PRIME CONGRUENCES OF IDEMPOTENT SEMIRINGS AND A NULLSTELLENSATZ FOR TROPICAL POLYNOMIALS

Kalina Mincheva
(joint work with Dániel Joó)
Johns Hopkins University,
Baltimore, MD, mincheva@math.jhu.edu

SUMMARY

- We give a new definition of **prime congruences** in additively idempotent semirings. These congruences have analogous properties to the prime ideals of commutative rings.
- A **complete description of prime congruences** is given in the polynomial and Laurent polynomial semirings over the tropical semifield $\mathbb{R}_{max}$ and the semifields $\mathbb{Z}_{max}$ and $\mathbb{B}$.
- The **minimal primes** of these semirings correspond to monomial orderings, and their intersection is the congruence that identifies polynomials that have the same Newton polytope.
- The **Krull dimension** of the (Laurent) polynomial semiring in n variables over K (where K one the three studied semifields above) is equal to $dim(K) + n$.
- The radical of every finitely generated congruence in the studied cases is the intersection of prime congruences with quotients of dimension 1.
- An improvement of a result by A. Bertram and R. Easton is proven which can be regarded as a **Nullstellensatz for tropical polynomials**.

CONGRUENCES OF IDEMPOTENT SEMIRINGS

Motivation: For the traditional tropical geometry (e.g. Sturmfels, MacLagan, Mikhalkin) a tropical variety (over $\mathbb{R}_{max}$) is a balanced polyhedral complex. But recently there has been a lot of work aiming at finding the appropriate definition of a tropical scheme.

Ideals of semirings do not fulfill the same role as in ring theory since they are no longer in bijection with the congruences of the base structure.

Definition: A **semiring** is a nonempty set R with two binary operations $(+, \cdot)$ such that R is a commutative monoid with respect to both (usual distributivity and unit axioms hold). A **semifield** is a semiring in which all nonzero elements have multiplicative inverse. Examples are:

- $\mathbb{B}$ the semifield with two elements $\{1, 0\}$, $1 + 1 = 1$.
- The **tropical semifield** $\mathbb{R}_{max}$ with underlying set $\{-\infty\} \cup \mathbb{R}$, addition being the usual maximum and multiplication the usual addition, with $-\infty$ playing the role of the 0 element.
- The semifield $\mathbb{Z}_{max}$ is just the subsemifield of integers in $\mathbb{R}_{max}$.

All of these are $\mathbb{B}$-**algebras** i.e. additively idempotent semirings with multiplicative unit (R is **idempotent** if $a + a = a$, $\forall a \in R$).

Definition: The **twisted product** of two ordered pairs (a, b) and (c, d) is the ordered pair $(ac + bd, ad + bc)$.

Motivation: Congruences whose quotients are cancellative i.e. $ab = ac$ implies $a = 0$ or $b = c$ generally fail to be intersection indecomposable.

Definition: A congruence P of a $\mathbb{B}$-algebra A **prime** if it is proper and for every $\alpha, \beta \in A \times A$ such that $\alpha\beta \in P$ either $\alpha \in P$ or $\beta \in P$.

THEOREM

A congruence I is prime if and only if it has cancellative quotient and is intersection indecomposable.

Definition: The **radical** of a congruence I is the intersection of all prime congruences containing I. It is denoted by $Rad(I)$. A congruence I is called a **radical congruence** if $Rad(I) = I$.

Definition:

- We denote **trivial congruence** of a semiring by Δ.
- For a pair $\alpha = (\alpha_1, \alpha_2)$ from the $\mathbb{B}$-algebra A, the **generalized powers** of α are the pairs of the form $(((\alpha_1 + \alpha_2)^k, 0) + (c, 0))\alpha^l$ where k, l are non-negative integers, and $c \in A$ an arbitrary element.
- The set of generalized powers of α is denoted by $GP(\alpha)$. A pair α is called **nilpotent** if some generalized power of α is in Δ.

THEOREM

For a congruence I of a $\mathbb{B}$-algebra A, $Rad(I) = \{\alpha \mid GP(\alpha) \cap I \neq \emptyset\}$. In particular the intersection of every prime congruence of A is precisely the set of nilpotent elements.

PRIME CONGRUENCES OF IDEMPOTENT SEMIRINGS

- Quotients by a prime are totally ordered with respect to the ordering coming from the idempotent addition.
- For a prime P of $\mathbb{B}(\boldsymbol{x})$ (resp. $\mathbb{B}[\boldsymbol{x}]$) the multiplicative monoid of $\mathbb{B}(\boldsymbol{x})/P$ (resp.$\mathbb{B}[\boldsymbol{x}]/P$) is isomorphic to a quotient of the additive group $(\mathbb{Z}^n, +)$ (resp. to the restriction of a quotient $(\mathbb{Z}^{n'}, +)$ to $(\mathbb{N}^{n'}, +)$, where $n - n' = |\{x_1, \dots, x_n\} \cap Ker(P)|$).
- To understand the prime quotients of $\mathbb{B}(\boldsymbol{x})$ and $\mathbb{B}[\boldsymbol{x}]$ we need to describe the group orderings on the quotients of $(\mathbb{Z}^n, +)$.

Criteria: These orderings can be given by a defining matrix U, so that $n_1 > n_2$ if only if $Un_1 > Un_2$ with respect to lex order. We denote by $P(U)$ the prime in $\mathbb{B}(\boldsymbol{x})$ corresponding to the ordering given by U.

Definition: The **dimension** of a $\mathbb{B}$-algebra A is the length of the longest chain (with respect to inclusion) of prime congruences in $A \times A$.

THEOREM

Let $\mathbb{B}(\boldsymbol{x})$ be the n-variable Laurent polynomial semialgebra, then:

- *The set of prime congruences of $\mathbb{B}(\boldsymbol{x})$ is of the form $P(U)$, where U has n columns (and non-redundant rows).*
- Every prime congruence P of $\mathbb{B}[\boldsymbol{x}]$ with trivial kernel is of the form $P(U)_{|\mathbb{B}[\boldsymbol{x}]}$. The primes with nonempty kernels correspond to primes with empty kernels in less variables.
- $dim(\mathbb{B}(\boldsymbol{x})/P(U)) = rank\ U$ and $dim(\mathbb{B}[\boldsymbol{x}]/P(U)_{|\mathbb{B}[\boldsymbol{x}]}) = rank\ U$, in particular $dim(\mathbb{B}[\boldsymbol{x}]) = dim(\mathbb{B}(\boldsymbol{x})) = n$.

THEOREM

- *The pair (f, g) lies in the radical of Δ of $\mathbb{B}(\boldsymbol{x})$ or $\mathbb{B}[\boldsymbol{x}]$ if and only if the Newton polytopes of f and g are the same.*
- *The $\mathbb{B}$-algebra $\mathbb{B}(\boldsymbol{x})/Rad(\Delta)$ is isomorphic to the $\mathbb{B}$-algebra with elements the lattice polytopes and addition being defined as the convex hull of the union, and multiplication as the Minkowski sum.*

Analogous results hold over the (Laurent) polynomial semialgebras over $\mathbb{Z}_{max}$ and $\mathbb{R}_{max}$ but instead the of Newton polytope $newt(f)$ consider,

$$\overline{newt(f)} = \{(y_0, \dots, y_k) \in newt(f) \mid \forall z > y_0 :\ (z, y_1, \dots, y_k) \notin newt(f)\}.$$

Those semialgebras have dimensions $n + 1$, where n is the number of variables.

TROPICAL NULLSTELLENSATZ

Motivation: We are interested in subsets of of $\mathbb{R}^n_{max}$ where some finite collection (f_i, g_i) of pairs of tropical polynomials agree, i.e. $\{a \in \mathbb{R}^n_{max} | f_i(a) = g_i(a)\}$. This is equivalent to looking at the zero locus of a finitely generated ideal in ring theory.

DEFINITIONS

- $V(E)$ is the set of points in $\mathbb{R}^k_{max}$ on which every pair in E agrees.
- $\boldsymbol{E}(H)$ is the congruence of pairs which agree on the set $H \subseteq \mathbb{R}^k_{max}$
- The primes $\boldsymbol{E}(\{\boldsymbol{a}\})$ we call **geometric congruences**, these are precisely the congruences whose quotient is $\mathbb{R}_{max}$.
- For $E \in \mathbb{R}_{max}$ and $\epsilon \notin \{0, 1\}$ define the set,

$$E_+ = \{(f, g) \mid (1, \epsilon)GP(f, g) \cap E \neq \emptyset\} = \{(f, g) \mid (f, g)(1, \epsilon) \in Rad(E)\}.$$

THEOREM

- *When E is finitely generated $E_+ = \boldsymbol{E}(V(E))$, hence E_+ is the intersection of all geometric congruences containing E, in particular E_+ is a congruence and $V(E) = V(E_+)$.*
- *If E is finitely generated then the set $V(E)$ is empty if and only if $E_+ = \mathbb{R}_{max}[\boldsymbol{x}] \times \mathbb{R}_{max}[\boldsymbol{x}]$ (also proven by A.Bertram and R.Easton).*
- *For a finitely generated congruence E in the (Laurent) polynomial semiring over $\mathbb{B}$, $\mathbb{Z}_{max}$ or $\mathbb{R}_{max}$ $Rad(E)$ is the intersection of the primes that contain E and have a quotient with dimension 1.*