Lecturer: Pablo A. Parrilo

Last week we learned about explicit conditions to determine the number of real roots of a univariate polynomial. Today we will expand on these themes, and study two mathematical objects of fundamental importance: the resultant of two polynomials, and the closely related discriminant.

The resultant will be used to decide whether two univariate polynomials have common roots, while the discriminant will give information about the existence of multiple roots. Furthermore, we will see the intimate connections between discriminants and the boundary of the cone of nonnegative polynomials.

Besides the properties described above, a direct consequence of their definitions, there are many other interesting applications of resultants and discriminant. We describe a few of them below, and we will encounter them again in later lectures, when studying elimination theory and the construction of cylindrical algebraic decompositions. For much more information about resultants and discriminants, particularly their generalizations to the sparse and multipolynomial case, we refer the reader to the very readable introductory article [Stu98] and the book [CLO97].

## 1 Resultants

Consider two polynomials $p(x)$ and $q(x)$, of degree $n, m$, respectively. We want to obtain an easily checkable criterion to determine whether they have a common root, that is, there exists an $x_{0} \in \mathbb{C}$ for which $p\left(x_{0}\right)=q\left(x_{0}\right)=0$. There are several approaches, seemingly different at first sight, for constructing such a criterion:

- Sylvester matrix: If $p\left(x_{0}\right)=q\left(x_{0}\right)=0$, then we can write the following $(n+m) \times(n+m)$ linear system:

$$
\left[\begin{array}{cccccccc}
p_{n} & p_{n-1} & \ldots & p_{1} & p_{0} & & & \\
& p_{n} & & \ddots & \ddots & \ddots & & \\
\vdots & & & & & & & \\
& & & & & & p_{1} & p_{0} \\
\\
q_{m} & q_{m-1} & \ldots & q_{0} & & & & \\
& q_{m} & & \ddots & p_{1} & p_{0} \\
& & \ddots & & & & & \\
& & & & & & q_{1} & q_{0} \\
& & & & \\
& & & & & & q_{2} & q_{1}
\end{array}\right]\left[\begin{array}{l}
x_{0}^{n+m-1} \\
x_{0}^{n+m-2} \\
\vdots \\
x_{0}^{n} \\
x_{0}^{n-1} \\
\vdots \\
\\
x_{0} \\
1
\end{array}\right]=\left[\begin{array}{l}
p\left(x_{0}\right) x_{0}^{m-1} \\
p\left(x_{0}\right) x_{0}^{m-2} \\
\vdots \\
p\left(x_{0}\right) x_{0} \\
p\left(x_{0}\right) \\
q\left(x_{0}\right) x_{0}^{n-1} \\
q\left(x_{0}\right) x_{0}^{n-2} \\
\vdots \\
q\left(x_{0}\right) x_{0} \\
q\left(x_{0}\right)
\end{array}\right]=0 .
$$

This implies that the matrix on the left-hand side, called the Sylvester matrix $\operatorname{Syl}_{x}(p, q)$ associated to $p$ and $q$, is singular and thus its determinant must vanish. It is not too difficult to show that the converse is also true; if $\operatorname{det} \operatorname{Syl}_{x}(p, q)=0$, then there exists a vector in the kernel of $\operatorname{Syl}_{x}(p, q)$ of the form shown in the matrix equation above, and thus a common root $x_{0}$.

- Root products and companion matrices: Let $\alpha_{j}, \beta_{k}$ be the roots of $p(x)$ and $q(x)$, respectively. By construction, the expression

$$
\prod_{j=1}^{n} \prod_{k=1}^{m}\left(\alpha_{j}-\beta_{k}\right)
$$

vanishes if and only if there exists a root of $p$ that is equal to a root of $q$. Although the computation of this product seems to require explicit access to the roots, this can be avoided. Multiplying by
a convenient normalization factor, we have:

$$
\begin{align*}
p_{n}^{m} q_{m}^{n} \prod_{j=1}^{n} \prod_{k=1}^{m}\left(\alpha_{j}-\beta_{k}\right) & =p_{n}^{m} \prod_{j=1}^{n} q\left(\alpha_{j}\right)=p_{n}^{m} \operatorname{det} q\left(\mathcal{C}_{p}\right) \\
& =(-1)^{n m} q_{m}^{n} \prod_{k=1}^{m} p\left(\beta_{k}\right)=(-1)^{n m} q_{m}^{n} \operatorname{det} p\left(\mathcal{C}_{q}\right) \tag{1}
\end{align*}
$$

- Kronecker products: Using a well-known connection to Kronecker products, we can also write (1) as

$$
p_{n}^{m} q_{m}^{n} \operatorname{det}\left(\mathcal{C}_{p} \otimes I_{m}-I_{n} \otimes \mathcal{C}_{q}\right) .
$$

- Bézout matrix

To be completed

If can be shown that all these constructions are equivalent. They define exactly the same polynomial, called the resultant of $p$ and $q$, denoted as $\operatorname{Res}_{x}(p, q)$ :

$$
\begin{aligned}
\operatorname{Res}_{x}(p, q) & =\operatorname{det} \operatorname{Syl}_{x}(p, q) \\
& =p_{n}^{m} \operatorname{det} q\left(\mathcal{C}_{p}\right) \\
& =(-1)^{n m} q_{m}^{n} \operatorname{det} p\left(\mathcal{C}_{q}\right) \\
& =p_{n}^{m} q_{m}^{n} \operatorname{det}\left(\mathcal{C}_{p} \otimes I_{m}-I_{n} \otimes \mathcal{C}_{q}\right) .
\end{aligned}
$$

The resultant is a homogeneous multivariate polynomial, with integer coefficients, and of degree $n+m$ in the $n+m+2$ variables $p_{j}, q_{k}$. It vanishes if and only if the polynomials $p$ and $q$ have a common root. Notice that the definition is not symmetric in its two $\operatorname{arguments,~} \operatorname{Res}_{x}(p, q)=(-1)^{n m} \operatorname{Res}(q, p)$ (of course, this does not matter in checking whether it is zero).
Remark 1. To compute the resultant of two polynomials $p(x)$ and $q(x)$ in Maple, you can use the command resultant ( $p, q, x$ ). In Mathematica, use instead Resultant $[p, q, x]$.

## 2 Discriminants

As we have seen, the resultant allow us to write an easily checkable condition for the simultaneous vanishing of two univariate polynomials. Can we use the resultant to produce a condition for a polynomial to have a double root? Recall that if a polynomial $p(x)$ as a double root at $x_{0}$ (which can be real or complex), then its derivative $p^{\prime}(x)$ also vanishes at $x_{0}$. Thus, we can check for the existence of a double root by computing the resultant betweeen a polynomial and its derivative.
Definition 2. The discriminant of a univariate polynomial $p(x)$ is defined as

$$
\operatorname{Dis}_{x}(p):=(-1)^{n(n-1) / 2} \frac{1}{p_{n}} \operatorname{Res}_{x}\left(p(x), \frac{d p(x)}{d x}\right) .
$$

Similar to what we did in the resultant case, the discriminant can also be obtained by writing a natural condition in terms of the roots $\alpha_{i}$ of $p(x)$ :

$$
\operatorname{Dis}_{x}(p)=p_{n}^{2 n-2} \prod_{j<k}\left(\alpha_{j}-\alpha_{k}\right)^{2} .
$$

If $p(x)$ has degree $n$, its discriminant is a homogeneous polynomial of degree $2 n-2$ in its $n+1$ coefficients $p_{n}, \ldots, p_{0}$.

Example 3. Consider the quadratic univariate polynomial $p(x)=a x^{2}+b x+c$. Its discriminant is:

$$
\operatorname{Dis}_{x}(p)=-\frac{1}{a} \operatorname{Res}_{x}\left(a x^{2}+b x+c, 2 a x+b\right)=b^{2}-4 a c
$$

For the cubic polynomial $p(x)=a x^{3}+b x^{2}+c x+d$ we have

$$
\operatorname{Dis}_{x}(p)=-27 a^{2} d^{2}+18 a d c b+b^{2} c^{2}-4 b^{3} d-4 a c^{3}
$$

## 3 Applications

### 3.1 Polynomial equations

One of the most natural applications of resultants is in the solution of polynomial equations in two variables. For this, consider a polynomial system

$$
\begin{equation*}
p(x, y)=0, \quad q(x, y)=0 \tag{2}
\end{equation*}
$$

with only a finite number of solutions (which is generically the case). Consider a fixed value of $y_{0}$, and the two univariate polynomials $p\left(x, y_{0}\right), q\left(x, y_{0}\right)$. If $y_{0}$ corresponds to the $y$-component of a root, then these two univariate polynomials clearly have a common root, hence their resultant vanishes.

Therefore, to solve (2), we can compute $\operatorname{Res}_{x}(p, q)$, which is a univariate polynomial in $y$. Solving this univariate polynomial, we obtain a finite number of points $y_{i}$. Backsubstituting in $p$ (or $q$ ), we obtain the corresponding values of $x_{i}$. Naturally, the same construction can be used by computing first the univariate polynomial in $x$ given by $\operatorname{Res}_{y}(p, q)$.

Example 4. Let $p(x, y)=2 x y+3 y^{3}-2 x^{3}-x-3 x^{2} y^{2}, q(x, y)=2 x^{2} y^{2}-4 y^{3}-x^{2}+4 y+x^{2} y$. The resultant (in the $x$ variable) is

$$
\operatorname{Res}_{x}(p, q)=y(y+1)^{3}\left(72 y^{8}-252 y^{7}+270 y^{6}-145 y^{5}+192 y^{4}-160 y^{3}+28 y+4\right)
$$

One particular root of this polynomial is $y_{\star} \approx 1.6727$, with the corresponding value of $x_{\star} \approx-1.3853$.

### 3.2 Implicitization of rational curves

To be completed

### 3.3 Random matrices

```
To be completed
```


## 4 The set of nonnegative polynomials

One of the main reasons why nonnegativity conditions about polynomials are difficult is because these sets can have a quite complicated structure, even though they are always convex.

Recall from last lecture that we have defined $P_{n} \subset \mathbb{R}^{n+1}$ as the set of nonnegative polynomials of degree $n$. It is easy to see that if $p(x)$ is in the boundary of the set $P_{n}$, then it must have a real root, of multiplicity at least two. Indeed, if there is no real root, then $p(x)$ is in the strict interior of $P$


Figure 1: The shaded region corresponds to the polynomial $x^{4}+2 a x^{2}+b$ being nonnegative. The numbers indicate how many real roots $p(x)$ has.


Figure 2: Region of nonnegativity of the polynomial $x^{4}+4 a x^{3}+6 b x^{2}+4 a x+1$, and number of real roots.
(small enough perturbations will not create a root), and if it has a simple real root it clearly cannot be nonnegative.

Thus, on the boundary of $P_{n}$, the discriminant of $p(x)$ must necessarily vanish. However, it turns out that $\operatorname{Dis}_{x}(p)$ does not vanish only on the boundary, but it also vanishes at points inside the set. Why is this?

Example 5. Consider the univariate polynomial $p(x)=x^{4}+2 a x^{2}+b$. For what values of $a, b$ does it hold that $p(x) \geq 0 \forall x \in \mathbb{R}$ ? Since the leading term $x^{4}$ has even degree and is strictly positive, $p(x)$ is strictly positive if and only if it has no real roots. The discriminant of $p(x)$ is equal to $256 b\left(a^{2}-b\right)^{2}$.

Here is a slightly different example, showing the same phenomenon.
Example 6. As another example, consider now $p(x)=x^{4}+4 a x^{3}+6 b x^{2}+4 a x+1$. Its discriminant, in factored form, is equal to $256(1+3 b+4 a)(1+3 b-4 a)\left(1+2 a^{2}-3 b\right)^{2}$. The corresponding nonnegativity region and number of real roots are presented in Figure 2.

As we can see, this creates some difficulties. For instance, even though we have a perfectly valid analytic expression for the boundary of the set, we cannot have a good sense of "how far we are" from the boundary by looking at the absolute value of the discriminant.

From the mathematical viewpoint, there are a couple of (unrelated?) reasons with these sets cannot be directly handled by "standard" optimization, at least if we want to keep the polynomial structure.


Figure 3: A three-dimensional convex set, described by one quadratic and one linear inequality, whose projection on the $(a, b)$ plane is equal to the set in Figure 1 .

One has to do with its algebraic structure, and the other one with convexity, and in particular its facial structure.

Lemma 7 (e.g., And03). The set described in Figure 1 is not basic closed semialgebraic.
Remark 8. Notice that the convex sets described in Figures 1 and 2 both have an uncommon feature. They both have proper faces that are not exposed, i.e., they cannot be isolated by a supporting hyperplan $母^{1}$. Indeed, in Figure 1 the origin $(0,0)$ is a non-exposed zero-dimensional face, while in Figure 2 the point $(1,1)$ has the same property. A non-exposed face is a known obstruction for a convex set to be the feasible set of a semidefinite program, see [RG95].

Even though these sets have these complicating features, it turns out that we can often provide some "good" representations. These are normally given as a projection from higher dimensional spaces, where the object "upstairs" is much more smooth and well-behaved. For instance, as a graphical illustration, in Figure 3 we can see a three dimensional convex set, whose projection on the plane $(a, b)$ is exactly the one discussed in Example 5 and Figure 1.

The presence of "extraneous" components of the discriminant inside the feasible set is an important roadblock for the availability of "easily computable" barrier functions. Indeed, every polynomial that vanishes on the boundary of the set $P_{n}$ must necessarily have the discriminant as a factor. This is an striking difference with the case of the case of the nonnegative orthant or the PSD cone, where the standard barriers are given (up to a logarithm) by products of the linear constraints or a determinant (which are polynomials). The way out of this problem is to produce non-polynomial barrier functions, either by partial minimization from a higher-dimensional barrier (i.e., projection) or using the "universal" barrier function introduced by Nesterov and Nemirovski.

In this direction, there have been several research efforts that aim at directly characterizing barrier functions for the set of nonnegative polynomials (or related modifications). Among them, we mention the work of Kao and Megretski KM02] and Faybusovich Fay02, both of which produce barriers that rely on the computation of one or more integral expressions. Given the fact that these integrals must be computed numerically, there is no clear consensus yet on how useful this approach is in practical optimization problems.

[^0]

Figure 4: The discriminant of the polynomial $x^{4}+4 a x^{3}+6 b x^{2}+4 c x+1$. The convex set inside the "bowl" corresponds to the region of nonnegativity. There is an additional one-dimensional component inside the set.

## References

[And03] C. Andradas. Characterization and description of basic semialgebraic sets. In Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001), volume 60 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., pages 1-12. Amer. Math. Soc., Providence, RI, 2003.
[CLO97] D. A. Cox, J. B. Little, and D. O'Shea. Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra. Springer, 1997.
[Fay02] L. Faybusovich. Self-concordant barriers for cones generated by Chebyshev systems. SIAM J. Optim., 12(3):770-781 (electronic), 2002.
[KM02] C. Y. Kao and A. Megretski. A new barrier function for IQC optimization problems. In Proceedings of the American Control Conference, 2002.
[RG95] M. Ramana and A. J. Goldman. Some geometric results in semidefinite programming. J. Global Optim., 7(1):33-50, 1995.
[Stu98] B. Sturmfels. Introduction to resultants. In Applications of computational algebraic geometry (San Diego, CA, 1997), volume 53 of Proc. Sympos. Appl. Math., pages 25-39. Amer. Math. Soc., Providence, RI, 1998.


[^0]:    ${ }^{1}$ A face of a convex set $S$ is a convex subset $F \subseteq S$, with the property that $x, y \in S, \frac{1}{2}(x+y) \in F \Rightarrow x, y \in F$. A face $F$ is exposed if it can be written as $F=S \cap H$, where $H$ is a supporting hyperplane of $S$.

