Poids et equivalence des codes lineaires

P.G. Bonneau

INRIA
CENTRE DE ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
BP 105
78153 Le Chesnay Cedex
France
Tél : (1) 39 63 55 11

Rapports de Recherche

N° 519

POIDS ET ÉQUIVALENCE DES CODES LINÉAIRES

Pierre G. BONNEAU

Avril 1986

POIDS ET EQUIVALENCE DES CODES LINEAIRES

Pierre G. Bonneau

INRIA
Domaine de Voluceau
F - 78153 - LE CHESNAY Cedex

RESUME

Sur F^n, où F est un corps fini, nous envisageons les poids W de la forme suivante : $W(x)=\sum_{i=1}^{n}\delta(x_i)$ où $x=(x_1,\cdots x_n)$ et δ est une application $F\dashrightarrow R_+$
telle que $\delta(0)=0$ et $\delta(a)>0$ pour au moins un $a\in F$. Nous montrons l'intérêt de cette notion dans de nombreuses questions de la théorie des codes correcteurs. Puis nous prouvons que les applications semi-linéaires $f:C\dashrightarrow F^n$, qui préservent le poids sur un code linéaire C dans F^n, se prolongent en des applications semi-linéaires définies sur F^n et qui préservent le poids de Hamming sur tout F^n. Si nous supposons de plus que le code linéaire C est projectif, alors un tel prolongement est unique. Il préserve W sur F^n.

ABSTRACT

I investigate weights W of the following kind on F^n, where F is a finite field : $W(x)=\sum_{i=1}^{n}\delta(x_i)$ where $x=(x_1,\ldots x_n)\in F^n$, and $\delta:F\dashrightarrow R_+$ satisfys $\delta(0)=0$ and $\delta(a)>0$ for at least one $a\in F$. I show that this idea is interesting in numerous topics in the theory of error-correcting codes. Then, I prove that, when C is a linear code in F^n, the semi-linear maps $f:C\dashrightarrow F^n$ which preserve W can be extended to semi-linear maps defined everywhere on F^n and which preserve the Hamming weight. If one assumes also that C is projective, then such an extension is unique. It preserves W on F^n.

I) INTRODUCTION

Deux questions ont inspiré cet article : la première concerne le problème de l'équivalence des codes linéaires, la seconde la définition d'un cadre général dans lequel on peut étudier les diverses métriques et compositions de la théorie des codes.

Commençons par ce dernier point qui conditionne tout l'article. Les métriques de Hamming et de Lee sont de la forme suivante : la distance $d(x,y)$ entre deux éléments $x=(x_1, \cdots x_n), y=(y_1,\ldots y_n)$ d'une puissance F^n d'un corps fini F est $d(x,y)=\sum_{i=1}^{n}\delta(x_i,y_i)$ où l'application $\delta:F\longrightarrow R+$ vérifie $\delta(0)=0, \delta(a)>0$ pour au moins un $a\in F$. Ces conditions n'entraînent pas que d est bien une distance, mais les résultats de cet article seront valables dans ce cadre. De plus ce cadre permet d'interpréter très simplement les compositions ("poids généralisés") envisagées par Goldberg dans [3]. Il s'adapte également aux problèmes métriques posées par la démultiplication.

Le second point concerne la notion d'équivalence entre codes. La définition qui nous semble la plus naturelle est la suivante : deux codes C,D dans F^n sont équivalents s'il existe une bijection $f:F^n\longrightarrow F^n$ qui préserve d —*i.e.* $d(f(x),f(y))=d(x,y)$ pour tout $x,y\in F^n$— et telle que $f(C)=D$. Ce point de vue a été adopté dans [2] chapitre 3 pour les métriques de Hamming. Nous avons prouvé qu'il est équivalent à celui de [5] p. 40. Les isométries de Hamming sont en effet de la forme $[\Pi,s]$ suivante, où Π désigne un $n$uplet $(\Pi_1, \cdots \Pi_n)$ de permutations de F et s une permutation de $\{1, \cdots n\}$:

$$[\Pi,s]:(x_1, \cdots x_n)\longrightarrow(y_1,\ldots\ldots,y_n)$$

avec $y_i=\Pi_{s^{-1}(i)}(x_{s^{-1}(i)})$. A la connaissance de l'auteur, un problème analogue, mais où d n'est pas nécessairement la distance de Hamming, n'a jamais été abordé.

Dans le cas où C et D sont supposés linéaires, il est naturel d'exiger de plus que l'application f soit semi-linéaire. Monpetit, dans un article

inédit [6], discute les changements que cela entraîne. Le cas où f est définie sur C seulement a été étudié. Dans le cas des "poids généralisés" de Goldberg, si une telle application est linéaire, alors elle se prolonge sur F^n en une application linéaire qui préserve d sur tout F^n. C'est le résultat principal de [3] qui généralise un résultat antérieur de Mac Williams [4].

Nos conclusions sont essentiellement les suivantes : une application semi-linéaire définie sur un code linéaire C et qui y préserve une application d comme ci-dessus se prolonge sur F^n en une application semi-linéaire qui préserve partout la distance de Hamming. Si de plus nous supposons C projectif, alors un tel prolongement est unique et préserve d partout.

Voici le plan de l'article :

* le paragraphe 2 est divisé en deux sections. La première étudie la structure et des exemples d'applications d. La seconde introduit certaines applications semi-linéaires (celles qui préservent d sur F^n ainsi que cela sera prouvé ultérieurement).

* le paragraphe 3 démontre les conclusions que nous avons annoncées ci-dessus. Il se termine par un contre-exemple.

II) POIDS ET APPLICATIONS ELEMENTAIRES

1) **Poids**

Soit F un corps fini, $n>0$ un entier. La composante d'indice i d'un élément x de F^n est notée x_i. Nous nous intéresserons à des applications $d : F^n \times F^n \dashrightarrow IR_+$ (ensemble des réels ≥ 0) de la forme suivante : $d(x,y)=\sum_{i=1}^{n} \delta(x_i-y_i)$ où δ est une application $F \dashrightarrow IR_+$. Nous supposerons que $\delta(0)=0$ et $\delta(a)>0$ pour au moins un $a \in F$.

Une telle application δ sera appelée **masse**. Nous appellerons $W(x)=\sum_{i=1}^{n} \delta(x_i)$ le **poids** d'un élément x de F^n. Nous adjoindrons δ en

indice quand il sera utile de préciser la masse considérée.

Ainsi que le montrent les exemples suivants, les poids ainsi définis ont un grand intérêt en théorie des codes correcteurs :

a) Un sous-groupe H du groupe multiplicatif $F^\times$ étant choisi, posons :

$$\delta_H(a)=1 \text{ si } x\in H$$

$$\delta_H(a)=0 \text{ si } x\in H$$

Lorsque $H=F^\times$,d est la **distance de Hamming**. Elle jouera un role particulièrement important dans cet article. Nous noterons h la masse dont elle se déduit et identifierons, si le besoin s'en fait sentir, les notions qui lui sont relatives par l'indice h ou le qualificatif "de Hamming".

Dans le cas général, choisissons un système de représentants $1=\alpha_1,\alpha_2,\ldots\alpha_v$ des classes de H dans $F^\times$. La famille $(\delta(\alpha_1^{-1}x),\cdots\delta(\alpha_v^{-1}x))$ n'est autre que le "poids généralisé" défini par Goldberg dans [3] pour un élément x de F^n. Ainsi que cet auteur le fait remarquer, on retrouve, outre le poids de Hamming, des notions très classiques en théorie des codes (voir [1], [5] par exemple) :

* pour $H=\{1\}$ le poids complet

* si l'ordre q de F est impair et $H=\{-1,1\}$, la composition de Lee.

b) Toujours quand $q=2r+1$ est impair et $H=\{-1,1\}$, choisissons un élément α d'ordre r dans $F^\times$ (i.e. un générateur du sous-groupe des carrés de $F^\times$). On voit facilement que le poids de Lee ([1], [5]) d'un élément x de F^n est $\sum_{i=1}^{r} iW(\alpha^{-i}x)$. C'est le poids associé à la masse $a\longrightarrow\sum_{i=1}^{r} i\delta_H(\alpha^{-i}a)$.

c) Supposons que $q=\rho^s$, s entier >0. Alors F est une extension de degré s de son unique sous-corps K d'ordre ρ. Soit $e_1, \cdots e_s$ une base de F en tant que K-espace vectoriel. Un élément a de F étant décomposé en $a=\sum_{k=1}^{s} \alpha_k e_k$ dans cette base, une masse δ_K sur F est définie par $\delta_K(a)=W_h(\alpha)$ où $\alpha=(\alpha_k)_{1\leq k\leq s}$. La distance déduite de la masse δ_K munit F^n d'une structure d'espace métrique isomètre à K^{ns} muni de la distance de Hamming. Le procédé qui consiste à déduire d'un code linéaire de longueur n sur F (i.e. un F- sous espace vectoriel de F^n), un code linéaire de longueur ns sur K en décomposant chacune des composantes d'un mot du F-code suivant la base $e_1, \ldots, e_s$ s'appelle démultiplication (voir [7]).

III) APPLICATIONS ELEMENTAIRES

Considérons une masse δ sur F. Les applications δ-élémentaires que nous introduisons ci-dessous seront caractérisées dans la proposition 1 du prochain paragraphe comme les seules applications semi-linéaires qui préservent sur F^n le poids W associé à δ. Toutes préservent le poids de Hamming.

Une **semi-homothétie** est une application semi-linéaire non nulle $F\longrightarrow F$ (i.e. une application de la forme suivante, où $a\neq 0$ appartient à F et σ au groupe Aut F des automorphismes de F: $x\longrightarrow a\,\sigma(x)$. Une δ-dilatation est une application semi-linéaire $F^n\longrightarrow F^n$ de la forme $(x_1, \cdots x_n)\longrightarrow(f_1(x_1), \cdots f_n(x_n))$ où les f_i sont des semi-homothéties qui préservent $\delta(\delta(f_i(x))=\delta(x)$ pour tout $x\in F$) et ont le même automorphisme associé (une δ-dilatation est donc semi-linéaire). Soient maintenant s un élément du groupe $\sum_n$ des permutations de $\{1,2, \cdots n\}$, $\sigma\in Aut F$, a_i une suite de n éléments non nuls de F. Notons $[s,\sigma,a_1, \cdots a_n]$ l'application $g: F^n\longrightarrow F^n$ définie par $g(x)_{s(i)}=a_i\sigma(x_i)$ pout tout $i\in\{1, \cdots n\}$. Une application δ-élémentaire est une application de cette forme où les semi-homothéties $x\longrightarrow a_i\sigma(x)$ préservent δ. Les h-dilatations et applications h-élémentaires sont appelées plus simplement dilatations et applications élémentaires.

Pour décrire les applications δ-élémentaires lorsque δ est une des

masses envisagées dans les exemples ci-dessous, il suffit de donner une condition nécessaire et suffisante portant sur le couple $(a,\sigma), a \in F^x, \sigma \in AutF$, pour que la semi-homothétie $x \longrightarrow a\sigma(x)$ préserve δ. Nous conservons les notations de chaque exemple. Il est facile de se convaincre que dans l'exemple a), la condition cherchée est : $a \in H$. De même, dans l'exemple b), c'est : $a \in \{-1,1\}$. L'exemple c) est plus difficile à traiter. Remarquons que $(a,b) \longrightarrow \delta(a-b)$ est la distance de Hamming, F étant identifié à K^s par décomposition sur la base $(e_1,\ldots e_s)$. Donc la condition que nous cherchons est équivalente à : pour tout $i \in \{1, \cdots s\}, a\sigma(e_i)$ est de la forme λe_j où $\lambda \in K$. Nous ne l'expliciterons pas plus dans le cas général. Remarquons seulement que les bases normales ([5] p. 120, 4) conduisent à un groupe cyclique d'ordre s d'applications préservant δ : les automorphismes de Galois.

IV) PROLONGEMENT

1) **Conventions et lemme sur les codes linéaires.**

Si C est un code linéaire dans F^n, sa **forme coordonnée** d'indice $i \in \{1, \cdots n\}$, notée l_i, ou $l_{i,C}$ si nécessaire, est la restriction à C de la forme linéaire :

$$F^n \longrightarrow F$$

$$x \longrightarrow x_i$$

Le noyau de cette forme est noté C_i. Puisque la condition "$l_i(x)=0$ pour tout i" entraîne que $x=0$, les l_i engendrent l'espace vectoriel C' dual de C. Nous noterons Z (ou $Z(C)$ si nécessaire) l'ensemble des indices i tels que $l_i=0$. Leur nombre est noté z. Le complémentaire de Z dans $\{1, \cdots n\}$ est noté N, son nombre d'éléments m. On remarquera que $z+m=n$, et que si $i \in N$, alors pour chaque $a \in F$, l'ensemble $C_i(a)$ formé par les éléments x de C tels que $x_i=a$ est un hyperplan affine de C de direction C_i. Son nombre d'éléments est donc q^{k-1}, k désignant la dimension de C. On remarquera également que $Z(C_i)$ a pour éléments les indices j tels que $l_{j,C}$ appartient à la droite vectorielle engendrée par

$l_{i,C}$. Nous noterons $Z_i=Z(C_i)$,$m_i=m(C_i)$ et ainsi de suite.

Le lemme suivant se déduit facilement des remarques précédentes, en considérant la contribution de chaque indice aux sommes envisagées.

Lemme : Soit y un élément de F^n. Avec les notations introduites ci-dessus, et $S=\sum_{a\in F}\delta(a)$

$a)\ \sum_{x\in C} W(y-x)=mSq^{k-1}+q^k\sum_{j\in Z}\delta(y_j)$

$b)$ *Si* $l_i\neq 0$,

$$\sum_{x\in C_i} W(y-x)=m_iSq^{k-2}+q^{k-1}\sum_{j\in Z_i}\delta(y_j)$$

c) Si H est un hyperplan vectoriel de C, et n'est pas un des C_i pour $i\in N$, $\sum_{x\in H} W(y-x)=mSq^{k-2}$.

2) **Les résultats de prolongement**

Considérons une application semi-linéaire $f:C\dashrightarrow F^n$ qui préserve W. Remarquons que f est injective (car si $x\in Kerf$, alors pour tout $\alpha\in F, W(\alpha x)=0$, ce qui entraîne clairement que $x=0$). L'image D de f est donc un code linéaire de dimension k. La formule a), appliquée à $y=0$, montre que C et D ont le même nombre de positions non nulles. En comparant b) et c) appliqués à $y=0$, on voit que parmi les hyperplans vectoriels de C (ou de D), ceux pour lesquels la somme des poids est maximale sont ceux qui ne sont pas de la forme C_i (ou D_i) pour $i\in N$. Un hyperplan de la forme C_i est donc appliqué sur un hyperplan de la forme D_j. La formule b) montre aussi que $m(C_i)=m(D_j)$.

Pour prouver le résultat suivant, on peut donc, quitte à remplacer D par un code qui s'en déduit par une permutation des indices, supposer que $f(C_i)=D_i$ pour tout $i\in\{1,\cdots n\}$.

Proposition 1 : Soit δ une masse, C un code linéaire de longueur n sur F, $f:C\dashrightarrow F^n$ une application semi-linéaire qui préserve W. Alors f se

prolonge en une application élémentaire.

Démonstration : Comme nous l'avons vu précédemment, il suffit de traiter le cas où $f(C_i)=D_i$ pour tout $i\in\{1,\cdots n\}$ (nous posons $D=f(C)$). Dans ce cas f se prolonge en une dilatation. En effet, un indice i étant fixé, $f(x)_i$ ne dépend que de x_i. Supposons que $C\neq\{0\}$.

Soit σ l'automorphisme associé à f. Définissons $f_i=\sigma$ pour $i\in Z$; sinon f_i est l'application telle que $f(x)_i=f_i(x_i)$ pour tout $x\in C$. Il est immédiat que $g:x\longrightarrow(f_1(x_1),\ldots,f_n(x_n))$ est bien une dilatation et que f et g coincident sur C.

Corollaire 1 : Sous les hypothèses de la proposition 1, f préserve le poids de Hamming.

Jusqu'à la fin de ce paragraphe, nous supposerons que C est un code **projectif**, c'est à dire que C est linéaire et que ses formes coordonnées sont linéairement indépendantes.

Proposition 2 : Soient $g=[s,\sigma,a_1,\cdots a_n]$ et $g'=[s',\sigma',a'_1,\cdots a'_n]$ des applications élémentaires qui coincident sur C. Alors $s=s',\sigma=\sigma',a_1=a'_1,\ldots,a_n=a'_n$.

Démonstration : Posons $D=f(C)$ et remarquons que $f^{-1}(D_i)=C_{s^{-1}(i)}=C_{s'^{-1}(i)}$ pour tout indice i. Puisque C est projectif, $s=s'$ et il suffit de traiter le cas où $s=s'=id$. Considérons $a\in F,i\in\{1,\cdots n\},x$ un mot de C tel que $x_i=a$. La composante en i de $f(x)$ est $a_i\sigma(a)=a'_i\sigma'(a)$. Ceci étant vrai pour tout $a,a_i=a'_i$ et $\sigma=\sigma'$.

La conclusion de la proposition 2 montre que $g=g'$. Mais cette proposition prouve de plus que toute application élémentaire s'écrit de manière unique sous la forme $[s,\sigma,a_1,\cdots a_n]$.

Proposition 3 : Toute application semi-linéaire $f:C\longrightarrow F^n$ qui préserve le poids W associé à une masse δ se prolonge en une application élémentaire.

Démonstration : Comme d'habitude, il suffit de traiter le cas où $f(C_i)=D_i$

pour tout indice i. Alors, l'unique prolongement g de f en une application élémentaire est une dilatation (ce prolongement existe d'après la proposition 1, c'est une dilatation d'après la démonstration de la proposition 2). En notant $g=[id,\sigma,a_1,\cdots a_n]$, il reste à voir que les applications $g_i: a \longrightarrow a_i\sigma(a)$ préservent δ. Pour ce faire, on applique l'assertion b) du lemme à un indice i quelconque. Puisque C, et donc son image D, sont projectifs, $Z(C_i)=Z(D_i)=\{i\}$. Soient $a\in F, i\in\{1,\cdots n\}, y$ un mot de C tel que $y_i=a$.

$$\sum_{x\in C_i} W(y-x)=(n-1)q^{k-2}S+q^{k-1}\delta(a)$$

$$=\sum_{x\in C_i} W(g(y)-g(x))$$

$$=\sum_{x\in D_i} W(g(y)-x)$$

$$=(n-1)q^{k-2}S+q^{k-1}\delta(g_i(a))$$

On obtient bien $\delta(a)=\delta(g_i(a))$.

3) **Commentaires.**

Dans [3], Goldberg considère des applications linéaires f qui préservent sur un code linéaire C sa notion de "poids généralisé" (voir l'exemple a) ci-dessus). Or une application linéaire qui préserve le "poids généralisé" associé à un sous-groupe H de $F^{\times}$ préserve δ_H et réciproquement. Goldberg conclut qu'une telle application se prolonge en une application δ_H-élémentaire et linéaire. Dans le cas des corps premiers et du poids de Hamming, ce résultat avait déjà été prouvé par Mac-Williams dans [4]. Nous n'avons pas retrouvé le résultat de Goldberg dans toute sa généralité, car nous avons supposé que C est projectif dans la proposition 3.

En revanche, la proposition 1 est valable pour des poids beaucoup plus généraux que ceux qui ont été considérés jusqu'à présent, et elle s'applique aux applications semi-linéaires et pas seulement linéaires. Les problèmes d'unicité des prolongements n'ont jamais été abordés.

4) **Un contre-exemple.**

Nous montrons que l'hypothèse de projectivité de la proposition 3 est utile si aucune restriction n'est faite sur la masse considérée.

Prenons $q=5$ et choisissons un élément primitif α de $F^{\times}$. Considérons la masse δ définie par $\delta(1)=\delta(-\alpha)=1, \delta(-1)=\delta(\alpha)=0$. Notons encore :

$C=\{(x,\alpha x,-x,-\alpha x), x\in F\}$

$D=\{(x,x,-x,-x), x\in F\}$

Le poids de chaque élément non nul de C et D est 2 (en effet $W(a)+W(-a)=1$ pour tout $a\in F^{\times}$). Prouvons qu'ils ne se déduisent pas l'un de l'autre par une application δ-élémentaire. Si tel était le cas, le code $C'=\{(x,\alpha x), x\in F\}$ qui s'obtient à partir de C en supprimant les 3e et 4e coordonnées, se déduirait par une application δ-élémentaire d'un code qui s'obtient à partir de D en supprimant deux coordonnées. Ces derniers codes sont soit $\{(x,x), x\in F\}$, soit $\{(x,-x), x\in F\}$. Leur distribution des poids est différente de celle de C', contradiction.

BIBLIOGRAPHIE

[1] Berlekamp E.R. "Algebraic Coding Theory" McGraw-Hill (1968)

[2] Bonneau P. "Codes et Combinatoire"
Thèse de troisième cycle - Université Paris 6 (1984)

[3] Goldberg D. "A generalized Weight for Linear Codes and a Witt-Mac Williams Theorem" J.C.T. Series A 29 (1980) p. 363-367

[4] Mac Williams F.J. "Combinatorial Problems of Elementary Group Theory"
Ph.D. Thesis, Harvard University (1962)

[5] Mac Williams F.J. et Sloane N.J.A. "The Theory of Error-Correcting Codes" North-Holland, third printing (1981)

[6] Montpetit A. "Note sur la Notion d'Equivalence entre Deux Codes" Manuscrit inédit (1985)

[7] Wolfmann J. "Différents Aspects de la Démultiplication des Codes" Traitement du Signal, Volume 1, No 2 hors série (1984)

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique