Université du Littoral Côte d'Opale — Année universitaire 2011–2012
Licence 2ème année — Informatique

Calcul Formel & Courbes et Surfaces

Durée : 2 h le mercredi 27 juin
Documents et calculatrices de l'ULCO autorisés
Les deux parties du devoir seront traitées sur des copies différentes.

Calcul Formel

Exercice 1 (5 points)**.** On pose $p = 3$ et $q = 7$ et $e = 5$

- **1)** Calculer $n = p \cdot q$ puis $\phi(n)$.
- **2)** Chercher d tel qu'on ait $ed \equiv 1 \mod \phi(n)$.
- **3)** Quels paramètres constituent la clé publique ? Et la clé privée ?
- **4)** Posons $M = 3$. Quel est le chiffré C de M ?
- **5)** Retrouver M à partir de C et de la clé privée.

Exercice 2 (6 points)**.** Notons E l'ensemble des polynômes à coefficents sur $\mathbb{Z}$ de degré inférieur ou égal à 9. On se propose de représenter un polynôme de E par :

```
struct{
 int coeffs[10];
}Poly;
```

Le polynôme $3x^8 + 2x^2 - 1$ aura alors le tableau `[-1,0,2,0,0,0,0,0,3,0]` comme `coeffs`.

- **1)** Ecrire une fonction `int degre(Poly P)` qui retourne le degré du polynome `P`.
- **2)** Ecrire une fonction `int eval(Poly P,int x)` qui retourne le polynôme `P` évalué en `x`.
- **3)** Ecrire une fonction `void racines(Poly P,int n)` qui affiche toutes les racines entières de `P` comprises entre `-n` et `n`.
- **4)** Ecrire une fonction `Poly deriv(Poly P)` qui retourne le polynôme dérivé de `P`.

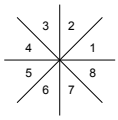
Exercice 3 (9 points)**.** Les éléments de $\mathbb{F}_2^n$ pourront être notés sous forme de n-uplets ou de vecteurs colonnes. Soit ϕ le code correcteur défini par

$$\begin{array}{rccc} \phi : & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & (b_1, b_2, b_3) & \mapsto & (b_1, b_2, b_3, b_1 + b_2, b_1 + b_2 + b_3) \end{array}$$

- **1)** Quel est le paramètre du code ϕ?
- **2)** Quelle est l'image du code ϕ.
- **3)** Quelle est la distance minimale de ϕ?
- **4)** Quelles sont les capacités de détection et de correction pour ϕ ?
- **5)** Le code ϕ est-il linéaire ? systématique ?
- **6)** Le code ϕ est-il MDS ?
- **7)** Donner la matrice génératrice de ϕ.
- **8)** Donner une matrice de contrôle pour ϕ.
- **9)** Calculer la table de décodage de ϕ.
- **10)** Décoder le mot 01010.

Courbe et Surfaces

Exercice 4 (10 points)**.** *Dans cet exercice on s'intétresse au tracet de demi-droites du deuxième octant à l'aide de l'algorithme de Bresenham. Soit $\mathcal{D}$ la demi-droite d'équation $y = mx$ pour $x \geqslant 0$.*



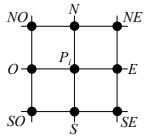
– **1)** Pour quelles valeurs de m, la demi-droite $\mathcal{D}$ se trouve dans le second octant ?

Pour la suite on suppose que $\mathcal{D}$ est dans le second octant et que m est un entier. L'équation cartésienne de $\mathcal{D}$ est $F_m(x, y) = y - mx$. Un point $M = (x_M, y_M)$ appartient alors à $\mathcal{D}$ si et seulement si $F_m(x_M, y_M) = 0$.

– **2)** Quelle est le signe de $F_m(x_M, y_M)$ pour un point $M = (x_M, y_M)$ se trouvant en dessous de $\mathcal{D}$.

Supposons que l'on trace à partir de $x = 0$ la demi-droite $\mathcal{D}$. L'algorithme de Bresenham consiste alors à allumer successivement des points $P_0, P_1, P_2, ...$ On note (x_i, y_i) les coordonnées du point P_i.

– **3)** Après avoir allumé le point P_i quels sont les deux pixels possibles parmi N, NE, E, SE, S, SO, O et NO pour P_{i+1}? Faire un dessin peut être très utile.



On note $M = (x_M, y_M)$ le point se trouvant au milieu du segment reliant les deux points possibles pour P_{i+1} et Q l'intersection de ce même segment avec la demi-droite $\mathcal{D}$. On choisira alors pour P_{i+1} le point du même côté que Q par rapport à M comme pour l'algorithme de tracé de segment vu en cours.

– **4)** Calculer les coordonnées (x_M, y_M) de M en fonction de (x_i, y_i).

– **5)** En fonction du signe de $F_m(x_M, y_M)$ déduire successivement, la position de M par rapport à la demi-droite $\mathcal{D}$, la position de Q par rapport à M, les cordonnées (x_{i+1}, y_{i+1}) du point P_{i+1}.

– **6)** Donner une expression δ_i qui soit du même signe que $F_m(x_M, y_M)$ mais nécessitant uniquement des calculs sur les entiers. On cherchera une expression développer de δ_i de la forme $K \times F_m(x_M, y_M)$ où K est un entier ne dépendant ni de m ni de i.

– **7)** En fonction du choix pour P_{i+1} donner une formule liant δ_i à δ_{i+1}.

Exercice 5 (10 points)**.** *Dans cet exercice, on calcule une courbe d'interpolation passant par les points $P_0 = (-1, 0)$, $P_1 = (0, 2)$ et $P_2 = (1, 1)$. Le couple (x_i, y_i) désigne les coordonnées de P_i pour $i = 0, 1, 2$.*

Nous utilisons dans un premier temps un polynôme d'interpolation de Lagrange

– **1)** Calculer les polynômes $L_0(X), L_1(X)$ et $L_2(X)$ de $\mathbb{Q}[X]$ tels que $L_0(-1) = 1$, $L_0(0) = 0$, $L_0(1) = 0$, $L_1(-1) = 0$, $L_1(0) = 1$, $L_1(1) = 0$, $L_2(-1) = 0$, $L_2(0) = 0$ et $L_2(1) = 1$.

– **2)** En déduire le polynôme $P(X)$ vérifiant $P(-1) = 0$, $P(0) = 2$ et $P(1) = 1$.

Nous utilisons maintenant une spline quadratique

– **3)** Rappeler la défintion d'une spline qudaratique.

On note q_0 et q_1 les polynômes constituant la spline quadratique d'interpolation de P_0, P_1 et P_2

– **4)** Quelles sont les équations que doivent vérifier les polynômes q_i ?

Pour $i = 0, 1$, on pose $q_i(x) = a_i(x - x_i)^2 + b_i(x - x_i) + c_i$

– **5)** Quelles sont les équations que doivent satisfaire a_0, a_1, b_0, b_1, c_0 et c_1. ?

– **6)** Quel est le nombre d'équations ? d'inconnues ? combien manque t-il d'équations ?

– **7)** Calculer les valeurs $a_0, a_1, b_0, b_1, c_0, c_1$ puis les polynômes q_0 et q_1 en ajoutant la condition initiale $q_0'(x_0) = 0$.