Separation Bounds
Lectures on November XXX

In the last lecture (handout "Circle Points and Predicates on Circle Points") we learned how to compute the sign of expressions with integer operands and operators $+$, $-$, $\times$, and $\sqrt{\ }$ by repeated squaring. Although general, the method is tedious. In this section, we learn about an alternative sign strategy. Sign computation by numerical calculation.

The idea is the following. Consider an expression E and assume that we compute a high-precision approximation $\tilde{E}$ of E, i.e,

$$|\tilde{E} - E| < B = 2^{-K} \quad \text{for some large } K.$$

We will learn later how to compute such approximations. If $|\tilde{E}| \geq B$, the signs of E and $\tilde{E}$ agree and we are done. If $|\tilde{E}| < B$, we cannot make any conclusion. OR CAN WE? *The crucial insight is that if B is small enough (K is large enough), we are allowed to conclude that E is zero.*

How small is small enough? I closed the previous section with a remark on complexity. If there are k distinct roots, we will go through k rounds of squaring. Squaring doubles the length of numbers involved. Hence if all operands of E are L bit integers, we should expect to work with integers of length about $2^k L$. This reasoning ignores the fact that squaring will also increase the number of terms and that this will lead to a further increase in bit size. It turns out that $K \approx 2^k L$ will work. The precise statement is as follows.

Theorem 1 *Let E be an expression with integer operands and operators $+$, $-$, $\times$, and $\sqrt{\ }$. Let k be the number of distinct square root operations in E and let $u(E)$ be the value of E after changing all minus signs into plus signs and after replacing all operands by their absolute value. Then $|E| \leq u(E)$ and*

$$E = 0 \quad \text{or} \quad |E| \geq \frac{u(E)}{u(E)^{2^k}} \ .$$

We may therefore take $B = u(E)^{1-2^k}/2$ in the numerical sign test.

More general results are proved in [BFMS00, BFM$^+$01, LY01]. We state and prove the simple result here, because it allows us to give a prove without algebraic prerequisites. It also reflects history. Our first proof was along the same lines.

The LEDA number class real supports sign tests for expressions with integer operands and operators $+$, $-$, $\times$, $/$, and $\sqrt[k]{\ }$ for arbitrary integer k. The sign test is based on the theorem above.

Guest Lecturer: Stefan Funke talks about the internals of LEDA reals.

Proof: The claim $|E| \leq u(E)$ is clear. We prove the other claim by induction on the number of roots in E. If $k = 0$ and $E \neq 0$, we have $|E| \geq 1$ since E is an integer. This establishes the induction base.

So consider an expression E involving at least one root. If $E = 0$, there is nothing to prove. Again we concentrate on an outermost root, say $\sqrt{C}$, and use the distributive law to rewrite E as $E_1 = A + B\sqrt{C}$ where A and B do not involve $\sqrt{C}$. Application of the distributive law has no effect on u and hence $u(E_1) = u(E)$. We want to derive a lower bound on the absolute value of E_1, if E_1 is non-zero.

We first deal with a special case. If $A = B\sqrt{C}$, $E = 2A$ and hence $|E| \geq |A| \geq 1/u(A)^{2^{k-1}-1} \geq 1/u(E)^{2^k-1}$. Observe that A contains at most $k-1$ distinct roots and hence the induction hypothesis applies to A.

So assume $A \neq B\sqrt{C}$. We have

$$|E_1| = |A + B\sqrt{C}| = |\frac{(A + B\sqrt{C})(A - B\sqrt{C})}{A - B\sqrt{C}}| = |\frac{A^2 - B^2C}{A - B\sqrt{C}}| \ .$$

Next observe that $|A - B\sqrt{C}| \leq |A| + |B\sqrt{C}| \leq u(E_1) = u(E)$. Also $D := A^2 - B^2C$ has one root less than E and hence

$$|D| \geq \frac{u(D)}{u(D)^{2^{k-1}}}$$

by induction hypothesis, Furthermore, $u(D) = u(A^2) + u(B^2C) = u(A)^2 + u(B\sqrt{C})^2 \leq (u(A) + u(B\sqrt{C})^2 = u(E_1)^2 = u(E)^2$. Thus

$$|E_1| \geq \frac{u(D)}{u(E)u(D)^{2^{k-1}}} \geq \frac{u(E)^2}{u(E)(u(E)^2)^{2^{k-1}}} = \frac{u(E)}{u(E)^{2^k}} \ .$$

∎

Let me next sketch an alternative proof. I refer the reader to [BFMS00] for the details. E is an algebraic number. Assume $E \neq 0$. Let P be its minimal polynomial and let $\alpha_1 = E$, α_2, ... , α_n be the roots of P (also called the conjugates of α_1). Then

1. $n \leq 2^k$,
2. P has integer coefficients and lead coefficient equal to one.
3. $\alpha_i \leq u(E)$ for all i
4. $|\prod_i \alpha_i| \geq 1$. Recall that the product of the roots is equal to the quotient of the tail coefficient and the lead coefficient. In our case the lead coefficient is one and hence the product of the α_i is an integer.

Given these facts, we obtain

$$|E| \geq \frac{1}{|\prod_{i \geq 2} \alpha_i|} \geq \frac{1}{u(E)^{n-1}} = \frac{1}{u(E)^{2^k-1}} \ .$$

The nice fact about the alternative proof is that is does not only work for square roots but also for higher order roots. Then 2^k is to be replaced by the product of the orders of the roots.

I mentioned already that the theorem above is the basis for the sign test in the LEDA number class *real*. I will next discuss some basic numerical analysis which is required for the implementation.

insert material on basic numerical analysis here.

1 Extensions of Theorem 1

I discuss extensions of the basic separation bound theorem.

Divisions: How can we deal with divisions? We reduce expressions with divisions to expressions without divisions. Use the slides for the talk in Leiden. Slides 18 and 19 are the relevant ones.

Zero Test: It is conceivable that testing whether a number is zero or not is simpler than determining the sign of the number. A partial positive answer was given by Johannes Blömer [Blo98]. He considers expressions with integer operands, operators $+$, $-$, $\times$ and $\sqrt[k]{\ }$ for arbitrary integer k, but no nested roots. Thus $\sqrt{4+\sqrt{7}}$ is not allowed.

Let $\alpha = \alpha_1$ be the value of the expression and let $\alpha_2, \ldots, \alpha_n$ be its conjugates. If $\alpha = 0$, all conjugates are zero and if $\alpha_1 \neq 0$, $\prod_i |\alpha_i| \geq |\prod_i \alpha_i| \geq 1$. Also $\alpha_i \leq u(E)$ for all i. For how many i can we have $|\alpha_i| \leq 1/u(E)$? For at most half of the i. Assume otherwise. Let $L = \{i\ ;\ |\alpha_i| \leq 1/u(E)\}$ and assume $|L| > n/2$. Then

$$\prod_i |\alpha_i| < u(E)^{n/2}(1/u(E))^{n/2} = 1\ ,$$

a contradiction.

Assume now that we could generate α_i for random i. We would compute its absolute value. If $|\alpha_i| \geq 1/u(E)$, we conclude $\alpha \neq 0$. Conversely, if $\alpha \neq 0$, the probability that $|\alpha_i| < 1/u(E)$ is less than $1/2$. We therefore err with probability less than $1/2$.

How can we generate a random conjugate? The basic idea is simple, but the details are non-trivial. Assume we have only square roots. Then we can view our expression as a polynomial $E = P(\sqrt{m_1}, \ldots, \sqrt{m_k})$ with integer coefficients in roots $\sqrt{m_i}$ where the m_i are integer. Blömer showed that if the roots are independent, i.e., $gcd(m_i, m_j) = 1$ for $i \neq j$, it is easy to generate a random conjugate of E. One simply chooses a random sign for each root, i.e., $\sqrt{m_i}$ is replaced by either $+\sqrt{m_i}$ or by $-\sqrt{m_i}$ each with probability one-half. If the roots are not independent, they are made independent in a preprocessing step.

The details are left for a seminar talk. WHO IS WILLING TO GIVE THE TALK?

Diamond Operator: Discuss the diamond operator. If E_i are expressions previously computed, $1 \le i \le n$, the diamond operator $\diamond(E_n, \ldots, E_0, j)$ denotes the j-th largest real root of the polynomial $P(x) = \sum_i E_i x^i$.

Challenge: Extend LEDA reals by the diamond operator. You may restrict yourself to the special case that the E_i are integers.

I will next present some of the theory required to answer the challenge.

insert treatment of Uspenky's method and Descartes Rule of Sign.

References

[BFM$^+$01] C. Burnikel, S. Funke, K. Mehlhorn, S. Schirra, and S. Schmitt. A separation bound for real algebraic expressions. In *ESA 2001*, Lecture Notes in Computer Science, page ???, 2001. `www.mpi-sb.mpg.de/~mehlhorn/ftp/ImprovedSepBounds.ps.gz`, `http://www.mpi-sb.mpg.de/~funke/SepBound/SepBoundESA01.html`.

[BFMS00] C. Burnikel, R. Fleischer, K. Mehlhorn, and S. Schirra. A strong and easily computable separation bound for arithmetic expressions involving radicals. *Algorithmica*, 27:87–99, 2000.

[Blo98] J. Bloemer. A probabilistic zero-test for expressions involving roots of rational numbers. *Lecture Notes in Computer Science*, 1461:151–??, 1998.

[LY01] C. Li and C. Yap. A new constructive root bound for algebraic expressions. In *Proceedings of the 12th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'01)*, pages 496–505, 2001.