Fondements de l'Algorithmique Algébrique
Introduction to Algebraic Algorithms

Instructions (English)

This page contains the main instructions.
Page 2 contains the exercises in English.
Page 3 contains the exercises in French.

Duration: 1h30.

Calculators and documents are forbidden.
Phones must be off or in silent mode, and kept in bags and out of sight.
All communication is forbidden, except with the teachers.

The precision, the clarity, and the mathematical rigour of the reasonings and explanations will play an important role in the grading.

Consignes (Français)

Cette page donne les consignes globales.
La page 2 contient les exercices, en anglais.
La page 3 contient les exercices, en français.

Durée : 1h30.

Les calculatrices et les documents sont interdits.
Les téléphones portables doivent être éteints ou en mode silencieux, et rangés dans les sacs et hors de vue.
Toute communication est interdite, sauf avec les surveillants.

La précision, la clarté, et la rigueur mathématique des raisonnements et explications seront des facteurs d'appréciation importants dans la notation.

Problem 1 (Knowledge of course material)**.**

1. *Give the Sylvester matrix of the polynomials $A = x^4 - x^3 - 7x^2 + 2x + 3$ and $B = x^3 - 4x^2 + 2x + 3$ whose coefficients are in $\mathbb{Q}$.*
2. *State the definition of the resultant $\mathrm{Res}_x(A, B)$ of two polynomials $A = a_m x^m + \cdots + a_0$ and $B = b_n x^n + \cdots + b_0$, whose degrees are respectively m and n (i.e. $a_m \neq 0$ and $b_n \neq 0$).*
3. *Consider the Sylvester matrix from Question 1: is it a structured matrix? If yes, give more details (what family of structure, value of the displacement rank, ...).*
4. *Give a complexity bound for the problem of solving a linear system whose matrix is $n \times n$, quasi-Toeplitz, with displacement rank α.*
5. *In error-correcting codes, what is the goal of "introducing redundancy", and why is it necessary?*
6. *Recall the Singleton bound for the minimum distance of a linear code. For a code of length $n = 256$ and dimension $k = 200$, what is the maximal number of errors we can hope to correct?*

Problem 2 (Computing the GCD and the resultant)**.**

Let A and B be nonzero polynomials in $\mathbb{K}[x]$, of respective degrees m and n. We are interested in the computation of $\gcd(A, B)$ and $\mathrm{Res}_x(A, B)$. For this, we recall the following result from the course. Let Q and R be the unique polynomials in $\mathbb{K}[x]$ such that $A = BQ + R$ and $\deg(R) < n$. Then, $\gcd(A, B) = \gcd(B, R)$. We recall that, by convention, $\gcd(B, 0) = 1$ (where B is nonzero).

1. *Based on this result, give an algorithm for computing the GCD of A and B.*
2. *What is the complexity of your algorithm?*

Now we also recall the similar property for the resultant. By convention, $\mathrm{Res}_x(B, 0) = 1$, where B is nonzero. And, if $R \neq 0$, defining $r = \deg(R)$ and writing b_n for the leading coefficient of B, then

$$\mathrm{Res}_x(A, B) = (-1)^{mn} b_n^{m-r} \mathrm{Res}_x(B, R).$$

3. *Based on this result, give an algorithm for computing the resultant of A and B.*
4. *What is the complexity of your algorithm?*

Problem 3 (Decoding Reed-Solomon codes)**.**

Consider a Reed-Solomon code of dimension k, defined by n pairwise distinct points $x_1, \ldots, x_n \in \mathbb{K}$, and let e be the error bound, with $e \leq \lfloor \frac{n-k}{2} \rfloor$. Define $G(x) = \prod_{1 \leq i \leq n} (x - x_i)$. We have seen in tutorial session ("TD") that for this code, the decoding problem is equivalent to finding the unique polynomial $\lambda \in \mathbb{K}[x]$ such that

$$\text{there exists } \omega \in \mathbb{K}[x] \text{ such that } \begin{cases} \lambda R = \omega \mod G, \\ \deg(\lambda) \leqslant e, \quad \deg(\omega) < e + k, \quad \lambda \text{ monic} \end{cases} \tag{1}$$

where R is a polynomial of degree less than n in $\mathbb{K}[x]$ which is defined from the received word. The goal of this exercise is to find λ efficiently, from the knowledge of (G, R, n, k, e), via structured linear system solving.

Define the reversed polynomials $\hat{R}(x) = x^{n-1} R(x^{-1})$ and $\hat{G}(x) = x^n G(x^{-1})$ (they are R and G with coefficients in reversed order). Consider the polynomial $S(x)$ of degree less than $n - k$ such that $S(x) = \hat{R}/\hat{G} \bmod x^{n-k}$.

1. *Explain why S is well-defined. Give the name of an algorithm to compute $1/\hat{G} \bmod x^{n-k}$; what is its complexity? Deduce a complexity bound for the computation of $S(x)$.*
2. *Show that, in order to find λ satisfying Eq. (1), it suffices to find a polynomial $p \in \mathbb{K}[x]$ such that*

$$\text{there exists } q \in \mathbb{K}[x] \text{ such that } \begin{cases} pS = q \mod x^{n-k}, \\ \deg(p) \leq e, \quad \deg(q) < e, \quad p(0) = 1. \end{cases} \tag{2}$$

   Hints: *write $\lambda R = \omega \bmod G$ as $\lambda R = FG + \omega$, and reverse both sides of this identity in degree $e + n - 1$: the side λR becomes $x^{e+n-1} \lambda(x^{-1}) R(x^{-1}) = \hat{\lambda}\hat{R}$ with $\hat{\lambda} = x^e \lambda(x^{-1})$, which is a polynomial since $\deg(\lambda) \leq e$. Similarly $FG + \omega$ becomes $x^{e+n-1}(F(x^{-1})G(x^{-1}) + \omega(x^{-1})) = x^{e-1} F(x^{-1}) \hat{G} + x^{n-k} \hat{\omega}$ with $\hat{\omega} = x^{e+k-1} \omega(x^{-1})$, a polynomial since $\deg(\omega) < e + k$. Is $x^{e-1} F(x^{-1})$ a polynomial? Find a link between p and $\hat{\lambda}$, and conclude.*

3. *Show that finding p satisfying Eq. (2) can be done by solving a homogeneous linear system whose matrix is square, Toeplitz, of size $n - k - e$. Give the complexity of Reed-Solomon decoding by this method.*

   Hint: *consider the coefficients of degree $e, e + 1, \ldots, n - k - 1$ in the equation $pS = q \bmod x^{n-k}$.*

Problème 1 (Connaissances du cours)**.**

1. *Donner la matrice de Sylvester des polynômes $A = x^4 - x^3 - 7x^2 + 2x + 3$ et $B = x^3 - 4x^2 + 2x + 3$ dont les coefficients sont dans $\mathbb{Q}$.*
2. *Donner la définition du résultant $\mathrm{Res}_x(A, B)$ de deux polynômes $A = a_m x^m + \cdots + a_0$ et $B = b_n x^n + \cdots + b_0$, qui ont respectivement degré m et n (i.e. $a_m \neq 0$ et $b_n \neq 0$).*
3. *Considérons la matrice de Sylvester de la Question 1: est-ce une matrice structurée ? Si oui, donner des détails (quelle famille de structure, valeur du rang de déplacement, ...).*
4. *Donner une borne de complexité pour le problème de résoudre un système linéaire dont la matrice est $n \times n$, quasi-Toeplitz, avec rang de déplacement α.*
5. *Pour les codes correcteurs d'erreurs, quel est l'objectif de "l'introduction de redondance", et pourquoi est-ce primordial ?*
6. *Rappeler la borne de Singleton pour la distance minimale d'un code linéaire. Pour un code de longueur $n = 256$ et de dimension $k = 200$, quel est le nombre maximal d'erreurs que l'on peut espérer corriger ?*

Problème 2 (Calcul du PGCD et du résultant)**.**

Soient A et B des polynômes non nuls de $\mathbb{K}[x]$, de degrés respectifs m et n. Nous nous intéressons aux calculs de $\gcd(A, B)$ et $\mathrm{Res}_x(A, B)$. Pour ceci, nous rappelons le résultat suivant du cours. Soient Q et R les uniques polynômes de $\mathbb{K}[x]$ tels que $A = BQ + R$ et $\deg(R) < n$. Alors, $\gcd(A, B) = \gcd(B, R)$. On rappelle que, par convention, $\gcd(B, 0) = 1$ (ici, B n'est pas nul).

1. *En utilisant ce résultat, donner un algorithme pour calculer le PGCD de A et B.*
2. *Quelle est la complexité de cet algorithme?*

Maintenant, nous rappelons également une propriété similaire pour le résultant. Par convention, $\mathrm{Res}_x(B, 0) = 1$, où B est non nul. De plus, si $R \neq 0$, en définissant $r = \deg(R)$ et en écrivant b_n pour le coefficient de tête de B, alors

$$\mathrm{Res}_x(A, B) = (-1)^{mn} b_n^{m-r} \mathrm{Res}_x(B, R).$$

3. *En utilisant ce résultat, donner un algorithme pour calculer le résultant de A et B.*
4. *Quelle est la complexité de cet algorithme?*

Problème 3 (Decoding Reed-Solomon codes)**.**

Nous considérons un code de Reed-Solomon de dimension k, défini par n points distincts $x_1, \ldots, x_n \in \mathbb{K}$; soit e la borne d'erreur, avec $e \leq \lfloor \frac{n-k}{2} \rfloor$. Soit $G(x) = \prod_{1 \leq i \leq n}(x - x_i)$. Nous avons vu en TD que pour ce code, le problème de décodage est équivalent à trouver l'unique polynôme $\lambda \in \mathbb{K}[x]$ tel que

$$\text{il existe } \omega \in \mathbb{K}[x] \text{ tel que } \begin{cases} \lambda R = \omega \mod G, \\ \deg(\lambda) \leqslant e, \quad \deg(\omega) < e + k, \quad \lambda \text{ unitaire} \end{cases} \tag{3}$$

où R est un polynôme de degré $< n$ dans $\mathbb{K}[x]$, qui est défini à partir du mot reçu. Le but de cet exercice est de calculer λ efficacement, en connaissant (G, R, n, k, e), via la résolution d'un système linéaire structuré.

Définissons les polynômes miroirs $\hat{R}(x) = x^{n-1}R(x^{-1})$ et $\hat{G}(x) = x^n G(x^{-1})$ (ce sont R et G avec les coefficients dans l'ordre inverse). Soit $S(x)$ le polynôme de degré $< n - k$ tel que $S(x) = \hat{R}/\hat{G} \bmod x^{n-k}$.

1. *Expliquer pourquoi S est bien défini. Donner le nom d'un algorithme pour calculer $1/\hat{G} \bmod x^{n-k}$; quelle est sa complexité? Déduire une borne de complexité pour le calcul de $S(x)$.*
2. *Montrer que, pour trouver λ qui satisfait Eq.* (3)*, il suffit de trouver un polynôme $p \in \mathbb{K}[x]$ tel que*

$$\text{il existe } q \in \mathbb{K}[x] \text{ tel que } \begin{cases} pS = q \mod x^{n-k}, \\ \deg(p) \leq e, \quad \deg(q) < e, \quad p(0) = 1. \end{cases} \tag{4}$$

   Indications: *réécrire $\lambda R = \omega \bmod G$ en $\lambda R = FG + \omega$, puis prendre le miroir de cette égalité en degré $e + n - 1$: le côté λR devient $x^{e+n-1}\lambda(x^{-1})R(x^{-1}) = \hat{\lambda}\hat{R}$ avec $\hat{\lambda} = x^e\lambda(x^{-1})$, qui est un polynôme car $\deg(\lambda) \leq e$. De même, $FG + \omega$ devient $x^{e+n-1}(F(x^{-1})G(x^{-1}) + \omega(x^{-1})) = x^{e-1}F(x^{-1})\hat{G} + x^{n-k}\hat{\omega}$ avec $\hat{\omega} = x^{e+k-1}\omega(x^{-1})$, un polynôme car $\deg(\omega) < e + k$. Est-ce que $x^{e-1}F(x^{-1})$ est un polynôme? Relier p et $\hat{\lambda}$, et conclure.*

3. *Montrer comment trouver p qui satisfait Eq.* (4) *en résolvant un système linéaire homogène dont la matrice est carrée, Toeplitz, de taille $n - k - e$. Donner la complexité du décodage de Reed-Solomon par cette méthode.*

   Hint: *consider the coefficients of degree $e, e + 1, \ldots, n - k - 1$ in the equation $pS = q \bmod x^{n-k}$.*