A NOTE ON COMPARING NUMBERS IN A REAL ALGEBRAIC FIELD

W. PATRICK HOOPER

Abstract. We describe an algorithm to determine the sign of an number in the field $\mathbb{Q}(\alpha)$, where α is a real root of a polynomial over the integers. The algorithm is elementary and short, and is derived from the Perron-Frobenius theorem.

Let $p(x)$ be the square-free polynomial $x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0$ with coefficients in $\mathbb{Q}$. Let α be a real root of p. Consider the field $\mathbb{Q}(\alpha)$, which is naturally embedded in $\mathbb{R}$.

In this note, we will explain how to decide the question, "Is a given element of $\beta \in \mathbb{Q}(\alpha)$ positive or negative?", in the case when $p(x)$ is irreducible.

The algorithm we describe is relevant to any endevour which needs to repeatedly compare numbers in a fixed algebraic field. For instance in dynamics, computing an orbit under an interval exchange with intervals that have lengths in the algebraic field $\mathbb{Q}(\alpha)$ requires repeated comparisons of algebraic numbers in $\mathbb{Q}(\alpha)$. More generally, it is relevant to any experimental problem which makes use of computational geometry over an algebraic field. Here, signed areas of simplices are expected by algorithms to obey the axioms, and signs of determinants need to be computed rigorously.

Our method requires as input information about the location of the root α. This information is easily given by existing root isolation techniques, which we cite as needed. Once some initial calculations involving α are done, we are able to decide the sign of $\beta \in \mathbb{Q}(\alpha)$ using a simple dynamical test, which is derived from the Perron-Frobenius theorem.

1. The principal idea

Let $q(x) = \frac{p(x)}{x-\alpha}$, which is a polynomial of degree $n-1$ over $\mathbb{R}$. Let $\hat{q}(x)$ be polynomial of degree $n-1$ over $\mathbb{Q}$ which approximates $q(x)$. For a suitable approximation $\hat{q}(x)$, we can assume

$$|\hat{q}(\alpha)| > |\hat{q}(\eta)| \text{ for all roots } \eta \text{ of } p(x) \text{ with } \eta \neq \alpha. \tag{1}$$

This is because $p(x)$ is square-free implies $q(\alpha) \neq 0$, but $q(\eta) = 0$.

Consider the polynomial ring $\mathbb{Q}[x]/p(x)$. We also consider $\hat{q}(x) \in \mathbb{Q}[x]/p(x)$. We identify this ring with $\mathbb{Q}^n$ using the standard basis $\mathcal{B} = \{1, x, \ldots, x^{n-1}\}$. There is an surjection $\phi : \mathbb{Q}[x]/p(x) \to \mathbb{Q}(\alpha) \subset \mathbb{R}$ given by evaluation at α, or equivalently

$$\phi : \mathbb{Q}^n \to \mathbb{Q}(\alpha) : \mathbf{b} \mapsto \mathbf{w} \cdot \mathbf{b}$$

where $\mathbf{w} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \end{bmatrix}^T \in \mathbb{R}^n$.

Lemma 1. *The vector* $\mathbf{v}_\alpha = \begin{bmatrix} a_0 & \frac{a_0+a_1\alpha}{\alpha} & \frac{a_0+a_1\alpha+a_2\alpha^2}{\alpha^2} & \ldots & \frac{a_0+a_1\alpha+\ldots+a_{n-2}\alpha^{n-2}}{\alpha^{n-2}} & \alpha \end{bmatrix}^T \in \mathbb{R}^n$ *is the unique eigenvector up to scaling for the action of multiplication by* x *on* $\overline{\mathbb{Q}[x]/p(x)} = \mathbb{R}^n$ *with eigenvalue* α.

2000 *Mathematics Subject Classification.* 11Y40, 12Y05; 37M99, 52C99.

This will be demonstrated later.

Theorem 2. *Suppose $\hat{q}(x)$ satisfies assumption 1. If $b \in \mathbb{Q}[x]/p(x)$ is chosen so that $\phi(b) \neq 0$, then*

$$\lim_{k\to\infty} \frac{\hat{q}^{2k}(x)b}{|\hat{q}^{2k}(x)b|} = \frac{\pm v_\alpha}{|v_\alpha|}$$

where $|*|$ denotes the Euclidean norm on $\mathbb{Q}^n$. Furthermore, the sign of the limit determines the sign of $\phi(\mathbf{b})$.

If $p(x)$ is irreducible then ϕ is a ring isomorphism. We get the following algorithm.

Corollary 3. *Suppose $p(x)$ is irreducible and that $\hat{q}(x)$ satisfies assumption 1. Let C_+ and C_- be open cones in $\mathbb{Q}^n \setminus \{\mathbf{0}\}$ such that*

1. *$\phi(\mathbf{x}_+) > 0$ for all $\mathbf{x}_+ \in C_+$ and $\phi(\mathbf{x}_-) < 0$ for all $\mathbf{x}_- \in C_-$*
2. *The eigenspace $\mathbb{R}\mathbf{v}_\alpha \setminus \{\mathbf{0}\}$ is contained in the interior of $\overline{C_+} \cup \overline{C_-}$.*

Let $\beta \in \mathbb{Q}(\alpha)$ be non-zero. Then $\beta > 0$ if and only if there is a $k \geq 0$ such that $\hat{q}^{2k}(x)\phi^{-1}(\beta) \in C_+$. And, $\beta < 0$ if and only if there is a $k \geq 0$ such that $\hat{q}^{2k}(x)\phi^{-1}(\beta) \in C_-$.

Proof of lemma 1. The matrix for the action of multiplication by x on $\mathbb{Q}[x]/p(x)$ in the basis $\mathcal{B}$ is given by

$$M_x = \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & a_0 \\ 1 & 0 & 0 & 0 & \cdots & a_1 \\ 0 & 1 & 0 & 0 & \cdots & a_2 \\ 0 & 0 & 1 & 0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & a_{n-1} \end{bmatrix}$$

The characteristic polynomial of M_x is precisely $\pm p(x)$ with a negative sign when n is odd and a positive sign when n is even. Eigenspaces are one-dimensional, because $p(x)$ is square-free. Furthermore, it is a simple check that $\mathbf{v}_\alpha$ is an eigenvector of M_x with eigenvalue α. □

Proof of theorem 2. The subspace of $\overline{\mathbb{Q}[x]/p(x)} = \mathbb{R}^n$ spanned by the other eigenvectors of M_x is precisely the kernel of the extended linear map $\overline{\phi} : \mathbb{R}^n \to \mathbb{R}$. (These are both the subspace spanned by the columns of $M_x - \alpha I$.) Thus the condition that $\phi(b) \neq 0$ implies that b is not within the span of the eigenvectors corresponding to eigenvalues not equal to α.

The matrix for multiplication by $\hat{q}^2(x)$ in the basis $\mathcal{B}$ of $\mathbb{Q}[x]/p(x)$ is given by $M_{\hat{q}^2} = \hat{q}^2(M_x)$. The vector $\mathbf{v}_\alpha$ is also eigenvector for $M_{\hat{q}^2}$ with real eigenvalue $\hat{q}^2(\alpha) > 0$. The other eigenvectors for the action of $M_{\hat{q}^2}$ lie in $\ker \overline{\phi}$. Thus, the action of $M_{\hat{q}^2}$ preserves the two components of $\mathbb{R}^n \setminus \ker \overline{\phi}$. Hence, $\operatorname{sign}\big(\phi(b)\big) = \operatorname{sign}\big(\phi(M_{\hat{q}^2}b)\big)$.

The eigenvalues of $M_{\hat{q}^2}$ are given by $\hat{q}^2(\eta)$ where η is a root of $p(x)$. By assumption 1, $\hat{q}^2(\alpha)$ is larger than the modulus of $\hat{q}^2(\eta)$ for any other root η of $p(x)$. Thus, for any $b \notin \ker \phi$, $M^k_{\hat{q}^2}b$ limits on the eigenspace with eigenvalue $\hat{q}^2(\alpha)$. The conclusion follows. □

2. Simplifying the assumption

Proposition 4. *Let $\hat{\alpha}$ be a rational approximation to α such that $|\alpha - \hat{\alpha}| < |\eta - \hat{\alpha}|$ for all roots $\eta \neq \alpha$ of $p(x)$. Then the approximation of $\frac{p(x)}{x-\alpha}$ given by $\hat{q}(x) = \frac{p(x)}{x-\hat{\alpha}}$ with the remainder term dropped satisfies condition 1.*

Proof. The remainder $r(x)$ is of the form $r(x) = \frac{k}{x-\hat{\alpha}}$ for some rational $k \neq 0$. Clearly, since $\hat{q}(x) + r(x) = \frac{p(x)}{x-\hat{\alpha}}$, we have $\hat{q}(\eta) = -r(\eta)$ for all roots η of $p(x)$. Thus,

$$|\hat{q}(\alpha)| - |\hat{q}(\eta)| = |r(\alpha)| - |r(\eta)| = \frac{1}{|\alpha - \hat{\alpha}|} - \frac{1}{|\eta - \hat{\alpha}|} > 0$$

because $|\alpha - \hat{\alpha}| < |\eta - \hat{\alpha}|$. Thus, $|\hat{q}(\alpha)| > |\hat{q}(\eta)|$ as required. □

Algorithms exist to find such a $\hat{\alpha}$. For example, by complex root isolation [CK92].

3. A cone via intervals

We will need to introduce a form of interval arithmetic. Let I be a non-degenerate closed interval in $\mathbb{R}$. We define I^n for $n \geq 0$ to be the closed interval which is the image of I under the map $x \mapsto x^n$. Similarly if $s \in \mathbb{R}$ we define $s + I$ to be the image of I under $x \mapsto s + x$ and sI to be the image of I under $x \mapsto sx$. And if J is another closed interval, we define $I + J$ to be the image of $I \times J$ under the map $(x, y) \mapsto x + y$.

Now let I be an interval containing α. We define the open convex cone

$$C_+^I = \{\mathbf{x} \in \mathbb{Q}^n \mid \text{the interval } x_0 + x_1 I + x_2 I^2 + \ldots + x_{n-1} I^{n-1} \text{ is all positive}\}.$$

And we set $C_-^I = -C_+^I$. This is the set of $\mathbf{x}$ such that the interval in the expression is all negative.

Remark 5. *The endpoints of each term $x_k I^k$ vary linearly in x_k, but the left endpoint depends on the sign of x_k. The condition is equivalent to saying that the sum of the left endpoints of the intervals in the expression is positive.*

Proposition 6. *If I is a sufficiently small interval containing the root α, then the cones C_+^I and C_-^I satisfy conditions 1 and 2 of corollary 3.*

Proof. Let $\mathbf{x} \in C_+^I$. Since $\alpha \in I$ we have

$$\phi(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x} = x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1} \ \in \ x_0 + x_1 I + x_2 I^2 + \ldots + x_{n-1} I^{n-1}.$$

So, $\phi(\mathbf{x}) > 0$. This verifies the condition that $\mathbf{x} \in C_+^I$ implies $\phi(\mathbf{x}) > 0$. A symmetric argument handles the negative case.

To see the second condition, consider that $\mathbf{w} \cdot \mathbf{v}_\alpha \neq 0$. This follows from the computation

$$\mathbf{w} \cdot \mathbf{v}_\alpha = na_0 + (n-1)a_1\alpha + (n-2)a_2\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

Thus, $\mathbf{w} \cdot \mathbf{v}_\alpha = -np(x) + x\frac{d}{dx}p(x)$. We know $p'(\alpha) \neq 0$, or else α would be a double root of $p(x)$. And, being a double root violates the assumption that $p(x)$ is square-free.

Abbreviate $\mathbf{v}_\alpha = \begin{bmatrix} v_0 & v_1 & \ldots & v_{n-1} \end{bmatrix}$. The interval

$$v_0 + v_1 I + v_2 I^2 + \ldots + v_{n-1} I^{n-1} \tag{2}$$

varies continuously in I. The previous paragraph showed that this expression does not contain zero when I is the degenerate interval $[\alpha, \alpha]$. Therefore, for a sufficiently small non-degenerate interval containing α, the interval in equation 2 does not contain zero. Hence $\mathbf{v}_\alpha \in C_+^I \cup C_-^I$. □

Requesting a interval that isolates α is a minor request, since there are many methods available to find intervals isolating a real root [Yap00] [BPR03]. Once the root is isolated, arbitrarily small intervals can be found by bisection, and then keeping the half interval where the signs of $p(x)$ differ when evaluated on the endpoints.

Remark 7 (Checking condition 2 of the corollary)**.** *We can provide a computable sufficient condition for I to satisfy condition of 2 of the corollary. We provide such a condition that implies that $\alpha^{n-1}\mathbf{v}_\alpha \in C^I_+ \cup C^I_-$. We chose $\alpha^{n-1}\mathbf{v}_\alpha$, because it is (without computation) an eigenvector with entries which are polynomial in α. The condition $\alpha^{n-1}\mathbf{v}_\alpha \in C^I_+ \cup C^I_-$ says*

$$0 \notin (a_0\alpha^{n-1}) + (a_0\alpha^{n-2} + a_1\alpha^{n-1})I + \ldots + (a_0 + a_1\alpha + \ldots a_{n-1}\alpha^{n-1})I^{n-1}.$$

Now we estimate powers of α using I again. Thus, the above condition is implied by

$$0 \notin (a_0 I^{n-1}) + (a_0 I^{n-2} + a_1 I^{n-1})I + \ldots + (a_0 + a_1 I + \ldots + a_{n-1}I^{n-1})I^{n-1}.$$

By regrouping we get the nicer form

$$0 \notin a_0(I^{n-1}I^0 + I^{n-2}I^1 + \ldots + I^0 I^{n-1}) + a_1(I^{n-1}I + \ldots + II^{n-1}) + \ldots + a_{n-1}(I^{n-1}I^{n-1}).$$

By the same argument as in the proposition, this must hold for a sufficiently small I containing α.

References

[BPR03] Saugata Basu, Richard Pollack, and Marie-Françoise Roy, *Algorithms in real algebraic geometry*, Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2003. MR1998147 (2004g:14064)

[CK92] George E. Collins and Werner Krandick, *An efficient algorithm for infallible polynomial complex root isolation*, International Conference on Symbolic and Algebraic Computation (Berkeley, 1992), Papers from the international symposium on Symbolic and algebraic computation, ACM, New York, 1992, pp. 189 – 194.

[Yap00] Chee Keng Yap, *Fundamental problems of algorithmic algebra*, Oxford University Press, New York, 2000. MR1740761 (2000m:12014)

Department of Mathematics, Northwestern University, 2033 Sheridan Road, Evanston, IL 60208-2730, USA (phone: 847-491-2853, fax: 847-491-8906)

E-mail address: wphooper@math.northwestern.edu