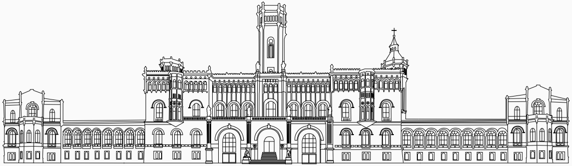
Gröbner Bases and Their Complexity

Leo Kayser

30.11.2022

Institut für Theoretische Informatik, LUH



Two computational problems

- Fix a field $\mathbb{K}$ whose elements can be represented in a computer, e.g. $\mathbb{Q}$
- Consider polynomials from $\mathbb{K}[X_1, \ldots, X_n]$ represented as strings, e.g.

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

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

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

Output: Decide whether $f \in \langle f_1, \ldots, f_s \rangle$.

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

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

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

A crash course in complexity theory

- An algorithm M computes a function $f\colon \Sigma^* \to \Delta^*$ in space $t\colon \mathbb{N} \to \mathbb{N}$ if on input $x \in \Sigma^*$ it writes $f(x)$ to the output and uses $\mathcal{O}(t(|x|))$ internal memory cells

$$\mathrm{ESPACE} = \left\{ A \,\middle|\, \chi_A \text{ can be computed in space } 2^{\mathcal{O}(n)} \right\}$$

- A language $A \subseteq \Sigma^*$ can be *log-lin reduced* to $B \subseteq \Delta^*$ (in symbols: $A \leq B$) if
  - ▷ there is a function $f\colon \Sigma^* \to \Delta^*$ computable in logarithmic space such that
  - ▷ $|f(x)| = \mathcal{O}(|x|)$ for all $x \in \Sigma^*$ and
  - ▷ $x \in A$ if and only if $f(x) \in B$
- A is *hard* for a class of languages $\mathcal{C}$ if $A_0 \leq A\ \forall A_0 \in \mathcal{C}$; it is *complete* if also $A \in \mathcal{C}$

$\rightsquigarrow$ If A is ESPACE-hard, then any algorithm deciding A requires working space $> 2^{\varepsilon|x|}$ for infinitely many $x \in \Sigma^*$

Summary of the main complexity results

Theorem 1: (Mayr & Meyer [MM82], Mayr [May89])

The problem $\mathrm{IM}_{\mathbb{Q}}$ is ESPACE-complete.

Theorem 2: (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 $> 2^{2^k}$.

Theorem 3: (Kühnle & Mayr [KM96])

A Gröbner basis of $\langle f_1, \ldots, f_s \rangle$ over $\mathbb{Q}$ can be enumerated using exponential space.

The path to ESPACE-hardness

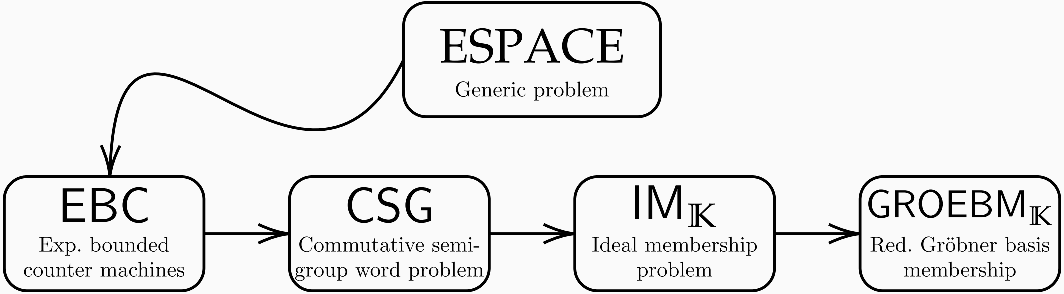


Figure 1: The chain of reductions proving ESPACE-hardness of $\mathsf{IM}_{\mathbb{K}}$ and $\mathsf{GROEBM}_{\mathbb{K}}$.

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

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

  - ▷ A configuration is a tuple $(q, c_1, \ldots, c_k) \in Q \times \mathbb{Z}^k$
  - ▷ $\mathtt{INC}_i \triangleq$ increment c_i, $\mathtt{DEC}_i \triangleq$ decrement c_i, $\mathtt{BZ}_i \triangleq$ branch program on $c_i \stackrel{?}{=} 0$
- A counter machine C *accepts* 0 if $(q_0, 0, \ldots, 0) \vdash_C^* (q_a, 0, \ldots, 0)$
- Its computation is *bounded by* e if $0 \leq c_i \leq e$ for all i in all steps
- The following language is ESPACE-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 $2^{2^{|Q|}}$.

EBC $\leq$ CSG: **Expressing counter machines with semigroups**

- 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: $q \mapsto (\mathtt{BZ}_i, q', q'')$ 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 $\{q \leftrightarrow q_\downarrow FC_i,\ q_\downarrow SC_i \leftrightarrow q_\uparrow SC_i,\ q_\uparrow FC_i \leftrightarrow q'\}$

$\mathrm{CSG} \leq \mathrm{IM}_{\mathbb{K}}$: From words to monomials

- 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 $X_1^{d_1} \cdots X_n^{d_n} \in R$

Lemma: (Mayr & Meyer [MM82]) For $\alpha, \beta \in \Sigma^{\oplus}$ the following are equivalent:

(a) $\alpha \equiv_{\mathcal{P}} \beta$;

(b) $X^{\alpha} - X^{\beta} \in \langle X^{\alpha_1} - X^{\beta_1}, \ldots, X^{\alpha_s} - X^{\beta_s} \rangle_{\mathbb{Z}[X_1,\ldots,X_n]}$;

(c) $X^{\alpha} - X^{\beta} \in \langle X^{\alpha_1} - X^{\beta_1}, \ldots, X^{\alpha_s} - X^{\beta_s} \rangle_{\mathbb{K}[X_1,\ldots,X_n]}$.

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

"$\mathrm{IM}_{\mathbb{K}} \leq \mathrm{GROEBM}_{\mathbb{K}}$": Exploiting the structure of binomial ideals

- Reduction from EBC shows that $\mathrm{IM}_{\mathbb{K}}$ is ESPACE-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: 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 $(f, f_1, \ldots, f_s) \mapsto (f, f_1, \ldots, f_s)$

Thank you!

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

[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.

[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.