Poids pour la métrique du rang dans les extensions finies

Lyon, ICJ, séminaire d'Algèbre

Odile Garotta

travail commun avec Jean Fasel et Grégory Berhuy *26 novembre 2020*

Table des matières

1 Introduction

Nous exposons le papier [BF–] *Rank weights for arbitrary finite field extensions*, Adv. Math. Comm. 2020 et arXiv :1902.00733 qui est un travail commun avec Jean Fasel et Grégory Berhuy.

Soient k un corps fini, L une extension finie de k, et $n \geq 1$ un entier. Suivant Gabidulin (85), on définit une métrique sur L^n en associant à tout n-uplet $\mathbf{c}$ de L^n son *rang sur* k, noté $\mathrm{Rwt}(\mathbf{c})$.

Un code est un L-sous-espace C de L^n. On considère les entiers r tels que $1 \leq r \leq \dim C$. Wei a défini en 91 les r*-poids généralisés pour la distance de Hamming* :

$$d_r^H(C) = \min_{\substack{D \subset C \\ \dim(D)=r}} |\mathrm{Supp}(D)| = \min_{\substack{V \in \Lambda(L^n) \\ \dim(C \cap V) \geq r}} \dim V,$$

où $\mathrm{Supp}(D)$ est la réunion des supports des $\mathbf{d} \in D$, et $\Lambda(L^n)$ est l'ensemble des sous-espaces de L^n engendrés par les vecteurs de la base canonique (la seconde égalité ci-dessus est aisée).

Notation. Le groupe de Galois cyclique G de l'extension L/k agit diagonalement sur L^n. Pour tout L-sous-espace V de L^n, on note V^* le plus petit sous-espace de L^n qui contient V et est stable sous G.

En vue d'obtenir une théorie semblable à celle des r-poids de Hamming généralisés, pour l'appliquer dans le cadre du codage en réseau, les définitions suivantes de r-poids généralisés pour la métrique du rang ont été proposées, depuis 2012 :

1. $OS_r(C) = \min\limits_{\substack{D\subset C \\ \dim(D)=r}} \max_{\mathbf{d}\in \mathrm{D}} \mathrm{Rwt}(\mathbf{d})$ **(Oggier-Sboui 12)**

2. $\mathcal{M}_r(C) = \min\limits_{\substack{V\subset L^n, V=V^* \\ \dim(C\cap V)\geq r}} \dim V$ **(Kurihara-Matsumoto-Uyematsu 15)**

   Ducoat a alors proposé un raffinement de la première :

3. $D_r(C) = \min\limits_{\substack{D\subset C \\ \dim(D)=r}} \max_{\mathbf{d}\in \mathrm{D}^*} \mathrm{Rwt}(\mathbf{d})$ **(Ducoat 15)**

   et montré notamment que si $n \leq m$, où $m = [L : k]$, alors $D_r(C) = \mathcal{M}_r(C)$.

Puis Jurrius-Pellikaan ont considéré des extensions du *polynôme énumérateur des r-poids généralisés* pour la métrique du rang, et ils ont proposé comme définition alternative son plus petit coefficient non nul

4. $d_{R,r}(C) = \min\limits_{\substack{D \subset C \\ \dim(D)=r}} \mathrm{Rwt}(D)$ **(J-P 17),**

où $\mathrm{Rwt}(D)$ sera défini plus loin. Ils ont prouvé notamment que
si $n \leq m$ ces quatre définitions coïncident *sur les corps finis.* Une étape clé pour cela est d'y montrer que, si $n \leq m$,

$$\boxed{\text{pour tout } C\text{, il existe } \mathbf{c} \in C \text{ tel que } \mathrm{Rwt}(\mathbf{c}) = \mathrm{Rwt}(C)}.$$

Dans [BF–] nous étendons leur résultat sur les r-Rpoids aux *extensions finies arbitraires* de corps ; nous donnons un argument de géométrie algébrique pour y prouver l'énoncé clé .

2 Rsupports

2.1 Généralités

Dans tout l'exposé, on se donne une extension de corps $k \subset L$, $n \geq 1$ un entier, et C un L-sous-espace de L^n.

Notations. On note alors $\mathrm{Res}(C) = C \cap k^n$, k-sous-espace de k^n.

Si D un k-sous-espace de k^n, on note D_L le L-sous-espace de L^n engendré par D. On a $D_L \simeq D \otimes_k L$ canoniquement.

Si $\varphi : D \to D'$ est k-linéaire, on note φ_L l'application L-linéaire $D_L \to D'_L$ qui s'en déduit.

On suppose que L/k est finie de degré m, on note $\alpha_1, \ldots, \alpha_m$ une base de L sur k. Pour tout n-uplet $\mathbf{c} = (c_1, \ldots, c_n) \in L^n$, chaque c_j s'écrit $\sum_{i=1}^m c_{ij}\alpha_i$. On obtient une matrice $M(\mathbf{c}) := (c_{ij}) \in M_{mn}(k)$.

Si $c^{(i)}$ désigne sa $i^{\text{ème}}$ ligne, on a

$$\mathbf{c} = \sum_{i=1}^{m} \alpha_i \mathbf{c}^{(i)}. \qquad (*)$$

Dans [J-P 17], Jurrius and Pellikaan ont introduit le “support de rang” ou Rsupport d’un vecteur et d’un sous-espace de L^n.

Définition 1. a) Si $\mathbf{c} \in L^n$, son *support de rang* ou *Rsupport* est le sous-espace de k^n engendré par les lignes de $M(\mathbf{c})$, on le note $\mathrm{Rsupp}(\mathbf{c})$. Sa dimension est le *Rpoids* de $\mathbf{c}$, noté $\mathrm{Rwt}(\mathbf{c})$.

b) Le *support de rang* ou *Rsupport* de C, noté $\mathrm{Rsupp}(C)$, est le k-sous-espace

$$\mathrm{vect}_k(\mathrm{Rsupp}(\mathbf{c}) |\, \mathbf{c} \in C)$$

de k^n. Sa dimension est dite le *Rpoids* de C, notée $\mathrm{Rwt}(C)$.

c) La *distance du rang* ou *Rdistance* $d_R(C)$ du sous-espace C est le plus petit rang d'une matrice $M(\mathbf{c})$, pour $\mathbf{c}$ non nul dans C. C'est-à-dire,

$$d_R(C) = \min_{\mathbf{c} \in C \setminus \{0\}} \mathrm{Rwt}(\mathbf{c})\,.$$

Proposition 1. [J-P 17], [BF–] *Soient* $\mathbf{c}$, $\mathbf{c}' \in L^n$ *et* $\alpha \in L^\times$. *Alors*

1. $\mathrm{Rsupp}(\mathbf{c})$ *ne dépend pas du choix de la* k*-base de* L.
2. $\mathrm{Rsupp}(\alpha\mathbf{c}) = \mathrm{Rsupp}(\mathbf{c})$.
3. $\mathrm{Rsupp}(\mathbf{c} + \mathbf{c}') \subset \mathrm{Rsupp}(\mathbf{c}) + \mathrm{Rsupp}(\mathbf{c}')$.
4. *Si* $C = \mathrm{vect}(\mathbf{c}_1, \ldots, \mathbf{c}_r)$, *alors* $\mathrm{Rsupp}(C)$ *est la somme des* $\mathrm{Rsupp}(\mathbf{c}_i)$ $i = 1, \ldots, r$.
5. *Si* $\mathbf{c} \neq 0$, *alors on a* $\mathrm{Rwt}(\mathbf{c}) = 1$ *si et seulement s'il existe* $\lambda \in L^\times$ *tel que* $\lambda\mathbf{c} \in k^n$. *Dans ce cas on a* $\mathrm{Rsupp}(\lambda\mathbf{c}) = k \cdot \lambda\mathbf{c}$.
6. *On a* $d_R(C) = 1$ *si et seulement si* $\mathrm{Res}(C) \neq \{0\}$.
7. *On a* $\mathrm{Res}(C) \subset \mathrm{Rsupp}(C) \subset k^n$.
8. *On a* $C \subset \mathrm{Rsupp}(C)_L \subset L^n$.

Démonstration. **1 :** $\mathrm{Rsupp}(\mathbf{c})$ *ne dépend pas du choix de la k-base de L :*
le choix d'une nouvelle base de L sur k modifie $M(\mathbf{c})$ en $PM(\mathbf{c})$, où P est la matrice de passage.

2 : $\mathrm{Rsupp}(\alpha\mathbf{c}) = \mathrm{Rsupp}(\mathbf{c})$ *:*
on regarde $\alpha\mathbf{c}$ dans la base des $(\alpha\alpha_i)_i$.

3 : $\mathrm{Rsupp}(\mathbf{c}+\mathbf{c}') \subset \mathrm{Rsupp}(\mathbf{c}) + \mathrm{Rsupp}(\mathbf{c}')$ *:*
on utilise que $M(\mathbf{c}+\mathbf{c}') = M(\mathbf{c}) + M(\mathbf{c}')$ et que les Rsupp respectifs sont les k-sous-espaces engendrés par les lignes de ces matrices.

4 : *Si $C = \mathrm{vect}(\mathbf{c}_1, \dots, \mathbf{c}_r)$, alors $\mathrm{Rsupp}(C)$ est la somme des $\mathrm{Rsupp}(\mathbf{c}_i)$ $i = 1, \dots, r$:*
Les points 3 et 2 prouvent l'inclusion dans 4 ; l'autre sens résulte de la définition de $\mathrm{Rsupp}(C)$.

5 : *Si $\mathbf{c} \neq 0$, alors $\mathrm{Rwt}(\mathbf{c}) = 1 \iff$ il existe $\lambda \in L^\times$ tel que $\lambda\mathbf{c} \in k^n$. On a alors $\mathrm{Rsupp}(\lambda\mathbf{c}) = k \cdot \lambda\mathbf{c}$:*

en effet on peut supposer que $\alpha_1 = 1$. Alors si $\mathbf{c}' \in k^n$ est non nul, $M(\mathbf{c}')$ a toutes ses lignes nulles sauf la première, qui est égale à $\mathbf{c}'$. Il vient que $\mathrm{Rsupp}(\mathbf{c}') = k \cdot \mathbf{c}'$ et $\mathrm{Rwt}(\mathbf{c}') = 1$, et on utilise 2.

Si maintenant $M(\mathbf{c})$ a rang 1, il existe un indice l tel que les m lignes de $M(\mathbf{c})$ soient colinéaires à la $l^{\text{ème}}$ ligne, non nulle : $\mathbf{c}^{(i)} = \mu_i \mathbf{c}^{(l)}$, $\mu_i \in k$, $1 \leq i \leq m$.
On trouve que $\mathbf{c} = (\sum_{i=1}^m \mu_i \alpha_i)\mathbf{c}^{(l)} \neq 0$, cad. $\lambda \mathbf{c} \in k^n$ avec λ l'inverse de $\sum_{i=1}^m \mu_i \alpha_i$. D'où 5.

6 : *On a* $d_R(C) = 1$ *si et seulement si* $\mathrm{Res}(C) \neq \{0\}$ *:*
on le déduit immédiatement de 5 par définition de la Rdistance $d_R(C)$.

7 : *On a* $\mathrm{Res}(C) \subset \mathrm{Rsupp}(C) \subset k^n$ *:* en effet si $\mathbf{c} \in \mathrm{Res}(C)$, l'assertion 5 donne $\mathrm{Rsupp}(\mathbf{c}) = k \cdot \mathbf{c}$.

8 : *On a* $C \subset \mathrm{Rsupp}(C)_L \subset L^n$ *:* on se ramène avec 4. au cas où $C = L \cdot \mathbf{c}$.
L'écriture (*) : $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}^{(i)}$ montre alors que $\mathbf{c} \in \mathrm{Rsupp}(\mathbf{c})_L$. $\square$

Proposition 2. *Les propriétés suivantes sont équivalentes :*

1. $\mathrm{Res}(C) = \mathrm{Rsupp}(C)$

2. C *admet une base dans* k^n*,*

3. $\dim_k \mathrm{Res}(C) = \dim C$*, (ou encore* $\mathrm{Res}(C)_L = C$*)*

4. $\mathrm{Rsupp}(C)_L = C$.

Démonstration. $2. \Rightarrow 1$: Si C a une base $\mathbf{e}_1, \ldots, \mathbf{e}_r$ dans k^n, on a $\mathrm{Rsupp}(\mathbf{e}_i) = k \cdot \mathbf{e}_i$ ($1 \leq i \leq r$). Par 4. de la prop, les $\mathbf{e}_i$ engendrent donc $\mathrm{Rsupp}(C)$. Comme $\mathbf{e}_i \in \mathrm{Res}(C)$, il vient $\mathrm{Rsupp}(C) \subset \mathrm{Res}(C)$. L'autre inclusion est connue.

$1. \Rightarrow 2$: Supposons inversement que $\mathrm{Res}(C) = \mathrm{Rsupp}(C)$ et $C \neq 0$. Donc $\mathrm{Res}(C) \neq 0$. Soit $\mathbf{e}_1, \ldots, \mathbf{e}_s$ une base de $\mathrm{Res}(C)$. C'est aussi une famille libre sur L. On montre qu'elle engendre C sur L : si $\mathbf{c} \in C$, $\mathrm{Rsupp}(C)$ contient $\mathrm{Rsupp}(\mathbf{c})$, donc par l'hypothèse $\mathrm{Rsupp}(\mathbf{c}) \subset \mathrm{Res}(C)$. Par suite $\mathbf{c}$ est une combinaison L-linéaire de vecteurs de $\mathrm{Res}(C)$, on trouve bien que $\mathbf{c} \in \mathrm{vect}_L(\mathbf{e}_1, \ldots, \mathbf{e}_s)$. Clairement cela équivaut à ce que $s = \dim C$.

Reste à montrer l'équivalence de 1,2,3 avec 4. En effet, 2. entraîne que $\mathrm{Res}(C)_L = C$, donc avec 1. on obtient 4. Et si 4 est vraie, on obtient que $\mathrm{Rsupp}(C) \subset k^n \cap C = Res(C) \subset \mathrm{Rsupp}(C)$, d'où 1. □

Définition 2. Un L-sous-espace C de L^n est dit *étendu de* k^n si C admet une base dans k^n, autrement dit si $C = \mathrm{Res}(C)_L$.

Définition 3. On suppose L/k galoisienne de groupe de Galois G.
La *clôture galoisienne* d'un L-sous-espace C de L^n, notée C^*, est le plus petit sous-espace de L^n qui contient C et qui est invariant sous l'action de G sur L^n composante par composante.
Le sous-espace C est dit *Galois clos* si C est G-invariant, cad. si $C = C^*$.

Théorème 1. [Giorgetti-Previtali, 2010] [1] Si L/k est galoisienne, C est Galois clos si et seulement si $C = \mathrm{Res}(C)_L$, cad. si et seulement si C est étendu de k^n.

1. Il s'agit en fait d'un résultat connu en théorie des groupes algébriques, voir [Springer, *Linear algebraic groups*, 11.1.4]

2.2 Rsupport et orthogonaux

On note $\langle \_\,, \_\rangle$ la forme bilinéaire standard sur L^n. On définit l'*orthogonal* du sous-espace C de L^n comme le sous-espace

$$C^\perp = \{\mathbf{d} \in L^n \,|\, \forall \mathbf{c} \in C,\ \langle \mathbf{c}, \mathbf{d}\rangle = 0\}\,.$$

Proposition 3. [BF–] *On a*

$$\boxed{\mathrm{Res}(C)^\perp = \mathrm{Rsupp}(C^\perp)}\,.$$

Démonstration. Montrons que $\mathrm{Rsupp}(C^\perp) \subset \mathrm{Res}(C)^\perp$. Soient $\mathbf{d} \in C^\perp$ et $\mathbf{c} \in \mathrm{Res}(C)$. On a $\mathbf{d} = \sum_{i=1}^m \alpha_i\, \mathbf{d}^{(i)}$, où $\alpha_1, \ldots, \alpha_m$ est une base de L sur k et les $\mathbf{d}^{(i)}$ appartiennent à $\mathrm{Rsupp}(C^\perp)$. On doit montrer que tous les $\langle \mathbf{d}^{(i)}, \mathbf{c}\rangle$ sont nuls. En effet, on a $0 = \langle \mathbf{d}, \mathbf{c}\rangle = \sum_{j=1}^n \big(\sum_{i=1}^m \alpha_i {d_j}^{(i)} c_j\big) = \sum_{i=1}^m \alpha_i \langle \mathbf{d}^{(i)}, \mathbf{c}\rangle$.

Pour l'autre inclusion, on montre de même que $\mathrm{Rsupp}(C^\perp)^\perp \subset \mathrm{Res}(C)$. □

Remarque 1. En particulier, comme $(C^\perp)^\perp = C$, on obtient

$$\boxed{\mathrm{Rsupp}(C) = \mathrm{Res}(C^\perp)^\perp}.$$

3 k-Enveloppe d'un sous-espace

On suppose que L/k est finie.

Lemme 1. Si C est étendu de k^n, alors $C^\perp$ l'est aussi.
Si D est un k-sous-espace de k^n, on a $(D^\perp)_L = (D_L)^\perp$, où l'orthogonal est pris respectivement dans k^n et L^n.

Démonstration. Soit $\mathbf{e}_1, \dots, \mathbf{e}_r$ une L-base de C dans k^n et soit D l'orthogonal de $\mathrm{Res}(C)$ relativement à la forme bilinéaire standard de k^n. Alors $C^\perp$ est l'intersection des $L\mathbf{e}_i^\perp$ $(1 \leq i \leq r)$, et D a la même description sur k. Par suite $C^\perp \supset D_L$. Comme ils ont même dimension, il vient $C^\perp = D_L$. □

Lemme 2. Si $(C_i)_{i\in I}$ est une famille de sous-espaces de L^n étendus de k^n, alors $\bigcap_{i\in I} C_i$ l'est aussi.

Démonstration. Pour tout $i \in I$, on peut écrire $C_i = ((D_i)_L)^\perp$, pour un k-sous-espace D_i de k^n.

On a donc

$$\bigcap_{i\in I} C_i = \bigcap_{i\in I} (D_i)_L^{\perp} = \mathrm{vect}_L((D_i)_L, i \in I)^{\perp} = (\mathrm{vect}_k(D_i, i \in I)^{\perp})_L\,.$$

Ainsi, $\bigcap_{i\in I} C_i$ est étendu de k^n. □

Corollaire 1. *Supposons que l'extension L/k est galoisienne. Alors la clôture C^* est l'intersection de tous les sous-espaces de L^n étendus de k^n et qui contiennent C.*

Démonstration. Notons C' l'intersection de tous les L-sous-espaces de L^n étendus de k^n et qui contiennent C.

Par le Théorème [Gior-Prev], C^* est un sous-espace de L^n étendu de k^n et qui contient C, donc on a $C' \subset C^*$.

Inversement, on a $C \subset C'$, et C' est aussi étendu de k^n, donc il est Galois clos. Ainsi $C^* \subset C'$. □

Ce corollaire motive la généralisation suivante de la notion de clôture galoisienne dans L^n.

Définition 4. La *k-enveloppe* de C, notée C^*, est l'intersection de tous les L-sous-espaces de L^n étendus de k^n et qui contiennent C.

Remarques.

1. Si L/k est galoisienne, on retrouve bien que C^* est la clôture galoisienne de C.
2. La définition de C^* entraîne immédiatement que :
   on a $C = C^*$ si et seulement si C est étendu de k^n. En particulier, $(C^*)^* = C^*$.

Proposition 4. [J-P 17],[BF–] *On a* $\boxed{C^* = \mathrm{Rsupp}(C)_L}$. *En particulier on a* $\underline{\dim C^* = \mathrm{Rwt}(C)}$.

Démonstration. On sait que $\mathrm{Rsupp}(C)_L$ contient C. Comme il est de plus étendu de k^n, $\mathrm{Rsupp}(C)_L$ contient C^*. Inversement, $\mathrm{Rsupp}(C)_L$ est inclus dans $\mathrm{Rsupp}(C^*)_L$, et comme C^* est étendu de k^n, la Prop. 2 donne que $\mathrm{Rsupp}(C^*)_L = C^*$, d'où l'inclusion de $\mathrm{Rsupp}(C)_L$ dans C^* et finalement l'égalité. On utilise alors que $\mathrm{Rsupp}(C)_L$ a dimension $\mathrm{Rwt}(C)$. $\square$

On donne deux corollaires, généralisation du cas galoisien.

Corollaire 2. *Soit* $\mathbf{c} \in C$. *Alors on a* $\mathrm{Rsupp}(C) = \mathrm{Rsupp}(\mathbf{c})$ *si et seulement si* $C^* = (L \cdot \mathbf{c})^*$*, cad., si et seulement si* $C \subset (L \cdot \mathbf{c})^*$.

Corollaire 3. *On a* $\mathrm{Rsupp}(C) = \mathrm{Rsupp}(C^*)$. *En particulier si* L/k *est séparable, on a* $\mathrm{Tr}(C) = \mathrm{Tr}(C^*)$*, où* $\mathrm{Tr}\colon L^n \to k^n$ *est l'application trace relative sur chaque composante.*

Démonstration. Par la Proposition 4, les k-sous-espaces $\mathrm{Rsupp}(C)$ et $\mathrm{Rsupp}(C^*)$ ont même dimension. L'inclusion $\mathrm{Rsupp}(C) \subset \mathrm{Rsupp}(C^*)$ est donc une égalité.

Si L/k est séparable, [J-P 17] montre (écrit pour L/k galoisienne) que Rsupp et Tr coïncident sur les L-sous-espaces de L^n, d'où la conclusion. $\square$

4 Le point de vue géométrique

On va prouver le

Théorème A [BF–] *On suppose L/k finie de degré m. Les conditions suivantes sont équivalentes :*

- i) $\dim \mathrm{Rsupp}(C) \leq m$,
- ii) *il existe* $\mathbf{c} \in C$ *tel que* $\mathrm{Rsupp}(C) = \mathrm{Rsupp}(\mathbf{c})$.

En particulier, si $n \leq m$ l'assertion (ii) est toujours vérifiée.

Démonstration. Justifions déjà que ii) $\Rightarrow$ i) : en effet, si ii) est vérifiée, la matrice $M(\mathbf{c})$ de $\mathbf{c}$ dans une base de L sur k a m lignes, donc $\dim \mathrm{Rsupp}(\mathbf{c}) \leq m$.

Passons à la **preuve de i) $\Rightarrow$ ii)**. On commence par réduire le problème à un problème de géométrie algébrique.

1. **On peut supposer que $n \leq m$ et $\mathrm{Rsupp}(C) = k^n$.**

   En effet, on a $C \subset \mathrm{Rsupp}(C)_L$. On peut choisir une base de $\mathrm{Rsupp}(C)$ et travailler avec cet espace vectoriel au lieu de k^n. Alors i) devient $n \leq m$.

2. **Réduction au cas où C est un plan**

   Le résultat est immédiat si C a dimension ≤ 1. Pour le cas général, on se ramène au cas $\dim(C) = 2$ grâce à une récurrence sur $\dim(C) = r \in [2, n]$:
   On écrit $C = D \oplus L\mathbf{e}$ où $\dim D = r - 1$ et $\mathbf{e} \neq \mathbf{0}$. L'hypothèse de récurrence nous fournit $\mathbf{d} \in D$ tel que $\mathrm{Rsupp}(\mathbf{d}) = \mathrm{Rsupp}(D)$. Or $\mathrm{Rsupp}(C)$ est engendré par $\mathrm{RSupp}(D)$ et $\mathrm{Rsupp}(\mathbf{e})$, cad. par $\mathrm{Rsupp}(\mathbf{d})$ et $\mathrm{Rsupp}(\mathbf{e})$. La Proposition 1 nous ramène alors à prouver l'énoncé pour $C' = \mathrm{vect}_L(\mathbf{d}, \mathbf{e})$, on conclut car c'est le cas d'un plan.

3. **Utilisation des formes linéaires**

   Lemme 3. *Soit $D \subset L^n$ un L-sous-espace, et soit $\varphi : k^n \to k$ linéaire. Alors*

   $$\varphi(\mathrm{Rsupp}(D))_L = \varphi_L(D).$$

En particulier, on a $\varphi_L(D) = 0$ *si et seulement si* $\varphi(\mathrm{Rsupp}(D)) = 0$.

Démonstration. On a $D \subset \mathrm{Rsupp}(D)_L$, donc $\varphi_L(D) \subset \varphi(\mathrm{Rsupp}(D))_L$. Or ce sont deux L-sous-espaces de la droite L, donc il suffit de prouver que
si $\varphi_L(D) = 0$, alors $\varphi(\mathrm{Rsupp}(D))_L = 0$, cad. $\varphi(\mathrm{Rsupp}(D)) = 0$.
Supposons donc que $\varphi_L(D) = 0$. Si $\mathbf{d} \in D$, on peut écrire

$$\mathbf{d} = \sum_{i=1}^{m} \alpha_i \mathbf{d}^{(i)} \in L^n,$$

avec $\mathbf{d}^{(i)} \in \mathrm{Rsupp}(D)$. Par définition,

$$\varphi_L(\mathbf{d}) = \sum_{i=1}^{m} \alpha_i \varphi(\mathbf{d}^{(i)}).$$

Les α_i étant linéairement indépendants sur k, on obtient que $\varphi(\mathbf{d}^{(i)}) = 0$ pour tout $i = 1, \ldots, m$.
Or $\mathrm{Rsupp}(D)$ est engendré par les $(\mathbf{d}^{(i)})_i$ pour $\mathbf{d} \in D$. On conclut que $\varphi(\mathrm{Rsupp}(D)) = 0$. $\square$

4. **Conséquence.** *(mêmes D, φ) Dans le cas où* $\mathrm{Rsupp}(D) = k^n$*, il vient que*

$$\varphi = 0 \textit{ si et seulement si } \varphi_L(D) = 0.$$

On se ramène ainsi à prouver la

Proposition 5. [BF–] *Soit L/k une extension de corps de degré fini m et soit $n \leq m$. Soit $C \subset L^n$ un plan tel que* $\mathrm{Rsupp}(C) = k^n$*. Alors il existe $\mathbf{c} \in C$ tel que*

$$\varphi_L(\mathbf{c}) = 0 \iff \varphi = 0$$

pour toute application k-linéaire $\varphi : k^n \to k$.

En effet, si alors $\mathrm{Rsupp}(\mathbf{c}) \neq k^n$, il existe ψ forme linéaire non nulle sur k^n telle que $\psi(\mathrm{Rsupp}(\mathbf{c})) = 0$. Par notre lemme 3 sur les formes linéaires, on a alors $\psi_L(\mathbf{c}) = 0$, mais cela contredit la propriété de $\mathbf{c}$. Ceci prouve le théorème.

Rappel : restriction de Weil des schémas quasi-projectifs

Soit X un schéma quasi-projectif sur L, alors sa *restriction de Weil* $\mathcal{R}_{L/k}X$ le long de l'extension L/k est le schéma quasi-projectif sur k défini par

$$\boxed{\mathrm{Hom}_k(\mathrm{Spec}(R), \mathcal{R}_{L/k}X) = \mathrm{Hom}_L(\mathrm{Spec}(R_L), X)} \text{ pour toute } k\text{-algèbre } R.$$

Exemples :

- si $X = \mathbb{A}^1_L$, alors $\mathcal{R}_{L/k}\mathbb{A}^1_L \simeq \mathbb{A}[\mathrm{Hom}_k(L, k)] \simeq \mathbb{A}^m_k$. En particulier, la dimension de Krull de $\mathcal{R}_{L/k}\mathbb{A}^1_L$ est m.
- si $X = \mathbb{P}^1_L$, alors $\mathcal{R}_{L/k}\mathbb{P}^1_L$ est connexe et une immersion ouverte $\mathbb{A}^1_L \subset \mathbb{P}^1_L$ induit une immersion ouverte $\mathcal{R}_{L/k}\mathbb{A}^1_L \subset \mathcal{R}_{L/k}\mathbb{P}^1_L$. On en déduit que $\underline{\mathcal{R}_{L/k}\mathbb{P}^1_L \text{ a dimension } m}$.

Pour prouver la Proposition 5, on va définir un morphisme de schémas

$$f : \mathbb{P}^{n-1}_k \to \mathcal{R}_{L/k}\mathbb{P}(C) \simeq \mathcal{R}_{L/k}\mathbb{P}^1_L.$$

Rappel. Soit R une k-algèbre de type fini. L'ensemble des *R-points de* $\mathbb{P}_k^{n-1}$ s'identifie à un couple $(M, \varphi_{\text{mod}} R^{\times})$ formé d'un R-module projectif M de rang 1 et d'une classe d'équivalence de surjections R-linéaires

$$\varphi : R^n \to M$$

pour l'action de $R^{\times}$ par multiplication.

On associe à une telle classe le noyau $\ker \varphi$, R-module projectif P de rang $n-1$. On étend les scalaires à L, on obtient un R_L-module projectif P_L, sous-module de R_L^n. On considère l'intersection

$$P_L \cap (C \otimes_L R_L) \subset C \otimes_L R_L$$

où $C \subset L^n$ est notre plan.

Lemme 4. Le sous-module $P_L \cap (C \otimes_L R_L)$ est localement libre de rang 1.

Démonstration. Il suffit de montrer que pour tout idéal maximal $\mathfrak{m}$ de R_L, le produit tensoriel de ce module avec $L(\mathfrak{m}) := R_L/\mathfrak{m}$ est libre de rang 1. Par construction, $P_{L(\mathfrak{m})} = \ker \varphi_{L(\mathfrak{m})}$ et on doit calculer la dimension de $P_{L(\mathfrak{m})} \cap C_{L(\mathfrak{m})}$. Or $P_{L(\mathfrak{m})}$ a dimension $n-1$ et $C_{L(\mathfrak{m})}$ dimension 2, donc leur intersection n'est pas triviale.
Supposons que $P_{L(\mathfrak{m})} \cap C_{L(\mathfrak{m})} = C_{L(\mathfrak{m})}$, cad. que $C_{L(\mathfrak{m})} \subset P_{L(\mathfrak{m})}$. Cela signifie que $\varphi_{L(\mathfrak{m})}(C_{L(\mathfrak{m})}) = 0$. Notons $\mathfrak{m}'$ l'idéal maximal préimage de $\mathfrak{m}$ par l'application naturelle $R \to R_L$. Alors $L(\mathfrak{m})$ est une extension finie du corps $k(\mathfrak{m}') := R/\mathfrak{m}'$. En tensorisant par $k(\mathfrak{m}')$ la suite exacte scindée
$0 \to P \to R^n \xrightarrow{\varphi} M \to 0$, on voit que $\varphi_{k(\mathfrak{m}')} \colon k(\mathfrak{m}')^n \to M_{k(\mathfrak{m}')}$ est surjective non nulle.
Comme $\varphi_{L(\mathfrak{m})}(C_{L(\mathfrak{m})}) = 0$ et $\mathrm{Rsupp}(C_{L(\mathfrak{m})}) = k(\mathfrak{m}')^n$, le lemme 3 donne la contradiction.
On conclut que $P_L \cap (C \otimes_L R_L)$ est localement libre de rang 1. $\square$

Conséquence : Le quotient de $C \otimes_L R_L$ par ce sous-module est projectif de rang 1, ainsi le sous-module $P_L \cap (C \otimes_L R_L)$ définit un R_L-point de $\mathbb{P}(C)$, cad. un R-point de sa restriction de Weil. Ceci définit bien un morphisme de schémas

$$f : \mathbb{P}_k^{n-1} \to \mathcal{R}_{L/k}\mathbb{P}(C).$$

Calculons l'image d'un k-point $[a_1 : \ldots : a_n]$ de $\mathbb{P}_k^{n-1}$
Un représentant de la classe d'équivalence d'applications linéaires $\varphi : k^n \to k$ associées à ce point est

$$\mathbf{a} : k^n \to k$$

donnée par $(u_1, \ldots, u_n) \mapsto \sum_{i=1}^n a_i u_i$.
Si $C = \mathrm{vect}(\mathbf{v}, \mathbf{w}) \subset L^n$ avec $\mathbf{v} = (v_1, \ldots, v_n)$ et $\mathbf{w} = (w_1, \ldots, w_n)$ vérifie $\mathrm{RSupp}(C) = k^n$, on voit qu'un élément de la forme $\alpha\mathbf{v} + \beta\mathbf{w}$ appartient au noyau de $\mathbf{a}_L$ si et seulement si $\alpha(\sum a_i v_i) + \beta(\sum a_i w_i) = 0$. Par suite

$$f([a_1 : \ldots : a_n]) = \Big[\sum a_i w_i : -\sum a_i v_i\Big].$$

Preuve de la Proposition 5. Comme $\mathrm{Rsupp}(C) = k^n$, la réduction ci-dessus nous ramène à prouver

qu'il existe $\mathbf{c} \in C$ tel que
(**) : pour toute forme k-linéaire φ sur k^n on a

$$\varphi_L(\mathbf{c}) = \varphi_L(L \cdot \mathbf{c}) = 0 \Rightarrow \varphi_L(C) = 0.$$

On utilise le morphisme

$$f : \mathbb{P}_k^{n-1} \to \mathcal{R}_{L/k}\mathbb{P}(C)$$

défini ci-dessus. Notons d'abord qu'un k-point de $\mathcal{R}_{L/k}\mathbb{P}(C)$ correspond à un L-point de $\mathbb{P}(C)$, cad. à une droite $L \cdot \mathbf{c}$ de C.

Affirmation : ce k-point *n'*est *pas* dans l'image de f si et seulement si $\mathbf{c}$ satisfait (**).

En effet ce k-point est dans l'image de

$$f : \mathbb{P}_k^{n-1} \to \mathcal{R}_{L/k}\mathbb{P}(C)$$

si et seulement s'il existe une surjection $\varphi : k^n \to k$ dont le noyau P vérifie $P_L \cap C = L \cdot \mathbf{c}$, c'est-à-dire une forme k-linéaire φ telle que $\varphi_L(\mathbf{c}) = 0$ et $\varphi_L(C) \neq 0$.

Il suffit donc de montrer que *le morphisme f n'est pas surjectif sur les k-points.*
Notons $Z \subset \mathcal{R}_{L/k}\mathbb{P}(C)$ l'adhérence de l'image de f. Alors Z a dimension au plus la dimension de $\mathbb{P}_k^{n-1}$, cad. au plus $n-1$, alors que $\mathcal{R}_{L/k}\mathbb{P}(C)$ a dimension $m = [L : k]$. Comme $m \geq n$, on voit que Z est un fermé propre de $\mathcal{R}_{L/k}\mathbb{P}(C)$.
Si k est infini, on en déduit qu'il existe un point rationnel dans le complémentaire ouvert de Z et le résultat est prouvé.
Si k est fini, on note que $\mathbb{P}_k^{n-1}$ possède $\frac{|k|^n-1}{|k|-1}$ points rationnels. D'autre part, les points (k-)rationnels de $\mathcal{R}_{L/k}\mathbb{P}(C)$ sont en bijection avec les (L)-points rationnels de $\mathbb{P}_L^1$, il y a donc $\frac{|L|^2-1}{|L|-1}$ tels points. On conclut en utilisant l'inégalité

$$\frac{|k|^n - 1}{|k| - 1} < \frac{|L|^2 - 1}{|L| - 1},$$

qui résulte de ce que $|k|^n - 1 < |k|^m + 1$.

$\square$

5 Rpoids généralisés pour les extensions finies

On suppose que L/k est finie de degré m. On considère les entiers r tels que $1 \leq r \leq \dim C$.

On commence par donner les différentes définitions qui ont été proposées pour les r-Rpoids généralisés du code C, à cela près qu'elles sont ici étendues au cadre des extensions finies arbitraires, et que *le symbole C^* désigne ici la k-enveloppe* de C.

Notation. On note $\max_{\mathrm{C}}\mathrm{Rwt}$ pour $\max\limits_{\mathbf{c}\in C} \mathrm{Rwt}(\mathbf{c})$.

Il est clair que $\max_{\mathrm{C}}\mathrm{Rwt} \leq \mathrm{Rwt}(C)$, et il y a égalité si et seulement s'il existe $\mathbf{c} \in C$ tel que $\mathrm{Rsupp}(C) = \mathrm{Rsupp}(\mathbf{c})$.

Définition 5. On définit

1. $OS_r(C) = \min_{\substack{D\subset C\\ \dim(D)=r}} \max_{\mathrm{D}} \mathrm{Rwt}$ (Oggier-Sboui 12)
2. $D_r(C) = \min_{\substack{D\subset C\\ \dim(D)=r}} \max_{\mathrm{D}^*} \mathrm{Rwt}$ (Ducoat 15)
3. $\mathcal{M}_r(C) = \min_{\substack{V\subset L^n, V=V^*\\ \dim(C\cap V)\geq r}} \dim V$ (Kurihara-Matsumoto-Uyematsu 15)
4. $d_{R,r}(C) = \min_{\substack{D\subset C\\ \dim(D)=r}} \mathrm{Rwt}(D)$ (J-P 17).

Jurrius-Pellikaan ont montré dans [J-P 17] que

- $d_{R,r}(C) = \mathcal{M}_r(C)$ quand L/k est galoisienne ;
- si $n \leq m$ et L/k est cyclique, alors $\mathcal{M}_r(C) = D_r(C)$ (voir aussi [Ducoat]) ;
- si $n \leq m$ et $k = \mathbb{F}_q$, l'assertion (ii) du Thm A est vérifiée et toutes ces définitions coïncident.

Théorème B [BF– 20]
Si $n \leq m$, ou même dès que la k-enveloppe de C vérifie $\dim C^* \leq m$, alors les quatre définitions ci-dessus coïncident.

Démonstration. Comme $\dim C^* \leq m$, notre Théorème A assure que

$$\max_{\mathrm{D}} \mathrm{Rwt} = \mathrm{Rwt}(D),$$

pour tout sous-espace D de L^n. Cela donne que $d_{R,r}(C) = OS_r(C)$.
Pour montrer que $OS_r(C) = D_r(C)$, on applique encore le Théorème A ; on a bien $\mathrm{Rwt}(D) = \mathrm{Rwt}(D^*)$ puisque $\mathrm{Rsupp}(D^*) = \mathrm{Rsupp}(D)$ (Corollaire 3).

Enfin, la preuve donnée dans [J-P 17] que $d_{R,r}(C) = \mathcal{M}_r(C)$ quand L/k est galoisienne se généralise à notre cadre. En effet l'égalité $\mathrm{Rwt}(D) = \dim D^*$ (voir notre Prop. 4) nous ramène à leur preuve que $\mathcal{M}_r(C) = \min\limits_{\substack{D \subset C \\ \dim(D)=r}} \dim D^*$. Celle-ci est vraie ici grâce aux propriétés immédiates de la k-enveloppe. $\square$

Références

- **[BF–]** G. Berhuy, J. Fasel and O. Garotta, *Rank weights for arbitrary finite field extensions*, *Adv. Math. Commun.*, (2020), doi : 10.3934/amc.2020083

- **[J-P 17]** R. Jurrius and G. R. Pellikaan, *On defining generalized rank weights*, *Adv. Math. Commun.*, **11** (2017), 225–235.

- M. Giorgetti and A. Previtali, *Galois invariance, trace codes and subfield subcodes*, *Finite Fields Appl.*, **16** (2010), 96–99.

- F. Oggier and A. Sboui, *On the existence of generalized rank weights*, in *2012 IEEE International Symposium on Information Theory*, (2012), 406–410.

- J. Kurihara, R. Matsumoto and T. Uyematsu, *Relative generalized rank weight of linear codes and its applications to network coding*, *IEEE Trans. Inform. Theory*, **61** (2015), 3912–3936.

- J. Ducoat, *Generalized rank weights : A duality statement.* Topics in Finite Fields, in *Contemporary Mathematics*, Vol. 632, Amer. Math. Soc., Providence, RI, 2015, 101–109.