Complément d'Algèbre, module M3201
DUT Informatique

Pierre-Cyrille Héam

12 janvier 2016

Chapitre 1

Cours-TD

Les polynômes jouent un rôle fondamental en mathématiques et en sciences. L'objectif du module sera d'étudier certains algorithmes sur les polynômes.

Dans ce cours nous confondrons polynômes et fonctions polynomiales.

1.1 Polynômes, opérations usuelles

Une **fonction polynomiale** P est une fonction qui à X associe $a_nX^n+\ldots+a_1X+a_0$ où les a_i sont des constantes. Les a_i sont appelés les coefficients du polynôme et, si $a_n \neq 0$, n est le **degré** du polynôme. Le réel a_i est le coefficient d'indice i. Le plus grand n tel que a_n soit non nul est appelé **coefficient dominant** du polynôme.

Si tous les a_i sont nuls, on dit que P est le **polynôme nul**. Par convention, son degré est $-\infty$. Par exemple, $P(x) = 5X^7 + 2X^3 - X^2 + 1$ est un polynôme de degré 7.

Exercice 1 *Donner un polynôme P de degré au plus 2 tel que $P(0) = 1$, $P(1) = 2$ et $P(2) = 11$.*

Soient $P = a_nX^n + \ldots + a_1X + a_0$ et $Q = b_nX^n + \ldots + b_1X + b_0$ deux polynômes (s'il ne sont pas de même degré, on peut ajouter des coefficients nuls au début afin d'avoir la bonne forme). La **somme** de P et de Q, notée $P + Q$ est le polynôme $c_nX^n + \ldots + c_1X + c_0$ où $c_i = a_i + b_i$. Par exemple si $P = X^3 + X - 2$ et $Q = X + 3$, alors $P + Q = X^3 + 2X + 1$.

Soient $P = a_nX^n + \ldots + a_1X + a_0$ et $\lambda \in \mathbb{R}$. On note λP le polynôme $= \lambda a_nX^n + \ldots + \lambda a_1X + \lambda a_0$; chaque coefficient est multiplié par λ.

Proposition 2 *Quelques soient les polynômes P et Q, quelques soient les réels λ et μ, on a*

$$P + Q = Q + P \quad et \quad \lambda(P + Q) = \lambda P + \lambda Q \quad et \quad (\lambda + \mu)P = \lambda P + \mu P \quad et \quad 1P = P.$$

Exercice 3 *Soient $P = X^4 + 2X^3 - X^2 + 1$ et $Q = X^2 - 2X + 2$. Calculer $P + Q$, $P - Q$, $2P + 3Q$, $3P - Q$.*

Soient $P = a_nx^n + \ldots + a_1x + a_0$ et $Q = b_mx^m + \ldots + b_1x + b_0$ deux polynômes. On note PQ, le produit de P par Q qui est le polynôme $c_\ell x^\ell + \ldots + c_1x + c_0$, où $\ell = m + n$ et

$$c_i = \sum_{p+q=i} a_pb_q = \sum_{p=0}^{i} a_pb_{i-p}.$$

Par exemple, si $P = X^5 + X^2 - 1$ et $Q = X^2 + X + 1$, on a $PQ = X^7 + X^6 + X^5 + X^4 + X^3 - X - 1$.

Proposition 4 *Quelques soient les polynômes P et Q, quelques soient les réels λ et μ, on a*

$$PQ = QP \quad et \quad (\lambda P)(\mu Q) = (\lambda\mu)PQ.$$

Exercice 5 *Soient $P = x^4 + 2x^3 - x^2 + 1$ et $Q = x^2 - 2x + 2$ et $R = x^3 + 2x^2 - x + 1$. Calculer PQ, PR, QR, P^2, Q^2, R^2.*

Soit $P = a_nX^n + \ldots + a_1X + a_0$ un polynôme. On appelle **polynôme dérivé** de P le polynôme, noté P', définit par : $P' = na_nX^{n-1} + \ldots + a_1$.

Par exemple, si $P = 2X^3 + X^2 - 4X + 7$, alors $P' = 6X^2 + 2X - 4$

Exercice 6 *Dériver les trois polynômes de l'exercice 5.*

1.2 Division de Polynômes

Soient P et Q deux polynôme. Si Q est non nul, alors il existe un unique couple (A, B) de polynômes tel que $P = AQ + B$ et le degré de B est strictement inférieur au degré de Q. Le polynôme A s'appelle le **quotient** de la division de P par Q et B le **reste.**

La division se pose comme pour les entiers. Divisons par exemple $P = X^3 + X^2 - 1$ par $X - 1$. On obtient la division :

$$\begin{array}{rrrr|rrr}
X^3 & +X^2 & & -1 & X & -1 & \\
\cline{5-7}
-X^3 & +X^2 & & & X^2 & +2X & +2 \\
\cline{1-2}
 & 2X^2 & & & & & \\
 & -2X^2 & +2X & & & & \\
\cline{2-3}
 & & 2X & & & & \\
 & & -2X & +2 & & & \\
\cline{3-4}
 & & & +1 & & &
\end{array}$$

Le quotient est $X^2 + 2X + 2$ et le reste 1.

Exercice 7 *Calculer les restes et quotients de P par Q dans les cas suivants :*

1. $P = X^4 + 2X^3 - X^2 + 3$ *et* $Q = X^3 + X - 1$.
2. $P = X^7 + 3X^5 - X^6 + X^4 - 3X^3 + X^2 + 2x - 1$ *et* $Q = X^4 + 3X$.
3. $P = X^5 - X^4 + 2X^3 - X^2 + 1$ *et* $Q = X + 3$.
4. $P = X^8 + X^3 + X^2 + 3X - 1$ *et* $Q = X^2 + 1$.
5. $P = X^7 - X^5 + 2X^4 - 3X^3 + 7X^2 + X + 1$ *et* $Q = X^2 + 2X + 1$.
6. $P = X^7 - X^5 + 2X^4 - 3X^3 + 7X^2 + X + 1$ *et* $Q = X^2 - 2X + 1$.
7. $P = X^7 - X^5 + 2X^4 - 3X^3 + 7X^2 + X + 1$ *et* $Q = X^2 + 2X - 1$.

Exercice 8 *Calculer les reste et le quotient de $X^n - 1$ par $X - 1$.*

On dit qu'un polynôme Q *divise* un polynôme P s'il existe un polynôme A tel que $P = AQ$. Si Q est non nul, cela équivaut à dire que le reste de la division de P par Q est nul.

Exercice 9 *A quelles conditions sur a, b et c le reste de la division de $X^4 + aX^2 + bX + c$ par $X^2 + X + 1$ est-il nul ?*

Exercice 10 *Soit $P = X^4 + X^3 - aX^2 + X + c$ et $Q = X^2 + aX$, où a et c sont des constantes. Quel est le quotient de la division de P par Q ? A quelles conditions sur a et c le reste de la division de P par Q est-il nul ?*

1.3 PGCD de deux polynômes

On dit qu'un polynôme P **divise** un polynôme Q si le reste de la division de P par Q est nul.

Soient P et Q deux polynômes. Il existe un unique polynôme D de coefficient dominant 1 tel que : D divise Q, D divise P, et si R est un polynôme qui divise P et Q, alors R divise D. Le polynôme D est appelé **PGDC** de P et de Q.

Considérons par exemple le polynôme $P = X^2 + 2X + 1$ et le polynôme $Q = X^2 + 4X + 3$. Le polynôme $X + 1$ est le PGCD de P et Q

1. $X + 1$ divise P, le quotient est $X + 1$,
2. $X + 1$ divise Q, le quotient est $X + 3$,
3. le coefficient dominant de $X + 1$ est 1,
4. Si R divise P et R divise Q, soit R est un polynôme de degré 0, soit R est un de la forme $aX + a$, avec $a \neq 0$. Dans les deux cas, R divise $X + 1$.

En pratique, le PGCD de deux polynômes se calcule grâce à l'algorithme d'Euclide. Pour cela, on a besoin de la proposition suivante.

Proposition 11 *Soient P et Q deux polynômes et R le reste de la division de P par Q. On a*

$$\mathrm{PGCD}(P, Q) = \mathrm{PGCD}(Q, R).$$

Par ailleurs, $\mathrm{PGCD}(P, 0) = \frac{1}{a}P$, *où a est le coefficient dominant de P.*

L'algorithme d'Euclide consiste à appliquer la proposition précédente tant que le reste de la division n'est pas nul. Par exemple, considérons les polynômes $P = X^3 + 2X^2 + X$ et $Q = X^3 + 3X^2 - X - 3$. On a

1. $\mathrm{PGCD}(P,Q) = \mathrm{PGCD}(Q,R)$ où R est le reste de la division de P par Q. Ici $R = -X^2+2X+3$. Donc $\mathrm{PGCD}(P,Q) = \mathrm{PGCD}(Q,-X^2+2X+3)$
2. En appliquant la propriété à nouveau, $\mathrm{PGCD}(Q,-X^2+2X+3) = \mathrm{PGCD}(-X^2+2X+3, 12X+12)$.
3. A nouveau $\mathrm{PGCD}(-X^2+2X+3,12X+12) = \mathrm{PGCD}(12X+12,0) = \frac{1}{12}(X+12) = X+1$.

Exercice 12 *Calculer les PGCD des polynômes suivants.*

1. X^3+X^2+X+1 *et* $X^3+6X^2+11X+6$.
2. $X^6+X^4+X^2+1$ *et* X^3-3X^2+X-3.
3. X^4+2X^2+1 *et* X^3-3X^2+3X-1.
4. $P = X^3+X^2-X-1$ *et* $Q = X^3-X^2+X-1$.

1.4 Racines d'un polynôme

Soit P un polynôme, et a un réel, on note $P(a)$ la valeur de P en a (P est ici considéré comme une fonction). On appelle **racine** d'un polynôme P tout réel a tel que $P(a)=0$. Par exemple 3 est une racine de X^2-3X.

Un polynôme (à coefficients réels) peut ne pas avoir de racine, par exemple X^2+1.

Proposition 13 *Soit P un polynôme. Le réel a est racine de P si et seulement si $X-a$ divise P.*

On dit que a est **racine d'ordre** k de P si $(X-a)^k$ divise P et $(X-a)^{k+1}$ ne divise pas P.

Proposition 14 *Soit P un polynôme. Le réel a est racine d'ordre k de P si et seulement si $P(a) = P'(a) = \ldots P^{(k)}(a) = 0$ où $P^{(i)}(a)$ est la dérivée i-ème de P (on a dérivé P i fois de suite).*

Exercice 15 *Soit $P = X^2+2X+1$, montrer que -1 est racine double (d'ordre 2).*

Exercice 16 *Soit $P = X^5-6X^4+13X^3-14X^2+12X-8$, montrer que 2 est racine d'ordre 3 (on dit aussi racine triple).*

Exercice 17 *Soit $P = aX^2+bX+c$ avec $a \neq 0$.*

1. *Sans utiliser le discriminant ni les formules connues sur les équations du second degré, retrouver que si α est racine double alors $\alpha = \frac{-b}{2a}$.*
2. *Sans utiliser le discriminant ni les formules connues sur les équations du second degré, retrouver que si P a une racine double, alors $b^2-4ac=0$.*

Exercice 18 *On considère le polynôme $P = X^3+bX^2+cX-1$ où b et c sont des réels.*

1. *A quelle condition 1 est-il racine de P ?*
2. *A quelle condition 1 est-il racine d'ordre au moins 2 ? Exactement 2 ?*

Proposition 19 *Soit P un polynôme. Le réel a est racine de P si et seulement si $X-a$ divise P.*

Proposition 20 *Soit P un polynôme. Le polynôme quotient de P par $\mathrm{PGCD}(P,P')$ a les même racines que P et elle sont toutes simples.*

Exercice 21 *Soit $P = aX^3+bX^2+cX+d$ où a,b,c,d sont des constantes et $a \neq 0$.*

1. *Quand dit-on que α est racine d'ordre k d'un polynome Q ?*
2. *Justifier que si α est racine d'ordre 3 de P, alors $\alpha = \frac{-b}{3a}$*
3. *Justifier que si P a une racine triple, alors $b^2-3ac=0$.*

Exercice 22 *On appelle ideal tout ensemble de polynômes I vérifiant les propriétés suivantes : (1) I est non vide, et (2) si $P,Q \in I$, alors $P+Q$ et $P-Q$ sont aussi dans I, et (3) si $P \in I$ et Q est un polynôme quelconque (pas nécessairement dans I), alors $PQ \in I$.*

1. *Justifier que si I est un idéal, alors il contient le polynôme nul.*
2. *Soit P_0 un polynôme. Justifier que l'ensemble des multiples de P_0 est un idéal.*
3. *Soit P et Q deux polynômes d'un idéal I. Justifier que le reste de la division euclidienne de P par Q est aussi dans I.*
4. *Soit P et Q deux polynômes d'un idéal I. Justifier que le PGCD de P et de Q est dans I.*
5. *Justifier que si I est un idéal, il existe un polynome P tel que I soit l'ensemble des multiples de P.*

1.5 Produits de polynômes, produits d'entiers

1.5.1 Polynômes et entiers

Pour illustrer les algorithmes, on va supposer que les entiers sont codés en décimal. Quelque soit la base, les techniques sont les mêmes.

Soit a un entier codé en décimal. Soit $a_n a_{n-1} \dots a_0$ (où $a_i \in \{0, \dots, 9\}$) l'écriture en décimale de a. Par exemple, pour $a = 45123$ on a $a_0 = 3$, $a_1 = 2$, $a_2 = 1$, $a_3 = 5$ et $a_4 = 4$. Par définition de la représentation on a

$$a = \sum_{i=0}^{n} a_i 10^i.$$

On va donc naturellement associer à a le polynôme suivant, noté P_a,

$$P_a(X) = \sum_{i=0}^{n} a_i X^i.$$

Et l'on a, pour tout a,

$$P_a(10) = a \tag{1.1}$$

On a donc, pour tout couple d'entiers a, b, $ab = P_a(10)P_b(10)$.

Exercice 23 *Soit P le produit $X^2 + 5X + 3$ par $8X + 4$. Que vaut $P(10)$? Comparer avec 153×84.*

Les algorithmes de multiplications de polynômes peuvent servir à multiplier des entiers.

1.5.2 Algorithme de Karatsuba

Pour calculer $(aX^n + b)(cX^n + d) = acX^{2n} + (ad + bc)X^n + bd$ et donc calculer les produits ac, ad, bc et bd (cela fait 4 multiplications et une addition).

L'idée de l'algorithme de Karatsuba est de remarquer que $ad + bc = (a + b)(c + d) - ac - bd$ et donc qu'il suffit de faire trois multiplications (et quatre additions) : ac, bd et $(a + b)(c + d)$.

Soient deux polynômes $P_1 = a_n x^n + Q_1$ (où Q_1 a un degré strictement inférieur à P_1) et $P_2 = b_n X^n + Q_2$ (où Q_1 a un degré strictement inférieur à P_2). On suppose, pour simplifier, que n est une puissance de 2. On a alors :

$$P_1 P_2 = a_n b_n X^{2n} + [(a_n + b_n)(Q_1 + Q_2) - a_n b_n - Q_1 Q_2]x^n + Q_1 Q_2.$$

Dans cette expression, il faut noter que $a_n b_n$ est le produit de deux coefficients. Il n'y a pas que des sommes de polynômes et de produits d'un polynôme par un réel à calculer, saut $Q_1 Q_2$, pour lequel on peut ré-appliquer la méthode.

On peut démontrer que par cette méthode, le nombre d'opération est de l'ordre de $n^{1.59}$ contre n^2 pour l'approche naïve.

Cherchons par exemple à multiplier $P = X^4 + 2X^3 + X^2 + 8X + 1$ par $Q = 2X^4 + X^2 + 2X + 1$. On a

$$\begin{aligned} PQ =& 2X^8 + [(2 + 1)(2X^3 + X^2 + 8X + 1 + X^2 + 2X + 1) - a_n b_n - Q_1 Q_2]X^4 \\ &+ (2X^3 + X^2 + 8X + 1)(X^2 + 2X + 1) \\ =& 2X^8 + [3(2X^3 + 2X^2 + 10X + 2) - 2 - Q_1 Q_2]X^4 \\ &+ (2X^3 + X^2 + 8X + 1)(X^2 + 2X + 1) \\ =& 2X^8 + (6X^3 + 6X^2 + 30X + 4 - Q_1 Q_2)X^4 - Q_1 Q_2 \end{aligned}$$

On peut ensuite ré-appliquer la méthode pour $Q_1 Q_2 = (2X^3 + X^2 + 8X + 1)(X^2 + 2X + 1)$.

Prenons un exemple sur des entiers et calculons $2468 * 1357$. On décompose

$$\begin{aligned} 2468 \times 1357 &= (24.10^2 + 68)(13.10^2 + 57) \\ &= 24.13.10^4 + [(24 + 13)(68 + 57) - 24.13 - 68.57].10^2 + 57.68 \end{aligned}$$

On a donc les trois produits à calculer 24×13, 57×68 et 37×125. On a de même :

$$\begin{aligned} 24 \times 13 &= (2.10 + 4)(10 + 3) \\ &= 2.10^2 + [(2 + 4)(1 + 3) - 2 - 3.4].10 + 3.4 \\ &= 200 + (24 - 14).10 + 12 = 200 + 100 + 12 = 312 \\ 57 \times 68 &= 5.6.10^2 + [(5 + 7)(6 + 8) - 5.6 - 7.8].10 + 7.8 \\ &= 30.100 + (12.14 - 30 - 56)10 + 56 = 3876 \\ 35 \times 125 &= 3.12.100 + (8.17 - 3.13 - 5.5).10 + 5.5 = 3600 + 720 + 25 = 4625. \end{aligned}$$

A la main, la méthode peut paraître fastidieuse (elle l'est), mais pour un ordinateur et pour des entiers longs, elle est plus efficace que la méthode *classique*.

Exercice 24 *Quels sont les trois produits que l'on obtient à calculer avec l'algorithme de Karatsuba pour les entiers suivants :*

1. 12344321×56788765 *?*
2. 1234×1234 *?*
3. 4321×4321 *?*
4. 5555 *?*

1.5.3 Transformée de Fourier Rapide (FFT)

Représentations par coefficients ou par valeurs

Par définition un polynôme est donné par la suite (finie) de ses coefficients. Cependant, d'un point de vue fonctionnel, on peut définir un polynôme (réel ou complexe) par une suite finie de points. On s'appuie pour cela sur le résultat suivant.

Pour tout ensemble $\{(\alpha_0, \beta_0), \ldots, (\alpha_{n-1}, \beta_{n-1})\}$ de cardinal n de couples de nombres complexes, il existe un unique polynôme R de degré $n-1$ tel que pour tout $1 \leq i \leq n$, $R(\alpha_i) = \beta_i$. Le polynôme R peut d'ailleurs s'exprimer par la formule de Lagrange :

$$R(X) = \sum_{k=0}^{n-1} \beta_k \frac{\prod_{j \neq k}(X - \alpha_j)}{\prod_{j \neq k}(\alpha_k - \alpha_j)}$$

L'ensemble $\{(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)\}$ est appelé représentation par valeurs de R. La représentation par valeurs est efficace pour certains calculs, comme l'addition ou la multiplication. En revanche, cette représentation n'est pas unique et la comparaison est plus délicate, tout comme la dérivation par exemple.

Il faut noter pour la suite que l'on peut avoir des représentations par valeurs redondantes. Par exemple, un polynôme de degré n peut être donnés par son évaluation en plus de $n+1$ points. Le calcul des coefficients de ce polynôme pourra alors se faire en choisissant $n+1$ points quelconque dans l'ensemble.

L'utilisation de données redondantes va nous être utile pour le calcul des produits. Soient A et B deux polynômes de degrés au plus $n-1$ donnés par $2n$ points. Le polynôme A est donné par

$$\{(\alpha_0, \beta_0), \ldots, (\alpha_{2n-1}, \beta_{2n-1})\}$$

et le polynôme B par

$$\{(\alpha_0, \beta'_0), \ldots, (\alpha_{2n-1}, \beta'_{2n-1})\}$$

Dans ce cas, le polynôme AB est donné par

$$\{(\alpha_0, \beta_0\beta'_0), \ldots, (\alpha_{2n-1}, \beta_{2n-1}\beta'_{2n-1})\}$$

Il faut noter ici que A,B et C sont donnés par des évaluations aux mêmes valeurs (les α_i).

Lorsque l'on connaît les coefficients d'un polynôme, il existe un algorithme efficace, appelé algorithme d'Hörner, afin d'évaluer la fonction associée en un point donné.

Enfin il est important de noter ici que calculer un polynôme d'interpolation (c'est-à-dire passer d'une représentation par valeurs à une représentation par coefficients) est équivalent à résoudre un système. Plus précisément, à partir de la représentation

$$\{(\alpha_0, \beta_0), \ldots, (\alpha_{n-1}, \beta_{n-1})\}$$

les coefficients a_i du polynôme $R(X) = a_0 + a_X + \ldots + a_{n-1}X^{n-1}$ correspondant vérifient

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^{n-1} \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-1} & \alpha_{n-1}^2 & \ldots & \alpha_{n-1}^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2n-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix} \tag{1.2}$$

Principe général de la FFT

Le schéma général de la FFT est illustré par la figure 1.1 :

L'idée de la FFT est d'améliorer les complexités générales en utilisant des racines de l'unité comme point d'évaluation :

- L'utilisation de ces racines et de leurs propriétés particulières permet de faire l'évaluation beaucoup plus efficacement que par l'algorithme de Hörner.
- Les résultats de ces évaluations ont des tailles modérées, ce qui rend les multiplications point à point plus efficaces.
- L'interpolation est aussi faisable de façon plus rapide (encore grâce aux propriétés particulières des racines de l'unité) que par la formule de Lagrange.

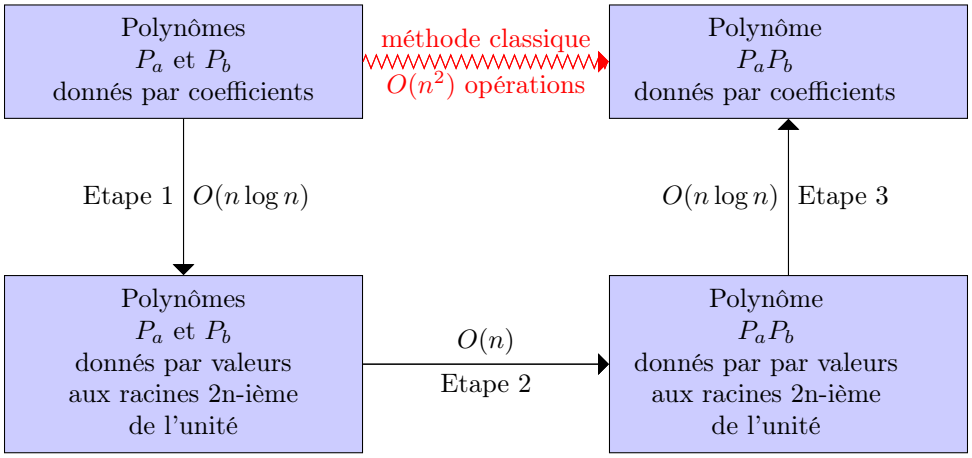

FIGURE 1.1 – Schéma général de la FFT

Évaluation aux racines de l'unité : étape 1

En reprenant les notations de la partie précédentes, on suppose que l'on a un polynôme $P = x_0 + x_1X + \ldots + x_{n-1}X^{n-1}$ de degré $n-1$ où n est une puissance de 2 (algorithmiquement, si ça n'est pas le cas on ajoute des coefficients nuls).

On pose

$$w = e^{i\frac{\pi}{n}}$$

On va chercher à calculer la représentation de P par valeur en calculant $P(w), P(w^2), \ldots, P(w^{2n-1}), P(w^n)$.

On va pour cela utiliser une approche récursive en décomposant P de la manière suivante :

$$P(X) = P_1(X^2) + XP_2(X^2) \tag{1.3}$$

où

$$P_1(X) = x_0 + x_2X + \ldots + x_{n-2}X^{\frac{n}{2}-1}$$

et

$$P_2(X) = x_1 + x_3X + \ldots + x_{n-1}X^{\frac{n}{2}-1}$$

On va estimer $P(w^k)$ en calculant $P_1(X^2)$ et $P_2(X^2)$ en w^k puis en utilisant (1.3). Comme les racines de l'unité sont de module 1, le calcul de (1.3) se fait sur des complexes de *petite taille*[1].

Le point clé est que pour estimer $P_1(X^2)$ pour les $2n$ valeurs de la forme w^k il n'y a que n évaluations à faire : en effet $(w^k)^2 = (w^{n+k})^2$ et les n premières évaluations fournissent directement les n suivantes.

Avec cette astuce, la complexité de l'algorithme chute immédiatement et ne demande plus que $O(n \log n)$ opérations élémentaires.

Multiplication point à point : étape 2

On a maintenant calculé les valeurs de P_a et P_b pour les différents w^k. En utilisant le fait que w^k est de module 1, les résultats se codent sur une petite taille. La multiplication point à point ne demande donc que $O(n)$ opérations élémentaires.

Interpolation : étape 3

Il reste la dernière étape. On connaît une représentation par valeurs de P_aP_b ; on souhaite en calculer les coefficients.

Posons

$$Q = P_aP_b(X) = y_0 + y_1X + \ldots + y_{2n-1}X^{2n-1}$$

On peut vérifier que (même chose que pour (1.2))

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & w & w^2 & \ldots & w^{2n-1} \\ 1 & w^2 & w^4 & \ldots & w^{4n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{2n-1} & w^{4n-2} & \ldots & w^{2n^2-n} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_{2n-1} \end{pmatrix} = \begin{pmatrix} Q(w^0) \\ Q(w) \\ Q(w^2) \\ \vdots \\ Q(w^{2n-1}) \end{pmatrix}$$

1. Il faut noter ici que l'utilisation de nombre complexe peut introduire des erreurs d'arrondi. la procédure de FFT peut être modifiée pour les calculs sur les entiers qui nous intéressent, sans perte de précision. La procédure s'appuie sur les mêmes idées mais est techniquement plus complexe.

Or

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{2n-1} \\ 1 & w^2 & w^4 & \dots & w^{4n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{2n-1} & w^{4n-2} & \dots & w^{2n^2-n} \end{pmatrix}^{-1} = \frac{1}{2n} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w^{-1} & w^{-2} & \dots & w^{-2n+1} \\ 1 & w^{-2} & w^{-4} & \dots & w^{-4n+2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{-2n+1} & w^{-4n+2} & \dots & w^{-2n^2+n} \end{pmatrix}$$

On pourrait alors calculer les y_i par produit de matrices, mais cela demanderait $O(n^2)$ opération.
Considérons donc plutôt le polynôme

$$\overline{Q} = \frac{1}{2n}(Q(w^0) + Q(w)X + \cdots + Q(w^{2n-1})X^{2n-1})$$

D'après le système vu ci-dessus, y_i est $\overline{Q}(w^{-i})$. Ces valeurs peuvent se calculer avec la même technique que la FFT (mais en utilisant w^{-1} au lieu de w), soit en $O(n \log n)$. On parle dans ce cas de transformée de Fourier inverse.

Chapitre 2

TP

2.1 Polynômes - fonctions élémentaires

Le TP se feront en `Python`. Un polynôme $P(x) = a_0 + a_1x + \ldots, +a_nx^n$, avec $a_n \neq 0$, sera codé par la liste

$$[a_0, a_1, \ldots, a_n]$$

Le polynôme nul sera codé par la liste vide `[]`.

Exercice 1

1. *On impose dans le codage que $a_n \neq 0$. Écrire une fonction qui étant donnée une liste tronque tous les coefficients nuls en partant de la fin. Tester votre fonction sur les exemples ci-dessous.*
   Sur [1,2,3,4] la fonction doit retourner [1,2,3,4]
   Sur [0,1,2,3,0,4] la fonction doit retourner [0,1,2,3,0,4]
   Sur [0,1,2,3,0,4,0,0,0] la fonction doit retourner [0,1,2,3,0,4]
   Sur [0,0,0] la fonction doit retourner []
2. *Programmer une fonction calculant la somme de deux polynômes.*
   Sur [1,2,3,4] et [1,2,3,4] la fonction doit retourner [2,4,6,8]
   Sur [1,2,3,4] et [1,2,3,4,5] la fonction doit retourner [2,4,6,8,5]
   Sur [1,2,3,4,5] et [1,2,3,4] la fonction doit retourner [2,4,6,8,5]
   Sur [1,2,-3,-4] et [1,2,3,4] la fonction doit retourner [2,4]
   Sur [-1,-2,-3,-4] et [1,2,3,4] la fonction doit retourner []
   Sur [1,2,3,4] et []la fonction doit retourner [1,2,3,4]
3. *Programmer une fonction calculant le produit d'un polynôme par une constante. Indiquer en commentaire de votre programme les tests effectués.*
4. *Programmer une fonction calculant le produit de deux polynômes. Indiquer en commentaire de votre programme les tests effectués.*
5. *Programmer une fonction calculant le quotient de deux polynômes. Indiquer en commentaire de votre programme les tests effectués.*
6. *Programmer une fonction dérivant un polynôme. Indiquer en commentaire de votre programme les tests effectués.*

2.2 Algorithme de Hörner et racines

Si $P = a_0 + a_1x + \ldots, +a_nx^n$, avec $a_n \neq 0$, et si $x \in \mathbb{R}$, $P(x)$ peut naïvement se calculer en calculant chacun des produits a_ix^i, puis en faisant leur somme. Un tel calcul demande de l'ordre de $n \log n$ multiplications et n additions. On peut faire beaucoup mieux en remarquant que pour calculer x^{i+1}, on peut réutiliser le calcul de x^i. Pour cela, on regroupe les les coefficients de P ainsi :

$$P = a_0 + a_1x + \ldots, +a_nx^n = a_0 + x(a_1 + x(a_2 + \ldots a_{n-1} + xa_n)).$$

Par exemple

$$1 + x + 2x^2 + 4x^3 - 2x^4 + 10x^5 - 7x^5 = 1 + x(1 + x(2 + x(4 + x(-2 + x(10 - 7x))))).$$

Ainsi exprimé, il y a de l'ordre de n multiplications et n addition. Cette façon de calculer s'appelle l'**algorithme de Hörner**.

Exercice 2 *Programmer l'algorithme de Sturm.*
Sur [1,2,3,4] et $x = 1$, la fonction doit retourner 10
Sur [1,2,3,4] et $x = -1$, la fonction doit retourner -2
Sur [] et $x = 1$ la fonction doit retourner 0
Indiquer en commentaire de votre programme les tests effectués.

Soit P un polynôme et a et b deux réels, avec $a < b$. On suppose que P a une unique racine, notée α entre a et b. On sait alors que $P(a)$ et $P(b)$ n'ont pas le même signe, c'est-à-dire que $P(a) \leq 0$ et $P(b) \geq 0$, ou le contraire. On cherche une valeur approchée de α à ε près : concrètement on cherche β tel que $|\alpha - \beta| \leq \varepsilon$. On peut trouver un tel β par dichotomie :

1. Si $|a - b| \leq \varepsilon$, alors on retourne a.
2. Sinon, on calcule $r = \frac{a+b}{2}$ et $P(r)$. Si $P(r)$ a le même signe de $P(a)$, alors on sait que la racine est entre r et b. Dans ce cas on repart à l'étape 1. avec comme bornes r et b. Dans le cas contraire, que la racine est entre a et r : on repart à l'étape 1. avec comme bornes a et r.

Exercice 3 *Programmer la recherche d'une valeur approchée d'une racine avec la méthode ci-dessus.*
Le polynôme $P = -2 + X - 2X^3 + X^4$ admet une unique racine est 2. Tester pour trouver cette valeur à 0.1 près, 0.3 près, avec différentes valeurs de a et de b.
Faire les mêmes tests avec $-P$.
Faire pour P et $-P$ un test avec $a = -2$ et $b = -1$ (pas de racine).
Faire un test avec P et $-P$ et $a = 2$
Indiquer en commentaire les tests effectués.

2.3 PGCD et suite de Sturm

Exercice 4 *Écrire une fonction calculant le PGCD de deux polynômes.*
Tester avec les exemples vus en TD.

Exercice 5 *Écrire une fonction qui étant donné un polynôme, ressort un polynôme ayant les mêmes racines, mais à racines simples. On s'appuiera sur la proposition 20 du cours.*
Indiquer en commentaire les tests effectués.

2.4 Algorithme de Sturm

Soit $x_0, x_1, \ldots, x_k$ une suite de nombres réels tous non nuls. On appelle **nombre de changements de signe**, le nombre de i tels que $x_i x_{i+1} < 0$. Si $x_0, x_1, \ldots, x_k$ est une suite (qui peut contenir des éléments nuls), son nombre de changements de signe est le nombre de changements de signe de la suite obtenue en supprimant les termes nuls. Par convention, le nombre de changements de signes de la suite vide est 0.

Exercice 6 *Écrire une fonction qui étant une suite de réels, retourne le nombre de changements de signes de cette suite.* Indiquer en commentaire les tests effectués.

Soit P un polynôme à racines simples. Soient $T_0 = P, T_1 = P', T_2, \ldots, T_\ell$ les restes des polynômes obtenus lors de l'application de l'algorithme d'Euclide sur P et P'. Notons que comme P est à racines simples, T_ℓ est un polynôme constant. On appelle **suite de Sturm** de P en a, la suite

$$\frac{T_0(a)}{T_\ell}, \ldots, \frac{T_\ell(a)}{T_\ell}.$$

Notons que le dernier terme de cette suite est toujours 1.

Théorème 25 *Soient P un polynôme à racine simples, a et b deux réels tels que $P(a) \neq 0$ et $P(b) \neq 0$. Soient s_a et s_b le nombre de changements de signes des suites de Sturm de P en a et b. Le polynôme P possède $|s_a - s_b|$ racines entre a et b.*

Exercice 7 *Écrire une fonction qui étant un polynôme P et un réel a, calcule la suite de Sturm correspondante.* Indiquer en commentaire les tests effectués.

Exercice 8 *Écrire une fonction qui étant un polynôme P à racines simples et deux réels a et b, calcule le nombre de racine de P entre a et b.* Indiquer en commentaire les tests effectués.

Exercice 9 *Écrire une fonction qui étant un polynôme P à racines simples et deux réels a et b, retourne une suite croissante $a_0 = a, a_1, \ldots, a_k = b$ tel que P a exactement une racine entre chaque a_i, a_{i+1}. On pourra procéder par dichotomie.* Indiquer en commentaire les tests effectués.

Exercice 10 *Écrire une fonction qui trouve les racines à ε près (ε est donné) d'un polynôme P entre deux valeurs a et b données.* Indiquer en commentaire les tests effectués.

Proposition 26 *Soit $P = a_o + a_1 X + \ldots + a_n X^n$ un polynôme et*

$$M = 1 + \max_{0 \leq i \leq n} |a_i|^2.$$

Si $P(\alpha) = 0$, alors $\alpha \in [-M, M]$.

Exercice 11 *Écrire une fonction qui trouve les racines à ε près (ε est donné) d'un polynôme P.* Indiquer en commentaire les tests effectués.

2.5 Exercices Annexes

Exercice 12 *Programmer l'algorithme de Karatsuba. Effectuer des tests de performances pour des polynômes de dégré élevé.*

Exercice 13 *An analyse numérique, les problèmes d'arrondis engendrent parfois des erreurs importantes. Reprogrammer les fonctions de bases (notamment la division) pour des polynômes à coefficients rationnels (fractions).*