Generalized weights: an anticode approach

Alberto Ravagnani

Institut de Mathématiques, Université de Neuchâtel
Emile-Argand 11, CH-2000 Neuchâtel, Switzerland

Abstract

In this paper we study generalized weights as an algebraic invariant of a code. We first describe anticodes in the Hamming and in the rank metric, proving in particular that optimal anticodes in the rank metric coincide with Frobenius-closed spaces. Then we characterize both generalized Hamming and rank weights of a code in terms of the intersection of the code with optimal anticodes in the respective metrics. Inspired by this description, we propose a new algebraic invariant (which we call Delsarte generalized weights) for Delsarte rank-metric codes based on optimal anticodes in the space of matrices with given size and entries in a finite field. We show that our invariant refines the generalized rank weights for Gabidulin codes introduced by Kurihara, Matsumoto and Uyematsu, and establish a series of properties of Delsarte generalized weights. In particular, we characterize Delsarte optimal codes and anticodes in terms of their generalized weights. We also present a duality theory for the new algebraic invariant, proving that the Delsarte generalized weights of a code completely determine the Delsarte generalized weights of the dual code. Our results extend the theory of generalized rank weights for Gabidulin codes. Finally, we establish the analogue for Gabidulin codes of a theorem of Wei, proving that the generalized rank weights proposed by Kurihara, Matsumoto and Uyematsu characterize the worst-case security drops of a Gabidulin rank-metric code.

Introduction

Linear codes with the Hamming metric can be employed in wiretap channels to secure a communication against an eavesdropper (see e.g. [8]). In [13], Wei proved that the performance of a code employed in such a channel is measured by an algebraic invariant of the code, namely, the collection of its generalized Hamming weights. Generalized Hamming weights have interesting mathematical properties. For example, they generalize the notion of minimum distance of a linear code, and they always form a strictly increasing sequence of integers (monotonicity). Another interesting combinatorial property is that the generalized Hamming weights of a linear code $C$ completely determine the generalized Hamming weights of the dual code $C^\perp$. The generalized Hamming weights of a code $C$ are defined in terms of the supports of the subcodes of $C$ of given dimension (see Section 4 for a precise definition).

*The author was partially supported by the Swiss National Science Foundation through grant no. 200021_150207.
Recently, Silva and Kschishang proposed a scheme based on Gabidulin rank-metric codes to secure a communication against an eavesdropper over a network in a universal way (see [12] for details). An important feature of the scheme proposed in [12] is that it is compatible with linear network coding. Generalized (and relative) rank weights were proposed by Kurihara, Matsumoto and Uyematsu in [6] to measure the performance of a Gabidulin code when employed in the scheme of [12]. The generalized rank weights of a Gabidulin code \( C \) are defined in terms of the intersections of \( C \) with Frobenius-closed spaces. Generalized rank weights also have interesting mathematical properties, including monotonicity and a duality theory (see [6] and [2]).

In [1] Delsarte defined rank-metric codes as linear spaces of matrices of given size over a finite field \( \mathbb{F}_q \). There exists a natural way to associate to a Gabidulin code a Delsarte code with the same metric properties. Hence Delsarte codes may be regarded as a generalization of Gabidulin codes. It is not clear however how to extend the definition of generalized rank weights for Gabidulin codes to Delsarte codes in a convenient way, i.e., producing a well-behaving algebraic invariant. This is the main problem that we address in our work.

Both linear Gabidulin and Delsarte codes have interesting applications in coherent and non-coherent linear network coding. For example, they play an important role in the construction of subspace codes to be used for random network coding following the approach of [5]. We address the interested reader to [11].

In this paper we focus on generalized weights for linear, Gabidulin and Delsarte codes from an algebraic point of view. We first investigate optimal anticodes in the Hamming and in the rank metric, and show that both generalized Hamming weights and generalized rank weights of a code can be characterized in terms of the intersection of the code with optimal anticodes in the respective metrics. In order to establish this characterization for generalized rank weights, we prove in particular that the Frobenius-closed spaces in \( \mathbb{F}_{q^m}^k \) are exactly the optimal anticodes in the rank metric. The result says in particular that the algebraic condition of being Frobenius-closed may be regarded as a metric condition. We also give a convenient method to compute a basis defined over \( \mathbb{F}_q \) of a Frobenius-closed space \( V \subseteq \mathbb{F}_{q^m}^k \) using linear algebra.

Inspired by the characterizations above, we propose a definition of generalized weights for Delsarte rank-metric codes based on optimal anticodes in the space of matrices. Then we prove that Delsarte generalized weights, as an invariant, refine generalized rank weights for Gabidulin codes. We establish several properties of Delsarte generalized weights, which may be regarded as the analogue for Delsarte codes of the classical properties of generalized Hamming and rank weights. In particular, we show that Delsarte optimal codes and anticodes are characterized by their Delsarte generalized weights. We also study how Delsarte generalized weights relate to the duality theory of Delsarte codes. In particular, we prove that the Delsarte generalized weights of a code determine the Delsarte generalized weights of the dual code. The proof of the result also shows how to compute the Delsarte generalized weights of the dual code starting from the generalized weights of the code.

Finally, we prove that the generalized rank weights proposed by Kurihara, Matsumoto and Uyematsu in [6] measure the worst-case security drops of a Gabidulin code employed in the scheme of [12]. More precisely, we establish the analogue for Gabidulin codes of a classical theorem of Wei on generalized Hamming weights.

The paper is organized as follows. In Section 1 we give preliminary definitions and results on linear and rank-metric codes. In Section 2 we characterize generalized Hamming weights
in terms of optimal anticodes in the Hamming metric. In Section 3 we prove that Frobenius-
closed spaces coincide with optimal anticodes in the rank metric, and characterize generalized
rank weights in terms of optimal anticode. Delsarte codes are introduced in Section 4 where
we also explain how they relate to Gabidulin codes. In Section 5 we define Delsarte generalized
weights, and prove that they refine generalized rank weights for Gabidulin codes. The main
properties of Delsarte generalized weights are derived in Section 6, while in Section 7 we focus
on the duality theory of Delsarte codes, proving that the generalized weights of a Delsarte
code determine the generalized weights of the dual code. We prove the analogue for Gabidulin
codes of a theorem of Wei on security drops in Section 8.

1 Preliminaries

In this section we briefly recall some notions of coding theory. In particular, we give the
definition of generalized weights for the Hamming and the rank metric.

Notation 1. Throughout this paper, \( q \) denotes a prime power, and \( \mathbb{F}_q \) the finite field with \( q \)
elements. We also work with a fixed positive integer \( n \). For \( s \in \mathbb{N}_{\geq 1} \), we denote by \([s]\) the set
\( \{1, 2, \ldots, s\} \). If \( \mathbb{F} \) is a field, the components of a vector \( v \in \mathbb{F}^s \) are \( v_1, \ldots, v_s \in \mathbb{F} \). The vector
space of matrices of size \( t \times s \) over the field \( \mathbb{F} \) is \( \text{Mat}(t \times s, \mathbb{F}) \), and if \( M \in \text{Mat}(t \times s, \mathbb{F}) \) we
denote by \( \text{rowsp}(M) \) the vector space generated over \( \mathbb{F} \) by the rows of \( M \). If we work with a
field extension \( K \supseteq \mathbb{F} \), to avoid confusion we may also write \( \text{rowsp}_K(M) \) for the subspace of
\( K^s \) generated over \( K \) by the rows of \( M \). The rank of a matrix \( M \) is \( \text{rk}(M) \), while \( M^t \) denotes
the transpose of \( M \). The trace of a square matrix \( M \) is \( \text{Tr}(M) \).

The following definition is well-known, but we include it for completeness.

Definition 2. Let \( s, t \) be positive integers, and let \( \mathbb{F} \) be a field. A matrix \( M \in \text{Mat}(t \times s, \mathbb{F}) \)
is said to be in \textbf{row-reduced echelon form} if the following properties hold.

1. Each row of \( M \) has more initial zeros than the previous rows.
2. The first non-zero entry of any non-zero row of \( M \) (called the \textbf{pivot entry} of the row) equals 1, and it is also the only non-zero entry in its column.

The columns on \( M \) that contain a pivot entry are called the \textbf{pivot columns} of \( M \). Notice
that each pivot column contains only one non-zero entry, and such entry equals 1.

Remark 3. It is well-known that any matrix can be put in row-reduced echelon form by
performing elementary operations on the rows. Moreover, the row-reduced echelon form of a
matrix is unique. As a consequence, given a field \( \mathbb{F} \), an integer \( s \geq 1 \) and a subspace \( V \subseteq \mathbb{F}^s \)
of dimension \( 1 \leq t \leq s \), there exists a unique matrix \( M \in \text{Mat}(t \times s, \mathbb{F}) \) in row-reduced echelon
form such that \( \text{rowsp}(M) = V \).

Notation 4. We denote the matrix \( M \) of Remark 3 by \( \text{RRE}(V) \).

Definition 5. A \textbf{linear code} \( C \) of length \( n \) and dimension \( t \) over \( \mathbb{F}_q \) is a \( t \)-dimensional \( \mathbb{F}_q \)
-vector subspace \( C \subseteq \mathbb{F}_q^n \). The \textbf{(Hamming) weight} of a vector \( v \in \mathbb{F}_q^n \) is defined as \( \text{wt}(v) := |\{i \in [n] : v_i \neq 0\}| \). The \textbf{minimum weight} of a non-zero code \( C \) is \( \text{minwt}(C) := \min\{\text{wt}(c) : c \in C, c \neq 0\} \), and the \textbf{maximum weight} of any code \( C \) is \( \text{maxwt}(C) := \max\{\text{wt}(c) : c \in C\} \).
The support of a subspace \( D \subseteq \mathbb{F}_q^n \) is defined as \( \chi(D) := \{ i \in [n] : \exists d \in D \text{ with } d_i \neq 0 \} \). Given a \( t \)-dimensional non-zero code \( C \subseteq \mathbb{F}_q^n \) and an integer \( 1 \leq r \leq t \), the \( r \)-th generalized Hamming weight of \( C \) is

\[
d_r(C) := \min\{ |\chi(D)| : D \subseteq C, \dim_{\mathbb{F}_q}(D) = r \}.
\]

**Remark 6.** In [13] Wei proved that generalized Hamming weights characterize the worst-case security drops of a linear code employed in the coding scheme for wiretap channels proposed in [8]. See [13], Corollary A, for a precise statement.

The main properties of generalized Hamming weights are summarized in the following result.

**Theorem 7** (see [13]). Let \( C \subseteq \mathbb{F}_q^n \) be a non-zero linear code of dimension \( 1 \leq t \leq n \) over \( \mathbb{F}_q \). The following facts hold.

1. \( d_1(C) = \min\{\text{wt}(c) \colon c \in C, c \neq 0\} \).
2. \( d_1(C) \leq n \).
3. For any \( 1 \leq r \leq t - 1 \) we have \( d_r(C) < d_{r+1}(C) \).
4. For any \( 1 \leq r \leq t \) we have \( d_r(C) \leq n - t + r \).

**Remark 8.** Property (1) of Theorem 7 motivates the name generalized Hamming weights. Property (3) is called monotonicity, and property (4) easily follows from (2) and (3).

Now we introduce Gabidulin rank-metric codes.

**Notation 9.** In the sequel we work with fixed positive integers \( k \) and \( m \) with \( k \leq m \).

**Definition 10.** A Gabidulin (rank-metric) code \( C \) of length \( k \) and dimension \( t \) over \( \mathbb{F}_q^m \) is a \( t \)-dimensional \( \mathbb{F}_q^m \)-vector subspace \( C \subseteq \mathbb{F}_q^k \). The rank of a vector \( v \in \mathbb{F}_q^k \) is denoted and defined by \( \text{rk}(v) := \min\{ \text{dim}_{\mathbb{F}_q}(\text{Span}_{\mathbb{F}_q}\{v_1, \ldots, v_k\}) \} \). The minimum rank of a non-zero Gabidulin code \( C \subseteq \mathbb{F}_q^m \) is \( \text{minrk}(C) := \min\{ \text{rk}(c) : c \in C, c \neq 0 \} \), and the maximum rank of any Gabidulin code \( C \) is \( \text{maxrk}(C) := \max\{ \text{rk}(c) : c \in C \} \).

**Definition 11.** Given a vector \( v = (v_1, \ldots, v_k) \in \mathbb{F}_q^m \), define \( v^q := (v_1^q, \ldots, v_k^q) \in \mathbb{F}_q^m \). A subspace \( V \subseteq \mathbb{F}_q^k \) is said to be Frobenius-closed if \( v^q \in V \) whenever \( v \in V \).

**Notation 12.** We denote by \( \Lambda_q(k, m) \) the set of Frobenius-closed spaces \( V \subseteq \mathbb{F}_q^k \).

**Definition 13.** Let \( C \subseteq \mathbb{F}_q^m \) be a non-zero Gabidulin code of dimension \( t \). For any integer \( 1 \leq r \leq t \), the \( r \)-th generalized rank weight of \( C \) is defined as

\[
m_r(C) := \min\{ \dim_{\mathbb{F}_q}(V) : V \in \Lambda_q(k, m), \dim_{\mathbb{F}_q}(V \cap C) \geq r \}.
\]

**Remark 14.** In [12], Silva and Kschischang proposed a coding scheme to secure a network communication against an eavesdropper based on Gabidulin rank-metric codes. The generalized rank weights of Definition [13] were introduced by Kurihara, Matsumoto and Uyematsu in [6] to measure the performance of a Gabidulin code when employed in the cited scheme.
Remark 15. In [7] Oggier and Sboui proposed a different definition of generalized rank weights for Gabidulin codes which we briefly describe. Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_{q^m}^k$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$. Given an integer $1 \leq r \leq t$, the $r$-th Oggier-Sboui generalized weight of $C$ is denoted and defined by

$$m'_r(C) := \min\{ \max \text{rk}(D) : D \subseteq C, \dim_{\mathbb{F}_{q^m}}(D) = r \}.$$ 

In [2] Ducoat showed how Oggier-Sboui generalized weights relate to the generalized rank weights proposed by Kurihara, Matsumoto and Uyematsu in [6]. We will comment again on this alternative definition of generalized weights for Gabidulin codes in the sequel (see Remark 50 and Remark 82).

In analogy with generalized Hamming weights, the main properties of generalized rank weights are summarized in the following result.

**Theorem 16** (see [6]). Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_{q^m}^n$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_{q^m}$. The following facts hold.

1. $m_1(C) = \min \text{rk}(C)$.
2. $m_t(C) \leq k$.
3. For any $1 \leq r \leq t - 1$ we have $m_r(C) < m_{r+1}(C)$.
4. For any $1 \leq r \leq t$ we have $m_r(C) \leq k - t + r$.

**Remark 17.** Property (1) of Theorem 16 motivates the name generalized rank weights. See also [2] for a different proof of property (3).

## 2 Generalized Hamming weights and anticodes

In this section we characterize the generalized Hamming weights of a linear code $C$ in terms of the intersections of $C$ with optimal anticodes in the Hamming metric.

**Proposition 18.** Let $C \subseteq \mathbb{F}_q^n$ be a linear code. We have $\dim_{\mathbb{F}_q}(C) \leq \max \text{wt}(C)$.

**Proof.** If $C = 0$ then the result is trivial. Assume $t := \dim_{\mathbb{F}_q}(C) \geq 1$, and let $M := \text{RRE}(C)$. By Definition 2 the sum of the rows of $M$ is an element of $C$ with Hamming weight at least $t$. Hence we have $\max \text{rk}(C) \geq t = \dim_{\mathbb{F}_q}(C)$. \hfill $\square$

**Definition 19.** A code $C \subseteq \mathbb{F}_q^n$ attending the bound of Proposition 18 is said to be an optimal linear anticode. We denote the set of optimal linear anticodes in $\mathbb{F}_q^n$ by $A_{\text{H}}^n(\mathbb{F}_q)$.

**Definition 20.** Let $S \subseteq [n]$ be a subset. The free code over $\mathbb{F}_q$ of length $n$ supported by $S$ is denoted and defined by $C_q(n,S) := \{ v \in \mathbb{F}_q^n : v_i = 0 \text{ for all } i \in [n] \setminus S \}$.

**Remark 21.** Any free code $C_q(n,S)$ satisfies $\dim_{\mathbb{F}_q}(C_q(n,S)) = \max \text{wt}(C_q(n,S)) = |S|$. In particular, free codes are optimal linear anticodes.

In the following Proposition 23 we show that for $q \geq 3$ all optimal linear anticodes are free codes. We will give a counterexample for the case $q = 2$ in Remark 25.
Lemma 22. Assume \( q \geq 3 \). Let \( t \geq 1 \) be an integer, and let \( c_1, \ldots, c_t \in \mathbb{F}_q \) be not all zero. There exist \( a_1, \ldots, a_t \in \mathbb{F}_q \setminus \{0\} \) such that \( \sum_{i=1}^t a_ic_i \neq 0 \).

Proof. Choose \( b_1, \ldots, b_t \in \mathbb{F}_q \setminus \{0\} \). If \( \sum_{i=1}^t b_ic_i \neq 0 \) then we may take \( a_i = b_i \) for \( i \in [t] \). Assume \( \sum_{i=1}^t b_ic_i = 0 \). By hypothesis, there exists \( j \in [t] \) such that \( c_j \neq 0 \). Let \( b \in \mathbb{F}_q \setminus \{0, 1\} \). Define \( a_j := bb_j \), and \( a_i := b_i \) for \( i \in [t] \setminus \{j\} \). Since \( b \neq 0 \) we have \( a_i \neq 0 \) for all \( i \in [t] \).

Moreover,

\[
\sum_{i=1}^t a_i c_i = bb_j c_j + \sum_{i \neq j} b_i c_i = b_j c_j + (b - 1) b_j c_j + \sum_{i \neq j} b_i c_i = \sum_{i = 1}^t b_i c_i + (b - 1) b_j c_j = (b - 1) b_j c_j.
\]

Since \( b \neq 1 \), \( b_j \neq 0 \) and \( c_j \neq 0 \) we have \( (b - 1) b_j c_j \neq 0 \). \( \square \)

Proposition 23. Assume \( q \geq 3 \). Let \( C \subseteq \mathbb{F}_q^n \) be a linear code of dimension \( t \). The following facts are equivalent.

1. \( C \in \mathcal{A}_q^H(n) \).
2. \( C = C_q(n, S) \) for some \( S \subseteq [n] \) with \( |S| = t \).

Proof. If \( t = 0 \) or \( t = n \) then the result is trivial. Hence we assume \( 0 < t < n \). Part (2) \( \Rightarrow \) (1) follows from Remark 21. Let us prove (1) \( \Rightarrow \) (2). If \( C \) is an optimal anticode, then we have \( t = \text{maxwt}(C) \). Define \( M := \text{RRE}(C) \). We will prove that any non-pivot column of \( M \) is zero. By contradiction, let \( j \in [n] \) be the index of a non-zero non-pivot column of \( M \), and let \( c_1^j, \ldots, c_t^j \) be the entries of such column. By Lemma 22 there exist \( a_1, \ldots, a_t \in \mathbb{F}_q \setminus \{0\} \) with \( \sum_{i=1}^t a_i c_i^j \neq 0 \). Hence, denoted by \( M_1, \ldots, M_t \in \mathbb{F}_q^n \) the rows of \( M \), we have that \( \sum_{i=1}^t a_i M_i \in C \) has Hamming weight at least \( t + 1 \), a contradiction. It follows \( c_i^j = 0 \) for all \( i \in [t] \). Hence we proved \( C \subseteq C_q(n, S) \), where \( S \subseteq [n] \) is the set of pivot columns of \( M \). In particular, \( |S| = t \). Since \( \dim_{\mathbb{F}_q}(C_q(n, S)) = |S| = t = \dim_{\mathbb{F}_q}(C) \), we have \( C = C_q(n, S) \). \( \square \)

Proposition 23 allows us to characterize the generalized Hamming weights of a linear code in terms of optimal anticodes.

Theorem 24. Assume \( q \geq 3 \). Let \( C \subseteq \mathbb{F}_q^n \) be a non-zero linear code of dimension \( 1 \leq t \leq n \) over \( \mathbb{F}_q \). For any integer \( 1 \leq r \leq t \) we have

\[
d_r(C) = \min \{ \dim_{\mathbb{F}_q}(A) : A \in \mathcal{A}_q^H(n), \dim_{\mathbb{F}_q}(A \cap C) \geq r \}.
\]

Proof. Fix \( 1 \leq r \leq t \). Define \( d_r' := \min \{ \dim_{\mathbb{F}_q}(A) : A \in \mathcal{A}_q^H(n), \dim_{\mathbb{F}_q}(A \cap C) \geq r \} \). Let \( A \in \mathcal{A}_q^H(n) \) with \( \dim_{\mathbb{F}_q}(A) = d_r'(C) \) and \( \dim_{\mathbb{F}_q}(A \cap C) \geq r \). By Proposition 23 \( A = C_q(n, S) \) for some \( S \subseteq [n] \) with \( |S| = \dim_{\mathbb{F}_q}(A) \). Let \( D \) be an \( r \)-dimensional subspace of \( A \cap C \). We have \( \chi(D) \subseteq \chi(A \cap C) \subseteq \chi(A) = \chi(C_q(n, S)) = S \), and so \( |\chi(D)| \leq |S| = \dim_{\mathbb{F}_q}(A) \). This proves \( d_r(C) \leq d_r'(C) \). Now we prove \( d_r'(C) \leq d_r(C) \). Let \( D \subseteq C \) with \( \dim_{\mathbb{F}_q}(D) = r \). Define \( A := C_q(n, \chi(D)) \). Since \( A \supseteq D \) and \( D \subseteq C \), we have \( \dim_{\mathbb{F}_q}(A \cap C) \geq \dim_{\mathbb{F}_q}(D \cap C) = \dim_{\mathbb{F}_q}(D) = r \). Moreover, \( \dim_{\mathbb{F}_q}(A) = |\chi(D)| = d_r(C) \), and so \( d_r'(C) \leq d_r(C) \), as claimed. \( \square \)
Remark 25. Theorem 24 and Proposition 23 do not hold in general when \( q = 2 \). Let e.g. \( n = 3 \), and take as \( C \) the linear code generated over \( \mathbb{F}_2 \) by \((1, 0, 1)\) and \((0, 1, 1)\). We have \( d_2(C) = |\chi(C)| = 3 \). On the other side, \( C \) is an optimal linear anticode of maximum weight 2, even if it is not of the form \( C_2(3, S) \) for some \( S \subseteq [n] \) with \(|S| = 2\). As a consequence, following the notation of the proof of Theorem 24, we have \( d'_2(C) = \dim_{\mathbb{F}_q}(C) = 2 \neq d_2(C) \).

Remark 26. It is well-known that the codes that give maximum information-theoretic security in the scheme of [8] are MDS codes. A linear MDS code \( C \subseteq \mathbb{F}_q^n \) is a non-zero linear code for which \( \minwt(C) = n - \dim_{\mathbb{F}_q}(C) + 1 \). It is easy to see that a non-zero code \( C \subseteq \mathbb{F}_q^n \) is MDS if and only if \( A \cap C = 0 \) for all optimal anticodes \( A \subseteq \mathbb{F}_q^n \) with \( \dim_{\mathbb{F}_q}(A) = \minwt(C) - 1 \). Theorem 24 says that the generalized Hamming weights of a code \( C \) may be interpreted as a measure of how far the code \( C \) is from being an MDS code.

Now we investigate optimal anticodes, Frobenius-closed spaces and generalized weights in the rank metric.

3 Generalized rank weights and anticodes

In this section we prove the analogue of Theorem 24 for Gabidulin codes. In this case we will not need to assume \( q \geq 3 \).

Proposition 27. Let \( 1 \leq k \leq m \) be integers, and let \( C \subseteq \mathbb{F}_q^m \) be Gabidulin code. We have \( \dim_{\mathbb{F}_q}(C) \leq \maxrk(C) \).

Proof. If \( C = 0 \) then the result is trivial. Assume \( t := \dim_{\mathbb{F}_q}(C) \geq 1 \) and define \( M := \text{RRE}(C) \in \text{Mat}(t \times k, \mathbb{F}_q^m) \). Let \( \alpha_1, \ldots, \alpha_t \in \mathbb{F}_q^m \) be independent over \( \mathbb{F}_q \), and denote by \( M_1, \ldots, M_t \) the rows of \( M \). Then \( \sum_{i=1}^t \alpha_i M_i \in C \) has \( \alpha_1, \ldots, \alpha_t \) among its components. In particular, \( \text{rk}(\sum_{i=1}^t \alpha_i M_i) \geq t \), and the thesis follows.

Definition 28. A Gabidulin code \( C \subseteq \mathbb{F}_q^m \) attaining the bound of Proposition 27 is said to be an optimal Gabidulin anticode. We denote the set of optimal Gabidulin anticodes in \( \mathbb{F}_q^m \) by \( \mathcal{A}_q(G/k,m) \).

We need a series of preliminary results.

Theorem 29 ([4], Theorem 1). Let \( V \subseteq \mathbb{F}_q^m \) be a non-zero subspace. Then \( V \in \Lambda_q(k,m) \) if and only if it has a basis over \( \mathbb{F}_q^m \) made of vectors with entries in \( \mathbb{F}_q \) (in short, defined over \( \mathbb{F}_q \)).

Theorem 29 has the following useful consequence.

Corollary 30. Let \( 1 \leq k \leq m \) be integers. Let \( V \subseteq \mathbb{F}_q^m \) be a non-zero subspace. The following facts are equivalent.

1. \( V \in \Lambda_q(k,m) \),
2. \( \text{RRE}(V) \) is a matrix with entries in \( \mathbb{F}_q \).

7
Proof. Part (2) ⇒ (1) is trivial. In order to prove (1) ⇒ (2), let \( v_1, \ldots, v_t \) be a basis of \( V \) defined over \( F_q \), where \( t := \dim_{\mathbb{F}_q^m}(V) \). Let \( M \) be the matrix having \( v_1, \ldots, v_t \) as rows. The row-reduced echelon form of \( M \), say \( \overline{M} \), can be obtained from \( M \) by elementary row operations over \( \mathbb{F}_q \). Hence \( \overline{M} \) has entries in \( \mathbb{F}_q \). Since \( \text{rows} \mathbb{F}_q^m(M) = \text{rows} \mathbb{F}_q^m(M) = V \), we have \( \overline{M} = \text{RRE}(V) \) by the uniqueness of the row-reduced echelon form (Remark 3).

Remark 31. Corollary 30 provides in particular an efficient way to compute a basis defined over \( \mathbb{F}_q \) of a Frobenius-closed space \( V \subseteq \mathbb{F}_q^m \) of given dimension \( 1 \leq t \leq k \). Indeed, it suffices to take any basis \( \{v_1, \ldots, v_t\} \subseteq \mathbb{F}_q^m \) of \( V \), construct the matrix \( M \) having \( v_1, \ldots, v_t \) as rows, and compute the row-reduced echelon form, say \( \overline{M} \), of \( M \). The rows of \( \overline{M} \) will automatically be a basis of \( V \) defined over \( \mathbb{F}_q \). The result may also be interpreted as an efficient test to check if a given subspace \( V \) is Frobenius-closed.

Example 32. Let \( q = 2 \) and \( k = m = 4 \). Write \( \mathbb{F}_{2^4} = \mathbb{F}_2[\xi] \), where \( \xi \) satisfies \( \xi^4 + \xi + 1 = 0 \). Consider the space \( V \subseteq \mathbb{F}_2^4 \) generated by the two vectors \((\xi, \xi^2, \xi^5, \xi)\) and \((\xi^2, \xi^4, \xi^10, \xi^2)\). One can check that \( V \) is Frobenius-closed. Following the notation of Remark 31 we have

\[
M = \begin{bmatrix}
\xi & \xi^2 & \xi^5 & \xi \\
\xi^2 & \xi^4 & \xi^{10} & \xi^2
\end{bmatrix}, \quad \overline{M} = \begin{bmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 1 & 0
\end{bmatrix}.
\]

We see that \( \overline{M} \) has entries in \( \mathbb{F}_2 \). Hence \( \{(1,0,1,1), (0,1,1,0)\} \) is a basis of \( V \) defined over \( \mathbb{F}_2 \).

Lemma 33. Let \( H \subseteq \mathbb{F}_q^m \) be an \( \mathbb{F}_q \)-subspace of dimension \( h \) over \( \mathbb{F}_q \), with \( 1 \leq h \leq m - 2 \). Let \( x \in \mathbb{F}_q^m \setminus H \), and \( y \in \mathbb{F}_q^m \). There exists \( \alpha \in \mathbb{F}_q^m \setminus H \) such that \( x + \alpha y \notin H \oplus \langle \alpha \rangle \), where \( \langle \alpha \rangle \subseteq \mathbb{F}_q^m \) denotes the space generated by \( \alpha \) over \( \mathbb{F}_q \).

Proof. Define \( U := \{a \in \mathbb{F}_q : a \neq y\} \) and \( U := \{\alpha \in \mathbb{F}_q^m : \exists v \in H, a \in U : \alpha = (v - x)/(y - a)\} \). We claim that \( x + \alpha y \in H \oplus \langle \alpha \rangle \) if and only if \( \alpha \in U \). Indeed, if \( \alpha \in U \) then \( \alpha = (v - x)/(y - a) \) for some \( v \in H \) and \( a \in U \subseteq \mathbb{F}_q \). Hence \( \alpha(y - a) = v - x \), and so \( x + \alpha y = v + a \alpha \in H \oplus \langle \alpha \rangle \). Vice versa, if \( x + \alpha y \in H \oplus \langle \alpha \rangle \) then there exist \( v \in H \) and \( a \in \mathbb{F}_q \) with \( x + \alpha y = v + a \alpha \). If \( a = y \) then \( x = v \in H \), a contradiction. It follows \( a \in U \), and \( \alpha = (v - x)/(y - a) \).

We clearly have \( |U| \leq |H| \cdot |U| \leq q^h q = q^{h+1} \). Hence \( |\mathbb{F}_q^m \setminus U| \geq q^m - q^{h+1} \). Since \( m - h \geq 2 \) by hypothesis, we have

\[
q^{m-h} - q \geq q^2 - q > 1.
\]

Multiplying both members of this inequality by \( q^h \) we obtain \( q^m - q^{h+1} > q^h \). Hence we have \( |\mathbb{F}_q^m \setminus U| \geq q^m - q^{h+1} > q^h \). Since \( |H| = q^h \), there exists \( \alpha \in (\mathbb{F}_q^m \setminus U) \setminus H \). Since \( \alpha \notin U \) we have \( x + \alpha y \notin H \oplus \langle \alpha \rangle \) by the claim above.

Notation 34. Let \( t \) and \( s \) be positive integers, \( \mathbb{F} \) a field, and \( \pi : [t] \to [t] \) a permutation. Let \( M \in \text{Mat}(t \times m, \mathbb{F}) \) be a matrix, and let \( M_1, \ldots, M_t \) the rows of \( M \). We denote by \( \pi(M) \) the matrix whose rows are \( M_{\pi(1)}, \ldots, M_{\pi(t)} \).

Definition 35. Let \( t \) and \( s \) be positive integers, and \( \mathbb{F} \) a field. A matrix \( M \in \text{Mat}(t \times s, \mathbb{F}) \) is said to be **almost** in row-reduced echelon form if \( \pi(M) \) is in row-reduced echelon form for some permutation \( \pi : [t] \to [t] \).
Proposition 36. Let $1 \leq t < k \leq m$ be integers, and let $M \in \text{Mat}(t \times k, \mathbb{F}_q^m)$ be a full-rank matrix almost in row-reduced echelon form. Denote by $M_1,...,M_t$ the rows of $M$. Assume that $M_1$ has at least one entry in $\mathbb{F}_q^m \setminus \mathbb{F}_q$. There exist $\mathbb{F}_q$-linearly independent elements $\alpha_1,...,\alpha_t \in \mathbb{F}_q^m$ such that $\text{rank}(\sum_{i=1}^t \alpha_iM_i) \geq t+1$.

Proof. We will prove the result by induction on $1 \leq t < k$. If $t = 1$ then $M$ has only one row, $M_1 \in \mathbb{F}_q^k$. Such row has among its components 1 and an element $M_{ij} \notin \mathbb{F}_q$. In particular, $M_1$ has rank at least 2. Hence we may take $\alpha_1 := 1$ and conclude the proof. Assume that the thesis is true for all non-negative integers smaller than $t$. Denote by $M' \in \text{Mat}(t-1,k,\mathbb{F}_q^m)$ the matrix obtained from $M$ deleting the last row. It is easy to see that $M'$ has full-rank and it is almost in row-reduced echelon form. By induction hypothesis, there exist $\alpha_1,...,\alpha_{t-1} \in \mathbb{F}_q^m$ independent over $\mathbb{F}_q$ such that $\text{rank}(\sum_{i=1}^{t-1} \alpha_iM_i) \geq t$. Since $M'$ is almost in row-reduced echelon form, the vector $\sum_{i=1}^{t-1} \alpha_iM_i$ has $\alpha_1,...,\alpha_{t-1}$ among its components. Hence there exists $j \in [k]$ with $\sum_{i=1}^{t-1} \alpha_iM_{ij} \notin \langle \alpha_1,...,\alpha_{t-1} \rangle$. Apply Lemma 33 with $H = \langle \alpha_1,...,\alpha_{t-1} \rangle$, $x = \sum_{i=1}^{t-1} \alpha_iM_{ij}$ and $y = M_{ij}$. We obtain $\alpha_t \in \mathbb{F}_q^m \setminus \langle \alpha_1,...,\alpha_{t-1} \rangle$ with $\sum_{i=1}^{t-1} \alpha_iM_{ij} + \alpha_t M_{ij} = \sum_{i=1}^{t} \alpha_iM_{ij} \notin \langle \alpha_1,...,\alpha_t \rangle$. It is easy to see that $\sum_{i=1}^{t} \alpha_iM_{ij}$ has rank at least $t+1$. \hfill \Box

Theorem 37. Let $1 \leq k \leq m$ be integers. We have $\Lambda_q(k, m) = \mathcal{A}_q^G(k, m)$.

Proof. Let $V \in \Lambda_q(k, m)$. Denote by $t$ the dimension of $V$ over $\mathbb{F}_q^m$. If $t = 0$ then clearly $V \in \mathcal{A}_q^G(k, m)$. Now assume $1 \leq t \leq k$. By Theorem 29 there exists a basis $\{v_1,...,v_t\}$ of $V$ defined over $\mathbb{F}_q$. Take any $v \in V$. There exist $\alpha_1,...,\alpha_t \in \mathbb{F}_q^m$ with $v = \sum_{i=1}^t \alpha_i v_i$. The space generated over $\mathbb{F}_q$ by the components of $v$ is contained in $\text{Span}_q \{\alpha_1,...,\alpha_t\}$. In particular we have $\text{rk}(v) \leq t$. Since $v \in V$ is arbitrary, this proves $\text{maxrk}(V) \leq t$. By Proposition 27 we have $\text{maxrk}(V) = t = \dim_{\mathbb{F}_q^m}(V)$, and so $V$ is an optimal Gabidulin anticode, i.e., $V \in \mathcal{A}_q^G(k, m)$. Now we prove $\mathcal{A}_q^G(k, m) \subseteq \Lambda_q(k, m)$. Let $A \in \mathcal{A}_q^G(k, m)$. Denote by $t$ the dimension of $A$ over $\mathbb{F}_q^m$. If $t = 0$ or $t = k$ then trivially $A \in \Lambda_q(k, m)$. Now assume $1 \leq t < k$, and set $M := \text{RRE}(A)$. By Corollary 30 it suffices to prove that $M$ has entries in $\mathbb{F}_q$. By contradiction, assume that $M$ has one entry, say $M_{ij}$, in $\mathbb{F}_q^m \setminus \mathbb{F}_q$. Exchanging the first and the $i$-th row of $M$ we obtain a new matrix, say $N$, almost in row-reduced echelon form and such that $\text{rowsp}_{\mathbb{F}_q^m}(N) = \text{rowsp}_{\mathbb{F}_q^m}(M) = A$. By Proposition 36 there exists $v \in \text{rowsp}_{\mathbb{F}_q^m}(N) = A$ with $\text{rk}(v) \geq t+1$. This contradicts the fact that $A$ is an optimal anticode of dimension $t$. \hfill \Box

Remark 38. Theorem 37 says in particular that the algebraic condition of being a Frobenius-closed space may be regarded as a metric condition.

The following corollary immediately follows from Definition 13 and Theorem 37.

Corollary 39. Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_q^m$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_q^m$. For any integer $1 \leq r \leq t$ we have

$$m_t(C) = \min \{ \dim_{\mathbb{F}_q^m}(A) : A \in \mathcal{A}_q^G(k, m), \dim_{\mathbb{F}_q^m}(A \cap C) \geq r \}.$$ 

Remark 40. Corollary 39 may be regarded as the analogue of Theorem 24 for Gabidulin codes. We notice that there is a formal perfect analogy between the two results.
4 Delsarte rank-metric codes

In [1] Delsarte proposed to define rank-metric codes as linear spaces of matrices over a finite field. In this section we briefly recall the main concepts of the theory of Delsarte rank-metric codes, and show how one can associate to a Gabidulin code a Delsarte code with the same metric properties.

Definition 41. A Delsarte (rank-metric) code of size $k \times m$ over $\mathbb{F}_q$ is defined to be a vector subspace $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$. The minimum rank of a non-zero code $C$ is denoted and defined by $\text{minrk}(C) := \min \{ \text{rk}(M) : M \in C, \text{rk}(M) > 0 \}$, while the maximum rank of any code $C$ is denoted and defined by $\text{maxrk}(C) := \max \{ \text{rk}(M) : M \in C \}$.

Theorem 42 ([1], Theorem 5.4). Let $1 \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a non-zero Delsarte code. We have

$$\dim_{\mathbb{F}_q}(C) \leq m(k - \text{minrk}(C) + 1).$$

Moreover, for any $1 \leq d \leq k$ there exists a non-zero code $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ of minimum rank $d$ which attains the upper bound.

Definition 43. A non-zero code attaining the bound of Theorem 42 is said to be a Delsarte optimal code.

In analogy with Proposition 18 and Proposition 27 we have the following bound.

Proposition 44 ([9], Proposition 43). Let $1 \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a Delsarte code. We have

$$\dim_{\mathbb{F}_q}(C) \leq m \cdot \text{maxrk}(C).$$

Definition 45. A code $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ which attains the upper bound of Proposition 44 is said to be a Delsarte optimal anticode. We denote by $A^D_q(k, m)$ the set of Delsarte optimal anticodes in $\text{Mat}(k \times m, \mathbb{F}_q)$.

Writing the components of a vector $v \in \mathbb{F}_q^k$ over a basis $G$ of $\mathbb{F}_q^m$ over $\mathbb{F}_q$, one can naturally associate to a Gabidulin code a Delsarte code with the same metric properties.

Definition 46. Let $G = \{ \gamma_1, ..., \gamma_m \}$ be a basis of $\mathbb{F}_q^m$ over $\mathbb{F}_q$. The matrix associated to a vector $v \in \mathbb{F}_q^k$ with respect to $G$ is the $k \times m$ matrix $M_G(v)$ with entries in $\mathbb{F}_q$ defined by $v_i = \sum_{j=1}^m M_G(v)_{ij} \gamma_j$ for all $i \in [k]$. The Delsarte code associated to a Gabidulin code $C \subseteq \mathbb{F}_q^m$ with respect to the basis $G$ is $C_G(C) := \{ M_G(c) : c \in C \} \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$.

Delsarte codes may be regarded as a generalization of Gabidulin codes. The proof of the following result is straightforward.

Proposition 47. Let $C \subseteq \mathbb{F}_q^m$ be a Gabidulin code. For any basis $G$ of $\mathbb{F}_q^m$ over $\mathbb{F}_q$, $C_G(C) \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ is a Delsarte rank-metric code with

$$\dim_{\mathbb{F}_q} C_G(C) = m \cdot \dim_{\mathbb{F}_q}(C).$$

Moreover, $\text{maxrk}(C) = \text{maxrk}(C_G(C))$, and if $C \neq 0$ we have $\text{minrk}(C) = \text{minrk}(C_G(C))$.

In the following two sections we propose a new invariant for Delsarte codes, show how it relates to the generalized rank weights of Gabidulin codes, and establish the analogue of Theorem 7 and Theorem 16 for Delsarte codes and Delsarte generalized weights.
5 An algebraic invariant for Delsarte codes

Our goal is to define an invariant for Delsarte codes in analogy with the generalized Hamming weights for linear codes and with the generalized rank weights for Gabidulin codes. Inspired by Theorem 24 and Corollary 39, we propose the following definition.

**Definition 48.** Let $1 \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a non-zero Delsarte code of dimension $1 \leq t \leq km$ over $\mathbb{F}_q$. For $1 \leq r \leq t$, the $r$-th Delsarte generalized weight of $C$ is denoted and defined by

$$a_r(C) := \frac{1}{m} \min \{ \dim_{\mathbb{F}_q}(A) : A \in \mathcal{A}_q^D(k, m), \ \dim_{\mathbb{F}_q}(A \cap C) \geq r \}.$$ 

**Remark 49.** By Definition 45, the dimension over $\mathbb{F}_q$ of any anticode $A \in \mathcal{A}_q^D(k, m)$ is a multiple of $m$. Hence Delsarte generalized weights are positive integers.

**Remark 50.** One may also define generalized weights for Delsarte codes in analogy with the definition of the generalized rank weights by Oggier and Sboui presented in Remark 15. Given integers $1 \leq k \leq m$, a Delsarte code $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ of dimension $1 \leq t \leq km$ and an integer $1 \leq r \leq t$, define the $r$-th Oggier-Sboui generalized weight of $C$ as

$$a'_r(C) := \{ \max \text{rk}(D) : D \subseteq C, \ \dim_{\mathbb{F}_q}(D) = r \}.$$ 

It can be proved that we always have $a'_r(C) \leq a_r(C)$, and equality does not hold in general, as we show in the following example. The reason why in this work we focus on the $a_r(C)$'s instead of on the $a'_r(C)$'s will be clear in Section 7. See in particular Remark 82.

**Example 51.** Let $q = 2$, $k = 2$ and $m = 3$. Denote by $C \subseteq \text{Mat}(2 \times 3, \mathbb{F}_2)$ the Delsarte code generated by the three $\mathbb{F}_q$-independent matrices

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad B := \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad C := \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$ 

The 2-dimensional subcode $D \subseteq C$ generated by $A$ and $C$ has $\max \text{rk}(D) = 1$. Hence $a'_2(C) = 1$. On the other side, it can be checked that there is no Delsarte optimal anticode $A \in \mathcal{A}_2^D(2, 3)$ with $\dim_{\mathbb{F}_q}(A) = 3$ and $\dim_{\mathbb{F}_q}(A \cap C) \geq 2$. It follows $a_2(C) = 6/3 = 2 \neq a'_2(C)$.

Before describing the properties of Delsarte generalized weights, it is natural to ask how the new invariant relates to the generalized rank weights for Gabidulin codes proposed by Kurihara, Matsumoto and Uyematsu. Indeed, since Delsarte codes generalize Gabidulin codes, one would expect that Delsarte generalized weights recover generalized rank weights. And this is the first fact that we establish. We start introducing some rank-preserving transformations.

**Definition 52.** Given a Gabidulin code $C \subseteq \mathbb{F}_q^{k \times m}$, a Delsarte code $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ and matrices $A \in \text{Mat}(k \times k, \mathbb{F}_q)$, $B \in \text{Mat}(m \times m, \mathbb{F}_q)$, we define:

1. $CA := \{ cA : c \in C \}$,
2. $AC := \{ AM : M \in C \}$,
3. $CB := \{ MB : M \in C \}$.
Remark 53. It is easy to see that if $A$ and $B$ are invertible matrices, then the multiplication maps introduced in Definition 52 are rank-preserving isomorphisms of Gabidulin and Delsarte codes. In particular, they preserve optimal anticodes in the respective metrics, generalized rank weights and Delsarte generalized weights.

Definition 54. Let $k \geq 1$ be an integer, and let $C \subseteq \text{Mat}(k \times k, \mathbb{F}_q)$ be a Delsarte code. The transpose code of $C$ is the Delsarte code defined by $C^t := \{M^t : M \in C \} \subseteq \text{Mat}(k \times k, \mathbb{F}_q)$.

Lemma 55. Let $k \geq 1$ be an integer, and let $C \subseteq \text{Mat}(k \times k, \mathbb{F}_q)$ be a non-zero Delsarte code. Then $C$ and $C^\perp$ have the same Delsarte generalized weights.

Proof. The transposition of matrices $\tau : \text{Mat}(k \times k, \mathbb{F}_q) \rightarrow \text{Mat}(k \times k, \mathbb{F}_q)$ is a rank-preserving isomorphism such that $\tau^{-1} = \tau$. In particular, it preserves optimal anticodes and Delsarte generalized weights. The lemma easily follows. □

Definition 56. Let $1 \leq k \leq m$ and $0 \leq R \leq k$ be integers. The standard Delsarte optimal anticode $S_q(m, k, R)$ of maximum rank $R$ is the vector space of $k \times m$ matrices over $\mathbb{F}_q$ whose last $k - R$ rows equal zero.

Remark 57. It is easy to check that the standard code $S_q(m, k, R)$ of Definition 45 is a Delsarte optimal anticode of maximum rank $R$.

The following result shows that, up to certain rank-preserving transformations, all Delsarte optimal anticodes are standard anticodes.

Theorem 58 (see [10], Theorem 4 and Theorem 6). Let $1 \leq R \leq k \leq m$ be integers, and let $A \in A_q^D(k, m)$ with $\text{maxrk}(A) = R$.

1. If $k < m$ then there exist invertible matrices $A \in \text{Mat}(k \times k, \mathbb{F}_q)$, $B \in \text{Mat}(m \times m, \mathbb{F}_q)$ such that $AAB = S_q(m, k, R)$.

2. If $k = m$ then there exist invertible matrices $A, B \in \text{Mat}(k \times k, \mathbb{F}_q)$ such that either $AAB = S_q(k, k, R)$, or $AAB = S_q(k, k, R)^t$.

Proof. If $R = 0$ or $R = k$ then the result is trivial. Assume $1 \leq R \leq k - 1$. If $k < m$ then the thesis follows (up to a transposition) from [10], Theorem 6(a). If $k = m$ and $R > 1$ then we may apply [10], Theorem 4(a). Finally, if $k = m$ and $R = 1$ then the thesis follows from [10], Theorem 4(b). □

We will also need the following preliminary results.

Lemma 59. Let $C \subseteq \mathbb{F}_q^k$ be a Gabidulin code, and let $A \in \text{Mat}(k \times k, \mathbb{F}_q)$ be an invertible matrix. For any basis $G$ of $\mathbb{F}_q^m$ over $\mathbb{F}_q$ we have

$$C_G(CA^t) = AC_G(C).$$

In particular, $C_G(C)$ and $C_G(CA^t)$ have the same Delsarte generalized weights.
Proof. Write $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$. Let $v \in \mathbb{F}_q^k$. By Definition 46, for any $i \in [k]$ we have

$$(v \cdot A^t)_i = \sum_{s=1}^k v_s A_{si} = \sum_{s=1}^k M_G(v)_{sj} \gamma_j A_{is} = \sum_{j=1}^m \left( \sum_{s=1}^k A_{is} M_G(v)_{sj} \right) \gamma_j = \sum_{j=1}^m (AM_G(v))_{ij} \gamma_j.$$ 

Hence we have $M_G(vA^t) = AM_G(v)$. The lemma easily follows from Definition 52, the definition of $M_G(CA^t)$, and Remark 53.

Lemma 60. Let $C \subseteq \mathbb{F}_q^k$ be a Gabidulin code, and let $\mathcal{G} = \{\gamma_1, ..., \gamma_m\}$, $\mathcal{F} = \{\varphi_1, ..., \varphi_m\}$ be bases of $\mathbb{F}_q^m$ over $\mathbb{F}_q$. Let $B \in \text{Mat}(m \times m, \mathbb{F}_q)$ be the invertible matrix defined by $\gamma_j = \sum_{s=1}^m B_{js} \varphi_s$ for all $j \in [m]$. We have

$$C_{\mathcal{F}}(C) = C_{\mathcal{G}}(C)B.$$ 

In particular, if $C \neq 0$ then the Delsarte generalized weights of $C_{\mathcal{G}}(C)$ do not depend on the choice of the basis $\mathcal{G}$.

Proof. Let $v \in \mathbb{F}_q^k$. By the definition of $B$ and Definition 46, for any $i \in [k]$ we have

$$v_i = \sum_{j=1}^m M_G(v)_{ij} \gamma_j = \sum_{j=1}^m M_G(v)_{ij} \sum_{s=1}^m B_{js} \varphi_s = \sum_{s=1}^m \left( \sum_{j=1}^m M_G(v)_{ij} B_{js} \right) \varphi_s = \sum_{s=1}^m (M_G(v)B)_{is} \varphi_s.$$ 

This proves $M_{\mathcal{F}}(v) = M_G(v)B$. The lemma now follows from Definition 52, Definition 46 and Remark 53.

The map that sends a Gabidulin code $C$ to the associated Delsarte code $C_{\mathcal{G}}(C)$ with respect to a basis $\mathcal{G}$ is injective. Hence we have the following result.

Lemma 61. Let $C, D \subseteq \mathbb{F}_q^k$ be Gabidulin codes, and let $\mathcal{G}$ be a basis of $\mathbb{F}_q^m$ over $\mathbb{F}_q$. We have $C_{\mathcal{G}}(C \cap D) = C_{\mathcal{G}}(C) \cap C_{\mathcal{G}}(D)$.

Now we prove that Delsarte generalized weights recover generalized rank weights.
Theorem 62. Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_{q}^{k}$ be a non-zero Gabidulin code of dimension $1 \leq t \leq k$. For any basis $G$ of $\mathbb{F}_{q}^{m}$ over $\mathbb{F}_{q}$, for any $1 \leq r \leq t$ and for any $0 \leq \varepsilon \leq m - 1$ we have

$$m_{r}(C) = a_{rm-\varepsilon}(C_{G}(C)).$$

In particular, the Delsarte generalized weights of a code $C$ arising from a Gabidulin code are determined by the Delsarte generalized weights of the form $a_{im}(C), i = 1, \ldots, \dim_{q}(C)/m$.

Proof. Fix $1 \leq r \leq t$ and $0 \leq \varepsilon \leq m - 1$. Let $\overline{A} \in A_{q}^{D}(k, m)$ with $\dim_{q}(\overline{A} \cap C) \geq r$. By Proposition 47 we have $C_{G}(\overline{A}) \subseteq A_{q}^{D}(k, m)$ and $\dim_{q}(C_{G}(\overline{A})) = m \cdot \dim_{q}(\overline{A}) = m \cdot m_{r}(C)$. Hence by Proposition 47 we have $\dim_{q}(C_{G}(\overline{A}) \cap C_{G}(C)) = \dim_{q}(C_{G}(\overline{A} \cap C)) \geq rm \geq rm - \varepsilon$. It follows $a_{rm-\varepsilon}(C_{G}(C)) \leq m_{r}(C)$.

Now we prove $m_{r}(C) \leq a_{rm-\varepsilon}(C_{G}(C))$. Set $C := C_{G}(C)$ to simplify the notation. Let $\overline{A} \in A_{q}^{D}(k, m)$ with $\dim_{q}(\overline{A} \cap C) \geq rm - \varepsilon$ and $a_{rm-\varepsilon}(C) = 1/m \cdot \dim_{q}(\overline{A})$. By Definition 45, $\dim_{q}(\overline{A}) = mR$, where $R = \max \mathbf{rk}(\overline{A})$. Hence we need to prove $m_{r}(C) \leq R$. By Theorem 58 there exist invertible matrices $A \in \text{Mat}(k \times k, \mathbb{F}_{q})$ and $B \in \text{Mat}(m \times m, \mathbb{F}_{q})$ such that either $A \overline{A}B = S_{q}(k, m, R)$, or $k = m$ and $A \overline{A}B = S_{q}(k, k, R)$. By Lemma 59 (replacing if necessary $C$ with $C^{\perp}$, $\overline{A}$ with $\overline{A}^{\perp}$, $A$ with $B^{t}$ and $B$ with $A^{t}$) without loss of generality we may assume to be in the former case. Let $G = \{\gamma_{1}, \ldots, \gamma_{m}\}$, and for $i \in [m]$ define $\varphi_{i} := \sum_{j=1}^{m} B_{ij}^{-1} \gamma_{j}$. Is is clear that $F := \{\varphi_{1}, \ldots, \varphi_{m}\}$ is a basis of $\mathbb{F}_{q^{m}}$ over $\mathbb{F}_{q}$. Define the optimal Gabidulin anticode $V := \{v \in \mathbb{F}_{q^{m}}^{k} : v_{i} = 0 \text{ for } i > R\} \subseteq \mathbb{F}_{q^{m}}^{k}$. Using Definition 45 one can check that $C_{F}(V) = S_{q}(k, m, R) = A \overline{A}B$. Since $V$ is an optimal Gabidulin anticode of dimension $R$ over $\mathbb{F}_{q^{m}}$, by Remark 58 $V(A^{t})^{-1}$ is an optimal Gabidulin anticode of dimension $R$ as well. Hence by Corollary 39 it suffices to prove $\dim_{q}(V(A^{t})^{-1} \cap C) \geq r$. By Proposition 47 and Lemma 61 we have

$$\dim_{q}(V(A^{t})^{-1} \cap C) = \dim_{q}(V(A^{t})^{-1} A^{t} \cap CA^{t}) = \dim_{q}(V \cap CA^{t}) = \frac{1}{m} \dim_{q}(C_{F}(V \cap CA^{t})) = \frac{1}{m} \dim_{q}(C_{F}(V) \cap C_{F}(CA^{t})).$$

By Lemma 59 and Lemma 60 we have $C_{F}(CA^{t}) = AC_{F}(C) = AC_{G}(C)B = ACB$. It follows $C_{F}(V) \cap C_{F}(CA^{t}) = A \overline{A}B \cap ACB = A(\overline{A} \cap C)B$. Since $\dim_{q}(A(\overline{A} \cap C)) = \dim_{q}(\overline{A} \cap C)$, we have

$$\frac{1}{m} \dim_{q}(C_{F}(V) \cap C_{F}(CA^{t})) = \frac{1}{m} \dim_{q}(\overline{A} \cap C) \geq \frac{1}{m}(rm - \varepsilon).$$

It follows $\dim_{q}(V(A^{t})^{-1} \cap C) \geq [(rm - \varepsilon)/m] = r$, as claimed.

Remark 63. Theorem 62 shows that the generalized rank weights of a Gabidulin code can be obtained from the Delsarte generalized weights of any associated Delsarte code.
Remark 64. It is not true in general that for a Delsarte code \( C \subseteq \text{Mat}(k \times m, \mathbb{F}_q) \) of dimension \( t \) we have \( d_{im} = d_{im-\epsilon} \) for all \( i \geq 1 \) and \( 1 \leq \epsilon \leq m - 1 \) with \( 1 \leq im - \epsilon \leq t \). For example, one can produce codes \( C \subseteq \text{Mat}(3 \times 3, \mathbb{F}_2) \) of dimension 6 having the Delsarte generalized weights given in Table 1. The examples reflect the fact that not all Delsarte codes \( C \) arise from a Gabidulin code, even when \( \dim_{\mathbb{F}_q}(C) \equiv 0 \mod m \).

| \( a_1(C) \) | \( a_2(C) \) | \( a_3(C) \) | \( a_4(C) \) | \( a_5(C) \) | \( a_6(C) \) |
|---|---|---|---|---|---|
| 1 | 1 | 2 | 2 | 3 |
| 1 | 1 | 2 | 2 | 3 |
| 1 | 1 | 2 | 3 | 3 |
| 1 | 1 | 2 | 2 | 3 |
| 1 | 1 | 2 | 3 | 3 |

Table 1: Examples of Delsarte generalized weights.

6 Properties of Delsarte generalized weights

In this section we prove the analogue of Theorem 7 and Theorem 16 for Delsarte codes and Delsarte generalized weights, and characterize optimal Delsarte codes and anticodes in terms of their generalized weights.

Lemma 65. Let \( 1 \leq k \leq m \) be integers, and let \( A \in \mathcal{A}_q^D(k,m) \) with \( \maxrk(A) \geq 1 \). There exists \( A' \in \mathcal{A}_q^D(k,m) \) with \( A' \subseteq A \) and \( \dim_{\mathbb{F}_q}(A') = \dim_{\mathbb{F}_q}(A) - m \).

Proof. Let \( R := \maxrk(A) \). By Theorem 58 there exist invertible matrices \( A \) and \( B \) over \( \mathbb{F}_q \) of size \( k \times k \) and \( m \times m \) (respectively) such that either \( AAB = S_q(k,m,R) \), or \( k = m \) and \( AAB = S_q(k,k,R)^t \). In the former case set \( A' := A^{-1}S_q(k,m,R-1)B^{-1} \subseteq A \), while in the latter case set \( A' := A^{-1}S_q(k,k,R-1)^tB^{-1} \subseteq A \). One can check that \( A' \) is a Delsarte code with the expected properties. \( \square \)

Theorem 66. Let \( 1 \leq k \leq m \) be integers, and let \( C \subseteq \text{Mat}(k \times m, \mathbb{F}_q) \) be a non-zero Delsarte code of dimension \( 1 \leq t \leq km \) over \( \mathbb{F}_q \). The following facts hold.

1. \( a_1(C) = \minrk(C) \).
2. \( a_t(C) \leq k \).
3. For any \( 1 \leq r \leq t - 1 \) we have \( a_r(C) \leq a_{r+1}(C) \).
4. For any \( 1 \leq r \leq t - m \) we have \( a_r(C) < a_{r+m}(C) \).
5. For any \( 1 \leq r \leq t \) we have \( a_r(C) \leq k - \lfloor (t-r)/m \rfloor \).
6. For any \( 1 \leq r \leq t \) we have \( a_r(C) \geq \lceil r/m \rceil \).

Proof. We will prove the six properties separately.
1. Let $M \in \mathcal{C}$ with $d := \text{rk}(M) = \text{minrk}(\mathcal{C}) \geq 1$. There exist invertible matrices $A$ and $B$ over $\mathbb{F}_q$ of size $k \times k$ and $m \times m$ (respectively) such that $AMB$ is the matrix whose first $d$ diagonal entries are ones and whose other entries equal zero. Clearly, $AMB \in \mathcal{S}_q(k, m, d)$. Set $\mathcal{A} := A^{-1} \mathcal{S}_q(k, m, d)B^{-1}$. By Remark 63, $\mathcal{A}$ is an optimal Delsarte anticode of dimension $md$ over $\mathbb{F}_q$ and such that $M \in \mathcal{C} \cap \mathcal{A}$. In particular we have $\text{dim}_{\mathbb{F}_q}(\mathcal{C} \cap \mathcal{A}) \geq 1$, and so $a_1(\mathcal{C}) \leq d$. Since $\mathcal{C}$ has minimum rank $d$, it is clear that $a_1(\mathcal{C}) \geq d$.

2. Any anticode $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ has dimension at most $km$.

3. Any anticode $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ with $\text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r + 1$ satisfies $\text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r$.

4. Let $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ with $\text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r + m$ and $\text{dim}_{\mathbb{F}_q}(\mathcal{A}) = m \cdot a_{r+m}(\mathcal{C})$. By Lemma 65 there exists an optimal anticode $\mathcal{A}' \subseteq \mathcal{A}$ with $\text{dim}_{\mathbb{F}_q}(\mathcal{A}') = \text{dim}_{\mathbb{F}_q}(\mathcal{A}) - m$. It suffices to prove $\text{dim}_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) \geq r$. Since $\mathcal{A}' \subseteq \mathcal{A}$, we have $\mathcal{A}' \cap \mathcal{C} = \mathcal{A}' \cap (\mathcal{A} \cap \mathcal{C})$. Hence $\text{dim}_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) = \text{dim}_{\mathbb{F}_q}(\mathcal{A}' \cap (\mathcal{A} \cap \mathcal{C})) = \text{dim}_{\mathbb{F}_q}(\mathcal{A}') + \text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - \text{dim}_{\mathbb{F}_q}(\mathcal{A}' + (\mathcal{A} \cap \mathcal{C}))$. Since $\mathcal{A}' + (\mathcal{A} \cap \mathcal{C}) \subseteq \mathcal{A}$, we have $\text{dim}_{\mathbb{F}_q}(\mathcal{A}' + (\mathcal{A} \cap \mathcal{C})) \leq \text{dim}_{\mathbb{F}_q}(\mathcal{A})$. As a consequence, $\text{dim}_{\mathbb{F}_q}(\mathcal{A}' \cap \mathcal{C}) \geq \text{dim}_{\mathbb{F}_q}(\mathcal{A}') + \text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - \text{dim}_{\mathbb{F}_q}(\mathcal{A}) = \text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) - m \geq r$.

5. Define $h := [(t-r)/m]$. By part (2) and (4) we find a strictly increasing sequence of integers

$$a_r(\mathcal{C}) < a_{r+m}(\mathcal{C}) < \cdots < a_{r+hm}(\mathcal{C}) \leq k.$$ 

It follows $k \geq a_r + h$, i.e., $a_r \leq k - h$, as claimed.

6. If $\mathcal{A} \in \mathcal{A}_q^D(k, m)$ satisfies $\text{dim}_{\mathbb{F}_q}(\mathcal{A} \cap \mathcal{C}) \geq r$ then, in particular, $\text{dim}_{\mathbb{F}_q}(\mathcal{A}) \geq r$. Hence we have $a_r(\mathcal{C}) \geq r/m$, i.e., $a_r(\mathcal{C}) \geq [r/m]$.

**Remark 67.** Following the notation of Theorem 66 if the Delsarte code $\mathcal{C}$ arises from a Gabidulin code $\mathcal{C}$ then we have $t \equiv 0 \pmod{m}$. Hence, by Theorem 62, Theorem 66 generalizes Theorem 16 for Gabidulin codes.

Theorem 66 allows us to characterize Delsarte optimal codes and antcodes in terms of their Delsarte generalized weights.

**Corollary 68.** Let $1 \leq R \leq k \leq m$ be integers, and let $\mathcal{C} \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a Delsarte code with $\text{dim}_{\mathbb{F}_q}(\mathcal{C}) = mR$. The following facts are equivalent.

1. $\mathcal{C}$ is a Delsarte optimal code,

2. $a_1(\mathcal{C}) = k - R + 1$,

3. for all $r \in [mR]$ we have $a_r(\mathcal{C}) = k - R + \lceil r/m \rceil$.

In particular, the Delsarte generalized weights of a Delsarte optimal code $\mathcal{C} \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ only depend on $k$, $m$ and minrk($\mathcal{C}$).

**Proof.** By Definition 63 and Theorem 66 (1) and (2) are equivalent. Assume $a_1(\mathcal{C}) = k - R + 1$. By Theorem 66 for all $r \in [mR]$ we have $a_r(\mathcal{C}) \leq k - \lfloor (mR - r)/m \rfloor = k - R + \lfloor r/m \rfloor$. Assume
Proof. Assume that we can find an optimal anticode $A \subseteq C$. Let us prove that $A$ is the code denoted and defined by $\dim F^m$, implies (2). Let us prove (2) $\Rightarrow$ (3). It is clear that (3) implies (2).

Finally, it is clear that (3) implies (2).

**Corollary 69.** Let $1 \leq R \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, F_q)$ be a Delsarte code with $\dim_{F_q}(C) = mR$. The following facts are equivalent.

1. $C$ is a Delsarte optimal anticode,
2. $a_{mR}(C) = R$,
3. for all $r \in [mR]$ we have $a_r(C) = \lceil r/m \rceil$.

In particular, the Delsarte generalized weights of a Delsarte optimal anticode $C \subseteq \text{Mat}(k \times m, F_q)$ only depend on $k$, $m$ and $\maxrk(C)$.

**Proof.** Assume that $C$ is an optimal anticode. By Theorem 66 for all $r \in [mR]$ we have $a_r(C) \geq \lceil r/m \rceil$. Let $r \in [mR]$. Since $\lfloor r/m \rfloor \leq mR/m = R$, by iterating Lemma 65 we can find an optimal anticode $A \subseteq C$ with $\dim_{F_q}(A) = m\lfloor r/m \rfloor$. We have $\dim_{F_q}(A \cap C) = \dim_{F_q}(A) = m\lfloor r/m \rfloor$, and so $a_r(C) \leq \lceil r/m \rceil$. This proves (1) $\Rightarrow$ (3). It is clear that (3) implies (2). Let us prove (2) $\Rightarrow$ (1). Assume $a_{mR}(C) = R$. By definition, there exists an optimal anticode $A \subseteq A^D_{q}(k,m)$ such that $\dim_{F_q}(A) = mR$ and $\dim_{F_q}(A \cap C) \geq mR$. Since $\dim_{F_q}(C) = mR$, we have $A = C$. In particular, $C \subseteq A^D_{q}(k,m)$.

7 **Delsarte generalized weights and duality**

In this section we recall the definition of Delsarte dual code, and show how the Delsarte generalized weights of a code $C$ relate to the Delsarte generalized weights of the dual code $C^\perp$.

We first recall two analogous results for linear and Gabidulin codes.

**Definition 70.** The dual of a linear code and the dual of a Gabidulin code are defined as follows.

1. Let $C \subseteq F_q^n$ be a linear code. The [5] of $C$ is the code denoted and defined by $C^\perp := \{v \in F_q^n : \langle c, v \rangle = 0 \text{ for all } c \in C \} \subseteq F_q^n$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of $F_q^n$.

2. Let $C \subseteq F_{qm}^k$ be a Gabidulin code. The [5] of $C$ is the code denoted and defined by $C^\perp := \{v \in F_{qm}^k : \langle c, v \rangle = 0 \text{ for all } c \in C \} \subseteq F_{qm}^k$, where $\langle \cdot, \cdot \rangle$ is the standard inner product of $F_{qm}^k$. 

17
The first part of the following result was proved by Wei, and the second part was proved by Ducoat.

**Theorem 71** ([13], Theorem 3, and [2]). The following facts hold.

1. Let \( C \subseteq \mathbb{F}_q^n \) be a linear code of dimension \( 1 \leq t \leq n \) over \( \mathbb{F}_q \). The generalized Hamming weights of \( C^\perp \) are determined by the generalized Hamming weights of \( C \).

2. Let \( C \subseteq \mathbb{F}_q^k \) be a Gabidulin code of dimension \( 1 \leq t \leq k \) over \( \mathbb{F}_q^k \). The generalized rank weights of \( C^\perp \) are determined by the generalized rank weights of \( C \).

In this section we prove the analogue of Theorem 71 for Delsarte codes and Delsarte generalized weights. The following notion of duality in Mat \((k \times m, \mathbb{F}_q)\) was proposed in the context of coding theory by Delsarte in [1].

**Definition 72.** The **trace-product** of matrices \( M, N \in \text{Mat}(k \times m, \mathbb{F}_q) \) is defined by

\[
\langle M, N \rangle := \text{Tr}(MN^t).
\]

It is easy to see that the map \( \langle \cdot, \cdot \rangle : \text{Mat}(k \times m, \mathbb{F}_q) \times \text{Mat}(k \times m, \mathbb{F}_q) \to \mathbb{F}_q \) is symmetric, bilinear and non-degenerate.

**Definition 73.** The **dual** of a Delsarte code \( C \subseteq \text{Mat}(k \times m, \mathbb{F}_q) \) is the Delsarte code denoted \( C^\perp \) and defined by

\[
C^\perp := \{ N \in \text{Mat}(k \times m, \mathbb{F}_q) : \langle M, N \rangle = 0 \text{ for all } M \in C \} \subseteq \text{Mat}(k \times m, \mathbb{F}_q).
\]

The following lemma summarizes some properties of the trace-product of matrices.

**Lemma 74.** Let \( C, D \subseteq \text{Mat}(k \times m, \mathbb{F}_q) \) be \( \mathbb{F}_q \)-subspaces. We have:

1. \( (C^\perp)^\perp = C \),
2. \( \dim_{\mathbb{F}_q}(C^\perp) = km - \dim_{\mathbb{F}_q}(C) \),
3. \( (C \cap D)^\perp = C^\perp + D^\perp \).

We will also need the following result.

**Theorem 75** ([9], Theorem 50). Let \( A \in \text{Mat}(k \times m, \mathbb{F}_q) \) be a Delsarte code. Then \( A \in A^D_q(k \times m) \) if and only if \( A^\perp \in A^D_q(k \times m) \).

The theorem that we present relates the Delsarte generalized weights of a code \( C \) to the Delsarte generalized weights of the dual code \( C^\perp \).

**Theorem 76.** Let \( 1 \leq k \leq m \) be integers, and let \( C \subseteq \text{Mat}(k \times m, \mathbb{F}_q) \) be a Delsarte code of dimension \( 1 \leq t \leq km - 1 \). Assume that \( p, i, j \in \mathbb{Z} \) satisfy:

1. \( 1 \leq p + im \leq km - t \),
2. \( 1 \leq p + t + jm \leq t \).

We have \( a_{p+im}(C^\perp) \neq k + 1 - a_{p+t+jm}(C) \).
Proof. Define }r := p + im\text{ and }s := t + r - m \cdot a_r(C^\perp).\text{ Notice that by Theorem }66\text{ we have }a_r(C^\perp) \geq r/m,\text{ and so in particular }s \leq t.\text{ We divide the argument into two parts. All dimensions in the proof are over }\mathbb{F}_q.\text{ }

1. We first assume }p + t + jm \leq s.\text{ Since, by hypothesis, }p + t + jm \geq 1,\text{ we have }1 \leq p + t + jm \leq s \leq t.\text{ Let }A \in \mathcal{A}_q^D(k, m)\text{ with dim}(A \cap C^\perp) \geq r\text{ and dim}(A) = m \cdot a_r(C^\perp).\text{ By Lemma }74\text{ we have }
r \leq \text{dim}(A \cap C^\perp) = \text{dim}(A) + \text{dim}(C^\perp) - \text{dim}(A + C^\perp) = m \cdot a_r(C^\perp) + (km - t) - (km - \text{dim}(A \cap C^\perp)) = m \cdot a_r(C^\perp) - t + \text{dim}(A^\perp \cap C^\perp).\text{ This implies }s = t + r - m \cdot a_r(C^\perp) \leq \text{dim}(A^\perp \cap C^\perp),\text{ and so, by Theorem }75\text{ we have }a_s(C) \leq \text{dim}(A^\perp)/m = (km - \text{dim}(A))/m = (km - m \cdot a_r(C^\perp))/m = k - a_r(C^\perp),\text{ i.e., }a_r(C^\perp) \leq k - a_s(C).\text{ Since }p + t + jm \leq s,\text{ by Theorem }66\text{ we have }a_s(C) \geq a_{p + t + jm}(C).\text{ As a consequence,}

a_r(C^\perp) \leq k - a_s(C) \leq k - a_{p + t + jm}(C) < k + 1 - a_{p + t + jm}(C).

In particular, }a_r(C^\perp) \neq k + 1 - a_{p + t + jm}(C).\text{ }

2. Now assume }p + t + jm > s,\text{ i.e., }i - j < a_r(C^\perp).\text{ There exists an integer }\varepsilon > 0\text{ with }i - j = a_r(C^\perp) - \varepsilon.\text{ By definition of }r\text{ we can write }
p + t + jm = r - im + t + jm = r - (a_r(C^\perp) - \varepsilon + j)m + t + jm = r - (i - j)m + t = r - (a_r(C^\perp) - \varepsilon)m + t = t + r - m \cdot a_r(C^\perp) + \varepsilon m = s + \varepsilon m.\text{ Assume by contradiction }a_r(C^\perp) = k + 1 - a_{p + t + jm}(C),\text{ i.e., }a_r(C^\perp) = k + 1 - a_{s + \varepsilon m}(C).\text{ Let }A \in \mathcal{A}_q^D(k, m)\text{ with dim}(A \cap C) \geq s + \varepsilon m\text{ and dim}(A) = m \cdot a_{s + \varepsilon m}(C) = m(k + 1 - a_r(C^\perp)).\text{ By Lemma }74\text{ we have }
s + \varepsilon m \leq \text{dim}(A \cap C) = \text{dim}(A) + \text{dim}(C) - \text{dim}(A + C) = m(k + 1 - a_r(C^\perp)) + t - (km - \text{dim}(A^\perp \cap C^\perp)) = m - m \cdot a_r(C^\perp) + t + \text{dim}(A^\perp \cap C^\perp).\text{ Since }s = t + r - m \cdot a_r(C^\perp),\text{ the inequality above becomes }t + r - m \cdot a_r(C^\perp) + \varepsilon m \leq m - m \cdot a_r(C^\perp) + t + \text{dim}(A^\perp \cap C^\perp),\text{ i.e., dim}(A^\perp \cap C^\perp) \geq r + \varepsilon m - m.\text{ By Theorem }75\text{, }A^\perp \in \mathcal{A}_q^D(k, m),\text{ and so }m \cdot a_{s + \varepsilon m - m}(C^\perp) \leq \text{dim}(A^\perp).\text{ On the other hand, by Lemma }74\text{ we have dim}(A) = km - \text{dim}(A) = km - m(k + 1 - a_r(C^\perp)) = m(a_r(C^\perp) - 1).\text{ It follows }m \cdot a_{s + \varepsilon m - m}(C^\perp) \leq \text{dim}(A^\perp) = m(a_r(C^\perp) - 1),\text{ i.e., }a_{s + \varepsilon m - m}(C^\perp) \leq a_r(C^\perp) - 1.\text{ Since }\varepsilon > 0,\text{ we have }r + \varepsilon m - m \geq r.\text{ Hence by Theorem }66\text{ we have }a_r(C^\perp) \leq a_{r + \varepsilon m - m}(C^\perp) \leq a_r(C^\perp) - 1,\text{ a contradiction.}\qed
Definition 77. Let $1 \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a Delsarte code of dimension $1 \leq t \leq km$. For any $s \in \mathbb{Z}$, the $s$-weight sets of $C$ are denoted and defined by
\[
W_s(C) := \{a_{s+im}(C) : i \in \mathbb{Z}, \ 1 \leq s + im \leq t\},
\]
\[
\overline{W}_s(C) := \{k + 1 - a_{s+im}(C) : i \in \mathbb{Z}, \ 1 \leq s + im \leq t\}.
\]

Theorem 76 has the following interesting consequence, which is the analogue of Theorem 71 for Delsarte codes.

Corollary 78. Let $1 \leq k \leq m$ be integers, and let $C \subseteq \text{Mat}(k \times m, \mathbb{F}_q)$ be a Delsarte code of dimension $1 \leq t \leq km - 1$. For any integer $1 \leq p \leq m$ we have
\[
W_p(C) = [k] \setminus \overline{W}_{p+t}(C).
\]
In particular, the Delsarte generalized weights of $C$ completely determine the Delsarte generalized weights of $C$.

Proof. Let us prove the first part of the statement. Assume $\overline{W}_{p+t}(C) = \emptyset$. This means that there are no integers of the form $p + t + im$, $i \in \mathbb{Z}$, in the set $[t]$. In particular we have $p + t - m \notin [t]$. Since $p \leq m$, it must be $p + t - m \leq 0$, i.e., $p \leq m - t$. It follows that for all $0 \leq i \leq k - 1$ we have $1 \leq p + im \leq p + (k-1)m \leq m - t + (k-1)m = km - t$. Hence by Theorem 66 we have $W_p(C) = [k]$, as claimed. Now assume $W_p(C) = \emptyset$. It must be $p > km - t$. Since $p \leq m$, for all $i \in \mathbb{Z}$ with $-k \leq i \leq -1$ we have $t \geq p + t + im > km - t + t + im = km + im \geq 0$. Hence by Theorem 66 we have $\overline{W}_{p+t}(C) = [k]$. Finally, assume that $W_p(C)$ and $\overline{W}_{p+t}(C)$ are both non-empty. By Theorem 76 we have $W_p(C) \cap \overline{W}_{p+t}(C) = \emptyset$, and by Theorem 66 we have $W_p(C) \cup \overline{W}_{p+t}(C) \subseteq [k]$. Hence it suffices to prove $|W_p(C)| + |\overline{W}_{p+t}(C)| = k$. By Theorem 66, the generalized weights $a_{p+im}(C)$, for all $i \in \mathbb{Z}$ such that $1 \leq p + im \leq km - t$, are distinct. Similarly, again by Theorem 66, the generalized weights $a_{p+t+im}(C)$, for all $i \in \mathbb{Z}$ such that $1 \leq p + t + im \leq t$, are also distinct. Hence it is easy to check that
\[
|W_p(C)| = \lceil (km - t - p)/m \rceil - \lfloor (1 - p)/m \rfloor + 1, \quad |\overline{W}_{p+t}(C)| = \lfloor -p/m \rfloor - \lceil (1 - p - t)/m \rceil + 1.
\]
Since $1 \leq p \leq m$, we have $\lceil (1 - p)/m \rceil = 0$ and $\lfloor -p/m \rfloor = -1$. Hence it suffices to prove
\[
\lceil (km - t - p)/m \rceil - \lfloor (1 - p - t)/m \rfloor = k - 1.
\]
Write $t + p = Am + B$ with $0 \leq B \leq m - 1$. If $B = 0$ then $\lceil (km - t - p)/m \rceil = k - A$ and $\lfloor (1 - p - t)/m \rfloor = -A + 1$. If $0 < B \leq k - 1$ then $\lceil (km - t - p)/m \rceil = k - A - 1$ and $\lfloor (1 - p - t)/m \rfloor = -A$. Hence in any case $\lceil (km - t - p)/m \rceil - \lfloor (1 - p - t)/m \rfloor = k - 1$, as claimed.

In order to prove the second part of the statement, we observe that by Theorem 66 the generalized weights of $C$ in $W_p(C)$ are ordered integers. Hence they are completely determined by the set $\overline{W}_{t+p}(C)$. The thesis now follows from the fact that any $a_t(C)$, $1 \leq r \leq km - t$, belongs to one set $W_p(C)$, for some $1 \leq p \leq m$.

Remark 79. Corollary 78 gives a method to compute the Delarte generalized weights of a code $C$ starting from the Delsarte generalized weights of $C$, as we show in the following example.
Example 80. Let e.g. \( q = 5 \) and \( k = m = 3 \). Let \( \mathcal{C} \subseteq \text{Mat}(3 \times 3, \mathbb{F}_5) \) be the code generated over \( \mathbb{F}_5 \) by the two matrices

\[
\begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}, \quad \begin{bmatrix}
0 & 0 & 0 \\
0 & 3 & 0 \\
0 & 0 & 0
\end{bmatrix}.
\]

It is easy to check that \( a_1(\mathcal{C}) = 1 \) and \( a_2(\mathcal{C}) = 2 \). We have \( t = \dim_{\mathbb{F}_4}(\mathcal{C}^\perp) = 9 - 2 = 7 \). We will compute the integers

\[
a_1(\mathcal{C}^\perp), \ a_2(\mathcal{C}^\perp), \ a_3(\mathcal{C}^\perp), \ a_4(\mathcal{C}^\perp), \ a_5(\mathcal{C}^\perp), \ a_6(\mathcal{C}^\perp), \ a_7(\mathcal{C}^\perp)
\]

employing Corollary 78. Start with \( p = 1 \). We have \( W_1(\mathcal{C}^\perp) = \{a_1(\mathcal{C}^\perp), a_4(\mathcal{C}^\perp), a_7(\mathcal{C}^\perp)\} \) and \( W_3(\mathcal{C}) = \emptyset \). Since \( a_1(\mathcal{C}^\perp) < a_4(\mathcal{C}^\perp) < a_7(\mathcal{C}^\perp) \) and \( W_1(\mathcal{C}^\perp) = [3] \setminus W_3(\mathcal{C}) \), it follows \( a_1(\mathcal{C}^\perp) = 1 \), \( a_4(\mathcal{C}^\perp) = 2 \), \( a_7(\mathcal{C}^\perp) = 3 \). Similarly, \( W_2(\mathcal{C}^\perp) = \{a_2(\mathcal{C}^\perp), a_5(\mathcal{C}^\perp)\} \) and \( W_4(\mathcal{C}) = \{3 + 1 - a_1(\mathcal{C})\} = \{3\} \). It follows \( a_2(\mathcal{C}^\perp) = 1 \) and \( a_5(\mathcal{C}^\perp) = 2 \). Finally, \( W_3(\mathcal{C}^\perp) = \{a_3(\mathcal{C}^\perp), a_6(\mathcal{C}^\perp)\} \) and \( W_5(\mathcal{C}) = \{3 + 1 - a_2(\mathcal{C})\} = \{2\} \). Hence \( a_3(\mathcal{C}^\perp) = 1 \) and \( a_6(\mathcal{C}^\perp) = 3 \). Summarizing, the Delsarte generalized weights of \( \mathcal{C}^\perp \) are the integers

\[
a_1(\mathcal{C}^\perp) = 1, \ a_2(\mathcal{C}^\perp) = 1, \ a_3(\mathcal{C}^\perp) = 1, \ a_4(\mathcal{C}^\perp) = 2, \ a_5(\mathcal{C}^\perp) = 2, \ a_6(\mathcal{C}^\perp) = 3, \ a_7(\mathcal{C}^\perp) = 3.
\]

Remark 81. Combining Theorem 62, Lemma 60 and [9], Theorem 18, one can see that Corollary 78 generalizes the second part of Theorem 71.

Remark 82. The existence of a duality theory is an important algebraic feature of generalized weights in the various metrics that we considered. The reason why in this work we focused on the Delsarte generalized weights given in Definition 48 and not on the Oggier-Sboui generalized weights of Remark 50 is precisely the duality theory. Indeed, it is not true in general that the Oggier-Sboui generalized weights of a Delsarte code determine the Oggier-Sboui generalized weights of the dual code, as we show in the following example.

Example 83. Let e.g. \( q = 2 \), \( k = 2 \) and \( m = 3 \). Consider the 2-dimensional Delsarte codes \( \mathcal{C}, \mathcal{D} \subseteq \text{Mat}(k \times m, \mathbb{F}_2) \) defined by

\[
\mathcal{C} := \langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rangle, \quad \mathcal{D} := \langle \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \rangle.
\]

One can easily check that \( a_1'(\mathcal{C}) = a_1'(\mathcal{D}) = 1 \) and \( a_2'(\mathcal{C}) = a_2'(\mathcal{D}) = 1 \). On the other hand, we have

\[
a_1'(\mathcal{C}^\perp) = 1, \ a_2'(\mathcal{C}^\perp) = 1, \ a_3'(\mathcal{C}^\perp) = 2, \ a_4'(\mathcal{C}^\perp) = 2,
\]

\[
a_1'(\mathcal{D}^\perp) = 1, \ a_2'(\mathcal{D}^\perp) = 1, \ a_3'(\mathcal{D}^\perp) = 1, \ a_4'(\mathcal{D}^\perp) = 2.
\]

Hence \( \mathcal{C} \) and \( \mathcal{D} \) have the same Oggier-Sboui generalized weights, while \( \mathcal{C}^\perp \) and \( \mathcal{D}^\perp \) have not. This means that we do not have an analogue of Corollary 78 for such invariant.

8 Generalized rank weights and security drops

In [12], Silva and Kschishang proposed a rank-metric coding scheme to secure a network communication against an eavesdropper. In this paper we are more interested in the algebraic
aspects of the problem, and so we do not describe the scheme into the details. In [12] the authors prove that when a Gabidulin code $C \subseteq \mathbb{F}_q^k$ is employed in their scheme, the information that an eavesdropper can obtain listening at $0 \leq \mu \leq k$ links of the channel is bounded by the quantity

$$\Delta_\mu(C) := \max\{\dim_{\mathbb{F}_q}(V \cap C) : V \in \Lambda_q(k, m), \dim_{\mathbb{F}_q}(V) = \mu\}.$$ 

In analogy with the theory of generalized Hamming weights developed by Wei, we give the following definition.

**Definition 84.** Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_q^k$ be a Gabidulin code. An integer $1 \leq \mu \leq k$ is said to be a **worst-case security drop** for $C$ if $\Delta_\mu(C) > \Delta_{\mu-1}(C)$.

The following result is the analogue for Gabidulin code of [12], Corollary A, for linear codes.

**Theorem 85.** Let $1 \leq k \leq m$ be integers, and let $C \subseteq \mathbb{F}_q^k$ be a Gabidulin code of dimension $1 \leq t \leq k$ over $\mathbb{F}_q$. Fix an integer $1 \leq \mu \leq k$. The following facts are equivalent.

1. $\Delta_\mu(C) > \Delta_{\mu-1}(C)$, i.e., $\mu$ is a worst-case security drop for $C$,

2. there exists $1 \leq r \leq t$ with $m_r(C) = \mu$.

**Proof.** Let us prove (1) $\Rightarrow$ (2). Take $V \in \Lambda_q(k, m)$ with $\dim_{\mathbb{F}_q}(V) = \mu$ and $\dim_{\mathbb{F}_q}(V \cap C) = \Delta_\mu(C)$. We have $m_{\Delta_\mu(C)}(C) \leq \mu$. Assume by contradiction $m_{\Delta_\mu(C)}(C) < \mu$. By definition, there exists $U \in \Lambda_q(k, m)$ with $\dim_{\mathbb{F}_q}(U \cap C) \geq \Delta_\mu(C)$ and $\dim_{\mathbb{F}_q}(U) < \mu$. Clearly, we can find $H \supseteq U$ with $H \in \Lambda_q(k, m)$ and $\dim_{\mathbb{F}_q}(H) = \mu - 1$. It follows

$$\Delta_{\mu-1}(C) \geq \dim_{\mathbb{F}_q}(H \cap C) \geq \dim_{\mathbb{F}_q}(U \cap C) \geq \Delta_\mu(C),$$

a contradiction. Hence we may take $r = \Delta_\mu(C)$. Now we prove (2) $\Rightarrow$ (1). Let $1 \leq r \leq t$ with $m_r(C) = \mu$. There exists $V \in \Lambda_q(k, m)$ with $\dim_{\mathbb{F}_q}(V \cap C) \geq r$ and $\dim_{\mathbb{F}_q}(V) = \mu$. Hence $\Delta_\mu(C) \geq r$. Assume by contradiction $\Delta_\mu(C) = \Delta_{\mu-1}(C)$. Let $U \in \Lambda_q(k, m)$ with $\dim_{\mathbb{F}_q}(U) = \mu - 1$ and $\dim_{\mathbb{F}_q}(U \cap C) = \Delta_{\mu-1}(C) = \Delta_\mu(C)$. By definition, $m_{\Delta_\mu(C)}(C) \leq \mu - 1$. Moreover, since $\Delta_\mu(C) \geq r$, by Theorem 66 we have $m_{\Delta_\mu(C)}(C) \geq m_r(C)$. It follows $\mu = m_r(C) \leq m_{\Delta_\mu(C)}(C) \leq \mu - 1$, a contradiction. This proves $\Delta_\mu(C) > \Delta_{\mu-1}(C)$.

**Remark 86.** Theorem 65 shows that the generalized rank weights introduced by Kurihara, Matsumoto and Uyematsu in [6] measure the worst-case security drops of a Gabidulin code when employed to secure a network communication through the scheme of [12].

**Acknowledgement**

I am grateful to Elisa Gorla for some observations that helped me to improve Theorem 62 and Remark 64.
References

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

[2] J. Ducoat, *Generalized rank weights: a duality statement*. Online preprint: http://arxiv.org/abs/1306.3899

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

[4] M. Giorgetti, A. Previtali, *Galois invariance, trace codes and subfield subcodes*. Finite Fields and Their Applications, 16 (2010), 2, pp. 96 – 99.

[5] R. Kötter, F. R. Kschischang, *Coding for Errors and Erasures in Random Network Coding*. IEEE Transactions on Information Theory, 54 (2008), 8, pp. 3579 – 3591.

[6] J. Kurihara, R. Matsumoto, T. Uyematsu, *Relative Generalized Rank Weight of Linear Codes and Its Applications to Network Coding*. Online preprint: http://arxiv.org/abs/1301.5482

[7] F. Oggier, A. Sboui, *On the Existence of Generalized Rank Weights*. IEEE International Symposium on Information Theory and its Applications (2012).

[8] L. H. Ozarow, A. D. Wyner, *Wire-tap-channel II*. Bell Labs Technical Journal, 63 (1984), pp. 2135 – 2157.

[9] A. Ravagnani, *Rank-metric codes and their MacWilliams identities*. Online preprint: http://arxiv.org/abs/1410.1333

[10] C. de Seguins Pazzis, *The classification of large spaces of matrices with bounded rank*. Israel Journal of Mathematics, to appear. Online preprint: http://arxiv.org/abs/1004.0298

[11] D. Silva, F. R. Kschischang, *On metrics for error correction in network coding*. IEEE Transactions on Information Theory, 55 (2009), 12, pp. 5479 – 5490.

[12] D. Silva, F. R. Kschischang, *Universal Secure Network Coding via Rank-Metric Codes*. IEEE Transactions on Information Theory, 57 (2011), 2, pp. 1124 – 1135.

[13] V. K. Wei, *Generalized Hamming Weights for Linear Codes*. IEEE Transactions on Information Theory, 37 (1991), 5, pp. 1412 – 1418.