Lecture 21  Infeasibility of Polynomial System

1 Hilbert’s Nullstellensatz

Let \( f_1(x), \ldots, f_m(x) \in \mathbb{C}[x] \). When do we know the polynomial equations
\[
f_1(x) = f_2(x) = \cdots = f_m(x) = 0
\]
does NOT have a complex solution? A certificate for the emptyness is that there exist polynomials \( q_1(x), \ldots, q_m(x) \) such that
\[
q_1(x)f_1(x) + \cdots + q_m(x)f_m(x) = 1.
\]

**Theorem 1** (Weak Nullstellensatz). Let \( f_1(x), \ldots, f_m(x) \in \mathbb{C}[x] \). They do NOT have a common complex zero point if and only if there exist polynomials \( q_1(x), \ldots, q_m(x) \) such that
\[
q_1(x)f_1(x) + \cdots + q_m(x)f_m(x) = 1.
\]

**Example 2.** The polynomial system
\[
1 + x^2 = 0, \quad 1 + x^2 + x^4 = 0
\]
has no complex roots, because
\[
-x^2(1 + x^2) + 1 + x^2 + x^4 = 1.
\]

Now suppose \( V(f_1, \ldots, f_m) \) is nonempty. How do we know \( f(x) = 0 \) for all \( x \in V(f_1, \ldots, f_m) \).

**Theorem 3** (Strong Nullstellensatz). Let \( f(x), f_1(x), \ldots, f_m(x) \in \mathbb{C}[x] \). If \( f(x) \) vanishes on the variety \( V(f_1, \ldots, f_m) \), then there exist a positive integer \( k > 0 \) and polynomials \( q_1(x), \ldots, q_m(x) \) such that
\[
f(x)^k = q_1(x)f_1(x) + \cdots + q_m(x)f_m(x).
\]
Furthermore, if the ideal \( \langle f_1, \ldots, f_m \rangle \) is radical, then we can choose \( k = 1 \) in the above.

**Proof.** Consider the polynomial system in \( (x_1, \ldots, x_n, y) \)
\[
1 - yf(x) = f_1(x) = \cdots = f_m(x) = 0.
\]
Then it has no complex solutions. By Weak Nullstellensatz, there exist \( p_i \) and \( q \) such that
\[
1 = p_1f_1 + \cdots + p_mf_m + q(1 - yf).
\]
Replace \( y \) be \( 1/f \), we get
\[
1 = p_1(x, 1/f)\frac{1}{f_1} + \cdots + p_m(x, 1/f)\frac{1}{f_m}.
\]
Now multiplying \( f^m \) for \( m \) big enough, we get
\[
f^m = q_1(x)f_1 + \cdots + q_m(x)f_m.
\]
2 Real Nullstellensatz

Let $f_1(x), \ldots, f_m(x) \in \mathbb{R}[x]$. When do we know the polynomial equations

$$f_1(x) = f_2(x) = \cdots = f_m(x) = 0$$

does NOT have a real solution? A certificate for the emptiness is that there exist polynomials $q_1(x), \ldots, q_m(x)$ and an SOS polynomial $s(x)$ such that

$$s(x) + q_1(x)f_1(x) + \cdots + q_m(x)f_m(x) = -1.$$

Theorem 4 (Real Nullstellensatz). Let $f_1(x), \ldots, f_m(x) \in \mathbb{R}[x]$. They do NOT have a common real zero point if and only if there exist polynomials $q_1(x), \ldots, q_m(x)$ and an SOS polynomial $s(x)$ such that

$$s(x) + q_1(x)f_1(x) + \cdots + q_m(x)f_m(x) = -1.$$

3 Positstellensatz

Let $f_1(x), \ldots, f_m(x), g_1(x), \ldots, g_r(x), h_1(x), \ldots, h_t(x) \in \mathbb{R}[x]$. When do we know the set

$$S = \{x \in \mathbb{R}^n : f_i(x) = 0, g_j(x) \geq 0, h_k(x) \neq 0, \forall i, j, k\}$$
does NOT have a real solution?

Theorem 5. Let $f_i, g_j, h_k$ be real polynomials in the above. Then the set $S$ is empty if and only if there exist real polynomials $q_i(x)$, sos polynomials $\sigma_\nu$ and integers $u_i$ such that and an SOS polynomial $s(x)$ such that

$$\sum_{i=1}^m q_i(x)f_i(x) + \sum_{\nu \in \{0,1\}^r} \sigma_\nu g_1(x)^{\nu_1} \cdots g_r(x)^{\nu_r} + \prod_{k=1}^t h_k(x)^{u_k} = 0.$$

Example 6. Consider the polynomial system

$$S = \{f = x - y^2 + 3 \geq 0, g = y + x^2 + 2 = 0\}$$
is empty. There exist $s_3$ and SOS $s_1, s_2$ such that

$$s_1 + s_2 f + s_3 \cdot g \equiv 0.$$

Here $s_i$ are given as

$$s_1 = \frac{1}{3} + 2(y + \frac{3}{2})^2 + 6(x - \frac{1}{6})^2, \quad s_2 = 2, \quad s_3 = -6.$$