First Order Extensions of Residue Classes and Uniform Circuit Complexity

Argimiro Arratia

argimiro@lsi.upc.edu

LARCA. Laboratory for Relational Algorithmics, Complexity and Learning

UNIVERSITAT POLITÈCNICA DE CATALUNYA

Joint work with **Carlos E. Ortiz** (Arcadia U., USA)

ortiz@arcadia.edu

Why finite residue classes

Main goal

To develop new tools to study separation problems for a collection of logics that are extensions of first order logic and whose models are finite residue classes.

Motivations

- Limitations of working with standard finite structures with built-in linear order in Descriptive Complexity Theory.
- Separation questions in the Circuit Complexity Hierarchy. ▸ Go
- There is a deep corpus of results from number theory on residue classes.

▸ Continue

Circuit complexity hierarchy

$$AC^0 \subseteq ACC(q) \subseteq ACC \subseteq TC^0$$

$AC^0 =$ class of languages accepted by poly. size, constant depth circuits w/ NOT gates, unbounded fan-in AND, OR gates.
$ACC(q)$ = AC^0 plus MOD_q gates.
TC^0= AC^0 plus MAJ gates. ▸ Go Back

Logics $\mathcal{R}ing(0,+,*)$ and $\mathcal{R}ing(0,+,*,<)$

For $m \in \mathbb{N}$, $\mathbb{Z}_m$ is the finite residue class ring of m elements. As an algebraic structure, $\mathbb{Z}_m$ consists of set of elements $\{0, 1, \ldots, m-1\}$, constant 0 and two binary functions $+$ and $*$ (corresponding to addition and multiplication mod m).

Definition: Logic of finite residue class rings

$\mathcal{R}ing(0,+,*)$ denote the collection of first order sentences over the set of built-in predicates $\{0,+,*\}$, where 0 is a constant symbol, and $+$ and $*$ are binary function symbols. The models of $\mathcal{R}ing(0,+,*)$ are the finite residue class rings $\mathbb{Z}_m$.

Definition: Logic of finite residue class rings with order

$\mathcal{R}ing(0,+,*,<)$ denote the logic $\mathcal{R}ing(0,+,*)$ extended with a 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 $\{0, 1, \ldots, m-1\}$. The constant 0 represents the first element in this order.

Modular Quantifiers

Notation given fmla $\phi(x, \overline{y})$, structure $\mathcal{A}$ and tuple $\overline{a}$ of elements in $\mathcal{A}$, $\phi(\mathcal{A}, \overline{a}) := \{b \in \mathcal{A} : \mathcal{A} \models \phi(b, \overline{a})\}$.

Definition

For every integer $n > 0$, $\mathcal{R}ing(0, +, *) + MOD(n)$ and $\mathcal{R}ing(0, +, *, <) + MOD(n)$ are the extensions of $\mathcal{R}ing(0, +, *)$ and $\mathcal{R}ing(0, +, *, <)$ obtained by the additional requirement that these logics be closed, $\forall r < n$, for the quantifiers $\exists^{(r,n)}x$, interpreted as follows:

$$\mathbb{Z}_m \models \exists^{(r,n)} x \phi(x, \overline{a}) \text{ iff } |\phi(\mathbb{Z}_m, \overline{a})| \equiv_n r$$

$\mathcal{R}ing(0, +, *) + MOD = \bigcup_{n>0} \mathcal{R}ing(0, +, *) + MOD(n)$,
$\mathcal{R}ing(0, +, *, <) + MOD = \bigcup_{n>0} \mathcal{R}ing(0, +, *, <) + MOD(n)$.

Note: Further extensions are obtained with *Majority* quantifiers, but we would not deal with them.

Definability of Circuit Complexity Classes

Theorem

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

Remark: a property of integers $P(x)$ is definable in $\mathcal{R}ing(0,+,*,<)$, or any fragment $\mathcal{L}$, means that there exists a sentence φ of $\mathcal{L}$ such that $\forall m$, $P(m)$ holds in $\mathbb{Z} \iff \mathbb{Z}_m \models \varphi$.
Circuit class $\mathcal{C}$ is definable in the ring logic $\mathcal{L}$ if every property $P(x)$ decidable in $\mathcal{C}$ is definable in $\mathcal{L}$ and, for all sentence φ in $\mathcal{L}$, the set of natural numbers m such that $\mathbb{Z}_m \models \varphi$, is decidable in $\mathcal{C}$.

Prime Spectra of sentences

Definition

The prime spectrum of a sentence σ of $\mathcal{R}ing(0,+,*,<)+MOD$, is the set of prime numbers

$$Sp(\sigma)=\{p\in\mathbb{P}:\mathbb{Z}_p\models\sigma\}$$

Notation Two sets $A,B\subset\mathbb{N}$ are almost identical, $A=^*B$ if and only if they differ by only a finite number of elements.

Example

From the Quadratic Reciprocity Law:

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

Characterizing spectra of sentences of $\mathcal{R}ing(0, +, *)$

Theorem (James Ax, 1968, Annals Math.)

The spectrum $Sp(\sigma)$ of any sentence σ of $\mathcal{R}ing(0, +, *)$ is, up to finitely many exceptions, 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. □

Hence, to characterize the spectra of sentences of $\mathcal{R}ing(0, +, *)$ it is sufficient to analyze the spectra of sentences of the form $\exists x(f(x) = 0)$ for polynomials $f \in \mathbb{Z}[x]$.

Boolean algebra on ring spectra

Consider systems of polynomial congruences:

$$(S): \qquad f_1(x_1,\ldots,x_n) \equiv_p 0, \ldots, f_m(x_1,\ldots,x_n) \equiv_p 0$$

with $f_i \in \mathbb{Z}[x_1,\ldots,x_n]$.
Let $\Sigma(S) = \{p \in \mathbb{P} : (S)$ is solvable $\}$.
Let $\mathcal{B}$ be the Boolean algebra of subsets of $\mathbb{P}$ generated by all the sets $\Sigma(S)$, and let B_k be the Boolean algebra generated by sets $\Sigma(S)$, where the polynomials in S are restricted to have at most k variables, i.e.,

$$f_1(x_1,\ldots,x_k) \equiv_p 0, \ldots, f_m(x_1,\ldots,x_k) \equiv_p 0 \tag{1}$$

The Boolean algebra $\mathcal{B}$ corresponds to the collection of spectra of sentences in $\mathcal{R}ing(0,+,*)$ which, by Ax's Theorem, collapses to its first level B_1.

Lagarias characterization of sets of prime congruences in $\mathcal{B}$

Theorem (J. C. Lagarias, 1983, Illinois J. Math.)

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 $(a, d) > 1$ or a is of order 1 or 2 in $\mathbb{Z}_d$ (i.e. $a \equiv_d 1$ or $a^2 \equiv_d 1$) □

Rephrasing this theorem in terms of spectra of sentences we obtain:

Theorem

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 $\mathcal{R}ing(0, +, *)$ if and only if $a^2 \equiv_d 1$ or $(a, d) > 1$. □

We use this theorem to separate $\mathcal{R}ing(0, +, *)$ from $\mathcal{R}ing(0, +, *) + MOD(d)$ for d an arbitrary positive integer.

Separating $\mathcal{R}ing(0,+,*)$ from $\mathcal{R}ing(0,+,*)+MOD(d)$

Remark

In $\mathcal{R}ing(0,+,*)+MOD(d)$ we have $\forall a<d$,

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

Hence, by Lagarias, find for every d an $1<a<d$ such that $(a,d)=1$, and $a^2\not\equiv_d 1$
Then we have a set of primes definable in $\mathcal{R}ing(0,+,*)+MOD(d)$ that is not definable in $\mathcal{R}ing(0,+,*)$.

Separation result for $\mathcal{R}ing(0,+,*) + MOD(n)$

Remark

For every natural number $n \neq 2^\alpha 3^\beta$*,* $0 \leq \alpha \leq 3$*,* $0 \leq \beta \leq 1$ *there exists* $a < n$ *with* $gcd(a,n) = 1$ *and* $a^2 \not\equiv_n 1$*.*

Theorem

For every natural number $n \neq 2,3,4,6,8,12,24$ *there exists* $a < n$ *such that there is no sentence* $\theta \in \mathcal{R}ing(0,+,*)$ *equivalent to* $\exists^{a,n}(x = x)$*.*

Hence, in terms of expressive power, for every $n \neq 2,3,4,6,8,12,24$*,* $\mathcal{R}ing(0,+,*) \subsetneq \mathcal{R}ing(0,+,*) + MOD(n)$*.*

Note The above theorem can be extended to $n = 2,3,4,6,8,12,24$

Asymptotic analysis: Density of prime spectra

Notation: $\pi_S(t) = |\{p \in S : p < t\}|$, $\pi(t) = |\{p \in \mathbb{P} : p < t\}|$

Natural density

For $S \subset \mathbb{P}$, the *natural density* of S is

$$\delta(S) = \lim_{t\to\infty} \frac{\pi_S(t)}{\pi(t)} = \lim_{t\to\infty} \frac{|\{p \in S : p < t\}|}{|\{p \in \mathbb{P} : p < t\}|}$$

Observations: 1) If S is finite then $\delta(S) = 0$
2) If $S =^* T$ then $\delta(S) = \delta(T)$
3) Using the Prime Number Thm $\left(\lim_{t\to\infty} \frac{\pi(t)}{t/\ln t} = 1\right)$,
$\delta(S) = \lim_{t\to\infty} \left(\frac{\ln t}{t}\right) \cdot |\{p \in S : p < t\}|$

Example (From Dirichlet's Thm & Quadratic Reciprocity Law)

$$\delta\left(Sp\left(\exists x(x^2 + 1 = 0)\right)\right) = \delta\left(\{p \in \mathbb{P} : p \equiv_4 1\}\right) = \frac{1}{2}$$

Density of $\mathcal{R}ing(0, +, *)$ spectra

Theorem (Weak Cĕbotarev Theorem)

If $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ of degree n, then $\delta(Sp(f)) = 1/n$. □

Corollary

Every element of the Boolean algebra B_1 has rational density, and it is 0 if and only if the set is finite.

Put together with Ax's Thm to obtain:

Theorem

The spectrum of any sentence in $\mathcal{R}ing(0, +, *)$ has rational density, and this density is 0 if and only if the spectrum is finite. □

Infinite spectrum, zero density in $\mathcal{R}ing(0, +, *, <)$

The set of primes

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

is infinite and has density $\delta(FI) = 0$. This follows from

Theorem (Friedlander and Iwanec, 1997)

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 $O(t^{3/4})$. (Hence, $\delta(FI) = \lim_{t\to\infty} \frac{\ln t}{t^{1/4}} = 0$) □

By Thm on spectra of ring (w/o order), FI can not be the spectrum of a sentence in $\mathcal{R}ing(0, +, *)$.

We show that FI is definable in $\mathcal{R}ing(0, +, *, <)$.

FI is definable in $\mathcal{R}ing(0,+,*,<)$

Theorem

For every polyn. $f(x,y) = h(x) + g(y) \in \mathbb{Z}[x,y]$ *there exists a sentence* $\phi_f \in \mathcal{R}ing(0,+,*,<)$ *s.t. for all* m*:*
$\mathbb{Z}_m \models \phi_f \iff$ *“m is prime and $\exists a, c < m$ s.t. $f(a,c) = m$”.* □

Theorem

$\mathcal{R}ing(0,+,*)$ *is properly contained in* $\mathcal{R}ing(0,+,*,<)$*.* □

On spectra without density

Theorem

There are sentences in $\mathcal{R}ing(0, +, *, <) + MOD$ whose spectrum has no density.

Proof sketch:

- There exists sentence θ in $\mathcal{R}ing(0, +, *, <)$ that is *thin* $\equiv$ the distance between consecutive primes in the spectrum increases exponentially.
- Using θ, let ψ be the statement: "The size of the model is a prime q and the number of primes $p < q$ such that $\mathbb{Z}_p \models \theta$ is even".
- ψ is expressible in $\mathcal{R}ing(0, +, *, <) + MOD(2)$
  Note: ψ asserts a property of $\mathbb{Z}_p$ for $p < q$. We need to code the modular semantics of $\mathcal{R}ing(0, +, *, <)$ within itself (Coding Thm.)

On spectra without density

Proof sketch:

- Coding Thm: For all $\varphi(\bar{x})$ in $\mathcal{R}ing(0,+,*,<)$ there exists a fmla $TRAN_\varphi(\bar{x},y)$ in $\mathcal{R}ing(0,+,*,<)$ s.t. $\forall q$, $\forall p < q$, $\forall \bar{a} < q$, $\mathbb{Z}_p \models \varphi(\bar{a}) \iff \mathbb{Z}_q \models TRAN_\varphi(\bar{a},p)$.
  Then
  $$\psi := PRIME \wedge \exists^{0,2} y\,(TRAN_\theta(y) \wedge TRAN_{PRIME}(y))$$
- Density of $Sp(\psi)$ does not exists.
  Intuition: the increasing sequence of all primes alternates between intervals of exponential length where any prime in it satisfies ψ, followed by intervals of exponential length where no prime in it satisfies ψ. Thus the $\limsup$ of $\delta(Sp(\psi))$ is strictly greater than $1/2$ but the $\liminf$ is strictly less than $1/2$.

Want more details? (continue or jump to ▸ CONCLUSIONS)

Details of no density for some modular spectrum

Definition (Thin spectrum)

θ in $\mathcal{R}ing(0,+,*,<) + MOD$ has a thin spectrum if $|Sp(\theta)| = \omega$ and $\exists\ r \geq 2$ s.t. on a list of elements of $Sp(\theta)$: $p_1 < p_2 < \ldots < p_n < \ldots$, we have $\forall^* n$, $rp_n < p_{n+1}$.

$\theta \in \mathcal{R}ing(0,+,*,<)$ thin

For q prime, let $FIRSTPRIME_q$ be the property:

> *The cardinality of the structure is a prime number p and, if $q^k < p < q^{k+1}$ for some positive integer k, then there is no prime h such that $q^k < h < p$.*

This is def. in $\mathcal{R}ing(0,+,*,<)$ since "x is a power of y" (i.e., usual exp. in $\mathbb{Z}$) is definable.
For $q > 6$, $FIRSTPRIME_q$ has thin spectrum. □

ETC ETC

Conclusions

Recap: We have established tools for discerning expressive power of subclasses of $\mathcal{R}ing(0,+,*,<) + MOD$ from: number theory, prime spectra of sentences and natural density.

- (J. Ax) $Spectra(\mathcal{R}ing(0,+,*)) = Bool(Sp(\exists t(f(t)=0)))$.
- $\forall 1 < a < d$, $\{p \in \mathbb{P} \,:\, p \equiv_d a\} \in Spectra(\mathcal{R}ing(0,+,*)) \iff a^2 \equiv_d 1$ or $(a,d) > 1$.
- $\forall n > 1$, $\mathcal{R}ing(0,+,*) \subsetneq \mathcal{R}ing(0,+,*) + MOD(n)$.
- Spectra of $\mathcal{R}ing(0,+,*)$ has rational density, and is $0 \iff$ the spectrum is finite.
- $\exists$ set definable in $\mathcal{R}ing(0,+,*,<)$, infinite and density 0
- $\mathcal{R}ing(0,+,*) \subsetneq \mathcal{R}ing(0,+,*,<)$.
- $\mathcal{R}ing(0,+,*,<) + MOD$ has sentences whose spectrum has no density.

Conclusions

Some open problems:

- Does every spectrum in $\mathcal{R}ing(0, +, *, <)$ has a density? If so, then this logic differs from $\mathcal{R}ing(0, +, *, <) + MOD(2)$ This has important implications to circuit complexity :

  $$DLOGTIME\text{-uniform } AC^0 \neq DLOGTIME\text{-uniform } ACC(2),$$

- Characterize the spectra of sentences in $\mathcal{R}ing(0, +, *) + MOD(n)$. The goal is to separate $\mathcal{R}ing(0, +, *) + MOD(n)$ from $\mathcal{R}ing(0, +, *) + MOD(m)$, for $m \neq n$ positive integers.
- Characterize the spectra of sentences in $\mathcal{R}ing(0, +, *, <) + Maj$. Here might need a different concept from natural density to study these spectra.

This is the END