Computer Science 355
Modern Computer Algebra

Assignment 5
solutions

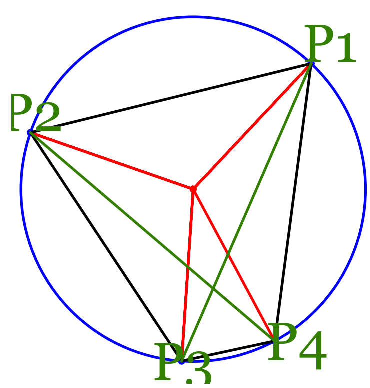
Problem 1 (Ptolemy's formula)

Statement

Let a quadrilateral be inscribed in a circle. Then the product of its two diagonals equals to the sum of the products of the two pairs of opposite sides:

P1P3 * P2P4 = P1P2 * P3P4 + P1P4 * P2P3

Prove this result by using the Gröbner bases technique.



Solution

We choose four arbitrary points in the plane

```
{p1, p2, p3, p4} = Table[{x[k], y[k]}, {k, 1, 4}];
```

Without loss of the generality, we can assume that coordinates of the circle and $x[1]$ are zeros:

```
c1 = c2 = x[1] = 0;
```

The system consists of 11 equations - two diagonals, four sides, four distances from the center to each vertex, and the equation for the product of two diagonals We use special notations for digonals and sides squared - this makes GroebnerBasis run faster (since we formallly decrease the complexity/order of the system)

```
system = {
   d1sq - (p3 - p1) . (p3 - p1),
   d2sq - (p4 - p2) . (p4 - p2),
   s1sq - (p2 - p1) . (p2 - p1),
   s2sq - (p3 - p2) . (p3 - p2),
   s3sq - (p4 - p3) . (p4 - p3),
   s4sq - (p4 - p1) . (p4 - p1),
   (-c1 + x[1])^2 + (-c2 + y[1])^2 - r^2,
   (-c1 + x[2])^2 + (-c2 + y[2])^2 - r^2,
   (-c1 + x[3])^2 + (-c2 + y[3])^2 - r^2,
   (-c1 + x[4])^2 + (-c2 + y[4])^2 - r^2,
   pdsq - d1sq d2sq
  };

gb = GroebnerBasis[system,
   {},
   {x[2], x[3], x[4], y[1], y[2], y[3], y[4], d1sq , d2sq, r},
   MonomialOrder → EliminationOrder] // Timing
```

$\{4.234, \{\mathrm{pdsq}^2 - 2\,\mathrm{pdsq}\,\mathrm{s1sq}\,\mathrm{s3sq} + \mathrm{s1sq}^2\,\mathrm{s3sq}^2 - 2\,\mathrm{pdsq}\,\mathrm{s2sq}\,\mathrm{s4sq} - 2\,\mathrm{s1sq}\,\mathrm{s2sq}\,\mathrm{s3sq}\,\mathrm{s4sq} + \mathrm{s2sq}^2\,\mathrm{s4sq}^2\}\}$

```
gb[[2, 1]] /.
 {s1sq → s1^2, s2sq → s2^2, s3sq → s3^2, s4sq → s4^2, pdsq → pd^2}
```

$\mathrm{pd}^4 - 2\,\mathrm{pd}^2\,\mathrm{s1}^2\,\mathrm{s3}^2 + \mathrm{s1}^4\,\mathrm{s3}^4 - 2\,\mathrm{pd}^2\,\mathrm{s2}^2\,\mathrm{s4}^2 - 2\,\mathrm{s1}^2\,\mathrm{s2}^2\,\mathrm{s3}^2\,\mathrm{s4}^2 + \mathrm{s2}^4\,\mathrm{s4}^4$

```
Factor[%]
```

$(\mathrm{pd} - \mathrm{s1}\,\mathrm{s3} - \mathrm{s2}\,\mathrm{s4})\,(\mathrm{pd} + \mathrm{s1}\,\mathrm{s3} - \mathrm{s2}\,\mathrm{s4})\,(\mathrm{pd} - \mathrm{s1}\,\mathrm{s3} + \mathrm{s2}\,\mathrm{s4})\,(\mathrm{pd} + \mathrm{s1}\,\mathrm{s3} + \mathrm{s2}\,\mathrm{s4})$

The first factor yeilds

$$d1\ d2 = s1\ s3 + s2\ s4$$

This completes the computational proof, though you have to explain the other factors.

Problem 2

Given a square marix $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$, find another square matrix B, such that $A = B * B$.

In analogy to the square root of a number, this matrix B is called the square root of the matrix A. You have to find all squre roots of A. Hint, use Groebner basis technique.

■ Computational Proof.

```
A = {{1, 0, 1}, {0, 1, 0}, {1, 0, 1}};
B = Array[b, {3, 3}];
gb = GroebnerBasis[Flatten[A - B.B], Flatten[B]];
sols = Solve[# == 0 & /@ gb, Flatten[B]] // Union
```

Problem 3

Prove this identity using the Gröbner bases technique.

$$\frac{\sin(2\pi/7)}{\sin^2(3\pi/7)} - \frac{\sin(\pi/7)}{\sin^2(2\pi/7)} + \frac{\sin(3\pi/7)}{\sin^2(\pi/7)} = \sqrt{28}$$

```
eqns = {s2^3 s1^2 - s1^3 s3^2 + s3^3 s2^2 - s1^2 s2^2 s3^2 r, 2 s1 c1 - s2, c1^2 - s1^2 - c2,
  s1 c2 + s2 c1 - s3, c1 c2 - s1 s2 - c3, s1^2 + c1^2 - 1, 1 - 4 c1 - 4 c1^2 + 8 c1^3}
```

$$\{-r\, s1^2\, s2^2\, s3^2 + s1^3\,(-s3^2) + s1^2\, s2^3 + s2^2\, s3^3,\ 2\, c1\, s1 - s2,\ c1^2 - c2 - s1^2,$$
$$c1\, s2 + c2\, s1 - s3,\ c1\, c2 - c3 - s1\, s2,\ c1^2 + s1^2 - 1,\ 8\, c1^3 - 4\, c1^2 - 4\, c1 + 1\}$$

The first equation comes from the problem, the next four equations are identities for sums of sines and cosines, the next equation is an identity of sine and cosine, and the last equation was derived in lecture when finding the value of Cos[Pi/7].

```
GroebnerBasis[eqns, {r}, {c1, c2, c3, s1, s2, s3}]
```

$$\{r^2 - 28\}$$

Problem 4

Given Boolean variables X_i and a number of Boolean clauses each with three literals, i.e., clauses of the form

$$Y_j \bigvee Y_k \bigvee Y_i, \qquad (Y_j, Y_k, Y_i) \in \{X_1, \ldots, X_n, \neg X_1, \ldots, \neg X_n\},$$

3-SAT is the problem of deciding whether there exists a Boolean assignment to the X_i's that makes all the clauses true simultaneously. Describe how you would solve 3-SAT problem using the Gröbner Bases.

Given an instance of 3-SAT we reduce it to a system of equations. If the Gröbner Basis is <1>, then the 3- SAT instance is not solvable. For each clause we create a polynomial that is zero if and only if the clause is satisfiable. For a clause $Y_j \bigvee Y_k \bigvee Y_i$, we map each literal to a term, and then form a polynomial for that clause using the following correspondence

$$Y_k \to x_k, \ \neg Y_k \to 1 - x_k, \ Y_j \bigvee Y_k \to x_j + x_k - x_j x_k$$

We also add the equations $x_k(1 - x_k) = 0$.

The Gröbner Basis for this ideal will be nontrivial if there exists some soution to all of these polynomials which means the 3-SAT instance is satisfiable. Solving the system would give the truth assignment of the variables.