Rank weights for arbitrary finite field extensions

Grégory Berhuy        Jean Fasel        Odile Garotta

Abstract

In this paper, we study several definitions of generalized rank weights for arbitrary finite extensions of fields. We prove that all these definitions coincide, generalizing known results for extensions of finite fields.

Contents

1 Introduction 1
2 Basics on rank supports 3
3 The geometric viewpoint 6
4 A generalization of the Galois closure of a subspace 9
5 Generalized rank weights for finite extensions 12

1 Introduction

Rank metric codes were introduced by Gabidulin in [Gab85] as linear codes over a finite extension of a given finite field. Their application to network coding has recently induced a lot of theoretical research, and many notions in the theory for codes with the Hamming metric have found an equivalent for codes with the rank metric. One of these is the definition of the generalized Hamming weights associated to the Hamming distance of a code, which has given rise to several proposed definitions of the generalized rank weights of a rank metric code. The first definition was given by Kurihara-Matsumoto-Uyematsu [KMU13], an alternative one was proposed by Oggier-Sboui in [OS12], then Ducoat proved in [Duc15, Prop II1] the equivalence of the first definition with a refinement of the second. In [JP17], motivated by their interest in the \( r \)-th generalized rank weight enumerator of a rank metric code, Jurrius-Pellikaan gave yet another definition of these weights. Moreover, they considered the general setting of finite Galois extensions, a study initiated by Augot-Loidreau-Robert in [ALR13].

They introduced the notion of rank support of a vector and of a code, proving for finite fields that, in case the length \( n \) of the code is bounded by the degree \( m \) of the extension, there exists a vector in the code \( C \) which has same rank support as \( C \) ([JP17, Proposition 3.6]). This was a crucial step in showing the equivalence of all the proposed definitions in the case of finite fields ([JP17, 5.2]) and [JP17, Remark 3.7] raised the question of whether this statement holds more generally. To study the case of general Galois extensions, Jurrius-Pellikaan used the field trace and the Galois closure of a code and proved the equivalence of their definition with the one given by Kurihara-Matsumoto-Uyematsu.
In the restricted case of cyclic extensions, they linked rank support and Galois closure and showed the equivalence of their definition with the refined definition of [Duc15], always under the hypothesis $n \leq m$.

In this paper we positively answer the question of generalizing [JP17, 3.6] for any finite extension (Theorem 3.1).

**Theorem.** Let $L/k$ be a finite field extension of degree $m$ and let $C \subset L^n$ be a linear subspace. If $m \geq n$, then there exists $c \in C$ such that

$$\text{Rsupp}(C) = \text{Rsupp}(c).$$

Moreover, we generalize the notion of the Galois closure of an $L$-linear code to an arbitrary finite field extension (Definition 4.4).

**Definition.** Let $L/k$ be any field extension, and let $n \geq 1$. For any $L$-linear subspace $C$ of $L^n$, we denote by $C^*$ the intersection of all $L$-linear subspaces of $L^n$ extended from $k^n$ and containing $C$.

We prove that $C^*$ coincides with the Galois closure of $C$ in case the field extension is Galois, using that for such an extension a linear code $C$ in $L^n$ is Galois invariant if and only if it has a basis in $k^n$ ([GP10]). This generalization of the Galois closure of an $L$-linear code allows to consider the following definitions (again, for an arbitrary extension of fields).

**Definition.**

1. $d_{R,r}(C) = \min_{D \subset C} \{ \text{wt}_R(D) : \text{dim}(D) = r \}$, following [JP17, Definition 2.5]

2. $M_r(C) = \min_{V \subset L^n, V = V^*} \{ \text{dim}(V) : \text{dim}(C \cap V) \geq r \}$, following [KMU13, Definition 5]

3. $OS_r(C) = \min_{D \subset C} \{ \max\text{wt}_R(D) : \text{dim}(D) = r \}$, following [OS12]

4. $D_r(C) = \min_{D \subset C} \{ \max\text{wt}_R(D^*) : \text{dim}(D) = r \}$, following [Duc15].

In this setting, we finally present a unified proof of the equivalence of all proposed definitions of generalized rank weights (Theorem 3.1).

**Theorem.** Let $L/k$ be a finite extension of degree $m$, let $n \geq 1$ be an integer such that $n \leq m$ and let $C$ be an $L$-linear subspace of $L^n$. Then the above four definitions coincide.

The paper is organized as follows. Section 2 presents basic results on rank supports and their relations with the restriction of a code. In particular, Proposition 2.11 may be seen as a generalization of the well-known result of Delsarte [Del75, Theorem 2] to arbitrary finite extensions. Section 3 is devoted to giving a geometric proof of Theorem 3.1. We warn the reader that this section involves some algebraic geometry, and in particular the notion of Weil restriction. In section 4 we present our generalization of the notion of Galois closure of an $L$-linear code for arbitrary field extensions (Definition 4.4). We show that our closure has nice properties, in particular we prove in Proposition 4.7 that for finite extensions it is precisely the $L$-extension of the rank support, thus generalizing the Galois case [JP17, 5.5]. In section 5, we use this proposition and Theorem 3.1 to prove the equivalence of all four (extended) definitions of the $r$-th generalized rank weights (under the hypothesis $m \geq n$), in the setting of arbitrary finite extensions (Theorem 5.3).
Acknowledgments

The authors warmly thank Frédérique Oggier for a gentle introduction to rank metric codes and to the paper [JP17].

2 Basics on rank supports

Let \( k \subset L \) be a finite field extension and let \( n \in \mathbb{N}^* \). Given an \( L \)-linear subspace \( C \) of \( L^n \), we define (following [GP10]) its restriction \( \text{Res}(C) \) as the \( k \)-linear subspace \( C \cap k^n \) of \( k^n \). Given a \( k \)-linear subspace \( D \) of \( k^n \), we let \( D_L \) denote the \( L \)-linear subspace of \( L^n \) generated by \( D \). Note that \( D_L \) is canonically isomorphic to \( D \otimes_k L \).

If \( \varphi : D \to D' \) is a \( k \)-linear map, we denote by \( \varphi_L \) the \( L \)-linear map \( D_L \to D'_L \).

Let \( m = [L : k] \) and let \( \alpha_1, \ldots, \alpha_m \) be a \( k \)-basis of \( L \). For any \( n \)-tuple \( e = (e_1, \ldots, e_n) \in L^n \), we may write \( e_j = \sum_{i=1}^m e_{ij} \alpha_i \) and obtain a matrix \( M(e) := (e_{ij}) \in M_{mn}(k) \).

The definitions of rank supports of a vector and of a subspace of \( L^n \) were introduced by Jurrius and Pellikaan [JP17].

**Definition 2.1.**

a) For any \( e \in L^n \), we call rank support of \( e \) the subspace of \( k^n \) generated by the rows of \( M(e) \) and write it \( \text{Rsupp}(e) \). Its dimension is the rank weight of \( e \), denoted by \( \text{wt}_R(e) \).

b) Let \( C \subset L^n \) be an \( L \)-linear subspace. We call rank support of \( C \) the \( k \)-linear subspace

\[
\text{Span}_k(\text{Rsupp}(e) | e \in C)
\]

and write it \( \text{Rsupp}(C) \). Its dimension is the rank weight of \( C \), denoted by \( \text{wt}_R(C) \).

c) The rank distance \( d_R(C) \) of an \( L \)-linear subspace \( C \) of \( L^n \) is the minimum rank of a matrix \( M(e) \), for \( e \) nonzero in \( C \). That is, we have \( d_R(C) = \min_{e \in C \setminus \{0\}} \text{wt}_R(e) \).

We now state some basic properties of rank supports.

**Proposition 2.2.** Let \( e, e' \in L^n \), let \( \alpha \in L^* \) and let \( C \) be an \( L \)-linear subspace of \( L^n \). Then

1. \( \text{Rsupp}(e) \) does not depend on the choice of the \( k \)-basis of \( L \).
2. \( \text{Rsupp}(\alpha e) = \text{Rsupp}(e) \).
3. \( \text{Rsupp}(e + e') \subset \text{Rsupp}(e) + \text{Rsupp}(e') \).
4. If \( e_1, \ldots, e_r \) generate \( C \) as an \( L \)-linear space, then \( \text{Rsupp}(C) \) is the \( k \)-linear sum of the \( \text{Rsupp}(e_i), i = 1, \ldots, r \).
5. Suppose \( e \neq 0 \). Then \( \text{wt}_R(e) = 1 \) if and only if there exists \( \lambda \in L^* \) such that \( \lambda e \in k^n \). In that case we have \( \text{Rsupp}(\lambda e) = k \lambda e \).
6. \( C \) has rank distance \( d_R(C) = 1 \) if and only if \( \text{Res}(C) \neq \{0\} \).
7. We have the inclusion of \( k \)-subspaces \( \text{Res}(C) \subset \text{Rsupp}(C) \).
8. We have the inclusion of $L$-subspaces $C \subset \text{Rsupp}(C)_L$.

**Proof.** Properties 1-4 are proved in [JP17, §2.3]. Let us prove statement 5: we may assume that the first vector $\alpha_1$ of our $k$-basis of $L$ is 1. Then for any nonzero $e' \in k^n$, all rows of $M(e')$ are zero except the first one, which is the $n$-tuple $e'$ itself. We then get $\text{Rsupp}(e') = ke'$ and $\text{wt}_R(e') = 1$. Thanks to statement 2, it remains to consider the situation when $M(c)$ has rank one. In that case there exists an $l$ such that all $m$ rows of $M(c)$ are colinear with the nonzero $l$-th row: $c^{(i)} = \mu_i e^{(l)}$, $\mu_i \in k$, $1 \leq i \leq m$. We get $c = (\sum_{i=1}^m \mu_i \alpha_i) e^{(l)} \neq 0$, that is $\lambda c \in k^n$ with $\lambda$ the inverse of $\sum_{i=1}^m \mu_i \alpha_i$. So property 5 is proved. Since the rank distance of $C$ is the minimum rank weight of a nonzero vector in $C$, it immediately yields statement 6. We turn to statement 7. If $c \in \text{Res}(C)$, we know from property 5 that $\text{Rsupp}(c) = kc$. This gives the inclusion $\text{Res}(C) \subset \text{Rsupp}(C)$. Finally we prove statement 8. Using property 4, it suffices to consider the case where $C = Lc$. So we need to prove that $c \in \text{Rsupp}(c)_L$. But this is clear using the definition of $\text{Rsupp}(c)$.

**Proposition 2.3.** Let $L/k$ be a finite extension, let $n \geq 1$, and let $C \subset L^n$ be an $L$-linear subspace. Then we have $\text{Res}(C) = \text{Rsupp}(C)$ if and only if $C$ has a basis in $k^n$ or, equivalently, if and only if $\dim_k \text{Res}(C) = \dim C$. In particular, we then have $\text{Rsupp}(C)_L = C$.

**Proof.** Suppose that $C$ has a basis $e_1, \ldots, e_r$ in $k^n$. Statement 5 of Proposition 2.2 shows that $\text{Rsupp}(e_i) = ke_i$, $(1 \leq i \leq r)$. Using statement 4 of the same proposition we see that the $e_i$’s generate $\text{Rsupp}(C)$. As $e_i \in \text{Res}(C)$, we get $\text{Rsupp}(C) \subset \text{Res}(C)$. We conclude that $\text{Res}(C) = \text{Rsupp}(C)$ using statement 7 in the previous proposition.

Suppose conversely that $\text{Res}(C) = \text{Rsupp}(C)$ and $C \neq 0$. Then $\text{R} \neq 0$. Let $e_1, \ldots, e_s$ be a basis of $\text{Res}(C)$. These vectors considered in $L^n$ are also independent over $L$. We show that they generate $C$ over $L$. Let $c \in C$. Then $\text{Rsupp}(C)$ contains $\text{Rsupp}(c)$, so our hypothesis implies that $\text{Rsupp}(c) \subset \text{Res}(C)$. Using a $k$-basis of the field $L$, we can thus write $c$ as an $L$-linear combination of vectors in $\text{Res}(C)$, therefore also of the vectors $e_1, \ldots, e_s$. Thus $e_1, \ldots, e_s$ is a basis of $C$ which is in $k^n$. Clearly this is equivalent to having $s = \dim C$.

The last equality then follows using the fact that $\text{Res}(C)_L = C$ if $C$ has a basis in $k^n$.  

We have the following general result.

**Proposition 2.4.** Let $L/k$ be a finite extension of degree $m$, and let $n \in \mathbb{N}^*$. Let $C$ be an $L$-linear subspace of $L^n$ of dimension $\leq m$ and suppose that $C$ admits an $L$-basis in $k^n$. Then there exists $c \in C$ such that $\text{Rsupp}(C) = \text{Rsupp}(c)$.

**Proof.** Let $e_1, \ldots, e_r$ denote an $L$-basis of $C$ in $k^n$, with $r \leq m$. From Proposition 2.3 we know that $\text{Rsupp}(C) = \text{Res}(C)$ is spanned by $e_1, \ldots, e_r$. Let $\alpha_1, \ldots, \alpha_m$ be a $k$-basis of $L$ and set $c = \sum_{i=1}^r \alpha_i e_i$. Then $c \in C$ and the matrix $M(c)$ has the $n$-tuples $e_1, \ldots, e_r$ as its first $r$ rows, and its $n-r$ remaining rows are zero. So $\text{Rsupp}(c)$ is spanned by $e_1, \ldots, e_r$ and therefore equal to $\text{Rsupp}(C)$.

**Remark 2.5.** Note that since $\text{wt}_R(c) \leq m$ for all $c$ in $L^n$, the hypothesis $\dim C \leq m$ in Proposition 2.4 is necessary. Indeed, if $C$ admits a basis in $k^n$, then $\text{Rsupp}(C)$ has dimension $\dim C$ by 2.3; see also Remark 4.8 for a stronger statement.

Recall that for any finite field extension $k \subset L$, we have the (field) trace $\text{Tr}: L \to k$, which is $k$-linear and non trivial in case $L/k$ is separable. We can extend this map to a trace map $\text{Tr}: L^n \to k^n$, which is the component-wise extension of the field trace.
Definition 2.6. Let \( k \subset L \) be a finite Galois extension with Galois group \( G \). The \textit{Galois closure} of an \( L \)-linear subspace \( C \) of \( L^n \), denoted by \( C^* \), is the smallest subspace of \( L^n \) that contains \( C \) and is invariant under the component-wise action of \( G \) on \( L^n \). The subspace \( C \) is called \textit{Galois closed} in case \( C \) is \( G \)-invariant, or equivalently in case \( C = C^* \).

The following result ([GP10, Theorem 1]) will play a crucial role in the sequel, notably in 4.3 when we set our generalized definition of the closure \( C^* \) of \( C \).

Theorem 2.7. If \( L/k \) be a finite Galois extension and \( C \) is an \( L \)-linear subspace of \( L^n \), then \( C = C^* \) if and only if \( C = \text{Res}(C)_L \) or, equivalently, if and only if \( C \) admits a basis in \( k^n \).

For Galois extensions, Jurrius-Pellikaan have shown in [JP17, Theorem 4.3] that the rank support of a subspace of \( L^n \) is equal to its image by \( \text{Tr} \). This actually holds (with same proof) for all \textit{separable} finite extensions \( L/k \).

Theorem 2.8. Suppose the finite field extension \( L/k \) is separable and let \( n \geq 1 \). Then for any \( L \)-linear subspace \( C \) of \( L^n \), we have \( \text{Rsupp}(C) = \text{Tr}(C) \).

Using this theorem we can generalize the setting of Theorem 9 in [GP10], which Giorgetti-Previtali have stated for Galois extensions (see 2.7).

Proposition 2.9. Let \( L/k \) be a finite separable extension and let \( C \) be an \( L \)-linear subspace of \( L^n \) for some \( n \geq 1 \). Then we have \( \text{Res}(C) = \text{Tr}(C) \) if and only if \( C \) admits a basis in \( k^n \).

Proof. This follows from Proposition 2.3 combined with Theorem 2.8.

We denote by \( \langle \cdot, \cdot \rangle \) the standard bilinear form on \( L^n \). Given any \( L \)-linear subspace \( C \) of \( L^n \), we define its orthogonal as the linear subspace

\[
C^\perp = \{ d \in L^n \mid \forall c \in C, \langle c, d \rangle = 0 \}.
\]

Lemma 2.10. Let \( L/k \) be any field extension and let \( C \) be an \( L \)-linear subspace of \( L^n \) for some \( n \geq 1 \). If \( C \) admits a basis in \( k^n \), then so does \( C^\perp \).

Proof. Let \( e_1, \ldots, e_r \) denote an \( L \)-basis of \( C \) in \( k^n \) and let \( D \) be the orthogonal of \( \text{Res}(C) \) relative to the standard bilinear form on \( k^n \). Then \( C^\perp \) is the intersection of the \( Le_i^\perp \) (\( 1 \leq i \leq r \)), and \( D \) has the same description over \( k \). Therefore \( C^\perp \supset D_L \). Since dimensions are the same we get \( C^\perp = D_L \), so \( C^\perp \) comes from \( k^n \).

For finite separable extensions, we know from Delsarte [Del75, Theorem 2] that \( \text{Res}(C)^\perp = \text{Tr}(C^\perp) \), for any \( L \)-linear subspace \( C \) of \( L^n \). Using Theorem 2.8, the following relation can be seen as a generalization of that equality to arbitrary finite extensions.

Proposition 2.11. Let \( L/k \) be a finite extension, let \( n \geq 1 \), and let \( C \) be an \( L \)-linear subspace of \( L^n \). Then we have

\[
\text{Res}(C)^\perp = \text{Rsupp}(C^\perp).
\]
Proof. We first show that $R_{\text{supp}}(C^\perp) \subset \text{Res}(C)^\perp$. Take $d \in C^\perp$ and $c \in \text{Res}(C)$. We have $d = \sum_{i=1}^{m} \alpha_i d^{(i)}$, where $\alpha_1, \ldots, \alpha_m$ is a $k$-basis of $L$ and the $d^{(i)}$s belong to $R_{\text{supp}}(C^\perp)$. We need to prove that all $\langle d^{(i)}, c \rangle$ are zero. Indeed we have $0 = \langle d, c \rangle = \sum_{j=1}^{n} (\sum_{i=1}^{m} \alpha_i d^{(i)} j) c_j = \sum_{i=1}^{m} \alpha_i \langle d^{(i)}, c \rangle$.

It now suffices to prove that $R_{\text{supp}}(C^\perp) \subset \text{Res}(C)$. Let $c \in k^n$ belong to $R_{\text{supp}}(C^\perp)$ and consider $d \in C^\perp$. As above, write $d = \sum_{i=1}^{m} \alpha_i d^{(i)}$, with all $d^{(i)}$s in $R_{\text{supp}}(C^\perp)$. Then we get $\langle c, d \rangle = \sum_{i=1}^{m} \alpha_i \langle c, d^{(i)} \rangle = 0$. Therefore $c \in (C^\perp)^\perp = C$. Since $c \in k^n$ the proof is complete.

Remark 2.12. In particular, the above proposition allows to compute the rank support of $C$. Indeed, as $(C^\perp)^\perp = C$, we get

$$R_{\text{supp}}(C) = \text{Res}(C)^\perp$$.

Finally we recover and complete the characterization of rank-degenerate codes given by Jurrius-Pellikaan in [JP17, Corollary 6.3]. Recall that these are the $L$-linear subspaces of $L^n$ such that $d_R(C^\perp) = 1$.

**Corollary 2.13.** Let $L/k$ be a finite extension and let $n \geq 1$. A linear code $C$ in $L^n$ is degenerate with respect to the rank metric if and only if we have $R_{\text{supp}}(C) \neq k^n$, or equivalently, if and only if $\text{Res}(C^\perp) \neq \{0\}$.

Proof. We apply statement 6 of Proposition 2.2 and combine it with Remark 2.12.

3 The geometric viewpoint

In this section, we prove the following theorem, which is our first main result.

**Theorem 3.1.** Let $L/k$ be a finite field extension of degree $m$ and let $C \subset L^n$ be a linear subspace. If $m \geq n$, then there exists $c \in C$ such that

$$R_{\text{supp}}(C) = R_{\text{supp}}(c).$$

We start with a few observations allowing to reduce the problem to an algebro-geometric problem. First, we note that we can suppose that $R_{\text{supp}}(C) = k^n$. Indeed, by Proposition 2.2, we have $C \subset R_{\text{supp}}(C)_L$. We may therefore choose a basis of $R_{\text{supp}}(C)$ and work with this vector space instead of $k^n$.

**Lemma 3.2.** Let $D \subset L^n$ be a $L$-linear subspace, and let $\varphi : k^n \rightarrow k$ be a linear map. Then

$$\varphi(R_{\text{supp}}(D))_L = \varphi(D).$$

Proof. As $D \subset R_{\text{supp}}(D)_L$, we have $\varphi(D)_L \subset \varphi(R_{\text{supp}}(D))_L$. Now, both terms are $L$-linear subspaces of $L$ and it suffices to prove that if $\varphi(D) = 0$, then $\varphi(R_{\text{supp}}(D))_L = 0$. Suppose then that $\varphi(D) = 0$ and let $d \in D$. We can write as before

$$d = \sum_{i=1}^{m} \alpha_i d^{(i)} \in k^n,$$
with \( d^{(i)} \in \text{Rsupp}(D) \). By definition, 
\[
\varphi_L(d) = \sum_{i=1}^{m} \alpha_i \varphi(d^{(i)})
\]
and linear independence implies that \( \varphi(d^{(i)}) = 0 \) for any \( i = 1, \ldots, m \). As \( \text{Rsupp}(D) \) is generated by the \( d^{(i)} \) for \( d \in D \), it follows that \( \varphi(\text{Rsupp}(D))_L = 0 \). \( \square \)

**Remark 3.3.** As a corollary, we see that \( \varphi(\text{Rsupp}(D)) = 0 \) if and only if \( \varphi_L(D) = 0 \), i.e. that 
\[
\text{Rsupp}(D) \subset \ker \varphi \iff D \subset \ker \varphi_L.
\]

In case \( \text{Rsupp}(D) = k^n \), this yields that \( \varphi = 0 \) if and only if \( \varphi_L(D) = 0 \).

**Proposition 3.4.** Let \( L/k \) be a finite field extension of dimension \( m \) and let \( n \leq m \). Let \( C \subset L^n \) be a plane with \( \text{Rsupp}(C) = k^n \). Then there exists \( \nu \in C \) such that 
\[
\varphi_L(\nu) = 0 \iff \varphi = 0
\]
for any \( k \)-linear map \( \varphi : k^n \to k \).

The proof of Proposition 3.4 will be of geometric nature. Before starting with it, we first recall a few facts about the Weil restriction of quasi-projective schemes. If \( X \) is a quasi-projective scheme over \( L \), then its Weil restriction \( \mathcal{R}_{L/k}X \) along the field extension \( L/k \) is the quasi-projective scheme over \( k \) satisfying 
\[
\text{Hom}_k(\text{Spec}(R), \mathcal{R}_{L/k}X) = \text{Hom}_L(\text{Spec}(R_L), X).
\]
for any \( k \)-algebra \( R \) (its existence is given by [BLR90, §7.6] and [CGP15, Proposition A.5.8]). For instance, if \( X = A^1_L \), then \( \mathcal{R}_{L/k}A^1_L \simeq A[\text{Hom}_L(L, k)] \simeq k^m_L \) as a direct computation shows (or [Poo17, §4.6]). In particular, we see that the Krull dimension of \( \mathcal{R}_{L/k}A^1_L \) is \( m \). If \( X = \mathbb{P}^1_L \), then [CGP15, Proposition A.5.9] shows that \( \mathcal{R}_{L/k}\mathbb{P}^1_L \) is connected and [CGP15, Proposition A.5.2] implies that an open immersion \( A^1_L \subset \mathbb{P}^1_L \) induces an open immersion \( \mathcal{R}_{L/k}A^1_L \subset \mathcal{R}_{L/k}\mathbb{P}^1_L \). This shows that \( \mathcal{R}_{L/k}\mathbb{P}^1_L \) is of dimension \( m \). More generally, one can prove that the Weil restriction \( \mathcal{R}_{L/k}X \) of a smooth quasi-projective scheme \( X \) of (pure) dimension \( d \) is of dimension \( dm \) but we don’t use this fact here.

The main ingredient of the proof of Proposition 3.4 is a morphism of schemes 
\[
f : \mathbb{P}^{n-1}_k \to \mathcal{R}_{L/k}\mathbb{P}(C) \simeq \mathcal{R}_{L/k}\mathbb{P}^1_L
\]
that we now define. Let \( R \) be a finitely generated \( k \)-algebra. Recall from [Gro61, Chapitre 4] that the set of \( R \) points of \( \mathbb{P}^{n-1}_k \) is identified with a line bundle \( M \) over \( R \) and an equivalence class of surjections 
\[
\varphi : R^n \to M
\]
under the natural action of \( R^\times \). To such a surjection, we can associate its kernel \( \ker \varphi \), which is a projective \( R \)-module \( P \) of rank \( n - 1 \). Extending scalars to \( L \), we obtain a projective \( R_L \)-module \( P_L \) which is a submodule of \( R^n_L \). We can then consider the intersection \( P_L \cap (C \otimes_L R_L) \subset C \otimes_L R_L \) where \( C \) is the plane in the problem.
Lemma 3.5. The submodule $P_L \cap (C \otimes_L R_L)$ is locally free of rank 1.

Proof. It suffices to prove that for any maximal ideal $m$ of $R_L$, the module is free of rank one after tensoring with $L(m) = R_L/m$. Now, $L(m)$ is a finite field extension of $L$, and thus of $k$. By construction, $P_{L(m)} = \ker \varphi_{L(m)}$ and we have to compute the dimension of $P_{L(m)} \cap C_{L(m)}$. As $P_{L(m)}$ is of dimension $n-1$ and $C_{L(m)}$ of dimension 2, the intersection can’t be trivial. Suppose that $P_{L(m)} \cap C_{L(m)} = C_{L(m)}$, i.e. that $C_{L(m)} \subset P_{L(m)}$. This means that $\varphi_{L(m)}(C_{L(m)}) = 0$ and then that $\varphi_L(C) = 0$. By Remark 3.3 this implies that $\varphi(\text{Supp}(C)) = 0$, i.e. that $\varphi = 0$, which is excluded. Thus, $P_L \cap (C \otimes_L R_L)$ is locally free of rank 1.

The lemma shows that the map

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

is well-defined. To make it more explicit, we compute the image of a $k$-point $[a_1 : \ldots : a_n]$ of $\mathbb{P}^{n-1}_k$. A representative of the equivalence class of linear maps $\varphi : k^n \to k$ associated to this point is

$$\alpha : k^n \to k$$

given by $(u_1, \ldots, u_n) \mapsto \sum_{i=1}^{n} a_i u_i$. If $C = \text{Span}(v, w) \subset L^n$ with $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$ is such that $\text{RSupp}(C) = k^n$, we see that an element of the form $\alpha v + \mu w$ is in the kernel of $\alpha_L$ if and only if $\alpha(\sum a_i v_i) + \beta(\sum a_i w_i) = 0$. It follows that

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

We are now ready to prove Proposition 3.4. We observe first that a rational point of $\mathcal{R}_{L/k}\mathbb{P}(C)$ corresponds to a $L$-point of $\mathbb{P}(C)$, i.e. to a $L$-linear subspace $L \cdot v$ of $C$, where $v \in C$ is non trivial. This rational point is in the image of $f$ if and only if there exists a surjection $\varphi : k^n \to k$ whose kernel $P$ has the property that $P_L \cap C = L \cdot v$, i.e. $\varphi_L(v) = 0$ and $\varphi_L(C) \neq 0$. In view of Lemma 3.2, we see that a rational point $L \cdot v \in \mathcal{R}_{L/k}\mathbb{P}(C)$ is in the image of $f$ if and only if there exists a surjection $\varphi : k^n \to k$ such that $\varphi_L(v) = 0$. Thus, we see that a rational point of $\mathcal{R}_{L/k}\mathbb{P}(C)$ not in the image of $f$ satisfies the conclusion of Proposition 3.4 and it suffices to show that the morphism $f$ is not surjective on $k$-points. Let $Z \subset \mathcal{R}_{L/k}\mathbb{P}(C)$ be the closure of the image of $f$. It is of dimension at most the dimension of $\mathbb{P}^{n-1}_k$, i.e. at most $n-1$, while $\mathcal{R}_{L/k}\mathbb{P}(C)$ is of dimension $m = [L : k]$. As $m \geq n$, we see that $Z$ is a proper closed subset of $\mathcal{R}_{L/k}\mathbb{P}(C)$. If $k$ is infinite, it follows that there is a rational point in the open complement of $Z$ and the result is proved. If $k$ is finite, we observe that $\mathbb{P}^{n-1}_k$ has $\frac{|k|^n - 1}{|k| - 1}$ rational points. On the other hand, the $(k)$-rational points of $\mathcal{R}_{L/k}\mathbb{P}(C)$ are in bijection with the $(L)$-rational points of $\mathbb{P}^1_L$ and it follows that there are $\frac{|L|^2 - 1}{|L| - 1}$ such points. We conclude using the fact that

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

We now proceed with the proof of theorem 3.1.
proof of Theorem 3.1. If $C$ is of dimension $\leq 1$, then there is nothing to do. Suppose then that $n \geq 2$ and that $C \subset L^n$ is a plane. As usual, we may assume that $\text{Resupp}(C) = k^n$. By Proposition 3.4, there exists $c \in C$ such that $c \in \ker(\varphi_L)$ if and only if $\varphi = 0$. If $\text{Resupp}(c) \neq k^n$, there exists a non-trivial linear form $\psi : k^n \to k$ such that $\psi(\text{Resupp}(c)) = 0$. By Lemma 3.2, this forces $\psi(c) = 0$ which contradicts the assumption on $c$. So the theorem holds in this case.

To prove the general case, we now work by induction on the dimension $2 \leq r \leq n$ of $C$. We can write $C = D \oplus Le$ for some $D$ of dimension $r - 1$ and some nontrivial $e$. By induction, there exists $d \in D$ such that $\text{Resupp}(d) = \text{Resupp}(D)$. Now, $\text{Resupp}(C)$ is spanned by $\text{Resupp}(d)$ and $\text{Resupp}(e)$, i.e. by $\text{Resupp}(d)$ and $\text{Resupp}(e)$. By Proposition 2.2 we are thus reduced to considering $C' = \text{Span}_L(d, e)$ and we can conclude using the case of a plane proved above. 

Remark 3.6. In particular, taking $C = L^n$ shows that the condition $m \geq n$ is necessary in order for such an element $c \in C$ to exist for any subspace $C$ of $L^n$ (indeed $M(e)$ have $m$ rows); see also Remark 4.8.

Finally, recall from Corollary 2.13 that a code $C$ in $L^n$ is nondegenerate with respect to the rank metric if and only if $\text{Resupp}(C) = k^n$. Theorem 3.1 thus yields the following equivalence:

Proposition 3.7. Let $L/k$ be an extension of degree $m$, and let $C$ be an $L$-linear code of length $n$ which is nondegenerate with respect to the rank metric. Then there is a $c \in C$ such that $\text{Resupp}(C) = \text{Resupp}(c)$ if and only if $m \geq n$. 

Proof. Since matrices $M(e)$ have $m$ rows, the equality $\text{Resupp}(c) = k^n$ forces $m \geq n$. The converse is a special case of Theorem 3.1.

4 A generalization of the Galois closure of a subspace

Definition 4.1. Let $L/k$ by any field extension, and let $n \geq 1$. We say that an $L$-linear subspace $C$ of $L^n$ is extended from $k^n$ if $C$ is spanned by a family of vectors in $k^n$. Equivalently, $C$ has a basis in $k^n$, or else we have $C = \text{Res}(C)_L$.

Lemma 4.2. Let $L/k$ be any field extension, and let $n \geq 1$. If $(C_i)_{i \in I}$ is a family of subspaces of $L^n$ extended from $k^n$, then $\bigcap_{i \in I} C_i$ is extended from $k^n$. 

Proof. For each $i \in I$, one may write $C_i = (D_i)_L$, for some $k$-linear subspace $D_i$ of $k^n$, where the orthogonal is taken with respect to the standard $L$-bilinear form on $L^n$. Indeed, $C_i$ is the orthogonal of $C_i^\perp$, which by Lemma 2.10 is extended from $k^n$. 

Therefore, we have 

$$\bigcap_{i \in I} C_i = \bigcap_{i \in I} (D_i)_L = \text{Span}_L((D_i)_L, i \in I) = (\text{Span}_k(D_i, i \in I))_L.$$ 

Thus, $\bigcap_{i \in I} C_i$ is extended from $k^n$. 

Note that, given an $L$-linear subspace $C$ of $L^n$, there is at least one $L$-linear subspace of $L^n$ extended from $k^n$ and containing $C$, namely $L^n$ itself. Therefore, in view of lemma 4.2, the following statement makes sense.
Corollary 4.3. Let \( L/k \) be a finite Galois extension with Galois group \( G \), let \( n \geq 1 \), and let \( C \) be an \( L \)-linear subspace of \( L^n \). Then \( C^* \) is the intersection of all \( L \)-linear subspaces of \( L^n \) extended from \( k^n \) and containing \( C \).

Proof. Let \( C' \) be the intersection of all \( L \)-linear subspaces of \( L^n \) extended from \( k^n \) and containing \( C \). Since \( C^* \) is an \( L \)-linear subspace of \( L^n \) extended from \( k^n \) (by Theorem 2.7) and containing \( C \), we have \( C' \subset C^* \). Conversely, we have \( C \subset C' \) by definition. Since \( C' \) is extended from \( k^n \) (by Lemma 4.2), Theorem 2.7 shows that it is \( G \)-invariant. By definition of \( C^* \), we get \( C^* \subset C' \). \( \square \)

This corollary motivates the following generalization of the definition of \( C^* \).

Definition 4.4. Let \( L/k \) be any field extension, and let \( n \geq 1 \). For any \( L \)-linear subspace \( C \) of \( L^n \), we denote by \( C^* \) the intersection of all \( L \)-linear subspaces of \( L^n \) extended from \( k^n \) and containing \( C \). It is the smallest \( L \)-linear subspace of \( L^n \) extended from \( k^n \) and containing \( C \).

Remark 4.5. 1. If \( L/k \) is a finite Galois extension, we recover the usual definition of \( C^* \), by Corollary 4.3. However, this generalization is more convenient, since its does not need the extension \( L/k \) to be Galois.

2. The definition of \( C^* \) immediately yields the following properties.

   (a) for all \( L \)-linear subspaces \( C \) of \( L^n \), we have \( C \subset C^* \).

   (b) for all \( L \)-linear subspaces \( C \) of \( L^n \), we have \( C = C^* \) if and only if \( C \) is extended from \( k^n \).

   In particular, \((C^*)^* = C^* \).

   (c) for all \( L \)-linear subspaces \( D \) of \( L^n \) extended from \( k^n \) such that \( C \subset D \), we have \( C^* \subset D \).

   (d) for all \( L \)-linear subspaces \( C, D \) of \( L^n \) such that \( C \subset D \), we have \( C^* \subset D^* \).

Proposition 4.6. Let \( L/k \) be any field extension and let \( C, C' \) be \( L \)-linear subspaces of \( L^n \) for some \( n \geq 1 \). Then we have \((C + C')^* = C^* + C'^* \).

Proof. By Remark 4.5 the subspace \((C + C')^* \) contains both \( C^* \) and \( C'^* \), thus it contains their sum. Now combining Lemmas 2.10 and 4.2, we see that given two subspaces \( D, D' \) of \( L^n \) which are extended from \( k^n \), their sum also is extended from \( k^n \). Indeed, the orthogonal of \( D + D' \) is the intersection of \( D^\perp + D'^\perp \). Therefore \( C^* + C'^* \) is extended from \( k^n \). Since it contains \( C + C' \), it also contains \((C + C')^* \). \( \square \)

Our next proposition generalizes Proposition 5.5 and Lemma 5.6 in [JP17]. In particular, it then follows from the first item in Remark 4.5 that their statements 5.5, 5.6 and 5.7 hold for any Galois extension, not necessarily cyclic.

Proposition 4.7. Let \( L/k \) be any finite extension and let \( C \) be an \( L \)-linear subspace of \( L^n \) for some \( n \geq 1 \). Then

\[ C^* = \text{Rsupp}(C)_L. \]

In particular we have \( \dim C^* = \text{wt}_R(C) \), so that \( \dim C \leq \text{wt}_R(C) \), and \( \dim(Lc)^* = \text{wt}_R(c) \) for any \( c \in L^n \).
Proof. We know from Proposition 2.2 that $\text{Rsupp}(C)_L$ contains $C$. Since it is also extended from $k^n$, $\text{Rsupp}(C)_L$ contains $C^*$. Conversely, $\text{Rsupp}(C)_L$ is included in $\text{Rsupp}(C^*)_L$, and since the subspace $C^*$ is extended from $k^n$, we have $\text{Rsupp}(C^*)_L = C^*$ (by Proposition 2.3). Whence $\text{Rsupp}(C)_L$ is equal to $C^*$. Now use that $\text{Rsupp}(C)_L$ has dimension $\dim \text{Rsupp}(C) = \text{wt}_R(C)$, and that $C \subset C^*$. Finally we write our equality for $C = Lc$ and use statement 2 of 2.2.

\[ \square \]

Remark 4.8. The equality $\dim C^* = \text{wt}_R(C)$ implies that the condition $\dim C^* \leq m$ is necessary for the existence of an element $c \in C$ such that $\text{Rsupp}(C) = \text{Rsupp}(c)$. Indeed, if $c \in L^n$ then its matrix $M(c)$ has $m$ rows so that $\dim \text{Rsupp}(c) \leq m$. In particular, the weaker condition $\dim C \leq m$ is necessary. Note that, whereas we have shown in Proposition 2.4 that in case $C$ is extended from $k^n$ this last condition is also sufficient, in case $C$ is not extended from $k^n$ and such an element $c$ exists, we deduce from our Proposition that $\dim C \leq m - 1$.

We give two corollaries to Proposition 4.7. Note that the second one admits an elementary proof, using the Galois group, in case the extension is Galois.

Corollary 4.9. Let $L/k$ be a finite extension, let $n \geq 1$, let $C$ be an $L$-linear subspace of $L^n$ and let $c \in C$. Then we have $\text{Rsupp}(C) = \text{Rsupp}(c)$ if and only if $C^* = (Lc)^*$, that is, if and only if $C \subset (Lc)^*$.

Proof. Since $\text{Rsupp}(c) \subset \text{Rsupp}(C)$ and $(Lc)^* \subset C^*$, both equalities are equivalent to the equality of the respective dimensions as $k$ and $L$-subspaces. But Proposition 4.7 shows that the $k$-dimension of $\text{Rsupp}(C)$ is the same as the $L$-dimension of $C^*$, and similarly when replacing $C$ with $Lc$.

Finally, if $c \in C$ and $C \subset (Lc)^*$, we deduce that $C^* = (Lc)^*$ by the second remark 4.5.

\[ \square \]

Corollary 4.10. Let $L/k$ be a finite extension, let $n \geq 1$ and let $C$ be an $L$-linear subspace of $L^n$. Then $\text{Rsupp}(C) = \text{Rsupp}(C^*)$. In particular if $L/k$ is separable, we have $\text{Tr}(C) = \text{Tr}(C^*)$.

Proof. Proposition 4.7 implies that the $k$-subspaces $\text{Rsupp}(C)$ and $\text{Rsupp}(C^*)$ have the same dimension. Thus the obvious inclusion $\text{Rsupp}(C) \subset \text{Rsupp}(C^*)$ is an equality.

If $L/k$ is separable, Theorem 2.8 tells us that $\text{Rsupp}$ and $\text{Tr}$ coincide on $L$-linear subspaces of $L^n$, so the proof is complete.

\[ \square \]

Finally, we slightly generalize Proposition 2.4, which similarly works even in case $m < n$.

Lemma 4.11. Let $L/k$ be a finite extension of degree $m$, let $n \geq 1$, and let $C$ be an $L$-linear subspace of $L^n$ such that $\dim C^* \leq m$. Suppose $C = C_1 \oplus Lc_2$, where $c_2 \in k^n$, and that there exists $c_1 \in C_1$ such that $\text{Rsupp}(C_1) = \text{Rsupp}(c_1)$. Then there exists $c \in C$ such that $\text{Rsupp}(C) = \text{Rsupp}(c)$.

Proof. Let $\alpha_1, \ldots, \alpha_m$ denote a $k$-basis of $L$. We know from Proposition 2.2 that $\text{Rsupp}(c_2) = kc_2$ and that $\text{Rsupp}(C)$ is thus the sum of $\text{Rsupp}(c_1)$ and $kc_2$. If $c_2 \in \text{Rsupp}(c_1)$ we are done, so we assume the contrary. Then the sum is direct, so that taking dimensions we get by Proposition 4.7 $\dim \text{Rsupp}(C) \leq m$ and $\text{wt}_R(c_1) \leq m - 1$. Thus one row of the matrix $M(c_1)$, say the last one, is a linear combination of the other ones. We change the vectors $\alpha_1, \ldots, \alpha_{m-1}$ of the basis of $L$ by adding to each of them a vector $\mu_i c_m$, where $\mu_i \in k$ is chosen so that, in the new basis of $L$, the last row of the corresponding matrix $M(c_1)$ is zero. We set $c = c_1 + \alpha_m c_2 \in C$ so that we have $\text{Rsupp}(c) = \text{Rsupp}(c_1) + kc_2 = \text{Rsupp}(C)$.

\[ \square \]
Corollary 4.12. Let $L/k$ be a finite extension of degree $m$, let $n \geq 1$, and let $C$ be an $L$-linear subspace of $L^n$ such that $\dim C^* \leq m$. Suppose that $C_1$ is an $L$-linear subspace such that $C = C_1 + \text{Res}(C)_L$, and that there exists $c_1 \in C_1$ such that $R\text{supp}(C_1) = R\text{supp}(c_1)$. Then there exists $c \in C$ such that $R\text{supp}(C) = R\text{supp}(c)$.

Proof. Let $e_1, \ldots, e_l$ be vectors of $\text{Res}(C)$ which complete a basis of $C_1$ to an $L$-basis of $C$. We may repeatedly apply Lemma 4.11, taking successively $C_1^{(i)} = C_1 + \sum_{j<i} L e_j$. $e_2 = e_i$, $1 \leq i \leq l$. \hfill $\Box$

5 Generalized rank weights for finite extensions

We now set notation in order to discuss the various definitions of the generalized rank weights of a code and their equivalence. In what follows, we let $k \subset L$ be a finite extension of degree $m$, and let $n \in \mathbb{N}^*$. We let $C$ be a linear subspace of $L^n$ and let $r$ be an integer such that $1 \leq r \leq \dim C$. Recall from Remark 4.5 that our definition 4.4 of $C^*$ generalizes the definition of Galois closure used in [JP17].

Notation 5.1. We will denote by $\max\max wt_R(C)$ the maximum value $\max_{c \in C} wt_R(c)$.

Clearly we have $\max\max wt_R(C) \leq wt_R(C)$, and equality holds if and only if there exists $c \in C$ such that $R\text{supp}(C) = R\text{supp}(c)$.

We now present, in the setting of an arbitrary finite extension, the various definitions which have been proposed for the $r$-th generalized rank weight of $C$. We insist that the star symbol used in definitions 2. and 4. refers to our definition 4.4, so that 2. and 4. are indeed generalized versions of the definitions considered in [JP17].

Definition 5.2. 1. $d_{R,r}(C) = \min_{\dim(D)=r} \max wt_R(D)$, following [JP17, Definition 2.5]
2. $M_r(C) = \min_{V \subset L^n, \dim(V) \geq r} \dim V$, following [KMU13, Definition 5]
3. $OS_r(C) = \min_{\dim(D) = r} \max\max wt_R(D)$, following [OS12]
4. $D_r(C) = \min_{\dim(D) = r} \max\max wt_R(D^*)$, following [Duc15].

Jurrius-Pellikaan have shown in [JP17, 4.4 and 5.4], that $d_{R,r}(C) = M_r(C)$ whenever $L/k$ is Galois. They also proved in [JP17, Theorem 5.8] that if $m \geq n$ and $L/k$ is cyclic, then $M_r(C) = D_r(C)$.

Our main statement in this section is the following result.

Theorem 5.3. Let $L/k$ be a finite extension of degree $m$, let $n \geq 1$ be an integer such that $n \leq m$ and let $C$ be an $L$-linear subspace of $L^n$. Then all four definitions 5.2 coincide.

Proof. Since $m \geq n$, Theorem 3.1 implies that $\max\max wt_R(D) = wt_R(D)$, for all subspaces $D$ of $L^n$. This gives $d_{R,r}(C) = OS_r(C)$. To prove $OS_r(C) = D_r(C)$, we combine Theorem 3.1 with the fact that, by Corollary 4.10, $D$ and $D^*$ have the same rank support, and therefore $wt_R(D) = wt_R(D^*)$. 

12
Finally, the proof given in [JP17, 4.4 and 5.4] that $d_{R,r}(C) = \mathcal{M}_r(C)$ whenever $L/k$ is Galois relies both on the equality $\dim D^* = \text{wt}_R(D)$, which we have proved in 4.7 in the setting of arbitrary finite extensions, and on the properties of $D^*$ and $V^*$ stated in the second remark 4.5. Thus this equality still holds in our setting.

References

[ALR13] D. Augot, P. Loidreau, and G. Robert. Rank metric and Gabidulin codes in characteristic zero. In *ISIT-2013 International Symposium on Information Theory*, pages 509–513, 2013.

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Band 21. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin-New York, 1990.

[CGP15] B. Conrad, O. Gabber, and G. Prasad. *Pseudo-reductive Groups*. New Mathematical Monographs. Cambridge University Press, Cambridge, 2015.

[Del75] P. Delsarte. On subfield codes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory* IT-21, 5:575–576, 1975.

[Duc15] J. Ducoat. Generalized rank weights: a duality statement. In *Topics in Finite fields*, volume 632, pages 101–109. American Mathematical Society, 2015.

[Gab85] É. M. Gabidulin. Theory of codes of maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[GP10] M. Giorgetti and A. Previtali. Galois invariance, trace codes and subfield codes. *Finite Fields and Their Applications*, 16:96–99, 2010.

[Gro61] Alexandre Grothendieck. Eléments de géométrie algébrique: II. Étude globale élémentaire de quelques classes de morphismes. *Publ. Math. Inst. Hautes Études Sc*., 8:5–222, 1961.

[JP17] R. Jurrius and R. Pellikaan. On defining generalized rank weights. *Advances in Mathematics of Communications*, 11(1):115–235, 2017.

[KMU13] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weights of linear codes and its applications to network coding. *IEEE Transactions on Information Theory*, 61(7):3912–3936, 2013.

[OS12] F. Oggier and A. Sboui. On the existence of generalized rank weights. In *ISIT-2012 International Symposium on Information Theory*, pages 406–410, 2012.

[Poo17] B. Poonen. *Rational Points on Varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, 2017.