

## HOMEWORK 2

Due: 20.03

### 1 Hermite Interpolation

For  $i \in \{1, \dots, n\}$ , let  $(x_i, y_i, z_i) \in \mathbb{K}^3$  with  $x_i$  pairwise distinct. An Hermite interpolating polynomial for  $(x_i, y_i, z_i)$  is a polynomial  $P$  of degree  $\leq 2n - 1$  such that  $P(x_i) = y_i$  and  $P'(x_i) = z_i$ .

1. Show that such a  $P$  exists and is unique.
2. Use the exercise about fast CRT (TD4) to give a quasi-linear time algorithm to find  $P$  (Hint: try to express the constraints  $P(x_i) = y_i$  and  $P'(x_i) = z_i$  as a unique constraint of the form  $P \equiv Q_i \pmod{(X - x_i)^2}$  for some polynomial  $Q_i$  of degree 1).
3. Can you state a generalization to higher order derivatives? With a different order at each point?

### 2 Hensel-type strategy for solving linear system

In this exercise, we study algorithms to solve  $Mx = b$ ,  $M \in \mathcal{M}_n(K[X])$ ,  $b \in K[X]^n$ . We shall assume that the degree of all coordinates of  $M, b$  is  $\leq d$ .

Cramer's formulas show that if  $x$  is a solution to  $Mx = b$ ,  $(\det M) \cdot x \in K[X]^n$ , and the coefficients of  $(\det M) \cdot x$  have degree  $\leq nd$ . We'll also assume that  $\det M(u) \neq 0$  for all  $u \in K$ .

1. What is the complexity of computing  $B := (M \bmod X)^{-1}$ ?  
Let  $y_i \in K[X]^n$  be a solution of  $My_i = b \bmod X^i$ , and define  $r_i = b - My_i$ .
2. Prove that  $r_i = \lambda_i X^i$  for some  $\lambda_i \in K[X]^n$ . If  $z_i = B\lambda_i \bmod X$ , prove that  $y_{i+1} = y_i + X^i z_i$  and  $r_{i+1} = r_i - X^i M z_i$ .
3. What is the complexity of computing  $y_{nd+1}$  using this method? Assuming that  $\det M$  is given as input or precomputed, deduce an algorithm for solving  $Mx = b$ .
4. If we need to compute  $\det M$  beforehand, then this computation is going to dominate the complexity of linear system solving. Can we avoid computing the determinant? (Hint: use rational reconstruction.)