A proof of Hilbert's Nullstellensats using Gröbner basis *

Yuji Kobayashi

Laboratory of Mathematics and Games
(https://math-game-labo.com)

Abstract

In this note, we present a clear and dynamic proof of Hilbert's Nullstellensatz involving Gröbner basis computations. The so-called weak form of the theorem easily implies the full statement, and we prove a result concerning generators of maximal ideals, which is equivalent to the weak form, using Gröbner bases.

1 Gröbner basis.

Let $R = K[X_1, X_2, \ldots, X_n]$ be a polynomial ring over a field K with n variables, and let $M = M(X_1, X_2, \ldots, X_n)$ denote the set of all monomials in R. We fix a term order $\geq$ that is, a total order on M which is compatible with multiplication and is a well-order.

For $f \in R$, we denote by $\mathrm{lt}(f)$, $\mathrm{lc}(f)$ and $\mathrm{lm}(f)$ the leading term, leading coefficient and leading monomial of f, respectively. We have

$$\mathrm{lt}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f), \ \ f = \mathrm{lt}(f) + \mathrm{rt}(f),$$

where the $\mathrm{rt}(f)$ is the sum of the remaining terms of f.

Let $g = u + \mathrm{rt}(g)$ be a monic polynomial, the is, $\mathrm{lc}(g) = 1$, with $u \in M$. If $f \in R$ contains a term av with $a \in K, v \in M$, such that $u \,|\, v$, that is, $v = uw$ for some $w \in M$, then f is reduced to

$$f_1 = f - awg = (f - av) - aw \cdot \mathrm{rt}(g).$$

In this situation, we write

$$f \to_g f_1.$$

Let G be a set of monic polynomials of R. We write

$$f \to_G f_1,$$

*This is a preliminary report and will not be published elsewhere in this current form.

if $f \to_g f_1$ for some $g \in G$. Fuethermore, we write

$$f \to_G^* \overline{f},$$

if there exists a sequence

$$f \to_{g_1} f_1 \to_{g_2} \cdots \to_{g_n} f_n = \overline{f}$$

with $g_1, g_2, \ldots, g_n \in G$.

We say that $f \in R$ is irreducible with respect to G, if no $g \in G$ can be applied to reduce f. An irreducible $\overline{f} \in R$ is called a normal form of f with respect to G, if $f \to_G^* \overline{f}$.

Proposition 1.1. *Any reduction sequence $f \to_G f_1 \to_G f_2 \to \cdots$ eventually teminates and yields a normal form $\overline{f}$ of f, that is, $\overline{f} = f_n$ for some n.*

Let $I(G)$ denote the ideal of R generated by G. We say that G is a Gröbner basis of I if $f \to_G^* 0$ for every $f \in I$.

Theorem 1.2. *Suppose that G is a Gröbner basis of $I(G)$. Then*

(1) *For every $f \in R$, there exists the unique normal from $\overline{f}$ of f with respect to G.*

(2) *For any $f, g \in R$, $f \equiv g \pmod{I}$ if and only if $\overline{f} = \overline{g}$ (in R).*

A Gröbner basis G is said to be reduced if every $g \in G$ is irreducible with respect to $G \setminus \{g\}$.

Theorem 1.3. *For any given term order, every ideal I of R admits a unique finite reduced Gröbner basis.*

2 Hilbert's Nullstellensats

From now on, K is an algebraically closed field. Let I be an ideal of $R = K[X_1, X_2, \ldots, X_n]$ and let $\sqrt{I}$ denote the radical of I, that is,

$$\sqrt{I} = \{f \in R \mid f^e \in I \text{ for some } e > 0\}.$$

For a point $p = (x_1, x_2, \ldots, x_n) \in K^n$, $f(p) = f(x_1, x_2, \cdots, x_n)$ is an element of K. Let $V(I)$ be the algebraic set defined by I, that is,

$$V(I) = \{p \in K^n \mid f(p) = 0 \text{ for all } f \in I\}.$$

Conversely, for a subset $V \subseteq K^n$, define an ideal $I(V)$ by

$$I(V) = \{f \in R \mid f(p) = 0 \text{ for all } p \in V\}.$$

Clearly, we have

$$I \subseteq I(V(I)).$$

Theorem 2.1. (Hilbert's Nullstellensatz). *It holds that*

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

In other words,

$$f(p) = 0 \text{ for all } p \in V(I) \iff f^e \in I \text{ for some } e > 0.$$

This theorem follows relatively easily from its weak form.

Theorem 2.2. *If $I \neq R$, then $V(I) \neq \emptyset$.*

This weak form is a straight consequence of

Lemma 2.3. *Every maximal ideal of R is generated by $\{X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n\}$ with $a_1, a_2, \ldots, a_n \in K$.*

Indeed, the ideal I is containsed in a maximal ideal $J = \{X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n\}$, and hence

$$p = (a_1, a_1, \ldots, a_n) \in V(J) \subseteq V(I),$$

showing that $V(I) \neq \emptyset$.

3 Proof of Lemma

We give a proof of Lemma 2.3 using Gröbner basis.

Let I be a maximal ideal of R, and let $\varphi : R \to R/I$ be the canonical homomorphism. Then, R/I is a field containing K, and φ is a K-algebra homomorphism.

If every $a_i = \varphi(X_i)$ is algebraic over K, then $a_i \in K$ because K is algebraically closed. In this case, $X_i - a_i \in I$, so I is generated by $X_1 - a_1, \ldots, X_n - a_n$, and we are done. Thus, we may suppose that a_1 is transcendental over K.

Let $\geq$ be a term order with $X_1 < X_2 < \cdots < X_n$, and let

$$G = \{g^{(1)}, g^{(2)}, \ldots, g^{(m)}\}$$

be the reduced Gröbnerbasis of I with respect to $\geq$. Each $g^{(i)}$ can be written in the form

$$g^{(i)} = f_1^{(i)} u_1^{(i)} - f_2^{(i)} u_2^{(i)} - \cdots - f_{m_i}^{(i)} u_{m_i}^{(i)},$$

where $f_1^{(i)}, f_2^{(i)}, \ldots, f_{m_i}^{(i)} \in K[X_1]$ are monic polynomials, and $u_1^{(i)} > u_2^{(2)} > \cdots > u_{m_i}^{(i)}$ are monomials in $M_1 = M(X_2, X_3, \ldots, X_n)$. Because a_1 is transcendental over K, we see that $u_1^{(i)} \neq 1$ for every i; otherwise we would have $g^{(i)}(a_1) = f_1^{(i)}(a_1) = 0$ for some i.

Now let $p \in K[X_1]$ be an irreducible polynomial that does not devide any $f_1^{(i)}$ $(i = 1, 2, \ldots, m)$. Let $q \in R$ be the inverse of p modulo I, that is,

$$pq \equiv 1 \pmod{I}.$$

If q contains a term $cX_1^e v u_1^{(i)}$ ($c \in K, e \in \mathbb{N}, v \in M_1$), then multiplying by $f_1^{(1)}$, we can apply a deduction

$$cX_1^e f_1^{(i)} v u_1^{(i)} \ \rightarrow_{g^{(i)}} \ cX_1^e (f_2^{(i)} v u_2^{(i)} + \cdots + f_{m_i}^{(i)} v u_{m_i}^{(i)}).$$

Hence, by choosing a sufficiently large enough integer e_i, the product $(f_1^{(i)})^{e_i} q$ is reduced to a polynomial in whith no term contains $u_1^{(i)}$. So, taking a much more large integer e, and letting $f = (f_1^{(i)} f_2^{(i)} \cdots f_{m_i}^{(i)})^e$, we see that fq is reduced to a polynomial $h \in R$ in which no term contains any $u_1^{(i)}$ (i=1,2,. . . ,m). We have

$$f \equiv fqp \equiv hp \pmod{I}.$$

Since the both sides are irreducible under G, Theorem 1.2, (2) implies that f and hp are equal in R, that is, $f = hp$. Because p was chosen not to devide f, this is a contradiction.

Q.E.D.

References

[1] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, 5th ed., Undergraduate Texts in Mathematics, Springer, 2021.