MATH 895, Course Project, Summer 2017
Computing with Black Boxes

Instructor: Michael Monagan
The project is worth 40% of your final grade. Due August 15th.

Let $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ be represented by a black box **B** such that given a prime p and an evaluation point $\alpha \in \mathbb{Z}_p^n$ $\mathbf{B}(\alpha, p)$ outputs $f(\alpha)$ mod p. The goal of this project is to design collection of operations on black boxes and implement them in Maple.

1. **evalBB**(B,α,p) outputs $f(\alpha)$ mod p.

2. **isBBzero**(B,D,ϵ) tests if B is the 0 polynomial. The input D is a total degree bound. Base this routine on the Schwartz-Zippel lemma. Design your routine so that if $f \neq 0$ then the probability that **isBBzero** outputs true is $< \epsilon$. Test your routine for $\epsilon = 10^{-50}$.

3. **degBB**(B,D) outputs $\deg f$ the total degree of f.
   degBB(B,i,D) outputs $\deg_{x_i} f$ the degree of f in x_i.
   If $f = 0$ then output -1.

4. **suppBB**(B,D,T) outputs the support of f i.e. the set of monomials of f.
   Here D is a total degree bound and T is a term bound on $\#f$.

5. **sintBB**(B,D,T,H) outputs the polynomial f i.e. interpolates f from the black box.
   Here H is a height bound i.e., $H \geq ||f||_\infty$.

Notes

- You will need a representation for a black box. And you will need a realistic application. For the application create an $m \times m$ matrix A of polynomials in $\mathbb{Z}[x_1, ..., x_n]$ that has a sparse determinant and let the black box be the pair $[A, [x_1, \ldots, x_n]]$. Program **evalBB** to compute $\det(A(\alpha_1, \ldots, \alpha_n))$ mod p.

- For the procedure **suppBB** use the Ben-Or/Tiwari sparse interpolation modulo a single p chosen randomly. Code two versions; for the first version use evaluation points $(2^i, 3^i, 5^i, \ldots, p_n^i)$ for $0 \leq i < 2T$. For the second pick a prime of the form

$$p = q_1 q_2 \ldots q_n + 1 \text{ with } \gcd(q_i, q_j) = 1 \text{ and } q_i > D.$$

  Use the evaluation points $(\omega_1^i, \omega_2^i, \ldots, \omega_n^i)$ for $0 \leq i < 2T$ where ω_i has order q_i mod p.

- For computing the $\lambda(z)$ polynomial use the Berlekamp-Massey algorithm (see website). This algorithm (as coded) does $O(T^2)$ arithmetic operations instead of $O(T^3)$.
- For computing discrete logarithms use Maple's `numtheory[mlog]` procedure.
- For the procedure **sint** you need to first determine the support of f then solve for the coefficients of f. Use additional primes and Chinese remaindering to determine the coefficients. Solve the transposed Vandermonde systems mod p_i using the $O(t^2)$ method.

What to hand in?

To present your work you may either write a report in LaTeX or create a poster for presentation at this years *Symposium on Mathematics and Computation* here at SFU on Tuesday August 15th. See

`https://www.sfu.ca/math/Events_and_News/ongoing_events/MathSymposium.html`

The main event at this meeting is the poster session where students in our department, both undergraduate and graduate, present their work. You may use my LaTeX poster on the course website as an outline. I will pay for the cost of printing your poster and the registration fee to attend the symposium. Submit also a printout of a Maple worksheet and Maple code that demonstrates that the codes are working correctly.

If you choose to write a report, it should be about 10 pages (11pt font). Submit also a printout of a Maple worksheet and Maple code that demonstrates that the codes are working correctly. The report (and poster) should introduce the black box model, describe the algorithms using pseudo-code, state and prove the probability that the output is correct, and state the arithmetic cost of each algorithm.

References

These papers/documents are on the website.
A Deterministic Algorithm for Interpolating Sparse Multivariate Polynomials by Ben-Or and Tiwari.
A Fast Parallel Sparse Polynomial GCD Algorithm.by Hu and Monagan.
Maple code for the Berlekamp-Massey algorithm.