Code Equivalence in the Sum-Rank Metric: Hardness and Completeness

Giuseppe D'Alconzo
giuseppe.dalconzo@polito.it
Department of Mathematical Sciences, Politecnico di Torino

Abstract

In this work, we define and study equivalence problems for sum-rank codes, giving their formulation in terms of tensors. Moreover, we introduce the concept of *generating tensors* of a sum-rank code, a direct generalization of the generating matrix for a linear code endowed with the Hamming metric. In this way, we embrace well-known definitions and problems for Hamming and rank metric codes. Finally, we prove the TI-completeness of code equivalence for rank and sum-rank codes, and hence, in the future, these problems could be used in the design of post-quantum schemes.

Keywords— Code Equivalence; Sum-Rank; Rank Metric; Tensor Isomorphism

1 Introduction

Code Equivalence. The problem of finding the equivalence between two linear codes in the Hamming metric was studied by Leon in 1982 [17], and later its hardness was analyzed in [26, 29, 30]. The Support Splitting Algorithm [28] finds a permutation between two codes in exponential time in the dimension of the hull, and, for random codes, it has been proven that the algorithm runs in practical time. Moreover, in [2, 26] are shown some links between the Code Equivalence and the Graph Isomorphism problem.
The code equivalence problem belongs to the large class of *isomorphism problems*, like Graph Isomorphism and Polynomial Isomorphism, contained in $\mathsf{NP} \cap \mathsf{coAM}$. A recent complexity class called TI links equivalence problems to *Tensor Isomorphism*: concepts like TI-hardness and completeness are formalized in [13]. These problems can be easily modelled by *Hard Homogeneous Spaces* (or Cryptographic Group Actions) [1, 6] and are relevant from a cryptographic point of view since they lead to a Sigma protocol, for example the one for Graph Isomorphism presented in [11]. Assuming that the underlying problem is intractable, a Sigma protocol can be converted to a digital signature using the Fiat-Shamir transform [10]. Many post-quantum signatures are based on this construction, for example [3, 4, 8, 9, 25, 32].
More recently, the hardness of the equivalence problem on matrix codes has been studied: in [7] it is proven that in the rank metric it is at least harder than the monomial equivalence in the Hamming metric, and in [27], it is shown that a problem on homogeneous quadratic polynomials is polynomially equivalent to deciding the equivalence between two matrix codes.

Sum-rank codes. Sum-rank codes are a generalization of both Hamming and matrix codes, and they were independently introduced in [24] and [18]. A sum-rank code is a subspace of the Cartesian product of t matrix spaces of (eventually) different sizes. Given a tuple of matrices, its *sum-rank weight* is the sum of their ranks. It can be seen as a generalization of

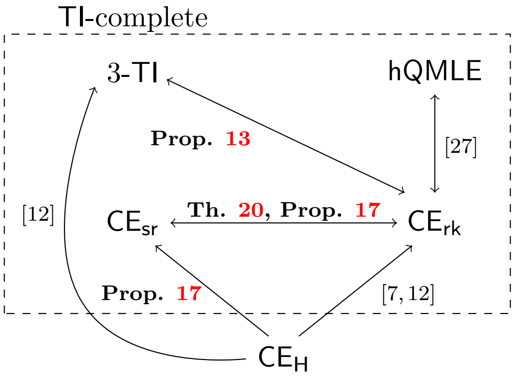

Figure 1: Reduction between problems and TI-completeness. "A→B" indicates that A reduces to B.

the Hamming weight and the rank. This field is still in its beginning and an introduction to the general theory for such codes can be found in [21]. Isometries of certain classes of codes are studied in [21] and a straightforward question is to decide whether two arbitrary sum-rank codes are equivalent, leading to the equivalence problem in the sum-rank metric, introduced in [20].

Our contribution. In this work, we define the linear equivalence problem for sum-rank codes $\mathsf{CE}_{\mathsf{sr}}$ and we study its hardness. It is also given a characterization of linear maps that preserve the sum-rank metric. We show that $\mathsf{CE}_{\mathsf{sr}}$ is polynomially equivalent to the same problem in the rank metric $\mathsf{CE}_{\mathsf{rk}}$ and we show the TI-completeness of both problems. Figure 1 summarises all the reductions between code equivalence and other problems. To ease the notation and the proofs, we generalize the concept of *generating matrix* to *generating tensors* of a linear code. In Section 2 some preliminaries on codes and tensors are given, while Section 3 sets the notation and define the generating tensors for sum-rank codes. Section 4 concerns the linear equivalence problem and shows some reductions between different formulations of it.

2 Preliminaries

For a prime power q, $\mathbb{F}_q$ is the finite field with q elements, and $\mathbb{F}_q^n$ is the n-dimensional vector space over $\mathbb{F}_q$. With $\mathbb{F}_q^{n\times m}$ we denote the linear space of $n\times m$ matrices with coefficients in $\mathbb{F}_q$. Let $\mathrm{GL}_n(q)$ be the group of invertible $n\times n$ matrices with coefficients in $\mathbb{F}_q$. A monomial $n\times n$ matrix is given by the product of a $n\times n$ diagonal matrix with non-zero entries on the diagonal, with a $n\times n$ permutation matrix. Monomial matrices form a subgroup of $\mathrm{GL}_n(q)$. The transpose of a matrix A is denoted with A^t. With $||$ we denote the concatenation of strings or vectors.

2.1 Tensors

For the scope of this paper, when we talk about tensors, we intend d-way arrays.

Definition 1. Let $d, n_1, \dots, n_d$ be positive numbers. A *d-tensor* $\mathbf{T}$ over the field $\mathbb{F}$ of side lengths $n_1, \dots, n_d$, written as

$$\mathbf{T} = T_{i_1,\dots,i_d} \quad 1 \le i_j \le n_j \text{ for every } 1 \le j \le d$$

is a d-dimensional array with entries in $\mathbb{F}$.

From here, we will consider mainly 3-tensors over the finite field $\mathbb{F}_q$.
Given a 3-tensor G_{ijk} of side length n, m, s, the s slices of G are 2-tensors ($n\times m$ matrices)

given by $G_{ij1}, \ldots, G_{ijs}$. Here we use the notation with indexes ij to denote that they are 2-tensors.
Like in the case of Graph Isomorphism, the problem of *3-Tensor Isomorphism* can be defined.

Definition 2. The *3-Tensor Isomorphism* (3-TI) problem is given by

- *Input*: two 3-tensors $\mathbf{G} = G_{ijk}$ and $\mathbf{G}' = G'_{ijk}$ of side length n, m, s.
- *Output*: YES if there exist matrices A in $\mathrm{GL}_n(q)$, B in $\mathrm{GL}_m(q)$ and C in $\mathrm{GL}_s(q)$ such that for every i, j, k the following holds:

$$G_{ijk} = \sum_{u,v,w} G'_{uvw} A_{iu} B_{jv} C_{kw}$$

and NO otherwise.

The *search* version s3-TI is the problem of finding such matrices, given two isomorphic 3-tensors.

The above problem can be generalized in the case of d-tensors, with d constant. In [12] it is shown that d-TI and 3-TI are polynomially equivalent. In the same flavour of the complexity class GI (the set of problems reducible in polynomial time to Graph Isomorphism [16]), the TI class is defined in [13], since a lot of different problems can be reduced to d-TI.

Definition 3. The *Tensor Isomorphism* class (TI) contains decision problems that can be reduced to d-TI for a certain d. A problem D is said TI-*hard* if d-TI can be reduced to D, for any d. A problem is said TI-*complete* if it is in TI and is TI-hard.

It is easy to see that TI is a subset of NP and we can adapt the AM protocol for the complement of Graph Isomorphism [11] and Code Equivalence [26] to show that TI is in coAM. This means that no problem in TI can be NP-complete unless the polynomial hierarchy collapses at the second level [5]. From a cryptographic point of view, this is not a big issue: problems in $\mathsf{NP} \cap \mathsf{coAM}$ have the interesting property that the hardest instance is as difficult to solve as a random one. More formally, given an arbitrary instance, it can be reduced to a random one. Such property is not held by any NP-complete problem, unless the polynomial hierarchy collapses at the third level.

2.2 Hamming metric

Let $\mathcal{C}$ be a $[n, k]_q$-code , i.e. a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of dimension k. The *Hamming weight* of a vector x in $\mathbb{F}_q^n$ is the number of its non-zero coordinates, and it is denoted with $\mathrm{w}_H(x)$. The Hamming distance is given by

$$\mathrm{d}_H(x, y) = \mathrm{w}_H(x - y)$$

and it is, indeed, a metric [14, Theorem 1.4.1].

Definition 4. An invertible map $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a *linear equivalence that preserves the Hamming weight* if it is $\mathbb{F}_q$-linear and for every x in $\mathbb{F}_q^n$ we have

$$\mathrm{w}_H(x) = \mathrm{w}_H(f(x)).$$

By linearity, f preserves the Hamming metric and we say that f is a *linear Hamming metric-preserving map.*

Two linear codes in the Hamming metric $\mathcal{C}$ and $\mathcal{C}'$ are *linearly equivalent* if there is a linear Hamming metric-preserving map f such that $\mathcal{C} = f(\mathcal{C}')$.

We can characterize linear metric-preserving maps in the Hamming metric, reporting a well-known result from [19].

Proposition 5. *If $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a linear Hamming metric-preserving map, then there exists a $n \times n$ monomial matrix Q such that $f(x) = xQ$ for all x in $\mathbb{F}_q^n$.*

Then two codes $\mathcal{C}$ and $\mathcal{C}'$ are linearly equivalent if there exists a monomial matrix Q such that

$$\mathcal{C} = \{yQ \in \mathbb{F}^n \mid y \in \mathcal{C}'\}.$$

The generator matrix G of a code $\mathcal{C}$ is not unique, hence, for every invertible matrix S, the matrix SG generate the same code $\mathcal{C}$. This must be considered since we state the equivalence problem for Hamming metric codes in terms of generator matrices.

Definition 6. The *Hamming Linear Code Equivalence* ($\mathsf{CE_H}$) problem is given by

- *Input*: two codes $\mathcal{C}$ and $\mathcal{C}'$ represented by their $k \times n$ generator matrices G and G', respectively.
- *Output*: YES if there exist a $k \times k$ invertible matrix S and a $n \times n$ monomial matrix Q such that $G = SG'Q$, and NO otherwise.

The *search* version $\mathsf{sCE_H}$ is the problem of finding such matrices given two linearly equivalent codes.

Observe that the matrix S in the above definition models a possible change of basis, while the monomial matrix Q is a permutation and a scaling of the coordinates of the code.

2.3 Rank metric

In this work we consider codes in the rank metric in their matrix representation. Let n, m be positive integers, a $[n \times m, k]_q$ matrix code $\mathcal{C}$ is a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{n\times m}$ of dimension k. The rank weight of a matrix is given by $\mathrm{w_{rk}}(A) = \mathrm{rk}_{\mathbb{F}_q}(A)$. The rank distance of two elements A, B in $\mathbb{F}_q^{n\times m}$ is given by

$$\mathrm{d_{rk}}(A, B) = \mathrm{rk}_{\mathbb{F}_q}(A - B)$$

and it is, indeed, a metric.

Definition 7. An invertible map $f : \mathbb{F}_q^{n\times m} \to \mathbb{F}_q^{n\times m}$ is a *linear equivalence that preserves the rank* if it is $\mathbb{F}_q$-linear and for every A in $\mathbb{F}_q^{n\times m}$ we have

$$\mathrm{w_{rk}}(A) = \mathrm{w_{rk}}(f(A)).$$

By linearity, f preserves the rank metric and we say that f is a *linear rank metric-preserving map.*

Two matrix codes in the rank metric $\mathcal{C}$ and $\mathcal{C}'$ are *linearly equivalent* if there is a linear rank metric-preserving map f such that $\mathcal{C} = f(\mathcal{C}')$.

From [22], linear rank metric-preserving maps can be characterized.

Proposition 8. *If $f : \mathbb{F}_q^{n\times m} \to \mathbb{F}_q^{n\times m}$ is a linear rank metric-preserving maps, then there exist a $n \times n$ invertible matrix A and a $m \times m$ invertible matrix B such that*

1. *$f(W) = AWB$ for all W in $\mathbb{F}_q^{n\times m}$, or*
2. *$f(W) = AW^tB$ for all W in $\mathbb{F}_q^{n\times m}$,*

where the latter case can occur only if $n = m$.

In the literature, for example [7, 27], the linear equivalence problem for matrix codes is defined taking into account only the first case of Proposition 8, even when $n = m$. In terms of hardness this is not a problem, since considering both cases requires at most twice the time of considering only the first case, and hence, just a polynomial overhead. For simplicity, we continue the approach from [7, 27] in the following definition.

Definition 9. The *rank Linear Code Equivalence* ($\mathsf{CE_{rk}}$) problem is given by

- *Input*: two $[n \times m, s]$ matrix codes $\mathcal{C}$ and $\mathcal{C}'$ represented by their bases.
- *Output*: YES if there exist matrices A in $\mathrm{GL}_n(q)$ and B in $\mathrm{GL}_m(q)$ such that for every W in $\mathcal{C}'$ we have that AWB is in $\mathcal{C}$, and NO otherwise.

The *search* version $\mathsf{sCE_{rk}}$ is the problem of finding such matrices given two linearly equivalent codes.

3 Sum-rank Codes

A generalization of both Hamming and rank metric is the *sum-rank metric*. Consider positive integers $t, n_1, \ldots, n_t, m_1, \ldots, m_t$. A *sum-rank code* is a $\mathbb{F}_q$-linear subspace of the Cartesian product

$$\mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t}.$$

In order to define the metric on which the code is based, we define the *sum-rank function* (or weight)

$$\begin{array}{rccl} \mathrm{w}_{sr}: & \mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t} & \to & \mathbb{N} \\ & (A_1, \ldots, A_t) & \mapsto & \sum_{i=1}^t \mathrm{rk}_{\mathbb{F}_q}(A_i). \end{array}$$

The *sum-rank distance* (or metric) is given by

$$\mathrm{d}_{sr}(A, B) = \mathrm{w}_{sr}(A - B),$$

where A and B are elements of $\mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t}$, i.e. t-tuples of matrices. It can be shown that the function d_{sr} is a metric [21, Proposition 1.1].

Observe that, for $n_1 = \cdots = n_t = m_1 = \cdots = m_t = 1$, the sum-rank metric coincides with the Hamming metric and sum-rank codes can be seen as linear codes of length t in $\mathbb{F}_q^t$. For $t = 1$ we have the rank metric, and sum-rank codes are matrix codes of size $n_1 \times m_1$.

It is useful to define maps that preserve the sum-rank metric.

Definition 10. An invertible map

$$f : \mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t} \to \mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t}$$

is a *linear equivalence that preserves the sum-rank* if it is $\mathbb{F}_q$-linear and for every $(A_1, \ldots, A_t)$ in $\mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t}$ we have

$$\mathrm{w}_{sr}((A_1, \ldots, A_t)) = \mathrm{w}_{sr}(f((A_1, \ldots, A_t))).$$

By linearity, f preserves the sum-rank metric and we say that f is a *linear sum-rank metric-preserving map.*

Two codes in the sum-rank metric $\mathcal{C}$ and $\mathcal{C}'$ are *linearly equivalent* if there is a linear sum-rank metric-preserving map f such that $\mathcal{C} = f(\mathcal{C}')$.

We recall the *vector representation* of a special class of sum-rank codes over $\mathbb{F}_q$. Suppose $m = m_1 = \cdots = m_t$ and set $N = n_1 + \cdots + n_t$, fix a basis $\mathcal{B}$ for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ as vector space. We can see tuples of matrices in $\mathbb{F}_q^{m \times n_1} \times \cdots \times \mathbb{F}_q^{m \times n_t}$ as vectors in $\mathbb{F}_{q^m}^N$: a matrix C_i in $\mathbb{F}_q^{m \times n_i}$ is associated to the vector $c^{(i)}$ in $\mathbb{F}_{q^m}^{n_i}$ and we take the concatenation of such vectors

$$(c^{(1)} || c^{(2)} || \cdots || c^{(t)}).$$

This transformation is invertible and its inverse is called the *total matrix representation map* [21]:

$$M_{\mathcal{B}} : \mathbb{F}_{q^m}^N \to \mathbb{F}_q^{m \times n_1} \times \cdots \times \mathbb{F}_q^{m \times n_t}.$$

This maps induces a sum-rank weight on vectors in $\mathbb{F}_{q^m}^N$

$$\mathrm{w}_v(c_1, \ldots, c_N) = \mathrm{w}_{sr}(M_{\mathcal{B}}(c_1), \ldots, M_{\mathcal{B}}(c_N))$$

and a distance $\mathrm{d}_v(x, y) = \mathrm{w}_v(x - y)$.
It can be shown that the choice of the basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ does not affect the metric [21]. This metric depends only on the $n_1, \ldots, n_t$ and m.
Linear sum-rank metric-preserving maps for sum-rank codes in the vector representation are characterized in [21] and we report here the result.

Proposition 11. *Let $N = n_1 + \cdots + n_t$. If $f : \mathbb{F}_{q^m}^N \to \mathbb{F}_{q^m}^N$ is a linear sum-rank metric-preserving maps, then there exist*

1. $\beta_1, \dots, \beta_t$ *in* $(\mathbb{F}_{q^m})^*$,

2. $n_i \times n_i$ *invertible matrices* A_i, *for* $i = 1, \dots, t$, *and*

3. a permutation σ *in* $\mathcal{S}_t$

such that

$$f(c^{(1)}||\cdots||c^{(t)}) = (\beta_1 c^{\sigma(1)} A_1||\cdots||\beta_t c^{\sigma(t)} A_t)$$

for all $c^{(i)}$ *in* $\mathbb{F}_{q^m}^{n_i}$.

Due to this result, we can define the equivalence problem for sum-rank codes in the next section.

3.1 Generating tensors

Since a sum-rank linear code $\mathcal{C}$ is a vector subspace of $\mathbb{F}_q^{n_1 \times m_1} \times \cdots \times \mathbb{F}_q^{n_t \times m_t}$, we can choose a basis for it of the form

$$\mathcal{B} = \left\{ \left(A_1^{(1)}, \dots, A_t^{(1)} \right), \dots, \left(A_1^{(s)}, \dots, A_t^{(s)} \right) \right\},$$

where $A_u^{(v)}$ is in $\mathbb{F}_q^{n_u \times m_u}$. We can pack, for every u from 1 to t, matrices $A_u^{(1)}, \dots, A_u^{(s)}$ in a 3-tensor of side length n_u, m_u, s. This is the intuition behind the definition of generating tensor(s).

Definition 12. Let $\mathcal{C}$ be a sum-rank linear code of sizes $t, n_1, \dots, n_t, m_1, \dots, m_t$ and dimension s. A *generating t-uple of tensors* $\mathbf{G}$ is an element of the form

$$\mathbf{G} = (G_1, \dots, G_t)$$

where, for $h = 1, \dots, t$, G_h is a 3-tensor of side length n_h, m_h, s

$$G_h = (G_h)_{ijk}$$

such that the s slices $(G_h)_{ij}$ of G_h generate the projection of $\mathcal{C}$ to $\mathbb{F}_q^{n_h \times m_h}$. In other words we have

$$\mathcal{C} = \operatorname{Span} \left\{ \left((G_1)_{ij1}, \dots, (G_t)_{ij1} \right), \dots, \left((G_1)_{ijs}, \dots, (G_t)_{ijs} \right) \right\}.$$

We can see that this definition embraces the more standard concept of *generating matrix* of a Hamming code $\mathcal{C}$: whenever $n_1 = \cdots = n_t = m_1 = \cdots = m_t = 1$ we have that the 3-tensor G_h, for $h = 1, \dots, t$, has side length $1, 1, s$ and hence it is a vector. A t-tuple of vectors of length s can be rearranged in a matrix, that is a generator matrix of the code, in fact we have

$$\mathcal{C} = \operatorname{Span} \left\{ (G_{11}, \dots, G_{t1}), \dots, (G_{1s}, \dots, G_{ts}) \right\}.$$

In the case of matrix code $\mathcal{C}$ with the rank metric, we have $t = 1$. This implies that we have a 1-tuple of generating tensor $\mathbf{G} = G_{ijk}$ of side length n, m, s. In terms of vector spaces we have that the slices of $\mathbf{G}$ generates the matrix code $\mathcal{C}$:

$$\mathcal{C} = \operatorname{Span} \left\{ G_{ij1}, \dots, G_{ijs} \right\}.$$

This formulation of generating tensors is useful to convert equivalence problems in tensors and matrices problems, as we can see in the following section.

With this notation we can translate the equivalence of code into isomorphism of tensors. Observe that, in [12], the problem 3-TI is implicitly assumed to be equivalent to the *Matrix Space Equivalence* problem. The latter is a reformulation of $\mathsf{CE}_{\mathsf{rk}}$: here we give the explicit reduction between $\mathsf{CE}_{\mathsf{rk}}$ and 3-TI, proving that the former is TI-complete.

Proposition 13. *The problem* $\mathsf{CE}_{\mathsf{rk}}$ *is* TI*-complete.*

Proof. We show the TI-completeness of $\mathsf{CE}_{\mathsf{rk}}$ proving the equivalence with 3-TI.
First we show the reduction from 3-TI to $\mathsf{CE}_{\mathsf{rk}}$. Given tensors $\mathbf{G} = G_{ijk}$ and $\mathbf{G}' = G'_{ijk}$ of side length n, m, s, we ask if there exist matrices A in $\mathrm{GL}_n(q)$, B in $\mathrm{GL}_m(q)$ and C in $\mathrm{GL}_s(q)$ such that

$$G_{ijk} = \sum_{u,v,w} G'_{uvw} A_{iu} B_{jv} C_{kw}. \tag{1}$$

We can consider $\mathbf{G}$ and $\mathbf{G}'$ as generating tensors of the two matrix codes $\mathcal{C}$ and $\mathcal{C}'$: the slices of $\mathbf{G}$ and $\mathbf{G}'$ generates $\mathcal{C}$ and $\mathcal{C}'$. Suppose that they are equivalent, then there exist $\widetilde{A}, \widetilde{B}$ such that for every W in $\mathcal{C}'$, we have $\widetilde{A} W \widetilde{B}$ is in $\mathcal{C}$. Moreover, a basis for $\mathcal{C}$ is given by

$$\left\{ \widetilde{A} G'_{ij1} \widetilde{B}, \ldots, \widetilde{A} G'_{ijs} \widetilde{B} \right\}$$

and for every matrix G_{ijk}, for $k = 1, \ldots, s$, we can write it with respect to this basis:

$$\begin{aligned} G_{ijk} &= \sum_w \lambda_w^{(k)} \widetilde{A} G'_{ijw} \widetilde{B} \\ &= \sum_w \lambda_w^{(k)} \sum_{u,v} \widetilde{A}_{iu} G'_{uvw} \widetilde{B}_{vj} \\ &= \sum_{u,v,w} \widetilde{A}_{iu} G'_{uvw} \widetilde{B}_{vj} \lambda_w^{(k)} \end{aligned}$$

Setting $A = \widetilde{A}$, $B = \left(\widetilde{B}\right)^t$ and $C = (\lambda_i^{(j)})_{ij}$, we obtain exactly (1).

Now we reduce $\mathsf{CE}_{\mathsf{rk}}$ to 3-TI. Suppose $\mathcal{C}$ and $\mathcal{C}'$ are two matrix codes of dimension s and parameters n, m with generator tensors $\mathbf{G} = G_{ijk}$ and $\mathbf{G}' = G'_{ijk}$, respectively. We ask if there exist matrices $\widetilde{A}$ in $\mathrm{GL}_n(q)$ and $\widetilde{B}$ in $\mathrm{GL}_m(q)$ such that for every W in $\mathcal{C}'$, we have $\widetilde{A} W \widetilde{B} \in \mathcal{C}$. If $\mathbf{G}$ and $\mathbf{G}'$ are isomorphic as 3-tensors, then there exist A in $\mathrm{GL}_n(q)$, B in $\mathrm{GL}_m(q)$ and C in $\mathrm{GL}_s(q)$ such that

$$G_{ijk} = \sum_{u,v,w} G'_{uvw} A_{iu} B_{jv} C_{kw}. \tag{2}$$

We set $\widetilde{A} = A$ and $\widetilde{B} = B^t$, and we show that $\widetilde{A} W \widetilde{B}$ is in $\mathcal{C}$ for each W' in $\mathcal{C}'$. Write a generic W in $\mathcal{C}$ with respect to the basis $\{G_{ij1}, \ldots, G_{ijs}\}$

$$W = \sum_k \lambda_k G_{ijk},$$

then we take the linear combination of (2) with coefficients λ_k:

$$\sum_k \lambda_k G_{ijk} = \sum_k \lambda_k \sum_{u,v,w} G'_{uvw} A_{iu} B_{jv} C_{kw}.$$

Observe that on the left hand side we have W, and rearranging the terms on the right hand side we have:

$$\begin{aligned} W &= \sum_w \left(\sum_k \lambda_k C_{kw} \right) \sum_{u,v} G'_{uvw} A_{iu} B_{jv} \\ &= \sum_w \left(\sum_k \lambda_k C_{kw} \right) A G'_{ijw} B^t \end{aligned}$$

and then W is in the space spanned by $\left\{ A G'_{ij1} B^t, \ldots, A G'_{ijs} B^t \right\}$. In particular, $\mathcal{C}$ is in this subspace and then we have the thesis. $\square$

We can adapt the proof even in the case of search problem: we obtain that $\mathsf{sCE}_{\mathsf{rk}}$ and s3-TI are polynomially equivalent.
Observe that, in [27], is proven that $\mathsf{CE}_{\mathsf{rk}}$ is equivalent to the problem of deciding the equivalence of homogeneous quadratic maps hQMLE. If we combine this result with the above proposition, we have the following corollary.

Corollary 14. *The problem* hQMLE *is* TI*-complete.*

This confirms the suggestion given in [27], stating that the homogeneous instances are the hardest for the quadratic map equivalence problem.

4 Linear Equivalence Problem for Sum-Rank Codes

The problem of equivalence between sum-rank codes was introduced in 2020 by Martínez-Peñas [20]. Before stating the problem, we characterize linear sum-rank metric-preserving maps, as is done in Proposition 11 for vector representation. This characterization regards sum-rank codes in matrix representation and is a slight generalization of a result from [23, Proposition 4.25]. For the next result we fix the following notation: for any matrix A, we define $A^{[0]} = A$ and $A^{[1]} = A^t$, where the latter occurs only if A is a square matrix.

Proposition 15. *Let $f : \mathbb{F}_q^{n_1\times m_1} \times\cdots\times \mathbb{F}_q^{n_t\times m_t} \to \mathbb{F}_q^{n_1\times m_1} \times\cdots\times \mathbb{F}_q^{n_t\times m_t}$ be a linear sum-rank metric-preserving map. Then there exist a vector $(b_1,\dots,b_t)$ in $\mathbb{F}_2^t$, invertible matrices A_i in $\mathrm{GL}_{n_i}(q)$ and B_i in $\mathrm{GL}_{m_i}(q)$ for each $i = 1,\dots,t$, and a permutation σ in $\mathcal{S}_t$ such that*

$$f(W_1,\dots,W_t) = \left(A_1 W_{\sigma(1)}^{[b_1]} B_1, \dots, A_t W_{\sigma(t)}^{[b_t]} B_t\right)$$

for each $W_i \in \mathbb{F}_q^{n_i\times m_i}$. Observe that b_i can be non-zero only if $n_i = m_i$.

Proof. Let f be a linear sum-rank metric-preserving map. Assume that M is a rank-1 matrix in $\mathbb{F}_q^{n_i\times m_i}$, then

$$1 = \mathrm{w}_{sr}(0,\dots,0,M,0,\dots,0) = \mathrm{w}_{sr}(f(0,\dots,0,M,0,\dots,0))$$

If we see f as a tuple of maps to $\mathbb{F}_q^{n_i\times m_i}$, $f = (f_1,\dots,f_t)$, then there exists a unique j such that $f_j(0,\dots,0,M,0,\dots,0)$ is a rank-1 matrix and $f_k(0,\dots,0,M,0,\dots,0) = 0$ for k different from j. Then every f_i sends the vector with a rank-1 matrix and all zeros to a rank-1 matrix. We can extend this argument to matrices with rank greater than 1 and we can conclude that for each matrix M in position k, there exists an index i_k, depending only on k, such that

$$\mathrm{rk}(M) = \mathrm{w}_{sr}((0,\dots,0,M,0,\dots,0)) = \mathrm{rk}(f_{i_k}\,(0,0,M,0,0))$$

and $f_j((0,\dots,0,M,0,\dots,0) = 0$ in $\mathbb{F}_q^{n_j\times m_j}$ for every j different from i_k. In other words, f_{i_k} preserves the rank of M when it is in position k. Since we can write

$$(M_1,\dots,M_t) = (M_1,0,\dots,0) + \cdots + (0,\dots,0,M_t),$$

due to the linearity of f_{i_k}, we can conclude that

$$f_{i_k}(M_1,\dots,M_t) = f_{i_k}(0,\dots,0,M_k,0,\dots,0) \in \mathbb{F}_q^{n_{i_k}\times m_{i_k}}. \tag{3}$$

Moreover, thanks to Proposition 8, there exist b_{i_k} in $\mathbb{F}_2$, A_{i_k} in $\mathrm{GL}_{n_{i_k}}(q)$ and B_{i_k} in $\mathrm{GL}_{m_{i_k}}(q)$ such that

$$f_{i_k}(M_1,\dots,M_t) = A_{i_k} M_k^{[b_{i_k}]} B_{i_k}.$$

We define σ as the permutation in $\mathcal{S}_t$ sending i_k to k, for each i_k in $\{1,\dots,t\}$ given by (3) and this concludes the proof. □

Using the tensors formalism, we can state the linear equivalence problem for sum-rank codes. As in the case of $\mathsf{CE_{rk}}$, we choose to not include the case of transposition of matrices.

Definition 16. The *sum-rank Linear Code Equivalence* ($\mathsf{CE_{sr}}$) problem is given by

- *Input*: two sum-rank codes $\mathcal{C}$ and $\mathcal{C}'$, of sizes $t, n_1,\dots,n_t, m_1,\dots,m_t$ and dimension s represented by their generator tensors $\mathbf{G} = (G_1,\dots,G_t)$ and $\mathbf{G}' = (G_1',\dots,G_t')$, respectively.

- *Output*: YES if there exist matrices $A_1, \ldots, A_t, B_1, \ldots, B_t$, where A_i is in $\mathrm{GL}_{n_i}(q)$ and B_i is in $\mathrm{GL}_{m_i}(q)$, and a permutation σ in $\mathcal{S}_t$ such that

$$\mathcal{C} = \mathrm{Span}\left\{\left(A_1\left(G'_{\sigma(1)}\right)_{ij1}B_1, \ldots, A_t\left(G'_{\sigma(t)}\right)_{ij1}B_t\right), \ldots, \left(A_1\left(G'_{\sigma(1)}\right)_{ijs}B_1, \ldots, A_t\left(G'_{\sigma(t)}\right)_{ijs}B_t\right)\right\},$$

  and NO otherwise.

The *search* version $\mathsf{sCE}_{\mathsf{sr}}$ is the problem of finding such matrices given two linearly equivalent codes.

This formulation embraces both the previous linear equivalence problems for Hamming and rank metric as special cases.

Proposition 17. CE_{H} *and* $\mathsf{CE}_{\mathsf{rk}}$ *are particular cases of* $\mathsf{CE}_{\mathsf{sr}}$*:*

1. $\mathsf{CE}_{\mathsf{rk}}$ *is equivalent to* $\mathsf{CE}_{\mathsf{sr}}$ *for sum-rank codes with* $t = 1$*;*
2. CE_{H} *is equivalent to* $\mathsf{CE}_{\mathsf{sr}}$ *for sum-rank codes with* $n_1 = \cdots = n_t = m_1 = \cdots = m_t = 1$*.*

Moreover, both CE_{H} *and* $\mathsf{CE}_{\mathsf{rk}}$ *can be polynomially reduced to* $\mathsf{CE}_{\mathsf{sr}}$*.*

Proof. 1. For $t = 1$ we have exactly two matrix codes $\mathcal{C}$ and $\mathcal{C}'$ of parameters $[n \times m, s]_q$. Suppose that $\mathbf{G} = G_{ijk}$ generates $\mathcal{C}$ and $\mathbf{G}' = G'_{ijk}$ generates $\mathcal{C}'$ and that the two matrix codes are linearly equivalent. This is equivalent (by the definition of $\mathsf{CE}_{\mathsf{rk}}$) to the fact that there exist two invertible matrices A, B such that for every Y in $\mathcal{C}'$ we have that AYB is in $\mathcal{C}$. Equivalently, we are saying that the space spanned by $AG'_{ij1}B, \ldots, AG'_{ijs}B$ is the code $\mathcal{C}$, and this is exactly the formulation of $\mathsf{CE}_{\mathsf{sr}}$, where the permutation is taken from $\mathcal{S}_1 = \{\mathrm{id}\}$.

2. For $n_1 = \cdots = n_t = m_1 = \cdots = m_t = 1$ we have two Hamming codes $\mathcal{C}$ and $\mathcal{C}'$, generated by t 1-tensors (vectors) of side length s. Let these t-tuples of length s row vectors be $\mathbf{G} = (G_1, \ldots, G_t)$ and $\mathbf{G}' = (G'_1, \ldots, G'_t)$. If we pack them into matrices, we obtain the well-known generator matrices. Observe that the problem $\mathsf{CE}_{\mathsf{sr}}$ now can be formulated as follows: there exist $a_1, \ldots, a_t, b_1, \ldots, b_t$ in $\mathbb{F}_q^*$ and σ in $\mathcal{S}_t$ such that

$$\mathcal{C} = \mathrm{Span}\left\{\left(a_1\left(G'_{\sigma(1)}\right)_1 b_1, \ldots, a_t\left(G'_{\sigma(t)}\right)_1 b_t\right), \ldots, \left(a_1\left(G'_{\sigma(1)}\right)_s b_1, \ldots, a_t\left(G'_{\sigma(t)}\right)_s b_t\right)\right\}.$$

   We can set $c_i = a_i b_i$ and these elements are still in $\mathbb{F}_q^*$, obtaining

$$\mathcal{C} = \mathrm{Span}\left\{\left(c_1\left(G'_{\sigma(1)}\right)_1, \ldots, c_t\left(G'_{\sigma(t)}\right)_1\right), \ldots, \left(c_1\left(G'_{\sigma(1)}\right)_s, \ldots, c_t\left(G'_{\sigma(t)}\right)_s\right)\right\}$$

   and such writing is a reformulation of

$$\mathcal{C} = \mathrm{Span}\left\{v'_1 DP, \ldots, v'_s DP\right\},$$

   where $v'_i = ((G'_1)_i, \ldots, (G'_t)_i)$, P is the permutation matrix associated to σ and D is the diagonal matrix with coefficients $c_1, \ldots, c_t$. Every monomial matrix can be written as multiplication of a diagonal and a permutation matrix, then let $Q = DP$ and we obtain

$$\mathcal{C} = \mathrm{Span}\left\{v'_1 Q, \ldots, v'_s Q\right\}. \tag{4}$$

   To conclude the proof we must formulate the problem in terms of the Definition 6. Let $\mathcal{B} = \{v_1, \ldots, v_s\}$ be a basis for $\mathcal{C}$, then due to (4), also $\mathcal{B}' = \{v'_1 Q, \ldots, v'_s Q\}$ is a basis. If S is the matrix sending $\mathcal{B}'$ into $\mathcal{B}$ and we have the thesis: given generator matrices A and A' with respect to bases $\mathcal{B}$ and $\mathcal{B}'$ for $\mathcal{C}$ and $\mathcal{C}'$ respectively, there exist an invertible $s \times s$ matrix S and a monomial $t \times t$ matrix Q such that $A = SA'Q$.

$\square$

The above result is stated for decision problems but both the statements and the proofs can be adapted for the search version of such problems.
Observe that, both in [7] and [12], $\mathsf{CE_H}$ is reduced to $\mathsf{CE_{rk}}$ and this implies the statement 2 of the previous proposition. We still keep the proof given here to highlight how the definition of $\mathsf{CE_{sr}}$ and generating tensors embrace $\mathsf{CE_H}$ and $\mathsf{CE_{rk}}$.

We recall that a sum-rank code is in vector representation when it is a linear subspace of $\mathbb{F}_{q^m}^N$ with the metric d_v from Section 3. Suppose $N = n_1 + \cdots + n_t$, then for each c in $\mathbb{F}_{q^m}^N$ we write

$$c = \left(c^{(1)}||\cdots||c^{(t)}\right),$$

where every $c^{(i)}$ is in $\mathbb{F}_{q^m}^{n_i}$.
Using the characterization of linear map that preserves d_v for vector representation of sum-rank codes in [21, Theorem 1.1], we state the correspondent equivalence problem.

Definition 18. The *vector sum-rank Linear Code Equivalence* ($\mathsf{vCE_{sr}}$) problem is given by

- *Input*: two sum-rank codes $\mathcal{C}$ and $\mathcal{C}'$ in their vector representation, with parameters $t, N = n_1 + \cdots + n_t, m$ and dimension s represented by their basis $\mathbf{G} = \{v_1, \ldots, v_s\}$ and $\mathbf{G}' = \{w_1, \ldots, w_s\}$, respectively.
- *Output*: YES if there exist elements $\beta_1, \ldots, \beta_t$ in $\mathbb{F}_{q^m}^*$, invertible matrices $A_1, \ldots, A_t$, where A_i is in $\mathrm{GL}_{n_i}(q)$ and a permutation σ in $\mathcal{S}_t$ such that

$$\mathcal{C} = \mathrm{Span}\left\{\left(\beta_1 w_1^{(\sigma(1))} A_1||\cdots||\beta_t w_1^{(\sigma(t))} A_t\right), \ldots, \left(\beta_1 w_s^{(\sigma(1))} A_1||\cdots||\beta_t w_s^{(\sigma(t))} A_t\right)\right\}$$

  and NO otherwise.

The *search* version $\mathsf{svCE_{sr}}$ is the problem of finding such matrices given two linearly equivalent codes.

The next technical lemma links the equivalence problem for vector representation of sum-rank codes to matrices codes in the rank metric.

Lemma 19. *The problem* $\mathsf{vCE_{sr}}$ *can be reduced to* $\mathsf{CE_{rk}}$ *in polynomial time.*

Proof. Suppose that $\mathcal{C}$ and $\mathcal{C}'$ are two sum-rank codes in their vector representation with parameters $t, N = n_1 + \cdots + n_t, m$ and dimension s, represented by their basis $\mathbf{G} = \{v_1, \ldots, v_s\}$ and $\mathbf{G}' = \{w_1, \ldots, w_s\}$, respectively, seen as subspaces of $\mathbb{F}_{q^m}^N$.
If $\mathcal{C}$ and $\mathcal{C}'$ are equivalent, then there exist $\beta_1, \ldots, \beta_t$ in $\mathbb{F}_{q^m}^*$, invertible matrices $A_1, \ldots, A_t$, where A_i is in $\mathrm{GL}_{n_i}(q)$ and a permutation σ in $\mathcal{S}_t$ such that

$$\mathcal{C} = \mathrm{Span}\left\{\left(\beta_1 w_1^{(\sigma(1))} A_1||\cdots||\beta_t w_1^{(\sigma(t))} A_t\right), \ldots, \left(\beta_1 w_s^{(\sigma(1))} A_1||\cdots||\beta_t w_s^{(\sigma(t))} A_t\right)\right\}.$$

Fix a basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and consider the total matrix representation map

$$M_{\mathcal{B}} : \mathbb{F}_{q^m}^N \to \mathbb{F}_q^{n_1 \times m} \times \cdots \times \mathbb{F}_q^{n_t \times m}.$$

For each basis element $w_i = \left(w_1^{(1)}||\cdots||w_1^{(t)}\right)$ for $i = 1, \ldots, s$, define the $mt \times N$ matrix W_i as the block diagonal matrix having as blocks the components of $M_{\mathcal{B}}(w_i)$:

$$W_i = \begin{pmatrix} (M_{\mathcal{B}}(w_i))_1 & & \\ & \ddots & \\ & & (M_{\mathcal{B}}(w_i))_t \end{pmatrix}$$

where with $\left(M_{\mathcal{B}}(w_i)\right)_j$ we denote the j-th matrix of the tuple.
Since the multiplication by scalar λ in $\mathbb{F}_{q^m}$

$$\begin{array}{rccc} \lambda: & \mathbb{F}_{q^m} & \to & \mathbb{F}_{q^m} \\ & x & \mapsto & \lambda x \end{array}$$

is a linear map when we see $\mathbb{F}_{q^m}$ a vector space over $\mathbb{F}_q$, we can associate to it a matrix $m \times m$ matrix with coefficients in $\mathbb{F}_q$, denoted with $\mathcal{M}_{\mathcal{B}}(\lambda)$. Let $\mathbf{P}$ be the $N \times N$ block permutation matrix associated to σ, having t identities I_n blocks with respect to σ. Set

$$\mathbf{B} = \begin{pmatrix} \mathcal{M}_{\mathcal{B}}(\beta_1) & & \\ & \ddots & \\ & & \mathcal{M}_{\mathcal{B}}(\beta_t) \end{pmatrix}$$

and

$$\mathbf{A} = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_t \end{pmatrix},$$

then, the linear map f leading the equivalence between $\mathcal{C}$ and $\mathcal{C}'$ is given in the following matrix terms

$$\begin{array}{rccc} f: & \mathbb{F}_q^{mt \times N} & \to & \mathbb{F}_q^{mt \times N} \\ & C & \mapsto & \mathbf{B}C\mathbf{PA}. \end{array}$$

The problem $\mathsf{vCE}_{\mathsf{sr}}$ is equivalent to decide if there exist an invertible matrix $\mathbf{B}$ in $\mathbb{F}_q^{mt \times mt}$ and an invertible $N \times N$ matrix $\mathbf{D}$ such that $\mathcal{C}$ is the vector space generated by

$$\mathbf{B}W_1\mathbf{D}, \ldots, \mathbf{B}W_s\mathbf{D},$$

and this, if we proceed as in the proof of Proposition 17, is equivalent to $\mathsf{CE}_{\mathsf{rk}}$. □

A straightforward reduction from $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$ can be done viewing a sum-rank code of parameters $t, n_1, \ldots, n_t, m_1, \ldots, m_t$ as a vector representation of a code with parameters t, N, m, where $N = n_1 + \cdots + n_t$ and $m = \operatorname{lcm}(m_1, \ldots, m_t)$, i.e. a code with coefficients in $\mathbb{F}_{q^m}$, the smallest extension containing each field $\mathbb{F}_{q^{m_i}}$. Then, applying Lemma 19 we reduce it to $\mathsf{CE}_{\mathsf{rk}}$. Unfortunately, in the worst case this extension can be exponentially large (in t) respect to $\mathbb{F}_q$.

Theorem 20. $\mathsf{CE}_{\mathsf{sr}}$ *can be reduced to a polynomial number of instances of* $\mathsf{CE}_{\mathsf{rk}}$.

Proof. Let $\mathcal{C}$ and $\mathcal{C}'$ be two sum-rank codes of sizes $t, n_1, \ldots, n_t, m_1, \ldots, m_t$ and dimension s represented by their generator tensors $\mathbf{G} = (G_1, \ldots, G_t)$ and $\mathbf{G}' = (G'_1, \ldots, G'_t)$.
Define $\Gamma(m) = \{i \mid m_i = m\}$ and $\Gamma'(m) = \{i \mid m'_i = m\}$, where m is a positive integer. Observe that for different m, the set of indices $1, \ldots, t$ is partitioned by $\Gamma(m)$ and $\Gamma'(m)$. Let σ be a permutation in $\mathcal{S}_t$ of the equivalence, it preserves the sum-rank metric only if it acts disjointly on such sets:

$$\sigma\left(\Gamma'(m)\right) = \Gamma(m)$$

for each m. Due to this fact, we can focus on each of these sets individually, let

$$\{1, \ldots, t\} = \Gamma'_1 \sqcup \cdots \sqcup \Gamma'_h,$$

with h at most t.
If $\Gamma'(m)$ has only one element j, the image of $\sigma(j)$ is determined by the (unique) element of $\Gamma(m)$. More generally, setting $N_i = \sum_{k \in \Gamma_i} n_k$, we can see codes $\mathcal{C}$ and $\mathcal{C}'$ as Cartesian products of vector representation of sum-rank codes over $\mathbb{F}_{q^{m_i}}^{N_i}$ and using Lemma 19, we obtain the thesis: we reduced $\mathsf{CE}_{\mathsf{sr}}$ to at most t instances of $\mathsf{CE}_{\mathsf{rk}}$. □

The above theorem shows that there is a Cook reduction from $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$ and it is natural to ask if there is a tight Karp reduction. Combining Theorem 20 with Proposition 17, we obtain the following result.

Corollary 21. $\mathsf{CE}_{\mathsf{sr}}$ *and* $\mathsf{CE}_{\mathsf{rk}}$ *are polynomially equivalent. Moreover,* $\mathsf{CE}_{\mathsf{sr}}$ *is* TI*-complete.*

5 Conclusions

We showed the TI-completeness of both $\mathsf{CE}_{\mathsf{rk}}$ and $\mathsf{CE}_{\mathsf{sr}}$, using a reduction from the vector representation of sum-rank codes to matrix codes. We point out that these results can be easily translated in the setting of semi-linear equivalences, in such case we have only a polynomial overhead since semi-linear maps are a composition of linear maps with a field automorphism. An algorithm for $\mathsf{CE}_{\mathsf{rk}}$ is presented in [27], with running time $\mathcal{O}^*\left(q^{\frac{2}{3}(m+n)}\right)$ and since the reduction from $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$ is not tight, a future application can be the design of a digital signature based on the equivalence problem for sum-rank codes. Recalling considerations at the end of Subsection 2.1, we can say that the TI-hardness of $\mathsf{CE}_{\mathsf{sr}}$ is a big clue that it could be intractable even in the average case. Many isomorphism problems still resist to the Shor's quantum algorithm [31], and so they can be used in the design of post-quantum cryptographic schemes. In particular, post-quantum signatures have been built on similar assumptions on TI-complete problems, like [32] and [15].

Acknowledgments

The author is a member of the INdAM Research group GNSAGA. The author acknowledges support from TIM S.p.A. through the PhD scholarship and Alessio Meneghetti for the helpful comments regarding this work.

References

[1] Alamati, N., Feo, L.D., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 411–439. Springer (2020)

[2] Bardet, M., Otmani, A., Saeed-Taha, M.: Permutation code equivalence is not harder than graph isomorphism when hulls are trivial. In: 2019 IEEE International Symposium on Information Theory (ISIT), pp. 2464–2468. IEEE (2019)

[3] Barenghi, A., Biasse, J.F., Persichetti, E., Santini, P.: Less-fm: fine-tuning signatures from the code equivalence problem. In: International Conference on Post-Quantum Cryptography, pp. 23–43. Springer (2021)

[4] Beullens, W., Kleinjung, T., Vercauteren, F.: Csi-fish: efficient isogeny based signatures through class group computations. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 227–247. Springer (2019)

[5] Boppana, R.B., Hastad, J., Zachos, S.: Does co-np have short interactive proofs? Information Processing Letters **25**(2), 127–132 (1987)

[6] Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive (2006)

[7] Couvreur, A., Debris-Alazard, T., Gaborit, P.: On the hardness of code equivalence problems in rank metric. arXiv preprint arXiv:2011.04611 (2020)

[8] De Feo, L., Galbraith, S.D.: Seasign: compact isogeny signatures from class group actions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 759–789. Springer (2019)

[9] De Feo, L., Kohel, D., Leroux, A., Petit, C., Wesolowski, B.: Sqisign: compact post-quantum signatures from quaternions and isogenies. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 64–93. Springer (2020)

[10] Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Conference on the theory and application of cryptographic techniques, pp. 186–194. Springer (1986)

[11] Goldreich, O., Micali, S., Wigderson, A.: Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. Journal of the ACM (JACM) **38**(3), 690–728 (1991)

[12] Grochow, J.A., Qiao, Y.: Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions. arXiv preprint arXiv:1907.00309 (2019)

[13] Grochow, J.A., Qiao, Y.: On the complexity of isomorphism problems for tensors, groups, and polynomials i: Tensor isomorphism-completeness. In: 12th Innovations in Theoretical Computer Science Conference (ITCS 2021). Schloss Dagstuhl-Leibniz-Zentrum für Informatik (2021)

[14] Huffman, W.C., Pless, V.: Fundamentals of error-correcting codes. Cambridge university press (2010)

[15] Ji, Z., Qiao, Y., Song, F., Yun, A.: General linear group action on tensors: a candidate for post-quantum cryptography. In: Theory of Cryptography Conference, pp. 251–281. Springer (2019)

[16] Kobler, J., Schöning, U., Torán, J.: The graph isomorphism problem: its structural complexity. Springer Science & Business Media (2012)

[17] Leon, J.: Computing automorphism groups of error-correcting codes. IEEE Transactions on Information Theory **28**(3), 496–511 (1982)

[18] Lu, H.f., Kumar, P.V.: A unified construction of space-time codes with optimal rate-diversity tradeoff. IEEE Transactions on Information Theory **51**(5), 1709–1730 (2005)

[19] MacWilliams, F.J.: Combinatorial problems of elementary abelian groups. Ph.D. thesis (1962)

[20] Martínez-Peñas, U.: Hamming and simplex codes for the sum-rank metric. Designs, Codes and Cryptography **88**(8), 1521–1539 (2020)

[21] Martínez-Peñas, U., Shehadeh, M., Kschischang, F.R., et al.: Codes in the sum-rank metric: Fundamentals and applications. Foundations and Trends® in Communications and Information Theory **19**(5), 814–1031 (2022)

[22] Morrison, K.: Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes. IEEE Transactions on Information Theory **60**(11), 7035–7046 (2014)

[23] Neri, A.: Twisted linearized reed-solomon codes: A skew polynomial framework. arXiv preprint arXiv:2105.10451 (2021)

[24] Nóbrega, R.W., Uchôa-Filho, B.F.: Multishot codes for network coding using rank-metric codes. In: 2010 Third IEEE International Workshop on Wireless Network Coding, pp. 1–6. IEEE (2010)

[25] Patarin, J.: Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 33–48. Springer (1996)

[26] Petrank, E., Roth, R.M.: Is code equivalence easy to decide? IEEE Transactions on Information Theory **43**(5), 1602–1604 (1997)

[27] Reijnders, K., Samardjiska, S., Trimoska, M.: Hardness estimates of the code equivalence problem in the rank metric. Cryptology ePrint Archive (2022)

[28] Sendrier, N.: Finding the permutation between equivalent linear codes: The support splitting algorithm. IEEE Transactions on Information Theory **46**(4), 1193–1203 (2000)

[29] Sendrier, N., Simos, D.E.: The hardness of code equivalence over $\mathbf{F}_q$ and its application to code-based cryptography. In: International Workshop on Post-Quantum Cryptography, pp. 203–216. Springer (2013)

[30] Sendrier, N., Simos, D.E.: How easy is code equivalence over fq? In: International Workshop on Coding and Cryptography-WCC 2013 (2013)

[31] Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science, pp. 124–134. Ieee (1994)

[32] Tang, G., Duong, D.H., Joux, A., Plantard, T., Qiao, Y., Susilo, W.: Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 582–612. Springer (2022)