Preliminary Tutorial 6

John Abbott

September 29, 2017

Red Question

Use CoCoA to compute approximations to within $\epsilon = 10^{-20}$ to each of the real roots of the polynomial $f = x^5 - 5x^4 - 3x^3 + 4x^2 - x + 1$. Print out the appoximate roots as decimal numbers. Verify that evaluating f at each of the approximate roots produces values close to zero.

Now repeat the exercise for the **Mignotte polynomial**: $g = x^{16} - (1000000x - 1)^2$. This polynomial has two real roots which are close to one another. Compute a good approximation to the *distance between these two roots*.

Useful CoCoA manual pages: `RealRootsApprox`, `FloatStr`, `eval`, `subst`.

Green Question

A positive integer p is a **Sophie Germain prime** if both p and $2p+1$ are prime. Write a CoCoA function called `IsSGPrime` which takes one (integer) argument `P`, and returns true if `P` is a Sophie Germain prime, otherwise it returns false.

Compute a list of all the Sophie Germain primes up to 1000.

A positive integer p is a **Twin Prime** if both p and $p+2$ are prime. Write a CoCoA function called `IsTwinPrime` which takes one (integer) argument `P`, and returns true if `P` is a twin prime, otherwise it returns false.

Compute a list of all numbers (from 1 to 1000) which are both Sophie Germain primes and twin primes.

Useful CoCoA manual entries: `IsPrime`, `define` and `list constructors`.

Blue Question

Use the CoCoA function `GroebnerFanIdeals` to compute all the different reduced Gröbner bases of the ideal $I = \langle x^2z + yz^2 + 1,\ x^3 + y^3,\ z^3 - y^2 \rangle$

How many different reduced Gröbner bases are there?

Find a term-ordering for which the reduced Gröbner basis of I contains just 3 elements. Remember that, in general, term orderings can be described by matrices (of integers); only very few term orderings have specific names.

Other useful CoCoA manual entries: `RingOf`, `OrdMat` and `list constructors`.

Yellow Question

In each of the following cases determine which of these three relations holds $A < B$ or $A > B$ or $A = B$.

case (α) $A = \sqrt{86} + \sqrt{990}$ $\qquad\qquad$ $B = \sqrt{165} + \sqrt{778}$

case (β) $A = \sqrt{176} + \sqrt{195} + \sqrt{2025}$ $\quad B = \sqrt{190} + \sqrt{398} + \sqrt{1482}$

case (γ) $A = \sqrt{17} + \sqrt{833} + \sqrt{2873} + \sqrt{9261}$ $\quad B = \sqrt{189} + \sqrt{1029} + \sqrt{2541} + \sqrt{7497}$

Hints:

- One possibility could be to compute approximations to the square roots, and then just evaluate the formulas. But how much precision do you need to be sure of getting the right answer? See the CoCoA manual page for `RealRootsApprox`.
- There is a more algebraic solution technique. Create a polynomial ring with one indeterminate for each square-root. Define an ideal with the minimial polynomials for each indeterminate: *e.g.* $I = \langle A^2 - 86, B^2 - 990, C^2 - 165, D^2 - 778\rangle$. This ideal will be useful for "reducing" expressions. Regroup the sums into two parts (say, LHS and RHS) so that all multiples of one of the square-roots are in LHS, and everything else is in RHS. Now square both LHS and RHS, and repeat the process until no square-roots are left. Useful CoCoA manual pages: `NF` and `NR`.

White Question

There are 4 distinct pythagorean triples with hypotenuse 65. Use CoCoA to find them.

Using the obvious reflections and rotations, produce 32 distinct points in the plane with integer coordinates all lying on the circle of radius 65. Compute I, the ideal of polynomials vanishing at these points.

The reduced (`DegRevLex`) Gröbner basis of I contains two polynomials: one is obviously $x^2 + y^2 - 65^2$. The other polynomial is reducible; what are its factors?

There are 40 distinct pythagorean triples with hypotenuse 32045. Use CoCoA to find them, and then repeat the steps above using these triples. Is there a quicker way to get the answer?

Useful CoCoA manual pages: `for`, `foreach`, `append`, `IdealOfPoints`, `factor`

Black Question

You have a rectangular box of size 37-by-47, and a rectangular bar of chocolate of size 5-by-55. Can you fit the bar into the box?

Try also these cases:

- Box: 57-by-77 Bar: 4-by-92
- Box: 54-by-59 Bar: 4-by-76
- Box: 25-by-32 Bar: 7-by-34

Hints:

- Useful CoCoA manual pages: `ideal`, `elim`, `MinPolyQuot`
- Given a box of size A-by-B, and a bar of size C-by-D, use Groebner bases to find the longest bar of width C which fits into a box A-by-B. If the longest bar has length greater than D then the bar fits, otherwise it does not.

- Here is an approach using coordinate geometry. Place the box with one corner at $(0,0)$ and the opposite corner at (A,B). The maximal length bar will touch the box at 4 points $P_1 = (x,0)$, $P_2 = (0,y)$, $P_3 = (A, B-y)$ and $P_4 = (A-x, B)$. We know the distance between P_1 and P_2. We know that the angle $P_1-P_2-P_4$ is a right-angle. The value we seek is the distance between P_1 and P_3 (or equivalently between P_2 and P_4). Use a new indeterminate L to represent this length, then compute the minimal polynomial of L (*e.g.* via elimination). Check that the minimal polynomial has a real root in the range 0 to $\sqrt{A^2+B^2}$; if so, this is the maximal length.

Pink Question

An ideal in a polynomial ring which can be generated by monomials is called a **monomial ideal**. We shall assume that all our ideals are *explicitly* monomial, *i.e.* the generators which we have are actually monomials. Such ideals enjoy a number of nice combinatorial properties; also, the *leading term ideal* of a general polynomial ideal captures several interesting proprties of the general ideal.

An ideal I is monomial iff for every polynomial $f \in I$ each term in $\mathrm{supp}(f)$ is in I, where $\mathrm{supp}(f)$ is just the set of terms in f. (Prove this.)

Let $I = \langle t_1, \ldots, t_s \rangle$ be an explicitly monomial ideal. Then for any term t we have $t \in I$ iff there is an index j such that $t_j \mid t$. (Prove this.)

Devise an algorithm to determine a **minimal set of generators** of a monomial ideal: given a set of terms $\{t_1, \ldots, t_s\}$, the algorithm finds a minimal subset which generates the same ideal. Is the minimal subset unique?

It is a standard result that the intersection of two ideals is an ideal; show that the intersection of two monomial ideals is a monomial ideal. Devise an algorithm to compute a (minimal?) set of generators for the intersection of two monomial ideals. What result does it produce if you intersect a monomial ideal with itself?

Let I be an ideal, then the **radical** of I is $\sqrt{I} = \{f \in P \mid f^n \in I \text{ for some } n \in \mathbb{N}\}$. It is a standard result that the radical is also an ideal. Prove that the radical of a monomial ideal is again a monomial ideal. Devise an algorithm to compute the radical of a monomial ideal.

Implement your algorithms in CoCoA, and run them on some test cases. Here are some monomial ideals: $\langle x \rangle$, $\langle x^2y, yz^2 \rangle$, $\langle x^2y, xy^2 \rangle$, $\langle x^3y^2, x^2y^3, x^2, y^2 \rangle$, $\langle x^2y, yz^2, x^3, y^4, z^5 \rangle$.

Orange Question

The CoCoA function `NumTerms` counts how many terms a polynomial has. We say that a polynomial f is **dense** if $\mathrm{NumTerms}(f) = 1+\deg(f)$. For example, $\mathrm{NumTerms}(x^9-1) = 2$, and $\mathrm{NumTerms}(x^3+2x^2+3x+4) = 4$.

Find a dense monic polynomial, f, of degree 4 such that $\mathrm{NumTerms}(f^2) = \mathrm{NumTerms}(f)$. Since f is dense of degree 4 it necessarily has 5 terms.

Let k be a positive integer, and define $g(x) = f(x)\, f(x^k)$. Show that there is at least one value of k for which $\mathrm{NumTerms}(g^2) < \mathrm{NumTerms}(g)$. Use CoCoA to find which values of k give the smallest ratio $\mathrm{NumTerms}(g^2)/\,\mathrm{NumTerms}(g)$.

A similar argument shows that there exists a positive integer k_2 such that the ratio $\mathrm{NumTerms}(h^2)/\,\mathrm{NumTerms}(h)$ is smaller than $\mathrm{NumTerms}(g^2)/\,\mathrm{NumTerms}(g)$ where $h(x) = g(x)\, g(x^{k_2})$. Use CoCoA to find which values of k_2 give the smallest ratio for $\mathrm{NumTerms}(h^2)/\,\mathrm{NumTerms}(h)$.

We can also find dense palindromic polynomials with sparse squares. We say that a polynomial f is **palindromic** if $f(x) = x^{\deg(f)} f(\frac{1}{x})$. Find a dense palindromic monic polynomial F of degree 6 such that $\mathrm{NumTerms}(F^2) = \mathrm{NumTerms}(F)$.

Prove that for any positive integer k the polynomial $G(x) = F(x)\,F(x^k)$ is palindromic. Find a palindromic polynomial G such that $\text{NumTerms}(G^2) < \text{NumTerms}(G)$.

Hints:

- Useful CoCoA manual pages: `CoeffListWRT`, `subsets`, `foreach`, `ReducedGbasis`
- Use a CoCoA ring like `QQ[x,a[0..3]]`, then a generic monic dense polynomial of degree 4 is `x^4+a[3]*x^3+a[2]*x^2+a[1]*x+a[0]`.
- For the palindromic polynomial the coefficients are not rational.

Violet Question

Write a CoCoA function `NaturalLog(X, N)` where `X` is a positive rational number, and `N` is a positive integer; the function should return a rational number L such that $|L - \ln(X)| < 2^{-N}$.

Hints:

- Useful CoCoA manual pages: `FloorSqrt`, `FloorLog2`
- Find a power of 2 such that $1 \leq 2^{-k}X < 2$. Compute $\ln(2)$ to sufficient precision. Compute $\ln(2^{-k}X)$ to sufficient precision. Return $k\ln(2) + \ln(2^{-k}X)$.
- Recall that $\ln(1+x) = x - x^2/2 + x^3/3 - \cdots$ valid for $|x| < 1$.
- Using the power series to compute $\ln(1+x)$ accurately needs many terms unless x is close to zero. We can use $\ln(1+x) = 2\ln(\sqrt{1+x}) = 4\ln(\sqrt[4]{1+x}) = \cdots$ We need the value $\sqrt{1+x}$ only approximately, and this can be found multiplying by a power of 2 and then using `FloorSqrt`.

Brown Question

Below you will find a CoCoA function to compute the GCD of two univariate polynomials using Euclid's algorithm. It also prints out the leading monomial of each successive remainder. Try using this function to compute the GCD of some pairs of polynomials. Observe that the leading coefficients can quickly become much more complicated than the coefficients of the original polynomials.

Use a modular approach to compute the GCD of the following polynomials: you can use CoCoA's own GCD function of compute the GCDs of polynomials with coefficients in a finite field.

Useful CoCoA Manual pages: `NewRingFp`, `CRTPoly`, `RatReconstructPoly`

```
define euclid(f,g)
  // First deal with the trivial cases
  if f=0 then return g; endif;
  if g=0 then return f; endif;
  if deg(f) = 0 then return f; endif;
  if deg(g) = 0 then return g; endif;
  if deg(f) < deg(g) then swap(ref f, ref g); endif;
  // Now deg(f) >= deg(g) >= 1, so enter general loop.
  P := RingOf(f);
  coeff := CoeffEmbeddingHom(P);
  x := indet(P, UnivariateIndetIndex(f));
  while g <> 0 do
```

```
    while f <> 0 and deg(f) >= deg(g) do
      delta := deg(f) - deg(g);
      f := f - coeff(LC(f)/LC(g)) * x^delta * g;
    endwhile;
    if f <> 0 then println "LM(rem) = ", LM(f); endif;
    swap(ref f, ref g);
  endwhile;
  return f;
enddefine; -- euclid


f1 := sum([random(-99,99)*x^k | k in 0..10]);
f2 := sum([random(-99,99)*x^k | k in 0..10]);
g := sum([random(-99,99)*x^k | k in 0..2]);

euclid(f1*g, f2*g);
-- The answer looks wrong: it should be just g.
factor(It); -- it is just g, but multiplied by an "ugly" scalar.
```