Computational Algebra: Lecture 7

Manuel Leclo.

Exercise: Prove that the cost of a single iteration of steps 4 through 6 in the modular bivariate gcd algorithm given in class for polynomials $f, g \in F[x,y] = R[x]$ with $R = F[y]$, F field is no more than $O(m^2 d^2)$ operations in F.

Theorem: Given $f, g \in F[x]$ with $\deg f = n$, $\deg g = m$, the Extended Euclid algorithm has a complexity bound of $O(nm)$ operations in F.

4: First of all, step 4 consists in computing $\bar{f} \leftarrow f \bmod p$ and $\bar{g} \leftarrow g \bmod p$. However, the degrees of f and g are bounded by d with respect to y, and $p \in R[y]$ is chosen to have degree greater than d, so both modular computations do not take any operation in F.
Secondly, this step consists in calling the Extended euclid algorithm over $R/\langle p \rangle$ (Recall $R = F[y]$). Recall that degree of f, g with respect to x is bounded by m, and so by theorem above, the number of operations over $R/\langle p \rangle$ is going to be bounded by $O(m^2)$. Moreover, each of those well operations (additions, multiplications, inversions) is going to be bounded by $\deg p > d \geq \deg_y f$, and so taking at most $O((\deg p)^2)$ operations in F.
Therefore, we can conclude that step 4 performs at most $O(m^2 (\deg p)^2)$. In fact, $O(m^2 d^2)$ since $\deg p = d + 1 + \deg b \leq 2d+1$.

5 In this step, we have to compute $w, f^*, g^* \in R[x]$ of degrees in y less $\deg_y p$ satisfying $w \equiv br \bmod p$, $f^* w \equiv bf \bmod p$, $g^* w \equiv bg \bmod p$. Hence, the latter implies 3 multiplications and 2 modular divisions (divisions with remainder), therefore $O(m^2)$ operations modulo p. As we argued before, each of those operation having a cost in terms of arithmetic operations in F bounded by $O(\deg p^2) = O(d^2)$ and so we conclude with step 5 having cost of $O(m^2 d^2)$

6 In step 6 we check that $\deg_y(f^* w) = \deg_y(bf)$ and $\deg_y(g^* w) = \deg_y(bg)$. Depending on the implementation this can be an instant check $O(1)$. However, at most $O(d)$ (going through all monomials until finding the max de

Total cost: By 4, 5 and 6, we conclude with $O(m^2 d^2)$. ☒