4. The Algebraic-Geometric Dictionary

- Equality constraints
- Ideals and Varieties
- 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 and Groebner bases
- Real variables and inequalities

Equality Constraints

Consider the feasibility problem

does there exist $x \in \mathbb{R}^n$ such that

$f_i(x) = 0 \qquad$ for all $i = 1, \ldots, m$

The function $f : \mathbb{R}^n \to \mathbb{R}$ is called a *valid equality constraint* if

$$f(x) = 0 \qquad \text{for all feasible } x$$

Given a set of equality constraints, we can generate others as follows.

(i) If f_1 and f_2 are valid equalities, then so is $f_1 + f_2$

(ii) For any $h \in \mathbb{R}[x_1, \ldots, x_n]$, if f is a valid equality, then so is hf

The Ideal of Valid Equality Constraints

A set of polynomials $I \subset \mathbb{R}[x_1, \ldots, x_n]$ is called an *ideal* if

(i) $f_1 + f_2 \in I$ for all $f_1, f_2 \in I$

(ii) $fh \in I$ for all $f \in I$ and $h \in \mathbb{R}[x_1, \ldots, x_n]$

- Given $f_1, \ldots, f_m$, we can generate an *ideal of valid equalities* by repeatedly applying these rules.
- This gives the *ideal generated by* $f_1, \ldots, f_m$, written $\mathbf{ideal}\{f_1, \ldots, f_m\}$.

$$\mathbf{ideal}\{f_1, \ldots, f_m\} = \left\{ \sum_{i=1}^{m} h_i f_i \mid h_i \in \mathbb{R}[x_1, \ldots, x_n] \right\}$$

  This is also written $\langle f_1, \ldots, f_m \rangle$.
- Every polynomial in $\mathbf{ideal}\{f_1, \ldots, f_m\}$ is a valid equality.

More on Ideals

- For $S \subset \mathbb{R}^n$, the ideal of S is

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

- $\mathbf{ideal}\{f_1, \ldots, f_m\}$ is the smallest ideal containing $f_1, \ldots, f_m$. The polynomials $f_1, \ldots, f_m$ are called the *generators* of the ideal.

- If I_1 and I_2 are ideals, then so is $I_1 \cap I_2$

- Every ideal in $\mathbb{R}[x_1, \ldots, x_n]$ is finitely generated. (This does not hold for non-commutative polynomials)

- An ideal generated by one polynomial is called a principal ideal.

Varieties

We'll need to work over both $\mathbb{R}$ and $\mathbb{C}$; we'll use $\mathbb{K}$ to denote either.

The *variety* defined by polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_m]$ is

$$\mathcal{V}\{f_1, \ldots, f_m\} = \left\{ x \in \mathbb{K}^n \mid f_i(x) = 0 \text{ for all } i = 1, \ldots, m \right\}$$

A variety is also called an *algebraic set*.

- $\mathcal{V}\{f_1, \ldots, f_m\}$ is the set of all solutions x to the feasibility problem

$$f_i(x) = 0 \qquad \text{for all } i = 1, \ldots, m$$

Examples of Varieties

- If $f(x) = x_1^2 + x_2^2 - 1$ then $\mathcal{V}(f)$ is the unit circle in $\mathbb{R}^2$.

- The graph of a polynomial function $h : \mathbb{R} \to \mathbb{R}$ is the variety of $f(x) = x_2 - h(x_1)$.

- The affine set

$$\left\{ x \in \mathbb{R}^n \mid Ax = b \right\}$$

  is the variety of the polynomials $a_i^T x - b_i$

Properties of Varieties

- If V, W are varieties, then so is $V \cap W$

  because if $V = \mathcal{V}\{f_1, \ldots, f_m\}$ and $W = \mathcal{V}\{g_1, \ldots, g_n\}$ then

  $$V \cap W = \mathcal{V}\{f_1, \ldots, f_m, g_1, \ldots, g_n\}$$

- so is $V \cup W$, because

  $$V \cup W = \mathcal{V}\{\, f_i g_j \mid i = 1, \ldots, m, j = 1, \ldots, n \,\}$$

- If V is a variety, the *projection* of V onto a subspace may not be a variety.

- The set-theoretic difference of two varieties may not be a variety.

Feasibility Problems and Duality

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

does there exist $x \in \mathbb{K}^n$ such that

$f_i(x) = 0 \qquad$ for all $i = 1, \ldots, m$

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

So if $1 \in \mathbf{ideal}\{f_1, \ldots, f_m\}$, 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

$$1 = h_1(x)f_1(x) + \cdots + h_m(x)f_m(x) \qquad \text{for all } x \in \mathbb{K}^n$$

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

$$1 \in \mathbf{ideal}\{f_1, \ldots, f_m\} \quad \Longleftrightarrow \quad \mathcal{V}_{\mathbb{C}}\{f_1, \ldots, f_m\} = \emptyset$$

Algebraically Closed Fields

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

$$1 \in \mathbf{ideal}\{f_1, \ldots, f_m\} \qquad \Longleftrightarrow \qquad \mathcal{V}\{f_1, \ldots, f_m\} = \emptyset$$

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

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

$$\begin{aligned} \mathcal{V}_{\mathbb{R}}\{f\} &= \left\{ x \in \mathbb{R} \mid f(x) = 0 \right\} \\ &= \emptyset \end{aligned}$$

But $1 \notin \mathbf{ideal}\{f\}$, since any multiple of f will have degree ≥ 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:

does there exist $x \in \mathbb{C}^n$ such that

$$f_i(x) = 0 \qquad \text{for all } i = 1, \ldots, m$$

The dual problem:

do there exist $h_1, \ldots, h_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that

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

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

Example: Nullstellensatz

Consider the polynomials

$$f_1(x) = x_1^2 \qquad\qquad f_2(x) = 1 - x_1 x_2$$

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

$$\mathcal{V}\{f_1, f_2\} = \emptyset$$

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

$$h_1(x) = x_2^2 \qquad\qquad h_2(x) = 1 + x_1 x_2$$

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

$$1 = h_1(x) f_1(x) + h_2(x) f_2(x) \qquad \text{for all } x$$

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 $\mathcal{V}\{f_1, \ldots, f_m\} = \emptyset$

Duality

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

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

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

with

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

- 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 $\mathcal{I}(S) \supset \mathcal{I}(T)$

The Ideal-Variety Correspondence

Given $S \subset \mathbb{K}^n$, we can construct the ideal

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

Also given an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ we can construct the variety

$$\mathcal{V}(I) = \left\{ x \in \mathbb{K}^n \mid f(x) = 0 \text{ for all } f \in I \right\}$$

If S is a variety, then

$$\mathcal{V}\big(\mathcal{I}(S)\big) = S$$

This implies $\mathcal{I}$ is one-to-one (since $\mathcal{V}$ is a left-inverse); i.e., no two distinct varieties give the same ideal.

The Ideal-Variety Correspondence

We'd like to consider the converse; do every two distinct ideals map to distinct varieties? i.e. is $\mathcal{V}$ one-to-one on the set of ideals?

The answer is no; for example

$$I_1 = \mathbf{ideal}\{(x-1)(x-3)\} \qquad I_2 = \mathbf{ideal}\{(x-1)^2(x-3)\}$$

Both give variety $\mathcal{V}(I_i) = \{1, 3\} \subset \mathbb{C}$.

But $(x-1)(x-3) \notin I_2$, so $I_1 \neq I_2$

The Ideal-Variety Correspondence

It turns out that that, except for multiplicities, ideals are uniquely defined by varieties.To make this precise, define the *radical* of an ideal

$$\sqrt{I} = \left\{ f \mid f^r \in I \text{ for some integer } r \geq 1 \right\}$$

An ideal is called radical if $I = \sqrt{I}$.

One can show, using the Nullstellensatz, that for any ideal $I \subset \mathbb{C}[x_1, \ldots, x_n]$

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

This implies

There is a one-to-one correspondence between radical ideals and varieties

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

We have the following results:

(i) *weak duality*:

$$V = \emptyset \qquad \Longleftarrow \qquad 1 \in I$$

(ii) *Nullstellensatz* (strong duality):

$$V = \emptyset \qquad \Longrightarrow \qquad 1 \in I$$

(iii) *Strong Nullstellensatz*:

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

Computation

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

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

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; 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.

Groebner Bases

We have seen that testing feasibility of a set of polynomial equations over $\mathbb{C}^n$ can be solved if we can test ideal membership.

given $g, f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$, is it true that

$$g \in \mathbf{ideal}\{f_1, \ldots, f_m\}$$

We would like to *divide* the polynomial g by the f_i; i.e. find quotients $q_1, \ldots, q_m$ and remainder r such that

$$g = q_1 f_1 + \cdots + q_m f_m + r$$

Clearly, if $r = 0$ then $g \in \mathbf{ideal}\{f_1, \ldots, f_m\}$.

The converse is not true, unless we use a special generating set for the ideal, called a *Groebner basis*. This is computationally expensive to compute in general.

Real Variables, and Inequalities

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 this does not deal with

- inequality constraints
- *real-valued* polynomials

As we shall see, these questions are linked.