# Tropical Nullstellensatz

Kalina Mincheva

joint work with Dániel Joó

Johns Hopkins University

April 18, 2015

# Tropical geometry and motivation

- A tropical variety (classically) is a balanced polyhedral complex with no scheme structure.
- J. and N. Giansiracusa propose a notion of tropical scheme structure for tropical varieties, which takes the form of a congruence on the semiring of tropical polynomials, subschemes are given by certain congruences.
- We study congruences of certain semirings to obtain a tropical version of the Nullstellensatz.

# Introduction

In this talk by a *semiring* we mean a commutative semiring with multiplicative unit, that is a nonempty set $R$ with two binary operations $(+, \cdot)$ satisfying:

(i) $(R, +)$ is a commutative monoid with identity element 0

(ii) $(R, \cdot)$ is a commutative monoid with identity element 1

(iii) For any $a, b, c \in R$: $a(b + c) = ab + ac$

(iv) $1 \neq 0$ and $a \cdot 0 = 0$ for all $a \in R$

A *semifield* is a semiring in which all nonzero elements have multiplicative inverse.
Every semiring we study here will be additively idempotent, that is $a + a = a, \forall a$. The idempotent addition defines an ordering via

$$a \geq b \iff a + b = a.$$

# Examples

- The *tropical semifield* $\mathbb{T} = \mathbb{R}_{max} = \{\{-\infty\} \cup \mathbb{R}, max, +\}$.
- $\mathbb{Z}_{max}$ - the subsemifield of integers in $\mathbb{T}$.
- $\mathbb{B} = \{0, 1\}$
- There is a morphism onto $\mathbb{B}$ from any idempotent semiring, i.e. $\mathbb{B}$ is the unique simple object.

# Congruences vs Ideals

- A *congruence* is an operation-preserving equivalence relation. We will write $(a, b) \in C$ whenever the elements $a$ and $b$ are congruent in $C$.
- Let $I$ be an ideal in a ring $R$ and define $C_I = \langle (a, 0), \forall a \in I \rangle$, then

$$R/I := R/C_I.$$

- In the ring case $(a, b) \in C \Leftrightarrow (a - b, 0) \in C$.

# Congruences vs Ideals

- The kernel of a congruence $C \subseteq R \times R$ is

$$Ker(C) = \{a \in R | (a, 0) \in C\}.$$

- $Ker(C)$ is an ideal.
- There is no bijection between ideals and congruences as in ring theory.
- In general $Ker(C)$ contains little information about the congruence $C$.

**Example**

*Let* $R = \mathbb{T}[x, y]$ *and* $C = \langle (x, y) \rangle$.
$Ker(C) = \{0\}$ *but* $C$ *is a non-trivial congruence and* $\mathbb{T}[x, y]/C \cong \mathbb{T}[x]$.

- In an idempotent semiring we have

$$(a + b, 0) \in C \Rightarrow (a, 0) \in C.$$

- A congruence is called *improper* if it identifies every element with 0, *proper* otherwise.
- The *trivial* congruence, denoted by $\Delta$, is the one that has only one element in each equivalence class.
  - In the case of rings $C_{(0)} = \Delta$.
- Quotients by proper congruences can be defined in the usual way.
  - They need to be proper since we require semirings to have a $1 \neq 0$.

# Notation

Let $F$ be a semifield, then

- $F[\boldsymbol{x}]$ is the $k$-variable polynomial semiring over $F$ in the variables $\boldsymbol{x} = (x_1, \ldots, x_k)$.
- $F(\boldsymbol{x})$ is the $k$-variable Laurent polynomial semiring over $F$ in the variables $\boldsymbol{x} = (x_1, \ldots, x_k)$.

**Remark**

*Every proper congruence of $F(\boldsymbol{x})$ has $\{0\}$ kernel.*

- The kernel of a morphism $\varphi$ is just the congruence

$$\{(a, b) \mid \varphi(a) = \varphi(b)\}.$$

- Elements of $F[\boldsymbol{x}]$ can be thought of as functions $F^k \to F$. In turn evaluating at a point $v \in F^k$ gives a morphism of semirings $\varphi_v : F[\boldsymbol{x}] \to F$.
- Similarly elements of $F(\boldsymbol{x})$ can be thought of as functions $(F \setminus \{0\})^k \to (F \setminus \{0\})$ and for $v \in (F \setminus \{0\})^k$ we have a morphism $\varphi_v : F(\boldsymbol{x}) \to F$.
- The kernels of the maps $\varphi_v$ are congruences with quotient $F$. We will call these *geometric congruences*. (these are not maximal congruences unless $F = \mathbb{B}$)

# Tropical Nullstellensatz

- The problem of trying to find an analogue of the Nullstellensatz for the tropical semifield $\mathbb{T}$ was raised by A. Bertram and R. Easton in a 2013 paper.
- First for a congruence $C$ of the k-variable polynomial semiring $\mathbb{T}[\boldsymbol{x}]$ we set
$$V(C) = \{v \in \mathbb{T}^k \mid f(v) = g(v),\ \forall (f,g) \in C\}$$
- For a subset $H \subseteq \mathbb{T}^k$ we define the congruence
$$\boldsymbol{E}(H) = \{(f,g) \in \mathbb{T}[\boldsymbol{x}] \times \mathbb{T}[\boldsymbol{x}] \mid f(v) = g(v)\ \forall v \in H\}$$
- The aim of a "Tropical Nullstellensatz" is to describe the set $\boldsymbol{E}(V(C))$ with some suitable formulas, when $C$ is finitely generated.

## Example

*In the 2-variable semiring* $\mathbb{T}[x, y]$ *consider the congruence* $C = \langle (x^2, y^2) \rangle$. *Since for* $a, b \in \mathbb{T}$ *we have*

$$a^2 = b^2 \Leftrightarrow a = b$$

*one can easily see that*

$$V(C) = \{(a, a) \mid a \in \mathbb{T}\}$$

*It follows that* $(x, y) \in \boldsymbol{E}(V(C))$, *and in fact it is not hard to show that* $\boldsymbol{E}(V(C)) = \langle (x, y) \rangle$. *Our goal - in the context of this example - is to show that this happens since some "power" (in a to-be-defined sense) of* $(x, y)$ *lies in the congruence* $C$.

# Questions

- Note that $\boldsymbol{E}(V(C))$ is the intersection of all geometric congruences lying above $C$ (because $v \in V(C)$ if and only if $C$ is contained in the geometric congruence $Ker(\varphi_v)$).
- Bertram and Easton showed that a set $C_+$ can be defined using certain "power formulas", such that $\boldsymbol{E}(V(C)) \subseteq C_+$.
- They showed that $C_+$ consists of certain limits of pairs of elements that lie in $\boldsymbol{E}(V(C))$.
- It was unclear if
  - $\boldsymbol{E}(V(C)) = C_+$.
  - $C_+$ is even a congruence in general (according to the first version of the paper).

# Solution outline

The plan to solve this problem:

- Find a suitable notion of prime congruences for any idempotent semiring.
- Define the radical of a congruence as the intersection of all prime congruences lying over it.
- Express the radical in terms of certain "power formulas".
- Explicitly describe the prime congruences in $\mathbb{T}[\boldsymbol{x}]$ and $\mathbb{T}(\boldsymbol{x})$.
- Show that the radical of a finitely generated congruence can be expressed as the intersection of certain congruences (including the geometric congruences).

# Quotient cancellative congruences

- A semiring is called *cancellative* if whenever $ac = bc$ we have either $a = b$ or $c = 0$.
- We call a congruence whose quotient is a cancellative semiring quotient cancellative or QC.

**Remark**

*Sometimes in the literature prime congruences are defined to be the QC ones. The drawback of this approach is that QC congruences are not in general intersection indecomposable. Moreover in the studied rings there are "too many" of them, and they do not provide a useful notion of dimension.*

# The twisted product

- The twisted product of two pairs of elements $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$ from $R \times R$ is defined as

$$\alpha\beta = (\alpha_1\beta_1 + \alpha_2\beta_2, \alpha_1\beta_2 + \alpha_2\beta_1).$$

- If $P$ is an ideal of a commutative ring and $C_P$ is the congruence with kernel $P$, then $P$ is prime if and only if whenever $\alpha\beta \in C_P$ either $\alpha \in C_P$ or $\beta \in C_P$. This can be verified by checking that

$$\alpha\beta \in C_P \Leftrightarrow ((\alpha_1 - \alpha_2)(\beta_1 - \beta_2), 0) \in C_P \Leftrightarrow (\alpha_1 - \alpha_2)(\beta_1 - \beta_2) \in P.$$

# Prime congruences

Following the above heuristic we define prime congruences,

- We call a congruence $C$ of a semiring to a *prime congruence* if it is proper and whenever for some $\alpha, \beta \in R \times R$ we have $\alpha\beta \in C$ then $\alpha \in C$ or $\beta \in C$.
- We will call a semiring a *domain* if its trivial congruence is prime.

**Theorem**

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

- The semifields $\mathbb{B}$, $\mathbb{Z}_{max}$ and $\mathbb{T}$ are domains. However the polynomial and Laurent polynomial semirings over them are not even cancellative. For example:

$$(1 + x + x^2)(1 + x^2) = (1 + x + x^2)(1 + x + x^2)$$

# Radical Congruences

- We define $Rad(C)$ - the radical of a congruence $C$ - to be the intersection of all prime congruences containing $C$. We call $C$ a radical congruence if $Rad(C) = C$.
- In a commutative ring it is easy to verify the following: If $I$ is an ideal, $Rad(I)$ its radical and $C_I$, $C_{Rad(I)}$ the corresponding congruences, then we have $(a, b) \in C_{Rad(I)}$ if and only if for a large enough n $(a, b)^n \in C_I$ where $(a, b)^n$ denotes the twisted n-th power. This follows from $(a, b)^n \in C_I \Leftrightarrow ((a - b)^n, 0) \in C_I$.
- For semirings the situation is somewhat more complicated.

## Example

*Consider again the congruence* $C = \langle (x^2, y^2) \rangle$ *in* $\mathbb{T}[x, y]$. *If* $C \subseteq P$ *for a prime congruence* $P$ *then we have*

$$(x^2 + xy, y^2 + xy) \in P$$

*hence*

$$(x + y, 0)(x, y) \in P$$

*It follows that either* $(x, y) \in P$ *or* $(x + y, 0) \in P$. *On the other hand if* $(x + y, 0) \in P$ *then* $(x, 0) \in P$ *and* $(y, 0) \in P$ *so again* $(x, y) \in P$. *It follows that* $(x, y) \in Rad(C)$. *However* $(x, y)^n$ *is not in* $C$ *for any* $n$.

- Generalizing the situation in the example, one observes that whenever for some pair $\alpha = (\alpha_1, \alpha_2)$ an element $h \in R$, integers $i, j$ we have

$$((\alpha_1 + \alpha_2)^i + h, 0)\alpha^j \in P$$

for a prime congruence $P$, we also have $\alpha \in P$.

- We define the generalized powers of the pair $\alpha$ to be the pairs $((\alpha_1 + \alpha_2)^i + h, 0)\alpha^j$, where we set the 0-th power of any pair to be $(1, 0)$. The set of generalized powers of $\alpha$ is denoted by $GP(\alpha)$.

**Theorem**

*For any congruence $C$ in an idempotent semiring $R$ we have*

$$Rad(C) = \{\alpha \in R \times R \mid GP(\alpha) \cap C \neq 0\}$$

# Prime congruences of polynomials over $\mathbb{T}$, $\mathbb{Z}_{max}$ and $\mathbb{B}$

First we make the following observation:

**Proposition**

*An idempotent semiring that is a domain is totally ordered under the ordering coming from the addition.*

**Proof.**

$$(a+b,a)(a+b,b) = (a^2+ab+b^2, a^2+ab+b^2)$$

Since the trivial congruence is prime this implies that for any $a, b$ either $a+b=a$ or $a+b=b$. □

- The quotient by any prime congruence is totally ordered, hence a prime congruence of a polynomial ring will identify every polynomial with one of its monomials.

## Example

*Let $P$ be a prime of the one variable Laurent polynomial ring $\mathbb{B}(x)$. Then by the proposition in the quotient $\mathbb{B}(x)/P$ we have either $1 = x$ or $x > 1$ or $1 > x$.*

- *If $1 = x$ then $P$ is the congruence that identifies every non-zero element with 1.*
- *If $x > 1$ then $x^i > x^j$ whenever $i > j$, so $P$ identifies every polynomial with it is highest degree term, and $\mathbb{B}(x)/P = \mathbb{Z}_{max}$.*
- *If $1 > x$ then every polynomial is identified with its lowest degree term and $\mathbb{B}(x)/P = \mathbb{Z}_{min}$.*

*We obtained that $\mathbb{B}(x)$ has precisely 3 prime congruences. It is easy to see that $Rad(\Delta)$ is then the congruence that identifies two polynomials if their highest and lowest degree terms agree. $Rad(\Delta)$ is QC but not prime.*

# Primes in the Laurent polynomial ring over $\mathbb{B}$

First we study the k-variable Laurent polynomial ring $\mathbb{B}(\boldsymbol{x})$.

- One can show that minimal primes are precisely the ones that have one monomial in each equivalence class.
- Let $P$ be a minimal prime. The multiplicative group of $\mathbb{B}(\boldsymbol{x})/P$ is isomorphic to $(\mathbb{Z}^k, +)$. The ordering given by the addition on $\mathbb{B}(\boldsymbol{x})/P$ has to be compatible with the multiplication.
- Hence minimal primes correspond to group orderings of $(\mathbb{Z}^k, +)$. These are the same as usual monomial orderings except $1 > x$ is allowed.
- Every such ordering gives a minimal prime that identifies each polynomial with its leading term.

- By a result of Robbiano all monomial orderings $\prec$ can be given by a matrix $U$ with $k$ columns and $l \leq k$ rows, so that $\boldsymbol{x}^{\boldsymbol{n}_1} \prec \boldsymbol{x}^{\boldsymbol{n}_2}$ if and only if $U\boldsymbol{n}_1 \prec_{lex} U\boldsymbol{n}_2$, or in other words if the first non-zero coordinate of $U(\boldsymbol{n}_2 - \boldsymbol{n}_1)$ is positive.
- In the case when $Ker(U) \cap \mathbb{Z}^k \neq \{0\}$, $U$ gives an ordering on a quotient of $\mathbb{Z}^k$, which in turn defines a prime of $\mathbb{B}(\boldsymbol{x})$ that identifies $\boldsymbol{x}^{\boldsymbol{n}_1}$ with $\boldsymbol{x}^{\boldsymbol{n}_2}$ whenever $\boldsymbol{n}_1 - \boldsymbol{n}_2 \in Ker(U)$.

- We will call an $U$ as above admissible if all of its rows are non-redundant.
- The prime corresponding to the admissible matrix $U$ will be denoted by $P(U)$. We allow $U$ to be possibly an "empty matrix" and then $P(U)$ identifies every element with 1.
- In the k-variable Laurent polynomial ring $\mathbb{B}(\boldsymbol{x})$ there are infinitely many prime congruences for $k > 1$.

## Example

*Let* $U = \begin{bmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, *that defines the prime* $P(U)$ *in* $\mathbb{B}(x, y, z)$. *We would like to compare the following monomials in* $\mathbb{B}(x, y, z)/P(U)$.

- *Let* $m_1 = x^2y^3z$ *and* $m_2 = x^3yz^2$.

$$\boldsymbol{n}_1 = \begin{bmatrix} 2 \\ 3 \\ 1 \end{bmatrix}, \boldsymbol{n}_2 = \begin{bmatrix} 3 \\ 1 \\ 2 \end{bmatrix} \text{ and } U\boldsymbol{n}_1 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}, U\boldsymbol{n}_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

$$U\boldsymbol{n}_1 - U\boldsymbol{n}_2 = \begin{bmatrix} 2 \\ 3 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \text{ hence } m_1 > m_2.$$

- *Let* $m_3 = xy^2z$ *and* $m_4 = x^2y^2z^2$ *we have that* $m_3 = m_4$ *since* $U\boldsymbol{n}_3 = U\boldsymbol{n}_4 = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$.

# Dimension

- The Krull dimension of a semiring is the number of strict inclusions in the longest chain of prime congruences. In particular $dim(\mathbb{B}) = 0$ and $dim(\mathbb{T}) = dim(\mathbb{Z}_{max}) = 1$.

**Theorem**

- *Every prime congruence of $\mathbb{B}(\boldsymbol{x})$ is of the form $P(U)$.*
- *For an admissible $U$ $dim(\mathbb{B}(\boldsymbol{x})/P(U))$ equals the number of rows of $U$*
- *In particular for the k-variable Laurent polynomial semiring $\mathbb{B}(\boldsymbol{x})$ we have $dim(\mathbb{B}(\boldsymbol{x})) = k$.*

- For an admissible matrix $U$ with $r$ rows, denoting by $U(i)$ the matrix that consists of the first $i$ rows of $U$, the unique chain of prime congruences lying over $P(U)$ is

$$P(U) \subset P(U(r-1)) \subset \cdots \subset P(U(0)).$$

- The Newton polytope of a polynomial is the convex hull of the exponent vectors of its monomials.
- Two polynomials $f$ and $g$ are identified in every prime congruence (or equivalently in the congruence $Rad(\Delta)$) if their leading terms agree in every monomial ordering i.e. if and only if their Newton polytopes are the same.

**Theorem**

- *For $f, g \in \mathbb{B}(\boldsymbol{x})$ we have $(f, g) \in Rad(\Delta)$ if and only if their Newton polytopes are the same.*
- *The semiring $\mathbb{B}(\boldsymbol{x})/Rad(\Delta)$ is isomorphic to the semiring whose elements are the lattice polytopes with addition - taking the convex hull of the union, and multiplication - the Minkowski sum.*

# Primes in the Laurent polynomial ring over $\mathbb{Z}_{max}$ and $\mathbb{T}$

- A similar description can be obtained over $\mathbb{Z}_{max}(\boldsymbol{x})$ by realizing that $\mathbb{Z}_{max} \cong \mathbb{B}(x)/\langle(x, 1+x)\rangle$.
- The primes of the k-variable semiring $\mathbb{Z}_{max}(\boldsymbol{x})$ will correspond to the primes a $k+1$ variable semiring $\mathbb{B}(\boldsymbol{x}, t)$ that contain $(t, 1+t)$.
- The primes of $\mathbb{T}(\boldsymbol{x})$ can also be described similarly, except that the notion of admissibility has to be relaxed, since rows that are redundant over $\mathbb{Z}_{max}$ might not be redundant over $\mathbb{T}$.

# Primes in the Laurent polynomial ring over $\mathbb{Z}_{max}$ and $\mathbb{T}$

- We can obtain a theorem similar to the ones for $\mathbb{B}$ by changing the notion of admissibility accordingly.
- $dim(\mathbb{Z}_{max}(\boldsymbol{x})) = dim(\mathbb{T}(\boldsymbol{x})) = k+1$ which is what we would expect, since these are k-variable rings over a semifield of dimension 1.
- For $Rad(\Delta)$ a similar result with Newton polytopes can be obtained in both cases with some technical changes.

# Primes in the polynomial semiring over $\mathbb{B}$, $\mathbb{Z}_{max}$ and $\mathbb{T}$

- In the case of a the polynomial semirings $\mathbb{B}[\boldsymbol{x}]$, $\mathbb{Z}_{max}[\boldsymbol{x}]$ and $\mathbb{T}[\boldsymbol{x}]$ prime congruences may have non-empty kernels.
- The kernel of a prime congruence in any of these cases is generated by a subset of the variables $(x_1, \ldots, x_k)$.
  - If a polynomial is in the kernel of a congruence then all of its monomials are.
  - If a monomial is in a kernel of a prime congruence, than at least one of its variables is.
- Prime congruences of the three polynomial semirings above correspond to prime congruences of a Laurent semiring in possibly less variables.

Using the description we obtained for the prime congruences of the polynomial and Laurent polynomial semirings over $\mathbb{B}$, $\mathbb{Z}_{max}$ and $\mathbb{T}$ one can prove the following theorem:

**Theorem**

*For a finitely generated congruence $C$ in one of $\mathbb{B}(\boldsymbol{x})$, $\mathbb{B}[\boldsymbol{x}]$, $\mathbb{Z}_{max}(\boldsymbol{x})$, $\mathbb{Z}_{max}[\boldsymbol{x}]$, $\mathbb{T}(\boldsymbol{x})$ or $\mathbb{T}[\boldsymbol{x}]$, we have that $Rad(C)$ is the intersection of the primes that contain $C$ and have an at most 1-dimensional quotient.*

# Tropical Nullstellensatz

- Recall that we are interested in describing the congruence $\boldsymbol{E}(V(C))$ for a congruence $C$ in $\mathbb{T}(\boldsymbol{x})$ or $\mathbb{T}[\boldsymbol{x}]$.
- $\boldsymbol{E}(V(C))$ is the intersection of the geometric congruences above $C$.
- Geometric congruences are precisely the ones that
  - have a 1-dimensional quotient
  - do not contain $(1, \epsilon)$ for any $\epsilon \in \mathbb{T} \setminus \{1\}$.
- Set $C_+$ to be the intersection of all primes that contain $C$ but do not contain $(1, \epsilon) \in \mathbb{T} \setminus \{1\}$.

- Using our theorem describing radicals one can verify that $C_+$ consists of pairs of elements $(f, g)$, such that there exists an $\epsilon \in \mathbb{T} \setminus \{1\}$, an integer $i$ and a polynomial $h$ such that

$$(1, \epsilon)((f + g, 0)^i + h)(f, g) \in C$$

- This is the way Bertram and Easton defined $C_+$. Now it is obvious that $C_+$ is a congruence since it can be obtained as the intersection of certain congruences.
- The key idea is the following - we can show that in an arbitrary idempotent semiring $R$ for a congruence $C$ and any pair $\alpha$ the intersection of the primes that contain $C$ but not $\alpha$ is just

$$\{\beta \in R \mid GP(\alpha\beta) \cap C \neq 0\}$$

## Theorem

*For a finitely generated congruence $C$ of $\mathbb{T}(\boldsymbol{x})$ or $\mathbb{T}[\boldsymbol{x}]$ we have:*

- $\boldsymbol{E}(V(C)) = C_+$.
- $\boldsymbol{E}(V(C))$ *consists of the pairs of polynomials* $(f, g)$ *such that there is an* $\epsilon \in \mathbb{T} \setminus \{1\}$, *an integer* $i$ *and a polynomial* $h$ *such that*

$$(1, \epsilon)((f + g, 0)^i + h)(f, g) \in C$$

# Thank you for your attention!