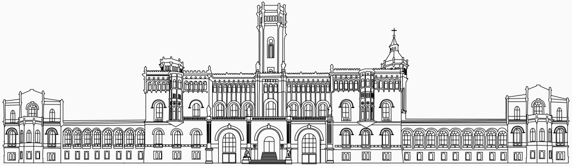
Gröbner Bases and Their Complexity

Master's thesis presentation

Leo Kayser

23.11.2022

Institut für Theoretische Informatik



Gröbner bases provide a vital tool for polynomial ideal computations in computer algebra and its applications. While useful in practice, its worst-case complexity is located in $\mathrm{EXPSPACE}$ and the size of a Gröbner basis may grow double-exponentially.

Polynomial equations are everywhere

Task: Given $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$, find solutions to $f_1(x) = \cdots = f_s(x) = 0$.

- Wide range of applications in areas such as robotics, biochemical reaction networks, computer vision, statistics, ...
- Applications in cryptography require exact solutions (e.g. over finite fields)
- Example: "Automatic" theorem proving

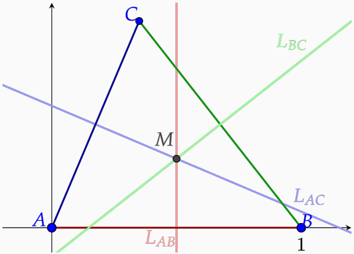


Figure 1: The perpendicular bisectors of a triangle meet in a common point.

The ideal membership problem

- Consider polynomials $f_1, \ldots, f_s \in R := \mathbb{Q}[X_1, \ldots, X_n]$, represented as strings, e.g.

$$f_1 = \texttt{3/10 X\_1\^{}3 - 4/2 X\_1X\_2}$$

- The *ideal generated by the* f_i is $\langle f_1, \ldots, f_s \rangle := \{ h_1 f_1 + \cdots + h_s f_s \mid h_i \in R \}$, any such set is called an ideal
- **Hilbert's Nullstellensatz:**

$$\exists x \in \mathbb{C}^n \text{ with } f_1(x) = \cdots = f_s(x) = 0 \qquad \text{if and only if} \qquad 1 \notin \langle f_1, \ldots, f_s \rangle$$

Problem: (Ideal membership problem, $\mathrm{IM}_{\mathbb{Q}}$)

Input: $(f, g_1, \ldots, g_s)$ multivariate polynomials from $\mathbb{Q}[X_1, \ldots, X_n]$

Output: Decide whether $f \in \langle g_1, \ldots, g_n \rangle$.

A first approach to solving ideal membership

- Intuitive approach for deciding $f \in \langle g_1, \dots, g_s \rangle$: "Divide f by the g_i and check if the remainder is zero":

$$f = q_1 g_1 + \cdots + q_s g_s + r, \qquad r \text{ "small" (?)}$$

$\leadsto$ Need a way to compare polynomials

- A *monomial order* $\prec$ is a total order on the set of monomials $\{ X^\alpha \mid \alpha \in \mathbb{N}^n \}$ with
  - ▷ $1 \prec X^\alpha$ for all $\alpha \neq 0$
  - ▷ if $X^\alpha \prec X^\beta$, then $X^\alpha X^\gamma \prec X^\beta X^\gamma$ for all γ
- Examples: Lexicographic $\prec_{\text{lex}}$, degree-lexicographic $\prec_{\text{deglex}}, \dots$
- The *leading term* $\mathrm{LT}(f)$ is the term in f with the largest monomial w.r.t. $\prec$, for example in the lexicographic order $(X_1 \succ X_2)$ we have $\mathrm{LT}(3X_1X_2 - X_2^3) = 3X_1X_2$

The normal form algorithm

- Given f and $g_1, \dots, g_s$, repeat the following steps until $f = 0$:
  - ▷ If $\mathrm{LT}(g_i) \mid \mathrm{LT}(f)$ for some i, then subtract a multiple of g_i from f (cancelling the leading term)
  - ▷ Otherwise move the leading term f to the remainder r.
- This produces a decomposition of the form

$$f = q_1 g_1 + \cdots + q_s g_s + r, \qquad \text{no term of } r \text{ divisible by any } \mathrm{LT}(g_i)$$

- If we always choose the least possible i, then $r =: \mathrm{rem}(f; g_1, \dots, g_s)$
- Example: $f = XY^2 - X$, $g_1 = XY + 1$, $g_2 = Y^2 - 1$ and $\prec = \prec_{\mathrm{lex}}$, then

$$\mathrm{rem}(f; g_1, g_2) = -X - Y, \quad \mathrm{rem}(f; g_2, g_1) = 0, \qquad f = X \cdot g_2 \in \langle g_1, g_2 \rangle$$

The star of the show: Gröbner bases

Theorem 1: (Characterizations of Gröbner bases)

Let I be an ideal and $\{g_1, \ldots, g_s\} \subseteq I$. The following are equivalent:

(a) For all $0 \neq f \in I$ there is a g_i with $\text{LT}(g_i) \mid \text{LT}(f)$

(b) For all $f \in R$ there is a *unique* $r \in R$ with $f - r \in I$ such that no $\text{LT}(g_i)$ divides any term in r.

(c) For all $f \in R$ we have $f \in I$ if and only if $\text{rem}(f; g_1, \ldots, g_s) = 0$.

- Any such sequence $g_1, \ldots, g_s$ is called a *Gröbner basis* of the ideal I
- *Buchberger's algorithm* computes a Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ [Buc06]

$\rightsquigarrow$ For Gröbner bases the normal form algorithm solves $\text{IM}_{\mathbb{Q}}$!

Uniqueness of Gröbner bases

- Gröbner bases are far from being unique, for example if G is a Gröbner basis, then so is $G \cup \{f\}$ for any $f \in I$
- A Gröbner basis $G = \{g_1, \ldots, g_s\}$ is *reduced* if the leading terms of all g_i have coefficient 1 and no term in g_i is divisible by any $\mathrm{LT}(g_j)$ for $i \neq j$.

Lemma Every ideal $I \subseteq R$ has a *unique* reduced Gröbner basis.

Problem: (Reduced Gröbner basis membership problem, $\mathrm{GROEBM}_{\mathbb{Q}}$)

Input: $(g, f_1, \ldots, f_s)$ multivariate polynomials from $\mathbb{Q}[X_1, \ldots, X_n]$

Output: Decide if g is contained in the reduced Gröbner basis of $\langle f_1, \ldots, f_n \rangle$.

Summary of the main complexity results

Theorem 2: (Mayr & Meyer [MM82], Mayr [May89], Kühnle & Mayr [KM96])

The problems $\mathrm{IM}_{\mathbb{Q}}$ and $\mathrm{GROEBM}_{\mathbb{Q}}$ are $\mathrm{EXPSPACE}$-complete. A Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ can be enumerated using exponential working space.

Theorem 3: (Möller & Mora [MM84], Huynh [Huy86])

There exists a sequence F_k of sets of polynomials of size $\mathcal{O}(k)$ such that the reduced Gröbner basis of $\langle F_k \rangle$ consists of $> 2^{2^k}$ elements of degree $> 2^{2^k}$.

$\rightsquigarrow$ Any algorithm which on input $F = (f_1, \ldots, f_s)$ computes the reduced Gröbner basis of $I = \langle F \rangle$ with respect to a degree-dominating monomial order uses in the worst case at least space $2^{\Omega(\mathrm{size}(F))}$ and time $2^{2^{\Omega(\mathrm{size}(F))}}$.

Deciding ideal membership in exponential space

- Given $f, g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$, $d = \max_i \deg(g_i)$
- **Hermann [Her26]:** If $f = h_1 g_1 + \cdots + h_s g_s$, then one can choose the h_i to satisfy

$$\deg(h_i) \leq D := \deg(f) + (sd)^{2^n}, \qquad i = 1, \dots, n.$$

- Consider the $h_i = \sum_{|\alpha| \leq D} h_{i,\alpha} X^\alpha$ with unknown coefficients $h_{i,\alpha} \in \mathbb{Q}$

(1) The equation $f = h_1 g_1 + \cdots + h_s g_s$ describes a system of linear equations in the $h_{i,\alpha}$ of size $2^{2^{\mathcal{O}(\ell)}}$, where $\ell = \mathrm{size}(f, g_1, \dots, g_s)$

(2) One can solve systems of linear equations of size $N \times N$ on a PRAM in parallel time $\mathcal{O}(\log^2 N)$ using $N^{\mathcal{O}(1)}$ processors

(3) **Parallel computation thesis [FW78]:** If L is accepted by a PRAM in parallel time $t(n)$, then $L \in \mathrm{SPACE}(t(n)^2)$

$\rightsquigarrow$ (1)+(2)+(3) yield an exponential space algorithm for $\mathrm{IM}_{\mathbb{Q}}$

Enumerating a Gröbner basis in exponential work space

- Consider $f_1, \ldots, f_s \in \mathbb{Q}[X_1, \ldots, X_n]$, $d = \max_i \deg(g_i)$
- **Dubé [Dub90]:** Any element g of the reduced Gröbner basis of I satisfies

$$\deg(g) \leq \tilde{D} := 2 \cdot \left(\tfrac{1}{2} d^2 + d\right)^{2^{n-1}}$$

(1) Idea: Enumerate monomials m of degree $\leq \tilde{D}$ and check if m is leading term of an element of the reduced Gröbner basis G of $I = \langle f_1, \ldots, f_s \rangle$

- Define the *normal form* $\mathrm{NF}_I(f) := \mathrm{rem}(f; G)$ for $f \in R$

(2) Criterion: $m = \mathrm{LT}(g)$ for an element $g \in G$ if and only if $m \neq \mathrm{NF}_I(m)$ but $\mathrm{NF}_I(m') = m'$ for all $m' \mid m$ (strictly); in that case $g = m - \mathrm{NF}_I(m)$

(3) There is an exponential work space algorithm calculating $\mathrm{NF}_I(f)$

$\rightsquigarrow$ (1)+(2)+(3) enumerate the reduced Gröbner basis in exponential work space

The path to EXPSPACE-hardness

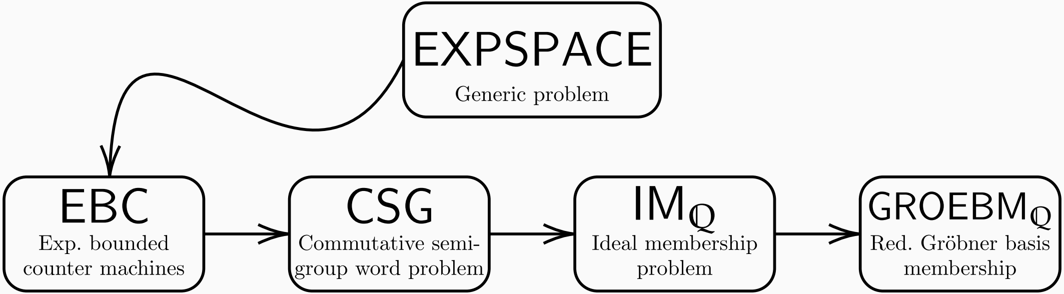


Figure 2: The chain of $\leq_m^P$-reductions proving EXPSPACE-hardness of IM$_{\mathbb{Q}}$ and GROEBM$_{\mathbb{Q}}$.

The starting point: Exponentially bounded counter machines

- A *k-counter machine* (Q, δ, q_0, q_a) consists of a finite set of states $Q \ni q_0, q_a$ and

  $$\delta\colon Q \to (\{\mathtt{INC}_1, \dots, \mathtt{INC}_k, \mathtt{DEC}_1, \dots, \mathtt{DEC}_k\} \times Q) \cup (\{\mathtt{BZ}_1, \dots, \mathtt{BZ}_k\} \times Q \times Q)$$

  - ▷ A configuration is a tuple $(q, c_1, \dots, c_k) \in Q \times \mathbb{Z}^k$
  - ▷ Instructions $\mathtt{INC}_i$, $\mathtt{DEC}_i$ increase/decrease the value of counter $c_i \in \mathbb{Z}$ by 1
  - ▷ $\mathtt{BZ}_i$ branches the program flow depending on the counter value $c_i \stackrel{?}{=} 0$
- A counter machine C *accepts* 0 if $(q_0, 0, \dots, 0) \vdash_C^* (q_a, 0, \dots, 0)$
- Its computation is *bounded by* e if $0 \leq c_i \leq e$ for all i in all steps
- The following language is $\mathrm{EXPSPACE}$-complete:

Problem: (Exponentially bounded 3-counter machines, EBC)

Input: $C = (Q, \delta, q_0, q_a)$, a 3-counter-machine

Output: Decide whether C accepts 0 and has computation bounded by $2^{2^{|Q|}}$.

From EBC to CSG

- A *commutative semigroup presentation* $(\Sigma, \mathcal{P})$ consists of
  - ▷ a finite set Σ of "commuting" letters; $\Sigma^{\oplus}$ is the set of commutative words
  - ▷ a set of replacement rules $\mathcal{P} = \{\alpha_1 \leftrightarrow \beta_1, \ldots, \alpha_s \leftrightarrow \beta_s\}$, $\alpha_i, \beta_i \in \Sigma^{\oplus}$
- $(\Sigma, \mathcal{P})$ induces a congruence relation $\equiv_{\mathcal{P}}$ on $\Sigma^{\oplus}$ by successive string replacement

Problem: (Word problem for commutative semigroups, CSG)

Input: $(\Sigma, \mathcal{P}, \alpha, \beta)$, where $(\Sigma, \mathcal{P})$ is a comm. semigroup presentation, $\alpha, \beta \in \Sigma^{\oplus}$

Output: Decide whether $\alpha \equiv_{\mathcal{P}} \beta$.

- One way to encode counter machines using commutative strings ($e := 2^{2^{|Q|}}$):

$$\mathrm{rep}(q, c_1, c_2, c_3) := qA_1^{c_1} B_1^{e-c_1} A_2^{c_2} B_2^{e-c_2} A_3^{c_3} B_3^{e-c_3} \in (Q \cup \{A_1, \ldots, B_3\})^{\oplus}$$

- Example: $q \mapsto (\mathrm{BZ}_i, q', q'')$ becomes $\{qB_i^e \leftrightarrow q'B_i^e,\ qA_i \leftrightarrow q''A_i\}$

A commutative semigroup counting to 2^{2^n}

- Problem: The rules and configurations require strings of length $e_n = 2^{2^n}$, $n = |Q|$

Theorem 4: (Mayr & Meyer [MM82])

There is a commutative semigroup presentation $(\Sigma_n, \mathcal{P}_n)$ of size $\mathcal{O}(n)$ containing $S, F, B_1, \ldots, B_4, C_1, \ldots, C_4 \in \Sigma_n$ such that

$$SC_i \equiv_{\mathcal{P}_n} FC_iB_i^{e_n}$$

and these are the only strings equivalent to SC_i containing S or F.

- Solution: Expand or collapse $B_i^{e_n}$ when needed using $(\Sigma_n, \mathcal{P}_n)$
- Example: $\{qB_i^{e_n} \leftrightarrow q'B_i^{e_n}\}$ becomes $\{q \leftrightarrow q_\downarrow FC_i,\ q_\downarrow SC_i \leftrightarrow q_\uparrow SC_i,\ q_\uparrow FC_i \leftrightarrow q'\}$

From CSG to $\mathsf{IM}_{\mathbb{Q}}$

- Let $(\Sigma = \{x_1, \ldots, x_n\}, \mathcal{P} = \{\alpha_1 \leftrightarrow \beta_1, \ldots, \alpha_s \leftrightarrow \beta_s\})$ be a commutative semigroup presentation
- For $\gamma = x_1^{d_1} \ldots x_n^{d_n} \in \Sigma^{\oplus}$ let X^{γ} be the monomial $X_1^{d_1} \cdots X_n^{d_n} \in R$

Theorem 5: (Mayr & Meyer [MM82])

For $\alpha, \beta \in \Sigma^{\oplus}$ we have

$$\alpha \equiv_{\mathcal{P}} \beta \qquad \text{if and only if} \qquad X^{\alpha} - X^{\beta} \in \langle X^{\alpha_1} - X^{\beta_1}, \ldots, X^{\alpha_s} - X^{\beta_s} \rangle.$$

$\rightsquigarrow$ Reduction $(\Sigma, \mathcal{P}, \alpha, \beta) \mapsto (X^{\alpha} - X^{\beta}, X^{\alpha_1} - X^{\beta_1}, \ldots, X^{\alpha_s} - X^{\beta_s})$

From $\mathsf{IM}_{\mathbb{Q}}$ to $\mathsf{GROEBM}_{\mathbb{Q}}$

- Reduction from EBC shows that $\mathsf{IM}_{\mathbb{Q}}$ is $\mathrm{EXPSPACE}$-hard even in the case that
  - ▷ all polynomials are *binomials* $X^{\alpha} - X^{\beta}$ with $\alpha, \beta \neq 0$;
  - ▷ the polynomial to test membership of has the form $g = X_1 - X_2$
- Let $I = \langle f_1, \ldots, f_s \rangle$ and G its reduced Gröbner basis
- Criterion (special case): Let $X^{\alpha} \succ X^{\beta}$, then

$$X^{\alpha} - X^{\beta} \in G \quad \text{if and only if} \quad X^{\alpha} - X^{\beta} \in I \text{ and } X^{\alpha} - X^{\beta'} \notin I \text{ for all } X^{\beta'} \prec X^{\beta}$$

- May assume X_2 is the smallest variable with respect to $\prec$, then $X_1 - X_2$ is in G if and only if $X_1 - X_2 \in I$

$\rightsquigarrow$ (Trivial) reduction $(g, f_1, \ldots, f_s) \mapsto (g, f_1, \ldots, f_s)$

Further results and outlook

- Consider special classes of ideals with (potentially) better bounds
  - ▷ For homogeneous ideals the complexity of ideal membership drops into PSPACE [May97], but the size of Gröbner bases doesn't necessarily improve
- Which parameters of an ideal determine the complexity/size of its Gröbner bases?
  - ▷ The dimension $r = \dim I$ of an ideal $I \subseteq \mathbb{Q}[X_1, \ldots, X_n]$ has some influence on the degree of a Gröbner basis of I, loosely described as $2^{n^{\Theta(1)} 2^{\Theta(r)}}$ [MR13]
  - ▷ The notion of *regularity* of I provides an insight on why Gröbner bases work well in *practice*, despite the Mayr & Meyer ideals [BM93]
- Instead of computing the whole Gröbner basis one might consider *approximations*
  - ▷ If one may restrict to an arbitrary ε-fraction of the input polynomials $f_1, \ldots, f_s$, then computing Gröbner bases is still NP-hard [RS19]

Thank you!

Bibliography i

[BM93] Dave Bayer and David Mumford. *What can be computed in algebraic geometry?* 1993. DOI: 10.48550/ARXIV.ALG-GEOM/9304003.

[Buc06] Bruno Buchberger. “Bruno Buchberger’s PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal”. In: *Journal of Symbolic Computation* 41.3 (2006). Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday), pp. 475–511. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2005.09.007.

[Dub90] Thomas W. Dubé. “The Structure of Polynomial Ideals and Gröbner Bases”. In: *SIAM Journal on Computing* 19.4 (Aug. 1990), pp. 750–773. DOI: 10.1137/0219053.

[FW78] Steven Fortune and James Wyllie. “Parallelism in Random Access Machines”. In: *Proceedings of the Tenth Annual ACM Symposium on Theory of Computing*. STOC ’78. San Diego, California, USA: Association for Computing Machinery, 1978, pp. 114–118. ISBN: 9781450374378. DOI: 10.1145/800133.804339.

[Her26] Grete Hermann. “Die Frage der endlich vielen Schritte in der Theorie der Polynomideale”. In: *Mathematische Annalen* 95 (1926), pp. 736–788.

[Huy86] Dung T. Huynh. “A Superexponential Lower Bound for Gröbner Bases and Church-Rosser Commutative Thue Systems”. In: *Inf. Control.* 68 (1986), pp. 196–206.

[KM96] Klaus Kühnle and Ernst W. Mayr. “Exponential Space Computation of Gröbner Bases”. In: *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*. ISSAC ’96. Zurich, Switzerland: Association for Computing Machinery, 1996, pp. 63–71. ISBN: 0897917960. DOI: 10.1145/236869.236900.

[May89] Ernst W. Mayr. “Membership in polynomial ideals over Q is exponential space complete”. In: *STACS 89*. Ed. by B. Monien and R. Cori. Berlin, Heidelberg: Springer Berlin Heidelberg, 1989, pp. 400–406. ISBN: 978-3-540-46098-5.

[May97] Ernst W. Mayr. “Some Complexity Results for Polynomial Ideals”. In: *Journal of Complexity* 13.3 (1997), pp. 303–325. ISSN: 0885-064X. DOI: 10.1006/jcom.1997.0447.

[MM82] Ernst W. Mayr and Albert R. Meyer. "The complexity of the word problems for commutative semigroups and polynomial ideals". In: *Advances in Mathematics* 46.3 (Dec. 1982), pp. 305–329. DOI: 10.1016/0001-8708(82)90048-2.

[MM84] H. Michael Möller and Ferdinando Mora. "Upper and lower bounds for the degree of Groebner bases". In: *EUROSAM 84*. Ed. by John Fitch. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984, pp. 172–183. ISBN: 978-3-540-38893-7.

Bibliography v

[MR13] Ernst W. Mayr and Stephan Ritscher. "Dimension-dependent bounds for Gröbner bases of polynomial ideals". In: *Journal of Symbolic Computation* 49 (2013). The International Symposium on Symbolic and Algebraic Computation, pp. 78–94. ISSN: 0747-7171. DOI: doi.org/10.1016/j.jsc.2011.12.018.

[RS19] David Rolnick and Gwen Spencer. "On the robust hardness of Gröbner basis computation". In: *Journal of Pure and Applied Algebra* 223.5 (2019), pp. 2080–2100. ISSN: 0022-4049. DOI: https://doi.org/10.1016/j.jpaa.2018.08.016.