Algorithms in Invariant Theory

With 0 Figures

Anakin Dey

Last Edited on 4/24/25 at 15:26

Contents

Preface

A core interest of mine (at the time of writing this) is algorithms in the context of commutative algebra and algebraic geometry. As such, Bernd Sturmfel's text *Algorithms in Invariant Theory* [Str08] is a good resource for first learning this stuff. Perhaps in the future I'll include notes and some source code

Chapter 1

Introduction

Symmetric Polynomials

Exercise 1 (Str08 1.1.5):

Prove the following explicit formula for elementary symmetric polynomials in terms of the power sums [Mac98, Page 29].

$$\sigma_k = \frac{1}{k!}\det\begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & p_1 & k-1 \\ p_k & p_{k-1} & \cdots & \cdots & p_1 \end{pmatrix}$$

Solution: From [Page 23, 2.11'][Mac98], we have the following identities

$$\begin{aligned} 1\cdot\sigma_1 &= p_1, \\ 2\cdot\sigma_2 &= p_1\sigma_1 - p_2, \\ 3\cdot\sigma_3 &= p_1\sigma_2 - p_2\sigma_1 + p_3, \\ &\vdots \\ k\cdot\sigma_k &= \sum_{r=1}^{k}(-1)^{r-1}p_r\sigma_{k-r}. \end{aligned}$$

Treating the σ_i as indeterminants, we can re-express the above system of equations:

$$\begin{aligned}
p_1 &= 1 \cdot \sigma_1, \\
p_2 &= p_1\sigma_1 - 2 \cdot \sigma_2, \\
p_3 &= p_2\sigma_1 - p_1\sigma_2 + 3 \cdot \sigma_3, \\
&\vdots \\
p_k &= \left(\sum_{r=1}^{k-1} (-1)^{r-1} p_{k-r}\sigma_r \right) + (-1)^{k-1} \cdot k\sigma_k.
\end{aligned}$$

Consider $\sigma_1, -\sigma_2, \sigma_3, \ldots, (-1)^n\sigma_{n-1}, \sigma_n$ as indeterminants. Thus, we obtain the following matrix equation:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ p_1 & 2 & 0 & \cdots & 0 \\ p_2 & p_1 & 3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & \cdots & (-1)^k \cdot k \end{pmatrix} \begin{pmatrix} \sigma_1 \\ -\sigma_2 \\ \vdots \\ (-1)^k \sigma_{k-1} \\ \sigma_k \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_{k-1} \\ p_k \end{pmatrix}.$$

Then, Cramer's rule yields that

$$\begin{aligned}
\sigma_k &= \det \begin{pmatrix} 1 & 0 & 0 & \cdots & p_1 \\ p_1 & 2 & 0 & \cdots & p_2 \\ p_2 & p_1 & 3 & \cdots & p_3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & \cdots & p_k \end{pmatrix} \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ p_1 & 2 & 0 & \cdots & 0 \\ p_2 & p_1 & 3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & \cdots & (-1)^k \cdot k \end{pmatrix}^{-1} \\
&= \frac{(-1)^k}{k!} \det \begin{pmatrix} 1 & 0 & 0 & \cdots & p_1 \\ p_1 & 2 & 0 & \cdots & p_2 \\ p_2 & p_1 & 3 & \cdots & p_3 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & \cdots & p_k \end{pmatrix} \\
&= \frac{(-1)^k}{k!} \cdot (-1)^k \det \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & p_1 & k-1 \\ p_k & p_{k-1} & \cdots & \cdots & p_1 \end{pmatrix} = \frac{1}{k!} \det \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & \cdots & p_1 & k-1 \\ p_k & p_{k-1} & \cdots & \cdots & p_1 \end{pmatrix}.
\end{aligned}$$

$\square$

Gröbner Bases

Exercise 2 (Str08 1.2.1):

Let $\prec$ be an monomial order and let I be any ideal in $\mathbb{C}[x_1, \ldots, x_n]$. A monomial m is called *minimally nonstandard* if m is nonstandard and all proper divisors of m are standard. Show that the set of minimally nonstandard monomials is finite.

Solution: Let M be a set of monomial generators for $\operatorname{init}(I)$ and let m be minimally nonstandard. Since m is a monomial and in $\operatorname{init}(I)$, we have that $m' \mid m$ for some monomial $m' \in M$. However, note that $m' \in \operatorname{init}(I)$ and furthermore by the fact that m is minimally nonstandard, we cannot have that m' strictly divides m. Thus, $m' = m$ and $m \in M$. Then by Dickson's Lemma, we have that M is a finite set and thus there are finitely many minimally nonstandard monomials. □

Exercise 3 (Str08 1.2.2):

Prove that the reduced Gröbner basis $\mathcal{G}_{\text{red}}$ of I with respect to $\prec$ is unique (up to multiplicative constants from $\mathbb{C}$). Given an algorithm which transforms an arbitrary Gröbner basis into $\mathcal{G}_{\text{red}}$.

Solution: This is [CLO15, Chapter 2, §7, Theorem 5]. □

Exercise 4 (Str08 1.2.3):

Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal, given by a finite set of generators. Using Gröbner bases, describe an algorithm for computing the *elimination ideals* $I \cap \mathbb{C}[x_1, \ldots, x_i]$ for $i = 1, \ldots, n-1$, and prove its correctness.

Solution: This is [CLO15, Chapter 3, §1, Theorem 2]. □

Exercise 5 (Str08 1.2.4):

Find a characterization of all monomial orders on the polynomial ring $\mathbb{C}[x_1, x_2]$. Hint: each variable receives a certain "weight" which behaves additively under multiplication of variables. Generalize your result to n variables.

Solution: **⟨⟨ Look at [CLO05, Chapter 1, §2, Exercise 6]. ⟩⟩** □

Exercise 6 (Str08 1.2.6):

Let $\mathcal{F}$ be a set of polynomials whose initial monomials are pairwise relatively prime. Show that $\mathcal{F}$ is a Gröbner basis for its ideal.

Solution: First, we recall some definitions. The S-polynomial of f and g is

$$S(f,g) := \frac{\operatorname{lcm}(\textsc{lm}(f), \textsc{lm}(g))}{\textsc{lt}(f)} f - \frac{\operatorname{lcm}(\textsc{lm}(f), \textsc{lm}(g))}{\textsc{lt}(g)} g.$$

For a set of polynomials $\mathcal{F} = \{f_1, \ldots, f_t\} \subseteq k[x_1, \ldots, x_n]$, we write $f \to_{\mathcal{F}} 0$ if there exists $a_1, \ldots, a_t \in k[x_1, \ldots, x_n]$

such that $a_1 f_1 + \cdots + a_t f_t = 0$. Then [CLO15, Chapter 2, §9, Theorem 3] says that a basis $\mathcal{F} = \{f_1, \ldots f_t\}$ is a Gröbner basis for G if and only if $S(f_i, f_j) \to_{\mathcal{F}} 0$ for all $i \neq j$. But [CLO15, Chapter 2, §9, Proposition 4] says that for $f, g \in \mathcal{F}$ with relatively prime initial monomials, we have that $S(f, g) \to_{\mathcal{F}} 0$. This proves the claim. $\square$

Bibliography

[CLO05] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, 2005. ISBN: 0387207066. DOI: 10.1007/b138611. URL: http://dx.doi.org/10.1007/b138611.

[CLO15] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 9783319167213. URL: https://books.google.com/books?id=yL7yCAAAQBAJ.

[Mac98] Ian Grant Macdonald. *Symmetric functions and Hall polynomials*. Oxford university press, 1998.

[Str08] Bernd Strumfels. *Algorithms in Invariant Theory*. Springer Vienna, 2008. ISBN: 9783211774175. DOI: 10.1007/978-3-211-77417-5. URL: http://dx.doi.org/10.1007/978-3-211-77417-5.