Computing a rational in between

Ioannis Emiris* Bernard Mourrain† Elias Tsigaridas†

May 3, 2008

We are interested in the following problem: Given two (distinct) real algebraic numbers and their order, can we compute a number between them as a rational polynomial function of the coefficients of the polynomials that define these two numbers?

Given intervals that contain the real algebraic numbers and a procedure to refine them, we can solve our problem as follows: We refine the intervals until they become disjoint, this will happen eventually since we assume that the real algebraic numbers are not equal, and then we compute a rational number between the intervals, which is, evidently, between the real algebraic numbers, as well. However, this an iterative approach and it depends on separation bounds, e.g. [11]. We present a direct method, which is applicable when we allow in addition to compute the floor of a polynomial expression that involves real algebraic numbers. In the end, we will also remove the assumption that the order of the real algebraic numbers is known.

The problem arises when we want to compute rational numbers that isolate the roots of an integer polynomial of small degree, say ≤ 5 [3]. Another motivation comes from geometry. In order to analyse the intersection of two quadrics P and Q [10], one need to determine the real roots of the polynomial $\det(P + xQ) = 0$, their multiplicities and a value in between each of these roots.

1 A rational between square roots

Let us first consider a simple problem. Given two expressions involving square roots, that is $\alpha = a_1 + \sqrt{b_1}$ and $\beta = a_2 + \sqrt{b_2}$, such that $\alpha < \beta$, can we compute a number $m = \frac{p}{q}$ such that $\alpha < m < \beta$, as a rational polynomial function of a_1, a_2, b_1, b_2?

Lemma 1. *Given $a_1, a_2 \in \mathbb{Z}$, $b_1, b_2 \in \mathbb{N}$, let $\beta > \alpha > 0$ be defined below. Then, it is possible to determine $m \in \mathbb{Q}$ as a function of a_1, a_2, b_1, b_2, such that*

$$\alpha = a_1 + \sqrt{b_1} \leq m \leq a_2 + \sqrt{b_2} = \beta.$$

Proof: Notice that α is a root of the polynomial $h_1(x) = x^2 - 2\,a_1 x - b_1 + {a_1}^2$, while β is a root of $h_2(x) = x^2 - 2\,a_2 x - b_2 + {a_2}^2$. We consider the following resultant w.r.t. y:

$$h(x) = \text{resultant}_y(h_1(y), h_2(x+y)) = x^4 + n_3 x^3 + n_2 x^2 + n_1 x + n_0, \tag{1}$$

*National Kapodistrian University of Athens, HELLAS. emiris(AT)di.uoa.gr

†INRIA Sophia Antipolis Méditerranée, FRANCE. FirstName.LastName(AT)sophia.inria.fr

where $n_3 = 4\,a_1 - 4\,a_2$,
$n_2 = -12\,a_2 a_1 + 6\,{a_2}^2 - 2\,b_1 - 2\,b_2 + 6\,{a_1}^2$,
$n_1 = -4\,(a_1 - a_2)\,(-{a_1}^2 + 2\,a_2 a_1 + b_1 + b_2 - {a_2}^2)$,
$n_0 = 4\,a_2 a_1 b_1 + 4\,a_2 a_1 b_2 + {b_1}^2 - 2\,b_1 b_2 - 2\,b_1 {a_1}^2 - 2\,b_1 {a_2}^2 + {b_2}^2 - 2\,b_2 {a_1}^2 - 2\,b_2 {a_2}^2 + 6\,{a_1}^2 {a_2}^2 - 4\,a_2 {a_1}^3 - 4\,{a_2}^3 a_1 + {a_1}^4 + {a_2}^4$.

Polynomial $h(x)$ has $\beta - \alpha > 0$ as one of its (four) real roots. We consider any of the possible lower bounds $k > 0$ on the positive roots of h, see [4, 5, 7, 8, 9, 11]. Independently of the precise value of k, the following holds:

$$a_1 + \sqrt{b_1} < k + a_1 + \sqrt{b_1} < a_2 + \sqrt{b_2}.$$

If $k \geq 1$, then we set

$$m = k + a_1 + \left\lfloor \sqrt{b_1} \right\rfloor,$$

which satisfies the inequalities because $\lfloor \sqrt{b_1} \rfloor + k \geq \sqrt{b_1}$. In this case, we could also choose $m = 1 + a_1 + \lfloor \sqrt{b_1} \rfloor$.

If $k < 1$, then $k = \frac{\lambda}{\mu}$ for integers $1 \leq \lambda < \mu$, and it holds that

$$\mu\alpha = \mu a_1 + \mu\sqrt{b_1} < \lambda + \mu a_1 + \mu\sqrt{b_1} < \mu a_2 + \mu\sqrt{b_2} = \mu\beta. \tag{2}$$

Then, we choose

$$m = \frac{\lambda}{\mu} + a_1 + \frac{\lfloor \mu\sqrt{b_1} \rfloor}{\mu},$$

because $m < \beta \Leftrightarrow \mu m < \mu\beta$, which follows from the right inequality (2). Moreover, $\mu m \geq \lambda + \mu a_1 + \mu\sqrt{b_1} - 1 \geq \mu\alpha$. □

2 A rational between real algebraic numbers

The technique of the proof of the previous lemma is quite generic. Thus we will extend the previous lemma to a more general theorem.

Consider two real algebraic numbers $\alpha < \beta$, defined as real roots of $A = \sum_{i=0}^{d_a} a_i\, x^i$ and $B = \sum_{i=0}^{d_b} b_i\, x^i \in \mathbb{Z}[x]$, respectively. We are seeking for a number m, such that $\alpha < m < \beta$, defined as a rational polynomial functions in the coefficients of A and B. We consider the polynomial

$$C(x) = \sum_{i=0}^{d_c} c_i\, x^i = \text{resultant}_y(A(y), B(x+y), y), \tag{3}$$

which has as real roots all the differences of the roots of the polynomials A and B. If the constant coefficient of C is zero, then we divide C by x until we obtain a polynomial with non zero constant term. By abuse of notation we denote this polynomial by C. Let $0 < k$ be a lower bound on the absolute value of the roots of C. Then it holds that

$$\alpha < k + \alpha < \beta.$$

If $k \geq 1$ then $m = k + \lfloor \alpha \rfloor$, since $\lfloor \alpha \rfloor + k \geq \alpha$. If $k < 1$, then let $k = \frac{\lambda}{\mu}$ for some numbers $1 \geq \lambda < \mu$. In this case, it holds that

$$\mu\,\alpha < \lambda + \mu\,\alpha < \mu\,\beta,$$

and so we can choose

$$m = \frac{\lambda}{\mu} + \frac{\lfloor \mu\,\alpha \rfloor}{\mu}. \tag{4}$$

The previous discussion allows us to state the following theorem:

Theorem 2. *Consider two real algebraic numbers $\alpha < \beta$. We can compute a number m, such that $\alpha < m < \beta$ as a rational polynomial function in the coefficients of the polynomials that define α and β, using the four basic operations and the $\lfloor \cdot \rfloor$ function.*

2.1 What we can choose as lower bound

If we can afford the computation of C, refer to Eq. (3), then in order to compute k, we can apply one of the various lower bounds [4, 5, 7, 8, 9, 11], available in the literature.

If we do not want to compute $C(X)$ then we can proceed as follows. Recall, e.g. [6], that for a real algebraic number, say γ, its measure, $\mathcal{M}(\gamma)$, is the Mahler measure of its minimum polynomial. It holds that $\frac{1}{\mathcal{M}(\gamma)} < |\gamma| < \mathcal{M}(\gamma)$, and $\mathcal{M}(\beta \pm \alpha) \leq 2^{d_a\,d_b}\mathcal{M}(\alpha)^{d_b}\,\mathcal{M}(\beta)^{d_a}$. Thus, we can choose

$$k = 2^{-d_a d_b}\,\mathcal{M}(A)^{-d_b}\,\mathcal{M}(B)^{-d_a}\,.$$

Remark 3. *If the polynomials that define α and β have degree bounded by d and maximum coefficient bit size bounded by τ, then using the fact that $\mathcal{M}(A) \leq \|A\|_2 \leq \sqrt{d}\,2^{\tau}$, we can choose as rational between α and β the number*

$$m = \frac{1}{d\,2^{d^2+2d\tau}} + \frac{\left\lfloor d\,2^{d^2+2d\tau}\,\alpha \right\rfloor}{d\,2^{d^2+2d\tau}},$$

or the more "simple" number

$$m = \frac{1}{2^{2d^2+2d\tau}} + \frac{\left\lfloor 2^{2d^2+2d\tau}\,\alpha \right\rfloor}{2^{2d^2+2d\tau}},$$

which can be implemented using only shift operations.

Other estimations, possible sharper, are possible using the inequalities $\mathcal{M}(A) \leq [A]_2 \leq \|A\|_2 \leq \sqrt{d}\|A\|_\infty$, where $[A]_2$ is the Bombieri norm [1].

Example 4. *We will compute a rational between $\alpha = \sqrt[5]{2} < \sqrt[5]{3} = \beta$, which are roots of $A(x) = x^5 - 2$ and $A(x) = x^5 - 3$, respectively. The polynomial $C(x)$ of (3) is $C(x) = x^{25} - 5\,x^{20} + 3760\,x^{15} + 11240\,x^{10} + 116255\,x^5 - 1$, and a lower bound on its roots is $k = \frac{1}{116256}$. Thus, a rational between α and β, refer to (4), is*

$$m = \frac{1}{116256} + \frac{\left\lfloor 116256\,\sqrt[5]{2} \right\rfloor}{115256} = \frac{1 + 133543}{116256} = \frac{16693}{14532}.$$

3 Further extensions

We can drop the assumption of Th. 2 that we know the order of the two real algebraic numbers. Initially, we assume $\alpha < \beta$ and we compute a rational m_1. Assuming $\alpha > \beta$ we compute a rational m_2. Then, $m = \min\{m_1, m_2\}$ is between α and β.

We hope that this result will help us to derive a probabilistic test for comparing two expressions involving roots of rational numbers, similar to the one for zero-testing [2].

References

[1] B. Beauzamy, E. Bombieri, P. Enflo, and H.L. Montgomery. Products of polynomials in many variables. *J. Number Theory*, 36:219–245, 1990.

[2] J. Blömer. A Probabilistic Zero-Test for Expressions Involving Root of Rational Numbers. *Proc. of the 6th Annual European Symposium on Algorithms (ESA)*, pages 151–162, 1998.

[3] I. Z. Emiris and E. P. Tsigaridas. Real algebraic numbers and polynomial systems of small degree. *Theoretical Computer Science*, 2008. (to appear).

[4] H. Hong. Bounds for absolute positiveness of multivariate polynomials. *J. of Symbolic Computation*, 25(5):571–585, May 1998.

[5] J. Kioustelidis. Bounds for the positive roots of polynomials. *J. of Computational and Applied Mathematics*, 16:241–244, 1986.

[6] M. Mignotte and D. Ştefănescu. *Polynomials: An algorithmic approach*. Springer, 1999.

[7] D. Ştefănescu. New bounds for the positive roots of polynomials. *J. of Universal Computer Science*, 11(12):2132–2141, 2005.

[8] D. Ştefănescu. Inequalities on polynomial roots. *Mathematical Inequalities and Applications*, 5(3):335–347, 2002.

[9] E. P. Tsigaridas. *Algebraic algorithms and applications to geometry*. PhD thesis, National Kapodistrian University of Athens, Aug 2006. (available at http://www-sop.inria.fr/galaad/elias).

[10] C. Tu, W. Wang, B. Mourrain, and J. Wang. Signature sequence of intersection curve of two quadrics for exact morphological classification. 2005. URL `citeseer.ist.psu.edu/tu05signature.html`.

[11] C.K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.