

Trinomial containment in polynomial ideals is undecidable

Tobias Boege¹

Anna Hofer²

Thomas Kahle²

¹UiT The Arctic University of Norway, Tromsø

²Otto-von-Guericke-Universität Magdeburg

Motivation

How short can a polynomial in an ideal be? The ideal

$$(x^4 + x^3 + x^2 + x + 1)$$

is generated by a five-term polynomial, yet it contains the binomial $x^5 - 1$. Short polynomials can hide in higher degree, and the difficulty of finding them grows sharply with the number of terms:

Monomials easy: I contains a monomial if and only if $I : (x_1 \cdots x_m)^\infty = (1)$

Binomials computable: the binomial part of I is an ideal, and Jensen–Kahle–Katthän [2] and Kreuzer–Walsh [3] compute it

Trinomials **undecidable** (this poster)

Derksen and Masser [1] write of “the problem of finding the ‘shortest’ polynomial in a given ideal”:

“In zero characteristic this problem is surprisingly difficult and probably there is in general no effective algorithm.”

Main result

A polynomial f has a unique representation

$$f = \sum_{a \in \text{supp}(f)} c_a x^a, \quad c_a \neq 0,$$

and its *number of terms* is $|\text{supp}(f)|$. For an ideal $I \subseteq K[x_1, \dots, x_m]$ over a field K put

$$\mathbf{t}(I) := \min \{ |\text{supp}(f)| : 0 \neq f \in I \}.$$

Theorem. There is an algorithm which computes, from any polynomial $P \in \mathbb{Z}[y_1, \dots, y_n]$, an integer N and generators of an ideal $I_P \subseteq \mathbb{Q}[S, T, D_1, \dots, D_N]$ with

$$\mathbf{t}(I_P) = \begin{cases} 3, & \mathcal{Z}_{\mathbb{Z}}(P) \neq \emptyset, \\ 4, & \mathcal{Z}_{\mathbb{Z}}(P) = \emptyset, \end{cases}$$

where $\mathcal{Z}_{\mathbb{Z}}(P) = \{ y \in \mathbb{Z}^n : P(y) = 0 \}$.

The ideal I_P is zero-dimensional, with at most $\binom{N+7}{5}$ generators of degree at most 5.

MRDP theorem [4]. Hilbert’s 10th problem asks for an algorithm that decides whether a polynomial $P \in \mathbb{Z}[y_1, \dots, y_n]$ has an integral zero. There is none, since every computably enumerable set is diophantine. Concretely, each Turing machine M yields a polynomial P_M with an integral zero if and only if M halts.

Together, the Theorem and the MRDP theorem give:

Corollary. For ideals $I \subseteq \mathbb{Q}[x_1, \dots, x_k]$ given by generators, each of the following is many-one equivalent to the halting problem:

- (A) does I contain a trinomial?
- (B) does I contain a nonzero polynomial with at most three terms?
- (C) given $\mathbf{t}(I) \in \{3, 4\}$, is $\mathbf{t}(I) = 3$?

All three problems are *computably enumerable*: enumerate finite supports and test each by Gröbner bases and linear algebra. No algorithm, however, can certify that I contains no trinomial. In particular, no bound on the degree of a shortest polynomial in I is computable from I .

How the reduction works

Halting problem

Does the Turing machine M halt?

MRDP: diophantine equations simulate Turing machines.

Hilbert’s 10th problem

For $P \in \mathbb{Z}[y_1, \dots, y_n]$, is there $y \in \mathbb{Z}^n$ with $P(y) = 0$?

Write P as a straight-line program, homogenise, and add guards against solutions at infinity.

Example. $P = y^3 - 2$

program $x_1 = y \cdot y, \quad x_2 = x_1 \cdot y, \quad x_2 = 2$

quadrics $x_1 t - y^2, \quad x_2 t - x_1 y, \quad x_2 t - 2t^2$

guards $h^2 - 3k^2 - t^2$ (Pell equation)

$$y^2 + x_1^2 + x_2^2 + u_1^2 + \dots + u_4^2 - ht$$

A guarded quadratic system

P becomes homogeneous quadrics $Q_1, \dots, Q_M$ in $(x_1, \dots, x_N, t)$. They have a common zero $(d, 1)$ with $d \in \mathbb{Z}^N$ if and only if $\mathcal{Z}_{\mathbb{Z}}(P) \neq \emptyset$.

Impose each form on the exponent vectors of trinomials by intersecting with a kernel.

The ideal I_P

A base ideal J_0 supplies one trinomial τ_d for every $d \in \mathbb{Z}^N$. A kernel $\ker \phi_{Q_i}$ keeps τ_d only if $Q_i(d, 1) = 0$.

$$I_P := (J_0 \cap \bigcap_i \ker \phi_{Q_i}) \cap \mathbb{Q}[S, T, D_1, \dots, D_N]$$

$$\mathbf{t}(I_P) = 3 \text{ if } P \text{ has an integral zero,} \\ \mathbf{t}(I_P) = 4 \text{ otherwise}$$

Example. The smallest instance: $N = 1$, one quadric, no guards needed. For $P = y^2 \pm 1$ the construction gives the ideals $I_{y^2 \pm 1} \subseteq \mathbb{Q}[S, T, D]$ generated by

$$(S - T)(D - 1), \quad (D - 1)^2 \mp 2(S + T - 1), \\ (D - 1)^3, \quad (S - T)^5.$$

Both are primary to $(2S - 1, 2T - 1, D - 1)$ with colength 7.

$$\mathbf{t}(I_{y^2 \pm 1}) = \begin{cases} 4, & \text{no trinomial in } I_{y^2 \pm 1}, \\ 3, & D\tau_1 = D - SD^2 - T \in I_{y^2 - 1}. \end{cases}$$

Construction of I_P

The base ideal. In the Laurent ring

$$L_N = \mathbb{Q}[S^{\pm 1}, T^{\pm 1}, D_1^{\pm 1}, \dots, D_N^{\pm 1}]$$

the *base ideal* J_0 is generated by

$$S + T - 1, \quad (S - T)^5, \\ (S - T)(D_i - 1), \quad (D_i - 1)(D_j - 1).$$

It contains no monomial and no binomial. Up to units its trinomials form two families:

- *affine* $\tau_d = 1 - S D^d - T D^{-d}$, one for each $d \in \mathbb{Z}^N$,
- *infinite* $\theta_e^{p,q} = (p - q) + q D^{pe} - p D^{qe}$ with $e \in \mathbb{Z}^N$ and integers $p \neq q$, unwanted but unavoidable.

Selecting trinomials. The map ϕ_Q sends D^d to an exponential of d in a finite-dimensional algebra, where Q is evaluated at d . So $\tau_d \in \ker \phi_Q$ if and only if $Q(d, 1) = 0$, while $\theta_e^{p,q}$ survives only if $Q(e, 0) = 0$, which the guards forbid. The quadrimial $\Omega = (S + T - 1)(S - T)$ always survives and caps the answer at four. The nilpotents of I_P carry all of this. The ideal is far from radical.

A universal family

Feeding a universal diophantine equation into the construction fixes the ring.

Corollary. For a Gödel numbering $(M_e)_{e \in \mathbb{N}}$ of Turing machines there is $N \in \mathbb{N}$ and a computable sequence of ideals $I_e \subseteq \mathbb{Q}[S, T, D_1, \dots, D_N]$ with

$$\mathbf{t}(I_e) = \begin{cases} 3, & M_e(0) \text{ halts,} \\ 4, & M_e(0) \text{ does not halt.} \end{cases}$$

Each I_e is primary to one fixed maximal ideal and has colength at most $\binom{N+6}{4}$.

Two effective cases

Independent methods give terminating algorithms in the following settings.

Proposition (squarefree univariate). For a number field K and squarefree $0 \neq f \in K[x]$ it is decidable whether (f) contains a nonzero polynomial with at most three terms.

Idea. Call two roots $\alpha, \beta \in \overline{K}$ of f equivalent if α/β is a root of unity. At most two classes: a resultant produces a trinomial multiple. Three or more: Bilu–Luca [5] bound the degree, and a finite search decides.

Proposition (finite fields). Over a finite field K and for an ideal $I \subseteq K[x_1, \dots, x_m]$ given by generators, it is decidable whether $\mathbf{t}(I) \leq k$, for every $k \in \mathbb{N}$.

Idea. An r -term relation becomes an S -unit equation in the quotient of the Laurent ring by I . By Dong–Shafirir [6] its exponent solutions form an effective p -automatic set, and emptiness of such sets is decidable.

References

- [1] H. Derksen, D. Masser, Linear equations over multiplicative groups, recurrences, and mixing III, *Ergodic Theory Dynam. Systems* 38 (2018), 2625–2643.
- [2] A. Jensen, T. Kahle, L. Katthän, Finding binomials in polynomial ideals, *Res. Math. Sci.* 4 (2017), 16.
- [3] M. Kreuzer, F. Walsh, Computing the binomial part of a polynomial ideal, *J. Symbolic Comput.* 124 (2024), 102298.
- [4] Y. V. Matiyasevich, Enumerable sets are Diophantine, *Soviet Math. Dokl.* 11 (1970), 354–358.
- [5] Y. Bilu, F. Luca, Trinomials with given roots, *Indag. Math.* 31 (2020), 33–42.
- [6] R. Dong, D. Shafirir, S -unit equations in modules and linear-exponential Diophantine equations, *STOC ’26*, 128–137.



arXiv:2608.31162

Lean 4 formalization: github.com/tom111/trinomials-undecidable-lean