Exercice : Montrer que $GRS(\alpha, v) = GRS(\alpha, w) \Leftrightarrow v = \lambda w$ pour $\lambda \in F_q^*$.

Problème : Soit $\mathbb{F}_{q^m}$ la plus petite extension de $\mathbb{F}_q$ contenant toutes les racines n^{eme} de 1 où n est un entier premier avec q. Soit α une racine primitive n^{eme} de 1 dans $\mathbb{F}_{q^m}$. ($\{1, \alpha, \cdots, \alpha^{n-1}\} \subset \mathbb{F}_{q^m}$ sont toutes les racines primitives n^{eme} de 1).

Pour $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[z]$, soit $\hat{c}(z) \in \mathbb{F}_{q^m}$ défini par

$$\hat{c}(z) = \sum_{j=1}^{n} \hat{c}_j z^{n-j}, \text{ où } \hat{c}_j = c(\alpha^j) = \sum_{i=0}^{n-1} c_i \alpha^{ij}.$$

1) Montrer que $c(x) = \frac{1}{n} \sum_{i=0}^{n-1} \hat{c}(\alpha^i) x^i$.

2) Pour $f(x) = \sum_{i=0}^{n-1} f_i x^i$ et $g(x) = \sum_{i=0}^{n-1} g_i x^i$ on note $f(x) * g(x) = \sum_{i=0}^{n-1} f_i g_i x^i$.

a) Montrer que $\widehat{(f+g)}(z) = \hat{f}(z) + \hat{g}(z)$.

b) Montrer que $h(x) = (f(x)g(x)(mod\ x^n - 1))$ si et seulement si $\hat{h}(z) = \hat{f}(z) * \hat{g}(z)$.

c) Montrer que $\hat{h}(z) = \frac{1}{n}(\hat{f}(z)\hat{g}(x)\ (mod\ z^n - 1))$ si et seulement si $h(x) = f(x) * g(x)$.

3) Soient $\hat{f}(z), \hat{g}(z) \in \mathbb{F}_{q^m}[z]$ des polynômes premiers avec $z^n - 1$ tels que $deg(\hat{f}(z)) \leq n-1$ et $t = deg(\hat{g}(z)) \leq n-1$. On définit

$$GBCH(\hat{f}, \hat{g}) = \{(c_0, \cdots, c_{n-1}) \in \mathbb{F}_q^n \ : \ \hat{c}(z)\hat{f}(z)(mod\ z^n - 1) \equiv 0\ (mod\ \hat{g}(z))\}$$

où $c(x) = \sum_{i=0}^{n-1} c_i x^i$.

a) Montrer que si $f(x) = \sum_{i=0}^{n-1} f_i x^i$ et $g(x) = \sum_{i=0}^{n-1} g_i x^i$, alors $f_i \neq 0$ et $g_i \neq 0$ pour tout $0 \leq i \leq n-1$.

b) Montrer que les conditions suivantes sont équivalentes :

i) $c = (c_0, \cdots, c_{n-1}) \in GBCH(\hat{f}, \hat{g})$;

ii) il existe un polynôme $\hat{u}(z)$ avec $deg(\hat{u}(z)) \leq n - t - 1$ tel que $\hat{c}(z)\hat{f}(z)\ (modz^n - 1)) = \hat{u}(z)\hat{g}(z)$;

iii) il existe un polynôme $u(x) \in \mathbb{F}_{q^m}[x]$ tel que $c(x) * f(x) = u(x) * g(x)$ et $\hat{u}_j = 0$ pour $1 \leq j \leq t$, où $\hat{u}(z) = \sum_{j=1}^{n} \hat{u}_j z^{n-j}$ et $u(x) = \sum_{i=0}^{n-1} u_i x^i$;

iv) il exist $u_0, \cdots, u_{n-1} \in \mathbb{F}_{q^m}$ tels que $c_i f_i = u_i g_i$, pour $0 \leq i \leq n-1$ et $\hat{u}_j = 0$ pour $0 \leq j \leq t$;

v) $\hat{u}_j = \sum_{i=0}^{n-1} c_i f_i \alpha^{ij} / g_i$ pour tout $0 \leq j \leq t$;

4) Montrer que $c \in GBCH(\hat{f}, \hat{g})$ si et seulement si $cH^t = 0$ où

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \alpha^{t-1} & \cdots & \cdots & \alpha^{(t-1)(n-1)} \end{pmatrix} \begin{pmatrix} f_0/g_0 & 0 & \cdots & 0 \\ 0 & f_1\alpha/g_1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & f_{n-1}\alpha^{n-1}/g_{n-1} \end{pmatrix}$$

$GBCH(\hat{f}, \hat{g})$ s'appelle code BCH généralisé.

5) Dans la suite on suppose n impair, $q = 2$ et $L = \{1, \alpha, \cdots, \alpha^{n-1}\}$. Pour $c = (c_0, \cdots, c_{n-1}) \in \mathbb{F}_2^n$ on note $c(x) = \sum_{i=0}^{n-1} c_i x^i$ et $R_c(z) = \sum_{i=0}^{n-1} c_i/(z + \alpha^i)$.

a) Montrer que $\hat{c}(z) = (z(z^n + 1)R_c(z)\ (mod\ z^n - 1))$ et $R_c(z) = \sum_{i=0}^{n-1} \hat{c}(\alpha^i)/(z + \alpha^i)$.

b) Montrer que le code de Goppa $\Gamma(L, g) = \{c \in \mathbb{F}_2^n \ : \ (z^{n-1}\hat{c}(z)\ (mod\ z^n - 1)) \equiv 0 (modg(z))\}$.

6) On suppose que $\Gamma(L, g)$ est un code cyclique.

a) Montrer que $g(z) = z^t$, où $t \in \mathbb{N}$.

b) Montrer que si $n = 2^m - 1$ alors $\Gamma(L, g)$ est un code BCH.