The Generalized Rabinowitsch's Trick

Dingkang Wang[1], Yao Sun[2], and Jie Zhou[1]

[1] KLMM, Academy of Mathematics and Systems Science, CAS, Beijing, China
[2] SKLOIS, Institute of Information Engineering, CAS, Beijing, China

The classical Rabinowitsch trick was proposed by J.L. Rabinowitsch in his 1-page paper *Zum Hilbertschen Nullstellensatz* in 1929. This ingenious trick was used to prove the famous Hilbert's Nullstellensatz theorem. Indeed, given polynomials $f, f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$ or $k[X]$. If f vanishes on the common zeros of $f_1, \ldots, f_s$, then there exists polynomials $a_0, a_1, \ldots, a_s$ in $k[X, y]$, such that

$$a_0(fy - 1) + a_1 f_1 + \cdots + a_s f_s = 1,$$

where y is an extra variable different from X. Substituting y by $1/f$, there exists an integer m such that f^m in the ideal which is generated by $f_1, \ldots, f_s$.

We present a generalization of Rabinoswitsch's trick, which is an integration of Rabinowitsch's trick with Bayer's idea. We consider the following polynomial ideal

$$J = I + \langle fy - z \rangle \subset k[X, y, z],$$

associated with I and f, where y and z are two new variables different from X.

We analyze the ideal J by studying its Gröbner bases using a block ordering in which $y \gg z \gg X$. Using the structure of this Gröbner bases, we give the main theoretical result as follows.

Theorem 1. *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a Gröbner basis of ideal $J = I + \langle fy - z \rangle \subset k[X, y, z]$ with respect to a block ordering such that $y \gg z \gg X$.*

1. *Let $P_s = \{\mathrm{lc}_{y,z}(g) \mid g \in G \cap k[X][z], \mathrm{lpp}_{y,z}(g) = z^k \text{ and } 0 \le k \le s\} \subset k[X]$. For any integer $s \ge 0$, P_s is a Gröbner bases of $I : f^s$.*
2. *Let $Q_s = P_s \cup \{\mathrm{lc}_{y,z}(g) \mid g \in G, \mathrm{lpp}_{y,z}(g) = yz^t, \text{ and } 0 \le t \le s\} \subset k[X]$. For any integer $s \ge 0$, Q_s is a Gröbner bases of $I : f^s + \langle f \rangle$.*

The following result serves as the basis for checking if a polynomial is invertible or a zero divisor in a residue class ring as well as for checking its membership in the radical of an ideal.

Theorem 2. *Let I be an ideal and f be a polynomial in $k[X]$. Let G be a minimal Gröbner basis of ideal $J = I + \langle fy - z \rangle \subset k[X, y, z]$ with respect to a block ordering such that $y \gg z \gg X$, and P_s, Q_s are constructed from G as stated in Theorem 1. Then the following asserts hold:*

1. *f is **invertible** in $k[X]/(I : f^s)$ if and only if $1 \in Q_s$ and $1 \notin P_{s+1}$, i.e. $I : f^s + \langle f \rangle = \langle 1 \rangle$ and $f \notin I : f^s$. That is, there is a polynomial $g = yz^t + p_{t-1}yz^{t-1} + \cdots + p_0 y + q_r z^r + \cdots + q_1 z + q_0$ in G, where $p_0, \ldots, p_{t-1}, q_0, \ldots, q_r \in k[X]$ and $0 \le t \le s$, and $-q_{t+1}$ is an inverse of f in $k[X]/(I : f^s)$.*

2. *f is a **zero divisor** in $k[X]/(I : f^s)$ if and only if $P_s \subsetneqq P_{s+1}$ and $1 \notin P_{s+1}$, i.e. $I : f^s \subsetneqq I : f^{s+1}$ and $f \notin I : f^s$.*
3. *f is **in the radical ideal** $\sqrt{I}$ if and only if there exists an integer s such that $1 \in P_s$, i.e. $I : f^s = \langle 1 \rangle$.*
4. *m is the **smallest** integer such that $I : f^\infty = I : f^m$, if and only if $P_{m-1} \subsetneqq P_m = P_s$ for all $s > m$. Further, P_m is a Gröbner bases of $I : f^\infty$.*

The above results can be applied to automatical proving of geometric theorems.