Calcul Formel - DM

Laure Danthony

Pour le 16 novembre 2001

Codes correcteurs, algorithmes de factorisation dans $\mathbb{F}_q[X]$.

Exercice : codes

On considère ici un code construit à partir de $\mathbb{F}_7$ qui va permettre de corriger une erreur ou de détecter deux erreurs.

1. Dans $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, on vérifie en calculant les puissances successives des éléments $1, 2, 3, 4, 5, 6$ que 3 et 5 sont :
   - des générateurs,
   - les seuls générateurs (car on sait que $(\mathbb{F}_7^*, \times) \simeq (\mathbb{Z}/6\mathbb{Z}, +)$ qui a $\varphi(6) = 2$ générateurs).
2. (a) On obtient en calculant les puissances dans $\mathbb{F}_7$:

$$H = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{pmatrix}$$

   (b) Les éléments du code $\mathcal{C}$ sont les vecteurs $(x_1, \dots x_7)$ vérifiant l'équation matricielle $H\,{}^tX$. Donc $\mathcal{C} = \mathrm{Ker}\,(H)$. Or $\dim(\mathrm{Ker}\,(H)) = 7 - \mathrm{rg}(H)$ d'après le théorème du rang. De plus, la première sous-matrice extraite $3 * 3$ de H a pour déterminant $2 - 24 - (3 - 12) + (12 - 4) = 2 \neq 0$ donc le rang est 3 d'où la dimension du code est de 4.
3. (c) Montrons que le code $\mathcal{C}$ est de poids minimal 4. Pour cela, on va montrer :
   - Il existe X élément du code dont le poids est 4.
   - Tous les autres éléments du code ont un poids inférieur ou égal à 4, *i.e.* il n'existe pas d'élément de poids 0, 1, 2 ou 3.

   On va tout d'abord expliciter les éléments de $\mathcal{C}$:

$$X \in \mathcal{C} \Leftrightarrow \begin{cases} x_1 + 3x_2 + 2x_3 + 6x_4 + 4x_5 + 5x_6 = 0 \\ x_1 + 2x_2 + 4x_3 + x_4 + 2x_5 + 4x_6 = 0 \\ x_1 + 6x_2 + x_3 + 6x_4 + x_5 + 6x_6 = 0 \end{cases}$$

   En appliquant les opérations de Gauss, et en réduisant dans $\mathbb{F}_7$, on

obtient l'équivalence :

$$X \in \mathcal{C} \Leftrightarrow \begin{cases} x_1 = 6x_4 + 3x_5 + x_6 \\ x_2 = x_4 + 3x_5 + 4x_6 \\ x_3 = 3x_4 + 6x_5 + 6x_6 \end{cases},$$

ce qui refournit le résultat précédent concernant le rang. On obtient en plus une base de $\mathcal{C}$: si l'on note $c_1 = (6, 3, 1, 1, 0, 0)$, $c_2 = (1, 3, 4, 0, 1, 0)$ et $c_3 = (3, 6, 6, 0, 0, 1)$, alors (c_1, c_2, c_3) forment une base de $\mathcal{C}$. En particulier, c_1 élément de $\mathcal{C}$ est de poids 4 (il a 2 zéros). Il ne reste plus qu'à montrer que les éléments de $\mathcal{C}$ ne peuvent être de poids 0, 1, 2 ou 3.

Pour cela prouvons d'abord le :

LEMME 1 *Dans la matrice H, si on prend un triplet quelconque de colonnes distinctes : (c_i, c_j, c_k), alors (c_i, c_j, c_k) forme une famille libre de $\mathcal{C}$.*

PREUVE : Il s'agit de calculer le déterminant suivant :

$$\begin{pmatrix} 3^i & 3^j & 3^k \\ 3^{2i} & 3^{2j} & 3^{2k} \\ 3^{3i} & 3^{3j} & 3^{3k} \end{pmatrix} = 3^{i+j+k} \begin{pmatrix} 1 & 1 & 1 \\ 3^i & 3^j & 3^k \\ (3^i)^2 & (3^j)^2 & (3^k)^2 \end{pmatrix}$$

Comme $3^i \neq 3^j \neq 3^k$ (3 est générateur de $\mathbb{F}_7$), le déterminant de Van der Monde est non nul, d'où le résultat. ■

Revenons à nos moutons : supposons qu'il existe un élément X de poids 3. Alors 3 des composantes de X sont non nulles, disons $x_{i'}, x_{j'}$, et $x_{k'}$. Les trois autres composantes de X sont nulles et sont notées x_i, x_j, x_k. Si $X \in \mathcal{C}$, alors $H\,{}^tX = 0$ ce qui équivaut d'après les résultats précédents à $H'\,{}^tX' = 0$, avec $H' = (c_{i'}|c_{j'}|c_{k'})$. Or H est inversible d'après le lemme, donc $X = 0$: absurde. On a bien montré que $\mathcal{C}$ est de poids minimal 4.

(b) Supposons que le message reçu X' comporte une erreur, *i.e.* $X' = X + E$ où $E = (0, 0, \alpha, 0, 0, 0)$, α se situant à la i-ème place qu'il s'agit de déterminer. Alors le receveur calcule le syndrome $S = H\,{}^tX' = H\,{}^tE$. Ce résultat est de la forme αc_i si c_i désigne la i-ème colonne de la matrice H. Le receveur à l'aide de S et de H détermine alors facilement le couple (i, α) et peut ainsi reconstituer le message initial. Comme les colonnes de la matrice H ne sont pas colinéaires deux à deux, la colonne c_i est bien déterminée de manière unique. Ainsi $\mathcal{C}$ corrige une erreur et l'algorithme précédent permet de corriger une éventuelle erreur.

(c) Application à $X' = (5, 3, 5, 6, 0, 0)$. Alors $S = \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix} = 1.c_5$ donc le message initial était $X = (5, 3, 5, 6, \mathbf{6}, 0)$.

4. Si on sait que le message a au plus deux erreurs, le message contient deux erreurs ssi le syndrome n'est pas de la forme αc_i où c_i est une colonne de H. Le receveur calcule donc le syndrome S :

– si S est une matrice-colonne nulle, alors le message ne comporte pas d'erreur,
– si S est de la forme αc_i, on sait qu'il y a une erreur et on décode selon l'algorithme précédent,
– sinon, on affirme que le message contient au moins 2 erreurs.

Notons que l'on ne peut corriger deux erreurs si elles existent du fait du poids minimal 4 : le mot $(6,3,0,0,0,0)$ est à distance 2 de au moins 2 mots du code : $(0,0,0,0,0,0)$ et $(6,3,1,1,0,0)$, donc pour ce mot on ne pourra déterminer les deux erreurs.

5. La taille du no-man's land est $7^6 - 7^3(1+6.6) \simeq \frac{6}{7}7^6$. 7^6 est le nombre d'éléments, 7^3 le nombre de boules de $\mathcal{C}$ de rayon 1 , chaque sphère ayant pour cardinal 6.6 (pour obtenir un mot à distance 1 d'un certain mot, on choisit la place du changement, et on met un élément différent dans cette case).

Factorisation de polynômes dans $\mathbb{F}_q[X]$

On considère ici p premier, $p > 2$

1. *On se place ici dans $\mathbb{F}_q$, q quelconque* Soit $x \in K^*$. Alors $x^{q-1} = 1$ (l'ordre de x dans le groupe $(\mathbb{F}_q^*, \times)$ divise $q-1$). Donc $x^{\frac{q-1}{2}}$ est racine de $X^2-1 = (X-1)(X+1)$. Comme on est dans un corps, les seules racines de ce polynôme sont 1 et -1.
   - Si x est un carré, $x = a^2$ donc $x^{\frac{q-1}{2}} = a^{q-1} = 1$.
   - Le polynôme $X^{\frac{q-1}{2}} - 1$ admet au plus $\frac{q-1}{2}$ racines (on est dans un corps) donc il existe un élément $x_0 \neq 0$ de $\mathbb{F}_q$ vérifiant $x_0^{\frac{q-1}{2}} = -1$. Soit E l'ensemble des x vérifiant $x^{\frac{q-1}{2}} = 1$ et F son complémentaire dans $\mathbb{F}_q$, c'est-à-dire $\{x | x^{\frac{q-1}{2}} = -1\}$. Alors l'application $\varphi : E \to F, x \mapsto xx_0$ est bijective (en effet si $\varphi(y_1) = \varphi(y_2)$, alors en divisant par $x_0 \neq 0$ - on est dans un corps - on obtient $y_1 = y_2$, pour la surjection si $x \in F$ s'écrit $y.x_0$ avec $y \in E$). Donc on obtient $Card(E) = Card(F)$.
   - Comme il y a au plus $\frac{q-1}{2}$ éléments vérifiant $t^{\frac{q-1}{2}} = 1$, on a au plus $\frac{q-1}{2}$ carrés. Considérons $f : \mathbb{F}_q^* \to \mathbb{F}_q^*, x \mapsto x^2$. Alors soit $y \in f(\mathbb{F}_q^*)$ alors $f = x^2 = (-x)^2$ donc y admet exactement 2 antécédents.
   - Finalement, le nombre de carrés est **exactement** $\frac{q-1}{2}$, et comme ils sont inclus dans l'ensemble E de cardinal $\frac{q-1}{2}$ d'après précédemment, ils forment exectement cet ensemble. Donc F est l'ensemble des éléments de F_q^* qui ne sont pas des carrés. On a bien obtenu que si $x \in K$ n'est pas un carré, alors $x^{\frac{q-1}{2}} = -1$.
2. D'après le cours, le polynôme $X^{p^k} - X$ est le produit de tous les polynômes irréductibles de degrés $\leq k$ dans $\mathbb{F}_p$. D'où :
   - Au premier tour de boucle, F_1 devient le pgcd des polynômes F et $X^p - X$. Donc F_1 contient tous les facteurs de F de degré 1,
   - Ensuite, $H := H/F_1$ ne possède plus de facteurs de degré 1.
   - Donc au deuxième tour de boucle, $F_2 = pgcd(H, X^{p^2} - X)$ contient tous

les facteurs de F de degré 2.

- En divisant : $H := H/F_2$, H ne possède plus de facteurs de degrés ≤ 2.
- *etc.*
- Ainsi, à chaque tour de boucle j , on fait en sorte que F_j contienne tous les facteurs irréductibles de F de degré **exactement** j.
- Remarquons que l'algorithme termine puisque la boucle while s'arrête au pire lorsque k vaut $n-1$. A ce moment là, comme F est de degré n, on obtient tous les facteurs irréductibles de F regroupés par degré.

On s'intéresse maintenant à la factorisation d'un polynôme dont tous les facteurs irréductibles sont de degré connu d. On pose dans la suite $q = p^d$

3. • Montrons que $F|T^{p^d} - T$: écrivons $T = \sum t_i X^i$ et donc

$$T^q - T = \big(\sum t_i X^i\big)^q - \big(\sum t_i X^i\big)$$

Comme $t_i^q = t_i$ (on se place dans $\mathbb{F}_p$), et comme $\forall k \in [\![1, p^n-1]\!],\ p^n | \mathrm{C}_{p^n}^k$ (voir plus loin), on a :

$$T^q - T = \sum t_i (X^q)^i - \sum t_i X^i = \sum t_i \big((X^q)^i - X^i\big)$$

Comme $X^{qi} - X^i = (X^q - X)B$, chaque terme de la somme divise $(X^q - X)$, et finalement $T^q - T = (X^q - X)Q$ et donc $F|T^q - T$.

Démontrons tout de même le résultat utilisé dans la preuve précédente, à savoir $\forall k \in [\![1, p^n-1]\!], p^n | \mathrm{C}_{p^n}^k$: de la formule $X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$ on déduit par translation :

$$(X+1)^{p^n} - (X+1) = \prod_{\alpha \in \mathbb{F}_q} (X + 1 - \alpha).$$

En posant $\beta = \alpha - 1$, β parcourt tout $\mathbb{F}_p$, et donc :

$$(X+1)^{p^n} - (X+1) = \prod_{\beta \in \mathbb{F}_q} (X + \beta) = X^{p^n} - X.$$

Alors $(X+1)^{p^n} = X^{p^n} + 1$ et le résultat sur les $\mathrm{C}_{p^n}^k$.

- On a montré juste avant que $T^q - T = QF$ d'où :

$$T\big(T^{\frac{q-1}{2}} - 1\big)\big(T^{\frac{q-1}{2}} + 1\big) = QF.$$

De plus, T, $T^{\frac{q-1}{2}} - 1$ et $T^{\frac{q-1}{2}} + 1$ sont premiers entre eux deux à deux (si on prend deux de ces polynômes, et un polynome I qui les divise, alors I divise un polynôme constant par soustraction). Donc les facteurs irréductibles de F sont partitionnés en les facteurs irréductibles de A, de B et de C. Finalement $F = ABC$.

- La procédure MAPLE fournie dans la feuille annexe réalise l'algorithme donné dans l'énoncé, F ayant été préalablement choisi. Il peut donc retourner `'echec'` si 2 des polynômes A, B ou C sont des constantes.

4. **Calcul de la probabilité de succès de la procédure précédente** pour $F = G_1G_2$, G_1, G_2 étant deux polynômes irréductibles de degré d.
   (a) Considérons l'application $\varphi : \mathbb{F}_{2d-1}[X] \to \mathbb{F}_{d-1}[X] \times \mathbb{F}_{d-1}[X]$ définie par $\varphi(T) = (T \ mod \ G_1, T \ mod \ G_2)$. Elle est clairement linéaire. Elle est injective : soit T vérifiant $\varphi(T) = (0, 0)$, alors $G_1|T$ et $G_2|T$, comme G_1 et G_2 sont premiers entre eux, $deg(G_1G_2) = 2d$, et comme $deg(T) < 2d$, $T = 0$. Les ensembles mis en jeu ayant même cardinal, on en déduit que φ est bijective. D'où l'équivalence demandée.

   (b) **Remarque : au vu de la question suivante, on va démontrer un "si et seulement si", c'est-à-dire regarder tous les cas possibles.** Cas possibles :
   - Si $T_1 = T_2 = 0$, alors G_1G_2 divise T, ce qui est impossible pour des questions de degrés.
   - Si $T_1T_2 \neq 0$ et $\left(\frac{T}{G_1}\right) = -\left(\frac{T}{G_2}\right)$, alors $G_1|B$ et $G_2|C$ et donc l'algorithme réussit.
   - Si $T_1T_2 \neq 0$ et $\left(\frac{T}{G_1}\right) = \left(\frac{T}{G_2}\right)$, alors G_1 et G_2 divisent B, donc $B = F$, donc $A = C = 1$ et l'algorithme échoue.
   - Si $T_1 = 0, T_2 \neq 0$, alors $G_1|A$ mais pas $G_2.F$ se décompose alors en $A = G_1$, $BC = G_2$ et l'algorithme réussit.
   - le dernier cas est similaire au précédent.

   (c) D'où la probabilité de succès : on compte tout d'abord le nombre de polynômes distincts de $\mathbb{F}_{d-1}[X]$, il y en a p^d (il y a p choix pour chaque coefficient).
   – "l'un des deux polynômes T_1 ou T_2 est nul, mais pas l'autre" : il y a $p^d - 1$ polynômes non nuls dans $\mathbb{F}_{d-1}[X]$ d'où une probabilité $\frac{2}{p^d} - \frac{2}{p^{2d}}$.
   – "$T_1T_2 \neq 0$ et $\left(\frac{T}{G_1}\right) = -\left(\frac{T}{G_2}\right)$". Or la probabilité d'obtenir $\left(\frac{T}{G_1}\right) = -\left(\frac{T}{G_2}\right)$ est égale à $\frac{1}{2}$ (voir plus loin), d'où une probabilité pour cet événement : $\frac{(p^d-1)(p^d-1)}{p^{2d}} \cdot \frac{1}{2}$.

   Montrons maintenant que la probabilité d'avoir $\left(\frac{T}{G_1}\right) = -\left(\frac{T}{G_2}\right)$ est égale à $\frac{1}{2}$: comme $T_1T_2 \neq 0$, $\left(\frac{T}{G_1}\right) = \left(\frac{T_1}{G_1}\right) \in \{-1, 1\}$. Montrons que chacune des deux valeurs a une probabilité $\frac{1}{2}$ d'apparaître si on choisit T_1 au hasard dans $\mathbb{F}_{d-1}[X]$. Pour cela, prenons $\alpha \in \mathbb{K}$; $\alpha^{\frac{q-1}{2}} = -1$. Alors $\left(\frac{T_1}{G_1}\right) = 1 \Leftrightarrow \left(\frac{\alpha T_1}{G_1}\right) = -1$ et $T \to \alpha T$ réalise une bijection de $\{T \mid \left(\frac{T}{G_1}\right) = 1\}$ sur $\{T \mid \left(\frac{T}{G_1}\right) = -1\}$, d'où l'équiprobabilité voulue.

   Au total, on a bien la probabilité voulue :

$$p_{succes} = \frac{1}{2} + \frac{1}{q} - \frac{3}{2q^2}$$

5. **Echecs de l'algorithme pour T de degré 1 :**

   (a) Considérons l'application $\varphi : I_d^p \to \{-1,0,1\}^p$ définie par $\varphi(G) = (a_0, \dots a_{p-1})$ où $a_i = \left(\frac{X+i}{G}\right)$. Montrons qu'il existe G_1 et G_2 tels que quel que soit T de degré 1, $T_1T_2 \neq 0$ et $\left(\frac{T}{G_1}\right) = \left(\frac{T}{G_2}\right)$.

   - Tout d'abord, $deg(G) \geq 2$ donc G ne divise aucun des $(X+i)$ donc $\forall i, a_i \neq 0$.
   - Comme $Card(I_d^p) > 2^p$ et $Card(\{-1,1\}) = 2^p$, il s'ensuit que l'application φ n'est pas injective, donc il existe des polynômes G_1 et G_2 irréductibles vérifiant $\varphi(G_1) = \varphi(G_2)$.
   - Il ne reste plus qu'à montrer que l'algorithme `FactoriseAvec` appliqué à $F = G_1G_2$ va échouer dans le cas d'erreur $T_1T_2 \neq 0$ et $\left(\frac{T}{G_1}\right) = \left(\frac{T}{G_2}\right)$. Comme $\varphi(G_1) = \varphi(G_2)$, on a :

     $$\forall i \in [\![0, p-1]\!], \left(\frac{X+i}{G_1}\right) = \left(\frac{X+i}{G_2}\right) \neq 0.$$

     Or si T est de degré 1, $T = X - i$ pour un certain i. Alors on a $\left(\frac{T}{G_1}\right) = \left(\frac{T}{G_2}\right)$ et $T_1 = T_2 = T \neq 0$ et l'algorithme échoue pour T de degré 1.

   (b) On applique la proposition précédente, sachant que d'après le cours $I_8^3 \geq \frac{1}{8}(3^8 - 2.3^4) > 9 > 2^3$. D'où le résultat.

On considère maintenant $p = 2$

6. Dans cette question, on prend $\mathbb{K}$ un corps de caractéristique 2, et de cardinal $q = 2^d$.

   (a) La quantité $s^2 = \left(t + t^2 + t^4 + \dots t^{2^{d-1}}\right)^2 = t^2 + t^4 + t^8 + \dots + t^{2^{d-1}} + t^{2^d}$ (les doubles produits sont nuls). Comme de plus, $t^{2^d} = t$ (corps de cardinal q), on obtient donc $s^2 = s$, soit encore $s(s-1) = 0$, ce qui signifie $s = 0$ ou $s = 1$ car on est dans un corps. Donc $s \in F_2$.

   (b) Montrons que $G | (T + T^2 + \dots + T^{2^{d-1}})(1 + T + T^2 + T^4 + \dots T^{2^{d-1}})$. Notons S la quantité $T + T^2 + T^4 + \dots + T^{2^{d-1}}$. Par des calculs similaires à la questions précédente dans le corps de caractéristique 2, on obtient

   $$S(1+S) = S + S^2 = S + \left(T^2 + T^4 + \dots + T^{2^d}\right) = S + \left(S + T^{2^d} - T\right) = T^{2^d} - T.$$

   Des calculs similaires à la question 3, sachant que le polynôme $X^{2^d} - X$ contient tous les facteurs irréductibles de degré inférieur ou égal à d dans $\mathbb{F}_2[X]$, montrent que G de degré d divise $T^{2^d} - T$.

   (c) **Un algorithme probabiliste pour factoriser un polynôme F dans $\mathbb{F}_2[X]$:**

   - On montre que si F est produit de polynômes irréductibles de degré d dans $\mathbb{F}_2[X]$, F se factorise en ABC où $A = (F, T)$, $B = (F, 1 + T + T^3 + \dots T^{2^{d-1}-1})$ et $C = (F, 1 + T + T^2 + T^4 + \dots T^{2^{d-1}})$ de manière similaire à la question 3.

- *D'où un algorithme probabiliste :* dans un premier temps, on sépare les facteurs irréductibles F_i selon leur degré i, et on traite le cas des facteurs irréductibles multiples en utilisant le fait que si P a un facteur de multiplicité 2, alors (P, P') contient ce même facteur, mais de multiplicité 1. Enfin, on applique pour chacun des polynômes obtenus l'alorithme suivant N fois :
  1 Choisir T au hasard dans $\mathbb{F}_2[X]$.
  2 Calculer A, B et C.
  3 Si deux des polynômes A, B, C sont constants, on renvoie `'echec'`. Sinon on a obtenu une factorisation non triviale de F_i.

  Si on tombe sur "échec", on recommence un essai de factorisation avec un autre polynôme de $\mathbb{F}_2[X]$ pris au hasard. Pour N assez grand, la probabilité de succès pour la factorisation tend vers 1. Et en pratique, $N = 20$ semble raisonnable.