Monomial Isomorphism for Tensors and Applications to Code Equivalence Problems

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

Abstract

Starting from the problem of d-Tensor Isomorphism (d-TI), we study the relation between various Code Equivalence problems in different metrics. In particular, we show a reduction from the sum-rank metric ($\mathsf{CE}_{\mathsf{sr}}$) to the rank metric ($\mathsf{CE}_{\mathsf{rk}}$). To obtain this result, we investigate reductions between tensor problems. We define the *Monomial Isomorphism* problem for d-tensors (d-TI^*), where, given two d-tensors, we ask if there are $d-1$ invertible matrices and a monomial matrix sending one tensor into the other. We link this problem to the well-studied d-TI and the TI-completeness of d-TI^* is shown. Due to this result, we obtain a reduction from $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$. In the literature, a similar result was known, but it needs an additional assumption on the automorphisms of matrix codes. Since many constructions based on the hardness of Code Equivalence problems are emerging in cryptography, we analyze how such reductions can be taken into account in the design of cryptosystems based on $\mathsf{CE}_{\mathsf{sr}}$.

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

1 Introduction

Equivalence problems. An *equivalence problem* is a computational problem where, given two objects A and B of the same nature, it asks whether there exists a map with some properties (an equivalence) sending A to B. Different problems can be stated, depending on the nature of the considered objects or the properties of the map. One of the most well-known equivalence problems is *Graph Isomorphism*, but in the literature one can find problems concerning groups, quadratic forms, algebras, linear codes, tensors, and many other objects. We will focus on the latter, with the *Code Equivalence* and the *Tensor Isomorphism* problems. An interesting fact is that the isomorphism problem for tensors seems "central" among others. In particular, a large class of equivalence problems can be polynomially reduced to it.

In other words, given a pair of objects (groups, algebras, graphs, etc.), a pair of tensors can be built such that they are isomorphic if and only if the starting objects are equivalent. This led to the definition of the complexity class TI in [GQ21]. Different reductions among these problems can be found in [GQ19; GQT21; PR97; CDG20; RST22]. In general, there are no known polynomial algorithms for most of the above problems. Because of this, many public key cryptosystems base their security on the hardness of solving these kinds of problems, for example, *Isomorphism of Polynomials* [Pat96], Code Equivalence [BBPS21; CNP+22], Tensor Isomorphism [JQSY19], *Lattice Isomorphism* [DPPW23], *Trilinear Forms Equivalence* [TDJ+22], and problems from isogenies of elliptic curves [DG19; DKL+20; BKV19; DFK+23].

Code Equivalence. One of the most studied equivalence problems concerns linear codes. In the Hamming metric, the maps that generate an equivalence were classified in [Mac62], leading to the *Monomial Equivalence Problem*, which was studied in [PR97; SS13]. Worth mentioning is the Support Splitting Algorithm [Sen00], which solves the above problem in *average* polynomial time for a large class of codes. For a detailed analysis, the interested reader can refer to [BBPS23]. Recently, the problem of equivalence in different metrics has been studied, and we will focus on the rank metric and the sum-rank one. Concerning the rank metric, the classification of equivalence maps is given in [Mor14], while in [CDG20], the authors analyze the *Matrix Code Equivalence*, and they reduce the Hamming case to it. The same result is given in an independent work [GQ19], where the former problem is called *Matrix Space Equivalence*. In [RST22], it is shown that Matrix Code Equivalence is polynomially equivalent to problems on bilinear and quadratic maps. Moreover, the link between the rank and the sum-rank metric is studied, leading to a reduction from the latter to the former in a special case. Here we extend this analysis, finding an unconditional reduction from the code equivalence in the sum-rank metric to the rank one.

Our contribution and techniques. In this work, we give two results of different nature. The first one concerns some relations between tensors problems. The *d-Tensor Isomorphism Problem* (d-TI) asks, given two d-tensors T_1 and T_2, if there are d invertible matrices $A_1, \dots, A_d$ sending T_1 to T_2. We introduce another problem called *d-Tensor Monomial Isomorphism Problem* (d-TI^*), where instead of having d invertible matrices, we require that one of them must be monomial. We show that d-TI^* reduces to 3-TI for every $d \geq 4$. To show this, we use techniques from [CDG20] where the authors exhibit a reduction from Monomial Code Equivalence to Matrix Code Equivalence. We reformulate this reduction in terms of tensors, and we generalize it in higher dimensions. In particular, we show that d-TI^* is reducible to $(2d-1)$-TI, and then, using a result from [GQ19], we get as corollary that d-TI^* reduces to 3-TI. Observe that techniques from [GQ19] can be adapted and used as well, but they are less efficient in terms of output dimension, since the reduction is looser with respect to the one given in [CDG20].
Another contribution is about the sum-rank code equivalence. Using the result from above, we reduce the problem of deciding whether two sum-rank codes are equivalent to the problem of deciding if two matrix codes are equivalent. Note that a similar result is given in [RST22] with the assumption that some automorphisms group are of a given form. While such hypothesis is mostly satisfied for randomly

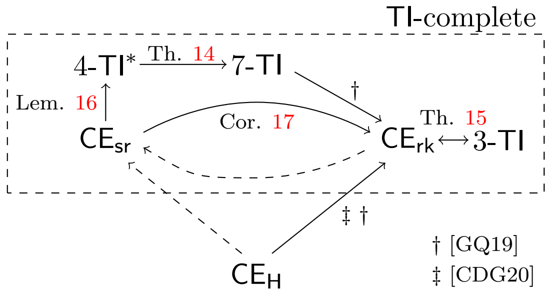

Figure 1: Reduction between problems and TI-completeness. "A → B" indicates that A reduces to B. Dashed arrows denote trivial reductions.

generated matrix codes (for example the ones used in Cryptography [CNP+22]), here we give an unconditional reduction. Unfortunately, our reduction produces matrix codes with dimension and sizes that are polynomially bigger than the starting parameters of the sum-rank codes. In particular, we get a $\mathcal{O}(x^6)$ overhead. Due to this result, we can conclude that for the three considered metrics (Hamming, rank, sum-rank), Code Equivalence problems are in the class TI. Figure 1 summarizes new and known reductions between code equivalence and other problems, showing the route we used.
This work is organized as follows. In Section 2 we give some preliminaries on tensors, linear codes and equivalence problems in different metrics. Section 3 introduces the Monomial Isomorphism problem for tensors and a proof of the TI-hardness is given. Section 4 concerns the proof that the Code Equivalence problem in the sum-rank metric can be reduced to the same problem in the rank metric. We use this reduction to make some observations in the use of such problems in Cryptography, as we see in Section 5.

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 $\mathrm{GL}(n, \mathbb{F}_q)$ be the group of invertible $n \times n$ matrices with coefficients in $\mathbb{F}_q$. When the field is implicit, we use $\mathrm{GL}(n)$ instead. 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. The group of $n \times n$ monomial matrices over the field $\mathbb{F}_q$ is denoted with $\mathrm{Mon}(n, \mathbb{F}_q)$ or $\mathrm{Mon}(n)$, and is a subgroup of $\mathrm{GL}(n)$. We denote with $\mathbb{W}_1 \oplus \mathbb{W}_2$ the direct sum of vector spaces $\mathbb{W}_1$ and $\mathbb{W}_2$ and its elements are written as (w_1, w_2), where w_i is in $\mathbb{W}_i$. With $\mathcal{S}_t$ we denote the symmetric group over a set of t elements. The transpose of a matrix A is denoted with A^t and I_ℓ denotes the $\ell \times \ell$ identity matrix. Through this work we will use the "big-O" notation $\mathcal{O}(\cdot)$.

2.1 Tensors

Given a positive integer d, a d-tensor over $\mathbb{F}_q$ is an element of the tensor space $\bigotimes_{i=1}^{d} \mathbb{F}_q^{n_i}$. If we fix the bases $\{e_1^{(i)}, \ldots, e_{n_i}^{(i)}\}$ for every linear space $\mathbb{F}_q^{n_i}$, we can represent a d-tensor T with respect to its coefficients $T(i_1, \ldots, i_d)$ in $\mathbb{F}_q$

$$T = \sum_{i_1,\ldots,i_d} T(i_1, \ldots, i_d) e_{i_1}^{(1)} \otimes \cdots \otimes e_{i_d}^{(d)}.$$

We say that T has size $n_1 \times \ldots \times n_d$. For example, observe that 1-tensors and 2-tensors can be represented as vectors and matrices, respectively.

A *rank one* (or *decomposable*) tensor is an element of the form $a_1 \otimes \cdots \otimes a_d$, where a_i is in $\mathbb{F}_q^{n_i}$. Given a d-tensor T, its *rank* is the minimal non-negative integer r such that there exist $t_1, \ldots, t_r$ rank one tensors for which $T = \sum_{i=1}^{r} t_i$. In general, computing the rank of a d-tensor is an hard task for $d \geq 3$ [Hås89; SŠ18; Shi16].

The projection to a can be defined for any a in $\mathbb{F}_q^{n_j}$. Since we are interested mainly in projections to an element of the base $e_k^{(j)}$ of $\mathbb{F}_q^{n_j}$, we define

$$\begin{aligned}\mathrm{proj}_{e_k^{(j)}} : &\mathbb{F}_q^{n_1} \otimes \ldots \otimes \mathbb{F}_q^{n_j} \otimes \ldots \otimes \mathbb{F}_q^{n_d} \to \mathbb{F}_q^{n_1} \otimes \ldots \otimes \mathbb{F}_q^{n_{j-1}} \otimes \mathbb{F}_q^{n_{j+1}} \otimes \ldots \otimes \mathbb{F}_q^{n_d}, \\ &\sum_{i_1,\ldots,i_d} T(i_1, \ldots, i_d) e_{i_1}^{(1)} \otimes \cdots \otimes e_{i_d}^{(d)} \\ &\mapsto \sum_{\substack{i_1,\ldots,i_{j-1},\\ i_{j+1},\ldots,i_d}} T(i_1, \ldots, i_{j-1}, k, i_{j+1}, \ldots, i_d) e_{i_1}^{(1)} \otimes \cdots \otimes e_{i_{j-1}}^{(j-1)} \otimes e_{i_{j+1}}^{(j+1)} \otimes \cdots \otimes e_{i_d}^{(d)}.\end{aligned} \tag{1}$$

In other words, we send to zero every component of $\sum_{i_1,\ldots,i_d} T(i_1, \ldots, i_d) e_{i_1}^{(1)} \otimes \cdots \otimes e_{i_d}^{(d)}$ which does not contain $e_k^{(j)}$, obtaining a $(d-1)$-tensor.

A group action can be defined on the vector space $\mathcal{T} = \bigotimes_{i=1}^{d} \mathbb{F}_q^{n_i}$ of d-tensors of size from the Cartesian product of invertible matrices $G = \mathrm{GL}(n_1) \times \ldots \times \mathrm{GL}(n_d)$ as follows

$$\begin{aligned}\star : &G \times \mathcal{T} \to \mathcal{T}, \\ &\left((A_1, \ldots, A_d), \sum_{i_1,\ldots,i_d} T(i_1, \ldots, i_d) e_{i_1}^{(1)} \otimes \cdots \otimes e_{i_d}^{(d)} \right) \\ &\quad \mapsto \sum_{i_1,\ldots,i_d} T(i_1, \ldots, i_d) A_1 e_{i_1}^{(1)} \otimes \cdots \otimes A_d e_{i_d}^{(d)}.\end{aligned}$$

It can be shown that the action defined above does not change the rank of a tensor [1]. In particular, this implies that the action of an element in $\mathrm{GL}(n_1) \times \ldots \times \mathrm{GL}(n_{i-1}) \times \mathrm{GL}(n_{i+1}) \times \ldots \times \mathrm{GL}(n_d)$ on the projection $\mathrm{proj}_{e_k^{(j)}}(T)$ of a tensor T has the same rank of T. We summarize these properties in formulas

1. $\mathrm{rk}\left((A_1, \ldots, A_d) \star T\right) = \mathrm{rk}\,(T)$,

[1] However, if we extend the action to non-invertible matrices, this property does not hold: the zero matrix sends every tensor into the zero tensor (which has rank zero by definition).

2. $\mathrm{rk}\left((A_1,\ldots,A_{i-1},A_{i+1},\ldots,A_d)\star\mathrm{proj}_{e_k^{(j)}}(T)\right)=\mathrm{rk}\left(\mathrm{proj}_{e_k^{(j)}}(T)\right)$.

The isomorphism problem between tensors has some interesting links and properties in computational complexity theory. Here we recall the formal definition of the problem.

Definition 1. The *d-Tensor Isomorphism* (d-TI) problem is given by

- *input*: two d-tensors T_1 and T_2 in $\bigotimes_{i=1}^d \mathbb{F}_q^{n_i}$;
- *output*: YES if there exists an element g of $\mathrm{GL}(n_1)\times\ldots\times\mathrm{GL}(n_d)$ such that $T_2 = g\star T_1$ and NO otherwise.

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

If we recall the decision problems *d-Colourability* (d-COL) and d-SAT, it is known that the first integer for which these problems are NP-complete is $d=3$. In particular, there are polynomial reductions from d-COL to 3-COL and from d-SAT to 3-SAT. The same happens for d-TI and 3-TI, as shown in the following astonishing result from [GQ19].

Theorem 2. *d-TI and 3-TI are polynomially equivalent.*

Since a lot of different problems can be reduced to d-TI, in the same flavor of the complexity class GI (the set of problems reducible in polynomial time to Graph Isomorphism [KST12]), the authors of [GQ21] define the TI class.

Definition 3. The *Tensor Isomorphism* class (TI) contains decision problems that can be polynomially 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 Graph Non-Isomorphism [GMW91] and Code Non-Equivalence [PR97] 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 [BHZ87].

2.2 Linear codes in different metrics

A *linear code* $\mathcal{C}$ of dimension k is a linear space of dimension k. A linear code can be embedded in different linear spaces $\mathbb{V}$ over $\mathbb{F}_q$, depending on the form of the code. A code is endowed with a map *weight* w defined on $\mathbb{V}$

$$\mathrm{w}:\mathbb{V}\to\mathbb{N}$$

such that $\mathrm{w}(x)=0$ if and only if $x=0$. We can define a metric d from a weight w

$$\mathrm{d}:\mathbb{V}\times\mathbb{V}\to\mathbb{N},\ (x,y)\mapsto \mathrm{w}(y-x).$$

Thought this paper, we will consider three weights with their metrics. We highlight that, even if we can endow the same code with two or more different metrics, we consider a code with just a metric.

The first one is the *Hamming* weight. Here we consider linear codes embedded in $\mathbb{F}_q^n$, and we say that the code $\mathcal{C}$ has length n. This weight is defined as the number of non-zero entries of a vector:

$$\mathrm{w_H} : \mathbb{F}_q^n \to \mathbb{N},\ (x_1, \dots, x_n) \mapsto |\{i \mid x_i \neq 0\}|.$$

We refer to the distance induced by $\mathrm{w_H}$ as $\mathrm{d_H}$. A useful representation of a k-dimensional code $\mathcal{C}$ of length n in the Hamming metric is given by its *generator matrix*, a $k \times n$ matrix having a base $\{v_1, \dots, v_k\}$ of $\mathcal{C}$ as rows. Notice that the generator matrix is not unique since there are many bases for the same linear code.

The second weight we consider is defined on matrices. This means that our code $\mathcal{C}$ is a space of matrices and usually we refer to it as a *matrix code*. If we consider $n \times m$ matrices, the code has *length* $n \times m$. The map

$$\mathrm{w_R} : \mathbb{F}_q^{n\times m} \to \mathbb{N},\ M \mapsto \mathrm{rk}(M)$$

is defined as the rank of the matrix M. Hence, the distance $\mathrm{d_R}$ between M_1 and M_2 is given by the rank of $M_2 - M_1$.

The last class of codes we consider is embedded into the direct sum (or Cartesian product) of spaces of matrices. Given natural numbers $d, n_1, \dots, n_d, m_1, \dots, m_d$, we have that the linear space $\mathbb{V}$ defined above is $\mathbb{F}_q^{n_1\times m_1} \oplus \dots \oplus \mathbb{F}_q^{n_d\times m_d}$. We can define the *Sum-rank* weight as the sum of the ranks

$$\begin{array}{rccl} \mathrm{w_{SR}} : & \mathbb{F}_q^{n_1\times m_1} \oplus \dots \oplus \mathbb{F}_q^{n_d\times m_d} & \to & \mathbb{N}, \\ & (M_1, \dots, M_d) & \mapsto & \sum_{i=1}^d \mathrm{rk}\,(M_i)\,. \end{array}$$

The distance $\mathrm{d_{SR}}$ induced by $\mathrm{w_{SR}}$ is called *sum-rank metric* and we call a code endowed with this distance a *sum-rank code* of parameters $d, n_1, \dots, n_d, m_1, \dots, m_d$.

Observe that the sum-rank metric is both a generalization of the Hamming and the rank distance. For $n_1 = \dots = n_d = m_1 = \dots = m_d = 1$, the sum-rank metric coincides with the Hamming metric, and sum-rank codes can be seen as linear codes of length d in $\mathbb{F}_q^d$. If we have $d = 1$, then $\mathrm{d_{SR}}$ is the rank metric, and sum-rank codes are matrix codes of size $n_1 \times m_1$.

2.3 Code Equivalence

We recall the general problem of deciding whether two linear codes are equivalent. Given a weight w and a metric d, we say that an invertible linear map f from the vector space $\mathbb{V}$ to itself preserves the metric (or, equivalentely, the weight) if $f(\mathrm{w}(x)) = \mathrm{w}(x)$ for every x in $\mathbb{V}$. We call such maps *linear isometries*, and they form a group with the composition. Two linear codes are *linearly equivalent* if there exists a linear isometry between them. The task of checking if two codes are equivalent is called *Linear Code Equivalence Problem*. Since in the rest of the paper we will consider only linear isometries, sometimes we drop the word "linear" when we talk about isometries or equivalences, in particular we refer to the problem above as *Code Equivalence* (CE). Its hardness depends on which codes and metric we consider. In the following, we define CE with respect to the three different metrics we saw in Subsection 2.2.

We can characterize linear isometries in the Hamming metric, reporting a well-known result from [Mac62].

Proposition 4. *If $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a linear isometry in the Hamming metric, 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 $\mathcal{D}$ are linearly equivalent if there exists a monomial matrix Q such that

$$\mathcal{C} = \left\{ yQ \in \mathbb{F}_q^n \mid y \in \mathcal{D} \right\}.$$

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

Definition 5. The *Hamming Linear Code Equivalence* (CE_H) problem is given by

- *input*: two codes $\mathcal{C}$ and $\mathcal{D}$ 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 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 base, while the monomial matrix Q is a permutation and a scaling of the coordinates of the code.

Now we consider the rank metric. From [Mor14], linear isometries for the rank metric can be characterized as follows.

Proposition 6. *If $f : \mathbb{F}_q^{n\times m} \to \mathbb{F}_q^{n\times m}$ is a linear isometry in the rank metric, then there exist a $n \times n$ invertible matrix A and a $m \times m$ invertible matrix B such that*

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

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

Usually, an isometry can be denoted with a pair of matrices (A, B).

In the literature, for example [CDG20; RST22], the linear equivalence problem for matrix codes is defined taking into account only the first case given in Proposition 6, even when we have $n = m$. In terms of the computational effort to solve the problem, this is not an issue, since considering both cases requires at most twice the time of considering only the first one, and hence, just a polynomial overhead that we can ignore. For simplicity, we continue the approach from [CDG20; RST22] in the following definition.

Definition 7. The *rank Linear Code Equivalence* (CE_rk) problem is given by

- *input*: two $n \times m$ matrix codes $\mathcal{C}$ and $\mathcal{D}$ of dimension s represented by their bases;
- *output*: YES if there exist matrices A in $\mathrm{GL}(n)$ and B in $\mathrm{GL}(m)$ such that, for every M in $\mathcal{D}$, we have that AMB is in $\mathcal{C}$, and NO otherwise.

The *search* version is the problem of finding such matrices given two linearly equivalent codes.

In the literature, this problem is also called *Matrix Code Equivalence* (MCE).

Given a matrix code $\mathcal{C}$, an *automorphism* of $\mathcal{C}$ is a linear isometry f such that $f(\mathcal{C}) = \mathcal{C}$. We say that $\mathcal{C}$ has *trivial automorphisms* if the only automorphisms of $\mathcal{C}$ are of the form $M \mapsto (\lambda I_n)\, M\, (\mu I_m)$ for some non-zero λ, μ in $\mathbb{F}_q$.

The equivalence problem between sum-rank codes was introduced in 2020 by Martínez-Peñas [Mar20]. Before stating the problem, we characterize linear sum-rank isometries. This result is given in [CGL+22] and a slightly less general statement can be found in [Ner22, Proposition 4.26].

Proposition 8. *Let $f : \mathbb{F}_q^{n_1\times m_1} \oplus \cdots \oplus \mathbb{F}_q^{n_d\times m_d} \to \mathbb{F}_q^{n_1\times m_1} \oplus \cdots \oplus \mathbb{F}_q^{n_d\times m_d}$ be a linear isometry in the sum-rank metric. Then there exists a permutation σ in $\mathcal{S}_d$ such that $n_i = n_{\sigma(i)}$ and $m_i = m_{\sigma(i)}$ for every i, and there exist $\psi_i : \mathbb{F}_q^{n_i\times m_i} \to \mathbb{F}_q^{n_i\times m_i}$ isometries in the rank metric such that*

$$f(M_1, \ldots, M_d) = \big(\psi_1(M_{\sigma(1)}), \ldots, \psi_d(M_{\sigma(d)})\big)$$

for each $M_i \in \mathbb{F}_q^{n_i\times m_i}$.

We are ready to state the linear equivalence problem for sum-rank codes. As in the case of $\mathsf{CE}_{\mathsf{rk}}$, we choose to not include the case of transposition of matrices. Recall that, as linear space, a sum-rank code $\mathcal{C}$ of parameters $d, n_1, \ldots, n_d, m_1, \ldots, m_d$ and dimension k admits a base of the form $\{\mathbf{C}_1, \ldots, \mathbf{C}_k\}$ where $\mathbf{C}_i = \left(C_i^{(1)}, \ldots, C_i^{(d)}\right)$ is a tuple of matrices. In particular, $C_i^{(j)}$ is in $\mathbb{F}_q^{n_j\times m_j}$ for each i and j.

Definition 9. The *sum-rank Linear Code Equivalence* ($\mathsf{CE}_{\mathsf{sr}}$) problem is given by

- *input*: two sum-rank codes $\mathcal{C}$ and $\mathcal{D}$, of parameters $d, n_1, \ldots, n_d, m_1, \ldots, m_d$ and dimension k represented by their bases $\{\mathbf{C}_i\}$ and $\{\mathbf{D}_i\}$, respectively;
- *output*: YES if there exist matrices $A_1, \ldots, A_d, B_1, \ldots, B_d$, where A_i is in $\mathrm{GL}(n_i)$ and B_i is in $\mathrm{GL}(m_i)$, and a permutation σ in $\mathcal{S}_d$ such that

$$\mathcal{C} = \mathrm{Span}\Big\{\Big(A_1 D_1^{(\sigma(1))} B_1, \ldots, A_d D_1^{(\sigma(d))} B_d\Big), \ldots, \Big(A_1 D_k^{(\sigma(1))} B_1, \ldots, A_d D_k^{(\sigma(d))} B_d\Big)\Big\},$$

  and NO otherwise.

The *search* version 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. Due to this, we can formulate the next result.

Proposition 10. *Both CE_{H} and $\mathsf{CE}_{\mathsf{rk}}$ polynomially reduce to $\mathsf{CE}_{\mathsf{sr}}$.*

A natural question is about the converse, whether problems in the Hamming or the sum-rank metric reduce to $\mathsf{CE}_{\mathsf{rk}}$. It has been show independently in [CDG20] and [GQ19] that CE_{H} can be reduced to $\mathsf{CE}_{\mathsf{rk}}$, using two different approaches. In [GQ19, Section 5], the reduction uses 3-tensors via an "individualization" argument to force a matrix to be monomial. In [CDG20], given a linear code of dimension k in $\mathbb{F}_q^n$, the reduction defines a matrix code in $\mathbb{F}_q^{k\times(k+n)}$. This approach will be generalized in the setting of d-tensors in the following section, and it will give us some reductions between tensors problem in dimensions higher than 3.

3 Monomial Isomorphism Problems

In this section, we will examine the relationship between tensors isomorphism problems when a matrix acting on a specific space is required to be monomial instead of using the action from the entire group $\mathrm{GL}(n_1) \times \cdots \times \mathrm{GL}(n_d)$. Specifically, there exists a j such that the action on the j-th space is given by $\mathrm{Mon}(n_j)$. For simplicity, we will refer to this special space as the last one throughout the remainder of the article and in the problems statements. Since $\mathrm{Mon}(n_d)$ is a subgroup of $\mathrm{GL}(n_d)$, the action of the group $\mathrm{GL}(n_1) \times \cdots \times \mathrm{GL}(n_{d-1}) \times \mathrm{Mon}(n_d)$ on d-tensors is well-defined. When there exists an element g sending the d-tensor T_1 into T_2, we say that they are *monomially isomorphic*.

Definition 11. The *Monomial d-Tensor Isomorphism* (d-TI^*) problem is given by

- *input*: two d-tensors T_1 and T_2 in $\bigotimes_{i=1}^d \mathbb{F}_q^{n_i}$;
- *output*: YES if there exists an element g of $\mathrm{GL}(n_1)\times\cdots\times\mathrm{GL}(n_{d-1})\times\mathrm{Mon}(n_d)$ such that $T_2 = g \star T_1$ and NO otherwise.

The *search* version is the problem of finding such matrices, given two monomially isomorphic d-tensors.

We recall that, if the action of the monomial matrix is not on the last vector space, we can permute the spaces to obtain the problem above. Observe that the problem 2-TI^* is exactly $\mathsf{CE_H}$ and the proof that $\mathsf{CE_H}$ reduces to $\mathsf{CE_{rk}}$ from [CDG20] can be viewed as a reduction from 2-TI^* to 3-TI. In the following, we generalize this approach to reduce d-TI^* to $(2d-1)$-TI.

For simplicity, we show the result when $d = 4$, but it can be easily generalized for any d (see the paragraph before Theorem 14). This choice is supported by the fact that it is the first case where some technical details get involved and, moreover, it models our applications in Section 4.

Let $\mathbb{A}, \mathbb{B}, \mathbb{C}, \mathbb{D}$ be vector spaces over $\mathbb{F}_q$ of dimension $n_1, \ldots, n_4$, respectively. Now let $\{a_i\}_i, \{b_i\}_i, \{c_i\}_i, \{d_i\}_i$ bases of the above spaces. We recall that $\mathbb{W}_1 \oplus \mathbb{W}_2$ is the direct sum of vector spaces $\mathbb{W}_1$ and $\mathbb{W}_2$ and its elements are of the form (w_1, w_2). The action of an element of $\mathrm{GL}(\dim(\mathbb{W}_1) + \dim(\mathbb{W}_2))$ is block-by-block:

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} A_{11}w_1 + A_{12}w_2 \\ A_{21}w_1 + A_{22}w_2 \end{pmatrix}.$$

The reduction used in our result is the following map, going from a space of 4-tensors to a space of 7-tensors,

$$\begin{aligned}
\Psi :&\mathbb{A} \otimes \mathbb{B} \otimes \mathbb{C} \otimes \mathbb{D} \to \mathbb{A} \otimes \mathbb{B} \otimes \mathbb{C} \otimes (\mathbb{A} \oplus \mathbb{D}) \otimes (\mathbb{B} \oplus \mathbb{D}) \otimes (\mathbb{C} \oplus \mathbb{D}) \otimes \mathbb{D}, \\
&\sum_{i_1,\ldots,i_4} T(i_1,\ldots,i_4) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes d_{i_4} \\
&\mapsto \sum_{\substack{i_1,\ldots,i_4,\\ j_1,\ldots,j_3}} T(i_1,\ldots,i_4) T(j_1,j_2,j_3,i_4) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (a_{j_1},0) \otimes (b_{j_2},0) \otimes (c_{j_3},0) \otimes d_{i_4} \\
&+ \sum_{i_1,\ldots,i_4} T(i_1,\ldots,i_4) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (0,d_{i_4}) \otimes (0,d_{i_4}) \otimes (0,d_{i_4}) \otimes d_{i_4}.
\end{aligned} \tag{2}$$

In the following, we show that two tensors T_1 and T_2 are monomially isomorphic if and only if $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic.

Proposition 12. *If T_1 and T_2 are two monomially isomorphic 4-tensors, then $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic as 7-tensors.*

Proof. Suppose that T_1 and T_2 are in $\mathbb{A}\otimes\mathbb{B}\otimes\mathbb{C}\otimes\mathbb{D}$ as defined above. Now, since T_1 and T_2 are monomially isomorphic, there exist invertible matrices L, R, S and a monomial matrix Q such that $(L, R, S, Q)\star T_1 = T_2$. Let Q be the product of the diagonal matrix $D = \mathrm{diag}(\alpha_1, \dots, \alpha_{n_4})$ and the permutation matrix P corresponding to the permutation σ in $\mathcal{S}_{n_4}$. More explicitly

$$\sum_{i_1,\dots,i_4} T_1(i_1, \dots, i_4) La_{i_1}\otimes Rb_{i_2}\otimes Sc_{i_3}\otimes\alpha_{i_4} d_{\sigma(i_4)} = \sum_{i_1,\dots,i_4} T_2(i_1, \dots, i_4) a_{i_1}\otimes b_{i_2}\otimes c_{i_3}\otimes d_{i_4}. \tag{3}$$

Our claim to obtain the thesis is that $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1) = \Psi(T_2)$, where

$$\tilde{L} = \begin{pmatrix} L & 0 \\ 0 & P \end{pmatrix}, \quad \tilde{R} = \begin{pmatrix} R & 0 \\ 0 & P \end{pmatrix}, \quad \tilde{S} = \begin{pmatrix} S & 0 \\ 0 & D^{-1}P \end{pmatrix}, \quad \text{and} \quad \tilde{Q} = D^2 P$$

Consider T_2, and, for a k in $\{1, \dots, n_4\}$, we write its projection to d_k

$$\mathrm{proj}_{d_k}(T_2) = \sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}. \tag{4}$$

Combining Eq. (3) and Eq. (4), we have

$$\sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1}\otimes b_{i_2}\otimes c_{i_3} = \sum_{i_1,i_2,i_3} \alpha_{\sigma^{-1}(k)} T_1(i_1, i_2, i_3, \sigma^{-1}(k)) La_{i_1}\otimes Rb_{i_2}\otimes Sc_{i_3} \tag{5}$$

We define ι to be the canonic injection of $\mathbb{A}\otimes\mathbb{B}\otimes\mathbb{C}$ into $(\mathbb{A}\oplus\mathbb{D})\otimes(\mathbb{B}\oplus\mathbb{D})\otimes(\mathbb{C}\oplus\mathbb{D})$, and we consider $\mathrm{proj}_{d_k}(T_2) \otimes \iota\left(\mathrm{proj}_{d_k}(T_2)\right)$, that is

$$\sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes \sum_{j_1,j_2,j_3} T_2(j_1, j_2, j_3, k)(a_{j_1}, 0) \otimes (b_{j_2}, 0) \otimes (c_{j_3}, 0)$$

and from Eq. (5), it is equal to

$$\begin{aligned} \sum_{i_1,i_2,i_3,j_1,j_2,j_3} & \alpha^2_{\sigma^{-1}(k)} T_1(i_1, i_2, i_3, \sigma^{-1}(k)) T_1(j_1, j_2, j_3, \sigma^{-1}(k)) \\ & La_{i_1} \otimes Rb_{i_2} \otimes Sc_{i_3} \otimes (La_{j_1}, 0) \otimes (Rb_{j_2}, 0) \otimes (Sc_{j_3}, 0). \end{aligned} \tag{6}$$

Observe that, if we tensorize this element with b_k and we take the sum over $k = 1, \dots, n_4$, we have the first term of $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1)$, that is equal to the first term of T_2. To complete the proof we compute the second term of $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1)$, and we show that it is equal to the second one of T_2. In fact

$$\begin{aligned} \sum_{i_4}\sum_{i_1,i_2,i_3} & T_1(i_1, \dots, i_4) La_{i_1} \otimes Rb_{i_2} \otimes Sc_{i_3} \\ & \otimes (0, d_{\sigma(i_4)}) \otimes (0, d_{\sigma(i_4)}) \otimes (0, \alpha_{i_4}^{-1} d_{\sigma(i_4)}) \otimes \alpha_{i_4}^2 d_{\sigma(i_4)} = \\ \sum_{i_4}\sum_{i_1,i_2,i_3} & T_2(i_1, \dots, i_4) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (0, d_{i_4}) \otimes (0, d_{i_4}) \otimes (0, d_{i_4}) \otimes d_{i_4}, \end{aligned} \tag{7}$$

where the equality comes from Eq. (5).
The first and the second terms of $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1)$ are equal to the ones of $\Psi(T_2)$, and we can conclude that $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1) = \Psi(T_2)$. To complete the proof we observe that matrices $\tilde{L}, \tilde{R}, \tilde{S}$ and $\tilde{Q}$ are invertible by construction, hence $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic as 7-tensors. □

Now we show the converse.

Proposition 13. *If $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic, then T_1 and T_2 are monomially isomorphic.*

Proof. Since $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic, there exist seven invertible matrices such that $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1) = \Psi(T_2)$. We want to exhibit three invertible matrices L', R', S' and a monomial matrix Q' such that $(L', R', S', Q') \star T_1 = T_2$. In particular, we will show that $L' = L$, $R' = R$ and $S' = S$. First, we claim that $\tilde{Q}$ is a monomial matrix. Consider $(I_{n_1}, I_{n_2}, I_{n_3}, I_{n_1+n_4}, I_{n_2+n_4}, I_{n_3+n_4}, \tilde{Q}) \star \Psi(T_1)$

$$\sum_{\substack{i_1,\dots,i_4,\\ j_1,\dots,j_3}} T_1(i_1,\dots,i_4)T_1(j_1,j_2,j_3,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (a_{j_1},0) \otimes (b_{j_2},0) \otimes (c_{j_3},0) \otimes \tilde{Q}d_{i_4}$$
$$+ \sum_{i_1,\dots,i_4} T_1(i_1,\dots,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (0,d_{i_4}) \otimes (0,d_{i_4}) \otimes (0,d_{i_4}) \otimes \tilde{Q}d_{i_4} \tag{8}$$

and, after explicating $\tilde{Q}d_{i_4} = \sum_{j=1}^{n_4} \tilde{Q}_{j,i_4} d_j$, project to d_k along the last space $\mathbb{D}$

$$\sum_{\substack{i_1,\dots,i_4,\\ j_1,\dots,j_3}} \tilde{Q}_{i_4,k}T_1(i_1,\dots,i_4)T_1(j_1,j_2,j_3,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (a_{j_1},0) \otimes (b_{j_2},0) \otimes (c_{j_3},0)$$
$$+ \sum_{i_1,\dots,i_4} \tilde{Q}_{i_4,k}T_1(i_1,\dots,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes (0,d_{i_4}) \otimes (0,d_{i_4}) \otimes (0,d_{i_4}). \tag{9}$$

Now consider Eq. (9) as a 2-tensor in $\Big(\mathbb{A}\otimes\mathbb{B}\otimes\mathbb{C}\Big)\otimes\Big((\mathbb{A}\oplus\mathbb{D})\otimes(\mathbb{B}\oplus\mathbb{D})\otimes(\mathbb{C}\oplus\mathbb{D})\Big)$. With this new view, we obtain

$$\sum_{i_4} \tilde{Q}_{i_4,k}\left[\left(\sum_{i_1,i_2,i_3} T_1(i_1,\dots,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3}\right) \otimes \left(\sum_{j_1,\dots,j_4} T_1(j_1,\dots,j_4)(a_{j_1},0) \otimes (b_{j_2},0) \otimes (c_{j_3},0)\right)\right]$$
$$+ \sum_{i_4} \tilde{Q}_{i_4,k}\left(\sum_{i_1,i_2,i_3} T_1(i_1,\dots,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3}\right) \otimes \Big((0,d_{i_4}) \otimes (0,d_{i_4}) \otimes (0,d_{i_4})\Big) =$$
$$\sum_{i_4} \tilde{Q}_{i_4,k}\left[\left(\sum_{i_1,i_2,i_3} T_1(i_1,\dots,i_4)a_{i_1} \otimes b_{i_2} \otimes c_{i_3}\right)\otimes\right.$$
$$\left.\left(\sum_{j_1,\dots,j_4} T_1(j_1,\dots,j_4)(a_{j_1},0) \otimes (b_{j_2},0) \otimes (c_{j_3},0) + \Big((0,d_{i_4}) \otimes (0,d_{i_4}) \otimes (0,d_{i_4})\Big)\right)\right], \tag{10}$$

having rank equal to the number of non-zero elements of $\tilde{Q}_{\cdot,k}$, the k-th column of the matrix $\tilde{Q}$. Now consider the action of $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, I_{n_4})$ on this tensor: the rank remains the same. If we repeat this process for $\Psi(T_2)$, we obtain the following rank-1 tensor in $\Big(\mathbb{A} \otimes \mathbb{B} \otimes \mathbb{C}\Big) \otimes \Big((\mathbb{A} \oplus \mathbb{D}) \otimes (\mathbb{B} \oplus \mathbb{D}) \otimes (\mathbb{C} \oplus \mathbb{D})\Big)$

$$\left(\sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}\right) \otimes \\ \left(\sum_{j_1,j_2,j_3} T_2(j_1, j_2, j_3, k)(a_{j_1}, 0) \otimes (b_{j_2}, 0) \otimes (c_{j_3}, 0) + (0, d_k) \otimes (0, d_k) \otimes (0, d_k)\right). \tag{11}$$

From the equality of the ranks, $\tilde{Q}_{\cdot,k}$ must have exactly a non-zero element for each k, and hence, $\tilde{Q}$ is a monomial matrix of the form DP, where $D = \mathrm{diag}(\alpha_1, \dots, \alpha_{n_4})$ is a diagonal matrix and P is a permutation matrix corresponding to the permutation σ in $\mathcal{S}_{n_4}$.

Without loss of generality, suppose that the permutation σ of the monomial matrix $\tilde{Q}$ is the identity. This avoid the use of σ on the index of d_{i_4}. Consider again $\Psi(T_2)$ and its projection to d_k along $\mathbb{D}$ as in Eq. (11). We project on elements of the base of $(\mathbb{A} \oplus \mathbb{D}) \otimes (\mathbb{B} \oplus \mathbb{D}) \otimes (\mathbb{C} \oplus \mathbb{D})$. For elements of the form $(a_{\ell_1}, 0) \otimes (b_{\ell_b}, 0) \otimes (c_{\ell_3}, 0)$ we get

$$\mathrm{proj}_{(a_{\ell_1},0)\otimes(b_{\ell_b},0)\otimes(c_{\ell_3},0)} \left(\mathrm{proj}_{d_k}(\Psi(T_2))\right) = \\ T_2(\ell_1, \ell_2, \ell_3, k) \sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}. \tag{12}$$

In particular, it is a multiple of $\sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}$ for every choice of ℓ_1, ℓ_2, ℓ_3. When we consider elements different from $(a_{\ell_1}, 0) \otimes (b_{\ell_b}, 0) \otimes (c_{\ell_3}, 0)$, the projection is always zero, except for the case $(0, d_k) \otimes (0, d_k) \otimes (0, d_k)$

$$\mathrm{proj}_{(0,d_k)\otimes(0,d_k)\otimes(0,d_k)} \left(\mathrm{proj}_{d_k}(\Psi(T_2))\right) = \\ \sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}. \tag{13}$$

Hence, every projection of $\mathrm{proj}_{d_k}(\Psi(T_2))$ is a multiple of $\sum_{i_1,i_2,i_3} T_2(i_1, i_2, i_3, k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3}$ and the linear space V_k generated by all the projections is generated by the 3-tensor in Eq. (13). Consider now the projection to d_k of $(L, R, S, \tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Psi(T_1)$, that is the 3-tensor

$$\alpha_k \left(\sum_{i_1,i_2,i_3} T_1(i_1, i_2, i_3, k) L a_{i_1} \otimes R b_{i_2} \otimes S c_{i_3}\right) \otimes \\ \left(\sum_{j_1,j_2,j_3} T_1(j_1, j_2, j_3, k) \tilde{L}(a_{j_1}, 0) \otimes \tilde{R}(b_{j_2}, 0) \otimes \tilde{S}(c_{j_3}, 0) + \right. \\ \left.\left(\tilde{L}(0, d_k) \otimes \tilde{R}(0, d_k) \otimes \tilde{S}(0, d_k)\right)\right). \tag{14}$$

Again, if we project to any element of the base of $(\mathbb{A} \oplus \mathbb{D}) \otimes (\mathbb{B} \oplus \mathbb{D}) \otimes (\mathbb{C} \oplus \mathbb{D})$, we obtain a multiple of the 3-tensor

$$\alpha_k \sum_{i_1,i_2,i_3} T_1(i_1,i_2,i_3,k) La_{i_1} \otimes Rb_{i_2} \otimes Sc_{i_3}. \tag{15}$$

By hypothesis, the space generated by these projections is equal to V_k, the space generated by the same projections of $\Psi(T_2)$, that can be written as

$$V_k = \langle \sum_{i_1,i_2,i_3} T_2(i_1,i_2,i_3,k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \rangle = \langle \alpha_k \sum_{i_1,i_2,i_3} T_1(i_1,i_2,i_3,k) La_{i_1} \otimes Rb_{i_2} \otimes Sc_{i_3} \rangle.$$

Hence there exists a non-zero λ_k in $\mathbb{F}_q$ such that

$$\sum_{i_1,i_2,i_3} T_2(i_1,i_2,i_3,k) a_{i_1} \otimes b_{i_2} \otimes c_{i_3} = \lambda_k \alpha_k \sum_{i_1,i_2,i_3} T_1(i_1,i_2,i_3,k) La_{i_1} \otimes Rb_{i_2} \otimes Sc_{i_3}. \tag{16}$$

Tensorizing Eq. (16) with d_k and taking the sum on k, we have that T_1 and T_2 are monomially isomorphic via (L, R, S, Q'), where $Q' = D'P$ with $D' = \mathrm{diag}(\lambda_1\alpha_1, \ldots, \lambda_{n_4}\alpha_{n_4})$, and hence we have the thesis. □

On the generalization to $d \geq 4$. Instead of having $\mathbb{A} \otimes \mathbb{B} \otimes \mathbb{C} \otimes \mathbb{D}$, we have the d-tuple of spaces $\mathbb{V}_1 \otimes \ldots \otimes \mathbb{V}_d$. The monomial matrix acts on the last one. The map Ψ from Eq. (2) can be easily generalized, from $\mathbb{V}_1 \otimes \ldots \otimes \mathbb{V}_d$ to $\mathbb{V}_1 \otimes \ldots \otimes \mathbb{V}_{d-1} \otimes (\mathbb{V}_1 \oplus \mathbb{V}_d) \otimes \ldots \otimes (\mathbb{V}_{d-1} \oplus \mathbb{V}_d) \oplus \mathbb{V}_d$. The proof of Proposition 12 follows as the case $d = 4$. Concerning Proposition 13, we have that $\Psi(T_1)$ and $\Psi(T_2)$ are isomorphic via $A_1, \ldots, A_{2d-1}$. We show that the last matrix A_{2d-1} is monomial: to see this we project to an element d_j of the base of $\mathbb{V}_d$ and we consider the resulting $(2(d-1))$-tensor as a 2-tensor in

$$(\mathbb{V}_1 \otimes \ldots \otimes \mathbb{V}_{d-1}) \otimes ((\mathbb{V}_1 \oplus \mathbb{V}_d) \otimes \ldots \otimes (\mathbb{V}_{d-1} \oplus \mathbb{V}_d)).$$

The rank of the projection to d_j of $(A_1, \ldots, A_{2d-1}) \star \Psi(T_1)$ as a 2-tensor is equal to the number of nonzero elements in the j-th column of A_{2d-1}. Since the rank of the same projection of $\Psi(T_2)$ is 1, we can conclude that every column of A_{2d-1} has exactly a non-zero element, hence the matrix is monomial. The rest of the proof follows the case $d = 4$, where, instead of having 3-tensors, we use the same argument for $(d-1)$-tensors and we can find the monomial isomorphism from T_1 to T_2.

The combination of Proposition 12 and Proposition 13 gives us the main result of this section.

Theorem 14. *The problem d-TI^* polynomially reduces to $(2d-1)$-TI. Moreover, d-TI^* is TI-complete.*

Let us analyze the sizes of the reduction Ψ. It takes a d tensor of size $n_1 \times \ldots \times n_d$ and returns a $(2d-1)$-tensor of size $n_1 \times \ldots \times n_{d-1} \times (n_1 + n_d) \times \ldots \times (n_{d-1} + n_d) \times n_d$. We will use this reduction to link Code Equivalence problems in the following section, but this result could be of independent interest and shows how powerful is the TI class [GQ21]. In particular, Theorem 14 proves that for every d, d-TI^* is in the class TI. Moreover, a trivial reduction can be found from d-TI to $(d+1)$-TI^* (send T to $T \otimes 1$), hence for $d \geq 4$ we have that d-TI^* is TI-complete.

4 Relations between Code Equivalence Problems

In this section, we show how to reduce the code equivalence problem for sum-rank code to the one in the rank metric. A reduction is given in [RST22], but it assumes that the automorphism group of the obtained rank code is trivial in the sense of Subsection 2.3. We recall the technique from [RST22], and we observe how this kind of reduction (sending a tuple of elements of $\mathbb{F}_q^m$ to a block-diagonal matrix) does not work without the trivial automorphisms assumptions.

Let $\mathcal{C}$ be a sum-rank code with base $\{\mathbf{C}_1, \dots, \mathbf{C}_k\}$, where $\mathbf{C}_i = \left(C_i^{(1)}, \dots, C_i^{(d)}\right)$ is a tuple of matrices. We denote with Φ the map from the set of sum-rank codes to the set of matrix codes used in [RST22]

$$\Phi\left(\langle \mathbf{C}_1, \dots, \mathbf{C}_k \rangle\right) = \langle W_1, \dots, W_k \rangle,$$

where W_i is the $(\sum_i n_i) \times (\sum_i n_i)$ block diagonal matrix with the elements of $\mathbf{C}_i$ on the diagonal. We show that if the automorphisms group of the image of Φ is not trivial, then, given an isometry in the rank metric, we cannot retrieve an isometry in the sum-rank setting since the two codes are not equivalent.

Example 1. Consider the field $\mathbb{F}_2$ and the one-dimensional sum-rank codes $\mathcal{C}$ and $\mathcal{D}$ with parameters $d = 2, n_1 = 3, n_2 = 2, m_1 = m_2 = 2$ generated by

$$C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad D_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively. It can be seen that $\mathcal{C}$ and $\mathcal{D}$ are not equivalent since there is not any sum-rank isometry between them: the permutation must be the identity since $n_1 \neq n_2$ and do not exist invertible matrices (A, B) in $\mathrm{GL}(3) \times \mathrm{GL}(2)$ such that AC_1B is in the space generated by D_1 (just look at their ranks). However, if we consider $\Phi(\mathcal{C})$ and $\Phi(\mathcal{D})$, we obtain the two one-dimensional matrix codes generated by

$$C' = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \quad \text{and} \quad D' = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right),$$

respectively. We can see that $\Phi(\mathcal{C})$ and $\Phi(\mathcal{D})$ are equivalent via the isometry given by permutation matrices P_σ and P_τ, where $\sigma = (2\ 4)$ is in $\mathcal{S}_5$ and $\tau = (2\ 3)$ is in $\mathcal{S}_4$. In fact, $P_\sigma C' P_\tau = D'$. This happens since the automorphisms groups of $\Phi(\mathcal{C})$ and $\Phi(\mathcal{D})$ are not trivial. For example, for $\Phi(\mathcal{C})$ it contains the isometry $(P_{(4\ 5)}, P_{(3\ 4)})$, where $(4\ 5)$ and $(3\ 4)$ are permutations in $\mathcal{S}_5$ and $\mathcal{S}_4$, respectively.

The 3-TI problem is equivalent to the Code Equivalence in the rank metric $\mathsf{CE}_{\mathsf{rk}}$ since the former can be stated in terms of matrix spaces, and the admissible maps between these spaces are exactly the isometries used for $\mathsf{CE}_{\mathsf{rk}}$ (see [GQ19]). A sketch of the reduction is the following. To a matrix code $\mathcal{C}$ generated by $C_1, \dots, C_k$ we associate the 3-tensor in the space $\mathbb{A} \otimes \mathbb{B} \otimes \mathbb{C}$

$$T_{\mathcal{C}} = \sum_{i_1, i_2, i_3} (C_{i_3})_{i_1, i_2}\, a_{i_1} \otimes b_{i_2} \otimes c_{i_3}.$$

In particular, $\mathbb{A}$ and $\mathbb{B}$ represent the spaces of rows and columns, respectively, while $\mathbb{C}$ is the space representing the dimension of the code (or the elements in the base). Hence, a matrix can be represented as a 2-tensor in $\mathbb{A}\otimes\mathbb{B}$, and the action $(A, B)\star M$ is the matrix multiplication AMB^t. The action regarding $\mathbb{C}$ is the map sending a k-uple of matrices into another k-uple. Therefore, given two matrix codes $\mathcal{C}$ and $\mathcal{D}$, with bases $C_1, \dots, C_k$ and $D_1, \dots, D_k$, equivalent via (A, B) and such that the invertible matrix M sends the base $AC_1B, \dots, AC_kB$ to $D_1, \dots, D_k$, the tensors $T_{\mathcal{C}}$ and $T_{\mathcal{D}}$ are isomorphic via (A, B^t, M). The vice versa is obtained similarly and we highlight that there is no overhead in the sizes of tensors and matrix spaces obtained in both directions.

Hence, we can resume the above observation in the following result.

Theorem 15. *The problem* $\mathsf{CE}_{\mathsf{rk}}$ *is* TI*-complete.*

By the TI-hardness of $\mathsf{CE}_{\mathsf{rk}}$ and since it can be reduced to $\mathsf{CE}_{\mathsf{sr}}$, we get that $\mathsf{CE}_{\mathsf{sr}}$ is TI-hard. If we want to show its TI-completeness, we need to prove that it is in TI, presenting a reduction from a TI-complete problem, for instance 4-TI^*.

Lemma 16. *The problem* $\mathsf{CE}_{\mathsf{sr}}$ *is polynomially reducible to* 4-TI^**.*

Proof. We model a sum-rank code as a 4-tensor. Given a sum-rank code $\mathcal{C}$ with parameters $d, n_1, \dots, n_d, m_1, \dots, m_d$ and base $\{\mathbf{C}_1, \dots, \mathbf{C}_k\}$, let N be the maximum among $n_1, \dots, n_d$ and M be the maximum among $m_1, \dots, m_d$. For each i from 1 to d, we can embed a $n_i \times m_i$ matrix into a $N \times M$ one, filling it with zeros. Hence, there are d embeddings g_i such that

$$g_i : \mathbb{F}_q^{n_i \times m_i} \to \mathbb{F}_q^{N \times M}.$$

In the rest of the proof, we consider sum-rank codes embedded via the functions g_i, this means that we work with codes having parameters $d, n_i = N, m_i = M$ for every $i = 1, \dots, d$. Let $\mathfrak{SR}(d, N, M)$ be the set of sum-rank codes of parameters $d, n_i = N, m_i = M$ and let $\mathbb{A}, \mathbb{B}, \mathbb{C}, \mathbb{D}$ be vector spaces of dimension N, M, k, d with bases $\{a_i\}_i$, $\{b_i\}_i$, $\{c_i\}_i$ and $\{d_i\}_i$, respectively. Here, $\mathbb{A}$ and $\mathbb{B}$ denotes the row and column spaces of the matrices, $\mathbb{C}$ denotes the dimension of the code, while $\mathbb{D}$ models the factors of the sum-rank code. Hence, the code generated by $\{\mathbf{C}_1, \dots, \mathbf{C}_k\}$ can be seen as the 4-tensor

$$\sum_{i_1,\dots,i_4} \left(C_{i_3}^{(i_4)}\right)_{i_1,i_2} a_{i_1} \otimes b_{i_2} \otimes c_{i_3} \otimes d_{i_4}.$$

The projection to a factor $\mathbb{F}_q^{n_j \times m_j}$ is a matrix code, which can be seen as the 3-tensor

$$\sum_{i_1,i_2,i_3} \left(C_{i_3}^{(j)}\right)_{i_1,i_2} a_{i_1} \otimes b_{i_2} \otimes c_{i_3},$$

where the action of (A, B, M) is intended as the left-right multiplication for A and B^t, while M is a change of base.

Let $\delta_{i,j}$ be the Kronecker's delta and define the map

$$
\begin{aligned}
\Phi :& \mathfrak{S}\mathfrak{R}(d, N, M) \to \left(\bigoplus_{i=1}^{d} \mathbb{A}\right) \otimes \left(\bigoplus_{i=1}^{d} \mathbb{B}\right) \otimes \left(\bigoplus_{i=1}^{d} \mathbb{C}\right) \otimes \mathbb{D}, \\
&\{\mathbf{C}_1, \dots, \mathbf{C}_k\} \\
&\mapsto \sum_{i_1,\dots,i_4} \left(C_{i_3}^{(i_4)}\right)_{i_1,i_2} (\delta_{i_4,1} a_{i_1}, \dots, \delta_{i_4,d} a_{i_1}) \\
&\otimes (\delta_{i_4,1} b_{i_2}, \dots, \delta_{i_4,d} b_{i_2}) \otimes (\delta_{i_4,1} c_{i_3}, \dots, \delta_{i_4,d} c_{i_3}) \otimes d_{i_4}.
\end{aligned} \tag{17}
$$

Now we show that sum-rank codes $\mathcal{C}$ and $\mathcal{D}$, with bases $\{\mathbf{C}_1, \dots, \mathbf{C}_k\}$ and $\{\mathbf{D}_1, \dots, \mathbf{D}_k\}$, are equivalent if and only if $\Phi(\mathcal{C})$ and $\Phi(\mathcal{D})$ are monomially isomorphic.

" $\Longrightarrow$ ". Suppose that $\mathcal{C}$ and $\mathcal{D}$ are linear equivalent via the matrices $A_1, \dots, A_d$, $B_1, \dots, B_d$ and the permutation σ in $\mathcal{S}_d$. Suppose that, for every i, M_i is the $k \times k$ invertible matrix sending the base $\{A_i C_j^{(\sigma(i))} B_i\}_j$ to the base $\{D_j^{(i)}\}_j$. Then we define the matrices

$$
\tilde{L} = \begin{pmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_d \end{pmatrix}, \quad \tilde{R} = \begin{pmatrix} B_1^t & 0 & \dots & 0 \\ 0 & B_2^t & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B_d^t \end{pmatrix},
$$

$$
\tilde{S} = \begin{pmatrix} M_1 & 0 & \dots & 0 \\ 0 & M_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M_d \end{pmatrix}, \quad \text{and} \quad \tilde{Q} = P_\sigma.
$$

We can see that $(\tilde{L}, \tilde{R}, \tilde{S}, \tilde{Q}) \star \Phi(\mathcal{C}) = \Phi(\mathcal{D})$, in fact

$$
\begin{aligned}
&\sum_{i_1,\dots,i_4} \left(C_{i_3}^{(i_4)}\right)_{i_1,i_2} (0, \dots, A_{i_1} a_{i_1}, \dots, 0) \\
&\otimes (0, \dots, B_{i_2} b_{i_2}, \dots, 0) \otimes (0, \dots, M_{i_3} c_{i_3}, \dots, 0) \otimes d_{\sigma(i_4)},
\end{aligned} \tag{18}
$$

and this, by construction, is exactly $\Phi(\mathcal{D})$.

" $\Longleftarrow$ ". Suppose that $\Phi(\mathcal{C})$ and $\Phi(\mathcal{D})$ are monomially isomorphic via invertible matrices L, R, S and the monomial matrix $Q = DP$. We can see matrices L, R and S as block matrices, for example, we have

$$
L = \begin{pmatrix} L_{11} & \dots & L_{1d} \\ L_{21} & \dots & L_{2d} \\ \vdots & \ddots & \vdots \\ L_{d1} & \dots & L_{dd} \end{pmatrix},
$$

where L_{ij} is a $n_1 \times n_1$ matrix for every i and j. Analogously, R and S have the same structure, with blocks of dimension $n_2 \times n_2$ and $n_3 \times n_3$, respectively. Now, for simplicity, we will focus on the action of L on $\Phi(\mathcal{C})$, but the same argument can be used for R and S. As in the proof of Proposition 13, we assume that the matrix

Q is the identity matrix, otherwise we need take care of the permutation σ in the indexes and the scalars of D. We write $\mathrm{proj}_{d_k}\left((L,R,S,Q)\star\Phi(\mathcal{C})\right)$

$$\begin{aligned}&\sum_{i_1,i_2,i_3}\left(C^{(k)}_{i_3}\right)_{i_1,i_2}(L_{1k}a_{i_1},\dots,L_{dk}a_{i_1})\\&\otimes(R_{1k}b_{i_2},\dots,R_{dk}b_{i_2})\otimes(S_{1k}c_{i_3},\dots,S_{dk}c_{i_3}).\end{aligned}\tag{19}$$

Consider the same projection of $\Phi(\mathcal{D})$

$$\sum_{i_1,i_2,i_3}\left(D^{(k)}_{i_3}\right)_{i_1,i_2}(0,\dots,a_{i_1},\dots,0)\otimes(0,\dots,b_{i_2},\dots,0)\otimes(0,\dots,c_{i_3},\dots,0),\tag{20}$$

this tensor is equal to the one of Eq. (19), and this holds for every k. Now consider the tensor

$$v^{(k)}_{\ell_2,\ell_3}=(0,\dots,\underbrace{b_{\ell_2}}_{k\text{-th}},\dots,0)\otimes(0,\dots,\underbrace{c_{\ell_3}}_{k\text{-th}},\dots,0).$$

The projection to $v^{(k)}_{\ell_2,\ell_3}$ of $\mathrm{proj}_{d_k}(\Phi(\mathcal{D}))$ is given by

$$\sum_{i_1}\left(D^{(k)}_{\ell_3}\right)_{i_1,\ell_2}(0,\dots,a_{i_1},\dots,0),\tag{21}$$

while, for $(L,R,S,Q)\star\Phi(\mathcal{C})$, we have

$$\sum_{i_1,i_2,i_3}(R_{kk})_{\ell_2,i_2}(S_{kk})_{\ell_3,i_3}\left(C^{(k)}_{i_3}\right)_{i_1,i_2}(L_{1k}a_{i_1},\dots,L_{dk}a_{i_1}).\tag{22}$$

By hypothesis, Eq. (21) and Eq. (22) are equal. Then, for $\bar{k}\neq k$, we have that $L_{\bar{k}k}=0$. We can use the same argument for R and S, using the following tensors and projection to them

$$(0,\dots,\underbrace{a_{\ell_1}}_{k\text{-th}},\dots,0)\otimes(0,\dots,\underbrace{c_{\ell_3}}_{k\text{-th}},\dots,0)\ ;$$
$$(0,\dots,\underbrace{a_{\ell_1}}_{k\text{-th}},\dots,0)\otimes(0,\dots,\underbrace{b_{\ell_2}}_{k\text{-th}},\dots,0).$$

Finally, we obtain that L, R and S are block diagonal of the form

$$L=\begin{pmatrix}L_{11}&0&\dots&0\\0&L_{22}&\dots&0\\\vdots&&\ddots&\vdots\\0&\dots&0&L_{dd}\end{pmatrix},\qquad R=\begin{pmatrix}R_{11}&0&\dots&0\\0&R_{22}&\dots&0\\\vdots&&\ddots&\vdots\\0&\dots&0&R_{dd}\end{pmatrix},$$
$$\text{and}\quad S=\begin{pmatrix}S_{11}&0&\dots&0\\0&S_{22}&\dots&0\\\vdots&&\ddots&\vdots\\0&\dots&0&S_{dd}\end{pmatrix}.$$

Since the matrices L, R and S are invertible, so are the matrices on their diagonal. We can conclude that codes $\mathcal{C}$ and $\mathcal{D}$ are equivalent via matrices $L_{11},\dots,L_{dd}$, $R^t_{11},\dots,R^t_{dd}$ and the permutation σ. □

Now we can use the result above, combined with Theorem 2 and Theorem 15 to obtain the following corollary.

Corollary 17. *The problem* $\mathsf{CE}_{\mathsf{sr}}$ *is* TI*-complete. In particular, it is polynomially reducible to* $\mathsf{CE}_{\mathsf{rk}}$.

A "proof" of the above result can be seen in Figure 1, showing the path of the reduction from $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$.

5 Applications to Cryptography

Sigma protocols and digital signatures. From an hard equivalence problem, one can design a sigma protocol in the same flavor of the one given in [GMW91] for Graph Isomorphism. Assume that the group G acts on the set X, and given a public element x_0 in X, the secret key is a random g in G, while the public key is the action of g on x_0. Given a security parameter λ, we obtain a sigma protocol with a commitment long $\lambda\ell_X$, a challenge of λ bits and a response long $\lambda\ell_G$, where ℓ_X and ℓ_G are the bit-lengths of an element in X and G, respectively. To obtain a digital signature, the Fiat-Shamir transform [FS86] is applied, producing a signature of $\lambda + \lambda\ell_G$ bits. Many signatures have been built with this technique. For example, the following two constructions use the code equivalence problem. *LESS* [BBPS21] is obtained starting from the CE_{H} problem on linear codes in the Hamming weight. In the same flavor, *MEDS* [CNP+22] uses the assumed hardness of $\mathsf{CE}_{\mathsf{rk}}$ to design a signature on matrix codes. Both works use some optimizations to obtain small keys and/or small signatures. This is a preparatory work for the study of a digital signature based on the Code Equivalence for sum-rank codes. We reduced $\mathsf{CE}_{\mathsf{sr}}$ to $\mathsf{CE}_{\mathsf{rk}}$, and we seen that the former is TI-complete: these are clues that $\mathsf{CE}_{\mathsf{sr}}$ could be hard to solve. To enrich our analysis, since the proposed reductions generate a grow in the code parameters, in the following paragraph we estimate this overhead. This is useful since a possible way to solve $\mathsf{CE}_{\mathsf{sr}}$ can be the following: given an instance consisting in two sum-rank codes $\mathcal{C}$ and $\mathcal{D}$, reduce it to an instance of $\mathsf{CE}_{\mathsf{rk}}$ and solve this problem. This leads to a solution of the original problem, saying whether $\mathcal{C}$ and $\mathcal{D}$ are equivalent. Since (non-polynomial) algorithms to solve $\mathsf{CE}_{\mathsf{rk}}$ are known [CNP+22; RST22], we estimates the dimensions of the obtained matrix codes.

About dimensions. In order to understand the hardness of $\mathsf{CE}_{\mathsf{sr}}$ and a possible use in cryptography, we estimate the size of the codes obtained from the reduction in Corollary 17. Given a sum-rank code of dimension k with parameters $d, n_1, \dots, n_d, m_1, \dots, m_d$, using Lemma 16, we obtain a 4-tensor of size $dN \times dM \times dk \times d$, where $N = \max_i\{n_i\}$ and $M = \max_i\{m_i\}$. From this, by Theorem 14, we get a 7-tensor of size $dN \times dM \times dk \times (dN + d) \times (dM + d) \times (dk + d) \times d$. Finally, using reductions from Theorem 2 and Theorem 15, we obtain a matrix code of dimension and size

$$\mathcal{O}\left(49d^6\left(\max\{N, M, k\} + 1\right)^6\right) \times \mathcal{O}\left(49d^6\left(\max\{N, M, k\} + 1\right)^6\right). \tag{23}$$

These numbers comes mainly from the overhead in the reduction given in [GQ19, Th. B], in fact to reduce d-TI to 3-TI, if we start with a $n_1 \times \ldots \times n_d$ tensor, we obtain a 3-tensor of sizes $\mathcal{O}(d^2n^{d-1}) \times \mathcal{O}(d^2n^{d-1}) \times \mathcal{O}(d^2n^{d-1})$, where $n = \max_i\{n_i\}$.

In Eq. (23), we left the constant 49 in the big-O notation to give a glance on the overhead of the obtained matrix code.

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. The author thanks Antonio J. Di Scala and Joshua A. Grochow for discussions on this work.

References

[BBPS21] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini, "LESS-FM: fine-tuning signatures from the code equivalence problem," in *International Conference on Post-Quantum Cryptography*, Springer, 2021, pp. 23–43 (cit. on pp. 2, 18).

[BBPS23] ——, "On the computational hardness of the code equivalence problem in cryptography," *Advances in Mathematics of Communications*, vol. 17, no. 1, pp. 23–55, 2023 (cit. on p. 2).

[BHZ87] R. B. Boppana, J. Hastad, and S. Zachos, "Does co-NP have short interactive proofs?" *Information Processing Letters*, vol. 25, no. 2, pp. 127–132, 1987 (cit. on p. 5).

[BKV19] W. Beullens, T. Kleinjung, and F. Vercauteren, "CSI-FiSh: efficient isogeny based signatures through class group computations," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2019, pp. 227–247 (cit. on p. 2).

[CDG20] A. Couvreur, T. Debris-Alazard, and P. Gaborit, "On the hardness of code equivalence problems in rank metric," *arXiv preprint arXiv:2011.04611*, 2020 (cit. on pp. 2, 3, 7–9).

[CGL+22] E. Camps-Moreno, E. Gorla, C. Landolina, E. L. Garcıéa, U. Martıénez-Peñas, and F. Salizzoni, "Optimal anticodes, MSRD codes, and generalized weights in the sum-rank metric," *IEEE Transactions on Information Theory*, vol. 68, no. 6, pp. 3806–3822, 2022 (cit. on p. 8).

[CNP+22] T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska, "Take your MEDS: Digital Signatures from Matrix Code Equivalence," *Cryptology ePrint Archive*, 2022 (cit. on pp. 2, 3, 18).

[DFK+23] L. De Feo, T. B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny, and B. Wesolowski, "SCALLOP: scaling the CSI-FiSh," *Cryptology ePrint Archive*, 2023 (cit. on p. 2).

[DG19] L. De Feo and S. D. Galbraith, "SeaSign: compact isogeny signatures from class group actions," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2019, pp. 759–789 (cit. on p. 2).

[DKL+20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, "SQISign: compact post-quantum signatures from quaternions and isogenies," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2020, pp. 64–93 (cit. on p. 2).

[DPPW23] L. Ducas, E. W. Postlethwaite, L. N. Pulles, and W. v. Woerden, "Hawk: Module LIP makes lattice signatures fast, compact and simple," in *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*, Springer, 2023, pp. 65–94 (cit. on p. 2).

[FS86] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Conference on the theory and application of cryptographic techniques*, Springer, 1986, pp. 186–194 (cit. on p. 18).

[GMW91] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM (JACM)*, vol. 38, no. 3, pp. 690–728, 1991 (cit. on pp. 5, 18).

[GQ19] J. A. Grochow and Y. Qiao, "Isomorphism problems for tensors, groups, and cubic forms: Completeness and reductions," *arXiv preprint arXiv:1907.00309*, 2019 (cit. on pp. 2, 3, 5, 8, 14, 18).

[GQ21] ——, "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 (cit. on pp. 2, 5, 13).

[GQT21] J. A. Grochow, Y. Qiao, and G. Tang, "Average-Case Algorithms for Testing Isomorphism of Polynomials, Algebras, and Multilinear Forms," in *38th International Symposium on Theoretical Aspects of Computer Science*, 2021 (cit. on p. 2).

[Hås89] J. Håstad, "Tensor rank is NP-complete," in *International Colloquium on Automata, Languages, and Programming*, Springer, 1989, pp. 451–460 (cit. on p. 4).

[JQSY19] Z. Ji, Y. Qiao, F. Song, and A. Yun, "General linear group action on tensors: A candidate for post-quantum cryptography," in *Theory of Cryptography Conference*, Springer, 2019, pp. 251–281 (cit. on p. 2).

[KST12] J. Kobler, U. Schöning, and J. Torán, *The graph isomorphism problem: its structural complexity*. Springer Science & Business Media, 2012 (cit. on p. 5).

[Mac62] F. J. MacWilliams, "Combinatorial problems of elementary abelian groups," PhD thesis, 1962 (cit. on pp. 2, 6).

[Mar20] U. Martıénez-Peñas, "Hamming and simplex codes for the sum-rank metric," *Designs, Codes and Cryptography*, vol. 88, no. 8, pp. 1521–1539, 2020 (cit. on p. 8).

[Mor14] K. Morrison, "Equivalence for rank-metric and matrix codes and automorphism groups of Gabidulin codes," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 7035–7046, 2014 (cit. on pp. 2, 7).

[Ner22] A. Neri, "Twisted linearized Reed-Solomon codes: A skew polynomial framework," *Journal of Algebra*, vol. 609, pp. 792–839, 2022 (cit. on p. 8).

[Pat96] J. Patarin, "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*, Springer, 1996, pp. 33–48 (cit. on p. 2).

[PR97] E. Petrank and R. M. Roth, "Is code equivalence easy to decide?" *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1602–1604, 1997 (cit. on pp. 2, 5).

[RST22] K. Reijnders, S. Samardjiska, and M. Trimoska, "Hardness estimates of the Code Equivalence Problem in the Rank Metric," *Cryptology ePrint Archive*, 2022 (cit. on pp. 2, 7, 14, 18).

[Sen00] N. Sendrier, "Finding the permutation between equivalent linear codes: The support splitting algorithm," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1193–1203, 2000 (cit. on p. 2).

[Shi16] Y. Shitov, "How hard is the tensor rank?" *arXiv preprint arXiv:1611.01559*, 2016 (cit. on p. 4).

[SS13] N. Sendrier and D. E. Simos, "The Hardness of Code Equivalence over F_q and Its Application to Code-Based Cryptography," in *Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings 5*, Springer, 2013, pp. 203–216 (cit. on p. 2).

[SŠ18] M. Schaefer and D. Štefankovič, "The complexity of tensor rank," *Theory of Computing Systems*, vol. 62, no. 5, pp. 1161–1174, 2018 (cit. on p. 4).

[TDJ+22] G. Tang, D. H. Duong, A. Joux, T. Plantard, Y. Qiao, and W. Susilo, "Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2022, pp. 582–612 (cit. on p. 2).