Bounds and Algorithms for Polynomial Rings over the Integers

Matthias Aschenbrenner

March 2003

Let R be a commutative ring. Given polynomials

$$f_0(X), f_1(X), \ldots, f_n(X) \in R[X],$$

where $X = (X_1, \ldots, X_N)$, are there $g_1, \ldots, g_n \in R[X]$ such that

$$f_0 = g_1 f_1 + \cdots + g_n f_n \quad ?$$

This is the *ideal membership problem for* $R[X]$.

Some aspects discussed in this talk:

- *decidability;*
- *existence of bounds;*
- *dependence on parameters.*

Theorem. (G. Hermann, J. König, A. Seidenberg)

Suppose that $R = K$ *is a field and* $\deg f_i \leqslant d$ *for* $i = 0, \ldots, n$*. If* $f_0 \in (f_1, \ldots, f_n)$*, then*

$$f_0 = g_1 f_1 + \cdots + g_n f_n$$

for certain $g_1, \ldots, g_n \in K[X]$ *of degree at most*

$$\beta(N, d) = (2d)^{2^N}.$$

Remarks.

(1) The "computable" character of the bound β implies the existence of a (naive) algorithm to solve ideal membership for $K[X]$ if K is "computable". (But there are "better" algorithms: Gröbner bases, ...)

(2) The doubly exponential nature of β is essentially unavoidable (Mayr-Meyer, 1982).

(3) In many particular cases, better bounds (single exponential) are known, e.g.:

- if $f_0 = 1$ (effective Hilbert Nullstellensatz: Brownawell, Kollár, ...),

- if $I = (f_1, \ldots, f_n)$ is zero-dimensional or a complete intersection (Berenstein-Yger), or if I is unmixed (Dickenstein-Fitchas-Giusti-Sessa).

(4) Dependence on parameters: if

$$f_0(C, X), \ldots, f_n(C, X) \in \mathbb{Z}[C, X]$$

are "general" polynomials, with parametric variables $C = (C_1, \ldots, C_M)$, then for each field K the set

$$\Big\{c \in K^M : f_0(c, X) \in \Big(f_1(c, X), \ldots, f_n(c, X)\Big)K[X]\Big\}$$

is a *constructible* subset of K^M.

Ideal membership in $\mathbb{Z}[X]$.

Algorithms for deciding ideal membership

$$f_0 \in (f_1, \ldots, f_n)\mathbb{Z}[X]$$

in $\mathbb{Z}[X]$ have been known for a long time. (Maybe Kronecker himself had found one already.)

For example, one can use the fact that the rings

$$\mathbb{Z}[X]/(f_1, \ldots, f_n)$$

are *residually finite:* if

$$f_0 \notin (f_1, \ldots, f_n),$$

then this is witnessed by a homomorphism $h \colon \mathbb{Z}[X] \to R$ with

$$h(f_1) = \cdots = h(f_n) = 0, h(f_0) \neq 0,$$

where R is a *finite* ring (commutative, with 1).

But the existence of bounds similar to the ones in Hermann's theorem for polynomial rings over fields was not known.

One difference to the case of fields: if a bound d on the degree of $f_0, \ldots, f_n \in \mathbb{Z}[X]$ is given and $f_0 \in (f_1, \ldots, f_n)\mathbb{Z}[X]$, then *there is no uniform bound on the degrees of the g_j's, depending only on N and d, such that*

$$f_0 = g_1 f_1 + \cdots + g_n f_n.$$

(Here we choose $\max_j \deg g_j$ minimally.)

Example. Let $p, d \in \mathbb{Z}$, $p > 1$, $d \geqslant 1$. We have

$$1 = \left(1 + pX + \cdots + p^{d-1}X^{d-1}\right)(1 - pX) + X^{d-1}p^d X,$$

with the degrees of

$$1 + pX + \cdots + p^{d-1}X^{d-1} \quad \text{and} \quad X^{d-1}$$

tending to infinity, as $d \to \infty$.

Theorem. (Gallo-Mishra, 1994)

Let $f_0, \dots, f_n \in \mathbb{Z}[X]$. *If* $f_0 \in (f_1, \dots, f_n)$, *then*

$$f_0 = g_1 f_1 + \cdots + g_n f_n$$

for certain polynomials $g_1, \dots, g_n \in \mathbb{Z}[X]$ *whose size* $|g_j|$ *is bounded by*

$$W_{4N+8}\Big(|f_0| + \cdots + |f_n|\Big).$$

Here, the size $|f|$ of a polynomial $f = \sum_\nu a_\nu X^\nu$ ($a_\nu \in \mathbb{Z}$) is a crude measure of its complexity:

$$|f| := \max\Big\{\max_\nu |a_\nu|, \max_i \deg_{X_i} f\Big\}.$$

The function W_k is the kth function in the "Wainer hierarchy of primitive recursive functions". These functions are rapidly growing:

$$W_0(n) = n + 1,$$
$$W_1(n) = 2n + 1,$$
$$W_2(n) \sim 2^n,$$
$$W_3(n) \sim 2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}} \ (n \text{ times}), \ \dots$$

Theorem. *Suppose* $f_0, f_1, \dots, f_n \in \mathbb{Z}[X]$ *are polynomials with* $f_0 \in (f_1, \dots, f_n)$, *and*

$$\deg f_j, \log ||f_j|| \leqslant B \qquad \textit{for all } j = 0, \dots, n.$$

Then

$$f_0 = g_1 f_1 + \cdots + g_n f_n$$

for certain polynomials $g_1, \dots, g_n \in \mathbb{Z}[X]$ *with*

$$\deg g_j, \log ||g_j|| \leqslant (2B)^{2^{O(N^2)}}$$

for $j = 1, \dots, n$.

Here, for $f = \sum_\nu a_\nu X^\nu \in \mathbb{Z}[X]$, we put

$$||f|| := \max_\nu |a_\nu|.$$

Remark. In principle, one can determine the constant hidden in the "O"-notation explicitly from the proof. Again, we also get a (naive) algorithm for deciding ideal membership in $\mathbb{Z}[X]$.

Height of polynomials. For a non-zero polynomial $f = \sum_\nu a_\nu X^\nu \in \mathbb{Z}[X]$, we define

$$m^+(f) = \int_0^1 \cdots \int_0^1 \log^+|f(e^{2\pi i\theta_1}, \ldots, e^{2\pi i\theta_N})| d\theta_1 \cdots d\theta_N,$$

where

$$\log^+ x = \max\{0, \log x\} \qquad \text{for } x \in \mathbb{R},\ x > 0.$$

We put $m^+(0) := 0$.

We also define

$$\deg_{X_i} f = \text{degree of } f \text{ in } X_i,$$
$$\deg_{(X)} f = \sum_{i=1}^{N} \deg_{X_i} f,$$

and

$$h(f) := m^+(f) + \deg_{(X)} f,$$

and we let $h(0) := 0$. We call $h(f) \geqslant 0$ the **height** of $f \in \mathbb{Z}[X]$.

Properties. For $f, g, f_1, \ldots, f_n \in \mathbb{Z}[X]$, $n > 0$:

(1) $h(f) = h(-f)$,

(2) $h(fg) \leqslant h(f) + h(g)$, and $h(f^n) = nh(f)$,

(3) $h(f_1 + \cdots + f_n) \leqslant h(f_1) + \cdots + h(f_n) + \log n$,

(4) $C_1 \deg_{(X)} f \leqslant h(f) - \log|f| \leqslant C_2 \deg_{(X)} f$, for some (universal) constants $C_1, C_2 > 0$. (Hence, given $C \geqslant 0$ there are only finitely many $f \in \mathbb{Z}[X]$ with $h(f) \leqslant C$.)

(5) h extends to a height function on $\mathbb{Q}(X)^{\mathrm{alg}}$ which is $\mathrm{Gal}\Big(\mathbb{Q}(X)^{\mathrm{alg}} | \mathbb{Q}(X)\Big)$-invariant.

Notation. For an $m \times n$-matrix $A = (a_{ij})$ with $a_{ij} \in \mathbb{Z}[X]$ put

$$h(A) = \max_{i,j} h(a_{ij}).$$

Let $A = (a_{ij}) \in \Big(\mathbb{Z}[X]\Big)^{m\times n}$, and let $b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$ be a column vector with entries b_i in $\mathbb{Z}[X]$, and consider the system of linear equations

$$Ay = b. \tag{$*$}$$

Theorem. *The system* $(*)$ *has a solution* $y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \in \Big(\mathbb{Z}[X]\Big)^n$ *if and only if it has such a solution with*

$$\deg y_j \leqslant \Big(m\Big(h(A,b)+1\Big)\Big)^{2^{O(N^2)}}$$

for $j = 1, \ldots, n$. (The case $m = 1$ yields Theorem 1.)

Note that $y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} \in \Big(\mathbb{Z}[X]\Big)^n$ is a solution to "$Ay = b$" if and only if

$$(A, -b)\begin{bmatrix} y \\ 1 \end{bmatrix} = 0.$$

So deciding whether "$Ay = b$" has a solution in $\mathbb{Z}[X]$ reduces to:

(a) *Constructing a collection of generators*

$$z^{(1)}, \ldots, z^{(L)} \in \Big(\mathbb{Z}[X]\Big)^{n+1}$$

for the module of solutions (in $\mathbb{Z}[X]$*) to* "$(A, -b)z = 0$", *and*

(b) *deciding whether the ideal in* $\mathbb{Z}[X]$ *generated by the last components of the vectors* $z^{(1)}, \ldots, z^{(L)}$ *contains* 1.

We will first concentrate on part (a):

Let $A \in \Big(\mathbb{Z}[X]\Big)^{m\times n}$. *How does one construct a finite set of generators for the submodule*

$$\mathsf{S}_{\mathbb{Z}[X]}(A) = \Big\{y \in \Big(\mathbb{Z}[X]\Big)^{n} : Ay = 0\Big\}$$

of the free $\mathbb{Z}[X]$*-module* $\Big(\mathbb{Z}[X]\Big)^{n}$ *?*

Restricted p-adic power series. (p prime.)

$$\begin{aligned}\mathbb{Z}_p &:= \text{completion of } \mathbb{Z} \text{ with respect to} \\ &\qquad \text{the } (p)\text{-adic topology} \\ &= \text{ring of } p\text{-adic integers.}\end{aligned}$$

We have $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, with residue homomorphism $a \mapsto \overline{a} \colon \mathbb{Z}_p \to \mathbb{F}_p$.

$$\begin{aligned}\mathbb{Z}_p\langle X\rangle &:= \text{completion of } \mathbb{Z}[X] \text{ with respect to} \\ &\qquad \text{the } (p)\text{-adic topology} \\ &= \text{ring of } p\text{-}\textbf{adic restricted} \\ &\qquad \textbf{power series.}\end{aligned}$$

We may regard $\mathbb{Z}_p\langle X\rangle$ as a subring of $\mathbb{Z}_p[[X]]$: Its elements are the power series

$$f = \sum_\nu a_\nu X^\nu \in \mathbb{Z}_p[[X]]$$

such that $a_\nu \to 0$ (in the (p)-adic topology on $\mathbb{Z}_p[[X]]$) as $\deg \nu \to \infty$. Here

$$\nu = (\nu_1, \dots, \nu_N) \in \mathbb{N}^N, \qquad X^\nu := X_1^{\nu_1} \cdots X_N^{\nu_N}.$$

Note $\mathbb{Z}_p\langle X'\rangle \subseteq \mathbb{Z}_p\langle X\rangle$, $X' := (X_1, \dots, X_{N-1})$.

We have $\mathbb{Z}_p\langle X\rangle/p\mathbb{Z}_p\langle X\rangle \cong \mathbb{F}_p[X]$, with residue homomorphism

$$f \mapsto \overline{f} = \sum_{\nu} \overline{a_\nu} X^\nu\colon\ \mathbb{Z}_p\langle X\rangle \to \mathbb{F}_p[X].$$

A power series $f \in \mathbb{Z}_p\langle X\rangle$ is called **regular in X_N of degree** $s \in \mathbb{N}$ if $\overline{f}$ is unit-monic in X_N of degree s.

Fact 1: Weierstrass Division.
Let $f \in \mathbb{Z}_p\langle X\rangle$ be regular in X_N of degree s. Then for each $g \in \mathbb{Z}_p\langle X\rangle$ there are uniquely determined $q \in \mathbb{Z}_p\langle X\rangle$ and $r \in \mathbb{Z}_p\langle X'\rangle[X_N]$ of degree $< s$ (in X_N) such that $g = qf + r$.

Fact 2: Weierstrass Preparation.
For every $f \in \mathbb{Z}_p\langle X\rangle$ regular in X_N of degree s there exists a uniquely determined unit $u \in \mathbb{Z}_p\langle X\rangle$ and a monic polynomial $g \in \mathbb{Z}_p\langle X'\rangle[X_N]$ of degree s such that $f = ug$.

(*If $f \in \mathbb{Z}_p\langle X'\rangle[X_N]$, then $u \in \mathbb{Z}_p\langle X'\rangle[X_N]$.*)

Fact 3: Flatness of $\mathbb{Z}_p\langle X\rangle$ over $\mathbb{Z}[X]$.
Let $A \in \Big(\mathbb{Z}[X]\Big)^{m\times n}$. The $\mathbb{Z}_p\langle X\rangle$-module

$$\mathsf{S}_{\mathbb{Z}_p\langle X\rangle}(A)$$

of solutions to

$$Ay = 0$$

in $\mathbb{Z}_p\langle X\rangle$ is generated by solutions in $\mathbb{Z}[X]$.

Fact 4: *Let $A \in \Big(\mathbb{Z}_{(p)}[X]\Big)^{m\times n}$. Suppose that*

$$y^{(1)}, \ldots, y^{(K)} \in \Big(\mathbb{Z}_{(p)}[X]\Big)^n$$

generate the $\mathbb{Q}[X]$-module $\mathsf{S}_{\mathbb{Q}[X]}(A)$, and

$$z^{(1)}, \ldots, z^{(L)} \in \Big(\mathbb{Z}_{(p)}[X]\Big)^n$$

generate the $\mathbb{Z}_p\langle X\rangle$-module $\mathsf{S}_{\mathbb{Z}_p\langle X\rangle}(A)$, then

$$y^{(1)}, \ldots, y^{(K)}, z^{(1)}, \ldots, z^{(L)}$$

generate the $\mathbb{Z}_{(p)}[X]$-module $\mathsf{S}_{\mathbb{Z}_{(p)}[X]}(A)$.

(Follows from faithful flatness of $\mathbb{Z}_p\langle X\rangle$ over its subring $S_e^{-1}\mathbb{Z}_{(p)}[X]$, where $S_e = 1 + p^e\mathbb{Z}_{(p)}[X]$, $e \geqslant 1$.)

Lemma. *Let* $A \in \left(\mathbb{Z}[X]\right)^{m\times n}$*. Suppose that*

$$y^{(1)}, \ldots, y^{(K)} \in \mathsf{S}_{\mathbb{Z}[X]}(A)$$

generate $\mathsf{S}_{\mathbb{Q}[X]}(A)$ *and* $\mathsf{S}_{\mathbb{Z}_p\langle X\rangle}(A)$ *for all primes* p*. Then they generate* $\mathsf{S}_{\mathbb{Z}[X]}(A)$*.*

Proof. By Fact 4, the $y^{(k)}$ generate $\mathsf{S}_{\mathbb{Z}_{(p)}[X]}(A)$ for all primes p. Suppose $y \in \mathsf{S}_{\mathbb{Z}[X]}(A)$. In particular $y \in \mathsf{S}_{\mathbb{Q}[X]}(A)$, hence there exists $0 \neq \delta \in \mathbb{Z}$ and $g_1, \ldots, g_K \in \mathbb{Z}[X]$ such that

$$\delta y = g_1 y^{(1)} + \cdots + g_K y^{(K)}.$$

Let $p_1, \ldots, p_L$ be the different prime factors of δ. So there exist $\delta_l \in \mathbb{Z} \setminus p_l\mathbb{Z}$ and $g_{1l}, \ldots, g_{Kl} \in \mathbb{Z}[X]$ such that

$$\delta_l y = g_{1l} y^{(1)} + \cdots + g_{Kl} y^{(K)}.$$

Since $\gcd(\delta, \delta_1, \ldots, \delta_L) = 1$, we can write 1 as $\mathbb{Z}$-linear combination of $\delta, \delta_1, \ldots, \delta_L$, and thus y as $\mathbb{Z}[X]$-linear combination of $y^{(1)}, \ldots, y^{(K)}$. $\square$

We now show how to construct $y^{(k)}$'s with the properties in the lemma. (= a constructive proof of Fact 3, uniform in p)

We proceed by induction on N. Consider the special case of one homogeneous equation:

$$f_1 y_1 + \cdots + f_n y_n = 0, \qquad (\diamond)$$

with $f_1, \ldots, f_n \in \mathbb{Z}[X]$. We may assume that $f_j \neq 0$ for some j. After dividing each f_j by the gcd of the coefficients of $f_1, \ldots, f_n$, we may assume moreover that for each prime p *some* f_j is non-zero mod p.

The equation $(\diamond)$ has the special solutions

$$\Big[0, \ldots, 0, -f_j, 0, \ldots, 0, f_i, 0, \ldots, 0\Big] \quad \text{for } 1 \leqslant i < j \leqslant n. \qquad (\diamond\diamond)$$

If $N = 0$, the solutions ($\diamond\diamond$) generate the $\mathbb{Q}$-vector space of solutions to ($\diamond$) in $\mathbb{Q}^n$, and the $\mathbb{Z}_p$-module of solutions to ($\diamond$) in ${\mathbb{Z}_p}^n$, for each prime p.

Suppose $N > 0$. Let $d = \max_j \deg_{X_N} f_j$. After applying a suitable $\mathbb{Z}_p$-automorphism of $\mathbb{Z}_p\langle X\rangle$ we may assume that

- each f_j, as element of $\mathbb{Q}[X]$, is unit-monic (so Euclidean Division by f_j is possible);

- for each prime p, *some* f_j, regarded as element of $\mathbb{Z}_p\langle X\rangle$, is regular in X_N (so Weierstrass Division by f_j is possible).

Write each unknown y_j as

$$y_j = y_{j0} + y_{j1}X_N + \cdots + y_{j,d-1}{X_N}^{d-1}$$

with new unknowns y_{jk} ($1 \leqslant j \leqslant n$, $0 \leqslant k < d$).

Comparing the coefficients of equal powers of X_N, ($\diamond$) gives rise to a homogeneous system

$$A'y' = 0 \qquad (\diamond')$$

of $2d$ equations in the nd unknowns $y' = (y_{jk})$, with coefficients in $\mathbb{Z}[X']$. Applying the induction hypothesis to ($\diamond'$), we obtain solutions

$$y^{(1)}, \ldots, y^{(K)} \in \Big(\mathbb{Z}[X]\Big)^n$$

to ($\diamond$) with the following properties:

- every solution $(y_1, \ldots, y_n) \in \Big(\mathbb{Q}[X]\Big)^n$ to ($\diamond$) with each y_j having X_N-degree $< d$ is a $\mathbb{Q}[X]$-linear combination of $y^{(1)}, \ldots, y^{(K)}$;

- for all primes p, every solution $(z_1, \ldots, z_n) \in \Big(\mathbb{Z}_p\langle X'\rangle[X_N]\Big)^n$ to ($\diamond$) with each z_j having X_N-degree $< d$ is a $\mathbb{Z}_p\langle X\rangle$-linear combination of $y^{(1)}, \ldots, y^{(K)}$.

Let now

$$y = (y_1, \dots, y_n) \in \Big(\mathbb{Q}[X]\Big)^n$$
$$z = (z_1, \dots, z_n) \in \Big(\mathbb{Z}_p\langle X\rangle\Big)^n \quad (p \text{ prime})$$

be any solutions to ($\diamond$). To complete the induction step, one shows:

- subtracting suitable $\mathbb{Q}[X]$-multiples of the special solutions ($\diamond\diamond$) from y, one can achieve $\deg_{X_N} y_j < d$ for all j (by Euclidean Division in $\mathbb{Q}[X]$);

- subtracting suitable $\mathbb{Z}_p\langle X\rangle$-multiples of the special solutions ($\diamond\diamond$) from z, one can achieve $\deg_{X_N} z_j < d$ for all j (by Weierstrass Division and Preparation for $\mathbb{Z}_p\langle X\rangle$).

Theorem. *Given an $m \times n$-matrix A with entries $a_{ij} \in \mathbb{Z}[X]$, one can construct generators*

$$y^{(1)}, \ldots, y^{(K)} \in \Big(\mathbb{Z}[X]\Big)^n$$

of the $\mathbb{Z}[X]$-module of solutions (in $\mathbb{Z}[X]$) to

$$Ay = 0$$

with

$$h\Big(y^{(1)}, \ldots, y^{(K)}\Big) \leqslant \Big(m\Big(h(A) + 1\Big)\Big)^{2^{O(N^2)}}.$$

Remark. The proof shows that the *degree* of the $y^{(k)}$ can be bounded from above by

$$(md + 1)^{2((N+1)^N - 1)}.$$

Note: This bound depends only on N, m, n, and $d = \max_{i,j} \deg a_{ij}$, *not* on $||a_{ij}||$. (K can be similarly bounded.)

Digression:

A ring R is called
• **hereditary** if every ideal of R is projective. (E.g., DVRs, Dedekind domains.)
• **semihereditary** if every finitely generated ideal of R is projective. (E.g., valuation rings, Prüfer domains.)

Theorem. *Given $N, d \in \mathbb{N}$ there is an integer $\beta = \beta(N, d)$ with the following property: If R is semihereditary and $f_1, \ldots, f_n \in R[X_1, \ldots, X_N]$ of degree $\leqslant d$, then every solution to*

$$f_1 y_1 + \cdots + f_n y_n = 0$$

is a linear combination of solutions of deg. $\leqslant \beta$.

Proof: uses some ideas inspired by model theory and a theorem of Vasconcelos (semihereditary rings are stably coherent).

Remark. For R hereditary we can take the same doubly exponential β as for $R = \mathbb{Z}$. (The proof for $R = \mathbb{Z}$ can be adapted.)

Subproblem (b): “Bezout identities”

Let $f_1, \ldots, f_n \in \mathbb{Z}[X]$*. Are there* $g_1, \ldots, g_n \in \mathbb{Z}[X]$ *such that*

$$1 = g_1 f_1 + \cdots + g_n f_n \text{ ?}$$

This problem can be reduced to similar problems over coefficient rings $\mathbb{Q}$ and $\mathbb{F}_p$, where Hermann’s Theorem may be used to compute bounds on the height and degree of the g_j as desired.

More efficiently, on can obtain such bounds using

- an “arithmetic” form of the Nullstellensatz over $\mathbb{Q}$ (Krick-Pardo, . . .);
- an effective form of the Nullstellensatz over $\mathbb{F}_p$ (Kollár).

Dependence on parameters. Consider "general" polynomials

$$f_0(C,X), f_1(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X],$$

with $C = (C_1, \dots, C_M)$ being parametric variables. How does ideal membership

$$f_0(c,X) \in \Big(f_1(c,X), \dots, f_n(c,X)\Big)$$

depend on $c \in R^M$, with R a ring of an "arithmetic" nature?

The case of DVRs. Let R be a DVR. Let "$|$" denote divisibility in R:

$$a|b \quad \Longleftrightarrow \quad b \in aR \qquad \text{for } a,b \in R.$$

A *divisibility condition* $\Phi(C)$ is a formal expression of the form

$$\text{“}p_1(C)|q_1(C) \text{ and } p_2(C)|q_2(C) \\ \dots \text{ and } p_r(C)|q_r(C)\text{”},$$

with $p_i, q_i \in \mathbb{Z}[C]$.

Theorem. *There are finitely many divisibility conditions* $\Phi_1(C,T),\dots,\Phi_K(C,T)$ *such that for all DVRs* R *with maximal ideal* tR*, we have: If* $c \in R^M$*, then*

$$f_0(c,X) \in \Big(f_1(c,X),\dots,f_n(c,X)\Big)R[X] \Longleftrightarrow \text{for some } k,\ \Phi_k(c,t) \text{ holds in } R.$$

The case of Bezout domains. Let R be a Bezout domain. If $a,b \in R$, let $\gcd(a,b)$ denote a generator of the ideal

$$(a,b) = \Big\{\lambda a + \mu b : \lambda,\mu \in R\Big\},$$

and let $(a:b) \in R$ denote a generator of

$$(a):(b) = \Big\{c \in R : bc \in (a)\Big\},$$

chosen so that $a = \gcd(a,b)\cdot(a:b)$ for all $a,b \in R$. A gcd-*term* in the indeterminates C is any expression built up from

$$0, 1, C_1,\dots,C_M, +, -, \cdot, \gcd \text{ and } (\ :\ ).$$

As usual, for an ideal I in a ring S,

$$\sqrt{I} = \Big\{a \in S : a^n \in I \text{ for some } n > 0\Big\}.$$

A *radical condition* is a formal expression $\Psi(V)$ of the form

$$\text{“}p_1(V) \in \sqrt{\Big(q_1(V)\Big)} \,\&\, \ldots \,\&\, p_r(V) \in \sqrt{\Big(q_r(V)\Big)}\text{”}$$

for $p_i, q_i \in \mathbb{Z}[V]$, $V = (V_1, \ldots, V_L)$.

Theorem. *There exists a finite collection*

$$\Psi_1(V), \ldots, \Psi_K(V),$$

consisting of radical conditions and negations thereof, and an L-tuple $\tau(C)$ of gcd-*terms, such that for all Bezout domains R and coefficient tuples $c \in R^M$:*

$$f_0(c, X) \in \Big(f_1(c, X), \ldots, f_n(c, X)\Big)R[X] \iff$$
$$\text{for some } k,\ \Psi_k\Big(\tau(c)\Big) \text{ holds in } R.$$

Some questions:

Let $f_1, \ldots, f_n \in \mathbb{Z}[X]$, where $X = (X_1, \ldots, X_N)$, and $h := h(f_1, \ldots, f_n)$.

• *Modular criteria for ideal membership:*
There exist non-zero $\delta, E \in \mathbb{Z}$ such that for every $f_0 \in \mathbb{Z}[X]$:

$$f_0 \in (f_1, \ldots, f_n) \Longleftrightarrow \\ \delta f_0 \in (f_0, \ldots, f_n) \;\&\; f_0 \in (f_1, \ldots, f_n, \delta^E).$$

Can you bound δ, E in terms of h?

• *Bounds and algorithms for other problems:*
If $R = \mathbb{Z}[X]/(f_1, \ldots, f_n)$ is reduced, then its group U of units is finitely generated (Samuel, Roquette). Can you bound the heights of generators of U?

• *Complexity of Gröbner basis calculations:*
Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for the ideal $(f_1, \ldots, f_n)$ of $\mathbb{Z}[X]$. Can you bound $h(g_1, \ldots, g_m)$ in terms of $h(f_1, \ldots, f_n)$?