MACM 401 / MATH 801 Bonus Assignment

Michael Monagan

This bonus assignment worth up to 50% of any assignment that you did poorly on. I will add the mark you get on this assignment to your worst assignment mark up to a maximum of 100%.

Due Monday April 8th at 4pm. Hand in to dropoff box 1a outside AQ 4100. No late bonus assignments will be accepted.

Question 1: Modular Algorithms

Let $a, b \in \mathbb{Z}[x, y]$. We will design a modular algorithm to multiply $c = a \times b$ and compare the cost of the modular algorithm with the classical multiplication algorithm. A general Homomorphism diagram describing the algorithm is attached. The modular algorithm will pick primes $p_1, p_2, \ldots$, multiply $a \times b \mod p_i$ then use Chinese remaindering to recover the integers in the product c. For each prime $p \in \{p_1, p_2, \ldots\}$, it will first evaluate x at integers mod p, then evaluated y at integers mod p then multiply integers modulo p then interpolate y then interpolate x.

(a) 8 marks

Write a Maple procedure `Multiply(a,b,x,y);` that multiplies $a \times b$ using a modular algorithm. Use primes $10007, 10009, 10037, \ldots$, that is, use primes $> 10^4$. Use evaluation points $x = 1, 2, 3, \ldots$ and $y = 1, 2, 3, \ldots$. Test your algorithm on the following inputs

```
> r := rand(-10^6..10^6):
> a := randpoly( [x,y], degree=3, coeffs=r, dense ):
> b := randpoly( [x,y], degree=3, coeffs=r, dense ):
> c := Multiply(a,b,x,y):
> c-expand(a*b); # should be zero
> dx := 10;
> dy := 20;
> r := rand(-10^20..10^20):
> C := proc(y,d) randpoly(y,degree=d,dense,coeffs=r) end:
> a := add( C(y,dy)*x^i, i=0..dx ):
> b := add( C(y,dy)*x^i, i=0..dx ):
> c := Multiply(a,b,x,y):
> c-expand(a*b); # should be zero
```

(b) 12 marks

Assume $\deg(a, x) \leq dx$, $\deg(b, x) \leq dx$, $\deg(a, y) \leq dy$, and $\deg(b, y) \leq dy$. Assume the integers coefficients of a and b are bounded by B^m in magnitude for some constant B. For simplicity, assume the primes p_i satisfy $B < p_i < 2B$.

If we multiply $a \times b$ using classical $O(m^2)$ integer multiplication and we multiply the polynomials using classical quadratic polynomial multiplication, what is the cost of this algorithm? Express your answer in the form $O(f(m, dx, dy))$.

Now, what is the cost of your modular multiplication algorithm? There will be several components; the modular reductions ϕ_{p_i}, evaluation of x and y, polynomial multiplications in $\mathbb{Z}_{p_i}[x]$, interpolating x and y, and Chinese remaindering.

Question 2: Factoring modulo p

Let p be a large prime and g be a product of d linear factors in $\mathbb{Z}_p[x]$. The factorization algorithm we've been studying splits g into two factors by picking a random integer α from $0 \le \alpha < p$ and computing

$$h = \gcd((x+\alpha)^{(p-1)/2} - 1, g) = \gcd([(x+\alpha)^{(p-1)/2} \mod g] - 1, g)$$

This splits g into two factors h and g/h in $\mathbb{Z}_p[x]$. If d is large, say $d = 100$, we expect h to have degree near 50. But it won't always be exactly 50. We would like to do an experiment to see the distribution of the degrees of h for different α.

(a) (14 marks)

Use $p = 2^{30} - 35 = 1073741789$ and $d = 100$.
Construct $g(x) = \prod_{i=1}^{d}(x - \beta_i)$ for 100 distinct $\beta_i \in \mathbb{Z}_p$.

Compute $\deg h$ for $N = 10,000$ randomly chosen α's. Let f_i be the number of α's for which $\deg h = i$. Print the values of f_i that you get for $20 \le i \le 80$.

To compute $(x+\alpha)^{\frac{p-1}{2}} \mod g$ in $\mathbb{Z}_p[x]$ use the Maple's Powmod command

```
> Powmod(x+alpha,(p-1)/2,g,x) mod p;
```

To generate a random $\alpha \in [0, p)$ in Maple use

```
> R := rand(p);
> alpha := R();
```

(b) (6 marks)

Let $w = (x+\alpha)^{\frac{p-1}{2}} - 1$ and let $h = \gcd(w, g)$ and $X = \deg h$. So X is the number of linear factors of g which are also linear factors of w.

If we assume that the probability that each linear factor of g is a linear factor of $w(x)$ is 0.5, then X will follow a binomial distribution $B(n, p)$ with parameters $n = d$ and $p = 0.5$. See Wikipedia for information about the binomial distribution.

Determine the probability that $X = 50$ for $n = 100$ and $p = 0.5$.
Calculate the standard deviation σ of X for $n = 100$ and $p = 0.5$.
Recall that σ is the square root of the variance.

Now for $N = 10,000$ trials compute the expected values for the f_i for $20 \le i \le 80$. Compare these with the actual values of f_i obtained from part (a). Use Maple for calculations.

Note, the binomial coefficient $\binom{6}{3}$ in Maple is

```
> binomial(6,3);
```

HOMOMORPHISM DIAGRAM

General strategy

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\text{Input } a \in \mathbb{Z}[x][y] \arrow[r, "\text{Compute solution}", "\text{in } \mathbb{Z}[x][y]"'] \arrow[d, "\phi_{p_i}"', "{i=1..n}", "{\prod p_i > \underline{2\|u\|_\infty}}"] & \text{Output } u \in \mathbb{Z}[x][y] \\
\bar{a}_i \in \mathbb{Z}_{p_i}[x][y] \arrow[r, "\text{Compute solution}", "\text{in } \mathbb{Z}_{p_i}[x][y]"'] \arrow[d, "\phi_{x=\alpha_j}"', "{j=1..m > \deg(u,x)}"] & u_i \in \mathbb{Z}_{p_i}[x][y] \arrow[u, "\text{Apply}", "{?\ \text{CRT } u_i}"'] \\
\tilde{a}_{ij} \in \mathbb{Z}_{p_i}[y] \arrow[r, "\text{Compute solution}", "\text{in } \mathbb{Z}_{p_i}[y]"'] \arrow[d, "\phi_{y=\beta_k}"', "{k=1..\ell > \deg(u,y)}"] & u_{ij} \in \mathbb{Z}_{p_i}[y] \arrow[u, "\forall i", "{?\ \text{Interpolate } x \ (\alpha_j, u_{ij})}"'] \\
\bar{a}_{ijk} \in \mathbb{Z}_{p_i} \arrow[r, "\text{Compute solution in}", "\mathbb{Z}_{p_i}"'] & u_{ijk} \in \mathbb{Z}_{p_i} \arrow[u, "{\forall i,j}", "{\text{Interpolate } y \ (\beta_k, u_{ijk})}"']
\end{tikzcd}
$$