Construction d'un code BCH 15-5

Mise en place, et codage

1. $\mathbb{F}_2$ est le corps à deux éléments. Vérifier que le polynôme $m_1 = x^4 + x^3 + 1$ est irréductible dans $\mathbb{F}_2[x]$.

2. Soit α une racine de m_1. Exprimer les $\alpha^i, 0 \leq i \leq 15$, en fonction de $1, \alpha, \alpha^2, \alpha^3$, et vérifier ainsi que $\mathbb{K} = \mathbb{F}_2[\alpha]$ est un corps à 16 elements, et que, en outre, α est un générateur du groupe cyclique des élements non nuls. Autrement dit (cf. fiche 4) le polynôme m_1 est primitif modulo 2.

   Les éléments du corps $\mathbb{K}$ seront identifiés aux expressions polynomiales en α de degré ≤ 3. On posera pour cela `alias(alpha = RootOf(`m_1`))`, et toutes les expressions polynomiales en α seront réduites en utilisant `evala(...) mod 2`.

3. Quelles sont les autres racines de m_1 ? Le vérifier en factorisant m_1 dans K par la commande `Factor(m1,alpha) mod 2`.

4. Quel est le polynôme minimal m_3 de α^3 ? Quel est le polynôme minimal m_5 de α^5 ?

5. On considère le code BCH construit sur le polynome $m = m_1 m_3 m_5$. On rappelle que ce code est l'espace vectoriel $\mathcal{C}$ formé des polynômes en x à coefficients dans $\mathbb{F}_2$ de degré ≤ 14, et divisibles par m. Le mot binaire de longeur 15, $a_{14}, a_{13}, \ldots, a_0$ étant identifiés au polynôme $\sum_{i=0}^{14} a_i x^i$. Ecrire la procédure de codage polynomial

   ```
   > encodepoly(message_binaire_de_longueur_5)
   ```

   qui reçoit une liste $[a_{14}\, a_{13}\, a_{12}\, a_{11}\, a_{10}]$ de cinq bits, et fabrique le polynôme en α de termes de plus hauts degrés

   $$a_{14}x^{14} + a_{13}x^{13} + a_{12}x^{12} + a_{11}x^{11} + a_{10}x^{10} + \ldots$$

   qui est divisble par m.

Rappel d'algèbre

Soit K un corps quelconque et $x_1, x_2, \ldots, x_r$, deux à deux distincts, des éléments de K. Pour tout $n \in \mathbb{N}$ on appelle *somme de Newton* d'indice n, et on note S_n la

somme $S_n = \sum_{i=1}^{r} x_i^n$. On note $P = x^r + a_{r-1}x^{r-1} + \cdots + a_0$ le polynôme unitaire de racines $x_1, x_2, \ldots, x_r$.

1. Montrer que le déterminant

$$D_r = \begin{vmatrix} S_0 & S_1 & \ldots & S_{r-1} \\ S_1 & S_2 & \ldots & S_r \\ & & \vdots & \\ S_{r-1} & S_r & \ldots & S_{2r-2} \end{vmatrix}$$

   est le carré du déterminant de Van der Mond de $(x_1, x_2, \ldots, x_r)$.

2. Montrer que la suite (S_n) vérifie la relation de récurrence linéaire

$$S_n + a_{r-1}S_{n-1} + a_{r-2}S_{n-2} + \cdots + a_0 S_{n-r} = 0. \qquad (n \geq r).$$

3. Montrer que, pour tout $n \geq r$, la matrice

$$M_n = \begin{pmatrix} S_0 & S_1 & \ldots & S_{n-1} \\ S_1 & S_2 & \ldots & S_n \\ & & \vdots & \\ S_{n-1} & S_n & \ldots & S_{2n-2} \end{pmatrix}$$

   est de rang r.

4. Montrer enfin que, si les x_i sont tous différents de 0, alors la matrice

$$A_n = \begin{pmatrix} S_1 & S_2 & \ldots & S_n \\ S_2 & S_3 & \ldots & S_{n+1} \\ & & \vdots & \\ S_n & S_{n+1} & \ldots & S_{2n-1} \end{pmatrix}$$

   est aussi de rang r pour tout $n \geq r$.

Décodage

1. Adoptant toujours la représentation polynômiale pour noter les mots binaires de longeur 15, on notera $C(x)$ le message envoyé, $R(x)$ le message reçu, et enfin

$$E(x) = C(x) - R(x) = \sum_{j=1}^{r} x^{i_j}$$

   le polynôme erreur, en supposant que le nombre d'erreurs, r est majoré par 3. Soit

$$x_1 = \alpha^{i_1}, \quad x_2 = \alpha^{i_2}, \quad x_3 = \alpha^{i_3}, \quad \ldots, x_r = \alpha^{i_r}$$

et $P \in \mathbb{K}[x]$ le **polynôme localisateur des errreurs** dont les racines sont les x_i.

$$P(z) = \prod_{i=1}^{r}(z - x_i) = z^r + \sum_{i=0}^{r-1} a_i z^i$$

Pour tout entier n notons $S_n = E(\alpha^n) = \sum_{i=1}^{r} x_i^n$. Montrer que le nombre d'erreurs, r, est le rang de la matrice

$$A_3 = \begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}$$

et qu'on a l'équation

$$\begin{pmatrix} S_1 & \dots & S_r \\ & \dots & \\ S_r & \dots & S_{2r-1} \end{pmatrix} \begin{pmatrix} a_0 \\ \dots \\ a_{r-1} \end{pmatrix} = \begin{pmatrix} S_{r+1} \\ \dots \\ S_{2r} \end{pmatrix}$$

Il suffit donc de connaitre les S_n, pour $1 \leq n \leq 6$, pour calculer les coefficients a_i du polynôme localisateur des erreurs. Il ne reste plus qu'à remarquer que $S_n = E(\alpha^n) = R(\alpha^n)$, pour $1 \leq n \leq 6$.

2. En déduire la procédure de décodage

```
> Decode := proc(R)
```

qui reçoit un message avec au plus 3 erreurs, sous la forme d'un polynôme `R` de $\mathbb{F}_2[x]$, de degré ≤ 14 et renvoie le message corrigé de ses éventuelles erreurs, sous la même forme.

Pour obtenir le rang de la matrice A_3, puis résoudre le système linéaire dans $\mathbb{K}$ on utilisera les fonctions prédéfinies Maple `Gaussjord` et `Linsolve`, en conjonction avec l'opérateur `mod`. Une fois obtenu les coefficents du polynôme localisateur des erreurs P, Pour obtenir les indices $i_1, i_2, \dots, i_r$ tels que α^i soit racine de P on se contentera d'une boucle, `for i from 0 to 14 ....`

3. Décoder le message

$$R = x^{14} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^3.$$

Rendement de ce code

On reprend le code de l'exercice précédent.

1. On suppose que la probabilité d'erreur du canal de communication lors de la transmission d'un bit est $p = 0.001$. Quelle est la probabilité pour qu'un message non codé de 5 bits soit reçu sans erreur ? Quelle est la probabilité pour que le même message codé au moyen du code BCH précédent (en un mot de longueur 15) soit décodé correctement ?

2. Quelle est la taille du no-man's-land ?