6. The Nullstellensatz

- Feasibility problems and duality
- The Nullstellensatz and strong duality
- The Bézout identity and fundamental theorem of algebra
- Partition of unity
- Certificates
- Abstract duality
- The ideal-variety correspondence
- Computation of ideals and division
- The division algorithm, and the Euclidean algorithm
- Every ideal of one-variable polynomials is principle
- Testing ideal membership
Feasibility Problems and Duality

Suppose $f_1, \ldots, f_m$ are polynomials, and consider the feasibility problem

\[
\begin{align*}
\text{does there exist } x \in \mathbb{K}^n \text{ such that } \\
f_i(x) &= 0 \quad \text{for all } i = 1, \ldots, m
\end{align*}
\]

Every polynomial in \text{ideal}\{f_1, \ldots, f_m\} is zero on the feasible set.

So if $1 \in \text{ideal}\{f_1, \ldots, f_m\}$, then the primal problem is infeasible. Again, this is proof by contradiction.

Equivalently, the primal is infeasible if there exist polynomials $h_1, \ldots, h_m \in \mathbb{K}[x_1, \ldots, x_n]$ such that

\[
1 = h_1(x)f_1(x) + \cdots + h_m(x)f_m(x) \quad \text{for all } x \in \mathbb{K}^n
\]
**Strong Duality**

So far, we have seen examples of weak duality. The *Hilbert Nullstellensatz* gives a *strong duality* result for polynomials over the complex field.

**The Nullstellensatz**

Suppose $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$. Then

\[
1 \in \text{ideal}\{f_1, \ldots, f_m\} \iff \mathcal{V}_{\mathbb{C}}\{f_1, \ldots, f_m\} = \emptyset
\]
Algebraically Closed Fields

For complex polynomials $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, we have

$$1 \in \text{ideal}\{f_1, \ldots, f_m\} \iff \mathcal{V}\{f_1, \ldots, f_m\} = \emptyset$$

This *does not hold* for polynomials and varieties over the real numbers.

For example, suppose $f(x) = x^2 + 1$. Then

$$\mathcal{V}_{\mathbb{R}}\{f\} = \{ x \in \mathbb{R} \mid f(x) = 0 \}$$

$$= \emptyset$$

But $1 \not\in \text{ideal}\{f\}$, since any multiple of $f$ will have degree $\geq 2$.

The above results requires an *algebraically closed field*. Later, we will see a version of this result that holds for real varieties.
The Nullstellensatz and Feasibility Problems

The primal problem:

\[
\text{does there exist } x \in \mathbb{C}^n \text{ such that } f_i(x) = 0 \quad \text{for all } i = 1, \ldots, m
\]

The dual problem:

\[
\text{do there exist } h_1, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n] \text{ such that } 1 = h_1 f_1 + \cdots + h_m f_m
\]

The Nullstellensatz implies that these are strong alternatives. Exactly one of the above problems is feasible.
Example: Nullstellensatz

Consider the polynomials

\[ f_1(x) = x_1^2 \quad \quad f_2(x) = 1 - x_1 x_2 \]

There is no \( x \in \mathbb{C}^2 \) which simultaneously satisfies \( f_1(x) = 0 \) and \( f_2(x) = 0 \); i.e.,

\[ \forall \{f_1, f_2\} = \emptyset \]

Hence the Nullstellensatz implies there exists \( h_1, h_2 \) such that

\[ 1 = h_1(x) f_1(x) + h_2(x) f_2(x) \]

One such pair is

\[ h_1(x) = x_2^2 \quad \quad h_2(x) = 1 + x_1 x_2 \]
Interpretations of the Nullstellensatz

• The feasibility question asks; do the polynomials $f_1, \ldots, f_m$ have a common root?

The Nullstellensatz is a Bézout identity. In the scalar case, the dual problem is: do the polynomials have a common factor?

• Suppose we look at $f \in \mathbb{C}[x]$, a scalar polynomial with complex coefficients. The feasibility problem is: does it have a root?

The Nullstellensatz says it has a root if and only if there is no polynomial $h \in \mathbb{C}[x]$ such that $1 = hf$

Since $\text{degree}(hf) \geq \text{degree}(f)$, there is no such $h$ if $\text{degree}(f) \geq 1$; i.e. all polynomials $f$ with $\text{degree}(f) \geq 1$ have a root.

So the Nullstellensatz generalizes the fundamental theorem of algebra.
Interpretation: Partition of Unity

The equation

\[ 1 = h_1 f_1 + \cdots + h_m f_m \]

is called a partition of unity.

For example, when \( m = 2 \), we have

\[ 1 = h_1(x) f_1(x) + h_2(x) f_2(x) \quad \text{for all } x \]

Let \( V_i = \left\{ x \in \mathbb{C}^n \mid f_i(x) = 0 \right\} \).

Let \( q(x) = h_1(x) f_1(x) \). Then for \( x \in V_1 \), we have \( q(x) = 0 \), and hence the second term \( h_2(x) f_2(x) \) equals one. Conversely, for \( x \in V_2 \), we must have \( q(x) = 1 \).

Since \( q(x) \) cannot be both zero and one, we must have \( V_1 \cap V_2 = \emptyset \).
Interpretation: Certificates

The functions $h_1, \ldots, h_m$ give a certificate of infeasibility for the primal problem.

Given the $h_i$, one may immediately computationally verify that

$$1 = h_1 f_1 + \cdots + h_m f_m$$

and this proves that $\forall\{f_1, \ldots, f_m\} = \emptyset$
Duality

The notion of duality here is parallel to that for linear functionals.

Compare, for $S \subset \mathbb{R}^n$

$$\mathcal{I}(S) = \left\{ f \in \mathbb{R}[x_1, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in S \right\}$$

with

$$S^\perp = \left\{ p \in (\mathbb{R}^n)^* \mid \langle p, x \rangle = 0 \text{ for all } x \in S \right\}$$

- There is a pairing between $\mathbb{R}^n$ and $(\mathbb{R}^n)^*$; we can view either as a space of functionals on the other
- The same holds between $\mathbb{R}^n$ and $\mathbb{R}[x_1, \ldots, x_n]$
- If $S \subset T$, then $S^\perp \supset T^\perp$ and $\mathcal{I}(S) \supset \mathcal{I}(T)$
Feasibility and the Ideal-Variety Correspondence

Given polynomials $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, we define two objects

- the ideal $I = \text{ideal}\{f_1, \ldots, f_m\}$
- the variety $V = \mathcal{V}\{f_1, \ldots, f_m\}$

We have the following results:

(i) *weak duality*:

$$V = \emptyset \iff 1 \in I$$

(ii) *Nullstellensatz* (strong duality):

$$V = \emptyset \implies 1 \in I$$

(iii) *Strong Nullstellensatz*:

$$\sqrt{I} = \mathcal{I}(V)$$
Computation

The feasibility problem is equivalent to the ideal membership problem; is it true that

$$1 \in \text{ideal}\{f_1, \ldots, f_m\}$$

Equivalently, are there polynomials $h_1, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that

$$1 = h_1 f_1 + \cdots + h_m f_m$$

How do we compute this?

- The above equation is linear in the coefficients of $h_i$; so if we have a bound on the degree of the $h_i$ we can easily find them.

- Since the feasibility problem is NP-hard, the bound must grow exponentially with the size of the $f_i$. 
Ideals and Division

For $f \in \mathbb{K}[x]$, the leading term of $f$ is the term with highest degree.

E.g., $f = 7x^3 + 3x + 1$ has leading term $\text{lt}(f) = 7x^3$.

For polynomials, it's simple to divide them.

$$
\begin{array}{c}
3x + 1 \\
\hline
x^2 + x + 1 & 3x^3 + 4x^2 + 5x + 2 \\
& 3x^3 + 3x^2 + 3x \\
& \hline
& x^2 + 2x + 2 \\
& x^2 + x + 1 \\
& \hline
& x + 1
\end{array}
$$
division algorithm

algorithm is

\[ q = 0; \quad r = f; \]

while \( r \neq 0 \) and \( \text{lt}(g) \) divides \( \text{lt}(r) \)

\[ q = q + \frac{\text{lt}(r)}{\text{lt}(g)} \]

\[ r = r - g \frac{\text{lt}(r)}{\text{lt}(g)} \]

it works because

- at the end of every iteration, \( f = qg + r \) holds
- and \( \deg(r) \) drops by at least 1
- it stops when \( r = 0 \) or \( \deg(r) < \deg(g) \)
division theorem

suppose $f, g \in \mathbb{K}[x]$ and $g \neq 0$; then there exists unique $q, r \in \mathbb{K}[x]$ such that

$$f = qg + r$$

and either $r = 0$ or $\deg(r) < \deg(g)$

it’s a smart way of solving a Toeplitz system of linear equations, e.g., if

$\deg(f) = 6$ and $\deg(g) = 4$

$$
\begin{bmatrix}
  f_0 \\
  f_1 \\
  f_2 \\
  f_3 \\
  f_4 \\
  f_5 \\
  f_6 \\
\end{bmatrix}
= 
\begin{bmatrix}
  g_0 \\
  g_1 & g_0 \\
  g_2 & g_1 & g_0 \\
  g_3 & g_2 & g_1 \\
  g_4 & g_3 & g_2 \\
  g_4 & g_3 \\
\end{bmatrix}
\begin{bmatrix}
  q_0 \\
  q_1 \\
  q_2 \\
\end{bmatrix}
+ 
\begin{bmatrix}
  r_0 \\
  r_1 \\
  r_2 \\
  r_3 \\
  0 \\
  0 \\
  0 \\
\end{bmatrix}$$
ideals and division

if $I \subseteq \mathbb{K}[x]$ is an ideal then there is a polynomial $g$ which generates it; i.e.,

$$I = \text{ideal}\{g\}$$

this is true only for *polynomials in one variable*

- so the set

$$I = \text{ideal}\{f_1, \ldots, f_m\}$$

$$= \left\{ \sum_{i=1}^{m} h_i f_i \mid h_i \in \mathbb{R}[x_1, \ldots, x_n] \right\}$$

can be generated using just one polynomial $g$; such an ideal is called a *principle ideal*

- in other words, every polynomial in $I$ is a multiple of $g$
ideals of one-variable polynomials

in fact, we can pick $g$ to be the polynomial of minimum degree in $I$

$$I = \text{ideal}\{g\}$$

then for any $f \in I$ we have

$$f = qg + r$$

and so $r = f - qg$ which implies $r \in I$ also; but we cannot have $\deg(r) < \deg(g)$ since $g$ has minimum degree, so we must have $r = 0$

in fact $g$ is unique up to multiplication by a constant
the greatest common divisor

polynomial $h \in \mathbb{K}[x]$ is called a **greatest common divisor** of $f_1, \ldots, f_m$ if

(i) $h$ divides all of the $f_i$

(ii) any other $p$ that divides all the $f_i$ also divides $h$

in fact, in $\mathbb{K}[x]$ the GCD is the generator of the ideal

$$\text{ideal}\{f_1, \ldots, f_m\} = \text{ideal}\{\text{gcd}\{f_1, \ldots, f_m\}\}$$
the greatest common divisor

let’s show this; we know that there is some polynomial \( g \) such that

\[
\text{ideal}\{f_1, \ldots, f_m\} = \text{ideal}\{g\}
\]

to show it’s a GCD, notice that

(i) \( g \) divides all the \( f_i \)
(ii) if any other \( p \) divides all the \( f_i \) then \( f_i = q_i p \) for some \( h_i \)

but since \( g \in \text{ideal}\{f_1, \ldots, f_m\} \) we must have

\[
g = \alpha_1 f_1 + \cdots + \alpha_m f_m
\]
\[
= (\alpha_1 q_1 + \cdots + \alpha_m q_m)p
\]

so \( p \) divides \( g \)
computing the GCD

if we can compute the GCD of two polynomials, we can compute it for many, since

\[
\gcd\{f_1, \gcd\{f_1, f_2\}\} = \gcd\{f_1, f_2, f_3\}
\]
**Euclidean algorithm (300 B.C.)**

to compute $h = \gcd\{f, g\}$, construct a sequence of polynomials

$$s_0, s_1, s_2, \ldots$$

start with $s_0 = f$ and $s_1 = g$, and define the next in sequence by

$$s_{k+1} = \text{remainder}(s_{k-1}, s_k)$$

stop when $s_n = 0$, then $s_{n-1} = \gcd(f, g)$

this works because if $f = qg + r$ then

$$\gcd(f, g) = \gcd(f - qg, g) = \gcd(r, g)$$

$$\text{ideal}\{f, g\} = \text{ideal}\{f - qg, g\} = \text{ideal}\{r, g\}$$
example

start with $s_0$ and $s_1$

$$s_0 = -3 - 2x - x^2 + 3x^6 + 2x^7 + x^8$$
$$s_1 = 3 - x - 3x^2 + x^3$$

let $s_2$ be the remainder on dividing $s_0$ by $s_1$

$$s_2 = -1638 + 1638x^2$$

let $s_3$ be the remainder on dividing $s_1$ by $s_2$

$$s_3 = 0$$

and normalizing gives $x^2 - 1 = \gcd(s_0, s_1)$
testing ideal membership

to test if $f \in \text{ideal}\{f_1, \ldots, f_m\}$

- compute $g = \gcd\{f_1, \ldots, f_m\}$
- then $f$ is in the ideal if and only if $g$ divides $f$

computing the coefficients

since $g \in \text{ideal}\{f_1, \ldots, f_m\}$ we know there are polynomials $h_1, \ldots, h_m$ such that

$$g = h_1 f_1 + \cdots + h_m f_m$$

if we know these, we can express any $f$ in the ideal in terms of the basis
computing the coefficients

the Euclidean algorithm allows us to find the $h_i$ such that

$$\gcd\{f_1, f_2\} = h_1 f_1 + h_2 f_2$$

in particular, when there is no solution to $f_1(x) = f_2(x) = 0$, this will give the **Nullstellensatz certificate**

to see this, suppose the algorithm terminates with $s_n = 0$; we have $s_{k-1} = q_k s_k + s_{k+1}$ for some $q_k$, so

$$s_{k+1} = s_{k-1} - q_k s_k$$

so we can write the gcd $s_{n-1}$ in terms of $s_{n-2}$ and $s_{n-3}$, and then continue substituting until we have

$$s_{n-1} = \alpha_1 s_0 + \alpha_2 s_1$$
example: Nullstellensatz refutation

suppose we have

\[ f_1 = -1 + 5x^5 + x^8 \quad f_2 = 1 - 2x + x^6 \]

we find \( \text{gcd}\{f_1, f_2\} = 1 \), so \( 1 \in \text{ideal}\{f_1, f_2\} \); i.e., the primal problem is infeasible

the certificate is

\[ h_1 = \frac{1}{48065}(-65287 + 3472x + 5457x^2 + 9892x^3 + 19922x^4 + 36157x^5) \]

\[ h_2 = \frac{1}{48065}(-17222 - 30972x - 56487x^2 - 103082x^3 - 186242x^4 \]

\[ - 9892x^5 - 19922x^6 - 36157x^7) \]
so far

- we have discussed the one-to-one correspondence between ideals and varieties.
- this allows us to convert questions about feasibility of varieties into questions about ideal membership
- but only over the complex numbers

we can compute certificates directly using

- linear algebra
- division algorithms, for polynomials in one variable