À travailler et rédiger par **groupe de 2** maximum et remettre **avant le 10 mai** en **C664**.

Les *corps binaires*, de la forme $\mathbf{F}_{2^n} = \mathrm{GF}(2^n)$, sont très utilisés dans les applications de par la facilité de représenter leurs éléments sous forme de suites de bits. Le corps à 256 éléments apparaît notamment dans l'algorithme de chiffrement symétrique le plus répandu, l'*Advanced Encryption Standard*, et dans les codes de Reed-Solomon utilisés pour la correction d'erreurs pour le stockage optique (CD/DVD/Blu-Ray) et les communications satellitaires.

Le corps des octets

Construisons le corps fini $\mathbf{F}_{256}$ à partir de $\mathbf{F}_2$ par adjonction d'un élément α satisfaisant

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha + 1, \tag{*}$$

de sorte que tout élément $\xi \in \mathbf{F}_{256}$ s'écrit uniquement

$$\xi = b_0 + b_1\,\alpha + b_2\,\alpha^2 + \cdots + b_7\,\alpha^7, \qquad b_0, \ldots, b_7 \in \mathbf{F}_2.$$

Exercice 1

a) Calculer les puissances α^{2^i}, $i = 0, 1, \ldots, 8$.

b) α est-il un élément primitif de $\mathbf{F}_{256}$?

Par souci d'économie notationnelle, on identifie souvent un élément $\xi \in \mathbf{F}_{256}$ comme ci-dessus à un octuplet

$$(b_0, b_1, b_2, \ldots, b_7) \in (\mathbf{F}_2)^8$$

qu'on peut interpréter comme la représentation binaire naturelle d'un entier compris entre 0 et 255, souvent écrit sur deux chiffres hexadécimaux. Par exemple,

$$\xi := 1 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^7 \;\longleftrightarrow\; (1,0,0,1,1,1,0,1) \;\longleftrightarrow\; 1011\,1001_2 = \mathrm{B9}_{16}\,(= 185_{10}).$$

Exercice 2

a) Déterminer l'inverse multiplicatif de l'élément ξ ci-dessus.

Indication : appliquer la variante de l'algorithme d'Euclide étendu aux polynômes

$$f(x) = x^7 + x^5 + x^4 + x^3 + 1 \qquad \text{et} \qquad g(x) = x^8 + x^4 + x^3 + x + 1.$$

b) Résoudre pour $\xi \in \mathbf{F}_{256}$ l'équation

$$\mathrm{7E} \cdot \xi + \mathrm{A2} = \mathrm{C7} \cdot \xi + 43.$$

Parmi tous les polynômes à coefficients dans $\mathbf{F}_{256}$, certains ont toutes leurs racines dans $\mathbf{F}_{256}$ et d'autres non. Considérons donc l'ensemble E de tous les polynômes $f(x) \in \mathbf{F}_{256}[x]$ de degré 3 pour lesquels il existe $\xi_1, \xi_2, \xi_3 \in \mathbf{F}_{256}$ tels que

$$f(x) = (x - \xi_1)(x - \xi_2)(x - \xi_3).$$

Exercice 3

a) Réaliser E comme l'ensemble des orbites pour l'action (à préciser) d'un groupe sur $(\mathbf{F}_{256})^3$.

b) Déterminer $|E|$ à l'aide de la formule de Cauchy-Frobenius.

Code de Hamming

Lors de la transmission (ou stockage) d'une suite de bits, il est fréquent que des erreurs surviennent et que certains soient inversés. Il est important de pouvoir détecter de telles erreurs, et si possible les corriger automatiquement. Cela se fait en introduisant de la redondance dans l'encodage : la façon la plus simple est de répéter chaque bit plusieurs fois, mais il existe des méthodes plus efficaces.

Considérons une suite de 4 bits $\mathbf{b} = (b_0, b_1, b_2, b_3)$ à transmettre, identifiée à un polynôme de degré $\leqslant 3$

$$\mathbf{b}(x) := b_0 + b_1\,x + b_2\,x^2 + b_3\,x^3 \;\in\; \mathbf{F}_2[x]_{\leqslant 3}.$$

L'*encodage de Hamming* consiste à représenter celle-ci à l'aide des 7 bits correspondants aux coefficients du polynôme

$$\mathbf{c}(x) := \mathbf{b}(x) \cdot (1 + x + x^3) \;\in\; \mathbf{F}_2[x]_{\leqslant 6}.$$

Exercice 4

a) Quel est la version encodée $\mathbf{c}$ de la suite $\mathbf{b} = (1, 0, 1, 1)$?

b) De façon générale : en notant $\mathbf{b}$ et $\mathbf{c}$ comme vecteurs colonnes, déterminer une matrice $H \in \mathcal{M}_{7\times 4}(\mathbf{F}_2)$ pour laquelle

$$\mathbf{c} = H \cdot \mathbf{b}.$$

(En d'autres termes : l'encodage est une application linéaire entre $\mathbf{F}_2$-espaces vectoriels.)

La version encodée $\mathbf{c} = H \cdot \mathbf{b}$ du message est transmise sur la canal de transmission (ou stockée) ; à la réception, on obtient

$$\mathbf{r} = \mathbf{c} + \mathbf{e},$$

où $\mathbf{e}$ est un vecteur indiquant la position des erreurs de transmission survenues (idéalement on aurait $\mathbf{e} = \mathbf{0}$, et on peut alors récupérer $\mathbf{b}(x)$ par division polynomiale de $\mathbf{r}(x) = \mathbf{c}(x)$ par $1 + x + x^3$).

Exercice 5

a) Supposons que $\mathbf{r} = (1, 0, 1, 0, 0, 1, 1)$ soit reçu. Vérifier que l'équation $\mathbf{r} = H \cdot \mathbf{b}$ n'admet pas de solution. Que peut-on en conclure ?

b) Montrer que toute erreur de transmission affectant au maximum 2 bits pourra être détectée avec cet encodage. Qu'en est-il des erreurs de transmissions affectant 3 bits ?

Non seulement l'encodage de Hamming permet de détecter (certaines) erreurs de transmissions (et par exemple déclencher une demande de retransmission), mais on peut également dans certains cas les corriger automatiquement.

Aidons-nous pour cela du corps $\mathbf{F}_8 = \mathbf{F}_2(\beta)$, où

$$\beta^3 = 1 + \beta \qquad (**)$$

(on peut remarquer qu'il s'agit d'un élément primitif). On peut obtenir de l'information sur les erreurs de transmission en évaluant le polynôme reçu $\mathbf{r}(x)$ en β.

Exercice 6

a) Si aucune erreur de transmission n'est survenue, montrer que $\mathbf{r}(\beta) = 0$. Si une erreur de transmission est survenue sur le i^{e} bit $(0 \leqslant i \leqslant 6)$, montrer qu'alors $\mathbf{r}(\beta) = \beta^i$, ce qui permet d'identifier la position de l'erreur (et donc de la corriger).

b) En supposant qu'une erreur de transmission affectant au maximum un bit soit survenue, identifier quelle était la suite $\mathbf{b}$ initiale si le message reçu est $\mathbf{r} = (1, 0, 1, 0, 1, 0, 1)$.