Etat de l'Art de l'Arithmétique des Corps Finis

Christophe Negre

État de l'Art de l'Arithmétique des Corps Finis

Christophe Nègre

10 décembre 2004

Généralités

L'objectif de ce chapitre est d'introduire les outils généraux pour implanter l'arithmétique dans les extensions de corps finis. Soit $\mathbb{F}_q = \mathbb{F}_p[T]/(Q)$ un corps fini à $q = p^m$ éléments construit avec un polynôme irréductible $Q \in \mathbb{F}_p[T]$ de degré m. Soit $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ une extension de degré n de $\mathbb{F}_q$ définie par le polynôme irréductible $P \in \mathbb{F}_q[X]$.

Le corps $\mathbb{F}_{q^n}$ a une structure naturelle de $\mathbb{F}_q$-espace vectoriel, dont la loi d'addition est l'addition du corps $\mathbb{F}_{q^n}$ et la loi de multiplication par les scalaires est donnée par $(\lambda, U) \in \mathbb{F}_q \times \mathbb{F}_{q^n} \mapsto \lambda U$. Cette structure d'espace vectoriel va nous permettre d'utiliser les outils de l'algèbre linéaire pour étudier l'arithmétique dans les extensions de corps finis.

Si l'on se donne $\mathcal{B} = (e_1, \ldots, e_n)$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$, un élément $U \in \mathbb{F}_{q^n}$ peut être représenté par ses coordonnées $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ dans $\mathcal{B}$, données par

$$U = u_1 e_1 + u_2 e_2 + \cdots + u_n e_n.$$

Nous avons donc un large choix pour la représentation du corps $\mathbb{F}_{q^n}$, chaque $\mathbb{F}_q$-base induisant une représentation possible du corps.

Exemple 1. On considère ici une extension de degré 3 de $\mathbb{F}_3$ donnée par $\mathbb{F}_{3^3} = \mathbb{F}_3[X]/(X^3 - X - 1)$. On peut représenter les éléments de $\mathbb{F}_{3^3}$ dans les trois $\mathbb{F}_3$-bases suivantes

$$\begin{array}{rcl} \mathcal{B}_1 & = & (e_1, e_2, e_3) = (1, X, X^2), \\ \mathcal{B}_2 & = & (e'_1, e'_2, e'_3) = (1 + X, 1 - X, X^2), \\ \mathcal{B}_3 & = & (e''_1, e''_2, e''_3) = (1 + X + X^2, X, X^2). \end{array}$$

L' élément $U = 1 - X + X^2$ s'écrit dans les bases $\mathcal{B}_1, \mathcal{B}_2$ et $\mathcal{B}_3$ comme

$$\begin{array}{rcl} U & = & e_1 + (-1)e_2 + e_3 \\ & = & e'_2 + e'_3 \\ & = & e''_1 + e''_2. \end{array}$$

$\diamondsuit$

A partir d'une représentation dans une base, nous allons voir que nous pouvons exprimer les opérations dans le corps $\mathbb{F}_{q^n}$ (addition, multiplication, inversion) en fonction des coordonnées dans la $\mathbb{F}_q$-base.

Tout d'abord l'addition se fait simplement en additionnant coordonnée par coordonnée. En effet si $U = \sum_{i=1}^n u_i e_i$ et $V = \sum_{i=1}^n v_i e_i$, leur somme W est alors donnée par $W = \sum_{i=1}^n (u_i + v_i) e_i$.

Pour la multiplication, nous allons voir que seule la connaissance des produits $e_i e_j$ des éléments de $\mathcal{B}$ va nous permettre de calculer le produit de tous éléments $U, V \in \mathbb{F}_{q^n}$. Chaque produit $e_i e_j$ se décompose dans $\mathcal{B}$ comme

$$e_i e_j = \sum_{s=1}^{n} \lambda_{i,j}(s) e_s.$$

Avec les coefficients $\lambda_{i,j}(s)$ nous allons construire les matrices de structure M_s associées à la base $\mathcal{B}$.

Définition 1 (Matrice de structure)**.** *Pour $s = 1, \ldots, n$, on définit la matrice $n \times n$ de structure d'indice s, $M_s = [\lambda_{i,j}(s)]_{i,j=1,\ldots,n}$ associée à la $\mathbb{F}_q$-base $\mathcal{B}$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.*

Ces matrices de structure encodent toute l'information nécessaire pour pouvoir calculer le produit de deux éléments U, V à partir de leurs coordonnées dans $\mathcal{B}$. En effet si $U = u_1 e_1 + \cdots + u_n e_n$ et $V = v_1 e_1 + \cdots + v_n e_n$ deux éléments de $\mathbb{F}_{q^n}$, le produit $W = UV$ s'exprime alors dans $\mathcal{B}$ comme

$$UV = \sum_{s=1}^{n} \left(\sum_{i,j \in \{1,\cdots,n\}} \lambda_{i,j}(s) u_i v_j \right) e_s.$$

Si l'on note w_s la coordonnée d'indice s de $W = UV$ dans $\mathcal{B}$, nous avons

$$w_s = \begin{bmatrix} u_1 & \cdots & u_n \end{bmatrix} \cdot \begin{bmatrix} \lambda_{1,1}(s) & \cdots & \lambda_{1,n}(s) \\ \vdots & & \vdots \\ \lambda_{n,1}(s) & \cdots & \lambda_{n,n}(s) \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = ({}^tU) \cdot M_s \cdot V \ . \tag{1}$$

Il est possible d'exprimer d'une façon différente le produit de deux éléments $U, V \in \mathbb{F}_{q^n}$. Pour cela considérons l'application suivante

$$\begin{array}{rccc} \phi_U : & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & V & \mapsto & \phi_U(V) = UV \end{array}$$

Cette application est une application $\mathbb{F}_q$-linéaire, car $\phi_U(V + V') = \phi_U(V) + \phi_U(V')$, et pour $\alpha \in \mathbb{F}_q$ nous avons $\phi_U(\alpha V) = \alpha \phi_U(V)$. On notera M_U la matrice dans $\mathcal{B}$ de ϕ_U. Si l'on connaît la matrice M_U associée à un élément $U \in \mathbb{F}_{q^n}$ alors W le produit de U par V dans $\mathbb{F}_{q^n}$ peut se calculer simplement en effectuant le produit matriciel suivant

$$W = M_U \cdot V.$$

En fait la matrice M_U peut se calculer à l'aide des matrices de structure M_s associée à la base $\mathcal{B}$. De (1) nous pouvons voir que M_U est donnée par

$$M_U = \begin{bmatrix} ({}^tU) \cdot M_1 \\ \vdots \\ ({}^tU) \cdot M_n \end{bmatrix}. \tag{2}$$

Remarque 1. Nous utiliserons assez fréquement l'abus de notation qui consiste à considérer un élément $U \in \mathbb{F}_{q^n}$ à la fois comme un élément du corps $\mathbb{F}_{q^n}$, et aussi comme un vecteur colonne à coefficient dans $\mathbb{F}_q$. Pour lever une partie de l'ambiguïté que peut causer cet abus de notation, nous différencierons un produit deux éléments corps en ne mettant pas de point entre les opérandes, et en mettant un point dans un produit matriciel.

Dans l'exemple qui suit nous construisons les matrices de structure M_s et la matrice M_U pour une extension de corps $\mathbb{F}_{3^3}/\mathbb{F}_3$.

Exemple 2. On considère ici l'extension de corps $\mathbb{F}_{3^3} = \mathbb{F}_3[X]/(X^3 - X - 1)$ sur $\mathbb{F}_3$. Les trois éléments

$$e_1 = X - 1, e_2 = X^2 + X + 1, e_3 = X,$$

forment une base $\mathcal{B}$ du $\mathbb{F}_3$-espace vectoriel $\mathbb{F}_{3^3}$. Un élément $U \in \mathbb{F}_{3^3}$ peut s'exprimer dans $\mathcal{B}$ comme $U = u_1e_1 + u_2e_2 + u_3e_3$ et en particulier pour $1, X, X^2$ on a

$$\begin{array}{rcl} 1 & = & -e_1 + e_3, \\ X & = & e_3, \\ X^2 & = & e_2 + e_1 + e_3. \end{array}$$

On peut exprimer dans $\mathcal{B}$ les produits e_ie_j

$$\begin{array}{rclrcl} e_1e_1 & = & X^2 + X + 1 = e_2, & e_2e_2 & = & X^4 + 1 - X - X^3 = X^2 - X = e_2 + e_1, \\ e_3e_3 & = & X^2 = e_2 + e_1 + e_3, & e_1e_2 & = & X^3 - 1 = e_3, \\ e_1e_3 & = & X^2 - X = e_2 + e_1, & e_2e_3 & = & X^3 + X^2 + X = e_2 + e_3. \end{array} \quad (3)$$

On en déduit les matrices de structure M_s d'indice s

$$M_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, M_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Et finalement nous obtenons la matrice M_U de multiplication par U relativement à la $\mathbb{F}_3$-base $\mathcal{B}$ de $\mathbb{F}_{3^3}$ en utilisant la formule (2)

$$M_U = \begin{bmatrix} u_3 & u_2 & u_1 + u_3 \\ u_1 + u_3 & u_2 + u_3 & u_1 + u_2 + u_3 \\ u_2 & u_1 + u_3 & u_2 + u_3 \end{bmatrix}.$$

♢

Pour le problème de l'inversion d'un élément $U \in \mathbb{F}_{q^n}$, nous avons un premier résultat. Nous établissons que la matrice M_U de multiplication par U et la matrice M_W de multiplication par $W = U^{-1}$, l'inverse de U dans $\mathbb{F}_{q^n}$, sont inverses l'une de l'autre, i.e., $M_W = (M_U)^{-1}$.

Lemme 1 (Inverse de M_U)**.** *Soit $\mathbb{F}_{q^n}$ un corps fini et $\mathcal{B}$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Soit $U \neq 0$ un élément de $\mathbb{F}_{q^n}$, et W l'inverse de U dans $\mathbb{F}_{q^n}$. Alors l'application linéaire ϕ_W est l'isomorphisme inverse de ϕ_U, et M_W la matrice de ϕ_W dans la base W est la matrice inverse de M_U.*

Exemple 3. Soit le corps $\mathbb{F}_{3^3} = \mathbb{F}_3[X]/(X^3 - X - 1)$ et la $\mathbb{F}_3$-base $\mathcal{B}$ de $\mathbb{F}_{3^3}$ constituée des trois éléments suivants

$$e_1 = X - 1, e_2 = X^2 + X + 1, e_3 = X.$$

Nous avions vu dans l'exemple 2 que la matrice M_U d'un élément $U = u_1e_1 + u_2e_2 + u_3e_3$ était donnée par

$$M_U = \begin{bmatrix} u_3 & u_2 & u_1 + u_3 \\ u_1 + u_3 & u_2 + u_3 & u_1 + u_2 + u_3 \\ u_2 & u_1 + u_3 & u_2 + u_3 \end{bmatrix}.$$

Si par exemple $U = e_1 + e_2 - e_3 = X^2 + X$, son inverses W dans $\mathbb{F}_{3^3}$ vaut alors $W = e_1$ et leurs matrices M_U et M_W associées sont

$$M_U = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad M_W = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

On peut vérifier dans ce cas que M_U et M_W sont bien inverse l'une de l'autre car

$$M_U \cdot M_W = M_W \cdot M_U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

♢

Démonstration. Nous allons montrer uniquement l'assertion sur ϕ_U et ϕ_W, l'assertion sur les matrices étant une conséquence directe de cette dernière. Pour montrer que ϕ_U et ϕ_W sont inverses l'une de l'autre, nous allons établir que pour tout $V \in \mathbb{F}_{q^n}$ nous avons $\phi_U \circ \phi_W(V) = \phi_W \circ \phi_U(V) = V$. Par hypothèse W est l'inverse de U dans $\mathbb{F}_{q^n}$, i.e., $WU = 1$. Nous en déduisons

$$\phi_W \circ \phi_U(V) = W(UV) = (WU)V = V,$$

et en inversant les rôles de U et W

$$\phi_U \circ \phi_W(V) = U(WV) = (UW)V = V.$$

Ce qui termine la preuve. □

Dans les extensions de corps l'opérateur trace et l'opérateur norme d'un élément sont deux opérateurs importants que l'on utilisera fréquemment par la suite. Nous rappelons donc ici leur définition.

Définition 2 (Trace et Norme)**.** *Soit une extension de corps finis $\mathbb{F}_{q^n}/\mathbb{F}_q$.*

1. *La norme $N_{q^n|q}(U)$ d'un élément $U \in \mathbb{F}_{q^n}$ est définie par*

$$N_{q^n|q}(U) = \prod_{i=0}^{n-1} U^{q^i}, \tag{4}$$

   et $N_{q^n|q}(U) \in \mathbb{F}_q$. De plus si M_U est la matrice de multiplication par U dans une $\mathbb{F}_q$-base quelconque $\mathcal{B}$ de $\mathbb{F}_{q^n}$ alors $N_{q^n|q}(U) = \det(M_U)$.

2. *La trace $Tr_{q^n|q}(U)$ d'un élément $U \in \mathbb{F}_{q^n}$ est définie par*

$$Tr_{q^n|q}(U) = \sum_{i=0}^{n-1} U^{q^i},$$

   et $Tr_{q^n|q}(U) \in \mathbb{F}_q$. De plus si M_U est la matrice de multiplication par U dans une $\mathbb{F}_q$-base $\mathcal{B}$ de $\mathbb{F}_{q^n}$ alors $Tr(U) = Tr(M_U)$; la trace d'une matrice $n \times n$ étant la somme de ses termes diagonaux.

Par la suite si l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ ne fait pas d'ambiguïté on notera simplement $N(U)$ la norme de $U \in \mathbb{F}_{q^n}$ et $Tr(U)$ sa trace.

Exemple 4. Considérons le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3 + X + 1)$ et l'élément $U = X + X^2 \in \mathbb{F}_{2^3}$. La norme et la trace de U sur $\mathbb{F}_2$ valent donc

$$\begin{aligned} N(U) &= U\, U^2\, U^4 = 1 \\ Tr(U) &= U + U^2 + U^4 = 0 \end{aligned}$$

La matrice de U dans la base polynomiale $(1, X, X^2)$ de $\mathbb{F}_{2^3}$ est donnée par

$$M_U = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

et nous pouvons vérifier que $N(U) = \det(M_U)$ et $Tr(U) = Tr(M_U)$.

♢

Nous avons maintenant tous les objets nécessaires pour étudier plus en détail les opérations importantes dans $\mathbb{F}_{q^n}$: l'inversion tout d'abord, et ensuite la multiplications. Cette dernière étant celle qui nous intéressera le plus dans cette thèse.

1 Inversion dans $\mathbb{F}_{q^n}$

Jusqu'à aujourd'hui ont été présentées trois méthodes pour le calcul de l'inverse dans des extensions de corps $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Nous ne donnons pas ici les algorithmes les plus efficaces surtout pour la deuxième et la troisième méthode pour alléger l'exposé.

- **Première méthode** : elle s'appuie sur le fait que la norme d'un élément $N(U)$ pour $U \in \mathbb{F}_{q^n}$ est dans $\mathbb{F}_q$. Avec l'expression (4) de la norme de U nous avons

$$N(U) = U \times (\prod_{i=1}^{n-1} U^{q^i}).$$

En multipliant par $N(U)^{-1}$ nous obtenons

$$1 = U \times \left(N(U)^{-1} \prod_{i=1}^{n-1} U^{q^i} \right).$$

Donc l'inverse de U dans $\mathbb{F}_{q^n}$ est donné par

$$U^{-1} = (N(U))^{-1} \prod_{i=1}^{n-1} U^{q^i}.$$

L'algorithme suivant calcule l'inverse de U en utilisant cette expression de U^{-1}.

Algorithme 1 Inversion d'Itoh-Tsujii [14]

Entrée. $n-1=(n_k,\ldots,n_0)_2$ la représentation binaire de $n-1$ avec $n_k=1$ et un élément $U\in\mathbb{F}_{q^n}$.

Initialisation. Poser $W\leftarrow U$ et si $n_0=0$ poser $Z\leftarrow 1$ sinon poser $Z\leftarrow U$.

pour i de 0 à $k-1$ **faire**

$W\leftarrow WW^{q^{2^i}}$.

si $n_{i+1}=1$ **alors**

$Z\leftarrow WZ^{q^{2^{i+1}}}$.

$\alpha\leftarrow UZ^q$.

Sortie. $U^{-1}\leftarrow\alpha^{-1}Z^q$. ▷ Le calcul de α^{-1} se fait dans $\mathbb{F}_q$

Exemple 5. Soit $\mathbb{F}_q$ un corps fini et $\mathbb{F}_{q^{12}}$ une extension de degré $n=12$ de $\mathbb{F}_q$. Soit $U\in\mathbb{F}_{q^{12}}$. Ici, l'écriture en binaire de $n-1$ vaut $12-1=11=(1,0,1,1)_2$. L'algorithme 1 procède comme suit pour calculer l'inverse de U.

D'abord dans la phase d'initialisation, on pose $W\leftarrow U$ et $Z\leftarrow U$ car le bit de poids faible de $n-1$ vaut 1. Ensuite on commence la boucle **pour** : on calcule

$$\begin{aligned} W &\leftarrow WW^q=UU^q,\\ Z &\leftarrow WZ^{q^2}=UU^qU^{q^2} \quad (\text{ car } n_1=1),\end{aligned}$$

puis on effectue

$$\begin{aligned} W &\leftarrow WW^{q^2}=UU^qU^{q^2}U^{q^3},\\ Z &\leftarrow Z=UU^qU^{q^2} \quad (\text{ car } n_2=0),\end{aligned}$$

enfin on termine la boucle **pour** avec $n_3=1$

$$\begin{aligned} W &\leftarrow WW^{q^4}=UU^qU^{q^2}U^{q^3}U^{q^4}U^{q^5}U^{q^6}U^{q^7},\\ Z &\leftarrow WZ^{q^8}=UU^qU^{q^2}U^{q^3}U^{q^4}U^{q^5}U^{q^6}U^{q^7}U^{q^8}U^{q^9}U^{q^{10}}.\end{aligned}$$

L'étape suivante dans l'algorithme est le calcul de la norme

$$\alpha\leftarrow UZ^q=UU^qU^{q^2}U^{q^3}U^{q^4}U^{q^5}U^{q^6}U^{q^7}U^{q^8}U^{q^9}U^{q^{10}}U^{q^{11}}=\prod_{i=0}^{n-1}U^{q^i},$$

Et finalement, l'algorithme renvoie $U^{-1}\leftarrow\alpha^{-1}Z^q$, le calcul de l'inverse de $\alpha\in\mathbb{F}_q$ se calculant dans $\mathbb{F}_q$.

♢

L'algorithme 1 est intéressant uniquement si l'élévation à la puissance q (ainsi que l'élévation aux puissance q^{2^i} pour $i\leq\log_2(n)$) est très efficace, car alors (si l'on néglige le coût des élévations à la puissance q ainsi que l'inversion dans $\mathbb{F}_q$ de $\alpha=N(U)$) le coût vaut $\log_2(n)+\omega(n-1)$ multiplications dans $\mathbb{F}_{q^n}$ (où $\omega(n-1)$ est le poids de Hamming de $n-1$, i.e., le nombre de 1 dans la représentation binaire de $n-1$).

- **Deuxième Méthode :** cette méthode utilise la représentation du corps $\mathbb{F}_{q^n}=\mathbb{F}_q[X]/(P)$ où P est un polynôme irréductible de $\mathbb{F}_{q^n}[X]$. Un élément $U\in\mathbb{F}_q[X]/(P)$ peut être vu comme un polynôme en X. Les deux polynômes U et P sont premiers entre eux, ils vérifient donc une relation de Bezout

$$UA+PC=1.$$

Si l'on réduit cette identité modulo P on voit que A est l'inverse de U modulo P. Le calcul de l'inverse A se fait avec l'algorithme d'Euclide étendu que l'on peut trouver dans le livre de Cohen [3] .

Algorithme 2 Inversion d'Euclide étendu

Entrée. $U, P \in \mathbb{F}_q[X]$.
  Initialisation. $A \leftarrow 1, C \leftarrow 0$ et $B_1 \leftarrow U, B_2 \leftarrow P$
  tant que $\deg B_1 \neq 0$ **faire**
    si $\deg B_1 < \deg B_2$ **alors**
      échanger A, C et B_1, B_2.
    $j \leftarrow \deg B_1 - \deg B_2$.
    $B_1 \leftarrow B_1 - \frac{lc(B_1)}{lc(B_2)} X^j B_2, A \leftarrow A - \frac{lc(A)}{lc(C)} C$.
Sortie. A

Où l'on a noté $lc(U)$ le coefficient du monôme de plus haut degré du polynôme U.
Le point important à souligner ici, c'est le fait que la représentation de U en polynôme en X est fondamentale. Dans d'autres représentations (i.e., d'autres bases de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$) il n'est pas possible d'utiliser cette méthode.

- **Troisième Méthode :** Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis et $\mathcal{B}$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Cette troisième méthode pour le calcul de l'inverse d'un élément $U \in \mathbb{F}_q$ s'appuie sur le calcul de l'inverse de la matrice M_U à coefficients dans $\mathbb{F}_q$. Le lemme 1 nous dit que $(M_U)^{-1} = M_{U^{-1}}$. Si on est dans le cas où les coefficients d'un élément U dans $\mathcal{B}$ apparaissent en tant que coefficients de la matrice M_U et si l'on sait calculer l'inverse de M_U efficacement, alors on peut calculer U^{-1} en récupérant dans $M_{U^{-1}} = (M_U)^{-1}$ les coefficients de U^{-1} dans $\mathcal{B}$. Dans ce cas, le calcul de l'inverse se ramène à calculer l'inverse de M_U (plus précisément les coefficients qui nous intéressent dans $(M_U)^{-1}$).

  Exemple 6. Considérons le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3 + X + 1)$ muni de la $\mathbb{F}_2$-base $\mathcal{B}$ définie par les trois éléments

$$e_0 = 1, \quad e_1 = X, \quad e_2 = X^2$$

  Contruisons d'abord les matrices de structures M_s associées à cette base. Pour cela nous exprimons d'abord les produits des éléments de la base

$$\begin{array}{ll} e_0e_0 = 1 = e_0, & e_1e_1 = X^2 = e_2, \\ e_2e_2 = X^4 = X^2 + X = e_2 + e_1, & e_0e_1 = e_1, \\ e_0e_2 = e_2, & e_1e_2 = X^3 = X + 1 = e_0 + e_1. \end{array}$$

  Les matrices de structure M_s sont alors comme suit

$$M_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad M_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

  Pour un élément $U = u_0e_0 + u_1e_1 + u_2e_2$, en utilisant l'expression de M_U donnée

$$M_U = \begin{bmatrix} u_0 & u_2 & u_1 \\ u_1 & u_0 + u_2 & u_1 + u_2 \\ u_2 & u_1 & u_0 + u_2 \end{bmatrix}.$$

Si $V = e_1 + e_2$ on peut calculer M_V et son inverse $(M_V)^{-1}$

$$M_V = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \qquad (M_V)^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

A partir de l'expression de M_U pour un élément U de $\mathbb{F}_{2^3}$, on voit que les coordonnées de U sont dans la première colonne de la matrice M_U. On peut en déduire alors les coordonnées dans $\mathcal{B}$ de V^{-1} avec la première colonne de $M_{V^{-1}} = (M_V)^{-1}$

$$V^{-1} = e_0 + e_1.$$

♢

Nous ne donnons pas d'algorithme dans ce cas. En général les algorithmes d'inversion de matrices s'appuient sur une série d'élimination de Gauss et ce type d'approche pour le calcul d'inverse n'est en général pas très efficace. Nous référons à l'article de Fenn, Benaissa et Taylor [6], pour un exemple de ce type d'approche.

2 Multiplication dans $\mathbb{F}_{q^n}$

L'opération majeure que nous étudierons tout au long de cette thèse est l'opération de multiplication dans $\mathbb{F}_{q^n}$. Il y a plusieurs manières d'effectuer cette opération. Une première méthode consiste à représenter les éléments de $\mathbb{F}_{q^n}$ comme éléments de $\mathbb{F}_q[X]/(P)$ où P est un polynôme irréductible quelconque. Dans le chapitre **??** nous présenterons une méthode pour implanter la multiplication lorsque l'on ne tient pas compte du polynôme générateur P de $\mathbb{F}_{q^n}$. Cette approche a l'avantage de pouvoir injecter de l'aléa dans l'arithmétique du corps, en choisissant P au hasard par exemple, et ainsi brouiller certaines informations lors d'attaques matérielles sur des cryptosystèmes.

L'autre approche pour implanter la multiplication tient compte elle du choix de P, ou plutôt d'une représentation du corps très spécifique qui permet de rendre les calculs plus efficaces. Une grande partie des travaux que l'on verra dans cette thèse s'appuient sur la construction de ¡¡bonnes¿¿ bases pour représenter l'extension de corps $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

2.1 Méthode générale pour le calcul du produit.

La plupart du temps la méthode que nous utiliserons ici pour le calcul du produit se fera en deux étapes

1. Calcul de la matrice M_U à partir des coordonnées de U dans $\mathcal{B}$ et des matrices M_s avec l'expression de M_U donnée par (2).
2. Calcul du produit matrice vecteur $M_U \cdot V$.

Le choix de la base $\mathcal{B}$ sera donc crucial lors du calcul de M_U : en général on cherchera une base $\mathcal{B}$ telle que les matrices de structure M_s soient les plus creuses possible, ce qui permet donc un calcul de M_U le plus simple possible.

2.2 Complexité

Nous présenterons dans cette thèse de nombreux algorithmes pour la multiplication dans les corps finis, dont une grande part concernerons surtout les corps $\mathbb{F}_{2^n}$. Ces algorithmes seront surtout pensés pour être implanter sur circuit, où il est possible de paralléliser de nombreuses opérations. Pour implanter la multiplication dans une extension de corps $\mathbb{F}_{q^n}/\mathbb{F}_q$, nous utiliserons des opérateurs élémentaires dans le corps de base $\mathbb{F}_q$: essentiellement des additionneurs, que l'on notera Add_q, des multiplieurs, noté eux Mult_q, et plus rarement des diviseurs. Lorsque $q = 2$ un additionneur sera une porte XOR et le multiplieur sera une porte AND.

La complexité en espace de l'algorithme correspondra alors au nombre d'additionneurs et de multiplieurs dans $\mathbb{F}_q$nécessairent. La complexité en temps correspondra, elle, au délai de parcours du circuit, i.e., le temps nécessaire pour avoir toutes les données en sorties. La complexité en temps s'exprimera en fonction du délai des différents opérateurs : on notera souvent T_{Add_q} pour le temps de parcours d'un additionneur dans $\mathbb{F}_q$, et T_{Mult_q} pour le temps de parcours d'un multiplieur. D'une manière similaire, pour le cas $q = 2$ on notera T_X le temps de parcours d'une porte XOR et T_A celui d'une porte AND.

Afin d'illustrer cette méthode de calcul de la complexité, nous allons étudier la complexité d'un circuit calculant la multiplication d'une matrice $A \in \mathcal{M}_n(\mathbb{F}_q)$ et d'un vecteur V. Ce calcul consiste en n produits ligne-colonne indépendants $L_i(A) \cdot V$. On dénommera souvent par abus de langage, produit scalaire, ce type de produit. On peut donc paralléliser le calcul de ces produits ligne-colonne. La complexité matérielle sera alors égale à n fois celle d'un produit ligne-colonne, et la complexité en temps sera égale au temps de calcul d'un seul produit ligne-colonne.

Voyons maintenant comment implanter ce type de produit ligne-colonne

$$L \cdot C = \begin{bmatrix} \alpha_1 & \cdot & \alpha_n \end{bmatrix} \cdot \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix} = \sum_{i=1}^{n} \alpha_i \beta_i,$$

Nous calculons les n produits $\mu_i = \alpha_i \beta_i$ en parallèle, ensuite nous additionnons les μ_i à travers un arbre d'addition. La complexité matérielle du produit scalaire est alors de $n\mathrm{Mult}_q$ et de $(n-1)\mathrm{Add}_q$, et la complexité en temps de $T_{Mult_q} + \lceil \log_2(n) \rceil T_{Add_q}$, i.e., le temps de traversée d'un multiplieur de $\mathbb{F}_q$ et d'un arbre d'addition dans $\mathbb{F}_q$.

Nous pouvons maintenant donner la complexité totale d'un produit matrice vecteur : la complexité en espace est égale à $n^2\mathrm{Mult}_q$ et $n(n-1)\mathrm{Add}_q$ et la complexité en temps $T_{Mult_q} + \lceil \log_2(n) \rceil T_{Add_q}$.

2.3 Densité

Le reste de cette section sera consacré à établir un outil pour mesurer la qualité d'une base : la densité d'une base qui mesure la creusité des matrices M_s. Nous donnerons quelques exemples de bases et leur densité, pour finir par une proposition sur la classification des bases minimales (celles qui ont une densité la plus faible possible).

Définition 3 (Poids de Hamming)**.** *Soient une extension de corps finis $\mathbb{F}_{q^n}/\mathbb{F}_q$ et $\mathcal{B} = (e_1, \ldots, e_n)$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Soit $U = u_1 e_1 + \ldots + u_n e_n$ avec $u_i \in \mathbb{F}_q$ un élément de $\mathbb{F}_{q^n}$.*

- *Nous noterons $\omega_{\mathcal{B}}(U)$ le poids de Hamming de U relativement à $\mathcal{B}$ le nombre de coefficients u_i non nuls.*

- *De la même manière, pour une matrice A à coefficients dans $\mathbb{F}_q$, son poids de Hamming $\omega(A)$ sera le nombre de coefficients non nuls de A.*

Si la base sur laquelle est défini le poids de Hamming d'un élément U ne fait pas d'ambiguité nous le noterons simplement $\omega(U)$.

Définition 4 (Densité [23])**.** *Soit une extension de corps finis $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathcal{B}$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$ et $M_1, \ldots, M_n$ les matrices de structure associées à $\mathcal{B}$. On définit $d(\mathcal{B})$ la densité de $\mathcal{B}$ par*

$$d(\mathcal{B}) = \frac{1}{n}\left(\sum_{i=s}^{n} \omega(M_s)\right). \tag{5}$$

La densité d'une base mesure la densité moyenne des matrices de structure M_s associées. L'expression de la densité d'une base peut être réexprimée de la manière suivante.

Lemme 2. *Soient $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis et $\mathcal{B} = (e_1, \ldots, e_n)$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$, alors*

$$d(\mathcal{B}) = \frac{1}{n} \sum_{i,j=1,\ldots,n} \omega_{\mathcal{B}}(e_i e_j). \tag{6}$$

Exemple 7. Nous avons vu dans l'exemple 2 que la base $\mathcal{B}$ formée des trois éléments $e_1 = X - 1, e_2 = X^2 + X + 1, e_3 = X$ de $\mathbb{F}_{3^3} = \mathbb{F}_3[X]/(X^3 - X - 1)$ avait les matrices de structure M_s suivantes

$$M_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix},\ M_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},\ M_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

Cette base a donc une densité de

$$d(\mathcal{B}) = \frac{1}{3}\left(\omega(M_1) + \omega(M_2) + \omega(M_3)\right) = \frac{1}{3}(4 + 7 + 5) = \frac{16}{3}$$

D'autre part dans l'exemple 2 nous avions exprimé les produits $e_i e_j$ dans la base $\mathcal{B}$

$$\begin{array}{rclcrcl} e_1e_1 & = & X^2 + X + 1 = e_2, & & e_2e_2 & = & X^4 + 1 - X - X^3 = X^2 - X = e_2 + e_1, \\ e_3e_3 & = & X^2 = e_2 + e_1 + e_3, & & e_1e_2 & = & X^3 - 1 = e_3, \\ e_1e_3 & = & X^2 - X = e_2 + e_1, & & e_2e_3 & = & X^3 + X^2 + X = e_2 + e_3. \end{array} \tag{7}$$

Alors si l'on calcule

$$\frac{1}{3} \sum_{i,j=1,2,3} \omega(e_i e_j) = \frac{1}{3}(1 + 2 + 3 + 2(1 + 2 + 2)) = \frac{16}{3},$$

on remarque que l'identité (6) du lemme est vérifiée dans ce cas.

♢

Exemple 8.

1. Soit $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(X^n - \alpha)$. Si l'on définit la $\mathbb{F}_q$-base $\mathcal{B} = (1, X, X^2, \ldots, X^n)$, on a $d(\mathcal{B}) = n$.

2. Considérons le corps $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(X^n - \alpha X - \beta)$ avec $\alpha \neq 0$. Soit $\mathcal{B} = (1, X, \ldots, X^{n-1})$. Pour calculer la densité de la base on va exprimer les produits $X^i X^j$ dans $\mathcal{B}$

$$X^i X^j = \begin{cases} X^{i+j} & \text{si } i+j < n, \\ \alpha X^{i+j-n+1} + \beta X^{i+j-n} & \text{si } i+j \geq n. \end{cases}$$

On en déduit l'expressions suivante de la densité

$$nd(\mathcal{B}) = \#\{(i,j) \mid i+j < n\} + 2\,\#\{(i,j) \mid i+j \geq n\} = n\left(\frac{3n-1}{2}\right).$$

Ce qui donne finalement $d(\mathcal{B}) = \frac{3n-1}{2}$.

3. Soit un polynôme $P = \sum_{m=0}^{r} X^{m\Delta} \in \mathbb{F}_2[X]$ supposé irréductible et soit $n = r\Delta$. Considérons le corps $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ et calculons la densité de la $\mathbb{F}_2$-base $\mathcal{B} = (1, X, \ldots, X^n)$. Nous avons

$$X^i X^j = \begin{cases} X^{i+j} & \text{si } i+j < n, \\ \sum_{m=0}^{r-1} X^{i+j-(r-m)\Delta} & \text{si } n \leq i+j < (r+1)\Delta, \\ X^{i+j-(r+1)\Delta} & \text{si } i+j \geq (r+1)\Delta. \end{cases}$$

Nous en déduisons que

$$\begin{aligned} nd(\mathcal{B}) &= \#\{(i,j) | i+j < n\} \;+\; \#\{(i,j) | i+j \geq (r+1)\Delta\} \\ &+ \; r\,\#\{(i,j) | r\Delta \leq i+j < (r+1)\Delta\} \\ &= n\frac{n+1}{2} + \frac{(n-(\Delta+1))(n-\Delta)}{2} + r\frac{\Delta(2n-(\Delta+1))}{2} \\ &= n\left(\frac{3n-1}{2} + \frac{\Delta(\frac{\Delta+1}{n} - 3)}{2}\right). \end{aligned}$$

♢

Nous avons la propriété suivante sur certaines spécificités des matrices de structure M_s associées à une base $\mathcal{B}$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.

Propriété 1. *Soit $\mathcal{B}$ une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$, et $M_1, \ldots, M_n$ les matrices de structure associées à $\mathcal{B}$. Alors nous avons*

1. $\det M_s \neq 0$ *pour tout* $s = 1, \ldots, n$
2. *Les n matrices $M_1, \ldots, M_n$ sont $\mathbb{F}_q$-linéairement indépendantes.*

Démonstration. Montrons que pour tout $s = 1, \ldots, n$, M_s est inversible. Raisonnons par l'absurde et supposons que pour un entier $s_0 \in \{1, \ldots, n\}$ nous avons $\det(M_{s_0}) = 0$. Il existe alors $U \neq 0 \in \mathbb{F}_{q^n}$ tel que ${}^tU \cdot M_{s_0} = 0$. Au vu de l'équation (2), la matrice M_U est donnée par

$$M_U = \begin{bmatrix} ({}^tU) \cdot M_1 \\ \vdots \\ ({}^tU) \cdot M_n \end{bmatrix},$$

ce qui montre que la matrice de l'application $\phi_U : V \mapsto UV$ a une ligne nulle : la ligne d'indice s_0, et donc ϕ_U n'est pas un isomorphisme ce qui contredit le résultat du lemme 1 sur l'inverse de M_U.

Démontrons le second point du lemme. Supposons que l'on aie une relation non triviale

$$\sum_{s=1}^{n} \alpha_s M_s = 0. \tag{8}$$

Si l'on multiplie (8) à gauche par ${}^tU$ et à droite par V, on obtient

$$\sum_{s=1}^{n} \alpha_s ({}^tU \cdot M_s \cdot V) = 0.$$

Nous voyons que pour $U, V \neq 0 \in \mathbb{F}_{q^n}$ quelconque, le produit $W = M_U \cdot V$ a ses coordonnées $w_s = {}^tU \cdot M_s \cdot V$ dans l'hyperplan d'équation $\sum_{s=1}^{n} \alpha_s x_s = 0$ de $\mathbb{F}_{q^n}$. Ceci contredirait le fait que M_U soit inversible, car l'application $V \mapsto M_U \cdot V$ enverrait tout élément V dans l'hyperplan d'équation $\sum_{s=0}^{n} \alpha_s x_s = 0$ et ne serait donc pas surjective. □

Ci-dessous on définit une relation d'équivalence entre deux bases.

Définition 5. *On dit que deux bases $\mathcal{B} = (e_1, \ldots, e_n)$, $\mathcal{B}' = (f_1, \ldots, f_n)$ sont équivalentes si il existe des éléments $\alpha_i \in \mathbb{F}_q^\times$ pour $i = 1, \ldots, n$ et une permutation $\sigma \in \mathcal{S}_n$ tels que $e_i = \alpha_i f_{\sigma(i)}$.*

Deux bases équivalentes vont en fait donner, d'une part une représentation du corps $\mathbb{F}_{q^n}$ très proche, et d'autre part une multiplication d'égale efficacité comme on le voit à travers le lemme suivant.

Lemme 3. *Soit $\mathcal{B}$, $\mathcal{B}'$ deux $\mathbb{F}_q$-bases équivalentes de $\mathbb{F}_{q^n}$. Si $M_s = [\lambda_{i,j}(s)]_{i,j=1,\ldots,n}$ et $M'_s = [\lambda'_{i,j}(s)]_{i,j=1,\ldots,n}$ sont les matrices de structure d'indice s associées à $\mathcal{B}$ et $\mathcal{B}'$ respectivement. Alors nous avons*

1. $\lambda_{i,j}(s) = \alpha_i \alpha_j \lambda'_{\sigma(i),\sigma(j)}(s)$
2. $d(\mathcal{B}') = d(\mathcal{B})$.

Pour finir ce chapitre nous nous intéressons aux bases minimales de $\mathbb{F}_{q^n}$. Celles-ci sont les meilleures bases que l'on puisse trouver pour implanter l'arithmétique dans une extension de corps, car elles ont une densité la plus faible possible, i.e., égale à n.

Proposition 1 ([23])**.** *Pour toute $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$, nous avons $d(\mathcal{B}) \geq n$. De plus si $d(\mathcal{B}) = n$ il existe alors $j \in \{1, \ldots, n\}$ et $\alpha \in \mathbb{F}_q$ tels que $\mathcal{B}$ soit équivalente à $(1, e_j, e_j^2, \ldots, e_j^{n-1})$ et $e_j^n - \alpha = 0$.*

Démonstration. Voyons d'abord que pour toute base $\mathcal{B}$, $d(\mathcal{B}) \geq n$. Nous allons pour montrer cette inégalité établir que pour tout s, la matrice de structure M_s a au moins n coefficients non nuls. On a vu dans la propriété 1 que les M_s étaient inversibles. Elles ont alors dans chaque colonne au moins un coefficient non nul. Autrement dit $\omega(M_s) \geq n$, et par conséquent

$$d(\mathcal{B}) = \frac{1}{n} \sum_{s=1}^{n} \omega(M_s) \geq \frac{1}{n} \sum_{s=1}^{n} n = n.$$

Nous allons montrer maintenant que si une base $\mathcal{B}$ vérifie $d(\mathcal{B}) = n$ il existe alors un élément e_j de $\mathcal{B}$ et $\alpha \in \mathbb{F}_q$ tels que $\mathcal{B}$ soit équivalente à $(1, e_j, e_j^2, \ldots, e_j^{n-1})$ et que $e_j^n - \alpha = 0$.

Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une telle base. D'après l'identité

$$d(\mathcal{B}) = \frac{1}{n} \sum_{i,j=1,\ldots,n} \omega(e_i e_j),$$

pour que l'on ait $d(\mathcal{B}) = n$ il faut que $\omega(e_i e_j) = 1$ pour tout i, j . Ceci est équivalent au fait que pour tout i, j, il existe un entier $s_j \in \{1, \ldots, n\}$ et $\alpha_j \in \mathbb{F}_q^\times$ tels que $e_i e_j = \alpha_j e_{s_j}$. Nous allons construire des permutations de $\{1, \ldots, n\}$ qui envoient j sur s_j.

Pour cela fixons le i et faisons varier le j parmi $\{1, \ldots, n\}$. Nous pouvons pour chaque j associer le s_j correspondant et nous obtenons une application

$$\begin{array}{rccc} \sigma_i\colon & \{1, \ldots, n\} & \to & \{1, \ldots, \} \\ & j & \mapsto & \sigma_i(j) \end{array}$$

telle que $\sigma_i(j) = s_j$. Montrons que σ_i est bijective. Par construction de σ_i nous avons

$$\begin{array}{rcl} \mathrm{Vect}(e_i e_1, e_i e_2, \ldots, e_i e_n) & = & \mathrm{Vect}(\alpha_1 e_{\sigma_i(1)}, \ldots, \alpha_n e_{\sigma_i(n)}) \\ & = & \mathrm{Vect}(e_{\sigma_i(1)}, \ldots, e_{\sigma_i(n)}). \end{array}$$

Si σ_i n'était pas bijective, le dernier espace serait de dimension $< n$. L'application ϕ_{e_i} qui envoie un élément de $\mathbb{F}_{q^n}$ sur $\phi_{e_i}(V) = e_i V$ serait à valeur dans $\mathrm{Vect}(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ et donc ne serait pas un isomophisme de $\mathbb{F}_{q^n}$ ce qui contredirait le lemme 1.

Maintenant, regardons ce que valent les puissances successives de e_i

$$\begin{array}{rcl} e_i^2 & = & \alpha_i e_{\sigma_i(i)} = \beta_2 e_{\sigma_i(i)}, \\ e_i^3 & = & e_i (e_i)^2 = \alpha_i (e_i e_{\sigma_i(i)}) = \alpha_i \alpha_{\sigma_i(i)} e_{\sigma_i^2(i)} = \beta_3 e_{\sigma_i^2(i)}, \\ \vdots & & \vdots \\ e_i^{m+1} & = & \beta_{m+1} e_{\sigma_i^m(i)}. \end{array}$$

Au bout d'un nombre $n_i \leq n$ d'itérations, on doit tomber sur $e_i^{n_i+1} = \beta_{n_i+1} e_i$, ce n_i vérifiant $\sigma_i^{n_i}(i) = i$. En divisant l'équation $e_i^{n_i+1} = \beta_{n_i+1} e_i$ par e_i on obtient $e_i^{n_i} = \beta_{n_i+1}$. Donc pour chaque élément e_i de la base nous avons montré qu'il était racine d'un polynôme $X^{n_i} - \beta_i$ avec $n_i \leq n$.

Maintenant il s'agit de déterminer l'entier i tel que tout e_j s'écrit comme une puissance de e_i. Pour cela nous considérons le sous-ensemble G de $\mathbb{F}_{q^n}^\times$

$$G = \left\{ \mu e_i \mid \mu \in \mathbb{F}_q^\times \text{ et } i \in \{1, \ldots, n\} \right\}.$$

Nous allons démontrer que G est un sous-groupe de $\mathbb{F}_{q^n}^\times$, pour cela il suffit de montrer que G est stable par multiplication. Soit $\mu_1 e_{i_1}$ et $\mu_2 e_{i_2}$ deux éléments de G, leur produit est donné par

$$\begin{array}{rcl} \mu_1 e_{i_1} \mu_2 e_{i_2} & = & \mu_1 \mu_2 \alpha_{i_2} e_{\sigma_{i_1}(i_2)} \\ & = & \rho e_{\sigma_{i_1}(i_2)} \in G, \end{array}$$

avec $\rho = \mu_1 \mu_2 \alpha_{i_2} \in \mathbb{F}_q$.

Comme G est un sous-groupe de $\mathbb{F}_{q^n}^\times$ il est cyclique et admet donc un générateur $\mu_0 e_{i_0}$. Nous savons que

$$e_{i_0}^{n_{i_0}} = \beta_{i_0}.$$

et du fait que $\mu_0 e_{i_0}$ est un générateur de G, il existe pour tout $i \in \{1, \ldots, n\}$ un $\rho_i \in \mathbb{F}_q$ et un entier $1 \leq m_i$ tels que $e_i = \rho_i e_{i_0}^{m_i}$. Après réduction avec l'identité $e_{i_0}^{n_{i_0}} = \beta_{i_0}$, on peut supposer le $m_i < n_{i_0} \leq n$.

Finalement, du fait que les e_i sont linéairement indépendants on doit avoir $n_{i_0} = n$ et $\mathcal{B}$ équivalente à $(1, e_{i_0}, \ldots, e_{i_0}^{n-1})$. □

Base Polynômiale

Ce chapitre est consacré à la description des opérateurs arithmétiques lorsque l'on utilise une représentation du corps en base polynômiale. Ces bases sont très utilisées pour implanter l'arithmétique dans les extensions de corps et de nombreux travaux ont été publiés sur ce sujet [19, 24, 22, 12, 1].

Nous allons partager l'étude de ce type de multiplieur en traitant d'abord le cas $\mathbb{F}_{2^n}$, puis le cas $\mathbb{F}_{q^n}$.

Nous construirons le multiplieur de Mastrovito [12] pour les corps $\mathbb{F}_{2^n}[X]/(P)$, d'abord dans le cas où P est un polynôme irréductible quelconque $P = 1 + X^{k_1} + \ldots, +X^{k_r} + X^n$. Nous présenterons ensuite le multiplieur de Mastrovito dans le cas particulier où $P = X^n + X^k + 1$ est un trinôme tel que $k \geq 2$, et nous verrons que sa complexité matérielle est de n^2 AND et $(n^2 - k - 1)$ XOR et sa complexité en temps est de $T_A + (2 + \lceil \log_2(n) \rceil)T_X$.

Ensuite nous présenterons l'algorithme de Koc et Rodriguez [22] pour multiplier modulo un pentanôme. Nous verrons que ce multiplieur a une complexité matérielle de n^2 AND et $((n-1)^2 + 3n + 2m - 1)$ XOR et temporelle de $T_A + (3 + \lceil \log_2(n) \rceil)T_X$. Pour finir, nous nous intéresserons aux polynômes équirépartis, et nous présenterons le multiplieur de Koc et Halbutogullari de [12].

Pour les corps $\mathbb{F}_{q^n}$, nous nous intéresserons dans un premier temps aux corps définis par un binômes. Nous établirons un multiplieur dans ces corps, et une méthode d'élévation à la puissance q. Nous clôturerons ce chapitre avec les corps $\mathbb{F}_{q^n}$ définis par un trinôme. Nous construirons un multiplieur dans ce corps, et nous verrons, lorsque $q = 3$, une méthode pour élever au cube un élément de $\mathbb{F}_{3^n}$.

3 Prérequis

La construction d'une base polynômiale consiste à prendre comme éléments de la base les puissances successives d'un élément $\zeta \in \mathbb{F}_{q^n}$,

$$1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}.$$

Bien sûr il faut s'assurer que ce procédé nous donne bien un système libre sur $\mathbb{F}_q$.

Définition 6. *Soit une extension de corps fini $\mathbb{F}_{q^n}/\mathbb{F}_q$. Nous appellerons base polynômiale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ une base du type $\mathcal{B} = (1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$ où $\zeta \in \mathbb{F}_{q^n}$.*

Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible et soit $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ l'extension définie par P. La représentation de $\mathbb{F}_{q^n}$ par $\mathbb{F}_q[X]/(P)$ nous fournit directement la $\mathbb{F}_q$-base polynômiale $(1, X, \ldots, X^{n-1})$. C'est avec ce type de représentation et de base associée que nous travaillerons le plus souvent dans la suite de ce chapitre.

Les éléments du corps peuvent, dans ce cas, être vus comme des polynômes en X de degré $\leq n - 1$. Ceci nous permettra souvent d'utiliser l'arithmétique des polynômes de $\mathbb{F}_q[X]$ pour implanter l'arithmétique dans le corps $\mathbb{F}_{q^n}$.

Soit $U = \sum_{i=0}^{n-1} u_i X^i$ un élément de $\mathbb{F}_2[X]/(P)$. Si l'on définit les deux sous $\mathbb{F}_q$-espaces vectoriels de $\mathbb{F}_q[X]$

$$E = \mathrm{Vect}(1, X, \ldots, X^{n-1}),$$
$$F = \mathrm{Vect}(1, X, \ldots, X^{2n-1}),$$

la multiplication par le polynôme U induit une application $\mathbb{F}_q$-linéaire

$$\begin{array}{rccc} \widehat{\phi}_U : & E & \to & F \\ & V & \mapsto & UV \end{array}$$

L'image d'un polynôme V par $\widehat{\phi}_U$ est le polynôme produit UV. On peut écrire la matrice $\widehat{M_U}$ de $\widehat{\phi}_U$ dans les bases polynômiales de E et F

$$\widehat{M_U} = \begin{bmatrix} u_0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ u_1 & u_0 & 0 & 0 & \cdots & 0 & 0 \\ u_2 & u_1 & u_0 & 0 & \cdots & 0 & 0 \\ \vdots & & \vdots & & \ddots & \vdots & \vdots \\ u_{n-2} & u_{n-3} & u_{n-4} & u_{n-5} & \cdots & u_0 & 0 \\ u_{n-1} & u_{n-2} & u_{n-3} & u_{n-4} & \cdots & u_1 & u_0 \\ 0 & u_{n-1} & u_{n-2} & u_{n-3} & \cdots & u_2 & u_1 \\ 0 & 0 & u_{n-1} & u_{n-2} & \cdots & u_3 & u_2 \\ \vdots & & \vdots & \ddots & & \vdots & \vdots \\ \vdots & & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u_{n-1} & u_{n-2} \\ 0 & 0 & 0 & 0 & \cdots & 0 & u_{n-1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Par ailleurs, nous noterons M_U la matrice relativement à la base polynômiale $(1, X, \ldots, X^{n-1})$ de $\mathbb{F}_{q^n}$ de l'application ϕ_U suivante

$$\begin{array}{rccc} \phi_U : & \mathbb{F}_{q^n} & \to & \mathbb{F}_{q^n} \\ & V & \mapsto & UV \end{array}$$

On peut voir ϕ_U comme une version réduite de l'application $\widehat{\phi}_U$, et d'une manière similaire M_U une version réduite modulo P de $\widehat{M_U}$.

Nous avons deux stratégies possibles pour implanter le calcul du produit $W = UV \mod P$:

1. La première consiste à effectuer le produit matrice vecteur $W' = \widehat{M_U} \cdot V$, c'est-à-dire calculer le produit des polynômes U et V, et ensuite réduire le polynôme W' modulo P pour trouver l'expression du produit dans la base polynômiale de $\mathbb{F}_{q^n}$.
2. La seconde stratégie consiste à réduire, non le produit W' des polynômes U et V, mais la matrice $\widehat{M_U}$. En un certain sens nous utilisons une technique de réduction pour calculer M_U la matrice de multiplication par U dans la base polynômiale $(1, X, \ldots, X^{n-1})$ de $\mathbb{F}_{q^n}$. C'est seulement après avoir calculé M_U que nous en déduisons le produit de U et V dans $\mathbb{F}_{q^n}$, exprimé dans $(1, X, \ldots, X^{n-1})$ en effectuant le produit $M_U V$.

C'est la seconde méthode que nous utiliserons le plus souvent, la première nous sera utile dans le cas où P sera un pentanôme (cf. section 4.3).

4 Corps binaire

Nous allons dans un premier temps nous intéresser au cas d'un polynôme irréductible général P définissant le corps $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$. Nous verrons ensuite les cas particuliers où l'on peut tirer parti d'une spécificité de P.

4.1 Base polynômiale pour un polynôme général

Dans cette section nous présentons le multiplieur proposé par Koc et Halbutogullari dans [12] pour un polynôme irréductible quelconque de $\mathbb{F}_2[X]$. Ce multiplieur est en fait une version légèrement modifiée du multiplieur original de Mastrovito [19]. Koc et Halbutogullari ont simplement amélioré la complexité matérielle du multiplieur de Mastrovito.

Fixons $P = 1 + X^{k_1} + \cdots + X^{k_r} + X^n \in \mathbb{F}_2[X]$, où $0 < k_1 < \cdots < k_r < n$, un polynôme irréductible et $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$. Notons $l_1 = n - k_1, \ldots, l_r = n - k_r$. C'est la deuxième stratégie que nous allons mettre ici en place pour calculer un produit UV modulo P, c'est-à-dire que nous allons calculer par des méthodes de réductions la matrice M_U de ϕ_U dans la base polynômiale de $\mathbb{F}_{2^n}$, et ensuite calculer le produit matriciel $M_U \cdot V$. Pour cela nous aurons besoin de l'opérateur de réduction $R\colon F \to F$ défini par

$$R(X^i) = \begin{cases} X^i & \text{si } i \leq n-1 \\ X^{i-n} + \sum_{i=1}^{r} X^{i-l_i} & \text{si } n \leq i \end{cases}$$

Nous confondrons par la suite l'opérateur R avec sa matrice dans la base polynômiale de l'espace vectoriel F. Cet opérateur va nous permettre de réduire progressivement la matrice $\widehat{M_U}$ en faisant monter dans la partie haute de la matrice les coefficients de la partie basse de $\widehat{M_U}$. La part important de notre travail ici, va être de décrire ce processus de réduction.

Nous allons couper en deux les matrices $2n \times 2$, pour pouvoir les manipuler plus facilement.

Notation. Soit A une matrice $2n \times n$, on notera $(A)_H$ la sous matrice carrée d'ordre n de A constituée des n premières lignes, et $(A)_B$ la sous matrice carrée constituée des n dernières lignes.

Notation. Soit A une matrice carrée d'ordre n à coefficient dans $\mathbb{F}_2$. Nous noterons

- $A[\leftarrow l]$ (resp. $A[\rightarrow l]$) la matrice dont les l dernières colonnes sont nulles (resp. les l premières), et $(A[\rightarrow l])_{i,j} = A_{i,j+l}$ pour $j \leq n - l$ (resp. $(A[\rightarrow l])_{i,j} = A_{i,j-l}$ pour $l \geq j$).
- $A[\uparrow l]$ (resp $A[\downarrow l]$) la matrice dont les l dernières lignes sont nulles (resp. les l premières) et $(A[\rightarrow l])_{i,j} = A_{i+l,j}$ pour $i \leq n - l$ (resp. $(A[\rightarrow l])_{i,j} = A_{i-l,j}$ pour $l \geq i$).

L'opérateur de réduction R agit sur les matrices $2n \times n$ en réduisant partiellement modulo P les X^i pour $i \geq n$. Plus précisément nous avons le résultat suivant.

Lemme 4. *Soit A une matrice $2n \times n$, décomposée en (A_H, A_B). Alors la matrice $R \cdot A$ vérifie*

$$(R \cdot A)_H = A_H + A_B + \sum_{i=1}^{r} A_B[\downarrow k_i] \quad \text{et} \quad (R \cdot A)_B = \sum_{i=1}^{r} A_B[\uparrow l_i].$$

Exemple 9. Soit $P = X^5 + X^3 + X^2 + 1$ et $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(P)$, $U = u_0 + u_1X + u_2X^2 + u_3X^3 + u_4X^4 \in \mathbb{F}_{2^5}$. La matrice $\widehat{M_U}$ dans ce cas est donnée par

$$(\widehat{M_U})_H = \begin{bmatrix} u_0 & 0 & 0 & 0 & 0 \\ u_1 & u_0 & 0 & 0 & 0 \\ u_2 & u_1 & u_0 & 0 & 0 \\ u_3 & u_2 & u_1 & u_0 & 0 \\ u_4 & u_3 & u_2 & u_1 & u_0 \end{bmatrix}, \quad (\widehat{M_U})_B = \begin{bmatrix} 0 & u_4 & u_3 & u_2 & u_1 \\ 0 & 0 & u_4 & u_3 & u_2 \\ 0 & 0 & 0 & u_4 & u_3 \\ 0 & 0 & 0 & 0 & u_4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Étudions le processus de réduction du lemme 4 : si l'on applique l'opérateur R à $\widehat{M_U}$ nous obtenons pour $(R \cdot \widehat{M_U})_H$

$$(R \cdot \widehat{M_U})_H = \begin{bmatrix} u_0 & 0 & 0 & 0 & 0 \\ u_1 & u_0 & 0 & 0 & 0 \\ u_2 & u_1 & u_0 & 0 & 0 \\ u_3 & u_2 & u_1 & u_0 & 0 \\ u_4 & u_3 & u_2 & u_1 & u_0 \end{bmatrix} + \begin{bmatrix} 0 & u_4 & u_3 & u_2 & u_1 \\ 0 & 0 & u_4 & u_3 & u_2 \\ 0 & 0 & 0 & u_4 & u_3 \\ 0 & 0 & 0 & 0 & u_4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & u_4 & u_3 & u_2 & u_1 \\ 0 & 0 & u_4 & u_3 & u_2 \\ 0 & 0 & 0 & u_4 & u_3 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & u_4 & u_3 & u_2 & u_1 \\ 0 & 0 & u_4 & u_3 & u_2 \end{bmatrix}.$$

Pour $(R\widehat{M_U})_B$ on obtient

$$(R \cdot \widehat{M_U})_B = \begin{bmatrix} 0 & 0 & 0 & 0 & u_4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & u_4 & u_3 \\ 0 & 0 & 0 & 0 & u_4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

♢

C'est en appliquant plusieurs fois R à $\widehat{M_U}$ que nous obtiendrons la matrice réduite M_U de l'application ϕ_U de multiplication par U dans $\mathbb{F}_{q^n}$.

Tout d'abord nous remarquons que R réduit le degré d'un polynôme $V \in F$ en $\deg(R \cdot V) \leq \max(n-1, \deg V - l_r)$. En appliquant i fois R à V, nous avons le résultat suivant sur la majoration du degré de $R^i \cdot V$.

Lemme 5. *Soit $V \in F$ alors nous avons* $\deg(R^i \cdot V) \leq \max(n-1, \deg V - il_r)$

En conséquence si nous appliquons R à un V de degré $\leq 2n-2$ un nombre $c = \lceil \frac{n-1}{n-k_r} \rceil$ de fois, nous aurons $\deg(R^c \cdot V) \leq n-1$. Autrement dit R^c enverra tout polynôme de F de degré $\leq 2n-2$ dans E et $R^c \cdot \widehat{M_U}$ sera à valeur dans E, car le produit de deux polynômes $U, V \in E$ est de degré $\leq 2n-2$.

Lemme 6 ([12])**.** *La matrice M_U de la multiplication par U dans la base polynômiale de $\mathbb{F}_2[X]/(P)$ est donnée par $(R^c \cdot \widehat{M_U})_H$ où l'entier c est défini par $c = \lceil \frac{n-1}{n-k_r} \rceil$.*

Nous avons vu comment R agissait sur une matrice A dans le lemme 4. Nous avons besoin de connaître l'action de l'itérée R^c sur $\widehat{M_U}$ pour calculer $M_U = (R^c \cdot \widehat{M_U})_H$. C'est ce que nous allons voir dans la proposition qui suit.

Proposition 2 ([12])**.** *Soit i un entier, R l'opérateur de réduction et $\widehat{M_U}$ la matrice de l'application $\widehat{\phi_U}$. Si l'on définit les suites de matrice Γ_i et Λ_i par*

$$\begin{gathered} \Gamma_0 = (\widehat{M_U})_B, \text{ et pour } i \geq 1, \Gamma_i = \sum_{j=1}^{r} \Gamma_{i-1}[\uparrow l_j], \\ \Lambda_0 = 0, \text{ et pour } i \geq 1, \Lambda_i = \Lambda_{i-1} + \Gamma_i. \end{gathered} \tag{9}$$

Alors on a

$$(R^i \cdot \widehat{M_U})_H = (\widehat{M_U})_H + \Lambda_i + \sum_{j=1}^{r} \Lambda_i[\downarrow k_j], \tag{10}$$

et

$$(R^i \cdot \widehat{M_U})_B = \Gamma_i.$$

Démonstration. Nous allons le montrer par récurrence sur i. Pour $i = 0$ l'assertion est vraie car

$$(R^0 \cdot \widehat{M_U})_H = (\widehat{M_U})_H = (\widehat{M_U})_H + \Lambda_0 + \sum_{j=1}^{r} \Lambda_0[\downarrow k_j],$$

vu que $\Lambda_0 = 0$ et $\Gamma_0 = (\widehat{M_U})_B$. Pour $i = 1$ il s'agit juste une réécriture du lemme 4.

Supposons le vrai au rang i et montrons le pour $i+1$. En appliquant le lemme 4 à la matrice $A = R^i \cdot \widehat{M_U}$ nous avons

$$(R^{i+1} \cdot \widehat{M_U})_H = (R^i \cdot \widehat{M_U})_H + (R^i \cdot \widehat{M_U})_B + \sum_{j=1}^{r} (R^i \cdot \widehat{M_U})_B[\downarrow k_j], \tag{11}$$

et

$$(R^{i+1} \cdot \widehat{M_U})_B = \sum_{j=1}^{r} (R^i \cdot \widehat{M_U})_B[\uparrow l_j]. \tag{12}$$

Par hypothèse de récurrence, nous avons

$$(R^i \cdot \widehat{M_U})_H = (\widehat{M_U})_H + \Lambda_i + \sum_{j=1}^{r} \Lambda_i[\downarrow k_j] \text{ et } (R^i \cdot \widehat{M_U})_B = \Gamma_i.$$

En remplaçant $(R^i \cdot \widehat{M_U})_H$ et $(R^i \cdot \widehat{M_U})_B$ dans l'expression (11) de $(R^{i+1} \cdot \widehat{M_U})_H$ nous obtenons

$$\begin{aligned}(R^{i+1} \cdot \widehat{M_U})_H &= ((\widehat{M_U})_H + \Lambda_i + \sum_{j=1}^{r} \Lambda_i[\downarrow k_j]) + \Gamma_i + \sum_{j=1}^{r} \Gamma_i[\downarrow k_j] \\ &= (\widehat{M_U})_H + (\Lambda_i + \Gamma_i) + \sum_{j=1}^{r} (\Lambda_i + \Gamma_i)[\downarrow k_j],\end{aligned}$$

or comme $\Lambda_{i+1} = \Lambda_i + \Gamma_i$, nous avons bien l'égalité cherchée pour $(R^{i+1}\widehat{M_U})_H$. Pour $(R^{i+1} \cdot \widehat{M_U})_B$, du fait que, par hypothèse de récurrence $(R^i \cdot \widehat{M_U})_B = \Gamma_i$, nous obtenons par (12) que $(R^{i+1} \cdot \widehat{M_U})_B$ est donné par

$$(R^{i+1} \cdot \widehat{M_U})_B = \sum_{j=1}^{r} \Gamma_i[\uparrow l_j] = \Gamma_{i+1}.$$

Ce qui termine la preuve. □

Le calcul de M_U se fait donc en deux étapes

- *Première étape.* Le calcul de Λ_c avec la relation de récurrence (9).
- *Deuxième étape.* Le calcul de M_U suivant la formule (10)

$$M_U = (R^c \cdot \widehat{M_U})_H = (\widehat{M_U})_H + \Lambda_c + \sum_{j=1}^{r} \Lambda_c[\downarrow k_j].$$

Soulignons un fait important : les matrices dans (9) et dans (10) sont des matrices de Toeplitz. C'est cela qui va nous permettre d'économiser de nombreuses opérations lors du calcul des coefficients de M_U.

Définition 7 (Matrice de Toeplitz)**.** *Soit A une matrice $n \times m$, on dit que A est de Toeplitz si le coefficient $(A)_{i,j}$ de A d'indice i, j vérifie $(A)_{i,j} = (A)_{i+1,j+1}$.*

Autrement dit, les coefficients d'une matrice de Toeplitz sont constants par déplacement diagonal. Cette propriété est intéressante ici du fait que si une matrice est de Toeplitz, seuls les termes de la première ligne et de la première colonne vont donner tous les coefficients de la matrice. Les matrices de Toeplitz ont les propriétés immédiates suivantes

Propriété 2. *Soit $A = [\alpha_{i,j}]_{i=1,\dots,n,j=1,\dots,m}$ et $A' = [\alpha'_{i,j}]_{i=1,\dots,n,j=1,\dots,m}$ deux matrices de Toeplitz $n \times m$ alors*

1. *$A + A'$ est de Toeplitz.*
2. *Si A est en plus triangulaire supérieure (resp. triangulaire inférieure) alors pour $k \geq 0$ on a $A[\uparrow k]$ et $A[\rightarrow k]$ (resp. $A[\downarrow k]$ et $A[\leftarrow k]$).*
3. *Pour tout $1 \leq i_1 \leq i_2 \leq n$ et $1 \leq j_1 \leq j_2 \leq m$ la matrice $[\alpha_{i,j}]_{i=i_1,\dots,i_2,j=j_1,\dots,j_2}$ est de Toeplitz.*

On va voir que les matrices Λ_i sont de Toeplitz et en particulier Λ_c sera aussi de Toeplitz. Ceci va ramener le calcul de Λ_c au calcul de sa première ligne, car Λ_c est triangulaire supérieure.

Lemme 7. *Soient Λ_i et Γ_i les matrices définies dans la proposition 2 par*

$$\Gamma_0 = (\widehat{M_U})_B, \text{ et pour } i \geq 1, \Gamma_i = \sum_{j=0}^{r} \Gamma_{i-1}[\uparrow l_j],$$
$$\Lambda_0 = 0, \text{ et pour } i \geq 1, \Lambda_i = \Lambda_{i-1} + \Gamma_i.$$

Ces matrices sont de Toeplitz, triangulaires supérieures avec une diagonale nulle.

Démonstration. On va le démontrer par récurrence sur i en utilisant le 1 et le 2 de la propriété 2.

Occupons nous d'abord de Γ_i. Pour $i = 0$, on voit bien que $\Gamma_0 = (\widehat{M_U})_B$ est de Toeplitz et triangulaire supérieure, avec une diagonale nulle. On suppose alors l'assertion vrai jusqu'au rang i, et on va le montrer pour le rang $i + 1$. Nous savons par hypothèse de récurrence que Γ_i est de Toeplitz et triangulaire supérieure avec une diagonale nulle, donc les matrices $\Gamma_i[\uparrow k_j]$ sont aussi de Toeplitz et triangulaires supérieures avec une diagonale nulle par la propriété 2. La matrice $\Gamma_{i+1} = \sum_{j=0}^{r} \Gamma_i[\uparrow l_j]$ est donc aussi de Toeplitz comme somme de matrice de Toeplitz et triangulaire supérieure avec une diagonale nulle.

On peut faire le même type raisonnement pour montrer que Λ_i est une matrice de Toeplitz. □

Le fait que Λ_c soit de Toeplitz a comme conséquence importante que la matrice M_U peut être découpée en $r + 1$ matrices de Toeplitz. Les coefficients de M_U à calculer sont alors sur la première colonne et sur $r + 1$ lignes de M_U. Plus précisément nous avons le théorème suivant qui décrit les lignes de M_U.

Théorème 1 (Matrice M_U modulo un polynôme P général [12])**.** *Soient $P = 1 + X^{k_1} + \ldots + X^{k_r} + X^n$ un polynôme irréductible de $\mathbb{F}_2[X]$, $U \in \mathbb{F}_{2^n}$ et M_U la matrice de ϕ_U l'application de multiplication par U dans la base polynômiale de $\mathbb{F}_{2^n}$.*

Soient $L_i(M_U)$ pour $i = 0, \ldots, n-1$ les lignes de M_U. Si la première ligne de Λ_c est donnée par

$$L_0(\Gamma_c) = \left[\begin{array}{cccc} 0 & \mu_1 & \ldots & \mu_{n-1} \end{array} \right],$$

si l'on définit les $r+1$ matrices lignes par

$$Y_0 = L_0(M_U) \text{ et } Y_j = L_{k_j}(M_U) \text{ pour } j = 1, \ldots, r,$$

et si l'on note

$$Y_j = \left[\begin{array}{ccc} y_{j,0} & \cdots & y_{j,n} \end{array} \right].$$

Les lignes $L_i(M_U)$ pour $k_j \leq i < k_{j+1}$ s'expriment en fonction de Y_j comme

$$L_i(M_U) = \left[\begin{array}{ccccccc} u_i & \cdots & u_{k_j+1} & y_{j,0} & \cdots & y_{j,n-(i-k_j)-1} \end{array} \right], \tag{13}$$

et les Y_j vérifient la relation de récurrence suivante

$$Y_{j+1} = \left[\begin{array}{ccccccc} u_{k_j} & u_{k_j-1} + \mu_1 & \cdots & u_{k_{j-1}} + \mu_{k_j-k_{j-1}} & y_{0,j-1} + \mu_{k_j-k_{j-1}-1} & \cdots & y_{n-k_j} + \mu_{k_j-k_{j-1}} \end{array} \right] \tag{14}$$

L'exemple suivant illustre la construction des lignes de M_U établie dans le théorème.

Exemple 10. Revenons à notre exemple $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(X^5 + X^3 + X^2 + 1)$. Avec les notations du théorème la matrice Λ_c est donnée par

$$\Lambda_c = \begin{bmatrix} 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \\ 0 & 0 & \mu_1 & \mu_2 & \mu_3 \\ 0 & 0 & 0 & \mu_1 & \mu_2 \\ 0 & 0 & 0 & 0 & \mu_1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

La matrice M_U est donnée avec l'identité (10) par

$$M_U = \widehat{M_U} + \Lambda_c + \Lambda_c[\downarrow 2] + \Lambda_c[\downarrow 3],$$

Nous obtenons alors

$$M_U = \begin{bmatrix} u_0 & 0 & 0 & 0 & 0 \\ u_1 & u_0 & 0 & 0 & 0 \\ u_2 & u_1 & u_0 & 0 & 0 \\ u_3 & u_2 & u_1 & u_0 & 0 \\ u_4 & u_3 & u_2 & u_1 & u_0 \end{bmatrix} + \begin{bmatrix} 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \\ 0 & 0 & \mu_1 & \mu_2 & \mu_3 \\ 0 & 0 & 0 & \mu_1 & \mu_2 \\ 0 & 0 & 0 & 0 & \mu_1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$+ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \\ 0 & 0 & \mu_1 & \mu_2 & \mu_3 \\ 0 & 0 & 0 & \mu_1 & \mu_2 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \\ 0 & 0 & \mu_1 & \mu_2 & \mu_3 \end{bmatrix}$$

Avec les notations du théorème, nous pouvons exprimer M_U en fonction des lignes Y_0, Y_1 et Y_2, qui sont respectivement les lignes d'indice $k_0 = 0, k_1 = 2$ et $k_2 = 3$ de M_U, comme

$$M_U = \begin{bmatrix} y_{0,0} & y_{0,1} & y_{0,2} & y_{0,3} & y_{0,4} \\ u_1 & y_{0,0} & y_{0,1} & y_{0,2} & y_{0,3} \\ y_{1,0} & y_{1,1} & y_{1,2} & y_{1,3} & y_{1,4} \\ y_{2,0} & y_{2,1} & y_{2,2} & y_{2,3} & y_{2,4} \\ u_4 & y_{2,0} & y_{2,1} & y_{2,2} & y_{2,3} \end{bmatrix}.$$

Avec la première ligne de Λ_c, $L_0(\Gamma_c) = \begin{bmatrix} 0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \end{bmatrix}$ nous obtenons les expressions suivante des Y_j

$$\begin{array}{rcl} Y_0 & = & \begin{bmatrix} u_0 & \mu_1 & \mu_2 & \mu_3 & \mu_4 \end{bmatrix} \\ Y_1 & = & \begin{bmatrix} u_2 & u_1+\mu_1 & y_{0,0}+\mu_2 & y_{0,1}+\mu_3 & y_{0,2}+\mu_4 \end{bmatrix} \\ Y_2 & = & \begin{bmatrix} u_3 & y_{1,0}+\mu_1 & y_{1,1}+\mu_2 & y_{1,2}+\mu_3 & y_{1,3}+\mu_4 \end{bmatrix} \end{array}$$

♢

Venons en maintenant à la preuve du théorème.

Démonstration. D'après le lemme 6 et la proposition 2, M_U est donnée par :

$$M_U = (\widehat{M_U})_H + \Lambda_c + \sum_{m=1}^{r} \Lambda_c[\downarrow k_m] \tag{15}$$

Définissons la séquence de matrice $M_{U,j}$ pour $j = 0, \ldots, r$ par

$$\begin{aligned} M_{U,0} &= (\widehat{M_U})_H + \Lambda_c, \\ M_{U,j} &= (\widehat{M_U})_H + \Lambda_c + \sum_{m=1}^{j} \Lambda_c[\downarrow k_m] \quad \text{pour } \ j = 1, \ldots, r. \end{aligned} \tag{16}$$

Soient $L_i(M_{U,j})$ pour $i = 0, \ldots, n-1$ les lignes de $M_{U,j}$. Remarquons d'abord que d'après (15) du fait que les lignes d'indice $i < k_{j+1}$ dans $\Lambda_c[\downarrow k_m]$ pour $m \geq j+1$ sont nulles, nous avons

$$L_i(M_U) = L_i(M_{U,j}) \quad \text{pour } \ i = 0, \ldots, k_{j+1} - 1, \tag{17}$$

et en particulier $Y_j = L_{k_j}(M_{U,j})$.

Par construction, Λ_c a une première colonne nulle, et donc la première colonne de M_U ainsi que celle de $M_{U,j}$ sont égales à la première colonne de $(\widehat{M_U})_H$. Si l'on étudie la sous matrice de $M_{U,j}$ constituée des $n - k_j$ dernières lignes, ce bloc forme une matrice de Toeplitz d'après l'équation (16) comme somme de matrices de Toeplitz (propriété 2). Comme on a noté

$$Y_j = \begin{bmatrix} y_{j,0} & \cdots & y_{j,n} \end{bmatrix},$$

on en déduit que les lignes $L_i(M_{U,j})$ pour $i \geq k_j$ sont données par

$$L_i(M_{U,j}) = \begin{bmatrix} u_i & \ldots & u_{k_j+1} & y_{j,0} & \ldots & y_{j,n-(i-k_j)-1} \end{bmatrix}. \tag{18}$$

L'assertion sur les lignes $L_i(M_U)$ pour $i = k_j, \ldots, k_{j+1} - 1$ découle de l'équation précédente et de l'équation (17).

Montrons à présent la relation de récurrence entre les Y_j. Par définition nous avons $M_{j+1} = M_j + \Lambda_c[\downarrow k_{j+1}]$, ceci implique d'après (17) que

$$Y_{j+1} = L_{k_j}(M_{U,j}) + L_0(\Lambda_c).$$

nous remplaçons alors $L_{k_j}(M_{U,j})$ par l'expression donnée par (18) et nous obtenons

$$\begin{array}{rcl} Y_{j+1} & = & \left[\begin{array}{ccccccc} u_{k_{j+1}} & u_{k_{j+1}-1} & \cdots & u_{k_j+1} & y_{0,j} & \cdots & y_{n-(k_{j+1}-k_j)-1,j} \end{array}\right] \\ & + & \left[\begin{array}{ccccccc} 0 & \mu_1 & \cdots & \mu_{k_{j+1}-k_j-1} & \mu_{k_{j+1}-k_j-2} & \cdots & \mu_{n-1} \end{array}\right] \end{array}$$

Ce qui termine la preuve.

□

A partir des résultats du théorème 1 donnant une construction des lignes de M_U à partir de Λ_c, nous pouvons établir l'algorithme 3 suivant. Cet algorithme calcule dans un premier temps la première ligne de la matrice Λ_c en utilisant la relation de récurrence des Λ_i et des Γ_i donnée dans la proposition 2. Ensuite avec le théorème précédent, on peut construire les lignes de M_U pour enfin calculer le produit $W = M_U \cdot V$.

Algorithme 3 Multiplieur pour polynôme général

Entrée. $U = [u_0, \ldots, u_{n-1}]$ et $V = [v_0, \ldots, v_{n-1}]$

Etape 1. *Calcul de la première ligne de* Λ_c

$L_0(\Gamma_0) \leftarrow [0\ u_{n-1}\ \cdots\ u_1]$
$L_0(\Lambda_0) \leftarrow 0$
pour i **de** 1 **à** c **faire**
  $L_0(\Gamma_i) \leftarrow \sum_{i=1}^{r} L_0(\Gamma_{i-1})[\rightarrow l_i]$
  $L_0(\Lambda_i) \leftarrow L_0(\Lambda_{i-1}) + L_0(\Gamma_i)$
$\left[\begin{array}{ccc} \mu_0 & \cdots & \mu_{n-1} \end{array}\right] \leftarrow L_0(\Lambda_c)$

Etape 2. *Calcul des* w_i

Initialisation $Y_0 \leftarrow \left[\begin{array}{cccc} u_0 & \mu_1 & \cdots & \mu_{n-1} \end{array}\right]$
pour $i = 0, \ldots, k_1 - 1$ **faire**
  $L_i(M_U) \leftarrow \left[\begin{array}{ccccccc} u_i & \ldots & u_0 & \mu_1 & \ldots & \mu_{i+1} \end{array}\right]$
  $w_i \leftarrow L_i(M_U) \cdot V$
pour $j = 0, \ldots, r - 1$ **faire**
  $Y_{j+1} \leftarrow \left[\begin{array}{l} u_{k_{j+1}}\ u_{k_{j+1}-1} + \mu_1\ \cdots\ u_{k_j+1} + \mu_{k_{j+1}-k_j}\ y_{j,0} + \mu_{k_{j+1}-k_j}\ \cdots \\ \qquad\qquad \cdots\ y_{j,n-1-(k_{j+1}-k_j)} + \mu_{n-1} \end{array}\right]$
  pour $i = k_{j+1}, \ldots, k_{j+2} - 1$ **faire**
    $L_i(M_U) \leftarrow \left[\begin{array}{ccccccc} u_i & \ldots & u_{k_j+1} & y_{j,0} & \cdots & y_{j,n-k_j} \end{array}\right]$
    $w_i \leftarrow L_i(M_U) \cdot V$

Sortie. $W \leftarrow [w_0, \ldots, w_{n-1}]$

Complexité. Nous allons évaluer la complexité de chacune des étapes de l'algorithme. Commençons par la première étape. En dehors du cas où $i = 1$, le calcul de $L_0(\Lambda_{i-1})$ est effectué en même temps que celui $L_0(\Gamma_i)$. Nous avons besoin de $(r-1)(n-1)$ XOR pour calculer $L_0(\Gamma_i)$

avec un arbre binaire et $(n-1)$ XOR pour le calcul de $L_0(\Lambda_i)$, d'où un total de $r(n-1)$ XOR. La complexité en temps est elle de $c\lceil \log_2(r) \rceil T_X$.

La seconde étape consiste à calculer d'une part les lignes Y_j de manière itérée. Cela nécessite $(n-1)$ XOR et se fait en temps rT_X. D'autre part elle consiste en n produits scalaires, qui nécessitent n^2 AND et $n(n-1)$ XOR et se font en temps $T_A + \lceil \log_2(n) \rceil T_X$.

La complexité matérielle totale est donc de

$$n^2 \text{ AND et } (n+r+1)(n-1) \text{ XOR},$$

et la complexité en temps est égale à

$$T_A + (c\lceil \log_2(r) \rceil + r + \lceil \log_2(n) \rceil) T_X.$$

Remarque 2. Koc et Halbutogullari dans [12] ont proposé une méthode de calcul pour $L_0(\Gamma_c)$ plus efficace que celle que l'on vient de présenter. Nous avons omis d'utiliser cette technique pour alléger l'exposé. Pour information, leur multiplieur a une complexité matérielle totale de

$$n^2 \text{ AND et } \left((n-1)(n-r) + \sum_{j \in \mathcal{S}^*} (2n-1-j) \right) \text{ XOR },$$

et une complexité en temps de

$$T_A + (\lceil \log_2 |\mathcal{S}| \rceil + r + \lceil \log_2(n) \rceil) T_X.$$

où l'ensemble $\mathcal{S}$ est un sous-ensemble de $\{n, n+(n-k_r), (n-k_r+1), \ldots, 2n-2\}$ dépendant du polynôme P.

4.2 Trinôme

Sur $\mathbb{F}_2$ les polynômes irréductibles les plus creux sont les trinômes. Plus le polynôme est creux plus l'opération de réduction modulo P est simple à effectuer.

Soit $P = X^n + X^k + 1$ un trinôme irréductible de $\mathbb{F}_2[X]$ et $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$. Nous avons vu dans la section précédente que le nombre de réduction de la matrice $\widehat{M_U}$ pour calculer M_U valait $c = \lceil \frac{n-1}{n-k_r} \rceil$. Pour notre trinôme P nous avons $c = \lceil \frac{n-1}{n-k} \rceil$. Ce nombre de réduction sera alors ≤ 2 si $k \leq \frac{n}{2}$, par contre si $k > \frac{n}{2}$, le nombre de réduction sera alors supérieur ou égal à 3.

Tout d'abord, nous allons voir que l'on peut en fait se restreindre au cas de trinôme avec un $k \leq \lfloor \frac{n}{2} \rfloor$. Le nombre de réduction de la matrice $\widehat{M_U}$ sera alors toujours ≤ 2.

Proposition 3. *Soit P un polynôme de degré n sur un corps fini $\mathbb{F}_q$. Soit $\widehat{P} = X^n P(X^{-1})$ son polynôme réciproque. Alors P est irréductible si et seulement si son polynôme réciproque l'est.*

Démonstration. Si $P = Q_1 Q_2$ alors $\widehat{P} = \widehat{Q_1}\widehat{Q_2}$, donc si P n'est pas irréductible alors $\widehat{P}$ non plus. De même, vu que $\widehat{\widehat{P}} = P$, si $\widehat{P}$ n'est pas irréductible, P ne l'est pas non plus. □

Proposition 4. *Si il existe un trinôme P irréductible de degré n, il existe alors au moins un trinôme de degré n avec un $k \leq \frac{n}{2}$.*

Démonstration. Si $P = X^n + \alpha X^k + \beta$ ne convient pas, i.e., si $k \geq \frac{n}{2}$, alors forcément $\widehat{P} = \beta X^n + \alpha X^{n-k} + 1$ convient. □

4.2.1 Multiplication

Nous allons présenter les multiplieurs dans une base polynômiale associée à un trinôme de $\mathbb{F}_2[X]$, sous l'hypothèse $k \leq \frac{n}{2}$. Cette étude consiste essentiellement à spécifier au cas des trinômes l'algorithme 3 qui calculait la multiplication de deux éléments U, V modulo un polynôme général P.

Remarque 3. Nous ne traiterons pas le cas des trinômes $X^n + X + 1$, i.e., avec un $k = 1$. Ce type de trinôme admet un multiplieur du même type que celui que nous allons construire ici, mais légèrement plus simple. Il se trouve que pour $k = 1$ les multiplieurs sont des plus efficaces car, dans ce cas, il suffit de réduire une seule fois $\widehat{M_U}$

$$M_U = (R\widehat{M_U})_H.$$

L'architecture du multiplieur dans le cas $k = 1$ est construite d'une manière similaire, et à titre indicatif il a une complexité matérielle de

$$n^2 \text{ AND } \text{ et } (n+1)(n-1) \text{ XOR},$$

et une complexité en temps de

$$T_A + (1 + \log_2(n))T_X.$$

Les détails concernant ce sujet pourront être trouvés dans la thèse de Mastrovito [19].

L'opérateur de réduction R est défini dans le cas où $P = X^n + X^k + 1$ par

$$R(X^i) = \begin{cases} X^i & \text{si} \quad i \leq n-1, \\ X^{i-n} + X^{i-(n-k)} & \text{si} \quad n \leq i < 2n-k, \\ X^{i-n} + X^{i-(2n-k)} + X^{i-(2n-2k)} & \text{si} \quad 2n-k \leq i. \end{cases}$$

Il opère sur la matrice $\widehat{M_U}$ dans le cas des trinômes comme

$$(R \cdot \widehat{M_U})_H = (\widehat{M_U})_H + (\widehat{M_U})_B + (\widehat{M_U})_B[\downarrow k] \tag{19}$$

$$(R \cdot \widehat{M_U})_B = (\widehat{M_U})_B[\uparrow (n-k)] \tag{20}$$

Du fait du lemme 4 on peut supposer que $k \in \{2, \ldots, \lfloor \frac{n}{2} \rfloor\}$ et dans ce cas le nombre de fois que l'on doit réduire $\widehat{M_U}$ vaut 2. Nous avons alors la proposition suivante qui établit la matrice M_U de multiplication par U dans $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(X^n + X^k + 1)$.

Proposition 5 ([24])**.** *Soit $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où $P = X^n + X^k + 1$ est un trinôme irréductible avec $2 \leq k \leq \lfloor \frac{n}{2} \rfloor$. La matrice M_U de la multiplication par*

$$U = u_0 + u_1 X + \cdots + u_{n-1} X^{n-1} \in \mathbb{F}_{2^n}$$

dans la $\mathbb{F}_2$-base polynômiale $(1, X, \ldots, X^{n-1})$ est donnée par

$$M_U = \begin{bmatrix} u_0 & u_{n-1} & u_{n-2} & \cdots & u_{k+1} & u_k & u'_{k-1} & \cdots & u'_1 \\ u_1 & u_0 & u_{n-1} & \cdots & u_{k+2} & u_{k+1} & u_k & \cdots & u'_2 \\ \vdots & & \ddots & \ddots & & & & \ddots & \vdots \\ & & & \ddots & \ddots & & & \cdots & u_k \\ u_{k-1} & u_{k-2} & u_{k-3} & \ddots & & & & & \\ u_k & u'_{k-1} & u'_{k-2} & \cdots & u'_0 & u''_{n-1} & & & u''_{k+1} \\ u_{k+1} & u_k & u'_{k-1} & \cdots & \cdots & u'_0 & u''_{n-1} & \cdots & u''_{k+2} \\ \vdots & & & & & & \ddots & \ddots & \vdots \\ u_{n-2} & \cdots & & & & & & \ddots & u''_{n-1} \\ u_{n-1} & \cdots & \cdots & \cdots & \cdots & u_k & u'_{k-1} & \cdots & u'_0 \end{bmatrix} \tag{21}$$

où

$$u'_i = u_i + u_{i+(n-k)} \quad \textit{pour} \quad i = 0, \ldots, k-1,$$
$$u''_i = \begin{cases} u_i + u_{i-k} + u_{i-k+(n-k)} = u_i + u'_{i-k} & \textit{pour} \quad i = k+1, \ldots, 2k-1, \\ u_i + u_{i-k} & \textit{pour} \quad i = 2k, \ldots, n-1. \end{cases}$$

Démonstration. Pour calculer M_U nous devons réduire $\widehat{M_U}$ et pour cela nous devons appliquer deux fois R à $\widehat{M_U}$. Notons $\Gamma = (\widehat{M_U})_B$. Les équations (19) et (20) deviennent

$$\begin{aligned} (R \cdot \widehat{M_U})_H &= (\widehat{MU})_H + \Gamma + \Gamma[\downarrow k], \\ (R \cdot \widehat{M_U})_B &= \Gamma[\uparrow (n-k)]. \end{aligned} \tag{22}$$

Si nous définissons $\Lambda = \Gamma[\uparrow (n-k)]$ et si nous réduisons une seconde fois, nous obtenons

$$M_U = (R^2 \cdot \widehat{M_U})_H = (\widehat{M_U})_H + \Lambda + \Gamma + (\Lambda + \Gamma)[\downarrow k].$$

Si l'on définit la matrice $\Lambda' = \Lambda + \Gamma$, nous avons

$$\Lambda' = \begin{bmatrix} 0 & u_{n-1} & u_{n-2} & \cdots & u_{k+1} & u_k & u'_{k-1} & \cdots & u'_1 \\ 0 & 0 & u_{n-1} & \cdots & u_{k+2} & u_{k+1} & u_k & \cdots & u'_2 \\ \vdots & & & \ddots & & & & \ddots & \vdots \\ 0 & & & & u_{n-1} & & & & u_k \\ \vdots & & & & & \ddots & & & \vdots \\ \vdots & & & & & & \ddots & & \vdots \\ \vdots & & & & & & & \ddots & \vdots \\ 0 & & & & & & & & u_{n-1} \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}$$

où les u'_i sont définis par $u'_i = u_i + u_{i+(n-k)}$. De l'égalité $M_U = (\widehat{M_U})_H + \Lambda' + \Lambda'[\downarrow k]$ nous déduisons l'expression de M_U donnée dans la proposition. Ce qui termine la preuve. □

Le calcul du produit $W = UV$ de deux éléments $U, V \in \mathbb{F}_{2^n}$ se fait donc en deux étapes : une première étape où l'on calcule les coefficients u'_i, u''_i. Avec ces coefficients on peut construire la matrice M_U et on peut alors calculer W en effectuant le produit matrice vecteur $W = M_U \cdot V$. Nous avons finalement l'algorithme suivant pour le calcul du produit de U et V modulo un trinôme en base polynômiale.

Algorithme 4 Multiplieur trinômial [24]

Entrée. $U = [u_0, \ldots, u_{n-1}], V = [v_0, \ldots, v_{n-1}]$

Etape 1. *Calcul de* u'_i, u''_i

pour $i = 0, \ldots, k-1$ **faire**
$u'_i \leftarrow u_i + u_{i+n-k}$
pour $i = k+1, \ldots, 2k-1$ **faire**
$u''_i \leftarrow u_i + u'_{i-k}$
pour $i = 2k, \ldots, n-1$ **faire**
$u''_i \leftarrow u_i + u_{i+k}$

Etape 2. *Calcul des coefficients* w_i

pour $i = 1, \ldots, k-2$ **faire**
$L_i(M_U) \leftarrow \left[\begin{array}{ccccccccccc} u_i & u_{i-1} & \cdots & u_0 & u_{n-1} & \cdots & u_k & u'_{k-1} & \ldots & u'_{i+1} \end{array} \right]$
$w_i \leftarrow L_i(M_U) \cdot V$
pour $i = k-1$ **faire**
$L_i(M_U) \leftarrow \left[\begin{array}{ccccccc} u_{k-1} & u_{k-2} & \cdots & u_0 & u_{n-1} & \cdots & u_k \end{array} \right]$
$w_i \leftarrow L_i(M_U) \cdot V$
pour $i = k, \ldots, n-2$ **faire**
$L_i(M_U) \leftarrow \left[\begin{array}{ccccccccc} u_i & \ldots & u_k & u'_{k-1} & \ldots & u'_0 & u''_{n-1} & \ldots & u''_{i+1} \end{array} \right]$
$w_i \leftarrow L_i(M_U) \cdot V$
pour $i = n-1$ **faire**
$L_i(M_U) \leftarrow \left[\begin{array}{ccccccc} u_{n-1} & \ldots & u_k & u'_{k-1} & \ldots & u'_0 \end{array} \right]$
$w_i \leftarrow L_i(M_U) \cdot V$

Sortie. $W \leftarrow [w_0, \ldots, w_{n-1}]$

Complexité. Dans la première étape $(n-k-1)$ XOR sont nécessaires pour le calcul de u'_i et de u''_i. La seconde étape consiste simplement en n produits scalaires en parallèle. Au total cette architecture a donc une complexité matérielle de

$$(n-k-1+n(n-1)) \text{ XOR et } n^2 \text{ AND},$$

et une complexité en temps totale de

$$(2 + \lceil \log_2(n) \rceil) T_X + T_A.$$

4.2.2 Mise au carré

Rappelons qu'ici la base pour représenter les éléments du corps $\mathbb{F}_2[X]/(X^n + X^k + 1)$ est la base polynômiale $\mathcal{B} = (1, X, \cdots, X^{n-1})$. Pour un élément $U = \sum_{i=0}^{n-1} u_i X^i$, du fait que l'on soit en caractéristique 2, son carré est donné par

$$U^2 = \left(\sum_{i=0}^{n-1} u_i X^i \right)^2 = \sum_{i=0}^{n-1} u_i X^{2i}. \tag{23}$$

Réduisons les X^{2i} modulo P pour obtenir l'expression de U^2 dans $\mathcal{B}$.

1. Pour $i < \frac{n}{2}$ on a $X^{2i} = X^{2i}$.

2. Pour $\frac{n}{2} \leq i < n - \frac{k}{2}$ on a $X^{2i} = X^{2i-(n-k)} + X^{2i-n}$.
3. Pour $n - \frac{k}{2} \leq i < n - 1$ on a $X^{2i} = X^{2i-2(n-k)} + X^{2i-(2n-k)} + X^{2i-n}$.

Si l'on remplace dans l'équation (23) le monôme X^{2i} par son expression réduite donnée ci-dessus nous obtenons

$$\begin{aligned} U^2 = \; & \textstyle\sum_{0\leq i<\frac{n}{2}} u_i X^{2i} + \sum_{\frac{n}{2}\leq i<n} u_i X^{2i-n} + \sum_{\frac{n}{2}\leq i<n-\frac{k}{2}} u_i X^{2i-(n-k)} \\ & + \textstyle\sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-2(n-k)} + \sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-(2n-k)}. \end{aligned}$$

On va arranger cette expression en effectuant le changement d'indice $2j = 2i - 2(n-k)$, i.e., $i = j + (n-k)$, dans la sommation $\sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-2(n-k)}$ qui devient alors

$$\sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-2(n-k)} = \sum_{\frac{k}{2}\leq j<k} u_{j+n-k} X^{2j}$$

L'expression précédente de U^2 devient alors

$$\begin{aligned} U^2 = \; & \textstyle\sum_{0\leq i<\frac{k}{2}} u_i X^{2i} + \sum_{\frac{k}{2}\leq i<k} (u_i + u_{i+n-k}) X^{2i} + \sum_{k\leq i<\frac{n}{2}} u_i X^{2i} \\ & + \textstyle\sum_{\frac{n}{2}\leq i<n} u_i X^{2i-n} + \sum_{\frac{n}{2}\leq i<n-\frac{k}{2}} u_i X^{2i-(n-k)} \\ & + \textstyle\sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-(2n-k)}. \end{aligned} \tag{24}$$

Nous devons, pour finir d'arranger l'expression précédente de U^2, diviser l'étude suivant la parité de n et k. Nous n'allons pas traiter le cas où n et k sont simultanément pairs, car nous nous intéressons essentiellement aux trinômes irréductibles. Nous obtenons les différentes situations suivantes

1. *Pour n pair et k impair.* Dans l'équation (24), nous allons d'abord arranger la somme $\sum_{\frac{n}{2}\leq i<n} u_i X^{2i-n}$ en posant $2j = 2i - n$ (car n est pair). Nous obtenons alors

$$\sum_{\frac{n}{2}\leq i<n} u_i X^{2i-n} = \sum_{0\leq j<\frac{n}{2}} u_{i+\frac{n}{2}} X^j,$$

ensuite, en effectuant le changement d'indice $2j + 1 = 2i - (2n-k)$ nous avons

$$\sum_{n-\frac{k}{2}\leq i<n} u_i X^{2i-(2n-k)} = \sum_{0\leq j<\frac{k-1}{2}} u_{j+n-\frac{k-1}{2}} X^{2j+1}.$$

Enfin, en posant $2j + 1 = 2i - (n-k)$ nous obtenons que

$$\sum_{\frac{n}{2}\leq i<n-\frac{k}{2}} u_i X^{2i-(n-k)} = \sum_{\frac{k-1}{2}\leq j<\frac{n-1}{2}} u_{j+\frac{n-k}{2}} X^{2j+1}.$$

En remplaçant toute ces sommes par leur nouvelle expression dans (24) nous en déduisons finalement que U^2 est donné par

$$\begin{array}{rl}\left(\sum_{i=0}^{n-1} u_i X^i\right)^2 & = \sum_{i=0}^{\frac{k-1}{2}} (u_i + u_{i+\frac{n}{2}}) X^{2i} + \sum_{i=\frac{k+1}{2}}^{k-1} (u_i + u_{i+\frac{n}{2}} + u_{i+n-k}) X^{2i} \\ & + \sum_{i=k}^{\frac{n}{2}-1} (u_i + u_{i+\frac{n}{2}}) X^{2i} + \sum_{i=0}^{\frac{k-3}{2}} u_{i+n-\frac{k-1}{2}} X^{2i+1} \\ & + \sum_{i=\frac{k-1}{2}}^{\frac{n}{2}-1} u_{i+\frac{n-k+1}{2}} X^{2i+1}\end{array} .$$

La complexité pour élever un élément U au carré lorsque les calculs sont effectués en parallèle pour chaque coordonnée, est la suivante.

Complexité. La complexité en espace vaut $(\frac{n}{2})$ XOR pour le calcul de $u_i + u_{i+\frac{n}{2}}$ suivi de $u_i + u_{i+\frac{n}{2}} + u_{i+n-k}$ et la complexité en temps vaut $2T_X$.

2. *Pour n impair et k impair.*
Reprenons l'expression (24) de U^2

$$\begin{array}{rl} U^2 = & \sum_{0 \le i < \frac{k}{2}} u_i X^{2i} + \sum_{\frac{k}{2} \le i < k} (u_i + u_{i+n-k}) X^{2i} + \sum_{k \le i < \frac{n}{2}} u_i X^{2i} \\ & + \underbrace{\sum_{\frac{n}{2} \le i < n} u_i X^{2i-n}}_{S_1} + \underbrace{\sum_{\frac{n}{2} \le i < n-\frac{k}{2}} u_i X^{2i-(n-k)}}_{S_2} + \underbrace{\sum_{n-\frac{k}{2} \le i < n} u_i X^{2i-(2n-k)}}_{S_3}.\end{array}$$

Nous allons arranger les sommes S_1, S_2, S_3 en effectuant comme précédemment différents changement d'indice. Pour S_1, en posant $2j+1 = 2i-n$, nous obtenons que

$$S_1 = \sum_{0 \le j < \frac{n-1}{2}} u_{j+\frac{n+1}{2}} X^{2j+1},$$

ensuite pour S_2 nous posons $2j = 2i-(n-k)$ et pour S_3 nous posons $2j+1 = 2i-(2n-k)$, ce qui nous donne

$$S_2 = \sum_{\frac{k}{2} \le j < \frac{n}{2}} u_{j+\frac{n-k}{2}} X^{2j} \quad \text{et} \quad S_3 = \sum_{0 \le j < \frac{k-1}{2}} u_{j+n-\frac{k-1}{2}} X^{2j+1}.$$

Ensuite pour obtenir l'expression de U^2 dans la base MP, il suffit juste de remplacer S_1, S_2 et S_3 par leur expression trouvée ci-dessus.

$$\begin{array}{rl}\left(\sum_{i=0}^{n-1} u_i X^i\right)^2 & = \sum_{i=0}^{\frac{k-1}{2}} u_i X^{2i} + \sum_{i=\frac{k+1}{2}}^{k-1} (u_i + u_{i+n-k} + u_{i+\frac{n-k}{2}}) X^{2i} \\ & + \sum_{i=k}^{\frac{n-1}{2}} (u_i + u_{i+\frac{n-k}{2}}) X^{2i} + \sum_{i=0}^{\frac{k-3}{2}} (u_{i+\frac{n+1}{2}} + u_{i+n-\frac{k-1}{2}}) X^{2i+1} \\ & + \sum_{\frac{k-1}{2}}^{\frac{n-3}{2}} u_{i+\frac{n+1}{2}} X^{2i+1}.\end{array}$$

Complexité. Nous avons besoin de $(\frac{n-1}{2} - \frac{k-1}{2})$ XOR pour le calcul de $u_i + u_{i+\frac{n-k}{2}}$ et de $u_i + u_{i+n-k} + u_{i+\frac{n-k}{2}}$, et nous avons aussi besoin de $\frac{k-1}{2}$ XOR pour le calcul de $u_{i+\frac{n+1}{2}} + u_{i+n-\frac{k-1}{2}}$. La mise au carré a dans ce cas une complexité matérielle de $\frac{n-1}{2}$ XOR . La complexité en temps est ici encore de $2T_X$.

3. *Pour n impair et k pair.*
   Revenons encore à l'expression (24) de U^2

$$U^2 = \sum_{0\le i<\frac{k}{2}} u_i X^{2i} + \sum_{\frac{k}{2}\le i<k}(u_i + u_{i+n-k})X^{2i} + \sum_{k\le i<\frac{n}{2}} u_i X^{2i} + \underbrace{\sum_{\frac{n}{2}\le i<n} u_i X^{2i-n}}_{S_1} + \underbrace{\sum_{\frac{n}{2}\le i<n-\frac{k}{2}} u_i X^{2i-(n-k)}}_{S_2} + \underbrace{\sum_{n-\frac{k}{2}\le i<n} u_i X^{2i-(2n-k)}}_{S_3}.$$

   Nous arrangeons les sommes S_1, S_2, S_3 en effectuant comme précédemment différents changements d'indice : pour S_1, nous posons $2j+1 = 2i-n$, ce qui donne

$$S_1 = \sum_{0\le j<\frac{n-1}{2}} u_{j+\frac{n+1}{2}} X^{2j+1},$$

   ensuite pour S_2 nous posons $2j+1 = 2i-(n-k)$ et pour S_3 nous posons $2j = 2i-(2n-k)$, ce qui nous donne

$$S_2 = \sum_{\frac{k-1}{2}\le j<\frac{n-1}{2}} u_{j+\frac{n-k+1}{2}} X^{2j+1} \quad \text{et} \quad S_3 = \sum_{0\le j<\frac{k}{2}} u_{j+n-\frac{k}{2}} X^{2j}.$$

   Nous obtenons finalement l'expression suivante de U^2

$$\left(\sum_{i=0}^{n-1} u_i X^i\right)^2 = \sum_{i=0}^{\frac{k-2}{2}}(u_i + u_{i+n-\frac{k}{2}})X^{2i} + \sum_{i=\frac{k}{2}}^{k-1}(u_i + u_{i-n+k})X^{2i} + \sum_{i=k}^{\frac{n-1}{2}} u_i X^{2i} + \sum_{i=0}^{\frac{k-2}{2}} u_{i+\frac{n+1}{2}} X^{2i+1} + \sum_{\frac{k}{2}}^{\frac{n-3}{2}}(u_{i+\frac{n+1}{2}} + u_{i+\frac{n-k+1}{2}})X^{2i+1}.$$

   Complexité. Dans ce cas $(\frac{n-1}{2} + \frac{k}{2})$ XOR sont nécessaires pour le calcul de U^2 et le délai est de T_X.

4.3 Pentanôme

Dans la section précédente nous avons décrit les multiplieurs en base polynômiale pour les trinômes. Il est aussi important d'expliciter la multiplication modulo un pentanôme car il n'existe pas de trinômes irréductibles dans $\mathbb{F}_2[X]$ de tout degré n. Pour calculer modulo un pentanôme P arbitraire de $\mathbb{F}_{2^n}[X]$, on peut utiliser l'algorithme 3 avec comme polynôme irréductible un pentanôme P. Ici on va voir qu'il est possible d'améliorer l'efficacité de la multiplication modulo un certain type de pentanôme. Cette section reprend le travail effectué par Koc et Rodriguez dans [22].

Les pentanômes auront la forme suivante

$$P = X^n + X^{m+1} + X^m + X + 1 \quad \text{où} \quad 2 \le m \le \lfloor \tfrac{n}{2} \rfloor - 1. \tag{25}$$

La stratégie utilisée ici pour la multiplication modulo P de deux éléments $U, V \in \mathbb{F}_{2^n}[X]/(P)$ est la première stratégie présentée dans le préambule de ce chapitre pour calculer un produit

dans une représentation en base polynômiale. Elle consiste à calculer le produit W' des polynômes U et V, en effectuant le produit matrice vecteur $\widehat{M}_U \cdot V$, et à calculer ensuite le reste de ce produit modulo P en appliquant un opérateur $R' \colon F \to E$ qui à un polynôme de $F = \mathrm{Vect}_{\mathbb{F}_2}(1, X, X^2, \ldots, X^{2n-1})$ renvoie son reste modulo P dans $E = \mathrm{Vect}_{\mathbb{F}_2}(1, X, X^2, \ldots, X^{n-1})$.

Par linéarité nous avons seulement besoin de connaître $R'(X^i)$ pour calculer l'image par R' de tout élément $W' \in F$.

Lemme 8 ([22])**.** *Soit P un pentanôme de la forme de* (25)*, on a alors les identités suivantes*

1. *Pour $i = n, \ldots, 2n - m - 2$,*

$$R'(X^i) = X^{(i-n)} + X^{(i-n)+1} + X^{m+(i-n)} + X^{m+(i-n)+1}.$$

2. *Pour $i = 2n - m - 1$,*

$$R'(X^i) = X^{(i-n)} + X^{(i-n)+1} + X^{m+(i-n)} + 1 + X + X^m + X^{m+1}.$$

3. *Pour $i = 2n - m, \ldots, 2n - 2$,*

$$R'(X^i) = X^{(i-n)} + X^{(i-n)+1} + X^{(i-n)-(n-m)} + X^{(i-n)-n+2m} + X^{(i-n)-(n-m)+2} + X^{(i-n)-n+2m}.$$

Démonstration. Nous allons utiliser la relation $X^n = X^{m+1} + X^m + X + 1$ donnée par le polynôme P pour réduire les monômes X^i. Effectuons une première réduction de X^i modulo P pour $i \geq n$

$$\begin{array}{rcl} X^i & = & X^{i-n}X^n = X^{i-n}(X^{m+1} + X^m + X + 1) \\ & = & X^{i-n} + X^{i-n+1} + X^{i-n+m} + X^{i-n+m+1}. \end{array} \tag{26}$$

Ceci nous donne déjà l'identité pour $R'(X^i)$ du lemme lorsque $n \leq i \leq 2n - m - 2$.

Maintenant pour $i = 2n - m - 1$, dans (26) le monôme $X^{i-n+m+1} = X^n$ n'est plus réduit, nous devons donc le remplacer par

$$X^{(i-n)+m+1-n} + X^{(i-n)+m+1-n+1} + X^{(i-n)+m+1-n+m} + X^{(i-n)+m+1-n+m+1}, \tag{27}$$

ce qui donne

$$X^{2n-m-1} = X^{n-m-1} + X^{n-m} + X + 1 + X + X^m + X^{m+1}.$$

Enfin pour $i \geq 2n - m$, on remplace dans (26) comme précédemment le monôme $X^{i-n+m+1}$ qui n'est pas réduit par l'expression donnée dans (27) et X^{i-n+m} par

$$X^{i-2n+m} + X^{i-2n+m+1} + X^{i-2n+2m} + X^{i-2n+2m+1},$$

nous obtenons alors que

$$X^i = X^{(i-n)} + X^{(i-n)+1} + X^{(i-n)-(n-m)} + X^{(i-n)-n+2m} + X^{(i-n)-(n-m)+2} + X^{(i-n)-n+2m}.$$

Ce qui conclut la preuve. □

Maintenant que nous connaissons l'action de R' sur les monôme X^i nous pouvons calculer l'action de R' sur tout polynôme W' de degré $\leq 2n - 2$

$$R'(W') = R'(\sum_{i=0}^{2n-2} w'_i X^i) = \sum_{i=0}^{2n-2} w'_i R'(X^i).$$

En remplaçant les expressions des $R'(X^i)$ donnés dans le lemme précédent nous obtiendrons W' réduit modulo P. Le corollaire suivant exprime chaque coefficient de $W = R'(W')$ en fonction des w'_i.

Corollaire 1 ([22]). *Soit $W' = \sum_{i=0}^{2n-2} w'_i X^i \in F = Vect_{\mathbb{F}_2}(1, X, \ldots, X^{2n-1})$, les coefficients w_i de $W = R'(W')$ dans la base polynômiale $(1, X, \ldots, X^{n-1})$ de $\mathbb{F}_{2^n}$ sont données alors par*

$$\begin{aligned}
w_0 &= w'_0 + w'_n + w'_{2n-m-1} + w'_{2n-m},\\
&\textit{Pour } i = 2, \ldots, m-2,\\
w_i &= w'_i + w'_{i+n-1} + w'_{i+n} + w'_{i+2n-m-2} + w'_{i+2n-m},\\
w_{m-1} &= w'_{m-1} + w'_{n+m-2} + w'_{n+m-1} + w'_{2n-3},\\
&\textit{Pour } i = m, \ldots, 2m-2,\\
w_i &= w'_i + w'_{i+n-m-1} + w'_{i+n-m} + w'_{i+n-1} + w'_{i+n} + w'_{i+2n-2m-2} + w'_{i+2n-2m},\\
w_{2m-1} &= w'_{2m-1} + w'_{n+m-2} + w'_{n+m-1} + w'_{n+2m-2} + w'_{n+2m-1} w'_{2n-3},\\
w_{2m} &= w'_{2m} + w'_{n+m-1} + w'_{n+m} + w'_{n+2m-1} + w'_{n+2m} + w'_{2n-2},\\
&\textit{Pour } i = 2m+1, \ldots, n-2,\\
w_i &= w'_i + w'_{i+n-m-1} + w'_{i+n-m} + w'_{i+n-1} + w'_{i+n},\\
w_{n-1} &= w'_{n-1} + w'_{2n-m-2} + w'_{2n-m-1} + w'_{2n-2}.
\end{aligned} \tag{28}$$

Démonstration. Nous allons montrer uniquement la formule du w_i pour $i = 2, \ldots, m-1$, la méthode étant la même pour les autres indices. Soit donc $1 \leq i \leq m-2$. Cherchons les $j \in \{0, \ldots, 2m-2\}$ tels que le monôme X^i apparaît dans l'expression de $R'(X^j)$ donné dans le lemme 8. D'abord notons que $R'(X^i) = X^i$, et que les autres $j \neq i$ sont forcément plus grands que n.

Pour $j \in \{n, \ldots, 2n-m-2\}$ nous avons

$$R'(X^j) = X^{(j-n)} + X^{(j-n)+1} + X^{m+(j-n)} + X^{m+(j-n)+1}.$$

Si $j = n+i$ et $j = n+i-1$, le monôme X^i apparaît dans l'expression de $R(X^j)$. D'autre part i ne peut pas être égal à un $m+(j-n)$ ou un $m+(j-n)+1$ car $i < m$ et $m+(j-n)+1 \geq m+(j-n) \geq m$. Ensuite pour $j \in \{2n-m, \ldots, 2n-2\}$ nous avons

$$R'(X^j) = X^{(j-n)} + X^{(j-n)+1} + X^{(j-n)-(n-m)} + X^{(j-n)-(n-m)+2} + X^{(j-n)-n+2m} + X^{(j-n)-n+2m+2}.$$

Ici encore si $j = 2n-m+i$ ou $2n-m+i+2$ nous avons que $R(X^j) = X^i + \cdots$.

D'autre part pour les monômes d'exposant $j-n$ nous avons $j-n \geq n-m \geq m$ car nous avons supposé, lors de la définition de P, que $m \leq \frac{n}{2}$. En conséquence $j-n$ ne peut être égal à i. Il en est de même pour $j-n+1$. D'autre part $(j-n)-n+2m+2 \geq (j-n)-n+2m \geq m$. Si $j = 2n-m-1$ on a

$$R'(X^{2n-m-1}) = X^{n-m-1} + X^{n-m} + X^{n-1} + 1 + X + X^m + X^{m+1},$$

et donc i n'apparaît pas ici. Nous avons donc regardé tous les X^j tels que X^i serait susceptible d'apparaître dans sa réduction modulo P. Nous obtenons finalement que

$$w_i = w'_i + w'_{i+n-1} + w'_{i+n} + w'_{i+2n-m-2} + w'_{i+2n-m}$$

comme voulu. □

Nous en déduisons l'algorithme ci-dessous pour la multiplication modulo P.

Algorithme 5 Multiplieur pentanômial [22]

Entrée. $U = \sum_{i=0}^{n-1} u_i X^i, V = \sum_{i=0}^{n-1} v_i X^i$
Produit des polynômes U *et* V $W' \leftarrow \widehat{M_U} \cdot V$
Calcul de $W \leftarrow R(W')$ *avec les formules* (28)
Sortie. W

Nous allons étudier la complexité de cet algorithme de multiplication.

Complexité. Seule la complexité de la phase de réduction est à déterminer, la phase de multiplication étant un simple produit matrice vecteur.

La phase de réduction consiste à sommer pour chaque coordonnée w_i certains w'_j. Le calcul des w_i sont effectués en parallèle. Et pour chaque w_i les sommes des w'_j sont effectuées à travers un arbre de XOR. Le nombre de XOR constituant un arbre pour sommer un nombre c de coefficients est égal à $c-1$, le délai du parcours de l'arbre est lui de $\lceil \log_2(c) \rceil T_X$.

Le tableau ci-dessous donne le nombre de portes nécessaire pour le calcul de chaque w_i avec les formules 28, sachant que pour chaque coordonnée on utilise un arbre de XOR.

Tab. 1 – Complexité de la Réduction

Coefficients	Nombre d'équations	Nombre d'opérandes	XOR Gates
w_0	1	4	3
$w_1, \ldots, w_{m-2}$	$m-2$	5	4
w_{m-1}	1	4	3
$w_m, \ldots, w_{2m-2}$	$m-1$	7	6
w_{2m-1}	1	6	5
w_{2m}	1	6	5
$w_{2m+1}, \ldots, w_{n-2}$	$n-2m-2$	5	4
w_{n-1}	1	4	3

Le temps de la réduction, i.e., du calcul de $W = R'(W')$, est égal au maximum des temps de calcul de chaque w_i. Il est donc égal à $3T_X = \lceil \log_2(7) \rceil T_X$. En additionnant les nombres de portes XOR utilisées pour chaque w_i nous obtenons la complexité matérielle suivante

$$3 + 4(m-2) + 3 + 6(m-1) + 5 + 5 + 4(n-2m-2) + 3 = 4n + 2m - 3 \text{ XOR},$$

pour la phase de réduction.

Nous avons finalement une complexité matérielle totale pour cette architecture de

$$((n-1)^2 + 4n + 2m - 3) \text{ XOR et } n^2 \text{ AND},$$

et une complexité totale en temps de $(\lceil \log_2 n \rceil + 3)T_X + T_A$.

Remarque 4. Koc et Rodriguez ont noté qu'une économie matérielle pouvait être faite lors de la reduction de W' car des calculs sont effectués de manière redondante dans des w_i. Ils ont obtenu une complexité matérielle de

$$((n-1)^2 + 3n + 2m - 1) \text{ XOR et } n^2 \text{ AND}.$$

Le lecteur pourra trouver plus de détails là dessus dans l'article de Koc et Rodriguez [22].

4.4 Polynômes équirépartis

Nous allons finir l'étude des corps binaires avec les corps définis par un polynôme P équiréparti. Ce type de polynôme a été largement étudiés car il permet d'une part d'implanter la multiplication dans $\mathbb{F}_{2^n}$ de manière efficace et d'autre part une bonne élévation au carré. Les polynômes équirépartis sont définis comme suit.

Définition 8 (Polynôme Equiréparti)**.** *Un polynôme équiréparti de pas Δ est un polynôme P du type*

$$P = \sum_{i=0}^{r} X^{i\Delta}.$$

Lorsque $\Delta = 1$ on dit que P est un ¡¡ All One Polynomial ¿¿ , abrégé en AOP, car dans ce cas $P = \sum_{i=0}^{r} X^i$ a tous ses coefficients égaux à 1.

Ces polynômes ont la propriété importante suivante :

Propriété 3. *Soit $P = \sum_{i=0}^{r} X^{i\Delta}$ un polynôme équiréparti de pas Δ, alors on a*

$$(X^{\Delta} + 1)P = X^{(r+1)\Delta} + 1$$

4.4.1 Stratégie

La propriété 3 ci-dessus des polynômes équirépartis va nous permettre d'implanter l'arithmétique modulo P de deux manières différentes. Le choix entre l'une ou l'autre de ces implantations dépendra de l'environnement dans lequel l'arithmétique dans ce corps est utilisée :

- *Première Implantation :* l'idée est d'effectuer les calculs modulo $X^{(r+1)\Delta} + 1$ plutôt que modulo P. La représentation du corps est dans ce cas redondante. L'intérêt est que cette implantation est en générale très efficace en temps, et, pourvu que Δ soit pas trop grand, elle n'est pas trop coûteuse en espace non plus.

  Cette implantation peut être utile lorsqu' une longue chaîne de calculs dans $\mathbb{F}_{2^n}$ est à effectuer, sans qu'un retour à une représentation non redondante soit nécessaire. Ceci pourrait être utilisé, par exemple, pour une multiplication scalaire sur une courbe elliptique : lors de la multiplication scalaire tous les calculs seraient alors faits modulo $X^{(r+1)\Delta} + 1$, et seulement à la fin une réduction modulo P serait effectuée pour revenir à une représentation non redondante.

- *Deuxième Implantation :* celle ci est l'implantation plus classique où l'on calcule modulo P d'une manière similaire à ce qui a été fait précédemment dans la section 4.1 traitant de la multiplication modulo un polynôme général. Nous exploiterons tout de même la spécificité de P lors de la réduction, car nous ferons une réduction en deux étapes, une première étape où l'on réduira modulo $X^{(r+1)\Delta} + 1$ ce qui se fait très simplement, puis une seconde réduction modulo P.

4.4.2 Calcul Modulo $X^{(r+1)\Delta} + 1$

Nous allons voir ici comment implanter l'arithmétique dans $\mathcal{A} = \mathbb{F}_2[X]/(X^{(r+1)\Delta} + 1)$. Pour multiplier deux éléments U, V nous procéderons comme dans le cas d'un polynôme général P (cf. section 4.1 de ce chapitre). Nous calculerons la matrice M_U dans la base polynômiale de l'application ϕ_U de multiplication par U dans $\mathcal{A}$, puis effectuer le produit matriciel $M_U \cdot V$.

Proposition 6 (Matrice M_U modulo $X^{n'}+1$)**.** *Soit $\mathcal{A} = \mathbb{F}_2[X]/(X^{(r+1)\Delta}+1)$, $n' = (r+1)\Delta$, et $U = \sum_{i=0}^{n'-1} u_i X^i$, alors la matrice M_U de l'application ϕ_U de multiplication par U dans la base polynômiale $\mathcal{B} = (1, \ldots, X^{(r+1)\Delta-1})$ de $\mathcal{A}$ est donnée par*

$$M_U = \begin{bmatrix} u_0 & u_{n'-1} & u_{n'-2} & \cdots & u_1 \\ u_1 & u_0 & u_{n'-1} & \cdots & u_2 \\ u_2 & u_1 & u_0 & \cdots & u_3 \\ \vdots & & & & \vdots \\ u_{n'-2} & u_{n'-3} & u_{n'-4} & \cdots & u_{n'-1} \\ u_{n'-1} & u_{n'-2} & u_{n'-3} & \cdots & u_0 \end{bmatrix}$$

Démonstration. La matrice M_U est la matrice dans la base polynômiale $\mathcal{B}$ de l'application linéaire $\phi_U : V \mapsto \phi_U(V) = V \mod (X^{n'}+1)$. Il suffit donc de calculer l'image par ϕ_U des éléments de la base polynômiale de $\mathcal{A}$, c'est-à-dire calculer $\phi_U(X^j) = UX^j \mod (X^{n'}+1)$ pour $j = 0, \ldots, n'-1$. Les colonnes de M_U seront alors données par les coefficients de $UX^j \mod (X^{n'}+1)$.

$$\begin{aligned} UX^j &= \sum_{i=0}^{n'-1} u_i X^{i+j} = \sum_{i=0}^{n'-1} u_i X^{[i+j]_{n'}} \\ &= \sum_{i=0}^{j-1} u_{n'-j+i} X^i + \sum_{i=j}^{n'-1} u_{i-j} X^i. \end{aligned}$$

où l'on a noté $[m]_{n'}$ le reste de m modulo n'. □

Si l'on utilise une architecture habituelle pour la multiplication matrice-vecteur, la multiplication dans $\mathcal{A}$ aura une complexité matérielle de

$$((r+1)\Delta)^2 \text{ AND } \text{ et } ((r+1)\Delta - 1)(r+1)\Delta \text{ XOR},$$

et une complexité temporelle de

$$T_A + \lceil \log_2 ((r+1)\Delta) \rceil T_X.$$

Mise au carré :

Si l'on suppose que $n' = (s+1)\Delta$ est premier avec 2, et si l'on définit l'ensemble $\mathcal{S} = \{0, \ldots, n'-1\}$ alors l'application

$$\begin{array}{rccl} \sigma : & \mathcal{S} & \to & \mathcal{S} \\ & i & \mapsto & 2i \mod n' \end{array}$$

est une bijection de $\mathcal{S}$. Elle admet donc une bijection inverse $\sigma^{-1} : \mathcal{S} \to \mathcal{S}$.

Dans ce cas nous obtenons le résultat suivant pour la mise au carré.

Lemme 9. *Sous l'hypothèse que n' soit premier avec 2, pour $U = \sum_{i=0}^{n'-1} u_i X^i \in \mathcal{A} = \mathbb{F}_2[X]/(X^{n'}+1)$ on a*

$$U^2 = \sum_{i=0}^{n-1} u_{\sigma^{-1}(i)} X^i \tag{29}$$

La mise au carré s'effectue donc en permutant les coefficients de U suivant la bijection σ^{-1}, c'est donc une opération très simple à effectuer.

4.4.3 Calcul modulo un équiréparti

Maintenant étudions le cas de la multiplication modulo P, où P est un équiréparti. Ceci reprend un travail dû à Koc et Halbutogullari dans [12].

Fixons d'abord quelques notations. Soit $E = \mathrm{Vect}(1, \ldots, X^{r\Delta-1})$ le sous $\mathbb{F}_2$-espace vectoriel de $\mathcal{A} = \mathbb{F}_2[X]/(X^{(r+1)\Delta}+1)$. Soit $U \in E$ et $\widehat{M}_U$ la matrice dans les bases polynômiales respectives de E et $\mathcal{A}$ de l'application

$$\begin{array}{rccc} \widehat{\phi}_U : & E & \to & \mathcal{A} \\ & V & \mapsto & UV \end{array}$$

Notons ici $R' : \mathcal{A} \to \mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ l'application de réduction modulo P . Par linéarité de la réduction, R' est complètement déterminée par son action sur les X^i. Or pour $i \leq r\Delta - 1$, on a $R(X^i) = X^i$, et pour $i = r\Delta, \ldots, n' - 1$ on a

$$R'(X^i) = \sum_{j=0}^{r-1} X^{i-r\Delta+j\Delta}$$

Pour multiplier deux éléments U, V, la méthode qu'ont utilisée Koc et Halbutogullari dans [12], consiste à faire d'abord le produit de $W' = \widehat{M}_U \cdot V$, c'est-à-dire calculer $UV \mod (X^{(r+1)\Delta} + 1)$ et ensuite à réduire modulo P en calculant $W = R'(W')$.

Etablissons la matrice $\widehat{M}_U$ de l'application $\widehat{\phi}_U$ qui envoie un élément V de $E = \mathrm{Vect}_{\mathbb{F}_2}(1, X, X^2, \ldots, X^{r\Delta-1})$ sur $UV \mod (X^{(r+1)\Delta} + 1)$ de $\mathcal{A}$ dans les bases polynômiales respectives de E et $\mathcal{A}$

Lemme 10 ([12])**.** *Soit $U = u_0 + \ldots + u_{r\Delta-1}X^{r\Delta-1} \in E$, alors la matrice $\widehat{M}_U$ est donnée par*

$$\widehat{M}_U = \begin{bmatrix} u_0 & 0 & 0 & \ldots & 0 & u_{r\Delta-1} & u_{r\Delta-2} & \ldots & u_{\Delta+1} \\ u_1 & u_0 & 0 & \ldots & 0 & 0 & u_{r\Delta-1} & \ldots & u_{\Delta+2} \\ \vdots & & & & & & & & \vdots \\ u_{r\Delta-1} & u_{r\Delta-2} & u_{r\Delta-3} & \ldots & u_{(r-1)\Delta-1} & u_{(r-1)\Delta-2} & u_{(r-1)\Delta-3} & \ldots & u_0 \\ 0 & u_{r\Delta-1} & u_{r\Delta-2} & \ldots & u_{(r-1)\Delta} & u_{(r-1)\Delta-1} & u_{(r-1)\Delta-2} & \ldots & u_1 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & 0 & \ldots & u_{r\Delta-1} & u_{r\Delta-2} & u_{r\Delta-3} & \ldots & u_{\Delta-1} \end{bmatrix}$$

Démonstration. La matrice $\widehat{M}_U$ peut se calculer à partir de la matrice M_U donnée dans la propriété 6. Tout d'abord, les coefficients de U suivant $X^{r\Delta}, \ldots, X^{(r+1)\Delta-1}$ sont nuls ; ensuite, on efface les Δ dernières colonnes de la matrice M_U de la propriété 6 car elles correspondent à l'image par $V \mapsto UV$ des vecteurs $X^{r\Delta}, \ldots, X^{(r+1)\Delta-1}$ de la base de $\mathcal{A}$ qui ne font pas parti de la base de E. Après avoir fait ceci on obtient la matrice $\widehat{M}_U$ cherchée. □

La seconde étape pour calculer le produit consiste à réduire W' modulo P. Nous avons le résultat suivant

Lemme 11 ([12])**.** *Soit $W' = w'_1 + w'_2 X + \ldots + w'_{(r+1)\Delta-1} X^{(r+1)\Delta-1} \in \mathcal{A}$, alors*

$$W = R'(W') = \sum_{i=0}^{r} \sum_{j=0}^{\Delta-1} (w'_{i\Delta+j} + w'_{r\Delta+j}) X^{i\Delta+j}.$$

Démonstration. Nous avons

$$\begin{aligned} R'(W') &= R'(\sum_{i=0}^{r-1}\sum_{j=0}^{\Delta-1} w'_{i\Delta+j}X^{i\Delta+j}) + R'(\sum_{j=0}^{\Delta-1} w'_{r\Delta+j}X^{r\Delta+j}) \\ &= \sum_{i=0}^{r-1}\sum_{j=0}^{\Delta-1} w'_{i\Delta+j}X^{i\Delta+j} + \sum_{j=0}^{\Delta-1} w'_{r\Delta+j}R'(X^{r\Delta+j}). \end{aligned}$$

Or pour tout $j \in \{0, \ldots, \Delta-1\}$

$$R'(X^{r\Delta+j}) = \sum_{i=0}^{r-1} X^{i\Delta+j},$$

ce qui finalement nous donne

$$W = R'(W') = \sum_{i=0}^{r-1}\sum_{j=0}^{\Delta-1} \left(w'_{i\Delta+j} + w'_{r\Delta+j}\right) X^{i\Delta+j}.$$

□

Maintenant nous allons pouvoir décrire totalement la multiplication dans la base polynômiale de $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où P est un polynôme équiréparti. Soient deux éléments $U, V \in \mathbb{F}_{2^n}$, nous effectuerons d'abord le produit matriciel $W' = \widehat{M}_U \cdot V$ où $\widehat{M}_U$ est donnée dans la proposition 10, puis réduirons $W = R'(W')$ modulo P avec la formule établie dans la proposition précédente.

Algorithme 6 Multiplieur pour equiréparti [12]

Entrée. $U = [u_0, \ldots, u_{r\Delta-1}]$ et $V = [v_0, \ldots, v_{r\Delta-1}]$.

Etape 1. *Calcul du produit modulo* $(r+1)\Delta$

$W' \leftarrow \widehat{M}_U \cdot V$

Etape 2. *Réduction modulo* P

pour $i = 0, 1, \ldots, r$ **et** $j = 0, 1, \ldots, \Delta-1$ **faire**

$w_i \leftarrow w'_{i\Delta+j} + w'_{r\Delta+j}$

Sortie. $W \leftarrow [w_0, \ldots, w_{r\Delta-1}]$.

Complexité. D'abord pour le produit $\widehat{M}_U \cdot V$, nous avons une complexité matérielle est de $r(r+1)\Delta^2$ AND et $(r\Delta-1)(r+1)\Delta$ XOR . En effet cette matrice est constituée de $(r+1)\Delta$ lignes, et ces lignes contiennent $r\Delta$ coefficients non nuls. La complexité temporelle de cette étape est égale à $(\lceil \log_2(r\Delta) \rceil) T_X + T_A$.

La réduction de W' en $W = R'(W')$ nécessite $r\Delta$ XOR et un délai de T_X.

Nous obtenons donc une complexité matérielle totale de

$$r(r+1)\Delta^2 \text{ AND et } ((r\Delta-1)(r+1)\Delta + r\Delta) \text{ XOR },$$

La complexité en temps est, elle, de

$$(\lceil \log_2(r\Delta) \rceil + 1) T_X + T_A.$$

5 Corps de caractéristique arbitraire

Cette section est dédiée à expliciter les mutiplieurs d'un corps fini $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ où P sera dans un premier temps un binôme et dans un second temps un trinôme de $\mathbb{F}_q[X]$. Nous nous intéresserons aussi à l'élévation à la puissance q dans le cas du binôme, et à la puissance 3 dans le cas du trinôme lorsque $q = 3$.

5.1 Binôme

Nous allons voir ici comment on multiplie modulo un binôme. Pour un exposé plus complet sur ce sujet le lecteur pourra se reporter à l'article de Bailey et Paar ¡¡ Optimal Extention Field (OEF) ¿¿ [1]. Soient donc $P = X^n - \alpha$ un binôme irréductible de $\mathbb{F}_q[X]$, l'extension $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ de $\mathbb{F}_q$ définie par P et $\mathcal{B}_P = (1, X, X^2, \ldots, X^{n-1})$ la $\mathbb{F}_q$-base polynômiale de $\mathbb{F}_{q^n}$.

La proposition suivante explicite les conditions nécessaires et suffisantes pour qu'un binôme $X^n - \alpha \in \mathbb{F}_q$ soit irréductible.

Proposition 7. *Un binôme $X^n - \alpha \in \mathbb{F}_q[X]$ est irréductible si et seulement si*
- *Tout p premier divisant n divise l'ordre de α dans $\mathbb{F}_{q^n}^{\times}$.*
- *On a $4 \mid n$ ou $4 \mid q-1$.*

Ceci implique que tout premier impair divisant n doit diviser $q - 1$, ce qui restreint à un nombre assez réduit (dépendant évidement de q) d'entiers n admettant un binôme $X^n - \alpha \in \mathbb{F}_q[X]$ irréductible.

La proposition suivante donne les matrices de structure M_s associées à la base polynômiale de $\mathbb{F}_q[X]/(X^n - \alpha)$, ainsi que la matrice M_U de l'application ϕ_U de multiplication par U dans $\mathbb{F}_{q^n}$, où $U \in \mathbb{F}_{q^n}$. Nous ne donnons aucune preuve car elle est à peu de chose près la même que celle de la proposition 6 traitant du calcul modulo $X^{n'} + 1$.

Théorème 2. *Soient $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(X^n - \alpha)$, $\mathcal{B} = (1, \ldots, X^{n-1})$ la $\mathbb{F}_q$-base polynômiale associée à X, et $M_s = [\lambda_{i,j}(s)]_{i,j=1,\ldots,n}$ la matrice de structure d'indice s associée à la base polynômiale $\mathcal{B}_P = (1, X, \ldots, X^{n-1})$ de $\mathbb{F}_{q^n}$. Les coefficients $\lambda_{i,j}(s)$ de $M_s = [\lambda_{i,j}(s)]_{i,j=0,\ldots,n-1}$ sont de la fome suivante*

$$\lambda_{i,j}(s) = \begin{cases} 1 & si\ i + j = s \\ \alpha & si\ i + j = n + s \\ 0 & sinon \end{cases}$$

La matrice M_U dans la base $\mathcal{B}_P$ de l'application ϕ_U de multiplication par l'élément $U \in \mathbb{F}_{q^n}$ est donnée par

$$M_U = \begin{bmatrix} u_0 & \alpha u_{n-1} & \alpha u_{n-2} & \cdots & \alpha u_1 \\ u_1 & u_0 & \alpha u_{n-1} & \cdots & \alpha u_2 \\ u_2 & u_1 & u_0 & \cdots & \alpha u_3 \\ \vdots & & & & \vdots \\ u_{n-2} & u_{n-3} & u_{n-4} & \cdots & \alpha u_{n-1} \\ u_{n-1} & u_{n-2} & u_{n-3} & \cdots & u_0 \end{bmatrix}.$$

La multiplication dans $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(X^n - \alpha)$ se fait alors en deux étapes, une première étape où l'on multiplie par α les coordonnées $u_1, \ldots, u_{n-1}$ de U. Une seconde étape où l'on calcule W le produit de U par V dans $\mathbb{F}_{q^n}$, en effectuant le produit matriciel $W = M_U \cdot V$.

Maintenant regardons comment s'effectue l'élévation à la puissance q.

Soit $i \in \{0, \dots n-1\}$, et soit $\tau(i)$ le quotient de la division euclidienne de iq par n et $\sigma(i)$ son reste. Autrement dit

$$qi = \tau(i)n + \sigma(i) \quad \text{et} \quad 0 \leq \sigma(i) < n.$$

Du fait que $X^n = \alpha$, on obtient $(X^i)^q = X^{iq} = \alpha^{\tau(i)} X^{\sigma(i)}$. Comme $U \mapsto U^q$ est un automorphisme de $\mathbb{F}_{q^n}$, l'application $i \mapsto \sigma(i)$ est obligatoirement une bijection de $\{0, \dots, n-1\}$.

L'élévation de $U = \sum_{i=0}^{n-1} u_i X^i \in \mathbb{F}_{q^n}$ peut finalement s'exprimer comme suit

$$U^q = \sum_{i=0}^{n-1} u_{\sigma^{-1}(i)} \alpha^{\tau(\sigma^{-1}(i))} X^i.$$

Elle est donc dans ce cas assez simple à effectuer : si les produits $u_j \alpha^{\tau(j)}$ dans $\mathbb{F}_q$ sont effectués en parallèle le coût est alors d'une multiplication par une constante.

5.2 Trinôme

Pour terminer ce chapitre nous allons étudier l'arithmétique des corps $\mathbb{F}_q[X]/(P)$ où P est un trinôme irréductible. Nous verrons dans un premier temps comment multiplier deux éléments U, V dans une représentation en base polynômiale, et ensuite, pour $q = 3$, comment élever les éléments $U \in \mathbb{F}_{q^n}$ au cube.

5.2.1 Multiplication

Nous allons établir ici un multiplieur dans le corps $\mathbb{F}_q[X]/(X^n - \alpha X^k - \beta)$. Nous nous restreindrons à un trinôme vérifiant $k \leq \frac{n}{2}$. D'après le lemme 4 on peut en fait toujours se ramener à ce cas. Le multiplieur que nous allons construire est toujours sur le même schéma : il s'agit de construire la matrice M_U de l'application ϕ_U de multiplication par U dans $\mathbb{F}_{q^n}$, ensuite on en déduit le produit de U par V en effectuant le produit matrice vecteur $M_U \cdot V$.

On va construire la matrice M_U en utilisant la méthode de réduction de $\widehat{M_U}$ que l'on a vu précédemment pour les corps $\mathbb{F}_{2^n}$. D'une manière similaire à ce qui a été fait dans le cas du trinôme de $\mathbb{F}_2[X]$, la matrice M_U dans la base polynômiale de la multiplication par U dans $\mathbb{F}_q[X]/(X^n - \alpha X^k - \beta)$ est donnée par

$$M_U = (\widehat{M_U})_H + \beta \left((\widehat{M_U})_B + \alpha (\widehat{M_U})_B [\uparrow (n-k)] \right) + \alpha \left((\widehat{M_U})_B + \alpha (\widehat{M_U})_B [\uparrow (n-k)] \right) [\downarrow k]$$

En utilisant cette expression, nous pouvons encore exprimer M_U à partir de trois types de coefficients u_i, u'_i, u''_i comme cela est expliqué dans la proposition suivante :

Proposition 8 (Multiplieur pour Trinome sur $\mathbb{F}_q$)**.** *Soient $P = X^n - \alpha X^k - \beta$ un trinôme irréductible de $\mathbb{F}_q[X]$, $U = u_0 + u_1 X + \cdots + u_{n-1} X^{n-1} \in \mathbb{F}_q[X]/(P)$ et soient les coefficients u_i, u'_i, u''_i suivants*

$$\begin{aligned} u'_i &= u_i + \alpha u_{i+(n-k)} \quad \textit{pour} \quad i = 0, \dots, k-1, \\ u''_i &= \begin{cases} \beta u_i + \alpha u'_{i-k} & \textit{pour} \quad i = k+1, \dots, 2k-1, \\ \beta u_i + \alpha u_{i-k} & \textit{pour} \quad i = 2k, \dots, n-1. \end{cases} \end{aligned} \tag{30}$$

La matrice de la multiplication par U dans la base polynômiale de $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(X^n - \alpha X^k - \beta)$ est donnée par

$$M_U = \begin{bmatrix} u_0 & \beta u_{n-1} & \beta u_{n-2} & \cdots & \beta u_{k+1} & \beta u_k & \beta u'_{k-1} & \cdots & \beta u'_1 \\ u_1 & u_0 & \beta u_{n-1} & \cdots & \beta u_{k+2} & \beta u_{k+1} & \beta u_k & \cdots & \beta u'_2 \\ \vdots & & \ddots & \ddots & & & & \ddots & \vdots \\ u_{k-1} & u_{k-2} & u_{k-3} & \cdots & \beta u_{n-1} & & & \cdots & \beta u_k \\ u_k & u'_{k-1} & u'_{k-2} & \cdots & u'_0 & u''_{n-1} & & & u''_{k+1} \\ u_{k+1} & u_k & u'_{k-1} & \cdots & \cdots & u'_0 & u''_{n-1} & \cdots & u''_{k+2} \\ \vdots & & & & & & \ddots & \ddots & \vdots \\ u_{n-2} & \cdots & & & & & & \ddots & u''_{n-1} \\ u_{n-1} & \cdots & \cdots & \cdots & \cdots & u_k & u'_{k-1} & \cdots & u'_0 \end{bmatrix} \tag{31}$$

A partir des résultats de la proposition précédente, la multiplication de deux éléments $U, V \in \mathbb{F}_{q^n}$ peut se faire comme suit.

– calcul des u_i, u'_i, u''_i suivant les formules (30), et de $\beta u_i, \beta u'_i$.
– calcul du produit matriciel $W = M_U \cdot V$.

Complexité. Nous allons d'abord déterminer la complexité de chaque étape du multiplieur indépendamment. Lors de la première étape, les calculs étant effectués en parallèle, le calcul des coefficients nous avons besoin $(n-k)$ multiplieurs par β, notés Mult_β, pour le calcul des $\beta u_i,\ i = k, \ldots, n-1$, qui serviront ensuite pour le calcul de $\beta u'_i,\ i = 0 \ldots, k-1$. Ensuite il faut $(n-1)$ multiplieurs par α, notés Mult_α, pour le calcul des αu_i. Enfin nous avons besoin de n additionneurs Add_q pour le calcul des u'_i, u''_i. D'où, au total, cette étape requiert $(n-k)\text{Mult}_\beta$ et $(n-1)\text{Mult}_\alpha + n\text{Add}_q$, et s'effectue en un temps $T_{Mult_\beta} + \max(T_{Mult_\beta}, T_{Mult_\alpha}) + T_{Add_q}$.

La seconde étape consiste en n produits ligne-colonne effectués parallèle, elle a donc une complexité spatiale de $n^2\text{Mult}_q$ et $n(n-1)\text{Add}_q$ et une complexité en temps de $T_{Mult_q} + \lceil \log_2(n) \rceil T_{Add_q}$.

Le complexité matérielle totale du multiplieur est, en fin de compte, égale à

$$(n-k)\text{Mult}_\beta, (n-1)\text{Mult}_\alpha, n^2\text{Mult}_q \text{ et } n^2\text{Add}_q,$$

et la complexité en temps est égale à

$$2T_{Mult_\beta} + T_{Mult_\alpha} + T_{Mult_q} + (1 + \lceil \log_2(n) \rceil) T_{Add_q}.$$

5.2.2 Elévation au cube quand $q = 3$

Comme nous l'avons déjà mentionné, il est parfois possible de tirer parti d'une bonne élévation à la puissance q dans $\mathbb{F}_{q^n}$, comme par exemple lors d'une inversion d'Itoh-Tsujii (cf. algorithme 1), ou d'une multiplication scalaire sur une courbe elliptique (cf. chapitre **??**). Nous allons déterminer des formules pour l'élévation à la puissance $q = 3$ lorsque les éléments sont représentés dans la base polynômiale de $\mathbb{F}_3[X]/(X^n - \alpha X^k - \beta)$. Afin de simplifier l'exposé nous nous restreindrons au cas des trinômes $X^n - \alpha X^k - \beta$ vérifiant $k < \frac{n}{3}$ et $(n-k) \equiv 1 \mod 3$ et $n \equiv 2 \mod 3$.

Soit $U = \sum_{i=0}^{n-1} u_i X^i$ un élément de $\mathbb{F}_3[X]/(X^n - \alpha X^k - \beta)$. L'objectif ici, c'est de déterminer les coordonnées v_i de $V = U^3$ dans la base polynômiale en fonction des coordonnées u_i de U. La

première chose que l'on remarque, parce que nous sommes en caractéristique 3, si on l'éléve U à la puissance 3 nous obtenons

$$U^3 = \sum_{i=0}^{n-1} u_i (X^i)^3 = \sum_{i=0}^{n-1} u_i X^{3i}.$$

A partir de cette expression, pour déterminer les v_i de $V = U^3$, il faut que nous réduisions les monômes X^{3i} de degré $3i \geq n$. Nous obtenons les différentes expressions suivantes.

– Pour $\frac{n}{3} \leq i \leq \frac{2n-1}{3}$

$$\begin{array}{rcll} X^{3i} & = & \alpha X^{3i-l} + \beta X^{3i-n} & \text{si} \quad \frac{n}{3} \leq i < \frac{n+l}{3}, \\ X^{3i} & = & \alpha^2 X^{3i-2l} + \alpha\beta X^{3i-l-n} + \beta X^{3i-n} & \text{si} \quad \frac{n+l}{3} \leq i < \frac{2n}{3}, \end{array}$$

– Pour $\frac{2n}{3} \leq i \leq n-1$

$$\begin{array}{rcll} X^{3i} & = & \alpha^2 X^{3i-2l} - \alpha\beta X^{3i-l-n} + \beta^2 X^{3i-2n} & \text{si} \quad \frac{2n}{3} \leq i < \frac{n+2l}{3}, \\ X^{3i} & = & \alpha X^{3i-3l} + \alpha^2\beta X^{3i-2l-n} - \alpha\beta X^{3i-n-l} + \beta^2 X^{3i-2n} & \text{si} \quad \frac{n+2l}{3} \leq i < \frac{2n+l}{3}, \\ X^{3i} & = & \alpha X^{3i-3l} - \alpha\beta^2 X^{3i-2n-l} + \beta^2 X^{3i-2n} & \text{si} \quad \frac{2n+l}{3} \leq i < n. \end{array}$$

Nous devons maintenant remplacer les X^{3i} par les expressions réduites trouvées ci-dessus dans l'expression de U^3. Nous obtenons

$$\begin{aligned} U^3 = & \sum_{0 \leq i < \frac{n}{3}} u_i X^{3i} + \sum_{\frac{n}{3} \leq i < \frac{n+l}{3}} \alpha u_i X^{3i-l} + \sum_{\frac{n}{3} \leq i < \frac{2n}{3}} \beta u_i X^{3i-n} + \sum_{\frac{n+l}{3} \leq i < \frac{n+2l}{3}} \alpha^2 u_i X^{3i-2l} \\ & + \sum_{\frac{n+l}{3} \leq i < \frac{2n}{3}} \alpha\beta u_i X^{3i-l-n} - \sum_{\frac{2n}{3} \leq i < \frac{2n+l}{3}} \alpha\beta u_i X^{3i-l-n} + \sum_{\frac{l+2n}{3} \leq i < \frac{2n+l}{2}} \alpha^2\beta u_i X^{3i-l+2n} \\ & - \sum_{\frac{2n+l}{3} \leq i < n} \alpha\beta^2 u_i X^{3i-2n-l} + \sum_{\frac{2n}{3} \leq i < n} \beta^2 u_i X^{3i-2l-n} + \sum_{\frac{2l+n}{3} \leq i < n} \alpha u_i X^{3i-3l} \\ & + \sum_{\frac{2n}{3} \leq i < n} \beta^2 u_i X^{3i-2n} \end{aligned} \tag{32}$$

Nous avons supposé que $l \equiv 1 \mod 3$ et $n \equiv 2 \mod 3$. Nous devons trier les différents monômes dans l' expression de U^3 selon que leur degré est congru modulo 3 d'une part à 0, d'autre part à 1, et finalement à 2.

1. *Les degrés congru à* 0 *modulo* 3 *:* ce sont les degrés $3j, 3j-3l, 3j-n-l$.
2. *Les degrés congru à* 1 *modulo* 3 *:* ce sont les degrés $3j-n, 3j-2n-l, 3j-2l$.
3. *Les degrés congru à* 2 *modulo* 3 *:* ce sont les degrés $3j-2l-n, 3j-l, 3j-2n$.

Nous rassemblons finalement, chacun des monômes de degré congru à 0 modulo 3 dans une somme de X^{3i}, chacun des monômes de degré congru à 1 modulo 3 dans une somme de X^{3i+1}, et chacun des monômes de degré congru à 2 modulo 3 dans une somme de X^{3i+2}.

Nous obtenons finalement l'expression suivante pour U^3

$$\begin{aligned}
U^3 = &\sum_{i=0}^{\frac{k+2}{3}-1} \left(u_i + \alpha\beta u_{i+\frac{n+l}{3}}\right) X^{3i} \\
&+ \sum_{i=\frac{k+2}{3}}^{k-1} \left(u_i + \alpha u_{i+l} + \alpha\beta u_{i+\frac{n+l}{3}}\right) X^{3i} + \sum_{i=k}^{\frac{n-2}{3}} \left(u_i - \alpha\beta u_{i+\frac{n+l}{3}}\right) X^{3i} \\
&+ \sum_{i=0}^{\frac{k-4}{3}} \left(\beta u_{i+\frac{n+1}{3}} - \beta^2\alpha u_{i+\frac{2n+l+1}{3}}\right) X^{3i+1} + \sum_{i=\frac{k-1}{3}}^{\frac{n-2}{3}} \left(\beta u_{i+\frac{n+1}{3}} + \alpha^2 u_{i+\frac{2l+1}{3}}\right) X^{3i+1} \\
&+ \sum_{i=0}^{\frac{k-4}{3}} \left(\alpha^2\beta u_{i+\frac{2l+n+2}{3}} + \beta^2 u_{i+\frac{2n+2}{3}}\right) X^{3i+2} + \sum_{i=\frac{k-1}{3}}^{\frac{n-2}{3}-1} \left(\alpha u_{i+\frac{l+2}{3}} + \beta^2 u_{i+\frac{2n+2}{3}}\right) X^{3i+2}.
\end{aligned}$$

Autrement dit, nous avons trouvé les différentes expressions suivantes des coordonnées v_i de $V = U^3$

$$\begin{aligned}
v_{3i} &= u_i + \alpha\beta u_{i+\frac{n+l}{3}} && \text{si} \quad 0 \le i \le \tfrac{k+2}{3} - 1, \\
v_{3i} &= u_i + \alpha u_{i+l} + \alpha\beta u_{i+\frac{n+l}{3}} && \text{si} \quad \tfrac{k+2}{3} < i \le k - 1, \\
v_{3i} &= u_i - \alpha\beta u_{i+\frac{n+l}{3}} && \text{si} \quad k < i \le \tfrac{n-2}{3}, \\
v_{3i+1} &= \beta u_{i+\frac{n+1}{3}} - \beta^2\alpha u_{i+\frac{2n+l+1}{3}} && \text{si} \quad 0 \le i \le \tfrac{k-4}{3}, \\
v_{3i+1} &= \beta u_{i+\frac{n+1}{3}} + \alpha^2 u_{i+\frac{2l+1}{3}} && \text{si} \quad \tfrac{k-1}{3} \le i \le \tfrac{n-2}{3}, \\
v_{3i+2} &= \alpha^2\beta u_{i+\frac{2l+n+2}{3}} + \beta^2 u_{i+\frac{2n+2}{3}} && \text{si} \quad 0 \le i \le \tfrac{k-4}{3}, \\
v_{3i+2} &= \alpha u_{i+\frac{l+2}{3}} + \beta^2 u_{i+\frac{2n+2}{3}} && \text{si} \quad \tfrac{k-1}{3} \le i \le \tfrac{n-2}{3} - 1.
\end{aligned}$$

Nous pouvons observer que l'élévation au cube est une opération relativement simple à effectuer : en effet pour le calcul de chaque coordonnée v_i nous devons seulement faire deux ou trois multiplications par des éléments constants de $\mathbb{F}_3$, suivies d'une ou deux additions dans $\mathbb{F}_3$.

Remarque 5. Pour d'autre types de trinômes de $\mathbb{F}_3[X]$ nous pouvons obtenir des formules semblables pour l'élévation au cube. De même pour d'autre valeur de q, par exemple pour $q = 5, 7, \ldots$, nous pouvons établir des formulations similaires de l'élévation à la puissance q dans $\mathbb{F}_{q^n}$.

Base Normale

6 Généralités

L'utilisation des bases normales pour l'implantation de l'arithmétique des corps finis, a d'abord été proposée par Massey et Omura dans [18]. Depuis, ce type de base a bénéficié d'une attention accrue de la communauté scientifique, et de nombreux travaux ont été publiés sur ce sujet [15, 16, 21, 13, 20, 4].

L'une des particularités des bases normales, c'est que l'élévation à la puissance q dans $\mathbb{F}_{q^n}$ est une opération très simple à effectuer. Il s'agit simplement de permuter cycliquement les coordonnées des éléments du corps. En particulier si $q = 2$, la mise au carré est alors très efficace.

Dans la section 6.1 de ce chapitre, nous donnerons des résultats généraux sur les bases normales : nous montrerons dans le lemme 12 que les matrices de structure se déduisent des une des autres par permutation circulaire et nous donnerons, dans la proposition 9, une borne minimale de la densité des bases normales. Dans la section suivante nous nous concentrerons sur la construction des bases normales optimales (les ONB). Nous construirons dans la proposition 10 un premier type de bases normales optimales les ONB I, et dans la proposition 11 un second type d'ONB, les ONB II. Nous introduirons ensuite les bases normales gaussiennes et nous donnerons une majoration de la densité de ces dernières dans la propriété 9.

Dans les sections 7 et 8 nous construirons les multiplieurs de $\mathbb{F}_{2^n}$ associés aux bases normales optimales. Nous verrons que le multiplieur associé à une ONB I a une complexité matérielle de n^2 AND et (n^2-1) XOR, et une complexité en temps de $T_A+(1+\lceil\log_2(n)\rceil)T_X$. Nous verrons aussi que multiplieur associé à une ONB II a, lui, une complexité en espace de n^2 AND et $\frac{3}{2}n(n-1)$ XOR, et une complexité en temps de $T_A + (1 + \lceil\log_2(n)\rceil)T_X$.

6.1 Définition et résultats généraux

La construction d'une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$, consiste à choisir un élément $\zeta \in \mathbb{F}_{q^n}$ et à élever $n-1$ fois ζ à la puissance q

$$\zeta, \zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{n-1}}.$$

Pour que ce procédé forme bien une base, il faut vérifier que le système formé est $\mathbb{F}_q$-linéairement indépendant.

Définition 9.

1. *Soit ζ un élément de $\mathbb{F}_{q^n}$, ζ est dit normal si le système $\mathcal{B}(\zeta) = \left(\zeta, \zeta^q, \cdots, \zeta^{q^{n-1}}\right)$ forme une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$.*
2. *Une base $\mathcal{B}$ sera dite normale si il existe un $\zeta \in \mathbb{F}_{q^n}$ normal sur $\mathbb{F}_q$ tel que $\mathcal{B} = \mathcal{B}(\zeta)$*

L'aspect le plus intéressant des bases normales tient au fait que l'élévation à la puissance q est une opération très simple : soit $U = (u_0, \ldots, u_{n-1})$ un élément de $\mathbb{F}_{q^n}$ exprimé dans $\mathcal{B}(\zeta)$, si on l'élève à la puissance q on obtient

$$U^q = (u_{n-1}, u_0, u_1, \ldots, u_{n-2}). \tag{33}$$

Dans le cas où $q = 2$, nous voyons que l'élévation au carré est donc une opération très simple dans $\mathbb{F}_{2^n}$.

Si nous nous donnons une base normale $\mathcal{B}(\zeta)$ de $\mathbb{F}_{q^n}$, pour construire un multiplieur dans $\mathbb{F}_{q^n}$ associé à cette base, nous avons besoin de déterminer les matrices de structure $M_s = [\lambda_{i,j}(s)]_{i,j=1,\ldots,n-1}$. Les coefficients $\lambda_{i,j}(s)$ de M_s proviennent des produits

$$\zeta^{q^i}\zeta^{q^j} = \sum_{s=0}^{n-1} \lambda_{i,j}(s)\zeta^{q^s}.$$

Si l'on l'on se donne deux éléments $U = \sum_{i=0} u_i\zeta^{q^i}$ et $V = \sum_{i=0} v_i\zeta^{q^i}$, et que l'on développe le produit UV dans la base $\mathcal{B}(\zeta)$ de $\mathbb{F}_{q^n}$, on obtient

$$\begin{aligned} UV &= \left(\sum_{i=0} u_i\zeta^{q^i}\right)\left(\sum_{i=0} v_i\zeta^{q^i}\right) \\ &= \sum_{i,j=0,\ldots,n-1} u_iv_j(\zeta^{q^i}\zeta^{q^j}) \\ &= \sum_{s=0}^{n-1}\left(\sum_{i,j=0,\ldots,n-1} u_iv_j\lambda_{i,j}(s)\right)\zeta^{q^s}. \end{aligned}$$

Nous voyons donc qu'à partir des matrices M_s, on peut calculer le produit de deux éléments $U, V \in \mathbb{F}_{q^n}$: si $W = UV$, alors le coefficient w_s d'indice s de W est donné par

$$w_s = \sum_{i,j=0,\ldots,n-1} u_iv_j\lambda_{i,j}(s) = ({}^tU)\cdot M_s \cdot V.$$

Nous allons voir maintenant un aspect remarquable des base normales : les matrices de structure M_s se déduisent des unes des autres par permutation circulaire.

Lemme 12 ([18])**.** *Soit $\mathcal{B}(\zeta)$ une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Si $M_s = (\lambda_{i,j}(s))_{i,j=0,\ldots,n-1}$ est une matrice de structure d'indice s associée à $\mathcal{B}(\zeta)$, alors nous avons*

$$\lambda_{i,j}(s) = \lambda_{i-s,j-s}(0). \tag{34}$$

Autrement dit, les matrices M_s se déduisent de M_0 en permutant de manière cyclique les colonnes et les lignes.

Exemple 11. Soit une extension de degré 3 de $\mathbb{F}_2$ définie par $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$. Soit $\zeta = X + 1$ un élément normal de $\mathbb{F}_8$ sur $\mathbb{F}_2$ qui engendre la base $\mathcal{B}(\zeta) = (\zeta, \zeta^2, \zeta^4)$. Dans ce cas nous avons

$$\begin{aligned} \zeta\zeta^2 &= \zeta + \zeta^{2^2}, \\ \zeta\zeta^{2^2} &= \zeta^2 + \zeta^{2^2}, \\ \zeta^2\zeta^{2^2} &= (\zeta\zeta^2)^2 = \zeta + \zeta^2, \end{aligned} \tag{35}$$

et $\zeta\zeta = \zeta^2, \zeta^2\zeta^2 = \zeta^{2^2}, \zeta^{2^2}\zeta^{2^2} = \zeta$. En récupérant les coefficients $\lambda_{i,j}(0)$ dans les produits $\zeta^{2^i}\zeta^{2^j}$, nous construisons la matrice M_0 ci-dessous.

$$M_0 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

En décalant cycliquement de 2 sur la droite les colonnes nous obtenons la matrice suivante

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Ensuite si nous décalons cycliquement de 2 vers le bas les lignes nous obtenons

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

On peut alors vérifier que cette dernière matrice est bien égale à M_2.

♢

Démonstration. Pour montrer les relations entre M_s et M_0, rappelons que $\lambda_{i,j}(l)$ provient de

$$\zeta^{q^i}\zeta^{q^j} = \sum_{l=0}^{n-1} \lambda_{i,j}(l)\zeta^{q^l}.$$

En élevant la précédente équation à la puissance q^{n-s} on obtient

$$\zeta^{q^{i-s}}\zeta^{q^{j-s}} \quad = \quad \textstyle\sum_{l=0}^{n-1} \lambda_{i,j}(l)\zeta^{q^{l-s}} = \sum_{l'=0}^{n-1} \lambda_{i,j}(l'+s)\zeta^{q^{l'}}.$$

On peut finalement remarquer que $\lambda_{i-s,j-s}(0) = \lambda_{i,j}(0+s) = \lambda_{i,j}(s)$. □

Soit U, V deux éléments de $\mathbb{F}_{q^n}$. La propriété précédente implique que le coefficient d'indice s de $W = UV$ est donné par

$$w_s = {}^tU^{q^{n-s}} \cdot M_0 \cdot V^{q^{n-s}}$$

Nous avons alors un premier algorithme pour la multiplication dans $\mathbb{F}_{q^n}$.

Algorithme 7 Multiplieur normal général [18]

Entrée. $U = (u_0, \ldots, u_{n-1}), V = (v_0, \ldots, v_{n-1})$ et $M_0 = [\lambda_{i,j}(0)]_{i,j=0,\ldots,n-1}$
pour i **de** 0 **à** $n-1$ **faire**
$w_s \leftarrow {}^tU^{q^{n-s}} \cdot M_0 \cdot V^{q^{n-s}}$.
Sortie. $W \leftarrow (w_0, \ldots, w_{n-1})$

Soit un élément $U \in \mathbb{F}_{q^n}$. On note M_U la matrice de $\phi_U \colon V \mapsto UV$ de multiplication par U dans $\mathbb{F}_{q^n}$ relativement à $\mathcal{B}(\zeta)$. Cette matrice s'exprime en fonction de U et des matrices de structure M_s par

$$M_U = \begin{bmatrix} ({}^tU) \cdot M_0 \\ \vdots \\ ({}^tU) \cdot M_{n-1} \end{bmatrix}. \tag{36}$$

Si l'on connaît la matrice M_U d'un élément U, on peut alors calculer W le produit de U et V dans $\mathbb{F}_{q^n}$, en effectuant le produit matriciel $W = M_U \cdot V$.

Rappelons que la densité d'une base $\mathcal{B} = (e_0, \ldots, e_{n-1})$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est définie comme

$$d(\mathcal{B}) = \frac{1}{n} \sum_{s=0}^{n-1} \omega(M_s),$$

où les M_s sont les matrices de structure associées à $\mathcal{B}$. Dans le lemme suivant, on met en relation la densité d'une base $\mathcal{B}(\zeta)$ avec la densité de la matrice M_ζ de multiplication par ζ dans $\mathbb{F}_{q^n}$. Ceci nous donnera un moyen plus simple pour calculer la densité d'une base normale.

Lemme 13 ([20])**.** *Soit $\zeta \in \mathbb{F}_{q^n}$ un élément normal sur $\mathbb{F}_q$ et $\mathcal{B}(\zeta)$ sa base normale associée. Soit M_ζ la matrice de $\phi_\zeta \colon U \in \mathbb{F}_{q^n} \mapsto \phi_\zeta(U) = \zeta U$ relativement à $\mathcal{B}(\zeta)$. Alors nous avons $d(\mathcal{B}(\zeta)) = \omega(M_\zeta)$.*

Exemple 12. Dans l'exemple 11 nous avions considéré le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3 + X + 1)$ et l'élément normal $\zeta = X + 1$.

Nous avions calculé les matrices de structure M_s associées à $\mathcal{B}(\zeta)$

$$M_0 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad M_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

La densité de la base vaut par définition $d(\mathcal{B}(\zeta)) = \frac{1}{3}\left(\omega(M_0) + \omega(M_1) + \omega(M_2)\right) = 5$. D'autre part avec l'expression de M_U de l'équation 36, on obtient que

$$M_\zeta = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

et l'on peut vérifier que $\omega(M_\zeta) = d(\mathcal{B}(\zeta))$.

♢

Démonstration. La colonne d'indice i de la matrice de M_ζ est, par définition, constituée des coefficients de $\phi_\zeta(\zeta^{q^i}) = \zeta\zeta^{q^i}$ dans la base $\mathcal{B}(\zeta)$. Nous voyons donc que

$$\omega(M_\zeta) = \sum_{i=0}^{n-1} \omega(\zeta\zeta^{q^i}).$$

Par ailleurs, dans le chapitre nous avons vu une seconde expression de la densité d'une base, donnée par l'équation (6) dans le lemme 2 page 11. En appliquant cette formule à la base $\mathcal{B}(\zeta)$ nous obtenons

$$d(\mathcal{B}(\zeta)) = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \omega((\zeta^{q^i}\zeta^{q^j})).$$

On arrange ensuite l'expression précédente en

$$d(\mathcal{B}(\zeta)) = \frac{1}{n} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \omega((\zeta\zeta^{q^i})^{q^j}).$$

Or avec l'expression (33) de l'élévation à la puissance q, on remarque que pour tout $U \in \mathbb{F}_{q^n}$, $\omega(U^{q^j}) = \omega(U)$. Ce qui nous donne l'expression suivante de la densité de $\mathcal{B}(\zeta)$

$$d(\mathcal{B}(\zeta)) = \frac{1}{n}\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}\omega(\zeta\zeta^{q^i}) = \sum_{i=0}^{n-1}\omega(\zeta\zeta^{q^i})$$

Ce qui est bien égal à $\omega(M_\zeta)$. □

Le nombre de bases normales (ou d'éléments normaux) de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est assez important comme le montre par exemple le travail de Gao dans [10] sur la densité des éléments normaux . Toutes ces bases offrent le même avantage pour l'élévation à la puissance q, mais pas forcément pour la multiplication. Comme on l'a vu dans le chapitre , une base est une ¡¡bonne¿¿ base si sa densité $d(\mathcal{B}(\zeta))$ est faible (i.e., que le nombre de $\lambda_{i,j}(s) \neq 0$ est faible). Il s'agit donc maintenant de trouver les meilleures bases normales, i.e., les bases de faible densité de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Commençons par établir une borne minimale sur la densité des bases normales.

Proposition 9 ([20])**.** *Si $\mathcal{B}(\zeta)$ est une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ alors $d(\mathcal{B}(\zeta)) \geq 2n-1$.*

Démonstration. Soit $\mathcal{B} = (\zeta, \ldots, \zeta^{q^{n-1}})$ une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Considérons la $n \times n$ matrice M_ζ de l'application ϕ_ζ de multiplication par ζ dans $\mathbb{F}_{q^n}$. On sait par le lemme 13 que la densité de $\mathcal{B}(\zeta)$ est donnée par

$$d(\mathcal{B}(\zeta)) = \omega(M_\zeta).$$

Nous allons montrer que les lignes $L_i(M_\zeta)$ pour $i = 1, \ldots, n-1$ ont au moins 2 coefficients non nuls et que $L_0(M_\zeta)$ a au moins un coefficient non nul.

D'abord remarquons que M_ζ a dans chaque ligne $L_i(M_\zeta)$ au moins un coefficient non nul : ceci vient du lemme 1 qui nous dit que M_ζ est inversible, et donc ne peut pas avoir de ligne nulle.

Montrons maintenant que les lignes $L_i(M_\zeta)$ pour $i = 1, \ldots, n-1$ ont, en fait, plus de deux coefficients non nuls. Nous allons pour cela utiliser l'expression de la trace de ζ suivante

$$\sum_{i=0}^{n-1}\zeta^{q^i} = Tr(\zeta).$$

Si l'on multiplie $Tr(\zeta)$ par ζ on obtient

$$Tr(\zeta)\zeta = \zeta\sum_{i=0}^{n-1}\zeta^{q^i} = \sum_{i=0}^{n-1}\zeta\zeta^{q^i}. \tag{37}$$

Par définition, la matrice M_ζ a pour colonne d'indice i les coefficients dans $\mathcal{B}(\zeta)$ de

$$\phi_\zeta(\zeta^{q^i}) = \zeta\zeta^{q^i}.$$

Autrement dit si l'on note $\alpha = Tr(\zeta) \in \mathbb{F}_q$ et $C_i(M_\zeta)$ la colonne d'indice i de la matrice M_ζ, on peut réécrire l'équation (37) en une somme de vecteurs colonnes

$$\begin{bmatrix} \alpha \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \sum_{i=0}^{n-1} C_i(M_\zeta).$$

La somme des colonnes de M_ζ est donc un vecteur ayant $\alpha = Tr(\zeta)$ comme première coordonnée, et 0 aux autres coordonnées. Autrement dit, la somme des coefficients de $L_i(M_\zeta)$ est égale à 0 lorsque $i \geq 1$. On sait déjà que parmi ces coefficients, un au moins était non nul.

Finalement nous avons montré que dans les lignes $L_i(M_\zeta)$, pour $i \geq 1$, il y avait au moins $2(n-1)$ coefficients non nuls, et dans la ligne $L_0(M_\zeta)$ il y en avait au moins un coefficient non nul. Ceci nous permet d'établir la minoration de la densité de la base normale $\mathcal{B}$

$$d(\mathcal{B}) = \omega(M_\zeta) \geq 2(n-1) + 1 = 2n - 1.$$

□

Nous savons maintenant que toute base normale $\mathcal{B}(\zeta)$ a toujours une densité supérieure à $2n-1$. Nous recherchons les meilleures bases normales de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, nous devrions donc chercher celles qui vérifient $d(\mathcal{B}(\zeta)) = 2n - 1$. La classification de ces bases dites optimales est complète, c'est l'objet de la section suivante.

6.2 Base normale optimale

Définition 10. *Une base normale sera dite optimale si elle atteint le minimum théorique de densité, i.e., si $\mathcal{B}(\zeta)$ vérifie*

$$d(\mathcal{B}(\zeta)) = 2n - 1$$

La proposition suivante donne une première construction d'une base normale atteignant la borne minimale de densité.

Proposition 10 ([20])**.** *Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps fini tel que $n+1$ soit premier. Le corps $\mathbb{F}_{q^n}$ admet une base normale optimale sur $\mathbb{F}_q$ constituée des racines $(n+1)^{eme}$ de l'unité, distinctes de 1 si, et seulement si, q est un élément primitif dans $\mathbb{Z}/(n+1)\mathbb{Z}$*

Démonstration. Avant toute chose, puisque $n+1$ est premier, $(n+1)$ divise $q^n - 1$ et $\mathbb{F}_{q^n}$ contient donc une racine primitive $(n+1)^{\text{eme}}$ l'unité ζ.

On va montrer dans un premier temps l'assertion

Si q primitif alors ζ est normal et $\mathcal{B}(\zeta)$ est optimale.

Nous supposons donc q primitif dans $\mathbb{Z}/(n+1)\mathbb{Z}$. Montrons d'abord que le système $\mathcal{B}(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}})$ est une $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Comme q est primitif dans $\mathbb{Z}/(n+1)\mathbb{Z}$, tout entier $1 \leq j \leq n$ est égal à un q^i modulo $n+1$. Ceci implique que

$$\{\zeta^{q^i} \mid i = 0, \ldots, n-1\} = \{\zeta^j \mid j = 1, \ldots, n\}. \tag{38}$$

Donc pour montrer que $\mathcal{B}$ est une base, il suffit de montrer que le système $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$ est libre. Or cela revient en fait, à montrer que le polynôme minimal de ζ est de degré n. On sait que le polynôme minimal de ζ divise $\sum_{i=0}^{n} X^i$ et qu'il a n racines : les ζ^{q^i}. Il est donc obligatoirement de degré n.

Nous avons donc montré que ζ est un élément normal de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. L'étape suivante consiste donc à montrer que $\mathcal{B}(\zeta)$ est optimale, i.e., que $d(\mathcal{B}(\zeta)) = 2n - 1$. Pour cela nous allons compter les coefficients non nuls de M_ζ, car d'après le lemme 13 $d(\mathcal{B}(\zeta)) = \omega(M_\zeta)$. La colonne $C_i(M_\zeta)$ de M_ζ est constituée, par définition de M_ζ, des coefficients dans $\mathcal{B}(\zeta)$ de l'élément $\zeta\zeta^{q^i}$.

Il s'agit donc de compter pour chaque i le nombre de coefficients non nuls de $\zeta\zeta^{q^i}$ dans $\mathcal{B}(\zeta)$. Si $\zeta^{q^i} \neq \zeta^{-1}$, $\zeta\zeta^{q^i}$ est donc une racine $(n+1)^{\text{eme}}$ de l'unité distincte de 1 et elle est donc égale à un ζ^{q^j} pour un certain j. Si $\zeta^{q^i} = \zeta^{-1}$, alors dans ce cas

$$\zeta\zeta^{q^i} = -\sum_{j=1}^{n} \zeta^j = \sum_{l=0}^{n-1} (-1)\zeta^{q^l}.$$

Le nombre de coefficients non nuls de M_ζ est, finalement, égal à $n-1+n = 2n-1$. La base $\mathcal{B}(\zeta)$ est donc bien optimale.

Montrons maintenant la réciproque :

si la base $\mathcal{B}(\zeta)$ est optimale alors q est primitif dans $(\mathbb{Z}/(n+1)\mathbb{Z})^\times$.

Supposons que $\mathcal{B}(\zeta)$ soit une base normale optimale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ constituée des racines $(n+1)^{\text{eme}}$ de l'unité, distinctes de 1. Remarquons que

$$\#\{\zeta^{q^i}, i = 0, \ldots, n-1\} = \#\{q^i \mod (n+1), i = 0, \ldots, n-1\}.$$

Or $\mathcal{B}(\zeta)$ est une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, donc les éléments ζ^{q^i} pour $i = 0, \ldots, n-1$ sont tous distincts. On doit donc avoir $n = \#\{q^i \mod n+1, i = 0, \ldots, n-1\}$, autrement dit q est bien primitif dans $\mathbb{Z}/(n+1)\mathbb{Z})^\times$. □

La proposition précédente ne produit pas de base optimale dans $\mathbb{F}_{q^n}$ pour des n premiers sauf pour $n = 2$. En effet, si l'on se place dans les conditions de la proposition précédente, l'entier $n+1 \geq 3$ est un premier impair, donc n est pair ; n n'est alors premier que lorsque $n = 2$. Dans les extensions de $\mathbb{F}_2$, dans certains cas il est possible de construire un autre type de base optimale comme on va le voir dans la proposition suivante. La base est construite à partir, non plus d'une racine $(n+1)^{\text{eme}}$, mais d'une racine $(2n+1)^{\text{eme}}$ primitive de l'unité. Nous verrons dans la section 6.3 sur les bases gaussiennes, une généralisation de ce type de base.

Proposition 11 ([20])**.** *Si $2n+1$ est premier et si l'une des deux conditions suivantes est vérifiée*

1. *2 est primitif dans $\mathbb{Z}/(2n+1)\mathbb{Z}$*
2. *$2n+1$ est congru a 3 modulo 4 et 2 engendre les résidus quadratiques de $\mathbb{Z}/(2n+1)\mathbb{Z}$,*

alors il existe une $\mathbb{F}_2$-base normale optimale de $\mathbb{F}_{2^n}$.

Démonstration. Nous remarquons tout d'abord, du fait $(2n+1)$ soit premier, que $(2n+1)|2^{2n}-1$, et qu'il existe donc une racine primitive $(2n+1)^{\text{eme}}$ de l'unité γ dans $\mathbb{F}_{2^{2n}}$. Définissons l'élément

$$\zeta = \gamma + \gamma^{-1}.$$

C'est avec ce ζ que l'on va construire une $\mathbb{F}_2$-base de $\mathbb{F}_{2^n}$. Dans un premier temps on va montrer que $\zeta \in \mathbb{F}_{2^n}$, i.e., que $\zeta^{2^n} = \zeta$, ensuite on verra que $\mathcal{B}(\zeta) = (\zeta, \ldots, \zeta^{2^{n-1}})$ est une base de $\mathbb{F}_{2^n}$. Finalement on calculera $d(\mathcal{B}(\zeta))$ pour montrer qu'elle est optimale.

Montrons d'abord que $\zeta \in \mathbb{F}_{2^n}$, ce qui est équivalent à $\zeta^{2^n} = \zeta$. Comme $2^n = \pm 1 \mod (2n+1)$, alors on a soit $\gamma^{2^n} = \gamma^{-1}$ soit $\gamma^{2^n} = \gamma$. Finalement on obtient pour ζ^{2^n}

$$\zeta^{2^n} = (\gamma + \gamma^{-1})^{2^n} = \gamma^{2^n} + \gamma^{-2^n} = \gamma + \gamma^{-1} = \zeta,$$

et ζ est donc bien un élément de $\mathbb{F}_{2^n}$.

Maintenant montrons que $\mathcal{B}(\zeta) = (\zeta, \zeta^2, \ldots, \zeta^{2^{n-1}})$ est une $\mathbb{F}_2$-base de $\mathbb{F}_{2^n}$. Il suffit en fait de vérifier que $\mathcal{B}(\zeta)$ est un système libre. On va donc supposer que l'on a une relation entre les éléments de la base et montrer que cette relation est en fait triviale. Supposons donc que

$$\sum_{i=0}^{n-1} \alpha_i \zeta^{2^i} = 0,$$

et en remplaçant ζ^{2^i} par $\gamma^{2^i} + \gamma^{-2^i}$ on obtient

$$\sum_{i=0}^{n-1} \alpha_i (\gamma^{2^i} + \gamma^{-2^i}) = 0 \tag{39}$$

Maintenant, comme 2 est, par hypothèse, un générateur du groupe multiplicatif $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$, ou un générateur du sous-groupe des résidus quadratiques de $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ avec $2n+1 \equiv 3 \mod 4$, on a

$$\sum_{i=0}^{n-1} \alpha_i (\gamma^{2^i} + \gamma^{-2^i}) = \sum_{i=0}^{n-1} \alpha_i \gamma^{2^i} + \sum_{i=0}^{n-1} \alpha_i \gamma^{-2^i} = \sum_{j=1}^{2n} \beta_j \gamma^j$$

où chaque α_i apparaît deux fois dans $(\beta_1, \ldots, \beta_{2n})$. Après avoir divisé l'expression précédente par γ, on remarque que γ est racine du polynôme

$$f = \sum_{i=0}^{2n-1} \beta_{i+1} X^i.$$

Si Q_γ est le polynôme minimal de γ alors Q_γ divise f. On va devoir traiter différemment le cas où l'hypothèse 1 de la proposition est vérifiée, et le cas ou c'est l'hypothèse 2 qui est vérifiée.

Tout d'abord si l'on est dans la situation où l'hypothèse 1 de la proposition est vérifié, nous avons

$$Q_\gamma = 1 + X + X^2 + \ldots + X^{2n}.$$

Dans ce cas, vu que $Q_\gamma | f$ et que $\deg f < \deg Q_\gamma$, on a $f = 0$ et donc tous les α_i sont nuls.

Si c'est l'hypothèse 2 qui est vraie alors Q_γ est de degré n ainsi que le polynôme minimal $Q_{\gamma^{-1}}$ de γ^{-1} et

$$X^{2n+1} + 1 = (X+1) Q_\gamma Q_{\gamma^{-1}}.$$

Mais nous avons $Q_\gamma | f$ car $f(\gamma) = 0$, et $Q_{\gamma^{-1}} | f$ car $f(\gamma^{-1}) = 0$ par l'expression 39. Finalement nous $Q_\gamma Q_{\gamma^{-1}} = (1+X+X^2+\cdots+X^{2n}) | f$, ce qui implique encore que $f = 0$ puisque $\deg f \leq 2n-1$ et les α_i sont donc nuls.

Nous avons donc montré que $\mathcal{B}(\zeta)$ est une base normale de $\mathbb{F}_{2^n}$.

Nous devons, pour terminer la preuve de la proposition 11, montrer que $\mathcal{B}(\zeta)$ est optimale, i.e., que $d(\mathcal{B}(\zeta)) = 2n - 1$. Pour cela nous allons utiliser l'expression suivante de la densité de $\mathcal{B}(\zeta)$

$$d(\mathcal{B}(\zeta)) = \frac{1}{n} \sum_{i,j=0,\ldots,n-1} \omega(\zeta^{2^i} \zeta^{2^j}).$$

Les produits $\zeta^{2^i} \zeta^{2^j}$ s'exprime comme suit

$$\begin{aligned} \zeta^{2^i} \zeta^{2^j} &= (\gamma^{2^i} + \gamma^{-2^i})(\gamma^{2^j} + \gamma^{-2^j}) \\ &= (\gamma^{(2^i+2^j)} + \gamma^{-(2^i+2^j)}) + (\gamma^{(2^i-2^j)} + \gamma^{-(2^i-2^j)}). \end{aligned}$$

Si 2 est primitif modulo $(2n+1)$ alors chaque élément de $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ est égal à un 2^k mod $(2n+1)$ avec $0 \leq k \leq 2n-1$.

Si par contre 2 engendre uniquement le sous-groupe des résidus quadratiques de $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$, où $2n+1 = 3 \mod 4$, alors chaque élément de $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ est égal soit à un 2^k soit à un -2^k avec $0 \leq k \leq n-1$.

Si $2^i \not\equiv \pm 2^j \mod (2n+1)$, il existe k et k' tels que

$$2^i + 2^j = \pm 2^k \text{ et } 2^i - 2^j = \pm 2^{k'}$$

pour au moins un choix du + ou du − dans chaque cas, autrement dit

$$\zeta^{2^i}\zeta^{2^j} = \zeta^{2^k} + \zeta^{2^{k'}}.$$

Si par contre on a $2^i = \pm 2^j \mod (2n+1)$, alors un des $2^i \pm 2^j$ est nul modulo $2n+1$ et il existe un k tel qu'au moins une des équations suivante soient satisfaites

$$\begin{array}{ll} 2^i + 2^j = 2^k, & 2^i + 2^j = -2^k, \\ 2^i - 2^j = 2^k, & 2^i - 2^j = -2^k. \end{array}$$

Dans ce cas, comme on a un corps de caractéristique 2, on obtient

$$\zeta^{2^i}\zeta^{2^j} = \zeta^{2^k}.$$

Au vu de ces résultats, on sait que $\omega(\zeta^{2^i}\zeta^{2^j})$ est égal à 1 ou 2. On obtient alors

$$\begin{array}{rcl} d(\mathcal{B}(\zeta) & = & \frac{1}{n}\sum_{i,j=0,\ldots,n-1}\omega(\zeta^{2^i}\zeta^{2^j})) \\ & \leq & \frac{1}{n}(\sum_{i=0}^{n}\omega(\zeta^{2^i}\zeta^{2^i}) + \sum_{i,j=0,\ldots,n-1,i\neq j}\omega(\zeta^{2^i}\zeta^{2^j})) \\ & \leq & \frac{1}{n}(n + 2n(n-1)) \\ & \leq & 2n-1. \end{array}$$

Et donc finalement $d(\mathcal{B}(\zeta)) = 2n-1$.

□

Nous avons vu deux types de bases optimales, une construite en caractéristique quelconque à partir d'une racine $(n+1)^{\text{eme}}$ de l'unité, et l'autre à partir de racine $(2n+1)^{\text{eme}}$ valable uniquement dans des extensions de $\mathbb{F}_2$. Ce sont en fait les seules situations où il existe des bases normales optimales. Ce résultat a été montré par Gao et Lenstra dans [9].

Proposition 12 (Classification des ONB [9])**.** *Soit $\mathcal{B} = (\zeta, \zeta^2, \ldots, \zeta^{2^{n-1}})$ une base normale optimale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Soit $\alpha = Tr_{q^n|q}(\zeta)$. Alors l'une des deux possibilités suivante est vérifiée*

1. *$n+1$ est premier, q est primitif dans $(\mathbb{Z}/(n+1)\mathbb{Z})^\times$ et $-\zeta/\alpha$ est une racine primitive $(n+1)^{eme}$ de l'unité*
2. *(a) $q = 2^m$ pour un entier m tel que $pgcd(m,n) = 1$,*
   (b) $2n+1$ est premier, 2 et -1 engendre le groupe multiplicatif $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$,
   (c) $\zeta/\alpha = \gamma + \gamma^{-1}$ pour une certaine racine primitive $(2n+1)^{eme}$ de l'unité γ.

Nous pouvons finalement classer les bases normales optimales en deux types : un type qui correspond à la situation 1 de la proposition et un second type à la situation 2 de la proposition 12.

Définition 11. *Soient une extension de degré n de corps fini $\mathbb{F}_{q^n}/\mathbb{F}_q$, $\mathcal{B}(\zeta)$ une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ associée à ζ. On définit alors*

1. *Base normale optimale de type I (ONB I).*
   Un base $\mathcal{B}(\zeta)$ sera dite base normale optimale de type I si $n+1$ est premier, q est primitif dans $(\mathbb{Z}/(n+1)\mathbb{Z})^\times$ et si ζ est une racine primitive n^{eme} de l'unité.
2. *Base normale optimale de type II (ONB II).*
   La base $\mathcal{B}(\zeta)$ sera dite base normale optimale de type II si $q = 2^m$ tel que $pgcd(m, n) = 1$, l'entier $(2n+1)$ est premier, $\langle 2, -1\rangle = (\mathbb{Z}/(2n+1)\mathbb{Z})^\times$ et si il existe une racine primitive $(2n+1)^{eme}$ de l'unité $\gamma \in \mathbb{F}_{q^{2n}}$ telle que $\zeta = \alpha(\gamma + \gamma^{-1})$ avec $\alpha \in \mathbb{F}_q$.

En pratique c'est ce type de base qui sera le plus utilisé car elle donne la possibilité d'implanter la multiplication très efficacement du fait de leur faible densité, et de permettre une élévation à la puissance q très efficace. Nous expliciterons plus en détail dans les sections 7 et 8 les multiplieurs pour les corps $\mathbb{F}_{2^n}$ construits sur des bases normales optimales sur $\mathbb{F}_2$.

6.3 Base gaussienne

Il n'est pas toujours possible de trouver une ONB pour toute extension $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Cependant il est possible de construire des bases de faible densité mais pas forcément optimales. Dans cette optique Blake, Ash et Vanstone ont introduit dans [4] une nouvelle famille de bases normales : les bases gaussiennes. Elles sont, en fait, une généralisation des ONB de type I et II. Elles ont souvent une densité faible. Dans cette section nous reprenons une partie des résultats exposés par Gao, Gathen et Panario dans [8].

La proposition suivante explique comment construire une base gaussienne.

Proposition 13 (Base Gaussienne [4])**.** *Soit un entier k tel que $r = kn + 1$ soit premier et $pgcd(r, q) = 1$, et soit e l'ordre de q dans $(\mathbb{Z}/r\mathbb{Z})^\times$. Soit $\mathcal{K}$ l'unique sous-groupe de $(\mathbb{Z}/r\mathbb{Z})^\times$ d'ordre k. Soit γ une racine primitive k^{eme} de l'unité. Alors*

$$\zeta = \sum_{a \in \mathcal{K}} \gamma^a$$

est un élément normal de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ si et seulement si $pgcd(nk/e, n) = 1$.

Démonstration. Nous allons prouver cette proposition en deux étapes. Dans un premier temps nous allons simplement montrer que l'élément ζ est dans $\mathbb{F}_{q^n}$: nous vérifierons que $\zeta^{q^n} = \zeta$. Dans un second temps nous montrerons que le système $\mathcal{B}(\zeta) = (\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}})$ est un système libre. Ce qui suffira à prouver que ζ est un élément normal.

Montrons que $\zeta \in \mathbb{F}_{q^n}$. Commençons par remarquer que $\#((\mathbb{Z}/r\mathbb{Z})^\times/\mathcal{K}) = n$. Ceci signifie que pour tout élément $c \in (\mathbb{Z}/r\mathbb{Z})^\times$ nous avons $c^n \in \mathcal{K}$. Et c'est vrai, en particulier, lorsque $c = q$. En élevant ζ à la puissance q^n nous obtenons

$$\zeta^{q^n} = \sum_{a \in \mathcal{K}} \gamma^{q^n a} = \sum_{a \in \mathcal{K}} \gamma^a,$$

et donc $\zeta^{q^n} = \zeta$. Autrement dit, $\zeta \in \mathbb{F}_{q^n}$.

Montrons maintenant que, sous l'hypothèse $\text{pgcd}(nk/e, n) = 1$, l'élément ζ est normal. Pour montrer cela, nous aurons besoin du fait suivant : si deux sous-groupes d'un groupe cyclique sont d'indice i_1 et i_2, alors le sous-groupe engendré par la réunion de ces deux sous-groupes est d'indice $\text{pgcd}(i_1, i_2)$. Si l'on applique cette propriété aux sous-groupes $\mathcal{K}$ et $\langle q \rangle$ de $(\mathbb{Z}/r\mathbb{Z})^\times$ d'indice n et nk/e respectivement, nous obtenons que

$$\text{pgcd}(nk/e, n) = 1 \Longleftrightarrow (\mathbb{Z}/r\mathbb{Z})^\times = \langle q, \mathcal{K} \rangle$$

La condition $\text{pgcd}(nk/e, n) = 1$ est donc équivalente au fait que $(\mathbb{Z}/r\mathbb{Z})^\times = \langle q, \mathcal{K} \rangle$. Sous cette condition tout élément $c \in (\mathbb{Z}/r\mathbb{Z})^\times$ peut s'écrire comme $c = q^j a$ avec $a \in \mathcal{K}$.

Pour montrer que ζ est normal, il faut simplement montrer que le système $(\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}})$ est libre. Supposons que l'on ait une relation entre les ζ^{q^i} pour $i = 0, \ldots, n-1$

$$\sum_{i=0}^{n-1} \alpha_i \zeta^{q^i} = 0,$$

en remplaçant ζ par son expression en fonction de γ nous obtenons

$$\sum_{i=0}^{n-1} \sum_{a \in \mathcal{K}} \alpha_i \gamma^{[aq^i]} = 0, \tag{40}$$

où l'on a noté $[aq^i]$ le résidu modulo r de aq^i. Définissons le polynôme

$$f(X) = \sum_{i=0}^{n-1} \sum_{a \in \mathcal{K}} \alpha_i X^{[aq^i]}.$$

Nous allons montrer que γ^{aq^j} avec $a \in \mathcal{K}$ est racine du polynôme $f(X)$. D'abord avec (40) en évaluant $f(\gamma^{q^j})$ on montre que $f(\gamma^{q^j}) = f(\gamma)^{q^j} = 0$. Maintenant pour $\rho = \gamma^{q^j}$ et $a' \in \mathcal{K}$ nous avons

$$\begin{aligned} f(\rho^{a'}) &= \sum_{i=0}^{n-1} \alpha_i \sum_{a \in \mathcal{K}} \rho^{aa'q^i} \\ &= \sum_{i=0}^{n-1} \alpha_i \sum_{a \in \mathcal{K}} \rho^{aq^i} \\ &= f(\rho) = 0. \end{aligned}$$

Or comme $(\mathbb{Z}/r\mathbb{Z})^\times = \langle q, \mathcal{K} \rangle$, nous avons pour tout $c \in (\mathbb{Z}/r\mathbb{Z})^\times$, $f(\gamma^c) = 0$ et nous devons donc avoir

$$\sum_{m=0}^{kn} X^m = \prod_{m=1}^{kn} (X - \gamma^m) | f(X).$$

Mais comme $\deg f(X) \leq kn$, nous avons alors $f(X) = \beta(1 + X + X^2 + \cdots + X^{kn})$ avec $\beta \in \mathbb{F}_q$. Par définition f a au plus nk coefficients non nuls, donc forcément $\beta = 0$. On en conclut que ζ est un élément normal de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. □

L'objectif maintenant est d'établir une majoration de la densité d'une base gaussienne $\mathcal{B}(\zeta)$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ construite à partir d'un couple (n,k) vérifiant les conditions de la prosposition précédente. Nous noterons à partir de maintenant $\mathcal{K}_i$ le sous-ensemble suivant de $(\mathbb{Z}/r\mathbb{Z})^\times$

$$\mathcal{K}_i = \{aq^i : a \in \mathcal{K}\}.$$

En particulier nous avons $\mathcal{K}_0 = \mathcal{K}$ et $\mathcal{K}_i$ se déduit de $\mathcal{K}$ par

$$\mathcal{K}_i = \mathcal{K}_{i-1}q = \mathcal{K}q^i.$$

Soit $\zeta = \sum_{a\in\mathcal{K}} \gamma^a$, l'élément ζ^{q^i} peut s'exprimer en fonction de $\mathcal{K}_i$ comme suit

$$\zeta^{q^i} = \sum_{a\in\mathcal{K}} \gamma^{aq^i} = \sum_{a\in\mathcal{K}_i} \gamma^a.$$

Sous les hypothèses de la proposition 13 le système $(\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}})$ est la base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ engendrée par ζ .

Nous allons maintenant exprimer chaque produit $\zeta^{q^i}\zeta^{q^j}$ dans la base $\mathcal{B}(\zeta)$, nous en déduirons une majoration de la densité de la base normale $\mathcal{B}(\zeta)$.

Définissons d'abord pour $0 \le j, h \le n$ l'entier $c_{j,h}$ comme étant le nombre d'éléments $a \in \mathcal{K}_j$ tel que $1 + a \in \mathcal{K}_h$, i.e.,

$$c_{j,h} = \#(1 + \mathcal{K}_j) \cap \mathcal{K}_h. \tag{41}$$

Soit $j_0 < n$ l'unique entier tel que $-1 \in \mathcal{K}_{j_0}$. Si k est pair alors $j_0 = 0$, et si k est impair alors $j_0 = \frac{n}{2}$ ($nk+1$ étant premier, si k est impair, n est forcément pair). Enfin pour $0 \le j < n$ on définit

$$\delta_j = \begin{cases} 0 & \text{si} \quad j \neq j_0, \\ 1 & \text{si} \quad j = j_0. \end{cases}$$

Le lemme suivant va nous permettre d'exprimer les produit $\zeta^{q^i}\zeta^{q^j}$ dans $\mathcal{B}(\zeta)$.

Lemme 14 ([8])**.** *Soit le polynôme* $\Phi_r = \sum_{i=0}^{r-1} X^i$*. Pour* $0 \le i, j \le n$*, nous avons*

$$\left(\sum_{a\in\mathcal{K}} X^{aq^i}\right)\left(\sum_{a'\in\mathcal{K}} X^{a'q^j}\right) \equiv k\delta_{j-i} + \sum_{0\le h<n} c_{j-i,h}\left(\sum_{a\in\mathcal{K}} X^{aq^{i+h}}\right) \mod \Phi_r. \tag{42}$$

Démonstration. Avant toute chose, notons que $X^r \equiv 1 \mod \Phi_r$, et donc si $a \equiv a' \mod r$, $X^a \equiv X^{a'} \mod \Phi_r$. En utilisant ceci, on peut déjà obtenir l'expression suivante

$$\left(\sum_{a\in\mathcal{K}} X^{aq^i}\right)\left(\sum_{a'\in\mathcal{K}} X^{a'q^j}\right) \equiv \sum_{a,a'\in\mathcal{K}} X^{aq^i+a'q^j} \equiv \left(\sum_{a,a'\in\mathcal{K}} X^{a(1+a'q^{j-i})}\right)^{q^i} \mod \Phi_r.$$

Pour chaque $a' \in \mathcal{K}$ on a $1 + a'q^{j-i} \equiv 0 \mod r$, ou bien $1 + a'q^{j-i} \in \mathcal{K}_h$ pour un unique h tel que $0 \le h < n$. Si $1 + a'q^{j-i} \equiv 0 \mod r$ alors

$$\sum_{a\in\mathcal{K}} X^{a(1+a'q^{j-i})} \equiv k \mod \Phi_r,$$

et si $1 + a'q^{j-i} \in \mathcal{K}_h$, nous avons

$$\sum_{a\in\mathcal{K}} X^{a(1+a'q^{j-i})} \equiv \sum_{a\in\mathcal{K}} X^{aq^h} \mod \Phi_r.$$

Finalement en tenant compte du fait qu'il y a exactement $c_{(j-i),h} = \#(1 + \mathcal{K}_{j-i}) \cap \mathcal{K}_h$ élément $a' \in \mathcal{K}$ vérifiant $1 + a'q^{j-i} \in \mathcal{K}_h$, on obtient bien l'identité (42) du lemme. □

Comme γ est une racine de Φ_r, en remplaçant X par γ dans le lemme précédent, nous obtenons l'expression des produits $\zeta^{q^i}\zeta^{q^j}$ dans la base $\mathcal{B}(\zeta)$. De cette expression nous en déduisons la majoration suivante de la densité des bases gaussiennes.

Propriété 4 (Majoration de la densité des bases gaussiennes [8])**.** *Pour tout entier $0 \leq i, j < n$ nous avons*

$$\zeta^{q^i}\zeta^{q^j} = k\delta_{j-i} + \sum_{0\leq h<n} c_{j-i,h}\zeta^{q^{h+i}} = \sum_{0\leq h<n} (c_{j-i,h} - k\delta_{j-i})\zeta^{q^{h+i}}, \tag{43}$$

et en particulier

$$d(\mathcal{B}(\zeta)) \leq (k+1)n.$$

Démonstration. En remplaçant γ dans l'équation (42) du lemme 14 on obtient

$$\zeta^{q^i}\zeta^{q^j} = k\delta_{j-i} + \sum_{0\leq h<n} c_{j-i,h}\zeta^{q^{h+i}}. \tag{44}$$

Pour avoir l'expression de $\zeta^{q^i}\zeta^{q^j}$ dans la base $\mathcal{B}(\zeta)$ il faut écrire $k\delta_{j-i}$ dans la base $\mathcal{B}(\zeta)$. Nous savons que

$$\sum_{0\leq j\leq nk} \gamma^j = 0.$$

D'autre part tout élément $j \in (\mathbb{Z}/r\mathbb{Z})^\times$ peut s'écrire sous la forme $j = aq^i$ avec $a \in \mathcal{K}$. L'équation précédente peut alors s'arranger en

$$1 + \sum_{i=0}^{n-1}\sum_{a\in\mathcal{K}} \gamma^{aq^i} = 0,$$

et l'on arrive à

$$1 = \sum_{i=0}^{n-1}(-1)\sum_{a\in\mathcal{K}} \gamma^{aq^i} = \sum_{i=0}^{n-1}(-1)\zeta^{q^i}.$$

En multipliant par $k\delta_{j-i}$ nous obtenons l'expression de $k\delta_{j-i}$ dans $\mathcal{B}(\zeta)$) suivante

$$k\delta_{j-i} = \sum_{i=0}^{n-1}(-k\delta_{j-i})\zeta^{q^i}.$$

Enfin en remplaçant cette dernière expression dans l'équation (44) nous obtenons

$$\zeta^{q^i}\zeta^{q^j} = \sum_{0\leq h<n} (c_{j-i,h} - k\delta_{j-i})\zeta^{q^{h+i}}.$$

Montrons maintenant la majoration $d(\mathcal{B}(\zeta)) \leq (k+1)n$. Nous allons utiliser l'expression de $d(\mathcal{B}(\zeta))$ suivante

$$d(\mathcal{B}(\zeta)) = \frac{1}{n}\sum_{i,j=0}^{n-1} \omega(\zeta^{q^i}\zeta^{q^j}).$$

Montrons que $\omega(\zeta^{q^i}\zeta^{q^j}) \leq k$ pour tout i, j tel que $j - i \neq j_0$. D'abord comme $j - i \neq j_0$ nous avons $\delta_{j-i} = 0$. Ensuite comme $1 + \mathcal{K}_{j-i}$ a k éléments non nuls puisque $j - i \neq j_0$ nous devons avoir $\sum_{h=0}^{n-1} c_{j-i,h} \leq k$. Ce qui donne bien la majoration souhaitée

$$\omega(\zeta^{q^i}\zeta^{q^j}) \leq k.$$

Lorsque $j = i + j_0$ nous majorons grossièrement $\omega(\zeta^{q^i}\zeta^{q^j}) \leq n$.

Finalement nous obtenons la majoration de $d(\mathcal{B}(\zeta))$ suivante

$$\begin{aligned} d(\mathcal{B}(\zeta)) &= \frac{1}{n}\sum_{i,j=0}^{n-1} \omega(\zeta^{q^i}\zeta^{q^j}) \\ &= \frac{1}{n}\sum_{i=0}^{n-1} \omega(\zeta^{q^i}\zeta^{q^{i+j_0}}) + \sum_{i,j\in\{0,\ldots,n-1\},\ j-i\neq j_0 \mod n} \omega(\zeta^{q^i}\zeta^{q^j}) \\ &\leq \frac{1}{n}\left(\sum_{i=0}^{n-1} n + \sum_{i,j\in\{0,\ldots,n-1\},\ j-i\neq j_0 \mod n} k\right) \\ &\leq \frac{1}{n}\left(n^2 + kn^2\right) \\ &\leq n(k+1). \end{aligned}$$

Ce qui conclut la preuve de la proposition 4 . □

Pour des extensions de $\mathbb{F}_2$, Mulin et al. ont pu établir un encadrement de la complexité des bases gaussiennes dans [4]. Ils affinent le résultat précédent en montrant que les matrices M_s des bases gaussiennes sur $\mathbb{F}_2$ construites à partir d'un couple (n, k), ont en moyenne k éléments non nuls par colonne.

Proposition 14. *Soit $\mathbb{F}_{2^n}$ un corps fini de caractéristique 2, soit $\mathcal{B}(\zeta)$ la base normale sur $\mathbb{F}_2$ de type (n, k) construite dans proposition 13. Alors les bornes suivantes sur la densité de $\mathcal{B}(\zeta)$ sont vérifiées :*

$$\begin{aligned} kn - (k^2 - k + 1) \leq d(\mathcal{B}(\zeta)) \leq kn - 1, \quad &\textit{si } k \textit{ est pair,} \\ (k+1)n - (k^2 - k + 1) \leq d(\mathcal{B}(\zeta)) \leq (k+1)n - k \quad &\textit{si } k \textit{ est impair.} \end{aligned}$$

Remarque 6. Une construction plus générale des bases gaussiennes a été proposée par Gathen et al. dans [5]. Les bases gaussiennes sont construites à partir d'un couple (n, k) tels que $nk = \#(\mathbb{Z}/m\mathbb{Z})^\times$, l'entier m n'est plus supposé premier. Dans ce cas encore on a une majoration de la densité de la base comme l'a montré Gao dans [7].

La fin de ce chapitre est consacrée à expliciter les implantations de la multiplication dans $\mathbb{F}_{2^n}$ pour des bases normales optimales de type I et II.

7 Base normale optimale de type I

Cette section reprend un travail de Koc et Sunar dans [15]. Supposons que le corps $\mathbb{F}_{2^n}$ soit construit par un AOP, i.e., $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ avec

$$P = 1 + X + X^2 + \ldots + X^n.$$

Dans cette situation, comme nous l'avons vu dans la proposition 10, la base normale

$$\mathcal{B}_N = (X, X^2, X^4, \ldots, X^{2^{n-1}})$$

est optimale. Cependant, nous allons représenter les éléments de $\mathbb{F}_{2^n}$ suivant une base équivalente à $\mathcal{B}_N$, la base polynomiale shiftée $\mathcal{B}_{PS}$ qui est plus simple à manipuler.

Définition 12. *On définit par $\mathcal{B}_{PS} = (X, X^2, \ldots, X^n)$ la base polynomiale shiftée de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_2$.*

Voyons comment s'effectue le changement de base de $\mathcal{B}_N$ vers $\mathcal{B}_{PS}$. D'après la proposition 10 sur les bases normales de type I, 2 est un générateur du groupe $(\mathbb{Z}/(n+1)\mathbb{Z})^\times$. L'application $i \mapsto \sigma(i) = 2^i \mod (n+1)$ est donc une permutation de $\{1, \ldots, n\}$. En conséquence si on écrit

$$U = \sum_{i=1}^{n} u_i X^{2^i},$$

U s'écrit alors comme

$$U = \sum_{j=1}^{n} u_{\sigma^{-1}(j)} X^j,$$

et le changement de base pour passer de la base $\mathcal{B}_N$ à la base $\mathcal{B}_{PS}$ n'est qu'une permutation des coefficients u_i de U.

Rappelons que les matrices de structure M_s associées à $\mathcal{B}_{PS}$ ont $2n-1$ coefficients non nuls. La proposition ci-dessous décrit une décomposition des matrices de structure M_s en somme de deux matrices D et M'_s ayant respectivement n et $n-1$ entrées non nulles. Cette décomposition va nous permettre d'implantater la multiplication d'une façon peu coûteuse en matériel.

Proposition 15. *Soit $\mathbb{F}_{2^n}$ défini par un AOP et $\mathcal{B}_{PS} = (X, \ldots, X^{n-1})$ la base polynômiale shiftée associée. Dans ce cas, si l'on définit la matrice*

$$D = \begin{bmatrix} 0 & 0 & \ldots & 1 \\ \vdots & & \iddots & \vdots \\ 0 & 1 & & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix},$$

les matrices de structure M_s, pour $s \in \{1, \ldots, n\}$, associées à la base $\mathcal{B}_{PS}$ se décomposent en $M_s = D + M'_s$, et si on note $M'_s = [\lambda'_{i,j}(s)]_{i,j=1,\ldots,n}$, les coefficients $\lambda'_{i,j}(s)$ de M'_s sont donnés par

$$\lambda'_{i,j} = \begin{cases} 1 & \textit{si} \quad i + j = s \mod (n+1), \\ 0 & \textit{sinon.} \end{cases}$$

Démonstration. Les matrices de structure $M_s = [\lambda_{i,j}(s)]$ se construisent à partir de l'expression suivante des produits $X^i X^j$

$$X^i X^j = \sum_{s=1}^{n} \lambda_{i,j}(s) X^s.$$

Nous devons donc dans un premier temps exprimer les produits $X^i X^j$ dans la base $\mathcal{B}_{PS}$

$$X^i X^j = \begin{cases} X^{i+j} & \text{si} \quad i+j < n+1, \\ X^{i+j-(n+1)} & \text{si} \quad i+j > n+1, \\ \sum_{s=1}^{n} X^s & \text{si} \quad i+j = n+1. \end{cases}$$

Nous en déduisons que les coefficients $\lambda_{i,j}(s)$ de M_s sont donc non nuls lorsque

- i, j vérifient $i + j = s$ ou $i + j = s + (n + 1)$. Ces coefficients correspondent aux coefficients de M'_s non nuls,
- i, j vérifient $i+j = (n+1)$. Ils correspondent alors aux coefficients non nuls de D. Finalement nous avons donc établi la décomposition $M_s = M'_s + D$.

□

Nous pouvons exploiter cette propriété afin de réduire le coût matériel du multiplieur normal de $\mathbb{F}_{2^n}$. Le calcul des coordonnées w_s de $W = UV$ s'effectue habituellement par le produit matriciel suivant

$$w_s = ({}^tU) \cdot M_s \cdot V.$$

En utilisant la décomposition de M_s donnée dans la prosposition précédente nous obtenons

$${}^tU \cdot M_s \cdot V = ({}^tU) \cdot M'_s \cdot V + ({}^tU) \cdot D \cdot V$$

Le calcul des coordonnées w_s peut finalement se faire en calculant d'abord

$$w'_s = ({}^tU) \cdot M_s \cdot V \qquad \text{et} \qquad \alpha = ({}^tU) \cdot D \cdot V,$$

ensuite nous en déduisons $w_s = w'_s + \alpha$.

La proposition suivante explicite la forme de $({}^t)U \cdot M'_s$ et de $({}^t)U \cdot D \cdot V$.

Proposition 16 ([15]). *Soit $U = \sum_{i=1}^{n} u_i X^i$ et $V = \sum_{i=1}^{n} v_i X^s$, deux éléments de $\mathbb{F}_{2^n}$ exprimés dans la base polynômiale shiftée. Nous avons alors*

$${}^tUDV = \sum_{i=1}^{n} u_i v_{n+1-i}$$

et

$${}^tUM'_s = \begin{bmatrix} u_{s-1} & \dots & u_1 & 0 & u_n & \dots & u_{s+1} \end{bmatrix}$$

Exemple 13. On considère dans cet exemple le corps $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + 1)$. La base polynômiale shiftée est dans ce cas

$$\mathcal{B}_{PS} = (X, X^2, X^3, X^4).$$

Les matrices M_s associées à cette base sont

$$M'_1 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad M'_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$M'_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad M'_4 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

la matrice D vaut ici

$$D = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

et la matrice M_U est donnée par

$$M_U = \begin{bmatrix} 0 & u_4 & u_3 & u_2 \\ u_1 & 0 & u_4 & u_3 \\ u_2 & u_1 & 0 & u_4 \\ u_3 & u_2 & u_1 & 0 \end{bmatrix} + \begin{bmatrix} u_4 & u_3 & u_2 & u_1 \\ u_4 & u_3 & u_2 & u_1 \\ u_4 & u_3 & u_2 & u_1 \\ u_4 & u_3 & u_2 & u_1 \end{bmatrix}.$$

♢

En utilisant les expressions de $({}^tU) \cdot D \cdot V$ et $({}^tU) \cdot M'_s$ de la proposition précédente, nous obtenons l'algorithme ci-dessous qui prend en entrée deux éléments U et V représentés dans la base $\mathcal{B}_{PS}$, et retourne leur produit $W = UW$ dans $\mathcal{B}_{PS}$.

Algorithme 8 Multiplieur ONB I [15]

Entrée. $U = [u_0, \ldots, u_{n-1}], V = [v_0, \ldots, v_{n-1}]$,
Calcul des w'_s *et de* α
$\alpha \leftarrow \sum_{i=1}^{n} u_i v_{n+1-i}$
pour $s = 1, \ldots, n$ **faire**
$w'_s = \sum_{i=1}^{s-1} u_i v_{s-i} + \sum_{i=s+1}^{n} u_i v_{n+1+s-i}$

Sortie. $W \leftarrow [w'_1 + \alpha, w'_2 + \alpha, \ldots, w'_n + \alpha]$

Complexité. Pour le calcul de α il faut n AND et $(n-1)$ XOR . Ensuite pour le calcul de chaque w'_s il faut $(n-1)$ AND et $(n-2)$ XOR . Et l'addition finale nécessite n XOR .

Au total la complexité matérielle est de

$$n^2 \text{ AND et } (n^2 - 1) \text{ XOR }.$$

La complexité en temps est de

$$T_A + (1 + \lceil \log_2(n) \rceil) T_X.$$

Remarque 7. Ce type de multiplieur est une version légèrement modifiée de celui présenté par Hasan dans [13], à la différence près qu'ils ont utilisé une représentation en base normale, et non en base polynômiale shiftée, et qu'ils ont décomposé M_s en $D + M'_s$ avec D une matrice $n \times n$ telle que ${}^t(U^2)D(U^2) = {}^tUDV$. En fait la matrice D de Hasan, correspond à notre matrice D, mais après avoir permuté des éléments de la base $\mathcal{B}_{PS}$ avec σ.

8 Base normale optimale de type II

Dans cette section nous établissons un multiplieur pour les corps $\mathbb{F}_{2^n}$ dans une base normale optimale de type II. Différents travaux ont été publiés sur ce sujet [16, 21]. Nous présenterons le multiplieur décrit par Koc et Sunar [16] dans une version légèrement modifiée.

Soit $\mathbb{F}_{2^n}$ une extension de $\mathbb{F}_2$ de degré n tel que $2n+1$ soit premier, et tel que 2 soit primitif, ou engendre le sous-groupe des résidus quadratiques dans $(\mathbb{Z}/(2n+1)\mathbb{Z})^\times$. Soit γ une racine primitive $(2n+1)^{\text{eme}}$ de l'unité dans $\mathbb{F}_{2^{2n}}$ et $\zeta = \gamma + \gamma^{-1}$. Enfin soit $\mathcal{B}(\zeta) = (\zeta, \zeta^2, \ldots, \zeta^{2^{n-1}})$ la base normale de type II engendrée par ζ. De la même manière que dans le cas des ONB de type I, au lieu de représenter les éléments dans la base $\mathcal{B}_N$, on va les représenter suivant une base équivalente $\mathcal{B}_{PS}$ plus facile à manipuler.

Définition 13. *On définit $\mathcal{B}_{PS} = (\zeta_1, \ldots, \zeta_n)$ la base polynômiale shiftée associée à ζ telle que $\zeta_i = \gamma^i + \gamma^{-i}$ pour $i = 1, \ldots, n$.*

Voyons d'abord comment on passe d'une expression suivant $\mathcal{B}_N$ à une expression suivant $\mathcal{B}_{PS}$. Pour cela définissons la bijection σ qui à $i \in \{0, \ldots, n-1\}$ associe $\sigma(i) = \min(2^i \mod 2n+1, -2^i \mod 2n+1)$ dans $\{1, \ldots, n\}$, où les restes modulo $2n+1$ sont pris entre 0 et $2n$. A partir des coefficients de U dans $\mathcal{B}_N$

$$U = \sum_{i=0}^{n-1} u_i \zeta^{2^i}$$

et à la l'aide de l'application inverse de σ, on peut exprimer U dans la base polynômiale shiftée

$$U = \sum_{j=1}^{n} u_{\sigma^{-1}(j)} \zeta_j.$$

Maintenant nous allons voir comment multiplier deux éléments dans $\mathbb{F}_{2^n}$ dans la base $\mathcal{B}_{PS}$ de $\mathbb{F}_{2^n}$. Soit U, V deux éléments de $\mathbb{F}_{2^n}$

$$U = \sum_{i=1}^{n} u_i \zeta_i, \quad V = \sum_{i=1}^{n} v_i \zeta_i.$$

Nous allons exprimer les coefficients du produit $W = UV$ dans la base $\mathcal{B}_{PS}$. Pour cela nous développons le produit suivant et nous le scindons en deux sommes W_1 et W_2.

$$\begin{aligned} W &= \left(\sum_{i=1}^{n} u_i (\gamma^i + \gamma^{-i}) \right) \left(\sum_{j=1}^{n} v_j (\gamma^j + \gamma^{-j}) \right) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j (\gamma^{i-j} + \gamma^{-(i-j)}) + \sum_{i=1}^{n} \sum_{j=1}^{n} u_i v_j (\gamma^{i+j} + \gamma^{-(i+j)}) = W_1 + W_2 \end{aligned}$$

Nous commençons par arranger la somme W_1. Nous la scindons en deux sommes S_1 et S_2. Dans S_1 nous ne gardons que les termes tels que $i < j$. Dans S_2 nous ne gardons que les termes tels que $j < i$

$$W_1 = \underbrace{\sum_{i=1}^{n} \sum_{j=i+1}^{n} u_i v_j \zeta_{j-i}}_{S_1} + \underbrace{\sum_{j=1}^{n} \sum_{i=j+1}^{n} u_i v_j \zeta_{i-j}}_{S_2}.$$

Dans S_1 nous faisons le changement d'indice $s = j - i$ et $i = j - s$ et dans S_2 nous faisons le changement d'indice $s = i - j$ et $i = s + j$.

$$W_1 = \sum_{s=1}^{n-1} \sum_{j=s+1}^{n} u_{j-s} v_j \zeta_s + \sum_{s=1}^{n-1} \sum_{j=1}^{n-s} u_{j+s} v_j \zeta_s.$$

Finalement nous obtenons l'expression suivante de W_1 après avoir séparé la somme sur s selon

que $s+1 \leq n-s$ ou que $n-s < s+1$.

$$\begin{aligned} W_1 = &\sum_{s=1}^{\lfloor \frac{n-1}{2} \rfloor} \left(\sum_{j=1}^{s} u_{j+s}v_j + \sum_{j=s+1}^{n-s} (u_{j+s}+u_{j-s})v_j + \sum_{j=n-s+1}^{n} u_{j-s}v_j \right) \zeta_s \\ &+ \sum_{s=\lfloor \frac{n-1}{2} \rfloor+1}^{n} \left(\sum_{j=1}^{n-s} u_{j+s}v_j + \sum_{j=s+1}^{n} u_{j-s}v_j \right) \zeta_s. \end{aligned} \tag{45}$$

Occupons nous maintenant de $W_2 = \sum_{i,j=1}^{n} u_i v_j (\gamma^{i+j} + \gamma^{-(i+j)})$. Nous allons séparer W_2 en deux sommes, selon que $i+j \leq n$ et que $i+j > n$.

$$W_2 = \underbrace{\sum_{j=1}^{n-1} \sum_{i=1}^{n-j} u_i v_j (\gamma^{i+j} + \gamma^{-(i+j)})}_{S_1} + \underbrace{\sum_{i=1}^{n} \sum_{j=n-i+1}^{n} u_i v_j (\gamma^{i+j} + \gamma^{-(i+j)})}_{S_2},$$

en effectuant le changement d'indice $s = i+j$ et $i = s-j$ dans S_1 et en effectuant le changement d'indice $s = 2n+1-(i+j)$ et $i = 2n+1-(s+j)$ nous obtenons

$$W_2 = \sum_{s=1}^{n} \sum_{j=1}^{s-1} u_{s-j}v_j\zeta_s + \sum_{s=1}^{n} \sum_{j=n-s+1}^{n} u_{2n+1-(s+j)}v_j\zeta_s.$$

Finalement nous allons séparer l'expression précédente de W_2 en une somme sur s telle que $s-1 < n-s+1$ et une seconde somme suivant que $n-s+1 \leq s-1$

$$\begin{aligned} W_2 = &\sum_{s=1}^{\lceil \frac{n}{2} \rceil} \left(\sum_{j=1}^{s-1} u_{s-j}v_j + \sum_{j=n-s+1}^{n} u_{2n+1-s-j}v_j \right) \zeta_s \\ &+ \sum_{s=\lceil \frac{n}{2} \rceil+1}^{n} \left(\sum_{j=1}^{n-s} u_{s-j}v_j + \sum_{j=n-s+1}^{s-1} (u_{s-j}+u_{2n+1-s-j})v_j + \sum_{j=s}^{n} u_{2n+1-s-j}v_j \right) \zeta_s. \end{aligned} \tag{46}$$

Maintenant de l'expression de W_1 et W_2 ci-dessus, nous déduisons les coefficients w_s de W dans $\mathcal{B}_{PS}$ sous l'hypothèse n impair pour simplifier.

Lemme 15. *Si l'on suppose n impair, et si w_s est le coefficient d'indice s de W dans la base $\mathcal{B}_{PS}$, alors w_s s'exprime en fonction des coefficients u_i, v_i comme*

- *Pour $1 \leq s \leq \frac{n-1}{2}$*

$$\begin{aligned} w_s = &\sum_{j=1}^{s-1} (u_{j+s}+u_{s-j})v_j + u_{2s}v_s + \sum_{j=s+1}^{n-s} (u_{j+s}+u_{j-s})v_j \\ &+ \sum_{j=n-s+1}^{n} (u_{j-s}+u_{2n+1-s-j})v_j. \end{aligned}$$

- *Pour $s = \frac{n+1}{2}$*

$$w_s = \sum_{j=1}^{s-1} (u_{j+s}+u_{s-j})v_j + u_{2n+1-2s}v_s + \sum_{j=s+1}^{n} (u_{j-s}+u_{2n+1-s-j})v_j.$$

- *Pour* $\frac{n+1}{2}+1 \leq s \leq n$

$$w_s = \sum_{j=1}^{n-s}(u_{j+s}+u_{s-j})v_j + \sum_{j=n-s+1}^{s-1}(u_{s-j}+u_{2n+1-s-j})v_j$$
$$+ u_{2n+1-2s}v_s + \sum_{j=s+1}^{n}(u_{j-s}+u_{2n+1-s-j})v_j.$$

Exemple 14. Considérons le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/(X^3+X+1)$. Vérifions que ce corps vérifie bien les hypothèses de la proposition 11 sur les base normales de type II. D'abord nous voyons bien que $2\times 3+1=7$ est premier, ensuite nous vérifions que 2 engendre bien le sous-groupe des résidus quadratiques de $(\mathbb{Z}/7\mathbb{Z})^\times$ et que $7 \equiv 3 \mod 4$. L'élément $\gamma = X$ de $\mathbb{F}_{2^3}$ est une racine primitive 7^{eme} de l'unité et l'inverse de γ est égal à $X^6 = 1+X^2$. Nous pouvons donc construire la base $\mathcal{B}_{PS}$ associée à γ

$$\mathcal{B}_{PS} = (\zeta_1 = 1+X+X^2, \zeta_2 = X+1, \zeta_3 = 1+X^2).$$

Les produits des éléments de la base $\mathcal{B}_{PS}$ valent ici

$$\zeta_1\zeta_2 = \zeta_1+\zeta_3, \quad \zeta_1\zeta_3 = \zeta_2+\zeta_3, \quad \zeta_2\zeta_3 = \zeta_1+\zeta_2$$

et les matrices de structures M_s asscociées à $\mathcal{B}_{PS}$ sont

$$M_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Soit $U = u_1\zeta_1 + u_2\zeta_2 + u_3\zeta_3 \in \mathbb{F}_{2^3}$. Avec les matrices M_s, nous obtenons la matrice M_U en utilisant la formule 36

$$M_U = \begin{bmatrix} u_2 & u_1+u_3 & u_2+u_3 \\ u_1+u_3 & u_3 & u_1+u_2 \\ u_2+u_3 & u_1+u_2 & u_1 \end{bmatrix}.$$

Les coordonnées du produit de $W = UV$ sont données par le produit $W = M_U \cdot V$. Nous en déduisons que les w_s s'expriment bien comme le spécifiait le lemme 15

$$\begin{aligned} w_1 &= u_2v_1 + (u_1+u_3)v_2 + (u_2+u_3)v_3, \\ w_2 &= (u_1+u_3)v_1 + u_3v_2 + (u_1+u_2)v_3, \\ w_3 &= (u_2+u_3)v_1 + (u_1+u_2)v_2 + u_1v_3. \end{aligned}$$

♢

Nous allons pouvoir multiplier deux éléments $U, V \in \mathbb{F}_{2^n}$ avec les formules données dans le lemme 15. Dans un premier temps nous allons calculer les $\frac{n(n+1)}{2}$ éléments $\mu_{i,j} = u_i + u_j$. Nous en déduirons les coordonnées w_s de $W = UV$ en calculant les n produits scalaires donnés dans le lemme 15. Nous obtenons l'algorithme suivant, pour multiplier deux éléments U, V de $\mathbb{F}_{2^n}$ dans une une base shiftée, lorsque n est impair.

Algorithme 9 Multiplieur ONB II

Entrée. $U = [u_1, \ldots, u_n]$, $V = [u_1 \ldots u_n]$.

Etape 1. *Calcul des coefficients* $\mu_{i,j}$.

pour $i, j = 1, \ldots, n$ et $i \neq j$ **faire**

$\mu_{i,j} \leftarrow u_i + u_j$.

Etape 2. *Calcul des* w_s

pour $1 \leq s \leq \frac{n-1}{2}$ **faire**

$w_s \leftarrow \sum_{j=1}^{s-1} \mu_{j+s,s-j} v_j + u_{2s} v_s + \sum_{j=s+1}^{n-s} \mu_{j+s,j-s} v_j + \sum_{j=n-s+1}^{n} \mu_{j-s,2n+1-s-j} v_j$

pour $s = \frac{n+1}{2}$ **faire**

$w_s \leftarrow \sum_{j=1}^{s-1} \mu_{j+s,s-j} v_j + u_{2n+1-2s} v_s + \sum_{j=s+1}^{n} \mu_{j-s,2n+1-s-j} v_j$

pour $\frac{n+1}{2} < s \leq n$ **faire**

$w_s \leftarrow \sum_{j=1}^{n-s} \mu_{j+s,s-j} v_j + \sum_{j=n-s+1}^{s-1} \mu_{s-j,2n+1-s-j} v_j + u_{2n+1-2s} v_s + \sum_{s+1}^{n} \mu_{j-s,2n+1-s-j} v_j$

Sortie. $W \leftarrow [w_1, \ldots, w_k]$

Complexité. La première étape de l'algorithme consiste simplement en un calcul des $\mu_{i,j}$, ce qui nécessite $\frac{n(n-1)}{2}$ XOR . La seconde étape, consistant en n produits scalaires, a donc un coût matériel de n^2 AND et $n(n-1)$ XOR et un coût en temps de $T_A + (\lceil \log_2(n) \rceil) T_X$. On en déduit que le coût total matériel vaut

$$n^2 \text{ AND et } \frac{3}{2} n(n-1) \text{ XOR },$$

et que le coût en temps vaut

$$T_A + (1 + \lceil \log_2(n) \rceil) T_X.$$

Remarque 8. On peut comparer les bases normales de type I et de type II, elles ont toutes deux une même complexité en temps, mais le nombre de XOR nécessaire pour le type II est $1,5$ fois plus important que celui du I.

Base Duale

Dans ce chapitre nous allons établir quelques résultats concernant la double représentation d'un corps $\mathbb{F}_{q^n}$ avec deux $\mathbb{F}_q$-bases $\mathcal{B}$ et $\mathcal{B}'$ qui vérifient une relation de dualité. Cette relation de dualité permet de faire un lien entre les coordonnées d'un élément dans $\mathcal{B}$ et dans $\mathcal{B}'$. Lorsque $\mathcal{B}$ est une base polynômiale, ce lien entre les deux systèmes de coordonnées va nous permettre de construire assez simplement un multiplieur-dual dans $\mathbb{F}_{q^n}$, dans la proposition 19. Ce multiplieur prendra en entrée deux éléments $U, V \in \mathbb{F}_{q^n}$ avec U exprimé dans $\mathcal{B}$ et V dans $\mathcal{B}'$ et retournera $W = UV$ exprimé dans $\mathcal{B}'$.

Dans la première section de ce chapitre nous établissons quelques résultats généraux concernant les bases duales, ensuite nous appliquons ces résultats pour la construction de multiplieur dual de $\mathbb{F}_{2^n}$ associé à des bases polynômiales bien choisies. Nous introduirons la représentation circulaire duale lorsque le polynôme est un AOP, et nous construirons le multiplieur proposé par Lee et Lim dans [17]. Ensuite nous construirons le multiplieur dual associé à un trinôme (cf. [11]) ; pour finir avec le multiplieur dual associé à un pentanôme.

9 Généralités

Soient $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps finis de degré n et $\mathcal{B} = (e_1, \ldots, e_n)$ une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Considérons une forme $\mathbb{F}_q$-linéaire φ de $\mathbb{F}_{q^n}$. La forme φ est complètement déterminée par les n coefficients $\varphi(e_i) = \mu_i \in \mathbb{F}_q$. En effet pour $U = u_1e_1 + u_2e_2 + \cdots + u_ne_n \in \mathbb{F}_{q^n}$, nous avons

$$\varphi(U) = \mu_1u_1 + \cdots + \mu_nu_n.$$

Étant donnée une forme φ et une base $\mathcal{B}$ de $\mathbb{F}_{q^n}$, nous pouvons définir la notion base duale de $\mathcal{B}$ relativement à φ.

Définition 14 (Base duale[6])**.** *Soit φ une forme $\mathbb{F}_q$-linéaire de $\mathbb{F}_{q^n}$ non nulle. Deux bases $\mathcal{B} = (e_i)_{i=1,\ldots,n}$ et $\mathcal{B}' = (f_i)_{i=1,\ldots,n}$ de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ seront dites duales relativement à φ si elles vérifient*

$$\varphi(e_if_j) = \begin{cases} 1 & si\ i = j \\ 0 & si\ i \neq j \end{cases}$$

On dira que $\mathcal{B}$ est autoduale relativement à φ si $\mathcal{B}' = \mathcal{B}$

Remarque 9. A l'origine deux bases étaient dites duales si elles vérifiaient les conditions de la définition 14 pour la forme $\varphi = Tr_{q^n|q}$. C'est d'abord sous cette hypothèse que Berlekamp dans [2] a proposé un multiplieur dans les corps $\mathbb{F}_{2^n}$ utilisant des bases duales. Cette notion a été généralisée plus tard à une forme φ quelconque par Fenn, Benaissa et Taylor dans [6].

Exemple 15. Soient le corps $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(X^4+X^3+1)$ et sa base polynômiale $\mathcal{B} = (1, X, X^2, X^3)$ associée à X. Nous allons calculer la base duale de $\mathcal{B}$ relativement à la $\mathbb{F}_2$-forme $Tr_{2^4|2}$. Par définition nous avons pour $U \in \mathbb{F}_{2^4}$

$$Tr(U) = U + U^2 + U^4 + U^8.$$

Si l'on effectue le calcul de la trace pour $U = 1, X, X^2, X^3$ nous obtenons

$$\begin{array}{rclrcl} Tr(1) & = & 0, & Tr(X) & = & 1, \\ Tr(X^2) & = & 1, & Tr(X^3) & = & 1. \end{array}$$

Nous en déduisons par linéarité que $Tr(u_0 + u_1X + u_2X^2 + u_3X^3) = u_1 + u_2 + u_3$. Si on définit les éléments suivant de $\mathbb{F}_{2^4}$

$$\begin{array}{rclcrcl} e'_0 & = & 1+X, & & e'_1 & = & 1+X^2+X^3, \\ e'_2 & = & X+X^3, & & e'_3 & = & X+X^2, \end{array}$$

on peut vérifier que pour $i, j = 0, 1, 2, 3$

$$Tr(X^i e'_j) = \begin{cases} 0 & \text{si } i \neq j, \\ 1 & \text{si } i = j. \end{cases}$$

La base $\mathcal{B}' = (e'_0, e'_1, e'_2, e'_3)$ de $\mathbb{F}_{2^4}$ est donc la base duale de $\mathcal{B}$.

$\diamondsuit$

Fenn, Benaissa et Taylor dans [6] ont montré que pour une $\mathbb{F}_q$-forme quelconque $\varphi \neq 0$, toute base $\mathcal{B}$ admet une base duale $\mathcal{B}'$ relativement à φ.

Proposition 17. *Soit $\mathbb{F}_{q^n}/\mathbb{F}_q$ une extension de corps fini, et φ une $\mathbb{F}_q$-forme linéaire non nulle. Toute $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$ a une unique base duale relativement à φ.*

Pour toute forme φ, il est donc possible de construire la base duale de $\mathcal{B}$ relativement à φ. Le choix de φ est un composant essentiel pour la construction de la base duale, c'est en agissant sur φ que l'on peut essayer de trouver une ¡¡bonne¿¿ base duale de $\mathcal{B}$. C'est en partie pour cette raison que Fenn, Benaissa et Taylor dans [6] ont généralisé la notion de base duale en prenant une $\mathbb{F}_q$-forme φ arbitraire au lieu de la fonction $Tr(\cdot)$.

La proposition suivante donne une procédure pour passer d'une représentation en base $\mathcal{B}$ vers la représentation suivant sa base duale $\mathcal{B}'$.

Proposition 18 (Changement de base [2])**.** *Soient $(e_i)_{i=1,\ldots,n}$ et $(e'_i)_{i=1,\ldots,n}$ deux bases duales de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ relativement à une $\mathbb{F}_q$-forme φ, alors chaque élément $U \in \mathbb{F}_{q^n}$ peut être représenté dans la base $\mathcal{B}' = (e'_i)_{i=0,\ldots,n-1}$ de la façon suivante*

$$U = \sum_{i=1}^{n} \varphi(Ue_i)e'_i$$

Démonstration. Décomposons U dans (e'_j)

$$U = \sum_{j=1}^{n} u'_j e'_j$$

Ensuite nous remplaçons l'expression de U dans $\varphi(Ue_i)$ et nous développons

$$\begin{aligned} \varphi(Ue_i) &= \varphi(\sum_{j=1}^{n} u'_j e'_j e_i) \\ &= \sum_{j=1}^{n} u'_j \varphi(e_i e'_j) = u'_i, \end{aligned}$$

car $\varphi(e_i e'_i) = 1$ et $\varphi(e_i e'_j) = 0$ pour $i \neq j$. $\square$

Base duale d'une base polynômiale

Une famille de bases particulièrement intéressantes pour une double représentation base-base duale des corps $\mathbb{F}_{q^n}$ sont les bases polynômiales. Rappelons que la base polynômiale associée à un élément $\zeta \in \mathbb{F}_{2^n}$ est la base $(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$. A partir de maintenant nous nous intéresserons uniquement aux corps $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ où P est un polynôme irréductible. Nous allons étudier la double représentation de $\mathbb{F}_{q^n}$ suivant la base polynômiale $\mathcal{B} = (1, X, \ldots, X^{n-1})$ et sa base duale $\mathcal{B}'$ par rapport à une $\mathbb{F}_q$-forme φ.

Pour deux éléments U et V de $\mathbb{F}_{q^n}$, dont on connait la représentation de U suivant $\mathcal{B}$ nous pouvons calculer le produit de U et V dans $\mathbb{F}_{q^n}$ comme dans la proposition suivante.

Proposition 19 ([2])**.** *Soit $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ avec $P = \sum_{i=0}^{n-1} p_i X^i + X^n \in \mathbb{F}_q[X]$ un polynôme irréductible, $\mathcal{B} = (1, X, \ldots, X^{n-1})$ la base polynômiale associée à X, et φ une $\mathbb{F}_q$-forme sur $\mathbb{F}_{q^n}$. Soient $\mathcal{B}' = (e'_0, \ldots, e'_{n-1})$ la base duale de $\mathcal{B}$ relativement à φ, $U = u_0 + u_1 X + \cdots + u_{n-1}X^{n-1}, V \in \mathbb{F}_{q^n}$ et W tel que $W = UV$. Nous avons alors*

$$\begin{bmatrix} \varphi(V) & \varphi(VX) & \cdots & \varphi(VX^{n-1}) \\ \varphi(VX) & \varphi(VX^2) & \cdots & \varphi(VX^n) \\ \vdots & & & \vdots \\ \varphi(VX^{n-1}) & \varphi(VX^n) & \cdots & \varphi(VX^{2n-2}) \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix} = \begin{bmatrix} \varphi(W) \\ \varphi(WX) \\ \vdots \\ \varphi(WX^{n-1}) \end{bmatrix} \tag{47}$$

Démonstration. Nous allons calculer le produit de la j^{eme} ligne de la matrice $[\varphi(WX^{i+j})]_{i,j=0,\ldots,n-1}$ avec le vecteur colonne constitué des coefficients de V. Nous arrangerons l'expression obtenue pour faire apparaître $\varphi(WX^j)$

$$\begin{aligned} \begin{bmatrix} \varphi(VX^j) & \cdots & \varphi(VX^{j+n-1}) \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ \vdots \\ u_{n-1} \end{bmatrix} &= \sum_{i=0}^{n-1} u_i \varphi(VX^{j+i}) \\ &= \varphi(VX^j(\sum_{i=0}^{n-1} u_i X^i)) \\ &= \varphi(VUX^j) = \varphi(WX^j). \end{aligned}$$

La proposition en découle. □

Nous noterons souvent par la suite $v'_i = \varphi(VX^i)$ pour $i = 0, \ldots, 2n-2$ et $\widetilde{M_V} = [v'_{i+j}]_{i,j=0,\ldots,n-1}$. Avec ces notations, les coordonnées w'_i suivant $\mathcal{B}'$ de $W = UV$ sont données par

$$w'_i = L_i(\widetilde{M_V}) \cdot U = \sum_{j=0}^{n-1} v'_{i+j} u_j.$$

Remarque 10. Au vu de l'équation (47), nous remarquons que si nous connaissons les coefficients $v'_j = \varphi(VX^j)$ pour $j = 0, \ldots, 2n-1$ nous pouvons calculer les coordonnées de $W = UV$ dans la base duale de $\mathcal{B}$ via un produit matrice vecteur. Il reste donc deux points à préciser pour compléter la construction d'un multiplieur dual

- une méthode de calcul pour $v'_j = \varphi(VX^j)$ pour $j = n, \ldots, 2n-2$,

- une formule de changement de base entre $\mathcal{B}'$ et $\mathcal{B}$ pour pouvoir à partir des coordonnées de U dans la base $\mathcal{B}'$ trouver les coordonnées de U dans $\mathcal{B}$.

Pour le second point, il n'y a pour le moment, à notre connaissance, aucune réponse générale. Il semble que dans certain cas, si le φ est bien choisi, la base duale de $\mathcal{B}$ est une base permutée de $\mathcal{B}$, et donc le changement de base revient à effectuer une permutation des coefficients de U.

Par contre pour le premier point nous avons le résultat suivant qui donne une méthode pour calculer les v'_j pour $j \geq n$ récursivement à partir de $v'_0, \ldots, v'_{n-1}$.

Proposition 20 ([2])**.** *Soient $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P)$ avec $P = \sum_{i=0}^{n-1} p_i X^i + X^n \in \mathbb{F}_q[X]$ un polynôme irréductible, $\mathcal{B} = (1, X, \ldots, X^{n-1})$ la base polynômiale associée à X, et φ une $\mathbb{F}_q$-forme sur $\mathbb{F}_{q^n}$. Soient $\mathcal{B}' = (e'_0, \ldots, e'_{n-1})$ la base duale de $\mathcal{B}$ relativement à φ, et $V = \sum_{i=0}^{n-1} v'_i e'_i \in \mathbb{F}_{q^n}$. Nous avons alors pour $j \leq n-1$*

$$\varphi(VX^j) = v'_j$$

et pour $j = n + j'$ avec $0 \leq j' \leq n-1$ nous avons la relation suivante

$$v'_{n+j'} = \varphi(VX^{n+j'}) = -\sum_{i=0}^{n-1} p_i \varphi(VX^{i+j'}) = -\sum_{i=0}^{n-1} p_i v'_{i+j'} \tag{48}$$

Exemple 16. Soit $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(X^4 + X^3 + 1)$ et $\mathcal{B} = (1, X, X^2, X^3)$ sa base polynômiale associée à X . On a vu dans l'exemple 15 que la base duale de $\mathcal{B}$ relativement à la $\mathbb{F}_2$-forme $Tr_{2^4|2}$ est donnée par

$$\begin{array}{rclcrcl} e'_0 & = & 1+X, & & e'_1 & = & 1+X^2+X^3, \\ e'_2 & = & X+X^3, & & e'_3 & = & X+X^2. \end{array}$$

Soit $V = v'_0 e'_0 + v'_1 e'_1 + v'_2 e'_2 + v'_3 e'_3$. Nous pouvons calculer les coefficients v'_i pour $i = 4, 5, 6$ de la matrice $\widetilde{M_V}$ récursivement avec l'équation (48) :

$$v'_4 = v'_0 + v'_3, \quad v'_5 = v'_1 + v'_4, \quad v'_6 = v'_2 + v'_5.$$

Finalement, soit $U = u_0 + u_1 X + u_2 X^2 + u_3 X^3 \in \mathbb{F}_{2^4}$ et $W = UV = w'_0 e'_0 + w'_1 e'_1 + w'_2 e'_2 + w'_3 e'_3$. Avec l'équation (47) nous pouvons exprimer les w'_i en fonction des u_i et des v'_i

$$\begin{bmatrix} w'_0 \\ w'_1 \\ w'_2 \\ w'_3 \end{bmatrix} = \begin{bmatrix} v'_0 & v'_1 & v'_2 & v'_3 \\ v'_1 & v'_2 & v'_3 & v'_4 \\ v'_2 & v'_3 & v'_4 & v'_5 \\ v'_3 & v'_4 & v'_5 & v'_6 \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \end{bmatrix}.$$

♢

Démonstatrion de la proposition 20. L'égalité pour $\varphi(VX^j)$ avec $j \leq n-1$ à déjà été montrée lors de la proposition 18 sur le changement de bases. Nous avons donc juste à démontrer l'identité suivante

$$\varphi(VX^{n+j'}) = -\sum_{i=0}^{n-1} p_i \varphi(VX^{j'+i}).$$

De l'identité $\sum_{i=0}^{n-1} p_i X^i + X^n = 0$ donnée par le polynôme constructeur P de $\mathbb{F}_{q^n}$, nous obtenons

$$\begin{aligned} X^{n+j'} = X^n X^{j'} &= (-\sum_{i=0}^{n-1} p_i X^i) X^{j'} \\ &= -\sum_{i=0}^{n-1} p_i X^{i+j'}. \end{aligned}$$

En multipliant cette identité par V et en appliquant ensuite φ nous obtenons

$$\begin{aligned} \varphi(V X^{n+j'}) &= \varphi\left(V(-\sum_{i=0}^{n-1} p_i X^{i+j'}) \right) \\ &= -\sum_{i=0}^{n-1} p_i \varphi(V X^{i+j'}), \end{aligned}$$

et nous avons bien l'égalité recherchée. □

Les relations entre les v'_i de la proposition 20 permettent de calculer récursivement les v'_i pour $i = n, \ldots, 2n-2$. Ceci permet d'implanter un multiplieur en série de $\mathbb{F}_{q^n}$.

Algorithme 10 Multiplieur dual en série [2]

Entrée. $U = \left[\begin{array}{ccc} u_0 & \cdots & u_{n-1} \end{array} \right]$, $V = \left[\begin{array}{ccc} v'_0 & \cdots & v'_{n-1} \end{array} \right]$ et $P = \sum_{i=0}^{n-1} p_i + X^n$.
pour $i = 0$ à $n-1$ **faire**
$w'_i \leftarrow u_0 v'_i + u_1 v'_{i+1} \ldots + u_{n-1} v'_{i+n-1}$.
$v'_{i+n} \leftarrow -\sum_{j=0}^{n-1} p_i v'_{i+j}$
Sortie. $W \leftarrow \left[\begin{array}{ccc} w'_0 & \cdots & w'_{n-1} \end{array} \right]$.

Dans l'algorithme précédent, les v'_i et les w'_i sont calculés en série en exploitant l'expression des v'_i donnée par la proposition 20. Un problème se pose si l'on veut calculer les w'_i en parallèle, car alors, il faudrait pouvoir calculer aussi les v'_i en parallèle. Ceci est possible lorsque le polynôme P définissant $\mathbb{F}_{q^n}$ est creux, car alors la formule de récurrence donnant les v'_i est particulièrement simple. Dans le cas de la caractéristique 2, nous étudierons le cas où P est un trinôme dans la section 11, et dans la section 12 nous étudierons le cas où P est un pentanôme.

Nous allons voir d'abord que lorsque P est un AOP, on peut s'arranger pour construire un multiplieur dual en parallèle très efficace.

10 Base duale et AOP

Soit $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où $P = \sum_{i=0}^{n} X^i$ est un AOP. Dans cette section nous présentons un travail effectué par Lee et Lim dans [17] sur la base duale de $(1, X, \ldots, X^{n-1})$ relativement à la fonction trace $Tr(\cdot)$.

La propriété suivante décrit la base duale, relativement à la fonction trace de la base polynômiale de $\mathbb{F}_2[X]/(P)$ où P est un AOP.

Propriété 5 (Base duale AOP [17]). *Soit le corps $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où le polynôme $P = \sum_{i=0}^{n} X^i \in \mathbb{F}_2[X]$ est un AOP irréductible. Soit $\mathcal{B} = (1, X, X^2, \ldots, X^{n-1})$ la base polynomiale de $\mathbb{F}_{2^n}$ associée à X. La base duale de $\mathcal{B}$ relativement à la fonction trace $Tr(\cdot)$ est donnée par*

$$e_i = X + X^{-i} = X + X^{n+1-i} \quad \textit{pour } i = 0, \ldots, n-1$$

Autrement dit les e_i sont donnés par

$$\begin{aligned} e_0 &= 1 + X, \\ e_1 &= 1 + \sum_{i=2}^{n-1} X^i, \\ e_j &= X^{n+1-j} + X, \qquad \textit{pour } 2 \leq j \leq n-1 \end{aligned}$$

Pour la preuve de la propriété précédente nous aurons besoin du résultat suivant, qui donne la trace des éléments X^i pour $0 \leq i \leq 2n-2$ de $\mathbb{F}_{2^n}$.

Lemme 16. *Sous les mêmes conditions que dans la propriété 5, on a pour $i \in \{0, \ldots, 2n-2\}$*

$$Tr(X^i) = \begin{cases} 0 & \textit{si } i = 0 \textit{ ou } i = n+1 \\ 1 & \textit{sinon} \end{cases} \tag{49}$$

Démonstration. Soit $U = u_0 + u_1 X + u_2 X^2 + \ldots + u_{n-1} X^{n-1} \in \mathbb{F}_{2^n}$, et soit M_U la matrice de la multiplication par U dans la base $\mathcal{B}$. Rappelons (cf. 2) que $Tr(U) = Tr(M_U)$, i.e., $Tr(U)$ est égal à la somme des termes diagonaux de M_U. Or M_U, la matrice de l'application ϕ_U de multiplication par U, est donnée par

$$M_U = \begin{bmatrix} u_0 & 0 & u_{n-1} & \cdots & u_2 \\ u_1 & u_0 & 0 & \cdots & u_3 \\ \vdots & & & & \vdots \\ u_{n-2} & u_{n-3} & \cdots & \cdots & 0 \\ u_{n-1} & u_{n-2} & u_{n-3} & \cdots & u_0 \end{bmatrix} + \begin{bmatrix} 0 & u_{n-1} & u_{n-2} & \ldots & u_1 \\ 0 & u_{n-1} & u_{n-2} & \ldots & u_1 \\ \vdots & & & & \vdots \\ \vdots & & & & \vdots \\ 0 & u_{n-1} & u_{n-2} & \ldots & u_1 \end{bmatrix}.$$

Nous obtenons donc

$$Tr(U) = n u_0 + \sum_{i=1}^{n-1} u_i.$$

Or, du fait que $P = \sum_{i=0}^{n} X^i$ soit irréductible, n doit être pair. Donc l'expression de la trace de U devient

$$Tr(U) = \sum_{i=1}^{n-1} u_i. \tag{50}$$

Pour obtenir (49) lorsque $i \leq n-1$, il suffit juste d'appliquer la formule ci-dessus à $U = X^i$

$$\begin{aligned} Tr(1) &= 0, \\ Tr(X^i) &= 1 \quad \text{pour } \; i = 1, \ldots, n-1. \end{aligned}$$

Pour $i = n, \ldots, 2n-2$ nous devons d'abord réduire X^i modulo P pour pouvoir appliquer la formule (50). Pour $i = n$, nous avons $X^n = \sum_{j=0}^{n-1} X^j$, ce qui donne

$$Tr(X^n) = \sum_{j=0}^{n-1} Tr(X^j) = \sum_{j=1}^{n-1} 1 = 1 \quad \text{(car n est pair)}$$

Pour $i = n+1$, nous avons $X^{n+1} = 1$ et donc $Tr(X^{n+1}) = Tr(1) = 0$.

Pour $n+2 \leq i \leq 2n-2$, nous avons $X^i = X^{i-(n+1)}$ et donc, comme $1 \leq i-(n+1) \leq n-1$, nous avons $Tr(X^i) = 1$. □

Revenons maintenant à la preuve de la propriété 5.

Démonstration de la propriété 5. Nous allons utiliser le lemme précédent pour le calcul de $Tr(X^i e_j)$. D'abord calculons $Tr(1e_i)$

$$\begin{aligned}
Tr(1e_0) &= Tr(1+X) = Tr(1) + Tr(X) = 1, \\
Tr(1e_1) &= Tr(1 + \sum_{i=2}^{n-1} X^i) = \sum_{i=2}^{n-1} 1 = 0, \\
Tr(1e_j) &= Tr(X^{n+1-j} + X) = 1 + 1 = 0 \quad \text{pour } 1 < j \leq n-1.
\end{aligned}$$

Faisons la même chose pour $Tr(Xe_i)$

$$\begin{aligned}
Tr(Xe_0) &= Tr(X + X^2) = 0, \\
Tr(Xe_1) &= Tr(X + \sum_{i=2}^{n-1} X^{i+1}) = 1 + \sum_{i=2}^{n-1} 1 = 1, \\
Tr(Xe_j) &= Tr(X^{n+1-j+1} + X^2) = 1 + 1 = 0 \quad \text{pour } 1 < j \leq n-1.
\end{aligned}$$

De la même manière nous vérifions que $Tr(X^i e_0) = Tr(X^i e_1) = 0$ pour $1 < i \leq n-1$.

Pour finir calculons $Tr(X^i e_j)$ avec $1 < i, j < n$

$$Tr(X^i e_j) = Tr(X^{n+1-j+i} + X^{i+1}) = Tr(X^{n+1-j+i}) + 1.$$

Si $i < j$, alors $0 \leq n+1-j+i < n+1$, et si $i > j$ on a $2n-2 \geq n+1-j+i > n+1$. D'après le lemme 16 nous avons dans ces deux cas

$$Tr(X^{n+1-j+i}) = 1,$$

et donc

$$Tr(X^i e_j) = 0.$$

Si $i = j$ alors $Tr(X^{n+1-j+i}) = Tr(X^{n+1}) = 0$ et donc $Tr(X^i e_j) = 1$. □

Nous déduisons de la proposition 18 le lemme suivant, qui décrit comment on calcule les coefficients d'un éléments $U \in \mathbb{F}_{2^n}$ dans la base $\mathcal{B}$ à partir des coefficients de U dans $\mathcal{B}'$.

Lemme 17 (Changement de base I [17]). *Soit* $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ *où* $P = \sum_{i=0}^{n} X^i$, $\mathcal{B} = (1, X, X^2, \ldots, X^{n-1})$ *la base polynômiale de* $\mathbb{F}_{2^n}$ *associée à* X, *et* $\mathcal{B}' = (e_i)_{i=0,\ldots,n-1}$ *la base duale de* $\mathcal{B}$ *associée à* $Tr(\cdot)$. *Pour* $U = \sum_{i=0}^{n-1} u'_i e_i$ *nous obtenons les coordonnées* u_i *dans* $\mathcal{B}$ *en effectuant le produit matriciel suivant*

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_{n-2} \\ u_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & \ldots & 1 & 0 & 0 \\ \vdots & & & & \ddots & \vdots & \vdots & \\ 0 & 1 & 0 & 1 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & \ldots & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} u'_0 \\ u'_1 \\ u'_2 \\ u'_4 \\ \vdots \\ u'_{n-2} \\ u'_{n-1} \end{bmatrix} \tag{51}$$

Lorsqu'on calcule les coordonnées u_i de U dans $\mathcal{B}$ à partir des coordonnées de U dans $\mathcal{B}'$, nous obtenons, pour le calcul de u_i pour $i \neq 1$, qu'une seule addition est nécessaire, mais pour u_1 nous avons

$$u_1 = u'_0 + \sum_{i=2}^{n-1} u'_i,$$

et donc $n-2$ additions sont nécessaires. Dans [17], Lee et Lim ont proposé d'ajouter un coefficient supplémentaire à la représentation dans la base $\mathcal{B}'$. Ce coefficient que noterons $\theta(U)$ est défini par

$$\theta(U) = \sum_{i=0}^{n-1} u'_i.$$

Nous verrons que le fait de rajouter ce coefficients permet d'une part d'améliorer l'efficacité du changement de base, mais d'autre part, comme on le verra plus loin d'améliorer aussi l'efficacité du multiplieur dual.

Définition 15 (Représentation circulaire duale). *Soit* $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ *où* $P = \sum_{i=0}^{n} X^i$, $\mathcal{B} = (1, \ldots, X^{n-1})$ *et* $\mathcal{B}' = (e_0, \ldots, e_{n-1})$ *la base duale donnée dans la proposition 5 relativement à la fonction* $Tr(\cdot)$. *La représentation de* $U \in \mathbb{F}_{2^n}$ *en représentation circulaire duale est un* $(n+1)$*-uplet* $(u'_0, \ldots, u'_{n-1}, \theta(U))$ *où les* u'_i *sont les coefficients de* U *dans* $\mathcal{B}'$ *et* $\theta(U) = \sum_{i=0}^{n-1} u'_i$.

Dans cette nouvelle représentation l'addition se fera simplement en additionnant coefficient à coefficient. En effet soit $U, V \in \mathbb{F}_{2^n}$ et $(u'_0, \ldots, u'_{n-1}, \theta(U))$, $(v'_0, \ldots, v'_{n-1}, \theta(V))$ leur représentation circulaire duale respective et $W = U + V$ dans $\mathbb{F}_{q^n}$. Les coefficients w'_i de W dans la base duale de $(1, X, \ldots, X^{n-1})$ sont donnés par $w'_i = u'_i + v'_i$, car

$$W = U + V = \sum_{i=0}^{n-1} (u'_i + v'_i) e_i.$$

Montrons que le coefficient redondant $\theta(W)$ se calcule de manière similaire, i.e., vérifions que $\theta(W) = \theta(U) + \theta(V)$. Par définissions de $\theta(W)$ nous avons

$$\theta(W) = \sum_{i=0}^{n-1} w'_i,$$

en remplaçant les w'_i par leur expressions en fonction des u'_i et v'_i nous obtenons

$$\begin{aligned}\theta(W) &= \textstyle\sum_{i=0}^{n-1}(u'_i + v'_i) \\ &= (\textstyle\sum_{i=0}^{n-1} u'_i) + (\sum_{i=0}^{n-1} v'_i) \\ &= \theta(U) + \theta(V).\end{aligned}$$

La proposition suivante donne le changement de base de $\mathcal{B}'$ vers $\mathcal{B}$, mais en utilisant cette fois la représentation circulaire duale dans $\mathcal{B}'$.

Lemme 18 (Changement de base II [17])**.** *Sous les mêmes conditions que dans le lemme 17. Les coordonnées u_i de U dans la base polynômiale s'obtiennent à partir de la représentation circulaire duale de $U = (u'_0, u'_1, \ldots, u'_{n-1}, \theta(U))$ comme*

$$\begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & & & & \iddots & & & \vdots \\ 0 & 1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} u'_0 \\ \vdots \\ u'_{n-1} \\ \theta(U) \end{bmatrix}. \tag{52}$$

On notera dans la suite de cette section D la matrice $(n+1) \times (n+1)$ de la partie droite de l'égalité.

On voit bien que le calcul de u_1 est nettement plus simple car $u_1 = \theta(U) + u'_1$.

Exemple 17. Soit $\mathbb{F}_{2^4} = \mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ et $\mathcal{B} = (1, X, X^2, X^3, X^4)$ sa base polynômiale. La proposition 5 nous donne la base duale de $\mathcal{B}$

$$\begin{aligned} e_0 &= 1 + X, & e_1 &= 1 + X^2 + X^3, \\ e_2 &= X + X^3, & e_3 &= X + X^2. \end{aligned}$$

Soit $U = u'_0 e_0 + u'_1 e_1 + u'_2 e_2 + u'_3 e_3$, nous pouvons calculer les coefficients de U dans la base $\mathcal{B}$ en remplaçant les e'_i par leur expression en fonction des X^i

$$\begin{aligned} U &= u'_0(1+X) + u'_1(1+X^2+X^3) + u'_2(X+X^3) + u'_3(X+X^2) \\ &= (u'_0 + u'_1) + (u'_0 + u'_2 + u'_3)X + (u'_1 + u'_3)X^2 + (u'_1 + u'_2)X^3. \end{aligned}$$

Si l'on note $\theta(U) = u'_0 + u'_1 + u'_2 + u'_3$, l'équation précédente devient

$$U = (u'_0 + u'_1) + (\theta(U) + u'_1)X + (u'_1 + u'_3)X^2 + (u'_1 + u'_2)X^3.$$

♢

Nous voyons donc que si nous utilisons une représentation circulaire duale, le changement de base est nettement moins coûteux en temps puisque dans ce cas une seule addition est nécessaire pour le calcul de chaque coefficient u_i . Nous allons voir que l'on peut aussi tirer parti de la représentation circulaire pour la multiplication dans $\mathbb{F}_{2^n}$. Lee et Lim dans [17] ont montré la proposition suivante permettant d'effectuer le produit de deux éléments dans une représentation circulaire duale.

Proposition 21 (Multiplication duale pour AOP [17])**.** *Soient* $U, V, W \in \mathbb{F}_2[X]/(P)$ *où* $P = \sum_{i=0}^{n} X^i$ *et* $W = U\,V$*. Soient*

$$\begin{aligned} U &= u'_0 e_0 + \cdots + u'_{n-1} e_{n-1}, \\ V &= v'_0 e_0 + \cdots + v'_{n-1} e_{n-1}, \\ W &= w'_0 e_0 + \cdots + w'_{n-1} e_{n-1}, \end{aligned}$$

leur expression dans $\mathcal{B}'$ *la base duale de* $(1, X, \ldots, X^{n-1})$ *relativement à* $Tr(\cdot)$*. Les coordonnées circulaires duales de* W *s'expriment alors en fonction de celle de* U *et* V *comme suit*

$$\begin{bmatrix} w'_0 \\ w'_1 \\ w'_2 \\ \vdots \\ w'_{n-1} \\ \theta(W) \end{bmatrix} = \begin{bmatrix} v'_0 & \theta(V) & v'_{n-1} & \cdots & v'_2 & v'_1 \\ v'_1 & v'_0 & \theta(V) & \cdots & v'_3 & v'_2 \\ v'_2 & v'_1 & v'_0 & \cdots & v'_4 & v'_3 \\ \vdots & & & & & \vdots \\ v'_{n-1} & v'_{n-2} & v'_{n-3} & \cdots & v'_0 & \theta(V) \\ \theta(V) & v'_{n-1} & v'_{n-2} & \cdots & v'_1 & v'_0 \end{bmatrix} \cdot \begin{bmatrix} u'_0 \\ u'_1 \\ u'_2 \\ \vdots \\ u'_{n-1} \\ \theta(U) \end{bmatrix}. \tag{53}$$

Démonstration. Afin d'établir l'expression (53), nous allons arranger l'expression (47) suivante

$$\begin{bmatrix} \varphi(W) \\ \varphi(WX) \\ \vdots \\ \varphi(WX^{n-1}) \end{bmatrix} = \begin{bmatrix} \varphi(V) & \varphi(VX) & \varphi(VX^2) & \cdots & \varphi(VX^{n-1}) \\ \varphi(VX) & \varphi(VX^2) & \varphi(VX^3) & \cdots & \varphi(VX^n) \\ \vdots & & & & \vdots \\ \varphi(VX^{n-1}) & \varphi(VX^n) & \varphi(VX^{n+1}) & \cdots & \varphi(VX^{2n-2}) \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix}$$

où les u_i sont les coordonnées de U dans $(1, X, \ldots, X^n)$. Dans un premier temps calculons les coefficients de $\widetilde{M_V}$. Nous avons d'abord

$$\begin{aligned} Tr(VX^i) &= v'_i \quad \text{pour } i = 0, \ldots n-1, \\ Tr(VX^n) &= Tr(V \sum_{i=0}^{n-1} X^i) = \sum_{i=0}^{n-1} v'_i = \theta(V), \end{aligned}$$

Ensuite, du fait que $X^{n+1+i} = X^i$ pour $i = 0, \ldots, n-1$, nous obtenons

$$Tr(VX^i) = v'_{i-(n+1)} \quad \text{pour } \; i = n+1, \ldots, 2n-2$$

De ces résultats, nous pouvons arranger l'équation (47), la dernière ligne s'obtenant en sommant les n premières

$$\begin{bmatrix} w'_0 \\ w'_1 \\ \vdots \\ w'_{n-1} \\ \theta(W) \end{bmatrix} = \begin{bmatrix} v'_0 & v'_1 & \cdots & v'_{n-1} & \theta(V) \\ v'_1 & v'_2 & \cdots & \theta(V) & v'_0 \\ \vdots & & & & \vdots \\ v'_{n-1} & \theta(V) & \cdots & v'_{n-3} & v'_{n-2} \\ \theta(V) & v'_0 & \cdots & v'_{n-2} & v'_{n-1} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \\ 0 \end{bmatrix} \tag{54}$$

Finalement nous remplaçons $\begin{bmatrix} u_0 \\ \vdots \\ u_{n-1} \\ 0 \end{bmatrix}$ par son expression donné dans l'identité (52) et nous obtenons le résultat recherché. □

D'après la proposition précédente pour multiplier deux éléments U, V de $\mathbb{F}_{2^n}$ donnés dans une représentation circulaire duale, nous devons effectuer le produit matrice vecteur (53). Nous pouvons donc implanter la multiplication dans la base duale $(e_i)_{i=0,\ldots,n-1}$ comme ci-dessous.

Algorithme 11 Multiplieur dual pour AOP [17]

Entrée. $U = (u'_0, \ldots, u'_{n-1}, \theta(U))$ et $V = (v'_1, \ldots, v'_{n-1}, \theta(V))$ en représentation circulaire duale.
pour $i = 0, \ldots, n-1$ **faire**
$w'_i \leftarrow u_0 v'_i + u_1 v'_{i-1} + \ldots + u_i v'_0 + u_{i+1}\theta(V) + u_{i+2} v'_{n-1} + \ldots + u_{n-1} v'_{i+2} + \theta(U) v'_{i+1}$
$\theta(W) \leftarrow u'_0\theta(V) + u'_1 v'_{n-1} + \ldots + u'_{n-1} v'_1 + \theta(U) u'_0$
Sortie. $W \leftarrow (w'_0, \ldots, w'_{n-1}, \theta(W))$

Complexité. Le coût de l'algorithme est le coût d'un produit matrice vecteur, i.e., le produit matriciel de l'équation (53). Le coût matériel est alors de $(n+1)^2$ AND et $(n+1)n$ XOR , et le coût en temps de $T_A + (\lceil \log_2(n+1) \rceil) T_X$.

En conclusion, nous voyons que le coût en temps de ce multiplieur dual est meilleur qu'avec un multiplieur en base normale de type I (cf. algorithme 8 du chapitre 5.2.2) qui a un coût de $T_A + (1 + \lceil \log_2(n) \rceil) T_X$. Le coût matériel du multiplieur dual pour un AOP est par contre légèrement supérieur au multiplieur en ONB I : le multiplieur ONB I a un coût en espace valant

$$n^2 \text{ AND et } (n^2 - 1) \text{ XOR} .$$

D'autre part, si l'on compare le multiplieur dual avec un multiplieur dans la base polynômiale de $\mathcal{A} = \mathbb{F}_2[X]/(X^{n+1} + 1)$ (cf. section sur les equirépartis 4.4), le coût en temps et en espace est le même.

11 Base duale et trinôme

Cette section reprend en partie un travail de Wu, Hasan et Blake dans [11]. Comme nous l'avons déjà noté, le multiplieur dual décrit dans la proposition 19 est d'autant plus efficace que le polynôme générateur P est creux. En effet, comme nous allons le voir dans la proposition qui suit, le fait que P soit un trinôme va nous permettre de calculer les v'_i plus simplement.

Proposition 22 ([11])**.** *Soient $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ avec $P = X^n + X^k + 1$ et $2 \leq k \leq \frac{n}{2}$. Soient $\mathcal{B} = (1, X, \ldots, X^{n-1})$ et $\mathcal{B}' = (e_0, e_1, \ldots, e_{n-1})$ sa base duale relativement à une $\mathbb{F}_2$-forme φ. Soit $V = \sum_{i=0}^{n-1} v'_i e_i$ nous avons alors*

$$\varphi(VX^j) = \begin{cases} v'_j & \text{pour} \quad j = 0, \ldots, n-1 \\ v'_{j-(n-k)} + v'_{j-n} & \text{pour} \quad j = n, \ldots, 2n-k-1 \\ v'_{j-2(n-k)} + v'_{j-2n+k} + v'_{j-n} & \text{pour} \quad j = 2n-k, \ldots, 2n-2 \end{cases} \tag{55}$$

Nous voyons donc que chaque v'_j pour $j \geq n$ peut se calculer en fonction des coordonnées v'_i de V dans la base duale de $(1, X, \ldots, X^{n-1})$ en effectuant, au plus, deux additions.

Exemple 18. Soient $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$ et une $\mathbb{F}_2$-forme φ quelconque de $\mathbb{F}_{2^5}$. Soit $\mathcal{B} = (1, X, X^2, X^3, X^4)$ la base polynômiale de $\mathbb{F}_{2^5}$ et $\mathcal{B}' = (e'_0, e'_1, e'_2, e'_3, e'_4)$ sa base duale relativement à φ.

Soit un élément $V = \sum_{i=0}^{4} v'_i e'_i$ de $\mathbb{F}_{2^5}$. On peut calculer les v'_5, v'_6, v'_7, v'_8 en terme des v'_i pour $i \leq 4$ en réduisant X^j modulo $X^5 + X^2 + 1$ et en développant le produit VX^j dans $\varphi(VX^j)$

$$\begin{aligned}
v'_5 &= \varphi(VX^5) = \varphi(V(X^2+1)) = \varphi(VX^2) + \varphi(V) = v'_2 + v'_0, \\
v'_6 &= \varphi(VX^6) = \varphi(V(X^3+X)) = v'_3 + v'_1, \\
v'_7 &= \varphi(VX^7) = \varphi(V(X^4+X^2)) = v'_4 + v'_2, \\
v'_8 &= \varphi(VX^8) = \varphi(V(X^2+1+X^3)) = v'_2 + v'_0 + v'_3.
\end{aligned}$$

♢

Démonstration. L'expression de $\varphi(VX^j)$ pour $j = 0, \ldots, n-1$ a déjà été vue dans la proposition 18 sur le changement de base. Pour $\varphi(VX^j)$ avec $j \geq n$, nous allons dans un premier temps réduire X^j modulo P. Ensuite en remplaçant X^j par son expression réduite dans $\varphi(VX^j)$ nous en déduirons les expressions souhaitées. Pour $j = n, \ldots, 2n-k-1$, du fait que

$$X^n \equiv X^k + 1 \mod P,$$

nous avons

$$X^j = X^{j-n}X^n = X^{j-n}(X^k+1) = X^{j-(n-k)} + X^{j-n}.$$

Si l'on remplace X^j par l'expression ci-dessus dans $\varphi(VX^j)$ nous obtenons

$$\begin{aligned}
\varphi(VX^j) &= \varphi(V(X^{j-(n-k)} + X^{j-n})) \\
&= \varphi(VX^{j-(n-k)}) + \varphi(VX^{j-n}) \\
&= v'_{j-(n-k)} + v'_{j-n}.
\end{aligned}$$

De même l'expression de $\varphi(VX^j)$ pour $j = 2n-k, \ldots, 2n-2$ s'obtient en remarquant que $X^j \equiv X^{j-2(n-k)} + X^{j-(2n-k)} + X^{j-n} \mod P$ et en remplaçant X^j par cette expression dans $\varphi(VX^j)$. □

Maintenant que nous avons des formules pour calculer tous les v'_i, nous pouvons implanter un multiplieur dual dans $\mathbb{F}_2[X]/(X^n + X^k + 1)$. Ce multiplieur calcule dans un premier temps les coefficients v'_i pour $i = n, \ldots, 2n-2$ de la matrice $\widetilde{M}_V$ en utilisant les formules établies dans la proposition 22 précédente. Dans un second temps on calcule les coordonnées de $W = UV$ dans la base duale en effectuant le produit matriciel

$$W = \widetilde{M}_V \cdot U \qquad \text{où } \widetilde{M}_V = [v'_{i+j}]_{i,j=0,\ldots,n-1}.$$

Nous pouvons maintenant établir l'algorithme suivant, pour multiplier deux éléments dans $\mathbb{F}_{2^n}$. Il prend en entrée deux éléments U, V de $\mathbb{F}_2[X]/(X^n + X^k + 1)$, où U est donné par ses coefficients dans la base polynômiale $\mathcal{B} = (1, X, \ldots, X^{n-1})$, $U = \sum_{i=0}^{n-1} u_i X^i$ et $V = \sum_{i=0}^{n-1} v'_i e_i$ par ses coefficients dans la base duale. L'algorithme renvoie le produit $W = UV$ dans $\mathbb{F}_{2^n}$ donné par ses coefficients dans la base duale $W = \sum_{i=0}^{n-1} w'_i e_i$.

Algorithme 12 Multiplieur dual trinomial [11]

Entrée. $U = \left[\begin{array}{ccc} u_0 & \cdots & u_{n-1} \end{array}\right]$ et $V = \left[\begin{array}{ccc} v'_0 & \cdots & v'_{n-1} \end{array}\right]$

Etape 1. *Calcul en parallèle des coefficients de* $\widetilde{M_V}$

pour $i = n, \ldots, 2n-k-1$ **faire**

$v'_i \leftarrow v'_{i-(n-k)} + v'_{i-n}$

pour $i = 2n-k, \ldots, 2n-2$ **faire**

$v'_i \leftarrow v'_{i-2(n-k)} + v'_{i-(2n-k)} + v'_{i-n}$

Etape 2. *Calcul en parallèle des coefficients* w'_i

pour $i = 0, \ldots n-1$ **faire**

$w'_i \leftarrow \sum_{j=0}^{n-1} u_j v'_{i+j}$

Sortie. $W \leftarrow \left[\begin{array}{ccc} w'_1 & \cdots & w'_{n-1} \end{array}\right]$

Complexité. Dans la première étape, $(n-1)$ XOR sont nécessaires pour le calcul des v'_i pour $i = n, \ldots, 2n-2$. La complexité temporelle de cette étape est de $2T_X$. Le calcul des w'_i dans la seconde étape requiert lui n^2 AND et $n(n-1)$ XOR pour une complexité en temps de $T_A + \lceil \log_2(n) \rceil T_X$. Ce qui donne une complexité matérielle totale de

$$n^2 \text{ AND et } (n+1)(n-1) \text{ XOR},$$

et une complexité en temps de

$$T_A + (\lceil \log_2(n) \rceil + 2) T_X.$$

Remarque 11. Le multiplieur ci-dessus est incomplet car on souhaiterait avoir tous les éléments en entrée et en sortie écrits dans la même base. Ceci nécessiterait donc que l'on spécifie la forme $\mathbb{F}_2$-linéaire φ, et donc la base duale $(e'_i)_{i=0,\ldots,n-1}$ de la base polynômiale. Ceci afin de pouvoir passer de la représentation dans la base $\mathcal{B}'$ à une représentation dans la base $\mathcal{B}$.

12 Base duale pour pentanôme

Nous allons dans cette section construire un multiplieur dual pour les corps $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où P est un pentanôme. Nous allons utiliser le résultat donné dans la proposition 19 : pour calculer le produit de deux éléments $U, V \in \mathbb{F}_{2^n}$ nous effectuerons les produits matriciels

$$W = \widetilde{M_V} \cdot U,$$

où la matrice $\widetilde{M_V}$ est définie par

$$\widetilde{M_V} = [\phi(VX^{i+j}]_{i,j=0,\ldots,n-1}.$$

Le principal problème que nous devons traiter, c'est de trouver une méthode pour calculer les coefficients $\phi(VX^{i+j})$ de $\widetilde{M_V}$. Dans cette optique, nous allons exploiter une partie des résultats obtenus dans le chapitre 2.3 sur les bases polynômiales. Nous avions étudié les bases polynômiales des corps $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ définis par un pentanôme $P \in \mathbb{F}_2[X]$ tel que $P = 1 + X + X^m + X^{m+1} + X^n$ avec $2 \leq m \leq \lfloor \frac{n}{2} \rfloor - 1$.

Soit $\mathcal{B} = (1, X, \ldots, X^{n-1})$ la base polynômiale de $\mathbb{F}_{2^n}$ associée à X, φ une forme $\mathbb{F}_2$-linéaire, et $\mathcal{B}' = (e_0, \ldots, e_{n-1})$ la base duale de $\mathcal{B}$ associée à φ.

Dans le chapitre 2.3 nous avons montré le lemme 8 suivant qui donne les formules de réduction modulo P des monômes X^i pour $i = n, \ldots, 2n-2$.

Lemme 19 ([22]). *Soit $P = 1+X+X^m+X^{m+1}+X^n$ un pentanôme de $\mathbb{F}_2[X]$ avec $2 \leq m \leq \lfloor \frac{n}{2} \rfloor$. On a alors les identités suivantes*

- *Pour $i = n, n+1, \ldots, 2n-m-2$*

$$X^i = X^{(i-n)} + X^{(i-n)+1} + X^{(i-n)+m} + X^{m+1+(i-n)} \mod P.$$

- *Pour $i = 2n-m-1$*

$$X^i = X^{(i-n)} + X^{(i-n)+1} + X^{(i-n)+m} + 1 + X + X^m + X^{m+1} \mod P.$$

- *Pour $i = 2n-m, \ldots, n-2$*

$$X^i = X^{(i-n)} + X^{(i-n)+1} + X^{i-2n+m} + X^{i-2n+2m} + X^{i-2n+2m+2} + X^{i-2n+m+2} \mod P.$$

A partir des formules donnant X^j modulo P pour $j \geq n$, nous allons pouvoir exprimer $v'_j = \varphi(VX^j)$ pour $j \geq n$, en fonction des coordonnées v'_i suivant $\mathcal{B}'$. C'est l'objet de la proposition suivante.

Proposition 23. *Soit $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ avec $P = 1+X+X^m+X^{m+1}+X^n$ et $2 \leq m \leq \lfloor \frac{n}{2} \rfloor - 1$. Soit $V = \sum_{i=0}^{n-1} v'_i e'_i$ où $(e_i)_{i=1,\ldots,n}$ est la base duale de $(1, X, \ldots, X^{n-1})$ relativement à une forme $\mathbb{F}_2$-linéaire φ. Nous avons alors*

- *Pour $i = n, n+1, \ldots, 2n-m-2$*

$$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{(i-n)+m} + v'_{m+1+(i-n)}.$$

- *Pour $i = 2n-m-1$*

$$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{(i-n)+m} + v'_0 + v'_1 + v'_m + v'_{m+1}.$$

- *Pour $i = 2n-m, \ldots, n-2$*

$$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{i-2n+m} + v'_{i-2n+2m} + v'_{i-2n+2m+2} + v'_{i-2n+m+2}.$$

Démonstration. Pour le calcul de $v'_i = \varphi(X^i)$ nous utilisons l'expression de X^i donnée dans le lemme 19, le résultat cherché s'en déduit en développant le produit et en remplaçant $\varphi(X^j)$ par v'_j.

Nous le montrons uniquement pour $i = n, n+1, \ldots, 2n-m-2$, la méthode étant la même pour les autres cas. Nous remplaçons donc X^i par $X^{(i-n)} + X^{(i-n)+1} + X^{(i-n)+m} + X^{m+1+(i-n)}$ dans $\varphi(VX^i)$ et nous développons

$$v'_i = \varphi(VX^i) = \varphi(VX^{(i-n)}) + \varphi(VX^{(i-n)+1}) + \varphi(VX^{(i-n)+m}) + \varphi(VX^{m+1+(i-n)}).$$

A présent en remplaçant $\varphi(VX^j)$ par v'_j nous obtenons

$$v'_i = v'_{i-n} + v'_{(i-n)+1} + v'_{(i-n)+m} + v'_{m+1+(i-n)},$$

ce que nous voulions. □

Exemple 19. Dans cet exemple le corps fini sera $\mathbb{F}_{2^7} = \mathbb{F}_2[X]/(P)$ où $P = X^7+X^3+X^2+X+1$, $\mathcal{B}$ la base polynômiale de $\mathbb{F}_{2^7}$ et $\mathcal{B}' = (e'_i)_{i=0,\ldots,6}$ la base duale de $\mathcal{B}$ par rapport à une $\mathbb{F}_2$-forme quelconque de $\mathbb{F}_{2^7}$. D'abord on peut vérifier les formules de réduction données par le lemme 19

$$\begin{array}{rclrcl} X^7 &=& X^3+X^2+X+1, & X^8 &=& X^4+X^3+X^2+X, \\ X^9 &=& X^5+X^4+X^3+X^2, & X^{10} &=& X^6+X^5+X^4+X^3, \\ X^{11} &=& X^6+X^5+X^4+X^3+X^2+X+1, & X^{12} &=& X^6+X^5+X^4+1. \end{array}$$

Ensuite nous obtenons les expressions suivantes de $\varphi(VX^i)$ pour $V \in \mathbb{F}_{2^7}$ et $i \geq 7$ en terme des coefficients v'_i de V dans $\mathcal{B}'$

$$\begin{array}{rclrcl} v'_7 &=& v'_3+v'_2+v'_1+v'_0, & v'_8 &=& v'_4+v'_3+v'_2+v'_1, \\ v'_9 &=& v'_5+v'_4+v'_3+v'_2, & v'_{10} &=& u'_6+v'_5+v'_4+v'_3, \\ v'_{11} &=& v'_6+v'_5+v'_4+v'_3+v'_2+v'_1+v'_0, & v'_{12} &=& v'_6+v'_5+v'_4+v'_0. \end{array}$$

♢

Nous pouvons maintenant construire un multiplieur dans $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ où $P = 1+X+X^m+X^{m+1}+X^n$. Dans un premier temps, avec les formules établies dans la proposition 23, nous calculons les coefficients v'_{i+j} de la matrice $\widetilde{M_V} = [v'_{i,j}]$ à partir des coordonnées de V dans $\mathcal{B}'$. Ensuite, d'après la proposition 23 nous pouvons calculer les coordonnées dans $\mathcal{B}'$ de W le produit de U et V dans $\mathbb{F}_{2^n}$, en effectuant le produit matriciel

$$W = \widetilde{M_V} \cdot U.$$

L'algorithme suivant prend en entrée un élément U exprimé dans la base polynômiale de $\mathbb{F}_{2^n}$ et V dans $\mathcal{B}'$ et calcule les coordonnées de W dans $\mathcal{B}'$ selon cette méthode.

Algorithme 13 Multiplieur dual pour pentanôme

Entrée. $U = \left[\begin{array}{ccc} u_0 & \cdots & u_{n-1} \end{array}\right]$ et $V = \left[\begin{array}{ccc} v'_0 & \cdots & v'_{n-1} \end{array}\right]$.

Etape 1. *Calcul des* v'_i *pour* $i = n, \ldots, 2n-1$.

pour $i = n, n+1, \ldots, 2n-m-2$ **faire**

$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{(i-n)+m} + v'_{m+1+(i-n)}$

pour $i = 2n-m-1$ **faire**

$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{(i-n)+m} + v'_0 + v'_1 + v'_m + v'_{m+1}$

pour $i = 2n-m, \ldots, 2n-2$ **faire**

$v'_i = v'_{(i-n)} + v'_{(i-n)+1} + v'_{i-2n+m} + v'_{i-2n+2m} + v'_{i-2n+2m+2} + v'_{i-2n+m+2}$

Etape 2. *Calcul des* w'_i *en parallèle.*

pour $i = 0, \ldots, n-1$ **faire**

$w'_i = \sum_{j=0}^{n} u_j v'_{i+j}$

Sortie. $W = [w'_0 \ \cdots \ w'_{n-1}]$.

Complexité. Nous allons d'abord calculer séparément la complexité de l'étape 1 et 2 de l'algorithme .

Dans l'étape 1 les v'_i sont calculés en parallèle et chacun d'eux avec un arbre d'additions. La complexité matérielle pour le calcul des v'_i pour $i = n, \ldots, 2n-m-2$, est alors de $3(n-m-$

1) XOR . Pour le calcul de v'_{2n-m+1} nous avons besoin de 6 XOR et de $5(m-1)$ XOR pour les v'_i tels que $i = 2n-m, \ldots, 2n-2$. D'où un total de $(3n+2m+10)$ XOR pour la première étape. Cette étape s'effectue dans un délai de $3T_X$.

La seconde étape consiste en un produit matrice-vecteur. La complexité matérielle de cette étape est donc de n^2 AND et $n(n-1)$ XOR et la complexité en temps de $T_A + \lceil \log_2(n) \rceil T_X$.

La complexité matérielle totale de l'algorithme vaut finalement

$$n^2 \text{ AND et } (n(n+2)+2m+10) \text{ XOR },$$

et la complexité en temps vaut

$$T_A + (3 + \lceil \log_2(n) \rceil) T_X.$$

Remarque 12. Notons encore ici que le choix de la représentation n'est pas fixé : le choix pour φ et donc pour $\mathcal{B}'$ reste libre. Ce choix se fera parmi les bases telles que le changement de représentation de la base duale vers la base polynômiale soit le moins coûteux possible. D'autre part, Koc et Rodriguez dans [22] ont introduit un nouveau type de pentanôme, qui permet de construire un multiplieur aussi efficace que celui de l'algorithme 13, mais dont les coefficients $\varphi(VX^i)$ sont calculés à partir des coefficients de V dans la base polynômiale.

Pour conclure ce chapitre, nous allons voir, dans l'exemple suivant, que deux choix de différentes $\mathbb{F}_2$-forme φ' et φ'' influent dans la phase d'écriture de U dans la base polynômiale de $\mathbb{F}_{2^n}$, mais n'influe pas dans la multiplication faite suivant la méthode de l'algorithme 13.

Exemple 20. Dans cet exemple le corps fini sera $\mathbb{F}_{2^7} = \mathbb{F}_2[X]/(P)$ où $P = X^7+X^3+X^2+X+1$ et $\mathcal{B} = (1, X, X^2, X^3, X^4, X^5, X^6)$ la base polynômiale de $\mathbb{F}_{2^7}$. Considérons les deux bases duales $\mathcal{B}', \mathcal{B}''$ associées, respectivement, aux deux $\mathbb{F}_2$-formes φ' et φ'' définies par

$$\begin{array}{rcl} \varphi'(\sum_{i=0}^{6} u_i X^i) & = & u_0+u_1+u_2+u_3+u_4+u_5, \\ \varphi''(\sum_{i=0}^{6} u_i X^i) & = & u_0. \end{array}$$

Nous allons effectuer le produit de deux éléments U, V en utilisant multiplieur dual associé dans un premier temps à $\mathcal{B}'$, et ensuite à la $\mathcal{B}''$. Nous obtenons les deux situations suivantes.

1. *Multiplieur dual associé à la base $\mathcal{B}'$.*
   La base duale $\mathcal{B}'$ de $\mathcal{B}$ relativement à φ' est dans ce cas donnée par

$$\begin{array}{lll} e_0 = X+X^2+X^6, & e_1 = 1+X^2+X^5+X^6, & e_2 = 1+X+X^4+X^5 \\ e_3 = X^3+X^4, & e_4 = X^2+X^3, & e_5 = X+X^2, \\ e_6 = 1+X. & & \end{array}$$

   Nous allons multiplier les deux éléments

$$\begin{array}{rcl} U & = & u'_0e_0+u'_1e_1+u'_2e_2+u'_3e_3+u'4e_4+u'_5e_5+u'_6e_6, \\ V & = & v'_0e_0+v'_1e_1+v'_2e_2+v'_3e_3+v'_4e_4+v'_5e_5+v'_6e_6, \end{array}$$

   à partir de leur expression dans la base duale $\mathcal{B}'$. Nous voulons utiliser la méthode décrite dans le théorème 19 décrivant la méthode générale du multiplieur dual : les coordonnées de W dans $\mathcal{B}'$ se calculent en effectuant le produit matriciel

$$W = \widetilde{M_V} \cdot U.$$

Nous devons donc calculer les coordonnées u_i de U dans la base $\mathcal{B}$, ainsi que les coefficients v'_{i+j} de la matrice $\widetilde{M}_V$.
Nous allons dans un premier temps déterminer les coordonnées de U dans $\mathcal{B}$. Pour cela, nous remplaçons dans $U = \sum_{i=0}^{6} u'_i e_i$ les e_i par leurs expressions en les X^i données précédemment. Nous obtenons

$$\begin{aligned} U &= u'_0(X+X^2+X^6)+u'_1(1+X^2+X^5+X^6)+u'_2(1+X+X^4+X^5) \\ &\quad +u'_3(X^3+X^4)+u'_4(X^2+X^3)+u'_5(X+X^2)+u'_6(1+X) \\ &= (u'_1+u'_2+u'_6)+(u'_0+u'_2+u'_5+u'_6)X+(u'_0+u'_1+u'_4+u'_5)X^2 \\ &\quad +(u'_3+u'_4)X^3+(u'_2+u'_3)X^4+(u'_2+u'_3)X^5+(u'_0+u'_1)X^6. \end{aligned}$$

Autrement dit, les coordonnées u_i de U dans $\mathcal{B}$ sont données par

$$\begin{array}{lll} u_0 = u'_1+u'_2+u'_6, & u_1 = u'_0+u'_2+u'_5+u'_6, & u_2 = u'_0+u'_1+u'_4+u'_5, \\ u_3 = u'_3+u'_4, & u_4 = u'_2+u'_3, & u_5 = u'_1+u'_2, \\ u_6 = u'_0+u'_1. & & \end{array}$$

Ensuite nous devons calculer les coefficients de la matrice $\widetilde{M}_V = [v'_{i+j}]_{i,j=1,\ldots,6}$, autrement dit, nous devons calculer les coefficients v'_i pour $i = 7, \ldots, 12$. Nous avons juste à appliquer les formules données dans la proposition 23.

$$\begin{array}{rclrcl} v'_7 &=& v'_3+v'_2+v'_1+v'_0, & v'_8 &=& v'_4+v'_3+v'_2+v'_1, \\ v'_9 &=& v'_5+v'_4+v'_3+v'_2, & v'_{10} &=& v'_6+v'_5+v'_4+v'_3, \\ v'_{11} &=& v'_6+v'_5+v'_4+v'_3+v'_2+v'_1+v'_0, & v'_{12} &=& v'_6+v'_5+v'_4+v'_0. \end{array}$$

Nous en déduisons finalement les coordonnées dans $\mathcal{B}'$ du produit de U et V :

$$\begin{bmatrix} w''_0 \\ w''_1 \\ w''_2 \\ w''_3 \\ w''_4 \\ w''_5 \\ w''_6 \end{bmatrix} = \begin{bmatrix} v'_0 & v'_1 & v'_2 & v'_3 & v'_4 & v'_5 & v'_6 \\ v'_1 & v'_2 & v'_3 & v'_4 & v'_5 & v'_6 & v'_7 \\ v'_2 & v'_3 & v'_4 & v'_5 & v'_6 & v'_7 & v'_8 \\ v'_3 & v'_4 & v'_5 & v'_6 & v'_7 & v'_8 & v'_9 \\ v'_4 & v'_5 & v'_6 & v'_7 & v'_8 & v'_9 & v'_{10} \\ v'_5 & v'_6 & v'_7 & v'_8 & v'_9 & v'_{10} & v'_{11} \\ v'_6 & v'_7 & v'_8 & v'_9 & v'_{10} & v'_{11} & v'_{12} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{bmatrix}.$$

2. *Multiplieur dual associé à la base $\mathcal{B}''$.*
La base duale $\mathcal{B}''$ associée à la $\mathbb{F}_2$-forme φ'' est donnée par les 7 éléments suivants

$$\begin{array}{llll} f_0 = 1, & f_1 = X+X^2+X^6, & f_2 = X+X^5 & \\ f_3 = X^4, & f_4 = X^3, & f_5 = X^2, & f_6 = X. \end{array}$$

L'objectif ici encore c'est de calculer le produit de deux éléments

$$\begin{aligned} U &= u''_0 f_0+u''_1 f_1+u''_2 f_2+u''_3 f_3+u''_4 f_4+u''_5 f_5+u''_6 f_6, \\ V &= v''_0 f_0+v''_1 f_1+v''_2 f_2+v''_3 f_3+v''_4 f_4+v''_5 f_5+v''_6 f_6, \end{aligned}$$

à partir de leur expression dans la base duale $\mathcal{B}''$. Nous devons donc calculer, ici encore, les coefficients u_i de U dans la base $\mathcal{B}$, ainsi que les coefficients v'_{i+j} de la matrice $\widetilde{M}_V$.

Nous allons d'abord déterminer les coordonnées de U dans $\mathcal{B}$: dans l'expression $U = \sum_{i=0}^{6} u''_i f_i$ nous remplaçons les f_i par leur expression en les X^i

$$\begin{aligned} U &= u''_0 + u''_1(X + X^2 + X^6) + u''_2(X + X^5) + u''_3 X^4 + u''_4 X^3 + u''_5 X^2 + u''_6 X \\ &= u''_0 + (u''_1 + u''_2 + u''_6)X + (u''_1 + u''_5)X^2 + u''_4 X^3 + u''_3 X^4 + u''_2 X^5 + u''_1 X^6. \end{aligned}$$

Nous obtenons alors

$$\begin{array}{llll} u_0 = u''_0, & u_1 = u''_1 + u''_2 + u''_6, & u_2 = u''_1 + u''_5, & \\ u_3 = u''_3, & u_4 = u''_4, & u_5 = u''_5, & u_6 = u''_6. \end{array}$$

D'autre part les coefficients v'_i pour $i = 7, \ldots, 12$ sont calculés suivant les formules données dans la proposition 23.

$$\begin{array}{llll} v''_7 = v''_3 + v''_2 + v''_1 + v''_0, & & v''_8 = v''_4 + v''_3 + v''_2 + v''_1, & \\ v''_9 = v''_5 + v''_4 + v''_3 + v''_2, & & v''_{10} = v''_6 + v''_5 + v''_4 + v''_3, & \\ v''_{11} = v''_6 + v''_5 + v''_4 + v''_3 + v''_2 + v''_1 + v''_0, & & v''_{12} = v''_6 + v''_5 + v''_4 + v''_0. & \end{array}$$

Nous pouvons finalement calculer les coordonnées dans $\mathcal{B}'_1$ du produit U, V :

$$\begin{bmatrix} w''_0 \\ w''_1 \\ w''_2 \\ w''_3 \\ w''_4 \\ w''_5 \\ w''_6 \end{bmatrix} = \begin{bmatrix} v''_0 & v''_1 & v''_2 & v''_3 & v''_4 & v''_5 & v''_6 \\ v''_1 & v''_2 & v''_3 & v''_4 & v''_5 & v''_6 & v''_7 \\ v''_2 & v''_3 & v''_4 & v''_5 & v''_6 & v''_7 & v''_8 \\ v''_3 & v''_4 & v''_5 & v''_6 & v''_7 & v''_8 & v''_9 \\ v''_4 & v''_5 & v''_6 & v''_7 & v''_8 & v''_9 & v''_{10} \\ v''_5 & v''_6 & v''_7 & v''_8 & v''_9 & v''_{10} & v''_{11} \\ v''_6 & v''_7 & v''_8 & v''_9 & v''_{10} & v''_{11} & v''_{12} \end{bmatrix} \cdot \begin{bmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{bmatrix}.$$

Cet exemple illustre bien le fait que le calcul des v'_j, les coefficients de la matrice $\widetilde{M_V}$, s'effectue de la même manière dans les deux bases duales $\mathcal{B}'$ et $\mathcal{B}''$. Seul le calcul des u_i varie d'une situation à l'autre : dans cet exemple, le calcul des u_i dans le cas de $\mathcal{B}''$ est nettement plus simple que dans le cas de $\mathcal{B}'$. Bien sûr la situation idéale est celle on l'on peut trouver, si elle existe, une forme φ telle que $\mathcal{B}$ soit autoduale.

$\diamondsuit$

Références

[1] D.V. Bailey and C. Paar. Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms. *Lecture Notes in Computer Science*, 1462 :472, 1998.

[2] E.R. Berlekamp. Bit-serial Reed-Solomon encoder. *IEEE Trans. Information Theory*, IT-28, 1982.

[3] H. Cohen. *A Course In Computational Algebraic Number Theory*, volume GTM 138. Springer Verlag, 1993.

[4] I.F. Blake D.W. Ash and S.A. Vanstone. Low Complexity Normal Bases. *Discrete Applied Mathmatics*, 1989.

[5] S. Feisel, J. Gathen, and A. Shokrollahi. Normal bases via general Gauss periods, 1997.

[6] S.T.J. Fenn, M. Benaissa, and D. Taylor. GF(2^m) Multiplication and Division Over the Dual Basis. *IEEE Trans. Comput.*, 45(3) :319–327, 1996.

[7] S. Gao. Abelian Groups, Gauss Periods, and Normal Bases, 2001.

[8] S. Gao, J. Von zur Gathen, and D. Panario. Gauss Periods, Primitive Normal Bases, And Fast Exponentiation In Finite Fields. *Lecture Notes in Computer Science*, 911 :311–322, 1995.

[9] S. Gao and H. W. Lenstra Jr. Optimal Normal Bases. *Designs, Codes and Cryptography*, 2(4) :315–323, 1992.

[10] S. Gao and D. Panario. Density of normal elements. *Finite Fields and Their Applications*, 3 :141–150, 1997.

[11] M.A. Hasan H. Wu and L.F. Blake. New Low-Complexity Bit-Parallel Finite Field Multipliers Using Weakly Dual Bases. *IEEE Trans. Computers*, 47, 1998.

[12] A. Halbutogullari and C.K. Koc. Mastrovito Multiplier for General Irreducible Polynomials. *IEEE Trans. Comput.*, 49(5) :503–518, 2000.

[13] M.A. Hasan, M.Z. Wang, and V.K. Bhargava. A Modified Massey-Omura Parallel Multiplier for a Class of Finite Fields. *IEEE Trans. Comput.*, 42(10) :1278–1280, 1993.

[14] T. Itoh and S. Tsujii. A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases. *Inf. Comput.*, 78(3) :171–177, 1988.

[15] C.K. Koc and B. Sunar. Low-Complexity Bit-Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields. *IEEE Transactions on Computers*, 47(3) :353–356, 1998.

[16] C.K. Koc and B. Sunar. An Efficient Optimal Normal Basis Type II Multiplier. *IEEE Trans. Computers*, 50, 2001.

[17] C.-H. Lee and J. I. Lim. A New Aspect of Dual Basis for Efficient Field Arithmetic. In *Proceedings of the Second International Workshop on Practice and Theory in Public Key Cryptography*, pages 12–28. Springer-Verlag, 1999.

[18] J.L. Massey and J.K. Omura. Computational Method and Apparatus for Finite Field Arithmetic, 1986.

[19] E.D. Mastrovito. *VLSI architectures for computations in Galois fields.* PhD thesis, Dep. Elec. Eng.,Linkoping Univ, 1991.

[20] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, and R.M. Wilson. Optimal Normal Bases in GF(p^n). *Discrete Appl. Math.*, 22(2) :149–161, 1989.

[21] A. Reyhani-Masoleh and M. A. Hasan. A New Construction of Massey-Omura Parallel Multiplier over GF(2^m). *IEEE Trans. Comput.*, 51(5) :511–520, 2002.

[22] F. Rodriguez-Henriquez and C.K. Koc. Parallel Multipliers based on Special Irreducible Pentanomials. *IEEE Transaction on Computers*, 2003.

[23] J.H. Silverman. Low complexity multiplication in rings.

[24] B. Sunar and C.K. Koc. Mastrovito Multiplier for All Trinomials. *IEEE Transaction on Computers*, May 1999.