TD 10 : Codes de Reed-Solomon

Exercice 1. *Distance d'un code de Reed-Solomon*

✎ Montrer que la distance d'un code de Reed-Solomon $[n, k]_q$ est exactement $n - k + 1$.

Exercice 2. *Évaluation des dérivées*

Soit k un corps infini et $P \in k[x]$ un polynôme de degré d. On note $\mathsf{M}(d)$ la complexité arithmétique de la multiplication de polynômes de degré au plus d.

1. Décrire et analyser un algorithme d'évaluation d'un polynôme P en un point $a \in k$. *L'objectif est d'obtenir une complexité $O(d)$. Cet algorithme s'appelle le schéma de Horner.*
2. On souhaite évaluer P et toutes ses dérivées $P', P'', \ldots, P^{(d)}$ sur un point $a \in k$, où $P^{(d)}$ désigne la dérivée d-ième du polynôme. Décrire et analyser un algorithme naïf pour ce problème.

Nous allons maintenant concevoir un algorithme de complexité quasi-linéaire résolvant ce dernier problème.

3. Rappeler la complexité arithmétique des meilleurs algorithmes vus en cours pour l'évaluation et pour l'interpolation d'un polynôme de degré d.
4. En utilisant une évaluation puis une interpolation de polynômes, concevoir un algorithme quasi-linéaire qui calcule le polynôme décalé $P(x + a)$ pour $a \in k$.
   Note : Par calculer le polynôme, nous entendons calculer la liste de ses coefficients.
5. Nous allons prouver la formule de Taylor en $a \in k$ pour les polynômes :

$$P(x) = \sum_{i=0}^{d} P^{(i)}(a) \frac{(x-a)^i}{i!}.$$

   (i) Prouvez la formule quand $a = 0$ et que P est un monôme X^ℓ.
   (ii) En déduire la formule pour tout polynôme quand $a = 0$.
   (iii) En déduire la formule générale.

6. En déduire un algorithme quasi-linéaire pour notre problème d'évaluation d'un polynôme et de toutes ses dérivées sur un point $a \in k$.