cdot d_{ij}. \tag{6}$$

Now for the first r factors of the a_i's which are all prime, we have that $m_j = p$ for some rational prime p, and $d_{ij} = d_i$.

For $m_j, r < j \le l$, first note that all m_j's are products of powers of primes larger than $\log a$. Thus the multiplicities of the primes appearing in the decompositions $m_j = p_1^{f_{j1}} \ldots p_s^{f_{js}}$, that is, all f_j's, are small. In particular, $f_j < \log m_j$ for all j, and furthermore $\gcd(f_{j1}, \ldots, f_{js}) < \log m_j$. Keeping this observation in mind, we can now show how to compute the d_{ij} in time polynomial in $\log m_j$.

Following (6), we go trough the candidates for the $\gcd(f_{j1}, \ldots, f_{js})$, $g_{ij} = 1, \ldots, \log m_j - 1$, computing $f = \frac{d_i}{g_{ij}}$, the candidate for our d_{ij} (note that if $f \notin \mathbb{Z}$, we discard it and move on). We then approximate $\sqrt[d_i]{m_j}^{f} = m_j^{\frac{f}{d_i}} = m_j^{\frac{1}{g_{ij}}}$ with absolute error less than $1/2$ to obtain the unique integer m with $|\sqrt[g_{ij}]{m_j} - m| < 1/2$. This can be done by doing $\log m_j < \log a$ iterations of the Newton iteration [13, Lemma 3.1]. We conclude by checking whether $m^{d_i} = m_j^{f}$. This can be efficiently computed by writing $d_i = fg$ and observing that we are checking whether $(m^{g_{ij}})^{f} = m_j^{e}$, which simplifies to $m^{g_{ij}} = m_j$, with g_{ij} unary.

Finally, we construct the new input radicals by setting $n_j = m_j^{\frac{1}{\mathrm{lcm}(d_{1j} \cdots d_{kj})}}$ and $t_j = \frac{d_1 \cdots d_k}{\mathrm{lcm}(d_{1j} \cdots d_{kj})}$. We complete the reduction by constructing the algebraic circuit C' from C by replacing the leaves x_i, $i \in \{1, \ldots, k\}$, with a small circuit that computes $\prod_{j=1}^{l} y_j^{\frac{e_{ij} d_1 \cdots d_k}{d_i}}$; see Figure 4.

B EXTENDED PRELIMINARIES

B.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.

B.2 Algebraic number theory

A complex number α is *algebraic* if it is a root of a univariate polynomial with integer coefficients. The defining polynomial of α, denoted f_α, is the unique (up to multiplication by ± 1) integer polynomial of least degree, whose coefficients have no common factor, that has α as a root. The *degree* of an algebraic number α is the degree of its minimal polynomial f_α. If f_α is monic then we say that α 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, $O_{\mathbb{Q}(i)} := \mathbb{Z}[i]$.

An *order* O in a number field K is a free $\mathbb{Z}$-submodule of O_K of rank $[K : \mathbb{Q}]$. Since 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 O_K/O is a finite abelian group. The order of this quotient, denoted $[O_K : O]$, is called the *index* of O in O_K. It is known that $mO_K \subset O$ for $m = [O_K : O]$. For example, $\mathbb{Z}[2i] = \mathbb{Z} + \mathbb{Z}2i$ 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.*, ζ such that $\zeta^n = 1$. If ζ_n is an n-th root of unity and for each $k < n$, $\zeta^k \neq 1$, then we call it a *primitive n-th root of unity*. We can always choose a primitive n-th root of unity by setting $\zeta_n = e^{2i\pi\frac{k}{n}}$ 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 Φ_n is the minimal polynomial of a primitive n-th root of unity, and its roots are all n-th primitive roots of unity.

B.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 completely over K. In other words, if $\alpha \in K$, then all conjugates of α over L (i.e., all roots of the minimal polynomial of α 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 α 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 4 (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 α is a primitive element.*

Given a Galois extension K/L, the *Galois group* of K/L, denoted by $Gal(K/L)$ is the group of automorphisms of K that fix L. That is, the group of all isomorphisms $\sigma : K \to K$ 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 $K \to K$ that are the identity map on L.

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

The *norm* of α is defined by

$$N_{K/L}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/L)} \sigma(\alpha)$$

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:

$$\mathrm{Tr}_{K/L}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/L)} \sigma(\alpha)$$

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

The ring of integers of K, 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 Δ_K the *discriminant*, and define it by

$$\Delta_K = \det(\mathrm{Tr}_{K/L}(\alpha_i \alpha_j))_{1 \le i,j \le n}$$

Note that Δ_K is always a non-zero rational integer.

B.4 Ramification theory

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

$$\begin{array}{ccccc} \mathfrak{p} & \subset O_K & \subset & K \\ & | & & \\ p & \subset \mathbb{Z} & \subset & \mathbb{Q}. \end{array}$$

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

$$pO_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}. \tag{7}$$

Using the vocabulary introduced above, we can observe that the prime ideals $\mathfrak{p}_i$ are all above p. Note that in the ring of integers of a number field, all prime ideals are maximal, hence all $\mathfrak{p}_i$ are also maximal ideals of O_K. In general, given a commutative ring R and a maximal ideal $\mathfrak{m}$ of R, the *residue field* is the quotient $k = R/\mathfrak{m}$. Intuitively, k can be thought of as the field of possible remainders. Now, given a maximal ideal $\mathfrak{p}$ of O_K, $O_K/\mathfrak{p}$ 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 $O_K/\mathfrak{p}$, that is:

$$f_\mathfrak{p} = \dim_{\mathbb{F}_p}(O_K/\mathfrak{p}).$$

Looking at the factorisation (7), we can define the residue class degree of each one of the $\mathfrak{p}_i$'s as follows:

$$f_i = [O_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}].$$

We say that p is *ramified* if the *ramification index* $e_i > 1$ for some $\mathfrak{p}_i$. A prime p is said to be *totally ramified* if $e = n$, $g = 1$, and $f = 1$. That is $pO_K = \mathfrak{p}^e$ for some $\mathfrak{p}$. Conversely, p is *non-ramified* if $pO_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ where the $\mathfrak{p}_i$ are distinct. We further say that a prime $p \in \mathbb{Z}$ is *inert* if the ideal pO_K is prime, in which case we have $pO_K = \mathfrak{p}$, that is $g = 1$, $e = 1$, and $f = n$. Finally, a prime is said to be *split* if $e_1 = \ldots = e_g = 1$.

For the Gaussian integers, the ideals $2\mathbb{Z}[i]$ and $5\mathbb{Z}[i]$ are not prime ideals and have respective factorisations $2\mathbb{Z}[i] = \mathfrak{p}^2$ and $5\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p} = (1 + i)\mathbb{Z}[i]$, $\mathfrak{p}_1 = (2 + i)\mathbb{Z}[i]$, and $\mathfrak{p}_2 = (2 - i)\mathbb{Z}[i]$ are prime ideals. The prime 2 is the unique ramified prime in the Gaussian integers.

B.5 The p-adic field $\mathbb{Q}_p$

Here, we give a brief preliminary on the field of p-adic numbers $\mathbb{Q}_p$; for more details see, e.g., [25]. The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$, given by $|a/b|_p = p^{v_p(b) - v_p(a)}$ for $a, b \in \mathbb{Z} \setminus \{0\}$, where $v_p(x)$ denotes the order to which p divides $x \in \mathbb{Z}$. We denote by $\mathbb{Z}_p$ the valuation ring $\{x \in \mathbb{Q}_p : |x|_p \le 1\}$. This is the local ring with unique maximal ideal generated by p. A basic result about $\mathbb{Q}_p$ is Hensel's Lemma:

Lemma 11. *[Hensel's lemma] Given $f(X) \in \mathbb{Z}[X]$, if there exists $\alpha \in \mathbb{F}_p$ such that*

$$f(\alpha) = 0 \text{ and } f'(\alpha) \neq 0$$

then there exists $x \in \mathbb{Z}_p$ with $f(x) = 0$ and $x \equiv \alpha \bmod p$.

Given a number field $K/\mathbb{Q}$, let p be a rational prime and $\mathfrak{p}$ a prime ideal of O_K lying above p. Then the p-adic absolute value $|\cdot|_p$ corresponding to p extends uniquely to an absolute value $|\cdot|_\mathfrak{p}$ corresponding to $\mathfrak{p}$ such that the restriction of $|\cdot|_\mathfrak{p}$ to $\mathbb{Q}$ coincides with $|\cdot|_p$. This, in turn, corresponds to a field extension $K_\mathfrak{p}/\mathbb{Q}_p$. This extension can be analysed using the ramification of p in K. In particular, if p completely splits in K, then $[K_\mathfrak{p} : \mathbb{Q}_p] = 1$, that is, the extension is trivial and we have $K_\mathfrak{p} = \mathbb{Q}_p$. If p is inert, then the degree of the extension $K_\mathfrak{p}$ over $\mathbb{Q}_p$ is equal to the inertial degree of p in K. Finally, if p is totally ramified, then the degree of the extension $K_\mathfrak{p}$ over $\mathbb{Q}_p$ is equal to the degree of K over $\mathbb{Q}$, i.e., $[K_\mathfrak{p} : \mathbb{Q}_p] = [K : \mathbb{Q}]$.

Given a prime ideal $\mathfrak{p}$ of O_K, we define the decomposition group $D_\mathfrak{p}$ of to be the set of all automorphisms $\mathrm{Gal}(K/\mathbb{Q})$ fixing $\mathfrak{p}$, that is $D_\mathfrak{p} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$. If the field K is Galois over $\mathbb{Q}$, the following isomorphism holds:

$$D_\mathfrak{p} \cong \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p).$$

This entails that the prime p completely splits in K if and only if the decomposition group $D_\mathfrak{p}$ is trivial for all prime factors $\mathfrak{p}$ of p in O_K.

C MISSING PROOFS FROM SECTION 3

C.1 Bound on the norm

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

Lemma 4 (Bound on the norm). *Denote by $\alpha \in O_K$ the algebraic integer computed by C evaluated on the $\sqrt[d_i]{a_i}$. We have*

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

for $s \geq 4$.

Proof. Recall that s is an upper bound on the number k of input radicands, the size of the circuit, and that the magnitude of a_i and d_i is at most 2^s.

Write $\alpha = \sum_i b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}$ where $e_{i_1} + \ldots + e_{i_k} \leq 2^s$, $b_i \in \mathbb{Z}$ with $b_i \leq 2^{2^s}$, i ranges over all monomials of the shape $x_i^{e_{i_1}} \cdots x_i^{e_{i_k}}$. 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:

$$M = \binom{k+D}{D} = \binom{k+D}{k} \leq \binom{s+2^s}{s} \leq (s+2^s)^s \leq 2^{s^2}$$

Denote by $G = \mathrm{Gal}(K/\mathbb{Q})$, and note that given the size bounds on our input $|G| \leq 2^{2s^2}$. Observe that the action of all $\sigma \in G$ is determined by their action on ζ_d, that is:

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

Then

$$\begin{aligned}
N(\alpha) &= N\left(\sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right) \\
&= \prod_{\sigma\in G} \sigma\left(\sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right) \\
&= \prod_{\sigma\in G} \sum_{i=1}^{M} b_i \left(\max_{j=1}^{k} x_j\right)^{\#e_i} \sigma\left(\zeta_d\right)^{\#e_i} \text{ where } \#e_i = e_{i_1} + \ldots e_{i_k} = \sum_{j=1}^{k} e_{i_j} \\
&= \prod_{l\in\mathbb{Z}_{|G|^*}} \sum_{i=1}^{M} b_i \left(\max_{j=1}^{k} x_j\right)^{\#e_i} \left(\zeta_d^l\right)^{\#e_i}
\end{aligned}$$

Finally, putting together all of our bounds yields

$$\begin{aligned}
|N(\alpha)| &\leq \prod_{l=1}^{2^{2s^2}} \left(\sum_{l=1}^{2^{s^2}} 2^{2^s} \cdot (2^s)^{2^s} \right) \\
&\leq \prod_{l=1}^{2^{2s^2}} \left(\sum_{l=1}^{2^{s^2}} 2^{2^s(s+1)} \right) \\
&\leq \prod_{l=1}^{2^{2s^2}} \left(2^{s^2} \cdot 2^{2^s(s+1)} \right) \\
&\leq \left(2^{s^2} \cdot 2^{2^s(s+1)} \right)^{2^{2s^2}} \\
&\leq 2^{2^{2s^2}(s2^s+2^s+s^3)} \\
&\leq 2^{2^{s^3}} \text{ for } s \geq 4.
\end{aligned}$$

□

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

The primitive element for number fields is as follows:

Theorem 5. *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, e.g., [18, Theorem 4.1.8] or [43, Theorem 5.1]), and computes the primitive element θ 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 θ is to be done inductively, constructing first a primitive element θ_2 for $L(\alpha_1, \alpha_2)$, then θ_3 for $L(\alpha_1, \alpha_2, \alpha_3)$, and so on until θ_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 θ, 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 [36, Proposition 6.6]):

Proposition 12. *Let α and β 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_θ of θ is monic and θ an algebraic integer.

Now let us prove our claim on the bounds on our primitive element θ:

Lemma 7 (Bound on the primitive element)**.** *The field K has a primitive element θ, computed as the linear combination*

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

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

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

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

In the spirit of the proof of the primitive element theorem, use Proposition 12 inductively as follows:

$$\begin{aligned}
\theta_2 &= \sqrt[d_1]{a_1} + c_2 \sqrt[d_2]{a_2} && c_2 \leq (2^s)^2(2^s)^2 + 1 \leq 2^{4s} \\
&\deg \theta_2 \leq 2^{2s} \\
\theta_3 &= \sqrt[d_1]{a_1} + c_2 \sqrt[d_2]{a_2} + c_3 \sqrt[d_3]{a_3} && c_3 \leq (2^{2s})^2(2^s)^2 + 1 \leq 2^{6s} \\
&\deg \theta_3 \leq 2^{3s} \\
&\vdots \\
\theta_k &= \sqrt[d_1]{a_1} + c_2 \sqrt[d_2]{a_2} + \ldots + c_k \sqrt[d_k]{a_k} && c_k \leq (2^{(k-1)s})^2(2^s)^2 + 1 \leq 2^{2s^2} \\
&\deg \theta_k \leq 2^{s^2} \\
\theta &= \theta_k + c_0 \zeta_d && c_0 \leq (2^{ks})^2(2^{s^2})^2 + 1 \leq 2^{4s^2} \\
&\deg \theta_2 \leq 2^{2s^2}
\end{aligned}$$

The claimed bounds on the degree of θ and the size of the constants c_i follow. □

C.3 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 $d = \operatorname{lcm}(d_1, \ldots, d_k)$, and ζ_d is a primitive d-th root of unity, and compute θ 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^s.

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

$$\Delta_f = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2 = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-2} \prod_{i \neq j} (r_i - r_j) \tag{8}$$

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

Lemma 8 (Bound on the discriminant)**.** *We have*

$$|\operatorname{Disc}(\mathbb{Z}[\theta])| \leq 2^{2^{5s^2}}$$

for $s \geq 4$.

Proof. Denote by $G = \operatorname{Gal}(K/\mathbb{Q})$ the Galois group of K. Recall we construct the primitive element θ 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 ζ_d as follows:

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

We choose the $c_i \in \mathbb{Z}$, hence θ is an algebraic integer. The minimal polynomial f_θ of the primitive element θ has roots $\theta = \theta_1, \ldots, \theta_{|G|}$. Note that the roots of f_θ 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 dth roots of unity, that is, given $\alpha \in K$, $\sigma_i(\alpha) = \alpha \zeta_d^i$ for some and $\sigma_i \in G$.

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

$$\deg \zeta_d \leq 2^{s^2}$$

As stated in Lemma 7, the constants c_i in the computation of the primitive element can be bound by:

$$c_i \leq 2^{4s^2}.$$

Now given $\sigma_j \in G$, write

$$\begin{aligned}\sigma_j(\theta) &= \sigma_j\left(c_0\zeta_d + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\right)\\ &= c_0\sigma_j(\zeta_d) + \sum_{i=1}^{k} c_i\sigma_j(\sqrt[d_i]{a_i})\\ &= c_0\zeta_d^{j+1} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\zeta_d^{ij}\end{aligned}$$

Then for $1 \le j, l \le |G|$, $j \ne l$

$$\begin{aligned}\sigma_j(\theta) - \sigma_l(\theta) &= \left(c_0\zeta_d^{j+1} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\zeta_d^{ij}\right) - \left(c_0\zeta_d^{l+1} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\zeta_d^{il}\right)\\ &= c_0\left(\zeta_d^{j+1} - \zeta_d^{l+1}\right) + \left(\sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\right)\left(\zeta_d^{ij} - \zeta_d^{il}\right)\end{aligned}$$

Note that for any two dth roots of unity ζ_d^j, ζ_d^l, we always have $\zeta_d^j - \zeta_d^l \le 2$, hence

$$\begin{aligned}\sigma_j(\theta) - \sigma_l(\theta) &\le 2c_0 + 2\left(\sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}\right)\\ &\le 2\cdot 2^{4s^2} + 2\left(\sum_{i=1}^{s} 2^{4s^2}\cdot 2^s\right)\\ &\le 2^{4s^2+1} + 2^{4s^2+s+1}s\\ &\le 2^{2s^3} \text{ for } s \ge 4.\end{aligned}$$

Thus

$$\begin{aligned}|\Delta_{f_\theta}| &= |\prod_{j\ne l}(\sigma_j(\theta) - \sigma_l(\theta))|\\ &\le \left(2^{2s^3}\right)^{|G|^2}\\ &\le \left(2^{2s^3}\right)^{\left(2^{2s^2}\right)^2}\\ &\le \left(2^{2s^3}\right)^{2^{4s^2}}\\ &\le 2^{2s^3\cdot 2^{4s^2}}\\ &\le 2^{2^{5s^2}} \text{ for } s \ge 4.\end{aligned}$$

□

C.4 Bound on the number of split primes

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

Lemma 9. *Assuming GRH,*

$$\pi_1(2^{4s^3}) \ge 2^{s^3} + 1.$$

Proof. Recall the bound on π_1 given in Proposition 5:

$$\pi_1(x) \ge \frac{1}{|\operatorname{Gal}(K/\mathbb{Q})|}\left[\pi(x) - \log\Delta_K - cx^{1/2}\log(\Delta_K x^{|\operatorname{Gal}(K/\mathbb{Q})|})\right]$$

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, note that $|\operatorname{Gal}(K/\mathbb{Q})| \leq 2^{2s^2}$.
Now compute

$$\begin{aligned}
\pi_1(2^{4s^3}) &\geq \frac{2^{4s^3}}{2^{2s^2} \cdot 4s^3} - 2^{3s^2} - c \cdot 2^{2s^3} \cdot 2^{3s^2} - c \cdot 2^{2s^3} \cdot 4s^3 \\
&\geq \frac{2^{4s^3}}{2^{s^3}} - 2^{2s^3} - c \cdot 2^{2s^3} \cdot 2^{3s^2} - c \cdot 2^{2s^3} \cdot 4s^3 \qquad \text{for } s \geq 4 \\
&\geq 2^{3s^3} - 2^{2s^3}(1 + c \cdot 2^{3s^2} + c \cdot 4s^3) \\
&\geq 2^{2s^3}(2^{s^3} - c \cdot 2^{3s^2} - c \cdot 4s^3) \\
&\geq 2^{2s^3} \text{ for a fixed constant } c \text{ and } s \geq \max(c, 5) \\
&\geq 2^{s^3} + 1.
\end{aligned}$$

□

D MISSING PROOFS FROM SECTION 4

D.1 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:

Pocklington's algorithm for $p = 8m + 5$	
Input:	Prime $p \equiv 5 \mod 8$ and integer a that is a quadratic residue modulo p
Output:	Solution of the equation $x^2 \equiv a \pmod p$
Step 1:	Write $p = 8m + 5$ with $m \in \mathbb{N}$.
Step 2:	If $a^{2m+1} \equiv 1 \pmod p$:
	Return $x = \pm a^{m+1}$.
	If $a^{2m+1} \equiv -1 \pmod p$:
	Write $y = \pm(4a)^{m+1}$ and return $x = \pm\frac{y}{2}$ if y is even, and $x = \pm\frac{p+y}{2}$ 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 $x = \pm a^{m+1}$.
(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, $x = \pm\frac{p+y}{2}$.

D.2 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 2-RIT problem.

Proposition 10. *Let C be an algebraic circuit of size at most s, and $a_1, \ldots, a_k$ primes of bit-length at most s, where $k \leq s$. Denote by α 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 (5). Then*

(i) p is prime with probability at least $\frac{1}{6s^3}$ assuming GRH, and

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

Proof. We follow the proof of [7, Proposition 9]. Recall that we set $a_i \leq 2^s$, which implies $A \leq 2^{s^2}$. For (i), we note that by Theorem 3, the probability that p is prime is at most

$$\begin{aligned}\frac{\pi_{8A,b+1}(2^{5s^3})}{2^{5s^3}/8A} &\geq \frac{8A}{\varphi(8A)\log 2^{5s^3}} - \frac{c\log 2^{5s^3} 8A}{(2^{5s^3})^{1/2}} \\ &\geq \frac{1}{5s^3} - \frac{c5s^3 2^{s^2+3}}{2^{2s^3}} \\ &\geq \frac{1}{5s^3} - \frac{c5s^3 2^{s^3}}{2^{2s^3}}\end{aligned}$$

where c is the absolute constant mentioned in the theorem. For k sufficiently large, the above is $\frac{1}{6s^3}$, which proves the claim.

For (ii), by Lemma 4 the norm of α has absolute value at most $2^{2^{s^3}}$, and hence $N(\alpha)$ has at most 2^{s^3} distinct prime factors. Then, for s sufficiently large, the probability that p divides $N(\alpha)$ given that p is prime is at most

$$\frac{6s^3 \cdot 8A \cdot 2^{s^3}}{2^{5s^3}} \leq 2^{-s^3}$$

□