THÈSE de DOCTORAT de l'UNIVERSITÉ PARIS 6

Spécialité : INFORMATIQUE

Présentée par

Nicolas SENDRIER

pour obtenir le titre de

DOCTEUR DE L'UNIVERSITÉ PARIS 6

Titre de la thèse :

Codes Correcteurs d'Erreurs à Haut Pouvoir de Correction

Soutenue le 20 décembre 1991, devant le jury composé de :

Daniel LAZARD	*Président*
Bernard COURTEAU	*Rapporteur*
Michel MINOUX	*Rapporteur*
Gérard COHEN	*Rapporteur*
Paul CAMION	*Directeur*
Pascale CHARPIN	
Thomas ERICSON	
Harold MATTSON	

En particulier pour les poids d et $d+1$

$$A_d = (q-1)\binom{n}{d} \tag{I.6}$$

$$A_{d+1} = (q-1)(q-d)\binom{n}{d+1} \tag{I.7}$$

3 Théorie algébrique du décodage

Dans toute cette section on considère un code linéaire $C(n,k,d)$ sur $\mathbb{F}_q$.

3.1 Position du problème

Etant donné

- que $\mathbf{x} \in C$ est le "message transmis",
- que $\mathbf{x}$ est perturbé dans un canal bruité par l'erreur $\mathbf{e} \in \mathbb{F}_q^n$,
- que $\mathbf{y} = \mathbf{x} + \mathbf{e}$, le "message reçu", est le seul mot auquel le décodeur a accès,

le problème du décodage est de retrouver $\mathbf{x}$ à partir de $\mathbf{y}$.

Un algorithme de décodage de C devra donc prendre comme argument un élément de $\mathbb{F}_q^n$, et s'il se termine, rendre un élément du code C. Il devra également être déterministe, c'est-à-dire qu'un mot de l'espace $\mathbb{F}_q^n$ sera toujours décodé de la même manière. Nous proposons la définition suivante.

Définition I.22 *Soit un code linéaire $C(n,k,d)$ sur $\mathbb{F}_q$, un* algorithme de décodage d'erreur de C *est une application*

$$\begin{array}{cccc} \gamma : & \mathbb{F}_q^n & \longrightarrow & C \cup \{\infty\} \\ & \mathbf{y} & \longmapsto & \gamma(\mathbf{y}) \end{array}$$

telle que $\forall\, \mathbf{x} \in C$, $\gamma(\mathbf{x}) = \mathbf{x}$. Le fait que $\gamma(\mathbf{y}) = \infty$ signifiant que $\mathbf{y}$ n'a pas été décodé.

Soit e un entier positif, on dira que γ est borné par e*, si*

$$\forall\, \mathbf{y} \in \mathbb{F}_q^n,\ \forall\, \mathbf{x} \in C,\quad d_H(\mathbf{x},\mathbf{y}) < \frac{e}{2} \Rightarrow \gamma(\mathbf{y}) = \mathbf{x}$$

où d_H est la métrique de Hamming sur $\mathbb{F}_q$, on dira que γ est borné strictement par e *si on a de plus*

$$\gamma(\mathbf{y}) = \mathbf{x} \neq \infty \Rightarrow d_H(\mathbf{x},\mathbf{y}) < \frac{e}{2}$$

On dira que γ respecte la métrique d*, si*

$$\forall\, \mathbf{y} \in \mathbb{F}_q^n,\ \forall\, \mathbf{x} \in C,\quad \gamma(\mathbf{y}) \in C \Rightarrow d(\gamma(\mathbf{y}),\mathbf{y}) \leq d(\mathbf{x},\mathbf{y})$$

On dira que γ est un algorithme linéaire *si*

$$\forall \mathbf{y} \in \mathbb{F}_q^n,\ \forall \mathbf{x} \in C, \quad \gamma(\mathbf{y}+\mathbf{x}) = \gamma(\mathbf{y}) + \mathbf{x},$$

avec la convention $\infty + \mathbf{x} = \infty$.

Remarque I.6 Une confusion est possible entre un algorithme linéaire et un algorithme de complexité linéaire. Nous reservons, dans tout ce travail, le terme d'algorithme linéaire à la propriété énoncée ci-dessus.

Proposition I.10 *Tout code C admet un algorithme de décodage d'erreur borné par sa distance minimale, respectant la distance de Hamming, et qui se termine pour toute entrée, on dit d'un tel algorithme de décodage qu'il est à* vraisemblance maximale *(*maximum likelyhood decoding*).*

preuve : Soit l'algorithme de décodage γ suivant

$$\forall \mathbf{y} \in \mathbb{F}_q^n,\ \gamma(\mathbf{y}) = \text{“le mot de } C \text{ le plus proche de } \mathbf{y} \text{ pour } d_H\text{”}$$

puisque C est fini, on peut parcourir le code pour trouver ce mot le plus proche, en cas de non unicité, les conflits peuvent être réglés en munissant C d'une relation d'ordre.

Notons que γ se termine pour toute entrée et respecte la distance de Hamming par définition.

Soit d la distance minimale de C, soient $\mathbf{y} \in \mathbb{F}_q^n$ et $\mathbf{x} \in C$, tels que

$$d_H(\mathbf{x}, \mathbf{y}) < \frac{d}{2}.$$

Alors $\mathbf{x}$ est le mot de C le plus proche de $\mathbf{y}$, sinon la définition de la distance minimale serait contredite, donc γ est borné par d. □

Notons que cet algorithme n'est pas unique en général, il suffit en fait qu'il existe un mot de $\mathbf{y} \in \mathbb{F}_q^n$ qui soit à égale distance de deux mots du code, auquel cas on a au moins deux algorithmes distincts à vraisemblance maximale.

Proposition I.11 *Soit un code linéaire $C(n, k, d)$ sur $\mathbb{F}_q$, muni d'un algorithme de décodage γ, la meilleure borne possible pour γ est*

$$2\left\lfloor\frac{d-1}{2}\right\rfloor + 1.$$

preuve : Notons que $2\lfloor\frac{d-1}{2}\rfloor + 1$ vaut $d+1$ si d est impair, et d si d est pair.

Soient $\mathbf{x}, \mathbf{x}' \in C$ tels que $d_H(\mathbf{x}, \mathbf{x}') = d$. Il existe alors $\mathbf{y} \in \mathbb{F}_q^n$ tel que

$$d_H(\mathbf{x}, \mathbf{y}) = \frac{d-1}{2}, \quad \text{et} \quad d_H(\mathbf{x}', \mathbf{y}) = \frac{d+1}{2},$$

si d est impair, ou

$$d_H(\mathbf{x}, \mathbf{y}) = \frac{d}{2}, \quad \text{et} \quad d_H(\mathbf{x}', \mathbf{y}) = \frac{d}{2},$$

si d est pair.

Donc si d est impair γ ne peut être borné par $d+2$, et si d est pair γ ne peut être borné par $d+1$. □

3.2 Matrice de parité – Syndrome

Définition I.23 *On appelle* matrice de parité *du code $C(n,k,d)$ une matrice H à $n-k$ lignes et n colonnes sur $\mathbb{F}_q$, telle que $C = \ker H = \{\mathbf{x} \mid H\mathbf{x}^t = 0\}$.*

La matrice H détermine le code C. Remarquons que par un théorème fondamental d'algèbre linéaire, les lignes de H forment une base de l'orthogonal de C dans $\mathbb{F}_q^n$ pour le produit scalaire usuel.

Définition I.24 *Soit $\mathbf{y} \in \mathbb{F}_q^n$. Le* syndrome *de $\mathbf{y}$ est le vecteur de $\mathbb{F}_q^{n-k}$*

$$S(\mathbf{y}) = H\mathbf{y}^t.$$

l'application $S : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ ainsi définie est $\mathbb{F}_q$-linéaire.

H induit une relation d'équivalence sur $\mathbb{F}_q^n$

$$\mathbf{x} \;\mathcal{R}\; \mathbf{y} \Leftrightarrow H\mathbf{x}^t = H\mathbf{y}^t \Leftrightarrow H(\mathbf{x}-\mathbf{y})^t = 0 \Leftrightarrow \mathbf{x}-\mathbf{y} \in C.$$

Chacune des classes de cette relation d'équivalence est appelée “classe latérale” ou “translaté” de C.

Le code C est la classe de l'élément nul de $\mathbb{F}_q^n$. Plus généralement, deux éléments sont dans un même translaté si et seulement si ils ont le même syndrome.

Proposition I.12 *Il existe au plus un mot de poids $< d/2$ dans un translaté donné.*

preuve : Soient $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ tels que $\mathbf{x} \;\mathcal{R}\; \mathbf{y}$, $w_H(\mathbf{x}) < d/2$ et $w_H(\mathbf{y}) < d/2$. Alors $\mathbf{x}-\mathbf{y} \in C$ et $w_H(\mathbf{x}-\mathbf{y}) = d(\mathbf{x},\mathbf{y}) \leq d(\mathbf{x},\mathbf{0}) + d(\mathbf{0},\mathbf{y}) < d/2 + d/2 = d$, en vertu de l'inégalité triangulaire. Donc $\mathbf{x} = \mathbf{y}$. □

3.3 Décodage des codes linéaires

A partir de la matrice de parité et des syndromes on peut définir l'algorithme de décodage γ suivant :

1. Dans tout translaté $\mathbf{y} + C$, on choisit un élément de plus petit poids, $e(\mathbf{y})$ que l'on met dans une table indexée par le syndrome de $\mathbf{y}$. Remarquons que $e(\mathbf{y}+\mathbf{x}) = e(\mathbf{y})$ pour tout $\mathbf{x} \in C$

2. Si $\mathbf{y}$ est le mot reçu, on calcule son syndrome $S(\mathbf{y})$, et on lit $e(\mathbf{y})$ dans la table.

3. l'algorithme retourne $\gamma(\mathbf{y}) = \tilde{\mathbf{x}} = \mathbf{y} - e(\mathbf{y})$.

Proposition I.13 *γ est un algorithme à vraisemblance maximale, donc il est borné par sa distance minimale, et respecte la distance de Hamming. De plus cet algorithme est linéaire.*

preuve : Soit $\mathbf{y} \in \mathbb{F}_q^n$, $\tilde{\mathbf{e}}$ un élément de plus petit poids de la classe de $\mathbf{y}$

- $\gamma(\mathbf{y}) \in C$, en effet $\mathbf{y} \mathcal{R} \tilde{\mathbf{e}}$, donc $\gamma(\mathbf{y}) = \mathbf{y} - \tilde{\mathbf{e}} \mathcal{R} \mathbf{0}$.
- $\forall \mathbf{x} \in C$, $\mathbf{y} - \mathbf{x} \mathcal{R} \tilde{\mathbf{e}}$, donc $d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{y} - \mathbf{x}) \geq w_H(\tilde{\mathbf{e}}) = d_H(\gamma(\mathbf{y}), \mathbf{y})$, donc $\gamma(\mathbf{y})$ est un élément du code réalisant le minimum de la distance à $\mathbf{y}$.
- L'algorithme est linéaire. En effet, pour tout $\mathbf{x} \in C$, $\mathbf{y} \in \mathbb{F}_q^n$

$$\gamma(\mathbf{y} + \mathbf{x}) = \mathbf{y} + \mathbf{x} - e(\mathbf{y} + \mathbf{x}) = \mathbf{y} + \mathbf{x} - e(\mathbf{y}) = \gamma(\mathbf{y}) + \mathbf{x},$$

  puisque $e(\mathbf{y} + \mathbf{x}) = e(\mathbf{y})$.

□

Le décodage des codes linéaires se ramène donc à la recherche d'un mot de plus petit poids d'un translaté donné par son syndrome. Cette recherche est généralement difficile, mais dans certains cas, comme celui des codes BCH, on possède un algorithme qui fonctionne pour certains translatés.

3.4 Décodage d'erreur et d'effacement simultanément

Un effacement étant un symbole erroné dont on connait la position, on convient de substituer le symbole ∞ en cette position. Nous sommes donc amené à raisonner sur des vecteurs dont les coordonnés sont dans $\mathbb{F}_q \cup \{\infty\}$. Nous étendons l'addition dans $\mathbb{F}_q$ en considérant ∞ comme un élément absorbant.

Dans la proposition suivante nous définissons une distance de Hamming généralisée sur $\mathbb{F}_q \cup \{\infty\}$qui diffère de celle définie par Wei dans [98], bien que portant le même nom.

Proposition I.14 *Soit $\delta_H : (\mathbb{F}_q \cup \{\infty\})^2 \to \{0, \frac{1}{2}, 1\}$ l'application définie par*

$$\delta_H(a,b) = \begin{cases} 0 & si\ a = b \\ \frac{1}{2} & si\ a \neq b,\ \ et\ a = \infty,\ \ ou\ b = \infty \\ 1 & si\ a \neq b,\ \ et\ a \neq \infty,\ b \neq \infty \end{cases}$$

Si $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q \cup \{\infty\})^n$, on définit $\Delta_H : (\mathbb{F}_q \cup \{\infty\})^n \to \frac{1}{2}\mathbb{Z}$ par

$$\Delta_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \delta_H(x_i, y_i),$$

Δ_H est une distance sur $(\mathbb{F}_q \cup \{\infty\})^n$, on l'appelera distance de Hamming généralisée *sur $\mathbb{F}_q$.*

preuve : δ_H est une distance sur $\mathbb{F}_q \cup \{\infty\}$, en effet

1. $\delta_H(a,b) = 0 \Leftrightarrow a = b$
2. $\delta_H(a,b) = \delta_H(b,a)$
3. soit $a, b, c \in \mathbb{F}_q \cup \{\infty\}$, distincts, on a
   (a) $a \neq \infty$, $b \neq \infty$, et $c \neq \infty$, δ_H restreint à $\mathbb{F}_q$ est la distance de Hamming (en longueur 1 !), donc
   $$\delta_H(a,c) \leq \delta_H(a,b) + \delta_H(b,c).$$
   (b) $a = \infty$, ou $c = \infty$, alors
   $$\delta_H(a,c) = \frac{1}{2} \leq \delta_H(a,b) + \delta_H(b,c) = \frac{3}{2}.$$
   (c) $b = \infty$
   $$\delta_H(a,b) + \delta_H(b,c) = 1 \geq \delta_H(a,c).$$
   si a, b, c ne sont pas distincts, l'inégalité triangulaire est triviale (l'un des trois termes au moins est nul, les autres sont égaux).

De la relation
$$\Delta_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} \delta_H(x_i, y_i),$$
on déduit que Δ_H est également une distance. □

Définition I.25 *On appellera* poids de Hamming généralisé *d'un mot* $\mathbf{x} \in (\mathbb{F}_q \cup \{\infty\})^n$*, noté* $\Omega_H(\mathbf{x})$*, sa distance de Hamming généralisée au mot nul*
$$\Omega_H(\mathbf{x}) = \Delta_H(\mathbf{x}, \mathbf{0}).$$

Remarque I.7

1. La métrique Δ_H restreinte à $\mathbb{F}_q^n$ coïncide avec la métrique de Hamming. En particulier la distance minimale est conservée.
2. Le symbole ∞ représentant un effacement, si $\mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n$ est effacé en ρ positions (i.e. $\mathbf{y}$ possède ρ fois le symbole ∞ dans son écriture), et diffère de $\mathbf{x} \in \mathbb{F}_q^n$ en ν des positions restantes, alors
   $$\Delta_H(\mathbf{x}, \mathbf{y}) = \frac{2\nu + \rho}{2}.$$
3. Le poids 1/2 qui est donné aux effacements, est le plus petit tel que Δ_H soit une distance, tout en conservant la même distance minimale pour le code, et il correspond bien a l'idée intuitive qu'un effacement "coûte" 2 fois moins cher à corriger qu'une erreur.

Définition I.26 *Soit un code linéaire $C(n,k,d)$ sur $\mathbb{F}_q$. Un* algorithme de décodage d'erreur et d'effacement de *C est une application*

$$\begin{array}{rccc}\gamma : & (\mathbb{F}_q \cup \{\infty\})^n & \longrightarrow & C \cup \{\infty\} \\ & \mathbf{y} & \longmapsto & \gamma(\mathbf{y})\end{array}$$

telle que $\forall\, \mathbf{x} \in C$, $\gamma(\mathbf{x}) = \mathbf{x}$. Le fait que $\gamma(\mathbf{y}) = \infty$ signifiant que $\mathbf{y}$ n'a pas été décodé.

Soit e un entier positif. On dira que γ est borné par *e, si*

$$\forall\, \mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n,\ \forall\, \mathbf{x} \in C, \quad \Delta_H(\mathbf{x},\mathbf{y}) < \frac{e}{2} \Rightarrow \gamma(\mathbf{y}) = \mathbf{x}$$

où Δ_H est la distance de Hamming généralisée sur $\mathbb{F}_q$. On dira que γ est borné strictement par *e si on a de plus*

$$\gamma(\mathbf{y}) = \mathbf{x} \neq \infty \Rightarrow \Delta_H(\mathbf{x},\mathbf{y}) < \frac{e}{2}.$$

On dira que γ respecte la distance *d si*

$$\forall\, \mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n,\ \forall\, \mathbf{x} \in C, \quad \gamma(\mathbf{y}) \in C \Rightarrow d(\gamma(\mathbf{y}),\mathbf{y}) \leq d(\mathbf{x},\mathbf{y}).$$

On dira que γ est un algorithme linéaire *si*

$$\forall\, \mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n,\ \forall\, \mathbf{x} \in C, \quad \gamma(\mathbf{y}+\mathbf{x}) = \gamma(\mathbf{y}) + \mathbf{x},$$

(on convient que $\mathbf{x} + \infty = \infty$ pour tout $x \in (\mathbb{F}_q \cup \{\infty\})^n$).

Remarque I.8 Le symbole ∞ est utilisé dans deux contexte différents, pour représenter l'effacement d'un symbole de $\mathbb{F}_q$ et pour représenter un echec au décodage.

Proposition I.15 *Tout code C admet un algorithme de décodage d'erreur et d'effacement borné par sa distance minimale, respectant la distance de Hamming généralisée, et qui se termine pour toute entrée, on dit d'un tel algorithme de décodage qu'il est à* vraisemblance maximale (maximum likelyhood decoding).

preuve : Soit l'algorithme de décodage γ suivant

$$\forall\, \mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n,\ \gamma(\mathbf{y}) = \text{“le mot de } C \text{ le plus proche de } \mathbf{y} \text{ pour } \Delta_H\text{”}$$

puisque C est fini, on peut parcourir le code pour trouver ce mot le plus proche, en cas de non unicité, les conflits peuvent être réglés en munissant C d'une relation d'ordre.

- γ se termine pour toute entrée et respecte la distance de Hamming généralisée par définition.
- Soit d la distance minimale de C, soient $\mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n$ et $\mathbf{x} \in C$, tels que
$$\Delta_H(\mathbf{x},\mathbf{y}) < \frac{d}{2}.$$
Alors $\mathbf{x}$ est le mot de C le plus proche de $\mathbf{y}$, sinon la définition de la distance minimale serait contredite, donc γ est borné par d.

□

Proposition I.16 *Soit un code linéaire $C(n,k,d)$ sur $\mathbb{F}_q$, muni d'un algorithme de décodage d'erreur et d'effacement γ, la meilleure borne possible pour γ est la distance minimale d de C.*

preuve :
Soit $\mathbf{x} \in C$, tel que $w_H(\mathbf{x}) = d$. Alors il existe $\mathbf{y} \in (\mathbb{F}_q \cup \{\infty\})^n$ tel que

$$\Delta_H(\mathbf{x},\mathbf{y}) = \frac{d}{2}, \quad \text{et} \quad \Delta_H(\mathbf{0},\mathbf{y}) = \frac{d}{2}.$$

En effet, supposons sans perte de généralité que $\mathbf{x} = (x_1, \ldots, x_d, 0, \ldots, 0)$. Si d est pair, on choisit

$$\mathbf{y} = (x_1, \ldots, x_{\frac{d}{2}}, 0, \ldots, 0),$$

et si d est impair, on choisit

$$\mathbf{y} = (x_1, \ldots, x_{\frac{d-1}{2}}, \infty, 0, \ldots, 0).$$

Donc γ ne peut pas être borné par $d+1$. □

4 Décodage des codes BCH

Soit α une racine n-ième primitive de l'unité dans le corps $\mathbb{F}_{q^m}$ où $n | q^m - 1$. $B_q(n,\delta,b)$ est le code BCH sur $\mathbb{F}_q$ de longueur n, et de distance construite δ, défini par

$$B_q(n,\delta,b) = \{c(X) \in \mathbb{F}_q[X]/(X^n - 1) \ | \ c(\alpha^b) = c(\alpha^{b+1}) = \ldots = c(\alpha^{b+\delta-2}) = 0\}.$$

Ce code admet pour matrice de parité :

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \ldots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \ldots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \ldots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}$$

Les sections 4.1, 4.2 et 4.3 sont inspirées de [67], la section 4.4 de [75]. Toutefois la présentation basée sur le théorème I.9 est originale.

4.1 Polynômes localisateur et évaluateur

Soit $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^n$ de poids w et soient :

$$a_{i_1}, a_{i_2}, \ldots, a_{i_w}$$

Chapitre III

Codes concaténés

Les codes concaténés ont été introduits par Forney dans [36] en 1966. Ces travaux ont ensuite été poursuivis par les russes Block, Zinoviev et Zyablov, qui ont abouti à un algorithme de décodage performant, s'inspirant des idées de Forney sur le décodage souple, et surtout aux codes concaténés généralisés [12], [103] et [104].

Nous nous sommes volontairement limité ici au cas linéaire. La plupart des résultats restent cependant valables dans le cas général. Cette limitation permet de donner des définitions qui nous semblent plus simples que celles données généralement. En particulier nous définissons, dans la section 3, les codes concaténés géneralisés comme une somme directe de codes concaténés d'ordre 1, cette représentation ayant déjà été utilisée par Jensen dans un cas particulier (cf. [50]).

Dans la section 1, outre la définition des codes concaténés d'ordre 1 et la description de leur décodage, nous introduisons la notion de décodage partiel qui nous permet dans la section 3 de donner une description récursive simple du décodage des codes concaténés géneralisés, description que Bossert donne en filigrane dans [14].

Dans la section 2, nous utilisons une approche originale pour l'évaluation des performances des codes concaténés d'ordre 1, faisant appel à la combinatoire énumérative. De telles évaluations avaient été faites sous une forme légèrement différente pour l'algorithme naïf dans [21]. Nous avons pu étendre ces résultats à tous les algorithmes décrits dans la section 1.

Soit un corps fini $\mathbb{F}_q$. Pour tout couple d'entiers n_b et n_e, nous identifierons chaque élément de $\mathbb{F}_q^{n_b n_e}$ à un élément de $(\mathbb{F}_q^{n_b})^{n_e}$. En particulier lorsque l'on posera $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathbb{F}_q^{n_b n_e}$, cela signifiera que pour tout i, $1 \leq i \leq n_e$, on a $x_i \in \mathbb{F}_q^{n_b}$. Le vecteur $\mathbf{x}$ aura comme composantes, dans l'ordre, les composantes de x_1, puis celles de x_2, jusqu'à celles de x_{n_e}.

1 Codes concaténés d'ordre 1 – Algorithmes de décodage

1.1 Définition

Soit un code linéaire $\mathcal{B} = \mathcal{B}(n_b, k_b, d_b)$ sur $\mathbb{F}_q$, $\mathcal{B}$ et $\mathbb{F}_{q^{k_b}}$ sont isomorphes en tant que $\mathbb{F}_q$-espaces vectoriels. Fixons un isomorphisme

$$\begin{array}{rcccl} \theta & : & \mathbb{F}_{q^{k_b}} & \longrightarrow & \mathcal{B} \\ & & x & \longmapsto & \theta(x). \end{array} \tag{III.1}$$

θ permet de représenter de façon unique tout élément de $\mathbb{F}_{q^{k_b}}$ par un élément du code $\mathcal{B}$, et réciproquement.

Soit n_e un entier positif. On définit l'isomorphisme $\mathbb{F}_q$-linéaire Θ comme suit :

$$\begin{array}{rcccl} \Theta & : & \mathbb{F}_{q^{k_b}}^{n_e} & \longrightarrow & \mathcal{B}^{n_e} \\ & & \mathbf{x} = (x_1, \ldots, x_{n_e}) & \longmapsto & \Theta(\mathbf{x}) = (\theta(x_1), \ldots, \theta(x_{n_e})) \end{array} \tag{III.2}$$

Définition III.1 *Soient $\mathcal{B} = \mathcal{B}(n_b, k_b, d_b)$ un code linéaire sur $\mathbb{F}_q$, $\mathcal{E} = \mathcal{E}(n_e, k_e, d_e)$ un code linéaire sur $\mathbb{F}_{q^{k_b}}$ et θ l'isomorphisme défini par* (III.1).

Le code concaténé admettant $\mathcal{B}$ comme code interne et $\mathcal{E}$ comme code externe est le code $\mathcal{C}$ sur $\mathbb{F}_q$ constitué des mots de $\mathcal{E}$ dans lesquels les symboles de $\mathbb{F}_{q^{k_b}}$ sont remplacés par des mots de $\mathcal{B}$ à l'aide de θ

$$\mathcal{C} = \{(\theta(x_1), \theta(x_2), \ldots, \theta(x_{n_e})) \mid (x_1, x_2, \ldots, x_{n_e}) \in \mathcal{E}\} = \Theta(\mathcal{E}).$$

On dira en abrégé que $\mathcal{C}$ est le code concaténé de $\mathcal{B}$ et de $\mathcal{E}$.

Remarque III.1 Le code $\mathcal{E}$ introduit dans la définition ci-dessus est un espace vectoriel sur $\mathbb{F}_{q^{k_b}}$ de dimension k_e, mais puisque $\mathbb{F}_{q^{k_b}}$ peut être considéré comme un espace vectoriel sur $\mathbb{F}_q$ de dimension k_b, on peut considérer $\mathcal{E}$ comme un espace vectoriel sur $\mathbb{F}_q$ de dimension $k_b k_e$.

Proposition III.1 *Soit Θ l'isomorphisme défini par* (III.2). *Si $\mathcal{C} = \Theta(\mathcal{E})$ est le code concaténé de $\mathcal{B}(n_b, k_b, d_b)$ et $\mathcal{E}(n_e, k_e, d_e)$, alors $\mathcal{C}$ est un code linéaire sur $\mathbb{F}_q$ de longueur $n_b n_e$, de dimension $k_b k_e$, et dont la distance minimale est au moins égale à $d_b d_e$.*

preuve : Puisque Θ est injectif et $\mathbb{F}_q$-linéaire, $\mathcal{C}$ a pour dimension $\dim_{\mathbb{F}_q}(\mathcal{E}) = k_b k_e$.

Montrons que tout mot non nul du code concaténé a un poids supérieur ou égal à $d_b d_e$. Soit $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathcal{E}$. Alors

$$w_H(\Theta(\mathbf{x})) = \sum_{i=1}^{n_e} w_H(\theta(x_i))$$

où w_H est le poids de Hamming sur $\mathbb{F}_q$. Si $\mathbf{x} \neq 0$, alors au moins d_e des x_i sont non nuls et pour chacun de ces x_i, $\theta(x_i) \in \mathcal{B} \setminus \{0\}$, donc $w_H(\theta(x_i)) \geq d_b$, d'où le résultat. □

Remarque III.2 Les codes concaténés sont définis ici comme des codes linéaires, Forney les a introduits dans [36] de façon plus générale.

Dans le cas non linéaire il suffit de pouvoir mettre en bijection l'ensemble des mots du code interne avec l'alphabet du code externe. Les résultats sur les paramètres donnés dans la proposition III.1 restent vrais en remplaçant la dimension par le nombre d'éléments.

1.2 Algorithme de décodage naïf

Supposons donnés :

- $\mathcal{B} = \mathcal{B}(n_b, k_b, d_b)$ le code interne sur $\mathbb{F}_q$ muni d'un algorithme de décodage d'erreur γ borné par la distance minimale,
- $\mathcal{E} = \mathcal{E}(n_e, k_e, d_e)$ le code externe sur $\mathbb{F}_{q^{k_b}}$ est muni d'un algorithme de décodage d'erreur et d'effacement Φ borné par la distance minimale,
- $\mathcal{C} = \Theta(\mathcal{E})$ le code concaténé de $\mathcal{B}$ et $\mathcal{E}$.

Proposition III.2 *Soit l'application* Γ

$$\begin{array}{rrcl} \Gamma \ : & (\mathbb{F}_q^{n_b})^{n_e} & \longrightarrow & (\mathbb{F}_{q^{k_b}} \cup \{\infty\})^{n_e} \\ & \mathbf{y} = (y_1, \ldots, y_{n_e}) & \longmapsto & \Gamma(\mathbf{y}) = (\theta^{-1}(\gamma(y_1)), \ldots, \theta^{-1}(\gamma(y_{n_e}))) \end{array} \tag{III.3}$$

(avec la convention $\theta^{-1}(\infty) = \infty$).

Alors $\Psi = \Theta \circ \Phi \circ \Gamma$ est un algorithme de décodage d'erreur du code concaténé $\mathcal{C}$ de $\mathcal{B}$ et de $\mathcal{E}$, borné par $\frac{d_b d_e}{2}$, autrement dit, pour tout $\mathbf{y} \in \mathbb{F}_q^{n_b n_e}$ et pour tout $\mathbf{x} \in \mathcal{C}$, on a

$$d_H(\mathbf{x}, \mathbf{y}) < \frac{d_b d_e}{4} \Rightarrow \Psi(\mathbf{y}) = \mathbf{x}.$$

preuve : Soient $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathcal{C}$, $\mathbf{y} = (y_1, \ldots, y_{n_e}) \in \mathbb{F}_q^{n_b n_e}$. Posons pour tout i

$$w_i = d_H(x_i, y_i),$$

et, par hypothèse,

$$d_H(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n_e} w_i < \frac{d_b d_e}{4}.$$

Les distances Δ_H et δ_H sont définies sur $\mathbb{F}_{q^{k_b}} \cup \{\infty\}$. Supposons que $\Psi(\mathbf{y}) = \Theta(\Phi(\Gamma(\mathbf{y}))) \neq \mathbf{x}$. Puisque Φ est borné par d_e, on a (cf. définition I.26)

$$\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma(\mathbf{y})) = \sum_{i=1}^{n_e} \delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) \geq \frac{d_e}{2}. \tag{III.4}$$

$$\begin{tikzcd}
 & (\mathcal{B} \cup \{\infty\})^{n_e} \arrow[dr, "(\theta^{-1})^{n_e}"] & \\
\mathbb{F}_q^{n_b n_e} \equiv (\mathbb{F}_q^{n_b})^{n_e} \arrow[ur, "\gamma^{n_e}"] \arrow[rr, "\Gamma"] \arrow[d, "\Psi"] & & (\mathbb{F}_{q^{k_b}} \cup \{\infty\})^{n_e} \arrow[d, "\Phi"] \\
\mathcal{C} \cup \{\infty\} & & \mathcal{E} \cup \{\infty\} \arrow[ll, "\Theta"']
\end{tikzcd}$$

Figure III.1 : Décodage naïf d'un code concaténé

Par définition, $\delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) \neq 0$ si et seulement si $\gamma(y_i) \neq x_i$, et puisque γ est borné par d_b, on peut écrire

$$\delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) \neq 0 \Rightarrow w_i = d_H(x_i, y_i) \geq \frac{d_b}{2}.$$

Si $I = \{i \mid \delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) \neq 0\}$, on a pour tout $i \in I$

$$w_i \geq \frac{d_b}{2},$$

de plus puisque δ_H est à valeur dans $\{0, \frac{1}{2}, 1\}$ et que

$$\sum_{i=1}^{n_e} \delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) = \sum_{i \in I} \delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma(y_i))) \geq \frac{d_e}{2},$$

le cardinal de I est au moins égal à $\frac{d_e}{2}$, d'où

$$\sum_{i=1}^{n_e} w_i \geq \frac{d_b d_e}{4}$$

ce qui contredit l'hypothèse. On a donc bien $\Psi(\mathbf{y}) = \mathbf{x}$. $\square$

Cette borne de $\frac{d_b d_e}{2}$ n'est pas excellente, puisque qu'on peut espérer atteindre $d_b d_e$. L'exemple suivant montre qu'il existe, pour au moins un code, des motifs d'erreur de poids inférieur à $\frac{d_b d_e}{2}$, et que Ψ ne peut pas décoder.

Exemple :

Considérons le code concaténé défini par les données suivantes :

- Le code interne $\mathcal{B}$ est le code de Hamming binaire $H(7,4,3)$, γ est un algorithme de décodage à vraisemblance maximale, capable de corriger toute erreur de poids 1.
- Le code externe $\mathcal{E}$ est le code de Reed-Solomon $RS(15,13,3)$ sur $\mathbb{F}_{16}$, Φ est l'algorithme d'Euclide étendu, capable de corriger tout motif de ν erreurs et ρ effacements tel que $2\nu+\rho < 3$, et aucun autre (*i.e.* Φ *est borné strictement par la distance minimale du code*).

Le code concaténé résultant possède une distance minimale supérieure ou égale à 9. Montrons qu'il existe des motifs d'erreur de poids 4 qui ne sont pas corrigibles par Ψ.

Prenons comme mot émis le mot nul, et supposons que le mot reçu soit $\mathbf{y} = (y_1, y_2, 0, \dots, 0) \in (\mathbb{F}_2^4)^{15}$, tel que $w_H(y_1) = w_H(y_2) = 2$. Ce mot $\mathbf{y}$ est à distance 4 du mot émis. Par exemple

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{15} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Le code de Hamming étant un code 1-correcteur parfait, $\gamma(y_1)$ et $\gamma(y_2)$ sont deux éléments non nuls de $H(7,4,3)$, et donc $\theta^{-1}(\gamma(y_1))$ et $\theta^{-1}(\gamma(y_2))$ sont deux éléments non nuls de $\mathbb{F}_{16}$. Dans notre exemple

$$\Gamma(\mathbf{y}) = (\beta, \beta, 0, \dots, 0), \text{ où } \beta \in \mathbb{F}_{16}^*.$$

Le décodeur externe Φ doit donc décoder un mot qui contient 2 erreurs ; or

$$\Delta_H(\Gamma(\mathbf{y}), \mathbf{0}) = 2 > 3/2 \;\Rightarrow\; \Phi(\Gamma(\mathbf{y})) \neq \mathbf{0}$$

car Φ est borné strictement par 3. Donc le décodage va échouer, c'est-à-dire aboutir

- soit à ∞,
- soit à un mot non nul du code concaténé à distance ≥ 5 du mot reçu.

1.3 Algorithme de Block-Zyablov

Soit $\mathcal{C}$ le code concaténé de $\mathcal{B}$ et $\mathcal{E}$ munis comme plus haut des données suivantes :

- $\mathcal{B} = \mathcal{B}(n_b, k_b, d_b)$ le code interne est muni d'un algorithme de décodage γ, borné par la distance minimale d_b.

- $\mathcal{E} = \mathcal{E}(n_e, k_e, d_e)$ le code externe est muni d'un algorithme de décodage d'erreur et d'effacement Φ borné par la distance minimale d_e.

Pour tout nombre réel r, $0 \leq r < \frac{d_b}{2}$, on définit l'algorithme de décodage suivant γ_r de $\mathcal{B}$

$$\forall\, y \in \mathbb{F}_q^{n_b},\ \gamma_r(y) = \begin{cases} \gamma(y) & \text{si } d_H(\gamma(y), y) \leq r \\ \infty & \text{sinon} \end{cases},$$

on en déduit l'application Γ_r

$$\begin{array}{rccl} \Gamma_r \quad : & \mathbb{F}_q^{n_b n_e} & \longrightarrow & (\mathbb{F}_{q^{k_b}} \cup \{\infty\})^{n_e} \\ & \mathbf{y} = (y_1, \ldots, y_{n_e}) & \longmapsto & \Gamma_r(\mathbf{y}) = (\theta^{-1}(\gamma_r(y_1)), \ldots, \theta^{-1}(\gamma_r(y_{n_e}))) \end{array}$$

et l'algorithme de décodage de $\mathcal{C}$, $\Phi_r = \Theta \circ \Phi \circ \Gamma_r$

$$\begin{array}{rccl} \Phi_r \ : & \mathbb{F}_q^{n_b n_e} & \longrightarrow & \mathcal{C} \cup \{\infty\} \\ & \mathbf{y} & \longmapsto & \Phi_r(\mathbf{y}) = \Theta(\Phi(\Gamma_r(\mathbf{y}))) \end{array}.$$

Remarque III.3 On a défini de cette manière une infinité de décodeurs, cependant un nombre finis d'entre eux seulement sont distincts, en effet

$$\forall\, s \in [r, r+1[\ ,\ \Phi_s = \Phi_r.$$

On a donc exactement $t+1$ décodeurs distincts $\Phi_0, \Phi_1, \ldots, \Phi_t$, où $t = \lfloor \frac{d_b - 1}{2} \rfloor$.

Définition III.2 *Soit d_b un entier strictement positif. Pour tout $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathbb{F}_q^{n_b n_e}$, et tout $\mathbf{y} = (y_1, \ldots, y_{n_e}) \in \mathbb{F}_q^{n_b n_e}$, on définit $D(\mathbf{x}, \mathbf{y})$, par*

$$D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n_e} \min(d_H(x_i, y_i), d_b).$$

Proposition III.3 *D est une distance sur $\mathbb{F}_q^{n_b n_e}$, dominée par la distance de Hamming,*

$$\forall\, \mathbf{x} \in \mathbb{F}_q^{n_b n_e},\ \forall\, \mathbf{y} \in \mathbb{F}_q^{n_b n_e}, \quad D(\mathbf{x}, \mathbf{y}) \leq d_H(\mathbf{x}, \mathbf{y}).$$

preuve : l'application $d : (x, y) \mapsto \min(d_H(x, y), d_b)$ est une distance sur $\mathbb{F}_q^{n_b}$. En effet, on a bien

1. $d(x, y) = 0 \Leftrightarrow \min(d_H(x, y), d_b) = 0 \Leftrightarrow d_H(x, y) = 0 \Leftrightarrow x = y$,
2. $d(x, y) = \min(d_H(x, y), d_b) = d(y, x)$,
3. si $d_H(x, y) \geq d_b$ ou $d_H(y, z) \geq d_b$, alors

$$d(x, y) + d(y, z) \geq d_b \geq d(x, z),$$

sinon $d(x, y) = d_H(x, y)$ et $d(y, z) = d_H(y, z)$, donc

$$d(x, y) + d(y, z) = d_H(x, y) + d_H(y, z) \geq d_H(x, z) \geq d(x, z).$$

Pour $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathbb{F}_q^{n_b n_e}$ et $\mathbf{y} = (y_1, \ldots, y_{n_e}) \in \mathbb{F}_q^{n_b n_e}$, on a que

$$D(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n_e} \min(d_H(x_i, y_i), d_b) = \sum_{i=1}^{n_e} d(x_i, y_i),$$

ce qui entraine que D est une distance. De plus pour tout i, $d(x_i, y_i) \leq d_H(x_i, y_i)$, donc $D(\mathbf{x}, \mathbf{y}) \leq d_H(\mathbf{x}, \mathbf{y})$. □

Proposition III.4 *Soit $\mathbf{y} \in \mathbb{F}_q^{n_b n_e}$. Pour tout entier r, $0 \leq r \leq t = \lfloor \frac{d_b - 1}{2} \rfloor$, on pose*

$$\tilde{\mathbf{y}}_r = \Phi_r(\mathbf{y}) \in \mathcal{C} \cup \{\infty\}.$$

Alors tous les r pour lesquels $D(\tilde{\mathbf{y}}_r, \mathbf{y}) < \frac{d_b d_e}{2}$ (par convention $D(\infty, \mathbf{y}) = \infty$), donnent la même valeur $\tilde{\mathbf{y}}$ de $\tilde{\mathbf{y}}_r$.

On peut alors définir le décodeur de Block-Zyablov de $\mathcal{C}$, noté Ψ :

$$\forall\, \mathbf{y} \in \mathbb{F}_q^{n_b n_e},\ \Psi(\mathbf{y}) = \begin{cases} \tilde{\mathbf{y}}_r & \textit{si } \exists\, r,\ \textit{tel que } D(\tilde{\mathbf{y}}_r, \mathbf{y}) < \frac{d_b d_e}{2} \\ \infty & \textit{sinon} \end{cases} . \tag{III.5}$$

preuve : Si $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathcal{C}$ et $\mathbf{x}' = (x'_1, \ldots, x'_{n_e}) \in \mathcal{C}$ sont distincts, alors d_e au moins de ces n_e composantes sont distinctes et, pour chacune d'elles $\min(d_H(x_i, x'_i), d_b) = d_b$ puisque $x_i, x'_i \in \mathcal{B}$. Donc

$$D(\mathbf{x}, \mathbf{y}) + D(\mathbf{x}', \mathbf{y}) \geq D(\mathbf{x}, \mathbf{x}') \geq d_b d_e,$$

et on ne peut donc pas avoir simultanément $D(\mathbf{x}, \mathbf{y})$ et $D(\mathbf{x}', \mathbf{y})$ inférieurs à $\frac{d_b d_e}{2}$. □

Théorème III.1 *Soit $\mathcal{C}$ le code concaténé de $\mathcal{B}(n_b, k_b, d_b)$ et $\mathcal{E}(n_e, k_e, d_e)$ muni d'un décodeur de Block-Zyablov Ψ. Alors Ψ est un algorithme de décodage de $\mathcal{C}$ borné par $d_b d_e$.*

Autrement dit, pour tout $\mathbf{y} \in \mathbb{F}_q^{n_b n_e}$ et pour tout $\mathbf{x} \in \mathcal{C}$ on a

$$d_H(\mathbf{x}, \mathbf{y}) < \frac{d_b d_e}{2} \Rightarrow \Psi(\mathbf{y}) = \mathbf{x}.$$

preuve : (*due à T. Ericson [35]*)

Soient $\mathbf{x} = (x_1, \ldots, x_{n_e}) \in \mathcal{C}$, $\mathbf{y} = (y_1, \ldots, y_{n_e}), \mathbf{z} = (z_1, \ldots, z_{n_e}) \in \mathbb{F}_q^{n_b n_e}$. On note

1. $\forall\, i,\ 1 \leq i \leq n_e,\quad w_i = d_H(x_i, y_i)$.

2. D la distance de la définition III.2

$$D(\mathbf{y}, \mathbf{z}) = \sum_{i=1}^{n_e} \min(d_H(y_i, z_i), d_b).$$

3. Définissons la fonction $E : \mathbb{R}^* \times [0, \frac{d_b}{2}[\to \{0, 1, 2\}$ par

$$E(w,r) = \begin{cases} 0 & 0 \leq w \leq r \\ 1 & r < w < d_b - r \\ 2 & w \geq d_b - r \end{cases}$$

où $w \in \mathbb{R}^*$ et $r \in [0, \frac{d_b}{2}[$.

Lemme III.1 *Pour tout réel r, $0 \leq r \leq \frac{d_b}{2}$ et pour tout réel $w > 0$, E vérifie les deux propriétés suivantes*

$$\sum_{i=1}^{n_e} E(w_i, r) \geq 2\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_r(\mathbf{y})), \tag{III.6}$$

$$\int_0^{\frac{d_b}{2}} E(w,r)dr = \min(w, d_b). \tag{III.7}$$

preuve : (du lemme)

- Montrons (III.6). Pour tout i distinguons deux cas :
  1. $\delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma_r(y_i))) = 1/2$: dans ce cas $\gamma_r(y_i) = \infty$ car $x_i \neq \infty$, donc $w_i = d_H(x_i, y_i) > r$, sinon on aurait $\gamma_r(y_i) = x_i \neq \infty$. On en conclut que $E(w_i, r) \geq 1$, par définition de E.
  2. $\delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma_r(y_i))) = 1$: dans ce cas on a $\gamma_r(y_i) = \gamma(y_i) \in \mathcal{B}$ et $\gamma(y_i) \neq x_i$, donc par l'inégalité triangulaire

  $$w_i = d_H(y_i, x_i) \geq d_H(\gamma(y_i), x_i) - d_H(y_i, \gamma(y_i)) \geq d_b - r.$$

  En effet $\gamma(y_i) \in \mathcal{B}$, et $x_i \in \mathcal{B}$ étant distincts, on a $d_H(\gamma(y_i), x_i) \geq d_b$ et $d_H(y_i, \gamma(y_i)) \leq r$, par définition de γ_r. Donc $E(w_i, r) = 2$ par définition de E.

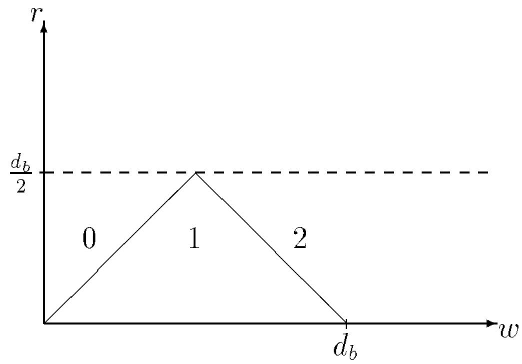
  Dans ces deux cas on a donc toujours

  $$E(w_i, r) \geq 2\delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma_r(y_i))),$$

  ce qui entraine (III.6) puisque par définition

  $$\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_r(\mathbf{y})) = \sum_{i=1}^{n_e} \delta_H(\theta^{-1}(x_i), \theta^{-1}(\gamma_r(y_i))).$$

- L'égalité (III.7) se déduit aisément de la figure suivante qui donne les valeurs de $E(w,r)$ dans le plan (w,r)



□

Supposons maintenant que $d_H(\mathbf{x}, \mathbf{y}) < \frac{d_b d_e}{2}$ et montrons que $\Psi(\mathbf{y}) = \mathbf{x}$. En utilisant les équations (III.6) et (III.7), la définition des w_i et le fait que la distance D est dominée par la distance de Hamming, il vient

$$\begin{aligned} D(\mathbf{x}, \mathbf{y}) &= \sum_{i=1}^{n_e} \min(w_i, d_b), \\ & \sum_{i=1}^{n_e} \int_0^{\frac{d_b}{2}} E(w_i, r)dr, \\ & \int_0^{\frac{d_b}{2}} \sum_{i=1}^{n_e} E(w_i, r)dr \geq d_b \min_r \{\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_r(\mathbf{y}))\}. \end{aligned}$$

Donc

$$\begin{aligned} \frac{d_b d_e}{2} &> d_b \min_r \{\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_r(\mathbf{y}))\}, \\ \frac{d_e}{2} &> \min_r \{\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_r(\mathbf{y}))\} \end{aligned}$$

et il existe un nombre réel r_0 tel que

$$\Delta_H(\Theta^{-1}(\mathbf{x}), \Gamma_{r_0}(\mathbf{y})) < \frac{d_e}{2}.$$

D'après la remarque III.3, on peut supposer que r_0 est un entier $0 \leq r_0 \leq t$. Comme Φ est borné par d_e et $\Theta^{-1}(\mathbf{x}) \in \mathcal{E}$, on a

$$\Phi_{r_0}(\mathbf{y}) = \Theta(\Phi(\Gamma_{r_0}(\mathbf{y}))) = \mathbf{x}$$

et la proposition III.4 nous assure alors que

$$\Psi(\mathbf{y}) = \mathbf{x}.$$

□

On a en fait un résultat plus fort en utilisant la distance D plutôt que la distance de Hamming.