18 juin 2024
Master 1 M.F., Orsay

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

Cet examen est consacré aux codes BCH, qui ont été abordés en cours. La partie 2 fournit notamment une preuve d'un résultat admis dans le poly.

Partie 1 : notations et préliminaires

1. Le groupe multiplicatif $\mathbb{F}_{2^r}^\times$ est cyclique et d'ordre 2^r-1 multiple de n, donc il possède un élément α d'ordre n.
2. On choisit $P \in \mathbb{F}_2[X]$ irréductible de degré r (ce qui est toujours possible), et on pose $\mathbb{F}_{2^r} = \mathbb{F}_2[X]/(P)$. Un élément $y \in \mathbb{F}_{2^r}$ est représenté par un polynôme $Q \in \mathbb{F}_2[X]_{<r}$. Le produit de deux éléments de $\mathbb{F}_{2^r}$ est représenté par le reste, dans la division euclidienne par P, du produit des deux polynômes de $\mathbb{F}_2[X]$ associés. On le calcule en $O(r^2)$ opérations élémentaires dans $\mathbb{F}_2$ (y compris avec l'algorithme naïf de multiplication des polynômes), i.e. en $O(r^2)$ opérations élémentaires sur les bits.
3. Comme n est premier, α est une racine primitive n-ième de l'unité si, et seulement si, $\alpha \neq 1$ et $\alpha^n = 1$. Cette dernière égalité se teste en calculant α^n par exponentiation rapide, avec un coût en $O(\log n)$ multiplications dans $\mathbb{F}_{2^r}$.
4. Comme $\alpha^n = 1$, la valeur de α^k est la même quelle que soit le représentant $k \in \mathbb{Z}$ de la classe de congruence σ. On peut donc noter α^σ cette valeur.
5. Notons $\sigma_1, \ldots, \sigma_s$ les éléments de Σ. Supposons avoir déjà calculé $g_j(X) = \prod_{i=1}^{j}(X - \alpha^{\sigma_i})$ pour un certain $j \in \{1, \ldots, s-1\}$. Comme $\deg g_j = j$, le coût du calcul de $g_{j+1}(X) = (X - \alpha^{\sigma_{i+1}})g_j(X)$ est de $O(j)$ opérations arithmétiques dans $\mathbb{F}_{2^r}$. En sommant sur j, le coût du calcul de $g = g_s$ est de $O(s^2)$ opérations arithmétiques dans $\mathbb{F}_{2^r}$.
6. Le code C est de dimension $n - s$ et de longueur n.
7. En utilisant la question précédente, la borne de Singleton donne $d \leq n+1-\dim C = s+1$, où d est la distance minimale de C.

Partie 2 : minoration de la distance minimale de C.

8. On a $\det R = (\prod_{j=1}^{w} \varrho_j) \det[\varrho_j^{i-1}]_{1 \leq i,j \leq w} \neq 0$ en factorisant le j-ième colonne de R par ϱ_j, et par propriété du déterminant de Vandermonde.
9. Supposons que $P(X) = X^{a_1} + \ldots + X^{a_w}$ s'annule en α^i pour tout $i \in \{1, \ldots, w\}$. Alors on a $\sum_{j=1}^{w} \alpha^{ia_j} = 0$ pour tout i. Notons R la matrice de la question précédente, associée aux $\varrho_j = \alpha^{a_j}$ qui sont deux à deux distincts car les a_j sont deux à deux distincts et compris entre 0 et $n-1$. Alors on a $RV = 0$ en notant V le vecteur colonne constitué uniquement de 1, ce qui contredit le fait que R soit inversible.
10. Supposons par l'absurde qu'il existe $c \in C \setminus \{0\}$ de poids $w \leq 2t$. On a $c = gT \in \mathbb{F}_2[X]_{<n}$ pour un certain $T \in \mathbb{F}_2[X]$ donc $c(\alpha^\sigma) = 0$ pour tout $\sigma \in \Sigma$. Par définition de Σ, c'est vrai en particulier pour tout $\sigma \in \{1, \ldots, 2t\}$, donc a fortiori pour tout $\sigma \in \{1, \ldots, w\}$. Cela contredit la question précédente.

11. D'après la question précédente, le code C peut détecter $2t$ erreurs, et en corriger t. Bien entendu, si la distance minimale de C est supérieure à la borne obtenue à la question précédente, ces valeurs peuvent être plus élevées.

Partie 3 : un exemple.

12. ($\star$) Il suffit de vérifier que le polynôme $X^4 + X + 1 \in \mathbb{F}_2[X]$ est irréductible, ce qui est immédiat avec la commande `P.is_irreducible()`.
13. ($\star$) Il suffit de vérifier que α est d'ordre 15, soit que $\alpha^{15} = 1$ avec $\alpha^3 \neq 1$ et $\alpha^5 \neq 1$.
14. ($\star$) Voir le Notebook ! On constate que Σ consiste en l'ensemble des puissances de 2 modulo 15 et que 2^4 est congru à $1 = 2^0$ modulo 15. Ainsi Σ consiste en la classe de 1, la classe de 2, la classe de 4 et la classe de 8 modulo 15.
15. Une base de C est donnée par les polynômes $X^j g(X)$ avec $0 \leq j \leq n-s-1$. La matrice génératrice associée a pour lignes ces polynômes, exprimés dans la base canonique de $\mathbb{F}_2^n$.
16. ($\star$) On obtient une distance minimale de 3. Il y a juste une subtilité : Sage doit interpréter le polynôme g comme étant à coefficients dans $\mathbb{F}_2$, et pas dans $\mathbb{F}_{2^r}$ (alors qu'a priori il a été calculé comme produit de polynômes à coefficients dans $\mathbb{F}_{2^r}$).

Partie 4 : un algorithme de décodage.

17. Le message d'origine est m : c'est lui qui contient l'information à transmettre. Le message codé est mg : c'est un élément du code C, qui contient une part de redondance. L'erreur de transmission est e ; elle ne concerne que t bits au maximum par hypothèse (sinon le code n'est pas forcément capable de la corriger). Enfin, ϱ est le message reçu.
18. Pour tout $k \in \{1, \dots, 2t\} \subset \Sigma$ on a $g(\alpha^k) = 0$ donc $\varrho(\alpha^k) = e(\alpha^k)$. On en déduit

$$S(Y) = \sum_{k=1}^{2t} \Big(\sum_{j=1}^{w} \alpha^{ki_j} \Big) Y^{k-1} = \sum_{j=1}^{w} \sum_{k=1}^{2t} \alpha^{ki_j} Y^{k-1}$$

ce qui donne

$$S(Y)\sigma(Y) = \sum_{j=1}^{w} \alpha^{i_j} \sigma(Y) \sum_{k=0}^{2t-1} \alpha^{ki_j} Y^k \equiv \tau(Y) \bmod Y^{2t}$$

car pour tout j on a

$$(1 - \alpha^{i_j} Y) \sum_{k=0}^{2t-1} \alpha^{ki_j} Y^k = 1 - \alpha^{2ti_j} Y^{2t} \equiv 1 \bmod Y^{2t}.$$

19. On a $r_j\sigma - v_j\tau = (u_j Y^{2t} + v_j S)\sigma - v_j\tau = u_i Y^{2t} + v_j(S\sigma - \tau)$ qui est multiple de Y^{2t} d'après la question précédente. Par ailleurs $\deg(r_j\sigma) < t + \deg\sigma = t + w \leq 2t$ et $\deg(v_j\tau) = \deg r_0 - \deg r_{j-1} + \deg\tau \leq 2t - t + (w-1) < t + w \leq 2t$. Donc $r_j\sigma - v_j\tau$ est de degré strictement plus petit que $2t$: c'est le polynôme nul.

20. On a

$$v_j(Y)S(Y)\sigma(Y) \equiv v_j(Y)\tau(Y) = r_j(Y)\sigma(Y) = u_jY^{2t}\sigma(Y)+v_j(Y)S(Y)\sigma(Y) \bmod v_j(Y)Y^{2t}$$

d'après les questions 18 et 19. Cela montre que $v_j(Y)Y^{2t}$ divise $u_jY^{2t}\sigma(Y)$; autrement dit, $v_j(Y)$ divise $u_j\sigma(Y)$. Comme u_j est premier avec v_j, on en déduit que v_j divise σ.

Par ailleurs, la question 19 montre que σ divise $v_j\tau$. Or σ est scindé sur $\mathbb{F}_{2^r}$, avec comme racines les α^{-i_j}, et pour tout j on a $\tau(\alpha^{-i_j}) = \alpha^{i_j}\prod_{\substack{1\leq\ell\leq w\\ \ell\neq j}}(1-\alpha^{i_\ell-i_j}) \neq 0$ car $\alpha^{i_1},\ldots,\alpha^{i_w}$ sont deux à deux distincts. Donc σ et τ sont premiers entre eux, donc σ divise v_j.

Finalement σ et v_j sont associés. Comme $\sigma(0) = 1$ on en déduit $\sigma(Y) = \frac{v_j(Y)}{v_j(0)}$. La question 19 donne alors

$$\tau(Y) = \frac{r_j(Y)\sigma(Y)}{v_j(Y)} = \frac{r_j(Y)}{v_j(0)}.$$

21. Supposons ρ connu, ainsi bien sûr que les données de la partie 1, mais pas m ni e. On peut calculer $S(Y)$ et mener à bien l'algorithme d'Euclide décrit dans l'énoncé ; on connaît t donc on peut déterminer j. La question 20 permet alors de calculer σ et τ. Il suffit alors de calculer $\sigma(\alpha^{-i})$ pour chaque entier $i \in \{0,\ldots,n-1\}$: ceux pour lesquels c'est nul sont parmi les i_j, c'est-à-dire que ce sont des bits qui ont été mal transmis. On récupère donc l'erreur e, puis $mg = \varrho - e$ et enfin m.

22. ($\star$) Voir le Notebook !