Circle Points and Predicates on Circle Points
Lectures on November 15 and 20

A *rational point* is a point with rational coordinates. A *rational line* is a line defined by a pair of rational points (alternatively, a line whose equation has rational coefficients). A *rational circle* is a circle whose center is a rational point and whose squared radius is a rational number.

A circle passing through three rational points is a rational circle. Is the converse also true, i.e., every rational circle contains at least three rational points? I do not know the answer.

A *circle point* is the intersection of a rational line and a rational circle.

Lemma 1 *Two rational circles intersect in circle points.*

Proof: Consider the equations of two distinct circles. Subtracting the two equations removes the quadratic terms and yields the equation of a line. ∎

We need geometric primitives for circle points. For example, we need to compare them by x-coordinate, we need to compute the orientation of three circle points, and so on.

Let us start with the simplest primitive, comparison of x-coordinates. We first derive explicit expressions for the coordinates of circle points.

Consider a circle $(x-a)^2+(y-b)^2=c$ where a, b, and c are rational numbers and a rational line $px+qy+r=0$. We assume for simplicity that $q \neq 0$. Then $y=-p/qx-r/q$. Substituting into the circle equation gives $(x-a)^2+(-p/qx-r/q-b)^2=c$. This is a quadratic equation for x. We multiply by q^2 and obtain

$$q^2(x-a)^2+(px+r+qb)^2=q^2c$$

or

$$Ax^2-2Bx+C=0$$

where

$$\begin{aligned}
A &= q^2+p^2>0 \\
B &= q^2a-rp-rpb \\
C &= q^2a^2+(r+qb)^2-q^2c\ .
\end{aligned}$$

The circle points have coordinates

$$x_{1,2}=\frac{1}{A}(B\pm\sqrt{B^2-CA})$$

Assume now that we have circles C_i and lines L_i for $i = 1, 2$. Each pair of circle and line defines two points which we denote l_1, r_1, l_2, r_2, respectively. For the definition of the l-points we take the minus-sign in the solution of our quadratic equation and for the r-points we take the plus sign. Then $(l_i + r_i)/2 = \frac{B_i}{A_i}$ and $(l_i - r_i)^2 = 4(B_i^2 - A_iC_i)$. Assume that we want to compare r_1 and l_2.

$$r_1 = \frac{1}{A_1}(B_1 + \sqrt{B_1^2 - C_1A_1}) \qquad l_2 = \frac{1}{A_2}(B_2 - \sqrt{B_2^2 - C_2A_2})$$

Here $A_i = p_i^2 + q_i^2 > 0$. We have $r_1 < l_2$ iff

$$A_2(B_1 + \sqrt{B_1^2 - C_1A_1}) < A_1(B_2 - \sqrt{B_2^2 - C_2A_2})$$

Using the abbreviation $I_i = B_i^2 - A_iC_i$ this is equivalent to

$$A_2\sqrt{I_1} + A_1\sqrt{I_2} < A_1B_2 - A_2B_1.$$

Thus $r_1 > l_2$ if $J = A_1B_2 - A_2B_1 < 0$. This condition can be interpreted geometrically. We have

$$J = A_1B_2 - A_2B_1 = A_1A_2\left(\frac{B_2}{A_2} - \frac{B_1}{A_1}\right) = A_1A_2\left(\frac{l_2 + r_2}{2} - \frac{l_1 + r_1}{2}\right),$$

i.e., $J < 0$ if the midpoint of the circle points on C_1 is right of the midpoint of the circle points on C_2. In this case r_1 is certainly right of l_2. I will continue with purely algebraic reasoning. Devillers et al. [DFMT00] showed that many of the expressions below also have geometric meaning. I am not sure whether this insight is significant or only amusing.

So assume $J > 0$. Then $r_1 < l_2$ iff

$$\begin{aligned} 2A_1A_2\sqrt{I_1I_2} &< J^2 - (A_2^2I_1 + A_1^2I_2) \\ &= A_1^2B_2^2 - 2A_1A_2B_1B_2 + A_2^2B_1^2 - A_2^2B_1^2 + A_2^2A_1C_1 - A_1^2B_2^2 + A_1^2A_2C_2 \\ &= A_1A_2(A_2C_1 + A_1C_2 - 2B_1B_2) \end{aligned}$$

iff

$$2\sqrt{I_1I_2} < A_2C_1 + A_1C_2 - 2B_1B_2.$$

Thus $r_1 > l_2$ if $K = A_2C_1 + A_1C_2 - 2B_1B_2 < 0$. So assume $K > 0$. Then $r_1 < l_2$ iff

$$4I_1I_2 < K^2 \quad \text{or} \quad K^2 - 4I_1I_2 < 0.$$

Observe that I_i is guaranteed to be non-negative. Simplification yields

$$\begin{aligned} K^2 - 4I_1I_2 &= A_2^2C_1^2 + A_1^2C_2^2 + 2A_1A_2C_1C_2 + 4B_1^2B_2^2 - 4B_1B_2A_2C_1 - 4B_1B_2A_1C_2 \\ &\quad -4B_1^2B_2^2 + 4B_1^2A_2C_2 + 4B_2^2A_1C_1 - 4A_1A_2C_1C_2 \\ &= (A_2C_1 - A_1C_2)^2 - 4(B_1A_2 - B_2A_1)(B_1C_2 - B_2C_1). \end{aligned}$$

Thus $r_1 > l_2$ if $(B_1A_2 - B_2A_1)(B_1C_2 - B_2C_1) < 0$. So assume $(B_1A_2 - B_2A_1)(B_1C_2 - B_2C_1) > 0$. Then $r_1 < l_2$ iff $(A_2C_1 - A_1C_2)^2 - 4(B_1A_2 - B_2A_1)(B_1C_2 - B_2C_1) < 0$.

WOW, this was a lot of tedious work. Can we follow the same strategy for more complex predicates? Yes, the strategy will always work (as I show below), but the details may be overwhelming. We advise to seek the use of Maple or Mathematica. In [BMS94, Bur96] the strategy was carried out for the predicates arising in the computation of Voronoi diagrams of line segments. I next want to show you that the strategy above always works.

Theorem 1 *The sign of an arbitrary expression E with integer operands and operators $+$, $-$, $\times$, and $\sqrt{\ }$ can be determined by the strategy of repeated squaring.*

Proof: We show that we can remove the roots one by one. If E contains no root its value is an integer and hence it is easy to compute its sign. So assume that E contains a root. We show how to eliminate one root. Before doing so, we give an example. Assume, we want to determine the sign of $E = \sqrt{19} + \sqrt{34} - \sqrt{20} - \sqrt{33}$. We isolate one of the roots, say $\sqrt{19}$, and obtain $E > 0$ iff $\sqrt{19} > -\sqrt{34} + \sqrt{20} + \sqrt{33}$. We use D for the expression on the right. We may assume inductively, that we know how to compute the sign of D. If $D \le 0$, we have $E > 0$. So assume $D > 0$. Then $E > 0$ iff

$$19 > D^2 = (-\sqrt{34} + \sqrt{20} + \sqrt{33})^2 = 34 + 20 + 33 + 2(\sqrt{20}\sqrt{33} - \sqrt{20}\sqrt{34} - \sqrt{33}\sqrt{34}) .$$

This is equivalent to

$$-68 > 2(+\sqrt{20}\sqrt{33} - \sqrt{20}\sqrt{34} - \sqrt{33}\sqrt{34}) .$$

I isolate another roots, say $\sqrt{20}$ and obtain the equivalent formula

$$-34 + \sqrt{33}\sqrt{34} > \sqrt{20}(\sqrt{33} - \sqrt{34}) .$$

This is of the form $A > B\sqrt{20}$. We determine the signs of A and B, which we know how to do by induction hypothesis. In our case $B < 0$ and $A < 0$. Thus our formula is equivalent to $(-A) < (-B)\sqrt{20}$. This is in turn equivalent to $A^2 < 20B^2$. Thus $E > 0$ if

$$(-34 + \sqrt{33}\sqrt{34})^2 < 20(\sqrt{33} - \sqrt{34})^2 .$$

This is equivalent to

$$1156 + 68\sqrt{33}\sqrt{34} + 33 \cdot 34 < 400(33 + 34 - 2\sqrt{33}\sqrt{34}$$

which in turn is equivalent to

$$868\sqrt{33}\sqrt{34} < 400 \cdot 67 - 1156 - 33 \cdot 34$$

One further round of squaring completes the job. Before we come to the general case, I want to stress one fact. In the derivation above, I always kept my original roots. For example, I never replaced $\sqrt{33}\sqrt{20}$ by $\sqrt{660}$. In this way I kept control over the number of distinct roots.

Assume now that our expression E contains roots. Concentrate on one of the outermost roots, i.e., a root not nested within another root, say $\sqrt{C}$. By using the distributive law we rearrange the expression into the form $A + B\sqrt{C}$. In A and $B\sqrt{C}$ we collect all terms not involving (involving) $\sqrt{C}$. The expressions A, B, and C involve one less root operation and hence, by induction hypothesis, we know how to compute their sign. If C is negative, the expression is ill-formed. If $C = 0$ or $B = 0$, the sign of E is simply the sign of A. So assume $B \neq 0$ and $C > 0$. If $A = 0$, the sign is the sign of B. So assume $A \neq 0$ and $B \neq 0$. If the signs of A and B agree, their common sign is the sign of E. If $A > 0$ and $B < 0$, the sign of E is the same as the sign of $E' = E(A - B\sqrt{C}) = A^2 - B^2C$. If $A < 0$ and $B > 0$, the sign of E is the same as the sign of $E'' = E(-A + B\sqrt{C}) = -A^2 + B^2C$. The crucial observation is now that E' and E'' contain one fewer distinct root that E.

I need to explain the latter sentence. Consider $(\sqrt{a} + \sqrt{b} + \sqrt{c} + \sqrt{d} + \sqrt{e})^2$. It seems that the result contains more roots or even new roots, e.g., $\sqrt{ab}$. The trick is to write it as $\sqrt{a}\sqrt{b}$ and then we only have the old roots. They appear more often, but that does not matter. The number of distinct roots did not increase.

We conclude that in A^2 and B^2C we only have roots that were already present before and hence E' and E'' have one fewer root than E; namely $\sqrt{C}$ disappeared. ∎

I close with a remark on complexity. If there are k distinct roots, we will go through k rounds of squaring. Squaring doubles the length of the 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. Nevertheless, it gives us a feeling for what we have to expect.

References

[BMS94] C. Burnikel, K. Mehlhorn, and S. Schirra. How to compute the Voronoi diagram of line segments: Theoretical and experimental results. In Springer, editor, *Proceedings of the 2nd Annual European Symposium on Algorithms - ESA'94*, volume 855 of *Lecture Notes in Computer Science*, pages 227–239, 1994.

[Bur96] C. Burnikel. *Exact Computation of Voronoi Diagrams and Line Segment Intersections*. PhD thesis, Max-Planck-Institut für Informatik, 1996.

[DFMT00] O. Devillers, A. Fronville, B. Mourrain, and M. Teillaud. Algebraic methods and arithmetic filtering for exact predicates on circle arcs. In *16th ACM Symposium on Computational Geometry*, pages 139–147, 2000.