UNIVERSITÉ PARIS CITÉ

École Doctorale Sciences Mathématiques de Paris Centre (ED 386)
Institut de Recherche en Informatique Fondamentale

Zero problems in polynomial models

Par KLARA NOSAN

Thèse de doctorat de INFORMATIQUE

Dirigée par MAHSA SHIRMOHAMMADI
Et par JAMES WORRELL

Présentée et soutenue publiquement le 4 octobre 2024

Devant un jury composé de :

MAHSA SHIRMOHAMMADI, CR	CNRS, Université Paris Cité	Directrice
JAMES WORRELL, PR	University of Oxford	Co-directeur
PASCAL KOIRAN, PR	ENS Lyon	Rapporteur
LAURA KOVÁCS, PR	TU Wien	Rapporteuse
VALÉRIE BERTHÉ, DR	CNRS, Université Paris Cité	Examinatrice
SÉBASTIEN TAVENAS, CR	CNRS, Université Savoie Mont Blanc	Examinateur

Abstract

Polynomial models are ubiquitous in computer science, arising in the study of automata and formal languages, optimisation, game theory, control theory, and numerous other areas. In this thesis, we consider models described by polynomial systems of equations and difference equations, where the system evolves through a set of discrete time steps with polynomial updates at every step. We explore three aspects of *zero problems* for polynomial models: zero testing for algebraic expressions given by polynomials, determining the existence of zeros for polynomial systems and determining the existence of zeros for sequences satisfying recurrences with polynomial coefficients.

In the first part, we study identity testing for algebraic expressions involving radicals. That is, given a k-variate polynomial represented by an algebraic circuit and k real radicals, we examine the complexity of determining whether the polynomial vanishes on the radical input. We improve on the existing **PSPACE** bound, placing the problem in **coNP** assuming the Generalised Riemann Hypothesis (GRH). We further consider a restricted version of the problem, where the inputs are square roots of odd primes, showing that it can be decided in randomised polynomial time assuming GRH.

We next consider systems of polynomial equations, and study the complexity of determining whether a system of polynomials with polynomial coefficients has a solution. We present a number-theoretic approach to the problem, generalising techniques used for identity testing, showing the problem belongs to the complexity class **AM** assuming GRH. We discuss how the problem relates to determining the dimension of a complex variety, which is also known to belong to **AM** assuming GRH.

In the final part of this thesis, we turn our attention to sequences satisfying recurrences with polynomial coefficients. We study the question of whether zero is a member of a polynomially recursive sequence arising as a sum of two hypergeometric sequences. More specifically, we consider the problem for sequences where the polynomial coefficients split over the field of rationals $\mathbb{Q}$. We show its relation to the values of the Gamma function evaluated at rational points, which allows to establish decidability of the problem under the assumption of the Rohrlich-Lang conjecture. We propose a different approach to the problem based on studying the prime divisors of the sequence, allowing us to establish unconditional decidability of the problem.

Key words: Algebraic Circuits, Computational Complexity, Decision Procedures, Hypergeometric Sequences, Identity Testing in Number Fields, Randomised Algorithms, Reachability

Résumé

Les modèles polynomiaux sont omniprésents en informatique, dans l'étude des automates et des langages formels, de l'optimisation, de la théorie des jeux, de la théorie du contrôle et de nombreux autres domaines. Dans cette thèse, nous considérons des modèles décrits par des systèmes d'équations polynomiales et des équations différentielles, où le système évolue à travers un ensemble discret de pas de temps avec des mises à jour polynomiales à chaque pas. Nous explorons trois aspects des *problèmes de zéros* pour les modèles polynomiaux : le test d'identité pour les expressions algébriques données par des polynômes, la détermination de l'existence de racines pour les systèmes polynomiaux et la détermination de l'existence de zéros dans les suites satisfaisant des récurrences à coefficients polynomiaux.

Dans la première partie, nous étudions les tests d'identité pour les expressions algébriques impliquant des radicaux. En d'autres termes, étant donné un polynôme à k variables représenté par un circuit algébrique et k radicaux réels, nous examinons la complexité de déterminer si le polynôme s'annule sur l'entrée. Nous améliorons la borne **PSPACE** existante, en plaçant le problème dans **coNP** en supposant l'hypothèse de Riemann généralisée (HRG). Nous considérons ensuite une version restreinte du problème, où les entrées sont des racines carrées de nombres premiers impairs, montrant qu'il peut être résolu en temps polynomial randomisé en supposant HRG.

Nous considérons ensuite les systèmes d'équations polynomiales et étudions la complexité de déterminer si un système de polynômes à coefficients polynomials a une solution. Nous présentons une approche du problème basée sur la théorie des nombres, généralisant les techniques utilisées pour les tests d'identité, et montrons que le problème appartient à la classe de complexité **AM** en supposant HRG. Nous analysons le lien entre ce problème et le problème de la détermination de la dimension d'une variété complexe, dont l'appartenance à **AM** a déjà été prouvé supposant HRG.

Dans la dernière partie de cette thèse, nous analysons les suites satisfaisant des récurrences à coefficients polynomiaux. Nous étudions la question de savoir si zéro appartient d'une suite récursive polynomiale résultant d'une somme de deux suites hypergéométriques. Plus précisément, nous considérons le problème pour les suites dont les coefficients polynomiaux se décomposent dans le corps des rationnels $\mathbb{Q}$. Nous montrons sa relation avec les valeurs de la fonction Gamma évaluées en des points rationnels, ce qui permet d'établir la décidabilité du problème supposant la conjecture de Rohrlich-Lang. Nous proposons une nouvelle approche basée sur l'étude des diviseurs premiers de la suite, ce qui nous permet d'établir la décidabilité inconditionnelle du problème.

Mots clés : circuits algébriques, complexité de calcul, procédures de décision, suites hypergéométriques, test d'identité dans les corps de nombres, algorithmes randomisés, atteignabilité

Résumé substantiel en français

Les polynômes sont les éléments constitutifs de nombreux modèles mathématiques en physique, chimie, biologie, économie, et dans de nombreuses autres disciplines. Calculer avec des polynômes est fondamental. En effet, nous apprenons tous à résoudre des équations quadratiques à l'école — mais comment feriez-vous pour trouver les zéros d'un polynôme de degré supérieur ? Ou mieux encore, pour résoudre tout un système d'équations polynomiales ?

Ces questions apparemment simples sont parmi les problèmes les plus classiques des mathématiques. Au début du XIXe siècle, par exemple, le résultat révolutionnaire de Galois a été de caractériser les polynômes qui sont résolubles par radicaux. À la fin du même siècle, Hilbert donne une condition caractérisant quand un système d'équations polynomiales n'est pas satisfaisable.

Avec le développement de l'informatique au XXe siècle, un nouveau point de vue sur les problèmes liés aux polynômes s'est présenté. Dans le contexte du calcul, de nombreuses nouvelles questions se posent : comment pouvons-nous représenter les polynômes de manière succincte ? Et quelle est la complexité de calcul avec de telles représentations succinctes ? Ici, calculer implique aussi bien déterminer si un polynôme s'annule sur une entrée donnée que trouver les zéros de polynômes, ou déterminer la satisfaisabilité de systèmes polynomiaux. Ces problèmes sont centraux dans la théorie de la complexité algébrique.

De nombreux résultats mathématiques sont constructifs, ce qui signifie que leurs preuves peuvent être interprétées comme une liste d'instructions permettant de construire la solution au problème computationnel associé — ou, en d'autres termes, un algorithme. Il existe cependant aussi un grand nombre de résultats mathématiques qui caractérisent les solutions des problèmes sans donner d'indication sur la manière de les construire effectivement. Pour donner un exemple, nous pouvons simplement revenir à la question par laquelle nous avons commencé. Il est bien connu que le corps des nombres complexes est algébriquement clos ; ainsi, étant donné un polynôme à coefficients entiers de degré positif, nous savons qu'il aura un zéro dans les nombres complexes. En revanche, écrire un algorithme permettant de trouver un tel zéro n'est pas du tout évident. Et, comme nous le verrons plus tard, le rendre efficace l'est encore moins.

Trouver les contreparties algorithmiques (efficaces) des résultats non constructifs a été et reste l'un des grands défis de l'informatique théorique. Dans cette thèse, nous considérons les aspects algorithmiques de cas spécifiques de *problèmes de zéro* pour des polynômes et des systèmes de polynômes. Nous allons un pas plus loin, et considérons également les problèmes de zéro pour des suites récurrentes à coefficients polynomiaux.

Contributions et organisation de la thèse

Nous étudions trois problèmes de zéro distincts pour des modèles polynomiaux.

Test d'identité pour les expressions de radicaux. Le test d'identité est une question algorithmique fondamentale avec de nombreuses applications. Dans le test d'identité algébrique, la tâche est de déterminer l'annulation d'une expression évaluée dans un anneau donné. Ce problème a de nombreuses versions différentes, selon la syntaxe de l'expression et l'anneau dans lequel l'évaluation doit être effectuée. Une instance de base du test d'identité algébrique est le problème de test d'identité de circuits arithmétiques (ACIT), qui consiste à décider de l'annulation d'un entier représenté par un circuit arithmétique. La difficulté de ce problème est que l'entier peut avoir une taille de bit exponentielle en fonction de la taille du circuit. Cependant, le problème admet un algorithme probabiliste en temps polynomial : on évalue le circuit modulo un nombre premier choisi au hasard dans un certain intervalle [1].

Dans cette thèse, nous étudions la complexité du problème de *test d'identité pour les expressions de radicaux* (RIT), c'est-à-dire, tester l'annulation d'une expression en radicaux, représentée par un circuit algébrique. Cela généralise le problème ACIT : l'évaluation du circuit se produit dans l'anneau des entiers d'un corps de nombres, plutôt que dans l'anneau des entiers des nombres rationnels. Formellement, le problème RIT demande, étant donné un circuit algébrique représentant un polynôme multivarié $f(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, et des entrées radicales $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ où les radicandes a_i, et les exposants d_i sont des entiers non négatifs, de déterminer si l'égalité

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

est vérifiée.

Une première borne de complexité pour le problème suit d'une réduction à la théorie existentielle des réels, qui est connue appartenir à **PSPACE** [2]. La réduction se fait en introduisant une nouvelle variable formelle pour chaque porte du circuit, et en ajoutant à la formule les équations $x_i^{d_i} - a_i = 0$ et $x_i > 0$ pour chaque radical. Pour décider RIT, il suffit maintenant de vérifier si le système résultant d'égalités et d'inégalités polynomiales a une solution dans les nombres réels.

Nous présentons une approche symbolique pour RIT, qui place le problème dans **coNP** en supposant l'Hypothèse de Riemann généralisée (HRG). L'idée principale derrière notre algorithme est que si $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \neq 0$, alors il existe un témoin de longueur polynomiale vérifiable en temps polynomial de ce fait — à savoir un nombre premier p et $\overline{\alpha}_1, \ldots, \overline{\alpha}_k \in \mathbb{F}_p$, satisfaisant $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$, tel que $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k)$ est non nul, où $\overline{f}$ est la réduction de f modulo p. La *transitivité conjointe* est cruciale pour notre approche : c'est l'observation que le groupe de Galois du corps réel sous-jacent agit conjointement de manière transitive sur les racines des différentes équations $x^{d_i} - a_i = 0$. Cela nous permet d'utiliser n'importe lequel des d_i conjugués α_i de $\sqrt[d_i]{a_i}$ dans $\mathbb{F}_p$ dans notre algorithme symbolique pour tester si $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$. En utilisant le théorème de densité de Chebotarev, et en choisissant un nombre premier approprié, nous montrons que RIT appartient à **coNP** en supposant HRG . Nous observons en outre que la transitivité conjointe seule peut être utilisée en conjonction avec un résultat de Koiran [3] pour placer RIT dans la classe de complexité **AM** en supposant HRG, ce qui nous permet de conclure que $\mathrm{RIT} \in \mathrm{AM} \cap \mathbf{coNP}$ sous HRG.

Nous considérons ensuite un cas particulier de RIT à savoir 2-RIT où les entrées du circuit sont des racines carrées de nombres premiers distincts, montrant que 2-RIT est dans **coRP** en supposant HRG et dans **coNP** sans condition. Nos preuves reposent sur la réciprocité quadratique et le théorème de Dirichlet sur la densité des nombres premiers dans les progressions arithmétiques. Enfin, nous généralisons également un algorithme existant pour la variante bornée du problème, où l'entrée comprend également une borne supérieure sur le degré du circuit.

Une variante paramétrique du problème de Nullstellensatz de Hilbert. Dans la deuxième partie de cette thèse, nous nous intéressons aux systèmes de polynômes. En géométrie algébrique, le *théorème des zéros de Hilbert* (aussi appelé le *Nullstellensatz de Hilbert*) est un résultat fondamental qui donne une condition caractérisant quand un système d'équations polynomiales n'est pas satisfaisable. Étant donné un système d'équations polynomiales

$$f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_k(x_1, \ldots, x_n) = 0 \tag{1}$$

où $f_i \in K[x_1, \ldots, x_n]$ pour K un corps algébriquement clos, la version faible du Nullstellensatz dit que le système n'as pas de solution dans K si et seulement si il existe des polynômes $g_1, \ldots, g_k \in K[x_1, \ldots, x_n]$ tels que

$$\sum_{i=1}^{k} f_i g_i = 1 \ . \tag{2}$$

Un problème de calcul naturellement associé demande de déterminer si une famille donnée de polynômes $f_1, \ldots, f_k$ a un zéro commun. Une version de ce problème, notée $\mathrm{HN}_{\mathbb{C}}$, demande de déterminer si un système donné d'équations polynomiales avec des coefficients entiers admet une solution dans $\mathbb{C}$.

La caractérisation donnée dans l'Équation (2) réduit essentiellement $\mathrm{HN}_{\mathbb{C}}$ à un *problème d'appartenance à un idéal*, à savoir si la constante 1 appartient à l'idéal généré par les f_i. Par un résultat de Mayr et Meyer [4], cela place $\mathrm{HN}_{\mathbb{C}}$ dans la classe de complexité **EXPSPACE**. D'un autre côté, il est facile de réduire le problème 3-SAT à $\mathrm{HN}_{\mathbb{C}}$, ce qui le rend au moins **NP**-difficile. Au fil des ans, divers *Nullstellensätze Effectifs* [5, 6, 7] ont donné des bornes de degré à croissance exponentielle sur les g_i, ce qui réduit le problème d'appartenance à un idéal venant du Nullstellensatz à celui de la résolution d'un système d'équations linéaires de taille exponentielle. Cela donne une borne supérieure en **PSPACE** pour $\mathrm{HN}_{\mathbb{C}}$. Dans un article influent [3, 8], Koiran a prouvé que $\mathrm{HN}_{\mathbb{C}}$ se trouve dans la classe de complexité **AM** (et donc au deuxième niveau de la hiérarchie polynomiale) si l'on suppose le HRG.

Dans cette thèse, nous inspectons la complexité d'une *version paramétrique du problème de Nullstellensatz de Hilbert* (notée $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$), qui, étant donné un système de polynômes $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ pour $\boldsymbol{x} := (x_1, \ldots, x_m)$, demande si ces polynômes ont une solution dans $\overline{\mathbb{Q}(\boldsymbol{x})}$. Ces systèmes d'équations polynomiales sont des objets centraux d'étude en combinatoire algébrique et en théorie des langages formels, où ils sont utilisés pour spécifier des fonctions génératrices d'objets combinatoires (voir, par exemple, les revues dans [9, 10]), et leurs solutions correspondent à des séries formelles dans les variables $x_1, \ldots, x_m$.

Nous présentons une généralisation de la technique introduite dans [3, 8], permettant l'utilisation d'arguments algébriques pour établir une réduction en temps polynomial aléa-

toire de $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ à $\mathrm{HN}_{\mathbb{C}}$. En particulier, étant donné un système de polynômes avec des coefficients dans $\mathbb{Z}[\boldsymbol{x}]$, nous calculons une borne D telle que si nous attribuons aux variables x_i des valeurs choisies uniformément au hasard parmi $\{1, \ldots, D\}$ et utilisons l'algorithme de Koiran pour déterminer si le système spécialisé est satisfaisable dans $\mathbb{C}$, avec une probabilité suffisamment élevée, l'algorithme donnera une réponse correcte au problème sur $\overline{\mathbb{Q}(\boldsymbol{x})}$. Nous montrons ainsi que $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}} \in \mathbf{AM}$ en supposant le HRG.

Nous discutons également de la relation de $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ avec le problème de déterminer si une variété dans $\mathbb{C}$ a une dimension d'au moins d, que nous notons $\mathrm{DIM}_{\mathbb{C}}$. Nous montrons qu'avec une petite modification, le protocole **AM** pour $\mathrm{DIM}_{\mathbb{C}}$ de [11] s'applique également à $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$, fournissant ainsi une preuve alternative de la même borne de complexité.

Le problème d'appartenance pour les suites hypergéométriques. Dans la dernière partie de cette thèse, nous nous concentrons sur les suites satisfaisant des récurrences à coefficients polynomiaux. Nous étudions le problème de trouver un terme zéro dans une suite donnée comme la somme de deux suites hypergéométriques, qui sont celles satisfaisant des récurrences de la forme $p(n)u_n = q(n)u_{n-1}$ avec des coefficients polynomiaux $p(x)$ et $q(x)$. Le problème que nous considérons s'inscrit dans le cadre plus général des tests de zéro pour les suites récursives. Peut-être que l'exemple le plus célèbre de ce type de problème d'appartenance (ou d'atteignabilité) est le Problème de Skolem, qui demande de décider de l'existence d'un terme zéro dans une suite définie par récurrence linéaire (à coefficients constants). Pour la majorité des problèmes de ce type, leur statut de décidabilité reste largement ouvert. Par exemple, le Problème de Skolem est considéré comme ouvert depuis au moins les années 1970, avec une décidabilité connue seulement pour les récurrences linéaires d'ordre au plus quatre [12, 13].

Nous montrons d'abord que le problème de trouver un terme zéro dans une suite donnée comme la somme de deux suites hypergéométriques se réduit au *problème d'appartenance* pour les suites hypergéométriques (MP), qui demande, étant donné une suite hypergéométrique $\langle u_n \rangle_{n=0}^{\infty}$ et une cible $t \in \mathbb{Q}$, s'il existe un n tel que $u_n = t$. Nous étudions, en particulier, la variante du problème pour les suites où les coefficients polynomiaux de l'équation définissant la suite se décomposent dans $\mathbb{Q}$, c'est-à-dire pour les suites hypergéométriques avec des paramètres rationnels.

Nous commençons par rappeler la relation entre le comportement asymptotique d'un produit de fonctions rationnelles et la fonction Gamma, une fonction étudiée en théorie des nombres. Nous montrons que l'établissement de la décidabilité du Problème d'Appartenance pour le cas des paramètres rationnels utilisant l'approche asymptotique est conditionné à l'hypothèse de la conjecture de Rohrlich-Lang, qui concerne les expressions algébriques dans les valeurs Gamma.

Notre contribution principale est un résultat de décidabilité inconditionnelle pour la variante du problème avec des paramètres rationnels. Nous abordons la décision du problème d'appartenance sous un autre angle–spécifiquement, en considérant les diviseurs premiers de u_n. Notre stratégie est de montrer que (à l'exception de quelques cas dégénérés) pour tout n suffisamment grand, u_n a un diviseur premier p qui n'est pas également un diviseur premier de la cible t. Cela nous permet de calculer une borne N telle que $u_n \neq t$ pour tout $n > N$. Nous étudions les valuations p-adiques et, étant donné un élément u_n de notre suite, déterminons les conditions sur les premiers p pour que p apparaisse dans la factorisation de u_n (en termes de valuations, $v_p(u_n) \neq 0$), alors qu'il ne divise pas la cible t (c'est-à-dire

$v_p(t) = 0$). L'une des conditions en question est que p appartienne à une progression arithmétique bien choisie. En fait, étant donné un premier p provenant de la progression, nous calculons un ensemble de valeurs n telles que $v_p(u_n) \neq 0$. En utilisant des résultats classiques sur la répartition des premiers dans les progressions arithmétiques, nous sommes alors capables de construire une suite infinie de premiers $\langle p_i \rangle_{i=0}^{\infty}$ et de montrer l'existence d'une borne N telle que l'ensemble des indices n pour lesquels $v_{p_i}(u_n) \neq 0$ à mesure que i tend vers l'infini couvre tous les $n > N$. Autrement dit, les p_i témoignent que $u_n \neq t$ pour tout $n > N$.

Structure de ce document. Nous commençons par un aperçu de l'état de l'art pour les problèmes zéro que nous considérons dans le Chapitre 1. Dans le Chapitre 2, nous donnons des préliminaires techniques relevant à la fois de l'informatique, notamment de la théorie de la complexité, ainsi que des définitions algébriques et de la théorie des nombres. Tous les chapitres suivants commencent par un renvoi à la section préliminaire pertinente pour les résultats en question. Le Chapitre 3 est consacré à nos résultats sur les tests d'identité pour les polynômes évalués sur des radicaux réels. Dans le Chapitre 4, nous considérons le problème plus général de déterminer si un système d'équations polynomiales admet une solution commune, en nous concentrant notamment sur les solutions paramétriques. Enfin, dans le Chapitre 5, nous nous concentrons sur un problème de zéro sur les suites satisfaisant des équations polynomiales récurrentes, dont nous montrons qu'il se réduit au problème d'appartenance pour les suites hypergéométriques.

Acknowledgements

First of all, I would like to thank my supervisors Mahsa Shirmohammadi and Ben (James) Worrell. Dear Mahsa, thank you for accepting to supervise my thesis, even though it came as a surprise. Thank you for your trust, for sharing your enthusiasm for research with me, encouraging me to think creatively, asking hard questions when they were due and being by my side in these last three+ years. You have taught me how to do research, collaborate with others, and stay resilient — thanks to you I know that any difficult problem can be tackled if we take it step by step, and I will take this with me, wherever I go next. Ben, I admire how you make any research problem seem approachable and interesting. Working with you I have learned that trying to think simple often is the best way to go, that most mathematical results are related much more closely than I thought, and that there *is* a perfect reference for any classical result out there. Thank you for always appearing when needed, especially in the case of a mathematical emergency.

Alongside my supervisors, I would like to thank my other coauthors whom I have had the pleasure to collaborate with in the past three years. Amaury, Sylvain, Nikhil, George, Lorenzo and Rida — thank you for kindly welcoming me in the scientific community, for all the interesting discussions, advice and your patience with my questions, confusions, and first attempts in writing scientific papers. The results presented in this thesis are all part of our joint works, and they would not be nearly as refined or clearly presented without you. Special thanks go to Nikhil (and Maha!) for hosting me in Delhi, and acting as an honorary cosupervisor whenever I needed one.

I am grateful to Pascal Koiran and Laura Kovács for taking the time to carefully read and review this manuscript. I would also like to thank Valérie Berthé and Sébastien Tavenas for showing interest in this thesis and agreeing to take part in the jury.

I have had the great pleasure to work on my thesis at IRIF, and would like to thank all colleagues who have made the lab a pleasant place I would look forward to come back to every morning. Special thanks go to Simon and Zhouningxin for welcoming me in office 4031. Minh Hang, Xinhong and Shamisa who joined me there in the following months — thank you for all the encouraging words, the coffee breaks, and sharing your cultures with me. Thank you Victor, for being my honorary academic brother, and taking time for me even when your own to-do list was overflowing. Srinidhi, thank you for always always always being there. Merci Lucie, for the weekly office visits after teaching that slowly turned into lunches, coffee breaks, and a friendship I am sure will last even after we will have both left IRIF. Roman, I will miss your clever remarks and our always insightful conversations. Thank you Clément, for all the encouraging words and cheerful moments, especially when I was annoyed about being in a bad mood. Merci Jemuel pour tout ! Thanks to Colin for sharing (and bearing with me during) the highs and the lows of the last months of our thesis writing. Thank you Enrique, Dániel and Filippo, for always taking the time to

listen, I will keep fond memories of all our dinners and office gossip sessions. Thanks also go to Esaïe, Mouna, Bernardo, Martin, Vincent, Quentin, Daniel, Anupa, Weiqiang, Robin, and everyone else who was always happy to have a chat in the hallway with me, join our cool kids' table for lunch now and again, or meet outside of work. Kind thoughts go to all other researchers and fellow PhD students whom I have had the chance to meet in the last three years, be it at conferences, summer schools, or during research visits.

To all my dear friends outside of IRIF, who, while scattered around the world, always seemed to be around when I needed them most — I truly couldn't have done it (or at least stayed as sane) without you. Thank you Hadrien, for becoming my friend when I needed one most. Thanks to Lara, Nana, Alexandre, Lana, Marie for always being a little escape from my academic life here in Paris. And to Maša, Liese, Nija, Jana, Nejc, Pia, Lea, Jan, Jure, Florian, Falk, Joshua — thank you for all the messages and phone calls, for visiting me in Paris again and again, for hosting me and travelling with me when I needed a holiday, and taking the time out of your life to meet me whenever I went home. I am still hoping one day you all move to Paris to be closer to me.

My final, and dearest thanks go to my family, who keep on supporting me in every challenge I decide to take on, patiently listen and encourage me while I navigate through it, and make me feel like home is just a phone call away.

Contents

Chapter 1

Introduction

Polynomials are the building blocks of many mathematical models in physics, chemistry, biology, economics, and numerous other disciplines. Computing with polynomials is fundamental. Indeed, we all learn how to solve quadratic equations in school — but how would you go about finding zeroes of a higher degree polynomial? Or better yet, solve a whole system of polynomial equations?

Such seemingly simple questions are among some of the most classical problems in mathematics. In the early 19th century, for example, Galois's groundbreaking result was characterising polynomials that admit solutions in radicals. At the end of the same century, Hilbert's fundamental result was giving a condition on when a system of polynomial equations is not satisfiable.

With the development of computer science in the 20th century, a new angle to problems on polynomials presented itself. In the context of computation many new questions arise: how can we represent polynomials in a succinct way? And how efficiently can we compute with such succinct representations? Here, computing involves everything from determining whether a polynomial vanishes on a given input, finding zeroes of polynomials, or determining satisfiability of polynomial systems. These problems are central to algebraic computational complexity theory.

Many mathematical results are constructive, meaning that their proofs can be interpreted as a list of steps allowing to construct the solution to the associated computational problem — or, in other words, an algorithm. There are, however, also a large number of mathematical results that characterise the solutions of problems without giving any indication on how to actually construct them. For an example, we can just go back to the question we started with. It is well known that the field of complex numbers is algebraically closed; thus, given a polynomial with integer coefficients of positive degree, we know that it will have a zero in the complex numbers. Writing down an algorithm allowing to find such a zero, on the other hand, is far from obvious. And, as we will see later, making it efficient even more so.

Finding the (efficient) algorithmic counterparts of non-constructive results has been and remains one of the big challenges in theoretical computer science. In this thesis we consider

algorithmic aspects of specific cases of *zero problems* for polynomials and systems of polynomials. We go one step further, and also consider zero problems for number sequences defined by recursive equations with polynomial coefficients.

Contributions and organisation of the thesis

We study three distinct zero problems for polynomial models.

Identity Testing for Radical expressions. We study the complexity of the *Radical Identity Testing* (RIT) problem, which 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, asks to determine whether the equality

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

holds.

We present a symbolic approach to the problem, placing it in **coNP**, assuming the generalised Riemann hypothesis (GRH), improving on the existing **PSPACE** upper bound. We also consider a special case of RIT namely 2-RIT where the inputs to the circuit are square roots of distinct primes, showing that 2-RIT is in **coRP** assuming GRH and in **coNP** unconditionally. Finally, we also generalise an existing algorithm for the bounded variant of the problem, where the input also includes an upper bound on the degree of the circuit that is given in unary.

A parametric variant of the Hilbert Nullstellensatz problem. We inspect the complexity of a *parametric version of the Hilbert Nullstellensatz* (HN) problem, which given a system of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ for $\boldsymbol{x} := (x_1, \ldots, x_m)$, asks whether they have a solution over $\overline{\mathbb{Q}(\boldsymbol{x})}$.

We give a number-theoretic proof showing that the problem is in **AM** assuming GRH via a reduction to HN over $\mathbb{C}$. We further recall that the problem is closely related to the problem of determining whether a variety over $\mathbb{C}$ has dimension least d, and show how the **AM** algorithm for the dimension problem applies to parametric HN.

The Membership Problem for hypergeometric sequences. We study the problem of finding a zero term in a sequence given as a sum of two hypergeometric sequences, which are those satisfying recurrences of the form $p(n)u_n = q(n)u_{n-1}$ with polynomial coefficients $p(x)$ and $q(x)$. We observe that the problem at hand reduces to the Membership Problem for hypergeometric sequences (MP), which asks, given a hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ and a target $t \in \mathbb{Q}$, whether there exists n with $u_n = t$.

We begin by recalling the relation between the asymptotic behaviour of a product of rational functions to the Gamma function, a function studied in number theory. We show that establishing decidability of the problem for the case of rational parameters using the

asymptotic approach is conditioned to the assumption of the Rohrlich-Lang conjecture, which concerns algebraic expressions in the Gamma values. Our main contribution is an unconditional decidability result for the variant of the problem with rational coefficients, which we obtain by analysing the prime divisors of the sequence. We show that (except in some degenerate cases) for all sufficiently large n, u_n has a prime divisor p that is not also a prime divisor of the target t. This allows us to compute a bound N such that $u_n \neq t$ for all $n > N$, reducing the membership test for t to that of searching within the finite set $\{u_0, \ldots, u_N\}$.

Organisation of the thesis. In the present chapter we give an overview of the state of the art for the zero problems that we consider. In Chapter 2, we give technical preliminaries relevant both from computer science, notably complexity theory, as well as algebraic and number-theoretic definitions. All following chapters begin with a pointer to the relevant preliminary section for the results at hand. Chapter 3 is dedicated to our results on identity testing for polynomials evaluated on real radicals. In Chapter 4, we consider the more general problem of determining whether a system of polynomial equations admits a common solution, focusing notably on parametric solutions. Finally, in Chapter 5, we shift our focus to a zero problem on sequences satisfying polynomially recursive equations, which we show reduces to the Membership Problem for hypergeometric sequences.

1.1 Zero testing for algebraic expressions

Identity testing is a fundamental problem in algorithmic algebra which asks to determine the zeroness of an expression evaluated in a given ring. The problem has many different variants, depending on the syntactic representation of the expression and the ring in which evaluation is to be carried out. Arguably the simplest instance of algebraic identity testing is the *Arithmetic Circuit Identity Testing* (ACIT) problem, which asks to decide the zeroness of an integer represented by an arithmetic circuit. An example input to ACIT is illustrated in Figure 1.1; recall that an algebraic circuit is a directed acyclic graph where the leaves are labelled by constants (or variables when representing a polynomial), and the inner vertices have labels in $\{+, -, \times\}$. We define the size of the circuit to be the number of addition, multiplication and subtraction gates.

While the problem may seem simple, it is still open whether it can be decided in polynomial time. A natural way to approach it could be to try to compute the integer in question explicitly, or approximate it to sufficient precision in order to separate the value from zero. The difficulty here is that the bitsize of an integer represented by a circuit can be exponential in the size of the circuit, precluding computing the integer and the intermediate values appearing in the circuit (explicitly or just approximately) in polynomial time. However, the problem has been shown to belong to the complexity class **coRP** in the late 70s [1]. The randomised polynomial time algorithm for the problem works by randomly choosing a prime p, and performing the evaluation in the finite field $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$. If the computed value is non-zero, then the integer represented by the circuit must be non-zero as well. On the other hand, if the computed value in the finite field is zero, then either the integer really

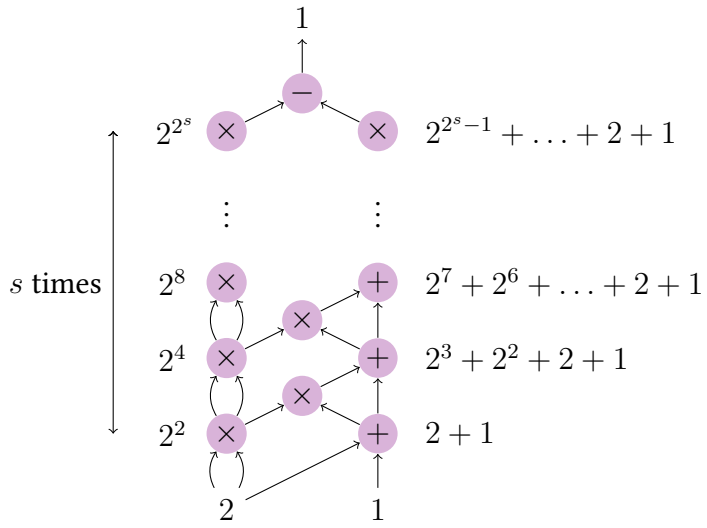

Figure 1.1 – An algebraic circuit of size $O(s)$ computing the integer 1 with intermediate values of bit size exponential in the size of the circuit.

is zero, or p is one of its prime divisors. Since the integer is of bitsize at most exponential in the circuit size, if we choose the prime p in a large enough range, the probability that p divides the computed value is polynomially small in the size of the instance. By repeating the randomised procedure polynomially many times, we can thus ensure the error probability of a false positive is bounded below $\frac{1}{2}$, which places the problem in **coRP**.

The ACIT problem has been shown to be polynomial-time interreducible with the *Polynomial Identity Testing* (PIT) problem which asks to determine zeroness of an arithmetic circuit evaluated in the ring of multivariate polynomials [14, Proposition 2.1]. The latter problem had also been shown to belong to **coRP** before the equivalence was known, notably in [15] using the Schwartz-Zippel Lemma [16, 17, 18]. Whether PIT admits a deterministic polynomial-time algorithm is one of the central open questions in complexity theory. Besides the interest that it has raised from this purely theoretical point of view, over the years, PIT has also found many applications in algorithm design. Such examples include program testing [19], detecting perfect matchings [20], factoring polynomials [21], pattern matching in compressed texts [22, 23], primality testing [24, 25], equivalence and minimisation of weighted automata [26, 27] and linear recurrence sequences [28, 29].

Algebraic identity testing has also been shown to relate to word problems on finitely generated groups and semigroups. Studied for over 100 years [30], these problems are arguably some of the first identity testing questions considered. In recent years, a growing body of work has been dedicated to the *Compressed Word problem* [31], where the words are represented succinctly by *straight line programs*, which, intuitively speaking, can be thought of as circuits with leaves labelled by the letters '0' and '1'. The relation of the computational complexity of problems on compressed words to algebraic identity testing has been explored in, e.g., [22, 32].

We will now focus on identity testing problems for cyclotomic and radical fields, which

are some of the most studied instances of algebraic identity testing problems. Before we do so, let us just mention another related, more difficult problem, which lies at the intersection of transcendental number theory and model theory. The *Elementary Constant problem* [33] asks, given a complex number built from rationals using addition, multiplication and exponentiation, to determine whether 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 for the problem assuming Schanuel's conjecture [34], it is not known to be decidable unconditionally, and no significant complexity lower or upper bounds are known.

The cyclotomic world. Algebraic identity testing has been extensively studied for rings of integers of cyclotomic number fields, that is, finite extensions of the field of rationals $\mathbb{Q}$ generated by adjoining a primitive nth root of unity ζ_n. Recall that an *nth root of unity* is a complex number ζ_n such that $\zeta_n^n = 1$. If for each $k < n$, $\zeta_n^k \neq 1$, then we call it a *primitive nth root of unity*. Here, the problem, in simple words, is to determine whether an algebraic integer in the field $\mathbb{Q}(\zeta_n)$ in a given representation is zero.

The *Sparse Cyclotomic Identity Testing problem* (sparse-CIT) asks, given a polynomial $f \in \mathbb{Z}[x]$, and an integer $n \in \mathbb{N}$ written in binary, whether f vanishes at a primitive nth root of unity $\zeta_n = e^{2\pi i/n}$. In this setting, the polynomial is assumed to be given in a *sparse representation*, that is, as a list of monomials with non-zero coefficients (whose degree can be exponential in the representation size). The problem was first considered by Plaisted, who showed that sparse-CIT $\in$ **coNP** [35, Theorem 4.3] and conjectured that the problem should be solvable in polynomial time. Cheng et al. [36, 37] proved his conjecture, showing that sparse-CIT $\in$ **P** by exhibiting two deterministic polynomial time algorithms. Their method presented in [37] was revisited in [32], and the complexity bound refined to **NC**, which can be thought of as the subclass of problems in **P** that are efficiently parallelisable.

A generalised version of the problem, which we call *Sparse Generalised Cyclotomic Identity Testing* (sparse-GCIT), asks, given a sparse polynomial $f \in \mathbb{Z}[x]$, whether there exists $n \in \mathbb{N}$ such that $f(\zeta_n) = 0$, where ζ_n is again an nth primitive root of unity. In his 1984 paper, Plaisted showed that this problem is **NP**-hard [35, Theorem 5.1]. Later sparse-GCIT was considered by Filaseta and Schinzel in [38], where they gave a subexponential time algorithm for the problem. Cheng et al. [37] showed that if an instance of the problem is positive, the certificate is at most polynomial in the size of the input. Namely, it consists of an integer $n \in \mathbb{N}$ such that $f(\zeta_n) = 0$. Since the roots of f are algebraic numbers of degree at most $\deg f$ over $\mathbb{Q}$, n must be bounded in magnitude by the degree of f. Their result that sparse-CIT $\in$ **P** furthermore ensures that the verification of a certificate can be done in polynomial time, allowing them to place the sparse-GCIT problem in **NP**, making the problem **NP**-complete.

An orthogonal generalisation of sparse-CIT is the *Torsion Point* (TP) problem which asks, given a system of multivariate polynomials $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_k]$ in sparse representation and a list of integers $d_1, \ldots, d_k \in \mathbb{N}$, whether

$$f_1(\zeta_{d_1}, \ldots, \zeta_{d_k}) = 0, \ \ldots, \ f_s(\zeta_{d_1}, \ldots, \zeta_{d_k}) = 0$$

is satisfiable.

Let us note in paranthesis that both the sparse-GCIT problem and the Torsion Point problem can be seen as special cases of the *Hilbert's Nullstellensatz* (HN) problem, which, given a system of polynomial equations

$$f_1(x_1, \ldots, x_k) = 0, \ \ldots, \ f_s(x_1, \ldots, x_k) = 0\,,$$

asks whether they have a common zero over a given ring or field. We defer a more detailed discussion on HN to Section 1.2, let us just recall the most influential result on the problem, which we will reference in this section. Over $\mathbb{C}$, the HN problem is known to be in the complexity class **AM** assuming the Generalised Riemann Hypothesis [3, 8].

Notice, however, that the Torsion Point problem does not ask about satisfiability over a fixed cyclotomic field, or even the ring of integers of a given cyclotomic fields, but rather asks whether the variety defined by the polynomials contains a point whose coordinates are all roots of unity. The first hardness result for the problem was again given by Plaisted [35, Theorem 3.3], who showed that the problem TP_1 where the input polynomials are univariate, i.e., when $f_1, \ldots, f_s \in \mathbb{Z}[x]$, is **NP**-hard. The result is stated in terms of polynomial divisibility, in particular, the author shows that the 3-SAT problem reduces to the problem of checking, given a finite set of sparse polynomials $\{p_1(x), \ldots, p_s(x)\}$, whether $x^n - 1$ is not a factor of $\prod_{i=1}^{s} p_i(x)$.

Later on, in [39] the TP problem was placed in the complexity class **AM** under the assumption of certain number theoretic hypotheses via a reduction to Koiran's result on HN [3]. In particular, the result is based on a preprint of the same author [40], where he shows that the assumption of GRH in Koiran's original paper on HN can be weakened to two "more plausible" hypotheses from analytic number theory. Furthermore, the univariate version of the problem, TP_1, was shown to be in $\mathbf{NP}^{\mathbf{NP}}$ unconditionally. The general version of the TP problem was shown to be in **P** for fixed n and $d_1, \ldots, d_n$. Here, the unconditional results are obtained by taking the evaluation to a finite field $\mathbb{F}_p$ where the prime p is chosen in a suitable arithmetic progression, and its existence ensured by Linnik's Theorem. Cheng et al. finally closed the complexity gap in [37] through their result on sparse-CIT, placing TP in **NP**, and hence showing that it is **NP**-complete.

A natural question that arises when considering the zero testing problems reviewed above is how efficiently one can decide zeroness when the polynomials are given in a different representation, namely using an algebraic circuit. The *Cyclotomic Identity Testing* (CIT) problem asks, given an algebraic circuit C representing a polynomial $f \in \mathbb{Z}[x]$ and an integer $n \in \mathbb{N}$ given in binary, whether $f(\zeta_n)$ is zero. In their seminal paper, Chen et al. raised the question of the complexity of CIT, which was then extensively studied in [32]. The algebraic circuits considered in [32] follow the standard definition of algebraic circuits via directed acyclic graphs with the additional condition of allowing leaves to be labelled with monomials $\{x^e \colon e \in \mathbb{N}\}$. Thus the syntactic degree of the circuit in this case is *not* an upper bound on the degree of the computed polynomials. Using this model, the authors show that CIT can be placed in **BPP** under the assumption of GRH, and in **coNP** unconditionally. Their approach to the problem follows the technique introduced for solving ACIT. In particular, they choose a prime $p \in \mathbb{Z}$ such that the finite field $\mathbb{F}_p$ corresponds to the quotient of the ring of cyclotomic integers $\mathbb{Z}[\zeta_n]$ by a prime ideal, and perform the evaluation in $\mathbb{F}_p$. In the non-deterministic algorithm, they guess a representative for ζ_n in $\mathbb{F}_p$, and

false positives appear essentially for the same reason as in the **coRP** algorithm for ACIT, namely, if the prime p divides the norm of the computed cyclotomic integer $f(\zeta_n)$. By contrast, in the probabilistic algorithm, non-deterministic guessing of the representative for ζ_n in $\mathbb{F}_p$ is replaced by a random guess, which makes the error two-sided.

The authors further consider a restricted variant of the problem, namely bounded-CIT. The input of the problem in this case, alongside a circuit C and integer $n \in \mathbb{N}$, also includes an upper bound on the syntactic degree of the circuit given in unary. That is, in this variant the degree of the circuit is at most the length of the input — note, however, that as the circuit is allowed to have monomials as inputs, the degree of the computed polynomial may again be a binary value. Balaji et al. exhibit a randomised **NC** procedure with two-sided error for deciding bounded-CIT. Their technique follows the approach introduced by Chen and Kao [41], who aimed at improving the number of random bits used for deciding PIT. In particular, they approached PIT by approximating the value of the input polynomial when evaluated at certain randomly chosen irrational inputs, namely linear combinations of real square roots. 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, for which they use numerical approximation. The idea, reused in [32], is to pick a Galois conjugate of the value that is being tested for zeroness uniformly at random, and determine the zeroness of the conjugate via numerical approximation. The correctness of the procedure is asserted by a probabilistic bound on the absolute value of conjugates of algebraic integers subsumed in Chen and Kao's [41, Lemma 2.2], which was also used for testing zeroness of bounded expressions involving radicals ([42, Lemma 3]) as discussed below, and finally restated as Proposition 12 in [32].

The parallel radical world. In this thesis, we study identity testing problems for algebraic expressions in the rings of integers of number fields generated by adjoining real radicals to $\mathbb{Q}$. Generally speaking, radical extensions of $\mathbb{Q}$ are more difficult to handle algorithmically than cyclotomic fields, and enjoy fewer "nice" properties. Cyclotomic extensions, for example, are known to be *abelian* extensions of $\mathbb{Q}$. In particular, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of a cyclotomic extension $\mathbb{Q}(\zeta_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. In fact, algorithmic approaches to solving problems over cyclotomic fields may be enough to cover all abelian extensions: the Kronecker–Weber theorem states that every finite abelian extension of $\mathbb{Q}$ is contained within some cyclotomic field. In simple words, the theorem states that every algebraic integer whose Galois group is abelian can be expressed as a sum of roots of unity with rational coefficients.

Now could we use this to handle radical extensions as well? As it turns out, radical extensions need not be abelian. Take for example the Galois extension of the field generated by adding the radical $\sqrt[4]{2}$ to $\mathbb{Q}$. The extension $\mathbb{Q}(\sqrt[4]{2})$ is not Galois, but is contained in the Galois extension $\mathbb{Q}(\sqrt[4]{2}, i)$ with Galois group D_4 — the 4th dihedral group, which is the group of symmetries of a regular polygon with 4 vertices, which is known not to be abelian. The Galois groups of radical extensions are, however, known to be *solvable*. Let us recall that a group G is said to be solvable if there exists a chain of normal subgroups $\{\mathrm{id}\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_n = G$ such that each quotient G_j/G_{j-1} is abelian. Intuitively speaking, a

sparse representation				
	cyclotomic		radical	
IT	sparse-CIT	**NC** [32]	sparse-RIT	subclass in **P** [43, 44]
generalised IT	sparse-GCIT	**NP**-complete [37]	sparse-GRIT	subclass in **NP**
special points	TP	**NP**-complete [37]	RadP	subclass in **P**

circuit representation				
	cyclotomic		radical	
IT	CIT	**coNP**, **BPP**✻ [32]	RIT	**coNP**✻
			2-RIT	**coNP**, **coRP**✻
bounded IT	bounded-CIT	**randNC** [32]	bounded-RIT	**coRP**

Figure 1.2 – An overview of the complexity results for identity testing problems over cyclotomic and radical number fields. The results marked with ✻ hold under the assumption of the Generalised Riemann Hypothesis (GRH), the results proved in these thesis are written in teal, whereas existing results are marked with corresponding references.

solvable group can be thought of a as group which can be constructed from abelian groups using extensions. In the case of our example, the group D_4 can be decomposed as $\{\mathrm{id}\} \triangleleft C_2 \triangleleft C_4 \triangleleft D_4$, where C_2 and C_4 denote the cyclic groups of orders 2 and 4 respectively.

The knowledge of the Galois group of the extension where the numbers live in is central to solving identity questions. In our overview of cyclotomic identity testing, we have seen that the technique of randomly guessing a Galois conjugate of a given value is an important step in many algebraic identity testing algorithms, such as the works [32] or [41] we cited above. This essentially boils down to randomly sampling an element of the Galois group, which as it turns out, algorithmically appears to be a difficult task.

Some of the first results on computational aspects of solvable Galois groups were published by Landau and Miller, who, given a polynomial f, exhibit a polynomial time algorithm to determine whether its group is solvable, and compute the intermediate field extensions between $\mathbb{Q}$ and the splitting field of f over $\mathbb{Q}$ [45]. Landau further provided polynomial time algorithms to determine whether the Galois group of a given polynomial is isomorphic to A_n or S_n, or, if the group is solvable, to compute the list of prime divisors of its order in [46]. The complexity of computational problems for solvable groups using a quantum computer were considered in [47], showing that the order of a solvable group can be computed in quantum polynomial time when given a list of generators of the group as input. The question of computing the Galois group of a polynomial was extensively considered by Arvind and Kurur in [48]. They show that, given a polynomial f, the order of its Galois group can be computed in the counting hierarchy. If the Galois group of f is solvable, then the computation of its order can be done in $\mathbf{RP}^{\mathbf{NP}}$. Finally, for polynomials with abelian Galois groups, the authors provide a randomised polynomial time algorithm computing the generators of the Galois group.

In contrast to the case of abelian Galois groups, finding an efficient algorithm computing the generators of a Galois group of a solvable extension has remained open since the work of Arvind and Kurur, and no algorithm to randomly sample from such groups is known. Let us also remark that in these works, the polynomial f whose Galois group is investigated is given in a dense representation. That is, the values of all coefficients, including those that are zero are part of the input, and the size of the input is thus a bound both on the degree and the bitsize of the coefficients. In the application at hand, one of the difficulties we face is the fact that the number fields we work with have degree exponential in the size of the input.

Another algorithmically convenient property of cyclotomic fields is that their rings of integers are generated by a single element. In particular, the ring of integers of a cyclotomic extension $\mathbb{Q}(\zeta_n)$ is equal to $\mathbb{Z}[\zeta_n]$. Such fields are said to be *monogenic*. From a computational point of view, this means that the algebraic integers of such fields admit very simple representations, and can be easily handled algorithmically. Alongside cyclotomic fields, all quadratic fields (i.e., extensions of the form $\mathbb{Q}(\sqrt{a})$ for $a \in \mathbb{Z}$) are also monogenic, however, this need not be the case for higher degree radical extensions. Examples of such non-monogenic fields are the cubic field $\mathbb{Q}(\sqrt[3]{198})$, or the biquadratic field $\mathbb{Q}(\sqrt{7}, \sqrt{10})$.

Because of the phenomena we just described, there are fewer established results in the radical setting compared to the results on cyclotomic identity testing. However, we are still

able to draw some parallels between the problems in the two contexts. We will now recall the state of the art in the radical world, defining the missing analogous problems for which we are not aware of any existing results in the literature along the way. For an illustration of the landscape, see Figure 1.2.

Radical identity testing for sparse expressions was first considered by Blömer in [43], where he studied the complexity of determining whether a linear combination of real radicals is equal to zero, that is, whether $S = \sum_{i=0}^{n} c_i \sqrt[d_i]{a_i}$ is zero, where c_i, d_i and a_i are integers given in binary. He gives a deterministic polynomial time algorithm for the problem, which relies on the fact that if $S = 0$, then there must exist two distinct radicals $\sqrt[d_i]{a_i}$ and $\sqrt[d_j]{a_j}$ such that $\sqrt[d_i]{a_i}/\sqrt[d_j]{a_j} \in \mathbb{Q}$. In other words, the radicals $R := \{\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}\}$ are linearly independent over $\mathbb{Q}$ if all possible pairs from R are linearly independent. The algorithm first partitions the radicals R into subsets $R_1, \ldots, R_h$ such that two radicals are in the same subset if and only if their ratio is rational. Suppose for simplicity that $\sqrt[d_i]{a_i} \in R_i$. In the second step the rational numbers $r_{ij} \in \mathbb{Q}$ such that if $\sqrt[d_i]{a_i}/\sqrt[d_j]{a_j} \in \mathbb{Q}$ then $\sqrt[d_i]{a_i}/\sqrt[d_j]{a_j} = r_{ij}$ are computed. Then S can be rewritten as

$$S = \sum_{i=0}^{h} \Big(\sum_{\sqrt[d_j]{a_j} \in R_i} c_j r_{ij} \Big) \sqrt[d_i]{a_i} = \sum_{i=0}^{h} c_i' \sqrt[d_i]{a_i}\,.$$

Since for every pair of different radicals in the set $R' = \{\sqrt[d_1]{a_1}, \ldots, \sqrt[d_h]{a_h}\}$ their ratio is not a rational number, $S = 0$ if and only if $c_i' = (\sum_{\sqrt[d_j]{a_j} \in R_i} c_j r_{ij}) = 0$ for all $i \in \{1, \ldots, h\}$. This can be verified in polynomial time, which completes the algorithm.

Blömer's approach was later extended in [44] to identity testing for sparse expressions of the form $\sum_{i=0}^{n} c_i \sqrt[d_i]{a_i}^{e_i}$, where c_i and a_i are integers given in binary and $\frac{e_i}{d_i} \in [0, 1]$ for all $i \in \{1, \ldots, n\}$. By adapting certain subroutines of Blömer's algorithm, the complexity bound was improved to $\mathbf{TC^0}$, which is considered to be one of the lowest classes of circuit complexity, and is included in $\mathbf{P}$. Note, however, that this result does not fully answer the radical analogue to sparse-CIT. To this aim, let us first formally define the *Sparse Radical Identity Testing* (sparse-RIT) problem as the problem of determining, given a sparse polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$, 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 written in binary, whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. That is, the question is to determine whether a sparse expression of the form $\sum_{i=0}^{n} c_i \sqrt[d_i]{a_i}^{e_i}$ where the integers c_i, a_i, d_i and e_i are given in binary, is equal to zero. Given such an instance, one may try to reduce the problem to an instance of the problem considered in [44], simply by writing

$$\sum_{i=0}^{n} c_i \sqrt[d_i]{a_i}^{e_i} = \sum_{i=0}^{n} c_i a_i^{t_i} \sqrt[d_i]{a_i}^{e_i'}$$

where $\frac{e_i}{d_i} = t_i + \frac{e_i'}{d_i}$ with $t_i \in \mathbb{Z}$ and $\frac{e_i'}{d_i} \in [0, 1]$. However, since a_i, d_i and e_i are assumed to be given in binary, the magnitude of t_i may be exponential in the size of the input, and the magnitude of $a_i^{t_i}$ doubly exponential in the size of the input. This means that the expression may not admit a sparse representation of size polynomial in the problem description, which would be required for the algorithm of [44] to run in polynomial time.

As in the cyclotomic case, we may again add an existential quantifier to the question, and pose the problem of *Sparse Generalised Radical Identity Testing* (sparse-GRIT): given a

sparse polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$, determine whether there exist radicals $\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}$ such that $f(\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}) = 0$. As discussed, the cyclotomic analogue of this problem is in **NP**, as the certificate for a positive instance of the problem is just the degree of the primitive root of unity that is the zero of the polynomial (which is polynomial in the size of the input), and the verification can be done in polynomial time by appealing to the algorithm of $\mathrm{sparse\text{-}CIT}$. Since the problem is also known to be **NP**, this upper bound is tight. In the radical case, the description of a certificate for a positive instance is again polynomial in the size of the instance, namely the integers $d_1, \ldots, d_k$ and $a_1, \ldots, a_k$ written in binary, such that $f(\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}) = 0$. However, as noted above, only restricted versions of the $\mathrm{sparse\text{-}RIT}$ problem are known to be in **P**, which implies that we can decide $\mathrm{sparse\text{-}GRIT}$ in **NP** under those same restrictions on the polynomial f.

Let us also see whether defining an analogue to the Torsion Point problem makes sense in this setting. We may try to define the *Radical Point* (RadP) problem as the problem of asking, given a system of multivariate polynomials $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_k]$ in sparse representation and a list of real radicals $\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}$, whether

$$f_1(\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}) = 0, \ \ldots, \ f_s(\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}) = 0$$

is satisfiable. However, notice that since the $\mathrm{sparse\text{-}GRIT}$ problem is already stated for multivariate polynomials, a (deterministic polynomial time) algorithm for $\mathrm{sparse\text{-}GRIT}$ can also be applied apply to the polynomials appearing as input of RadP individually and the complexities of the two problems are the same.

To the best of our knowledge, in contrast to the cyclotomic setting, neither the RadP problem nor the $\mathrm{sparse\text{-}GRIT}$ problem are known to be **NP**-hard. As the hardness proof for their cyclotomic equivalents in [35], they do not just carry over to the radical case. Let us note, however, that if we modify the Radical Point problem to ask whether a system of equations is satisfiable in radicals and their conjugates, as opposed to just real radicals, the variant can easily be seen to be **NP**-hard. To this end, we reduce the modified problem from the **NP**-complete problem $\mathrm{BOOLSYS}$. Given a system of equations of the form $x_i = true$, $x_i = \overline{x_j}$ and $x_i = x_j \vee x_k$ over n logical variables $x_1, \ldots, x_n$, the problem asks, whether the system admits a satisfying assignment. We take an instance of $\mathrm{BOOLSYS}$ and construct a sparse polynomial f in $n+1$ variables such that f vanishes on radicals $\{\sqrt{2}, -\sqrt{2}\}$ if and only if the system of Boolean equations is satisfiable. To this aim, we first construct a system of polynomials that is satisfiable over radicals if and only if the instance of $\mathrm{BOOLSYS}$ is positive. For every literal $x_1, \ldots, x_n$, we introduce an equation $x_i^2 = x_{n+1}^2$, and add the equation $x_{n+1}^2 = 2$. Then, for every formula $x_i = x_j \vee x_k$, we introduce an equation $4x_i x_{n+1} = (x_j + x_k)^2 + 2x_{n+1}(x_j + x_k) - 4x_{n+1}^2$. The constructed system is satisfiable for the values x_i taking values $\sqrt{2}$ and $-\sqrt{2}$ if and only if the Boolean system is satisfiable.

Let us now look at identity testing for expressions involving radicals represented via algebraic circuits. Here, the most general version of the problem, as defined before, is the *Radical Identity Testing* (RIT) problem. 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 written in binary, RIT asks whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. A first complexity bound for the problem can be inferred by a reduction to the existential theory of reals [2], which is known to be in **PSPACE**.

The reduction goes by introducing a new formal variable for every gate of the circuit, and adding the equations $x_i^{d_i} - a_i = 0$ and $x_i > 0$ for every radical to the formula. To decide RIT, it now suffices to check whether the resulting system of polynomial equalities and inequalities has a solution over the real numbers.

One may wonder whether it would be possible to avoid the order relation in the reduction and decide RIT by reducing the problem to determining the satisfiability of a system of polynomial equations. In this thesis we observe a fact that allows to do just that. In particular, we note that the Galois group of the underlying real field acts *jointly transitively* on the roots of the various equations $x^{d_i} - a_i = 0$. Intuitively speaking, this means that if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$, then the expression will be equal to zero if we replace each one of the input radicals $\sqrt[d_i]{a_i}$ by any of its d_i conjugates (which need not be real). We can thus again construct a system of polynomial equations by introducing a new formal variable for every gate of the circuit, add the equations $x_i^{d_i} - a_i = 0$ for every radical $\sqrt[d_i]{a_i}$, and verify whether it is satisfiable over $\mathbb{C}$. As mentioned above, the latter can be done in **AM** assuming GRH [3, 8], which places RIT in the polynomial hierarchy. We further use joint transitivity in order to generalise the technique introduced for ACIT and take the computation to a finite field $\mathbb{F}_p$ corresponding to a quotient of the radical number field of the expression by a suitable prime ideal. Here the transitivity condition allows 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 $f(\alpha_1, \ldots, \alpha_k) = 0$ in $\mathbb{F}_p$. Using this approach, we place RIT in **coNP** assuming GRH.

We further study the special case of RIT, where the radicals are square roots of prime numbers, written in binary, which we call 2-RIT. Using the same general technique, we place 2-RIT in **coRP** assuming GRH and in **coNP** unconditionally.

The case of Radical Identity Testing for expressions given by circuits that has been given most attention prior to our work is the problem of *Bounded Radical Identity Testing* (bounded-RIT). Here, the input to the problem again includes a bound on the degree of the polynomial represented by the circuit. Blömer showed in [42] that the problem can be decided in randomised polynomial time when the exponents d_i are given in unary. His algorithm relies on separation bounds for algebraic numbers, as discussed in connection to the bounded-CIT problem above. In particular, it relies on the fact that whenever an algebraic number α is non-zero, a random Galois conjugate α' of α has large absolute value with probability at least $\frac{2}{3}$. In the first step of the algorithm, pairwise coprime factors $m_1, \ldots, m_\ell$ of the input radicands $a_1, \ldots, a_k$ such that $\sqrt[d_i]{a_i} = \prod_{j=0}^{\ell} \sqrt[d_i]{m_j}^{e_{ij}}$ are computed. Then, using a clever trick, the algorithm randomly samples conjugates of the new radicals $\sqrt[d_i]{m_j}$, thus computing a conjugate of the original expression. If the expression is not identically zero, the computed conjugate will have large absolute value with high probability, and numerically approximating it to sufficient precision gives the answer to the problem. Now if the input radicals $\sqrt[d_i]{a_i}$ are given with both the radicands a_i and the exponents d_i given in binary, Blömer's algorithm no longer runs in polynomial time. The steps of the algorithm that increase in complexity are those prior to the random guessing of conjugates. In this thesis, we show that a slight modification of the initial steps of his algorithm allows us to place the general version of bounded-RIT in **coRP**.

Let us note that the work of Chen and Kao on PIT [41] also inherently solves the bounded-2-RIT problem (i.e. the variant of bounded-RIT where the radical inputs are

just square roots) in randomised polynomial time. As discussed above, they also rely on the same large conjugate result as Blömer.

The Sum of Square Roots problem. Expressions in radicals naturally arise in optimisation problems on graphs embedded in Euclidean space, such as the Euclidean Traveling Salesperson problem, which asks, given a list of cities and the distances between each pair of cities, what is the shortest possible route that visits each city exactly once and returns to the origin city. The problem is not known to belong to **NP**, but is easily seen to be in **NP** relative to the *Sum of Square Roots* problem. In the latter, the question is, given a list of positive integers $a_1, \ldots, a_k$ and signs $\delta_1, \ldots, \delta_k \in \{+, -\}$, to infer the sign of $\sum_{i=1}^{k} \delta_i \sqrt{a_i}$.

The problem has been conjectured to belong to **P**, but the best known complexity bound to date was given in [14, Corollary 1.6], showing it to be decidable in the counting hierarchy. The question of determining its precise computational complexity remains open since it was explicitly posed by Garey, Graham and Johnson [49] in 1976, and has been revisited in various works, such as [50, 51].

Besides its relation to the Euclidean Traveling Salesperson problem, the Sum of Square Roots problem has also been used as a tool for proving hardness and obtaining upper bounds in quantitative verification [52, 53, 54, 55], algorithmic game theory [56, 57, 58], formal language theory and logic [59, 60]. Improving its complexity would thus have great impact on a large number of problems all across theoretical computer science.

Let us note that a more general version of the problem is known as the PosSLP problem, which asks, given an integer represented by an algebraic circuit to determine whether it is positive. The is easily seen to belong to **PSPACE** by a reduction to the existential theory of the reals [2], and the current best complexity bound known for the problem is the counting hierarchy [14, Theorem 1.5].

On nested radicals and denesting. In this thesis, we focus on identity testing for the simplest kind of algebraic expressions involving radicals — those only containing unnested radicals; we do not consider expressions such as $\sqrt{5 + 4\sqrt{2}}$. The same holds for works we cited above, such as, e.g. [42]. There is, however, also a line of work dedicated to studying nested radicals. There, the identity problem most often considered is to determine whether a nested radical can be simplified to a radical expression involving only radicals of lower depth. Denesting radicals of bounded degree is considered in, e.g, [61] (for radical expressions of degree at most d for fixed d and depth 2) or in [62] (for expressions of degree at most d for fixed d and possibly greater depth). The denesting algorithms referenced here run in time polynomial in the description of the number field of the radicals. Note that denesting algorithms implicitly provide zero tests for nested radical expressions. However, denesting is a more general problem than zero testing, and those algorithms may thus be less efficient for the application in hand than zero testing algorithms based on, say, root separation bounds.

Polynomial factorisation as a technique to solving over number fields. Identity testing or searching for torsion points is closely related to a more general problem of inspecting whether a polynomial factors into any linear factors over $\mathbb{Z}$, $\mathbb{Q}$, a cyclotomic field, or more generally a number field. As opposed to the Torsion Point and the Radical Point problems we discussed above, where the aim is to determine the existence of points whose coordinates are all roots of unity or real radicals respectively, factoring over a (cyclotomic or radical) number field is as general as the HN problem over these fields.

When the polynomial is given in a dense representation, we can factor it using the well-known LLL algorithm, which was introduced in the early 80s [63]. For the case of sparsely represented polynomials, the first breakthrough result on the problem was given by Cucker, Koiran and Smale in 1997 [64]. They designed a deterministic polynomial time algorithm, which given a sparse univariate polynomial $f \in \mathbb{Z}[x]$ as input, computes all of its integer roots.

The authors first show that given a sparse polynomial $f \in \mathbb{Z}[x]$ and an integer $a \in \mathbb{Z}$, the sign of $f(a)$ can be computed deterministically in time polynomial in $size(f)$ and the bitsize of a. Next they prove that given $M \in \mathbb{Z}$, one can compute a list of subintervals of $[-M, M]$ with integer end points each containing at most one root of f. The algorithm then follows by noting that it suffices to compute the list of subintervals, and then verify the sign of f evaluated at the end points of the subintervals to find the roots. Furthermore, the authors conclude with an observation, which has later become known as the *Gap Theorem*: if $f = \sum_{i=0}^{n} c_i x^{d_i}$, and there exists d_k such that the gap between d_k and d_{k+1} is large enough (with the respect to the magnitude of the c_i's), then $a \in \mathbb{Z}$ with $|a| \geq 2$ is a root of f if and only if a is a root of both $g = \sum_{i=0}^{k} c_i x^{d_i}$ and $h = \sum_{i=k+1}^{d} c_i x^{d_i}$. In the case where the polynomials have a small number of terms compared to their degree, this simple fact can improve the complexity of their algorithm by first computing the roots of say g (or h) and then simply verifying whether h (or g in the opposite case) also vanishes on them.

The authors left open the problem of adapting the algorithm of finding *all* rational roots of a univariate polynomial in a sparse representation. The problem was answered positively by Lenstra in 1999 [65]. In fact, the author proves a result that is more general – given an algebraic number field K of degree at most m over $\mathbb{Q}$, a polynomial $f \in K[x]$, and a positive integer d, he exhibits a polynomial time algorithm that computes all irreducible factors of f in $K[x]$ of degree at most d. At the same time, this work is also a generalisation of [66], where the same author showed that the number of irreducible factors of f in $K[x]$ of degree at most d, counted with multiplicities, is bounded by a constant depending only on m, d and the number of non-zero terms of f. (Note that [66] essentially generalises Descartes' rule of signs which gives a bound on the number of real zeroes of univariate polynomial). The number field K is assumed to be represented by the means of an irreducible monic polynomial $h \in \mathbb{Z}[x]$ in dense representation, such that $K = \mathbb{Q}(\alpha)$ for a zero α of h. The algorithm works by first finding the cyclotomic factors (of degree polynomial in the problem description) of the polynomial, then computing a bound at which the polynomial should be split according to the Gap theorem, and splitting the polynomial. The resulting polynomials have few factors, and thus admit small dense representations. Computing their factorisation, which is the final step of the algorithm, can be done in polynomial time using the Euclidean algorithm.

In [67], Kaltofen and Koiran extended Lenstra's technique presenting algorithms to compute linear and quadratic irreducible factors of bivariate polynomials over the rationals. Both algorithms run in time polynomial in the size of the input; the algorithm computing linear factors is deterministic, and the algorithm finding quadratic factors is randomised (Monte Carlo). The authors further generalised their result in [68], where they give a randomised polynomial time algorithm computing all irreducible factors of degree at most d of sparse multivariate polynomials over algebraic number fields. We note here the generalisation is two-fold: the computed factors of degree at most d may belong to an arbitrary number fields (as opposed to a fixed one as above), and the input polynomial may be multivariate.

A few years later, a different line of work generalising Lenstra's approach was initiated. The aim was to simplify the above mentioned results, avoiding the deep number theoretic results on heights of algebraic numbers that some of them rely on. Chattopadhyay et al. [69] proposed a new Gap Theorem that does not depend on the height of an algebraic number, but rather on the valuation of the polynomial. (We recall that the valuation of a polynomial $f \in \mathbb{Z}[x]$ is the largest integer v such that x^v divides f.) In this work, similarly to Kaltofen and Koiran [67], the authors consider bivariate polynomials. Using the new Gap Theorem they give a deterministic polynomial time algorithm for computing irreducible multilinear factors of degree at most d of bivariate polynomials over algebraic number fields. As in Lenstra's work [65], the field in question is specified by a dense univariate polynomial.

This approach was further developed by Grenet [70, 71], who subsequently proposed an algorithm for computing factors of degree at most d of multivariate polynomials, running in time polynomial in d and the size of the polynomial, analogous to the generalisation [68]. The algorithm is valid for any field of zero characteristic. The new Gap Theorem that it is based on, allows the author to reduce the problem to several instances of the univariate case via the Newton polygon of the input polynomial. These algorithms are practical, and were implemented in [72].

Another aspect of factoring sparse polynomials that has been explored is whether the lower-degree factors also admit a succinct representation. In [73] it was shown that any factor of a sparse n-variate polynomial with at most s terms of individual degree bounded by d can itself have at most $s^{O(d^2 \log n)}$ terms. Here by the bound on the individual degree we mean that in all monomials in the factor, every variable x_i appears with exponent at most d. The authors noted that the best known lower bound for the sparsity is $s^{\log d}$ for fields of characteristic zero and about s^d for general fields. It has thus been conjectured that the upper bound could be improved to $s^{\mathrm{poly}}(d)$, which was further explored in [74]. The problem has also been considered for the case of circuits; recent works on the subject are, e.g. [75, 76].

Factoring polynomials over other fields. Across this section, we have seen that computing with polynomials is often done by reducing modulo a prime p and taking the computation to a finite fields $\mathbb{F}_p$. A significant body of work has also been dedicated to factoring polynomials over finite fields, see, e.g., [77] for a survey. More recently, the problem of factoring (or at least root counting) modulo composite numbers has also attracted attention. We refer the reader to the recent PhD thesis on the subject [78] for an overview of results

in the area.

Another line of work concerns finding real roots of polynomials, or more generally, determining intervals in which real roots of a polynomial appear. For examples of such work, see, e.g., [79] and the references therein.

1.2 Testing for the existence of zeros in algebraic expressions

We have just gone through an extensive overview of identity testing problems, which, given a polynomial and a possible solution, boils down to verifying whether the polynomial vanishes on the given input. We have seen that a first generalisation of the problem asks to determine, given a polynomial, whether it admits a solution in a given ring or field. In the second part of this thesis, we consider an even more general variant of the latter problem, namely, verifying whether a *system* of polynomials admits a solution in a given field.

The question has been considered by mathematicians for centuries. In 1893, David Hilbert showed a fundamental result, known as the *Hilbert's Nullstellensatz*, which gives a condition characterising when a system of polynomial equations is not satisfiable. Given a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = 0, \ \ldots, \ f_k(x_1, \ldots, x_n) = 0 \tag{1.1}$$

where $f_i \in K[x_1, \ldots, x_n]$ for K an algebraically closed field, the weak version of the Nullstellensatz says that the system is unsatisfiable if and only if there exist polynomials $g_1, \ldots, g_k \in K[x_1, \ldots, x_n]$ such that

$$\sum_{i=1}^{k} f_i g_i = 1 \ . \tag{1.2}$$

A naturally associated computational problem asks to determine whether a given family of polynomials $f_1, \ldots, f_k$ have a common zero. One version of this problem, denoted $\mathrm{HN}_{\mathbb{C}}$, asks to determine whether a given system of polynomial equations with integer coefficients admits a common solution over $\mathbb{C}$.

The characterisation given in Equation (1.2) essentially reduces $\mathrm{HN}_{\mathbb{C}}$ to an *ideal membership problem*, namely whether the constant 1 lies in the ideal generated by the f_i's. By a result of Mayr and Meyer [4], this places $\mathrm{HN}_{\mathbb{C}}$ in the complexity class **EXPSPACE**. On the other hand, it is easy to reduce the Boolean satisfiability problem to $\mathrm{HN}_{\mathbb{C}}$, making it at least **NP**-hard.

To this end, recall that a formula is said to be in conjunctive normal form (CNF) if it is a conjunction of clauses, where each clause is a disjunction of literals. The 3-SAT problem asks, given a formula φ in CNF, where each clause contains exactly 3 literals, whether φ admits a satisfying assignment. We take an instance of 3-SAT comprising a formula φ which is a conjunction of k clauses over n logical variables $x_1, \ldots, x_n$, and construct a

system of $n + k$ polynomials over n variables $x_1, \ldots, x_n$ that is satisfiable over $\mathbb{C}$ if and only if φ admits a satisfying assignment. For every variable appearing in φ, we introduce an equation $x_i(x_i - 1) = 0$, ensuring that the variables can only take values 0 or 1. The remaining k equations in the system represent each one clause of the formula φ, where we write x_i for every positive literal x_i in the formula, $(1 - x_i)$ for every negative literal $\overline{x_i}$, and replace every disjunction by a multiplication. Take for example the formula $\varphi := (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_3} \vee \overline{x_4})$. Determining whether φ admits a satisfying assignments reduces to verifying whether the system comprising $x_i(x_i - 1) = 0$ for all $i = 1, \ldots, 4$, and $x_1(1 - x_2)x_3 = 0$, $x_2(1 - x_3)(1 - x_4) = 0$ is satisfiable over $\mathbb{C}$.

The ideal membership problem is known to be **EXSPACE**-complete, which is far from the **NP**-lower bound for $\mathrm{HN}_{\mathbb{C}}$ we have just recalled. The challenge over the years has been to match the latter and improve the complexity of $\mathrm{HN}_{\mathbb{C}}$. A first improvement came with various versions of *Effective Nullstellensätze* [5, 6, 7], which gave single-exponential degree bounds on the g_i's. This in turn helps reduce the Nullstellensatz to solving a single-exponential-sized system of linear equations, placing $\mathrm{HN}_{\mathbb{C}}$ in **PSPACE**, since linear equations can be solved in polylogarithmic space. In particular, we introduce new variables for all coefficients of the g_i's and construct a system of equations from Equation (1.2) by adding one equation for each one of the monomials $x_1^{e_1} \cdots x_n^{e_n}$ appearing in (1.2). The new system has a solution if and only if $f_1, \ldots, f_k$ are unsatisfiable. Furthermore, the upper bound on the degree of the g_i's ensures that we had to introduce exponentially-many variables, implying that the size of the newly-constructed system is also exponential.

In an influential paper [3, 8], Koiran proved that $\mathrm{HN}_{\mathbb{C}} \in \mathbf{AM}$ assuming GRH. For any system $\mathcal{S}$ of polynomial equations with integer coefficients, the idea behind his approach is to examine the satisfiability of $\mathcal{S}$ in $\mathbb{F}_p$ for primes p. In particular, he shows that if the system is unsatisfiable in $\mathbb{C}$, it is satisfiable in $\mathbb{F}_p$ only for a small number of primes p, whereas if the system is satisfiable in $\mathbb{C}$, it will be satisfiable in $\mathbb{F}_p$ for many primes p. More precisely, there exist effective bounds A and x_0 such that if the system is unsatisfiable in $\mathbb{C}$, the number of primes $p \leq x_0$ such that the system is satisfiable in $\mathbb{F}_p$ is at most A. On the other hand, if the system is satisfiable in $\mathbb{C}$, the number of primes $p \leq x_0$ such that the system is satisfiable in $\mathbb{F}_p$ is shown to be at least $B = O(A \log A)$. Here $A < B$ are both numbers whose magnitude is a single-exponential function of the parameters (namely, number of variables, degree, bitsize of coefficients, and number of polynomial equations) of the system $\mathcal{S}$. Therefore to decide $\mathrm{HN}_{\mathbb{C}}$ it suffices to count the number of primes for which $\mathcal{S}$ is satisfiable over $\mathbb{F}_p$; the latter task has an easy **NP** algorithm when the primes are small (single-exponential in magnitude). This already implies a $\#\mathbf{P}^{\mathbf{NP}}$ algorithm for $\mathrm{HN}_{\mathbb{C}}$. By further observing that there is a sufficiently large gap between A and B, Koiran proves that it suffices to approximately count the number of primes following the techniques introduced by Stockmeyer [80], which yields the claimed upper bound for the problem.

$\mathbf{AM}$ is well-known to be included in the complexity class $\mathbf{RP}^{\mathbf{NP}}$. Since $\mathrm{HN}_{\mathbb{C}}$ is $\mathbf{NP}$-hard, Koiran's complexity upper bound is tight up to randomisation. In fact, no improvements have been shown since its publication in the late 90s. Furthermore, he exhibits an example showing that his technique cannot be easily modified to yield a **NP** algorithm for the problem. Intuitively speaking, the problem is that there may be exponentially many

primes such that an unsatisfiable system becomes satisfiable modulo p. This means that a certificate of a positive (i.e. satisfiable) instance of $\mathrm{HN}_{\mathbb{C}}$ cannot comprise solely polynomially many primes p and the corresponding solutions in $\mathbb{F}_p$ witnessing satisfiability of the system in $\mathbb{F}_p$.

The complexity of $\mathrm{HN}_{\mathbb{C}}$ has also been studied in relation to the *transcendence degree* of the input polynomials. Given polynomials $f_1, \ldots, f_k$, their transcendence degree r is defined as the size of any maximal subset of the polynomials that are algebraically independent. In [81], Garg and Saxena show that $\mathrm{HN}_{\mathbb{C}}$ can be solved in time single-exponential in the transcendence degree. They state their result in terms of *radical membership testing*. In particular, they show that given polynomials $f_1, \ldots, f_k$ of transcendence degree r, testing whether a polynomial f belongs to the radical ideal $\sqrt{\langle f_1, \ldots, f_k \rangle}$ can be performed in time polynomial in d^r, k and n, where d is the degree-bound on the polynomials and n is the number of variables. Furthermore, they show that when the system is unsatisfiable, the g_i's such that $f_1 g_1 + \cdots + f_s g_s = 1$ are of degree at most d^{r+1}. They also exhibit an algorithm computing the transcendence degree of the polynomials that runs in time polynomial in d^r, k and n. That is, the running time of the algorithm is bounded by a function in the size of the output.

Let us also note that $\mathrm{HN}_{\mathbb{C}}$ is the canonical $\mathbf{NP}_{\mathbb{C}}$-complete problem for the Blum-Shub-Smale computation model. We recall that a Blum-Shub-Smale machine is a Random Access Machine, where registers can store arbitrary complex (or real) numbers and that can compute rational functions over the complexes (respectively reals) in a single time step. See the survey [82] for more details on the model and known results related to it.

Hilbert's Nullstellensatz in proof complexity. Hilbert's Nullstellensatz has also found its application in the field of proof complexity, a branch of computational complexity theory that studies the complexity of theorem proving in proof systems, with the main complexity measure being the size of proofs. Propositional proof systems, in particular, are systems of proofs for the set of all unsatisfiable Boolean formulas. There are two types of proof systems: dynamic proof systems, which consist of a set of deduction rules, and every proof is a tree-like derivation using the rules, and static proof systems, where the formula is encoded in a suitable algebraic structure, and the proof boils down to exhibiting a property of the structure.

The *Nullstellensatz System* (NS) [83] is a static proof system based on Hilbert's Nullstellensatz. The NS proof system works by encoding a propositional formula into a system of polynomial equations $f_1, \ldots, f_k$ such that the system of polynomials is satisfiable if and only if the formula is satisfiable. A proof that a formula is unsatisfiable thus consists of the polynomials $g_1, \ldots, g_k$ witnessing that a system (more precisely, the encoding $f_1, \ldots, f_k$) is unsatisfiable. The complexity measures of such proofs are the size and degree of the polynomials.

Hilbert's Nullstellensatz over other fields and rings. The computational complexity of solving systems of polynomial equations depends on the underlying field or ring. Over the ring of rational integers $\mathbb{Z}$, for example, $\mathrm{HN}_{\mathbb{Z}}$ is also known as *Hilbert's tenth problem*.

After being open for 70 years, the problem was shown to be undecidable by Matiyasevich, Robinson, Davis and Putnam [84]. Whether one can decide the existence of a common zero in rational numbers, on the other hand, remains open [85]. Over the reals, the problem is a special case of the existential theory of the reals, and is thus decidable in **PSPACE** [2].

Over finite fields, the problem is **NP**-complete. Indeed, the hardness proof follows analogously to the one over $\mathbb{C}$, and the non-deterministic algorithm just guesses a solution and verifies it. For finite fields of small prime characteristic (e.g. $p = 2$) and low degree polynomials, the search variant of the problem has also been studied extensively, as it has applications in coding theory and cryptology. Most recently, the search variant of the Hilbert's Nullstellensatz problem has been inspected over the ring of integers modulo a prime power p^k [86]. Here, the authors no longer work over finite fields, but rather *Galois rings* (which are isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$ and admit fewer algorithmically-nice properties), proposing a randomised polynomial time algorithm for the case when the number of variables and the exponent k of the prime power is constant. HN over Galois rings may be seen as a first generalisation of the problem between its variants over finite fields and $\mathbb{Z}_p$. To the best of our knowledge, no nontrivial upper bounds for $\mathrm{HN}_{\mathbb{Z}_p}$ are known.

Related problems. The Hilbert's Nullstellensatz problem has been shown to relate to several other well-studied problems on polynomials. One such example is the problem of testing equivalence of polynomials under shifts, which given two polynomials $f, g \in R[x_1, \ldots, x_n]$ over a ring R, asks whether there exists a vector $(a_1, \ldots, a_n) \in R$ such that $f(x_1 + a_1, \ldots, x_n + a_n) = g(x_1, \ldots, x_n)$. In [87] this problem was shown to be at least as hard as checking if a given system of polynomial equations over $R[x_1, \ldots, x_n]$ has a solution, thus making it undecidable for the case when $R = \mathbb{Z}$. The problem is actually a special case of the *affine polynomial projection* problem. Formally, an m-variate polynomial f is said to be an affine projection of some n-variate polynomial g if there exists an $n \times m$ matrix A and an n-dimensional vector $\boldsymbol{b}$ such that $f(\boldsymbol{x}) = g(A\boldsymbol{x} + \boldsymbol{b})$. The latter is closely related to many well-known problems from arithmetic complexity theory, the most notable being the **VP** versus **VNP** problem, which is the arithmetic equivalent of the **P** versus **NP** problem in classical complexity theory. Concretely, a way to prove that **VP** is not equal to **VNP** would be to show that the permanent polynomial of an $n \times n$ matrix is not an affine projection of the determinant polynomial of some $m \times m$ matrix. For more details, we refer the reader to, e.g., [88].

Hilbert's Nullstellensatz is also related to the *tensor rank* problem, which asks, whether a given tensor with entries in a ring R has rank at most r. Let us recall that the *rank* of a tensor T is the smallest integer r such that T can be decomposed into a sum of r simple tensors. The tensor rank problem has been known to be **NP**-complete over finite fields since the late 80s [89], and has later been shown to be polynomial time equivalent to HN, see, e.g. [90, Theorem 3].

Geometric interpretation and dimension. Given a system of polynomial equations such as in Equation (1.1), when satisfiable, the polynomials define an *algebraic variety* in K^n. One of the most important parameters we can look at is its *dimension*. The complexity of computing the dimension of a variety was first studied by Giusti and Heintz [91], who

gave a randomised exponential time algorithm for the problem. Under GRH, Koiran [11] showed that the dimension of a variety can be computed in **AM**. More formally, he studied the $\mathrm{DIM}_{\mathbb{C}}$ problem, which asks, given an integer $d \leq n$, whether the variety $V \subseteq \mathbb{C}^n$ defined by polynomials $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ has dimension at least d, exhibiting a randomised polynomial time reduction of $\mathrm{DIM}_{\mathbb{C}}$ to $\mathrm{HN}_{\mathbb{C}}$. Note here that $\mathrm{HN}_{\mathbb{C}}$, which asks whether the variety defined by the given polynomials is non-empty, is precisely the problem $\mathrm{DIM}_{\mathbb{C}}$ specialised to $d = 0$.

The reduction works by first applying a random linear transformation A to the variety V such that with high probability the coordinates in which the image AV of the variety takes infinitely many values are $x_1, \ldots, x_d$, if the dimension of V is at least d. The second step of the reduction involves randomly choosing an integer point $(a_1, \ldots, a_d)$, and adding equations $x_1 = a_1, \ldots, x_d = a_d$ to the system defining the image AV. If $\dim V \geq d$, then with high probability this new system (with more polynomials but fewer variables) is satisfiable over $\mathbb{C}$, which can be verified using the **AM** algorithm for $\mathrm{HN}_{\mathbb{C}}$. The error analysis relies on a result from [92] on the proportion of integer points in a real variety. Applying it requires an intricate analysis of the number of connected components of the variety V embedded in $\mathbb{R}^{2n}$, as well as studying the Lebesgue measure of $V \cap \mathbb{R}^n$.

Koiran further proved that the $\mathrm{DIM}_{\mathbb{C}}$ problem is $\mathbf{NP}_{\mathbb{C}}$-complete in the Blum-Shub-Smale computation model, and in a later work [93] showed that the same holds for the problem of computing dimensions of constructible sets. Other related problems, such as computing the decomposition of a variety in equidimensional components, or determining the degree of variety are known to belong to **PSPACE** [94].

A significant body of literature has been devoted to *real* varieties as well. Koiran showed that given a set of polynomials with real coefficients, determining whether the real variety they define is of dimension at least d is $\mathbf{NP}_{\mathbb{R}}$-complete in the Blum-Shub-Smale computation model [95]. The problem of finding actually practical algorithms for computing the dimension of a real variety has also been considered, see, e.g., [96, 97].

Parametric versions of Hilbert's Nullstellensatz. In this thesis we study parametric versions of the HN problem. That is, given a system of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ we examine the existence and properties of solutions parametrised with respect to a subset of variables $\boldsymbol{x} := (x_1, \ldots, x_m)$ for $m < n$, or even a function in $\boldsymbol{x}$.

In this setting, we may regard $f_1, \ldots, f_k$ as parametric equations in $\mathbb{Q}(\boldsymbol{x})[x_{m+1}, \ldots, x_n]$. Such systems of polynomial equations with coefficients in $\mathbb{Q}(\boldsymbol{x})$ are central objects of study in algebraic combinatorics and in the theory of formal languages, where they are used to specify generating functions of combinatorial objects (see, e.g., the overviews in [9, 10]), and their solutions correspond to formal series in the variables $x_{m+1}, \ldots, x_n$.

Studying the complexity of problems over $\overline{\mathbb{Q}(\boldsymbol{x})}$ has also been used as a method to try to understand their analogues over $\mathbb{C}$ or $\mathbb{R}$. An example of such an application is the work of Kayal and Saha on the Sum of Square Roots problem [50]. Given an expression $S = \sum_{i=1}^{n} c_i \sqrt{f_i(x)}$, where the f_i are univariate polynomials not identically zero of degree at most d, they study the problem of determining whether, if $S \neq 0$, the maximum exponent of x which has a nonzero coefficient in the power series S is bounded by a polynomial in n

and the maximum degree of the f_i's. The idea behind their approach is to use such a bound on the valuation of the power series in order to deduce a separation bound for sums of square roots over $\mathbb{R}$.

Going back to systems of polynomials, let us note that the first effective versions of Hilbert's Nullstellensatz we cited above concerned explicit solutions over $\mathbb{C}$. An effective version for the parametric case of Hilbert's Nullstellensatz was first proven by Smietanski [98], who showed degree bounds when the polynomials have at most 2 parameters. The general case (for an arbitrary number of parameters) was considered in [99], where the authors showed single-exponential bounds on the degrees of the g_i's as well as the degrees of the parameters appearing in the coefficients of the g_i's. Analogously to the case over $\mathbb{C}$, these bounds allow to reduce $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to solving a single-exponential system of linear equations, placing the problem in **PSPACE**. In our work, we prove an improved bound of the problem, and observe its relation to the dimension problem over $\mathbb{C}$ discussed above.

In general, parametric solutions may be arbitrary algebraic expressions in the parameters $\boldsymbol{x}$ and need not admit representations that are easy to be handled computationally. One of the problems studied with respect to parametric systems is thus when they admit "nice" solutions. The paper [100], for example, studies a specific class of well-behaved parametric solutions that can be represented via rational functions in the parameters. The author exhibits bounds on the degrees of the polynomials that appear in such well-behaved solutions and, furthermore, gives a probabilistic algorithm for computing this type of solutions, running in time polynomial in the size of the output.

Parametric solutions of systems of polynomial equalities and inequalities were also considered in [101]. The author builds on the work of [102], computing solutions via the *discriminant variety* in time exponential in the size of the input. Finally, computing irreducible components of parametric algebraic varieties was considered in [103]; the proposed algorithm for the problem runs in time doubly exponential in the size of the input.

1.3 Testing for the existence of zeros in sequences

In the last part of this thesis, we turn our attention to the problem of determining whether a target value appears in a given hypergeometric sequence. The problem we consider fits into the more general landscape of zero testing for recursive sequences. Here the first class of sequences usually considered are sequences satisfying linear recurrences with constant coefficients, which we call *C-finite sequences*. They are also commonly referred to as Linear Recurrence Sequences (LRS for short) in the literature. Formally, an infinite sequence $\langle u_n \rangle_{n=0}^{\infty}$ over a field K is said to be C-finite if it satisfies a recurrence $u_n = \sum_{k=1}^{d} c_k u_{n-k}$, where $c_i \in K$ and $c_d \neq 0$. We call the number of previous terms d appearing in the recurrence relation defining an element u_n the *order* of the recurrence.

A fundamental result in the study of C-finite sequences is the Skolem-Mahler-Lech theorem, which states that the set $\{n \in \mathbb{N} \colon u_n = 0\}$ is a union of finitely many arithmetic progressions and a finite set. The theorem was first proven for sequences defined over the rationals by Skolem in the 1930s [104], then extended to sequences over algebraic numbers

by Mahler [105], and finally to all fields of characteristic zero by Lech [106]. The result was reproved several times, and later generalised to recurrences defined over fields of positive characteristic as well, see, e.g. [107, 108, 109, 110]. Linear algebraic and algebro-geometric interpretation of the theorem have also been explored, for example in [111]. All known proofs of the theorem and its variants rely on p-adic techniques, and none of them are constructive. That is, while the theorem describes the shape of the zero set of such sequences, its proofs give no indication on how to actually compute it, or determine whether it is non-empty. In the context of computation, this gives rise to a decision problem known as the *Skolem problem*, which asks, given a C-finite sequence $\langle u_n \rangle_{n=0}^{\infty}$, whether there exists $n \in \mathbb{N}$ such that $u_n = 0$.

The first positive decidability results for the problem appeared in the 1980s for sequences of order up to 4 [12, 13]. Notoriously, decidability for sequences of order 5 or more remains widely open to this day. There is, however, an ongoing sequence of work on the Skolem problem for various subclasses and generalisations of C-finite sequences, with positive decidability results often conditioned to number theoretical hypotheses. For more details, see the survey [112] by Ouaknine and Worrell and later works such as [113, 114, 115].

Let us now go back to our setting, where we consider sequences satisfying recurrences with polynomial coefficients. The first generalisation of the Skolem-Mahler-Lech theorem to P-finite sequences appeared in [116]. The authors show that for a sequence $\langle u_n \rangle_{n=0}^{\infty}$ satisfying a polynomial recurrence $u_n = \sum_{k=1}^{d} p_k(n) u_{n-k}$, under the assumption that p_d is a non-zero constant polynomial, the set $\{n \in \mathbb{N} : u_n = 0\}$ is the union of a finite set and finitely many arithmetic progressions. As in the linear setting, the proof relies on techniques from p-adic analysis, namely Strassman's Theorem (which, loosely speaking, asserts that convergent power series over $\mathbb{Z}_p$ are either identically zero or have only finitely many zeroes). The proof again is not constructive, and it remains open whether the result extends to general P-finite sequences.

From a computational point of view, one may consider the problem of determining whether there exists $n \in \mathbb{N}$ such that $u_n = 0$ for a P-finite sequence $\langle u_n \rangle_{n=0}^{\infty}$. Here we consider general P-finite sequences again, that is sequences satisfying polynomial relations

$$p_0(n)u_n + p_1(n)u_{n-1} + \cdots p_d(n)u_{n-d} = 0\,,$$

where $p_0(x)$ has non-negative integer zeros and $p_d(x)$ is not identically zero (but need not be constant) as defined in Section 2.4.1. Let us note that for hypergeometric sequences, that is, P-finite sequences of order 1, the problem is trivial. To see this, fix $\langle u_n \rangle_{n=0}^{\infty}$ where $p(n)u_n = q(n)u_{n-1}$ and note that if such an n exists, then the sequence is ultimately zero. This is the case if and only if $q(x)$ has a positive integer zero, which is easily decidable by verifying whether $q(n) = 0$ for all $n \in \mathbb{N}$ up to a certain bound depending only on the polynomial q.

A polynomially recursive sequence is said to be in *(hypergeometric) closed form* if it is the sum of hypergeometric sequences [117, Definition 8.1.1]. In this thesis, we study the problem of determining whether there exists $n \in \mathbb{N}$ such that $u_n = 0$, where u_n is the sum of two hypergeometric sequences. This is arguably the first case of P-finite sequences for which the zeroness problem is not trivially decidable. It is not difficult to show that

the problem reduces to the problem of verifying, given a hypergeometric sequence and a target value t, whether t appears in the sequence. To see this, fix hypergeometric sequences $\langle v_n \rangle_{n=0}^{\infty}$, and $\langle w_n \rangle_{n=0}^{\infty}$ with respective initial terms u_0, and v_0, satisfying

$$p(n)v_n = q(n)v_{n-1} \qquad \text{and} \qquad f(n)w_n = g(n)w_{n-1}.$$

We aim to decide whether 0 appears in the sequence $\langle u_n \rangle_{n=0}^{\infty}$ given by $u_n = v_n + w_n$.

Writing $v_n = v_0 \prod_{k=1}^{n} \frac{q(n)}{p(n)}$ and $w_n = w_0 \prod_{k=1}^{n} \frac{g(n)}{f(n)}$, notice that $u_n = 0$ if and only if

$$v_0 \prod_{k=1}^{n} \frac{q(n)}{p(n)} + w_0 \prod_{k=1}^{n} \frac{g(n)}{f(n)} = 0.$$

By multiplying out the denominators, we can write

$$v_0 \prod_{k=1}^{n} q(n)f(n) = -w_0 \prod_{k=0}^{n} g(n)p(n).$$

and finally rearrange the above equality as

$$\prod_{k=1}^{n} \frac{q(n)f(n)}{g(n)p(n)} = -\frac{w_0}{v_0}.$$

Thus asking whether $u_n = 0$ is equivalent to determining whether the target $-\frac{w_0}{v_0}$ appears in the hypergeometric sequence given by the shift quotient $\frac{q(x)f(x)}{g(x)p(x)}$ and initial term 1. We refer to the latter problem as Membership Problem for hypergeometric sequences, and study this formulation instead. In this thesis, we present decidability results for the problem when the sequences have rational parameters (that is, when the defining polynomials in the recurrence split over $\mathbb{Q}$). The approach was later extended to several classes of sequences with higher-degree algebraic parameters — we defer the discussion on these extensions to Section 5.4.

To the best of our knowledge, this is the first step towards testing zeroness for P-finite sequences, and the problem remains widely open for general sequences of order 2 or more.

Threshold problems for sequences. A related domain of study of sequences are threshold problems. Given a sequence of real numbers, the *Threshold Problem* asks whether every term in the sequence lies above a given threshold. A notable instance often considered is the *Positivity Problem*, which asks whether all terms of the sequence are positive. In fact, one can show that the Skolem Problem for C-finite sequences actually reduces to the Positivity Problem, entailing a quadratic increase in the order. Threshold problems find applications across many areas, such as biology, economics, software verification, probabilistic model checking, and more. From the point of view of program verification, for example, the sequence can be seen as a simple loop program, and deciding the Threshold Problem corresponds to determining whether a given loop program's variables remain above a fixed threshold before and after each iteration of the loop. In automated verification, deciding such problems can answer questions regarding program termination (e.g., Is the loop condition ever satisfied?), correctness and reachability (e.g., Is a *bad* state ever reached?).

As in the zero testing case, a significant body of work has been dedicated to studying the Positivity Problem for C-finite sequences. An example of such work is say [118], where decidability of both the Positivity and the Ultimate Positivity Problems is established for C-finite sequences of order 5 or less. Here the Ultimate Positivity Problem asks, given a sequence $\langle u_n \rangle_{n=0}^{\infty}$, whether there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $u_n > 0$.

How about P-finite sequences? Let us first look at order-1 P-finite sequence satisfying recurrences of the form $p(n)u_n = q(n)u_{n-1}$. It is not difficult to notice that since p and q are ultimately monotonic, the same will hold for the sequence $\langle u_n \rangle_{n=0}^{\infty}$. As long as the sequence is not ultimately zero (which we can decide, as discussed above), it will either be ultimately positive or ultimately negative. To determine the Positivity problem, it thus suffices to check for zeroness and then compute sufficiently many initial terms of the sequence until it stabilises.

As for order-2 P-finite sequences, the problem of deciding positivity has been considered by various different authors. A common thread to all the work that has been published on it seems to be that they all place syntactic restrictions on the degrees of the polynomial-coefficients involved in the recurrences, and give algorithms that are not guaranteed to terminate for all initial values of a given recurrence. In the work [119], the authors give partial algorithms for deciding Positivity Problem (as well as zeroness) for sequences of the satisfying recurrences of the form $u_n = p(n)u_{n-1} + q(n)u_{n-2}$ where the degree of q is smaller or equal to the degree of p. The work [120], for example, considers sequences satisfying recurrences of the form $r(n)u_n = p(n)u_{n-1} + q(n)u_{n-2}$, but the polynomial coefficients are assumed to have degree at most 1. The paper [121], later extended in [122] studies positivity for sequences satisfying balanced recurrences; a recurrence is said to be balanced if the leading and trailing coefficient have the same degree and all other coefficients are bounded by this degree. Given a converging hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ and a target value t, the sequence $u_n - t$ satisfies a balanced second order recurrence. One might hope that by deciding positivity of $u_n - t$, we could simply determine the Membership Problem for $\langle u_n \rangle_{n=0}^{\infty}$ and t. However, the algorithms given in [121] are only guaranteed to terminate for certain classes of sequences. As it turns out, these exclude precisely the instances of MP that we identify as the non-trivial cases in Section 5.2. Most recently, in [123], the problem of giving explicit positivity certificates for order-2 P-finite sequences was considered, again excluding the sequences corresponding to the non-trivial cases we study in this thesis.

Chapter 2

Preliminaries

2.1 Notation

Given a field K, we denote by $K[x]$ the ring of univariate polynomials with rational coefficients, and by $K(x)$ the field of univariate rational functions with rational coefficients.

We denote by $\mathbb{Z}$ for the ring of rational integers, and by $\mathbb{N}$ the positive integers. We write $\mathbb{Q}$ for the field of rational numbers, $\mathbb{R}$ for the field of real numbers, and $\mathbb{C}$ for the field of complex numbers.

We use $\sim$ to denote asymptotic equivalence. That is, we write $f(x) \sim g(x)$ if and only if $\lim_{x\to\infty} \frac{f(x)}{g(x)}$ exists and is equal to 1. We use the Landau's big O notation $O(\cdot)$ to denote that a function $f(x)$ is asymptotically bounded by $g(x)$. That is, we write $f(x) = O(g(x))$ is there exists $M \in \mathbb{R}_{>0}$ and $x_0 \in \mathbb{R}_{>0}$ such that $|f(x)| \leq Mg(x)$ for all $x \geq x_0$.

We denote by $\log$ the logarithm function with base 2 and by $\ln$ the natural logarithm.

Given a rational number $\frac{a}{b}$, we write $\mathrm{ht}(\frac{a}{b}) = \log \max\{|a|, |b|\}$ for its (logarithmic) height.

2.2 Complexity theoretical preliminaries

2.2.1 Representation of polynomials and models of computation

Let $X = \{x_1, \ldots, x_n\}$ be a set of commutative variables. Given an n-variate polynomial $f \in \mathbb{Z}[X]$ of degree d, one natural way to represent it using a computer is via a list of coefficients for every possible exponent vector $(e_{i,1}, \ldots, e_{i,n})$ with $\sum_{j=1}^{n} e_{i,j} \leq d$. We call this the *dense representation*. We define the *size* of the representation in this case to be the number of possible monomials of total degree at most d (which is equal to $\binom{n+d}{d}$) alongside the bitsize of the corresponding coefficients. The size thus upper-bounds the degree and

the (logarithmic) height of the polynomial. The latter is defined as the maximum height its coefficients. For polynomials which have many zero terms, such a representation may seem wasteful, which leads to the following, alternative representation.

The *sparse (lacunary) representation* of an n-variate polynomial f is a list of t non-zero terms $(c_0, e_{2,1}, \ldots, e_{0,n}), (c_1, e_{1,1}, \ldots, e_{1,n}), \ldots, (c_t, e_{t,1}, \ldots, e_{t,n})$ such that

$$f(X) = \sum_{i=0}^{t} c_i x_1^{e_{i,1}} \cdots x_n^{e_{i,n}},$$

with each coefficient c_i non-zero and all exponent tuples $(e_{i,1}, \ldots, e_{i,n}) \in \mathbb{N}^n$ distinct. We call the number of non-zero terms t the *sparsity* of the polynomial. We define the *size* of the representation as

$$size(f) = \sum_{i=1}^{t} (size(c_i) + size(e_{i,1} \cdots e_{i,n} + 2))$$

where the size of an integer refers to its logarithmic size. The degree of the polynomial can be exponential in the sparsity. Let us now look at a model of computation which subsumes the sparse representation, and allows for an efficient representation of an even larger class of polynomials.

An *algebraic circuit* over X is a directed acyclic graph with labelled vertices and edges. Vertices of in-degree zero (leaves) are labelled with the constants $0, 1$ or with variables in X; and the remaining vertices have labels in $\{+, -, \times\}$. Each gate of such a circuit represents a polynomial in $\mathbb{Z}[X]$. There is a unique vertex of out-degree zero which determines the output of the circuit, an n-variate polynomial, computed in an obvious bottom-up manner. The *size* of a circuit is the number of its gates; see Figure 2.1. 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 bitsize of the coefficients of a polynomial represented by a circuit is at most exponential in the size of the circuit.

The following proposition shows that circuits can be exponentially more succinct than polynomials.

Proposition 2.1. *Given $m \in \mathbb{N}$, there is a circuit of size $O(\log m)$ that represents the polynomial $\sum_{i=0}^{m} x^i$.*

Proof. Define $S_m := \sum_{i=0}^{m} x^i$. Note that

$$\begin{bmatrix} S_{m+1} \\ 1 \end{bmatrix} = \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} S_m \\ 1 \end{bmatrix}$$

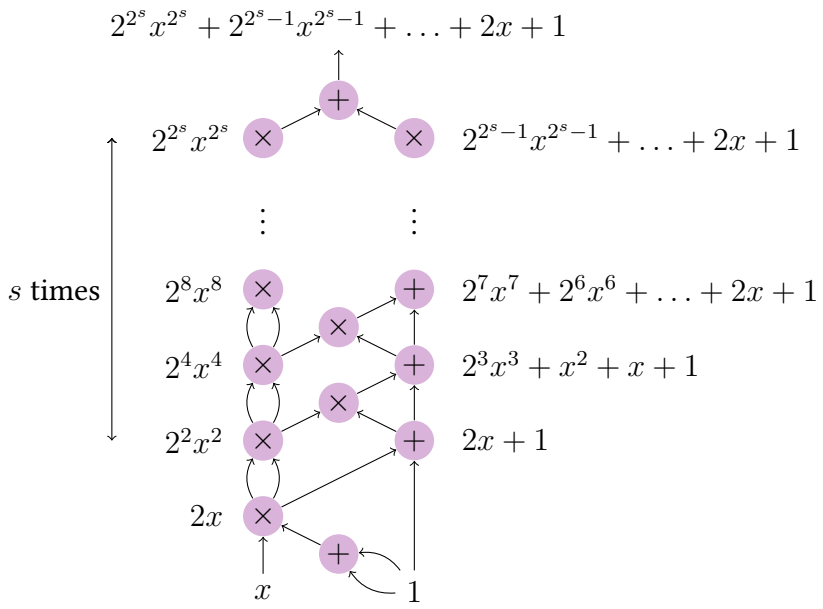

Figure 2.1 – An algebraic circuit representing the polynomial $\sum_{i=0}^{2^s} 2^i x^i$ of size $3s+2$. This is a modified case of Proposition 2.1 with $m = 2^s$.

and thus

$$\begin{bmatrix} S_m \\ 1 \end{bmatrix} = \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix}^m \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

for all m. Since exponentiation of a matrix to the power m can be implemented via $O(\log m)$ steps of repeated squaring, the statement follows.

□

As a conclusion to this section, let us note that while algebraic circuits can be used to represent polynomials of degree and with the number of monomials exponential in the size of the circuit, as well as with coefficients of magnitude doubly exponential in the size of the circuit, not every polynomial of this size admits a small circuit. The question of whether a polynomial f admits a succinct representation in the form of an algebraic circuit is the main object of study in the field of arithmetic complexity theory.

2.2.2 Complexity classes

In this section we recall the definitions of the complexity classes we use in our results. For more details and extended definitions, we refer the reader to a standard reference, such as [124].

In computational complexity theory, *polynomial time* (**P**, also **PTIME**) is the class of computational problems that are considered to be "efficiently solvable" or "tractable". For-

mally, **P** contains all decision problems that can be solved by a deterministic Turing machine in polynomial time. In terms of languages, a language L is in **P** if and only if there exists a deterministic Turing machine M, such that M runs for polynomial time on all inputs, and for all x in L, M outputs "yes", and for all x not in L, M outputs "no".

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

The complexity class *randomised polynomial time* (**RP**) is the class of problems for which there is a probabilistic Turing machine that runs in polynomial time in the input size, always returns "no" if the correct answer is "no", and, if the correct answer is "yes", returns "yes" with probability at least $\frac{1}{2}$. Analogously, **coRP** is the class of problems whose complements are in **RP**. That is, problems for which there is a probabilistic Turing machine that runs in polynomial time in the input size, always returns "yes" if the correct answer is "yes", and, if the correct answer is "no", returns "no" with probability at least $\frac{1}{2}$. The class *bounded-error probabilistic polynomial time* (**BPP**) is the class of decision problems solvable by a probabilistic Turing machine in polynomial time with an error probability bounded by $\frac{1}{3}$ for all instances. In terms of languages, a language L is in **BPP** if and only if there exists a probabilistic Turing machine M, such that M runs for polynomial time on all inputs, and for all x in L, M outputs "yes" with probability at least $\frac{2}{3}$, and for all x not in L, M outputs "yes" with probability at most $\frac{1}{3}$.

The complexity class *polynomial space* (**PSPACE**) is the class of all decision problems that can be solved by a Turing machine using a polynomial amount of space.

An *oracle machine* M^B is a Turing machine M equipped with an oracle B to which M may ask membership queries on a special oracle tape. The oracle B is a black-box able to solve a specific problem (e.g., a decision problem or a function problem) in a single operation. We write A^L for the complexity class of decision problems solvable by an algorithm in class A with an oracle for a language L. We extend the notation to a set of languages B (or a complexity class B), by writing $A^B = \bigcup_{L \in B} A^L$.

The *polynomial hierarchy* (**PH**) is a hierarchy of complexity classes that generalises the classes **NP** and **coNP**. We define $\Delta_0^{\mathbf{P}} := \Sigma_0^{\mathbf{P}} := \Pi_0^{\mathbf{P}} := \mathbf{P}$. Then for $i > 0$, we define

$$\Delta_{i+1}^{\mathbf{P}} := \mathbf{P}^{\Sigma_i^{\mathbf{P}}} \qquad \Sigma_{i+1}^{\mathbf{P}} := \mathbf{NP}^{\Sigma_i^{\mathbf{P}}} \qquad \Pi_{i+1}^{\mathbf{P}} := \mathbf{coNP}^{\Sigma_i^{\mathbf{P}}} .$$

PH is known to be included in **PSPACE**.

The *Arthur-Merlin protocol* (**AM**) is an interactive proof system, formalising the interaction between a prover P and a verifier V such that the prover is trying to convince the verifier of the truth of some statement x. In this case, Merlin is the (all-powerful, i.e.,

nondeterministic) prover trying to convince the (polynomial-time) verifier Arthur that a statement is true by providing a proof π for it. Here, additionally, Arthur has access to randomness, and may use some public random bits in order to verify the statement. For the class **AM** specifically, Arthur acts first by sending its random bits to Merlin, then Merlin sends a proof that uses these random bits, and Arthur verifies it. Formally, a language L is in **AM** if there exists a deterministic algorithm V (Arthur, the verifier) running in polynomial time (in the length of its first input) such that if $x \in L$, then for all random strings r there exists a proof π such that $V(x, r, \pi) = 1$, and if $x \notin L$, then $\Pr[\exists \pi : V(x, r, \pi) = 1] \leq \frac{1}{2}$. The class **AM** is known to belong to the second level of the polynomial hierarchy, in particular, $\mathbf{AM} \subseteq \mathbf{RP}^{\mathbf{NP}} \subseteq \mathbf{\Pi_2^P}$. Both **NP** and **BPP** are contained in **AM**.

2.3 Algebraic preliminaries

2.3.1 Ring theory

In this thesis we assume all rings to be commutative with unity.

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.

The *radical* of an ideal I of R is the set

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{N}\}.$$

Equivalently, the radical of I can be defined as the intersection of all prime ideals P of R containing I.

An *R-module* over a ring R is a generalisation of the notion of vector space over a field. Formally, given a commutative ring R, an R-module is an additive abelian group M equipped with a map $\cdot : R \times M \to M$, called *scalar multiplication*, such that for all $r, s \in R$ and all $m, n \in M$, we have $(r \cdot s) \cdot m = r \cdot (s \cdot m)$, $(r + s) \cdot m = r \cdot m + s \cdot m$, $r \cdot (m + n) = r \cdot m + r \cdot n$, and $1 \cdot m = m$.

2.3.2 Algebraic number theory

In this and the following two sections we recall some important definitions concerning algebraic number fields and their Galois groups. For more details, we refer the reader to [125, 126].

A complex number α is *algebraic* if it is a root of a univariate polynomial with integer coefficients. The minimal 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, denoted by $\deg \alpha$, 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 are algebraic numbers; this means that the set of all algebraic numbers is a *field*, commonly denoted by $\overline{\mathbb{Q}}$. The sum, the difference, and the product of two algebraic integers is again an algebraic integer; the set of all algebraic integers forms a ring. Complex numbers that are not algebraic, such as π and e, are called *transcendental numbers*.

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 $\mathbb{Q}$. We further denote by $\mathcal{O}_K$ the subring of K comprised by the algebraic integers in K. The ring $\mathcal{O}_K$ is a finitely generated free abelian group.

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

An *order* $\mathcal{O}$ in a number field K is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank $[K : \mathbb{Q}]$. Since $\mathcal{O}_K$ is also a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$, it follows from the structure theorem for $\mathbb{Z}$-modules that the quotient $\mathcal{O}_K/\mathcal{O}$ is a finite abelian group. The order of this quotient, denoted $[\mathcal{O}_K : \mathcal{O}]$, is called the *index* of $\mathcal{O}$ in $\mathcal{O}_K$. It is known that $m\mathcal{O}_K \subset \mathcal{O}$ for $m = [\mathcal{O}_K : \mathcal{O}]$. For example, $\mathbb{Z}[2i] = \mathbb{Z} + \mathbb{Z}2i$ 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 nth root of unity and for each $k < n$, $\zeta^k \neq 1$, then we call it a *primitive nth root of unity*. We can always choose a primitive nth root of unity by setting $\zeta_n = e^{2i\pi\frac{k}{n}}$ for k with $k \in \mathbb{Z}_n^*$. The nth *cyclotomic polynomial*, for any positive integer n, is the unique irreducible polynomial $\Phi(x) \in \mathbb{Z}[x]$ that is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$. The nth cyclotomic polynomial Φ_n is the minimal polynomial of a primitive nth root of unity, and its roots are all nth primitive roots of unity. The number field $\mathbb{Q}(\zeta_n)$ is an extension of $\mathbb{Q}$ obtained by adjoining ζ_n to Q; the degree $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ of the extension is 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.

2.3.3 Galois theory

An algebraic field extension K/L is *normal* (we say 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 separable. A *Galois extension* is an algebraic field extension that is normal and separable. In other words, a field extension K/L is Galois if it is the splitting field of some polynomial over L. If K'/L is a separable field extension, the *Galois closure* K of K' over L is a field K that is a Galois extension of L and is minimal in that respect, i.e., no proper subfield of K containing K' is normal over L.

Separable (and hence also Galois) extensions admit the following important property.

Theorem 2.2 (Primitive Element Theorem)**.** *Let K/L be a separable extension of finite degree. Then $K = L(\theta)$ for some $\theta \in K$; that is, the extension is simple and θ is a primitive element.*

The proof of the Primitive Element Theorem is constructive (see, for example, [127, Theorem 4.1.8] or [128, Theorem 5.1]), and computes the primitive element θ as a linear combination of the generators of the finite extension. That is, if $K := L(\alpha_1, \ldots, \alpha_k)$, then $\theta = \sum_{i=1}^{k} c_i \alpha_i$. The computation of θ is 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 is obtained. Furthermore, one can show that only finitely many combinations of the constants c_i fail to generate a primitive element for the field extension K. In particular, if L is an extension of $\mathbb{Q}$, the constants can be chosen in $\mathbb{Z}$, as summarised in the following lemma (which is a generalisation of [129, Proposition 6.6]).

Lemma 2.3. *Let L be an extension of $\mathbb{Q}$, and K/L an extension of finite degree. Let $\alpha, \beta \in K$ be algebraic elements of respective degrees ℓ and m over L. There exists an integer $c \in \{1, \ldots, \ell^2 m^2 + 1\}$ such that $\alpha + c\beta$ is a primitive element for $L(\alpha, \beta)$.*

Proof. Let p and q be minimal polynomials of α and β over L, and let F be a splitting field for pq containing L. Let $\alpha_1 = \alpha, \ldots, \alpha_\ell$ be the roots of p in F and let $\beta_1 = \beta, \ldots, \beta_m$ be the roots of q in F.

Notice that for $j \neq 1$, we have $\beta_j \neq \beta$ and thus the equation

$$\alpha_i + X\beta_j = \alpha + X\beta\,,$$

has exactly one solution, namely $X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$. By choosing $c \in L$ different from any of these solutions, we obtain that

$$\alpha_i + c\beta_j \neq \alpha + c\beta \text{ unless } i = j = 1.$$

Furthermore, notice that the set of values $\frac{\alpha_i - \alpha_r}{\beta_s - \beta_j}$ with $s \neq j$ consists of $\binom{\ell}{2} \cdot \binom{m}{2}$ values from F. Hence c can be chosen in the set $\{1, \ldots, \ell^2 m^2 + 1\}$.

Now let $\theta = \alpha + c\beta$. We will show that $L(\alpha, \beta) = L(\theta)$. To this aim, note that the polynomials $q(x)$ and $p(\theta - cx)$ have coefficients in $L(\theta)$ and both have β as a root, since $q(\beta) = 0 = p(\alpha) = p(\theta - c\beta)$. Furthermore, β is their only common root, since c was chosen such that $\theta - c\beta_j \neq \alpha_i$ unless $i = j = 1$. It follows that $\gcd(q(x), p(\theta - cx) = x - \beta$. Hence $\beta \in L(\theta)$, implying that $\alpha = \theta - c\beta \in L(\theta)$. □

Given a Galois extension K/L, the *Galois group* of K/L, denoted by $\mathrm{Gal}(K/L)$ is the group of automorphisms of K that fix L pointwise. That is, the group of all isomorphisms $\sigma : K \to K$ such that $\sigma(x) = x$ for all $x \in L$.

Fix α to be an algebraic number 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 $k \in \mathbb{Z}_n^*$ (i.e., $\gcd(k, n) = 1$); and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ includes all automorphisms σ defined by $\sigma(\zeta_n) = \zeta_n^k$ for $k \in \mathbb{Z}_n^*$.

Given a separable algebraic field extension K/L, every $\alpha \in K$ defines an L-linear map of the L-vector space K into itself

$$\begin{aligned} \mu_\alpha \; &: K \to K \\ &x \mapsto \alpha x \end{aligned}$$

We define the *norm* of $\alpha \in K/L$ by

$$\mathrm{N}_{K/L}(\alpha) = \det(\mu_\alpha)\,.$$

If K/L is Galois, then the norm of α can equivalently be defined by

$$\mathrm{N}_{K/L}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/L)} \sigma(\alpha)\,.$$

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 $\mathrm{N}(\alpha) = (a + bi)(a - bi) = a^2 + b^2$. Recall that the norms of all Galois conjugates are equal, and the norm of an algebraic integer is always a rational integer.

The *trace* of $\alpha \in K/L$ is defined by

$$\mathrm{Tr}_{K/L}(\alpha) = \mathrm{tr}(\mu_\alpha)\,.$$

If K/L is Galois, then the trace of α can equivalently be 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 $\mathcal{O}_K$ of 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 as

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

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

2.3.4 Ramification theory

Given a number field K, the ring of integers $\mathcal{O}_K$ may not be a unique factorisation domain. However, we do have unique factorisation of ideals into products of prime ideals. Let $p \in \mathbb{Z}$ be a rational prime and assume K to be a Galois extension of $\mathbb{Q}$ of degree n. The ideal $p\mathcal{O}_K$ may not be prime in $\mathcal{O}_K$, but does factorise into prime ideals as

$$p\mathcal{O}_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_g^e. \tag{2.1}$$

For all prime ideals $\mathfrak{p}_i$ in the equation above, we have that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and we say that $\mathfrak{p}_i$ *is above* p.

Note that in the ring of integers of a number field, all prime ideals are maximal, hence all $\mathfrak{p}_i$'s are also maximal ideals of $\mathcal{O}_K$. In general, given a commutative ring R and a maximal ideal $\mathfrak{m}$ of R, the *residue field* is the quotient $k = R/\mathfrak{m}$. Now, given a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is an $\mathbb{F}_p$-vector space of finite dimension. The *residual class degree* (*inertial degree*), denoted $f_\mathfrak{p}$, is the dimension of the $\mathbb{F}_p$-vector space $\mathcal{O}_K/\mathfrak{p}$, that is,

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

If K is a Galois extension, the residue class degrees of each one of the $\mathfrak{p}_i$'s appearing in (2.1) are equal, and we denote them by f. We call e the *ramification index* of the prime p, and we have that $efg = n$.

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

Whether or not a prime is ramified is directly related to the discriminant of the field.

Theorem 2.4. *Let K be a number field. If p is ramified, then p divides the discriminant Δ_K.*

For the Gaussian integers, the ideals $2\mathbb{Z}[i]$ and $5\mathbb{Z}[i]$ are not prime ideals and have respective factorisations $2\mathbb{Z}[i] = \mathfrak{p}^2$ 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.

2.3.5 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., [130].

Let p be a prime. We denote by $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ the p-adic valuation on $\mathbb{Q}$. Recall that for a non-zero rational number x, the valuation $v_p(x)$ is the unique integer such that x can be written in the form $x = p^{v_p(x)}\frac{a}{b}$ with $p \nmid ab$. Following the standard convention, we define $v_p(0) := \infty$.

The field $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$, given by $|x|_p = p^{-v_p(x)}$. We denote by $\mathbb{Z}_p$ the valuation ring $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. This is the local ring with unique maximal ideal generated by p. A basic result about $\mathbb{Q}_p$ is Hensel's lemma.

Lemma 2.5 (Hensel). *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 a unique $x \in \mathbb{Z}_p$ 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 $\mathcal{O}_K$ 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 $K_\mathfrak{p}/\mathbb{Q}_p$, which is the completion of K with respect to the absolute value $|\cdot|_\mathfrak{p}$. Equivalently, $K_\mathfrak{p}/\mathbb{Q}_p$ can be obtained by adjoining the generators of K over $\mathbb{Q}$ to $\mathbb{Q}_p$.

The extension $K_\mathfrak{p}/\mathbb{Q}_p$ 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 $\mathcal{O}_K$, we define the *decomposition group* $D_\mathfrak{p}$ of $\mathfrak{p}$ to be the set of all automorphisms of $\mathrm{Gal}(K/\mathbb{Q})$ 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; see, e.g., [131, Proposition 8.10].

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

This entails that 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 $\mathcal{O}_K$.

2.3.6 Prime density

In this section we briefly recall well-known results on the distribution of prime numbers which we use in our proofs. We only give the asymptotic versions of the results, and defer the concrete effective statements we require in our proofs to later chapters.

We denote by $\pi(x)$ the number of primes less than or equal to x. The Prime Number Theorem describes the asymptotic distribution of the prime numbers among the positive integers, formalising the intuitive idea that primes become less common as they become larger.

Theorem 2.6 (Prime Number Theorem). *The prime counting function π is asymptotically equivalent to the function $\frac{x}{\ln x}$, that is, $\pi(x) \sim \frac{x}{\ln x}$.*

A generalisation of the Prime Number Theorem for primes in arithmetic progressions was first proved by Dirichlet, showing that arithmetic progressions also contain infinitely many primes.

Theorem 2.7 (Dirichlet). *Given coprime numbers $a, n \in \mathbb{N}$, there are infinitely many primes of the form $n \cdot k + a$ for $k \in \mathbb{N}$.*

Analogous to the assertion of the Prime Number Theorem, primes in arithmetic progressions also get less frequent. Given $n \in \mathbb{N}$, the number of arithmetic progressions of the shape $n\mathbb{N} + a$ for $a \in \{1, \dots, n-1\}$ that differ by infinitely many terms is given by Euler's totient function $\varphi(n)$. Thus the proportion of primes in each of those is $\frac{1}{\varphi(n)}$. Given coprime numbers $a, n \in \mathbb{N}$ with $a < n$, we write $\pi_{n,a}(x)$ for the number of primes less than x that are congruent to a modulo n. Combining the observation on the number of distinct arithmetic progressions with the Prime Number Theorem, the function $\pi_{n,a}(x)$ is asymptotically equivalent to $\frac{x}{\varphi(n) \ln x}$.

Another generalisation of the Prime Number Theorem concerns the density of primes splitting in a certain pattern in the ring of integers $\mathcal{O}_K$ of a finite Galois extension K/L. We recall that a set of primes S is said to have *(natural) density* δ if

$$\frac{\#\{p \leq x \ : \ p \in S\}}{\#\{p \leq x \ : \ p \text{ prime}\}} \to \delta \text{ for } x \to \infty \,.$$

Chebotarev [132] proved that the different classes of splitting patterns correspond to conjugacy classes of the Galois group $\mathrm{Gal}(K/L)$ of K and their density relates to the ratios of automorphisms corresponding to the given class. The statement of his theorem, in particular, is in terms of the conjugacy classes given by the Frobenius endomorphism. We recall that given a prime p, the Frobenius endomorphism maps every element to its pth power. The Frobenius conjugacy class $F_\mathfrak{p}$ of a prime ideal $\mathfrak{p}$ is the class of automorphisms $\sigma \in D_\mathfrak{p}$ that act as the Frobenius automorphism on the residue field $\mathcal{O}_K/\mathfrak{p}$.

Theorem 2.8 (Chebotarev). *Let K be a finite Galois extension of a number field L with Galois group G. Let X be a subset of G that is stable under conjugation. The set of primes $\mathfrak{p}$ of L that are unramified in K and whose associated Frobenius conjugacy class $F_\mathfrak{p}$ is contained in X has density $\frac{|X|}{|G|}$.*

In our results, we generally rely on primes that split completely in K. As it turns out, those primes correspond to the conjugacy class $\{id\}$ containing solely the identity element id of $\mathrm{Gal}(K/L)$. The asymptotic version of the theorem then asserts that the set of completely split primes has density $\frac{1}{|\mathrm{Gal}(K/L)|}$.

2.3.7 Algebraic geometry

In this section we introduce some of the basic definitions and results from algebraic geometry we use. For a more detailed introduction we refer the reader to, e.g., [133, 134].

An *(affine) algebraic set* or *affine (algebraic) variety* is the set of common zeroes of a finite collection of polynomials S, i.e., a set of the form

$$V(S) = \{x \in K^n \colon \forall p \in S \,.\, p(x) = 0\}$$

where $S \subseteq K[x_1, \dots, x_n]$. For an arbitrary S, $V(S) = V(I)$, where I is the ideal generated by S.

Algebraic sets are equipped with a topology called the *Zariski topology*, which is defined by specifying its closed sets. Given an algebraic set $V \subseteq K^n$, the Zariski topology on V has as closed sets all the algebraic subsets of V, i.e., those sets $A \in V$ that are themselves algebraic sets in K^n. The *Zariski closure* of a subset W of an algebraic set $V \subseteq K^n$, denoted $\overline{W}$, is the smallest algebraic subset of V, such that $W \subseteq \overline{W}$.

An algebraic set V is said to be *irreducible* if it is not the union of two proper closed subsets. In other words, $V \in K^n$ is irreducible if for all algebraic subsets $A, B \subseteq V$ such that $V \subseteq A \cup B$, we have either $V \subseteq A$ or $V \subseteq B$. Note that in some literature, irreducible algebraic sets are called affine varieties, while we have chosen to follow the alternative convention and defined affine (algebraic) varieties to be algebraic sets.

Given a variety $V \subset K^n$, we define

$$I(V) = \{f \in K[x_1, \ldots, x_n] \colon f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\},$$

that is, $I(V)$ is the ideal of all polynomials simultaneously vanishing on V.

Hilbert's Nullstellensatz is a fundamental result in algebraic geometry that asserts that the ideal of a variety is *radical*.

Theorem 2.9 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field.*

1. *If $J \subsetneq K[x_1, \ldots, x_n]$ then $V(J) \neq \emptyset$.*
2. *$I(V(J)) = \sqrt{J}$; in other words, for $f \in K[x_1, \ldots, x_n]$,*

$$f(P) = 0 \text{ for all } P \in V \iff f^k \in J \text{ for some } k \in N.$$

Given an affine variety $V \in K^n$, the quotient ring $K[x_1, \ldots, x_n]/I(V)$ is called the *coordinate ring* of V. If V is irreducible, then $I(V)$ is prime and its coordinate ring $K[V]$ is an integral domain. We denote its field of fractions by $K(V)$ and call it the *function field* of the variety.

If V and W are subvarieties of K^n and K^m respectively, then a *regular map* $f \colon V \to W$ is the restriction of a polynomial map $K^n \to K^m$. Explicitly, it has the form $f = (f_1, \ldots, f_m)$ where the f_i's are in the coordinate ring $K[V]$ of V. A rational function $f \in K(V)$ is *regular at* $a \in V$ if it can be written as $f = \frac{g}{h}$ with $g, h \in K(V)$ and $h(a) \neq 0$. A rational function $f \in K(V)$ that is regular at all points of a closed subset of V is a regular map, i.e., $f \in K[V]$.

The *tangent space* to an affine variety V at a point a, denoted $T_{V,a}$ is defined as the set of all lines through a tangent to V.

Given an irreducible affine variety V, the *local ring* of V at point $a \in V$, denoted $\mathcal{O}_a$, is defined to be the subring of the function field $K(V)$ consisting of all functions $f \in K(V)$ that are regular at a. We denote by $\mathfrak{m}_a$ the maximal ideal of $\mathcal{O}_a$. The tangent space $T_{V,a}$ at a point a is isomorphic to the vector space of all linear forms on $\mathfrak{m}_a/\mathfrak{m}_a^2$ (i.e. the dual space of $\mathfrak{m}_a/\mathfrak{m}_a^2$). The map d_a defines an isomorphism of the vector spaces $\mathfrak{m}_a/\mathfrak{m}_a^2$ and $T_{V,a}^*$. The vector space $\mathfrak{m}_a/\mathfrak{m}_a^2$ is called the *cotangent space* to V at a.

Suppose that $f_1, \ldots, f_k$ generate the ideal of the variety V. Then $T_{V,a}$ is the linear

subspace defined by

$$\sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(x_i - a_i) = 0 \text{ for all } j \in \{1, \ldots, k\}.$$

That is, $T_{V,a}$ is equal to the kernel of the Jacobian of the system $f_1, \ldots, f_k$.

The dimension of V at a point a, denoted by $\dim_a V$ is the maximum of the dimensions of the irreducible components of V through a. We say that a is *nonsingular* if $\dim T_{V,a} = \dim_a V$.

An algebraic variety in K^n of dimension $n-1$ is called a *hypersurface*. A hypersurface that is also an affine space (i.e., satisfies a linear equation) is a *hyperplane*. A variety of dimension 1 is said to be an *algebraic curve*.

We have the following definition of dimension [134, Section 9.5, Theorem 2].

Theorem 2.10. *Let $V \subseteq K^n$ be an affine variety. Then the dimension of V equals the maximal number of elements of $K[V]$ which are algebraically independent over K.*

If the variety V is irreducible, then its function field $K(V)$ is well-defined. The dimension of V is equal to the transcendence degree of $K(V)$ over K.

We recall another equivalent definition of the dimension of an algebraic variety [134, Section 9.5, Corollary 4].

Theorem 2.11. *Let $V \subseteq K^n$ be an affine variety. Then the dimension of V is equal to the largest integer d for which there exist d variables $x_{i_1}, \ldots, x_{i_d}$ such that $I(V) \cap K[x_{i_1}, \ldots, x_{i_d}] = \{0\}$ (i.e., such that $I(V)$ contains no non-zero polynomials in only these variables).*
Furthermore, if K is algebraically closed, the statement above remains true if we replace $I(V)$ with any defining ideal I of V.

Let $\mathcal{I} \subseteq \{1, \ldots, n\}$ be a set of indices. We denote by $\pi_{\mathcal{I}} : k^n \to k^{|\mathcal{I}|}$ the projection on the $|\mathcal{I}|$-dimensional subspace defined by the system of equations $\{x_i = 0, i \notin \mathcal{I}\}$. In terms of projections, one can deduce from Theorem 2.11 that the dimension of V is the largest dimension of a coordinate subspace for which the projection of V is Zariski dense in the subspace. To prove this, the following theorem [134, Section 3.2, Theorem 3] is needed.

Theorem 2.12 (Closure Theorem)**.** *Let k be algebraically closed. Let $V = V(f_1, \ldots, f_s) \subseteq K^n$ and let $I_\ell = \langle f_1, \ldots, f_s \rangle \cap K[x_{\ell+1}, \ldots, x_n]$ be the ℓth elimination ideal of $\langle f_1, \ldots, f_s \rangle$. Then*

(i) $V(I_\ell)$ is the smallest affine variety containing $\pi_\ell(V) \subseteq K^{n-\ell}$.

(ii) When $V \neq \emptyset$, there is an affine variety $W \subsetneq V(I_\ell)$ such that $V(I_\ell) \setminus W \subseteq \pi_\ell(V)$.

Item (i) of the Closure theorem thus asserts that $V(I_\ell)$ is the Zariski closure of $\pi_\ell(V)$. Item (ii) furthermore shows that even if $\pi_\ell(V)$ is not equal to $V(I_\ell)$, it almost fills up $V(I_\ell)$. In particular, all the points that are missing lie in a smaller variety W.

Proposition 2.13. *Let K be algebraically closed. Given a subvariety $V \subseteq K^n$, its dimension is the largest dimension of a coordinate subspace for which the projection of V is Zariski dense in the subspace.*

Proof. Fix variables $x_{i_1}, \ldots, x_{i_d}$ such that $I(V) \cap K[x_{i_1}, \ldots, x_{i_d}] = \{0\}$, the existence of which is asserted in Theorem 2.11. Let π be the projection map from K^n to K^d defined by $\pi(a_1, \ldots, a_n) = (a_{i_1}, \ldots, a_{i_d})$.

Let $\tilde{I} = I(V) \cap K[x_{i_1}, \ldots, x_{i_d}]$. By the Closure Theorem (Theorem 2.12) $V(\tilde{I}) \cap K^d$ is the smallest variety containing the projection $\pi(V)$. Since

$$\begin{aligned}
\tilde{I} = \{0\} &\iff V(\tilde{I}) = k^d \\
&\iff V(\tilde{I}) \cap k^d = k^d \\
&\iff \text{the smallest variety containing } \pi(V) \text{ is precisely } K^d \text{ (Theorem 2.12)} \\
&\iff \pi(V) \text{ is dense in } K^d.
\end{aligned}$$

□

That is, for a variety $V \subseteq \mathbb{C}^n$, if $\dim V = d$, then

- for $r \leq d$ there exists a set $\mathcal{I}$ of r indices such that $\pi_{\mathcal{I}}(V)$ is dense in $\mathbb{C}^r$,
- for $r > d$ there does not exist a set of r indices with this property.

2.4 Sequences and series

In this section we give a brief overview of recursively defined sequences and their generating series. For more details, we refer the reader to [135].

2.4.1 Sequences

Let K be a field. An infinite sequence $\langle u_n \rangle_{n=0}^{\infty}$ of elements from K is said to be *C-finite* if it satisfies a recurrence

$$c_0 u_n + c_1 u_{n-1} + \cdots + c_d u_{n-d} = 0$$

where $c_1, \ldots, c_d \in K$ and $c_d \neq 0$. We call the number of previous terms d appearing in the recurrence relation defining an element u_n the *order* of the recurrence. C-finite sequences are also commonly referred to as Linear Recurrence Sequences (LRS for short) in the literature.

Arguably the most well-known example of C-finite sequences is the Fibonacci sequence $\langle F_n \rangle_{n=0}^{\infty}$, which satisfies the equation $F_n = F_{n-1} + F_{n-2}$ and is given by the initial terms $F_0 = F_1 = 0$.

An infinite sequence $\langle u_n \rangle_{n=0}^{\infty}$ of elements from K is said to be *P-finite* if it satisfies a recurrence

$$p_0(n)u_n + p_1(n)u_{n-1} + \cdots + p_d(n)u_{n-d} = 0 \tag{2.2}$$

where $p_0(x), \ldots, p_d(x) \in K[x]$, the polynomial $p_d(x) \neq 0$ and $p_0(x)$ has no non-negative integer zeros. By the latter assumption on $p_0(x)$, the recurrence relation (2.2) uniquely defines an infinite sequence once the initial values $u_0, \ldots, u_d \in K$ are specified. Here d is again called the *order* of the sequence.

A simple example of a P-finite sequence is the factorial sequence $\langle f_n \rangle_{n=0}^{\infty}$ where for each term we have $f_n = n!$. The sequence is given by the initial term $f_0 = 0$ and satisfies the recurrence $f_n = n \cdot f_{n-1}$.

P-finite sequences of order 1 are known as hypergeometric sequences. Formally, the sequence $\langle u_n \rangle_{n=0}^{\infty}$ is called a univariate *hypergeometric sequence* if it satisfies a recurrence of the form

$$p(n)u_n - q(n)u_{n-1} = 0\,, \tag{2.3}$$

where $p(x), q(x) \in K[x]$ are polynomials, and $p(x)$ has no non-negative integer zeros. Recurrence (2.3) can be reformulated as

$$u_n = r(n)u_{n-1}\,,$$

where $r(x) = \frac{q(x)}{p(x)} \in \mathbb{Q}(x)$ is a rational function that, by the assumption above, has no nonnegative integer pole. The rational function $r(x)$ is called the *shift quotient* of $\langle u_n \rangle_{n=0}^{\infty}$.

An example of a hypergeometric sequence often used in computer science is the sequence of Catalan numbers $\langle C_n \rangle_{n=0}^{\infty}$, which counts, for example, the number of well parenthesised expressions of length n or, say, the number of full binary trees with $n+1$ leaves. The sequence satisfies the relation $C_n = \frac{2(2n-1)}{n+1} C_{n-1}$, and we define its initial term to be $C_0 = 1$.

2.4.2 Power series

Number sequences are one of the principal objects of study in combinatorics as well. Given a field K, and a sequence $\langle a_n \rangle_{n=0}^{\infty}$ of values from K, a standard way to represent it is via its *generating series*, which we define as a *univariate formal power series*

$$a(x) = \sum_{n=0}^{\infty} a_n x^n.$$

More generally, a (multivariate) *formal power series* in variables $x_1, \ldots, x_m$ is defined by

$$a(x_1, \ldots, x_m) = \sum_{(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m} a_\alpha x_1^{\alpha_1} \cdots x_m^{\alpha_m}.$$

The formal power series in the variables $\boldsymbol{x} := (x_1, \ldots, x_m)$ over K with pointwise addition and Cauchy product form a ring, which we denote by

$$K[\![\boldsymbol{x}]\!] = \Big\{ \sum_{\boldsymbol{\alpha} \in \mathbb{N}^m} a_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}} \mid a_{\boldsymbol{\alpha}} \in K \Big\}.$$

We define the *support* of a formal series by

$$\operatorname{supp}(a) := \{\boldsymbol{\alpha} \in \mathbb{N}^m \mid a_{\boldsymbol{\alpha}} \neq 0\}.$$

If $f = a_0 + a_1\boldsymbol{x}^{\boldsymbol{\alpha}_1} + a_2\boldsymbol{x}^{\boldsymbol{\alpha}_2} + \cdots$ is a formal power series then f has an inverse in $K[\![\boldsymbol{x}]\!]$ if and only if $a_0 \neq 0$.

If K is a field, the quotient field of the ring of rational functions $K[\![\boldsymbol{x}]\!]$ is the field of *(formal) Laurent series*, which we denote by $K(\!(\boldsymbol{x})\!)$. It consists of series of the form

$$a(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha}\in\mathbb{Z}^n} a_{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\alpha}}$$

whose support $\operatorname{supp}(a) := \{\boldsymbol{\alpha} \in \mathbb{Z}^m \mid a_{\boldsymbol{\alpha}} \neq 0\}$ takes values in the set $\{n_0, n_0 + 1, \ldots, -1, 0\} \cup \mathbb{N}$ for some integer n_0. Explicitly, we can write it as

$$K(\!(\boldsymbol{x})\!) = \Big\{ \sum_{\boldsymbol{\alpha}\in\mathbb{Z}^m} a_{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\alpha}} \mid a_{\boldsymbol{\alpha}} \in K \Big\}.$$

A *Puiseux series* in the variables $\boldsymbol{x} := (x_1, \ldots, x_m)$ is a formal series

$$a(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha}\in\mathbb{Q}^n} a_{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\alpha}}$$

whose support $\operatorname{supp}(a) := \{\boldsymbol{\alpha} \in \mathbb{Q}^m \mid a_{\boldsymbol{\alpha}} \neq 0\}$ satisfies $\operatorname{supp}(a) \subseteq \frac{1}{k}\mathbb{Z}^m$ for some positive integer k. The field of *Puiseux series* in $\boldsymbol{x}$ over a field K is defined as

$$K\{\{\boldsymbol{x}\}\} = \Big\{ \sum_{\boldsymbol{\alpha}\in\mathbb{Q}^m} a_{\boldsymbol{\alpha}}\boldsymbol{x}^{\boldsymbol{\alpha}} \mid a_{\boldsymbol{\alpha}} \in K \Big\}.$$

It is the algebraic closure of the field of Laurent series.

A series $a(\boldsymbol{x}) \in K[\![\boldsymbol{x}]\!]$ is said to be *algebraic* over $K[\boldsymbol{x}]$ if there exist polynomials $p_0(\boldsymbol{x}), \ldots, p_d(\boldsymbol{x}) \in K[\boldsymbol{x}] \subseteq K[\![\boldsymbol{x}]\!]$, not all zero, such that

$$p_0(\boldsymbol{x}) + p_1(\boldsymbol{x})a(\boldsymbol{x}) + p_2(\boldsymbol{x})a(\boldsymbol{x})^2 + \ldots + p_d(\boldsymbol{x})a(\boldsymbol{x})^d = 0.$$

Taking the $p_i(\boldsymbol{x})$ as rational functions allows us to regard

$$p(\boldsymbol{x}, y) := p_0(\boldsymbol{x}) + p_1(\boldsymbol{x})y + p_2(\boldsymbol{x})y^2 + \ldots + p_d(\boldsymbol{x})y^d = 0$$

as a univariate polynomial in y over the coefficient field $K(\boldsymbol{x})$. The substitution $p(\boldsymbol{x}, a(\boldsymbol{x}))$ for $a(\boldsymbol{x}) \in K(\boldsymbol{x})$ then takes place in the bigger domain $K(\!(\boldsymbol{x})\!)$ of Laurent series with coefficients in K, which contains both $K(\boldsymbol{x})$ and $K[\![\boldsymbol{x}]\!]$ as subrings.

Given an algebraic power series $a(\boldsymbol{x})$ we denote by $A \subseteq K(\boldsymbol{x})[y]$ the ideal of all univariate polynomials with coefficients in $K(\boldsymbol{x})$ which vanish on the power series $a(\boldsymbol{x})$. That is, all polynomials $p(\boldsymbol{x}, y) \in K(\boldsymbol{x})[y]$ such that $p(\boldsymbol{x}, a(\boldsymbol{x})) = 0$. We say that A is the *ideal of annihilating polynomials for* $a(\boldsymbol{x})$. The generator $m(\boldsymbol{x}, y)$ of A (where the leading term in y is monic) is called the *minimal polynomial* of $a(\boldsymbol{x})$. By virtue of being monic, the minimal

polynomial $m(\boldsymbol{x}, y)$ is uniquely defined. Furthermore, the minimal polynomial $m(\boldsymbol{x}, y)$ is always irreducible.

In the univariate setting, the Newton-Puiseux theorem [136, 137] gives a characterisation of the field $\overline{K(x)}$ in terms of Puiseux series. The theorem says that given a polynomial equation $p(x, y) = 0$ with coefficients in an algebraically closed field of characteristic zero, its solutions in y, viewed as functions of x, may be expanded as Puiseux series in x that are convergent in some neighbourhood of 0. In terms of fields, the theorem asserts that the set of Puiseux series over an algebraically closed field of characteristic 0 is itself an algebraically closed field. In other words, the algebraic closure $K(x)$ for K a field of characteristic 0 is a subfield of $\overline{K}\{\{x\}\}$. The algebraic closure $\overline{\mathbb{Q}(x)}$, for example, is equal to the subfield of the field of Puiseux series $\mathbb{C}\{\{x\}\}$ consisting of those series that are algebraic over the field $\mathbb{Q}(x)$ of rational functions.

This characterisation does not extend directly to the multivariate setting, that is, to $K(x_1, \ldots, x_n)$. Take for example the equation $z^2 - x_1 - x_2$ with solution $\sqrt{x_1 + x_2}$, which does not admit a Puiseux series expansion. The closest result to the Newton-Puiseux theorem here is McDonald's theorem [138], which asserts that the elements that are algebraic over $K[x_1, \ldots, x_m]$ can be expressed as series with support in the translation of a strongly convex rational cone. As discussed above, if $\operatorname{supp}(a) \subset \frac{1}{k}\mathbb{Z}$ for some k, then the series is a Puiseux series, whereas in McDonald's theorem the series have the support is a subset of a cone instead. More generally, characterising the algebraic closure of the field of multivariate rational functions or say the field Laurent series is still an active area of research; see, e.g., [139] and the introduction therein.

Chapter 3

The Radical Identity Testing problem

In this chapter we study the Radical Identity Testing (RIT) problem, which asks, given a polynomial $f(x_1, \ldots, x_k)$ represented by an algebraic circuit, and radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, whether $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. We further consider two restricted variants of the problem: the 2-RIT problem and the $\mathrm{bounded}$-RIT problem.

The results presented in this chapter are based on a joint work with Nikhil Balaji, Mahsa Shirmohammadi, and James Worrell [140].

Organisation of the chapter. We begin this chapter by recalling notation and the statements of the problems we consider in Section 3.1. In Section 3.2 we discuss our approach to solving RIT, which generalises the well-known randomised polynomial time algorithm for ACIT. We outline the ring of computation in the radical setting and give an overview of our algorithm. In Section 3.3 we generalise a subroutine of the well-known algorithm for $\mathrm{bounded}$-RIT and show that we can always assume that the input radicands a_i are pairwise coprime and the minimal polynomials of the radicals $\sqrt[d_i]{a_i}$ over $\mathbb{Q}$ are $x^{d_i} - a_i$. Our arguments actually allow to generalise the algorithm for the $\mathrm{bounded}$-RIT problem as well, which we observe in Section 3.3.1.

Section 3.4 is dedicated to the complexity of the general variant of RIT. In Section 3.4.1, we give the arguments ensuring the soundness of our algorithm when taking the computation to a finite field. As a parenthesis, we show that one of the soundness lemmas also allows us to reduce RIT to determining the satisfiability of a system of polynomial equations in Section 3.4.2. We then go back to our algorithm, showing how to choose suitable primes for the computation in Section 3.4.3, and stating the algorithm in Section 3.4.4.

In Section 3.5 we turn our attention to a restricted variant of the problem, namely the 2-RIT problem, wherein the input radicals are square roots of primes, and show an improved complexity bound for this case. Finally, we conclude the chapter by discussing possible extensions of our approach and listing some open questions in Section 3.6.

Relevant preliminaries. The preliminary sections useful for reading this chapter are Section 2.2 and Sections 2.3.1 to 2.3.6.

3.1 Notation

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 and the bitsize of the radicands a_i and exponents d_i.

The 2-RIT problem 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 is a variant of RIT 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.

3.2 Approaching the problem

We approach the Radical Identity Testing problem with the aim of generalising the well-known fingerprinting procedure for solving ACIT [1], which involves evaluating an arithmetic circuit modulo a randomly chosen prime. The soundness of the latter approach relies on the fact that if the integer $z \in \mathbb{Z}$ computed by the circuit is non-zero, then one can with high probability randomly sample a prime $p \in \mathbb{Z}$ of size polynomial in the bitsize of the input such that z is non-zero modulo p.

Formally speaking, in the setting of ACIT, the computation occurs in the ring of integers $\mathbb{Z}$. The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$, for (rational) primes p. The algorithm evaluates the circuit in the finite field $\mathbb{F}_p$ by a surjective homomorphism $\varphi : \mathbb{Z} \to \mathbb{F}_p$ with kernel $p\mathbb{Z}$.

The approach was first generalised to identity testing over number fields in [32], namely to deciding the CIT problem, which asks, given an algebraic circuit C representing a polynomial $f \in \mathbb{Z}[x]$ and an integer $n \in \mathbb{N}$ given in binary, whether $f(\zeta_n) = 0$. There, the computation occurs in the ring of integers $\mathbb{Z}[\zeta_n]$ of a cyclotomic field $\mathbb{Q}(\zeta_n)$. In the algorithm, the computation is done in a finite field $\mathbb{F}_p$ corresponding to the quotient of $\mathbb{Z}[\zeta_n]$ by a prime ideal factor $\mathfrak{p}$ of $p\mathbb{Z}[\zeta_n]$. Concretely, the algorithm chooses a prime p such that $\mathbb{F}_p$ contains an nth primitive root of unity, and evaluates the polynomial modulo p. If the result is non-zero, then the instance of CIT is negative. Otherwise, the prime p must divide the norm of the cyclotomic integer computed by the circuit, which means that there are only finitely many primes for which the finite field evaluation could give a false positive.

In our work, we further generalise the CIT technique of [32] to identity testing for radical expressions. To understand the differences between the two problems, let us see what is the ring of evaluation in the case of RIT. To this aim, first note that given $a, d \in \mathbb{N}$, the radical $\sqrt[d]{a}$ is an algebraic integer. 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 $1 \leq j \leq t$, where ζ_t is a tth primitive root of unity.

The number field $\mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k})$ is the smallest extension of $\mathbb{Q}$ that contains the radicals $\sqrt[d_i]{a_i}$. Since we are in characteristic zero, the extension is separable over $\mathbb{Q}$, but note that it is normal (hence Galois) over $\mathbb{Q}$ if and only if $d_i = 2$ for all $i \in \{1, \ldots, k\}$. 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 $d = \operatorname{lcm}(d_1, \ldots, d_k)$, to $\mathbb{Q}$.

In the RIT problem, we may thus think of the evaluation as occurring in the ring of integers $\mathcal{O}_K$ of K. Again, the idea behind our approach is to work modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that the quotient $\mathcal{O}_K/\mathfrak{p}$ is isomorphic to $\mathbb{F}_p$ for some rational prime p. As discussed in Section 1.1, the Galois group of the radical number field K we work with may not be as well-behaved as $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Furthermore, in contrast to cyclotomic fields, the ring of integers of a radical field extension need not be monogenic. That is, it may not admit a power basis given by a single element such as $\mathbb{Z}[\zeta_n]$. This makes choosing a suitable rational prime p more challenging.

We manage to get around these problems by examining primitive elements for the number field K in order to deduce a bound on primes p suitable for the finite field computation. The main correctness proof of our algorithm relies on the characteristics of the Galois group of K and concepts from number theory.

We will now give a brief overview of our algorithm, and sketch its correctness.

Our non-deterministic algorithm 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 $i \in \{1, \ldots, k\}$. To do this we generalise the reduction in [42] and use the *factor refinement* algorithm [141]; see Section 3.3.

Our algorithm then proceeds in two steps. In Step 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 size 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 dth 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 $x^{d_i} - a_i$.

In Step 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'.

The algorithm we just described (stated fully in Figure 3.3) allows us to place the RIT

problem in **coNP** assuming GRH. 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-size 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. 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 Step 1, and ideals in K only feature in the proof of correctness of the algorithm, which we will briefly outline now.

The first element of the correctness proof of the **coNP** algorithm is to argue that the prime p chosen in Step 1 completely splits in the ring of integers $\mathcal{O}_K$. In this situation, for any prime-ideal factor $\mathfrak{p}$ of p, each quotient field $\mathcal{O}_K/\mathfrak{p}$ is isomorphic to the finite field $\mathbb{F}_p$. By standard results in algebraic number theory we know that p completely splits in $\mathcal{O}_K$ 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.

The latter requirement is guaranteed by Hensel's Lemma in tandem with Conditions (i) and (ii) in Step 1 that determine the choice of p in the algorithm. In more detail, Condition (i), that $p \equiv 1 \pmod{d}$, entails that $\mathbb{F}_p$ contains a primitive dth root of unity. To see this, first recall that the powers of a root of unity are also all roots of unity themselves. Now since the multiplicative group $\mathbb{F}_p^*$ is cyclic, it is clear that $\mathbb{F}_p^*$ contains a primitive dth root of unity if and only if $d \mid p - 1$. In combination with Condition (ii), requiring 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 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 $i \in \{1, \ldots, k\}$, 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 σ in $\mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\tau_1) = \tau_2$. We will call this property joint transitivity; see Lemma 3.3.

Now for every prime ideal factor $\mathfrak{p}$ of $p\mathcal{O}_K$ there is a surjective homomorphism $\varphi : \mathcal{O}_K \to \mathbb{F}_p$ with kernel $\mathfrak{p}$. For each choice of $\mathfrak{p}$ and for all $i \in \{1, \ldots, k\}$, 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 $i \in \{1, \ldots, k\}$, $\overline{\alpha}_i$ 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 $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ 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 3.4.

We complete our correctness proof by employing a quantitative version of the Cheb-

otarev density theorem. Informally speaking, Chebotarev's density theorem states that the set of rational primes p that split completely in $\mathcal{O}_K$ has density $\frac{1}{|\operatorname{Gal}(K/\mathbb{Q})|}$. The original statement of the theorem is asymptotic, whereas for our algorithm we use its quantitative version in order to obtain a bound on the number of totally split primes p of size polynomial in the bitsize of the input, which requires GRH. 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.

Our randomised algorithm for 2-RIT**.** In contrast to the algorithm for ACIT, or its generalisation to CIT, our algorithm runs in non-deterministic polynomial time, as opposed to randomised polynomial time. In order to be able to choose the prime randomly, we would require the density of split primes to be polynomial in the size of the input instance. However, since the size of the Galois group of K over $\mathbb{Q}$ is exponential in the size of the input, by Chebotarev's density theorem, totally split primes do not have sufficient density in order to directly be chosen randomly. This is the case even if the exponents d_i are prime numbers written in unary.

Nonetheless, we manage to 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 odd rational primes (written in binary). As explained above, the density of arbitrary primes in this case is not good enough for random sampling either, however, we show that there is an arithmetic progression with a good density of primes, and that all primes in this progression are suitable. The latter allows us to improve the complexity for 2-RIT, placing it into **coRP** assuming GRH. 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 input radicals are of the form $x^2 - q_i$ where q_i is an odd rational prime. The condition entails that the equations $x^2 \equiv q_i$ have solutions in $\mathbb{F}_p$, that is, that q_i is a quadratic residue modulo p for all $i \in \{1, \ldots, k\}$. Now 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 intuition we have just given, 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 an additional condition on A and b, based on Pocklington's algorithm, ensuring that a root of each $x^2 - q_i$ can be computed in deterministic polynomial time in the size of the problem instance.

Finally, we use effective versions of Dirichlet's theorem on the density of primes in an arithmetic progression, see Theorem 3.14, to show that the 2-RIT problem is in **coRP** assuming GRH and in **coNP** unconditionally.

Now that we have given an outline of our algorithms and their correctness proofs, let us go to the technical details.

3.3 A reduction to coprime radical inputs

In this section we show that without loss of generality, we can assume the input radicands $a_1, \ldots, a_k$ to be pairwise coprime. In particular, given an algebraic circuit C representing a 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 $f'(\sqrt[t_1]{n_1}, \ldots, \sqrt[t_\ell]{n_\ell}) = 0$.

To this aim, we rely on the *factor-refinement* algorithm, introduced in [141]. Given a set of integers $a_1, \ldots, a_k$, the algorithm 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 $1 \leq j < k \leq \ell$, 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 $a = \operatorname{lcm}(a_1, \ldots, a_k)$, the factor-refinement algorithm runs in time $\mathcal{O}(\log^2(a))$(see also [42, Lemma 3.1]), and the number ℓ of factors is bounded by $\sum_{i=1}^{k} \log(|a_i|)$.

The reduction algorithm is illustrated in Figure 3.1. Let us now verify its correctness and show that it runs in polynomial time in the size of the input instance of RIT.

In Step 1, we first compute the partial factorisation of each one of the a_i's by going through all primes up to $\log a$, where $a = \operatorname{lcm}(a_1, \ldots, a_k)$. This can clearly be done in time polynomial in $\log a$. We denote by $m_1, \ldots, m_r$, the primes p appearing in the factorisations of the a_i.

In Step 2, we 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 $a_i = \prod_{j=1}^{l} m_j^{e_{ij}}$. As discussed above, this can again be done in time polynomial in $\log a$. 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 $x^{t_i} - n_i$, in Step 3, 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 $d_i | \gcd(f_{j1}, \ldots, f_{js}) \cdot d_{ij}$. Furthermore, observe that d_{ij} will be the smallest such power precisely when

$$d_i = \gcd(f_{j1}, \ldots, f_{js}) \cdot d_{ij}. \tag{3.1}$$

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, $r < j \leq l$, 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 $m_j =$

Reduction	
Input:	Algebraic circuit C of size at most s computing a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$ with input radicals $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$ where the bitsize of the d_i and a_i is at most s, and the a_i are mutually coprime.
Output:	Algebraic circuit C' of size at most polynomial in s computing a polynomial $f' \in \mathbb{Z}[x_1, \ldots, x_k]$ with input radicals $\sqrt[t_1]{n_1}, \ldots, \sqrt[t_\ell]{n_\ell}$ where the bitsize of the t_i and n_i is at most s, and the n_i are mutually coprime such that $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ if and only if $f'(\sqrt[t_1]{n_1}, \ldots, \sqrt[t_\ell]{n_\ell}) = 0$.
Step 1:	For each a_i, compute a partial factorisation $a_i = m_1^{e_{i1}} \cdots m_r^{e_{ir}} a_i'$, where $m_1, \ldots, m_r$ are primes of magnitude at most $\log a$ and $a = \operatorname{lcm}(a_1, \ldots, a_k)$.
Step 2:	Apply factor-refinement to the unfactored part a_i' of each a_i to compute a set of pairwise coprime factors $\{m_{r+1}, \ldots, m_\ell\}$ such that $a_i = \prod_{j=1}^{l} m_j^{e_{ij}}$.
Step 3:	For each $\sqrt[d_i]{m_j}$, compute the smallest d_{ij} such that $\sqrt[d_i]{m_j}^{d_{ij}} \in \mathbb{Z}$.
Step 4:	Construct the new input radicals by setting $n_j = m_j^{\frac{1}{\operatorname{lcm}(d_{1j} \cdots d_{kj})}}$ and $t_j = \frac{d_1 \cdots d_k}{\operatorname{lcm}(d_{1j} \cdots d_{kj})}$.
Step 5:	Construct the algebraic circuit C' from C by replacing the leaves x_i, $i \in \{1, \ldots, k\}$, with a small circuit that computes $\prod_{j=1}^{l} y_j^{\frac{e_{ij} d_1 \cdots d_k}{d_i}}$.

Figure 3.1 – Our polynomial time reduction of an instance of RIT to an instance of the problem where the input radicands are mutually coprime.

$p_1^{f_{j1}} \ldots p_s^{f_{js}}$, 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 (3.1), we go trough the candidates for the $\gcd(f_{j1}, \ldots, f_{js})$. That is, we consider $g_{ij} = 1, \ldots, \log m_j - 1$, 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 [142, 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

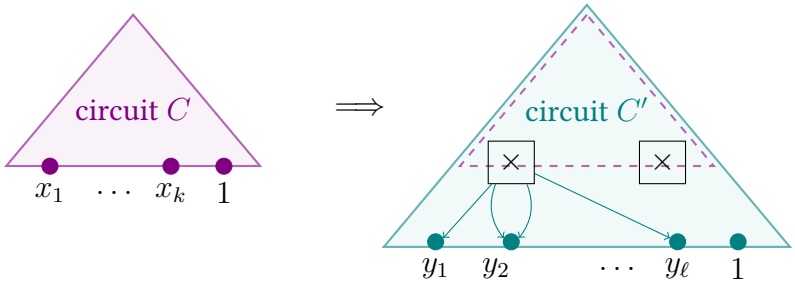

Figure 3.2 – The scheme of the reduction from RIT to its variant where the input radicands are pairwise coprime and the exponents are all equal. In this simple example, a_1 is factored to $m_1 m_2^2 m_\ell$.

$m^{g_{ij}} = m_j$, with g_{ij} unary.

Finally, in Step 4, we construct the new input radicals by setting $n_j = m_j^{\frac{1}{\operatorname{lcm}(d_{1j} \cdots d_{kj})}}$ and $t_j = \frac{d_1 \cdots d_k}{\operatorname{lcm}(d_{1j} \cdots d_{kj})}$.

We complete the reduction in Step 5 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 3.2.

3.3.1 The complexity of bounded-RIT

The reduction presented in Section 3.3 is a generalisation of a subroutine proposed by Blömer in [42], where it is used as a first step in the randomised polynomial time algorithm for a variant of the bounded-RIT problem. In particular, the work studies bounded-RIT where the exponents d_i of the radical input $\sqrt[d_i]{a_i}$ are given in unary. The algorithm works by computing an approximation of a random conjugate of the algebraic integer α computed by evaluating the input circuit C on the radical input. Then, following a result on separation bounds for algebraic numbers, whenever α is non-zero, a random conjugate α' of α has a large absolute value with probability at least $\frac{2}{3}$.

Let us note again that such a numerical approach does not yield good complexity bounds for the general variant of RIT, as the coefficients of polynomials represented by algebraic circuits could be doubly exponential in the size of the circuit. In particular, this means that numerical approximation in this case would require too much space in order to be feasible in polynomial time. This is why the algorithms we develop in this thesis all work by reducing the polynomials modulo some prime p, and taking the computation to the finite field $\mathbb{F}_p$ instead.

Given an instance of bounded-RIT where the exponents d_i are given in binary, the correctness argument behind the algorithm presented in [42] still applies, however the algorithm no longer runs in polynomial time. The increase in complexity appears in Steps 1 and 2 of the algorithm, that is, when sampling a random conjugate of α.

Denote by K the Galois closure of the field we obtain by adjoining the input radicals to $\mathbb{Q}$. Given an element $\alpha \in K$ that can be computed as a polynomial expression in $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, its Galois conjugates are given by evaluating the same expression on the conjugates of the $\sqrt[d_i]{a_i}$'s if the a_i's are pairwise coprime. The idea presented in the original paper [42] is thus to first compute pairwise coprime factors $m_1, \ldots, m_\ell$ of the input radicands $a_1, \ldots, a_k$, such that $\sqrt[d_i]{a_i} = \prod_{j=1}^{\ell} \sqrt[d_i]{m_j}^{e_{ij}}$. Then, if we compute the minimal $d_{ij} \in \mathbb{Z}$ such that $\sqrt[d_i]{m_j}^{d_{ij}} \in \mathbb{Z}$, given a primitive d_ith root of unity ζ_{d_i}, the Galois conjugates conjugates of $\sqrt[d_i]{m_j}$ are given by $\sqrt[d_i]{m_j}\zeta_{d_i}, \ldots \sqrt[d_i]{m_j}\zeta_{d_i}^{d_i-1}$. In the paper [42], a clever way to randomly choose primitive d_ith roots of unity is described. This, in combination with factor refinement, gives an algorithm to sample conjugates of the $\sqrt[d_i]{m_j}\zeta_{d_{ij}}$, thus computing a conjugate of α.

Now when the input exponents are given in binary, computing the minimal d_{ij} such that $\sqrt[d_i]{m_j}^{d_{ij}} \in \mathbb{Z}$ can no longer be done in polynomial time. However, by first partially factoring the radicands a_i as done in our reduction in Section 3.3, we can avoid the complexity-increase of the first two steps of Blamer's algorithm. Thus, replacing the first two steps of Blömer's algorithm by our reduction allows us to extend his result to the most general case of bounded-RIT and conclude that

Corollary 3.1. *The* bounded-RIT *problem is in* **coRP**.

3.4 The complexity of RIT

In this section we present a nondeterministic polynomial time algorithm for the complement of RIT. As discussed in Section 3.2, 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 RIT comprising 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 Section 3.3. We denote by s the size of our fixed RIT instance; that is, the size of the circuit is bounded by s, and the magnitude of the a_i and d_i is at most 2^s. Note that $k \leq s$, by the definition of size of an algebraic circuit. 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 dth root of unity ζ_d, with $d = \operatorname{lcm}(d_1, \ldots, d_k)$. We denote by $\mathcal{O}_K$ 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 $\mathcal{O}_K$. That is, such that $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are distinct prime ideals of $\mathcal{O}_K$, and n is the degree of the number field K.

As discussed in Section 2.3.4, in general, given a number field L and a rational prime q with prime ideal $\mathfrak{q}$ dividing $q\mathcal{O}_L$, we say that $\mathfrak{q}$ lies above q in $\mathcal{O}_L$. The residue field $\mathcal{O}_L/\mathfrak{q}$ 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 $\mathcal{O}_K$, all residue fields $\mathcal{O}_K/\mathfrak{p}_i$ 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.

It is a well-known result in number theory that all irreducible polynomials of degree at most d split completely in $\mathbb{F}_{p^d}$ for every prime p. It may thus be tempting to consider working instead in a finite extension of $\mathbb{F}_p$. However, 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 bitsize of d. Moreover, specialising to 2-RIT, where F_{p^2} contains all the input square roots for all rational primes p, not all primes p are suitable for such a computation either. Let us illustrate this with an example.

Example 3.1. *Consider the polynomial $f(x_1, x_2) = x_1 - 4x_2$ with input $\sqrt{2}$ and $\sqrt{7}$. The polynomial f clearly does not vanish on $(\sqrt{2}, \sqrt{7})$. Let us choose the prime $p = 11$, and observe that both $x^2 - 2$ and $x^2 - 7$ are irreducible in $\mathbb{F}_{11}$, and their respective minimal polynomials both split over $\mathbb{F}_{11^2}$. Assume we choose the field $\mathbb{F}_{11}[x]/(x^2 - 7)$ obtained by adjoining $\sqrt{7}$ to $\mathbb{F}_{11}$ as the finite field of our computation. Let $\overline{\alpha}_1$ be a solution of $x^2 - 7$ in $\mathbb{F}_{11^2}$. Notice that $(4\overline{\alpha}_1)^2$ is a solution of $x^2 - 4$ in F_{11^2}. Indeed,*

$$(4\overline{\alpha}_1)^2 \equiv 16\overline{\alpha}_1^2 \equiv 16 \cdot 7 \equiv 2 \pmod{11}.$$

This implies that $\sqrt{2} - 4\sqrt{7}$ converts to $4\overline{\alpha}_1 - 4\overline{\alpha}_1 \equiv 0$ modulo 11, which is clearly a false positive.

The example above illustrates that for 2-RIT, working in $\mathbb{F}_{p^2}$ is only sound if the latter does actually arise as quotient of the number field K by a suitable prime ideal. In particular, if p has inertial degree 2 over K (i.e., p is *inert* in K). By Chebotarev's density theorem, such primes correspond to a conjugacy class of the Galois group, and their asymptotic density is the same as for those that split over K. We thus focus our attention onto split primes that allow for a sound computation both in the general variant of RIT, as well as its restriction 2-RIT.

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 dth cyclotomic polynomial (the minimal polynomial of ζ_d) split into distinct linear factors in $\mathbb{F}_p$. As discussed in Section 2.3.5, the splitting pattern of a rational prime q in a number field L relates to the degree of the local extension $L_\mathfrak{q}$ of $\mathbb{Q}_q$, which is obtained by adding the generators of L over $\mathbb{Q}$ to $\mathbb{Q}_q$. We use this correspondence in order to prove our claim.

Proposition 3.2. *Given a monic polynomial $h \in \mathbb{Z}[x]$ and its splitting field L, a prime $q \in \mathbb{Z}$ splits completely in L if h splits into distinct linear factors in $\mathbb{F}_q$.*

Proof. Write n for the degree of L over $\mathbb{Q}$, and recall that $|\operatorname{Gal}(L/\mathbb{Q})| = n$. Denote by $L_\mathfrak{q}$ the finite field extension of $\mathbb{Q}_q$ obtained by adjoining the roots of h to $\mathbb{Q}_q$. Let $\mathfrak{q}$ be a prime ideal lying above q in L. Recall this means that $\mathfrak{q}$ is one of the prime ideals $\mathfrak{q}_i$ appearing in the factorisation

$$q\mathcal{O}_L = \mathfrak{q}_1^e \cdots \mathfrak{q}_g^e \tag{3.2}$$

of the ideal $q\mathcal{O}_L$ in $\mathcal{O}_L$.

Recall, furthermore, that the decomposition group of a prime ideal $\mathfrak{q} \subset \mathcal{O}_L$ is defined as the set of all automorphisms of $\operatorname{Gal}(L/\mathbb{Q})$ that fix $\mathfrak{q}$, i.e., $D_\mathfrak{q} = \{\sigma \in \operatorname{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$.

In other words, $D_{\mathfrak{q}}$ is the stabiliser subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ with respect to $\mathfrak{q}$. Moreover, since the field extension L is Galois over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set of prime ideals $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_g\}$ above q (see, e.g., the proof of [131, Theorem 3.34]). That is, for every pair $\mathfrak{q}_i, \mathfrak{q}_j$, there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\mathfrak{q}_i) = \mathfrak{q}_j$. Furthermore, the following isomorphism holds (cf. [131, Proposition 8.10]).

$$D_{\mathfrak{q}} \cong \mathrm{Gal}(L_{\mathfrak{q}}/\mathbb{Q}_q) \tag{3.3}$$

Now given that h splits into distinct linear factors in $\mathbb{F}_q$, it follows that for each $x \in \mathbb{F}_q$ such that $h(x) \equiv 0 \pmod q$, we have $h'(x) \not\equiv 0 \pmod q$. We may thus apply Hensel's lemma to assert that each root of h in $\mathbb{F}_q$ lifts to a unique solution in $\mathbb{Q}_q$, that is, h splits completely in $\mathbb{Q}_q$.

This, in turn, implies that $L_{\mathfrak{q}} = \mathbb{Q}_q$ and the group $\mathrm{Gal}(L_{\mathfrak{q}}/\mathbb{Q}_q)$ is trivial. Equation (3.3) asserts that the same holds for $D_{\mathfrak{q}}$. This entails that the only automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ that fixes the prime ideal $\mathfrak{q}$ is the identity, and that the index $[\mathrm{Gal}(L/\mathbb{Q}) : D_{\mathfrak{q}}]$ of $D_{\mathfrak{q}}$ in $\mathrm{Gal}(L/\mathbb{Q})$ is equal to $|\mathrm{Gal}(L/\mathbb{Q})| = n$.

By the orbit-stabiliser theorem, $[\mathrm{Gal}(L/\mathbb{Q}) : D_{\mathfrak{q}}]$ is equal to the number of elements in the orbit $\mathrm{Orb}(\mathfrak{q})$ of $\mathfrak{q}$ under the action of $\mathrm{Gal}(L/\mathbb{Q})$. But since $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on set $\{\mathfrak{q}_1, \ldots \mathfrak{q}_g\}$, we have that $\mathrm{Orb}(\mathfrak{q}) = \{\mathfrak{q}_1, \ldots \mathfrak{q}_g\}$ and $|\mathrm{Orb}(\mathfrak{q})| = g$. Thus the number g of prime ideal factors of $q\mathcal{O}_L$ in (3.2) must be equal to n, which implies that q splits completely in L. □

With the proposition we have just proved in hand, we are now ready to prove the correctness of our algorithm. Before we do so, let look at yet another example illustrating why totally split primes are indeed a good choice for our finite field evaluation.

Example 3.2. *Consider an RIT instance 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 $\mathcal{O}_L = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.*

We can observe that 11 is a completely split prime and note that the principal ideal of $\mathcal{O}_L$ generated by 11 factors as $11\mathcal{O}_L = (4 + \sqrt{5})(4 - \sqrt{5})$. Since 11 totally splits in $\mathcal{O}_L$, we have $\mathcal{O}_L/\mathfrak{q} \cong \mathbb{F}_{11}$ 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 consequently 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 $5\mathcal{O}_L = (\sqrt{5})^2$. 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.

Similarly to Example 3.1, in the example above 5 is also not a suitable prime for computing in $\mathbb{F}_{5^2}$ as its inertial degree over $L = \mathbb{Q}(\sqrt{5})$ is equal to 1. An example of a prime with inertial degree 2 in this case is 7, as $7\mathcal{O}_L$ is itself already a prime ideal in $\mathcal{O}_L$.

3.4.1 Proof of correctness

Given a polynomial $h \in \mathbb{Z}[x]$ that is irreducible over $\mathbb{Q}$, the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of the splitting field L of h acts transitively on the roots of h [126, Proposition 22.3]. That is, for every pair of roots α, β of h, there exists an automorphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\alpha = \sigma(\beta)$. We show that a stronger notion of transitivity holds for our real radicals $\sqrt[d_i]{a_i}$.

Lemma 3.3. *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 [42, 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 now follows by repeated use of the Isomorphism extension theorem, cf. [126, 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 $\mathcal{S}$. □

In simple words, the lemma above asserts that given any two tuples $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ of solutions of the minimal polynomials $x^{d_1} - a_i$ of our input radicals, there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $(\alpha_1, \ldots, \alpha_k) = \sigma(\beta_1, \ldots, \beta_k)$.

We now show that for an instance of RIT, 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 $h(x) \in \mathbb{Z}[x]$ we denote by $\bar{h} \in \mathbb{F}_p[x]$ the reduction of h modulo p.

Lemma 3.4. *Let* p *be a prime that completely splits in* $\mathcal{O}_K$*, 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* $p \mid \mathrm{N}_{K/\mathbb{Q}}(f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}))$.

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 $p\mathcal{O}_K$. The quotient homomorphism $\mathcal{O}_K \to \mathbb{F}_p$ with kernel $\mathfrak{p}$ maps the d_i distinct roots of each polynomial $x^{d_i} - a_i$ in $\mathcal{O}_K$ 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 3.3, there is a homomorphism $\varphi : \mathcal{O}_K \to \mathbb{F}_p$ 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 $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = \varphi(f(\sqrt[d]{a_1}, \ldots, \sqrt[d]{a_k})) = 0$. For Item 2, note that the kernel of φ is a prime ideal of $\mathcal{O}_K$ lying above p. Thus if $\overline{f}(\overline{\alpha}_1, \ldots, \overline{\alpha}_k) = 0$ then $p \mid \mathrm{N}_{L/\mathbb{Q}}(f(\overline{\alpha}_1, \ldots, \overline{\alpha}_k))$. □

We have just shown that given an instance of RIT, the computation can be taken to a finite field $\mathbb{F}_p$ for some rational prime p. In Section 3.4.3 we discuss how to choose an appropriate prime p that satisfies the two conditions given in Lemma 3.4.

Lemma 3.3 plays an important role in the construction of our algorithm, and furthermore is one of the properties of the input to RIT that makes our technique difficult to generalise to more general identity testing problems. In particular, joint transitivity ensures that in Lemma 3.4(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, as illustrated in the following example.

Example 3.3. *Consider the polynomial $f(x_1, x_2) = x_2^2 - x_1x_2 + 1$ with input $\sqrt{2}$ and a primitive 8th root of unity ζ_8. The polynomial f vanishes at $(\sqrt{2}, \zeta_8)$. 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. 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 $\mathbb{Q}(\sqrt{2})$. This implies that as soon as we choose 6 as a representative for $\sqrt{2}$, we may only choose the roots of $(x^2 - 6x + 1)$ as representatives for ζ_8 in order for the computation to remain sound, whereas 2 is a root of the polynomial $(x^2 + 6x + 1)$ in $\mathbb{F}_{17}$.

Lemma 3.3 also ensures that deciding RIT can be reduced to deciding $\mathrm{HN}_{\mathbb{C}}$ by constructing a system of polynomial equations representing the intermediate computations of the circuit. We give this alternative way of proving that RIT belongs to the polynomial hierarchy in the next section.

3.4.2 A reduction placing RIT in the polynomial hierarchy

In the Introduction we recalled that arguably the simplest complexity bound for RIT can be obtained by reducing the problem to the existential theory of the reals, which is known to belong to **PSPACE**. The reduction involves constructing a system of polynomial equalities and inequalities representing the circuit, and calling to $\exists\mathbb{R}$ to determine whether it is satisfiable. Here the inequalities in the construction ensure that the solutions of the system are real positive radicals, and may seem necessary for the reduction to be sound. However, it turns out that once we observe the property of joint transitivity, we can avoid them completely, and simply reduce the problem to determining satisfiability of a system of polynomial equations.

We will now show how we can use this observation to apply the algorithm of [3, 8] for $\mathrm{HN}_{\mathbb{C}}$ to our problem, which allows us to give a first improvement on the **PSPACE** bound.

Corollary 3.5. *The* RIT *problem is in* **AM** *assuming GRH.*

Proof. The proof follows by a reduction to $\mathrm{HN}_{\mathbb{C}}$. Given an instance of RIT comprising an algebraic circuit C representing a k-variate polynomial f and radical inputs $\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}$, 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 $i = 1, \ldots, k$ as discussed in Section 3.3. We now construct a system of polynomial equations which is satisfiable over $\mathbb{C}$ if and only if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$.

To this end, we first add equations $x_i^{d_i} - a_i = 0$ for all $i \in \{1, \ldots, k\}$. We then introduce a new formal variable x_j for every gate of the circuit, adding the equations $x_j = x_\ell \odot x_m$ with $\odot \in \{+, -, \times\}$, where x_j is an $\odot$-gate, and x_ℓ and x_m are the two inputs of x_j in C. Finally, we add an equation $x_n = 0$ where x_n is the topmost (output) gate of the circuit.

The constructed system has a solution $(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_n) \in \mathbb{C}^n$ if and only if $f(\alpha_1, \ldots, \alpha_k) = 0$. Recall we denote by K the splitting field of the polynomial $\prod_{i=1}^{k}(x_i^{d_i} - a_i)$, and note that by construction, the first k coordinates of the solution will in fact belong to K^k. Now given $(\alpha_1, \ldots, \alpha_k) \in K^k$ satisfying $\alpha_i^{d_i} = a_i$ for $i \in \{1, \ldots, k\}$, the joint transitivity condition given in Lemma 3.3 asserts that there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = \sigma(\alpha_1, \ldots, \alpha_k)$. Hence $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = f(\sigma(\alpha_1, \ldots, \alpha_k)) = \sigma(f(\alpha_1, \ldots, \alpha_k))$. That is, $f(\alpha_1, \ldots, \alpha_k)$ is a Galois conjugate of $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k})$. Since the only Galois conjugate of zero is zero, $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$ if and only if $f(\alpha_1, \ldots, \alpha_k) = 0$.

The constructed system thus has a solution over $\mathbb{C}$ if and only if $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) = 0$. By [3, 8] verifying whether a system of polynomial equations has a solution over $\mathbb{C}$ can be done in **AM** assuming GRH, which completes our proof. □

Let us now go back to our main algorithm, which allows us to improve on this bound and place RIT in **coNP** assuming GRH.

3.4.3 Choice of the prime p for the non-deterministic algorithm

In Lemma 3.4 we have shown that a prime suitable for our finite field computation is one that splits completely in the number field K, and does not divide the norm $\mathrm{N}(\alpha)$ of the algebraic integer α computed by the circuit. In this section we show that we can always find such a prime of bitsize polynomial in the size of the input.

To this aim, let us first note that the norm $\mathrm{N}(\alpha)$ has at most $\log|\mathrm{N}(\alpha)|$ prime divisors. In simple terms, this means that if we have a set of $\log|\mathrm{N}(\alpha)|+1$ split primes, at least one of them will not be a divisor of $\mathrm{N}(\alpha)$. To upper-bound the number of prime divisors of $\mathrm{N}(\alpha)$, we thus first compute an upper bound on $|\mathrm{N}(\alpha)|$. Next, we compute a bound B such that the number of totally split primes in K of magnitude at most B is greater than $\log|\mathrm{N}(\alpha)|+1$. Since the computed bound B has bitsize polynomial in the size of the input instance, this completes our construction.

Recall that the norm of an algebraic number in a Galois field can be computed as the product of its Galois conjugates. Thus in order to bound the magnitude of $\mathrm{N}(\alpha)$, we need a bound on the number and the magnitude of the conjugates of α. Now the number of conjugates of an algebraic number in a Galois field is given by the cardinality of the Galois group, which is equal to the degree of number field itself. For our fixed instance of RIT, the latter can be bounded as follows.

Proposition 3.6. $|\mathrm{Gal}(K/\mathbb{Q})| \leq 2^{2s^2}$.

Proof. 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's are of magnitude at most 2^s, it follows that $d=\mathrm{lcm}(d_1,\ldots,d_k)$ is of magnitude at most 2^{s^2}. Thus the degree of K and hence the cardinality its Galois group over $\mathbb{Q}$ is at most 2^{2s^2}. □

We will repeatedly use the bound above in our reasoning. As a first application, we show the following bound on $\mathrm{N}(\alpha)$.

Lemma 3.7. *Denote by $\alpha\in\mathcal{O}_K$ the algebraic integer computed by C evaluated on the $\sqrt[d_i]{a_i}$. We have*

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

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 $b_i\leq 2^{2^s}$, and i ranges over all monomials of the shape $x_1^{e_{i_1}}\cdots x_k^{e_{i_k}}$. Let us denote by M the number of all such monomials, and count how many of them we can construct. Denote by $D=\max(d_1,\ldots,d_k)$, then

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

We can thus write

$$\begin{aligned}\mathrm{N}(\alpha) &= \mathrm{N}\left(\sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right) \\ &= \prod_{\sigma\in G} \sigma\left(\sum_{i=1}^{M} b_i x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right) \\ &= \prod_{\sigma\in G} \sum_{i=1}^{M} b_i \sigma\left(x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right).\end{aligned} \tag{3.4}$$

Denote by $G = \mathrm{Gal}(K/\mathbb{Q})$, and recall that by Proposition 3.6 $|G| \leq 2^{2s^2}$. Observe that the action of all $\sigma \in G$ is determined by their action on ζ_d, that is,

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

For every term $x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}$ appearing in α, we thus have

$$\sigma(x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}) = \sigma(x_1^{e_{i_1}}) \cdots \sigma(x_k^{e_{i_k}}) = x_1^{e_{i_1}} \cdots x_k^{e_{i_k}} \sigma(\zeta^d)^{\#e_i} ,$$

where $\#e_i = e_{i_1} + \cdots + e_{i_k}$. This observation in combination with Equation (3.4) allows us to write

$$\begin{aligned}|\mathrm{N}(\alpha)| &= \prod_{\sigma\in G} \sum_{i=1}^{M} \left|b_i \sigma\left(x_1^{e_{i_1}} \cdots x_k^{e_{i_k}}\right)\right| \\ &\leq \prod_{\sigma\in G} \sum_{i=1}^{M} |b_i| \left(\max_{j=1}^{k} |x_j|\right)^{\#e_i} |\sigma\left(\zeta_d\right)|^{\#e_i} \\ &= \prod_{\sigma\in G} \sum_{i=1}^{M} |b_i| \left(\max_{j=1}^{k} |x_j|\right)^{\#e_i} ,\end{aligned}$$

where the last equality follows since $|\zeta_d|$ is equal to 1, and the same holds for all of its conjugates.

Finally, putting together the bounds on $|G|$, M, b_i, x_i and $\#e_i$ yields

$$|\mathrm{N}(\alpha)| \leq \prod_{l=1}^{2^{2s^2}} \left(\sum_{l=1}^{2^{s^2}} 2^{2^s} \cdot (2^s)^{2^s}\right) = \prod_{l=1}^{2^{2s^2}} \left(\sum_{l=1}^{2^{s^2}} 2^{2^s(s+1)}\right).$$

We can further simplify this expression to write

$$|\mathrm{N}(\alpha)| \leq \left(2^{s^2} \cdot 2^{2^s(s+1)}\right)^{2^{2s^2}} = 2^{2^{2s^2}(s2^s+2^s+s^2)}.$$

For $s \geq 4$ the value above is at most $2^{2^{s^3}}$, which completes the proof. □

In the context of our algorithm, this means that if we find $2^{s^3} + 1$ primes that split completely in $\mathcal{O}_K$, at least one of them will not divide $\mathrm{N}(\alpha)$, and hence our finite field computation will be sound. We will now see how to ensure we are able to find enough primes splitting completely in $\mathcal{O}_K$ of bitsize polynomial in the size of the input to complete our reasoning.

To this aim, we use a quantitative version of the Chebotarev density theorem. As discussed in Section 2.3.6, 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 $\mathcal{O}_L$. The different classes of splitting patterns correspond to conjugacy classes of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of L. In our case, we are interested in completely split primes, which 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 $\pi_1(x)$ the number of completely split primes less or equal to x, the quantitative version of the theorem is as follows [143, 144].

Proposition 3.8 (Bound on $\pi_1(x)$)**.** *Assuming GRH,*

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

where c is an effective constant.

To obtain a bound on the number of split primes in our setting using the proposition above, we require a bound on the discriminant Δ_K of the number field K. Recall that given a $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\}$ of the ring of integers $\mathcal{O}_L$ of a number field L, the discriminant Δ_L is defined as the determinant of the matrix $\mathrm{tr}(b_i b_j)$ 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 $\mathcal{O}_L$ is not known to be feasible in polynomial time (see, e.g., [145, Theorem 1.3]). In order to avoid this computation, we upper-bound the discriminant using the discriminant of an order of our ring of integers $\mathcal{O}_K$ instead.

Recall that an order $\mathcal{O}$ in a number field L is a free $\mathbb{Z}$-submodule of $\mathcal{O}_L$ of rank $[L : \mathbb{Q}]$. Looking again at the number field $L = \mathbb{Q}(\sqrt{5})$ with ring of integers $\mathcal{O}_L = \mathbb{Z}[\frac{\sqrt{5}+1}{2}]$ we considered in Example 3.2, note that $\mathbb{Z}[\sqrt{5}] \subset \mathcal{O}_L$. In particular, $\mathbb{Z}[\sqrt{5}]$ is an order of index 2 in $\mathcal{O}_L$.

We have the following relation between the discriminant of the ring of integers $\mathcal{O}_L$ of a number field L and the discriminant of an order $\mathcal{O}$ of $\mathcal{O}_L$ (see, e.g., [127, Proposition 4.4.4]).

Proposition 3.9. *Suppose $\mathcal{O}$ is an order in $\mathcal{O}_L$. Then*

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

We will now see how to construct an order $\mathcal{O}$ of $\mathcal{O}_K$, the discriminant of which we can bound using a standard result in algebraic number theory. To this aim, we rely on the Primitive Element Theorem, which states that any number field L can be generated by adjoining a single element θ, called the primitive element, to $\mathbb{Q}$, i.e., $L = \mathbb{Q}(\theta)$. If $\theta \in \mathcal{O}_L$, then the subring $\mathbb{Z}[\theta]$ of $\mathcal{O}_L$ is an order of $\mathcal{O}_L$.

As discussed in Section 2.3, the proof of the Primitive Element Theorem is constructive, and computes the primitive element θ of a number field L as a linear combination of its generators. That is, if $L := \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, then $\theta = \sum_{i=1}^{k} c_i \alpha_i$. Furthermore, only finitely many combinations of the constants c_i fail to generate a primitive element for the field extension L. This gives rise to an effective version of the theorem (see Lemma 2.3), which induces a bound on the degree of the primitive element θ, as well as on the magnitude of the c_i's. We use this to construct a primitive element for our number field K.

Lemma 3.10. *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 $c_i \leq 2^{4s^2} + 1 \in \mathbb{Z}$ and $\deg \theta \leq 2^{2s^2}$.

Proof. We follow the proof of the Primitive Element Theorem and use Lemma 2.3 inductively to compute the bounds on the degree of θ and the size of the constants c_i. Recall that Lemma 2.3 states that given α and β of respective degrees ℓ and m over $\mathbb{Q}$, there exists $c \in \{1, \ldots, \ell^2 m^2 + 1\}$ such that $\alpha + c\beta$ is a primitive element of $\mathbb{Q}(\alpha, \beta)$.

For $j \in \{1, \ldots, k\}$, define $\theta_j = \sum_{i=0}^{j} c_i \sqrt[d_i]{a_i}$ to be the primitive element of the field $\mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_j]{a_j})$. Note that since for all $i \in \{1, \ldots, k\}$, $\deg \sqrt[d_i]{a_i} \leq 2^s$, the degree of θ_j is at most $2^{j \cdot s}$.

Now for every $j \in \{2, \ldots, k\}$, $\theta_j = \theta_{j-1} + c_j \sqrt[d_j]{a_j}$, where $\deg \theta_{j-1} \leq 2^{(j-1)\cdot s}$ and $\deg \sqrt[d_j]{a_j} \leq 2^s$, hence by Lemma 2.3,

$$c_j \leq (2^s)^2 (2^{(j-1)\cdot s})^2 = 2^{j \cdot 2s} + 1.$$

Since $k \leq s$, the value above is upper bounded by $2^{4s^2} + 1$ for all j.

Finally, let $\theta = c_0 \zeta_d + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} + c_0 \zeta_d + \theta_k$. Recall that since $d_1, \ldots, d_k \leq 2^s$, their least common multiple is upper-bounded by 2^{s^2}, and hence $\deg \zeta_d \leq 2^{s^2}$. Thus $\deg \theta \leq 2^{2s^s}$ and by Lemma 2.3,

$$c_0 \leq (2^{s^2})^2 (2^{k \cdot s})^2 + 1 \leq 2^{4s^2} + 1.$$

□

Note that in general, we may choose the constants $c_i \in \mathbb{Q}$ with only finitely many combinations of the c_i's not yielding a primitive element — thus the primitive element need not be an algebraic integer in general. However, by picking $c_i \in \mathbb{Z}$ we ensure the minimal polynomial f_θ of θ is monic and θ an algebraic integer. Henceforth, we fix a primitive element θ for our number field K, computed as in Lemma 3.10. Now Proposition 3.9 suggests that $\Delta_K \leq \Delta_{f_\theta}$, where $\Delta_{f_\theta} = \mathrm{Disc}(\mathbb{Z}[\theta])$.

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

$$\Delta_f = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2 = (-1)^{\frac{\mathrm{N}(n-1)}{2}} a_n^{2n-2} \prod_{i \neq j} (r_i - r_j) \,. \tag{3.5}$$

We use Equation (3.5) to obtain the following bound.

Lemma 3.11 (Bound on the discriminant)**.** *We have*

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

for $s \geq 4$.

Proof. Denote by $G = \mathrm{Gal}(K/\mathbb{Q})$ the Galois group of K. By Lemma 3.10, we construct the primitive element $\theta = c_o \zeta_d + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i}$, where $c_i \in \mathbb{Z}$ with $c_i \leq 2^{4s^2}$ for all $i \in \{0, \ldots, k\}$. The minimal polynomial f_θ of θ has roots $\theta = \theta_1, \ldots, \theta_{|G|}$, which are given by the elements of G. That is, $\theta_i = \sigma_j(\theta)$ for some $\sigma_j \in G$. 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 $\alpha \in K$, $\sigma_j(\alpha) = \alpha \zeta_d^t$ for some $t \leq d$.

Now given $\sigma_j \in G$, write

$$\begin{aligned}
\sigma_j(\theta) &= \sigma_j \left(c_0 \zeta_d + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \right) \\
&= c_0 \sigma_j(\zeta_d) + \sum_{i=1}^{k} c_i \sigma_j(\sqrt[d_i]{a_i}) \\
&= c_0 \zeta_d^{j_0} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \zeta_d^{j_i} .
\end{aligned}$$

Then for $1 \leq j, \ell \leq |G|$ with $j \neq \ell$

$$\begin{aligned}
\sigma_j(\theta) - \sigma_\ell(\theta) &= \left(c_0 \zeta_d^{j_0} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \zeta_d^{j_i} \right) - \left(c_0 \zeta_d^{\ell_0} + \sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \zeta_d^{\ell_i} \right) \\
&= c_0 \left(\zeta_d^{j_0} - \zeta_d^{\ell_0} \right) + \left(\sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \right) \left(\zeta_d^{j_i} - \zeta_d^{\ell_i} \right) .
\end{aligned}$$

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

$$\sigma_j(\theta) - \sigma_\ell(\theta) \leq 2c_0 + 2 \left(\sum_{i=1}^{k} c_i \sqrt[d_i]{a_i} \right) .$$

By using the bounds shown in Lemma 3.10, we can rewrite the inequality above as

$$\begin{aligned}\sigma_j(\theta) - \sigma_\ell(\theta) &\leq 2 \cdot (2^{4s^2} + 1) + 2\left(\sum_{i=1}^{s}(2^{4s^2} + 1) \cdot 2^s\right) \\ &\leq 2^{4s^2+2} + s \cdot 2^{4s^2+s+2}.\end{aligned}$$

For $s \geq 4$, the value above is at most 2^{2s^3}, hence

$$|\Delta_{f_\theta}| = |\prod_{j\neq\ell}(\sigma_j(\theta) - \sigma_\ell(\theta))| \leq \left(2^{2s^3}\right)^{|G|^2}.$$

We now employ the bound on $|G|$ to write

$$|\Delta_{f_\theta}| \leq \left(2^{2s^3}\right)^{\left(2^{2s^2}\right)^2} = 2^{2s^3 \cdot 2^{4s^2}}.$$

Noting that for $s \geq 4$, the value above is at most $2^{2^{5s^2}}$ completes the proof. □

Recall that our aim was to find enough totally split primes p of bitsize polynomial in s so that at least one of them does not divide the norm of the computed algebraic integer. In concrete words, we would like to ensure that B such that $\pi_1(B) \geq 2^{s^3} + 1$ can be chosen of bitsize polynomial in s. Using Lemma 3.11 in combination with the effective version of the Chebotarev density theorem in Proposition 3.8, we claim that this is the case for $B \geq 2^{4s^3}$.

Lemma 3.12. *Assuming GRH,*

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

Proof. We will use the bound on π_1 given in Proposition 3.8

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

which we rewrite as

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

by replacing the prime counting function $\pi(x)$ by $\frac{x}{\log x}$.

Lemma 3.11 in combination with Proposition 3.9 implies that $\Delta_K \leq 2^{2^{5s^2}}$. Recall also that $|\operatorname{Gal}(K/\mathbb{Q})| \leq 2^{2s^2}$ as shown in Proposition 3.6 and Lemma 3.10.

We can thus write

$$\begin{aligned}\pi_1(2^{4s^3}) &\geq \frac{1}{2s^2}\left(\frac{2^{4s^3}}{4s^3} - 2^{5s^2} - c \cdot 2^{2s^3} \cdot 2^{5s^2} - c \cdot 2^{2s^3} \cdot 2^{2s^2} \cdot 4s^3\right) \\ &= \frac{2^{4s^3}}{2^{2s^2} \cdot 4s^3} - 2^{3s^2} - c \cdot 2^{2s^3} \cdot 2^{3s^2} - c \cdot 2^{2s^3} \cdot 4s^3.\end{aligned}$$

Note that for $s \geq 4$, $2^{2s^2} \cdot 4s^3 \leq 2^{s^3}$ and $2^{3s^2} \leq 2^{2s^3}$, which allows us to rewrite the inequality above as

$$\begin{aligned}\pi_1(2^{4s^3}) &\geq \frac{2^{4s^3}}{2^{s^3}} - 2^{2s^3} - c \cdot 2^{2s^3} \cdot 2^{3s^2} - c \cdot 2^{2s^3} \cdot 4s^3 \\ &= 2^{2s^3}(2^{s^3} - 1 - c \cdot 2^{3s^2} - c \cdot 4s^3) \geq 2^{2s^3}.\end{aligned}$$

Finally, for a fixed constant c and $s \geq \max(c, 5)$ the inequality rewrites as

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

which completes the proof. □

3.4.4 The coNP algorithm for RIT

In the previous section we have shown that there exists a prime p suitable for our finite field evaluation that is of bitsize polynomial in the size of the RIT instance. We can now finally state our algorithm, see Figure 3.3, and prove its complexity.

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 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.
Step 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 $\overline{\alpha}_i^{d_i} \equiv a_i \pmod{p}$.
Step 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 3.3 – Our nondeterministic algorithm for the complement of RIT.

Theorem 3.13. *The* RIT *problem is in* **coNP** *assuming GRH.*

Proof. Figure 3.3 presents a nondeterministic polynomial time algorithm for the complement of RIT 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 3.10.

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 $\overline{\alpha}_i^{d_i} \equiv a_i$

$(\mathrm{mod}\ p)$ 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**. Suppose $f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}) \neq 0$. Under GRH, the lower bound in Lemma 3.12 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

- $p \nmid \mathrm{N}(f(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_k]{a_k}))$, 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 3.4, 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 representation $\overline{\alpha}_1, \ldots, \overline{\alpha}_k$ of the 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 3.4, which concludes the proof. □

3.5 The complexity of 2-RIT

Our algorithm for RIT uses non-determinism to guess a suitable prime p in order for the computation in $\mathbb{F}_p$ to be sound. It is natural to wonder whether such primes can instead be randomly sampled. This is what is done, say, in the **coRP** algorithm for deciding ACIT [1], or the **BPP** algorithm for CIT [32] that we are adapting. Recall we require that the prime p have bitsize polynomial in the size of the input, and that the congruences $x^{d_i} \equiv a_i \pmod{p}$ are solvable in $\mathbb{F}_p$. In order to be able to choose the prime randomly, we would require the density of split primes to be polynomial in s^{-1}. However, by the Chebotarev density theorem, the density of such primes is roughly $\frac{1}{|\mathrm{Gal}(K/\mathbb{Q})|}$. Since the size of the Galois group of K over $\mathbb{Q}$ is exponential in the size of the input, totally split primes do not have sufficient density in order to directly be chosen randomly. The density remains insufficient even if the radicals are square roots.

Let us note that in the CIT setting, the degree of the number field may also be exponential in the size of the input, however, randomisation is possible as the suitable primes all lie in one arithmetic progression. Indeed, the authors of [32] use the fact that a prime p is totally split for a cyclotomic field $\mathbb{Q}(\zeta_n)$ if and only if $p \equiv 1 \pmod{n}$. This, in particular, implies that all primes suitable for the finite field computation lie in the arithmetic progression $n\mathbb{N} + 1$. Now Dirichlet's theorem on the density of primes in arithmetic progressions asserts that the proportion of all primes lying in $n\mathbb{N}+1$ is roughly $\frac{1}{\varphi(n)}$. That is, the function counting primes in $n\mathbb{N} + 1$ is asymptotically equivalent to $\frac{x}{\varphi(n)\ln x}$. An effective version of Dirichlet's theorem then implies that assuming GRH, the density is high enough in order for the algorithm to choose a suitable prime randomly.

In general, given a radical number field, the totally split primes need not lie in one arithmetic progression. However, we observe that if the radical number field is generated by square roots of odd primes, then a majority of totally split primes lie in a certain arithmetic

progression, and the density of split primes within this progression is good. We apply this intuition to the 2-RIT problem, which recall, is the identity testing problem for an algebraic circuit C evaluated on square roots $\sqrt{a_1}, \ldots, \sqrt{a_k}$ for k odd rational primes $a_1, \ldots, a_k$. In particular, we show that 2-RIT is in **coRP** assuming GRH, and in **coNP** unconditionally.

The proofs from Section 3.4.1 ensure that the finite field computation in our algorithm is sound. In this section, we show how to choose a completely split prime p and determine the solutions to the equations $x^2 \equiv a_i \pmod{p}$ in $\mathbb{F}_p$. That is, we 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 $\sqrt{a_1}, \ldots, \sqrt{a_k}$. To this aim, we use 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 $\{1, -1, 0\}$, defined as

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

The Legendre symbol can be defined explicitly as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}.$$

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

Let us now see how we apply the law of quadratic reciprocity in order to choose the right field $\mathbb{F}_p$ for deciding 2-RIT. Recall that 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, we require a_i to be 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 $4\mathbb{N} + 1$, i.e., 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 the latter, it suffices to choose p such that $p \equiv 1 \pmod{a_i}$ for all i. Indeed, as 1 is a perfect square modulo a_i for all i, $p \equiv 1 \pmod{a_i}$ implies that p is a quadratic residue modulo a_i.

We have just argued that if we choose p satisfying all the above-mentioned congruences, the polynomials $x^2 - a_i$ all split and have non-zero roots in $\mathbb{F}_p$. Furthermore, following Pocklington's algorithm, if $p \equiv 5 \pmod{8}$, there is a deterministic way to solve the

equations $x^2 - a_i$. In particular, writing $p = 8m + 5$, the solution of the equation $x^2 \equiv a \pmod{p}$ is given by the following function.

$$x = \begin{cases} \pm a^{m+1} & \text{if } a^{2m+1} \equiv 1 \pmod{p}, \\ \pm \frac{y}{2} & \text{if } a^{2m+1} \equiv -1 \pmod{p} \text{ and} \\ & y = \pm(4a)^{m+1} \text{ is even}, \\ \pm \frac{p+y}{2} & \text{if } a^{2m+1} \equiv -1 \pmod{p} \text{ and} \\ & y = \pm(4a)^{m+1} \text{ is odd}. \end{cases} \tag{3.6}$$

Let us briefly elaborate on the correctness of the function above. 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 $a^{4m+2} \equiv 1 \mod p$. We now consider two separate cases for a:

(i) If $a^{2m+1} \equiv 1 \mod p$, then $a^{2m+2} \equiv a \mod p$. That is, $(a^{m+1})^2 \equiv a \mod p$, hence $x = \pm a^{m+1}$.

(ii) For the case when $a^{2m+1} \equiv -1 \mod p$, first note that 2 is a quadratic non-residue since $p \equiv 5 \mod 8$. Hence $4^{2m+1} \equiv -1 \mod p$ and $4^{2m+1}a^{2m+1} \equiv 1 \mod p$. 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 $y^2 = 4a$. Thus $x = \pm\frac{y}{2}$, or if y is odd, $x = \pm\frac{p+y}{2}$.

We now show how to construct an arithmetic progression such that all primes p in the progression satisfy the above congruences. Let us first note that the congruence $p \equiv 5 \pmod{8}$ encompasses the restriction on p being congruent to 1 modulo 4. Denote by $A = \prod_{i=1,a_i}^{k} a_i$ the product of all input radicands a_i and notice that since the a_i's are odd primes, their product A is also an odd number. Let us look now at the arithmetic progression

$$8A\mathbb{N} + b + 1, \tag{3.7}$$

where b is a solution of the following system of equations

$$\begin{aligned} b &\equiv 4 \pmod{8} \\ b &\equiv 0 \pmod{a_i} \text{ for all } a_i. \end{aligned} \tag{3.8}$$

Since all the moduli in the equations (3.8) 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 suitable for our finite field computation. 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

$$\Big\{p \leq 2^{5s^3} \mid p \in 8A\mathbb{N} + b + 1 \text{ where } A = \prod_{i=1}^{k} a_i \text{ and } b \text{ is a solution of (3.8)}\Big\}. \tag{3.9}$$

We now show that the density of primes in the set $S(a_1, \ldots, a_k)$ is high enough in order to randomly sample them in our 2-RIT algorithm. To this aim, we rely on effective versions of Dirichlet's theorem on the density of primes in an arithmetic progression. In particular,

we make use of the following estimates, which have been shown in [146, Chapter 20, page 125] and [147, Corollary 18.8], respectively.

Theorem 3.14. *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 $n < c_1 x^{c_1}$,

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

Applying the results above to arithmetic progression defining the set $S(a_1, \ldots, a_k)$, we show the following.

Proposition 3.15. *Let C be an algebraic circuit of size at most s, and $a_1, \ldots, a_k$ primes of bit-length at most s. Denote by α the algebraic integer obtained by evaluating C on the $\sqrt{a_i}$. Suppose that p is chosen uniformly at random from the set $S(a_1, \ldots, a_k)$ defined in (3.9). 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 $\mathrm{N}(\alpha)$ is at most 2^{-s^3} unconditionally.

Proof. We follow the proof of [32, 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 3.14, the probability that p is prime is at most

$$\frac{\pi_{8A,b+1}(2^{5s^3})}{2^{5s^3}/8A} \geq \frac{8A}{\varphi(8A)\cdot\log 2^{5s^3}} - \frac{c\cdot\log 2^{5s^3}\cdot 8A}{(2^{5s^3})^{1/2}}.$$

Since $\varphi(n) \leq n$ for all $n \in \mathbb{N}$ and $(2^{5s^3})^{1/2} \geq 2^{2s^3}$, the inequality rewrites as

$$\frac{\pi_{8A,b+1}(2^{5s^3})}{2^{5s^3}/8A} \geq \frac{1}{5s^3} - \frac{c\cdot 5s^3\cdot 2^{s^2+3}}{2^{2s^3}}.$$

For $s \geq 2$, we have $2^{s^2+3} \leq 2^{s^3}$ and hence

$$\frac{\pi_{8A,b+1}(2^{5s^3})}{2^{5s^3}/8A} \geq \frac{1}{5s^3} - \frac{c5s^3 2^{s^3}}{2^{2s^3}},$$

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

For (ii), by Lemma 3.7 the norm of α has absolute value at most $2^{2^{s^3}}$, and hence $\mathrm{N}(\alpha)$ has at most 2^{s^3} distinct prime factors. Then the probability that p divides $\mathrm{N}(\alpha)$ given that p is prime is at most

$$\frac{\Pr\left(p \mid \mathrm{N}(\alpha)\right)}{\Pr\left(p \text{ prime}\right)} \leq \frac{6s^3\cdot 8A\cdot 2^{s^3}}{2^{5s^3}}$$

which is at most 2^{-s^3} for s sufficiently large. □

With Proposition 3.15 in hand, we can state our algorithm, see Figure 3.4, and prove its complexity.

Radical Identity Testing for square root inputs	
Input:	Algebraic circuit C of size at most s and a list of k odd 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 (3.9).
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 (3.6).
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 3.4 – Our randomised polynomial time algorithm for the complement of 2-RIT.

Theorem 3.16. *The* 2-RIT *problem is in* **coRP** *assuming GRH and in* **coNP** *unconditionally.*

Proof. Figure 3.4 presents a randomised polynomial time algorithm for the complement of 2-RIT. It is clear that the algorithm runs in polynomial time; we will now argue its correctness.

First, suppose that $f(\sqrt{a_1}, \ldots, \sqrt{a_k}) = 0$. By Lemma 3.4, we have $\overline{f}(\alpha_1, \ldots, \alpha_k) = 0$, and hence the output is 'Zero'. Second, suppose that $f(\sqrt{a_1}, \ldots, \sqrt{a_k}) \neq 0$. Then the output will be 'Non-Zero' provided that p does not divide $\mathrm{N}(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$. By Proposition 3.15(ii), the probability that p does not divide $\mathrm{N}(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$ is at least $1 - 2^{-s^3}$. Thus, the probability that the algorithm gives the wrong output is at most 2^{-s^3}.

It remains to show that 2-RIT is in **coNP** unconditionally. The idea is to modify the algorithm in Figure 3.4, replacing randomisation with guessing. Theorem 3.14 shows that

$$\pi_{8A,b+1}(2^{3s^3}) > 2^{s^3} \tag{3.10}$$

for s sufficiently large. It follows that there exists a prime $p \leq 2^{3s^3}$ that does not divide $\mathrm{N}(f(\sqrt{a_1}, \ldots, \sqrt{a_k}))$. The rest of the argument follows as in the proof of Theorem 3.13. □

Note that 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 progres-

sions is not strong enough for our purposes (due to the presence of a $\sqrt{x}$ factor in the denominator in Theorem 3.14(ii)): The number of primes less than 2^{3s^3} which are favourable is just 2^{s^3}, as computed in (3.10). 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.

3.6 Discussion and perspectives

In this chapter we studied the Radical Identity Testing problem, and improved on the previously known **PSPACE** bound, placing the problem in **coNP** assuming GRH. We also considered a restricted variant of the problem, namely 2-RIT, and showed it is in **coRP** assuming GRH, and in **coNP** unconditionally.

Our algorithms work by reducing the polynomials modulo a "small" prime p and performing the computation in the finite field $\mathbb{F}_p$. Intrinsically, we choose a prime p such that the finite field $\mathbb{F}_p$ corresponds to the quotient of the ring of integers $\mathcal{O}_K$ of the Galois field K containing the radical inputs by a well-chosen prime ideal. The underlying approach is analogous to that in the work [32] on CIT and preceding works on versions of ACIT such as [1], however, the correctness proof is more involved. The Galois group in the case of a radical extension is not abelian anymore, which precludes a direct generalisation of the results in the cyclotomic case. Ensuring the correctness of our procedure, in particular, involves identifying a special transitivity condition on the Galois group of K over $\mathbb{Q}$. Notably, we observe that the group acts jointly transitively on the tuples of the conjugates of the input radicals. In Example 3.3 we show that the transitivity condition is crucial in our approach, whereas it has no equivalent in [32]. Furthermore, as opposed to the cyclotomic setting, the ring of integers of the number field K here is no longer monogenic, and computing the basis of $\mathcal{O}_K$ is not known to be tractable.

In Section 3.4.2 we further employ the joint transitivity condition to show that the RIT problem also belongs to the complexity class **AM**. This in combination with our main result places RIT in $\mathbf{coNP} \cap \mathbf{AM}$ assuming GRH. This indicates that RIT most likely is not **coNP**-hard, as the result $\mathbf{coNP} \subseteq \mathbf{AM}$ would imply that the polynomial hierarchy collapses to **AM** [148]. A natural question that arises now is whether this complexity bound for RIT really is tight. One way to indicate this could be to relate RIT to another problem known to belong to $\mathbf{coNP} \cap \mathbf{AM}$, such as the graph, group or ring non-isomorphism problem.

In our overview of identity testing for expressions in Section 1.1, we discussed existing results for the case when the polynomial is given in a sparse representation. In particular, we outlined a deterministic polynomial time algorithm developed for the problem, noting however, that the algorithm only works for certain subvariants of the sparse-RIT problem. As any sparse polynomial can also be represented by a polynomial size circuit, our result on RIT also gives an upper bound for the general version of sparse-RIT (as well as the RadP problem, as discussed in Section 1.1). This furthermore implies a complexity bound on the sparse-GRIT problem, which, recall, given a sparse polynomial $f \in \mathbb{Z}[x_1, \ldots, x_k]$, asks

to determine whether there exist radicals $\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}$ such that $f(\sqrt[d_1]{a_1}, \ldots \sqrt[d_k]{a_k}) = 0$. Assuming GRH, sparse-GRIT can be placed in the second level of the polynomial hierarchy, namely in Σ_2. Indeed, the algorithm first non-deterministically guesses a polynomial-size certificate (a list of k radicands $a_1, \ldots, a_k$ with respective degrees $d_1, \ldots, d_k$ that make the input polynomial vanish), which via our RIT algorithm can be verified in **coNP**.

Open questions. In Section 3.3.1 we have shown that a clever modification of the reduction proposed [42] allows us to place the general version of the bounded-RIT problem, wherein the input degrees d_i are given in binary, in **coRP**. Can a similar argument, possibly in combination with our joint transitivity condition, help to improve the complexity of the general version of sparse-RIT as well?

As discussed above, it is not clear whether the complexity bound we have proved for RIT is tight. Let us point out that the authors of [32] observed that CIT is at least as hard as PIT, which is known to be **P**-hard [149, Theorem 2.4.6, Theorem 2.6.3]. It is not difficult to see that the same can be said for RIT, but can we show any tighter hardness results for RIT?

The observation that RIT is at least **P**-hard implies that the general variant of RIT does not admit efficient parallel algorithms. In the Introduction we recalled that efficient parallel algorithms have been developed for variants of the sparse-RIT problem. In the circuit setting the following question still remains open: Are there any subclasses of RIT which are efficiently parallelisable?

Considering the underlying similarities of our approach and the CIT algorithm in [32], a next natural generalisation would be to inspect the complexity of determining whether a polynomial represented by an algebraic circuit vanishes on an input comprising real radicals and a primitive root of unity. As shown in Example 3.3, joint transitivity does not hold anymore in this setting, hence such a generalisation would require new insights on the Galois group of the underlying field. A first step in this direction may be to consider the combination of 2-RIT and CIT, i.e., an input comprising positive square roots alongside a primitive root of unity. In this case, the Galois group of the input is abelian, as both cyclotomic fields and multi-quadratic extensions are known to be abelian, and the compositum of two abelian Galois extension is abelian as well. To see this, suppose that K and L are both Galois extensions of a field k. Then the map $\mathrm{Gal}(KL/k) \to \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k)$ is an injective group isomorphism (see, e.g., [150, Chapter VI, Theorem 1.14]). Hence if K and L are abelian, then $\mathrm{Gal}(KL/k)$ must be abelian too. As discussed in Section 1.1, abelian Galois groups are better understood algorithmically than solvable Galois groups, which may help in designing the algorithm for the problem we just posed. Considering that CIT and 2-RIT both admit randomised polynomial time algorithms, we may even wonder whether their combination does as well? Could the latter be the case if the degree of the input circuit is bounded?

A related, more general question that may help in improving the complexity of the problem we just posed is to determine, given real radicals and an nth primitive root of unity, whether the root of unity already exists in the Galois closure of the extension generated by the radicals. Or, in other words, does the nth cyclotomic polynomial factor into lower-

degree factors in the radical field?

Finally, throughout our survey on identity testing in number fields, we have seen its relation to the Galois group of the field at hand. As mentioned in Section 1.1, computational problems on Galois groups for radical field extensions are not yet well-understood. The best known results are on the problem of determining the order of a Galois group of such an extension, which has been shown to belong to the second level of the polynomial hierarchy [48]. Can the insights we have on the RIT problem be used in more general Galois group problems, such as efficient random sampling of automorphisms of a Galois group of a radical extension? Or could the Galois group of a field extension be handled algorithmically when given an oracle for identity testing over that field?

Chapter 4

A parametric version of the Hilbert Nullstellensatz problem

In this chapter we study a parametric version of the Hilbert Nullstellensatz problem, which asks whether a system of multivariate polynomials with coefficients in $\mathbb{Z}[\boldsymbol{x}]$ has a solution in $\overline{\mathbb{Q}(\boldsymbol{x})}$ for $\boldsymbol{x} := (x_1, \ldots, x_m)$. We further consider the problem of determining the dimension of an algebraic variety defined by such a system.

We recall that over $\mathbb{C}$, the two respective related problems are the Hilbert Nullstellensatz problem ($\mathrm{HN}_{\mathbb{C}}$) which, given $f_1, \ldots, f_k \in \mathbb{Z}[y_1, \ldots, y_n]$, asks whether the system admits a common solution over $\mathbb{C}^n$, and the dimension problem ($\mathrm{DIM}_{\mathbb{C}}$), which, given $f_1, \ldots, f_k \in \mathbb{Z}[y_1, \ldots, y_n]$ and an integer d, asks whether the subvariety of $\mathbb{C}^n$ defined by the system is of dimension at least d.

The results presented in this chapter are based on a joint work with Rida Ait El Manssour, Nikhil Balaji, Mahsa Shirmohammadi, and James Worrell [151].

Organisation of the chapter. We begin this chapter by recalling notation and some simplifications that we may apply without loss of generality to the systems of polynomials we consider in Section 4.1. In Section 4.2 we introduce a number-theoretic approach to the parametric HN problem ($\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ for short), which generalises the **AM** algorithm for $\mathrm{HN}_{\mathbb{C}}$. We give an overview of the approach in Section 4.2.1, then turn our attention to unsatisfiable systems in Section 4.2.2 and satisfiable ones in Section 4.2.3. We combine the results for the two kinds of systems in Section 4.2.4 and reduce the problem to $\mathrm{HN}_{\mathbb{C}}$.

In Section 4.3 we look at the $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ problem from a geometric point of view. We observe that a system of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ has a solution in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ for $\boldsymbol{x} := (x_1, \ldots, x_m)$ if and only if the parameters $x_1, \ldots, x_m$ when treated as variables are algebraically independent in the coordinate ring $\mathbb{C}[V]$ of the variety V the system defines in $\mathbb{C}^{m+n}$ (which implies that V has dimension at least m). We give examples illustrating the geometry behind the problem, and then formally relate the parametric dimension of a variety to its complex dimension in Section 4.3.1. We thus show how the existing algorithm

for the $\mathrm{DIM}_{\mathbb{C}}$ problem can be used to reduce $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$ in Section 4.3.2.

We conclude the chapter by comparing the approaches we developed and possible generalisations in Section 4.4.

Relevant preliminaries. The preliminary sections useful for reading this chapter are Sections 2.2, 2.3.1 to 2.3.3, 2.3.7 and 2.4.2.

4.1 Notation and initial simplifications

Let $\boldsymbol{x} := (x_1, \ldots, x_m)$, and recall that $\overline{\mathbb{Q}(\boldsymbol{x})}$ denotes the algebraic closure of the field of rational functions in m variables over $\mathbb{Q}$. We investigate the complexity of deciding whether the system of polynomial equations

$$f_1(y_1, \ldots, y_n) = 0, \ \ldots, \ f_k(y_1, \ldots, y_n) = 0 \tag{4.1}$$

with $f_i \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ has a solution in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$. We call this the Hilbert Nullstellensatz problem over $\overline{\mathbb{Q}(\boldsymbol{x})}$, and abbreviate it as $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$.

Assumption on the degrees and coefficients of the f_i's and the size of the system. We consider systems with coefficients in $\mathbb{Z}[\boldsymbol{x}]$. This is without loss of generality since any system with coefficients in $\mathbb{Q}(\boldsymbol{x})$ can be transformed by scaling to one with coefficients in $\mathbb{Z}[\boldsymbol{x}]$ that has the same solution set over $\overline{\mathbb{Q}(\boldsymbol{x})}$.

It is customary to describe the system by its *size*, which we define to be the maximum of the number m of *parameters*, number n of variables, number k of polynomials, the logarithm of the degrees of the polynomials in $\boldsymbol{x}$ and $\boldsymbol{y}$, and the bitsize of the integer coefficients.

We assume that the degrees of the polynomials f_i in $\boldsymbol{x}$ and $\boldsymbol{y}$ are at most 2 and the integer constants of bitsize at most 1. We claim this assumption is without loss of generality. Indeed, given a polynomial in a sparse representation, the degree of the system and the integer constants of the coefficients can be at most exponential in the system's size. By introducing new intermediate variables and repeated squaring, we obtain a new system of polynomials of degree at most 2, constants of bitsize 1, and system size polynomial in the size of the input. In what follows, the size of the systems we consider is thus equal to $\max(m, n, k)$.

4.2 A number-theoretic approach to parametric HN

We approach the $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ problem with the aim of generalising Koiran's **AM** protocol for $\mathrm{HN}_{\mathbb{C}}$ [8], which relies on examining the satisfiability of the system modulo primes p. Technically speaking, for each one of the primes p, his idea can be understood as performing the evaluation under a ring homomorphism, whose kernel is a prime ideal above p.

We tackle $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ by studying the satisfiability of the system over $\mathbb{C}$ when specialised at a given vector of values $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_m)$ in $\mathbb{C}^m$. That is, we reduce our problem to that of examining the satisfiability of the system under a ring homomorphism

$$\varphi_{\boldsymbol{\alpha}} : \mathbb{Q}[\boldsymbol{x}][y_1, \ldots, y_n] \to \mathbb{Q}[\boldsymbol{\alpha}][y_1, \ldots, y_n] \,.$$

By choosing the specialisation $\boldsymbol{\alpha}$ randomly, we exhibit a **BPP** reduction of our problem to $\mathrm{HN}_{\mathbb{C}}$, which by [8] allows us to conclude that $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}} \in \mathbf{AM}$, and thus in the polynomial hierarchy. We give a more detailed overview of the approach in Section 4.2.1.

Let $\boldsymbol{x} := (x_1, \ldots, x_m)$ and $\boldsymbol{y} := (y_1, \ldots, y_n)$. Throughout Section 4.2, we fix an instance of $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ comprising a system $\mathcal{S}$ of polynomial equations in $\mathbb{Z}[\boldsymbol{x}][\boldsymbol{y}]$ as in (4.1). As discussed in Section 4.1, we assume the degree of the polynomials in $\boldsymbol{x}$ and $\boldsymbol{y}$ to be at most 2. We write s to denote the size of our fixed instance.

Given $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_m) \in \mathbb{C}^m$, we denote by $\mathcal{S}_{\boldsymbol{\alpha}}$ the system $\mathcal{S}$ specialised at $x_i = \alpha_i$ for $i \in \{1, \ldots, m\}$.

4.2.1 Overview of the approach

In order to compute the probability that the system $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable over $\mathbb{C}$, when $\boldsymbol{\alpha}$ is an integer point chosen uniformly at random in a fixed range, we rely on the Schwartz-Zippel Lemma [16, 17, 18], which we recall here.

Lemma 4.1 (Schwartz–Zippel). *Let $f \in K[x_1, \ldots, x_n]$ be a non-zero polynomial of total degree $d \geq 0$ over a commutative ring K. Let S be a finite subset of K and let $r_1, \ldots, r_n$ be selected independently and uniformly at random from S. Then*

$$\Pr\left(f(r_1, \ldots, r_n) = 0\right) \leq \frac{d}{|S|}.$$

We will now give a brief overview of how we use the Schwartz-Zippel Lemma in combination with algebraic and number-theoretic arguments in order to decide $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$.

Unsatisfiable systems. Assume that $\mathcal{S}$ is not satisfiable in $\overline{\mathbb{Q}(\boldsymbol{x})}$. The weak version of Hilbert Nullstellensatz implies that the ideal generated by $f_1, \ldots, f_k$ contains the constant 1. In particular, there must exist a non-zero polynomial $a \in \mathbb{Z}[\boldsymbol{x}]$ and polynomials $g_1, \ldots, g_k \in \mathbb{Z}[\boldsymbol{x}][\boldsymbol{y}]$ such that

$$a = g_1 f_1 + \cdots + g_k f_k.$$

Observe that if the above equation holds in $\overline{\mathbb{Q}(\boldsymbol{x})}$, the system $\mathcal{S}$ can only have a solution when specialised at $\boldsymbol{\alpha} \in \mathbb{C}^m$ if $\boldsymbol{\alpha}$ is a zero of $a(\boldsymbol{x})$. An effective parametric version of Hilbert's Nullstellensatz [99, Theorem 5 and Corollary 4.20] gives a degree bound on $a(\boldsymbol{x})$. We may thus apply the Schwartz-Zippel Lemma to deduce a bound on the probability that $a(\boldsymbol{\alpha}) = 0$, and hence an upper-bound on the probability of $\mathcal{S}_{\boldsymbol{\alpha}}$ admitting a solution over $\mathbb{C}$, when $\boldsymbol{\alpha}$ is an integer point chosen uniformly at random in a fixed range; see Proposition 4.3.

Satisfiable systems. Assume, conversely, that the system $\mathcal{S}$ is satisfiable. We first show that in that case, there exists a "small" solution $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \overline{\mathbb{Q}(\boldsymbol{x})}^n$ of $\mathcal{S}$. In particular, in Proposition 4.5, we exhibit a bound on the degree (in $\boldsymbol{x}$ and $\boldsymbol{y}$) of the defining polynomials of the β_i's. To this end, we use results on quantifier elimination for algebraically closed fields.

Fix $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\beta_1, \ldots, \beta_n)$ to be the finite extension of $\mathbb{Q}(\boldsymbol{x})$ obtained by adjoining the solution $\boldsymbol{\beta}$ to $\mathbb{Q}(\boldsymbol{x})$. The extension $\mathbb{K}$ is separable over $\mathbb{Q}(\boldsymbol{x})$, hence by the Primitive Element Theorem there exists an element $\theta \in \overline{\mathbb{Q}(\boldsymbol{x})}$ such that $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\theta)$. That is, every element $\gamma \in \mathbb{K}$ can be written as

$$\gamma = \sum_{j=0}^{N-1} p_j(\boldsymbol{x})\theta^j \tag{4.2}$$

where $p_j \in \mathbb{Q}(\boldsymbol{x})$, and N is the degree of $\mathbb{K}$ over $\mathbb{Q}(\boldsymbol{x})$.

Furthermore, θ can be constructed as a linear combination of the generators $\beta_1, \ldots, \beta_n$. Denote by $m_\theta(\boldsymbol{x}, y) \in \mathbb{Q}(\boldsymbol{x})[y]$ the minimal polynomial of θ over $\mathbb{Q}(\boldsymbol{x})$. In Proposition 4.6 we exhibit an upper bound on the degree N of $m_\theta(\boldsymbol{x}, y)$ in y and the degree of its coefficients in $\boldsymbol{x}$ (when considered as polynomials in $\mathbb{Q}[\boldsymbol{x}]$).

We then compute a bound on the denominators of the coefficients $p_j(\boldsymbol{x})$ that appear when expressing the β_i's as polynomials in θ as in (4.2). More specifically, in Proposition 4.8, we show that for all $i \in \{1, \ldots, n\}$,

$$\beta_i = \frac{P_i(\theta)}{b},$$

where $P_i(y) \in \mathbb{Q}[\boldsymbol{x}][y]$ is of degree at most $N-1$ in y, and $b \in \mathbb{Q}[\boldsymbol{x}]$ of total degree at most polynomial in N.

Now given $\boldsymbol{\alpha} \in \mathbb{C}^m$, we claim that the system $\mathcal{S}_{\boldsymbol{\alpha}}$ may be unsatisfiable over $\mathbb{C}$ only if $b(\boldsymbol{\alpha}) = 0$. Otherwise, if $b(\boldsymbol{\alpha}) \neq 0$, we can define a homomorphism $\varphi_{\boldsymbol{\alpha}} \colon \frac{1}{b(\boldsymbol{x})}\mathbb{Q}[\boldsymbol{x}][\theta] \to \mathbb{C}$ by

$$\frac{1}{b(\boldsymbol{x})} \sum_{i=0}^{N-1} q_j(\boldsymbol{x})\theta^j \mapsto \frac{1}{b(\boldsymbol{\alpha})} \sum_{j=0}^{N-1} q_j(\boldsymbol{\alpha})\omega^j$$

where $q_j(\boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{x}]$, and ω is a root of $m_\theta(\boldsymbol{\alpha}, y) \in \mathbb{C}[y]$. The homomorphism $\varphi_{\boldsymbol{\alpha}}$ is surjective, hence every solution of $\mathcal{S}_{\boldsymbol{\alpha}}$ in $\mathbb{C}^n$ is the image of a solution of $\mathcal{S}$ in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ under $\varphi_{\boldsymbol{\alpha}}$. In other words, for all $\boldsymbol{\alpha}$ such that $b(\boldsymbol{\alpha}) \neq 0$, a certificate that $\mathcal{S}_{\boldsymbol{\alpha}}$ has a solution over $\mathbb{C}$ witnesses that $\mathcal{S}$ has a solution over $\overline{\mathbb{Q}(\boldsymbol{x})}$.

Reducing the problem to $\mathrm{HN}_{\mathbb{C}}$. Finally, we combine the results on the unsatisfiable and satisfiable systems to compute a bound D such that if we choose $\alpha_1, \ldots, \alpha_m$ in $\{1, 2, \ldots, D\}$ independently and uniformly at random, with high probability the satisfiability of the system remains unchanged over $\mathbb{C}^n$ when specialised to $x_i = \alpha_i$ for $i \in \{1, \ldots, m\}$. We thus exhibit a randomised polynomial-time reduction from $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$, which places $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ in **AM** assuming GRH.

This completes the overview of our approach, so let us now look at the technical details of the proofs.

4.2.2 Choosing specialisations for unsatisfiable systems

We use an effective version of the weak Hilbert Nullstellensatz for $\overline{\mathbb{Q}(\boldsymbol{x})}$ given in [99, Theorem 5 and Corollary 4.20].

Theorem 4.2 (Effective Parametric Hilbert's Nullstellensatz)**.** *Let $f_1, \dots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \dots, y_n] \setminus \mathbb{Z}[\boldsymbol{x}]$ be a family of k polynomials of degree at most 2 in $\boldsymbol{x}$ and $\boldsymbol{y}$ that have no common zero in $\overline{\mathbb{Q}(\boldsymbol{x})}$. Then there exists $a \in \mathbb{Z}[\boldsymbol{x}] \setminus \{0\}$ and $g_1, \dots, g_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \dots, y_n]$ such that*

$$a = g_1 f_1 + \cdots + g_k f_k, \tag{4.3}$$

with

- $\deg_{\boldsymbol{y}}(g_i f_i) \leq 2^k$,
- $\deg_{\boldsymbol{x}}(a), \deg_{\boldsymbol{x}}(g_i f_i) \leq k2^k$.

Now if the system $\mathcal{S}$ is not satisfiable in $\overline{\mathbb{Q}(\boldsymbol{x})}$, Theorem 4.2 in combination with the Schwartz-Zippel Lemma allows us to compute a bound on the probability of $\mathcal{S}_{\boldsymbol{\alpha}}$ admitting a solution over $\mathbb{C}$, when $\boldsymbol{\alpha}$ is an integer point chosen uniformly at random in a fixed range. Recall we use s to denote the size of our fixed system.

Proposition 4.3. *Let $D \in \mathbb{N}$ be such that $D \geq s2^s$. If $\mathcal{S}$ has no solution in $\overline{\mathbb{Q}(\boldsymbol{x})}$, then for $\alpha_1, \dots, \alpha_m$ chosen independently and uniformly at random from $\{1, 2, \dots, D\}$*

$$\Pr\left(\mathcal{S}_{\boldsymbol{\alpha}} \text{ is satisfiable in } \mathbb{C}\right) \leq \frac{s2^s}{D}.$$

Proof. If $\mathcal{S}$ has no solution in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ then by the weak Hilbert Nullstellensatz, the ideal generated by the polynomials in $\mathcal{S}$ contains the constant 1. Furthermore, Theorem 4.2 asserts that there exists $a \in \mathbb{Q}[\boldsymbol{x}]$ of degree at most $s2^s$ that can be computed as a $\mathbb{Z}[\boldsymbol{x}]$-linear combination of the polynomials in $\mathcal{S}$, i.e., Equation (4.3) holds. For all $\boldsymbol{\alpha}$ such that $a(\boldsymbol{\alpha}) \neq 0$, the specialised system $\mathcal{S}_{\boldsymbol{\alpha}}$ cannot be satisfiable in $\mathbb{C}$. That is, by the union bound

$$\Pr\left(\mathcal{S}_{\boldsymbol{\alpha}} \text{ is satisfiable in } \mathbb{C}\right) \leq \Pr\left(a(\alpha_1, \dots, \alpha_r) = 0\right).$$

But a has degree at most $s2^s$, and hence by Lemma 4.1 the bound follows. □

4.2.3 Choosing specialisations for satisfiable systems

Satisfiable systems admit "small" solutions

We work with the first-order theory of algebraically closed fields of characteristic zero. Let K be a field, and denote by $\overline{K}$ its algebraic closure. We consider the first-order lan-

guage $\mathcal{L}$ with constant symbols for all elements of K, function symbols $+, -, \cdot$, and the relation symbol $=$. Atomic formulas have the form $P(x_1, \ldots, x_n) = 0$, where $P \in K[x_1, \ldots, x_n]$. We say that a formula Φ is *built over a set of polynomials* $\mathcal{P}$ if every polynomial mentioned in Φ lies in $\mathcal{P}$. It is well-known that the theory of algebraically closed fields admits quantifier elimination. We use the following quantitative formulation of quantifier elimination over $\overline{\mathbb{Q}(\boldsymbol{x})}$, which is a specialisation of [152, Theorem 2], and its reformulation stated in [3, Theorem 6], to $\overline{\mathbb{Q}(\boldsymbol{x})}$.

Theorem 4.4. *Let $\mathcal{P}$ be a set of k polynomials each of degree at most d. Fix $Y = (y_1, \ldots, y_{k_1})$ and $Z = (z_1, \ldots, z_{k_2})$ to be tuples of first-order variables. Consider the formula*

$$\Phi(Y) := \exists Z\, \Psi(Y, Z)\,,$$

where $\Psi(Y, Z)$ is a quantifier-free formula built over $\mathcal{P}$. There exists an equivalent quantifier-free formula $\Phi'(Y)$ that is built over a set of polynomials $\mathcal{Q}$ with degree bounded by $2^{n^{O(1)}(\log kd)^{O(1)}}$. The number of polynomials in $\mathcal{Q}$ is $O\big((kd)^{n^{O(1)}}\big)$.
Moreover, when the coefficients of the polynomials in Ψ are elements of $\mathbb{Z}[\boldsymbol{x}]$, and the combined degree of the polynomials in $\boldsymbol{x}, Y$ and Z is bounded by d, then the coefficients of the polynomials in Φ' are elements of $\mathbb{Z}[\boldsymbol{x}]$ of degree at most $2^{(n+r)^{O(1)}(\log kd)^{O(1)}}$ in $\boldsymbol{x}$.

We now use the above result to show that polynomial systems with coefficients in $\mathbb{Z}[\boldsymbol{x}]$, when satisfiable, admit a bounded-degree algebraic solution. We closely follow the proof [8, Theorem 7], adapting it to $\overline{\mathbb{Q}(\boldsymbol{x})}$.

Proposition 4.5. *Let $\mathcal{P}$ be a system of k polynomial equations in n variables $\boldsymbol{y} = (y_1, \ldots, y_n)$ with coefficients in $\mathbb{Z}[\boldsymbol{x}]$ of degree at most 2 in $\boldsymbol{x}$ and $\boldsymbol{y}$. There exists an effective constant $c \in \mathbb{N}$ such that if $\mathcal{P}$ has a solution over $\overline{\mathbb{Q}(\boldsymbol{x})}$, then there exists a solution $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ such that each component β_i is a root of a polynomial of degree at most $2^{(n \log k)^c}$ with coefficients that are polynomials in $\mathbb{Z}[\boldsymbol{x}]$ of degree at most $2^{((n+m) \log k)^c}$ in $\boldsymbol{x}$.*

Proof. We first prove the claim for the case when the system $\mathcal{P}$ has a finite number of solutions. Let $S \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}^n$ be the solution set of $\mathcal{P}$ and suppose it is finite. Write $S_i \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}$ for the projection of S on the ith coordinate axis. By Theorem 4.4, there exists an effective constant $c \in \mathbb{N}$ such that S_i can be defined by a quantifier-free formula built over a set of polynomials $\mathcal{Q}$ having degree bounded by $2^{(n \log kd)^c}$ and coefficients that are polynomials in $\mathbb{Z}[\boldsymbol{x}]$ of degree at most $2^{((n+m) \log kd)^c}$ in $\boldsymbol{x}$. If S is finite, then each S_i is finite. Hence each element of S_i is a root of some polynomial in $\mathcal{Q}$. Now given a solution $\boldsymbol{\beta} \in S$, its components are contained in $S_1, \ldots, S_n$, and thus are roots of polynomials in $\mathcal{Q}$.

Let us now assume that $\mathcal{P}$ has infinitely many solutions. We prove the claim by induction on n. Let $S \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}^n$ be the solution set of $\mathcal{P}$. By the assumption on $\mathcal{P}$, at least one of the projections S_i must be infinite. Now S_i is a constructible set, and its algebraic closure $\overline{S_i}$ is a whole line, hence its complement $\overline{\mathbb{Q}(\boldsymbol{x})} \setminus S_i$ must be finite. Furthermore, by Theorem 4.4 the elements of $\overline{\mathbb{Q}(\boldsymbol{x})} \setminus S_i$ are chosen among the roots of $O\big(k^{n^{O(1)}}\big)$ polynomials of degree at most $2^{n^{O(1)}(\log kd)^{O(1)}}$. Hence $|\overline{\mathbb{Q}(\boldsymbol{x})} \setminus S_i| < 2^{(n \log k)^c}$ for some effective constant $c \in \mathbb{N}$. This implies that there exists an integer $m \in S_i$ with $0 \leq m \leq 2^{(n \log k)^c}$. By substituting y_i

with m in $\mathcal{P}$, we obtain a new satisfiable system in $n-1$ variables where the polynomials are of combined degree at most 2 in $\boldsymbol{x}$ and $\boldsymbol{y} \setminus \{y_i\}$. By the induction hypothesis, the result follows. □

The primitive element

Assume that the system $\mathcal{S}$ is satisfiable. Fix $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ to be a solution of $\mathcal{S}$ in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ and let $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\beta_1, \ldots, \beta_n)$. The aim of this section is to upper-bound the degree and coefficients of the minimal polynomial of a primitive element θ for $\mathbb{K}$. We furthermore construct θ to be integral over $\mathbb{Q}[\boldsymbol{x}]$.

Recall that an element b of a commutative ring B is said to be *integral* over A, a subring of B, if b is a root of a monic polynomial with coefficients in A. Given an algebraic extension K of $\mathbb{Q}(\boldsymbol{x})$, we define $\mathcal{O}_K$ to be the subring of elements of K that are integral over $\mathbb{Q}[\boldsymbol{x}]$.

Let us note that given an element $\alpha \in K$, we can always find a polynomial $d \in \mathbb{Q}[\boldsymbol{x}]$ such that $\alpha d = \beta \in \mathcal{O}_K$. Indeed, let $f(y) \in \mathbb{Q}(\boldsymbol{x})[y]$ be the minimal (monic) polynomial of α and choose d to be the least common multiple of the denominators of the coefficients of $f(y)$. Then, since f is monic,

$$d^{\deg f} f\left(\frac{y}{d}\right) = g(y),$$

and $g(y) \in \mathbb{Q}[\boldsymbol{x}][y]$ is monic, with αd as a root. Thus $\alpha d \in \mathcal{O}_K$. Furthermore, αd and α have the same degree over $\mathbb{Q}(\boldsymbol{x})$.

Recall we write s to denote the size of our fixed system. By Proposition 4.5, the generators β_i of the field $\mathbb{K}$ are algebraic over $\mathbb{Q}(\boldsymbol{x})$ of degree at most $2^{(s \log s)^{c'}}$ for an effective constant $c' \in \mathbb{N}$. By the argument above, for each β_i, there must exist a polynomial $d_i \in \mathbb{Q}[\boldsymbol{x}]$ of degree at most $2^{(s \log s)^{c'}}$ in $\boldsymbol{x}$ such that $d_i \beta_i \in \mathcal{O}_{\mathbb{K}}$. Let $d = \operatorname{lcm}_{i=1}^n d_i$ and observe that its total degree is again bounded by $2^{(s \log s)^{c''}}$ for an effective constant $c'' > c'$. Fix $\tilde{\beta}_i := d\beta_i \in \mathcal{O}_{\mathbb{K}}$ for all $i \in \{1, \ldots, n\}$. We compute the primitive element $\theta \in \mathcal{O}_{\mathbb{K}}$ as a $\mathbb{Z}$-linear combination of the generators $\tilde{\beta}_1, \ldots, \tilde{\beta}_n$, following a standard construction (see Section 2.3.3) also used in Section 3.4.3.

Proposition 4.6. *There exists a primitive element θ of $\mathbb{K}$ with monic minimal polynomial $m_\theta(\boldsymbol{x}, y) \in \mathbb{Q}[\boldsymbol{x}][y]$ of degree at most $2^{(s \log s)^c}$ in y, and coefficients of degree at most $2^{(s \log s)^c}$ in $\boldsymbol{x}$, where c is an effective constant.*

Proof. Denote by $D := 2^{(s \log s)^{c'}}$ the bound on the degrees of the β_i's (and hence the $\tilde{\beta}_i$'s) given by Proposition 4.5. We follow the proof of the Primitive Element Theorem and construct the primitive element as $\theta = \sum_{i=1}^n c_i \tilde{\beta}_i$ where the $c_i \in \mathbb{Z}$ are of magnitude at most $D^{2n} + 1$, and θ is of degree at most D^n. To prove the bound on the constants c_i, we use an effective version of the theorem given in Lemma 2.3, which, recall, states that given α and β of respective degrees ℓ and m over $\mathbb{Q}(\boldsymbol{x})$, there exists $c \in \{1, \ldots, \ell^2 m^2 + 1\}$ such that $\alpha + c\beta$ is a primitive element of $\mathbb{Q}(\boldsymbol{x})(\alpha, \beta)$.

We prove the claim by induction on n. For $n = 2$, we construct a primitive element $\theta_2 = \tilde{\beta}_1 + c_2\tilde{\beta}_2$ for the field $\mathbb{Q}(\boldsymbol{x})(\tilde{\beta}_1, \tilde{\beta_2})$. By Lemma 2.3, we can choose c_2 of magnitude at most $d^4 + 1$. To obtain the bound on the degree of θ_2, denote by $p(y), q(y) \in \mathbb{Q}[\boldsymbol{x}](y)$ the respective minimal polynomials of $\tilde{\beta}_1$ and $\tilde{\beta}_2$ over $\mathbb{Q}(\boldsymbol{x})$. That is, we have $p(\tilde{\beta}_1) = q(\tilde{\beta}_2) = 0$. Notice that the polynomials $p(\theta_2 - cy)$ and $q(y)$ have a common root $\tilde{\beta}_2$. Now recall that the resultant of two polynomials is a polynomial expression of their coefficients that is equal to zero if and only if the polynomials have a common root. That is, the resultant of $p(\theta_2 - cy)$ and $q(y)$ is a polynomial expression in θ_2 equal to zero. Since the resultant is of degree at most D^2, θ_2 must be of degree at most D^2 over $\mathbb{Q}(\boldsymbol{x})$.

Now let us assume that the bounds hold for $n - 1$, that is, the primitive element θ_{n-1} of the field $\mathbb{Q}(\boldsymbol{x})(\tilde{\beta}_1, \ldots, \tilde{\beta}_{n-1})$ can be constructed as $\theta_{n-1} = \sum_{i=1}^{n-1} c_i\tilde{\beta}_i$ with c_i integers of magnitude at most $D^{2(n-1)} + 1$, and that it is algebraic of degree at most D^{n-1} over $\mathbb{Q}(\boldsymbol{x})$. By Lemma 2.3, we can construct the primitive element of the field $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\theta_{n-1}, \tilde{\beta}_n)$ as a linear combination $\theta_{n-1} + c_n\tilde{\beta}_n$ where c_n is an integer of magnitude at most $(D^{n-1})^2D^2 + 1 = D^{2n} + 1$. The bound on the degree of θ again follows from the resultant argument applied to the minimal polynomials of θ_{n-1} and $\tilde{\beta}_n$ over $\mathbb{Q}(\boldsymbol{x})$.

We have thus shown that the minimal polynomial $m_\theta(\boldsymbol{x}, y)$ of θ is of degree at most $D^{2n} \leq 2^{(s \log s)^c}$ where c is an effective constant. In remains to prove the bound on the coefficients of m_θ. To this aim, we construct a system of $k+1$ polynomial equations in $n+1$ variables with coefficients in $\mathbb{Z}[\boldsymbol{x}]$ such that one of its solutions will be $(\beta_1, \ldots, \beta_n, \theta)$.

For all $i \in \{1, \ldots, k\}$, let $g_i(y_1, \ldots, y_n, z) = f_i(y_1, \ldots, y_n)$, where f_i is as in $\mathcal{S}$. Define

$$g_{k+1}(y_1, \ldots, y_n, z) := z - \sum_{i=1}^{n} c_i d y_i,$$

where $d \in \mathbb{Q}[\boldsymbol{x}]$ is the polynomial such that $\tilde{\beta}_i = d\beta_i$ for all $i \in \{1, \ldots, n\}$. Then the system

$$g_1(y_1, \ldots, y_n, z) = 0, \ \ldots, \ g_{k+1}(y_1, \ldots, y_n, z) = 0 \tag{4.4}$$

is satisfiable and admits the claimed solution. Furthermore, notice that the combined degree of the polynomial g_{k+1} in $\boldsymbol{x}$, $\boldsymbol{y}$ and z is at most $2^{(s \log s)^{c''}}$, where c'' is an effective constant. By using the same reasoning as in Section 4.1, we can transform the system in (4.4) into a system of polynomials of total degree bounded by 2, of size polynomial in s. We may now apply Proposition 4.5 to this new system to assert that the coefficients of $m_\theta(\boldsymbol{x}, y)$ are of degree at most $2^{(s \log s)^c}$ in $\boldsymbol{x}$. Moreover, since $\theta \in \mathcal{O}_\mathbb{K}$ by construction, its minimal polynomial must be monic. □

Expressing the solution via the primitive element

We have just constructed a primitive element θ for $\mathbb{K}$ that is integral over $\mathbb{Q}[\boldsymbol{x}]$. We have that for all i, we can write

$$\beta_i = \sum_{j=0}^{N-1} p_{i,j}(\boldsymbol{x})\theta^j, \tag{4.5}$$

where $p_{i,j} \in \mathbb{Q}(\boldsymbol{x})$ and N is the degree of $\mathbb{K}$ over $\mathbb{Q}(\boldsymbol{x})$. In this section we show that the denominators of the coefficients $p_{i,j}$ cannot be of arbitrarily large degree in $\boldsymbol{x}$.

To this end, we rely on the following proposition.

Proposition 4.7. *Let $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\theta)$ where $\theta \in \mathcal{O}_{\mathbb{K}}$ has minimal polynomial $m_\theta \in \mathbb{Q}[\boldsymbol{x}][y]$ over $\mathbb{Q}(\boldsymbol{x})$ of degree N. Then $\mathcal{O}_{\mathbb{K}} \subseteq \frac{1}{\operatorname{disc}(m_\theta)} \sum_{i=0}^{N-1} \mathbb{Q}[\boldsymbol{x}]\theta^i$.*

Proof. Given $\alpha \in \mathcal{O}_{\mathbb{K}}$, write $\alpha = \sum_{i=0}^{N-1} q_i\theta^i$, where $q_0, \ldots, q_{N-1} \in \mathbb{Q}(\boldsymbol{x})$. Let $\sigma_0, \ldots, \sigma_{N-1}$ be a list of the monomorphisms $\mathbb{K} \hookrightarrow \overline{\mathbb{Q}(\boldsymbol{x})}$ that fix $\mathbb{Q}(\boldsymbol{x})$. Applying these monomorphisms to the previous equation gives $\sigma_j(\alpha) = \sum_{i=0}^{N-1} q_i\sigma_j(\theta^i)$ for $j = 0, \ldots, N-1$. Solving this system of linear equations for $q_0, \ldots, q_{N-1}$ using Cramer's rule we obtain

$$q_i = \frac{\det(D_i)}{\det(D)} = \frac{\det(D_i)\det(D)}{\det(D)^2}, \tag{4.6}$$

where $D = (\sigma_j(\theta^i))_{i,j}$ and D_i is the matrix obtained from D by replacing the ith column with the vector $(\sigma_0(\alpha), \ldots, \sigma_{N-1}(\alpha))^\top$.

The denominator $\det(D)^2$ on the right-hand side of (4.6) is the discriminant of m_θ; see, e.g. [153, p. 15, Equation (1.25.a)]. Moreover the numerator $\det(D_i)\det(D)$ on the right-hand side of (4.6) lies in $\mathbb{Q}(\boldsymbol{x})$ and is integral over $\mathbb{Q}[\boldsymbol{x}]$. Since $\mathbb{Q}[\boldsymbol{x}]$ is integrally closed we thus have that $\det(D_i)\det(D) \in \mathbb{Q}[\boldsymbol{x}]$. □

Proposition 4.8. *There exists $b \in \mathbb{Z}[\boldsymbol{x}]$ of degree at most $2^{(s\log s)^c}$ in $\boldsymbol{x}$ and $P_1, \ldots, P_n \in \mathbb{Z}[\boldsymbol{x}][y]$ such that for all $i \in \{1, \ldots, n\}$, $\beta_i = \frac{P_i(\theta)}{b}$, where c is an effective constant.*

Proof. By Proposition 4.7 we have $\mathcal{O}_{\mathbb{K}} \subseteq \frac{1}{\operatorname{disc}(m_\theta)} \sum_{i=0}^{N-1} \mathbb{Q}[\boldsymbol{x}]\theta^i$, where $\operatorname{disc}(m_\theta) \in \mathbb{Q}[\boldsymbol{x}]$ is the discriminant of the minimal polynomial m_θ of θ. In general, the discriminant of a polynomial of degree N is a polynomial in its coefficients of total degree $2N-1$. Thus, by Proposition 4.5, $\operatorname{disc}(m_\theta)$ is a polynomial in $\mathbb{Q}[\boldsymbol{x}]$ of total degree at most $(2N-1)\cdot 2^{(s\log s)^c} \leq 2^{(s\log s)^{c'}}$, where $c' > c$ is again an effective absolute constant.

Recall that $\tilde{\beta}_i = d\beta_i \in \mathcal{O}_{\mathbb{K}}$ for all $i \in \{1, \ldots, n\}$ where $d \in \mathbb{Q}[\boldsymbol{x}]$ of total degree at most $2^{(s\log s)^c}$. We can thus write $\beta_i = \frac{P_i(\theta)}{b}$, where $b := d \cdot \operatorname{disc}(m_\theta)$ is of total degree at most $2^{(s\log s)^{c''}}$ for an effective absolute constant c''. □

Choosing the specialisation

We now show that if the denominator b from Proposition 4.8 does not vanish on $\boldsymbol{\alpha} \in \mathbb{C}^m$, the system $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable in $\mathbb{C}$. The degree bound on b in combination with the Schwartz-Zippel Lemma allows us to compute a bound on the probability of $\mathcal{S}_{\boldsymbol{\alpha}}$ admitting a solution over $\mathbb{C}$, when $\boldsymbol{\alpha}$ is an integer point chosen uniformly at random in a fixed range.

Proposition 4.9. *There exists an effectively computable constant c such that for all $D \in \mathbb{N}$ with $D \geq 2^{(s \log s)^c}$, if $\mathcal{S}$ has a solution in $\overline{\mathbb{Q}(\boldsymbol{x})}$, then for $\alpha_1, \ldots, \alpha_m$ chosen independently and uniformly at random from $\{1, 2, \ldots, D\}$*

$$\Pr\left(\mathcal{S}_{\boldsymbol{\alpha}} \text{ is satisfiable in } \mathbb{C}\right) \geq 1 - \frac{2^{(s \log s)^c}}{D}.$$

Proof. Suppose $\mathcal{S}$ has a solution $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$. Recall we set θ to be a primitive element for $\mathbb{K} = \mathbb{Q}(\boldsymbol{x})(\beta_1, \ldots, \beta_n)$ that is integral over $\mathbb{Q}[\boldsymbol{x}]$ and denote by $m_\theta(\boldsymbol{x}, y) \in \mathbb{Q}[\boldsymbol{x}][y]$ its minimal polynomial. By Proposition 4.8, there exist polynomials $P_1, \ldots, P_n \in \mathbb{Z}[\boldsymbol{x}][y]$ and $b \in \mathbb{Z}[\boldsymbol{x}]$ such that for all $\beta_i = \frac{P_i(\theta)}{b}$. Furthermore, the degree of b is at most $2^{(s \log s)^c}$ where c is an effective constant.

We first show that given $\boldsymbol{\alpha} \in \mathbb{C}^m$, the system $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable over $\mathbb{C}$ if b does not vanish on $\boldsymbol{\alpha}$. For all $i \in \{1, \ldots, k\}$, let

$$g_i(y) = b^2 f_i\left(\frac{P_1(y)}{b}, \ldots, \frac{P_n(y)}{b}\right). \tag{4.7}$$

As discussed in Section 4.1, we assume the degrees of the f_i's in y are at most 2, thus it must be that $g_i \in \mathbb{Z}[\boldsymbol{x}]$. Furthermore, the polynomials g_i must be multiples of m_θ since m_θ is irreducible and $g_i(\theta) = 0$.

If b does not vanish on $\boldsymbol{\alpha}$, (4.7) must also hold in $\mathbb{C}$ when specialised at $\boldsymbol{x} = \boldsymbol{\alpha}$. This implies that if ω is a solution of $m_\theta(\boldsymbol{\alpha}, y)$ in $\mathbb{C}$, then $\left(\frac{P_1(\boldsymbol{\alpha},\omega)}{b(\boldsymbol{\alpha})}, \ldots, \frac{P_n(\boldsymbol{\alpha},\omega)}{b(\boldsymbol{\alpha})}\right)$ is a solution of $\mathcal{S}_{\boldsymbol{\alpha}}$ in $\mathbb{C}$. Note that such a solution ω of $m_\theta(\boldsymbol{\alpha}, y) \in \mathbb{Q}[y]$ exists for all $\boldsymbol{\alpha} \in \mathbb{C}^m$ as the polynomial m_θ is monic in y, hence $m_\theta(\boldsymbol{\alpha}, y)$ is not constant.

Thus

$$\Pr\left(\mathcal{S}_{\boldsymbol{\alpha}} \text{ is satisfiable in } \mathbb{C}\right) \geq \Pr\left(b(\boldsymbol{\alpha}) \neq 0\right) = 1 - \Pr\left(b(\boldsymbol{\alpha}) = 0\right),$$

which by the Schwartz-Zippel Lemma is at least $1 - \frac{2^{(s \log s)^c}}{D}$. □

4.2.4 Reduction to $\mathrm{HN}_{\mathbb{C}}$

We have just given estimates on the probability that the system $\mathcal{S}$ specialised at an integer point $\boldsymbol{\alpha}$ randomly chosen in a fixed range, is satisfiable over $\mathbb{C}$. We will now use

them to exhibit a randomised polynomial-time reduction of $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$. This allows us to use Koiran's **AM** protocol for $\mathrm{HN}_{\mathbb{C}}$ to decide $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ in **AM** assuming GRH as well.

The **AM** protocol for $\mathrm{HN}_{\mathbb{C}}$ admits perfect correctness. That is, given a system of polynomial equations in $\mathbb{Z}[y_1, \ldots, y_n]$ that is satisfiable in $\mathbb{C}$, the algorithm outputs "satisfiable" with probability 1, whereas given a system that is not satisfiable over $\mathbb{C}$, the probability of outputting "satisfiable" is at most $1/2$. We note that by standard amplification techniques, the error bound for false positives can be improved to $1/2^{\ell}$ for a fixed $\ell \in \mathbb{N}$.

Theorem 4.10. $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}} \in \mathbf{AM}$ *assuming GRH.*

Proof. Let $D := 3{\cdot}2^{(s \log s)^c}$ where c is the effective constant from Proposition 4.9. We reduce our fixed instance of $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to an instance of $\mathrm{HN}_{\mathbb{C}}$ by choosing the values $\alpha_1, \ldots, \alpha_m$ independently and uniformly at random from the set $\{1, 2, \ldots, D\}$, and running Koiran's algorithm from [8] on $\mathcal{S}_{\boldsymbol{\alpha}}$. Let us now analyse the probabilistic correctness of our reduction.

Denote by $\mathcal{A}$ the event that Koiran's algorithm outputs "satisfiable", and by $\mathcal{A}^c$ its complement, i.e., the event that the algorithm outputs "unsatisfiable". Let $\mathcal{B}$ be the event that for $\alpha_1, \ldots, \alpha_m$ chosen uniformly at random from $\{1, 2, \ldots, D\}$, the system $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable in $\mathbb{C}$, and let $\mathcal{B}^c$ be the complement of $\mathcal{B}$, i.e., the event that $\mathcal{S}_{\boldsymbol{\alpha}}$ is not satisfiable in $\mathbb{C}$.

Suppose that the system $\mathcal{S}$ is not satisfiable over $\overline{\mathbb{Q}(\boldsymbol{x})}$. By Proposition 4.3, if we choose $\alpha_1, \ldots, \alpha_m$ uniformly at random in $\{1, 2, \ldots, D\}$ the probability that $\mathcal{S}_{\alpha}$ is satisfiable over $\mathbb{C}$ (the event $\mathcal{B}$) is at most $\frac{s2^s}{D}$. That is, since $D \geq 4s2^s$, we have $\Pr(\mathcal{B}) \leq \frac{1}{4}$.

We recall that Koiran's algorithm admits perfect correctness, that is, $\Pr(\mathcal{A}^c \mid \mathcal{B}) = 0$. By amplifying the error probability for unsatisfiable instances and repeating his algorithm $\ell = 4$ times, we further have $\Pr(\mathcal{A} \mid \mathcal{B}^c) \leq \frac{1}{16}$.

We can now bound from below the probability of the algorithm outputting "unsatisfiable" as follows.

$$\begin{aligned}
\Pr(\mathcal{A}^c) &= \Pr(\mathcal{B}) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}) + \Pr(\mathcal{B}^c) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}^c) \\
&= \Pr(\mathcal{B}^c) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}^c) \\
&\geq \left(1 - \frac{1}{4}\right) \cdot \left(1 - \frac{1}{16}\right) = \frac{45}{64} \geq \frac{2}{3}\,,
\end{aligned}$$

which is the desired probability of correctness for unsatisfiable instances.

Let us now suppose the system $\mathcal{S}$ is satisfiable over $\overline{\mathbb{Q}(\boldsymbol{x})}$. By Proposition 4.9, the probability that $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable over $\mathbb{C}$ when $\alpha_1, \ldots, \alpha_m$ are chosen uniformly at random in $\{1, 2, \ldots, D\}$ (the event $\mathcal{B}$) is at least $\frac{2^{(s \log s)^c}}{D}$. In particular, our choice of $D = 3 \cdot 2^{(s \log s)^c}$, implies that $\Pr(\mathcal{B}) \geq \frac{2}{3}$.

Recall that Koiran's algorithm admits perfect correctness, hence $\Pr(\mathcal{A} \mid \mathcal{B}) = 1$.

We can bound the probability of the algorithm outputting "satisfiable" as follows.

$$\begin{aligned}\Pr(\mathcal{A}) &= \Pr(\mathcal{C}) \cdot \Pr(\mathcal{B} \mid \mathcal{C}) + \Pr(\mathcal{C}^c) \cdot \Pr(\mathcal{B} \mid \mathcal{C}^c) \\ &\geq \Pr(\mathcal{B}) \cdot \Pr(\mathcal{A} \mid \mathcal{B}) \\ &\geq \frac{2}{3} \cdot 1 = \frac{2}{3}\end{aligned}$$

We have again obtained the required probability of correctness for satisfiable instances, which completes our **BPP** reduction. Since **AM** is closed under probabilistic reductions, this proves the theorem.

□

4.3 A geometric approach to parametric HN

In the previous section we have shown that the problem of determining whether a system of polynomials with coefficients in $\mathbb{Z}[\boldsymbol{x}]$ has a solution in $\overline{\mathbb{Q}(\boldsymbol{x})}$ reduces to deciding whether a system of polynomials with integer coefficients is satisfiable over $\mathbb{C}$. We did this through a number-theoretic approach, generalising the **AM** algorithm for $\mathrm{HN}_{\mathbb{C}}$ given in [8].

Systems of polynomials have a very natural algebraic interpretation, namely they define algebraic varieties. Given a system $\mathcal{S}$ of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ for $\boldsymbol{x} := (x_1, \ldots, x_m)$, it makes sense to ask what is the geometric interpretation of its solutions in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$. Our arguments in Section 4.2.3 assert that if the system is satisfiable over $\overline{\mathbb{Q}(\boldsymbol{x})}$, the parameters $\boldsymbol{x}$ keeping the system satisfiable over $\mathbb{C}$ can be chosen from a Zariski-open set. In particular, we have shown that given a solution $\boldsymbol{\beta} \in \overline{\mathbb{Q}(\boldsymbol{x})}^n$ of $\mathcal{S}$, we can compute a polynomial $b \in \mathbb{Q}[\boldsymbol{x}]$ such that for all $\boldsymbol{\alpha} \in \mathbb{C}^m$ with $b(\boldsymbol{\alpha}) \neq 0$, the system $\mathcal{S}_{\boldsymbol{\alpha}}$ has a solution in $\mathbb{C}^n$, and that solution is the image of $\boldsymbol{\beta}$ under a ring homomorphism whose kernel contains $\boldsymbol{\alpha}$. We could, in fact, compute such a polynomial b_i for every solution $\boldsymbol{\beta}_i$ of $\mathcal{S}$ in $\overline{\mathbb{Q}(\boldsymbol{x})}^n$. Denoting by B the set of common zeroes of the b_i's in $\mathbb{C}^m$ (which, note, is Zariski-closed), our argument states that for all $\boldsymbol{\alpha}$ in the Zariski-open complement $\mathbb{C}^m \setminus B$, the system $\mathcal{S}_{\boldsymbol{\alpha}}$ is satisfiable over $\mathbb{C}$, and its solution in $\mathbb{C}^n$ is the image of one of the solutions $\boldsymbol{\beta}_i$.

Furthermore, if we write V for the subvariety of $\mathbb{C}^{m+n}$ defined by the system $\mathcal{S}$ when treating the parameters $x_1, \ldots, x_m$ as variables, the satisfiability of $\mathcal{S}$ over $\overline{\mathbb{Q}(\boldsymbol{x})}$ is equivalent to $x_1, \ldots, x_m$ being algebraically independent in the coordinate ring $\mathbb{C}[V]$. To see this, it suffices to note that $x_1, \ldots, x_m$ are algebraically independent in $\mathbb{C}[V]$ if and only if $I(V) \cap \mathbb{C}[x_1, \ldots, x_m] = \{0\}$ (see Section 2.3.7 for details). But the weak Hilbert Nullstellensatz for $\overline{\mathbb{Q}(\boldsymbol{x})}$ that we restated in Theorem 4.2 asserts precisely that $I(V) \cap \overline{\mathbb{Q}}[x_1, \ldots, x_m] \neq \{0\}$ if and only if the system $\mathcal{S}$ is not satisfiable over $\overline{\mathbb{Q}(\boldsymbol{x})}$. Now $I(V) \cap \overline{\mathbb{Q}}[x_1, \ldots, x_m] \neq \{0\}$ if $I(V) \cap \mathbb{C}[x_1, \ldots, x_m] \neq \{0\}$; thus deciding $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ boils down to verifying whether the variety V is of dimension at least m in $\mathbb{C}^{m+n}$ and, in particular, whether the projection of the variables $x_1, \ldots, x_m$ is dense in $\mathbb{C}^m$.

As discussed in Section 1.2, the complexity of determining the dimension of complex al-

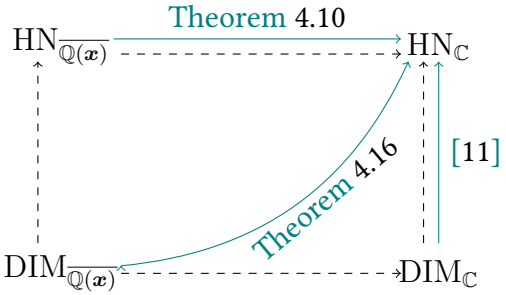

Figure 4.1 – An illustration of the relations between the problems HN and DIM over $\overline{\mathbb{Q}(\boldsymbol{x})}$ and $\mathbb{C}$ respectively. We use $A \longrightarrow B$ to denote a randomised polynomial-time reduction from the problem A to the problem B, and $A \dashrightarrow B$ to denote that the problem A is a generalisation of the problem B.

gebraic varieties was first studied in [91]. Formally, the problem, denoted $\mathrm{DIM}_{\mathbb{C}}$, asks, given a system of polynomial equations $f_1, \ldots, f_k \in \mathbb{Z}[y_1, \ldots, y_n]$, and an integer $d < n$, whether the variety $V \subseteq \mathbb{C}^n$ defined the system has dimension at least d. Let us note here that $\mathrm{HN}_{\mathbb{C}}$ is precisely the problem $\mathrm{DIM}_{\mathbb{C}}$ specialised to $d = 0$. In [11] a randomised polynomial-time reduction of $\mathrm{DIM}_{\mathbb{C}}$ to $\mathrm{HN}_{\mathbb{C}}$ is established, thus placing $\mathrm{DIM}_{\mathbb{C}}$ in **AM** assuming GRH.

The reduction works by first applying a random linear transformation A to the variety V such that with high probability the projection of the coordinates $y_1, \ldots, y_d$ of the image AV of the variety under A is dense in $\mathbb{C}^d$, if V has dimension at least d. The second step of the algorithm involves randomly choosing an integer point $(\alpha_1, \ldots, \alpha_d)$, adding equations $y_1 = \alpha_1, \ldots, y_d = \alpha_d$ to the system defining AV and verifying the satisfiability of the new system (with more polynomials but fewer variables) over $\mathbb{C}$ via the $\mathrm{HN}_{\mathbb{C}}$ algorithm. Geometrically speaking, the reduction corresponds to intersecting the variety $V \in \mathbb{C}^n$ with a generic affine subspace of dimension $n - d$. This coincides with yet another characterisation of the dimension, as such an intersection is non-empty precisely if the variety has dimension at least d.

The technique presented in Section 4.2 is in essence equivalent to the second step of the reduction we just described, however, the proof techniques ensuring its correctness and error analysis are conceptually different. Our proof is a generalisation of Koiran's proof that $\mathrm{HN}_{\mathbb{C}}$ belongs to **AM** [8] and relies on algebraic number theory, whereas [11] relies on arguments from (real) algebraic geometry. More specifically, the bound on the probability of a randomly chosen integer point lying in the variety follows through an analysis of the number of connected components of the variety V when embedded in $\mathbb{R}^{2n}$ in combination with a result on approximating the Lebesgue measure of $V \cap \mathbb{R}^n$ from [92]. The technique of [11] thus relies on the fact that we are working over a field containing $\mathbb{R}$, whereas the number-theoretic approach uses the property that the field extensions we consider are separable.

We now show that with minimal changes the randomised polynomial-time reduction of $\mathrm{DIM}_{\mathbb{C}}$ to $\mathrm{HN}_{\mathbb{C}}$ carries over to $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$. Furthermore, the technique can be extended to a common generalisation of the two problems: the $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ problem, which asks, given a system of polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ and an integer $d < n$, whether the

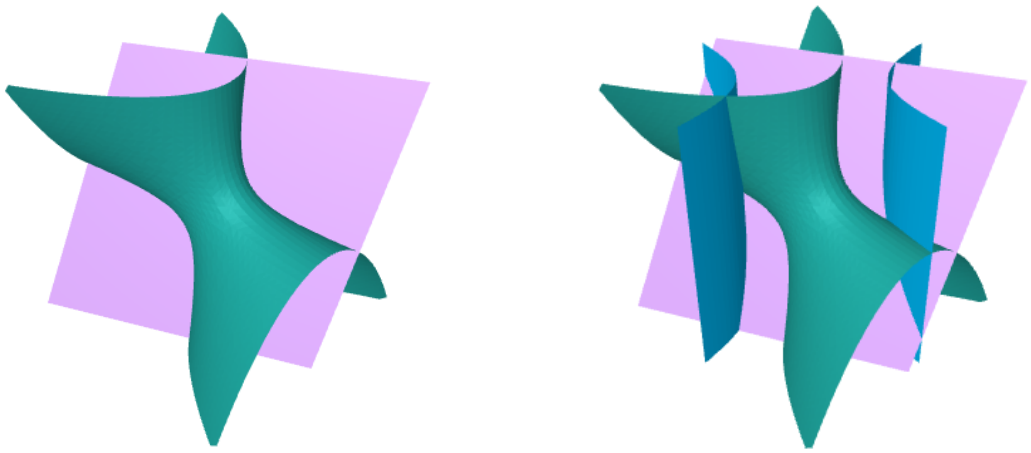

Figure 4.2 – An illustration of the system of polynomials from Example 4.1. On the left hand side the hypersurface defined by the polynomial $x_1^2 + y_1y_2 - 1 = 0$ is plotted in teal and the one defined by $2x_1 + y_1 + y_2 = 0$ in pink. We can see that the intersection of the hypersurfaces is an algebraic curve. On the right hand side, the plot is completed with the hypersurface given by the polynomial $x_1y_1 + 2 = 0$ in blue. The three hypersurfaces on the illustration intersect in two real points.

subvariety of $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ defined by the system is of dimension at least d. We observe that to decide $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$, it suffices to verify whether the subvariety of $\mathbb{C}^{m+n}$ defined by the system (when we consider the parameters $x_1, \ldots, x_m$ as variables) is of dimension at least $m + d$, with the additional restriction that the projection of the coordinates $x_1, \ldots, x_m$ is dense in $\mathbb{C}^m$ before applying the linear transformation. We thus adjust the reduction to choose a linear transformation that keeps the coordinates $x_1, \ldots, x_m$ unchanged.

Given an instance of $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$, our algorithm directly reduces the problem to $\mathrm{HN}_{\mathbb{C}}$. Note that we could also first verify that the system is satisfiable over $\overline{\mathbb{Q}(\boldsymbol{x})}$, and then use the $\mathrm{DIM}_{\mathbb{C}}$ algorithm directly (with the promise that $x_1, \ldots, x_m$ are algebraically independent in $\mathbb{C}[V]$) to determine the dimension of the variety they define. However, separating the two steps would entail choosing a random integer point and calling to the $\mathrm{HN}_{\mathbb{C}}$ algorithm twice, which our direct reduction to $\mathrm{HN}_{\mathbb{C}}$ avoids. For an illustration of the relation between the Hilbert Nullstellensatz and dimension problems over $\overline{\mathbb{Q}(\boldsymbol{x})}$ and $\mathbb{C}$, and the reductions we establish, see Figure 4.1.

Before proceeding to the technical proofs, let us look at an example illustrating how satisfiability over $\overline{\mathbb{Q}(\boldsymbol{x})}$ relates to the geometry of the variety over $\mathbb{C}$.

Example 4.1. *Consider the system*

$$x_1^2 + y_1y_2 - 1 = 0$$
$$2x_1 + y_1 + y_2 = 0$$

in $\mathbb{Z}[x_1][y_1, y_2]$. *The system admits two parametric solutions in the variable* x_1, *namely* $(-x_1 + \sqrt{2x_1^2 - 1}, -x_1 - \sqrt{2x_1^2 - 1})$ *and* $(-x_1 - \sqrt{2x_1^2 - 1}, -x_1 + \sqrt{2x_1^2 - 1})$. *If we briefly go back*

to the technique introduced in Section 4.2, we can note that the system remains satisfiable in $\mathbb{C}^2$ *for all positive integer specialisations* $\alpha_1 \in \mathbb{N}$ *for* x_1*.*

When considered as a variety in $\mathbb{C}^3$*, the two polynomials define each a hypersurface, that is, a* 2*-dimensional variety. The points satisfying the system are precisely those lying in the intersection of the hypersurfaces, namely an algebraic curve, i.e., a variety of dimension* 1*. For an illustration see Figure 4.2.*

Now let us consider adding the polynomial $x_1y_1 + 2 = 0$ *to the system above. The intersection of the hypersurfaces defined by the three polynomials in* $\mathbb{C}^3$ *is finite (i.e. 0-dimensional), as illustrated on Figure 4.2. As expected, the system does not admit parametric solutions.*

We give a second example that shows why it is essential that our reduction keeps the parameters $x_1, \ldots, x_m$ unchanged when applying the linear transformation.

Example 4.2. *Consider the system*

$$\begin{aligned} x_2y_1^2y_2^2 + x_1^2 + 2x_2 - 1 &= 0 \\ y_1y_2 - 3x_1^2 + 2 &= 0\,. \end{aligned}$$

in $\mathbb{Z}[x_1, x_2][y_1, y_2]$*. Notice that similarly to Example 4.1, the two polynomials define each a hypersurface in* $\mathbb{C}^4$*, and the variety* V *they define in* $\mathbb{C}^4$ *is of dimension* 2*. However, in contrast to the previous example, the system here does not admit a parametric solution in* $\overline{\mathbb{Q}(x_1, x_2)}$*, as the parameters* x_1 *and* x_2 *(when considered as variables) are not algebraically independent in* $\mathbb{C}[V]$*. In particular, we have that* $9x_1^4x_2 - 12x_1^2x_2 + x_1^2 + 6x_2 - 1 \in \mathbb{Z}[x_1, x_2]$ *belongs to* $I(V)$*.*

4.3.1 Parametric dimension versus complex dimension

Given a subset of variables $\mathcal{I} \subseteq \{x_1, \ldots, x_n\}$, we denote by $\pi_{\mathcal{I}} : K^n \to K^{|\mathcal{I}|}$ the projection on the $|\mathcal{I}|$-dimensional subspace defined by the system of equations $\{x_i = 0, x_i \notin \mathcal{I}\}$. We say that a variety $V \subseteq K^n$ is in *normal position* with respect to the set of variables $\mathcal{I}$ if $\pi_{\mathcal{I}}(V)$ is dense in $K^{|\mathcal{I}|}$.

In this section we formally relate the dimension of a variety over $\mathbb{C}$ to its dimension over $\overline{\mathbb{Q}(\boldsymbol{x})}$. To this end, we require several concepts from algebraic geometry, which we introduced in Section 2.3.7. Given $V \subseteq K^n$, we first rely on the characterisation of the dimension of V as the largest integer d for which there exist d variables $x_{i_1}, \ldots, x_{i_d}$ such that $I(V) \cap K[x_{i_1}, \ldots, x_{i_d}] = \{0\}$, given in Theorem 2.11.

From now on, we fix polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ for $\boldsymbol{x} = (x_1, \ldots, x_m)$, and write $V^* \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}^n$ for the variety defined by the ideal $I^* := \langle f_1, \ldots, f_k \rangle_{\overline{\mathbb{Q}(\boldsymbol{x})}} \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}[y_1, \ldots, y_n]$. We can consider the parameters $x_1, \ldots, x_m$ as variables, and write $V \subseteq \mathbb{C}^{m+n}$ for the variety defined by the ideal $I := \langle f_1, \ldots, f_k \rangle_{\mathbb{C}} \subseteq \mathbb{C}[x_1, \ldots, x_m, y_1, \ldots, y_n]$.

Proposition 4.11. *If* V *is a subvariety of* $\mathbb{C}^{m+n}$ *in normal position with respect to* $\{x_1, \ldots, x_m, y_1, \ldots, y_d\}$*, then* V^* *is a subvariety of* $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ *in normal position with respect to* $\{y_1, \ldots, y_d\}$*.*

Proof. V is a subvariety of $\mathbb{C}^{m+n}$ in normal position with respect to $\{x_1, \ldots, x_m, y_1, \ldots, y_d\}$, hence by Theorem 2.11, $I \cap \mathbb{C}[x_1, \ldots, x_m, y_1, \ldots, y_n] = \{0\}$. Since $\overline{\mathbb{Q}} \subset \mathbb{C}$, we furthermore have that

$$I \cap \overline{\mathbb{Q}}[x_1, \ldots, x_m, y_1, \ldots, y_d] = \{0\}. \tag{4.8}$$

Notice that since $\{x_1, \ldots, x_m\} \subset \overline{\mathbb{Q}(\boldsymbol{x})}$,

$$\overline{\mathbb{Q}(\boldsymbol{x})}[x_1, \ldots, x_m, y_1, \ldots, y_d] = \overline{\mathbb{Q}(\boldsymbol{x})}[y_1, \ldots, y_d] \ .$$

Similarly, since $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}(\boldsymbol{x})}$, we can write

$$I^* = \langle f_1, \ldots, f_k \rangle_{\overline{\mathbb{Q}(\boldsymbol{x})}} = \overline{\mathbb{Q}(\boldsymbol{x})} \langle f_1, \ldots, f_k \rangle_{\overline{\mathbb{Q}}}.$$

Furthermore, since $\overline{\mathbb{Q}} \subset \mathbb{C}$, the expression above rewrites as $\overline{\mathbb{Q}(\boldsymbol{x})} \langle f_1, \ldots, f_k \rangle_{\mathbb{C}} = \overline{\mathbb{Q}(\boldsymbol{x})} I$.

Altogether this allows us to write

$$\begin{aligned} I^* \cap \overline{\mathbb{Q}(\boldsymbol{x})}[y_1, \ldots, y_d] &\subset \overline{\mathbb{Q}(\boldsymbol{x})} I \cap \overline{\mathbb{Q}(\boldsymbol{x})}[x_1, \ldots, x_m, y_1, \ldots, y_d] \\ &= \overline{\mathbb{Q}(\boldsymbol{x})}(I \cap \overline{\mathbb{Q}}[x_1, \ldots, x_m, y_1, \ldots, y_d]) \end{aligned}$$

By (4.8), we get that $I^* \cap \overline{\mathbb{Q}(\boldsymbol{x})}[y_1, \ldots, y_d] = \{0\}$. Now Theorem 2.11 implies that V^* is a subvariety of $\overline{\mathbb{Q}(\boldsymbol{x})}^n$ in normal position with respect to the variables $\{y_1, \ldots, y_d\}$, and hence of dimension at least m. □

Given an $(m+n) \times (m+n)$ matrix A, we write AV to denote the image of $V \subseteq \mathbb{C}^{(m+n)}$ by the linear transformation $x \mapsto Ax$. We now reiterate the proof of Theorem 2.1 in [11], which gives a condition on matrices A such that the variety AV is in normal position with respect to the first $m + d$ variables. The theorem relies on the fact that A is invertible if and only if $\det A \neq 0$, and in this case AV is a variety of the same dimension. Under the additional assumption of the variety over $\mathbb{C}$ being in normal position with respect to the first m variables $\{x_1, \ldots, x_m\}$ before applying the linear transformation A, the claim follows through an analogous proof.

The proof uses an alternative characterisation of dimension, namely via the dimension of the tangent spaces to a variety; see Section 2.3.7. It relies, more specifically, on the fact that invertible linear transformations preserve tangent spaces.

Theorem 4.12. *Suppose $V \subseteq \mathbb{C}^{(m+n)}$ is a variety of dimension $m+d$ in normal position with respect to $\{x_1, \ldots, x_m, y_1, \ldots, y_d\}$. Let $S_V \subseteq \mathbb{C}^{(m+n)^2}$ be the set of matrices $A \in \mathcal{M}_n(\mathbb{C})$ such that*

- *A is invertible,*
- *A as a linear transformation acts as the identity on the first m coordinates $\{x_1, \ldots, x_m\}$,*
- *AV is a variety of dimension $m + d$ in normal position with respect to $\{x_1, \ldots, x_m, y_1, \ldots, y_d\}$.*

S_V contains a set of the form $P_V(A) \cdot \det A \neq 0$ where $P_V \in \mathbb{C}[X_1, \ldots, X_{(m+n)^2}]$ is a multilinear polynomial of degree at most $m + d$.

As in [11], we first show that the theorem holds for varieties defined by systems of linear equations. We write π_{m+d} for the projection from $\mathbb{C}^{m+n}$ to the $(m+d)$-dimensional subspace given by the system of equations $x_i = 0$ for $i \in \{1, \ldots, m\}$ and $y_j = 0$ for $j \in \{1, \ldots, d\}$.

Lemma 4.13. *Theorem 4.12 holds when V is an affine subspace.*

Proof. Let $\{v_1, \ldots, v_{m+d}\}$ be a basis of V. Then$\{Av_1, \ldots, Av_{m+d}\}$ is a basis of AV, hence $\{\pi_{m+d}(Av_1), \ldots, \pi_{m+d}(Av_{m+d})\}$ generates $\pi_{m+d}(AV)$.

Thus $\pi_{m+d}(AV) = \mathbb{C}^d$ if and only if $\pi_{m+d}(Av_1), \ldots, \pi_{m+d}(Av_{m+d})$ are linearly independent, that is, if

$$\det(\pi_{m+d}(Av_1), \ldots, \pi_{m+d}(Av_{m+d})) \neq 0.$$

We claim that this is a multilinear condition of degree $m+d$ in the coefficients of A. Indeed, note that the degree bound follows since the determinant of a matrix of dimension $(m+d) \times (m+d)$ is a polynomial of degree at most $m+d$. To see that it is multilinear, it suffices to note that

$$\pi_{m+d}(Av_i)_j = \sum_{\ell=1}^{m+d} A_{j,\ell} v_{i,\ell}$$

Hence if we multiply the jth row of A by λ, the entries of the jth row matrix $\pi_{m+d}(Av_i)_j$ are also multiplied by λ. Since $\det$ is multilinear, the claim follows. □

Proof of Theorem 4.12. By decomposing V in irreducible components if necessary, we may assume that V is irreducible. Let x_0 be a smooth point of V, and denote by T the tangent space to V in x_0. Since x_0 is a smooth point, T has dimension $m+d$.

Let us apply Lemma 4.13 to T; we will show that $P_V = P_T$. Indeed, let A be a matrix in S_T. Since A is an invertible linear transformation from $\mathbb{C}^{m+n}$ to $\mathbb{C}^{m+n}$, AT is the tangent space to AV in Ax_0 and by the definition of S_T, $\pi_{m+d}(AT) = \mathbb{C}^{m+d}$. Recall that $AT \cong (\mathfrak{m}_{Ax_0}/\mathfrak{m}_{Ax_0}^2)^*$. This, in particular, implies that $x_1, \ldots, x_m, y_1, \ldots, y_d$, when considered as functions in $\mathcal{O}_{Ax_0}$, are a system of local parameters for AV at Ax_0. (Indeed, $x_1, \ldots, x_m, y_1, \ldots, y_d \in \mathfrak{m}_{Ax_0}$, and $x_1, \ldots, x_m, y_1, \ldots, y_d$ span $\mathfrak{m}_{Ax_0}/\mathfrak{m}_{Ax_0}^2$).

By the implicit function theorem (see [133, Chapter 2, Section 2.3]) there exists a system of power series $\phi_1, \ldots, \phi_{n-d}$ in $m+d$ variables $x_1, \ldots, x_m, y_1, \ldots, y_d$ and $\epsilon > 0$ such that

$$\phi_j(x_1, \ldots, x_m, y_1, \ldots, y_d) \text{ converges for all } x_i, y_j \text{ with } |x_i|, |y_j| < \epsilon$$

and

$$f_i(\boldsymbol{x}, \boldsymbol{y}, \phi_1(\boldsymbol{x}, \boldsymbol{y}), \ldots, \phi_{n-d}(\boldsymbol{x}, \boldsymbol{y})) = 0 \text{ for all } i \in \{1, \ldots, k\},$$

where $\boldsymbol{x} := (x_1, \ldots, x_m)$ and $\boldsymbol{y} := (y_1, \ldots, y_d)$. In other words, there exists $\eta > 0$ such that any point $(a_1, \ldots, a_{m+n}) \in AV$ with $a_i \leq |\eta|$ for $i \in \{1, \ldots, m+n\}$ is given by the form $a_{m+d+i} = \phi_i(a_1, \ldots, a_{m+d})$ for $i \in \{1, \ldots, n-d\}$. It follows that $(a_1, \ldots, a_{m+n}) \mapsto$

$(a_1, \ldots, a_{m+d})$ is a homeomorphism of the set $\{(a_1, \ldots, a_{m+n}) \in AV \mid |a_i| < \eta\}$ to a domain of a $(m+d)$-dimensional space.

Recall that a domain is a nonempty connected Euclidean-open set. That is, the implicit function theorem asserts that $\pi_{m+d}(AV)$ contains an Euclidean-open set. It is well-known that for all $\ell \in \mathbb{N}$, all nonempty Euclidean-open subsets of $\mathbb{C}^\ell$ are Zariski-dense in $\mathbb{C}^\ell$, hence $\pi_{m+d}(AV)$ must be dense in $\mathbb{C}^d$. □

Proposition 4.11 in combination with Theorem 4.12 ensures we can reduce deciding $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to deciding $\mathrm{HN}_{\mathbb{C}}$, which we do in the next section.

4.3.2 Reduction to $\mathrm{HN}_{\mathbb{C}}$

We are now ready to present our randomised polynomial-time reduction from $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$. We follow the reduction presented in [11], using the results from Section 4.3.1 to ensure its correctness in our setting. To this end, we fix an instance of $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ with input polynomials $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ where $\boldsymbol{x} := (x_1, \ldots, x_m)$, and an integer and $d < n$. The problem here is to determine whether $\dim V^* \geq d$, where $V^* = V(f_1, \ldots, f_k) \subseteq \overline{\mathbb{Q}(\boldsymbol{x})}^n$. We denote by $V := V(f_1, \ldots, f_k) \subseteq \mathbb{C}^{m+n}$ the complex variety defined by the polynomials when we consider the parameters $x_1, \ldots, x_m$ as variables. Recall that without loss of generality, we assume the polynomials to be of degree at most 2, as explained in Section 4.1.

Our reduction proceeds in two steps: In Step 1 we randomly choose an integer-valued matrix A such that the coordinates $x_1, \ldots, x_m$ of AV are the same as those of V and that with high probability AV is in normal position (i.e., $\pi_{m+d}(AV)$ is dense in $\mathbb{C}^{m+d}$) if $\dim V^* \geq d$. The correctness of this step is ensured by Proposition 4.11. In Step 2 we randomly choose positive integer values $\alpha_1, \ldots, \alpha_{m+d}$ and construct a system of polynomials

$$\begin{aligned} f_1 = 0,\ \ldots,\ f_k = 0 \\ x_1 = \alpha_1,\ \ldots,\ x_m = \alpha_m \\ y_1 = \alpha_{m+1},\ \ldots,\ y_d = \alpha_{m+d} \end{aligned}$$

which with high probability is satisfiable over $\mathbb{C}$ if $\dim V^* \geq d$.

In order to estimate the error probabilities in our reduction, we rely on the following two theorems from [11], which we rephrase to fit our setting. The first theorem allows us to estimate the probability of a randomly-chosen integer point belonging to the projection $\pi_{m+d}(AV)$.

Theorem 4.14 (Theorem 3.9 in [11]). *Let $V \subseteq \mathbb{C}^{m+n}$ be a variety defined by a system of degree-2 equations, and fix $\ell < n$.*

- *If $\pi_{m+d}(V)$ is dense in $\mathbb{C}^{m+d}$, then the probability that $\boldsymbol{\alpha} \in \{1, 2, \ldots, D\}^{m+d}$ is in $\pi_{m+d}(V)$ is at least $1 - C/D$, where $C = 6(m+d) \cdot 2^{4(n-d)}$.*
- *If $\pi_{m+d}(V)$ is not dense in $\mathbb{C}^{m+d}$, then the probability that $\boldsymbol{\alpha} \in \{1, 2, \ldots, D\}^{m+d}$ is in $\pi_{m+d}(V)$ is at most C/D.*

The second theorem concerns the probability of a randomly-chosen integer-valued matrix belonging to the set S_V defined in Theorem 2.11.

Theorem 4.15 (Theorem 3.10 in [11]). *Let $V \subseteq \mathbb{C}^n$ be a variety of dimension $d \geq 1$, the probability that a matrix A with entries from $\{1, 2, \ldots, D\}$ vanishes on the polynomial P_V defined in Theorem 2.11 is at most $2n^2/D$.*

Let us now prove the correctness and complexity of our reduction.

Theorem 4.16. $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}} \in \mathbf{AM}$ *assuming GRH.*

Proof. Let $D := 2^4 \cdot 3(m+d) \cdot 2^{4(n-d)}$. We reduce our fixed instance of $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to an instance of $\mathrm{HN}_{\mathbb{C}}$ as discussed above, applying Koiran's $\mathrm{HN}_{\mathbb{C}}$ algorithm [8] to decide the problem.

Denote by $\mathcal{A}$ the event that Koiran's $\mathrm{HN}_{\mathbb{C}}$ algorithm outputs "satisfiable", and by $\mathcal{A}^c$ its complement, i.e., the event that the algorithm outputs "unsatisfiable". We recall here that given a system of polynomial equations in $\mathbb{Z}[x_1, \ldots, x_n]$ that is satisfiable in $\mathbb{C}$, the $\mathrm{HN}_{\mathbb{C}}$ algorithm outputs "satisfiable" with probability 1, whereas given a system that is not satisfiable over $\mathbb{C}$, the probability of outputting "satisfiable" is at most $1/2$. We note that by standard amplification techniques, the error bound for false positives can be improved to $1/2^\ell$ for a fixed $\ell \in \mathbb{N}$.

Let $\mathcal{B}$ be the event that for $\alpha_1, \ldots, \alpha_{m+d}$ chosen uniformly at random from $\{1, 2, \ldots, D\}$, the system defining AV with the added polynomials $x_i = \alpha_i$ for $i \in \{1, \ldots, m\}$ and $y_j = \alpha_{m+j}$ for $j \in \{1, \ldots, d\}$ is satisfiable in $\mathbb{C}^{n-d}$. Write $\mathcal{B}^c$ for its complement. Finally, let $\mathcal{C}$ be the event that for a matrix A with entries from $\{1, 2, \ldots, D\}$ chosen uniformly at random, the variety AV is in normal position with respect to $\{x_1, \ldots, x_d\}$. Let $\mathcal{C}^c$ be the complement of $\mathcal{C}$.

If our fixed instance of $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ is negative, i.e., $\dim V^* < d$, then $\dim V < m + d$, and for all linear transformations A, $\dim AV < m + d$. Hence $\Pr(\mathcal{C}) = 0$ for all A, and $\Pr(\mathcal{B}) = \Pr(\mathcal{B} \mid \mathcal{C}^c)$. That is, we have that $\pi_{m+d}(AV)$ is not dense in $\mathbb{C}^{m+d}$. However, it may be that we choose an integer point $\boldsymbol{\alpha} \in \{1, 2, \ldots, D\}^{m+d}$ such that $\boldsymbol{\alpha} \in \pi_{m+d}(AV)$. By Theorem 4.14 the probability $\Pr(\mathcal{B})$ that an integer point of height at most D is in $\pi_{m+d}(AV)$ is at most $\frac{C}{D}$, where $C = 6(m+d) \cdot 2^{4(n-d)}$ (using the assumption the the polynomials defining V are of degree at most 2). For the choice of D we have made, $\Pr(\mathcal{B}) \leq 1/8$.

Now for $\ell = 3$ repetitions, the probability that the $\mathrm{HN}_{\mathbb{C}}$ outputs "yes" if the input system is unsatisfiable over $\mathbb{C}$ is at most $1/8$. That is, $\Pr(\mathcal{A}^c \mid \mathcal{B}^c) \geq 1 - 1/8$. The probability of the algorithm applied to our system outputting "no" is then

$$\begin{aligned}
\Pr(\mathcal{A}^c) &= \Pr(\mathcal{B}) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}) + \Pr(\mathcal{B}^c) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}^c) \\
&\geq \Pr(\mathcal{B}^c) \cdot \Pr(\mathcal{A}^c \mid \mathcal{B}^c) \\
&\geq \left(1 - \frac{1}{8}\right) \cdot \left(1 - \frac{1}{8}\right) = \frac{49}{64} \geq \frac{2}{3}
\end{aligned}$$

If our fixed instance of $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ is positive, i.e., $\dim V^* \geq d$, then $\dim V \geq m + d$ and V is in normal position with respect to the variables $\{x_1, \ldots, x_m, y_1, \ldots, y_d\}$ as asserted by Proposition 4.11. We rely on Theorem 4.12 in order to compute the probability of $\pi_{m+d}(AV)$ being dense in $\mathbb{C}^{m+d}$ where A is a randomly chosen linear transformation. Following the theorem, $\pi_{m+d}(AV)$ may not be dense in $\mathbb{C}^{m+d}$ if the polynomial P_V defined in the theorem vanishes on A, i.e., $P_V(A) = 0$. By Theorem 4.15, the probability that the polynomial P_V vanishes on a randomly chosen integer-valued matrix with entries from $\{1, 2, \ldots, D\}$ is at most $\frac{2(m+n)^2}{D}$. That is, $\Pr(\mathcal{C}^c) \leq \frac{2(m+n)^2}{D}$, which for our choice of D is at most $1/8$.

Now if we choose A such that $\pi_{m+d}(AV)$ is dense in $\mathbb{C}^{m+d}$, we may still choose an integer point $\boldsymbol{\alpha} \in \{1, 2, \ldots, D\}^{m+d}$ such that $\boldsymbol{\alpha} \notin \pi_{m+d}(AV)$. By Theorem 4.14 the probability that an integer point of height at most D is in $\pi_{m+d}(AV)$ if $\pi_{m+d}(AV)$ is dense in $\mathbb{C}^{m+d}$ is at least $1 - \frac{C}{D}$, where $C = 6(m + d) \cdot 2^{4(n-d)}$ (using the assumption the the polynomials defining V are of degree at most 2). For our choice of D, the latter is at least $1 - 1/8$.

The probability of the system defining AV being satisfiable over $\mathbb{C}$ for a random choice of A and $\alpha_1, \ldots, \alpha_{m+d}$ is thus

$$\begin{aligned}\Pr(\mathcal{B}) &= \Pr(\mathcal{C}) \cdot \Pr(\mathcal{B} \mid \mathcal{C}) + \Pr(\mathcal{C}^c) \cdot \Pr(\mathcal{B} \mid \mathcal{C}^c) \\ &\geq \Pr(\mathcal{C}) \cdot \Pr(\mathcal{B} \mid \mathcal{C}) \\ &\geq \left(1 - \frac{1}{8}\right) \cdot \left(1 - \frac{1}{8}\right) = \frac{49}{64} \geq \frac{2}{3}\end{aligned}$$

Since the $\mathrm{HN}_{\mathbb{C}}$ algorithm admits perfect correctness $\Pr(\mathcal{A}^c \cap \mathcal{B}) = 1$. The final probability $\Pr(\mathcal{A}^c)$ of the algorithm outputting "yes" is thus greater or equal to $\Pr(\mathcal{B}) \geq 2/3$.

We have thus established a **BPP** reduction from $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$. Since **AM** is closed under probabilistic reductions, this proves the theorem. □

4.4 Discussion and perspectives

In this chapter we studied a parametric version of the Hilbert's Nullstellensatz problem. We began by showing that the problem of determining whether a system of polynomial equations with polynomial coefficients admits a solution belongs to the complexity class **AM** assuming GRH. We exhibited two proofs of the result, both reducing the problem to $\mathrm{HN}_{\mathbb{C}}$, which was shown to belong to **AM** assuming GRH in [8]. We first approached $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ using number-theoretic techniques generalising the approach presented in [8]. We then discussed the relation of $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to the dimension problem over $\mathbb{C}$, and showed that with a small modification, the **AM** protocol for $\mathrm{DIM}_{\mathbb{C}}$ from [11] applies to $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ and $\mathrm{DIM}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ as well.

The number-theoretic approach relies on an effective parametric variant of Hilbert's Nullstellensatz [99] for the negative instances and the fact that we are considering separable algebraic extensions for the positive instances. The geometric approach taken from [11], on the other hand, relies on the fact that the field contains $\mathbb{R}$ as a subfield. More specifically,

the arguments are based on results on approximating the proportion of points with integer coordinates that lie in a real variety by the Lebesgue measure of the variety. This, in turn, requires a bound on the number of connected components of the variety. The arguments are used both for positive and negative instances. Interestingly enough, to the best of our understanding, the paper [99] on an effective parametric variant of Hilbert's Nullstellensatz does not seem to use techniques related to Koiran's approach via connected components, but rather works with the height of numbers, the Mahler measure, and resultants.

Both approaches to $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ we discussed boil down to reducing the problems to $\mathrm{HN}_{\mathbb{C}}$, but rely on conceptually different techniques. It is natural to wonder whether either of them could be generalised to other variants of the HN problem. Could they be extended, say, to other fields of characteristic zero (not necessarily algebraically closed)? Or, more generally, separable fields? The field $\overline{\mathbb{Q}(\boldsymbol{x})}$ can also be seen as a valued field where the valuation of a formal series $a(\boldsymbol{x}) = \sum_{\boldsymbol{e}\in\mathbb{Q}^m} a_{\boldsymbol{e}}\boldsymbol{x}^{\boldsymbol{e}} \in \overline{\mathbb{Q}(\boldsymbol{x})}$ is defined as the lowest exponent $\boldsymbol{e}$ such that the support $a_{\boldsymbol{e}}$ is non-zero. While we do not use the properties of this valuation directly, it is tempting to wonder whether one could use any of the insights on $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to handle other valued fields. A notable example of those is the field of p-adic numbers $\mathbb{Q}_p$ for a prime p, or better yet $\mathbb{C}_p$, which is the algebraically closed and complete extension of $\mathbb{Q}_p$.

Open problems. As discussed above, we leave a more comprehensive comparison of the two approaches to $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ and their possible extensions as a first open question. One such extension could be to study the problem of determining, given polynomials $f_1, \ldots, f_k$ with coefficients in $\mathbb{Z}[\boldsymbol{x}]$, whether they admit a solution in an algebraically closed subfield of $\overline{\mathbb{Q}(\boldsymbol{x})}$. As a possible approach, let us mention the paper [154], which gives a characterising theorem that, if made effective, may provide another algebraic technique to tackle $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$, and more importantly, its variants over other fields of characteristic zero. Using a combination of the primitive element theorem and the asymptotic version of Chebotarev's density theorem, the authors show that a finite set S in a characteristic zero integral domain can be mapped to $\mathbb{Z}/p\mathbb{Z}$ for infinitely many primes p, preserving all algebraic incidences in S. Could applying their reasoning circumvent the reduction to $\mathrm{HN}_{\mathbb{C}}$ and allow for examining satisfiability of a system $f_1, \ldots, f_k \in \mathbb{Z}[\boldsymbol{x}][y_1, \ldots, y_n]$ in a finite field $\mathbb{F}_p$ directly?

In [11, Section 5] Koiran provided an alternative approach to proving that $\mathrm{DIM}_{\mathbb{C}}$ is in **AM** in the bit model assuming GRH, namely by showing that $\mathrm{DIM}_{\mathbb{C}}$ is in $\mathbf{NP}_{\mathbb{C}}$ for the Blum-Shub-Smale model, and using an independent result showing that all problems in $\mathbf{NP}_{\mathbb{C}}$ are in **AM** under GRH. (The proof follows as $\mathrm{HN}_{\mathbb{C}}$ is the canonical $\mathbf{NP}_{\mathbb{C}}$ problem as discussed in Section 1.2, and its boolean counterpart is in **AM** under GRH). He also showed through the same reasoning that the problem which for a fixed $d \in \mathbb{N}$, given a constructible set, asks to determine whether the set contains an irreducible component of codimension at least d is in **AM** under GRH [93]. Could one build on the work we did in this chapter and show the same result via an algebraic reasoning through the standard bit model?

Another interesting observation that we reprove in Section 4.2.3 and that is also used in [11, Section 5] is that if a variety $V \subseteq \mathbb{C}^n$ defined by a system of equations $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ has dimension at least d over $\mathbb{C}$ and the d algebraically independent coordinates in $\mathbb{C}[V]$ are $x_1, \ldots, x_d$, then the values which we can choose for $x_1, \ldots, x_d$ such that the specialised system remains satisfiable over $\mathbb{C}^{n-d}$ belong to an open set. In other words,

the set of values for $x_1, \ldots, x_d$ in $\mathbb{C}^d$ keeping the system satisfiable over $\mathbb{C}^{n-d}$ is dense in $\mathbb{C}^d$. The positive instance of the problem could thus be read as "for almost all $x_1, \ldots, x_d \in \mathbb{C}^d$, there exist $x_{d+1}, \ldots, x_n \in \mathbb{C}^{n-d}$ such that $f_1(x_1, \ldots, x_n) = 0, \ldots, f_k(x_1, \ldots, x_n) = 0$ hold." It seems that deciding the $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ or the $\mathrm{DIM}_{\mathbb{C}}$ problem respectively is not far from deciding first-order formulas with one quantifier alternation over $\mathbb{C}$. The latter problem is known to be decidable in **PSPACE** for a fixed number of quantifier alternations. Could one use algebraic and number-theoretic techniques to improve the complexity of deciding formulas with one quantifier alternation to **AM** or even just the polynomial hierarchy?

Chapter 5

The Membership Problem for hypergeometric sequences

In this chapter we study the problem of deciding whether zero appears in a polynomially recursive sequence arising as a sum of two hypergeometric sequences. As shown in Section 1.3, the problem at hand reduces to the problem of determining, given a hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ and a target $t \in \mathbb{Q}$, whether t is a member of $\langle u_n \rangle_{n=0}^{\infty}$, which we call the Membership Problem for hypergeometric sequences (MP).

The results presented in this chapter are based on a joint work with Amaury Pouly, Mahsa Shirmohammadi, and James Worrell [155].

Organisation of the chapter. We begin this chapter by recalling notation and listing some simplifications that we may apply without loss of generality when studying the Membership Problem in Section 5.1. In Section 5.2 we discuss the natural idea of deciding MP by studying the asymptotic behaviour of the sequence, identifying the non-trivial cases of MP to be those where the shift quotient $r(x)$ converges to ± 1 as x tends to infinity. In Section 5.2.1, we discuss how solving this class of instances of MP relates to the Gamma function, and in Section 5.2.2 give a decidability proof for the Membership Problem for hypergeometric sequences with rational parameters conditioned to the assumption of the Rohrlich-Lang Conjecture.

We then introduce our prime divisibility approach, which allows us to establish unconditional decidability for the Membership Problem for hypergeometric sequences with higher-degree algebraic parameters. In Section 5.3.1 we give an overview of the approach, followed by the technical lemmas and proofs in Sections 5.3.2 to 5.3.5. We conclude by discussing extensions of the approach to MP for hypergeometric sequences with higher-degree algebraic parameters in Section 5.4.

Relevant preliminaries. The preliminary sections useful for reading this chapter are Sections 2.3.5, 2.3.6 and 2.4.1.

5.1 Notation and initial simplifications

Recall that we say a sequence $\langle u_n \rangle_{n=0}^{\infty}$ of rational numbers is *hypergeometric* if it satisfies a recurrence of the form

$$p(n)u_n - q(n)u_{n-1} = 0\,, \tag{5.1}$$

where $p(x)$, $q(x) \in \mathbb{Q}[x]$ are polynomials. We call the roots of the polynomials $p(x)$ and $q(x)$ the *parameters* of the sequence. If both $p(x)$ and $q(x)$ split completely over $\mathbb{Q}$, we say that such an induced sequence is a *hypergeometric sequence with rational parameters*.

When we reformulate recurrence (5.1) as

$$u_n = r(n)u_{n-1}\,, \tag{5.2}$$

we call $r(x) = \frac{q(x)}{p(x)} \in \mathbb{Q}(x)$ the *shift quotient* of $\langle u_n \rangle_{n=0}^{\infty}$.

We say that $t \in \mathbb{Q}$ is a *member* of a sequence $\langle u_n \rangle_{n=0}^{\infty}$ if there exists $n \in \mathbb{N}$ such that $u_n = t$; we further refer to n as an index of t in the sequence. The *Membership Problem (*MP*)* for hypergeometric sequences is the problem of deciding, given a hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ (specified by a a recurrence of the form (2.3) with a given initial value u_0) and a target $t \in \mathbb{Q}$, whether t is a member of $\langle u_n \rangle_{n=0}^{\infty}$.

Assumption on $p(x)$. We recall the assumption that $p(x)$ has no non-negative integer zeroes. This assumption on $p(x)$ implies that the recurrence relation (5.1) uniquely defines an infinite sequence of rational numbers once the initial value $u_0 \in \mathbb{Q}$ is specified.

Assumption on u_0. We will assume that in instances of MP, the initial term of the sequence u_0 is equal to one. This assumption is without loss of generality. Indeed, given an instance of the Membership Problem comprising a sequence $\langle u_n \rangle_{n=0}^{\infty}$ defined by $r(x)$ and u_0, and a target t, deciding whether t is a member of $\langle u_n \rangle_{n=0}^{\infty}$ is equivalent to deciding whether the target $t' = \frac{t}{u_0}$ is a member of the sequence $\langle u'_n \rangle_{n=0}^{\infty}$ defined by the shift quotient $r(x)$ and initial value $u'_0 = 1$.

Assumption on $q(x)$ and t. We will assume that in instances of MP, the numerator $q(x)$ of the shift quotient has no non-negative integer zeros and that the target t is non-zero. The assumption on $q(x)$ is without loss of generality as otherwise, the sequence $\langle u_n \rangle_{n=0}^{\infty}$ will be ultimately always zero. Indeed, if $q(x)$ has non-negative integer zeros, $u_n = 0$ for all $n \geq m$ where m is the smallest non-negative integer root of $q(x)$. Consequently, the search domain for indices of t in MP will be limited to the finite set $\{u_0, \ldots, u_m\}$. We note that determining whether a univariate polynomial has a non-negative integer zero is clearly decidable, as the magnitude of integer zeros of univariate polynomials are upper-bounded by the height of the polynomial. This assumption on $q(x)$ will exclude the membership of zero in the sequence $\langle u_n \rangle_{n=0}^{\infty}$, and will allow us to further assume that $t \neq 0$.

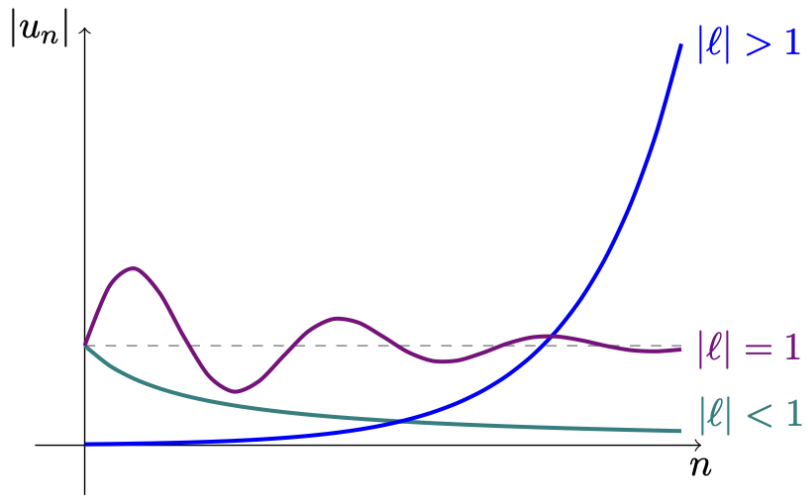

Figure 5.1 – Asymptotic behaviour of the sequence $|u_n|$ for three different cases: when $r(x)$ converges to a limit ℓ with $|\ell| > 1$ or diverges to $\pm\infty$ in blue, when $r(x)$ converges to a limit ℓ with $|\ell| < 1$ in teal, and when $r(x)$ converges to ± 1 as x tends to infinity in violet.

5.2 Asymptotic behaviour of hypergeometric sequences

Fundamentally, determining whether a target t appears in a sequence $\langle u_n \rangle_{n=0}^{\infty}$ requires us to understand how the sequence behaves as n goes to infinity. In this section we study the asymptotic behaviour of hypergeometric sequences, and explore whether the Membership Problem could be solved using analytic techniques. We initially consider the general case of the Membership Problem for hypergeometric sequences with complex parameters.

Recall that by Equation (5.2) we can define the seqence $\langle u_n \rangle_{n=0}^{\infty}$ via the recurrence $u_n = r(n)u_{n-1} = \prod_{k=1}^{n} r(k)$. and notice that the asymptotics of the sequence really depend on the asymptotic behaviour of $r(x)$. Furthermore, $r(x)$ is ultimately monotonic as x tends to infinity, and the same holds for the sequence $\langle u_n \rangle_{n=0}^{\infty}$.

The possible behaviours of u_n as $n \to \infty$ are illustrated in Figure 5.1. Before analysing the three cases in the figure, let us recall that an infinite product $\prod_{k=1}^{\infty} r(k)$ is said to *converge* if the sequence of its partial products converges to a nonzero limit. In the context of hypergeometric sequences, we thus say that the sequence $\langle u_n \rangle_{n=0}^{\infty}$ converges if and only if $\prod_{k=1}^{\infty} r(k)$ converges, and we use the two terms interchangeably.

As $x \to \infty$ the shift quotient $r(x) \in \mathbb{Q}(x)$ either converges to a limit in $\mathbb{Q}$ or diverges to $\pm\infty$. In case $r(x)$ diverges to $\pm\infty$ or converges to some $\ell \in \mathbb{Q}$ with $|\ell| > 1$, then the sequence $\langle u_n \rangle_{n=0}^{\infty}$ diverges to $\pm\infty$ as well (as illustrated in blue in Figure 5.1). Thus there exists $n_0 \in \mathbb{N}$ such that

$$|u_n| = \left| \prod_{k=1}^{n} r(k) \right| > |t| \text{ for all } n \geq n_0.$$

In this case, it is sufficient to try all values of n up to this bound to solve the problem. Furthermore, it is not difficult to decide whether this situation occurs and to compute a

suitable n_0.

The second case on Figure 5.1 (illustrated in green) is when $r(x) = \frac{q(x)}{p(x)}$ converges to some ℓ with $|\ell| < 1$. In this case determining whether there exists $n \in \mathbb{N}$ such that $\prod_{k=1}^{n} \frac{q(n)}{p(n)} = t$ is equivalent to determining whether for some $n \in \mathbb{N}$, we have $\prod_{k=1}^{n} \frac{p(n)}{q(n)} = t^{-1}$. We can thus consider an instance of MP comprising the inverse sequence $\langle u'_n \rangle_{n=0}^{\infty}$ given by the shift quotient $r'(x) = \frac{p(x)}{q(x)}$ converging to the limit $\ell' := \ell^{-1}$ and target $t' := t^{-1}$ and apply the argument given above. Henceforth we will refer to the instances of MP defined by shift quotients converging to a limit $\ell \neq \pm 1$ or diverging to $\pm\infty$ as the *trivial* instances.

The remaining case is when $r(x)$ converges to ℓ with $|\ell| = 1$ as x tends to infinity, which is the only case when $\prod_{k=1}^{\infty} r(k)$ may converge as well. Assume that the infinite product converges, and denote by ω its limit. Suppose furthermore that the product is eventually strictly increasing as on Figure 5.1. In this case we can compute n_0 such that $u_n < \omega$ for all $n > n_0$. If $\omega \leq t$ then we have $u_n \neq t$ for all $n > n_0$, and it suffices to check whether $t \in \{u_0, \ldots, u_{n_0}\}$ to decide the problem. On the other hand, if $\omega > t$, then we can find $n_1 \geq n_0$ such that $u_n > t$ for all $n > n_1$. Again, this leaves only a finite number of cases to check. The case when $\prod_{k=1}^{\infty} r(k)$ is eventually strictly decreasing follows analogously.

To decide the final (*non-trivial*) case of MP via the asymptotic approach, we thus need to understand how to compute the limit of $\prod_{k=1}^{\infty} r(k)$. We will now see how the latter relates to a problem involving Gamma functions.

5.2.1 Reducing MP to a problem on Gamma functions

We have noted that the limit of the infinite product $\prod_{k=1}^{\infty} r(k)$ may converge if and only if $r(x)$ converges to ± 1 as x tends to infinity. Observe that if $r(x)$ converges to ± 1, the degrees of its numerator and denominator must be equal. That is, we can write

$$r(x) = \frac{(x + \alpha_1) \cdots (x + \alpha_d)}{(x + \beta_1) \cdots (x + \beta_d)} \tag{5.3}$$

Note that $\alpha_1, \ldots, \alpha_d$ and $\beta_1, \ldots, \beta_d$ are complex numbers, none of which are negative integers. The latter is ensured by our initial assumptions on the roots of the polynomials $p(x), q(x) \in \mathbb{Q}[x]$ defining our hypergeometric sequences as discussed in Section 5.1.

Now in order to understand the limit of the infinite product $\prod_{k=1}^{\infty} r(k)$, let us take a closer look at the infinite product of a linear factor of the expression, say $\prod_{k=1}^{\infty}(k + \alpha)$ for some $\alpha \in \{\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d\}$. Notice that if $\alpha \in \mathbb{N}$, the product

$$\prod_{k=1}^{n}(k + \alpha) = (n + \alpha)(n - 1 + \alpha) \cdots (1 + \alpha)$$

corresponds to the expression $\frac{(\alpha+n)!}{\alpha!}$. Following this intuition, we relate the asymptotic behaviour of $\prod_{k=1}^{\infty} r(k)$ to the Gamma function Γ, which is a generalisation of the factorial function to all complex numbers but non-positive integers. In particular, for every positive integer n, we have $\Gamma(n) = (n - 1)!$.

Let us recall that the Gamma function was first derived by David Bernoulli, who defined it as the integral

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}\,dt.$$

Euler later defined the function in terms of an infinite product

$$\Gamma(x) = \frac{1}{x}\prod_{n=1}^{\infty}\frac{n}{n+x}\left(1+\frac{1}{n}\right)^x. \tag{5.4}$$

There is also a third definition of the Gamma function due to Weierstrass, and the three definitions are known to be equivalent.

Furthermore, for all $x \in \mathbb{C} \setminus \mathbb{Z}_{\leq 0}$, the function satisfies the following three relations.

$$\begin{aligned} \Gamma(x+1) &= x\Gamma(x) && \text{(Translation)},\\ \Gamma(x)\Gamma(1-x) &= \tfrac{\pi}{\sin(\pi x)} && \text{(Reflection)},\\ \textstyle\prod_{k=0}^{n-1}\Gamma\left(x+\frac{k}{n}\right) &= (2\pi)^{\frac{n-1}{2}}n^{\frac{1}{2}-nx}\Gamma(nx) && \text{(Multiplication)} \end{aligned} \tag{5.5}$$

For more details on the Gamma function and its relation to hypergeometric sequences, see [135, Section 5.2].

Recall we are interested in the limit of the infinite product $\prod_{k=1}^{\infty} r(k)$. As one might expect by examining the definitions of the function we have listed above, Euler's infinite-product characterisation (5.4) allows us to relate the limit of $\prod_{k=1}^{\infty} r(k)$ to an expression involving Gamma functions. Indeed, it is standard that certain infinite products of rational functions converge to quotients of values of the Gamma function. For a more detailed discussion, see, e.g., [156]. The result of the cited paper which is of particular interest to us is Theorem 1.1, which we restate below.

Proposition 5.1. *Let $d \leq 1$ and $\alpha_1, \ldots, \alpha_d$ and $\beta_1, \ldots, \beta_d$ be nonzero complex numbers, none of which are negative integers. If $\alpha_1 + \ldots + \alpha_d = \beta_1 + \ldots + \beta_d$ then*

$$\prod_{k=1}^{\infty}\frac{(k+\alpha_1)\cdots(k+\alpha_d)}{(k+\beta_1)\cdots(k+\beta_d)} = \frac{\beta_1\cdots\beta_d}{\alpha_1\cdots\alpha_d}\frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)}, \tag{5.6}$$

otherwise the infinite product diverges.

Proof. Use Euler's definition of the Γ function (5.4) to write

$$\begin{aligned} \frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)} &= \frac{\alpha_1\cdots\alpha_d}{\beta_1\cdots\beta_d}\prod_{k=1}^{\infty}\left[\frac{\prod_{i=1}^{d}\frac{k}{k+\beta_i}}{\prod_{i=1}^{d}\frac{k}{k+\alpha_i}}\left(1+\frac{1}{k}\right)^{\sum_{i=1}^{d}\beta_i-\sum_{i=1}^{d}\alpha_i}\right]\\ &= \frac{\alpha_1\cdots\alpha_d}{\beta_1\cdots\beta_d}\prod_{k=1}^{\infty}\frac{(k+\alpha_1)\cdots(k+\alpha_d)}{(k+\beta_1)\cdots(k+\beta_d)}\prod_{k=1}^{\infty}\left(1+\frac{1}{k}\right)^{\sum_{i=1}^{d}\beta_i-\sum_{i=1}^{d}\alpha_i} \end{aligned}$$

We deduce that the infinite product $\prod_{k=1}^{\infty} \frac{(k+\alpha_1)\cdots(k+\alpha_d)}{(k+\beta_1)\cdots(k+\beta_d)}$ is equal to

$$\frac{\beta_1 \cdots \beta_d}{\alpha_1 \cdots \alpha_d} \frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)} \prod_{n=1}^{\infty} \left(1+\frac{1}{n}\right)^{\sum_{i=1}^{d}\alpha_i - \sum_{i=1}^{d}\beta_i}.$$

Since $\frac{\beta_1\cdots\beta_d}{\alpha_1\cdots\alpha_d}\frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)}$ is constant, the infinite product we are studying will converge if and only if $\prod_{n=1}^{\infty}\left(1+\frac{1}{n}\right)^{\sum_{i=1}^{d}\alpha_i-\sum_{i=1}^{d}\beta_i}$ converges. Observing that the latter converges to 1 if $\sum_{i=1}\alpha_i = \sum_{i=1}\beta_i$, and diverges otherwise, proves the proposition. □

The result we just proved gives us a characterisation of the limit of the sequence $\langle u_n\rangle_{n=0}^{\infty}$, which is exactly what we required in order to show decidability of the non-trivial instances of the Membership Problem. Indeed, let us look at an example of the decision procedure in this case.

Example 5.1. *Consider the sequence $\langle w_n\rangle_{n=0}^{\infty}$ defined by the shift quotient*

$$s(x) := \frac{(x+\frac{9}{2})(x+\frac{7}{2})(x+\frac{5}{2})}{(x+\frac{11}{2})(x+4)(x+1)}.$$

We study an instance of the Membership Problem for the sequence $\langle w_n\rangle_{n=0}^{\infty}$ and target $t = \frac{13}{6}$.

The rational function $s(x)$ converges to 1 from above as $x \to \infty$. This implies that the sequence $\langle w_n\rangle_{n=0}^{\infty}$ is monotonically increasing to its limit value, that is

$$\prod_{k=1}^{\infty}\frac{(k+\frac{9}{2})(k+\frac{7}{2})(k+\frac{5}{2})}{(k+\frac{11}{2})(k+4)(k+1)} = \frac{\frac{11}{2}\cdot 4\cdot 1}{\frac{9}{2}\cdot\frac{7}{2}\cdot\frac{5}{2}}\frac{\Gamma(\frac{11}{2})\Gamma(4)\Gamma(1)}{\Gamma(\frac{9}{2})\Gamma(\frac{7}{2})\Gamma(\frac{5}{2})} = \frac{2^9\cdot 11}{3\cdot 5^2\cdot 7\cdot\pi}.$$

Here, we compute the limit value above using the known relations $\Gamma(n) = (n-1)!$ and $\Gamma(\frac{n}{2}) = \sqrt{\pi}\frac{(n-2)!!}{2^{\frac{n-1}{2}}}$ for $n \in \mathbb{N}$. We recall that the double factorial $n!!$ of a natural number n is defined to be the product of all the positive integers up to n that have the same parity (odd or even) as n.

Using the fact $\langle w_n\rangle_{n=0}^{\infty}$ is strictly increasing, it suffices to observe that $w_6 > \frac{13}{6}$. By verifying that none of $w_0, \ldots, w_5$ equals $\frac{13}{6}$, we conclude that $\frac{13}{6}$ is not a member of the sequence. Let us note that such an argument is possible because w_n does not converge to $\frac{13}{6}$.

More generally, we are able to show that deciding instances of the Membership Problem with converging shift quotients reduces to deciding a relation among values of the Gamma function.

Proposition 5.2. *The Membership Problem for hypergeometric sequences* with real parameters *reduces to deciding, given $d \geq 1$ and $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d \in \mathbb{R} \setminus \mathbb{Z}_{<0}$, whether*

$$\Gamma(\beta_1)\cdots\Gamma(\beta_d) = \Gamma(\alpha_1)\cdots\Gamma(\alpha_d). \tag{5.7}$$

Proof sketch. As discussed in the beginning of Section 5.2, the only case of the Membership Problem that is not trivially decidable is when the sequence $\langle u_n \rangle_{n=0}^{\infty}$ converges. This is when the shift quotient $r(x) \in \mathbb{Q}(x)$ of the sequence $\langle u_n \rangle_{n=0}^{\infty}$ converges to ± 1 as $x \to \infty$, and by Proposition 5.1, if and only if $\alpha_1 + \ldots + \alpha_d = \beta_1 + \ldots + \beta_d$. We assume without loss of generality that for the instances of the problem we reason about below, the sequence is converging. We treat the case that the product

$$\prod_{k=1}^{n} \frac{(k+\alpha_1)\cdots(k+\alpha_d)}{(k+\beta_1)\cdots(k+\beta_d)}, \tag{5.8}$$

is eventually strictly increasing. The case that it is eventually strictly decreasing follows *mutatis mutandis*.

Write $\omega := C \cdot \frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)}$ for the limit (5.6) of the finite product (5.8) as n tends to ∞, where $C = \frac{\beta_1 \cdots \beta_d}{\alpha_1 \cdots \alpha_d}$. By the assumption that (5.8) is eventually strictly increasing, we can compute n_0 such that $u_n < \omega$ for all $n > n_0$. If $\omega \leq t$ then we have $u_n \neq t$ for all $n > n_0$, and it remains to check by exhaustive search whether $t \in \{u_0, \ldots, u_{n_0}\}$. On the other hand, if $\omega > t$, then we can find $n_1 \geq n_0$ such that $u_n > t$ for all $n > n_1$. Again, this leaves only a finite number of cases to check.

We thus need only to decide whether or not $\omega \leq t$. First, let us note that we can decide whether $\omega < t$ and whether $\omega > t$ by computing ω to sufficient precision. Thus the Membership Problem for real parameters reduces to deciding whether $\omega = t$. Now note that $\Gamma\left(\frac{t}{C} + 1\right) = \frac{t}{C}\Gamma\left(\frac{t}{C}\right)$, hence

$$\omega = t \;\Leftrightarrow\; \frac{\Gamma(\beta_1)\cdots\Gamma(\beta_d)\Gamma\left(\frac{t}{C}\right)}{\Gamma(\alpha_1)\cdots\Gamma(\alpha_d)\Gamma\left(\frac{t}{C}+1\right)} = 1.$$

The equation above is an instance of (5.7) with two extra parameters, $\alpha_{d+1} := \frac{t}{C} + 1$ and $\beta_{d+1} := \frac{t}{C}$. This completes the reduction. □

Let us remark that the reduction above applies to the Membership Problem for hypergeometric sequences with *real* parameters, as we use the total order on $\mathbb{R}$ in the decision procedure.

Proposition 5.2 implies that MP can be solved simply by deciding whether (5.7) holds. Unfortunately, the latter appears to be a difficult problem. In particular, just like the limit of the shift quotient in Example 5.1, the values of the Gamma function (even) at rational points may be transcendental. Unlike the special cases of values of the Gamma function we chose in Example 5.1, in general, no simple expressions are known for the values of the Gamma function at rational points. The following example from [156] illustrates a case where a quotient is an integer but in which none of the values of Γ involved are known to be algebraic

$$\frac{\Gamma(\frac{1}{14})\Gamma(\frac{9}{14})\Gamma(\frac{11}{14})}{\Gamma(\frac{3}{14})\Gamma(\frac{5}{14})\Gamma(\frac{13}{14})} = 2.$$

A standard technique for deciding equality of algebraic expressions is via numerical approximation. That is, we may try to compute approximations to the left and right hand side of (5.7) and decide equality by comparing the approximate values. If the approximations differ at a given digit, we know that the expressions are not equal. However, we are not aware of any lower bound on the difference between the two terms of (5.7). This means that we do not have a bound on the precision that suffices to decide that if the two approximates are equal up until a given digit, the same must hold for the expressions involving the Gammas, and our algorithm can terminate.

To summarise, we have just shown that the problem of deciding (5.7), and thus the Membership Problem, is at least semi-decidable, and known techniques do not seem to allow us to show it is decidable. However, algebraic relations among values of the Gamma function are still an active area of research in number theory, and we are able to use the intuitions there to obtain conditional decidability.

5.2.2 A conditional decidability result

In this section we highlight the link between the Membership Problem for hypergeometric sequences and the Rohrlich-Lang conjecture, which concerns algebraic relations among values of the Gamma function at rational points.

The question of giving a complete list of all *multiplicative relations* among the values of the Gamma function *at rational points* was first considered by Rohrlich, who conjectured the following.

Conjecture 5.3 (Rohrlich)**.** *Any multiplicative relation of the form*

$$\pi^{b/2} \prod_{a \in \mathbb{Q}} \Gamma(a)^{m_a} \in \overline{\mathbb{Q}}$$

with b and m_a in $\mathbb{Z}$ is a consequence of the standard relations (5.5)*.*

The conjecture was formalised by Lang in terms of "universal distributions" on $\mathbb{Q} \setminus \mathbb{Z}$ [157], and generalised to what is now known as the Rohrlich-Lang conjecture for polynomial relations in Gamma values. Intuitively speaking, the conjecture predicts that all polynomial relations between Gamma values over $\mathbb{Q}$ come from the functional equations (5.5) satisfied by the Gamma function. The closest result to our problem is a theorem by Koblitz and Ogus [158] giving a sufficient condition under which a quotient of products of Gamma values over $\mathbb{Q}$ is algebraic: they show that if such a quotient is an algebraic number, then it can be evaluated by using only the reflection and multiplication formulae. The Rohrlich-Lang conjecture remains wide open and is part of the larger work on the transcendence of periods [159]. For more details on these conjectures, see [160, Section 24.6].

Note that the Rohrlich-Lang conjecture is only concerned with rational parameters and, as far as we are aware, there is no analog of this conjecture for algebraic parameters. We now observe that if the Rohrlich-Lang conjecture is true, then the Membership Problem becomes decidable for rational parameters.

Theorem 5.4. *The Membership Problem for hypergeometric sequences with rational parameters is decidable if the Rohrlich-Lang conjecture is true.*

Proof sketch. By Proposition 5.2 the Membership Problem reduces to the question of deciding equations of the form (5.7), in which the parameters α_i and β_i are rational. Assuming the Rohrlich-Lang conjecture, the latter problem is recursively enumerable: if equality holds, then the equation has a finite derivation using the standard relations (5.5). On the other hand, the problem is also straightforwardly co-recursively enumerable: if Equation (5.7) does not hold, then by computing the left and right-hand sides to sufficient precision we will eventually conclude that the two terms are not equal. □

As discussed in Section 1.3, MP is not the only zero problem for recursive sequences the decidability of which can be related to results from transcendence theory. Furthermore, while studying Threshold Problems goes beyond the scope of this thesis, let us note that the Threshold Problem for hypergeometric sequences with rational parameters can also be decided subject to the Rohrlich-Lang conjecture. For more details on this, see [155, Proposition 3 and Theorem 5] or the preprint [161, Section 3]. What is more, the Threshold Problem and deciding the equality (5.7) are interreducible. This suggests that the Threshold Problem is strictly more difficult than the Membership Problem. In the rest of this chapter, we present our unconditional result on the decidability of the Membership Problem. The techniques we use do not allow us to extend the unconditional decidability to the Threshold Problem, again showing that, in general, threshold problems are more difficult to tackle.

5.3 Unconditional decidability

In the previous section we showed that approaching the Membership Problem for hypergeometric sequences with rational parameters analytically does not seem to yield an algorithm for deciding the problem, unless we assume the Rohrlich-Lang conjecture. In this section we present an alternative approach to the problem, notably by studying the prime divisors of the sequence $\langle u_n \rangle_{n=0}^{\infty}$. As announced in the Introduction, the approach allows us to show that the Membership Problem for hypergeometric sequences with rational parameters is decidable (unconditionally).

To this aim we will use p-adic valuations, which we introduced in Section 2.3.5. We will not require the full generality of $\mathbb{Q}_p$, but will instead work in a subring $\mathbb{Z}_{(p)}$ of $\mathbb{Q}_p$, which we present briefly here. We write $\mathbb{Z}_{(p)}$ to denote the ring $\{x \in \mathbb{Q} : v_p(x) \geq 0\}$. Alternatively, we have $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$. This is a local ring, whose unique maximal ideal is the principal ideal $p\mathbb{Z}_{(p)}$. The quotient $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ is isomorphic to the finite field $\mathbb{F}_p$. Specifically, we consider the quotient map $\mathrm{rem}_p : \mathbb{Z}_{(p)} \to \mathbb{F}_p$, given by

$$\mathrm{rem}_p\left(\frac{a}{b}\right) := ab^{-1} \bmod p\,.$$

Henceforth, when we say that $\frac{a}{b} \in \mathbb{Z}_{(p)}$ has p as a prime divisor we refer to divisibility in $\mathbb{Z}_{(p)}$.

5.3.1 Overview of the approach

We begin by giving a high-level overview of our unconditional decidability result. As discussed in Section 5.2, to prove decidability of MP it remains to handle the non-trivial instances, that is, the instances in which the shift quotient $r(x) \in \mathbb{Q}(x)$ converges to ± 1 as $x \to \infty$. In such instances, $r(x)$ is necessarily the quotient of two polynomials of equal degree. Throughout this section, we fix such an instance of MP, consisting of a rational value t and a hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ with rational parameters.

We will show that we can compute a bound N such that all indices of t in $\langle u_n \rangle_{n=0}^{\infty}$ are at most N. This allows us to reduce deciding MP to a finite search problem in $\{u_1, \ldots, u_N\}$. Our strategy is to find N such that for all $n > N$ there exists a prime p that is a prime divisor of u_n but not of t. To explain this idea in more detail, rewrite the shift quotient $r(x)$ as

$$\frac{(x-\alpha_1)\cdots(x-\alpha_d)}{(x-\beta_1)\cdots(x-\beta_d)},$$

where the α_i and the β_i are in $\mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$. We denote by A the multiset $\{\alpha_1, \ldots, \alpha_d\}$ consisting of all the (possibly repeated) roots of the numerator and by B the multiset $\{\beta_1, \ldots, \beta_d\}$ of the roots of the denominator. Denote by $\mathrm{Supp}(C)$ the underlying set of a multiset C. For each element $x \in \mathrm{Supp}(C)$ we write $m_C(x)$ for its multiplicity in C. We write $A \uplus B$ for the multiset with underlying set $\mathrm{Supp}(A) \cup \mathrm{Supp}(B)$ where the multiplicity of each of its elements x is $m_A(x) + m_B(x)$.

Given a prime p, we have that $v_p(u_n) = v_p\Big(\prod_{k=1}^{n} r(k)\Big)$ for all $n \in \mathbb{N}$. In particular, if

$$v_p\Big(\prod_{k=1}^{n} r(k)\Big) \neq 0\,,$$

then p appears in the factorisation of either the numerator or the denominator of the reduced form of the product $\prod_{k=1}^{n} r(k)$ when considered as a fraction in $\mathbb{Q}$. If furthermore $v_p(t) = 0$, then p does not appear in the factorisation of t, and is thus a witness that $u_n \neq t$. Notice we can rewrite the expression $v_p\Big(\prod_{k=1}^{n} r(k)\Big)$ as

$$S_p(n) := \sum_{k=1}^{n} \left(\sum_{\alpha \in A} v_p(k-\alpha) - \sum_{\beta \in B} v_p(k-\beta) \right). \tag{5.9}$$

We study the behaviour of the sum $S_p(n)$ for well-chosen primes p and increasing n and show that there exists a bound $N \in \mathbb{N}$ such that for all $n > N$, we can find a prime p witnessing that $u_n \neq t$.

The preorder $\preceq_r$. We begin our construction by defining a preorder on the parameters of r. Given an integer prime p, we first define a preorder $\preceq_p$ on $\mathbb{Z}_{(p)}$ by writing

$$\frac{a}{b} \preceq_p \frac{a'}{b'} \text{ if and only if } \mathrm{rem}_p(\tfrac{a}{b}) \leq \mathrm{rem}_p(\tfrac{a'}{b'})\,, \tag{5.10}$$

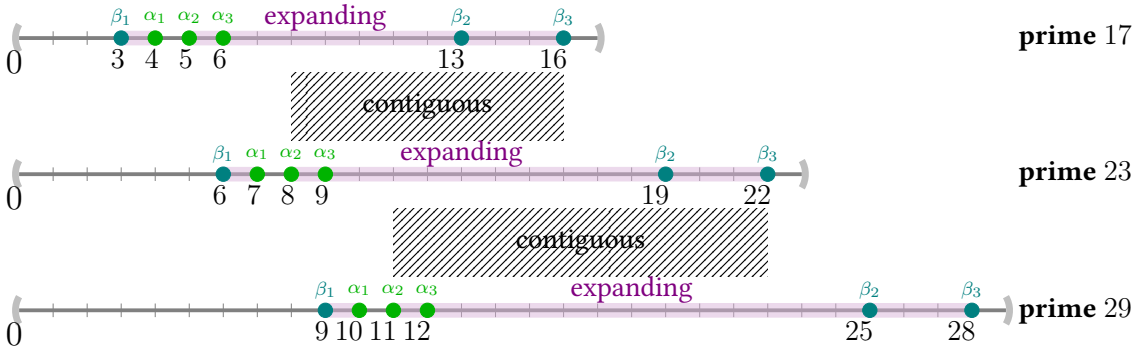

Figure 5.2 – Consider the sequence $\langle w_n \rangle_{n=0}^{\infty}$ given in Example 5.2. Observe that $\beta_1 \preceq_p \alpha_1 \preceq_p \alpha_2 \preceq_p \alpha_3 \preceq_p \beta_2 \preceq_p \beta_3$ for all primes $p \in \{17, 23, 29\}$. The two families of intervals (β_1, α_1) and (α_2, β_3) are s-unbalanced, where only the latter is s-expanding. In particular, the distance between residues of α_2 and β_3 modulo 23 is greater than their respective distance modulo 17. The same holds for their distance modulo 29 compared to their distance modulo 23. The s-expanding s-unbalanced intervals for 17, 23 and 29 are contiguous, which in turn ensures that for all $n \in \{5, \ldots, 27\}$ either 17 or 23 or 29 divides w_n. See Example 5.2 for a more detailed discussion.

where $\leq$ is the usual order on $\{0, \ldots, p-1\}$.

Denote by b the least common denominator of all fractions in $A \uplus B$. For every prime p in the arithmetic progression $b\mathbb{N} + 1$, all elements of $A \uplus B$ are in $\mathbb{Z}_{(p)}$. Notice that this follows from the characterisation of $\mathbb{Z}_{(p)}$ as the set of fractions $\{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$, which we gave in the beginning of Section 5.3. In Proposition 5.6 we show that for all sufficiently large primes $p \in b\mathbb{N} + 1$ the orders $\preceq_p$ restricted to $A \uplus B$ are identical. We denote this common preorder by $\preceq_r$, where r is the shift quotient of our fixed sequence.

Unbalanced intervals. Given a prime p, let $\frac{a}{b} \in \mathbb{Z}_{(p)}$ be such that $gcd(a, b) = 1$. Note that $v_p(b) = 0$, and for all $k \in \{1, \ldots, p-1\}$ such that $0 < |kb - a| < p^2$ we have

$$v_p\left(k - \frac{a}{b}\right) = \begin{cases} 1 & \text{if } \mathrm{rem}_p(\frac{a}{b}) = \mathrm{rem}_p(k), \\ 0 & \text{otherwise.} \end{cases} \tag{5.11}$$

Indeed, the condition on $|kb - a|$ ensures that p can only appear in the factorisations of the numerator and denominator of the reduced form of the fraction $k - \frac{a}{b}$ with exponents 0 or 1.

Recall that $A \uplus B \subseteq \mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$, and assume that all its elements are given in a reduced form (i.e., $\gcd(a, b) = 1$ for all $\frac{a}{b} \in A \uplus B$). Let p be a prime such that all elements of $A \uplus B$ are in $\mathbb{Z}_{(p)}$. Let $n \in \{1, \ldots, p-1\}$ be such that for all $k \in \{1, \ldots, n\}$, for all $\frac{a}{b} \in A \uplus B$, the inequalities $0 < |kb - a| < p^2$ hold. In this case, by Equation (5.11), the p-adic valuations in Equation (5.9) all take value 0 or 1. This means that $S_p(n)$ is non-zero if and only if the number of $\alpha \in A$ such that $\mathrm{rem}_p(\alpha) \in \{1, \ldots, n\}$ is not equal to the number of $\beta \in B$ such that $\mathrm{rem}_p(\beta) \in \{1, \ldots, n\}$. That is, by Definition (5.10), $S_p(n) \neq 0$ if and only if

$$|\{\alpha \in A : \alpha \preceq_p n\}| \neq |\{\beta \in B : \beta \preceq_p n\}|. \tag{5.12}$$

We say that $n \in \mathbb{N}$ is *p-unbalanced* if $S_p(n) \neq 0$. We extend this notion to sub-intervals of $\mathbb{N}$ by saying that an interval $I \subseteq \mathbb{N}$ is *p-unbalanced* if all $n \in I$ are p-unbalanced. By Equation (5.12), the maximal p-unbalanced sub-intervals of $\{1, \ldots, p-1\}$ will have endpoints that are equal or adjacent to the images $\mathrm{rem}_p(\frac{a}{b})$ of $\frac{a}{b} \in A \uplus B$. For more intuition on this, see Example 5.2 and the accompanying illustration in Figure 5.2.

Let γ and γ' be distinct elements of $A \uplus B$ such that $\gamma \prec_r \gamma'$. We denote by $\overline{(\gamma, \gamma')}$ the family of sub-intervals $\{n \in \mathbb{N} : \mathrm{rem}_p(\gamma) \leq n < \mathrm{rem}_p(\gamma')\}$ of $\mathbb{N}$ indexed by primes $p \in b\mathbb{N}+1$ whose respective orders agree with $\prec_r$ (i.e., indexed by sufficiently large primes in $b\mathbb{N}+1$). We show that for such a family of sub-intervals, indexed by primes p, either every interval is p-unbalanced or none of the intervals is p-unbalanced. In the former case we say that the family of intervals is r-unbalanced, where r is the shift quotient.

Expanding families and a degenerate case. Let $\gamma, \gamma' \in A \uplus B$ such that $\gamma \prec_r \gamma'$. In Proposition 5.7 we prove that for a sufficiently large prime p belonging to the arithmetic progression $b\mathbb{N}+1$, the *distance* $\mathrm{rem}_p(\gamma') - \mathrm{rem}_p(\gamma)$ between the respective residues of γ and γ' modulo p is a strictly increasing function of p, if and only if $\gamma - \gamma' \notin \mathbb{Z}$. In this case we say that the family of intervals $\overline{(\gamma, \gamma')}$ is *r-expanding*.

The identification of expanding families of unbalanced intervals is a crucial element in our proof, as it means that larger and larger primes p witness the non-equality $u_n \neq p$ for larger sets and larger sets of indices n. We further show in Proposition 5.8 that either there exists an r-expanding r-unbalanced family of intervals, or every hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ with shift quotient $r(x)$ is a rational function of n.

For the case when $\langle u_n \rangle_{n=0}^{\infty}$ is a rational function of n, we can rewrite it as $u_n = \frac{f(n)}{g(n)}$ with $f, g \in \mathbb{Q}[x]$. In order to test membership of t in $\langle u_n \rangle_{n=0}^{\infty}$, it suffices to check whether the polynomial $f(x) - tg(x)$ has an integer root, which is known to be decidable, as summarised in Corollary 5.9. Henceforth, we assume without loss of generality that there exists an r-expanding r-unbalanced family of intervals for our fixed instance of MP.

An infinite sequence of primes with contiguous unbalanced intervals. Fix $\gamma, \gamma' \in A \uplus B$ such that $\overline{(\gamma, \gamma')}$ is an r-expanding r-unbalanced family of intervals. Let $p, q \in b\mathbb{N}+1$ be primes sufficiently large that their respective orders agree with $\prec_r$. In Proposition 5.10 we show that if $p < q < p(1 + \frac{1}{b}) + C$ with C a constant depending only on r, the respective intervals between γ and γ' for primes p and q are *contiguous*. That is, we show that $\mathrm{rem}_q(\gamma) \leq \mathrm{rem}_p(\gamma')$ where $\leq$ is the usual order on $\mathbb{Z}$. By previous arguments, for all n with $\mathrm{rem}_p(\gamma) \leq n < \mathrm{rem}_q(\gamma')$ either $v_p(u_n) \neq 0$ or $v_q(u_n) \neq 0$.

We use effective bounds on the density of primes in arithmetic progressions to construct a sequence $\langle p_i \rangle_{i=0}^{\infty}$ of primes with contiguous r-unbalanced intervals. In particular, in Proposition 5.12 we prove that given if a prime $p_i \in b\mathbb{N}+1$ is large enough there always exists another prime $p_{i+1} \in b\mathbb{N}+1$ where $p_{i+1} < p_i(1 + \frac{1}{b}) + C$.

We have thus constructed an r-expanding r-unbalanced family of intervals that covers $\{n \in \mathbb{N} : n > N\}$ for some effectively computable finite bound N. Hence in order to decide our fixed instance of MP, it suffices to verify whether $t \in \{u_1, \ldots, u_N\}$, which completes

our unconditional decidability proof.

Let us now illustrate the approach we just presented with an example.

Example 5.2. *Consider again the sequence $\langle w_n\rangle_{n=0}^{\infty}$ defined by $w_0 = 1$ and the shift quotient*

$$s(x) := \frac{(x+\frac{9}{2})(x+\frac{7}{2})(x+\frac{5}{2})}{(x+\frac{11}{2})(x+4)(x+1)}$$

introduced in Example 5.1.

We have already given an argument that $\frac{13}{6}$ does not lie in the sequence by computing the limit of $r(x)$. We will now prove the non-membership of $\frac{13}{6}$ in the sequence using our approach based on prime divisors of the elements w_n of the sequence $\langle w_n\rangle_{n=0}^{\infty}$. To this end, let

$$\alpha_1 := \frac{-9}{2} \qquad \alpha_2 := \frac{-7}{2} \qquad \alpha_3 := \frac{-5}{2}$$
$$\beta_1 := \frac{-11}{2} \qquad \beta_2 := -4 \qquad \beta_3 := -1$$

Considering that $v_{13}(\frac{13}{6}) = 1$, in our approach, we use larger primes to rule out the membership of $\frac{13}{6}$. For the prime 17, as depicted in Figure 5.2, we have that

$$\beta_1 \preceq_{17} \alpha_1 \preceq_{17} \alpha_2 \preceq_{17} \alpha_3 \preceq_{17} \beta_2 \preceq_{17} \beta_3.$$

The maximal 17-unbalanced intervals in our example are $\{3\}$ and $\{5,6,\ldots,15\}$. This implies that, for $n \in \{1,\ldots,16\}$, $S_{17}(n)$ is non-zero if and only if n belongs to $\{3\} \cup \{5,\ldots,15\}$.

As it turns out 17 is sufficiently large so that, for all primes $p \geq 17$, the respective order $\prec_p$ agrees with $\prec_s$. Consequently, the families of intervals $\overline{(\beta_1,\alpha_1)}$ and $\overline{(\alpha_2,\beta_3)}$ are s-unbalanced. Furthermore, the family $\overline{(\alpha_2,\beta_3)}$ is s-expanding, whereas $\overline{(\beta_1,\alpha_1)}$ is not. As shown in Figure 5.2, the intervals between α_2 and β_3 are contiguous for primes in $\{17,23,29\}$. This, in turn, ensures that for all $n \in \{5,\ldots,27\}$ either 17, 23, or 29 divides w_n.

By the main theorem in [162], for all primes $p \geq 8$, there exists another prime less than $p(1+\frac{1}{2})$. This, in combination with the arguments above, guarantees that for all $n \geq 5$, there exists a prime p other than 13 appearing in the factorisation of w_n. This reduces the membership test of $\frac{13}{6}$ to the finite set $\{w_1,\ldots,w_4\}$.

5.3.2 Constructing the preorder

Recall that the elements in $A \subseteq \mathbb{Q}\setminus\mathbb{Z}_{\geq 0}$ are the roots of the numerator, and the elements in $B \subseteq \mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$ are the roots of the denominator of the shift quotient $r(x)$ of the fixed sequence $\langle u_n\rangle_{n=0}^{\infty}$. In this section we give the proofs of the technical lemmas allowing us to determine the order of the parameters $A \uplus B$ with respect to the preorder $\preceq_r$, and determine which of the subintervals are r-expanding and r-unbalanced.

Let $b > 0$ be the least common denominator of the fractions in $A \uplus B$. Then every element $\gamma \in A \uplus B$ admits a unique representation in the form $\gamma = c - \frac{a}{b}$ under the conditions $c \in \mathbb{Z}$ and $a \in \{1, \dots, b\}$. We call this the *canonical representation.* Associated with this, define a nonnegative integer

$$N_\gamma := \begin{cases} \max\left(c, \lceil \frac{bc}{b-a} \rceil\right) & \text{if } c \geq 1, \\ \max\left(-c, \lceil \frac{-bc}{a} \rceil\right) & \text{if } c \leq 0. \end{cases}$$

Note that N_γ is well-defined, i.e., there is no division by zero. Indeed, if $c \geq 1$, by the convention that $\gamma \notin \mathbb{Z}_{\geq 0}$, the value $b - a$ is non-zero, whereas $a \neq 0$ ensures well definedness in the second case.

In the following proposition we give an explicit formula that allows us to compute $\mathrm{rem}_p(\gamma)$ for all primes p in the arithmetic progression $b\mathbb{N} + 1$ that are greater than N_γ.

Proposition 5.5. *Let $\gamma = c - \frac{a}{b}$ be a canonical representation. Then for all primes $p > N_\gamma$ such that $p \in b\mathbb{N} + 1$ we have $\mathrm{rem}_p(\gamma) = c + \frac{(p-1)a}{b}$.*

Proof. The assumption that $p \in b\mathbb{N} + 1$ implies that $\mathrm{rem}_p\left(-\frac{1}{b}\right) = \frac{p-1}{b}$. Thus, by the homomorphism property of rem_p, it only remains to verify that $c + \frac{(p-1)a}{b} \in \{0, \dots, p-1\}$. To this end, there are two cases, following the definition of N_γ.

The first case is that $c \geq 1$. Here we clearly have $c + \frac{(p-1)a}{b} \geq 0$. Furthermore, by the assumption $p > N_\gamma$, we have $p - 1 \geq \frac{bc}{b-a}$. Recall also that $a \neq b$ due to the assumption that $\gamma \notin \mathbb{Z}_{\geq 0}$. Thus, multiplying the previous inequality by $b - a > 0$, we have $(b-a)(p-1) \geq bc$. Dividing by b and rearranging terms, we conclude that $c + \frac{(p-1)a}{b} \leq p - 1$.

The second case is that $c \leq 0$. Here, since $a \leq b$, it is clear that $c + \frac{(p-1)a}{b} \leq p - 1$. Furthermore, by the assumption $p > N_\gamma$, we have $p - 1 \geq \frac{-bc}{a}$. Multiplying the latter inequality by $\frac{a}{b}$ and rearranging terms, we get $c + \frac{(p-1)a}{b} \geq 0$.

□

Next we use Proposition 5.5 to show that, given distinct γ and γ' in $A \uplus B$, for all large enough primes p in the arithmetic progression $b\mathbb{N} + 1$, their order respective to $\prec_p$ is fixed.

Proposition 5.6. *Let $\gamma = c - \frac{a}{b}$ and $\gamma' = c' - \frac{a'}{b}$ be canonical representations. For all primes $p > b(N_\gamma + N_{\gamma'}) + 1$ such that $p \in b\mathbb{N} + 1$ we have:*

$$\gamma \prec_p \gamma' \text{ if and only if } ((a < a') \text{ or } (a = a' \text{ and } c < c')).$$

Proof. For the first direction, assume that $\gamma \prec_p \gamma'$. Following Proposition 5.5, since $p > N_\gamma + N_{\gamma'}$ and $p \in b\mathbb{N} + 1$, we can rewrite the assumption as $c + \frac{(p-1)a}{b} < c' + \frac{(p-1)a'}{b}$. We can rearrange the inequality to obtain

$$cb - c'b + a' - a < p(a' - a).$$

Towards a contradiction, assume that $a > a'$. In this case, the above yields $\frac{c-c'}{a'-a}b + 1 > p$. Since $N_\gamma \geq |c|$ and $N_{\gamma'} \geq |c'|$, by the assumption that $p > b(N_\gamma + N_{\gamma'}) + 1$ we have that $p > (c - c')b + 1 > \frac{c-c'}{a'-a}b + 1$, a contradiction. Again, towards a contradiction, assume that $a = a'$ but $c \geq c'$. Since $b > 0$ we can multiply the inequality by b to get $cb \geq c'b$, a contradiction. The claim follows.

To show the other direction of the equivalence, we need to look at two cases depending on a and a'. First assume that $a < a'$. By $p > b(N_\gamma + N_{\gamma'}) + 1$ we can write

$$p > (c - c')b + 1 \geq \frac{c - c'}{a' - a}b + 1 = \frac{cb - c'b + a' - a}{a' - a}.$$

Since $a' - a > 0$, we can multiply the above inequality by $(a' - a)$ to obtain $p(a' - a) > cb - c'b + a' - a$. By rearranging the terms, we get $(p - 1)a + cb < (p - 1)a' + c'b$. As $p > N_\gamma + N_{\gamma'}$ and $p \in b\mathbb{N} + 1$ by Proposition 5.5, it follows that $\gamma \prec_p \gamma'$.

For the second case, assume $a = a'$ and $c < c'$. Since $b > 0$, we can write $cb < c'b$. It follows that $(p - 1)a + cb < (p - 1)a + c'b$. Again, since $p > N_\gamma + N_{\gamma'}$ and $p \in b\mathbb{N} + 1$ by Proposition 5.5, it follows that $\gamma \prec_p \gamma'$. □

Associated to the shift quotient $r(x)$ of the sequence $\langle u_n \rangle_{n=0}^{\infty}$, define the nonnegative integer

$$N_r := b \sum_{\gamma \in A \uplus B} N_\gamma + 1. \tag{5.13}$$

From Proposition 5.6 it follows that for all primes $p > N_r$ in the arithmetic progression $b\mathbb{N} + 1$

- $\operatorname{rem}_p(\gamma)$, $\operatorname{rem}_p(\gamma')$ are distinct for all distinct $\gamma, \gamma' \in A \uplus B$,
- the orders $\preceq_p$ on $A \uplus B$ are identical.

We henceforth denote by $\preceq_r$ the common order on $A \uplus B$ for all primes $p > N_r$ in the arithmetic progression $b\mathbb{N}+1$. Let $\gamma, \gamma' \in A \uplus B$. In the following proposition we show that for larger and larger primes $p \in b\mathbb{N} + 1$ whose orders agree with $\prec_r$, the distance between $\operatorname{rem}_p(\gamma)$ and $\operatorname{rem}_p(\gamma')$ gets larger and larger if and only if $\gamma - \gamma' \notin \mathbb{Z}$.

Proposition 5.7. *Let $p, q \in b\mathbb{N} + 1$ be primes with $q > p > N_r$. Let $\gamma, \gamma' \in A \uplus B$ be such that $\gamma \prec_r \gamma'$. Then $\gamma - \gamma' \notin \mathbb{Z}$ if and only if*

$$\operatorname{rem}_p(\gamma') - \operatorname{rem}_p(\gamma) < \operatorname{rem}_q(\gamma') - \operatorname{rem}_q(\gamma)$$

where $<$ is the total order on $\mathbb{Z}$.

Proof. For the first direction, assume that $\gamma - \gamma' \notin \mathbb{Z}$. Given the canonical representations $\gamma = c - \frac{a}{b}$ and $\gamma' = c' - \frac{a'}{b}$, this implies that $a \neq a'$. Now since $\gamma \prec_r \gamma'$, by Proposition 5.6 we have $a < a'$.

Since $p < q$ and $b > 0$, we can write $\frac{p-1}{b} < \frac{q-1}{b}$. We can multiply the inequality by $(a' - a)$ to obtain

$$\frac{p-1}{b}(a'-a) < \frac{q-1}{b}(a'-a).$$

Now by adding $(c' - c)$ on both sides of the above inequality we get

$$c' + \frac{p-1}{b}a' - \left(c + \frac{p-1}{b}a\right) < c' + \frac{q-1}{b}a' - \left(c + \frac{q-1}{b}a\right).$$

By the assumption that $p, q \in b\mathbb{N}+1$ with $p, q > N_r$, we can use Proposition 5.5 to conclude that

$$\mathrm{rem}_p(\gamma') - \mathrm{rem}_p(\gamma) < \mathrm{rem}_q(\gamma') - \mathrm{rem}_q(\gamma).$$

For the other direction, assume that $\mathrm{rem}_p(\gamma') - \mathrm{rem}_p(\gamma) < \mathrm{rem}_q(\gamma') - \mathrm{rem}_q(\gamma)$. Towards a contradiction, assume furthermore that $\gamma - \gamma' \in \mathbb{Z}$. Using the canonical representations $\gamma = c - \frac{a}{b}$ and $\gamma' = c' - \frac{a'}{b}$, by Proposition 5.5 we can rewrite the inequality as:

$$\left(c' + \frac{p-1}{b}a'\right) - \left(c + \frac{p-1}{b}a\right) < \left(c' + \frac{q-1}{b}a'\right) - \left(c + \frac{q-1}{b}a\right).$$

The inequality simplifies to

$$\frac{p-1}{b}(a'-a) < \frac{q-1}{b}(a'-a).$$

The assumption $\gamma - \gamma' \in \mathbb{Z}$ implies that $a = a'$, which with the above gives $0 < 0$, a contradiction. □

Let us now examine in which instances of MP we can always ensure the existence of such an r-expanding family.

5.3.3 Non-trivial sequences have unbalanced families

In this section we identify yet another trivially decidable case of instances of MP. In particular, we prove that given $r(x) \in \mathbb{Q}(x)$ converging to ± 1, either there exists an r-expanding r-unbalanced family of intervals for the parameters of $r(x)$, or the all instances of MP for the hypergeometric sequences defined by $r(x)$ are easily decidable. We begin by an observation that will help us to identify these instances.

Proposition 5.8. *Given $r(x) \in \mathbb{Q}(x)$ converging to ± 1 as $x \to \infty$, either*

1. *there exists an r-expanding r-unbalanced family of intervals, or*
2. *otherwise, the hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ with shift quotient $r(x)$ is a rational function of n.*

Proof. Recall we denote by A the multiset $\{\alpha_1, \ldots, \alpha_d\}$ consisting of all the (possibly repeated) roots of the numerator and by B the multiset $\{\beta_1, \ldots, \beta_d\}$ of the roots of the denominator of the shift quotient $r(x)$. Our proof relies on the following observation: if there exists a bijective function $f : A \to B$ such that for all $\alpha \in A$ we have $\alpha - f(\alpha) \in \mathbb{Z}$, then Item 2 holds. Otherwise, Item 1 holds.

Towards Item 2, assume that there exists a bijective function $f : A \to B$ such that for all $\alpha \in A$ we have $\alpha - f(\alpha) \in \mathbb{Z}$. Given an enumeration $\alpha_1, \ldots, \alpha_d$ on A, enumerate the elements of B so that $f(\alpha_i) = \beta_i$. Then given a pair α_i, β_i, write $\ell_i = |\alpha_i - \beta_i| \in \mathbb{N}$.

Recall that given an instance of MP with a target value $t \in \mathbb{Q}$, the problem asks to decide whether there exists $n \in \mathbb{N}$ such that

$$\prod_{k=1}^{n} r(k) = t. \tag{5.14}$$

Observe that we can expand the left hand side of the equation above in the following way.

$$\begin{aligned}\prod_{k=1}^{n} r(k) &= \prod_{k=1}^{n} \frac{(k-\alpha_1)\cdots(k-\alpha_d)}{(k-\beta_1)\cdots(k-\beta_d)} \\ &= \prod_{k=1}^{n} \frac{(k-\alpha_1)}{(k-\beta_1)} \cdots \prod_{k=1}^{n} \frac{(k-\alpha_d)}{(k-\beta_d)}\end{aligned}$$

Now if we look at the product $\prod_{k=1}^{n} \frac{(k-\alpha_i)}{(k-\beta_i)}$. If $\beta_i > \alpha_i$, observe that we can write

$$\frac{k-\alpha_i}{k-\beta_i} = \frac{k+(\beta_i-\alpha_i)-\beta_i}{k-\beta_i} = \frac{k+\ell_i-\beta_i}{k-\beta_i}.$$

We can thus write

$$\begin{aligned}&\prod_{k=1}^{n} \frac{(k-\alpha_i)}{(k-\beta_i)} \\ &= \prod_{k=1}^{n} \frac{(k+\ell_i-\beta_i)}{(k-\beta_i)} \\ &= \frac{(1+\ell_i-\beta_i)}{(1-\beta_i)} \cdots \frac{((\ell_i+1)+\ell_i-\beta_i)}{((\ell_i+1)-\beta_i)} \cdots \frac{(n+\ell_i-\beta_i)}{(n-\beta_i)} \\ &= \frac{\cancel{(1+\ell_i-\beta_i)}}{1-\beta_i)} \cdots \frac{((\ell_i+1)+\ell_i-\beta_i)}{\cancel{((\ell_i+1)-\beta_i)}} \cdots \frac{(n+\ell_i-\beta_i)}{(n-\beta_i)}\end{aligned}$$

Note how in the last line above, we were able to simplify at least two terms. Observe that we will be able to do so for all but ℓ_i terms in the numerator and all but ℓ_i terms in the denominator. That is, we transform

$$\prod_{k=1}^{n} \frac{(k-\alpha_i)}{(k-\beta_i)} = \frac{(n+1-\beta_i)\cdots(n+\ell_i-\beta_i)}{(1-\beta_i)\cdots(\ell_i-\beta_i)} = \frac{f_i(n)}{g_i(n)}$$

for $n > \ell_i$.

Similarly, observe that if $\alpha_i > \beta_i$, we can write

$$\frac{k-\alpha_i}{k-\beta_i} = \frac{k-\alpha_i}{k+(\alpha_i-\beta_i)-\alpha_i} = \frac{k-\alpha_i}{k+\ell_i-\alpha_i}$$

By repeating the above computation, we obtain

$$\prod_{k=1}^{n} \frac{(k-\alpha_i)}{(k-\beta_i)} = \frac{(1-\alpha_i)\cdots(\ell_i-\alpha_i)}{(n+1-\alpha_i)\cdots(n+\ell_i-\alpha_i)} = \frac{f_i(n)}{g_i(n)}$$

for $n > \ell_i$.

By applying the above transformation to all pairs α_i, β_i with their respective distance ℓ_i, we can rewrite $\prod_{k=1}^{n} r(k)$ as

$$\prod_{k=1}^{n} r(k) = \frac{f_1(n)}{g_1(n)} \cdots \frac{f_d(n)}{g_d(n)} = \frac{\hat{f}(n)}{\hat{g}(n)}$$

The above is well-defined for all $n > \max(\ell_1, \ldots, \ell_d)$, and implies that the product $\prod_{k=1}^{n} r(k)$ can be decomposed as a product of a constant number of rational functions in n.

To show Item 1, assume that there is no bijective function $f : A \to B$ such that for all $\alpha \in A$ we have $\alpha - f(\alpha) \in \mathbb{Z}$. Let $\gamma_1, \ldots, \gamma_{2d}$ be a fixed permutation of the elements of $A \uplus B$, such that $\gamma_j \preceq_r \gamma_k$ for all $1 \leq j < k \leq 2d$.

We claim that there exists an index j such that $\overline{(\gamma_j, \gamma_{j+1})}$ is an r-expanding r-unbalanced family of intervals. That is, j is such that

- $\gamma_j - \gamma_{j+1} \notin \mathbb{Z}$, and
- the number of α_i in the block $\gamma_1 \preceq_r \ldots \preceq_r \gamma_j$ is not equal to the number of β_i in the block $\gamma_1 \preceq_r \ldots \preceq_r \gamma_j$.

Indeed, if there is no such j, then we can take each block of the α_i and β_i with integer distances and construct a bijection mapping from the set of α_i's to the set of β_i's appearing in the block alone. Putting together the mappings given by the block bijections gives us a bijection $f : A \to B$ such that $\alpha_i - f(\alpha_i) \in \mathbb{Z}$ for all i, which would lead to a contradiction.

□

The proposition we have just proved has a straightforward corollary identifying the new degenerate case of MP.

Corollary 5.9. *Given $r(x) \in \mathbb{Q}(x)$ converging to ± 1 as $x \to \infty$, either*

1. *there exists an r-expanding r-unbalanced family of intervals, or*
2. *otherwise, the Membership Problem for the hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ with shift quotient $r(x)$ is trivially decidable.*

Proof. To prove the corollary it suffices to show that Item 2 of Proposition 5.8 implies Item 2 above. Indeed, assume that there exists no r-expanding r-unbalanced family of intervals. Then by Proposition 5.8 every hypergeometric sequence $\langle u_n \rangle_{n=0}^{\infty}$ with shift quotient $r(x)$ is a rational function of n. That is, there exist polynomials $f, q \in \mathbb{Q}[x]$ such that

$$u_n = \frac{f(n)}{g(n)}.$$

Given a target $t \in \mathbb{Q}$, $u_n = t$ for some $n \in \mathbb{N}$ if and only if there exists $n \in \mathbb{N}$ such that $f(n) - g(n)t = 0$. In other words, the problem reduces to verifying whether the polynomial $F(x) = f(x) - g(x)t \in \mathbb{Q}[x]$ has a positive integer zero. This problem is clearly decidable, as the magnitude of all integer zeroes of a univariate polynomial is bounded by the height of the polynomial; it suffices to check the equality for a finite number of values n. □

We have thus established that all instances of MP that are not trivially decidable admit r-unbalanced families. Let us now see how we can construct the sequence of primes witnessing decidability.

5.3.4 Constructing the prime sequence

Let $\gamma, \gamma' \in A \uplus B$ be such that $\overline{(\gamma, \gamma')}$ is an r-expanding r-unbalanced family of intervals. For a prime $p \in b\mathbb{N} + 1$ with $p > N_r$, we obtain a condition on larger primes $q \in b\mathbb{N} + 1$ that ensures the intervals $\{n \in \mathbb{N} : \mathrm{rem}_p(\gamma) \leq n < \mathrm{rem}_p(\gamma')\}$ and $\{n \in \mathbb{N} : \mathrm{rem}_q(\gamma) \leq n < \mathrm{rem}_q(\gamma')\}$ are contiguous.

Proposition 5.10. *Let $p, q \in b\mathbb{N} + 1$ be primes with $q > p > N_r$. Let $\gamma, \gamma' \in A \uplus B$ such that $\gamma - \gamma' \notin \mathbb{Z}$ and $\gamma \prec_r \gamma'$. We have $\mathrm{rem}_q(\gamma) < \mathrm{rem}_p(\gamma')$ if*

$$q < p + \frac{p-1}{b} + C$$

for some effective constant C depending on γ and γ'.

Proof. Given the canonical representations $\gamma = c - \frac{a}{b}$ and $\gamma' = c' - \frac{a'}{b}$, write $C := \frac{c'-c}{a} b$. Then the initial assumption can be rewritten as

$$q < p + \frac{p-1}{b} + \frac{c'-c}{a} b.$$

We can further rewrite the above inequality as

$$q - 1 < (p-1)\big(1 + \frac{1}{b}\big) + \frac{c'-c}{a} b.$$

Note that since $\gamma - \gamma' \notin \mathbb{Z}$, we have $a \neq a'$. Now by Proposition 5.6, from $\gamma \prec_r \gamma'$ it follows that $a < a'$. By further recalling that $a < a' \leq b$, we have $\frac{a'}{a} = \big(1 + \frac{a'-a}{a}\big) \geq \big(1 + \frac{1}{b}\big)$. Then from the above it follows that

$$q - 1 < (p-1)\frac{a'}{a} + \frac{c'-c}{a} b.$$

Since $\frac{a}{b} > 0$, we can multiply the inequality by $\frac{a}{b}$ to obtain

$$\frac{(q-1)a}{b} + c < \frac{(p-1)a'}{b} + c'.$$

By the assumption that $p, q \in b\mathbb{N} + 1$ with $p, q > N_r$, we can now use Proposition 5.5 to conclude that $\mathrm{rem}_q(\gamma) < \mathrm{rem}_p(\gamma')$. □

We will now show that we can indeed construct a sequence of primes in the arithmetic progression $b\mathbb{N} + 1$ that are close enough to satisfy the condition we have just shown in Proposition 5.10. To this end, we rely on an effective version of Dirichlet's Theorem on the density of primes in arithmetic progressions. As discussed in Section 2.3.6, there are several effective variants of the theorem. We use the following estimates which can be found [163, Theorem 1.3], as they give a matching upper and lower bound on $\pi_{n,a}(x)$.

Theorem 5.11. *Given $n \geq 3$ and $a \in \mathbb{N}$ coprime to n, there exist explicit positive constants c and x_0 depending on n such that*

$$\left|\pi_{n,a}(x) - \frac{Li(x)}{\varphi(n)}\right| < c\frac{x}{(\log x)^2} \text{ for all } x > x_0.$$

Note that in the above theorem $Li(x)$ denotes the *offset logarithmic integral function*, which is defined as

$$Li(x) = \int_2^x \frac{dt}{\log t}. \tag{5.15}$$

Asymptotically, the function behaves as the prime number counting function $\pi(x)$, that is, as $O\left(\frac{x}{\log x}\right)$.

Proposition 5.12. *Let $b \in \mathbb{N}$ and $C \in \mathbb{Z}$. There exist an effectively computable bound $M \in \mathbb{N}$ such that for all primes $p \in b\mathbb{N} + 1$ greater than M, there exists a prime $q \in b\mathbb{N} + 1$ with $p < q < p + \frac{p-1}{b} + C$.*

Proof. Let $x \in b\mathbb{N}+1$, and denote by $y = x(1+\frac{1}{b})$. We would like to show that there exists a bound $M \in \mathbb{N}$ such that $\pi_{b,1}(y) - \pi_{b,1}(x) > 0$ for all $x > M$. Using Theorem 5.11 to estimate $\pi_{b,1}(y)$ and $\pi_{b,1}(x)$, it suffices to show that

$$\frac{Li(y)}{\varphi(b)} - c\frac{y}{(\log y)^2} > \frac{Li(x)}{\varphi(b)} + c'\frac{x}{(\log x)^2}.$$

The above then simplifies to

$$\frac{Li(y) - Li(x)}{\varphi(b)} > 2c\frac{y}{(\log y)^2}. \tag{5.16}$$

Now write $y = x(1+\epsilon)$ with $\epsilon = \frac{1}{b}$, and observe that following (5.15)

$$Li(y) - Li(x) = \int_x^y \frac{dt}{\log t} = \frac{y}{\log y} - \frac{x}{\log x} \sim \frac{\epsilon x}{\log x}$$

where $\sim$ denotes asymptotic equivalence. As for the right hand side of (5.16), note that

$$\frac{y}{(\log y)^2} \sim \frac{x}{(\log x)^2}.$$

It remains to note that $\frac{x}{\log x} \gg \frac{x}{(\log x)^2}$. □

The above proposition ensures that we can construct an infinite sequence of primes $\langle p_i \rangle_{i=0}^{\infty}$ in $b\mathbb{N}+1$ such that for all p_i its successor p_{i+1} is between p_i and $p_i + \frac{p_i - 1}{b} + C$. Proposition 5.10 then implies that if we choose $p_0 > \max(M, N_r)$, for every $\gamma, \gamma' \in A \uplus B$ such that $\overline{(\gamma, \gamma')}$ is an r-expanding r-unbalanced family of intervals, for all i, the intervals $\{n \in \mathbb{N} : \operatorname{rem}_{p_i}(\gamma) \leq n < \operatorname{rem}_{p_i}(\gamma')\}$ and $\{n \in \mathbb{N} : \operatorname{rem}_{p_{i+1}}(\gamma) \leq n < \operatorname{rem}_{p_{i+1}}(\gamma')\}$ are contiguous.

The sequence $\langle p_i \rangle_{i=0}^{\infty}$ is the last part of our construction, allowing us to prove our main result.

5.3.5 Putting everything together

In this section we combine all the lemmas we have just proved to prove our unconditional decidability result for for the Membership Problem.

Theorem 5.13. *The Membership Problem for hypergeometric sequences with rational parameters is decidable.*

Proof. As discussed in Section 5.2, the only case of MP that is not trivially decidable is when the shift quotient $r(x) \in \mathbb{Q}(x)$ of the sequence $\langle u_n \rangle_{n=0}^{\infty}$ converges to ± 1 as $x \to \infty$. Given such an instance of MP, we write $r(x)$ as

$$\frac{(x - \alpha_1) \cdots (x - \alpha_d)}{(x - \beta_1) \cdots (x - \beta_d)}.$$

We denote by A the multiset $\{\alpha_1, \ldots, \alpha_d\}$ consisting of all the (possibly repeated) roots of the numerator and by B the multiset $\{\beta_1, \ldots, \beta_d\}$ of the roots of the denominator. As discussed in Section 5.1, all elements in $A \uplus B$ are in $\mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$.

We now show that there exists a bound $N \in \mathbb{N}$ such that for all $n > N$, there exists a prime p appearing in the factorisation of u_n but not in the factorisation of t. This implies that it suffices to check whether $u_n = t$ for all $n \in \{1, \ldots, N\}$ to decide MP. In particular, we show that for all $n > N$, we can find a prime p with $v_p(t) = 0$ such that $S_p(n)$, as defined in Equation (5.9), is non-zero.

Write $t = \frac{v}{w}$. Now define

$$N' = \max(|v|, |w|, N_r)$$

where N_r is defined as in Equation (5.13). Note that none of the primes $p > N'$ divide the target t.

Following Corollary 5.9, we can assume without loss of generality that there exists an r-expanding r-unbalanced family of intervals $\overline{(\gamma, \gamma')}$ for some $\gamma, \gamma' \in A \uplus B$. Let M be the bound computed in Proposition 5.12. Let $p_0 \in b\mathbb{N} + 1$ be a prime with $p_0 > \max(M, N')$. Observe that for all n in

$$\{k \in \mathbb{N} : \mathrm{rem}_{p_0}(\gamma) \leq k < \mathrm{rem}_{p_0}(\gamma')\},$$

the sum $S_{p_0}(n)$ defined in Equation (5.9) is indeed non-zero.

Following Proposition 5.12, we can construct an infinite sequence of primes $\langle p_i \rangle_{i=0}^{\infty}$ with initial element p_0 such that for every prime p_i in the sequence, its successor p_{i+1} is between p_i and $p_i + \frac{p_i - 1}{b}$ in the arithmetic progression $b\mathbb{N} + 1$. By Proposition 5.10, for all i, the intervals $\{k \in \mathbb{N} : \mathrm{rem}_{p_i}(\gamma) \leq k < \mathrm{rem}_{p_i}(\gamma')\}$ and $\{k \in \mathbb{N} : \mathrm{rem}_{p_{i+1}}(\gamma) \leq k < \mathrm{rem}_{p_{i+1}}(\gamma')\}$ are contiguous. Therefore we can cover all $n > \mathrm{rem}_{p_0}(\gamma)$, which concludes our proof.

□

5.4 Discussion and perspectives

In this chapter we studied the Membership Problem for hypergeometric sequences with rational parameters. We recalled that the asymptotic behaviour of a product of rational functions can be related to the Gamma function, implying that the decidability of the problem can be established using the asymptotic approach under the assumption of the Rohrlich-Lang conjecture.

Our main contribution was an unconditional decidability result. We approached deciding the Membership Problem from a different angle–specifically, by considering the prime divisors of u_n. Our strategy is to show that (except in some degenerate cases) for all sufficiently large n, u_n has a prime divisor p that is not also a prime divisor of the target t. This allows us to compute a bound N such that $u_n \neq t$ for all $n > N$. We studied p-adic valuations, and, given an element u_n of our sequence, determined conditions on primes p such that p appears in the factorisation of u_n (in terms of valuations, $v_p(u_n) \neq 0$), whereas it does not divide the target t (i.e., $v_p(t) = 0$). One of the conditions in question is that p belongs to a well-chosen arithmetic progression. Actually, given a prime p from the progression, we computed a set of values n such that $v_p(u_n) \neq 0$. Using classical results on the distribution of primes in arithmetic progressions, we were then able to construct an infinite sequence of primes $\langle p_i \rangle_{i=0}^{\infty}$, and show the existence of a bound N such that the set of indices n for which $v_{p_i}(u_n) \neq 0$ as i goes to infinity covers all $n > N$. That is, the p_i witness that $u_n \neq t$ for all $n > N$.

In our work, we analysed divisibility of the sequence $\langle u_n \rangle_{n=0}^{\infty}$ for well-chosen primes p. Let us note that studying the p-valuation of sequences is not a novel idea. The works [164, 165], for example, consider sequences of the form $\langle v_p(q(n)) \rangle_{n=0}^{\infty}$, where q is a polynomial with rational coefficients. The paper [166] is closer to the sequences we consider, as it studies the asymptotic behaviour of sequences of the form $v_p(u_n)$, where v_p is the p-adic

valuation and $\langle u_n \rangle_{n=0}^{\infty}$ is a sequence of integers satisfying a recurrence $u_n = q(n)u_{n-1}$, i.e., an order-1 polynomial recurrence whose leading coefficient is constant.

p-adic techniques have also been used to study integrality of hypergeometric sequences. The work [167], in particular, formal power series whose coefficients are given by the terms of a hypergeometric sequence with rational parameters. Given two tuples of parameters $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_r)$ and $\boldsymbol{\beta} := (\beta_1, \ldots, \beta_s)$ in $\mathbb{Q} \setminus \mathbb{Z}_{\leq 0}$, the authors study *generalised hypergeometric series*, which they define as

$$F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(z) := \sum_{n=0}^{\infty} \frac{(\alpha_1)_n \cdots (\alpha_s)_n}{(\beta_1)_n \cdots (\beta_s)_n} z^n.$$

Here, $(x)_n$ denotes the Pochhammer symbol $(x)_n = x(x+1)\cdots(x+n-1)$ if $n \geq 1$ and $(x)_0 = 1$ otherwise. Notice that $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(z)$ is essentially just a formal power series in the variable z whose coefficients are given by the hypergeometric sequence defined by the shift quotient with parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Through analysing the p-adic valuation of $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}$, they obtain results on when $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(z) \in \mathbb{Z}[\![z]\!]$, and what is the minimal constant $C \in \mathbb{Q}_{\geq 0}$ such that $F_{\boldsymbol{\alpha},\boldsymbol{\beta}}(C \cdot z) \in \mathbb{Z}[\![z]\!]$. In contrast to our work, the authors here analyse p-adic valuations of the series for arbitrary primes p, whereas in order to decide the Membership Problem, we carefully select our primes ensuring that the valuations we consider have simple closed forms (i.e. take value 0 or 1 for linear factors of our sequence).

The next natural step in the study of the Membership Problem would be to extend our approach to more general instances of the problem, that is, to sequences specified with polynomial coefficients with algebraic roots of degree greater than one. A continuation of the work in that direction, which is beyond the scope of this thesis, appears in [168]. The paper establishes decidability of the Membership Problems for two cases: for sequences defined by shift quotients where the numerator and the denominator (1) have distinct splitting fields, and (2) both split over the ring of integers of a quadratic field.

The proofs of both results again follow by analysing the prime divisors of the hypergeometric sequence. In the case (1), it is shown that one can find a single prime $p \in \mathbb{Z}$ that does not divide the target t but divides all members of the sequence u_n for $n > N$. Here the reason why a single prime suffices as witness of non-equality comes from the observation that the valuations $v_p(f(k))$ and $v_p(g(k))$ for $k \in \mathbb{N}$ depend on the splitting pattern of the prime p in their respective splitting fields. The Chebotarev density theorem asserts that given distinct number fields K and L, there are infinitely many primes that split completely in one, but not in the other, ensuring the existence of the bound N.

In the case (2), the construction is similar in spirit to the approach we take for hypergeometric sequences with rational parameters. That is, it is shown that for all $n > N$, there exists a prime p (that may depend on n) dividing u_n, but not t. Here the proof follows from a generalisation of a result of [169] concerning primitive prime divisors of the values of a quadratic polynomial. We recall that given a sequence $\langle u_n \rangle_{n=0}^{\infty}$, a primitive divisor of a term u_n is a divisor of u_n that is coprime to every nonzero term u_m with $m < n$. A natural question that arises is whether this approach can be generalised to shift quotients with parameters from higher-degree number fields. This does not seem easily feasible, as it would require new results on large prime divisors on the values of such polynomials, which is an active area of research in number theory; see, e.g., [170].

A parallel result in the same direction is given in the recent paper by Kenison [171]. Decidability of both the Membership and Threshold problems for sequences defined by shift quotients where the numerator and the denominator both split over the ring of integers of a quadratic field K are established. The approach in the paper relies on transcendence theory for the Gamma function and the decidability results are unconditional when K is imaginary decidable unconditionally, whereas for the case when K is real, decidability is conditioned to the assumption of Schanuel's conjecture.

Open questions. As discussed above, the first result of [168] is that the Membership Problem is decidable for sequences defined by shift quotients where the numerator and the denominator have distinct splitting fields, and the decidability is witnessed by a single prime. Our decidability proof for the Membership Problem for hypergeometric sequences with rational parameters, on the other hand, uses an infinite sequence of primes. The variant we solve can hence be seen as the easiest sub-case of the Membership Problem not known to belong to the class that can be decided using a single prime. We thus ask: could a single prime suffice to establish decidability for our case as well? Or could one show that one prime is not enough?

We pointed out above that the techniques we introduce do not seem to generalise easily to sequences with parameters of degree higher than 2. However, could similar techniques be used for zero testing problems for higher-order P-finite sequences with low-degree algebraic parameters?

Finally, in the world of C-finite sequences, the problem of determining the complexity of zero testing has also been considered. While the Skolem problem is not known to be decidable in general, it has been shown to be **NP**-hard [172]. Most known decidability results for the problem for low order recurrences, such as [12, 13, 112, 113, 114, 115], do not include complexity upper bounds, but there are some exceptions. The authors of [29], for example, identify a large subclass of sequences such that the Skolem problem is decidable in $\mathbf{NP}^{\mathbf{RP}}$; this complexity bound is tight up to randomisation. Similar complexity results are obtained for a subclass of the Orbit problem in [28], which is closely related to the Skolem problem as well. What can be said about the complexity of the Membership Problem for hypergeometric sequences? Are there subclasses of the Membership Problem for hypergeometric sequences, such as, e.g. sequences given by shift quotients with linear numerator and denominator, that have better complexity than the general case?

Conclusion and outlook

In this thesis we studied a family of *zero problems* for polynomial models encompassing both identity testing and root finding. We developed algorithms relying on algebraic and number-theoretic results in order to decide subproblems of both the existential theory of real closed fields as well as the existential theory of algebraically closed fields. The overarching idea behind our algorithms is to perform the evaluation modulo a well-chosen (prime) ideal. While our work focuses on specific subproblems of elimination theory, we believe that the techniques we developed can be generalised to other related problems, and that there are many connections between these problems yet to be explored.

We began the thesis by considering a subproblem of the existential theory of real closed fields, namely the Radical Identity Testing problem, which asks whether a polynomial represented by an algebraic circuit vanishes on a given real radical input. We improved on the existing **PSPACE** bound and completed some of the gaps in the understanding of identity testing in radical field extensions, drawing parallels to the better-studied cyclotomic setting. As noted in the Introduction, many of the existing techniques are limited to algebraic inputs having degree polynomial in the problem description, such as polynomial factorisation, which can be used for identity testing of sparse expressions in polynomial-degree number fields. Our approach, on the other hand, allows us to handle identity testing in number fields of exponential degree and can be seen as a first step towards many generalisations. A first one would be to adapt the techniques to verify whether a given sparse polynomial admits exponential-degree irreducible factors. Or, at least whether it admits linear factors in cyclotomic or radical field extensions of exponential degree. An orthogonal direction would be to adapt these techniques to study the complexity of factoring algebraic circuits in number fields, starting with the case where the degree of the number field is polynomial in the problem description. Besides identity testing for nested radical inputs as mentioned in Section 1.1, one could also consider, e.g., identity testing for real algebraic numbers given by the minimal polynomial and the interval where the root of interest appears, or the minimal polynomial and a rational approximation of the root. As in the Radical Identity Testing problem, testing identities in these settings can be encoded in the existential theory of reals, however, the exact complexity of the problems remains open.

We also exhibited a reduction from the RIT problem to the Hilbert Nullstellensatz problem over $\mathbb{C}$, which, in turn, belongs to the existential theory of algebraically closed fields. We further studied a variant of the HN problem in Chapter 4, focusing on parametric solutions, again reducing $\mathrm{HN}_{\overline{\mathbb{Q}(\boldsymbol{x})}}$ to $\mathrm{HN}_{\mathbb{C}}$, using similar number-theoretic arguments as in Chapter 3, and suggested some of the possible generalisations. While constructing a sys-

tem of polynomial equations encoding the constraints given by an algebraic circuit is relatively well-understood, we believe that it would be interesting to explore the relation in the opposite direction, that is, try to leverage identity testing techniques (over circuits) to decide satisfiability of systems of equations over subfields of algebraically closed fields. An example of such a relation yet to be explored is studying HN over real radical extensions. As the input polynomials to HN are assumed to be given in the sparse representation, they admit polynomial-size circuits. For example, if one could guess small circuits for the input solutions, then deciding HN over $\mathbb{Q}(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_n]{a_n})$ would non-deterministically reduce to RIT, placing the radical variant of HN in the polynomial hierarchy. (As discussed in Section 3.6, the complexity bound we showed for RIT is also the best we can do for general sparse radical expressions). Another tie between the two problems to be explored is to look at parametric variants of identity testing problems. Following the intuition of Kayal and Saha who studied the Sum of Square Roots problem for polynomial integers [88], we believe that studying parametric identities could give insights on the complexity of the problem over other number fields, or, maybe even unify some of the existing results.

In the final part of this thesis we revisited the idea of studying algebraic objects modulo prime ideals, and applied it to the problem of deciding whether a polynomially recursive sequence has a zero term. We focused, in particular, on the problem for the case of sequences arising as sums of two hypergeometric sequences, which in turn, reduces to deciding whether a given rational value appears in a hypergeometric sequence. We showed decidability of the problem for the case where the defining polynomials of the hypergeometric sequence split over $\mathbb{Q}$, which, as mentioned in Section 5.4 was later generalised to sequences defined by polynomials splitting over quadratic fields. While the technique we developed would require new advances in number theory in order to be generalised to number fields of degree more than two directly, our work has shown that the general approach is a good framework for studying reachability problems as well. Despite the most natural generalisation seeming to be out of reach for now, many interesting related problems, such as its variant for sequences arising as sums of more than two hypergeometric sequences, or, say, the complexity of the variants we now know are decidable, remain to be explored.

References

[1] Arnold Schönhage. "On the Power of Random Access Machines". In: *Automata, Languages and Programming, 6th Colloquium, Graz, Austria, July 16-20, 1979, Proceedings*. Ed. by Hermann A. Maurer. Vol. 71. Lecture Notes in Computer Science. Springer, 1979, pp. 520–529. DOI: 10.1007/3-540-09510-1_42 (on pages vi, 3, 44, 64, 69).

[2] John Canny. "Some algebraic and geometric computations in PSPACE". In: *Proceedings of the twentieth annual ACM symposium on Theory of computing*. 1988, pp. 460–467 (on pages vi, 11, 13, 19).

[3] Pascal Koiran. "Hilbert's Nullstellensatz Is in the Polynomial Hierarchy". In: *Journal of Complexity* 12.4 (1996), pp. 273–286. ISSN: 0885-064X. DOI: 10.1006/jcom.1996.0019 (on pages vi, vii, 6, 12, 17, 56, 78). Corrected in *Eratum to Hilbert's Nullstellensatz Is in the Polynomial Hierarchy*. 1997. URL: http://perso.ens-lyon.fr/pascal.koiran/Publis/elimination.erratum.ps.

[4] Ernst W. Mayr and Albert R. Meyer. "The complexity of the word problems for commutative semigroups and polynomial ideals". In: *Advances in mathematics* 46.3 (1982), pp. 305–329 (on pages vii, 16).

[5] János Kollár. "Sharp effective Nullstellensatz". In: *Journal of the American Mathematical Society* 1.4 (1988), pp. 963–975 (on pages vii, 17).

[6] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. "Sharp estimates for the arithmetic Nullstellensatz". In: (2001) (on pages vii, 17).

[7] Zbigniew Jelonek. "On the effective Nullstellensatz". In: *Inventiones mathematicae* 162.1 (2005), pp. 1–17 (on pages vii, 17).

[8] Pascal Koiran. *Hilbert's Nullstellensatz Is in the Polynomial Hierarchy*. Tech. rep. 96-27. DIMACS, July 1996 (on pages vii, 6, 12, 17, 56, 74, 75, 78, 83–85, 91, 92).

[9] Cyril Banderier and Michael Drmota. "Formulae and Asymptotics for Coefficients of Algebraic Functions". In: *Comb. Probab. Comput.* 24.1 (2015), pp. 1–53. DOI: 10.1017/S0963548314000728 (on pages vii, 20).

[10] Werner Kuich and Arto Salomaa. *Semirings, Automata, Languages*. Monographs in Theoretical Computer Science. An EATCS Series. Springer Berlin Heidelberg, 1986. ISBN: 978-3-642-69961-0. DOI: 10.1007/978-3-642-69959-7 (on pages vii, 20).

[11] Pascal Koiran. “Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties”. In: *38th Annual Symposium on Foundations of Computer Science, FOCS’97, Miami Beach, Florida, USA, October 19-22, 1997*. IEEE Computer Society, 1997, pp. 36–45. DOI: 10.1109/SFCS.1997.646091 (on pages viii, 20, 85, 88–93).

[12] Maurice Mignotte, TN Shorey, and Robert Tijdeman. “The distance between terms of an algebraic recurrence sequence”. In: *Journal für die reine und angewandte Mathematik* 349 (1984), pp. 63–76 (on pages viii, 22, 118).

[13] Nikolai K. Vereshchagin. “The problem of appearance of a zero in a linear recurrence sequence”. In: *Mat. Zametki* 38.2 (1985), pp. 609–615 (on pages viii, 22, 118).

[14] Eric Allender, Peter Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. “On the Complexity of Numerical Analysis”. In: *21st Annual IEEE Conference on Computational Complexity (CCC 2006), 16-20 July 2006, Prague, Czech Republic*. IEEE Computer Society, 2006, pp. 331–339. DOI: 10.1109/CCC.2006.30 (on pages 4, 13).

[15] Oscar H. Ibarra and Shlomo Moran. “Probabilistic Algorithms for Deciding Equivalence of Straight-Line Programs”. In: *J. ACM* 30.1 (1983), pp. 217–228. DOI: 10.1145/322358.322373 (on page 4).

[16] Richard A. Demillo and Richard J. Lipton. “A probabilistic remark on algebraic program testing”. In: *Information Processing Letters* 7.4 (1978), pp. 193–195. ISSN: 0020-0190. DOI: 10.1016/0020-0190(78)90067-4 (on pages 4, 75).

[17] Jacob T. Schwartz. “Fast Probabilistic Algorithms for Verification of Polynomial Identities”. In: *J. ACM* 27.4 (Oct. 1980), pp. 701–717. ISSN: 0004-5411. DOI: 10.1145/322217.322225 (on pages 4, 75).

[18] Richard Zippel. “Probabilistic Algorithms for Sparse Polynomials”. In: *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*. EUROSAM ’79. Berlin, Heidelberg: Springer-Verlag, 1979, pp. 216–226. ISBN: 3540095195 (on pages 4, 75).

[19] Richard A. Demillo and Richard J. Lipton. “A probabilistic remark on algebraic program testing”. In: *Information Processing Letters* 7.4 (1978), pp. 193–195 (on page 4).

[20] László Lovász. “On determinants, matchings, and random algorithms”. In: *FCT*. Vol. 79. 1979, pp. 565–574 (on page 4).

[21] Erich Kaltofen. “Factorization of Polynomials Given by Straight-Line Programs.” In: *Adv. Comput. Res.* 5 (1989), pp. 375–412 (on page 4).

[22] Daniel König and Markus Lohrey. “Parallel identity testing for skew circuits with big powers and applications”. In: *Int. J. Algebra Comput.* 28.6 (2018), pp. 979–1004 (on page 4).

[23] Piotr Berman, Marek Karpinski, Lawrence L. Larmore, Wojciech Plandowski, and Wojciech Rytter. "On the complexity of pattern matching for highly compressed two-dimensional texts". In: *Journal of Computer and System Sciences* 65.2 (2002), pp. 332–350 (on page 4).

[24] Manindra Agrawal and Somenath Biswas. "Primality and identity testing via chinese remaindering". In: *Journal of the ACM (JACM)* 50.4 (2003), pp. 429–443 (on page 4).

[25] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. "PRIMES is in P". In: *Annals of mathematics* (2004), pp. 781–793 (on page 4).

[26] Stefan Kiefer, Andrzej S. Murawski, Joël Ouaknine, Björn Wachter, and James Worrell. "On the Complexity of Equivalence and Minimisation for Q-weighted Automata". In: *Logical Methods in Computer Science* 9 (2013) (on page 4).

[27] Stefan Kiefer, Ines Marušić, and James Worrell. "Minimisation of Multiplicity Tree Automata". In: *Foundations of Software Science and Computation Structures LNCS 9034* (2015), p. 297 (on page 4).

[28] Ventsislav Chonev, Joël Ouaknine, and James Worrell. "On the Complexity of the Orbit Problem". In: *J. ACM* 63.3 (2016), 23:1–23:18. DOI: 10.1145/2857050 (on pages 4, 118).

[29] S. Akshay, Nikhil Balaji, Aniket Murhekar, Rohith Varma, and Nikhil Vyas. "Near-Optimal Complexity Bounds for Fragments of the Skolem Problem". In: *37th International Symposium on Theoretical Aspects of Computer Science, STACS 2020, March 10-13, 2020, Montpellier, France*. Ed. by Christophe Paul and Markus Bläser. Vol. 154. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 37:1–37:18. DOI: 10.4230/LIPIcs.STACS.2020.37 (on pages 4, 118).

[30] Max Dehn. "Transformation der Kurven auf zweiseitigen Flächen". In: *Mathematische Annalen* 72.3 (1912), pp. 413–421 (on page 4).

[31] Markus Lohrey. *The compressed word problem for groups*. Springer, 2014 (on page 4).

[32] Nikhil Balaji, Sylvain Perifel, Mahsa Shirmohammadi, and James Worrell. "Cyclotomic Identity Testing and Applications". In: *ISSAC'21: International Symposium on Symbolic and Algebraic Computation, Virtual Event, Russia, July 18-23, 2021*. Ed. by Frédéric Chyzak and George Labahn. ACM, 2021, pp. 35–42. DOI: 10.1145/3452143.3465530 (on pages 4–9, 44, 45, 64, 67, 69, 70).

[33] Daniel Richardson. "The elementary constant problem". In: *Papers from the international symposium on Symbolic and algebraic computation*. 1992, pp. 108–116 (on page 5).

[34] Daniel Richardson. "How to recognize zero". In: *Journal of Symbolic Computation* 24.6 (1997), pp. 627–645 (on page 5).

[35] David A. Plaisted. “New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems”. In: *Theor. Comput. Sci.* 31 (1984), pp. 125–138. DOI: 10.1016/0304-3975(84)90130-0 (on pages 5, 6, 11).

[36] Qi Cheng. “Derandomization of Sparse Cyclotomic Integer Zero Testing”. In: *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20-23, 2007, Providence, RI, USA, Proceedings*. IEEE Computer Society, 2007, pp. 74–80. DOI: 10.1109/FOCS.2007.23 (on page 5).

[37] Qi Cheng, Sergey P. Tarasov, and Mikhail N. Vyalyi. “Efficient Algorithms for Sparse Cyclotomic Integer Zero Testing”. In: *Theory Comput. Syst.* 46.1 (2010), pp. 120–142. DOI: 10.1007/S00224-008-9158-2 (on pages 5, 6, 8).

[38] Michael Filaseta and Andrzej Schinzel. “On testing the divisibility of lacunary polynomials by cyclotomic polynomials”. In: *Math. Comput.* 73.246 (2004), pp. 957–965. DOI: 10.1090/S0025-5718-03-01589-8 (on page 5).

[39] J. Maurice Rojas. “Efficiently Detecting Torsion Points and Subtori”. In: (2007). arXiv: math/0501388 (on page 6).

[40] J. Maurice Rojas. *Dedekind Zeta Functions and the Complexity of Hilbert’s Nullstellensatz*. 2003. arXiv: math/0301111 [math.NT] (on page 6).

[41] Zhi-Zhong Chen and Ming-Yang Kao. “Reducing Randomness via Irrational Numbers”. In: *SIAM J. Comput.* 29.4 (2000), pp. 1247–1256. DOI: 10.1137/S0097539798341600 (on pages 7, 9, 12).

[42] Johannes Blömer. “A Probabilistic Zero-Test for Expressions Involving Root of Rational Numbers”. In: *Algorithms - ESA’98, 6th Annual European Symposium, Venice, Italy, August 24-26, 1998, Proceedings*. Ed. by Gianfranco Bilardi, Giuseppe F. Italiano, Andrea Pietracaprina, and Geppino Pucci. Vol. 1461. Lecture Notes in Computer Science. Springer, 1998, pp. 151–162. DOI: 10.1007/3-540-68530-8_13 (on pages 7, 12, 13, 45, 48, 50, 51, 54, 70).

[43] Johannes Blömer. “Computing Sums of Radicals in Polynomial Time”. In: *32nd Annual Symposium on Foundations of Computer Science, San Juan, Puerto Rico, 1-4 October 1991*. IEEE Computer Society, 1991, pp. 670–677. DOI: 10.1109/SFCS.1991.185434 (on pages 8, 10).

[44] Paul Hunter, Patricia Bouyer, Nicolas Markey, Joël Ouaknine, and James Worrell. “Computing Rational Radical Sums in Uniform TC0”. In: *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2010, December 15-18, 2010, Chennai, India*. Ed. by Kamal Lodaya and Meena Mahajan. Vol. 8. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2010, pp. 308–316. DOI: 10.4230/LIPICS.FSTTCS.2010.308 (on pages 8, 10).

[45] Susan Landau and Gary Lee Miller. “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, 1983, pp. 140–151 (on page 9).

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

[47] John Watrous. "Quantum algorithms for solvable groups". In: *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*. Ed. by Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis. ACM, 2001, pp. 60–67. DOI: 10.1145/380752.380759 (on page 9).

[48] V. Arvind and Piyush P. Kurur. "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*. Vol. 2906. Lecture Notes in Computer Science. Springer, 2003, pp. 716–725 (on pages 9, 71).

[49] Michael R. Garey, Ronald L. Graham, and David S. Johnson. "Some NP-complete geometric problems". In: *Proceedings of the eighth annual ACM symposium on Theory of computing*. ACM. 1976, pp. 10–22 (on page 13).

[50] Neeraj Kayal and Chandan Saha. "On the sum of square roots of polynomials and related problems". In: *ACM Transactions on Computation Theory (TOCT)* 4.4 (2012), pp. 1–15 (on pages 13, 20).

[51] Gorav Jindal and Louis Gaillard. "On the Order of Power Series and the Sum of Square Roots Problem". In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation, ISSAC 2023, Tromsø, Norway, July 24-27, 2023*. Ed. by Alicia Dickenstein, Elias P. Tsigaridas, and Gabriela Jeronimo. ACM, 2023, pp. 354–362. DOI: 10.1145/3597066.3597079 (on page 13).

[52] Javier Esparza, Stefan Kiefer, and Michael Luttenberger. "Solving monotone polynomial equations". In: *Fifth Ifip International Conference On Theoretical Computer Science–Tcs 2008*. Springer. 2008, pp. 285–298 (on page 13).

[53] Christoph Haase and Stefan Kiefer. "The odds of staying on budget". In: *International Colloquium on Automata, Languages, and Programming*. Springer. 2015, pp. 234–246 (on page 13).

[54] Stefan Kiefer and Dominik Wojtczak. "On probabilistic parallel programs with process creation and synchronisation". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 2011, pp. 296–310 (on page 13).

[55] Michael Benedikt, Rastislav Lenhardt, and James Worrell. "LTL model checking of interval Markov chains". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer. 2013, pp. 32–46 (on page 13).

[56] Kousha Etessami and Mihalis Yannakakis. "On the Complexity of Nash Equilibria and Other Fixed Points". In: *SIAM J. Comput.* 39.6 (2010), pp. 2531–2597 (on page 13).

[57] Michael Ummels and Dominik Wojtczak. “The complexity of Nash equilibria in limit-average games”. In: *International Conference on Concurrency Theory*. Springer. 2011, pp. 482–496 (on page 13).

[58] Krishnendu Chatterjee and Rasmus Ibsen-Jensen. “The complexity of ergodic mean-payoff games”. In: *International Colloquium on Automata, Languages, and Programming*. 2014, pp. 122–133 (on page 13).

[59] Christoph Haase, Stefan Kiefer, and Markus Lohrey. “Counting problems for Parikh images”. In: *Leibniz International Proceedings in Informatics, LIPIcs*. Vol. 83. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. 2017, p. 12 (on page 13).

[60] Antonia Lechner, Joël Ouaknine, and James Worrell. “On the complexity of linear arithmetic with divisibility”. In: *2015 30th Annual ACM/IEEE Symposium on Logic in Computer Science*. IEEE. 2015, pp. 667–676 (on page 13).

[61] Johannes Blömer. “How to Denest Ramanujan’s Nested Radicals”. In: *33rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, 1992, pp. 447–456 (on page 13).

[62] Johannes Blömer. “Denesting by Bounded Degree Radicals”. In: *Algorithms - ESA ’97, 5th Annual European Symposium, Proceedings*. Ed. by R. E. Burkard and G. J. Woeginger. Vol. 1284. Lecture Notes in Computer Science. Springer, 1997, pp. 53–63 (on page 13).

[63] Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische annalen* 261.ARTICLE (1982), pp. 515–534 (on page 14).

[64] Felipe Cucker, Pascal Koiran, and Steve Smale. “A Polynomial Time Algorithm for Diophantine Equations in One Variable”. In: *J. Symb. Comput.* 27.1 (1999), pp. 21–29. DOI: 10.1006/JSCO.1998.0242 (on page 14).

[65] Hendrik W. Lenstra. “Finding small degree factors of lacunary polynomials”. In: *Proceedings of the International Conference on Number Theory organized by the Stefan Banach International Mathematical Center in Honor of the 60th Birthday of Andrzej Schinzel, Zakopane, Poland, June 30-July 9, 1997*. Ed. by Kálmán Györy, Henryk Iwaniec, and Jerzy Urbanowicz. Berlin, Boston: De Gruyter, 1999, pp. 267–276. ISBN: 9783110285581. DOI: doi:10.1515/9783110285581.267 (on pages 14, 15).

[66] Hendrik W. Lenstra Jr. “On the factorization of lacunary polynomials”. In: *Number theory in progress* 1 (1999), pp. 277–291 (on page 14).

[67] Erich L. Kaltofen and Pascal Koiran. “On the complexity of factoring bivariate supersparse (Lacunary) polynomials”. In: *Symbolic and Algebraic Computation, International Symposium ISSAC 2005, Beijing, China, July 24-27, 2005, Proceedings*. Ed. by Manuel Kauers. ACM, 2005, pp. 208–215. DOI: 10.1145/1073884.1073914 (on page 15).

[68] Erich L. Kaltofen and Pascal Koiran. "Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields". In: *Symbolic and Algebraic Computation, International Symposium, ISSAC 2006, Genoa, Italy, July 9-12, 2006, Proceedings*. Ed. by Barry M. Trager. ACM, 2006, pp. 162–168. DOI: 10.1145/1145768.1145798 (on page 15).

[69] Arkadev Chattopadhyay, Bruno Grenet, Pascal Koiran, Natacha Portier, and Yann Strozecki. "Factoring bivariate lacunary polynomials without heights". In: *International Symposium on Symbolic and Algebraic Computation, ISSAC'13, Boston, MA, USA, June 26-29, 2013*. Ed. by Manuel Kauers. ACM, 2013, pp. 141–148. DOI: 10.1145/2465506.2465932 (on page 15).

[70] Bruno Grenet. "Computing low-degree factors of lacunary polynomials: a Newton-Puiseux approach". In: *International Symposium on Symbolic and Algebraic Computation, ISSAC'14, Kobe, Japan, July 23-25, 2014*. Ed. by Katsusuke Nabeshima, Kosaku Nagasaka, Franz Winkler, and Ágnes Szántó. ACM, 2014, pp. 224–231. DOI: 10.1145/2608628.2608649 (on page 15).

[71] Bruno Grenet. "Bounded-degree factors of lacunary multivariate polynomials". In: *J. Symb. Comput.* 75 (2016), pp. 171–192. DOI: 10.1016/J.JSC.2015.11.013 (on page 15).

[72] Bruno Grenet. "Lacunaryx: computing bounded-degree factors of lacunary polynomials". In: *ACM Commun. Comput. Algebra* 49.4 (2015), pp. 121–124. DOI: 10.1145/2893803.2893807 (on page 15).

[73] Vishwas Bhargava, Shubhangi Saraf, and Ilya Volkovich. "Deterministic Factorization of Sparse Polynomials with Bounded Individual Degree". In: *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*. Ed. by Mikkel Thorup. IEEE Computer Society, 2018, pp. 485–496. DOI: 10.1109/FOCS.2018.00053 (on page 15).

[74] Pranav Bisht and Ilya Volkovich. "On Solving Sparse Polynomial Factorization Related Problems". In: *42nd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2022, December 18-20, 2022, IIT Madras, Chennai, India*. Ed. by Anuj Dawar and Venkatesan Guruswami. Vol. 250. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 10:1–10:22. DOI: 10.4230/LIPICS.FSTTCS.2022.10 (on page 15).

[75] Pranjal Dutta, Nitin Saxena, and Amit Sinhababu. "Discovering the roots: uniform closure results for algebraic classes under factoring". In: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*. Ed. by Ilias Diakonikolas, David Kempe, and Monika Henzinger. ACM, 2018, pp. 1152–1165. DOI: 10.1145/3188745.3188760 (on page 15).

[76] Amit Sinhababu and Thomas Thierauf. "Factorization of Polynomials Given By Arithmetic Branching Programs". In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 33:1–33:19. DOI: 10.4230/LIPICS.CCC.2020.33 (on page 15).

[77] Joachim Von Zur Gathen and Daniel Panario. "Factoring polynomials over finite fields: A survey". In: *Journal of Symbolic Computation* 31.1-2 (2001), pp. 3–17 (on page 15).

[78] Ashish Dwivedi. "Polynomials over composites: Compact root representation via ideals and algorithmic consequences". PhD thesis. Ph. D. Dissertation. CSE, IIT Kanpur, India, 2023 (on page 15).

[79] Gorav Jindal and Michael Sagraloff. "Efficiently Computing Real Roots of Sparse Polynomials". In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017*. Ed. by Michael A. Burr, Chee K. Yap, and Mohab Safey El Din. ACM, 2017, pp. 229–236. DOI: 10.1145/3087604.3087652 (on page 16).

[80] Larry Stockmeyer. "On Approximation Algorithms for #P". In: *SIAM Journal on Computing* 14.4 (1985), pp. 849–861. DOI: 10.1137/0214060 (on page 17).

[81] Abhibhav Garg and Nitin Saxena. "Special-case algorithms for blackbox radical membership, nullstellensatz and transcendence degree". In: *ISSAC'20: International Symposium on Symbolic and Algebraic Computation, Kalamata, Greece, July 20-23, 2020*. Ed. by Ioannis Z. Emiris and Lihong Zhi. ACM, 2020, pp. 186–193. DOI: 10.1145/3373207.3404030 (on page 18).

[82] Martijn Baartse and Klaus Meer. "Topics in real and complex number complexity theory". In: *Recent Advances in Real Complexity and Computation, Contemporary Mathematics* 604 (2012), pp. 1–53 (on page 18).

[83] Paul Beame, Russell Impagliazzo, Jan Krajícek, Toniann Pitassi, and Pavel Pudlák. "Lower Bound on Hilbert's Nullstellensatz and propositional proofs". In: *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*. IEEE Computer Society, 1994, pp. 794–806. DOI: 10.1109/SFCS.1994.365714 (on page 18).

[84] Martin Davis, Yuri Matijasevič, and Julia Robinson. "Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution". In: *American Math. Soc Providence* 1 (1976) (on page 19).

[85] Marcus Schaefer and Daniel Štefankovič. "The complexity of tensor rank". In: *Theory of Computing Systems* 62 (2018), pp. 1161–1174 (on page 19).

[86] Sayak Chakrabarti, Ashish Dwivedi, and Nitin Saxena. "Solving polynomial systems over non-fields and applications to modular polynomial factoring". In: *Journal of Symbolic Computation* 125 (2024), p. 102314. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2024.102314 (on page 19).

[87] Suryajith Chillara, Coral Grichener, and Amir Shpilka. "On Hardness of Testing Equivalence to Sparse Polynomials Under Shifts". In: *40th International Symposium on Theoretical Aspects of Computer Science, STACS 2023, March 7-9, 2023, Hamburg, Germany*. Ed. by Petra Berenbrink, Patricia Bouyer, Anuj Dawar, and Mamadou Moustapha Kanté. Vol. 254. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 22:1–22:20. DOI: 10.4230/LIPICS.STACS.2023.22 (on page 19).

[88] Neeraj Kayal. "Affine projections of polynomials: extended abstract". In: *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*. Ed. by Howard J. Karloff and Toniann Pitassi. ACM, 2012, pp. 643–662. DOI: 10.1145/2213977.2214036 (on pages 19, 120).

[89] Johan Håstad. "Tensor Rank is NP-Complete". In: *Automata, Languages and Programming, 16th International Colloquium, ICALP89, Stresa, Italy, July 11-15, 1989, Proceedings*. Ed. by Giorgio Ausiello, Mariangiola Dezani-Ciancaglini, and Simona Ronchi Della Rocca. Vol. 372. Lecture Notes in Computer Science. Springer, 1989, pp. 451–460. DOI: 10.1007/BFb003577 (on page 19).

[90] Yaroslav Shitov. "How hard is the tensor rank?" In: *arXiv preprint arXiv:1611.01559* (2016) (on page 19).

[91] Marc Giusti and Joos Heintz. "La determination des points isoles et de la dimension d'une variété algébrique peut se faire en temps polynomial". In: *Computational algebraic geometry and commutative algebra (Cortona, 1991)* (1993), pp. 216–256 (on pages 19, 85).

[92] Pascal Koiran. "Approximating the Volume of Definable Sets". In: *36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, USA, 23-25 October 1995*. IEEE Computer Society, 1995, pp. 134–141. DOI: 10.1109/SFCS.1995.492470 (on pages 20, 85).

[93] Pascal Koiran. "The Complexity of Local Dimensions for Constructible Sets". In: *J. Complex.* 16.1 (2000), pp. 311–323. DOI: 10.1006/JCOM.1999.0536 (on pages 20, 93).

[94] Guillermo Matera and Jose Maria Turull Torres. "The Space Complexity of Elimination Theory: Upper Bounds". In: *Foundations of Computational Mathematics*. Ed. by Felipe Cucker and Michael Shub. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 267–276. ISBN: 978-3-642-60539-0 (on page 20).

[95] Pascal Koiran. "The Real Dimension Problem Is NPR-Complete". In: *J. Complex.* 15.2 (1999), pp. 227–238. DOI: 10.1006/JCOM.1999.0502 (on page 20).

[96] Ivan Bannwarth and Mohab Safey El Din. "Probabilistic Algorithm for Computing the Dimension of Real Algebraic Sets". In: *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath, United Kingdom, July 06 - 09, 2015*. Ed. by Kazuhiro Yokoyama, Steve Linton, and Daniel Robertz. ACM, 2015, pp. 37–44. DOI: 10.1145/2755996.2756670 (on page 20).

[97] Pierre Lairez and Mohab Safey El Din. “Computing the Dimension of Real Algebraic Sets”. In: *ISSAC'21: International Symposium on Symbolic and Algebraic Computation, Virtual Event, Russia, July 18-23, 2021*. Ed. by Frédéric Chyzak and George Labahn. ACM, 2021, pp. 257–264. DOI: 10.1145/3452143.3465551 (on page 20).

[98] Frédéric Smietanski. “A Parametrized Nullstellensatz”. In: *Computational Algebraic Geometry*. Ed. by Frédéric Eyssette and André Galligo. Boston, MA: Birkhäuser Boston, 1993, pp. 287–300. ISBN: 978-1-4612-2752-6 (on page 21).

[99] Carlos d'Andrea, Teresa Krick, and Martín Sombra. “Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze”. In: *Annales scientifiques de l'École Normale Supérieure*. Vol. 46. 4. 2013, pp. 549–627 (on pages 21, 75, 77, 92, 93).

[100] Éric Schost. “Computing Parametric Geometric Resolutions”. In: *Appl. Algebra Eng. Commun. Comput.* 13.5 (2003), pp. 349–393. DOI: 10.1007/S00200-002-0109-X (on page 21).

[101] Guillaume Moroz. “Complexity of the resolution of parametric systems of polynomial equations and inequations”. In: *Symbolic and Algebraic Computation, International Symposium, ISSAC 2006, Genoa, Italy, July 9-12, 2006, Proceedings*. Ed. by Barry M. Trager. ACM, 2006, pp. 246–253. DOI: 10.1145/1145768.1145810 (on page 21).

[102] Daniel Lazard and Fabrice Rouillier. “Solving parametric polynomial systems”. In: *J. Symb. Comput.* 42.6 (2007), pp. 636–667. DOI: 10.1016/J.JSC.2007.01.007 (on page 21).

[103] Ali Ayad. “On computing absolutely irreducible components of algebraic varieties with parameters”. In: *Computing* 89.1-2 (2010), pp. 45–68. DOI: 10.1007/S00607-010-0099-7 (on page 21).

[104] Thoralf Skolem. “Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen”. In: *C. r* 8 (1934), pp. 163–188 (on page 21).

[105] Kurt Mahler. *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*. Vol. 38. Noord-Hollandsche Uitgevers Mij, 1935 (on page 22).

[106] Christer Lech. “A note on recurring series”. In: *Arkiv för Matematik* 2.5 (1953), pp. 417–421 (on page 22).

[107] Georges Hansel. “Une démonstration simple du théorème de Skolem-Mahler-Lech”. In: *Theoretical Computer Science* 43 (1986), pp. 91–98. ISSN: 0304-3975. DOI: 10.1016/0304-3975(86)90168-4 (on page 22).

[108] Jean-Paul Bézivin. “Une généralisation du théorème de Skolem-Mahler-Lech”. In: *The Quarterly Journal of Mathematics* 40.2 (June 1989), pp. 133–138. ISSN: 0033-5606. DOI: 10.1093/qmath/40.2.133 (on page 22).

[109] Harm Derksen. “A Skolem–Mahler–Lech theorem in positive characteristic and finite automata”. In: *Inventiones mathematicae* 168 (2005), pp. 175–224 (on page 22).

[110] Boris Adamczewski and Jason P. Bell. "On vanishing coefficients of algebraic power series over fields of positive characteristic". In: *Inventiones mathematicae* 187.2 (2012), pp. 343–393 (on page 22).

[111] Jason P. Bell. "A Generalised Skolem–Mahler–lech Theorem for Affine Varieties". In: *Journal of the London Mathematical Society* 73.2 (Apr. 2006), pp. 367–379. ISSN: 0024-6107. DOI: 10.1112/S002461070602268X (on page 22).

[112] Joël Ouaknine and James Worrell. "Decision Problems for Linear Recurrence Sequences". In: *Reachability Problems - 6th International Workshop, RP 2012, Bordeaux, France, September 17-19, 2012. Proceedings*. Ed. by Alain Finkel, Jérôme Leroux, and Igor Potapov. Vol. 7550. Lecture Notes in Computer Science. Springer, 2012, pp. 21–28. DOI: 10.1007/978-3-642-33512-9_3 (on pages 22, 118).

[113] Richard Lipton, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. "On the Skolem Problem and the Skolem Conjecture". In: *LICS'22: 37th Annual ACM/IEEE Symposium on Logic in Computer Science, Haifa, Israel, August 2 - 5, 2022*. Ed. by Christel Baier and Dana Fisman. ACM, 2022, 5:1–5:9. DOI: 10.1145/3531130.3533328 (on pages 22, 118).

[114] Florian Luca, Joël Ouaknine, and James Worrell. "Universal Skolem Sets". In: *36th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2021, Rome, Italy, June 29 - July 2, 2021*. IEEE, 2021, pp. 1–6. DOI: 10.1109/LICS52264.2021.9470513 (on pages 22, 118).

[115] Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. "Skolem Meets Schanuel". In: *47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria*. Ed. by Stefan Szeider, Robert Ganian, and Alexandra Silva. Vol. 241. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 20:1–20:15. DOI: 10.4230/LIPICS.MFCS.2022.20 (on pages 22, 118).

[116] Jason P. Bell, Stanley N. Burris, and Karen Yeats. "On the set of zero coefficients of a function satisfying a linear differential equation". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 153.2 (May 2012), pp. 235–247. DOI: 10.1017/S0305004112000114 (on page 22).

[117] Marko Petkovšek, Herbert S. Wilf, and Doron Zeilberger. *A = B*. CRC Press, 1996. ISBN: 9781439864500 (on page 22).

[118] Joël Ouaknine and James Worrell. "Positivity Problems for Low-Order Linear Recurrence Sequences". In: *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*. Ed. by Chandra Chekuri. SIAM, 2014, pp. 366–379. DOI: 10.1137/1.9781611973402.27 (on page 24).

[119] Eike Neumann, Joël Ouaknine, and James Worrell. “Decision Problems for Second-Order Holonomic Recurrences”. In: *48th International Colloquium on Automata, Languages, and Programming, ICALP*. Vol. 198. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 99:1–99:20 (on page 24).

[120] George Kenison, Oleksiy Klurman, Engel Lefaucheux, Florian Luca, Pieter Moree, Joël Ouaknine, Markus A. Whiteland, and James Worrell. “On Positivity and Minimality for Second-Order Holonomic Sequences”. In: *46th International Symposium on Mathematical Foundations of Computer Science, MFCS 2021, August 23-27, 2021, Tallinn, Estonia*. Ed. by Filippo Bonchi and Simon J. Puglisi. Vol. 202. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 67:1–67:15. DOI: 10.4230/LIPICS.MFCS.2021.67 (on page 24).

[121] Manuel Kauers and Veronika Pillwein. “When can we detect that a P-finite sequence is positive?” In: *Symbolic and Algebraic Computation, International Symposium, ISSAC, Proceedings*. Ed. by Wolfram Koepf. ACM, 2010, pp. 195–201 (on page 24).

[122] Veronika Pillwein and Miriam Schussler. “An efficient procedure deciding positivity for a class of holonomic functions”. In: *ACM Commun. Comput. Algebra* 49.3 (2015), pp. 90–93 (on page 24).

[123] Alaa Ibrahim and Bruno Salvy. “Positivity Certificates for Linear Recurrences”. In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. Society for Industrial and Applied Mathematics, Jan. 2024, pp. 982–994. ISBN: 9781611977912. DOI: 10.1137/1.9781611977912.37 (on page 24).

[124] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009. ISBN: 978-0-521-42426-4. URL: http://www.cambridge.org/catalogue/catalogue.asp?isbn=9780521424264 (on page 27).

[125] Ian N. Stewart and David Tall. *Algebraic Number Theory and Fermat’s Last Theorem: Third Edition*. Ak Peters Series. Taylor & Francis, 2001. ISBN: 9781568811192 (on page 29).

[126] Ian N. Stewart. *Galois theory*. Chapman and Hall, 1973. ISBN: 0412108003 9780412108006 (on pages 29, 54).

[127] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013. ISBN: 9783662029459 (on pages 31, 59).

[128] James S. Milne. *Fields and Galois Theory*. Lecture notes (version 5.0). 2021. URL: https://www.jmilne.org/math/CourseNotes/FT.pdf (on page 31).

[129] Piyush P. Kurur. “Complexity Upper Bounds using Permutation Group theory”. PhD thesis. University of Madras, Chennai, 2006. URL: https://piyush-kurur.github.io/research/publication/Thesis/2006-01-13-Thesis.pdf (on page 31).

[130] Fernando Q. Gouvea. *p-adic Numbers: An Introduction*. Universitext. Springer Berlin Heidelberg, 2003. ISBN: 9783540629115 (on page 33).

[131] James S. Milne. *Algebraic Number Theory*. Lecture notes (version 3.08). 2020. URL: https://www.jmilne.org/math/CourseNotes/ANT.pdf (on pages 34, 53).

[132] Peter Stevenhagen and Hendrik W. Lenstra Jr. *Chebotarev and his density theorem*. 1995 (on page 35).

[133] Igor R. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer Berlin Heidelberg, 2013. ISBN: 9783642379567. DOI: 10.1007/978-3-642-37956-7. URL: 10.1007/978-3-642-37956-7 (on pages 35, 89).

[134] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013 (on pages 35, 37).

[135] Manuel Kauers and Peter Paule. *The Concrete Tetrahedron - Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates*. Texts & Monographs in Symbolic Computation. Springer, 2011. ISBN: 978-3-7091-0444-6. DOI: 10.1007/978-3-7091-0445-3 (on pages 38, 99).

[136] Isaac Newton, Derek Thomas Whiteside, et al. "The mathematical papers of Isaac Newton". In: *The Mathematical Papers of Isaac Newton* (2008) (on page 41).

[137] Victor Puiseux. "Recherches sur les fonctions algébriques". In: *Journal de mathématiques pures et appliquées* 15 (1850), pp. 365–480 (on page 41).

[138] John McDonald. "Fiber polytopes and fractional power series". In: *Journal of Pure and Applied Algebra* 104.2 (1995), pp. 213–233. ISSN: 0022-4049. DOI: https://doi.org/10.1016/0022-4049(94)00129-5 (on page 41).

[139] Fuensanta Aroca, Julie Decaup, and Guillaume Rond. "The minimal cone of an algebraic Laurent series". In: *Mathematische Annalen* 382.3 (2022), pp. 1745–1773. DOI: 10.1007/s00208-021-02338-9 (on page 41).

[140] Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. "Identity Testing for Radical Expressions". In: *LICS'22: 37th Annual ACM/IEEE Symposium on Logic in Computer Science, Haifa, Israel, August 2 - 5, 2022*. Ed. by Christel Baier and Dana Fisman. ACM, 2022, 8:1–8:11. DOI: 10.1145/3531130.3533331 (on pages 43, 137).

[141] Eric Bach, James Driscoll, and Jeffrey Shallit. "Factor Refinement". In: *Journal of Algorithms* 15.2 (1993), pp. 199–222. ISSN: 0196-6774 (on pages 45, 48).

[142] Richard P. Brent. "Fast multiple-precision evaluation of elementary functions". In: *Pi: The Next Generation: A Sourcebook on the Recent History of Pi and Its Computation*. Springer International Publishing, 2016, pp. 9–20. ISBN: 978-3-319-32377-0 (on page 49).

[143] Jeffrey C. Lagarias and Andrew M. Odlyzko. "Effective versions of the Chebotarev density theorem". In: *Algebraic Number Fields*. Academic Press, 1977, pp. 409–464. ISBN: 9780122689604 (on page 59).

[144] Jean-Pierre Serre. "Quelques applications du théoreme de densité de Chebotarev". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 54.1 (1981), pp. 123–201 (on page 59).

[145] Johannes A. Buchmann and Hendrik W. Lenstra. "Approximating rings of integers in number fields". In: *Journal de théorie des nombres de Bordeaux* 6.2 (1994), pp. 221–260 (on page 59).

[146] Harold Davenport and Hugh L. Montgomery. *Multiplicative Number Theory*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475759273 (on page 67).

[147] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*. Vol. 53. AMS, 2004 (on page 67).

[148] László Babai and Shlomo Moran. "Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes". In: *J. Comput. Syst. Sci.* 36.2 (1988), pp. 254–276. DOI: 10.1016/0022-0000(88)90028-1 (on page 69).

[149] Johannes Mittmann. "Independence in Algebraic Complexity Theory". PhD thesis. University of Bonn, Germany, 2013 (on page 70).

[150] Serge Lang. *Algebra*. Vol. 211. Springer Science, 2012 (on page 70).

[151] Rida Ait El Manssour, Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. *A parametric version of the Hilbert Nullstellensatz*. Accepted to appear in SOSA'25. 2024. arXiv: 2408.13027 [cs.CC]. URL: https://arxiv.org/abs/2408.13027 (on pages 73, 137).

[152] Noah Fitchas, André Galligo, and Jacques Morgenstern. "Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields". In: *Journal of Pure and Applied Algebra* 67.1 (1990), pp. 1–14. ISSN: 0022-4049. DOI: 10.1016/0022-4049(90)90159-F (on page 78).

[153] Albrecht Fröhlich and Martin J Taylor. *Algebraic number theory*. 27. Cambridge University Press, 1991 (on page 81).

[154] Van H Vu, Melanie Matchett Wood, and Philip Matchett Wood. "Mapping incidences". In: *Journal of the London Mathematical Society* 84.2 (2011), pp. 433–445 (on page 93).

[155] Klara Nosan, Amaury Pouly, Mahsa Shirmohammadi, and James Worrell. "The Membership Problem for Hypergeometric Sequences with Rational Parameters". In: *ISSAC'22: International Symposium on Symbolic and Algebraic Computation, Villeneuve-d'Ascq, France, July 4 - 7, 2022*. Ed. by Marc Moreno Maza and Lihong Zhi. ACM, 2022, pp. 381–389. DOI: 10.1145/3476446.3535504 (on pages 95, 103, 137).

[156] Marc Chamberland and Armin Straub. "On gamma quotients and infinite products". In: *Advances in Applied Mathematics* 51.5 (2013), pp. 546–562 (on pages 99, 101).

[157] Serge Lang. "Relations de distributions et exemples classiques". In: *Séminaire Delange-Pisot-Poitou. Théorie des nombres* 19.2 (1977-1978) (on page 102).

[158] Neal Koblitz and Arthur Ogus. "Algebraicity of some products of values of the F function, Appendix of Valeurs de fonctions L et periodes d'intégrales". In: *Proceedings of Symposia in Pure Mathematics* 33 (1979), part 2, 313–346 (on page 102).

[159] Michel Waldschmidt. "Transcendence of periods: the state of the art". In: *Pure and Applied Mathematics Quarterly* 2.2 (2006), pp. 435–463 (on page 102).

[160] Yves André. *Une introduction aux motifs (motifs purs, motifs mixtes, périodes).* Vol. 17. Panoramas et Synthèses. Société Mathématique de France, 2004 (on page 102).

[161] George Kenison, Oleksiy Klurman, Engel Lefaucheux, Florian Luca, Pieter Moree, Joël Ouaknine, Markus A. Whiteland, and James Worrell. "On Inequality Decision Prolems for Low-Order Holonomic Sequences". Submitted. 2023 (on page 103).

[162] Jitsuro Nagura. "On The Interval Containing At Least One Prime Number". In: *Proceedings of the Japan Academy* 28.4 (1952), pp. 177–181. DOI: 10.3792/pja/1195570997 (on page 107).

[163] Michael A. Bennett, Greg Martin, Kevin O'Bryant, and Andrew Rechnitzer. "Explicit bounds for primes in arithmetic progressions". In: *Illinois Journal of Mathematics* 62.1-4 (2018), pp. 427–532 (on page 114).

[164] Jason P. Bell. "p-adic valuations and k-regular sequences". In: *Discret. Math.* 307.23 (2007), pp. 3070–3075. DOI: 10.1016/J.DISC.2007.03.009 (on page 116).

[165] Luis A. Medina, Victor H. Moll, and Eric Rowland. "Periodicity in the p-adic valuation of a polynomial". In: *Journal of Number Theory* 180 (2017), pp. 139–153. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2017.03.006 (on page 116).

[166] Teowodros Amdeberhan, Louis A. Medina, and Victor H. Moll. "Asymptotic valuations of sequences satisfying first order recurrences". In: *Proceedings of the American Mathematical Society* 137.3 (2009), pp. 885–890 (on page 116).

[167] Erci Delaygue, Tanguy Rivoal, and Julien Roques. "On Dwork's p-adic formal congruences theorem and hypergeometric mirror maps". In: *Memoirs of the American Mathematical Society* 246 (Sept. 2013). DOI: 10.1090/memo/1163 (on page 117).

[168] George Kenison, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. "The Membership Problem for Hypergeometric Sequences with Quadratic Parameters". In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation, ISSAC 2023, Tromsø, Norway, July 24-27, 2023.* Ed. by Alicia Dickenstein, Elias P. Tsigaridas, and Gabriela Jeronimo. ACM, 2023, pp. 407–416. DOI: 10.1145/3597066.3597121 (on pages 117, 118, 137).

[169] Graham Everest, Shaun Stevens, Duncan Tamsett, and Tom Ward. "Primes Generated by Recurrence Sequences". In: *The American Mathematical Monthly* 114.5 (2007), pp. 417–431. ISSN: 00029890, 19300972 (on page 117).

[170] Cécile Dartyge and James Maynard. “On the largest prime factor of quartic polynomial values: the cyclic and dihedral cases”. In: *arXiv preprint arXiv:2212.03381* (2022) (on page 117).

[171] George Kenison. “The Threshold Problem for Hypergeometric Sequences with Quadratic Parameters”. In: *51st International Colloquium on Automata, Languages, and Programming, ICALP 2024*. Vol. 297. 2024, 124:1–124:20. DOI: 10.4230/LIPIcs.ICALP.2024.124 (on page 118).

[172] Vincent D. Blondel and Natacha Portier. “The presence of a zero in an integer linear recurrent sequence is NP-hard to decide”. In: *Linear algebra and its Applications* 351 (2002), pp. 91–98 (on page 118).

[173] Klara Nosan, Amaury Pouly, Sylvain Schmitz, Mahsa Shirmohammadi, and James Worrell. “On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices”. In: *ISSAC’22: International Symposium on Symbolic and Algebraic Computation, Villeneuve-d’Ascq, France, July 4 - 7, 2022*. Ed. by Marc Moreno Maza and Lihong Zhi. ACM, 2022, pp. 129–138. DOI: 10.1145/3476446.3536172 (on page 137).

[174] Nikhil Balaji, Lorenzo Clemente, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. “Multiplicity Problems on Algebraic Series and Context-Free Grammars”. In: *LICS*. 2023, pp. 1–12. DOI: 10.1109/LICS56636.2023.10175707 (on page 137).

Publications

Some of the results presented in this thesis are based on the following publications:

Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. "Identity Testing for Radical Expressions". In: *LICS'22: 37th Annual ACM/IEEE Symposium on Logic in Computer Science, Haifa, Israel, August 2 - 5, 2022*. Ed. by Christel Baier and Dana Fisman. ACM, 2022, 8:1–8:11. DOI: 10.1145/3531130.3533331

Klara Nosan, Amaury Pouly, Mahsa Shirmohammadi, and James Worrell. "The Membership Problem for Hypergeometric Sequences with Rational Parameters". In: *ISSAC'22: International Symposium on Symbolic and Algebraic Computation, Villeneuve-d'Ascq, France, July 4 - 7, 2022*. Ed. by Marc Moreno Maza and Lihong Zhi. ACM, 2022, pp. 381–389. DOI: 10.1145/3476446.3535504

Rida Ait El Manssour, Nikhil Balaji, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. *A parametric version of the Hilbert Nullstellensatz*. Accepted to appear in SOSA'25. 2024. arXiv: 2408.13027 [cs.CC]. URL: https://arxiv.org/abs/2408.13027

Other publications beyond the scope of this thesis are:

Klara Nosan, Amaury Pouly, Sylvain Schmitz, Mahsa Shirmohammadi, and James Worrell. "On the Computation of the Zariski Closure of Finitely Generated Groups of Matrices". In: *ISSAC'22: International Symposium on Symbolic and Algebraic Computation, Villeneuve-d'Ascq, France, July 4 - 7, 2022*. Ed. by Marc Moreno Maza and Lihong Zhi. ACM, 2022, pp. 129–138. DOI: 10.1145/3476446.3536172

Nikhil Balaji, Lorenzo Clemente, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. "Multiplicity Problems on Algebraic Series and Context-Free Grammars". In: *LICS*. 2023, pp. 1–12. DOI: 10.1109/LICS56636.2023.10175707

George Kenison, Klara Nosan, Mahsa Shirmohammadi, and James Worrell. "The Membership Problem for Hypergeometric Sequences with Quadratic Parameters". In: *Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation, ISSAC 2023, Tromsø, Norway, July 24-27, 2023*. Ed. by Alicia Dickenstein, Elias P. Tsigaridas, and Gabriela Jeronimo. ACM, 2023, pp. 407–416. DOI: 10.1145/3597066.3597121