Université Claude Bernard (Lyon-I)
École Normale Supérieure de Lyon
Magistère Informatique et Modélisation

Novembre 2001
Devoir en temps non limité.

Exercice

On rappelle qu'un *code linéaire* de *longueur* n, et de *dimension* r, sur le corps fini K, est un sous-espace vectoriel $\mathcal{C}$ de dimension r de l'espace vectoriel K^n. Une *matrice de contrôle* du code $\mathcal{C}$ est une matrice H telle que les éléments de $\mathcal{C}$ sont les vecteurs $X = (x_1, x_2, \ldots, x_n)$ qui vérifient l'équation matricielle

$$H\,{}^tX = 0$$

en notant ${}^tX$ la colonne transposée de la ligne X. Le *poids* d'un élément $c \in \mathcal{C}$ est le nombre des composantes non nulles de c. Le *poids minimal* du code $\mathcal{C}$ est le plus petit des poids des éléments non nuls de $\mathcal{C}$.

1. On note $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$. Quels sont les générateurs du groupe multiplicatif $\mathbb{F}_7^*$?

2. On considère le code linéaire $\mathcal{C}$ défini par sa matrice de contrôle H,

$$H = \begin{pmatrix} 1 & 3 & 3^2 & 3^3 & 3^4 & 3^5 \\ 1 & (3^2) & (3^2)^2 & (3^2)^3 & (3^2)^4 & (3^2)^5 \\ 1 & (3^3) & (3^3)^2 & (3^3)^3 & (3^3)^4 & (3^3)^5 \end{pmatrix}.$$

   (a) Calculer la matrice H, c'est à dire évaluer ses éléments dans $\mathbb{F}_7$.

   (b) Quelle est la dimension du code $\mathcal{C}$?

3. (a) Montrer que $\mathcal{C}$ est de poids minimal 4.

   (b) Montrer que que $\mathcal{C}$ corrige une erreur. Donner un algorithme corrigeant un message présentant une erreur.

   (c) Décoder le message $(5, 3, 5, 6, 0, 0)$ en supposant qu'il présente au plus une erreur.

4. Sachant qu'un message ne présente pas plus de deux erreurs, indiquer une condition nécessaire et suffisante simple pour qu'il contienne exactement deux erreurs. En déduire un algorithme qui, recevant un message comportant au plus deux erreurs, selon les cas,

   - Affirme que le message reçu ne comporte pas d'erreur.
   - Affirme que le message reçu présente une erreur et la corrige.
   - Affirme que le message reçu présente au moins deux erreurs.

Problème

Rappels et notations : p est un nombre premier impair, et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Si G est un polynôme de $\mathbb{F}_p[X]$, de degré d, la congruence modulo G dans $\mathbb{F}_p[X]$ est définie par

$$A \equiv B \pmod{G} \iff G \mid (A - B).$$

On note K_G l'ensemble des classes d'équivalence pour la congruence modulo G. On rappelle que K_G, muni des opérations définies par

$$\overline{A} + \overline{B} = \overline{A+B}, \qquad \overline{A} \cdot \overline{B} = \overline{A \cdot B}, \qquad \lambda\overline{A} = \overline{\lambda A}.$$

est une $\mathbb{F}_p$-algèbre, et que c'est un corps si et seulement si G est irréductible. Tout élément de K_G est la classe d'équivalence d'un unique polynôme de degré plus petit que d. Il en résulte que K_G est de cardinal p^d, car il y a p^d polynômes de degré plus petit que d. L'objet du problème est l'étude d'un algorithme donnant les facteurs irréductibles de degré d d'un polynôme F arbitraire dans $\mathbb{F}_p[X]$.

1. Soit K un corps fini de cardinal q. Montrer que tout élément non nul t de K vérifie $t^{\frac{q-1}{2}} = \pm 1$, et que cet élément t est un carré si et seulement si $t^{\frac{q-1}{2}} = 1$.

Dans la suite de ce problème, si G est un polynôme irréductible de degré d sur $\mathbb{F}_p$, $q = p^d$, et T un polynôme arbitraire dans $\mathbb{F}_p[X]$, on appelle *caractère quadratique de T modulo G,* et on note $\left(\dfrac{T}{G}\right)$, l'élément de $\{0, 1, -1\}$ défini par

$$\left(\frac{T}{G}\right) = \begin{cases} 0 & \text{si } G \,|\, T \\ +1 & \text{si } T^{\frac{q-1}{2}} \equiv +1 \pmod{G} \\ -1 & \text{si } T^{\frac{q-1}{2}} \equiv -1 \pmod{G}. \end{cases}$$

2. Soit F un polynôme de $\mathbb{F}_p[X]$ de degré n, sans racines multiples. On considère la procédure `Separedegres` définie par :

   `Separedegres(F)`

   `1)` $k := 0$, $H := F$;

   `2) Tant que` $\deg(H) > 0$ `et que` $k < n$ `faire`

   $\qquad k := k + 1$;

   $\qquad F_k := \mathrm{pgcd}(H, X^{p^k} - X)$;

   $\qquad H := H/F_k$;

   `3) renvoyer` $[F_1, F_2, \ldots, F_k]$

   Montrer que cette procédure renvoie la suite $(F_1, \ldots, F_k)$ définie par $F = F_1 \cdot F_2 \ldots F_k$, où chaque F_j est produit de polynômes irréductibles de degré j.

3. L'algorithme précédent ramène la factorisation d'un polynôme à celle d'un polynôme dont tous les facteurs irréductibles sont de degré d. Soit donc $F \in \mathbb{F}_p[X]$, un polynôme dont tous les facteurs irréductibles sont de même degré d, et deux à deux distincts. Notons $q = p^d$. Soit T un polynôme de $\mathbb{F}_p[X]$. Démontrer que F divise le polynôme $T^q - T$. En déduire la factorisation

   $$F = ABC$$

   avec

   $$A = (F, T), \qquad B = (F, T^{\frac{q-1}{2}} - 1), \qquad C = (F, T^{\frac{q-1}{2}} - 1),$$

   qui conduit à l'algorithme probabiliste suivant, pour factoriser F :

```
1) Choisir $T$ au hasard dans $\mathbb{F}_p[X]$.

2) Calculer $A = (F,T)$, $B = (F,T^{\frac{q-1}{2}} - 1)$, $C = (F,T^{\frac{q-1}{2}} + 1)$.

3) Si deux des polynômes $A, B, C$ sont des constantes,
l'algorithme a échoué.  Sinon on a obtenu une factorisation
non triviale de $F$.
```

Ecrire la procédure Maple `FactoriseAvec(F,X,p,d,T)` qui effectue les parties 2 et 3 de l'algorithme ci-dessus, avec le polynôme T choisi.

4. Soit F un polynôme qui est le produit $F = G_1 G_2$ de deux facteurs irréductibles de degré d. On applique l'algorithme précédent en choisissant au hasard, avec la probabilité uniforme, un polynôme T de degré strictement plus petit que $2d = \deg(F)$. On veut déterminer la probabilité de succès de l'appel `FactoriseAvec(F,X,p,d,T)`.

   (a) Montrer que se donner le polynôme T de degré $< 2d$, équivaut à se donner T_1 et T_2 les restes respectifs de la division de T par G_1 et G_2.

   (b) Montrer que l'algorithme réussit si :
   - Ou bien l'un des deux polynômes T_1, T_2 est nul, mais pas l'autre.
   - Ou bien $T_1 T_2 \neq 0$ et $\left(\dfrac{T}{G_1}\right) = -\left(\dfrac{T}{G_2}\right)$.

   (c) En déduire que la probabilité de succès est $\dfrac{1}{2} + \dfrac{1}{q} - \dfrac{3}{2q^2}$.

5. (a) L'expérience sur des polynômes F de petit degré montre que l'appel `FactoriseAvec(F,X,p,d,T)` réussit souvent en choisissant pour T un polynôme de degré 1. On se propose dans cette question de montrer que cela n'est pas toujours vrai. Soit I_d^p le nombre des polynômes irréductibles unitaires de degré d sur $\mathbb{F}_p[X]$. Montrer que si $d \geq 2$ et $I_d^p > 2^p$, il existe un polynôme F qui est le produit de deux facteurs irréductibles de degré d et tel que, pour tout polynôme T de degré 1, l'appel `FactoriseAvec(F,X,p,d,T)` échoue. Indication : on pourra considérer l'application φ définie sur l'ensemble des polynômes irréductibles de degré d définie par

   $$G \mapsto \varphi(G) = (a_0, a_1, \ldots, a_{p-1}), \qquad a_i = \left(\frac{X+i}{G}\right).$$

   (b) Montrer que si $p = 3$, il existe un polynôme F de degré 8 tel que l'appel `FactoriseAvec(F,X,3,4,T)` échoue pour tout polynôme T de degré 1.

6. La méthode de factorisation étudiée dans les questions précédentes suppose que le nombre premier p est impair. On se propose ici de l'adapter au cas $p = 2$.

   (a) Soit K un corps de caractéristique 2, et de cardinal $q = 2^d$. Soit t un élément de K. On pose
   $$s = t + t^2 + t^4 + \ldots t^{2^{d-1}}.$$
   Montrer que $s^2 = s$, et en déduire que $s \in \mathbb{F}_2$.

   (b) Soit G est un polynôme irréductible de degré d dans $\mathbb{F}_2[X]$, et T un polynôme arbitraire dans $\mathbb{F}_2[X]$. Montrer que

   $$G \mid (T + T^2 + \ldots + T^{2^{d-1}})(1 + T + T^2 + \ldots + T^{2^{d-1}}).$$

   (c) En déduire un algorithme probabiliste, analogue à celui décrit dans la question 3, qui factorise un polynôme $F \in \mathbb{F}_2[X]$.