Vincent's Zero-finder

1 Introduction

Vincent [Vin36, CA76, Akr80, RZ01] gave an algorithm for finding isolating intervals for the real zeroes of a polynomial p with real coefficients. The algorithm is based on Descartes' rule of sign.

2 Descartes' Rule of Sign

For a polynomial $P(x) = \sum_{0 \le i \le n} a_i x^i \in \mathbb{R}[x]$, let $V(P)$ be the number of sign variations in its coefficient sequence, i.e., number of pairs i, j with $0 \le i < j \le n = \deg P$, $a_i a_j < 0$ and $a_{i+1} = \ldots = a_{j-1} = 0$ and let $pos(P)$ be the number of positive real roots counted with multiplicity.

Theorem 1 *Let $P(x) = \sum_{0 \le i \le n} a_i x^i \in \mathbb{R}[x]$. Then $\Delta(P) = V(P) - pos(P)$ is an even non-negative integer.*

Proof: We may assume w.l.o.g. that the lead coefficient a_n is positive and that the tail coefficient a_0 is non-zero. We proceed in two steps. We first show that Δ is an even integer ($\Delta \in 2\mathbb{Z}$) and then $\Delta \ge -1$.

We first observe that $pos(P)$ is even if $a_0 > 0$ and is odd if $a_0 < 0$. The same is true for $V(P)$. We conclude that Δ is an even integer.

We next show that Δ is non-negative. We use induction on the degree. The claim is certainly true for a constant polynomial. Assume now that P has degree $n \ge 1$ and let P' be the derivative of P. The number of zeros of P is at most one larger than the number of zeros of P', because any two zeros of P are separated by a zero of P'. Also $V(P) \ge V(P')$. Thus

$$\begin{aligned}
\Delta(P) &= V(P) - pos(P) \\
&\ge V(P') - pos(P') - 1 \\
&= \Delta(P') - 1 \\
&\ge -1 \ ,
\end{aligned}$$

where the last line uses the induction hypothesis. Together with the fact that Δ is even, this implies $\Delta \ge 0$. ∎

In general, Descartes' rule only gives an upper bound on the number of roots. However, if $V(P) = 0$ or $V(P) = 1$, the bound is sharp. In the former case there is no positive real root and in the latter case there is exactly one positive real root.

3 Vincent's Algorithm

We describe an algorithm for determining the number of real roots of P in the interval $(0,1)$. In the exercises, we ask you to extend the algorithm so that it also computes isolating intervals or determines the number of positive (negative, non-negative, all) roots. For example, in order to determine the postive real roots, we simply consider the polynomial $Q(x) = P(x/B)$, where B is an upper bound on the real roots of P. We next describe the algorithm.

Consider $Q(x) = (1+x)^n P(\frac{1}{1+x})$. The mapping $x \mapsto \frac{1}{1+x}$ maps $(0,+\infty)$ to $(0,1)$ and hence the number of positive zeros of Q is equal to the number of zeros of P in $(0,1)$.

We apply Descartes' rule to Q. If there is no sign variation, we conclude that P has no zero in $(0,1)$. If there is exactly one sign variation, we conclude that P has exactly one zero in $(0,1)$ and hence $(0,1)$ is an isolating interval.

So assume that there are at least two sign changes. We first test whether $P(1/2) = 0$. If so, $[1/2, 1/2]$ is an isolating interval for the zero $1/2$.

We consider $P_1(x) = P(x/2)$ and $P_2(x) = P((1+x)/2)$. Observe that the zeroes of P_1 in $(0,1)$ correspond to the zeroes of P in $(0,1/2)$ and the zeroes of P_2 correspond to the zeroes of P in $(1/2,1)$. We apply the method recursively to P_1 and P_2.

This completes the description of the algorithm. The following procedure *Vincent* summarizes it and returns the number of real zeros of P in the interval $(0,1)$.

int Vincent(polynomial P)

1. determine the number δ of sign variations in $Q(x)$.
2. if $\delta \leq 1$ return δ.
3. let $d = 1$ if $P(1/2) = 0$ and let $d = 0$ otherwise.

$$\text{return } d + \textit{Vincent}(P1) + \textit{Vincent}(P2);$$

The partial correctness of the algorithm follows from Descartes' rule of sign. Why does it terminate? It does not always terminate. If P has a double root (which is not of the form $i/2^k$ for integers i and k), the algorithm does not terminate.

Theorem 2 *If P is square-free (i.e., has no double roots), Vincent(P) terminates and returns the number of real zeroes of P in the interval $(0,1)$.*

Proof: The algorithm repeatedly splits the unit interval. Thus in the generic step it searches for the zeroes of P in an interval $I = (i/2^k, (i+1)/2^k)$ for some integers i and k with $0 \leq i < 2^k$. It maps the unit interval $(0,1)$ onto I through the map $x \mapsto \frac{i+x}{2^k}$ and considers the polymomial $Q(x) = P(\frac{i+x}{2^k})$. It applies Descartes' rule to the polynomial $R(x) = (1+x)^n Q(\frac{1}{1+x}) = (1+x)^n P(l + \frac{r-l}{1+x})$. We need conditions on Q under which Descartes rule applied to R implies termination, i.e., conditions on Q under which $V(R) \leq 1$ is guaranteed. The following Lemmas do the job.

Lemma 1 *If Q has no roots inside the disk of radius $1/2$ centered at the point $(1/2, 0)$ then the transformed polygon has no sign variation in its coefficient sequence, i.e., $V(R(x)) = 0$, where $R(x) = (1+x)^n P(\frac{1}{1+x})$.*

Lemma 2 *If Q has exactly one real root in $(0, 1)$ and no non-real root inside the open disks centered at $1/2 \pm i/(2\sqrt{3})$ and passing through the origin (and hence radius $1/\sqrt{3}$), then $V(R(x)) = 1$, where $R(x) = (1+x)^n P(\frac{1}{1+x})$.*

Let us believe these lemmas for the moment. Let

$$\epsilon = \min \{ |z_1 - z_2| \ ; \ P(z_1) = P(z_2) = 0 \text{ and } z_1 \neq z_2 \}$$

and consider an interval $I = (i/2^k, (i+1)/2^k)$, where $2^{-k} < \epsilon/2$, and the associated polynomial $Q(x) = P(\frac{i+x}{2^k}$. Then

$$\min \{ |z_1 - z_2| \ ; \ Q(z_1) = Q(z_2) = 0 \text{ and } z_1 \neq z_2 \} \geq \epsilon 2^k \geq 2 \ .$$

Any two points in the disks mentioned in the Lemmas above have distance at least two and hence Q satisfies the hypothesis of one of the Lemmas. It has at most one real root in the interval $(0, 1)$ and no non-real root in the disks mentioned in the Lemmas (recall that non-real roots come in pairs and hence if there would be one non-real root in one of the disks there would be two). We conclude that Descartes rule of sign applied to $Q(x) = (1+x)^n P(l + \frac{r-l}{1+x})$ will return either zero or one. This proves termination (modulo the proofs of the lemmas above). ∎

We give a proof of the first lemma here and refer the reader to [Meh01] for a proof of the second lemma. I change notation for remainder of the section. What I called Q above, I call P from now on.

Lemma 3 *If all zeros of a real polynomial P have non-positive real part then $V(P) = 0$. Alternatively, if P has no zeroes in the right half-plane, Descartes' rule is strong enough to decide that there are no positive real roots.*

Proof: We can write $P(x) = Q(x)R(x)$ where all zeros of Q are real and all zeros of R are non-real. The reals of R come in pairs. Consider a pair of roots. We have

$$\begin{aligned}(x - \alpha_i)(x - \overline{\alpha_i}) &= x^2 - x(\alpha_i + \overline{\alpha_i}) + \alpha_i \cdot \overline{\alpha_i} \\ &= x^2 - 2x\Re\alpha_i + (\Re\alpha_i)^2 + (\Im\alpha_i)^2\end{aligned}$$

and hence all coefficients are non-negative. Similarly, if $\alpha \in \mathbb{R}$ and $\alpha \leq 0$, the coefficients of $x - \alpha$ are non-negative. The product of polynomials with non-negative coefficients has non-negative coefficients. ∎

Consider now a polynomial R. We want to prove that it has no real root in the interval $(0,1)$. We consider $Q(x) = x^n R(1/x)$ (the roots of R in $(0,1)$ correspond to the roots of Q in $(1,\infty)$) and $P(x) = Q(1+x)$. Then we are interested in positive real roots of P. The Lemma above tells us: If P has no roots in the right half-plane then $V(P) = 0$. What does the hypothesis mean for Q and R? Q must have no roots with real part larger than one, call this region $\mathcal{Q}$, and R must have no root in the region obtained by inversion of $\mathcal{Q}$. This region is $\{1/z\ ;\ \Re z > 1\}$.

Consider the ray passing through the point $1 + iy$. The points in the forbidden region and lying on this ray lie on the ray starting in the origin and ending in the point $(1/L, y/L)$ where $L = 1 + y^2$. Thus the forbidden region for R is an oval shaped region symmetric to the x-axis. In parametric form the boundary of this region is described by $(1/L, t/L)$ where $L = 1 + t^2$ and $t \geq 0$. The boundary of the forbidden region for R is given by the points $(1/L, t/L)$ where $L = 1 + t^2$ and $t \in \mathbb{R}$, i.e., $x = 1/L$ and $y = t/L$. Solving for t yields $t = \pm\sqrt{(1-x)/x}$ and hence $y = tx = \pm\sqrt{x(1-x)}$. Squaring gives $y^2 = x(1-x)$. This is the equation of the disk of radius 1/2 centered at the point (1/2,0). We summarize:

Lemma 4 *If P has no roots inside the disk of radius $1/2$ centered at the point $(1/2, 0)$ then the transformed polygon has no sign variation in its coefficient sequence.*

References

[Akr80] A. G. Akritas. The fastest exact algorithms for the isolation of the real roots of a polynomial equation. *Computing*, 24(4):299–313, 1980.

[CA76] G. E. Collins and A.-G. Akritas. Polynomial real root isolation using Descartes' rule of sign. In *SYMSAC*, pages 272–275, Portland, OR, 1976.

[CJ89] G. E. Collins and J. R. Johnson. Quantifier elimination and the sign variation method for real root isolation. In Gaston H. Gonnet, editor, *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*, pages 264–271, Portland, OR, July 1989. ACM Press.

[CL82] G. E. Collins and R. Loos. Real zeros of polynomials. *Computing*, Suppl. 4:83–94, 1982.

[Meh01] K. Mehlhorn. A remark on the sign variation method for real root isolation. www.mpi-sb.mpg.de/˜mehlhorn/ftp/Descartes.ps, 2001.

[Mig92] M. Mignotte. *Mathematics for Computer Algebra.* Springer, 1992.

[RZ01] F. Rouillier and P. Zimmermann. Efficient isolation of polynomial real roots. Technical Report 4113, INRIA, 2001.

[Vin36] A. J. H. Vincent. Sur la résolution des equation numériques. *Journal de Mathématiques Pures et Appliquées*, pages 341–372, 1836.