Complex and Tropical Nullstellensatze

Undergrad Colloquium, October 2017

The **complex numbers** $\mathbb{C}$ are an algebraically closed field. That is,

(*) Every non-constant polynomial in one variable:

$$f(x) \in \mathbb{C}[x]$$

has a complex root. Iterating this, $f(x)$ factors completely:

$$f(x) = c(x - r_1) \cdots (x - r_d)$$

Example. The polynomials $f(x) = x^d - c$ ($c \neq 0$) have distinct roots:

$$f(x) = (x - c^{\frac{1}{d}})(x - \omega c^{\frac{1}{d}}) \cdots (x - \omega^{d-1} c^{\frac{1}{d}})$$

where $c^{\frac{1}{d}} = r^{\frac{1}{d}} e^{i\theta/d}$ if $c = re^{i\theta}$ and $\omega = e^{2\pi i/d}$ is the basic dth root of 1.

There are algebraic, analytic and topological proofs of this fact, but in this talk I want to explore the implications of this for systems of polynomial equations. In one variable, this is:

(**) If $f_1, ..., f_m \in \mathbb{C}[x]$ share no collective common roots, then:

$$1 = \sum g_i f_i$$

can be solved with polynomials $g_1, ..., g_m \in \mathbb{C}[x]$.

Proof. Let $h(x) = \gcd(f_1(x), ..., f_m(x))$. If $h(x)$ is not constant, then $f_1, ..., f_m$ have a common root! The rest is Euclid's algorithm.

Nulltellensatz. (**) is also true for polynomials in n variables.

Remark. Euclid's algorithm is not available in more variables.

Background. The span of **vectors** $v_1, ..., v_m$ in a vector space V is:

$$\langle v_1, ..., v_m \rangle = \left\{ \sum c_i v_i \in V \mid c_i \in \mathbb{C} \text{ are arbitrary scalars} \right\} \subset V$$

and by the fundamental theorem of linear algebra,

$$\langle v_1, ..., v_m \rangle = \ker \left(V \mapsto V / \langle v_1, ..., v_m \rangle \right)$$

is the kernel subspace of the map to the quotient space.

Similarly, the span of polynomials $f_1, ..., f_m \in \mathbb{C}[x_1, ..., x_n]$ is:

$$\langle f_1, ..., f_m \rangle = \left\{ \sum g_i f_i \mid g_i \in \mathbb{C}[x_1, ..., x_n] \right\}$$

which is an *ideal* in the ring of polynomials, and once again:

$$\langle f_1, ..., f_m \rangle = \ker \left(\mathbb{C}[x_1, ..., x_n] \to \mathbb{C}[x_1, ..., x_n] / \langle f_1, ..., f_m \rangle \right)$$

is the kernel of the map to the quotient ring. But this is not a subring.

Ideals. Ideals in $\mathbb{C}[x_1, ..., x_n]$ are subspaces that are also closed under multiplication by the variables $x_1, ..., x_n$, hence by multiplication by all polynomials. Like subspaces of $\mathbb{C}^n$, all ideals in $\mathbb{C}[x_1, ..., x_n]$ have a finite generating set (the Hilbert Basis Theorem).

Example. The "vanishing ideal" at a subset $S \in \mathbb{C}^n$ is the ideal:

$$I(S) = \{f \in \mathbb{C}[x_1, ..., x_n] \mid f(s) = 0 \text{ for all } s \in S\}$$

By Zorn's Lemma, an ideal that is not equal to $\mathbb{C}[x_1, ..., x_n]$ is always contained in a *maximal* ideal I whose quotient is a field:

$$\mathbb{C}[x_1, ..., x_n]/I = K$$

Conversely, the kernel of a map from $\mathbb{C}[x_1, ..., x_n]$ to a field is maximal.

Example. The vanishing ideal of the point $(a_1, ..., a_n) \in \mathbb{C}^n$ is:

$$\langle x_1 - a_1, ..., x_n - a_n \rangle$$

and the map to quotient is the evaluation map to $\mathbb{C}$ given by $f \mapsto f(a)$.

Nullstellensatz reformulated. These are all the maximal ideals.

Not even a Sketch. The quotient by a maximal ideal is a field:

$$\mathbb{C}[x_1, ..., x_n] \to K$$

and therefore $\mathbb{C} \subset K$. This is, in particular, a complex vector space which must have finite dimension (by a Theorem of Emmy Noether). But if $\mathbb{C} \neq K$, choose $\alpha \in K - \mathbb{C}$ and consider:

$$1, \alpha, \alpha^2, ... \in K$$

These vectors are eventually dependant, which determines a polynomial with α as a root. But $\mathbb{C}$ is algebraically closed, so all roots are in $\mathbb{C}$.

Maximal ideals and prime ideals are the building blocks of algebraic geometry, as they correspond to points and irreducible algebraic sets, respectively. The subject can be developed with $\mathbb{C}$ replaced by any algebraically closed field. But recently there has been interest in:

The algebraic geometry of the **tropical numbers**. This is the set:

$$\mathbb{T} = \mathbb{R} \cup \{-\infty\}$$

with $s + t = \max(s, t)$ and $s \cdot t = s + t$ (real addition), which is an additively idempotent $(t + t = t)$ semi-ring:

• There is no subtraction in $\mathbb{T}$. The tropical number $-\infty$ is an additive identity, but $s+t = -\infty$ has no solutions besides $s = t = -\infty$.
• Every "non-zero" tropical number t has reciprocal $-t$ so $\mathbb{T}$ behaves like a field with no subtraction.

But there is a surjective map to the Boolean semi-field:

$$\mathbb{T} \to \mathbb{B}, \quad -\infty \mapsto 0, \ \mathbb{R} \mapsto 1$$

so $\mathbb{T}$ itself shouldn't properly be called a semi-field.

Ideals. Rob Easton and I decided to work with *congruence ideals.* These are the "kernels" whose quotient is another semi-ring:

$$I = \ker\left(\pi : \mathbb{T}[x_1, ..., x_n] \to R\right)$$

But there is no subtraction, so these are not subsets of $\mathbb{T}[x_1, ..., x_n]$! The kernel of a map is properly a relation:

$$I = \{(f, g) \in \mathbb{T}[x_1, ..., x_n] \times \mathbb{T}[x_1, ..., x_n] \mid \pi(f) = \pi(g)\}$$

In the complex case, we can replace (f, g) with $(f - g, 0)$ and get equivalent information, but without subtraction, we can't do this.

Significant problems result. E.g., we cannot find bases of subspaces. But it gets even worse:

Let $(t_1, t_2) \in \mathbb{T}^2$ be a vector. Then:

$$s \cdot (t_1, t_2) = (t_1 + s, t_2 + s) \text{ with real addition}$$

is the line with slope 1 through (t_1, t_2). Two vectors span the strip between the corresponding lines, and a series of vectors map span larger strips with no limit. In other words, the "subspace" given by an open strip cannot be generated by finitely many vectors.

Definition. A subspace $W \subset \mathbb{T}^n$ is finitely determined if there are finitely many linear relations:

$$r_j = (\sum_{i=1}^{n} a_{i,j} x_i, \sum_{i=1}^{n} b_{i,j} x_i)$$

whose common locus of solutions is W.

- In $\mathbb{T}^1$, they are either $\mathbb{T}^1$ or zero.
- In $\mathbb{T}^2$, they are (maybe unbounded) strips.
- In $\mathbb{T}^3$ they develop kinks (see the projective version).

Exercise. Are finitely determined tropical subspaces always generated by finitely many vectors?

Definition. An ideal $I \subset \mathbb{T}[x_1, ..., x_n] \times \mathbb{T}[x_1, ..., x_n]$ is finitely determined if I there are finitely many relations $r_j = (f_j, g_j) \in I$ such that I is the smallest ideal containing the r_j.

Remark. Such an ideal determines a **subset** of $\mathbb{T}^n$:

$$Z(I) = \{v = (t_1, ..., t_n) \in \mathbb{T}^n \mid f_j(v) = g_j(v) \text{ for all } j\}$$

and also an ideal of relations vanishing on Z:

$$I(Z(I)) = \{(f, g) \mid f(v) = g(v) \text{ for all } v \in Z(I)\}$$

The strong Nullstellensatz explains how to relate I, $Z(I)$ and $I(Z(I))$. In the classical case, for example,

(a) if I is the zero ideal, then $I(Z(I))$ is also the zero ideal

(b) if $Z(I)$ is empty, then I contains a constant (weak Nullstellensatz)

Rob Easton and I proved a Nullstellensatz for tropical ideals.

Theorem. (Weak version).

If I is finitely determined and $Z(I) = \emptyset$, then:

$$(f, c \cdot f) \in I$$

for some $f \in \mathbb{T}[x_1, ..., x_n]$ with a non-zero constant term and $c \neq$ "1".

(This is the tropical analogue of having a constant function!).

Not even a sketch. Interestingly, we prove this by proving a fact about tropical ideals that is **false** for ideals in the complex case. Namely, if I is finitely determined, then there is a **single** relation in I such that:

$$Z(f, g) = Z(I)$$

Then we use a lovely trick to deduce the result. If $Z(f, g) = \emptyset$, then by the intermediate value theorem, either $f(v) < g(v)$ for all v or else $f(v) > g(v)$ for all v. Assume the former. Then for some $\epsilon > 0$,

$$(f, g) \in I \Rightarrow (f + \epsilon f, g + \epsilon f) \in I \Rightarrow (\epsilon f, g) \in I$$

which finally implies that $(f, \epsilon f) \in I$ by transitivity!