Methods of class field theory to separate logics over finite residue classes and circuit complexity

ARGIMIRO ARRATIA, *Department of Computer Science / BGSMath, Universitat Politècnica de Catalunya, Barcelona, Spain.*
E-mail: argimiro@cs.upc.edu

CARLOS E. ORTIZ, *Department of Computer Science and Mathematics, Arcadia University, USA.*
E-mail: ortiz@arcadia.edu

Abstract

Separations among the first-order logic $\mathcal{R}es(0,+,\times)$ of finite residue classes, its extensions with generalized quantifiers, and in the presence of a built-in order are shown in this article, using algebraic methods from class field theory. These methods include classification of spectra of sentences over finite residue classes as systems of congruences, and the study of their h-densities over the set of all prime numbers, for various functions h on the natural numbers. Over ordered structures, the logic of finite residue classes and extensions are known to capture DLOGTIME-uniform circuit complexity classes ranging from AC^0 to TC^0. Separating these circuit complexity classes is directly related to classifying the h-density of spectra of sentences in the corresponding logics of finite residue classes. General conditions are further shown in this work for a logic over the finite residue classes to have a sentence whose spectrum has no h-density. A corollary of this characterization of spectra of sentences is that in $\mathcal{R}es(0,+,\times,<)+\mathrm{M}$, the logic of finite residue classes with built-in order and extended with the majority quantifier M, there are sentences whose spectrum have no exponential density.

Keywords: Circuit complexity, congruence classes, density, finite model theory, prime spectra.

1 Introduction

A first-order logic for finite residue classes, denoted as $\mathcal{R}es(0,+,\times)$ with $+$ and $\times$ being modular addition and multiplication, and extensions of this logic with certain generalized quantifiers, were shown by us in [2] to coincide with the first-order logic, and corresponding extensions, for the standard finite models with arithmetic operations as considered in [16]. Therefore, from the descriptive complexity perspective, the computational complexity classes that can be described with these logics for finite residue classes are the DLOGTIME-uniform circuit complexity classes, consisting of circuits of constant depth and polynomial size for which a description can be efficiently computed from the size of their inputs.

The perspective of finite residue classes as instances of problems in these circuit complexity classes allow us to leverage the algebraic machinery proper of finite rings and fields of integer polynomials, algebraic number theory and, in general, from class field theory to study expressibility problems in these logics. In [2] we gave a brief account of the use of some of these algebraic tools to distinguish the expressive power of the logic of finite residue classes from its extensions with generalized quantifiers and in the addition of a built-in order. In this article, we review those tools in more detail and expand our methods and results.

doi:10.1093/logcom/exx007

The algebraic methodology stems from the class field notion of spectra of polynomials over finite fields adapted to sets of sentences in the logics of finite residue classes. The spectrum of a sentence θ is the collection of primes p such that θ holds in the residue class mod p. This spectra for first-order sentences was extensively studied by Ax in [3, 4] in connection with the decidability of the elementary theory of finite fields.

Working with the concept of spectra of sentences, our strategy to show separation among two logics, say $\mathcal{L}$ and $\mathcal{L}'$, over finite structures, can be described as follows:

> *Prove that the spectra of all sentences in $\mathcal{L}$ have property P, but there exists a sentence in $\mathcal{L}'$ whose spectrum does not have property P.*

From the algebraic machinery of class field theory we exploit as candidates for property P the following:

- certain characterization of spectra of polynomial congruences as specific sets of congruent integers;
- different notions of density of sets of primes, in particular, the natural and the exponential density.

We illustrate the power of these methods derived from class field theory in solving definability problems in descriptive complexity in many ways. In fact, to illustrate the richness of methods that can be obtained from the proposed algebraic setting, we will provide three proofs of the separation of $\mathcal{R}es(0,+,\times)$ from its ordered extension $\mathcal{R}es(0,+,\times,<)$ by different methods, one of combinatorial nature and the other two analytical, based on the concept of density.

The purpose of the methods we introduce in this article is to provide new tools and an alternative framework to the standard ones in use in finite model theory, such as Ehrenfeucht-Fraïssé (EF) games, which has been shown to have limited potential or to be hard to apply when separating computational complexity classes, in particular circuit complexity classes. Proofs of this limitation are given in [16, Ch. 6], where a measure of the difficulty (almost impossibility) of success in separating logics with the method of EF games in the presence of ordered structures is given; the paper [18], which investigates the feasibility of using EF games to prove lower bounds for the circuit class AC^0; or the work [20] on the 'bounded degree property' which amounts to saying that it is futile to weaken the order relation and compensate it with adding some counting mechanism to get meaningful separation results. In the light of this evidence, we sought for a new context and new tools for descriptive complexity. We move from standard finite structures to finite rings and fields, consider the full linear order, and substitute combinatorial games for tools from algebraic number theory and analysis.

The article is organized as follows. After some necessary preliminaries in circuit complexity and descriptive complexity (Section 2), we define in Section 3 the logic of finite residue classes, and state without proof our result from [2] on capturing circuit complexity classes by these logics. In Section 4 we review the notion of the prime spectrum of a sentence, its characterization as the spectrum of polynomial equations and the properties of the Boolean algebra of this spectra, derived from the seminal results by Ax [3, 4]. In Section 5, we exhibit a characterization of the spectra of sentences in $\mathcal{R}es(0,+,\times)$ in terms of sets of integer congruences, using a result of Lagarias [19] on spectra of polynomial equations. This tool allows us to show that $\mathcal{R}es(0,+,\times)$ and its extensions with modular quantifiers, namely $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(q)$ for each natural $q>2$, have different expressive power. We also show how to apply this number-theoretic tool to differentiate the expressive power of $\mathcal{R}es(0,+,\times)$ and its ordered counterpart $\mathcal{R}es(0,+,\times,<)$. In Section 6, we introduce the general measure of h-density for subsets of prime numbers, and the particular cases of interest, namely, the natural and exponential densities. We show that the natural density of the spectra of sentences in the logic $\mathcal{R}es(0,+,\times)$ (over unordered structures) always exists, but differs in an essential way in their possible values from the spectra of sentences in the extension with built-in order. We give in Section 7 conditions based solely on the function h under which we can construct sets of primes with no h-density, and use this tool to show, in Section 8, two results on different densities: One showing the existence of a spectrum of a sentence in $\mathcal{R}es(0,+,\times,<)$ with no natural density (although this spectrum does have exponential density); the other showing the existence of a spectrum of a sentence in $\mathcal{R}es(0,+,\times,<)+\mathrm{M}$ with no exponential density. We observe that showing that every spectrum of a sentence of $\mathcal{R}es(0,+,\times,<)$ has exponential density will yield a class field theory proof of the known, yet remarkable, separation of the (uniform) circuit classes AC^0 and TC^0, a result that was obtained from seminal work [1, 12]. All the examples that we know so far of spectra of sentences of $\mathcal{R}es(0,+,\times,<)$ have exponential density. Section 9 contains our final remarks and conclusions.

2 Preliminaries

2.1 Circuit complexity

We are interested in the uniform version of the circuit complexity classes ranging from AC^0 to TC^0. Recall that AC^0 is the class of problems (defined as Boolean predicates or functions) accepted by polynomial size, constant depth circuits with NOT gates and unbounded fan-in AND and OR gates. Extending AC^0 circuits with unbounded MOD_q gates, for a fixed integer $q>1$, one obtains the class $\mathrm{ACC}(q)$. For each integer $q>1$, a MOD_q gate reads its Boolean input and returns a 1 if the sum of the input bits is divisible by q (i.e. the sum is equal to 0 mod q); otherwise it returns 0. Putting together all the $\mathrm{ACC}(q)$ classes we get the class ACC, i.e. $\mathrm{ACC}=\bigcup\limits_{q>1}\mathrm{ACC}(q)$. On the other hand, extending AC^0 circuits with unbounded MAJ gates one obtains the class TC^0. A MAJ (or *majority*) gate returns a 1 if the sum of n bits given as input is greater or equal to $n/2$; otherwise it returns a 0. The problems decided with the use of MOD_q gates can be decided by using MAJ gates instead. This fact, together with all given definitions of these circuit classes, give us for all $q>1$ (cf. [7, 16])

$$\mathrm{AC}^0\subseteq\mathrm{ACC}(q)\subseteq\mathrm{ACC}\subseteq\mathrm{TC}^0.$$

A circuit family is uniform if a description of each circuit can be computed efficiently from the size of the input; otherwise, it is non-uniform. DLOGTIME uniformity means that circuits can be described by a random-access deterministic Turing machine in time logarithmic on the size of the input expressed in binary. This is a very weak form of computation but which has an equivalent interpretation as a first-order reduction in finite model theory (we discuss this further in Section 2.2 below). The uniformity condition is crucial to relate time and space complexity with size and depth (see [8]), the measures for circuit complexity, since it can be shown that in the non-uniform setting there are sets with trivial circuit complexity that are not recursive.

Various bounds are known for the aforementioned circuit complexity classes; see the survey [7], and for a more in-depth and up-to-date account consult [17]. The first significant lower bounds were given by Furst, Saxe and Sipser in [12] and Ajtai in [1], with further improvement by Hastad [15], demonstrating that the PARITY function, which can be decided with MOD_2 gates, cannot be decided in AC^0. Therefore, $\mathrm{AC}^0\neq\mathrm{ACC}(2)$. Another bound given by Smolensky in [22], proves that if p and q are distinct primes then $\mathrm{ACC}(p)\neq\mathrm{ACC}(q)$. This implies that MAJ gates are more powerful than MOD_p gates, for single prime p. Nonetheless, it is yet unknown if compositions of different MOD gates are sufficient for deciding all problems that are decided by MAJ gates; that is, it is unknown if ACC coincides or not with TC^0.

2.2 Descriptive complexity

Our approach to circuit complexity is through finite model theory, and as a consequence we are working with circuit classes that are DLOGTIME-uniform since, as it has been shown in [5], the problems in DLOGTIME-uniform circuit classes AC^0 to TC^0 are definable in first-order logic with built-in arithmetic predicates and some generalized quantifiers. This works as follows. Consider first the basic logic $FO(\leq,\oplus,\otimes)$, which is first-order logic with built-in order relation $\leq$, and two ternary predicates $\oplus$ and $\otimes$. In a finite model for this logic, denoted here as $\mathcal{A}_m$ (m is the cardinality of the model, and its universe is $|\mathcal{A}_m|=\{0,1,\dots,m-1\}$), the interpretation of $\leq$ on $\mathcal{A}_m$ is as a total ordering on $|\mathcal{A}_m|$, and the interpretations of $\oplus$ and $\otimes$ are as truncated addition and multiplication (e.g. any pair of elements that add up -or multiplies- to a quantity greater than m is not a defined triple). Consider further the following generalized quantifiers:

($G1$) *Modular* quantifiers, $\exists^{(r,q)}$, which for integers r and q, with $0\leq r<q$, and formula $\phi(\overline{x},z)$, the quantified formula $\exists^{(r,q)}z\phi(\overline{a},z)$ holds in $\mathcal{A}_m$ if and only if the number of values for z that makes $\phi(\overline{a},z)$ true is equal to r modulo q.

($G2$) *Majority* quantifier, M, which for a formula $\phi(\overline{x},z)$, $(\mathrm{M}z)\phi(\overline{a},z)$ holds in $\mathcal{A}_m$ if and only if $\phi(\overline{a},z)$ is true for more than half of the possible values for z.

Let $FO(\leq,\oplus,\otimes)+MOD(q)$, for a fixed integer $q>1$, be the logic $FO(\leq,\oplus,\otimes)$ extended with modular quantifiers with moduli q; i.e. the set of first-order formulas as before plus the quantifiers $\exists^{(r,q)}$ with $0\leq r<q$.

Let $FO(\leq,\oplus,\otimes)+MOD=\bigcup_{q>1}(FO(\leq,\oplus,\otimes)+MOD(q))$, and $FO(\leq,\oplus,\otimes)+M$ the logic extended with the majority quantifier M (cf. [16]). Barrington et al. proved

THEOREM 2.1 ([5])
The problems in DLOGTIME-uniform class $\mathcal{C}$ are exactly those definable in the logic $\mathcal{L}$, where $\mathcal{C}$ is AC^0, $ACC(q)$, ACC or TC^0, and $\mathcal{L}$ is $FO(\leq,\oplus,\otimes)$, $FO(\leq,\oplus,\otimes)+MOD(q)$, $FO(\leq,\oplus,\otimes)+MOD$ or $FO(\leq,\oplus,\otimes)+M$, respectively.

We will also need an alternative logical description of TC^0, namely, via FO(COUNT) the first-order logic over structures with numbers and counting quantifiers (refer to [16, §12.3] for details). This is first-order logic interpreted over two sorted structures consisting of a standard structure $\mathcal{A}$ over a vocabulary τ, a numeric domain which is an initial segment of the naturals of length the size of $\mathcal{A}$, and numeric predicates. The syntax is extended with formulae of the form $(\exists ix)\phi(x)$, with i ranging over the numeric domain and x over $\mathcal{A}$, and its meaning is $|\{a\in\mathcal{A}:\phi(a)\}|\geq i$. Moreover, the quantifier $(\exists!ix)$ is used to denote that there exists exactly i x:

$$(\exists!ix)\phi(x):=(\exists ix)\phi(x)\wedge\neg(\exists i+1x)\phi(x).$$

We can also have quantifiers bounding the numeric elements and acting on numeric predicates. So, for example, in a vocabulary for graphs $\tau=\{E\}$, one can express that a vertex x has odd degree by the formula in FO(COUNT):

$$ODD(x):=(\exists i)(\forall j)((j+j\neq i)\wedge(\exists!iy)E(x,y)).$$

We have the following fact (see [16, Prop. 12.16]):

THEOREM 2.2
Over ordered structures, $FO(COUNT)=TC^0$.

3 The logic of finite residue classes and circuit complexity

We use $\mathbb{Z}$ to denote the integers, $\mathbb{R}$ for the reals and $\mathbb{P}$ to denote the set of prime numbers. For integers a, b and d, $b \equiv_d a$ denotes that b is congruent to a modulo d, and (a, b) stands for the greatest common divisor of a, b. For each $m \in \mathbb{Z}$, $m > 0$, we denote by $\mathbb{Z}_m$ the finite residue class of m elements. As an algebraic structure $\mathbb{Z}_m$ consists of a set of elements $\{0, 1, \ldots, m-1\}$, and two binary functions $+$ and $\times$ which corresponds to addition and multiplication modulo m, respectively.

DEFINITION 3.1
By $\mathcal{R}es(0, +, \times)$ we denote the logic of finite residue classes. This is the set of first-order sentences over the built-in predicates $\{0, +, \times\}$, where 0 is a constant symbol, and $+$ and $\times$ are binary function symbols. The models of $\mathcal{R}es(0, +, \times)$ are the finite residue classes $\mathbb{Z}_m$, and in each $\mathbb{Z}_m$, the 0 is always interpreted as the 0-th residue class (mod m), and $+$ and $\times$ are addition and multiplication modulo m.

By $\mathcal{R}es(0, +, \times, <)$ we denote the logic $\mathcal{R}es(0, +, \times)$ further extended with an additional (built-in) order relation $<$. In this extension, each finite ring $\mathbb{Z}_m$ is endowed with an order of its residue classes, given by the natural ordering of the representatives of each class from $\{0, 1, \ldots, m-1\}$. Also, in this case, the constant 0 represents the first element in this order.

We can further extend $\mathcal{R}es(0, +, \times)$ or $\mathcal{R}es(0, +, \times, <)$ with modular quantifiers and the majority quantifier.

DEFINITION 3.2
For every integer $q > 0$, we denote by $\mathcal{R}es(0, +, \times) + \mathrm{MOD}(q)$ and $\mathcal{R}es(0, +, \times, <) + \mathrm{MOD}(q)$ the extensions of the logics $\mathcal{R}es(0, +, \times)$ and $\mathcal{R}es(0, +, \times, <)$ obtained by the additional requirement that these logics be closed, for every $r = 0, 1, \ldots, q-1$, for the quantifiers $\exists^{(r,q)}x$, interpreted in $\mathbb{Z}_m$ as in $(G1)$ of Section 2.2.

We define $\mathcal{R}es(0, +, \times) + \mathrm{MOD} = \mathcal{R}es(0, +, \times) + \bigcup_{q>0} \mathrm{MOD}(q)$ and $\mathcal{R}es(0, +, \times, <) + \mathrm{MOD} = \mathcal{R}es(0, +, \times, <) + \bigcup_{q>0} \mathrm{MOD}(q)$. Finally, we denote by $\mathcal{R}es(0, +, \times) + \mathrm{MOD} + \mathrm{M}$ and $\mathcal{R}es(0, +, \times <) + \mathrm{MOD} + \mathrm{M}$ the extensions of the logic $\mathcal{R}es(0, +, \times) + \mathrm{MOD}$ and $\mathcal{R}es(0, +, \times, <) + \mathrm{MOD}$ obtained by the additional requirement that these logics be closed for the majority quantifier $\mathrm{M}z$, interpreted in $\mathbb{Z}_m$ as in $(G2)$ of Section 2.2.

In the presence of a built-in order relation it is logically indistinct to work with the standard finite models $\mathcal{A}_m$ or with the finite residue classes $\mathbb{Z}_m$. This is the contents of the following theorem whose proof can be found in [2].

THEOREM 3.3
For every formula $\phi(x_1, \ldots, x_k)$ of $\mathrm{FO}(\leq, \oplus, \otimes)$, there exists a formula $\Phi(x_1, \ldots, x_k)$ of $\mathcal{R}es(0, +, \times, <)$ such that for every finite structure $\mathcal{A}_m$ and integers $a_1, \ldots, a_k < m$,

$$\mathcal{A}_m \models \phi(a_1, \ldots, a_k) \text{ if and only if } \mathbb{Z}_m \models \Phi(a_1, \ldots, a_k).$$

Conversely, for every formula $\phi(x_1, \ldots, x_k)$ of $\mathcal{R}es(0, +, \times, <)$, there exists a formula $\Phi(x_1, \ldots, x_k)$ of $\mathrm{FO}(\leq, \oplus, \otimes)$ such that for every finite structure $\mathbb{Z}_m$ and integers $a_1, \ldots, a_k < m$,

$$\mathbb{Z}_m \models \phi(a_1, \ldots, a_k) \text{ if and only if } \mathcal{A}_m \models \Phi(a_1, \ldots, a_k).$$

The result also applies to the respective extensions of the logics with modular quantifiers and the majority quantifier.

REMARK 3.4
Definability (or expressibility) in the logic of finite residue classes is given in terms of the finite residue structures $\mathbb{Z}_m$. That is, whenever we say that a property of integers $P(x)$ is definable in $\mathcal{R}es(0,+,\times,<)$+MOD+M, or any fragment $\mathcal{L}$ thereof, we mean that there exists a sentence φ of $\mathcal{L}$ such that for every natural m,

$$P(m) \text{ holds in } \mathbb{Z} \Longleftrightarrow \mathbb{Z}_m \models \varphi.$$

For a given circuit class $\mathcal{C}$, we say that it is definable in the logic of residue classes $\mathcal{L}$, if every property $P(x)$ decidable in $\mathcal{C}$ is definable in $\mathcal{L}$ and, for every sentence φ in $\mathcal{L}$, the set of natural numbers m such that $\mathbb{Z}_m \models \varphi$ is decidable in $\mathcal{C}$.

As a consequence of the logical equivalence in Theorem 3.3, any separation result proved for fragments of $\mathcal{R}es(0,+,\times,<)$+MOD+M can be translated into a corresponding separation result in fragments of FO$(\leq,\oplus,\otimes)$+MOD+M, with the respective implications to circuit complexity. Moreover, since modular quantifiers are definable in terms of majority quantifier in the presence of built-in linear order, so just as we write FO$(\leq,\oplus,\otimes)$+M instead of FO$(\leq,\oplus,\otimes)$+MOD+M, we will from now on write $\mathcal{R}es(0,+,\times,<)$+M instead of $\mathcal{R}es(0,+,\times,<)$+MOD+M.

Thus, from Theorem 3.3 and Theorem 2.1 we have the following definability of uniform circuit classes in the logics of residue classes.

THEOREM 3.5

(1) DLOGTIME-uniform AC^0 is definable by $\mathcal{R}es(0,+,\times,<)$.
(2) DLOGTIME-uniform ACC(q) is definable by $\mathcal{R}es(0,+,\times,<)$+MOD$(q)$, for every natural q.
(3) DLOGTIME-uniform ACC is definable by $\mathcal{R}es(0,+,\times,<)$+MOD.
(4) DLOGTIME-uniform TC^0 is definable by $\mathcal{R}es(0,+,\times,<)$+M.

Our purpose is to work in the theory of $\mathcal{R}es(0,+,\times,<)$ to exploit many algebraic properties and results of residue classes, and in particular of finite fields.

4 The prime spectrum of a sentence and systems of polynomial congruences

DEFINITION 4.1
The prime spectrum of a sentence σ of $\mathcal{R}es(0,+,\times,<)$+M is defined as the set of primes $Sp(\sigma) = \{p \in \mathbb{P} : \mathbb{Z}_p \models \sigma\}$.

The set $Sp(\sigma)$ was introduced by James Ax in connection with his proof of decidability of the theory of finite fields [4]. In particular, Ax proved the following:

THEOREM 4.2 ([4])
The spectrum $Sp(\sigma)$ of any sentence σ of $\mathcal{R}es(0,+,\times)$ is, up to finitely many primes, a Boolean combination of sets of the form $Sp(\exists t(f(t)=0))$, where $f(t) \in \mathbb{Z}[t]$ is a polynomial with integer coefficients.

Therefore to characterize the spectra of sentences of $\mathcal{R}es(0,+,\times)$ it is sufficient to analyze the spectra of sentences of the form $\exists x(f(x)=0)$ for polynomials $f \in \mathbb{Z}[x]$. Given a polynomial $f(x) \in \mathbb{Z}[x]$ we will indistinctly denote $Sp(f)$ or $Sp(\exists x(f(x)=0))$ the spectrum of the sentence $\exists x(f(x)=0)$. A basic result of Schur states that every non constant polynomial has an infinite number of prime divisors; that is, $Sp(f)$ is infinite for any $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$ (see [13, Thm. 1] for an elementary proof of this fact).

Thus, we have

THEOREM 4.3
For any $f \in \mathbb{Z}[x] \setminus \mathbb{Z}$, $Sp(f)$ is infinite.

In what follows, we say that two spectra are *almost equal* (or essentially the same) if they coincide in all but a finite number of primes, and we denote this by $Sp(f) =^* Sp(g)$. Moreover, we denote by $Sp(\sigma) \subseteq^* Sp(\theta)$ the fact that *almost all* of $Sp(\sigma)$ is contained in $Sp(\theta)$ (i.e. all but a finite number of primes).

The following result from [13] will be useful for obtaining further properties of spectra, by exploiting the relation between irreducible polynomials and algebraic finite extensions of the rational field $\mathbb{Q}$. (These extensions can be defined by adjoining to $\mathbb{Q}$ a root of a polynomial irreducible over $\mathbb{Q}$. Such a root is called a *primitive element* of the extension.)

THEOREM 4.4 ([13, Thm. 2])
Let $\mathbb{Q}$ be the rational field and $f(x)$ and $g(x)$ two non-constant irreducible polynomials in $\mathbb{Q}[x]$. If R and S are algebraic extensions of $\mathbb{Q}$ such that $R \subseteq S$, f has a root which is a primitive element of R and g has a root which is a primitive element of S, then $Sp(g) \subseteq^* Sp(f)$.

Using Theorem 4.4 we can prove that the intersection of prime spectra of polynomial congruences contains a prime spectrum of some polynomial congruence, and hence it is also infinite.

THEOREM 4.5
If $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x] \setminus \mathbb{Z}$ are irreducible polynomials, then there is $g(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ such that

$$Sp(g) \subseteq^* Sp(f_1) \cap Sp(f_2) \cap \ldots \cap Sp(f_k).$$

PROOF. We set $k=2$, the general case follows by induction. Let α_1 and α_2 be zeros of f_1 and f_2 respectively in $\overline{\mathbb{Q}}$ (the algebraic closure of the rationals). Consider the algebraic extensions $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$. Then the composite field $\mathbb{Q}(\alpha_1, \alpha_2)$ is also a finite simple extension of $\mathbb{Q}$, for which a primitive element $\alpha \in \overline{\mathbb{Q}}$ exists (e.g. such α can be taken as $\alpha = \alpha_1 + q\alpha_2$ for a suitable chosen integer q). Consequently, $\mathbb{Q}(\alpha_1, \alpha_2) \subseteq \mathbb{Q}(\alpha)$, and let $g(x) \in \mathbb{Z}[x]$ be an irreducible polynomial with $g(\alpha) = 0$. Then $\mathbb{Q}(\alpha_1) \subseteq \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha_2) \subseteq \mathbb{Q}(\alpha)$, and by Theorem 4.4, $Sp(g) \subseteq^* Sp(f_1)$ and $Sp(g) \subseteq^* Sp(f_2)$. The result now follows. ■

5 From systems of polynomial congruences to sets of congruent integers

EXAMPLE 5.1
From the Quadratic Reciprocity Law [21, Ch. IV], the prime spectrum of the sentence $\exists x(x^2+1=0)$ is almost identical to the set $\{p \in \mathbb{P} : p \equiv_4 1\}$, i.e.

$$Sp\Big(\exists x(x^2+1=0)\Big) =^* \{p \in \mathbb{P} : p \equiv_4 1\}.$$

This number theoretical characterization of the solution set of certain Diophantine equations is part of a large body of knowledge within algebraic number theory, from where we obtain several tools to classify the spectra of residue classes formulae. As a further illustration of this point consider the following basic relation between prime spectra and sets of congruent integers, given by the prime divisors of the nth cyclotomic polynomial $F_n(x)$, and shown in [21, Thm. 94, p. 164]. The polynomial $F_n(x)$ is the irreducible monic polynomial whose roots are the primitive nth roots of unity.

THEOREM 5.2
For $n>1$, let $F_n(x)$ be the n-th cyclotomic polynomial. Then $Sp(F_n) =^* \{p \in \mathbb{P} : p \equiv_n 1\}$.

This result implies that, for each $n>1$, the set $\{p \in \mathbb{P} : p \equiv_n 1\}$ is definable in the theory of finite residue classes by the elementary sentence $\exists x(F_n(x)=0)$. This does not goes through for any congruence of the form $p \equiv_n r$, for $r>1$, as we show below.

COROLLARY 5.3
For integers $n>2$ and $1<r<n$, the set of prime numbers $\{p \in \mathbb{P} : p \equiv_n r\}$ is not the prime spectrum of an irreducible polynomial over a field.

Furthermore, for two integers $n, m > 1$ and $1<r<n$, $1<t<m$, the union $\{p \in \mathbb{P} : p \equiv_n r\} \cup \{p \in \mathbb{P} : p \equiv_m t\}$ cannot be the prime spectrum of a polynomial over a field.

PROOF. If for some irreducible polynomial $g(x)$ over a field K, we have

$$\{p \in \mathbb{P} : p \equiv_n r\} =^* Sp(g),$$

then considering the nth cyclotomic polynomial $F_n(x)$ over K, we have

$$\{p \in \mathbb{P} : p \equiv_n r\} \cap \{p \in \mathbb{P} : p \equiv_n 1\} =^* Sp(g) \cap Sp(F_n).$$

But the intersection on the left-hand side of the above equality is empty, while the intersection on the right-hand side is infinite by Theorem 4.5, and we have a contradiction. To prove the second statement repeat the previous argument with the nth and the mth cyclotomic polynomials together. ■

The next example shows that the unrepresentability of a spectrum by congruences, stated in Corollary 5.3, does not hold in general for Boolean combinations of spectra.

EXAMPLE 5.4
Consider the polynomials $f(x)=x^2+1$ and $g(x)=x^2-2$. Using the Quadratic Reciprocity Law we can see that $Sp(f)=\{p \in \mathbb{P} : p=2 \vee p \equiv_8 1 \vee p \equiv_8 5\}$ and $Sp(g)=\{p \in \mathbb{P} : p=2 \vee p \equiv_8 1 \vee p \equiv_8 7\}$. Now, $Sp(g)^c=\{p \in \mathbb{P} : p \equiv_8 3 \vee p \equiv_8 5\}$, and

$$Sp(g)^c \cap Sp(f) = \{p \in \mathbb{P} : p \equiv_8 5\}.$$

We now jump to a more definitive result in this line of research on sets of primes determined by polynomial congruences. Lagarias in [19] considered the sets $\Sigma(S)$ of prime divisors of systems S of polynomial congruences, and the Boolean algebra $\mathcal{B}$ generated by these sets. The Boolean algebra $\mathcal{B}$ corresponds to the collection of spectra of sentences in $\mathcal{R}es(0, +, \times)$ which, by Theorem 4.2, collapses to the Boolean algebra generated by sets $\Sigma(S)$ where the polynomials in S are restricted to have at most 1 variable. Lagarias gave the following characterization of the sets of integer congruences $\{p \in \mathbb{P} : p \equiv_d a\}$, for given positive integers d and a, that are in $\mathcal{B}$.

THEOREM 5.5 ([19, Thm. 1.4])
For any pair of integers a and d, the set $\{p \in \mathbb{P} : p \equiv_d a\}$ is in the Boolean algebra $\mathcal{B}$ if and only if a is of order 1 or 2 in $\mathbb{Z}_d$ (i.e. $a \equiv_d 1$ or $a^2 \equiv_d 1$), or $(a,d)>1$.

Rephrasing this theorem in terms of spectra of sentences we obtain the following result.

THEOREM 5.6
For any pair of positive integers a and d, with $1<a<d$, the set $\{p \in \mathbb{P} : p \equiv_d a\}$ is the spectrum of a sentence in $\mathcal{R}es(0, +, \times)$ if and only if $a^2 \equiv_d 1$ or $(a,d)>1$.

This theorem allow us to show some undefinability results. Any set of the form $\{p\in\mathbb{P}:p\equiv_d a\}$, for $1<a<d$, $(a,d)=1$ and $a^2\not\equiv_d 1$, is not the spectrum of some sentence of $\mathcal{R}es(0,+,\times)$. For example, $\{p:p\equiv_5 2\}$ is not in the spectra of residue class sentences. On the other hand observe that $5^2=25\equiv_8 1$, and according to the theorem the set $\{p:p\equiv_8 5\}$ is the spectrum of some sentence of $\mathcal{R}es(0,+,\times)$, a fact we already knew from explicit calculations in Example 5.4. We show in the next subsections that these sets of primes are definable in the extension of $\mathcal{R}es(0,+,\times)$ with modular quantifiers, and in the ordered extension; hence separating $\mathcal{R}es(0,+,\times)$ from these logical extensions.

5.1 *The spectra of sentences in* $\mathcal{R}es(0,+,\times)+\mathrm{MOD}$

Remark 5.7
In $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$ we have that $\forall a<d$,

$$Sp\left(\exists^{a,d}(x=x)\right)=^{*}\{p\in\mathbb{P}:p\equiv_d a\}.$$

Therefore, by Theorem 5.6, if we can find for every d an $1<a<d$ that is relatively prime to d, and such that $a^2\not\equiv_d 1$, then we have a set of primes definable in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$ that is not definable in $\mathcal{R}es(0,+,\times)$. The question is: *for which natural numbers d does there exist $1<a<d$, relatively prime to d and such that $a^2\not\equiv_d 1$?* To answer this question we look first at the prime numbers. Fix $p\in\mathbb{P}$. Note first that if there exists $a<p$ with $a^2\not\equiv_p 1$ then for every α, $a^2\not\equiv_{p^\alpha} 1$. Note now that for every prime $p>3$ we have that $2^2=4\not\equiv_p 1$. Hence, for any prime $p>3$ and any α we have that $(2,p)=1$ and $2^2\not\equiv_{p^\alpha} 1$.

Consider now an arbitrary integer d and its prime decomposition: $d=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$. If one of the p_i is greater than 3 then $(2,p_i)=1$ and $2^2\not\equiv_{p_i^{\alpha_i}} 1$. We know that

$$\mathbb{Z}_d\cong\mathbb{Z}_{p_1^{\alpha_1}}\times\mathbb{Z}_{p_2^{\alpha_2}}\times\ldots\times\mathbb{Z}_{p_n^{\alpha_n}}.$$

Then note that the element $(1,\dots,2,\dots,1)$, with 2 in the i-th coordinate and 1 everywhere else, is relatively prime to d (the only elements that are not relatively prime to d are the ones of the form $(a_1,a_2,\dots,a_n)$ where for some i, $a_i=0$ or $a_i=p_i^\beta$ with $1<\beta<\alpha_i$. Also note that $(1,\dots,2,\dots,1)^2\not\equiv_d (1,\dots,1,\dots,1)$.

Looking now at powers of 3 and 2, note that $3^2\equiv_{2^4}9\not\equiv_{2^4}1$, and that $2^2\equiv_{3^2}4\not\equiv_{3^2}1$. Hence, for any d such that there is a prime greater than 3 that divides d, or 3^2 or 2^4 divides d, we have that there exists $a<d$ such that $(a,d)=1$ and $a^2\not\equiv_d 1$. Hence, by Theorem 5.6 for such a d, $\{p\in\mathbb{P}:p\equiv_d a\}$ is not expressible in $\mathcal{R}es(0,+,\times)$.

We summarize these remarks in the following propositions.

Proposition 5.8
For every natural number $d\neq 2^\alpha 3^\beta$, $0\leq\alpha\leq 3$, $0\leq\beta\leq 1$, there exists $a<d$ with $(a,d)=1$ and $a^2\not\equiv_d 1$.

Proposition 5.9
For every natural number $d\neq 2,3,4,6,8,12,24$ there exists $a<d$ such that there is no sentence $\theta\in\mathcal{R}es(0,+,\times)$ equivalent to $\exists^{a,d}(x=x)$. Hence, in terms of expressive power, for every $d\neq$ 2,3,4,6,8,12,24,

$$\mathcal{R}es(0,+,\times)\subsetneq\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d).$$

The problem with $d=2,3,4,6,8,12,24$ is that for each one of these d, $\forall a\in\mathbb{Z}_d$, either a and d are not relatively prime, or $a^2\equiv_d 1$. Hence for such integers we can not use the canonical counterexample above to separate $\mathcal{R}es(0,+,\times)$ from $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$. However, we have obtained the desired inexpressibility for these integers (except $d=2$), through direct combinatorial arguments.

For each one of the integer values of d listed above, the key idea is to define in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$ a set of the form $\{p : p \equiv_{nd} c\}$, such that $(c, nd)=1$ and $c^2 \not\equiv_{nd} 1$, for some integers n and $c < nd$. Then, from Theorem 5.6 we can conclude that this set is not expressible in $\mathcal{R}es(0,+,\times)$.

We are going to need some facts about power residues, and for the necessary background we refer the reader to [21, Ch. III, §34]. First, we recall that for an integer $m \neq 0$ and an integer b prime to m, if $n \geq 2$ is a natural number such that $x^n \equiv_m b$ is solvable, then one says that b is a *n-th power residue modulo m*.

The following theorem is an immediate consequence of Theorem 71 in [21].

THEOREM 5.10
Let $n \geq 2$ be a natural number and p an odd prime such that $p \equiv_n 1$. Then there are $\frac{p-1}{n}$ n-th power residues incongruent modulo p (i.e. the number of non-zero n-th powers in $\mathbb{Z}_p$ is $(p-1)/n$).

We have now a result that allows us to obtain expressibility of some sets of the form $\{p \in \mathbb{P} : p \equiv_{nd} r\}$ in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$.

THEOREM 5.11
For all natural numbers $n, d > 1$ and for every $0 \leq r < d$, there exists a sentence $\theta_{n,r}$ in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$ such that

$$Sp(\theta) =^* \{p \in \mathbb{P} : p \equiv_{nd} rn+1\}.$$

PROOF. Fix $n, d > 1$ and $0 \leq r < d$. Using theorems 5.2 and 5.10, we have that for almost all primes p,

$$\begin{aligned} p \equiv_{nd} rn+1 \quad &\text{iff} \quad p \equiv_n 1 \text{ and } \frac{p-1}{n} \equiv_d r \\ &\text{iff} \quad \mathbb{Z}_p \models \exists x (F_n(x)=0) \wedge \exists^{r,d} y \exists z (z^n = y) \end{aligned}$$

where $F_n(x)$ is the n-th cyclotomic polynomial. ■

We use Theorem 5.11 to obtain the desired inexpressibility results for $d=3$, 4, 6, 8, 12, 24:

- For $d=3$, use $n=3$ and $r=1$. Then Theorem 5.11 guarantees that $\{p \in \mathbb{P} : p \equiv_9 4\}$ is expressible in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(3)$. Furthermore, $(4,9)=1$ and $4^2 \not\equiv_9 1$ (so this set is not expressible in $\mathcal{R}es(0,+,\times)$).
- For $d=4$, use $n=4$ and $r=1$. Theorem 5.11 guarantees that $\{p \in \mathbb{P} : p \equiv_{16} 5\}$ is expressible in $\mathcal{R}es(0,+,\times)+\mathrm{MOD}(4)$. Furthermore, $(5,16)=1$ and $5^2 \not\equiv_{16} 1$.
- For $d=6$, use $n=3$ and $r=4$; for $d=8$, use $n=4$ and $r=1$; for $d=12$, use $n=3$ and $r=2$; and for $d=24$, use $n=3$ and $r=2$.

This completes the proof for all the integer values of $d > 2$. Thus, we can generalize Proposition 5.9 to obtain the following separation theorem:

THEOREM 5.12
For all integers $d > 2$, $\mathcal{R}es(0,+,\times) \subsetneq \mathcal{R}es(0,+,\times)+\mathrm{MOD}(d)$.

The remaining case, $d=2$, cannot be solved with the above ideas, and its solution is left as an open problem.

5.2 *The spectra of sentences in* $\mathcal{R}es(0,+,\times,<)$

We now apply Theorem 5.6 to show that the logic $\mathcal{R}es(0,+,\times,<)$ strictly contains $\mathcal{R}es(0,+,\times)$. As in the previous section, it is enough to show that any set of the form $\{p\in\mathbb{P}:p\equiv_d a\}$ is the spectrum of a sentence in $\mathcal{R}es(0,+,\times,<)$.

We need the following lemma which characterizes the fact that a sum $x+y$ has overflowed in $\mathbb{Z}_p$.

Lemma 5.13 (Overflow for addition)
For every prime p and positive integers $x,y<p$ we have that $\mathbb{Z}_p\models x+y<x$ if and only if $\mathbb{Z}\models x+y\geq p$.

Proof. If $\mathbb{Z}_p\models x+y<x$ then $x+y\geq p$ in $\mathbb{Z}$, otherwise we will get $x+y\geq x$.

For the other direction, if $\mathbb{Z}\models x+y\geq p$ then the actual value of $x+y$ in $\mathbb{Z}_p$ is $(x+y)-p$. Since $y<p$ we get that $\mathbb{Z}\models 0\leq(x+y)-p<x<p$ which yields $\mathbb{Z}_p\models x+y<x$. ■

Using this lemma we can define, for fixed $a<d$, the congruence $p\equiv_d a$ by a formula expressing that $dn+a=p$, for some n, and that neither dn or the partial sums $dn+k$, for $k<a$, have overflowed. We proceed to show this in the following theorem.

Theorem 5.14
For every positive integers a and d, with $a<d$, there exists a sentence θ of $\mathcal{R}es(0,+,\times,<)$, such that for every prime $p>d$,

$$p\equiv_d a \text{ if and only if } \mathbb{Z}_p\models\theta.$$

In other words, $Sp(\theta)=^*\{p\in\mathbb{P}:\ p\equiv_d a\}$.

Proof. Fix $a<d$. The sentence θ expresses that there exists a $y>1$ such that:

- $\forall z[z>0\wedge z\leq y\Rightarrow dz\geq d]$, and
- $dy+a=0$ and, for every $s<a$, $dy+s\geq dy$.

For a prime $p>d$, such that $\mathbb{Z}_p\models\theta$ we get from the first item of the sentence θ that $dy<p$ (i.e. no overflow for dy): just apply Lemma 5.13 to $dz=d+\overset{z}{\cdots}+d\geq d$, for each $z\leq y$. From the second item of θ and Lemma 5.13 applied to $dy+s\geq dy$, for $s<a$, we get that $dy+1<p$, $dy+2<p$, …, $dy+(a-1)<p$ (no overflow for the partial sums $dy+s$), and that $dy+a=p$. But this is equivalent to saying $p\equiv_d a$. ■

The previous result, together with Theorem 5.6 establishes the following fundamental difference between the logics $\mathcal{R}es(0,+,\times)$ and $\mathcal{R}es(0,+,\times,<)$:

Theorem 5.15
The logic $\mathcal{R}es(0,+,\times)$ is weaker than the logic $\mathcal{R}es(0,+,\times,<)$.

Having discerned the expressive power of $\mathcal{R}es(0,+,\times)$ with respect to its extension with modular quantifiers, on the one hand, and with order, on the other hand, the next step is to discern the differences in expressive power between $\mathcal{R}es(0,+,\times,<)$ (the logic of residue classes with order) and its possible extensions, either with modular or majority quantifiers. In this case, the manipulations of specific sets of integer congruences will be of no use, since in the presence of order or with the generalized quantifiers we can express these sets of congruences beyond those restricted by Theorem 5.5. Hence we need to introduce another tool for separating these logics, and this will be based on the analytical notion of density.

6 The density of the prime spectrum of a sentence

A way of discerning infinite sets of primes is to compare their relative sizes. For that matter, a measure of density of subsets of natural numbers will come in hand. There are various notions of density, but in this work we deal only with the *natural* and the *exponential* densities. (See the survey [14]. However, we note that our definition of density differs from [14] in that ours are relative to the set of all primes, as opposed to all natural numbers.)

Definition 6.1
For a positive real x, $\pi(x) = |\{q \in \mathbb{P} : q \leq x\}| = |\mathbb{P} \cap [1,x]|$ is the counting function of primes below x. Similarly, for a given subset $S \subset \mathbb{P}$ define $\pi_S(x) = |\{q \in S : q \leq x\}| = |S \cap [1,x]|$; and for a given sentence ψ of the logic $\mathcal{R}es(0,+,\times,<)+\mathrm{M}$ we define $\pi_\psi(x) = |\{q \in \mathbb{P} : q \leq x \wedge \mathbb{Z}_q \models \psi\}|$.

The Prime Number Theorem (PNT) states that for all $x > 0$, $\pi(x)$ is asymptotic to $x/\log x$; that is

$$\lim_{x \to +\infty} \frac{\pi(x) \log x}{x} = 1 \qquad \text{(PNT)}.$$

This is equivalent to saying that for all $\epsilon > 0$, there is $N > 0$, such that for all $x > N$, $(1-\epsilon)\dfrac{x}{\log x} < \pi(x) < (1+\epsilon)\dfrac{x}{\log x}$. In what follows we will fix $\epsilon = 1/2$ and work with the following bounds for $\pi(x)$, which hold for almost all x:

$$\frac{1}{2}\frac{x}{\log x} < \pi(x) < \frac{3}{2}\frac{x}{\log x}. \tag{1}$$

We work with a family of densities given by the following definition.

Definition 6.2
Let h be a real positive, continuous, unbounded and increasing function defined on $(0,+\infty)$. For a given non-empty set $S \subset \mathbb{P}$, the lower h-density of S is defined by

$$\underline{\delta}_h(S) = \liminf_{n \to \infty} \frac{h(\pi_S(n))}{h(\pi(n))}$$

and its upper h-density by

$$\overline{\delta}_h(S) = \limsup_{n \to \infty} \frac{h(\pi_S(n))}{h(\pi(n))}$$

If these limits are equal, i.e., $\underline{\delta}_h(S) = \overline{\delta}_h(S)$, we say that the set S has h-density, and its value is the limit $\delta_h(S) = \lim\limits_{n \to \infty} \dfrac{h(\pi_S(n))}{h(\pi(n))}$.

The basic properties of an h-density are the following

- If S is finite and non-empty then $\delta_h(S) = 0$.
- $\delta_h(\mathbb{P}) = 1$.
- If S and T are two sets of primes such that $S \subseteq T$ and both sets have h-density, then $\delta_h(S) \leq \delta_h(T)$ (monotonicity).

Two cases of h-densities are of particular interest to us. When h is the identity function we have the *natural* density, denoted as $\delta(S)$, when the limit exists, i.e.,

$$\delta(S) = \lim_{n \to \infty} \frac{\pi_S(n)}{\pi(n)}.$$

The lower and upper natural densities, $\underline{\delta}(S)$ and $\overline{\delta}(S)$, are defined accordingly taking $\limsup$ and $\liminf$. The other case of interest is when $h = \log$, then we have the *exponential* density denoted $\varepsilon(S)$ when the limit exists, i.e.,

$$\varepsilon(S) = \lim_{n\to\infty} \frac{\log(\pi_S(n))}{\log(\pi(n))}$$

and we always have the lower and upper exponential densities, $\underline{\varepsilon}(S)$ and $\overline{\varepsilon}(S)$, defined by taking $\limsup$ and $\liminf$. (The reason for the name *exponential*, given in [14] for the unrelativized version of h-density, is that the exponential density ε acts as a magnifying glass on subsets of the naturals with natural density zero.)

The following observations are useful for making further calculations.

Remark 6.3
Recall the notation $f(x) \sim g(x)$ means $f(x)$ is asymptotic to $g(x)$, this means that $\lim_{x\to+\infty} \frac{f(x)}{g(x)} = 1$. Some useful properties of $\sim$ are:

(1) If f, g, h, k are all real value functions such that $f(x) \sim g(x)$ and $h(x) \sim k(x)$ and $\lim_{x\to+\infty} \frac{f(x)}{h(x)}$ exists or is $+\infty$, then $\lim_{x\to+\infty} \frac{f(x)}{h(x)} = \lim_{x\to+\infty} \frac{g(x)}{k(x)}$.

(2) For any two real value functions $f(x)$ and $g(x)$, with $\lim_{x\to+\infty} g(x) = +\infty$, if $f(x) \sim g(x)$ then $\log f(x) \sim \log g(x)$. This can be seen from the following equalities:

$$\frac{\log\left(\frac{f(x)}{g(x)}\right)}{\log g(x)} = \frac{\log f(x) - \log g(x)}{\log g(x)} = \frac{\log f(x)}{\log g(x)} - 1.$$

As $x \to +\infty$ the first term of these equalities goes to 0, and hence $\lim_{x\to+\infty} \frac{\log f(x)}{\log g(x)} = 1$.

(3) Using the previous observations and the PNT, we have that for h the identity or the logarithm function it holds that

$$\delta_h(S) = \lim_{n\to\infty} \frac{h(\pi_S(n))}{h(\pi(n))} = \lim_{n\to\infty} \frac{h(\pi_S(n))}{h(n/\log n)}. \tag{2}$$

Observe that if a set $S \subset \mathbb{P}$ has natural density, then it has exponential density. In fact, we have a stronger result:

Theorem 6.4
If $\delta(S)$ exists and is not zero then $\varepsilon(S) = 1$.

Proof. Let $\alpha = \delta(S) = \lim_{n\to\infty} \frac{\pi_S(n)}{\pi(n)}$. Then, by the PNT, $\pi_S(n) \sim \alpha \frac{n}{\log n}$ and

$$\lim_{n\to\infty} \frac{\log(\pi_S(n))}{\log(\pi(n))} = \lim_{n\to\infty} \frac{\log\alpha + \log\frac{n}{\log n}}{\log\frac{n}{\log n}} = 1$$

using Remark (6.3). ■

The following weaker variation of the previous theorem is also useful to show that a set has exponential density 1.

PROPOSITION 6.5
Let S be an infinite set of primes and $0<r<1$ such that for almost all natural numbers n, $r<\frac{\pi_S(n)}{\pi(n)}\leq 1$. Then the exponential density of S is 1.

PROOF. Since $r<\frac{\pi_S(n)}{\pi(n)}\leq 1$ for almost all natural n and log is increasing, we have that

$$\log(r\pi(n))<\log(\pi_S(n))\leq\log(\pi(n)).$$

This implies that

$$\frac{\log r}{\log(\pi(n))}+1<\frac{\log(\pi_S(n))}{\log(\pi(n))}\leq 1$$

from which it follows that $\varepsilon(S)=1$. ■

The Chebotarev's Density Theorem (cf. [23, §5]) implies that every element of the Boolean algebra $\mathcal{B}$, namely, the class of spectra of sentences in $\mathcal{R}es(0,+,\times)$, has rational natural density, and it is 0 if and only if the set is finite. This together with Ax's result (Theorem 4.2) gives:

THEOREM 6.6
The spectrum of any sentence in $\mathcal{R}es(0,+,\times)$ has rational natural density, and this density is 0 if and only if the spectrum is finite.

We are going to prove that this is not the case for the spectra of sentences in $\mathcal{R}es(0,+,\times,<)$. We will see that there exist sentences $\sigma\in\mathcal{R}es(0,+,\times,<)$ such that the natural density of $Sp(\sigma)$ is zero, but the cardinality of $Sp(\sigma)$ is infinite. This give us another way of showing that $\mathcal{R}es(0,+,\times)$ is properly contained in $\mathcal{R}es(0,+,\times,<)$.

We begin by recalling an outstanding result by Friedlander and Iwaniec in [10] (and further extended in [11]) which shows that the polynomial $f(x,y)=x^2+y^4$ has infinitely many prime values, but the sequence of its values is "thin" in the sense that it contains fewer than t^θ integers up to t for some $\theta<1$. More specifically,

THEOREM 6.7 ([10, 11])
There are infinitely many primes p of the form $p=a^2+b^4$, for integers a and b, and the number of these primes $p<t$ is $O(t^{3/4})$.

Using this result and Equation (2), the natural density of the set of primes

$$FI:=\{p\in\mathbb{P}:p=a^2+b^4,\ a,b\in\mathbb{Z}\}$$

is $\lim_{t\to\infty}\frac{\log t}{t^{1/4}}=0$. By Theorem 6.6, such set FI cannot be the spectrum of a sentence in $\mathcal{R}es(0,+,\times)$. It remains to show that the set FI is definable in $\mathcal{R}es(0,+,\times,<)$. We will in fact show a stronger result.

THEOREM 6.8
Consider a polynomial in $\mathbb{Z}[x,y]$ of the form $f(x,y)=h(x)+g(y)$, with n the degree of h and d the degree of g. Assume that $n,d\geq 1$ and that the leading coefficients of $h(x)$ and $g(x)$ are positive. Then there is a sentence θ in $\mathcal{R}es(0,+,\times,<)$, such that for almost every m, $\mathbb{Z}_m\models\theta$ if and only if in $\mathbb{Z}$ the following property holds:

'There exists naturals $b,c<m$ such that $f(b+1,c)=m$'.

Proof. The idea is that h and g will be increasing from some threshold μ and onward, since their leading coefficients are positive. Then, for all $m>\mu$, such b and c will be characterized by a sentence in $\mathcal{R}es(0,+,\times,<)$ that says '$f(b+1,c)=0$ and $b+1<m$ is the first element greater than μ such that $f(b+1,c)<f(b,c)$'.

Note first that if $h(x)$ is a polynomial of degree $n\geq 1$ with positive leading coefficient, then for every $1\leq i\leq n$, the ith derivative of $h(x)$, $h^{(i)}(x)$, is a polynomial of degree $n-i$ with positive leading coefficient, and eventually increasing. Hence there exists a natural μ such that h, g, and $h^{(1)},h^{(2)},\ldots,h^{(n)}$ are increasing and positive in the interval $[\mu,+\infty)$ and for every $x>\mu$,

$$h(x)>h^{(1)}(x)+\frac{h^{(2)}(x)}{2!}+\ldots+\frac{h^{(n)}(x)}{n!}. \tag{3}$$

Fix a natural number $m>\mu+1$. We make the following claim.

Claim: For every pair of integers $b,c\in(\mu,m-1)$,
if $\mathbb{Z}\models h(b)+g(c)<m\leq h(b+1)+g(c)$ then in $\mathbb{Z}$:

$$h(b+1)+g(c)-m<h(b)+g(c)<m.$$

The proof of this claim is as follows. By the Taylor polynomial expansion,

$$h(b+1)=h(b)+h^{(1)}(b)+\frac{h^{(2)}(b)}{2!}+\ldots+\frac{h^{(n)}(b)}{n!}.$$

Using that $h(b)<m$ and $b>\mu$, it follows from Equation (3) that

$$\begin{aligned}h(b+1)+g(c)-m &\leq h^{(1)}(b)+\frac{h^{(2)}(b)}{2!}+\ldots+\frac{h^{(n)}(b)}{n!}+g(c)\\ &< h(b)+g(c)<m\end{aligned}$$

which is the the desired result.

Now it follows that there exists integers b,c, $\mu<b,c<m-1$ such that

$$\mathbb{Z}\models h(b)+g(c)<m\leq h(b+1)+g(c) \tag{4}$$

if and only if we have:

- $g(c)<m$,
- for every a with $\mu<a<b$, $h(a)+g(c)<h(a+1)+g(c)<m$,
- $m\leq h(b+1)+g(c)<2m$, and
- $h(b+1)+g(c)-m<h(b)+g(c)<m$.

It follows that (4) can be expressed by the following formula in $\mathcal{R}es(0,+,\times,<)$:

$$\begin{aligned}\psi(b,c) := {}&\mu<b,c<m-1\wedge h(b+1)+g(c)<h(b)+g(c)\wedge\\ &\forall a((\mu<a<b)\Rightarrow h(a)+g(c)<h(a+1)+g(c))\end{aligned}$$

which says that $b+1<m$ is the first element bigger than μ for which

$$f(b+1,c)=h(b+1)+g(c)<h(b)+g(c)=f(b,c)$$

in $\mathbb{Z}_m$. Putting together the previous observations we obtain that

$$\text{for every } m > \mu,\ \mathbb{Z}_m \models \exists b, c(\psi(b,c) \wedge f(b+1,c) = 0)$$

if and only if

$$\mathbb{Z} \models \exists b, c(\mu < b, c < m-1 \wedge f(b+1,c) = m).$$

This completes the proof of the desired result. ■

COROLLARY 6.9
$\mathcal{R}es(0,+,\times)$ is properly contained in $\mathcal{R}es(0,+,\times,<)$.

7 A sufficient condition for the existence of sets without *h*-density

Our overall goal is to classify spectra in terms of h-density; hence, a first step is to elaborate some tools to determine when a set has no h-density. We are going to canonically construct sets of primes without h-density from sequences of integers $\{s_n\}$. The idea is that certain combinatorial properties of these sequences will guarantee that the associated set of primes do not have h-density. The necessary combinatorial properties are defined around the notion of thinness of a sequence of numbers, which has been mentioned in the previous section in the intuitive form as employed by Friedlander and Iwaniec in their work [10].

DEFINITION 7.1
Let h be a real positive, continuous, unbounded and increasing function defined on $(0,+\infty)$. An increasing sequence of numbers $\{s_n\}_{n>0}$ is **h-thin** if there exists some real $r > 3$ such that for almost all n,

$$rh(\pi(s_n)) < h(\pi(s_{n+1})).$$

When h is the identity function we call the associated sequence thin.

Essentially a sequence of numbers is 'h-thin' if the distance between the number of primes below consecutive elements in the sequence, filtered through h, increases exponentially.

For the measures of density that we consider here, we focus on functions that are *eventually semi-additive* in the following sense.

DEFINITION 7.2
A function $h : \mathcal{D} \subseteq \mathbb{R} \to \mathbb{R}$ is **eventually semi-additive**, if there exists $\mu > 0$ such that for $x,\ y \in \mathcal{D}$, $x \geq y > \mu$, $h(x+y) \leq h(x) + h(y)$.

EXAMPLE 7.3
The identity function is trivially eventually semi-additive, as well as any additive function. The function $h(x) = \log x$ is eventually semi-additive, since for all $x \geq y > 2$ we have that $x + y \leq xy$, and hence

$$\log(x+y) \leq \log(xy) = \log x + \log y.$$

A similar argument applies to $\log\log x$, taking $\mu = e^2$. Hence this and other iterations of the logarithm function are eventually semi-additive.

REMARK 7.4
We have the following properties for semi-additive functions h defined on $(0,+\infty)$ that are real positive, continuous, unbounded and increasing.

(i) For all x and y such that $x > 2y > 2\mu$, where μ is the bound in Definition 7.2, we have $h(x-y) \geq h(x) - h(y)$.
Indeed, observe that $x-y > y > \mu$ and by semi-additiveness $h(x) = h(x-y+y) \leq h(x-y) + h(y)$.

(ii) If a sequence $\{s_n\}$ is h-thin then for every β, $2 < \beta < 3$, for almost all natural numbers n we have that:

$$\beta\pi(s_n) < \pi\left(s_{n+1}\right).$$

To see this, observe that by semi-additivity and the fact that h is increasing we have that , for every $x > \mu$, $h(3x) \leq 3h(x)$, so for a β, $2 < \beta < 3$, and for almost all natural numbers n,

$$h(\beta\pi(s_n)) \leq h(3\pi(s_n)) \leq 3h(\pi(s_n)) \leq h\big(\pi\left(s_{n+1}\right)\big).$$

It follows that

$$\beta\pi(s_n) \leq \pi\left(s_{n+1}\right).$$

(iii) If a sequence $\{s_n\}$ is h-thin then for almost all natural numbers $m < n$ we have that:

$$h(\pi(s_n) - \pi(s_m)) \geq h(\pi(s_n)) - h(\pi(s_m))$$

To see this, note that if a sequence $\{s_n\}$ is h-thin, then for every μ there exists a bound B_μ such that if $n > m > B_\mu$ we have by (ii) that $\pi(s_n) > 2\pi(s_m) > 2\mu$. Then apply ($i$) above to get the desired result.

For every sequence of natural numbers $\{s_n\}$ we are going to construct an associated set of primes $\mathcal{H}(\{s_n\})$, which will be instrumental in showing counterexamples to h-density for various classes of spectra.

DEFINITION 7.5
Fix an increasing sequence of natural numbers $\{s_n\}_{n\geq 0}$. The **alternating** set of primes associated with $\{s_n\}$, denoted by $\mathcal{H}(\{s_n\})$, is defined as:

$$\begin{aligned}\mathcal{H}(\{s_n\}) &= \{p \in \mathbb{P} : \exists n(s_{2n} < p < s_{2n+1})\}\\ &= \mathbb{P} \cap ((s_2, s_3) \cup (s_4, s_5) \cup \ldots \cup (s_{2n}, s_{2n+1}) \cup \ldots).\end{aligned}$$

The following theorem gives conditions on the sequence $\{s_n\}$ that guarantee that the set $\mathcal{H}(\{s_n\})$ has no h-density.

THEOREM 7.6
Let $h : (0,+\infty) \rightarrow [0,+\infty)$ be a continuous, unbounded and increasing function defined on $(0,+\infty)$. Assume additionally that h is eventually semi-additive. Let $\{s_n\}_{n>0}$ be an increasing sequence of numbers that is h-thin. Then the set of alternating primes $\mathcal{H}(\{s_n\})$ has no h-density.

PROOF. Put $\mathcal{H} = \mathcal{H}(\{s_n\})$. First note that

$$\pi_{\mathcal{H}}(s_{2n}) = \pi_{\mathcal{H}}(s_{2n-1}) + |\mathcal{H} \cap (s_{2n-1}, s_{2n})| = \pi_{\mathcal{H}}(s_{2n-1}).$$

Then using that h is increasing and the sequence is h-thin for a real $r>3$, we have for almost all n:

$$\frac{h(\pi_{\mathcal{H}}(s_{2n}))}{h(\pi(s_{2n}))}=\frac{h(\pi_{\mathcal{H}}(s_{2n-1}))}{h(\pi(s_{2n}))}\leq\frac{h(\pi(s_{2n-1}))}{h(\pi(s_{2n}))}<\frac{1}{r}.$$

Hence, $\liminf\limits_{n\to+\infty}\delta_h(\mathcal{H})\leq\frac{1}{r}$. On the other hand, by definition of $\mathcal{H}(\{s_n\})$

$$\pi_{\mathcal{H}}(s_{2n+1})\geq\pi(s_{2n+1})-\pi(s_{2n}),$$

hence, using that h is increasing, Remark 7.4 (*iii*) and the fact that $\{s_n\}$ is h-thin, we have that for almost all n:

$$\frac{h(\pi_{\mathcal{H}}(s_{2n+1}))}{h(\pi(s_{2n+1}))}\geq\frac{h(\pi(s_{2n+1})-\pi(s_{2n}))}{h(\pi(s_{2n+1}))}\geq$$
$$\frac{h(\pi(s_{2n+1}))-h(\pi(s_{2n}))}{h(\pi(s_{2n+1}))}=1-\frac{h(\pi(s_{2n}))}{h(\pi(s_{2n+1}))}>1-\frac{1}{r}.$$

Hence, since $r>3$, $\limsup\limits_{n\to+\infty}\delta_h(\mathcal{H})\geq 1-\frac{1}{r}>\frac{1}{r}$. Therefore, $\underline{\delta}_h(\mathcal{H})\neq\overline{\delta}_h(\mathcal{H})$ and the set $\mathcal{H}$ has no h-density.

■

The theorem above is useful to prove that there exists a sentence whose spectrum has no h-density: Find a sequence $\{s_n\}$ that is h-thin, and find a sentence θ such that $Sp(\theta)=\mathcal{H}(\{s_n\})$.

We conclude this section with a criteria for a sequence $\{s_n\}$ to be thin.

LEMMA 7.7
Let $\{s_n\}_{n>0}$ be a non-decreasing sequence of numbers such that for some $R>18$, for all $n>N$, $Rs_n<s_{n+1}$. Then $r\pi(s_n)<\pi(s_{n+1})$, for some $r>3$ and for almost all natural numbers n.

PROOF. Using Equation (1) and that $f(x)=x/\log x$ is strictly increasing, we get

$$R\pi(s_n)<\frac{3}{2}\frac{Rs_n}{\log\left(\frac{R}{R}s_n\right)}=\frac{3}{2\left(1-\frac{\log R}{\log(Rs_n)}\right)}\left(\frac{Rs_n}{\log(Rs_n)}\right)<3\frac{s_{n+1}}{\log s_{n+1}}<6\pi(s_{n+1}).$$

Therefore, $r\pi(s_n)<\pi(s_{n+1})$ for $r=R/6>3$. ■

8 On the density of spectra of residue class formulae with order

We use Theorem 7.6 to show the existence of a sentence in $\mathcal{R}es(0,+,\times,<)$ whose spectrum has no natural density.

THEOREM 8.1
There exists a sentence $\psi\in\mathcal{R}es(0,+,\times,<)$ such that its spectrum $Sp(\psi)$ has no natural density.

PROOF. Fix a prime $q\geq 19$ and consider the sequence $s_n=q^n$, for $n=2,3,\ldots$. It is immediate that for R such that $18<R<19$, $Rq^n<q^{n+1}$ and by Lemma 7.7 the sequence is thin for $r>3$. Then, by Theorem 7.6, the alternating set

$$\mathcal{H}(\{q^n\})=\mathbb{P}\cap\Big((q^2,q^3)\cup(q^4,q^5)\cup\cdots\cup(q^{2k},q^{2k+1})\cup\cdots\Big)\tag{5}$$

has no natural density.

We will define a sentence $\psi \in \mathcal{R}es(0,+,\times,<)$ so that for any structure $\mathbb{Z}_p$, $\mathbb{Z}_p \models \psi$ if and only if the size of the model is a prime p such that $q^{2n} < p < q^{2n+1}$, for some natural n. Then the spectrum of such sentence ψ is $Sp(\psi) = \mathcal{H}(\{q^n\})$.

From Theorem 3.3 (see [2] for details) we know that $\otimes(x,y,z)$, true multiplication in $\mathbb{Z}_m$ (i.e. $\mathbb{Z}_m \models \otimes(x,y,z)$ if and only if $\mathbb{Z} \models x \times y = z$) is expressible in $\mathcal{R}es(0,+,\times,<)$. Hence, for a given prime q, we can express in $\mathcal{R}es(0,+,\times,<)$ "*z is a power of q*" by saying that every divisor of z different from 1 must be divisible by q (this equivalence only holds if q is prime). Here is the formula:

$$EXP_q(z) := \forall x([\exists y(\otimes(x,y,z) \wedge x \neq 1] \Rightarrow [\exists w(\otimes(q,w,x)]). \tag{6}$$

We can also have a formula $EXP_{q^2}(z)$ that says '*z is a square of a power of q*':

$$EXP_{q^2}(z) := \exists x\big(\otimes(x,x,z) \wedge EXP_q(x)\big). \tag{7}$$

From these formulas we can express the property '*z is the maximal power of q in the structure*', by a formula $MAXEXP_q(z)$:

$$MAXEXP_q(z) := EXP_q(z) \wedge \forall w(w > z \Rightarrow \neg EXP_q(w)) \tag{8}$$

and the property '*z is the maximal power of q^2 in the structure*' by the formula

$$MAXEXP_{q^2}(z) := EXP_{q^2}(z) \wedge \forall w(w > z \Rightarrow \neg EXP_{q^2}(w)). \tag{9}$$

Finally, we need the sentence *PRIME* which expresses that the size of the structure is prime (it is enough to say that every element has a multiplicative inverse). We thus have, for a fixed prime $q \geq 19$,

$$\psi := PRIME \wedge \exists z\Big(MAXEXP_q(z) \wedge MAXEXP_{q^2}(z)\Big)$$

the required sentence in $\mathcal{R}es(0,+,\times,<)$ such that $Sp(\psi) = \mathcal{H}(\{q^n\})$, which has no natural density.

■

As an immediate corollary we have a third proof of the difference in expressive power of the logic of residue classes with order and without order. This result also attest to the strength of the logic $\mathcal{R}es(0,+,\times,<)$. We had conjectured in [2] that the spectrum of any sentence in $\mathcal{R}es(0,+,\times,<)$ has natural density, and had shown there that the set $\mathcal{H}(\{q^n\})$ in (5) is the spectrum of a sentence of $\mathcal{R}es(0,+,\times,<)+$MOD(2). Now, Theorem 8.1 refines that expressibility result and knocks down our conjecture. However, we believe in the following.

Conjecture 8.2
Every sentence in $\mathcal{R}es(0,+,\times,<)$ has exponential density.

In what follows we provide some evidence for this conjecture. Every sentence in the unordered fragment $\mathcal{R}es(0,+,\times)$ has exponential density. This is a consequence of the general fact that a set for which the natural density exists, it then has the exponential density, and in fact, this exponential density is always 1 (Theorem 6.4). Furthermore, all the properties that we have defined so far in $\mathcal{R}es(0,+,\times,<)$ have exponential density. In particular, the set $\mathcal{H} := \mathcal{H}(\{q^n\})$ in Theorem 8.1 has exponential density. Let us show this.

Let $w_n = \dfrac{\log \pi_{\mathcal{H}}(n)}{\log \pi(n)}$. It will be sufficient to show that $\liminf_{n \to +\infty} w_n = 1$.

First observe that, for every n, choosing m such that $q^m \leq n < q^{m+1}$, we obtain the following inequalities due to the definition of $\mathcal{H}(\{q^n\})$:

$$\pi(q^{m-1}) - \pi(q^{m-2}) \leq \pi_{\mathcal{H}}(n)$$

Hence $\dfrac{\pi_{\mathcal{H}}(n)}{\pi(n)} \geq \dfrac{\pi(q^{m-1}) - \pi(q^{m-2})}{\pi(q^{m+1})}$. Now, observe that, in general, if $1 < y < x$ then

$$\pi(x) - \pi(y) = \sum_{y<p\leq x} 1 \geq \sum_{y<p\leq x} \frac{\log p}{\log x} \geq \frac{(x-y)\log y}{\log x}.$$

Therefore, for any $z > 1$,

$$\frac{\log(\pi(x) - \pi(y))}{\log \pi(z)} \geq \frac{\log\left(\frac{x-y}{\log x}\right) + \log\log y}{\log \pi(z)}. \tag{10}$$

Additionally we will use from Equation (1) that for $z > 3$, $\frac{1}{\pi(z)} > \frac{2\log z}{3z} > \frac{1}{3z}$.

Now, putting $x = q^{m-1}$, $y = q^{m-2}$ and $z = q^{m+1}$, it follows from the previous observations that

$$\begin{aligned} w_n &\geq \frac{\log(\pi(q^{m-1}) - \pi(q^{m-2}))}{\log \pi(q^{m+1})} \geq \frac{\log\left(\frac{q^{m-1}(q-1)}{\log q^{m-1}}\right) + \log((m-2)\log q)}{\log \pi(q^{m+1})} \\ &\geq \frac{(m-1)\log q + \log(q-1) - \log((m-1)\log q) + \log((m-2)\log q)}{(m+1)\log q + \log 3} \\ &\sim \frac{m-1}{m+1} \end{aligned}$$

As n grows, m also grows and $\dfrac{m-1}{m+1} \to 1$. Therefore $\liminf_{n\to+\infty} w_n = 1$. We then have that

$$\varepsilon(\mathcal{H}(\{q^n\})) = \lim_{n\to\infty} \frac{\log \pi_{\mathcal{H}}(q^n)}{\log \pi(q^n)} = 1.$$

Here is another interesting set from number theory to witness our conjecture.

EXAMPLE 8.3
Benford's law [6] states that $\log_{10} 2$ percent of all randomly found integers have their first digit equal to 1. This has been difficult to prove formally, but it is known that the natural density of the set S_1 of all numbers which begin with 1 does not exist because the ratio $\frac{\pi_{S_1}(n)}{\pi(n)}$ varies between 1/9 and 5/9 indefinitely [9]. However, since the liminf of S_1 is 1/9 by Proposition 6.5 the exponential density $\varepsilon(S_1)$ is 1. On the other hand, the arithmetical property of beginning with a one in decimal notation is FO definable with order. This follows from the fact that exponentiation is definable with order.

We now show the existence of a sentence in $\mathcal{R}es(0,+,\times,<)+\mathrm{M}$ such that its spectrum has no exponential density. Here we need the logical description of $\mathrm{TC}^0 = \mathcal{R}es(0,+,\times,<)+\mathrm{M}$ via FO(COUNT) (see Theorem 2.2).

THEOREM 8.4
There exists a sentence $\theta \in \mathcal{R}es(0,+,\times,<)+\mathrm{M}$ such that its spectrum $Sp(\theta)$ has no exponential density.

PROOF. Fix a prime $q \geq 7$ and consider the sequence $s_n = q^{q^n}$, $n=2,3,\ldots$. We need to find $r>3$ such that $r\log\pi(s_n) < \log\pi(s_{n+1})$.

Let $4<a<q$. Then, using Equation (1),

$$\begin{aligned} a\log\pi(q^{q^n}) &< a\log\left(\frac{3}{2}\frac{q^{q^n}}{\log q^{q^n}}\right) = \log\left(\frac{3}{2}\right)^a + \log\left(\frac{q^{aq^n}}{q^{an}\log^a q}\right) \\ &< \log\left(\frac{3}{2}\right)^a + \log\left(\frac{q^{qq^n}}{q^{n+1}\log q}\right) < \log\left(\frac{3}{2}\right)^a + \log 2\pi(q^{q^{n+1}}) \end{aligned}$$

Therefore, for n large we have

$$(a-1)\log\pi(q^{q^n}) < \left(a - \frac{\log 2\left(\frac{3}{2}\right)^a}{\log\pi(q^{q^n})}\right)\log\pi(q^{q^n}) < \log\pi(q^{q^{n+1}})$$

and we have that the sequence $\{q^{q^n}\}$ is log-thin for $r=a-1>3$. Now, by Theorem 7.6, the alternating set

$$\mathcal{H}(\{q^{q^n}\}) = \mathbb{P} \cap \left((q^{q^2}, q^{q^3}) \cup (q^{q^4}, q^{q^5}) \cup \cdots \cup (q^{q^{2k}}, q^{q^{2k+1}}) \cup \cdots\right) \tag{11}$$

has no exponential density.

We need to define a sentence θ whose spectrum is the set $\mathcal{H}(\{q^{q^n}\})$. The sentence θ will be such that for any structure $\mathbb{Z}_p \models \theta$ we have that

the size of the model is a prime p with $q^{q^{2n}} < p < q^{q^{2n+1}}$, for some natural n.

We begin by producing a formula $SUPEXP_q(z)$ in FO(COUNT) that expresses '$z = q^{q^n}$ for some $n>0$'. Formally, this is equivalent to saying that

'z is a power of q and the number of powers of q below z is a power of q'

The first clause of the above conjunction have been already defined in the logic $\mathcal{R}es(0,+,\times,<)$ by the formula $EXP_q(z)$ in (6). To logically define the second clause we need the counting quantifiers. The required formula is the following:

$$\begin{aligned} SUPEXP_q(z) := {} & EXP_q(z) \wedge (\exists i)[(\exists! iy)(y<z \wedge EXP_q(y)) \\ & \wedge\ \forall j(j \neq 1 \wedge \exists k(k\cdot j = i) \rightarrow \exists h(q\cdot h = j))]. \end{aligned}$$

If we additionally require that the number i (of powers of q below z) is a square, we have a logical expression for $z = q^{q^{2n}}$. The formula is the following:

$$\begin{aligned} SUPEXP_{q^2}(z) := {} & EXP_q(z) \wedge (\exists i)[(\exists! iy)(y<z \wedge EXP_q(y)) \\ & \wedge\ \forall j(j \neq 1 \wedge \exists k(k\cdot j = i) \rightarrow \exists h(q\cdot h = j)) \wedge \exists k(k\cdot k = i)]. \end{aligned}$$

We now express the properties:

- *'z is the maximal power of the form* q^{q^n}*'*
- *'z is the maximal power of the form* $q^{q^{2n}}$*'*

with formulas $SUPMAXEXP_q(z)$ and $SUPMAXEXP_{q^2}(z)$, which are similar in their form to formulas $MAXEXP_q(z)$ and $MAXEXP_{q^2}(z)$ in (8) and (9), respectively, but using our new formulas $SUPEXP_q(z)$ and $SUPEXP_{q^2}(z)$. Then, the required sentence θ is

$$\theta := PRIME \wedge \exists z \Big(SUPMAXEXP_q(z) \wedge SUPMAXEXP_{q^2}(z) \Big).$$

This sentence belongs to FO(COUNT), hence to $\mathcal{R}es(0,+,\times,<)+$M, and its spectrum has no exponential density. ■

9 Conclusions

We have established the separation of subclasses of $\mathcal{R}es(0,+,\times,<)+$M using results from number theory, the notion of prime spectra of sentences and analysing their natural and exponential densities. We believe that the algebraic methodology employed is interesting in its own right and should be further exploited. Of particular interest to us are the following questions:

- Does every spectrum in $\mathcal{R}es(0,+,\times,<)$ has a exponential density? If that is the case, then this would separate this logic from $\mathcal{R}es(0,+,\times,<)+$M. This would constitute a proof from the perspective of class field theory of the known result

$$\text{DLOGTIME-uniform AC}^0 \neq \text{DLOGTIME-uniform TC}^0.$$

- What can be said of the spectrum of a sentence in $\mathcal{R}es(0,+,\times)+$MOD($n$) for n a positive integer? The goal here is to separate $\mathcal{R}es(0,+,\times)+$MOD($n$) from $\mathcal{R}es(0,+,\times)+$MOD($m$), for $m \neq n$ positive integers. The same separation when the built-in order is present will yield separations among the ACC(n) classes improving Smolensky results [22].
- Is $\mathcal{R}es(0,+,\times) \neq \mathcal{R}es(0,+,\times)+$MOD(2)? (cf. Theorem 5.12)
- What can be said of the spectrum of a sentence in $\mathcal{R}es(0,+,\times,<)+$M? We expect these sets to be much more untamed than the spectra of sentences in $\mathcal{R}es(0,+,\times,<)$ because of the expressive power of the majority quantifier. Thus, possibly a refined version of the exponential density is necessary to study these spectra.

Acknowledgements

The authors gratefully acknowledge the fruitful comments of the two anonymous reviewers that lead to an improvement of the original manuscript.

Funding

This work was supported by the Ministerio de Economía, Industria y Competitividad, Spain, project APCOM [TIN2014-57226-P to A. A.]; and Generalitat de Catalunya, project MACDA [SGR2014-890 to A. A.].

References

[1] M. Ajtai. Σ_1^1 formulae on finite structures. *Annals of Pure and Applied Logic*, **24**, 1–48, 1983.

[2] A. Arratia and C. E. Ortiz. First order extensions of residue classes and uniform circuit complexity. In *Logic, Language, Information and Computation, WoLLIC 2013*, Vol. 8071 of *Lecture Notes in Computer Science*, L. Libkin, ed., pp. 49–63. Springer-Verlag, 2013.

[3] J. Ax. Solving Diophantine problems modulo every prime. *Annals of Mathematics*, **85**, 161–183, 1967.

[4] J. Ax. The elementary theory of finite fields. *Annals of Mathematics*, **88**, 239–271, 1968.

[5] D. Barrington, N. Immerman and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Sciences*, **41**, 274–306, 1990.

[6] F Benford. The law of anomalous numbers. *Proceedings of the American Philosophical Society*, **78**, 551–572, 1938.

[7] R. Boppana and M. Sipser. The complexity of finite functions. In *Handbook of Theoretical Computer Science, Algorithms and Complexity*, Vol. A, J. van Leeuwen, ed., pp. 757–804. Elsevier, 1990.

[8] A. Borodin. On relating time and space to size and depth. *SIAM Journal of Computing*, **6**, 733–744, 1977.

[9] D. Cohen. An explanation of the first digit phenomenon. *Journal of Combinatorial Theory (A)*, **20**, 367–370, 1976.

[10] J. Friedlander and H. Iwaniec. Using a parity-sensitive sieve to count prime values of a polynomial. *Proceedings of the National Academy Science USA*, **94**, 1054–1058, 1997.

[11] J. Friedlander and H. Iwaniec. The polynomial x^2+y^4 captures its primes. *Annals of Mathematics*, **148**, 945–1040, 1998.

[12] M. Furst, J. B. Saxe and M. Sipser. Parity, circuits, and the polynomial time hierarchy. *Mathematical Sytems Theory*, **17**, 13–27, 1984.

[13] I. Gerst and J. Brillhart. On the prime divisors of polynomials. *American Mathematical Monthly*, **78**, 250–266, 1971.

[14] G. Grekos. On various definitions of density (survey). *Tatra Mountain Mathematical Publications*, **31**, 17–27, 2005.

[15] J. Håstad. Almost optimal lower bounds for small depth circuits. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, pp. 6–20. ACM, 1986.

[16] N. Immerman. *Descriptive Complexity*. Springer, 1998.

[17] S. Jukna. *Boolean Function Complexity: Advances and Frontiers*, Vol. 27. Springer, 2012.

[18] M. Koucky, C. Lautemann, S. Poloczek and D. Therien. Circuit lower bounds via Ehrenfeucht-Fraissé games. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pp. 190–201. IEEE, 2006.

[19] J. C. Lagarias. Sets of primes determined by systems of polynomial congruences. *Illinois Journal of Mathematics*, **27**, 224–239, 1983.

[20] L. Libkin and L. Wong. Lower bounds for invariant queries in logics with counting. *Theoretical Computer Science*, **288**, 153–180, 2002.

[21] T. Nagell. *Introduction to Number Theory*. 2nd. edn, John Wiley & Sons, Inc., 1964.

[22] R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th ACM STOC*, pp. 77–82, 1987.

[23] B. F. Wyman. What is a reciprocity law? *American Mathematical Monthly*, **79**, 571–586, 1972.

Received 14 March 2016