Codes pseudo-lineaires

C. Carlet

INRIA

UNITE DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P. 105
78153 Le Chesnay Cedex
France
Tel (1) 39 63 55 11

Rapports de Recherche

N° 1334

Programme 1
Programmation, Calcul Symbolique
et Intelligence Artificielle

CODES PSEUDO-LINEAIRES

Claude CARLET

Novembre 1990

RR_1334

CODES PSEUDO-LINEAIRES

PSEUDO-LINEAR CODES

Claude Carlet[1]
Université d'Amiens, France

ABSTRACT

We introduce a new class of binary codes, called pseudo-linear, whose weight enumerators are changed by the Mac Williams transform into the weight enumerators of some codes, called their pseudo-dual codes.
We deduce a new proof - and an explanation - of the formal duality between the Kerdock codes and the generalized Preparata codes of same lengths, and between the Delsarte-Goethals codes $DG(m,(m-2)/2)$ and the Goethals codes $T(m)$.

RESUME

Nous introduisons une nouvelle classe de codes binaires : celle des codes pseudo-linéaires. Le transformé de Mac Williams du polynôme énumérateur des poids d'un code pseudo-linéaire est le polynôme des poids d'un code, son pseudo-dual. Nous en déduisons une nouvelle preuve - et une explication - de la dualité formelle des codes deKerdock et de Preparata généralisés de même longueur d'une part, et des codes $DG(m,(m-2)/2)$ de Delsarte-Goethals et $T(m)$ de Goethals d'autre part.

[1] Chercheur Extérieur - Programme 1
INRIA Bat 10, Domaine de Voluceau BP 105, 78153 Le Chesnay, France

INTRODUCTION

Let n be a positive integer. We denote by $< , >$ the usual dot product on F^n, where $F=\{0, 1\}$.
A binary code of length n is a subset of F^n. Its weight enumerator :

$W_C(X, Y) = \sum_{a \in C} X^{n-w(a)} Y^{w(a)}$, where w(a) denotes the Hamming weight of the word a,
satisfies the following equality :
$W_C(X+Y, X-Y) = \sum_{b \in F^n} \sum_{a \in C} (-1)^{<a, b>} X^{n-w(b)} Y^{w(b)}$ (Mac Williams cf [12]) .

Its distance enumerator , $D_C(X, Y) = \frac{1}{|C|} \sum_{a_1, a_2 \in C} X^{n-w(a_1+a_2)} Y^{w(a_1+a_2)}$, satisfies :

$$D_C(X+Y, X-Y) = \frac{1}{|C|} \sum_{b \in F^n} \left(\sum_{a \in C} (-1)^{<a, b>} \right)^2 X^{n-w(b)} Y^{w(b)} .$$

C is linear if and only if for any element b of F^n, the sum $\sum_{a \in C} (-1)^{<a, b>}$ is equal either to 0, or to the cardinal of C :
the condition is necessary since the functions $a \rightarrow < a , b >$ are then linear forms on C, and it is sufficient since, by the inverse formula of the Fourier transform, we have, denoting by $C^{\perp}$ the linear space $\{b \in F^n / \forall a \in C, < a , b > = 0 \}$, and by 1_C the characteristical function of C :

$$\left(\forall b \in F^n, \sum_{a \in F^n} 1_C(a) \ (-1)^{<a, b>} = |C| 1_{C^{\perp}}(b) \right) \Rightarrow$$

$$\left(\forall a \in F^n, 1_C(a) = \frac{|C|}{2^n} \sum_{b \in F^n} 1_{C^{\perp}}(b) \ (-1)^{<a, b>} = \frac{|C||C^{\perp}|}{2^n} 1_{C^{\perp\perp}}(a) \right) \Rightarrow \left(C = C^{\perp\perp} \right).$$

We have then :
$W_C = D_C$, $W_{C^{\perp}} = D_{C^{\perp}}$, $W_C(X+Y, X-Y) = |C| W_{C^{\perp}}(X, Y)$ (Mac Williams identity)
and : $D_C(X+Y, X-Y) = |C| D_{C^{\perp}}(X, Y)$.

There are examples of non linear codes C and C° such that the relation :
$D_C(X+Y, X-Y) = |C| D_{C^{\circ}}(X, Y)$
is still valid (cf [9], [12] ch 15).

We will say then that the codes C and C° are formally dual.

The most famous is the case of the Kerdock codes and the Preparata codes of same length : Semakov and Zinov'ev proved their formal duality in 1969.
But, as Paul Camion and J.H.Van Lint notice it in [2] and [15], their proof does not explain completely why $\frac{1}{|C|} D_C(X+Y, X-Y)$ belongs to $\mathbb{N}[X, Y]$ when C is a Kerdock code (respectively a Preparata code), and, *a fortiori* , why it is the distance enumerator of the Preparata code (respectively the Kerdock code) of same length.

J. M. Goethals [9] gives another example of nonlinear formally dual codes :
the Delsarte-Goethals codes $\mathcal{DG}(m,(m-2)/2)$ and the Goethals codes $\mathcal{T}(m)$.
His result, more difficult than the previous one, is proved by the same general way.

Paul Camion [2] asks for a new analytic proof of Zinov'ev and Semakov's result, and wonders if there exists a new kind of duality between (nonlinear) codes which would explain the phenomenon.

W.Kantor [10] proves that the generalized Preparata codes defined in [1] are inequivalent and concludes that the formal duality between the Kerdock codes and the Preparata codes is "merely a coïncidence".

We introduce a new class of binary codes : a code C is called pseudo-linear if there exists a linear binary code C ' of same length , a set of permutations τ_α on $\{1, \dots , n\}$ ($\alpha \in A$), and a permutation ϕ on F^n such that , for any $b \in F^n$, denoting by b_α the element $(b_{\tau_\alpha(1)}, \dots, b_{\tau_\alpha(n)})$:

1) $\phi^{-1}(b_\alpha)$ has same weight as $\phi^{-1}(b)$

2) $$\sum_{a \in C,\ \alpha \in A} (-1)^{<a_\alpha, b>} = \sum_{a' \in C',\ \alpha \in A} (-1)^{<a'_\alpha, \phi(b)>} .$$

We prove that the weight enumerators of the codes C and $\phi^{-1}(C'^{\perp})$ satisfy then the Mac williams identity .
We obtain a new analytic proof of the result of Semakov and Zinov'ev (respectively Goethals) by proving that there exists codes which :

- have same weight enumerators as the Kerdock codes (respectively the $\mathcal{DG}(m,(m-2)/2)$ codes),
- are pseudo-linear,
- admit the generalized Preparata codes of same lengths (respectively the $\mathcal{T}(m)$ codes) as formally dual codes.

I PSEUDO-LINEAR CODES

DEFINITION 1

Two binary codes of same length C and C° are called formally dual if their distance enumerators D_C and D_{C° satisfy the following relation :

$$D_C(X+Y, X-Y) = |C| D_{C^\circ}(X, Y) .$$

Remark

1) if n is the length of C and C°, then $|C^{\circ}| = \frac{2^n}{|C|}$ (apply the equality with X=Y=1)

2) the previous definition is symmetric : apply the equality where X and Y are respectively replaced by X+Y and X-Y.

DEFINITION 2

A binary code C is called pseudo-linear if there exists a binary linear code C' of same length n and same cardinal, a set of permutations τ_α on {1, ... , n}(where α ranges over a set A) , and a permutation ϕ on F^n such that , for any $b = (b_1 , ..., b_n) \in F^n$, denoting by b_α the element $(b_{\tau_\alpha(1)} , ..., b_{\tau_\alpha(n)})$:

1) $\phi^{-1}(b_\alpha)$ has same weight as $\phi^{-1}(b)$

2) $$\sum_{a \in C \, , \alpha \in A} (-1)^{<a_\alpha , b>} = \sum_{a' \in C' , \alpha \in A} (-1)^{<a'_\alpha , \phi (b)>} .$$

ϕ is then called an associated permutation , and C ' an associated linear code .

Remark
Linear codes are among pseudo-linear codes those for which A may contain only one element since a binary code C is linear if and only if for any $b \in F^n$, the sum

$\sum_{a \in C} (-1)^{< a, b >}$ is equal either to the cardinal of C or to 0 .

THEOREM

Let C be a pseudo-linear code, ϕ an associated permutation, and C ' an associated linear code for C, then the weight enumerators of C and $\phi^{-1}(C'^{\perp})$ satisfy the Mac Williams identity : $W_C(X+Y, X-Y) = |C| W_{\phi^{-1}(C'^{\perp})}(X, Y)$.

Proof:

For any α, τ_α is a permutation on {1, ... , n}, so the code $C_\alpha = \{a_\alpha , a \in C\}$ has same weight distribution as C, and we have :

$W_C(X,Y) = \frac{1}{|A|} \sum_{\alpha \in A} W_{C_\alpha}(X,Y)$ and therefore :

$$W_C(X+Y, X-Y) = \frac{1}{|A|} \sum_{a \in C, \, \alpha \in A} \sum_{b \in F^n} (-1)^{< a_\alpha , b >} X^{n-w(b)} Y^{w(b)} .$$

Using property 2 of ϕ, we obtain :

$$W_C(X+Y, X-Y) = \frac{1}{|A|} \sum_{a' \in C',\, \alpha \in A} \sum_{b \in F^n} (-1)^{\langle a'_\alpha,\, \phi(b) \rangle} X^{n-w(b)} Y^{w(b)}$$

$$= \frac{1}{|A|} \sum_{a' \in C',\, \alpha \in A} \sum_{b \in F^n} (-1)^{\langle a'_\alpha,\, b \rangle} X^{n-w(\phi^{-1}(b))} Y^{w(\phi^{-1}(b))}$$

$$= \frac{1}{|A|} \sum_{a' \in C',\, \alpha \in A} \sum_{b \in F^n} (-1)^{\langle a'_\alpha,\, b_\alpha \rangle} X^{n-w(\phi^{-1}(b_\alpha))} Y^{w(\phi^{-1}(b_\alpha))}$$

(since the mapping $b \rightarrow b_\alpha$ is a permutation on F^n)

$$= \frac{1}{|A|} \sum_{a' \in C',\, \alpha \in A} \sum_{b \in F^n} (-1)^{\langle a'_\alpha,\, b_\alpha \rangle} X^{n-w(\phi^{-1}(b))} Y^{w(\phi^{-1}(b))}$$

(since $w(\phi^{-1}(b_\alpha)) = w(\phi^{-1}(b))$)

$$= \sum_{a' \in C'} \sum_{b \in F^n} (-1)^{\langle a',\, b \rangle} X^{n-w(\phi^{-1}(b))} Y^{w(\phi^{-1}(b))}$$

$$= |C|\ W_{\phi^{-1}(C'^{\perp})}(X,Y) \quad \left(\text{since } \sum_{a' \in C'} (-1)^{\langle a', b \rangle} \text{ is equal to :}\right.$$

$|C'| = |C|$ if $b \in C'^{\perp}$ and 0 otherwise).

DEFINITION 3

$\phi^{-1}(C'^{\perp})$ is called pseudo-dual to C.

Remark

if ϕ and $C'^{\perp}$ satisfy the following property :

$\forall\, b \in C'^{\perp}, \exists\, \alpha \in A / \forall\, b' \in C'^{\perp}$, $(\phi^{-1}(b) + \phi^{-1}(b'))_\alpha \in \phi^{-1}(C'^{\perp})$,

then $\phi^{-1}(C'^{\perp})$ is distance invariant . Its weight and distance enumerators are then equal .

II KERDOCK AND PREPARATA CODES

From now on, we consider codes which are sets of boolean functions on a Galois field $G = GF(2^m)$. This corresponds to the point of view on codes that we had in the previous paragraph since if we write $G = \{x_1, \ldots, x_n\}$ (with $n = 2^m$), a boolean function f on G

can be identified with the element a = ($f(x_1)$, ... , $f(x_n)$) of F^n .

If a word a corresponds to a function f, then the word a_α will correspond to the function $f \circ \tau_\alpha$ where τ_α is now considered a permutation on G.

Let us recall that for m even ≥ 4, the Kerdock code K_m of length 2^m is the union of the Reed-Muller code of order 1, R(1, m), with $(2^{m-1}-1)$ cosets of R(1, m), all constituted of bent functions belonging to R(2, m) (a function f of R(2, m) is bent if and only if its associated symplectic form :
$(u, v) \in G^2 \rightarrow f(0) + f(u) + f(v) + f(u+v)$ is non-degenerated).
Moreover, K_m is distance invariant .

In the following , the Galois field G= $GF(2^m)$ is identified with the cartesian product : $GF(2^{m'})xF = G'xF$ where m'=m-1, so that R(1, m) and R(2, m) are considered as sets of boolean functions on G'xF .
The dot product between two such functions is :

$$< f, g> = \sum_{x \in G'} \big(f(x,0)\, g(x,0) + f(x,1)\, g(x,1)\big).$$

Let j be an integer prime to m'.
The generalized Preparata code $\mathcal{P}_{m,j}$ is the set of all functions g on G'xF such that (cf [1]) :
(i) the supports of the functions on G' : $x \rightarrow g(x,0)$ and $x \rightarrow g(x,1)$ have

even cardinals, and : $\sum_{x \in G'/g(x,0) = 1} x = \sum_{x \in G'/g(x,1) = 1} x$

(ii) $$\sum_{x \in G'/g(x,0)+g(x,1) = 1} x^{2^j+1} = \left(\sum_{x \in G'/g(x,1) = 1} x \right)^{2^j+1}.$$

$\mathcal{P}_{m,j}$ is distance invariant.

tr denotes the trace function from $GF(2^{m'})$ to F.

Lemma 1

Let j be a positive integer prime to m' .
Let E_j be the set of all functions f_u defined on $G = GF(2^{m'})xF$ by :
$f_u(x,\varepsilon) = tr[(ux)^{2^j+1} + \varepsilon ux]$, where u ranges over G'.
Then the code $C_j = E_j + R(1, m)$ has same weight distribution as K_m .

Proof :

f_0 is the zero function, so $f_0 + R(1, m) = R(1, m)$.

For $u \neq 0$, f_u belongs to R(2, m) and its associated symplectic form (cf [12] ch 15) :
$((x,\varepsilon),(y,\eta)) \rightarrow tr[ux(uy)^{2^j} + uy(ux)^{2^j} + \varepsilon uy + \eta ux] = tr([(ux)^{2^{m'-j}} + (ux)^{2^j} + \varepsilon]uy + \eta ux)$

is non-degenerated since :

1) its kernel is the linear space :
$\{(x,\varepsilon)\in GF(2^{m'})xF / (ux)^{2^{m'-j}}+ (ux)^{2^j}+\varepsilon=0$ and $tr(ux)=0\}$
$= \{(x,\varepsilon)\in GF(2^{m'})xF / (ux)^{2^{m'-j}}+ (ux)^{2^j}= \varepsilon=0$ and $tr(ux)=0\}$ (since $tr((ux)^{2^{m'-j}}+ (ux)^{2^j})=0$)
$= \{(x,\varepsilon)\in GF(2^{m'})xF / (ux)+ (ux)^{2^{2j}}= \varepsilon=0$ and $tr(ux)=0\}$
$= \{(x,\varepsilon)\in GF(2^{m'})xF / (ux) = 0$ or $(ux)^{2^{2j-1}}= 1, \varepsilon=0$ and $tr(ux)=0\}$;

2) 2j beeing prime to m', $2^{2j}-1$ is prime to $2^{m'}-1$, and the mapping $x \rightarrow x^{2^{2j}-1}$ is one to one. So, the kernel is equal to :

$\{(x,\varepsilon)\in GF(2^{m'})xF / ux=0$ or $1, \varepsilon=0$ and $tr(ux)=0\}= \{(0,0)\}$.

Therefore, if $u \neq 0$, all the elements of $f_u+ R(1, m)$ are bent functions, and C has same weight distribution as K_m.

PROPOSITION 1

For any j prime to m', the code C_j is pseudo-linear and $\mathcal{P}_{m,j}$ is pseudo-dual to C_j. .

Proof :

Let E'_j be the set of all the functions f'_u defined on $G = GF(2^{m'})xF$ by :

$f'_u(x,\varepsilon) = tr[(ux)^{2^j+1}]$, where u ranges over G'.
Let C'_j be the code equal to : $E'_j+ R(1, m)$.
u^{2^j+1} ranges over all G' when u ranges over G', therefore E'_j is the set of all functions of the type : $(x,\varepsilon) \rightarrow tr[vx^{2^j+1}]$, $(v\in G')$, and C'_j is a linear code .

Let τ_α , $(\alpha\in G')$, be the permutation on G : $(x, \varepsilon) \rightarrow (x + \varepsilon\,\alpha, \varepsilon)$ equal to $(x, 0)$ if $\varepsilon = 0$, and $(x + \alpha, 1)$ if $\varepsilon = 1$.

Let us recall (cf [12] , [5]) that $R(1, m)^\perp = R(m-2, m)$ is the set of all boolean functions on G'xF such that the supports of the functions on G' : $x \rightarrow g(x,0)$ and $x \rightarrow g(x,1)$ have even cardinals, and that : $\sum_{x \in G'/g(x,0) = 1} x = \sum_{x \in G'/g(x,1) = 1} x$.

If a boolean function g on G does not belong to $R(1, m)^{\perp}$,we have (cf [9]) :

$$\sum_{f \in C, \alpha \in G'} (-1)^{<f \circ \tau_\alpha, g>} = \sum_{f' \in C', \alpha \in G'} (-1)^{<f' \circ \tau_\alpha, g>} = 0 .$$

If g belongs to $R(1, m)^{\perp}$, then :

$$\sum_{f \in C, \alpha \in G'} (-1)^{<f \circ \tau_\alpha, g>} = \sum_{u \in G', \alpha \in G'} \sum_{h \in R(1, m)} (-1)^{<f_u \circ \tau_\alpha + h, g>}$$

$$= |R(1, m)| \sum_{u \in G', \alpha \in G'} (-1)^{<f_u \circ \tau_\alpha, g>}$$

since we know that $R(1, m) \circ \tau_\alpha = R(1, m)$ and that R(1, m) is linear.

Lemma 2

Let $\{f_u , u \in A\}$ be a set of elements of R(2,m), h_u and k_u the functions on G' such that: $f_u(x,\varepsilon) = h_u(x) + \varepsilon k_u(x)$ ($h_u \in R(2,m')$, $k_u \in R(1,m')$) , and F_u the kernel of the symplectic form φ_u associated with h_u . Let τ_α be the permutation on G : $(x,\varepsilon) \rightarrow (x+\varepsilon\alpha,\varepsilon)$.

Then, for any element g of $R(1,m)^{\perp}$, if we denote by λ_g the sum $\sum_{x \in G' / g(x,1) = 1} x$,

we have :

$$\sum_{u \in A , \alpha \in G'} (-1)^{<f_u \circ \tau_\alpha, g>} = |G'| \sum_{u \in A / \lambda_g \in F_u} (-1)^{<f_u, g>} .$$

Proof :

Let $g_0(x) = g(x,0)$ and $g_1(x) = g(x,1)$.

We have , denoting by t_α the translation on G' of vector α :

$$\sum_{u \in A,\, \alpha \in G'} (-1)^{<f_u \circ \tau_\alpha, g>} = \sum_{u \in A,\, \alpha \in G'} (-1)^{<h_u,\, g_0> + <h_u \circ t_\alpha,\, g_1> + <k_u,\, g_1>}$$

$$\sum_{u \in A,\, \alpha \in G'} (-1)^{<h_u,\, g_0 + g_1> + \varphi_u(\alpha,\, \lambda_g) + <k_u,\, g_1>} = |G'| \sum_{u \in A / \lambda_g \in F_u} (-1)^{<f_u,\, g}$$

(since $\varphi_u(\alpha, \lambda_g) = \sum_{x \in /g_1(x)=1} \varphi_u(\alpha, x) = \sum_{x \in /g_1(x)=1} \left(h_u(0) + h_u(\alpha) + h_u(x) + h_u(x+\alpha) \right) =$

$< h_u + h_u \circ t_\alpha,\, g_1 >$ and since the linear form $\alpha \to \varphi_u(\alpha, \lambda_g)$ is either null or balanced on G')

L

Here we have :

$$h_u(x) = tr\left((ux)^{2^j+1}\right),\ \varphi_u(x,y) = tr\left(u^{2^j+1}\left(x^{2^j}y + y^{2^j}x\right)\right) = tr\left(uy\left((ux)^{2^j} + (ux)^{2^{m-j}}\right)\right)$$

$F_u = \left\{0, \frac{1}{u}\right\}$ if $u \neq 0$, and G' if $u = 0$.

Therefore :

$$\sum_{f \in C_j,\, \alpha \in G'} (-1)^{<f \circ \tau_\alpha,\, g>} =$$

$$|R(1, m)|\ |G'| \sum_{u \in G'/\lambda_g u = 0 \text{ or } 1} (-1)^{tr\left(\sum_{x \in G'/g(x,0)+g(x,1)=1} (ux)^{2^j+1} + \sum_{x \in G'/g(x,1)=1} (ux)\right)}.$$

For the same reasons :

$$\sum_{f' \in C'_j,\, \alpha \in G'} (-1)^{<f' \circ \tau_\alpha,\, g>} =$$

$$|R(1, m)||G'| \sum_{u \in G'/\lambda_g u = 0 \text{ or } 1} (-1)^{tr\left(\sum_{x \in G'/g(x,0)+g(x,1)=1} (ux)^{2^j+1}\right)}.$$

Let k be any element of $R(1, m)^{\perp}$ such that :

$$\sum_{x \in G'/k(x,0)=1} x^{2^j+1} = 1 \text{ and } \forall\, x \in G',\ k(x,1)=0.$$

For any element λ of G', different from 0, let k_λ be defined by : $k_\lambda(x,\varepsilon) = k(x/\lambda,\varepsilon)$.
We have :

$$\sum_{x\in G'/\, k_\lambda(x,0)\,=\,1} x^{2^j+1} = \lambda^{2^j+1} \text{ and } \forall\, x\in G',\ k_\lambda(x,1)=0.$$

We can take : $\phi(g) = g$ if $\lambda_g = 0$ or if $g \notin R(1, m)^\perp$, and $\phi(g) = g + k_{\lambda_g}$ otherwise since the relation :

$$\sum_{f\in C_j,\ \alpha\in G'} (-1)^{<f\circ\tau_\alpha,\ g>} = \sum_{f'\in C'_j,\ \alpha\in G'} (-1)^{<f'\circ\tau_\alpha,\ \phi(g)>}$$

stands : if $g \in R(1, m)^\perp$ and $\lambda_g \neq 0$,

$$\lambda_g u = 1 \Rightarrow \sum_{x\,\in\, G'/g(x,1)=1} ux = 1 = \sum_{x\,\in\, G'/k_{\lambda_g}(x,0)+k_{\lambda_g}(x,1)\,=1} (ux)^{2^j+1} .$$

So, condition 2 of the definition is satisfied by ϕ.
ϕ is a permutation : $\phi^{-1} = \phi$.
Condition 1 is clearly fullfilled since : $(\forall\, x \in G', k(x,0) = 0) \Rightarrow (\phi(g\circ\tau_\alpha) = \phi(g)\circ\tau_\alpha)$.
So, all the conditions of the definition are fullfilled.

Let us prove now that $\phi^{-1}(C'^{\perp}_j) = \phi(C'^{\perp}_j)$ is equal to the generalized Preparata code $\mathcal{P}_{m,j}$.
Condition (i) of the definition of $\mathcal{P}_{m,j}$ is equivalent to : $g \in R(m-2, m)$.

$C'^{\perp}_j$ is the set of all the functions $g \in R(m-2, m)$ such that : $\forall u \in G', <f'_u, g> = 0$, or, equivalently :

$$\forall\, u \in G',\ \mathrm{tr}\Big(\sum_{x\,\in\, G'/g(x,0)+g(x,1)\,=\,1} (ux)^{2^j+1} = 0\Big),$$

$$\forall\, v \in G',\ \mathrm{tr}\Big(v \sum_{x\,\in\, G'/g(x,0)+g(x,1)\,=\,1} x^{2^j+1}\Big) = 0 ,$$

$$\sum_{x\,\in\, G'/g(x,0)+g(x,1)\,=\,1} x^{2^j+1} = 0 .$$

For any $g \in R(m-2, m)$ such that $\lambda_g = 0$, g belongs to $C'^{\perp}_j$ if and only if g belongs to $\mathcal{P}_{m,j}$.
Any $g \in R(m-2, m)$ such that $\lambda_g \neq 0$ belongs to $C'^{\perp}_j$ if and only if $\phi(g)$ belongs to $\mathcal{P}_{m,j}$ since :

$$\sum_{x \in G'/\phi(g)(x,0)+\phi(g)(x,1)=1} x^{2^j+1} = \sum_{x \in G'/g(x,0)+g(x,1)=1} x^{2^j+1} + \lambda_g{}^{2^j+1}.$$

This finishes the proof.

Notice that $C'_j{}^{\perp}$ and ϕ satisfy the condition stated in the remark which follows the theorem :

If g and g' are two elements of $C'_j{}^{\perp}$, then we have :

$\phi(\phi^{-1}(g) + \phi^{-1}(g')) \circ \tau_{\lambda_g} = \phi(\phi(g) + \phi(g')) \circ \tau_{\lambda_g} =$

$g + g \circ \tau_{\lambda_g} + g' + g' \circ \tau_{\lambda_g} + k\lambda_g + k\lambda_{g'} + k\lambda_g + \lambda_{g'}$

and it is easy to check that this function belongs to $C'_j{}^{\perp}$.

Since the Kerdock and the Preparata codes are both distance invariant, we deduce :

COROLLARY 1

The Kerdock codes and the generalized Preparata codes of same length are formally dual.

III DELSARTE-GOETHALS AND GOETHALS CODES

Another example of nonlinear formally dual codes (cf [8], [9]) is the case of Delsarte-Goethals

$\mathfrak{DG}(m,(m-2)/2)$ and Goethals $\mathfrak{T}(m)$ codes :

$m = 2t+2 \geq 4$, $\mathfrak{T}(m)$ is the intersection of $\mathfrak{P}_{m,t}$ and $\mathfrak{P}_{m,t-1}$ and $\mathfrak{DG}(m,t)$ is the set of all boolean functions on G of the type :

$$(x,\varepsilon) \rightarrow tr\left(\sum_{j=1}^{t} (ux)^{2^j+1} + vx^3 + \varepsilon ux\right) + l(x,\varepsilon)$$

where u and v range over G', and l over R(1,m). The symplectic form associated with any of these functions (with $u \neq 0$ or $v \neq 0$) has a rank at least equal to 2t .
Moreover, the symplectic form associated with the sum of two different functions of this type

has a rank at least equal to 2t , and $\mathfrak{DG}(m,t)$ has as many elements as any code having this property (ie it is optimal, just as the Kerdock code). The distance distribution of such a code is
fixed by this property (cf [8]).
Both codes are distance invariant.

Lemma 3

For any u and v in G', let $f_{u,v}$ be the function on G defined by :

$\forall (x,\varepsilon) \in G, f_{u,v}(x,\varepsilon) = tr(ux^{2^t+1} + vx^{2^{t-1}+1}) + \varepsilon h_{u,v}(x)$

where $h_{u,v}$ is any linear form on G' whose restriction to the kernel of the symplectic form

$\varphi_{u,v}$ associated with the function $f_{u,v} : (x,\varepsilon) \rightarrow tr(ux^{2^t+1} + vx^{2^{t-1}+1})$ takes the same

values as $f'_{u,v}$ *itself .*

Then the code $D = \{ f_{u,v} \ , u,v \in G' \} + R(1,m)$ *has same weight distribution as* $DG(m,t)$.

Proof :

Notice that there exists such an $h_{u,v}$ since we know that the restriction of a quadratic function
to the Kernel of its associated symplectic form is affine (here, linear).

We have :

$$\varphi_{u,v}(x,y) = tr[u(x\,2^t y + y\,2^t x) + v(x\,2^{t-1} y + y\,2^{t-1} x)]$$
$$= tr[(u\ x\,2^t + (ux)\,2^{m'-t} + v\ x\,2^{t-1} + (vx)\,2^{m'-t+1})y]$$
$$= tr[(u\ x\,2^t + (ux)\,2^{t+1} + v\ x\,2^{t-1} + (vx)\,2^{t+2})y]$$

and the kernel of $\varphi_{u,v}$ is the linear space :

$$\{x \in G' / u\ x\,2^t + (ux)\,2^{t+1} + v\ x\,2^{t-1} + (vx)\,2^{t+2} = 0\} =$$
$$\{x \in G' / u\,2^{t+2} x\,2 + (ux)\,2^2 + v\,2^{t+2}\ x + (vx)\,2^3 = 0\} =$$
$$\{x \in G' / (vx)\,8 + (ux)\,4 + u\,2^{t+2} x\,2 + v\,2^{t+2}\ x = 0\} .$$

Therefore, the dimension of this kernel is at most 3 and the rank of $\varphi_{u,v}$ is at least equal to m'-3 = m-4.

Let $\psi_{u,v}$ the symplectic form associated with $f_{u,v}$.
We know (cf Delsarte-Goethals [8])) that $\psi_{u,v}$'s rank is equal to $\varphi_{u,v}$'s one if $h_{u,v}$ takes always the 0 value on the kernel of $\varphi_{u,v}$, or, equivalently (cf [5]) if the function
$f'_{u,v}$ is not balanced on G'. Otherwise $\psi_{u,v}$'s rank is equal to $\varphi_{u,v}$'s one plus 2.

Let a, b, c, and d be the cardinals respectively of the sets :
$\{(u,v) \in G'^2$ / rank $\psi_{u,v}$ = m, rank $\varphi_{u,v}$= m-2$\} = \{(u,v) \in G'^2$ / $f'_{u,v}$balanced, rank $\varphi_{u,v}$= m-2$\}$
$\{(u,v) \in G'^2$/ rank $\psi_{u,v}$=m-2, rank $\varphi_{u,v}$= m-2$\} = \{(u,v) \in G'^2$/ $f'_{u,v}$not balanced, rank $\varphi_{u,v}$= m-2$\}$
$\{(u,v) \in G'^2$ / rank $\psi_{u,v}$=m-2 , rank $\varphi_{u,v}$=m-4$\} = \{(u,v) \in G'^2$ / $f'_{u,v}$balanced , rank $\varphi_{u,v}$= m-4$\}$
$\{(u,v) \in G'^2$ / rank $\psi_{u,v}$=m-4 , rank $\varphi_{u,v}$=m-4$\} = \{(u,v) \in G'^2$ / $f'_{u,v}$not balanced, rank $\varphi_{u,v}$=m-4$\}$.

According to [9], table IV, d is equal to 0.

We want to prove that the rank distribution of the set $\{\psi_{u,v}, u,v \in G'\}$ is the same as the rank distribution of the set of the symplectic forms $\rho_{u,v}$ associated with the functions

$$(x,\varepsilon) \to tr\left(\sum_{j=1}^{t} (ux)^{2^j+1} + vx^3 + \varepsilon ux\right).$$

Let us recall that for any symplectic form φ on G' of rank 2h, we have (cf [5]):

$$\left(\sum_{x,\, y\in G'} (-1)^{\varphi(x,y)}\right) = 2^{2m'-2h}$$

and that if f' is a quadratic function on G', of symplectic form φ :

$$\left(\sum_{x \in G'} (-1)^{f'(x)}\right)^2 = \left(\sum_{x,\, y\in G'} (-1)^{\varphi(x,y)}\right)$$ if f' is not balanced, and 0 otherwise.

So, a, b and c satisfy the following relations :

1) $a + b + c + 1 = 2^{2m-2}$

2) $(a+b)\, 2^m + c\, 2^{m+2} + 2^{2m-2} = \sum_{u,v\in G'} \left(\sum_{x,y\in G'} (-1)^{\varphi_{u,v}(x,y)}\right) =$

$$\sum_{u,v\in G'} \left(\sum_{x,y\in G'} (-1)^{tr\,(u[x^{2^t}y+y^{2^t}x]+v[x^{2^{t-1}}y+y^{2^{t-1}}x])}\right) =$$

$$|G'|^2 \left|\{x,y\in G' / x^{2^t}y+y^{2^t}x = 0 \text{ and } x^{2^{t-1}}y+y^{2^{t-1}}x = 0\}\right| = |G'|^2 \left|\{x,y\in G' / x = 0 \text{ or } y = 0 \text{ or } x = y\}\right| =$$

$$|G'|^2 (3\,|G'| - 2) = 2^{2m-2}\left(3 \times 2^{m-1} - 2\right).$$

3) $b\, 2^m + 2^{2m-2} = \sum_{u,v\in G'} \left(\sum_{x,y\in G'} (-1)^{tr\,(ux^{2^t+1}+vx^{2^{t-1}+1})}\right)^2 =$

$$\sum_{u,v\in G'} \left(\sum_{x,y\in G} (-1)^{tr\,(u[x^{2^t+1}+y^{2^t+1}]+v[x^{2^{t-1}+1}+y^{2^{t-1}+1}])}\right) =$$

$$|G'|^2 \left|\{x,y\in G' / x^{2^t+1} = y^{2^t+1} \text{ and } x^{2^{t-1}+1} = y^{2^{t-1}+1}\}\right| =$$

$$|G'|^3 = 2^{3m-3}.$$

From these equalities, we deduce :

$a = (2^{m-1}-1)(2^{m-1}+4)/3$, and $b+c = (2^{m-1}-1)(2^m-1)/3$,

and therefore,according to [12], ch 15, th 5, the weight distribution of D is :

i =	number of the elements of weight i =
0 or 2^{2t+2}	1
$2^{2t+1} \pm 2^{t+1}$	$2^{2t}(2^{2t+1}-1)(2^{2t+2}-1)/3$
$2^{2t+1} \pm 2^{t}$	$2^{2t+2}(2^{2t+1}-1)(2^{2t+1}+4)/3$
2^{2t+1}	$2(2^{2t+2}-1)(2^{4t+1}-2^{2t}+1)$

which is the same as $\mathfrak{DG}(m,t)$'s one, according to Goethals ([9], table III).

PROPOSITION 2

The code D is pseudo-linear and $\mathcal{T}(m)$ is pseudo-dual to D.

Proof :

Let E' be the set of all the functions $f'_{u,v}$.
Let D' be the linear code equal to : E'+ R(1, m).

τ_α ($\alpha \in G'$) is as before the permutation on G : $(x, \varepsilon) \rightarrow (x + \varepsilon\,\alpha, \varepsilon)$.
Let us define ϕ :

If a function g does not belong to $R(1, m)^\perp$, then : $\phi(g) = g$.
If g belongs to $R(1, m)^\perp$, then :

$$\sum_{f \in D,\ \alpha \in G'} (-1)^{<f \circ \tau_\alpha,\ g>} = \sum_{u,v \in G',\ \alpha \in G'} \sum_{h \in R(1,m)} (-1)^{<f_{u,v} \circ \tau_\alpha + h,\ g>}$$

$$= |R(1, m)| \sum_{u,v \in G',\ \alpha \in G'} (-1)^{<f_{u,v} \circ \tau_\alpha,\ g>}$$

Let $F_{u,v}$ be the kernel of $\varphi_{u,v}$. By Lemma 2, we have :

$$\sum_{u,v \in G',\ \alpha \in G'} (-1)^{<f_{u,v} \circ \tau_\alpha,\ g>} = |G'| \sum_{u,v \in G'/\lambda_g \in F_{u,v}} (-1)^{<f_{u,v},\ g>}$$

$$= |G'| \sum_{u,v \in G'/\lambda_g \in E_{u,v}} (-1)^{<f'_{u,v},\ g_0+g_1> + h_{u,v}(\lambda_g)}, \text{ since } h_{u,v} \text{ is linear}$$

$$= |G'| \sum_{u,v \in G'/\lambda_g \in E_{u,v}} (-1)^{<f'_{u,v},\ g_0+g_1> + f'_{u,v}(\lambda_g)} .$$

Let k be any element of $R(1, m)^{\perp}$ such that :

$$\sum_{x \in G'/\, k(x,0) = 1} x^{2^t+1} = \sum_{x \in G'/\, k(x,0) = 1} x^{2^{t-1}+1} = 1 \text{ and } \forall\, x \in G',\ k(x,1)=0.$$

For any element λ of G', different from 0, let k_λ be defined by : $k_\lambda(x,\varepsilon) = k(x/\lambda,\varepsilon)$.

We have :

$$\sum_{x \in G'/\, k_\lambda(x,0) = 1} x^{2^t+1} = \lambda^{2^t+1},\quad \sum_{x \in G'/\, k_\lambda(x,0) = 1} x^{2^{t-1}+1} = \lambda^{2^{t-1}+1} \text{ and } \forall\, x \in G',\ k_\lambda(x,1)=0.$$

We have : $f'_{u,v}(\lambda) = \langle f'_{u,v}, k_\lambda \rangle$, and so, if we take : $\phi(g) = g$ if $\lambda_g = 0$, and $\phi(g) = g + k_{\lambda_g}$ otherwise, then D is clearly pseudo-linear, and ϕ is an associated permutation
with D .

Let us prove now that $\phi^{-1}(D'^{\perp}) = \phi(D'^{\perp})$ is equal to $\mathcal{T}(m)$.

$D'^{\perp}$ is the set of all the functions $g \in R(m-2, m)$ such that : $\forall u,v \in G'$, $\langle f'_{u,v}, g \rangle = 0$, or, equivalently :

$$\forall\, u,v \in G',\ tr\Big(\sum_{x \in G'/g(x,0)+g(x,1) = 1} (u\, x^{2^t+1} + v\, x^{2^{t-1}+1}\Big) = 0 \text{ , and so :}$$

$$\sum_{x \in G'/g(x,0)+g(x,1) = 1} x^{2^t+1} = 0 \text{ , and } \sum_{x \in G'/g(x,0)+g(x,1) = 1} x^{2^{t-1}+1} = 0 .$$

For any $g \in R(m-2, m)$ such that $\lambda_g = 0$, and any $g \notin R(m-2, m)$, g belongs to $D'^{\perp}$ if and only if g belongs to $\mathcal{T}(m)$.
Clearly, any $g \in R(m-2, m)$ such that $\lambda_g \neq 0$ belongs to $D'^{\perp}$ if and only if $\phi(g)$ belongs to $\mathcal{T}(m)$.

This finishes the proof .
Notice that $D'^{\perp}$ and ϕ satisfy the condition stated in the remark which follows the theorem .

COROLLARY 2

$\mathcal{T}(m)$ and $\mathcal{DG}(m,t)$ are formally dual.

CONCLUSION

We have obtained a generalization of the Mac Williams' result to some nonlinear codes . The notion of pseudo-linearity gives an explanation of the most known formal dualities between nonlinear codes .
In this new framework, we lose the nice symmetry which exists between a linear code and its dual code, since the pseudo-dual code does not seem to be always pseudo-linear. Moreover, a pseudo-linear code does not need to be distance invariant (as we see it on the codes C_j and D met in lemmas 1 and 2), but its pseudodual code is distance invariant under a
rather natural condition stated in the remark which follows the theorem (this condition is satisfied in the cases studied in Propositions 1 and 2).
Nevertheless, this may lead to new distance invariant nonlinear codes (which are known to be
good candidates for optimum properties) whose weight enumerators and dual weight enumerators
would be both "known".

REFERENCES

(1) Ronald D. Baker, Jacobus H. Van Lint and Richard M. Wilson, "On the Preparata and Goethals codes" IEEE Trans Inform Theory. Vol IT 29

(2) P. Camion, "Codes de Preparata et Codes de Kerdock" théorie des codes ENSTA, pp 21-29, 1979.

(3) C. Carlet, "An analytic proof of the formal duality between Kerdock and Preparata Codes", Publication du L.I.T.P. n° 89-19 (L.I.T.P. 4 place Jussieu, 75251
Paris Cédex 05).

(4) C. Carlet, "Le groupe d'automorphismes du code de Kerdock" C. R. Acad. Sci. Paris t.309, Série I, p. 843-845, 1989.

(5) C. Carlet, thèse, "codes de Reed-Muller , codes de Kerdock et de Preparata ", Publication du L.I.T.P., 1990.

(6) C. Carlet, "A general case of formal duality between binary nonlinear codes", Publication du L.I.T.P. n° 90-59.

(7) P. Charpin, Thèse, "Codes cycliques étendus invariants sous le groupe affine", Rapport du L.I.T.P. n°87-6.

(8) P. Delsarte, J.-M. Goethals, "Alternating bilinear forms over GF(q), J. Combin. Theory, 19 A (1975) 26-50 [15, 21, A]

(9) J.M. Goethals, "Nonlinear codes defined by quadrative forms over GF(2)", Information and control, 31 (1976) 43-74.

(10) W. M. Kantor, "On the inequivalence of generalized Preparata Codes", IEEE Trans Inform Theory. Vol IT.29, pp 345-348, May 1983.

(11) A. M. Kerdock, "A class of low-rate non linear codes", Information and Control, 20 (1972), pp 182-187.

(12) F. J. Mac Williams and N. J. Sloane, "The theory of error-correcting codes", Amsterdam, North Holland.

(13) F. P. Preparata, "A class of optimum non linear double-error correcting codes" Information and Control, 13 (1968), pp 378-400.

(14) J. Simonis "Reed Muller codes", Report of the faculty of math.and information n° 87-23 Delft (1987).

(15) J. H. Van Lint, "Kerdock codes and Preparata codes", Congressus Numerantium, Vol. 39 (1983), pp 25-41.

(16) J. H. Van Lint, "Coding Theory", Springer Verlag 201.

(17) H.C.A. Van Tilborg "On weights in codes" Report 71-WSK03, Dep.of math. Technological University of Eindhoven, Netherlands (1971).

(18) J. Wolfmann, "Aspects géométriques et combinatoires de l'étude des codes correcteurs"
Thèse de Doctorat d'Etat, Université Paris VII, (1978)

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

ISSN 0249 - 6399