MATH 895, Assignment 7, Fall 2023

Instructor: Michael Monagan

Please hand in the assignment by 11:00pm Monday December 4th.
Late Penalty -20% off for up to 24 hours late, zero after than.
For Maple problems, please submit a printout of a Maple worksheet containing your Maple code and Maple output.

Question 1: The Schwartz-Zippel Lemma [6 marks]

Let D be an integral domain and S be a finite subset of D. Let $f \in D[x_1, \ldots, x_n]$ be non-zero. The Schwartz-Zippel Lemma says if α is chosen at random from S^n then

$$\Pr[f(\alpha) = 0] \leq \frac{\deg f}{|S|}.$$

Let p be a large prime. Let $f \in \mathbb{Z}_p[x, y]$ be non-zero of total degree d. If we pick $\alpha \in \mathbb{Z}_p^2$ at random, the Schwartz-Zippel Lemma says the probability $f(\alpha) = 0 \leq d/p$. Equivalently, f can have at most dp roots. Find a polynomial $f \in \mathbb{Z}_p[x, y]$ of total degree d that has dp roots. Conclude that the Schwartz-Zippel Lemma is tight.

Question 2: Black Boxes [12 marks]

Construct a modular black box $B : (\mathbb{Z}_p^n, p) \rightarrow \mathbb{Z}_p$ as a Maple procedure for evaluating the polynomial $f = \det(V_4) \in \mathbb{Z}[x_1, x_2, x_3, x_4]$ where where V_4 is the 4 by 4 Vandermonde matrix

$$V_4 = \begin{bmatrix} 1 & x_1 & x_1^2 & x_1^3 \\ 1 & x_2 & x_2^2 & x_2^3 \\ 1 & x_3 & x_3^2 & x_3^3 \\ 1 & x_4 & x_4^2 & x_4^3 \end{bmatrix}$$

So for $\alpha \in \mathbb{Z}^4$, $B(\alpha, p)$ should output $f(\alpha) \bmod p$. Now implement Algorithm GetDegree and the algorithm for computing $\deg(f)$, the total degree of f for $p = 2^{62} + 135$. To get random values from $[0, p)$ you can use

```
> p := 2^62+135;
> R := rand(0..p-1):
> R(), R(); # two random values
```

$$2342493223442167775, 2441597211547797803$$

Test your algorithm on the black-box for $f = \det(V_4)$.
Repeat this experiment for T_4 the symmetric 4 by 4 Toeplitz matrix.

Question 3: Sparse Interpolation Algorithms [12 marks]

(a) Apply Ben-Or/Tiwari sparse interpolation to interpolate

$$f(w,x,y,u) = 101w^5x^3y^2u + 103w^3xy^3u^2 + 107w^2x^5y^2 + 109x^2y^3u^5$$

over $\mathbb{Q}$ using Maple. You will need to compute the integer roots of the $\lambda(z)$ polynomial and solve a linear system over $\mathbb{Q}$.

Now it is very inefficient to run the algorithm over $\mathbb{Q}$. Repeat the method modulo a prime p, i.e., interpolate f modulo p. Assume you know that $\deg f < 16$. Pick p suitably large so that you can recover all monomials of total degree $d \leq 15$. See the `Roots(...) mod p` and `Linsolve(...) mod p` commands.

(b) The Ben-Or/Tiwari sparse interpolation algorithm interpolates a polynomial $f(x_1, x_2, \ldots, x_n)$ in two main steps. First it determines the monomials then it solves a linear system for the unknown coefficients of the polynomial. Let

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{t} a_i M_i$$

where a_i are the coefficients and M_i are the monomials. Let $a = [a_1, a_2, \ldots, a_t]$ be the vector of unknown coefficients. Let $v = [v_0, v_1, \ldots, v_{t-1}]$ be the vector of values where $v_j = f(2^j, 3^j, 5^j, \ldots, p_n^j)$. Let $m_i = M_i(2, 3, 5, \ldots, p_n)$ be the value of the monomial M_i. The linear system to be solved is $V^T a = v$ where

$$V^T = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ m_1 & m_2 & m_3 & \ldots & m_t \\ m_1^2 & m_2^2 & m_3^2 & \ldots & m_t^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ m_1^{t-1} & m_2^{t-1} & m_3^{t-1} & \ldots & m_t^{t-1} \end{bmatrix}$$

is a transposed Vandermonde matrix. Use Maple to solve this linear system for the problem in part (a) using Zippel's the $O(t^2)$ method.