Codes à métrique du rang

Ambroise Minot
Université Grenoble Alpes

Introduction

Le but de ce travail d'étude et de recherche est d'examiner la théorie de base des codes à métrique du rang, en se basant sur l'article [1] d'Elisa Gorla et d'Alberto Ravagnani.
Après avoir effectué quelques rappels de résultats préliminaires, on commencera donc à poser les définitions des codes et de certaines notions aidant à les caractériser, comme leurs distributions de poids ou leurs distances minimales. On établira ensuite le lien entre deux visions possibles de ces codes, l'approche matricielle et l'approche vectorielle, qui nous sera très utile par la suite pour obtenir certains résultats.
On s'intéressera ensuite aux identités de MacWilliams, qui établissent une relation entre la distrubtion de poids d'un code et de celle de son code dual. Analogues du théorème de MacWilliams pour les codes munis de la distance Hamming, on les établira ici pour les codes à métrique du rang.
Avoir établi ces deux sections nous permettra alors d'étudier les codes MRD, c'est à dire les codes ayant le plus grand cardinal possible pour des paramètres donnés : on verra comment les construire, comment les caractériser, et les informations qu'il est possible d'obtenir sur leurs distributions de poids.
Après cela, on pourra s'intéresser aux anticodes, c'est-à-dire aux codes auxquels on impose une distance maximale, constrastant avec les sections précédentes où la distance minimal était très utilisée. On introduira en particulier la notion d'anticode optimal, analogue au code MRD de par l'idée de plus grand cardinal possible.

1 Prolégomènes

Notation 0.1 On notera $\mathbb{F}_q$ le corps fini contenant q éléments.

Notation 0.2 On notera $\mathcal{M}_{k\times m}(\mathbb{F}_q)$ l'espace des matrices $k \times m$ sur $\mathbb{F}_q$, en supposant $k \leq m$.

Lemme 0.3 Soit $Tr : \mathcal{M}_{k\times k}(\mathbb{F}_q) \to \mathbb{F}_q$ la trace d'une matrice $k \times k$.
L'application $\Upsilon : (M, N) \mapsto Tr(MN^t)$, pour $M, N \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$, est une forme bilinéaire symétrique non dégénérée.

— On montre aisément que Υ est bilinéaire : en notant $M = (m_{i,j})_{\substack{1\leq i\leq k\\ 1\leq j\leq m}}$, on obtient

1. $Tr(MN^t) = \sum_{i=1}^{k}\sum_{j=1}^{m} m_{i,j}n_{i,j} = Tr(NM^t)$ donc Υ est symétrique.
2. $Tr((a.M + M')N^t) = \sum_{i=1}^{k}\sum_{j=1}^{m}(a.m_{i,j} + m_{i,j})'n_{ij}$
   $= \sum_{i=1}^{k}\sum_{j=1}^{m} a.m_{i,j}n_{i,j} + m'_{i,j}n_{i,j} = a.Tr(MN^t) + Tr(M'N^t)$
   donc Υ est linéaire en une coordonnée.

Υ est donc bien bilinéaire.

— On montre maintenant que Υ est non dégénérée :
Soit $M \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$ telle que $\forall N \in \mathcal{M}_{k\times m}(\mathbb{F}_q), Tr(MN^t) = 0$.
Définissons alors, pour $a \in [1, ..., k], b \in [1, ..., m], D_{a,b} = (d_{i,j}^{a,b})_{\substack{1\leq i\leq k\\ 1\leq j\leq m}}$ telle que

$$d_{i,j}^{a,b} = \begin{cases} 1 & \text{si } (i,j) = (a,b) \\ 0 & \text{si } (i,j) \neq (a,b) \end{cases}$$

Alors $\forall a, b \in [1, ..., k] \times [1, ..., m], Tr(MD_{a,b}^t) = 0$,
i.e. $\sum_{i=1}^{k}\sum_{j=1}^{m} m_{i,j}d_{i,j}^{a,b} = 0$, et donc $m_{a,b} = 0$.
$\forall a, b \in [1, ..., k] \times [1, ..., m], m_{a,b} = 0$ donc $M = 0_{\mathcal{M}_{k\times m}(\mathbb{F}_q)}$.
Υ est donc non-dégénérée.

Notation 0.4 On notera $rg : \mathcal{M}_{k\times m}(\mathbb{F}_q) \to \mathbb{N}$ l'application qui associe à une matrice son rang.

Propriétés 0.5 On a, pour tout corps $\mathbb{K}$ et pour tout $M, N \in \mathcal{M}_{k\times m}(\mathbb{K})$:

1. $rg(M) = rg(-M)$
2. $rg(M) = 0 \Leftrightarrow M = 0$
3. $rg(M + N) \leq rg(M) + rg(N)$

En notant C_{M_i} la i-ième colonne de M, on peut démontrer ces propriétés ainsi :

1. $rg(M) = dim(vect(C_{M_1}, ..., C_{M_m})) = dim(vect(-C_{M_1}, ..., -C_{M_m}))$
   $= rg(-M)$
2. $rg(M) = 0 \Leftrightarrow dim(vect(C_{M_1}, ..., C_{M_m})) = 0$
   $\Leftrightarrow vect(C_{M_1}, ..., C_{M_m}) = 0 \Leftrightarrow \forall i \in [1, ..., m], C_{M_i} = 0 \Leftrightarrow M = 0$
3. $\forall i \in [1, ..., m], C_{(M+N)_i} = C_{M_i} + C_{N_i}$
   donc $vect(C_{(M+N)_i}) \subset vect(C_{M_i}) + vect(C_{N_i})$
   donc $vect(C_{(M+N)_1}, ..., C_{(M+N)_m}) \subset vect(C_{M_1}, ..., C_{M_m}) + vect(C_{N_1}, ..., C_{N_m})$

donc $dim(vect(C_{(M+N)_1}, ..., C_{(M+N)_m})) \leq dim(vect(C_{M_1}, ..., C_{M_m}) + vect(C_{N_1}, ..., C_{N_m}))$
$\leq dim(vect(C_{M_1}, ..., C_{M_m})) + dim(vect(C_{N_1}, ..., C_{N_m}))$
Ainsi $rg(M+N) \leq rg(M) + rg(N)$

Notation 0.6 Notons $Tr_q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ l'application définie par $Tr_q(\alpha) = \alpha + \alpha^q + ... + \alpha^{q^{m-1}}$, dite **trace relative**.
On remarque que $(Tr_q(\alpha))^q = (\alpha + \alpha^q + ... + \alpha^{q^{m-1}})^q$
$= \alpha^q + \alpha^{q+1} + ... + \alpha^{q^{m-1}} + \alpha^{q^m} = \alpha + \alpha^q + ... + \alpha^{q^{m-1}} = Tr_q(\alpha)$ car $\alpha^{q^m} = \alpha$.
Donc $Tr_q(\alpha)$ est un point fixe du morphisme de Frobenius, ce que signifie que $Tr_q(\alpha)$ est un élément de $\mathbb{F}_q$.
Tr_q est donc bien à valeurs dans $\mathbb{F}_q$.

Propriété 0.7 La trace relative est $\mathbb{F}_q$-linéaire surjective.

En effet, si on prend $\alpha, \beta \in \mathbb{F}_{q^m}, c \in \mathbb{F}_q$, on a alors :

$$\begin{aligned}
Tr_q(c\alpha + \beta) =& c\alpha + \beta + (c\alpha + \beta)^q + ... + (c\alpha + \beta)^{q^{m-1}} \\
=& c\alpha + \beta + (c\alpha)^q + \beta^q + ... + (c\alpha)^{q^{m-1}} + \beta^{q^{m-1}} \\
=& c\alpha + c^q\alpha^q + ... + c^{q^{m-1}}\alpha^{q^{m-1}} + \beta + \beta^q + ... + \beta^{q^{m-1}} \\
=& c\alpha + c\alpha^q + ... + c\alpha^{q^{m-1}} + \beta + \beta^q + ... + \beta^{q^{m-1}} \\
=& c(\alpha + \alpha^q + ... + \alpha^{q^{m-1}}) + \beta + \beta^q + ... + \beta^{q^{m-1}} \\
=& cTr_q(\alpha) + Tr_q(\beta)
\end{aligned}$$

Comme Tr_q est linéaire, son image dans $\mathbb{F}_q$ est donc un sous-espace vectoriel. Mais $dim_{\mathbb{F}_q}(\mathbb{F}_q) = 1$, il n'y a donc que deux sous-espaces possibles ; on a soit $Im(Tr_q) = \mathbb{F}_q$, soit $Im(Tr_q) = \{0\}$.
Or Tr_q est polynomiale de degré q^{m-1}, et $|\mathbb{F}_{q^m}| = q^m$. Avoir $Im(Tr_q) = \{0\}$ est impossible,car Tr_q aurait alors q^m racines. Il est donc toujours possible de trouver un élément d'image non nulle, et on a $Im(Tr_q) \neq 0$. Tr_q est alors surjective, avec $Im(Tr_q) = \mathbb{F}_q$.

Définition 0.8 Soient $\Gamma = \{\gamma_1, ..., \gamma_m\}, \Gamma' = \{\gamma'_1, ..., \gamma'_m\}$ deux bases sur $\mathbb{F}_q$ de l'extension de corps $\mathbb{F}_{q^m} \supset \mathbb{F}_q$.
Γ et Γ' sont appelées **mutuellement orthogonales** si $Tr_q(\gamma'_i\gamma_j) = \delta_{i,j}$ pour tout $i, j \in [1, ..., m]$.

Lemme 0.9 Toute application linéaire L de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$ est de la forme $L(\alpha) = Tr_q(\beta\alpha)$, avec $\beta \in \mathbb{F}_{q^m}$ unique.

En effet, si on prend une application L_β fixée de la forme $L_\beta(\alpha) = Tr_q(\beta\alpha)$, alors L_β est linéaire de par la linéarité de la trace.
De plus, si $\beta \neq \gamma$, alors $L_\beta(\alpha) - L_\gamma(\alpha) = Tr_q(\beta\alpha) - Tr_q(\gamma\alpha) = Tr_q((\beta-\gamma)\alpha) \neq 0$ pour un certain α car $\beta - \gamma \in \mathbb{F}_{q^m}^x$ et Tr_q est surjective, donc $L_\beta(\alpha) \neq L_\gamma(\alpha)$.
Donc on peut donc trouver q^m applications différentes de cette forme.
D'autre part, chaque application linéaire de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$ est entièrement déterminée par le choix de m éléments arbitraires de $\mathbb{F}_q$ que l'on assigne à chacun des m éléments d'une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$, ce qui peut être fait de q^m façons différentes.
Ll'ensemble des applications de la forme L_β est donc contenu dans l'ensemble des applications linéaires, et est de même cardinal ; c'est donc que ces deux ensembles coïncident.

Propriété 0.10 Toute base Γ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ a une unique base orthogonale Γ'. Notons $\Gamma = (\gamma_1, ..., \gamma_m)$.

Pour montrer cela, on remarque que, pour tout $a \in \mathbb{F}_{q^m}, a = a_1\gamma_1 + ... + a_m\gamma_m$, où pour tout $i \in [1, ..., m]$, $a_i \in \mathbb{F}_q$, si on considère l'application coordonnée $c_i : (a \mapsto a_i)$ allant de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_q$, celle-ci est linéaire.
Par le lemme 0.8, il existe alors un unique $\beta_i \in \mathbb{F}_{q^m}$ tel que $\forall a \in \mathbb{F}_{q^m}$, $c_i(a) = Tr_q(\beta_i a)$.
De plus, $\forall i \in [1, ..., m], \gamma_i$ s'écrit $1 \cdot \gamma_i$, donc $Tr_q(\beta_i\gamma_i) = 1$, et $Tr_q(\beta_i\gamma_j) = 0 \ \forall \ j \in [1, ..., m] \setminus \{i\}$.
En notant $\Gamma' = \{\beta_1, ..., \beta_m\}$, on a alors que Γ' est une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ car
$|\Gamma'| = m = dim_{\mathbb{F}_q}\mathbb{F}_{q^m}$, et Γ' est une famille libre.
En effet, si

$$d_1\beta_1 + ... + d_m\beta_m = 0 \text{ avec } d_i \in \mathbb{F}_q \text{ pour tout } i \in [1, ..., m]$$

Alors pour tout $i \in [1, ..., m]$,

$$\gamma_i(d_1\beta_1 + ... + d_m\beta_m) = 0 \Rightarrow Tr_q(\gamma_i(d_1\beta_1 + ... + d_m\beta_m)) = 0$$
$$\Rightarrow d_1 Tr_q(\gamma_i\beta_1) + ... + d_m Tr_q(\gamma_i\beta_m) = 0 \text{ c'est-à-dire } d_i = 0.$$

On a donc que Γ' est une base orthogonale à Γ, et elle est unique par l'unicité de β_i dans le lemme 0.9 .

Notation 0.11 Soit $M \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$. On notera $colspc(M)$ le $\mathbb{F}_q$-sous-espace de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$ engendré par les colonnes de M.

Notation 0.12 Soient deux entiers $a, b \in \mathbb{N}$. On note $\begin{bmatrix} a \\ b \end{bmatrix}_q$ le coefficient q-binomial de a et b ; c'est-à-dire le nombre de sous-espaces de dimension b dans un espace U de

dimension a sur $\mathbb{F}_q$.

Propriété 0.12
a) Si $a, b \in \mathbb{N}$ tels que $b \leq a$, le coefficient q-binomial de a et b est donné par

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \frac{(q^a-1)(q^a-q)...(q^a-q^{b-1})}{(q^b-1)(q^b-q)...(q^b-q^{b-1})}$$

b) Si on suppose $0 \leq b \leq a$, on a $\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{bmatrix} a \\ a-b \end{bmatrix}_q$.

Pour montrer la première assertion, on commence par considérer N le nombre de familles libres $(v_1, ...v_b)$ de b vecteurs dans U. U contenant $q^a - 1$ éléments non-nuls, on peut choisir v_1 de $q^a - 1$ façons différentes. On cherche ensuite un vecteur v_2 linéairement indépendant de v_1 ; sachant que $|Vect_{\mathbb{F}_q}(v_1)| = q$, on a alors que $|U \setminus Vect_{\mathbb{F}_q}(v_1)| = q^a - q$, et on peut donc choisir ce vecteur de $q^a - q$ façons différentes. En répétant ce processus, on obtient alors que :

$$N = (q^a-1)(q^a-q)...(q^a-q^{b-1})$$

D'autre part, on peut également obtenir $(v_1, ...v_b)$ en choisissant d'abord un sous-espace B de dimension b parmi les $\begin{bmatrix} a \\ b \end{bmatrix}_q$ possibles, puis en choisissant v_1 dans B ce qui possible de $q^b - 1$ façons différentes, puis v_2 de $q^b - q$ façons différentes, et ainsi de suite, nous donnant alors :

$$N = \begin{bmatrix} a \\ b \end{bmatrix}_q (q^b-1)(q^b-q)...(q^b-q^{b-1})$$

L'égalité $(q^a-1)(q^a-q)...(q^a-q^{b-1}) = \begin{bmatrix} a \\ b \end{bmatrix}_q (q^b-1)(q^b-q)...(q^b-q^{b-1})$ nous permettant enfin d'obtenir le résultat.

Pour montrer la seconde assertion, on se sert de l'espace dual U^* de U à qui il est isomorphe. On cherche le nombre de sous-espaces de dimension b contenu dans un espace U de dimension a. Si V est un tel sous-espace, alors son orthogonal $V^\perp$ dans U^* est de dimension $dim(U) - dim(V) = b - a$.
A tout sous-espace de U correspond un orthogonal, donc il y a au moins autant de sous-espaces de dimension $a - b$ dans U^* que d'espaces de dimension b dans U. Inversement, si V est un sous-espace de dimension $a - b$ dans U^*, son orthogonal dans

$U^{**} \simeq U$ est de dimension b.
Il y a donc exactement autant de sous-espace de dimension b dans U de dim a, que de sous-espaces de dimension $a-b$ dans U^* de dim a.
On a ainsi le résultat.

Notation 0.13 Soit U un espace vectoriel sur $\mathbb{F}_q$. On notera $\mathcal{S}(U)$ l'ensemble des sous-espaces vectoriels de U.

Propriété 0.14 Soient U et V deux espaces vectoriels sur $\mathbb{F}_q$ tels que $U \subset V$, de dimensions respectives u et v.
Soit s tel que $u \leq s \leq v$. Le nombre de sous-espaces S de dimension s tels que $U \subset S \subset V$ est alors donné par $\begin{bmatrix} v-u \\ s-u \end{bmatrix}_q$.

En effet : on définit l'application $\Pi : \{S \in \mathcal{S}(V), U \subset S \subset V\} \to \{S+U \in \mathcal{S}(V/U), U \subset S \subset V\}$ qui associe à chacun de ces sous-espaces sa classes d'équivalence dans le quotient V/U. On a alors a $dim(\Pi(S)) = dim(S/U) = dim(S) - dim(U) = s-u$.
Cette application est surjective par construction, et elle est également injective :
Soient $S, S' \in \{S \in \mathcal{S}(V), U \subset S \subset V\}$ tels que $\Pi(S) = \Pi(S')$, i.e. $S+U = S'+U$.
Alors $\forall s \in S, s' \in S', s-s' \in U$. Or $U \subset S'$, donc $s-s' \in S'$, et on a donc $s'+s-s' = s \in S'$.
Donc $S \subset S'$, et de la même façon on peut montrer que $S' \subset S$, donc $S = S'$.
On a donc une bijection, ce qui signifie qu'il y a autant de sous-espaces S de dimension s tels que $U \subset S \subset V$ que de sous-espaces S/U de dimension $s-u$ dans V/U de dimension $v-u$. On obtient donc le résultat.

2 Codes à métrique du rang

Dans cette section, on commencera par donner les éléments essentiels nous permettant de définir et de caractériser les codes à métrique du rang d'un point de vue matriciel ; on présentera ensuite le point de vue vectoriel, et on établira des relations entre ces deux approches.
On commence donc par introduire les notions de base.

Définition 1 La **distance du rang** est la fonction $d : \mathcal{M}_{k\times m}(\mathbb{F}_q) \times \mathcal{M}_{k\times m}(\mathbb{F}_q) \to \mathbb{N}$ définie par $d(M,N) = rg(M-N)$ pour toutes $M, N \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$

On peut alors montrer d est effectivement une distance en utilisant les propriétés du

rang vues en 0.5 : pour toutes $M, N, Z \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$, on a que

—

$d(M,N) = rg(M-N) \in \mathbb{N}$, donc $d(M,N) \geqslant 0$
d satisfait donc la condition de positivité.

—

$d(M,N) = 0 \Leftrightarrow rg(M-N) = 0 \Leftrightarrow M-N = 0 \Leftrightarrow M = N$
d satisfait donc la condition de coincidence.

—

$d(M,N) = rg(M-N) = rg(-(N-M)) = rg(N-M) = d(N,M)$
d satisfait donc la condition de symétrie.

—

$$\begin{aligned} d(M,N) = rg(M-N) = rg(M-Z+Z-N) &\leq rg(M-Z) + rg(Z-N) \\ &\leq d(M,Z) + d(Z,N) \end{aligned}$$

d satisfait donc l'inégalité triangulaire.

Définition 2 Un **code (à métrique de rang)** $\mathcal{C}$ sur $\mathbb{F}_q$ est un sous-ensemble non vide de $\mathcal{M}_{k\times m}(\mathbb{F}_q)$.
Si $\mathcal{C}$ possède au moins deux éléments, on note alors $d(\mathcal{C})$ la **distance minimale** de $\mathcal{C}$, exprimée par

$$d(\mathcal{C}) = \min\{d(M,N) \mid M, N \in \mathcal{C}, M \neq N\}$$

Le code $\mathcal{C}$ est linéaire s'il est un $\mathbb{F}_q$-sous-espace-vectoriel sur $\mathcal{M}_{k\times m}(\mathbb{F}_q)$.
On définit alors son **code dual** comme

$$\mathcal{C}^{\perp} = \{N \in \mathcal{M}_{k\times m}(\mathbb{F}_q) \mid Tr(MN^t) = 0, \forall M \in \mathcal{C}\} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$$

Tr réfère ici à la trace d'une matrice $k \times k$ tel qu'elle a été vue dans le lemme 0.3 développé dans les prolégomènes.

Du fait de ce lemme, le dual d'un code linéaire est lui-même un code linéaire, de dimension $dim(\mathcal{C}^{\perp}) = km - dim(\mathcal{C})$.

On va maintenant introduire des valeurs importantes liée aux codes.

Définition 3 La **distribution de poids** d'un code $\mathcal{C}$ est la famille $\{W_i(\mathcal{C}) \mid i \in \mathbb{N}\}$, où $W_i(\mathcal{C})$ est défini par

$$W_i(\mathcal{C}) = |\{M \in \mathcal{C} \mid rg(M) = i\}|$$

Définition 4 La **distribution de distance** d'un code $\mathcal{C}$ est la famille $\{D_i(\mathcal{C}) \mid i \in \mathbb{N}\}$, où $D_i(\mathcal{C})$ est défini par

$$D_i(\mathcal{C}) = 1/|\mathcal{C}| \cdot |\{(M,N) \in \mathcal{C}^2 \mid d(M,N) = i\}|$$

Si $\mathcal{C}$ est un code linéaire, alors en prenant $P \in \mathcal{C}$, on a : $\forall M \in \mathcal{C}, \exists! N \in \mathcal{C}$ tel que $M - N = P$.
Il existe donc précisément $|\mathcal{C}|$ paires $(M,N) \in \mathcal{C}^2$ telles que $M - N = P$
On a donc que, pour tout $i \in \mathbb{N}$,

$$\begin{aligned} D_i(\mathcal{C}) =& 1/|\mathcal{C}| \cdot |\{(M,N) \in \mathcal{C}^2 \mid d(M,N) = i\}| = 1/|\mathcal{C}| \cdot \sum_{\substack{P \in \mathcal{C} \\ rg(P)=i}} |\{(M,N) \in \mathcal{C}^2 \mid M - N = P\}| \\ =& 1/|\mathcal{C}| \cdot \sum_{\substack{P \in \mathcal{C} \\ rg(P)=i}} |\mathcal{C}| = \sum_{\substack{P \in \mathcal{C} \\ rg(P)=i}} 1 = |\{P \in \mathcal{C} \mid rg(P) = i\}| \\ =& W_i(\mathcal{C}) \end{aligned}$$

De plus, si $|\mathcal{C}| \geq 2$, alors $d(\mathcal{C}) = \min\{rg(M) \mid M \in \mathcal{C}, M \neq 0\}$

Une notion différente de code muni de la métrique du rang avait été proposée de façon indépendante par E.Gabidulin, dans laquelle les éléments du code sont des vecteurs sur une extension de corps $\mathbb{F}_{q^m}$ plutôt que des matrices sur $\mathbb{F}_q$.
Cette vision est notamment développée dans le document [2], et on va en faire ici une présentation.

Définition 5 Soit $v = (v_1, ..., v_k)^t, w = (w_1, ..., w_k)^t \in \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ deux vecteurs sur l'extension de corps $\mathbb{F}_{q^m}$.
On note $rg_G(v) = dim(vect(v_1, ...v_k))$ le **rang** du vecteur v, c'est à dire la dimension de l'espace vectoriel sur $\mathbb{F}_q$ engendré par les v_i.
On note $d_G(v,w) = rg_G(v - w)$ la **distance de rang** entre ces deux vecteurs.

On peut montrer que d_G est une distance de la même façon que pour la définition 1, car on remarque que rg_G possède les mêmes propriétés que rg.

Définition 6 Un **code vectoriel (à métrique de rang)** $\mathcal{C}$ est un sous-ensemble non-vide de $\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$.
Si $\mathcal{C}$ possède au moins deux éléments, on note alors $d_G(\mathcal{C})$ la **distance minimale** de $\mathcal{C}$, exprimée par

$$d_G(\mathcal{C}) = \min\{d_G(v,w) \mid v,w \in \mathcal{C}, v \neq w\}$$

Le code $\mathcal{C}$ est linéaire s'il est $\mathbb{F}_{q^m}$-sous-espace-vectoriel de $\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$.
On définit alors son **dual** comme

$$\mathcal{C}^{\perp} = \left\{ w \in \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m}) \mid \sum_{i=1}^{k} v_i w_i = 0, \forall v \in \mathcal{C} \right\} \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$$

L'application $(v,w) \mapsto \sum v_i w_i$ est une forme bilinéaire symétrique non-dégénérée sur $\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$, sa matrice dans la base canonique étant la matrice identitée.
Par suite, si $\mathcal{C}$ est un code vectoriel linéaire,

$$dim_{\mathbb{F}_{q^m}}(\mathcal{C}^{\perp}) = k - dim_{\mathbb{F}_{q^m}}(\mathcal{C})$$

Définition 7 La **distribution de poids** d'un code vectoriel $\mathcal{C}$ est la famille $\{W_i(\mathcal{C}) \mid i \in \mathbb{N}\}$, où $W_i(\mathcal{C})$ est défini par

$$W_i(\mathcal{C}) = |\{v \in \mathcal{C} \mid rg_G(v) = i\}|$$

Définition 8 La **distribution de distance** d'un code vectoriel $\mathcal{C}$ est la famille $\{D_i(\mathcal{C}) \mid i \in \mathbb{N}\}$, où $D_i(\mathcal{C})$ est défini par

$$D_i(\mathcal{C}) = 1/|\mathcal{C}| \cdot |\{(v,w) \in \mathcal{C}^2 \mid d_G(v,w) = i\}|$$

Il y a un moyen naturel d'associer un code vectoriel à un code en représentation matricielle qui conserve sa cardinalité et ses propriétés métriques.

Définition 9 Notons $\Gamma = \{\gamma_1, ..., \gamma_m\}$ une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.
La matrice **associée** à un vecteur $v \in \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ selon la base Γ est la matrice $\Gamma(v) \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$ définie par

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{i,j}\gamma_j \quad \text{pour tout } \ i = 1, ..., k.$$

Ainsi, la i-ième ligne de $\Gamma(v)$ correspond aux coordonnées de v_i dans la base Γ.

On peut ensuite se servir de cette matrice pour établir une relation entre les codes vectoriels et matriciels.

Proposition 10 Pour chaque base Γ de $\mathbb{F}_{q^m}$, l'application $v \mapsto \Gamma(v)$ est une isométrie bijective $\mathbb{F}_q$-linéaire $(\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m}), d_G) \to (\mathcal{M}_{k\times m}(\mathbb{F}_q), d)$.
En particulier, si $\mathcal{C} \subset \mathbb{F}_{q^m}$ est un code vectoriel, alors $\Gamma(\mathcal{C})$ a les mêmes cardinal, distribution de poids et distribution de distance que $\mathcal{C}$.
De plus, si $|\mathcal{C}| \geq 2$, alors $d_G(\mathcal{C}) = d(\Gamma(\mathcal{C}))$.

Preuve
Soient $v = (v_1, ..., v_k), w = (w_1, ..., w_k) \in \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$. On a alors :

- Pour tout $i \in [1, \ ... \ , k], a \in \mathbb{F}_q$,
  $a.v_i + w_i = \sum_{j=1}^{m} \Gamma(a.v + w)_{i,j}\gamma_j = \sum_{j=1}^{m}(a.\Gamma(v)_{i,j} + \Gamma(w)_{i,j})\gamma_j$
  donc $\Gamma(a.v + w) = a.\Gamma(v) + \Gamma(w)$
  Donc l'application est bien $\mathbb{F}_q$-linéaire.
- Par définition de $\Gamma(v)$, on a immédiatement que l'application est surjective.
- Supposons que $\Gamma(v) = 0_{\mathcal{M}_{k\times m}(\mathbb{F}_q)}$. Par définition, cela signifie que pour tout $i \in [1, ..., k]$, les coordonnées des v_i sont nulles, donc que les v_i sont nuls, et donc que $v = 0_{\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})}$.
  On a donc que $Ker(v \mapsto \Gamma(v)) = \{0_{\mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})}\}$, donc l'application est injective.
- En notant L_{v_i} la i-ième ligne de $\Gamma(v)$, correspondant donc au vecteur des coordonnées de v_i dans Γ, on obtient :

$$\begin{aligned} d(\Gamma(v), \Gamma(w)) &= rg(\Gamma(v) - \Gamma(w)) = dim(vect(L_{v_1} - L_{w_1}, ..., L_{v_k} - L_{w_k})) \\ &= dim(vect_{\mathbb{F}_q}(v_1 - w_1, ..., v_k - w_k)) = rg_G(v - w) = d_G(v, w) \end{aligned}$$

L'application est donc bien une isométrie bijective $\mathbb{F}_q$-linéaire.
Il s'ensuit que, si $\mathcal{C} \subset \mathbb{F}_{q^m}$ est un code vectoriel ,on a $|\mathcal{C}| = |\Gamma(\mathcal{C})|$ par bijectivité ; de plus, pour tout $i \in [1, ..., k]$, $\mathcal{C}$ et $\Gamma(\mathcal{C})$ ont la même distribution de poids du fait que l'application conserve le rang, la même distribution de distance du fait que l'application est une isométrie, et de même si $|\mathcal{C}| \geq 2$ alors $d_G(\mathcal{C}) = d(\Gamma(\mathcal{C}))$ par isométrie.

Une telle relation ayant été établie, il est alors légitime de se demander si, en prenant un code vectoriel $\mathcal{C} \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ et une base Γ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$, les codes $\Gamma(\mathcal{C}^\perp)$ et $\Gamma(\mathcal{C})^\perp$ coïncident.
On peut voir que cela est faux dans le cas général en prenant un contre-exemple :

Exemple 11 Soit $q = 3, k = m = 2$ et $\mathbb{F}_{3^2} = \mathbb{F}_3[\xi]$, en posant ξ tel que $\xi^2 = -1$. Posons $\alpha = (\xi, 2)$. Soit $\mathcal{C} \subset \mathbb{F}_{3^2}^2$ le code vectoriel de dimension 1 engendré par α sur $\mathbb{F}_{3^2}$.
Prenons $\Gamma = \{1, \xi\}$ comme base de $\mathbb{F}_{3^2}$ sur $\mathbb{F}_3$. On a donc que pour tout $z \in \mathbb{F}_{3^2}$, il existe $x, y \in \mathbb{F}_3$ tels que $z = x + y\xi$.

Les éléments de $\mathcal{C}$ sont alors de la forme $z\alpha$, i.e., $x\alpha + y\xi\alpha$.
Il s'en suit que les éléments de $\Gamma(\mathcal{C})$ sont de la forme $x\Gamma(\alpha) + y\Gamma(\xi\alpha)$, donc engendrés par

$$\Gamma(\alpha) = \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \text{ et } \Gamma(\xi\alpha) = \begin{bmatrix} -1 & 0 \\ 0 & 2 \end{bmatrix}$$

Soit $\beta = (\xi, 1) \in \mathbb{F}_{3^2}^2$. On a alors $\alpha_1\beta_1 + \alpha_2\beta_2 = \xi^2 + 2 = -1 + 2 = 1 \neq 0$. Donc $\beta \notin \mathcal{C}^\perp$, et donc $\Gamma(\beta) \notin \Gamma(\mathcal{C}^\perp)$.
D'autre part, on a

$$\Gamma(\beta) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Or $Tr(\Gamma(\alpha)\Gamma(\beta)^t) = 1 + 2 = 3 = 0_{\mathbb{F}_3}$ et $Tr(\Gamma(\xi\alpha)\Gamma(\beta)^t) = 0 + 0 = 0_{\mathbb{F}_3}$, donc on a que $\Gamma(\beta) \in \Gamma(\mathcal{C})^\perp$.
Il en résulte donc que $\Gamma(\mathcal{C}^\perp) \neq \Gamma(\mathcal{C})^\perp$.

On va ensuite établir le lien entre le dual d'un code vectoriel et celui de son équivalent matriciel.
Pour le théorème suivant, on rappel que, selon la propriété 0.10 des prolégomènes, toute base possède une unique base orthogonale.

Théorème 12 Soit $\mathcal{C}$ un code vectoriel linéaire sur $\mathbb{F}_{q^m}$, tel que $\mathcal{C} \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$. Soient Γ, Γ' deux bases mutuellement orthogonales de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. Alors on a

$$\Gamma'(\mathcal{C}^\perp) = \Gamma(\mathcal{C})^\perp$$

En particulier, $\mathcal{C}$ et $\Gamma(\mathcal{C})$ ont la même distribution de poids, et de même pour $\mathcal{C}^\perp$ et $\Gamma(\mathcal{C})^\perp$.

Preuve
Notons $\Gamma = \{\gamma_1, ..., \gamma_m\}, \Gamma' = \{\gamma'_1, ..., \gamma'_m\}$ deux bases mutuellement orthogonales de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.
Soient $M \in \Gamma'(\mathcal{C}^\perp)$ et $N \in \Gamma(\mathcal{C})$. Alors il existe $\alpha \in \mathcal{C}^\perp$ et $\beta \in \mathcal{C}$ tels que $M = \Gamma'(\alpha)$ et $N = \Gamma(\beta)$.
Par la définition 9 , on a

$$0 = \sum_{i=1}^{k} \alpha_i\beta_i = \sum_{i=1}^{k}\sum_{j=1}^{m} M_{i,j}\gamma'_j \sum_{t=1}^{m} N_{i,t}\gamma_t = \sum_{i=1}^{k}\sum_{j=1}^{m}\sum_{t=1}^{m} M_{i,j}N_{i,t}\gamma'_j\gamma_t \qquad (1)$$

En appliquant la fonction trace $Tr_q : \mathbb{F}_{q^m} \to \mathbb{F}_q$ on obtient :

$$\begin{aligned} 0 = Tr_q(0) =& Tr_q\left(\sum_{i=1}^{k}\sum_{j=1}^{m}\sum_{t=1}^{m} M_{i,j}N_{i,t}\gamma'_j\gamma_t\right) = \sum_{i=1}^{k}\sum_{j=1}^{m}\sum_{t=1}^{m} M_{i,j}N_{i,t}Tr_q(\gamma'_j\gamma_t) \\ =& \sum_{i=1}^{k}\sum_{j=1}^{m}\sum_{t=1}^{m} M_{i,j}N_{i,t}\delta_{j,t} = \sum_{i=1}^{k}\sum_{j=1}^{m} M_{i,j}N_{i,j} = Tr(MN^t) \end{aligned}$$

Donc, $\forall M \in \Gamma'(\mathcal{C}^\perp), \forall N \in \Gamma(\mathcal{C}), Tr(MN^t) = 0$. C'est donc que $\Gamma'(\mathcal{C}^\perp) \subset \Gamma(\mathcal{C})^\perp$.

De plus, on a par la proposition 10 que $|\Gamma'(\mathcal{C}^\perp)| = |\mathcal{C}^\perp|$.
Or $|\Gamma'(\mathcal{C}^\perp)| = q^{dim(\Gamma'(\mathcal{C}^\perp))}$ et $|\mathcal{C}^\perp| = q^{m dim_{\mathbb{F}_{q^m}}(\mathcal{C}^\perp)} = q^{m(k-dim_{\mathbb{F}_{q^m}}(\mathcal{C}))} = q^{mk-m\cdot dim_{\mathbb{F}_{q^m}}(\mathcal{C})}$
On a donc $q^{dim(\Gamma'(\mathcal{C}^\perp))} = q^{mk-m\cdot dim_{\mathbb{F}_{q^m}}(\mathcal{C})}$, donc $dim(\Gamma'(\mathcal{C}^\perp)) = (mk-m)\cdot dim_{\mathbb{F}_{q^m}}(\mathcal{C})$.

D'autre part, par définition 2, on a que $dim(\Gamma(\mathcal{C})^\perp) = mk - dim(\Gamma(\mathcal{C}))$,
or $|\Gamma(\mathcal{C})| = |\mathcal{C}| \Rightarrow q^{dim(\Gamma(\mathcal{C}))} = (q^m)^{dim_{\mathbb{F}_{q^m}}(\mathcal{C})}$; par suite, $dim(\Gamma(\mathcal{C})) = m\cdot dim_{\mathbb{F}_{q^m}}(\mathcal{C})$.
Donc $dim(\Gamma(\mathcal{C})^\perp) = mk - m\cdot dim_{\mathbb{F}_{q^m}}(\mathcal{C})$.

On a alors que $\Gamma'(\mathcal{C}^\perp)$ et $\Gamma(\mathcal{C})^\perp$ ont la même dimension sur $\mathbb{F}_q$. Ainsi, les deux codes sont égaux.

Le théorème 12 montre ainsi que la théorie de la dualité des codes linéaires en représentation matricielle peut être vue comme la généralisation de cette même théorie en représentation vectorielle.
Dans la suite, on se concentrera principalement sur la représentation matricielle.

3 Identités de MacWilliams pour la métrique du rang

Dans cette section, on s'intéresse à la relation qu'entretiennent les codes avec leurs codes duaux. On va se concentrer en particulier sur les codes linéaires, afin de prouver les identités de MacWilliams qui nous fourniront une relation directe entre la distribution de poids d'un code et celle de son dual ; elles sont l'analogue du théorème de MacWilliams (1963) pour les codes munis de la distance de Hamming.
Pour cela, on commence par quelques résultats préliminaires.

Notation 13 Soient $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code et $U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ un $\mathbb{F}_q$-sous-espace. On note alors

$$\mathcal{C}(U) = \{M \in \mathcal{C} \mid colspc(M) \subset U\} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$$

l'ensemble des matrices de $\mathcal{C}$ dont l'espace engendré par les colonnes est contenu dans U.

On peut noter que, pour tous $M, N \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$, on a $colspc(M+N) \subset colspc(M) + colspc(N)$.
En conséquence, si U est un sous-espace vectoriel, et $\mathcal{C}$ un code linéaire, alors $\mathcal{C}(U)$est également un code linéaire.

Dans la suite, on munit $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$ de la forme bilinéaire non-dégénérée standard : $< \cdot, \cdot >: \mathcal{M}_{k\times 1}(\mathbb{F}_q) \times \mathcal{M}_{k\times 1}(\mathbb{F}_q) \to \mathbb{F}_q$. On pourra alors noter $U^\perp$ l'orthogonal de U par rapport à celle-ci.

Lemme 14 Soit $U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)m$ un sous-espace. On a :

1. $dim(\mathcal{M}_{k\times m}(\mathbb{F}_q)(U)) = m \cdot dim(U)$
2. $\mathcal{M}_{k\times m}(\mathbb{F}_q)(U)^\perp = \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)$

Preuve

1. Notons $s = dim(U)$, et posons
   $V = \{(x_1, ..., x_k)^t \in \mathcal{M}_{k\times 1}(\mathbb{F}_q) \mid x_i = 0 \text{ pour tout } i > s\}$. De façon évidente, V est un sous-espace vectoriel de dimension s.
   Soit $\beta = (u_1, ..., u_s)$ une base de U. On la complète en une base
   $\beta' = (u_1, ..., u_s, u_{s+1}, ..., u_k)$ de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$.
   On peut alors définir l'isomorphisme $g : \mathcal{M}_{k\times 1}(\mathbb{F}_q) \to \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ tel que, pour $i \in [1, ..., k], g(u_i) = (\delta_{1,i}, ..., \delta_{k,i})$. On a alors que $g(\beta)$ est une base de V, et donc $g(U) = V$.
   Notons $G \in \mathcal{M}_{k\times k}(\mathbb{F}_q)$ la matrice inversible de g dans la base canonique $(e_1, ..., e_k)$ de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$. Ainsi,

   $$g(e_j) = \sum_{i=1}^{k} g_{i,j} e_i \text{ pour tout } j = 1, ..., k$$

   L'application $M \mapsto GM$ est alors un isomorphisme de $\mathcal{M}_{k\times m}(\mathbb{F}_q)(U)$ dans $\mathcal{M}_{k\times m}(\mathbb{F}_q)(V)$, et ainsi $dim(\mathcal{M}_{k\times m}(\mathbb{F}_q)(U)) = dim(\mathcal{M}_{k\times m}(\mathbb{F}_q)(V))$.

Or $\mathcal{M}_{k\times m}(\mathbb{F}_q)(V)$ est l'ensemble des matrices de $\mathcal{M}_{k\times m}(\mathbb{F}_q)$ dont seules les s premières lignes sont éventuellement non nulles. On a donc que $dim(\mathcal{M}_{k\times m}(\mathbb{F}_q)(V))$ $= m \cdot s = m \cdot dim(U)$, et on a ainsi le résultat.

2. Soient $N \in \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)$ et $M \in \mathcal{M}_{k\times m}(\mathbb{F}_q)(U)$. En notant M_j la j-ième colonne de M, on a alors que $Tr(MN^t) = \sum_{j=1}^{k} < M_j, N_j >$.
Chaque colonne de N appartient à $U^\perp$, et chaque colonne de M appartient à U. On a donc que, pour tout $i \in [1, ..., k], < M_i, N_i >= 0$ et donc $Tr(MN^t) = 0$.
Donc $N \in \mathcal{M}_{k\times m}(\mathbb{F}_q)(U)^\perp$, et on a $\mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp) \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)(U)^\perp$. De plus, par la première propriété, les deux espaces sont de même dimension sur $\mathbb{F}_q$. Ils sont donc égaux.

Proposition 15 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire, et soit $U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ un sous-espace de dimension u sur $\mathbb{F}_q$. Alors on a

$$|\mathcal{C}(U)| = \frac{|\mathcal{C}|}{q^{m(k-u)}}|\mathcal{C}^\perp(U^\perp)|$$

Preuve
On a que $\mathcal{C}(U)^\perp = (\mathcal{C} \cap \mathcal{M}_{k\times m}(\mathbb{F}_q)(U))^\perp = \mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U)^\perp$. De plus, le lemme précédent nous donne que $\mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U)^\perp = \mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)$. Or $\mathcal{C}(U)$ est un code linéaire, et on a $dim(\mathcal{C}(U)) + dim(\mathcal{C}(U)^\perp) = km$ comme cela est remarqué dans la définition 2. On a alors :

$$\begin{aligned} |\mathcal{C}(U)| \cdot |\mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)| =& |\mathcal{C}(U)| \cdot |\mathcal{C}(U)^\perp| = q^{dim(\mathcal{C}(U))} \cdot q^{dim(\mathcal{C}(U)^\perp)} \\ =& q^{dim(\mathcal{C}(U))+dim(\mathcal{C}(U)^\perp)} = q^{km} \end{aligned} \tag{2}$$

D'autre part, la première assertion du lemme précédent et la formule de Grassmann nous donne que

$$dim(\mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)) = dim(\mathcal{C}^\perp) + m \cdot dim(U^\perp) - dim(\mathcal{C}^\perp(U^\perp))$$

En conséquence,

$$|\mathcal{C}^\perp + \mathcal{M}_{k\times m}(\mathbb{F}_q)(U^\perp)| = \frac{q^{km} \cdot q^{m(k-u)}}{|\mathcal{C}| \cdot |\mathcal{C}^\perp(U^\perp)|} \tag{3}$$

Le résultat s'obtient alors en appliquant l'égalité (3) au (2).

On se servira de cette proposition lors de la preuve des identités de MacWilliams. Mais avant de présenter celles-ci, il nous faut encore montrer un lemme important

pour sa preuve, qui donne la formule d'inversion de Möbius pour le treillis des sous-espaces de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$. Pour ce lemme, on va se servir des coefficients q-binomiaux tels qu'ils ont été présentés dans la notation 0.11.

Lemme 16 Soit $\mathcal{S}(\mathcal{M}_{k\times 1}(\mathbb{F}_q))$ l'ensemble de tous les sous-espaces de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$, et $f : \mathcal{S}(\mathcal{M}_{k\times 1}(\mathbb{F}_q)) \to \mathbb{Z}$ une application.
On définit $g : \mathcal{S}(\mathcal{M}_{k\times 1}(\mathbb{F}_q)) \to \mathbb{Z}$ par $g(V) = \sum_{U\subset V} f(U)$ pour tout sous-espace V de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$.
Alors pour tout $i \in [0, ..., k]$ et pour tout sous-espace V de dimension i de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$, on a :

$$f(V) = \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} g(U)$$

Preuve
On fixe un entier $i \in [0, ..., k]$ et un sous-espace V de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$ avec $dim(V) = i$.
On définit une fonction $\mu : \{U \in \mathcal{S}(\mathcal{M}_{k\times 1}(\mathbb{F}_q)) \mid U \subset V\} \to \mathbb{Z}$ par $\mu(U) = 1$ si $U = V$, et $\mu(U) = -\sum_{U\subsetneq S\subset V} \mu(S)$ si $U \subsetneq V$.
Par définition de g on a :

$$\sum_{U\subset V} \mu(U)g(U) = \sum_{U\subset V} \mu(U) \sum_{S\subset U} f(S) = \sum_{S\subset V} f(S) \sum_{S\subset U\subset V} \mu(U) = f(V)$$

où la dernière égalité vient du fait que
$\sum_{S\subset V} f(S) \sum_{S\subset U\subset V} \mu(U) = f(V)\mu(V) + \sum_{S\subsetneq V} f(S) \sum_{S\subset U\subset V} \mu(U)$.
Or $\mu(V) = 1$, et $\mu(S) = -\sum_{S\subsetneq U\subset V} \mu(U)$ donc $\mu(S) + \sum_{S\subsetneq U\subset V} \mu(U) = 0$ donc $\sum_{S\subset U\subset V} \mu(U) = 0$.
Il suffit alors de montrer que, pour tout $U \subset V$, en notant $dim(U) = u$, on a :

$$\mu(U) = (-1)^{i-u} q^{\binom{i-u}{2}}$$

Car en insérant ceci dans l'égalité $f(V) = \sum_{U\subset V} \mu(U)g(U)$, on obtiendra le résultat.
Pour montrer ceci, on procède par récurrence sur $i - u$.
Si $i-u = 0$, alors $U = V$ et on a donc $\mu(U) = \mu(V) = 1 = (-1)^0 q^{\binom{0}{2}}$ et la condition est bien vérifiée. On suppose maintenant que $i > u$. Par la définition de μ et l'hypothèse de récurrence, on obtient :

$$\mu(U) = -\sum_{U\subsetneq S\subset V} \mu(S) = -\sum_{s=u+1}^{i} (-1)^{i-s} q^{\binom{i-s}{2}} \begin{bmatrix} i-u \\ s-u \end{bmatrix}_q .$$

En effet, l'hypothèse de récurrence dit que l'entier $\mu(S)$ dépend uniquement de la dimension de S, on fait donc la somme sur toutes les dimensions possibles et on

multiplie par le nombre de sous-espaces S correspondants, donné par la propriété 0.13 .
On effectue ensuite un changement de variable, $i-s$ devenant s :

$$\begin{aligned}\mu(U) &= -\sum_{s=0}^{i-u-1}(-1)^s q^{\binom{s}{2}} \begin{bmatrix} i-u \\ s \end{bmatrix}_q \\ &= -\left(\sum_{s=0}^{i-u}(-1)^s q^{\binom{s}{2}} \begin{bmatrix} i-u \\ s \end{bmatrix}_q - (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} i-u \\ i-u \end{bmatrix}_q\right) \\ &= -\sum_{s=0}^{i-u}(-1)^s q^{\binom{s}{2}} \begin{bmatrix} i-u \\ s \end{bmatrix}_q + (-1)^{i-u} q^{\binom{i-u}{2}}\end{aligned}$$

On fait alors appel au **théorème q-binomial** tel qu'il est énoncé dans le document [3], p.74 qui nous dit que $\sum_{k=0}^{j} x^k q^{\binom{k}{2}} \begin{bmatrix} j \\ k \end{bmatrix}_q = \prod_{i=0}^{j-1}(1+xq^i)$.
Dans notre cas, on a donc que $\sum_{s=0}^{i-u}(-1)^s q^{\binom{s}{2}} \begin{bmatrix} i-u \\ s \end{bmatrix}_q = \prod_{k=0}^{i-u-1}(1-q^k) = 0$, car pour $k = 0, 1-q^k = 1-1 = 0$.
On a ainsi montré le résultat.

On montre maintenant le résultat principal de cette section, initialement établi par Delsarte dans [4][Théorème 3.3].

Théorème 17 *(identités de MacWilliams pour la métrique du rang.)*
Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire. Pour tout $i \in [0, ..., k]$, on a :

$$W_i(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\sum_{j=0}^{k} W_j(\mathcal{C}) \sum_{u=0}^{k}(-1)^{i-u} q^{mu+\binom{i-u}{2}} \begin{bmatrix} k-u \\ k-i \end{bmatrix}_q \begin{bmatrix} k-j \\ u \end{bmatrix}_q$$

Preuve
Pour tout sous-espace $V \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ on définit

$$f(V) = |\{M \in \mathcal{C}^\perp \mid colspc(M) = V\}| \quad \text{et} \quad g(V) = \sum_{U\subset V} f(U) = |\mathcal{C}^\perp(V)|.$$

En appliquant le lemme 16, on a que pour tout sous-espace vectoriel V de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$ de dimension i :

$$\begin{aligned} f(V) &= \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} g(U) \\ &= \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} |\mathcal{C}^{\perp}(U)| \end{aligned}$$

on effectue un changement de variables en notant $T = U^{\perp}$

$$f(V) = \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{T\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ T\supset V^{\perp} \\ dim(T)=k-u}} |\mathcal{C}^{\perp}(T^{\perp})|$$

En appliquant l'égalité donnée par la proposition 15, on obtient :

$$\begin{aligned} f(V) &= \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{T\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ T\supset V^{\perp} \\ dim(T)=k-u}} \frac{|\mathcal{C}(T)|}{|\mathcal{C}|} q^{mu} \\ &= \frac{1}{|\mathcal{C}|} \sum_{u=0}^{i} (-1)^{i-u} q^{mu+\binom{i-u}{2}} \sum_{\substack{T\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ T\supset V^{\perp} \\ dim(T)=k-u}} |\mathcal{C}(T)| \end{aligned}$$

On peut maintenant observer que

$$\begin{aligned}
W_i(\mathcal{C}^\perp) &= \sum_{\substack{V\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(V)=i}} f(V)\\
&= \sum_{\substack{V\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(V)=i}} \frac{1}{|\mathcal{C}|}\sum_{u=0}^{i}(-1)^{i-u}q^{mu+\binom{i-u}{2}} \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ T\supset V^\perp\\ dim(T)=k-u}} |\mathcal{C}(T)|\\
&=\frac{1}{|\mathcal{C}|}\sum_{u=0}^{i}(-1)^{i-u}q^{mu+\binom{i-u}{2}} \sum_{\substack{V\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(V)=i}} \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ T\supset V^\perp\\ dim(T)=k-u}} |\mathcal{C}(T)|\\
&=\frac{1}{|\mathcal{C}|}\sum_{u=0}^{i}(-1)^{i-u}q^{mu+\binom{i-u}{2}} \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}} |\mathcal{C}(T)| \sum_{\substack{V\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ V\supset T^\perp\\ dim(V)=i}} 1
\end{aligned}$$

La dernière somme compte le nombre de sous-espaces V de dimension i tels que $T^\perp \subset V \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$, avec $dim(T^\perp) = k-(k-u) = u$.

La propriété 0.13 nous donne alors que :

$$\begin{aligned}
W_i(\mathcal{C}^\perp) =&\frac{1}{|\mathcal{C}|}\sum_{u=0}^{i}(-1)^{i-u}q^{mu+\binom{i-u}{2}} \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}} |\mathcal{C}(T)| \begin{bmatrix} k-u \\ i-u \end{bmatrix}_q\\
=&\frac{1}{|\mathcal{C}|}\sum_{u=0}^{i}(-1)^{i-u}q^{mu+\binom{i-u}{2}} \begin{bmatrix} k-u \\ i-u \end{bmatrix}_q \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}} |\mathcal{C}(T)|
\end{aligned}$$

D'autre part, on a que

$$\begin{aligned}\sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}}|\mathcal{C}(T)| &= \sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}}\sum_{j=0}^{k-u}\sum_{\substack{S\subset T\\ dim(S)=j}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|\\ &=\sum_{j=0}^{k-u}\sum_{\substack{S\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(S)=j}}\sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ T\supset S\\ dim(T)=k-u}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|\\ &=\sum_{j=0}^{k-u}\sum_{\substack{S\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(S)=j}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|\sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ T\supset S\\ dim(T)=k-u}}1\end{aligned}$$

La dernière somme compte le nombre de sous-espaces T de dimension $k-u$ tels que $S\subset T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)$, avec $dim(S)=j$. La propriété 0.13 nous donne alors que

$$\begin{aligned}\sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}}|\mathcal{C}(T)| &=\sum_{j=0}^{k-u}\sum_{\substack{S\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(S)=j}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|\begin{bmatrix}k-j\\ k-u-j\end{bmatrix}_q\\ &=\sum_{j=0}^{k-u}\begin{bmatrix}k-j\\ k-j-u\end{bmatrix}_q\sum_{\substack{S\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(S)=j}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|\end{aligned}$$

La propriété 0.12 donne alors que cette somme vaut

$$=\sum_{j=0}^{k-u}\begin{bmatrix}k-j\\ u\end{bmatrix}_q\sum_{\substack{S\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(S)=j}}|\{M\in\mathcal{C}\mid colspc(M)=S\}|$$

La dernière somme décrit ici le nombre de matrices de $\mathcal{C}$ dont l'espace engendré par les colonnes est de dimension j, c'est-à-dire le nombre de matrices de rang j, et on a donc :

$$\sum_{\substack{T\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(T)=k-u}}|\mathcal{C}(T)|=\sum_{j=0}^{k-u}\begin{bmatrix}k-j\\ u\end{bmatrix}_q W_j(\mathcal{C}).$$

En insérant cette égalité dans l'expression de $W_i(\mathcal{C}^\perp)$ trouvée précédemment, et en intervertissant les notations, on obtient la formule souhaitée.

Exemple 18 Soit $q = 5, k = 2, m = 3$.
Soit $\mathcal{C} \subset \mathcal{M}_{2\times 3}(\mathbb{F}_5)$ le code linéaire de dimension 2 engendré sur $\mathbb{F}_5$ par les matrices suivantes :

$$A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 4 \end{bmatrix} \text{ et } B = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 4 & 0 \end{bmatrix}$$

Tout élément $R \in \mathcal{C}$ est alors de la forme $R = x \cdot A + y \cdot B, \quad x, y \in \mathbb{F}_5$. Pour simplifier, on notera un tel élément $[x, y]_{\mathbb{F}_5}$.
On cherche à connaitre la distribution de poids de $\mathcal{C}$. Pour cela, on va regarder les droites vectorielles de $\mathcal{C}$, le rang étant constant sur la droite privée de 0.

Soit $R = [x, y]_{\mathbb{F}_5} \in \mathcal{C}$. Alors, si $x = 0$, on a que $R = y \cdot [0, 1]_{\mathbb{F}_5}$, i.e. $R \in Vect_{\mathbb{F}_5}([0, 1]_{\mathbb{F}_5})$.
Si $x \neq 0$, alors $R = x \cdot [1, x^{-1}y]_{\mathbb{F}_5}$, i.e. $R \in Vect_{\mathbb{F}_5}([1, x^{-1}y]_{\mathbb{F}_5})$ avec $x^{-1}y \in \mathbb{F}_5$, et donc R appartient à une droite de la forme $Vect_{\mathbb{F}_5}([1, r]_{\mathbb{F}_5}), r \in \mathbb{F}_5$.
On peut donc écrire l'ensemble des droites de $\mathcal{C}$ comme
$Vect_{\mathbb{F}_5}([0, 1]_{\mathbb{F}_5}) \cup \left(\bigcup_{r\in F_5} Vect_{\mathbb{F}_5}([1, r]_{\mathbb{F}_5})\right)$.
$\mathbb{F}_5$ ayant 5 éléments, il a 5 possibilités pour r et on a donc 6 droites possibles. Chacune de ces droites contient 4 éléments non-nuls. On peut donc obtenir la distribution de poids de $\mathcal{C}$ en calculant le rang d'un vecteur non-nul de chaque droite.
Par exemple, pour la droite $Vect_{\mathbb{F}_5}([0, 1]_{\mathbb{F}_5})$, on calcule le rang de $B = [0, 1]_{\mathbb{F}_5}$: on voit que la première ligne est égale à 2 fois la deuxième ligne, et donc $rg(B) = 1$, donc les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([0, 1]_{\mathbb{F}_5})$ sont de rang 1.
On fait de même :
$rg([1, 0]_{\mathbb{F}_5}) = rg(A) = 2$ car les deux lignes de A sont clairement $\mathbb{F}_5$-indépendantes : les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([1, 0]_{\mathbb{F}_5})$ sont donc de rang 2.
$rg([1, 1]_{\mathbb{F}_5}) = rg\left(\begin{bmatrix} 3 & 3 & 2 \\ 1 & 1 & 4 \end{bmatrix}\right) = 1$ car la première ligne est égale à 3 fois la deuxième : les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([1, 1]_{\mathbb{F}_5})$ sont donc de rang 1.
$rg([1, 2]_{\mathbb{F}_5}) = rg\left(\begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 4 \end{bmatrix}\right) = 2$ car les deux lignes sont clairement $\mathbb{F}_5$-indépendantes : les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([1, 2]_{\mathbb{F}_5})$ sont donc de rang 2.
$rg([1, 3]_{\mathbb{F}_5}) = rg\left(\begin{bmatrix} 2 & 4 & 2 \\ 3 & 4 & 4 \end{bmatrix}\right) = 2$ car les deux lignes sont clairement $\mathbb{F}_5$-indépendantes : les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([1, 3]_{\mathbb{F}_5})$ sont donc de rang 2.
$rg([1, 4]_{\mathbb{F}_5}) = rg\left(\begin{bmatrix} 4 & 2 & 2 \\ 4 & 3 & 4 \end{bmatrix}\right) = 2$ car les deux lignes sont clairement $\mathbb{F}_5$-indépendantes : les 4 éléments non-nuls de $Vect_{\mathbb{F}_5}([1, 4]_{\mathbb{F}_5})$ sont donc de rang 2.
A cela s'ajoute la matrice nulle, unique élément de $\mathcal{C}$ de rang 0.

On trouve ainsi que $W_0(\mathcal{C}) = 1, W_1(\mathcal{C}) = 8$ et $W_2(\mathcal{C}) = 16$.

En utilisant le théorème 17 et la propriété 0.12, on trouve que $W_0(\mathcal{C}^\perp) = 1, W_1(\mathcal{C}^\perp) = 64$ et $W_2(\mathcal{C}^\perp) = 560$.
De plus, on a $dim(\mathcal{C}^\perp) = 6 - dim(\mathcal{C}) = 6 - 2 = 4$, donc $|\mathcal{C}^\perp| = 5^4 = 625$, et donc on retrouve bien que $|\mathcal{C}^\perp| = \sum_{i=0}^{2} W_i(\mathcal{C}^\perp)$.

On peut également montrer une autre version des identités de MacWilliams, qui se présente comme une "formule sommatoire de Poisson".

Théorème 19 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire. Pour tout $0 \leq v \leq k$, on a :

$$\sum_{i=0}^{k-v} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ v \end{bmatrix}_q = \frac{|\mathcal{C}|}{q^{mv}} \sum_{j=0}^{v} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ v-j \end{bmatrix}_q$$

Preuve
La proposition 15 nous donne :

$$\begin{aligned}
\sum_{\substack{\mathcal{U}\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(\mathcal{U})=k-v}} |\mathcal{C}(\mathcal{U})| &= \sum_{\substack{\mathcal{U}\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(\mathcal{U})=k-v}} \frac{|\mathcal{C}|}{q^{mv}} |\mathcal{C}^\perp(\mathcal{U}^\perp)| \\
&= \frac{|\mathcal{C}|}{q^{mv}} \sum_{\substack{\mathcal{U}\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(\mathcal{U})=k-v}} |\mathcal{C}^\perp(\mathcal{U}^\perp)| \\
&= \frac{|\mathcal{C}|}{q^{mv}} \sum_{\substack{\mathcal{U}\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(\mathcal{U})=v}} |\mathcal{C}^\perp(\mathcal{U})|
\end{aligned}$$

On peut écrire que :

$$\begin{aligned}
\sum_{\substack{U\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(U)=k-v}} |\mathcal{C}(U)| &= |\{(U, M) \mid U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q), dim(U) = k-v, M \in \mathcal{C}, colspc(M) \subset U\}| \\
&= \sum_{M\in\mathcal{C}} |\{U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q), dim(U) = k-v, colspc(M) \subset U\}| \\
&= \sum_{i=0}^{k} \sum_{\substack{M\in\mathcal{C} \\ rg(M)=i}} |\{U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q), dim(U) = k-v, colspc(M) \subset U\}|
\end{aligned}$$

la somme à i, M fixé est le nombre de sous-espaces U de dimension $k - v$ tels que $colspc(M) \subset U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$, avec $dim(colspc(M)) = i$. La propriété 0.13 nous donne

alors que :

$$\sum_{\substack{U\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(U)=k-v}} |\mathcal{C}(U)| = \sum_{i=0}^{k} \sum_{\substack{M\in\mathcal{C}\\ rg(M)=i}} \begin{bmatrix} k-i \\ k-v-i \end{bmatrix}_q = \sum_{i=0}^{k-v} W_i(\mathcal{C}) \begin{bmatrix} k-i \\ v \end{bmatrix}_q$$

En reprenant le même raisonnement avec $\mathcal{C}^\perp$, on trouve que :

$$\sum_{\substack{U\subset\mathcal{M}_{k\times 1}(\mathbb{F}_q)\\ dim(U)=v}} |\mathcal{C}^\perp(U)| = \sum_{j=0}^{k-v} W_j(\mathcal{C}^\perp) \begin{bmatrix} k-j \\ v-j \end{bmatrix}_q$$

En appliquant ces deux résultats à l'égalité dérivée de la proposition 15, on obtient l'énoncé du théorème.

Remarque 20 Les formulations des identités de MacWilliams données par les théorèmes 17 et 19 sont équivalentes.
Le premier sens de l'implication est fait dans le document [5],[Théorème 64], dans la démonstration du théorème 19 utilisant le théorème 17, tandis que la réciproque est faite dans le document [6],[Corollaire 1 et Proposition 3].

On obtient le résultat de dénombrement suivant en appliquant le théorème 17.

Corollaire 21 Soit $I \subset \{(i,j) \in [1,\ \dots\ ,k] \times [1,\ \dots\ ,m] \mid i = j\}$ un ensemble de positions de coefficietns diagonaux.
Pour tout $0 \leq r \leq k$, le nombre de matrices $M \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$ de rang r telles que $m_{i,j} = 0$ pour tout $(i,j) \in I$ est :

$$q^{-|I|} \sum_{t=0}^{k} \binom{|I|}{t} (q-1)^t \sum_{u=0}^{k} (-1)^{r-u} q^{mu+\binom{r-u}{2}} \begin{bmatrix} k-u \\ k-r \end{bmatrix}_q \begin{bmatrix} k-t \\ u \end{bmatrix}_q$$

Preuve
On définit le code linéaire $\mathcal{C} = \{M \in \mathcal{M}_{k\times m}(\mathbb{F}_q) \mid m_{i,j} = 0 \text{ pour tout } (i,j) \notin I\} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$.
On a alors que $dim(\mathcal{C}) = |I|$, toute $M \in \mathcal{C}$ étant nulle sauf peut-être sur ses coefficients d'indices dans I. Il en découle également que M peut être au plus de rang $|I|$, et que si on cherche à exhiber une matrice $M \in \mathcal{C}$ de rang $t \leq |I|$, alors il s'agit de choisir t

coefficients possibles parmi les éléments de I, et associer à chacun un élément de ${\mathbb{F}_q}^*$. On en déduit que :

$$W_t(\mathcal{C}) = \begin{cases} 0 \text{ pour } |I| < t \leq k \\ \binom{|I|}{t}(q-1)^t \text{ pour } 0 \leq t \leq |I| \end{cases}$$

De plus $\mathcal{C}^\perp = \{M \in \mathcal{M}_{k\times m}(\mathbb{F}_q) \mid m_{i,i} = 0 \text{ pour tout } (i,i) \in I\}$.
Ainsi le nombre de matrices $M \in \mathcal{M}_{k\times m}(\mathbb{F}_q)$ de rang r telles que $m_{i,j} = 0$ pour tout $(i,j) \in I$ est $W_r(\mathcal{C}^\perp)$.
Le théorème 17 nous dit alors que ce nombre a bien la valeur recherchée.

4 Codes MRD

Dans cette section, on va s'intéresser aux codes ayant le plus grand cardinal possible pour leurs paramètres.On dénommera ces codes comme **MRD**, pour "maximum rank distance".
On commencera par établir la borne de Singleton, qui impose une borne supérieure au cardinal d'un code. On verra ensuite qu'il est toujours possible de construire un code qui atteint cette borne, puis on caractérisera les codes qui atteignent les bornes en se servant d'une relation avec leurs codes duaux.
Enfin, on s'intéressera aux distributions de poids et de distance pour ces codes.

Théorème 22 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code avec $|\mathcal{C}| \geq 2$ et de distance minimale d. Alors $|\mathcal{C}| \leq q^{m(k-d+1)}$.

Preuve
Notons $\pi : \mathcal{C} \to \mathcal{M}_{(k-d+1)\times m}(\mathbb{F}_q)$ la projection qui à une matrice de $\mathcal{C}$ associe ses $k-d+1$ dernières lignes.
On montre que π est injective : en effet, si il existe $M, N \in \mathcal{C}$ tels que $\pi(M) = \pi(N)$, alors les $k-d+1$ dernières lignes de ces deux matrices sont égales, ce qui signifie que $M - N$ a au plus $d-1$ lignes non-nulles. On a donc que $d(M,N) = rg(M-N) \leq d-1 < d$, or $\mathcal{C}$ a pour distance minimale d, on a donc $M = N$.
π étant injective, on a $|\mathcal{C}| = |\pi(\mathcal{C})| \leq q^{m(k-d+1)}$.

Définition 23 On dit qu'un code $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ est un code **MRD** is $|\mathcal{C}| = 1$, ou $|\mathcal{C}| \geq 2$ et $|\mathcal{C}| = q^{m(k-d+1)}$, d étant la distance minimale de $\mathcal{C}$.

On veut maintenant prouver qu'il est toujours possible de construire un code MRD pour une distance minimale donnée. La preuve de ce théorème utilisant des polynômes linéarisés, on va commence par rappeler les propriétés qu'on compte utiliser.

Remarque 24
On rapelle qu'un **polynôme linéarisé** p sur $\mathbb{F}_{q^m}$ est un polynôme de la forme :

$$p(x) = \alpha_0 x + \alpha_1 x^q + \alpha_2 x^{q^2} + ... + \alpha_s x^{q^s}, \quad \text{avec } \alpha_i \in \mathbb{F}_{q^m} \quad \text{pour } i \in [0, \ ... \ , s]$$

Un tel polynôme est $\mathbb{F}_q$-linéaire car, pour tout $i \in [0, ..., s]$, l'application $x \mapsto x^{q^i}$ est une itération de morphismes de Frobenius.
On appellera q-degré de p le plus grand i tel que $\alpha_i \neq 0$, noté $deg_q(p)$. L'ensemble des polynômes linéarisés sur $\mathbb{F}_{q^m}$ de degré au plus s forme un espace vectoriel sur $\mathbb{F}_{q^m}$, noté $Lin_q(m, s)$.
On peut facilement voir que $dim_{\mathbb{F}_{q^m}}(Lin_q(m, s)) = s + 1$, l'ensemble des e_i, pour $0 \leq i \leq s$, définis par $e_i(x) = x^{q^i}$ formant une base.
Les racines d'un polynôme linéarisé p forment un sous-espace vectoriel de $\mathbb{F}_{q^m}$, du fait de la $\mathbb{F}_q$-linéarité de p,que l'on notera comme $V(p)$. Le polynôme aura au plus $q^{deg_q(p)}$ racines distinctes au vu de son degré, et on a ainsi que $|V(p)| \leq q^{deg_q(p)}$, i.e. $dim_{\mathbb{F}_q} V(p) \leq deg_q(p)$.

Théorème 25 Pour tout $1 \leq d \leq k$, il existe un code vectoriel $\mathbb{F}_{q^m}$-linéaire $\mathcal{C} \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ tel que $d_G(\mathcal{C}) = d$ et $dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = k - d + 1$.
En particulier, il existe un code linéaire MRD $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ tel que $d(\mathcal{C}) = d$

Preuve
Soit $E = \{b_1, ..., b_k\}$ une famille $\mathbb{F}_q$-libre d'éléments de $\mathbb{F}_{q^m}$. On suppose $k \leq m$, donc il est bien possible de trouver k éléments $\mathbb{F}_q$-linéairement indépendants dans $\mathbb{F}_{q^m}$.
On considère l'application $\mathbb{F}_{q^m}$-linéaire $ev_E : Lin_q(m, k-d) \to \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ définie par $ev_E(p) = (p(b_1), ..., p(b_k))$.
On cherche maintenant à montrer que, si on définit $\mathcal{C}$ comme $\mathcal{C} = ev_E(Lin_q(m, k - d)) \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$, alors $\mathcal{C}$ est un code vectoriel ayant les propriétés désirées.
De plus, la proposition 10 nous permettra d'obtenir un code linéaire de distance minimale d et de dimension $m(k - d + 1)$ et qui sera donc MRD.

On a clairement que $\mathcal{C}$ est $\mathbb{F}_{q^m}$-linéaire de par la linéarité de ev_E.
Soit $p \in Lin_q(m, k-d)$ un polynône linéarisé non-nul, et soit $W \subset \mathbb{F}_{q^m}$ le sous-espace vectoriel engendré par les évaluations $p(b_1), ..., p(b_k)$, i.e. $W = Vect_{\mathbb{F}_q}(p(b_1), ...p(b_k))$.
Ce polynôme p induit une application linéaire évaluation $\widetilde{p} : Vect_{\mathbb{F}_q}(b_1, ..., b_k) \to \mathbb{F}_{q^m}$.
De par la linéarité de $\widetilde{p}$, l'image de cette application est W, car $\widetilde{p}(Vect_{\mathbb{F}_q}(b_1, ..., b_k)) = Vect_{\mathbb{F}_q}(p(b_1), ...p(b_k))$, tandis que le noyau de $\widetilde{p}$, c'est-à-dire l'ensemble de ses racines,

est $V(p)$. Le théorème du rang nous donne alors que $dim_{\mathbb{F}_q}(Im(\widetilde{p}))+dim_{\mathbb{F}_q}(Ker(\widetilde{p})) = dim_{\mathbb{F}_q}(Vect_{\mathbb{F}_q}(b_1,...,b_k))$, i.e. $dim_{\mathbb{F}_q}(W) + dim_{\mathbb{F}_q}(V(p)) = k$.
On a donc que $dim_{\mathbb{F}_q}(W) = k - dim_{\mathbb{F}_q}(V(p))$, et la remarque 24 nous dit que $dim_{\mathbb{F}_q}V(p) \leq deg(p) \leq k-d$, ce qui aboutit à $dim_{\mathbb{F}_q}(W) \geq k-(k-d) = d$.
Cela signifie que la dimension de l'espace engendré par un vecteur quelconque non-nul v de
$\mathcal{C} = ev_E(Lin_q(m, k-d))$ est au moins d, i.e. on a que $rg_G(v) \geq d$. Or $\mathcal{C}$ est linéaire, donc en reprenant le raisonnement fait après la definition 4 et en l'étendant aux codes vectoriels, on a que $d_G(\mathcal{C}) = min\{rg_G(v)|v \in \mathcal{C}, v \neq 0\}$. On en déduit que $d_G(\mathcal{C}) \geq d$.
En particulier, vu que $d \geq 1$, l'application ev_E est injective, et il en découle que $dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = dim_{\mathbb{F}_{q^m}}(Lin_q(m, k-d)) = k-d+1$.
La proposition 10 nous donne alors que le code linéaire matriciel associé est de dimension $m(k-d+1)$, et le théorème 22 nous dit que cette dimension doit être inférieure ou égale à $m(k-d_G(\mathcal{C})+1)$. On en déduit que $d_G(\mathcal{C}) \leq d$.
On peut donc conclure que $d_G(\mathcal{C}) = d$, et $dim_{\mathbb{F}_{q^m}}(\mathcal{C}) = k-d+1$: le code vectoriel $\mathcal{C}$ a bien les propriétés souhaitées ,et cela montre le théorème.

On va maintenant montrer un lemme et un théorème qui nous seront utiles pour caractériser les codes MRD par une relation avec leurs codes duaux.
Le lemme nous servira à montrer le théorème, qui permettra directement d'obtenir la caractérisation recherchée.

Lemme 26 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code MRD avec $|\mathcal{C}| \geq 2$ et distance minimale d. Pour tout sous-espace vectoriel $U \subset \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ avec $u = dim(U) \geq d-1$, on a alors :

$$|\mathcal{C}(U)| = q^{m(u-d+1)}$$

ou $\mathcal{C}(U)$ suit la notation 13.

Preuve
On définit comme dans le lemme 14 le sous-espace vectoriel $V = \{(x_1,...,x_k)^t \in \mathcal{M}_{k\times 1}(\mathbb{F}_q) \mid x_i = 0 \text{ pour tout } i > u\}$.
Soit $g : \mathcal{M}_{k\times 1}(\mathbb{F}_q) \to \mathcal{M}_{k\times 1}(\mathbb{F}_q)$ un isomorphisme tel que $g(U) = V$. On note $G \in \mathcal{M}_{k\times k}(\mathbb{F}_q)$ sa matrice dans la base canonique de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$. On définit alors le code $\mathcal{D} = G\mathcal{C} = \{GM|M \in \mathcal{C}\}$.
De façon évidente, $\mathcal{D}$ a la même dimension et la même distance minimale que $\mathcal{C}$. En particulier, $\mathcal{D}$ est un un code MRD.
De plus, si $M \in \mathcal{C}(U)$, alors ses colonnes forment une base d'un sous-espace de U, donc les colonnes de GM forment une base d'un sous-espace de $g(U) = V$. Il en découle que $\mathcal{D}(V) = g(\mathcal{C}(U))$. On considère maintenant les applications linéaires

$$\mathcal{D} \xrightarrow{\pi_1} \mathcal{M}_{(k-d+1)\times m}(\mathbb{F}_q) \xrightarrow{\pi_2} \mathcal{M}_{(k-u)\times m}(\mathbb{F}_q)$$

où π_1 est la projection sur les $k-d+1$ dernières lignes, et π_2 la projection sur les $k-u$ dernières lignes.
On a que la distance minimale de $\mathcal{D}$ est d, et on peut donc montrer que π_1 est injective de la même façon que dans la preuve du théorème 22. $\mathcal{D}$ étant MRD, on a donc également que $|\mathcal{D}| = q^{(k-d+1)m} = |\mathcal{M}_{(k-d+1)\times m}(\mathbb{F}_q)|$. π_1 est donc également surjective. On a ainsi que π_1 est bijective.
De plus, π_2 est $\mathbb{F}_q$-linéaire, et est surjective car pour toute matrice dans $\mathcal{M}_{(k-u)\times m}(\mathbb{F}_q)$, on peut toujours trouver un antécédent dans $\mathcal{M}_{(k-d+1)\times m}(\mathbb{F}_q)$.
En effet, si on prend $M \in \mathcal{M}_{(k-u)\times m}(\mathbb{F}_q)$, alors $\pi_2^{-1}(M)$ est l'ensemble des matrices de $\mathcal{M}_{(k-d+1)\times m}(\mathbb{F}_q)$ telles que leurs $k-u$ dernières lignes soient fixées pour correspondre aux lignes de M, tandis que leurs $(k-d+1)-(k-u) = u-d+1$ premières lignes sont quelconques ; on a donc $m(u-d+1)$ coefficients qu'on peut choisir librement dans $\mathbb{F}_q$. On a donc alors que, pour tout $M \in \mathcal{M}_{(k-u)\times m}(\mathbb{F}_q)$:

$$|\pi_2^{-1}(M)| = |\pi_2^{-1}(0)| = q^{m(u-d+1)}$$

L'application π_1 étant bijective, on peut étendre le raisonnement, et si on considère l'application $\pi = \pi_2 \circ \pi_1$ qui est surjective, on a alors que, pour tout $M \in \mathcal{M}_{(k-u)\times m}(\mathbb{F}_q)$:

$$|\pi^{-1}(M)| = |\pi^{-1}(0)| = q^{m(u-d+1)}$$

Enfin, pour $M \in \mathcal{D}$, dire que $colspc(M) \subset V$ revient à dire que les $k-u$ dernières lignes de M sont nulles. On a donc que $\mathcal{D}(V) = \pi^{-1}(0)$.
Le lemme découle alors de l'égalité $|\mathcal{C}(U)| = |\mathcal{D}(V)| = |\pi^{-1}(0)|$.

Théorème 27 Soit $\mathcal{C}$ un code linéaire MRD. Alors $\mathcal{C}^\perp$ est également MRD.

Preuve

Si $dim(\mathcal{C}) \in \{0, km\}$, alors $dim(\mathcal{C}^\perp) \in \{km, 0\}$ et le résultat est immédiat. On considère donc le cas où $1 \leq dim(\mathcal{C}) \leq km-1$.
Notons d et $d^\perp$ les distances minimales de $\mathcal{C}$ et $\mathcal{C}^\perp$. En appliquant le théorème 22, on obtient

$$dim(\mathcal{C}) \leq m(k-d+1), \text{ et } dim(\mathcal{C}^\perp) \leq m(k-d^\perp+1).$$

Ainsi, $km = dim(\mathcal{C}) + dim(\mathcal{C}^\perp) \leq 2mk - m(d+d^\perp) + 2m$ et en reformulant on obtient

$$d + d^\perp \leq k+2. \tag{4}$$

Soit U un sous-espace vectoriel de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$ tel que $dim(U) = k-d+1$. En utilisant la proposition 15, on a que

$$|\mathcal{C}^\perp(U)| = \frac{|\mathcal{C}^\perp|}{q^{m(d-1)}} |\mathcal{C}(U^\perp)|. \tag{5}$$

Or $dim(U^\perp) = k - dim(U) = d - 1$. En appliquant le lemme 26, on trouve que $|\mathcal{C}(U^\perp)| = q^{m(d-1-d+1)} = q^0 = 1$. De plus, $\mathcal{C}$ est MRD donc $|\mathcal{C}| = q^{m(k-d+1)}$, i.e. $dim(\mathcal{C}) = m(k-d+1)$ et $dim(\mathcal{C}^\perp) = km - dim(\mathcal{C}) = km - m(k-d+1) = m(d-1)$, donc $|\mathcal{C}^\perp| = q^{m(d-1)}$.
On peut donc simplifier (5) pour obtenir :

$$|\mathcal{C}^\perp(U)| = \frac{|\mathcal{C}^\perp|}{q^{m(d-1)}}|\mathcal{C}(U^\perp)| = \frac{q^{m(d-1)}}{q^{m(d-1)}} = 1$$

On en déduit donc que $\mathcal{C}^\perp(U) = \{0\}$, et ce pour tout U tel que $dim(U) = k - d + 1$; c'est donc que toutes les matrices non-nulles de $\mathcal{C}^\perp$ ont un rang strictement supérieur à $k-d+1$. Or $\mathcal{C}^\perp$ est un code linéaire comme $\mathcal{C}$, et on a donc que $d^\perp = \min\{rg(M) \mid M \in \mathcal{C}^\perp, M \neq 0\}$. Ceci nous permet de déduire que $d^\perp \geq k - d + 2$.
Cette inégalité, associée à (4), nous permet d'obtenir que $d^\perp = k-d+2$, et on a déjà vu plus haut que que $|\mathcal{C}^\perp| = q^{m(d-1)} = q^{m(k-(k-d+2)+1)} = q^{m(k-d^\perp+1)}$. On a donc que $\mathcal{C}^\perp$ est MRD.

Ce lemme et ce théorème étant démontrés, on peut maintenant les utiliser pour montrer la caractérisation suivante.

Proposition 28 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire tel que $1 \leq dim(\mathcal{C}) \leq km - 1$. Les propositions suivantes sont équivalentes :

1. $\mathcal{C}$ est MRD
2. $\mathcal{C}^\perp$ est MRD
3. $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 2$

Preuve
Puisque $\mathcal{C} = (\mathcal{C}^\perp)^\perp$, l'équivalence entre 1) et 2) découle directement du théorème 27. On peut donc se contenter de montrer que 1) et 2) entraînent 3), et que 3) entraîne 1)
Supposons que $\mathcal{C}$ et $\mathcal{C}^\perp$ sont MRD.
On a que $dim(\mathcal{C}) = m(k - d(\mathcal{C}) + 1)$ et $dim(\mathcal{C}^\perp) = m(k - d(\mathcal{C}^\perp) + 1)$. On obtient donc :

$$\begin{aligned} km &= dim(\mathcal{C}) + dim(\mathcal{C}^\perp) = m(k - d(\mathcal{C}) + 1) + m(k - d(\mathcal{C}^\perp) + 1) \\ k &= k - d(\mathcal{C}) + 1 + k - d(\mathcal{C}^\perp) + 1 \\ d(\mathcal{C}) &+ d(\mathcal{C}^\perp) = k + 2 \end{aligned}$$

et on a ainsi montré 3). Supposons maintenant que $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 2$.
En appliquant le théorème 22, on a alors

$$dim(\mathcal{C}) \leq m(k - d(\mathcal{C}) + 1)$$

et également

$$\begin{aligned} dim(\mathcal{C}^\perp) &\leq m(k - d(\mathcal{C}^\perp) + 1) \\ km - dim(\mathcal{C}) &\leq m(k - (k + 2 - d(\mathcal{C})) + 1) \\ dim(\mathcal{C}) &\geq km - m(d(\mathcal{C}) - 1) \\ dim(\mathcal{C}) &\geq m(k - d(\mathcal{C}) + 1) \end{aligned}$$

Les deux inégalités nous donnent que $dim(\mathcal{C}) = m(k - d(\mathcal{C}) + 1)$ et donc que $\mathcal{C}$ est MRD : on a prouvé 1).

On va maintenant chercher à calculer la distribution de poids d'un code MRD. Le théorème suivant est très utile car qu'il nous donne directement l'expression des éléments de la distribution de poids.

Théorème 29 Soit $\mathcal{C}$ un code MRD tel que $|\mathcal{C}| \geq 2$ et $0 \in \mathcal{C}$. Notons $d = d(\mathcal{C})$.
Alors $W_0(\mathcal{C}) = 1$; pour $1 \leq i \leq d-1$ on a $W_i(\mathcal{C}) = 0$, et pour $d \leq i \leq k$ on a

$$W_i(\mathcal{C}) = \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2} + m(u-d+1)} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q$$

Preuve
On a $0 \in \mathcal{C}$, donc $W_0(\mathcal{C}) = 1$, et pour $1 \leq i \leq d-1$ on a $W_i(\mathcal{C}) = 0$ par définition de d.
Pour tout sous-espace vectoriel V de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$, on définit

$$f(V) = |\{M \in \mathcal{C} | colspc(M) = V\}|, \qquad g(V) = \sum_{U \subset V} f(U) = |\mathcal{C}(V)|.$$

On fixe $d \leq i \leq k$ et on choisit un sous-espace vectoriel V de dimension i. En appliquant le lemme 16, on obtient :

$$f(V) = \sum_{u=0}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U \subset V \\ dim(U) = u}} g(U)$$

De plus, $\mathcal{C}$ est MRD avec $0 \in \mathcal{C}$, donc le lemme 26 nous permet d'obtenir que pour tout sous-espace vectoriel U de $\mathcal{M}_{k\times 1}(\mathbb{F}_q)$,

$$g(U) = \begin{cases} 1 & \text{si } 0 \leq dim(U) \leq d-1 \\ q^{m(u-d+1)} & \text{si } d \leq dim(U) \leq k \end{cases}$$

On a donc que

$$\begin{aligned} f(V) &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} g(U) + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} g(U) \\ &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} 1 + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} q^{m(u-d+1)} \\ &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \sum_{\substack{U\subset V \\ dim(U)=u}} 1 + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}+m(u-d+1)} \sum_{\substack{U\subset V \\ dim(U)=u}} 1 \\ &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} i \\ u \end{bmatrix}_q \end{aligned}$$

Pour obtenir le résultat, il suffit alors de considérer l'égalité

$$\begin{aligned} W_i(\mathcal{C}) &= \sum_{\substack{V\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(V)=i}} f(V) \\ &= \sum_{\substack{V\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(V)=i}} \left(\sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} i \\ u \end{bmatrix}_q \right) \\ &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} i \\ u \end{bmatrix}_q \sum_{\substack{V\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(V)=i}} 1 + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} i \\ u \end{bmatrix}_q \sum_{\substack{V\subset \mathcal{M}_{k\times 1}(\mathbb{F}_q) \\ dim(V)=i}} 1 \\ &= \sum_{u=0}^{d-1} (-1)^{i-u} q^{\binom{i-u}{2}} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i} (-1)^{i-u} q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q \end{aligned}$$

Ce théorème montre en particulier que la distribution de poids d'un code MRD, éventuellement non-linéaire mais contenant 0, est entièrement déterminée par k, m et sa distance minimale.
Il en découle immédiatement un résultat analogue sur la distribution de distances.

Corollaire 30 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code MRD tel que $|\mathcal{C}| \geq 2$ et de distance minimale d.
On a alors $D_0(\mathcal{C}) = 1$; pour $1 \leq i \leq d-1$ on a $D_i(\mathcal{C}) = 0$, et pour $d \leq i \leq k$

$$D_i(\mathcal{C}) = \sum_{u=0}^{d-1}(-1)^{i-u}q^{\binom{i-u}{2}} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i}(-1)^{i-u}q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q$$

Preuve
On peut calculer aisément pour $i = 0$, car $D_0(\mathcal{C}) = \frac{1}{|\mathcal{C}|} \cdot |\{(M, N) \in \mathcal{C}^2 \mid M - N = 0\}| = \frac{|\mathcal{C}|}{|\mathcal{C}|} = 1$.
Pour les cas $1 \leq i \leq d-1$, on a $D_i(\mathcal{C}) = 0$ puisque la distance minimale de $\mathcal{C}$ est d.
On fixe maintenant i tel que $d \leq i \leq k$. Pour tout $N \in \mathcal{C}$, on note $\mathcal{C} - N = \{M - N | M \in \mathcal{C}\}$. On a alors que

$$|\mathcal{C}| \cdot D_i(\mathcal{C}) = |\{(M, N) \in \mathcal{C}^2 \mid rg(M - N) = i\} = \sum_{N\in\mathcal{C}} W_i(\mathcal{C} - N)$$

Or $|\mathcal{C} - N| = |\mathcal{C}|$, donc $\mathcal{C} - N$ est un code MRD et par construction $0 \in \mathcal{C} - N$.
En notant $T = \sum_{u=0}^{d-1}(-1)^{i-u}q^{\binom{i-u}{2}} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q + \sum_{u=d}^{i}(-1)^{i-u}q^{\binom{i-u}{2}+m(u-d+1)} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} i \\ u \end{bmatrix}_q$,
on a par le théorème 29 que pour tout $N \in \mathcal{C}$, $W_i(\mathcal{C} - N) = T$.
Par suite

$$|\mathcal{C}| \cdot D_i(\mathcal{C}) = \sum_{N\in\mathcal{C}} T = |\mathcal{C}| \cdot T$$

et cela termine la preuve.

Ces résultats se situent dans le cas où $\mathcal{C}$ est un code MRD, ce qui est équivalent selon la proposition 28 à dire que $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 2$.
On va voir si on ne peut pas obtenir des informations sur la distribution de poids, même avec une condition légèrement différente.
Le théorème suivant nous permettra de déduire un tel corollaire dans le cas où $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k+1$; on l'admet sans preuve, mais celle-ci peut se trouver dans [7], Théorème 25.

Théorème 31 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire avec $dim(\mathcal{C}) = t$, tel que $1 \leq t \leq km - 1$. On note sa distance minimale $d = d(\mathcal{C})$, et la distance minimale de son code dual $d^\perp = d(\mathcal{C}^\perp)$.

Soit $\epsilon = 1$ si $\mathcal{C}$ est MRD, et $\epsilon = 0$ sinon. On a alors que, pour tout $1 \leq i \leq d^\perp$,

$$\begin{aligned} W_{k-d^\perp+i}(\mathcal{C}) =& (-1)^i q^{\binom{i}{2}} \sum_{u=d^\perp}^{k-d} \begin{bmatrix} u \\ d^\perp - i \end{bmatrix}_q \begin{bmatrix} u - d^\perp + i - 1 \\ i - 1 \end{bmatrix}_q W_{k-u}(\mathcal{C}) \\ &+ \begin{bmatrix} k \\ d^\perp - i \end{bmatrix}_q \sum_{u=0}^{i-1-\epsilon} (-1)^u q^{\binom{u}{2}} \begin{bmatrix} k - d^\perp + i \\ u \end{bmatrix}_q (q^{t-m(d^\perp-i+u)} - 1) \end{aligned}$$

En particulier, les paramètres $k, m, t, d, d^\perp$ ainsi que $W_d(\mathcal{C}), ..., W_{k-d^\perp}(\mathcal{C})$ déterminent complètement la distribution de poids de $\mathcal{C}$.

Corollaire 32 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code linéaire tel que $1 \leq dim(\mathcal{C}) \leq km - 1$ et $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 1$.
Alors $dim(\mathcal{C}) \not\equiv 0\ [m]$, et $d(\mathcal{C}) = k - \lceil dim(\mathcal{C})/m \rceil + 1$, où $\lceil . \rceil$ réfère à l'arrondi au supérieur, i.e. si $\lfloor . \rfloor$ est la partie entière, alors $\lceil x \rceil = \lfloor x \rfloor + 1$.
De plus, pour $d \leq i \leq k$ on a

$$W_i(\mathcal{C}) = \begin{bmatrix} k \\ i \end{bmatrix}_q \sum_{u=0}^{i-d(\mathcal{C})} (-1)^u q^{\binom{u}{2}} \begin{bmatrix} i \\ u \end{bmatrix}_q \left(q^{dim(\mathcal{C})-m(k+u-i)} - 1\right)$$

Preuve
On suppose par l'absurde qu'il existe $a \in \mathbb{N}$ tel que $dim(\mathcal{C}) = am$. En appliquant le théorème 22, on obtient :

$$\begin{aligned} dim(\mathcal{C}) &\leq m(k - d(\mathcal{C}) + 1) \\ am &\leq m(k - d(\mathcal{C}) + 1) \\ d(\mathcal{C}) &\leq k - a + 1 \end{aligned}$$

Et pour $\mathcal{C}^\perp$, avec $dim(\mathcal{C}^\perp) = mk - dim(\mathcal{C}) = m(k - a)$, on a de même

$$\begin{aligned} dim(\mathcal{C}^\perp) &\leq m(k - d(\mathcal{C}^\perp) + 1) \\ m(k - a) &\leq m(k - d(\mathcal{C}^\perp) + 1) \\ d(\mathcal{C}^\perp) &\leq a + 1 \end{aligned}$$

On obtient ainsi deux inégalités :

$$d(\mathcal{C}) \leq k - a + 1, \quad \text{et} \quad d(\mathcal{C}^\perp) \leq a + 1$$

Si l'une de ces deux inégalités était une égalité, on pourrait remonter les calculs pour obtenir que $\mathcal{C}$ ou $\mathcal{C}^\perp$ est MRD. $\mathcal{C}$ étant linéaire, par la proposition 28 les deux serait

MRD et on aurait également que $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 2$, ce qui est en contradiction avec l'énoncé.
On a donc que ces deux inégalités sont strictes, ce qui peut se formuler sous la forme des inégalités

$$d(\mathcal{C}) \leq k - a, \quad \text{et} \quad d(\mathcal{C}^\perp) \leq a \tag{6}$$

Or ceci entraîne que $d(\mathcal{C}) + d(\mathcal{C}^\perp) \leq k$, ce qui est également en contradiction avec l'énoncé.
On en déduit donc qu'il n'existe pas de $a \in \mathbb{N}$ tel que $dim(\mathcal{C}) = am$, et donc que $dim(\mathcal{C}) \not\equiv 0\ [m]$.
D'autre part, si on pose $dim(\mathcal{C}) = am + b$, avec $a \in \mathbb{N}$ et $1 \leq b \leq m - 1$, le théorème 22 nous donne :

$$\begin{aligned} dim(\mathcal{C}) &\leq m(k - d(\mathcal{C}) + 1) \\ am + b &\leq m(k - d(\mathcal{C}) + 1) \\ d(\mathcal{C}) &\leq k - \frac{am + b}{m} + 1 \end{aligned}$$

Du fait que $d(\mathcal{C})$ est entier, on a

$$d(\mathcal{C}) \leq k - \left\lceil \frac{am + b}{m} \right\rceil + 1 = k - a$$

Un raisonnement analogue pour $\mathcal{C}^\perp$ nous permet d'obtenir deux inégalités :

$$d(\mathcal{C}) \leq k - \left\lceil \frac{am + b}{m} \right\rceil + 1 = k - a, \quad \text{et} \quad d(\mathcal{C}^\perp) \leq k - \left\lceil \frac{km - am - b}{m} \right\rceil = a + 1$$

Or, pour que la condition $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 1$ soit respectée, il faut que les deux inégalités soient des égalités ; on abtient alors que :

$$d(\mathcal{C}) = k - \left\lceil \frac{am + b}{m} \right\rceil + 1 = k - \left\lceil \frac{dim(\mathcal{C})}{m} \right\rceil + 1$$

Reste à calculer la valeur de $W_i(\mathcal{C})$ pour $d(\mathcal{C}) \leq i \leq k$.
Si $1 \leq j \leq d(\mathcal{C}^\perp)$, alors par hypothèse que $(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 1$,

$$\begin{aligned} &1 \leq j \leq k + 1 - d(\mathcal{C}) \\ &0 \leq j + 1 \leq k - d(\mathcal{C}) \\ &d(\mathcal{C}) \leq j + d(\mathcal{C}) + 1 \leq k \\ &d(\mathcal{C}) \leq j + k - d(\mathcal{C}^\perp) \leq k \end{aligned}$$

donc on peut obtenir les $W_i(\mathcal{C})$ en calculant les $W_{k-d^\perp+j}(\mathcal{C})$, avec $k - d^\perp + j = i$.
Or, si on note $t = dim(\mathcal{C})$, le théorème 31 nous dit que

$$\begin{aligned} W_{k-d^\perp+j}(\mathcal{C}) =& (-1)^j q^{\binom{j}{2}} \sum_{u=d^\perp}^{k-d} \begin{bmatrix} u \\ d^\perp - j \end{bmatrix}_q \begin{bmatrix} u - d^\perp + j - 1 \\ j - 1 \end{bmatrix}_q W_{k-u}(\mathcal{C}) \\ &+ \begin{bmatrix} k \\ d^\perp - j \end{bmatrix}_q \sum_{u=0}^{j-1-\epsilon} (-1)^u q^{\binom{u}{2}} \begin{bmatrix} k - d^\perp + j \\ u \end{bmatrix}_q (q^{t-m(d^\perp-j+u)} - 1) \end{aligned}$$

Dans notre situation, on sait que $d + d^\perp = k + 1$ donc $k - d = d^\perp - 1 < d^\perp$, donc la première somme est nulle ; de plus $\mathcal{C}$ n'est pas MRD donc $\epsilon = 0$.
On peut donc simplifier pour obtenir

$$\begin{aligned} W_{k-d^\perp+j}(\mathcal{C}) &= \begin{bmatrix} k \\ d^\perp - j \end{bmatrix}_q \sum_{u=0}^{j-1} (-1)^u q^{\binom{u}{2}} \begin{bmatrix} k - d^\perp + j \\ u \end{bmatrix}_q (q^{t-m(d^\perp-j+u)} - 1) \\ &= \begin{bmatrix} k \\ k - d^\perp + j \end{bmatrix}_q \sum_{u=0}^{j-1} (-1)^u q^{\binom{u}{2}} \begin{bmatrix} k - d^\perp + j \\ u \end{bmatrix}_q (q^{t-m(d^\perp-j+u)} - 1) \end{aligned}$$

où le changement dans le coefficient q-binomial nous est permis par la propriété 0.12.
On obtient alors le résultat en faisant le changement d'indice $i = k - d^\perp + j$.

Ainsi, dans le cas où $\mathcal{C}$ n'est pas MRD, la condition assez proche $d(\mathcal{C}) + d(\mathcal{C}^\perp) = k + 1$ nous permet de tirer des conclusions sur les distributions de poids de $\mathcal{C}$.

5 Anticodes à métrique du rang

Dans cette section on s'intéresse aux anticodes, c'est-à-dire aux codes auxquels on fixe une borne supérieure pour la distance du rang entre deux éléments.
On commence par donner une définition précise d'un anticode, puis quelques exemples pour montrer que certains codes qu'on a déjà manipulés étaient également des anticodes.

Définition 33 Soit un entier $0 \leq \delta \leq k$. Un **δ-anticode** est un sous-espace non vide $\mathcal{A} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ tel que pour tout $M, N \in \mathcal{A}$, $d(M, N) \leq \delta$.
Si $\mathcal{A}$ est un sous-espace vectoriel de $\mathcal{M}_{k\times m}(\mathbb{F}_q)$, on dit qu'il est linéaire.

Exemple 34 Toute partie $\mathcal{A} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ ne contenant qu'un unique élément est un 0-anticode.

L'espace $\mathcal{M}_{k\times m}(\mathbb{F}_q)$ est un k-anticode.
Le sous-espace vectoriel $U \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ des matrices dont les $k-\delta$ dernières lignes sont nulles est un δ-anticode linéaire de dimension $m\delta$.

On va maintenant donner une borne pour le cardinal d'un anticode, et voir les conditions sous-lesquelles cette borne est atteinte.

Théorème 35 Soit $\mathcal{A} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un δ-anticode. Alors $|\mathcal{A}| \leq q^{m\delta}$, et si $\delta \leq k-1$ les assertions suivantes sont équivalentes :

1. $|\mathcal{A}| = q^{m\delta}$
2. $\mathcal{A} + \mathcal{C} = \mathcal{M}_{k\times m}(\mathbb{F}_q)$ pour un code MRD $\mathcal{C}$ tel que $d(\mathcal{C}) = \delta + 1$
3. $\mathcal{A} + \mathcal{C} = \mathcal{M}_{k\times m}(\mathbb{F}_q)$ pour tout code MRD $\mathcal{C}$ tel que $d(\mathcal{C}) = \delta + 1$

Preuve
On commence par montrer la majoration sur le cardinal de $\mathcal{A}$, et on s'en servira pour montrer l'équivalence.
Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code MRD tel que $d(\mathcal{C}) = \delta + 1$. On est assuré de l'existence d'un tel code par le théorème 25.
Pour tout $M \in \mathcal{A}$, définissons $[M] = M + \mathcal{C} = \{M + N | N \in \mathcal{C}\}$. Ces ensembles sont disjoint ; en effet, si on prend $M, M' \in \mathcal{A}, M \neq M'$, et qu'on suppose qu'il existe $L \in [M] \cap [M']$, alors il existe $N, N' \in \mathcal{C}$ tels que $L = M + N = M' + N'$, et on peut en tirer que $M - M' = N' - N$. On a donc que $rg(M - M') = rg(N' - N)$, i.e. $d(M, M') = d(N, N')$. Or $d(M, M') \leq \delta$ et $d(N, N') \geq \delta + 1$; il ne peut donc pas exister de tel L.
Ces ensembles étant disjoints et contenus dans $\mathcal{M}_{k\times m}(\mathbb{F}_q)$, on a

$$|\mathcal{M}_{k\times m}(\mathbb{F}_q)| \geq \left| \bigcup_{M\in\mathcal{A}} [M] \right| = \sum_{M\in\mathcal{A}} |[M]|.$$

Or on sait que $|[M]| = |\mathcal{C}| = q^{m(k-\delta)}$, $\mathcal{C}$ étant MRD. Ainsi,

$$|\mathcal{M}_{k\times m}(\mathbb{F}_q)| \geq \sum_{M\in\mathcal{A}} |[M]| = \sum_{M\in\mathcal{A}} |\mathcal{C}| = |\mathcal{C}| \cdot |\mathcal{A}| = |\mathcal{A}| \cdot q^{m(k-\delta)}$$

Et on en tire

$$\begin{aligned} |\mathcal{M}_{k\times m}(\mathbb{F}_q)| &\geq |\mathcal{A}| \cdot q^{m(k-\delta)} \\ |\mathcal{M}_{k\times m}(\mathbb{F}_q)|/q^{m(k-\delta)} &\geq |\mathcal{A}| \\ q^{mk}/q^{m(k-\delta)} &\geq |\mathcal{A}| \\ q^{m\delta} &\geq |\mathcal{A}| \end{aligned}$$

Et on obtient ainsi l'inégalité.
De plus, $\mathcal{A}+\mathcal{C} = \{M+N | M \in \mathcal{A}, N \in \mathcal{C}\} = \bigcup_{M\in\mathcal{A}}[M] \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$, et $|\mathcal{A}+\mathcal{C}| = |\mathcal{A}|\cdot|\mathcal{C}|$, donc si $|\mathcal{A}| = q^{m\delta}$, on a $|\mathcal{A}+\mathcal{C}| = q^{m\delta+m(k-\delta)} = q^{mk} = |\mathcal{M}_{k\times m}(\mathbb{F}_q)|$, et donc $\mathcal{A}+\mathcal{C} = \mathcal{M}_{k\times m}(\mathbb{F}_q)$ pour tout tel code $\mathcal{C}$. Cela montre l'implication "1. $\Rightarrow$ 3." .
D'autre part, si on a $\mathcal{A}+\mathcal{C} = \mathcal{M}_{k\times m}(\mathbb{F}_q)$ pour un certain tel $\mathcal{C}$, on a naturellement que $|\mathcal{A}+\mathcal{C}| = |\mathcal{A}|\cdot|\mathcal{C}| = |\mathcal{M}_{k\times m}(\mathbb{F}_q)|$ ce qui nous permet d'obtenir $|\mathcal{A}| = q^{m\delta}$ et prouve l'implication "2. $\Rightarrow$ 1.".
L'implication "3. $\Rightarrow$ 2." étant évidente, on a bien l'équivalence entre les trois assertions.

Définition 36 On dit qu'un δ-anticode $\mathcal{A}$ est (de cardinalité) **optimal(e)** si il atteint la borne obtenue dans le théorème 35.

Remarque 37 L'exemple U de 34 34 montre qu'on peut trouver un δ-anticode linéaire optimal pour tout choix du paramètre δ.

Pour conclure cette section, on montre un résultat analogue au théorème 27 en prouvant que le dual d'un δ-anticode linéaire optimal est un $(k-\delta)$-anticode linéaire optimal.
Il faut pour cela montrer deux résultats préliminaires, le premier étant dans une certaine mesure une conséquence du théorème 29.

Lemme 38 Soit $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un code MRD tel que $0 \in \mathcal{C}$, $|\mathcal{C}| \geq 2$ et $d(\mathcal{C}) = d$. Alors, pour tout $0 \leq l \leq k-d$, on a $W_{d+l}(\mathcal{C}) > 0$.

Preuve
Le théorème 29 nous donnant une expression des $W_{d+l}(\mathcal{C})$ qui dépend uniquement des paramètres du code MRD $\mathcal{C}$, il suffit de montrer le résultat pour un code de notre choix possédant ces paramètres.
Soit $C \subset \mathcal{M}_{k\times 1}(\mathbb{F}_{q^m})$ le code vectoriel construit dans la preuve du théorème 25 ; on conserve les notations pour $E = \{b_1, ..., b_k\}$ et ev_E, et on a donc $C = ev_E(Lin_q(m, k-d))$. Soit Γ une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$. Alors, par proposition 10, $\mathcal{D} = \Gamma(C) \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ est un code linéaire de dimension $dim(\mathcal{D}) = m(k-d+1)$ et ayant la même distribution de poids que C. En particulier, $|\mathcal{D}| \geq 2$, $\mathcal{D}$ est linéaire donc $0 \in \mathcal{D}$, et $d(\mathcal{D}) = d(C) = d$, donc il possède bien les paramètres du lemme : c'est pour ce code qu'on va effectuer la démonstration.
Posons l et t tels que $0 \leq l \leq k-d$, et $t = k-d-l$. On définit ensuite $U \subset \mathbb{F}_{q^m}$ comme le $\mathbb{F}_q$-sous-espace vectoriel engendré par $\{b_1, ..., b_t\}$. Si $t = 0$, on prend $U = \{0\}$.

On définit ensuite le polynôme p_U sur $\mathbb{F}_{q^m}$ par

$$p_U(x) = \prod_{\gamma \in U} (x - \gamma)$$

Selon [8], Théorème 3.52, p_U est un polynôme linéarisé de degré $t = k - d - l \leq k - d$. on a donc que $p_U \in Lin_q(m, k-d)$. Or $C = ev_E(Lin_q(m, k-d))$, donc $ev_E(p_U) \in C$. On va chercher à déterminer le rang de $ev_E(p_U)$.
De façon évidente, $V(p_U) = U$, où $V(p_U)$ désigne l'ensemble des racines de p_U. On a donc que

$$ev_E(p_U) = (p_U(b_1), ..., p_U(b_t), p_U(b_{t+1}), ..., p_U(b_k)) = (0, ..., 0, p_U(b_{t+1}), ..., p_U(b_k)).$$

Montrons que la famille $(p_U(b_{t+1}), ..., p_U(b_k))$ est $\mathbb{F}_q$-linéairement indépendante.
Soient $a_{t+1}, ..., a_k \in \mathbb{F}_q$ tels que

$$\sum_{i=t+1}^{k} a_i p_U(b_i) = 0$$

p_U étant un polynôme linéarisé donc $\mathbb{F}_q$-linéaire, on a

$$p_U\left(\sum_{i=t+1}^{k} a_i b_i\right) = 0$$

C'est-à-dire que $\sum_{i=t+1}^{k} a_i b_i \in V(p_U) = U$. Il existe donc $a_1, ..., a_t \in \mathbb{F}_q$ tels que $\sum_{i=1}^{t} a_i b_i = \sum_{i=t+1}^{k} a_i b_i$ et on a donc que $\sum_{i=1}^{t} a_i b_i - \sum_{i=t+1}^{k} a_i b_i = 0$.
Les $b_1, ..., b_k$ étant $\mathbb{F}_q$-linéairement indépendants, on a forcément que, pour tout $i \in [1, ..., k]$, $a_i = 0$. En particulier, pour tout $i \in [t+1, ..., k]$, $a_i = 0$. Doncla famille $(p_U(b_{t+1}), ..., p_U(b_k))$ est $\mathbb{F}_q$-linéairement indépendante. On a donc que $rg_G(ev_E(p_U)) = rg_G((0, ..., 0, p_U(b_{t+1}), ..., p_U(b_k))) = k - t = d + l$. Il y a donc au moins un élement de C de rang $d + l$ et ce pour tout $0 \leq l \leq k - d$, i.e. $W_{d+l}(\mathcal{C}) > 0$.
$\mathcal{D}$ et C partageant la même distribution de poids, on a donc que pour tout $0 \leq l \leq k - d$, $W_{d+l}(\mathcal{D}) > 0$ et le lemme est ainsi prouvé.

On va maintenant caractériser les anticodes linéaires optimaux en termes de leur intersection avec des codes linéaires MRD.

Propostion 39 On suppose $0 \leq \delta \leq k - 1$.
Soit $\mathcal{A}$ un code linéaire tel que $dim(\mathcal{A}) = m\delta$. Les assertions suivantes sont équivalentes :

1. $\mathcal{A}$ est un δ-anticode optimal.
2. Pour tout code linéaire MRD non-nul $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ tel que $d(\mathcal{C}) = \delta + 1$, on a $\mathcal{A} \cap \mathcal{C} = \{0\}$.

Preuve
On commence par supposer que $\mathcal{A}$ est un δ-anticode optimal. Soit $\mathcal{C}$ un code MRD linéaire non-nul avec $d(\mathcal{C}) = \delta + 1$. $\mathcal{A}$ et $\mathcal{C}$ étant tout les deux des codes linéaires, on sait que $0 \in \mathcal{A} \cap \mathcal{C}$. Supposons qu'il existe $M \in \mathcal{A} \cap \mathcal{C}, M \neq 0$. Alors $d(M, 0) \leq \delta$, car $M, 0 \in \mathcal{A}$ anticode ; mais $d(M, 0) \geq \delta + 1$ car $M, 0 \in \mathcal{C}$. Un tel M ne peut donc pas exister, et on a bien $\mathcal{A} \cap \mathcal{C} = \{0\}$, ce qui prouve l'implication "1. $\Rightarrow$ 2.".
On va maintenant supposer que pour tout code linéaire MRD $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ non-nul, tel que $d(\mathcal{C}) = \delta + 1$, on a $\mathcal{A} \cap \mathcal{C} = \{0\}$.
La dimension de $\mathcal{A}$ nous permet de remarquer que $|\mathcal{A}| = q^{m\delta}$, donc il s'agit uniquement de montrer que $\mathcal{A}$ est un δ-anticode ; le fait qu'il soit optimal sera évident. Pour cela, on va procéder par l'absurde.
Supposons que $\mathcal{A}$ n'est pas un δ-anticode. Alors, comme $\mathcal{A}$ est linéaire, il existe $N \in \mathcal{A}$ tel que $rg(N) = d(N, 0) \geq \delta + 1$. Soit $\mathcal{D}$ un code linéaire MRD non-nul tel que $d(\mathcal{D}) = \delta + 1$. On sait qu'un tel code existe par le théorème 25. Le lemme 38 nous dit que $W_{rg(N)}(\mathcal{D}) > 0$, i.e. il existe au moins un élément $M \in \mathcal{D}$ tel que $rg(M) = rg(N)$. Il existe alors deux matrices inversibles, $A \in \mathcal{M}_{k\times k}(\mathbb{F}_q)$ et $B \in \mathcal{M}_{m\times m}(\mathbb{F}_q)$. telles que $N = AMB$.
Définissons alors l'ensemble $C = A\mathcal{D}B = \{ARB | R \in \mathcal{D}\}$. L'application $R \mapsto ARB$ de $\mathcal{M}_{k\times m}(\mathbb{F}_q)$ dans lui-même étant un isomorphisme, C est également un code linéaire MRD non-nul tel que $d(C) = \delta + 1$. Vu que $M \in \mathcal{D}$, on a que $N = AMB \in C$, et donc $N \in \mathcal{A} \cap C$. De plus, $rg(N) \geq \delta + 1 \geq 1$ donc N n'est pas la matrice nulle, ce qui signifie que $\mathcal{A} \cap C \neq \{0\}$. Cette contradiction nous donne donc que $\mathcal{A}$ est nécessairement un δ-anticode, et on a donc l'implication "2. $\Rightarrow$ 1.".
Les deux assertions sont bien équivalentes.

On peut enfin appliquer ces résultats pour montrer le théorème liant un anticode à son orthogonal.

Théorème 40 Soit $\mathcal{A} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un δ-anticode linéaire optimal. Alors $\mathcal{A}^\perp$ est un $(k - \delta)$-anticode linéaire optimal.

Preuve
Soit $\mathcal{A} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ un δ-anticode linéaire optimal.
Si $\delta = k$, alors $\mathcal{A} = \mathcal{M}_{k\times m}(\mathbb{F}_q)$ et $\mathcal{A}^\perp = \{0\}$, et le résultat est alors trivial. On va donc supposer que $0 \leq \delta \leq k - 1$.

$\mathcal{A}$ est optimal, donc par la définition 36 $dim(\mathcal{A}) = m\delta$, et donc $dim(\mathcal{A}^\perp) = km - dim(\mathcal{A}) = km - km\delta = k(m-\delta)$. Ainsi, la proposition 39 nous permet de montrer que $\mathcal{A}^\perp$ est un $(k-\delta)$-anticode optimal en prouvant que, pour tout code linéaire MRD non-nul $\mathcal{C} \subset \mathcal{M}_{k\times m}(\mathbb{F}_q)$ tel que $d(\mathcal{C}) = k - \delta + 1$, on a $\mathcal{A}^\perp \cap \mathcal{C} = \{0\}$.
Considérons un tel code $\mathcal{C}$. On a alors que

$$dim(\mathcal{C}) = m(k - (k - \delta + 1) + 1) = m\delta < mk$$

Par la proposition 28, on a que $\mathcal{C}^\perp$ est également un code linéaire MRD et $d(\mathcal{C}^\perp) = k + 2 - d(\mathcal{C}) = k + 2 - (k - \delta + 1) = \delta + 1$.
$\mathcal{A}$ étant un δ-anticode optimal, la proposition 39 nous dit alors que $\mathcal{A} \cap \mathcal{C} = \{0\}$. De plus, $dim(\mathcal{A}) + dim(\mathcal{C}^\perp) = m\delta + m(k-\delta) = mk = dim(\mathcal{M}_{k\times m}(\mathbb{F}_q))$, et on peut donc en déduire que $\mathcal{A} \oplus \mathcal{C}^\perp = \mathcal{M}_{k\times m}(\mathbb{F}_q)$.
On a alors $\mathcal{A}^\perp \cap \mathcal{C} = (\mathcal{A} \oplus \mathcal{C}^\perp)^\perp = (\mathcal{M}_{k\times m}(\mathbb{F}_q))^\perp = \{0\}$. Le théorème s'en déduit par la proposition 39.

Références

[1] Elisa Gorla, Alberto Ravagnani (2018), Codes Endowed With the Rank Metric, in Net-work Coding and Subspace Designs, M. Greferath et al. Eds., Springer, 3-23.

[2] E. Gabidulin Theory of codes with maximum rank distance. Problems of Information Transmission, 1 (1985), 2, pp. 1 – 12.

[3] P. Stanley, Enumerative Combinatorics, vol. 1, Cambridge Stud. Adv. Math., vol. 49. Cambridge University Press (2012).

[4] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory A, 25 (1978), 3, pp. 226 – 241.

[5] A. Ravagnani, Rank-metric codes and their duality theory. Designs, Codes and Cryptog-raphy, 80 (2016), 1, pp. 197 – 216.

[6] M. Gadouleau, Z. Yan MacWilliams Identities for Codes with the Rank Metric.EURASIP Journal on Wireless Communications and Networking, 2008.

[7] J. De la Cruz, E. Gorla, H. H. Lopez, A. Ravagnani, Rank distribution of Delsarte codes, 2015

[8] R. Lidl, H. Niederreiter, Finite Fields. Addison-Wesley Publishing Company (1983).