15 juin 2022
Master 1 M.F., Orsay

Corrigé de l'examen de M.A.O. Calcul Formel

Le but du problème est d'étudier le code de Fire, introduit en 1959 par Philip Fire et utilisé à un moment dans les disques durs. Il permet de corriger efficacement des erreurs en rafale, c'est-à-dire des erreurs assez nombreuses mais portant sur des bits plus ou moins consécutifs.

Exercice : ombre portée par un ruban

1. Étant donné un point de coordonnées $(x_0, y_0, 0)$, le rayon lumineux qui provient du soleil et éclaire ce point est la droite passant par ce point ayant $(1, 2, 1)$ pour vecteur directeur. Il a pour équations paramétriques : $x = x_0 + t$, $y = y_0 + 2t$, $z = t$. En remplaçant x, y et z par ces valeurs dans les équations du ruban, on trouve $P(t) = 0$ et $Q(t) = 0$. La condition pour être dans l'ombre est que ce rayon passe par un point du ruban, c'est-à-dire qu'il existe $t \in \mathbb{R}$ tel que $P(t) = Q(t) = 0$.

   ```
   A.<x,y,z,t> = PolynomialRing(QQ)
   f=(x-2)^2+(y-1)^2+(z-10)^2-50
   g=(x+5)^2+(y+2)^2+(z-8)^2-30
   f.substitute(x=x+t,y=y+2*t,z=t).polynomial(t)
   g.substitute(x=x+t,y=y+2*t,z=t).polynomial(t)
   ```

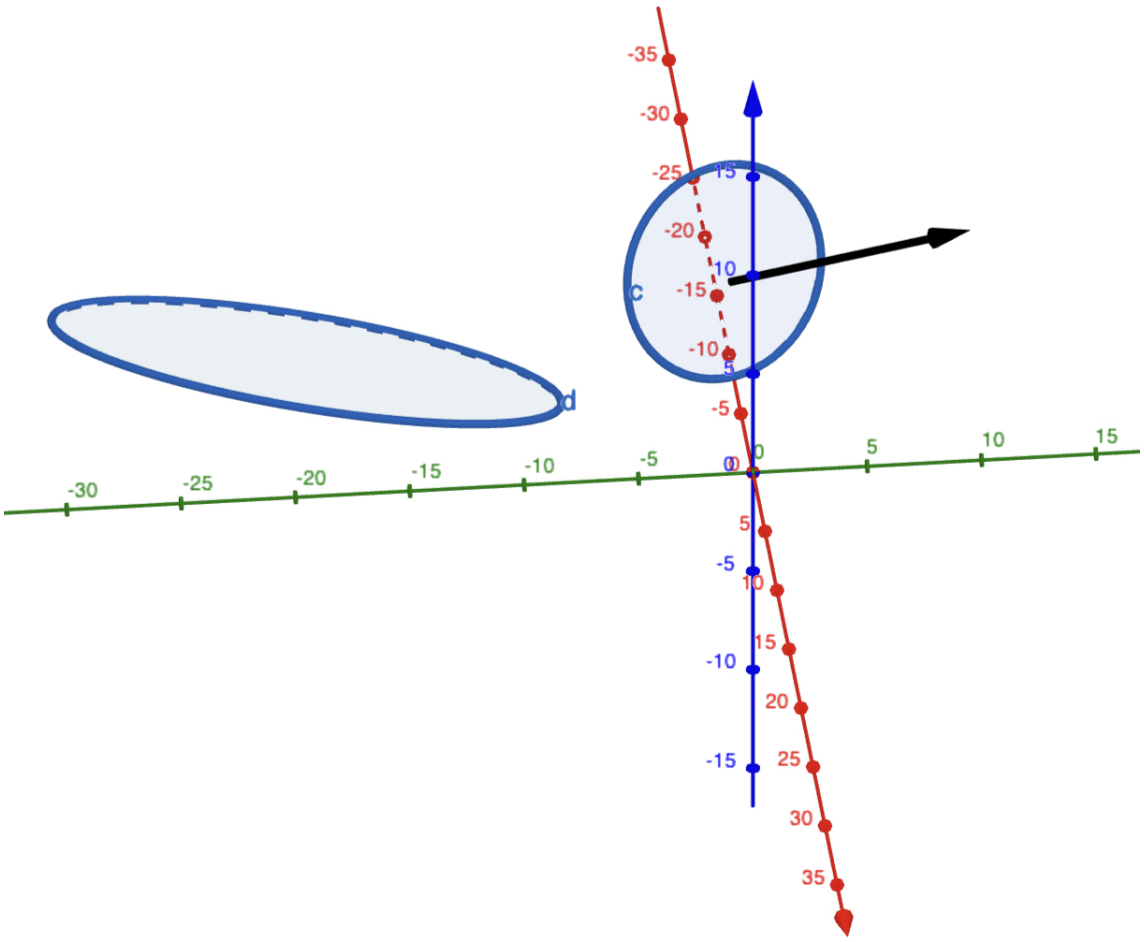
2. On a $P(T) - Q(T) = -14X - 6Y - 30T - 8$. S'il existe $t \in \mathbb{C}$ tel que $P(t) = Q(t) = 0$, alors $(P - Q)(t) = 0$ donc $t = \frac{-1}{30}(14x + 6y + 8) \in \mathbb{R}$ puisque $x, y \in \mathbb{R}$.
3. Posons $P(X, Y, T) = 6T^2 + (2X + 4Y - 28)T + X^2 + Y^2 - 4X - 2Y + 55$ et $Q(X, Y, T) = 6T^2 + (2X + 4Y + 2)T + X^2 + Y^2 + 10X + 4Y + 63$, et notons $R \in \mathbb{Q}[X, Y]$ le résultant de $P(X, Y, T)$ et $Q(X, Y, T)$ vus dans $(\mathbb{Q}[X, Y])[T]$. Soit $(x, y) \in \mathbb{R}^2$. Alors les polynômes $P(x, y, T)$ et $Q(x, y, T)$ obtenus en évaluant X et Y en x et y sont de degré 2 en T, comme $P(X, Y, T)$ et $Q(X, Y, T)$. Donc $R(x, y) \in \mathbb{R}$ est le résultant des polynômes $P(x, y, T)$ et $Q(x, y, T)$ qui appartiennent à $\mathbb{R}[X]$. Ce résultant est nul si, et seulement si, ces polynômes ont une racine commune dans $\mathbb{C}$, puisqu'ils sont scindés sur $\mathbb{C}$. D'après la question 2 cela signifie que le point $(x, y, 0)$ est dans l'ombre du ruban.
4. ($\star$)

   ```
   P.resultant(Q,t)
   ```

   On obtient

   $$R(X, Y) = 7416X^2 - 6192XY + 2376Y^2 + 54144X + 17136Y + 339624$$

   et $R(0, 0) = 339624$. En particulier, l'origine n'appartient pas à l'ombre portée ! On obtient le dessin suivant (qui n'était pas demandé !).


-35
-30
-25
-20
-15
-10
-5
5
10
15
c
d
-30
-25
-20
-15
-10
-5
5
10
15
-5
-10
-15
5
10
15
20
25
30
35

Problème

Partie 1 : Erreurs en rafale

1. Pour $e = 00101100100$ on a $\ell_e(2) = 7$ car $e_9 = e_{10} = e_{11} = e_{12} = 0$, puisque $n = 11$ et $e_0 = e_1 = 0$. On en déduit $r(e) \leq 7$. Pour $e = 11000001010$ on a $r(e) \leq \ell_e(7) = 6$ car $e_{13} = \cdots = e_{17} = 0$ puisque $n = 11$ et $e_2 = \cdots = e_6 = 0$.
2. Soit $e \in \mathbb{F}_2^n$. L'égalilté $r(e) = 0$ signifie que $\ell_e(j) = 0$ pour au moins une valeur de j, i.e. $e_j = e_{j+1} = \cdots = e_{j+n-1} = 0$. Comme la suite $(e_0, \ldots, e_{n-1})$ a été prolongée par périodicité, cela signifie $e = 0$. A l'inverse, $r(e) = n$ signifie $\ell_e(j) = n$ pour tout j, i.e. $e_{j+n-1} = 1$: cela équivaut à $e = (1, 1, \ldots, 1)$.
3. Si on ne pense pas directement à l'algorithme de la question suivante, on peut procéder comme suit. Pour chaque $j \in [\![0, n-1]\!]$, on initialise un compteur s à la valeur $n-1$. Tant que $s \geq 0$ et $e_{j+s} = 0$, on remplace s par $s - 1$. A la sortie de cette boucle `tant que`, on a $\ell_e(j) = s + 1$. Puis on met à jour le record de la plus petite valeur obtenue : si ce record (initialisé à n) est strictement plus grand que $s + 1$, on le remplace par $s + 1$. Quand on sort de la boucle sur j, la variable `record` contient la valeur de $r(e)$.

   Pour chaque valeur de j, cet algorithme évalue e_{j+s} pour n valeurs de s dans le pire des cas (celui où $e = 0$). Comme j varie de 0 à $n - 1$, on utilise donc n^2 accès au vecteur e. Il faut éventuellement en ajouter n, ce qui est négligeable, si on allonge préalablement le vecteur e en posant $e_n = e_0$, ..., $e_{2n-1} = e_{n-1}$. Une autre méthode pour pouvoir évaluer e_{j+s} consiste à noter λ le reste dans la division euclidienne de $j + s$ par n, et à considérer e_λ. Enfin on peut aussi trouver λ en distinguant le cas où $j + s \leq n - 1$ (qui donne $\lambda = j + s$) du cas où $n \leq j + s \leq 2n - 1$ (qui donne $\lambda = j + s - n$).
4. Ce coût minimal imaginable est de n accès au vecteur e : il faut bien lire les n bits de e. Pour obtenir ce coût, on peut déterminer la longueur N de la plus longue plage de zéros dans le mot e (prolongé par périodicité) ; on a alors $r(e) = n - N$. On peut le faire de la façon suivante (voir la question 5 pour une implémentation). On parcourt une seule fois le vecteur e, de e_0 à e_{n-1}, en déterminant la longueur $N_d \geq 0$ de la plage de zéros (éventuellement vide) qui commence à e_0, puis la longueur N_i de chaque plage intermédiaire de zéros entre deux 1 consécutifs (on mémorise la plus grande valeur prise par N_i), et enfin la longueur $N_f \geq 0$ de la plage de zéros (éventuellement vide) qui se termine par e_{n-1}. Alors N est le plus grand entre $N_d + N_f$ et la plus grande valeur prise par N_i.
5. ($\star$) Voir le Notebook !
6. ($\star$) On retrouve bien les valeurs attendues.
7. ($\star$) On obtient $r(e) = 84$.

Partie 2 : Détection et correction d'erreurs en rafale

8. Notons c le message envoyé, r le message reçu, et $e = r - c$ l'erreur. On suppose que t erreurs en rafale (au maximum) ont été commises, c'est-à-dire que $r(e) \leq t$, et que $e \neq 0$. En utilisant C on peut détecter ce problème si on est sûr d'avoir $r = c + e \notin C$.

Comme C est linéaire, cela équivaut à $e \notin C$. La condition qui apparaît, i.e. $e \notin C$ pour tout $e \neq 0$ tel que $r(e) \leq t$, est bien celle de l'énoncé.

Le code C permet de corriger t erreurs en rafale si pour tous $c' \in C$ et $e' \in \mathbb{F}_2^n$ tels que $r(e') \leq t$ et $e' + c' = e + c$, on a $e' = e$ (c'est-à-dire $c' = c$). Par linéarité cela signifie que pour tous $e, e' \in \mathbb{F}_2^n$, les conditions $r(e) \leq t$, $r(e') \leq t$ et $e' - e \in C$ impliquent $e = e'$. Étant donné que $e' - e = e' + e$ en caractéristique 2, c'est bien la condition de l'énoncé.

9. Soit $c \in C \cap (\mathbb{F}_2^t \times \{0\}^{n-t})$; supposons $c \neq 0$. Comme C détecte t erreurs en rafale, on a $r(c) > t$. Or $c_t = c_{t+1} = \cdots = c_{n-1} = 0$, donc $\ell_c(0) \leq t$. On a donc $r(c) \leq \ell_c(0) \leq t < r(c)$, ce qui est contradictoire. Donc C est en somme directe avec $\mathbb{F}_2^t \times \{0\}^{n-t}$, d'où $\dim C + \dim(\mathbb{F}_2^t \times \{0\}^{n-t}) \leq \dim \mathbb{F}_2^n = n$, ce qui donne $t \leq n - k$.

10. Supposons que C est cyclique, et qu'il existe $c = (c_0, \ldots, c_{n-1}) \in C \setminus \{0\}$ tel que $r(c) \leq n - k$. Comme C est invariant par l'application qui à $(x_0, \ldots, x_{n-1})$ associe $(x_1, \ldots, x_{n-1}, x_0)$, on peut supposer que $\ell_c(k) = r(c) \leq n-k$ d'où $c_n = \cdots = c_{n+k-1} = 0$, c'est-à-dire $c_0 = c_1 = \cdots = c_{k-1} = 0$. En identifiant $c = (c_0, \ldots, c_{n-1})$ au polynôme $c_0 X^{n-1} + \cdots + c_{n-2} X + c_{n-1} \in \mathbb{F}_2[X]/(X^n - 1)$, on obtient un polynôme $S(X) \in C$ non nul tel que $\deg S \leq n - k - 1$. Or on sait que C possède un polynôme générateur g de degré $n - k$, et qu'une base de C est donnée par les polynômes g, Xg, …, $X^{k-1}g$ (qui appartiennent à $\mathbb{F}_2[X]_{<n} \simeq \mathbb{F}_2[X]/(X^n - 1)$). L'existence de $S(X) \in C$ non nul tel que $\deg S \leq n - k - 1$ est donc contradictoire.

11. On peut penser à un CD rayé : les bits correspondants à la rayure peuvent être des bits successifs. De même pour un QR code imprimé sur papier qui a été plié ou raturé. Dans une communication (notamment spatiale), on peut imaginer une interruption ou une perturbation temporaire. Dans tous ces cas, et dans beaucoup d'autres, t bits consécutifs ont une grande probabilité d'avoir été mal transmis, alors que les autres bits du message ne sont pas affectés.

12. On a $\dim C + \dim(\mathbb{F}_2^{n-k+1} \times \{0\}^{k-1}) > n$ donc C et $\mathbb{F}_2^{n-k+1} \times \{0\}^{k-1}$ ne sont pas en somme directe : il existe $c \in C$ non nul tel que $c_{n-k+1} = \cdots = c_{n-1} = 0$. Notons $t_0 = \lfloor \frac{n-k}{2} \rfloor$. Posons $e_i = c_i$ pour tout $i \in [\![0, t_0]\!]$ et $e_i = 0$ pour tout $i \in [\![t_0 + 1, n - 1]\!]$, si bien que $r(e) \leq t_0 + 1$. Posons aussi $e'_i = c_i$ pour tout $i \in [\![t_0 + 1, n - k]\!]$ et $e'_i = 0$ pour les autres valeurs de i. On a alors $e + e' = c \in C \setminus \{0\}$ et $r(e') \leq n - k - t_0 \leq t_0 + 1$, cette dernière inégalité étant facile à vérifier en distinguant selon la parité de $n - k$. Cela démontre que C ne peut pas corriger $t_0 + 1$ erreurs en rafale : si il en corrige t alors $t \leq t_0$.

13. Les majorations de t qu'on obtient aux questions 9 et 12 sont les mêmes que celles qui découlent, lorsque les erreurs sont aléatoires et indépendantes les unes des autres, de la borne de Singleton sur la distance de C. Cependant il peut être plus facile de s'approcher de cette borne (voire de l'atteindre) quand les erreurs sont en rafale. C'est notamment ce que montre la question 10 : à longueur et dimension fixées, tout code cyclique détecte le nombre maximal possible d'erreurs en rafale, alors que bien peu de codes atteignent la borne de Singleton sur la distance.

Partie 3 : Intermède sur les diviseurs de $X^n - 1$ dans $\mathbb{F}_q[X]$

14. Le fait que $S(X)$ divise $X^n - 1$ signifie que $X^n = 1$ dans le quotient $\mathbb{F}_q[X]/(S)$; cela équivaut à $n_S | n$, en notant n_S l'ordre de la classe de X dans le groupe multiplicatif $(\mathbb{F}_q[X]/(S))^*$. Cela a bien un sens car $S(0) \neq 0$ donc X est premier avec S, et la classe de X appartient bien à ce groupe. Enfin l'unicité d'un n_S vérifiant la propriété de l'énoncé est immédiate : c'est le plus petit $n \geq 1$ tel que S divise $X^n - 1$.

15. Supposons S irréductible. Alors $\mathbb{F}_q[X]/(S)$ est un corps de cardinal $q^{\deg S}$, donc le groupe fini $(\mathbb{F}_q[X]/(S))^*$ est de cardinal $q^{\deg S} - 1$. Donc l'ordre de X, qui vaut n_S, divise $q^{\deg S} - 1$: on a $q^{\deg S} \equiv 1 \bmod n_S$. Cela signifie que l'ordre de q dans le groupe multiplicatif $(\mathbb{Z}/n_S\mathbb{Z})^*$, noté d, divise $\deg S$. Or n_S divise $q^d - 1$ donc $S(X)$ divise $X^{q^d-1} - 1$ d'après la question 14 ; il en découle que $S(X)$ divise $X^{q^d} - X$. Or $X^{q^d} - X$ est le produit des polynômes $P \in \mathbb{F}_q[X]$ irréductibles unitaires dont le degré divise d. Comme S est irréductible, cela montre que $\deg S$ divise d, d'où $d = \deg S$.

16. Le théorème chinois donne un isomorphisme entre les anneaux $\mathbb{F}_q[X]/(S)$ et $\prod_{i=1}^{\ell}(\mathbb{F}_q[X]/(S_i))$, donc entre les groupes $(\mathbb{F}_q[X]/(S))^*$ et $\prod_{i=1}^{\ell}((\mathbb{F}_q[X]/(S_i))^*)$. Par cet isomorphisme, $X \bmod S$ correspond à $(X \bmod S_1, \ldots, X \bmod S_\ell)$. Ces éléments ont donc le même ordre : $n_S = \mathrm{ppcm}(n_{S_1}, \ldots, n_{S_\ell})$ puisque l'ordre d'un élément dans un produit de groupes finis est le ppcm des ordres de ses composantes.

17. ($\star$) Il suffit de vérifier que $S(X)$ n'a aucune racine dans une extension de $\mathbb{F}_2$ de degré $\leq \frac{\deg S}{2}$, c'est-à-dire dans $\mathbb{F}_2$ et $\mathbb{F}_4$. Voir le Notebook ou en calculant les polynômes irréductibles de degré 2 sur $\mathbb{F}_2$.

18. On peut simplement tester, pour les valeurs successives de $n \geq 2$, si $S(X)$ divise $X^n - 1$. Comme $n_S \leq 2^{14} - 1$ d'après la question 15, ce ne sera pas trop long. Sinon il suffit d'appliquer la question 16 avec $S_1(X) = X^9 + 1 = X^9 - 1$ et $S_2(X) = X^5 + X^2 + 1$; on a $n_{S_1} = 9$. En outre S_2 est irréductible d'après la question 17, donc n_{S_2} divise 31 d'après la question 15. Comme $n_{S_2} > 1$ et que 31 est premier, on en déduit $n_{S_2} = 31$. Enfin S_2 est irréductible et ne divise pas $X^9 - 1$ (puisque $n_{S_2} = 31$), donc $\mathrm{pgcd}(S_1, S_2) = 1$ et $n_S = \mathrm{ppcm}(9, 31) = 279$.

Partie 4 : Un code cyclique particulier

19. Modulo $X^{2t-1} - 1$ on a $X^{(2t-1)k+\ell} \equiv X^\ell$ pour tous $k, \ell \in \mathbb{N}$, donc

$$Q(X) \equiv \sum_{\ell=0}^{2t-2} \Big(\sum_{\substack{0 \leq i \leq d \\ i \equiv \ell \bmod 2t-1}} a_i \Big) X^\ell.$$

Le polynôme à droite est donc le reste dans la division euclidienne de Q par $X^{2t-1} - 1$: il est nul si, et seulement si, $X^{2t-1} - 1$ divise Q.

20. Le polynôme $X^{2t-1} - 1$ divise g donc divise $S - X^j T$. En notant $S(X) = \sum_{i=0}^{t-1} s_i X^i$ et $T(X) = \sum_{i=0}^{t-1} t_i X^i$, et en posant $s_i = 0$ pour tout $i \geq t$, la question 19 donne

$$s_\ell + \sum_{\substack{0 \leq i \leq t-1 \\ i \equiv \ell - j \bmod 2t-1}} t_i = 0 \tag{1}$$

pour tout $\ell \in [\![0, 2t-2]\!]$. Dans cette expression, la deuxième somme contient exactement un terme si le reste dans la division euclidienne de $\ell - j$ par $2t-1$ est compris entre 0 et $\ell - 1$, et aucun terme (c'est une somme vide) sinon. Quitte à remplacer j par son reste dans la division euclidienne par $2t-1$, on peut supposer que $0 \leq j \leq 2t-2$. Comme $t_0 = 1$, la relation (1) appliquée avec $\ell = j$ donne $s_j = 1$ d'où $j \leq t-1$. On a aussi $s_0 = 1$, donc en prenant $\ell = 0$ dans (1) on obtient l'existence de $i \in [\![0, t-1]\!]$ tel que $i \equiv -j \bmod 2t-1$, c'est-à-dire tel que $2t-1$ divise $i+j$. Comme $i+j \leq 2(t-1) < 2t-1$ et $i, j \geq 0$, on en déduit $i = j = 0$. Cela termine la preuve que $(2t-1)|j$. Il en découle que $X^j \equiv 1 \bmod (X^{2t-1}-1)$, donc $S - T \equiv S - X^j T \equiv 0 \bmod (X^{2t-1}-1)$. Comme $\deg(S-T) < t \leq 2t-1$, on obtient $S = T$.

21. La question 20 montre que $P(X)$ divise $(X^j-1)S(X)$, puisque $P|g$. Or P est irréductible et $\deg S < t \leq \deg P$, donc P est premier avec S, et P divise $X^j - 1$. De plus $X^{2t-1}-1$ divise aussi $X^j - 1$ puisque $2t-1$ divise j, et P est premier avec $X^{2t-1}-1$ (puisque P est irréductible et ne divise pas $X^{2t-1}-1$), donc $g(X)$ divise $X^j - 1$. Par définition de $n = n_g$, cela impose $j = 0$ puisque $j < n$. On aurait aussi pu utiliser la question 16 pour démontrer que $n_g = \mathrm{ppcm}(2t-1, n_P)$.

22. Soient $e_1, e_2 \in \mathbb{F}_2^n$ tels que $r(e_1) \leq t$, $r(e_2) \leq t$ et $e_1 + e_2 \in C$; d'après la question 10 on peut supposer $e_1, e_2 \neq 0$. Le code étant cyclique, on peut supposer que e_1 correspond à un polynôme S tel que $S(0) = 1$ et $\deg S < t$. Comme e_2 est formé par une plage de t bits au maximum qui sont susceptibles d'être non nuls (les autres étant nuls), il correspond à un polynôme de la forme $X^j T$ (vu modulo $X^n - 1$), avec $j \in [\![0, n-1]\!]$, $T(0) = 1$ et $\deg T < t$. Le fait que $e_1 + e_2 \in C$ signifie que $S + X^j T$ est un multiple de g. Les questions 20 et 21 montrent alors que $j = 0$ et $S = T$, c'est-à-dire $e_1 = e_2$; autrement dit, on a $e_1 + e_2 = 0$.

23. ($\star$) On obtient $k = 265$, $n = 279$, $d =$. D'après la question 14, le code détecte donc $n - k = 14$ erreurs en rafales. En général, C peut détecter $d-1$ erreurs et en corriger $\lfloor \frac{d-1}{2} \rfloor$.