Chapter 2: Real solutions to univariate polynomials

Before we study the real solutions to systems of multivariate polynomials, we will review some of what is known for univariate polynomials. The strength and precision of results concerning real solutions to univariate polynomials forms the gold standard in this subject of real roots to systems of polynomials. We will discuss two results about univariate polynomials: Descartes' rule of signs and Sturm's Theorem. Descartes' rule of signs, or rather its generalization in the Budan-Fourier Theorem, gives a bound for the number of roots in an interval, counted with multiplicity. Sturm's theorem is topological—it simply counts the number of roots of a univariate polynomial in an interval without multiplicity. From Sturm's Theorem we obtain a simple symbolic algorithm to count the number of real solutions to a system of multivariate polynomials in many cases. We underscore the topological nature of Sturm's Theorem by presenting a new and very elementary proof due to Burda and Khovanskii [64]. These and other fundamental results about real roots of univariate polynomials were established in the 19th century. In contrast, the main results about real solutions to multivariate polynomials have only been established in recent decades.

2.1 Descartes' rule of signs

Descartes' rule of signs [25] is fundamental for real algebraic geometry. Suppose that f is a univariate polynomial and write its terms in increasing order of their exponents,

$$f \;=\; c_0 t^{a_0} + c_1 t^{a_1} + \cdots + c_m t^{a_m}\,, \tag{2.1}$$

where $c_i \neq 0$ and $a_0 < a_1 < \cdots < a_m$.

Theorem 2.1 (Descartes' rule of signs) *The number, r, of positive roots of f, counted with multiplicity, is at most the variation in sign of the coefficients of f,*

$$r \;\leq\; \#\{i \mid 1 \leq i \leq m \text{ and } c_{i-1}c_i < 0\}\,,$$

and the difference between the variation and r is even.

We will prove a generalization, the Budan-Fourier Theorem, which provides a similar estimate for any interval in $\mathbb{R}$. We first formalize this notion of variation in sign that appears in Descartes' rule.

The *variation* $\mathrm{var}(c)$ in a finite sequence c of real numbers is the number of times that consecutive elements of the sequence have opposite signs, after we remove any 0s in the sequence. For example, the first sequence below has variation four, while the second has variation three.

$$8, -4, -2, -1, 2, 3, -5, 7, 11, 12 \qquad\qquad -1, 0, 1, 0, 1, -1, 1, 1, 0, 1\,.$$

Suppose that we have a sequence $F = (f_0, f_1, \ldots, f_k)$ of polynomials and a real number $a \in \mathbb{R}$. Then $\mathrm{var}(F, a)$ is the variation in the sequence $f_0(a), f_1(a), \ldots, f_k(a)$. This notion also makes sense when $a = \pm\infty$: We set $\mathrm{var}(F, \infty)$ to be the variation in the sequence of leading coefficients of the $f_i(t)$, which are the signs of $f_i(a)$ for $a \gg 0$, and set $\mathrm{var}(F, -\infty)$ to be the variation in the leading coefficients of $f_i(-t)$.

Given a univariate polynomial $f(t)$ of degree k, let δf be the sequence of its derivatives,

$$\delta f \;:=\; (f(t), f'(t), f''(t), \ldots, f^{(k)}(t))\,.$$

For $a, b \in \mathbb{R} \cup \{\pm\infty\}$, let $r(f, a, b)$ be the number of roots of f in the interval $(a, b]$, counted with multiplicity. We prove a version of Descartes' rule due to Budan [17] and Fourier [38].

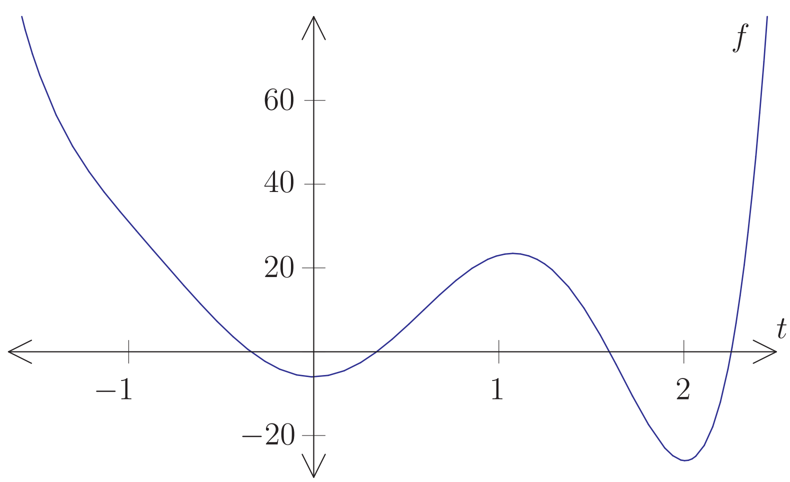
Theorem 2.2 (Budan-Fourier) *Let $f \in \mathbb{R}[t]$ be a univariate polynomial and $a < b$ two numbers in $\mathbb{R} \cup \{\pm\infty\}$. Then*

$$\mathrm{var}(\delta f, a) \;-\; \mathrm{var}(\delta f, b) \;\geq\; r(f, a, b)\,,$$

and the difference is even.

We may deduce Descartes' rule of signs from the Budan-Fourier Theorem once we observe that for the polynomial $f(t)$ (2.1), $\mathrm{var}(\delta f, 0) = \mathrm{var}(c_0, c_1, \ldots, c_m)$, while $\mathrm{var}(\delta f, \infty) = 0$, as the leading coefficients of δf all have the same sign.

Example 2.3 The the sextic $f = 5t^6 - 4t^5 - 27t^4 + 55t^2 - 6$ whose graph is displayed below



has four real zeroes at approximately -0.3393, 0.3404, 1.598, and 2.256. If we evaluate the derivatives of f at 0 we obtain

$$\delta f(0) \;=\; -6,\ 0,\ 110,\ 0,\ -648,\ -480,\ 3600\,,$$

which has 3 variations in sign. If we evaluate the derivatives of f at 2, we obtain

$$\delta f(2) \;=\; -26,\, -4,\, 574,\, 2544,\, 5592,\, 6720,\, 3600\,,$$

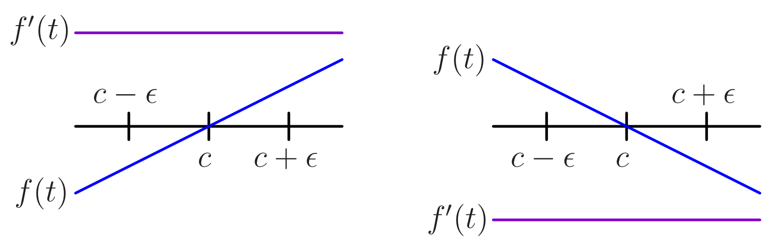
which has one sign variation. Thus, by the Budan-Fourier Theorem, f has either 2 or 0 roots in the interval $(0, 2)$, counted with multiplicity. This agrees with our observation that f has 2 roots in the interval $[0, 2]$.

Proof of Budan-Fourier Theorem. Observe that $\mathrm{var}(\delta f, t)$ can only change when t passes a root c of some polynomial in the sequence δf of derivatives of f. Suppose that c is a root of some derivative of f and let $\epsilon > 0$ be a positive number such that no derivative $f^{(i)}$ has a root in the interval $[c - \epsilon, c + \epsilon]$, except possibly at c. Let m be the order of vanishing of f at c. We will prove that

$$\begin{aligned}
&(1)\quad \mathrm{var}(\delta f, c) = \mathrm{var}(\delta f, c + \epsilon), \ \text{ and}\\
&(2)\quad \mathrm{var}(\delta f, c - \epsilon) \geq \mathrm{var}(\delta f, c) + m, \quad \text{and the difference is even.}
\end{aligned} \tag{2.2}$$

We deduce the Budan-Fourier theorem from these conditions. As t ranges from a to b, $r(f, a, t)$ and $\mathrm{var}(\delta f, t)$ can only change when t passes a root c of f or one of its derivatives. At such a point, $r(f, a, t)$ jumps by the multiplicity m of the point c as a root of f, while $\mathrm{var}(\delta f, t)$ drops by m, plus a nonnegative even integer. Thus the sum $r(f, a, t) + \mathrm{var}(\delta f, t)$ can only change at roots c of f or its derivatives, where it drops by an even integer. The Budan-Fourier Theorem follows, as this sum equals $\mathrm{var}(\delta f, a)$ when $t = a$.

Let us now prove our claim about the behavior of $\mathrm{var}(\delta f, t)$ in a neighborhood of a root c of some derivative $f^{(i)}$. We argue by induction on the degree of f. When f has degree 1, then we are in one of the following two cases, depending upon the sign of f'



In both cases, $\mathrm{var}(\delta f, c - \epsilon) = 1$, but $\mathrm{var}(\delta f, c) = \mathrm{var}(\delta f, c + \epsilon) = 0$, which proves the claim when f is linear.

Now suppose that the degree of f is greater than 1 and let m be the order of vanishing of f at c. We first treat the case when $f(c) = 0$, and hence $m > 0$ so that f' vanishes at c to order $m-1$. We apply our induction hypothesis to f' and obtain that

$$\mathrm{var}(\delta f', c) \;=\; \mathrm{var}(\delta f', c + \epsilon), \qquad \text{and} \qquad \mathrm{var}(\delta f', c - \epsilon) \;\geq\; \mathrm{var}(\delta f', c) \;+\; (m - 1)\,,$$

and the difference is even. By Lagrange's Mean Value Theorem applied to the intervals $[c - \epsilon, c]$ and $[c, c + \epsilon]$, f and f' must have opposite signs at $c - \epsilon$, but the same signs at $c + \epsilon$, and so

$$\begin{aligned}
\mathrm{var}(\delta f, c) \;&=\; \mathrm{var}(\delta f', c) \;=\; \mathrm{var}(\delta f', c + \epsilon) \;=\; \mathrm{var}(\delta f, c + \epsilon)\,,\\
\mathrm{var}(\delta f, c - \epsilon) \;&=\; \mathrm{var}(\delta f', c - \epsilon) + 1 \;\geq\; \mathrm{var}(\delta f', c) + (m - 1) + 1 \;=\; \mathrm{var}(\delta f, c) + m\,,
\end{aligned}$$

and the difference is even. This proves the claim when $f(c) = 0$.

Now suppose that $f(c) \neq 0$ so that $m = 0$. Let n be the order of vanishing of f' at c. We apply our induction hypothesis to f' to obtain that

$$\mathrm{var}(\delta f', c) \;=\; \mathrm{var}(\delta f', c+\epsilon), \qquad \text{and} \qquad \mathrm{var}(\delta f', c-\epsilon) \;\geq\; \mathrm{var}(\delta f', c) \;+\; n\,,$$

and the difference is even. We have $f(c) \neq 0$, but $f'(c) = \cdots = f^{(n)}(c) = 0$, and $f^{(n+1)}(c) \neq 0$. Multiplying f by -1 if necessary, we may assume that $f^{(n+1)}(c) > 0$. There are four cases: n even or odd, and $f(c)$ positive or negative. We consider each case separately.

Suppose that n is even. Then both $f'(c-\epsilon)$ and $f'(c+\epsilon)$ are positive and so for each $t \in \{c-\epsilon, c, c+\epsilon\}$ the first nonzero term in the sequence

$$f'(t),\; f''(t),\; \ldots,\; f^{(k)}(t) \tag{2.3}$$

is positive. When $f(c)$ is positive, this implies that $\mathrm{var}(\delta f, t) = \mathrm{var}(\delta f', t)$ and when $f(c)$ is negative, that $\mathrm{var}(\delta f, t) = \mathrm{var}(\delta f', t){+}1$. This proves the claim as it implies that $\mathrm{var}(\delta f, c) = \mathrm{var}(\delta f, c+\epsilon)$ and also that

$$\mathrm{var}(\delta f, c-\epsilon) \;-\; \mathrm{var}(\delta f, c) \;=\; \mathrm{var}(\delta f', c-\epsilon) \;-\; \mathrm{var}(\delta f', c)\,,$$

but this last difference exceeds n by an even number, and so is even as n is even.

Now suppose that n is odd. Then $f'(c-\epsilon) < 0 < f'(c+\epsilon)$ and so the first nonzero term in the sequence (2.3) has sign $-,+,+$ at $t = c-\epsilon, c, c+\epsilon$, respectively. If $f(c)$ is positive, then $\mathrm{var}(\delta f, c-\epsilon) = \mathrm{var}(\delta f', c-\epsilon) + 1$ and the other two variations are unchanged, but if $f(c)$ is negative, then the variation at $t = c-\epsilon$ is unchanged, but it increases by 1 at $t = c$ and $t = c+\epsilon$. This again implies the claim, as $\mathrm{var}(\delta f, c) = \mathrm{var}(\delta f, c+\epsilon)$, but

$$\mathrm{var}(\delta f, c-\epsilon) - \mathrm{var}(\delta f, c) \;=\; \mathrm{var}(\delta f', c-\epsilon) - \mathrm{var}(\delta f', c) \;\pm\; 1\,.$$

Since the difference $\mathrm{var}(\delta f', c-\epsilon) - \mathrm{var}(\delta f', c)$ is equal to the order n of the vanishing of f' at c plus a nonnegative even number, if we add or subtract 1, the difference is a nonnegative even number. This completes the proof of the Budan-Fourier Theorem.

2.2 Sturm's Theorem

Let f, g be univariate polynomials. Their *Sylvester sequence* is the sequence of polynomials

$$f_0 \;:=\; f,\;\; f_1 \;:=\; g,\;\; f_2,\; \ldots,\; f_k\,,$$

where f_k is a greatest common divisor of f and g, and

$$-f_{i+1} \;:=\; \mathrm{remainder}(f_{i-1}, f_i)\,,$$

the usual remainder from the Euclidean algorithm. Note the sign. We remark that we have polynomials $q_1, q_2, \ldots, q_{k-1}$ such that

$$f_{i-1}(t) \;=\; q_i(t) f_i(t) \;-\; f_{i+1}(t)\,, \tag{2.4}$$

and the degree of f_{i+1} is less than the degree of f_i. The *Sturm sequence* of a univariate polynomial f is the Sylvester sequence of f, f'.

Theorem 2.4 (Sturm's Theorem) *Let f be a univariate polynomial and $a, b \in \mathbb{R} \cup \{\pm\infty\}$ with $a < b$ and $f(a), f(b) \neq 0$. Then the number of zeroes of f in the interval (a, b) is the difference*

$$\mathrm{var}(F, a) \;-\; \mathrm{var}(F, b)\,,$$

where F is the Sturm sequence of f.

Example 2.5 The sextic f of Example 2.3 has Sturm sequence

$$\begin{aligned}
f &= 5t^6 - 4t^5 - 27t^4 + 55t^2 - 6\\
f_1 := f'(t) &= 30t^5 - 20t^4 - 108t^3 + 110t\\
f_2 &= \tfrac{84}{9}t^4 + \tfrac{12}{5}t^3 - \tfrac{110}{3}t^2 - \tfrac{22}{9}t + 6\\
f_3 &= \tfrac{559584}{36125}t^3 + \tfrac{143748}{1445}t^2 - \tfrac{605394}{7225}t - \tfrac{126792}{7225}\\
f_4 &= \tfrac{229905821875}{724847808}t^2 + \tfrac{1540527685625}{4349086848}t + \tfrac{7904908625}{120807968}\\
f_5 &= -\tfrac{280364022223059296}{58526435357253125}t + \tfrac{174201756039315072}{292632176786265625}\\
f_6 &= -\tfrac{17007035533771824564661037625}{162663080627869030112013128}\,.
\end{aligned}$$

Evaluating the Sturm sequence at $t = 0$ gives

$$-6,\;\; 0,\;\; 6,\;\; -\tfrac{126792}{7225},\;\; \tfrac{174201756039315072}{292632176786265625},\;\; -\tfrac{17007035533771824564661037625}{162663080627869030112013128}\;,$$

which has 4 variations in sign, while evaluating the Sturm sequence at $t = 2$ gives

$$-26,\;\; -4,\;\; \tfrac{1114}{45},\;\; \tfrac{3210228}{36125},\;\; -\tfrac{1076053821625}{2174543424},\;\; -\tfrac{2629438466191277888}{292632176786265625},\;\; -\tfrac{17007035533771824564661037625}{162663080627869030112013128}\;,$$

which has 2 variations in sign. Thus by Sturm's Theorem, we see that f has 2 roots in the interval $[0, 2]$, which we have already seen by other methods.

An application of Sturm's Theorem is to isolate real solutions to a univariate polynomial f by finding intervals of a desired width that contain a unique root of f. When $(a, b) = (-\infty, \infty)$, Sturm's Theorem gives the total number of real roots of a univariate polynomial. In this way, it leads to an algorithm to investigate the number of real roots of generic systems of polynomials. We briefly describe this algorithm here. This algorithm was used in an essential way to get information on real solutions which helped to formulate many results discussed in later chapters.

Suppose that we have a system of real multivariate polynomials

$$f_1(x_1, \ldots, x_n) \;=\; f_2(x_1, \ldots, x_n) \;=\; \cdots \;=\; f_N(x_1, \ldots, x_n) \;=\; 0\,, \tag{2.5}$$

whose number of real roots we wish to determine. Let $I \subset \mathbb{R}[x_1, \ldots, x_n]$ be the ideal generated by the polynomials $f_1, f_2, \ldots, f_N$. If (2.5) has finitely many complex zeroes, then the dimension of the quotient ring $\mathbb{R}[x_1, \ldots, x_n]/I$ (the *degree* of I) is finite. Thus, for each variable x_i, there is a univariate polynomial $g(x_i) \in I$ of minimal degree, called an *eliminant* for I. The significance of eliminants comes from the following observation.

Proposition 2.6 *The roots of an eliminant $g(x_i) \in I$ form the set of ith coordinates of solutions to* (2.5)*.*

The algorithm for counting the number of real solutions to (2.5) is a consequence of Sturm sequences and the Shape Lemma [5].

Theorem 2.7 (Shape Lemma) *Suppose that I has an eliminant $g(x_i)$ whose degree is equal to the degree of I. Then the number of real solutions to* (2.5) *is equal to the number of real roots of g.*

Suppose that the coefficients of the polynomials f_i in the system (2.5) lie in a computable subfield of $\mathbb{R}$, for example, $\mathbb{Q}$ (e.g. if the coefficients are integers). Then the degree of I may be computed using Gröbner bases, and we may also use Gröbner bases to compute an eliminant $g(x_i)$. Since Buchberger's algorithm does not enlarge the field of the coefficients, $g(x_i) \in \mathbb{Q}[x_i]$ has rational coefficients, and so we may use Sturm sequences to compute the number of its real roots. We state this more precisely.

Algorithm
GIVEN: $I = \langle f_1, \ldots, f_N \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$

1. Use Gröbner bases to compute the degree d of I.
2. Use Gröbner bases to compute an eliminant $g(x_i) \in I \cap \mathbb{Q}[x_i]$ for I.
3. If $\deg(g) = d$, then use Sturm sequences to compute the number r of real roots of $g(x_i)$, and output "The ideal I has r real solutions."
4. Otherwise output "The ideal I does not satisfy the hypotheses of the Shape Lemma for the variable x_i."

If this algorithm halts with a failure (step 4), it may be called again to compute an eliminant for a different variable. Another strategy is to apply a random linear transformation before eliminating. An even more sophisticated form of elimination is Roullier's rational univariate representation [94].

2.2.1 Traditional Proof of Sturm's Theorem

Let $f(t)$ be a real univariate polynomial with Sturm sequence F. We prove Sturm's Theorem by looking at the variation $\mathrm{var}(F, t)$ as t increases from a to b. This variation can only change when t passes a number c where some member f_i of the Sturm sequence has a root, for then the sign of f_i could change. We will show that if $i > 0$, then this has no effect on the variation of the sequence, but when c is a root of $f = f_0$, then the variation decreases by exactly 1 as t passes c. Since multiplying a sequence by a nonzero number does not change its variation, we will at times make an assumption on the sign of some value $f_j(c)$ to reduce the number of cases to examine.

Observe first that by (2.4), if $f_i(c) = f_{i+1}(c) = 0$, then f_{i-1} also vanishes at c, as do all the other polynomials f_j. In particular $f(c) = f'(c) = 0$, so f has a multiple root at c. Suppose first that this does not happen, either that $f(c) \neq 0$ or that c is a simple root of f.

Suppose that $f_i(c) = 0$ for some $i > 0$. The vanishing of f_i at c, together with (2.4) implies that $f_{i-1}(c)$ and $f_i(c)$ have opposite signs. Then, whatever the sign of $f_i(t)$ for t near c, there is exactly one variation in sign coming from the subsequence $f_{i-1}(t), f_i(t), f_{i+1}(t)$, and so the vanishing of f_i at c has no effect on the variation as t passes c. Note that this argument works equally well for any Sylvester sequence.

Now we consider the effect on the variation when c is a simple root of f. In this case $f'(c) \neq 0$, so we may assume that $f'(c) > 0$. But then $f(t)$ is negative for t to the left of c and positive for t to the right of c. In particular, the variation $\operatorname{var}(F, t)$ decreases by exactly 1 when t passes a simple root of f and does not change when f does not vanish.

We are left with the case when c is a multiple root of f. Suppose that its multiplicity is $m+1$. Then $(t-c)^m$ divides every polynomial in the Sturm sequence of f. Consider the sequence of quotients,

$$G \;=\; (g_0, \ldots, g_k) \;:=\; (f/(t-c)^m,\; f'/(t-c)^m,\; f_2/(t-c)^m,\; \cdots,\; f_k/(t-c)^m)\,.$$

Note that $\operatorname{var}(G,t) = \operatorname{var}(F,t)$ when $t \neq c$, as multiplying a sequence by a nonzero number does not change its variation. Observe also that G is a Sylvester sequence. Since $g_1(c) \neq 0$, not all polynomials g_i vanish at c. But we showed in this case that there is no contribution to a change in the variation by any polynomial g_i with $i > 0$.

It remains to examine the contribution of g_0 to the variation as t passes c. If we write $f(t) = (t-c)^{m+1}h(t)$ with $h(c) \neq 0$, then

$$f'(t) \;=\; (m+1)(t-c)^m h(t) \;+\; (t-c)^{m+1}h'(t)\,.$$

In particular,

$$g_0(t) \;=\; (t-c)h(t) \qquad \text{and} \qquad g_1(t) \;=\; (m+1)h(t) \;+\; (t-c)h'(t)\,.$$

If we assume that $h(c) > 0$, then $g_1(c) > 0$ and $g_0(t)$ changes from negative to positive as t passes c. Once again we see that the variation $\operatorname{var}(F,t)$ decreases by 1 when t passes a root of f. This completes the proof of Sturm's Theorem.

2.3 A topological proof of Sturm's Theorem

We present a second, very elementary, proof of Sturm's Theorem due to Burda and Khovanskii [64] whose virtue is in its tight connection to topology. We first recall the definition of topological degree of a continuous function $\varphi\colon \mathbb{RP}^1 \to \mathbb{RP}^1$. Since $\mathbb{RP}^1$ is isomorphic to the quotient $\mathbb{R}/\mathbb{Z}$, we may pull φ back to the interval $[0,1]$ to obtain a map $[0,1] \to \mathbb{RP}^1$. This map lifts to the universal cover of $\mathbb{RP}^1$ to obtain a map $\psi\colon [0,1] \to \mathbb{R}$. Then the *mapping degree*, $\operatorname{mdeg}(\varphi)$, of φ is simply $\psi(1) - \psi(0)$, which is an integer. We call this the mapping degree to distinguish it from the usual algebraic degree of a polynomial or rational function.

The key ingredient in this proof is a formula to compute the mapping degree of a rational function $\varphi\colon \mathbb{RP}^1 \to \mathbb{RP}^1$. Any rational function $\varphi = f/g$ where $f, g \in \mathbb{R}[t]$ are polynomials has a continued fraction expansion of the form

$$\varphi \;=\; q_0 \;+\; \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k}}}} \tag{2.6}$$

where $q_0, \ldots, q_k$ are polynomials. Indeed, this continued fraction is constructed recursively. If we divide f by g with remainder h, so that $f = q_0 g + h$ with the degree of h less than the degree of g, then

$$\varphi \;=\; q_0 + \frac{h}{g} \;=\; q_0 + \cfrac{1}{\cfrac{g}{h}}\,.$$

We may now divide g by h with remainder, $g = q_1 h + k$ and obtain

$$\varphi \;=\; q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{h}{k}}}\,.$$

As the degrees of the numerator and denominator drop with each step, this process terminates with an expansion (2.6) of φ.

For example, if $f = 4t^4 - 18t^2 - 6t$ and $g = 4t^3 + 8t^2 - 1$, then

$$\frac{f}{g} \;=\; t - 2 \;+\; \cfrac{1}{-2t + 1 \;+\; \cfrac{1}{-2t - 3 \;+\; \cfrac{1}{t+1}}}$$

This continued fraction expansion is just the Euclidean algorithm in disguise.

Suppose that $q = c_0 + c_1 t + \cdots + c_d t^d$ is a real polynomial of degree d. Define

$$[q] \;:=\; \operatorname{sign}(c_d) \cdot (d \mod 2) \;\in\; \{\pm 1, 0\}\,.$$

Theorem 2.8 *Suppose that φ is a rational function with continued fraction expansion* (2.6). *Then the mapping degree of φ is*

$$[q_1] - [q_2] + \cdots + (-1)^{k-1}[q_k]\,.$$

We may use this to count the roots of a real polynomial f by the following lemma.

Lemma 2.9 *The number of roots of a polynomial f, counted without multiplicity is the mapping degree of the rational function f/f'.*

We deduce Sturm's Theorem from Lemma 2.9. Let $f_0, f_1, f_2 \ldots, f_k$ be the Sturm sequence for f. Then $f_0 = f$, $f_1 = f'$, and for $i > 1$, $-f_{i+1} :=$ remainder(f_{i-1}, f_i). That is, $\deg(f_i) < \deg(f_{i-1})$ and there are univariate polynomials $g_1, g_2, \ldots, g_k$ with

$$f_{i-1} \;=\; g_i f_i - f_{i+1} \qquad \text{for} \quad i = 1, 2, \ldots, k{-}1\,.$$

We relate these polynomials to those obtained from the Euclidean algorithm applied to f, f' and thus to the continued fraction expansion of f/f'. It is clear that the f_i differ only by a sign from the remainders in the Euclidean algorithm. Set $r_0 := f$ and $r_1 = f'$, and for $i > 1$, $r_i :=$ remainder(r_{i-2}, r_{i-1}). Then $\deg(r_i) < \deg(r_{i-1})$, and there are univariate polynomials $q_1, q_2, \ldots, q_k$ with

$$r_{i-i} \;=\; q_i r_i + r_{i+1} \qquad \text{for} \quad i = 1, \ldots, k{-}1\,.$$

We leave the proof of the following lemma as an exercise for the reader.

Lemma 2.10 *We have $g_i = (-1)^{i-1} q_i$ and $f_i = (-1)^{\lfloor \frac{i}{2} \rfloor} r_i$, for $i = 1, 2, \ldots, k$.*

Write F for the Sturm sequence $(f_0, f_1, f_2 \ldots, f_k)$ for f and f^{top} for the leading coefficient of f_i. Then var(F, ∞) is the variation in the leading coefficients $(f_0^{\text{top}}, f_1^{\text{top}}, \ldots, f_k^{\text{top}})$ of the polynomials in F. Similarly, var$(F, -\infty)$ is the variation in the sequence

$$((-1)^{\deg(f_0)} f_0^{\text{top}},\ (-1)^{\deg(f_1)} f_1^{\text{top}},\ \ldots,\ (-1)^{\deg(f_k)} f_k^{\text{top}})\,.$$

Note that the variation in a sequence $(c_0, c_1, \ldots, c_k)$ is just the sum of the variations in each subsequence (c_{i-1}, c_i) for $i = 1, \ldots, k$. Thus

$$\begin{aligned} &\operatorname{var}(F, -\infty) - \operatorname{var}(F, \infty) \\ &\quad = \sum_{i=1}^{k} \left[\operatorname{var}((-1)^{\deg(f_{i-1})} f_{i-1}^{\text{top}}, (-1)^{\deg(f_i)} f_i^{\text{top}}) \;-\; \operatorname{var}(f_{i-1}^{\text{top}}, f_i^{\text{top}})\right]\,. \end{aligned} \tag{2.7}$$

Since $f_{i-1} = g_i f_i - f_{i+1}$ and $\deg(f_{i+1}) < \deg(f_i) < \deg(f_{i-1})$, we have

$$f_{i-1}^{\text{top}} \;=\; g_i^{\text{top}} f_i^{\text{top}} \qquad \text{and} \qquad \deg(f_{i-1}) \;=\; \deg(g_i) + \deg(f_i)\,.$$

Thus we have

$$\begin{aligned} \operatorname{var}(f_{i-1}^{\text{top}}, f_i^{\text{top}}) \;&=\; \operatorname{var}(g_i^{\text{top}}, 1)\,, \qquad \text{and} \\ \operatorname{var}((-1)^{\deg(f_{i-1})} f_{i-1}^{\text{top}}, (-1)^{\deg(f_i)} f_i^{\text{top}}) \;&=\; \operatorname{var}((-1)^{\deg(g_i)} g_i^{\text{top}}, 1)\,. \end{aligned}$$

Thus the summands in (2.7) are

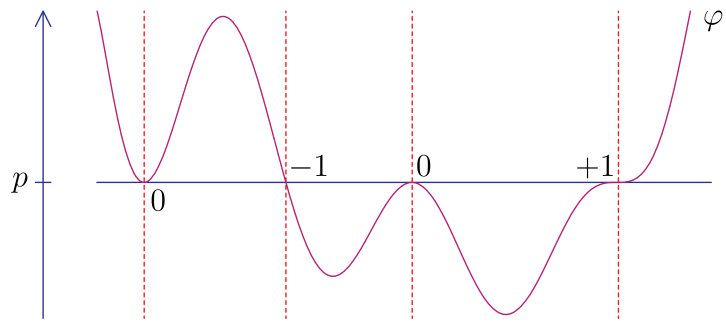
$$\begin{aligned} \operatorname{var}((-1)^{\deg(g_i)} g_i^{\text{top}}, 1) \;-\; \operatorname{var}(g_i^{\text{top}}, 1) \;&=\; \operatorname{sign}(g_i^{\text{top}})(\deg(g_i) \mod 2) \\ &=\; [g_i] \;=\; (-1)^{i-1}[q_i]\,, \end{aligned}$$

This proves that

$$\begin{aligned} \operatorname{var}(F,-\infty)-\operatorname{var}(F,\infty) &= [g_1]+[g_2]+\cdots+[g_k] \\ &= [q_1]-[q_2]+\cdots+(-1)^{k-1}[q_k]\,. \end{aligned}$$

But this proves Sturm's Theorem, as this is the number of roots of f, by Theorem 2.8 and Lemma 2.9.

The key to the proof of Lemma 2.9 is an alternative formula for the mapping degree of a continuous function $\varphi\colon \mathbb{RP}^1 \to \mathbb{RP}^1$. Suppose that $p \in \mathbb{RP}^1$ is a point with finitely many inverse images $\varphi^{-1}(p)$. To each inverse image we associate an index that records the behavior of $\varphi(t)$ as t increases past the inverse image. The index is $+1$ if $\varphi(t)$ increases past p, it is -1 if $\varphi(t)$ decreases past p, and it is 0 if φ stays on the same side of p. (Here, increase/decrease are taken with respect to the orientation of $\mathbb{RP}^1$.) For example, here is a graph of a function φ in relation to the value p with the indices of inverse images indicated.



With this definition, the mapping degree of φ is the sum of the indices of the points in a fiber $\varphi^{-1}(p)$, whenever the fiber is finite. That is,

$$\operatorname{mdeg}(\varphi) \;=\; \sum_{a\in\varphi^{-1}(p)} \text{index of } a\,.$$

Proof of Lemma 2.9. The zeroes of the rational function $\varphi := f/f'$ coincide with the zeroes of f. Suppose $f(a)=0$ so that a lies in $\varphi^{-1}(0)$. The lemma will follow once we show that a has index $+1$. Then we may write $f(t)=(t-a)^d h(t)$, where h is a polynomial with $h(a)\neq 0$. We see that $f'(t)=d(t-a)^{d-1}h(t)+(t-a)^d h'(t)$, and so

$$\varphi(t) \;=\; \frac{f(t)}{f'(t)} \;=\; \frac{(t-a)h(t)}{dh(t)+(t-a)h'(t)} \;\approx\; \frac{t-a}{d}\,,$$

the last approximation being valid for t near a as $h(t)\neq 0$. Since d is positive, we see that the index of the point a in the fiber $\varphi^{-1}(0)$ is $+1$.

Proof of Theorem 2.8. Suppose first that φ and ψ are rational functions with no common poles. Then

$$\operatorname{mdeg}(\varphi+\psi) \;=\; \operatorname{mdeg}(\varphi)+\operatorname{mdeg}(\psi)\,.$$

To see this, note that $(\varphi+\psi)^{-1}(\infty)$ is just the union of the sets $\varphi^{-1}(\infty)$ and $\psi^{-1}(\infty)$, and the index of a pole of φ equals the index of the same pole of $(\varphi+\psi)$.

Next, observe that $\mathrm{mdeg}(\varphi) = -\mathrm{mdeg}(1/\varphi)$. For this, consider the behavior of φ and $1/\varphi$ near the level set 1. If $\varphi > 1$ than $1/\varphi < 1$ and vice-versa. The two functions have index 0 at the same points, and opposite index at the remaining points in the fiber $\varphi^{-1}(1) = (1/\varphi)^{-1}(1)$.

Now consider the mapping degree of $\varphi = f/g$ as we construct its continued fraction expansion. At the first step $f = f_0 g + h$, so that $\varphi = f_0 + h/g$. Since f_0 is a polynomial, its only pole is at ∞, but as the degree of h is less than the degree of g, h/g does not have a pole at ∞. Thus the mapping degree of φ is

$$\mathrm{mdeg}(f_0 + h/g) \;=\; \mathrm{mdeg}(f_0) + \mathrm{mdeg}\big(\tfrac{h}{g}\big) \;=\; \mathrm{mdeg}(f_0) - \mathrm{mdeg}\big(\tfrac{g}{h}\big)\,.$$

The theorem follows by induction, as $\mathrm{mdeg}(f_0) = [f_0]$.

We close this chapter with an application of this method. Suppose that we are given two polynomials f and g, and we wish to count the zeroes a of f where $g(a) > 0$. If $g = (x-b)(x-c)$ with $b < c$, then this will count the zeroes of f in the interval $[b, c]$, which we may do with either of the main results of this chapter. If g has more roots, it is not *a priori* clear how to use the methods in the first two sections of this chapter to solve this problem.

A first step toward solving this problem is to compute the mapping degree of the rational function

$$\varphi \;:=\; \frac{f}{gf'}\,.$$

We consider the indices of its zeroes. First, the zeroes of φ are those zeroes of f that are not zeroes of g, together with a zero at infinity if $\deg(g) > 1$. If $f(a) = 0$ but $g(a) \neq 0$, then $f = (t-a)^d h(t)$ with $h(a) \neq 0$. For t near a,

$$\varphi(t) \;\approx\; \frac{t-a}{d \cdot g(a)}\,,$$

and so the preimage $a \in \varphi^{-1}(0)$ has index $\mathrm{sign}\,(g(a))$. If $\deg(g) = e > 1$ and $\deg(f) = d$ then the asymptotic expansion of φ for t near infinity is

$$\varphi(t) \;\approx\; \frac{1}{d g_e t^{e-1}}\,,$$

where g_e is the leading coefficient of g. Thus the index of $\infty \in \varphi^{-1}(0)$ is $\mathrm{sign}\,(g_e)(e-1 \mod 2) \;=\; [g']$. We summarize this discussion.

Lemma 2.11 *If* $\deg(g) > 1$, *then*

$$\sum_{\{a \mid f(a)=0\}} \mathrm{sign}\,(g(a)) \;=\; \mathrm{mdeg}(\varphi) \;-\; [g']\,,$$

and if $\deg(g) = 1$, *the correction term* $-[g']$ *is omitted.*

Since $\mathrm{mdeg}(\varphi) = -\mathrm{mdeg}(1/\varphi)$, we have the alternative expression for this sum.

Lemma 2.12 *Let $q_1, q_2, \ldots, q_k$ be the successive quotients in the Euclidean algorithm applied to the division of $f'g$ by f. Then*

$$\sum_{\{a|f(a)=0\}} \mathrm{sign}\,(g(a)) \;=\; [q_2] - [q_3] + \cdots + (-1)^k [q_k]\,.$$

Proof. We have

$$\mathrm{mdeg}\frac{f}{f'g} \;=\; -\mathrm{mdeg}\frac{f'g}{f} \;=\; -[q_1] + [q_2] - \cdots + (-1)^k [q_k]\,,$$

by Theorem 2.8. Note that we have $f'g = q_1 f + r_1$. If we suppose that $\deg(f) = d$ and $\deg(g) = e$, then $\deg(q_1) = e - 1$. Also, the leading term of q is dg_e, where g_e is the leading term of g, which shows that $[q_1] = [g']$. Thus the lemma follows from Lemma 2.11, when $\deg(g) \geq 2$.

But it also follows when $\deg(g) < 2$ as $[q_1] = 0$ in that case.

Now we may solve our problem. For simplicity, suppose that $\deg g > 1$. Note that

$$\tfrac{1}{2}\big(\,\mathrm{sign}\,(g^2(a)) + \mathrm{sign}(g(a))\big) \;=\; \begin{cases} 1 & \text{if } g(a) > 0 \\ 0 & \text{otherwise} \end{cases} \quad .$$

And thus

$$\#\{a \mid f(a) = 0,\; g(a) > 0\} \;=\; \frac{1}{2}\mathrm{mdeg}\left(\frac{f}{g^2 f'}\right) \;+\; \frac{1}{2}\mathrm{mdeg}\left(\frac{f}{g f'}\right)\,,$$

which solves the problem.