Faster Isomorphism for p-Groups of Class 2 and Exponent p

Xiaorui Sun[*]

Abstract

The group isomorphism problem determines whether two groups, given by their Cayley tables, are isomorphic. For groups with order n, an algorithm with $n^{(\log n + O(1))}$ running time, attributed to Tarjan, was proposed in the 1970s [Mil78]. Despite the extensive study over the past decades, the current best group isomorphism algorithm has an $n^{(1/4+o(1))\log n}$ running time [Ros13].

The isomorphism testing for p-groups of (nilpotent) class 2 and exponent p has been identified as a major barrier to obtaining an $n^{o(\log n)}$ time algorithm for the group isomorphism problem. Although the p-groups of class 2 and exponent p have much simpler algebraic structures than general groups, the best-known isomorphism testing algorithm for this group class also has an $n^{O(\log n)}$ running time.

In this paper, we present an isomorphism testing algorithm for p-groups of class 2 and exponent p with running time $n^{O((\log n)^{5/6})}$ for any prime $p > 2$. Our result is based on a novel reduction to the skew-symmetric matrix tuple isometry problem [IQ19]. To obtain the reduction, we develop several tools for matrix space analysis, including a matrix space individualization-refinement method and a characterization of the low rank matrix spaces.

---

[*]`xiaorui@uic.edu`. University of Illinois at Chicago.

1 Introduction

The group isomorphism problem is to determine whether two groups, given by their Cayley (multiplication) tables, are isomorphic. The problem is among a few classes of problems in NP that are not known to be solvable in polynomial time or NP-Complete [GJ79]. The group isomorphism problem and its variants have close connections to cryptography, computational group theory, and algebraic complexity theory [BGL+19]. Furthermore, following Babai's breakthrough on the quasi-polynomial time algorithm for graph isomorphism [Bab16, Bab19], group isomorphism has become a bottleneck for the $n^{o(\log n)}$ time algorithm of graph isomorphism because group isomorphism reduces to graph isomorphism.

The group isomorphism problem has been extensively studied since the 1970s [FN70, Mil78, Sav80, O'B94, Vik96, Kav07, LG09, Wil09a, Wil09b, BCGQ11, BCQ12, BQ12, BW12, LW10, QST12, Ros13, BMW15, Luk15, RW15, LQ17, BLQW20, GQ21a, DW22, GQ21b]. A simple algorithm for group isomorphism, attributed to Tarjan, picks a generating set in one of the groups and checks for all possible images of the generating set in the other group, whether the partial correspondence extends to an isomorphism [Mil78]. Since every group of order n has a generating set of size at most $\log_2 n$, this algorithm results in an $n^{\log_2 n + O(1)}$ running time. The current best-known algorithm for the group isomorphism problem has an $n^{(1/4+o(1))\log_2 n}$ running time [Ros13].

It is long believed that the isomorphism testing of p-groups of class 2 and exponent p is a major bottleneck for the group isomorphism problem [LW10, BCGQ11, BW12, Ros13, BMW15, LQ17, BGL+19]. A group G is a p-group of (nilpotent) class 2 and exponent p for some prime number p if every element except the identity has an order of p, and G is not abelian but $[G, [G, G]]$ only contains the identity element, where $[G, H]$ denotes the group generated by $xyx^{-1}y^{-1}$ for all $x \in G, y \in H$.

The best-known algorithm for the isomorphism testing of p-groups of class 2 and exponent p does not have a major advantage in the running time, being $n^{O(\log_2 n)}$ [Ros13], over the general groups, even though the structure of p-groups of class 2 and exponent p was well understood [Bae38, Web83, Wil09a, Wil09b], and the isomorphism testing of this group class has been studied in depth [LW10, BW12, Ros13, BMW15, LQ17, BGL+19, Sch19]. Hence, to develop a better algorithm for isomorphism testing of general groups, it is necessary to provide a faster algorithm for p-groups of class 2 and exponent p.

1.1 Our result

In this paper, we present an isomorphism testing algorithm for p-groups of class 2 and exponent p with $n^{o(\log n)}$ running time for any odd prime p.

Theorem 1.1. *Let G and H be two groups of order n. If both G and H are p-groups of class 2 and exponent p for some prime number $p > 2$, then given the Cayley tables of G and H, there is an algorithm with running time $n^{O((\log n)^{5/6})}$ to determine whether G and H are isomorphic.*

Theorem 1.1 utilizes the Baer's correspondence [Bae38], which reduces the group isomorphism problem for p-groups of class 2 and exponent p to the isometry testing problem of skew-symmetric matrix spaces.

A square matrix A is a skew-symmetric matrix if $A^T = -A$. In the isometry testing problem for skew-symmetric matrix spaces, the input consists of the linear bases of two skew-symmetric matrix spaces $\mathfrak{A}$ and $\mathfrak{B}$. The problem is to decide whether there is an isometry S from $\mathfrak{A}$ to $\mathfrak{B}$, i.e., an invertible matrix S such that $S\mathfrak{A}S^T = \mathfrak{B}$, where $S\mathfrak{A}S^T$ is the linear span of the matrices SAS^T for all the matrices $A \in \mathfrak{A}$. We prove the following result for the isometry testing problem of skew-symmetric matrix spaces.

Theorem 1.2. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be two linear matrix spaces, both of dimension m, such that every matrix in $\mathfrak{A}$ or $\mathfrak{B}$ is an $n \times n$ skew-symmetric matrix over $\mathbb{F}_p$ for some prime number $p > 2$ and positive integers m, n. There is an algorithm with running time $p^{O((n+m)^{1.8} \cdot \log(p))}$ to determine whether there is an invertible $n \times n$ matrix S over $\mathbb{F}_p$ such that $S\mathfrak{A}S^T = \mathfrak{B}$.*

We obtain Theorem 1.2 by combining several new tools to analyze matrix spaces, including an individualization-refinement method for matrix spaces, a characterization of low rank matrix spaces, and a reduction from the isometry testing of skew-symmetric matrix spaces to the isometry testing of skew-symmetric matrix tuples [IQ19].

To obtain Theorem 1.1, let k denote $\log_p(n)$. We apply Theorem 1.2 for the case of $k > (\log_2(p))^5$ by constructing the skew-symmetric matrix spaces for both input groups according to the Baer's correspondence [Bae38]. Theorem 1.2 implies the running time for this case is $n^{O((\log n)^{5/6})}$. For the case of $k \le (\log_2(p))^5$, we run the aforementioned generating set enumeration algorithm [Mil78]. Because every p group of order p^k has a generating set of size at most k, the running time of the algorithm for this case is $p^{O(k^2)}$, which is also $n^{O((\log n)^{5/6})}$.

1.2 Related work

The group isomorphism problem has been studied for variant group classes. Polynomial time algorithms have been developed for abelian groups [Kav07, Sav80, Vik96], groups formed by semidirect products of an abelian group and a cyclic group [LG09, Wil09a, Wil09b], groups with normal Hall subgroups [QST12], groups with abelian Sylow towers [BQ12], and groups with no abelian normal subgroups [BCQ12]. Dietrich and Wilson recently showed that the group isomorphism problem can be solved in nearly linear time for most orders [DW22].

For p-groups of class 2 and exponent p, algorithms for some nontrivial subclasses of this group class have been proposed [LW10, BW12, BMW15]. Li and Qiao showed that if the p-groups of class 2 and exponent p are generated randomly, then the isomorphism testing problem can be solved in polynomial time in the average case [LQ17]. In [BGL$^+$19], the average case running time was further improved to linear. In this work, we focus on the isomorphism testing for p-groups of class 2 and exponent p in the worst case.

The refinement methods, such as the naive refinement [BES80] and Weisfeiler-Leman refinement [WL68], have been powerful tools for the graph isomorphism problem. The refinement methods have been successfully used for graph isomorphism testing algorithms [Bab80, BES80, Bab81, BL83, ZKT85, Spi96, DLN$^+$09, BCS$^+$13, BW13, CST13, SW15, LPPS17, GN19, KPS19, Wie20, GNS20, GWN20, Neu22], including the celebrated quasi-polynomial time algorithm for graph isomorphism [Bab16, Bab19].

The refinement approach does not extend to groups in a naive way. Several representations of groups that allow refinement have been proposed recently. In [BGL$^+$19], the authors defined a hypergraph using recursively refinable filters and proposed applying the Weisfeiler-Leman refinement on the hypergraph. Brachter and Schweitzer proposed defining colors of group element tuples by group operation patterns of the elements involved in the tuple and applying the Weisfeiler-Leman refinement to refine the colors of element tuples [BS20]. Both approaches can distinguish between several non-isomorphic constructions of p-groups of class 2 and exponent p. However, it was unclear how these refinement methods could be used to develop faster worst case isomorphism testing algorithms.

The isometry testing of skew-symmetric matrix spaces was studied in [LQ17, BLQW20, GQ21a, GQ21b]. Its applications in cryptography were investigated in [BGL$^+$19, JQSY19, TDJ$^+$22].

1.3 Technique overview

We provide an overview of the algorithm for the isometry testing of skew-symmetric matrix spaces (Theorem 1.2).

Isometry Testing for Skew-Symmetric Matrix Tuples We start by introducing the skew-symmetric matrix tuple isometry problem, which is related to our problem. A skew-symmetric matrix tuple $\mathcal{A} = (A_1, \ldots, A_k)$ of length k is a sequence of k skew-symmetric matrices of the same dimensions. For matrices P and Q, we use $P\mathcal{A}Q$ to denote the matrix tuple $(PA_1Q, PA_2Q, \ldots, PA_kQ)$.

Similar to the isometry between two skew-symmetric matrix spaces, we also define the isometry between two skew-symmetric matrix tuples. For two skew-symmetric matrix tuples $\mathcal{A}$ and $\mathcal{B}$, a matrix S is an isometry from $\mathcal{A}$ to $\mathcal{B}$ if $S\mathcal{A}S^T = \mathcal{B}$, i.e., $SA_iS^T = B_i$ for all the $A_i \in \mathcal{A}$. The isometry problem of skew-symmetric matrix tuples determines whether there is an isometry between two input skew-symmetric matrix tuples. The difference between the skew-symmetric matrix tuple isometry problem and the skew-symmetric matrix space isometry problem is that the correspondence between matrices from two matrix tuples is fixed by the indices of the matrices, but for matrix spaces, no such correspondence is given. Ivanyos and Qiao presented a polynomial time algorithm for the isometry testing of skew-symmetric matrix tuples [IQ19].

Theorem 1.3 (Theorem 1.7 of [IQ19]). *Let $\mathcal{A} = (A_1, \ldots, A_k)$ and $\mathcal{B} = (B_1, \ldots, B_k)$ be two skew-symmetric matrix tuples of length k such that the matrices in $\mathcal{A}$ and $\mathcal{B}$ are of dimension $n \times n$ over $\mathbb{F}_p$ for some prime $p > 2$. There is an algorithm with running time $\mathrm{poly}(n, k, p)$ to determine whether there is an isometry from $\mathcal{A}$ to $\mathcal{B}$. If yes, the algorithm also returns an isometry from $\mathcal{A}$ to $\mathcal{B}$.*

Our approach for the isometry testing of skew-symmetric matrix spaces is obtained by providing a $p^{O((n+m)^{1.8} \cdot \log p)}$ time reduction to the skew-symmetric matrix tuple isometry problem, where m is the dimension of the matrix space, and n is the number of rows or columns for each square matrix in the matrix space.

Individualization-refinement for matrix spaces One powerful technique for graph isomorphism is the individualization-refinement method [Bab80, BES80, Bab81, ZKT85, Spi96, BCS$^+$13, BW13, CST13, SW15, Bab16]. For graphs, the individualization-refinement method first chooses a set of a small number of vertices and assigns each chosen vertex a distinct vertex color, and then it refines the vertex colors by assigning distinguished vertices different colors in a canonical way until vertices of the same color cannot be further distinguished.

A natural question for the group isomorphism problem is whether it is possible to define individualization-refinement operations for group isomorphism. Based on the connection between group isomorphism for p-groups of class 2 and exponent p and the skew-symmetric matrix space isometry problem [Bae38], Li and Qiao proposed a matrix space individualization-refinement method, which follows the individualization-refinement for random graphs [BES80], and analyzed the isometry testing of skew-symmetric matrix spaces in the average case [LQ17].

In this work, we propose a different matrix space individualization-refinement to enable the analysis of the isometry of skew-symmetric matrix spaces in the worst case. Consider an $m \times n$ matrix space $\mathfrak{A}$. The individualization in our scenario is defined by a left individualization matrix L and a right individualization matrix R, where L is a matrix with m columns and R is a matrix with n rows. In the refinement, we compute LAR for each matrix $A \in \mathfrak{A}$. If $LA'R$ does not equal $LA''R$ for some $A', A'' \in \mathfrak{A}$, then A' and A'' are distinguished.

3

Ideally, if $LA'R$ does not equal $LA''R$ for any two matrices $A', A'' \in \mathfrak{A}$, then each matrix A in the space can be uniquely identified by LAR, and thus all the matrices in $\mathfrak{A}$ are distinguished. Consider two isometric skew-symmetric matrix spaces $\mathfrak{A}$ and $\mathfrak{B}$. Let $L_{\mathfrak{A}}$ and $R_{\mathfrak{A}}$ be individualization matrices for $\mathfrak{A}$ that distinguish all the matrices in $\mathfrak{A}$. Let $L_{\mathfrak{B}}$ and $R_{\mathfrak{B}}$ be individualization matrices for $\mathfrak{B}$ such that $L_{\mathfrak{B}}$ equals $L_{\mathfrak{A}} S^{-1}$, and $R_{\mathfrak{B}}$ equals $(S^T)^{-1} R_{\mathfrak{A}}$ for some isometry S from $\mathfrak{A}$ to $\mathfrak{B}$. One can distinguish all the matrices in both spaces by their individualization matrices and then establish a bijection between the matrices in the two spaces. Thus the skew-symmetric matrix space isometry problem reduces to the skew-symmetric matrix tuple isometry problem, which can be efficiently solved by Theorem 1.3. Furthermore, suppose $L_{\mathfrak{A}}$ contains a small number of rows and $R_{\mathfrak{A}}$ contains a small number of columns. Then one can solve the skew-symmetric matrix space isometry problem efficiently by enumerating all the possible corresponding $L_{\mathfrak{B}}$ and $R_{\mathfrak{B}}$.

We show that the number of rows for the left individualization matrices and the number of columns for the right individualization matrices are related to the rank of matrices in the matrix space. More specifically, we show that for a matrix space of dimension d and any parameter k, there exist left and right individualization matrices L and R with $O(\max\{d\log(p), k\}/\sqrt{k})$ rows and columns, respectively, such that for each matrix A in the matrix space with rank at least k, LAR is a non-zero matrix (Lemma 3.2). In other words, if every matrix (except the zero matrix) in a skew-symmetric matrix space is of high rank, then the skew-symmetric matrix space isometry problem reduces to the skew-symmetric matrix tuple isometry problem efficiently.

Low rank matrix space characterization   The hard case for the matrix space individualization/refine method is that there are some matrices A in the space such that LAR are zero matrices. Because of the linearity, such matrices form a linear subspace of the original matrix space. To tackle this hard case, we characterize the structure of the matrix space in which every matrix is of low rank. Such a matrix space is called a low rank matrix space.

As our main technical result for the low rank matrix space characterization, we show that, for a matrix space $\mathfrak{A}$ such that every matrix in the space is of rank at most r, there are invertible matrices P and Q, called left and right formatting matrices, such that for each $A \in \mathfrak{A}$, PAQ has non-zero entries only in the last $O(r^2)$ rows or columns (Lemma 4.6). Furthermore, if $\mathfrak{A}$ is a skew-symmetric matrix space, then $Q = P^T$.

Together with matrix space individualization-refinement, we can represent a matrix space in a more structured way. First, we construct a "semi-canonical" basis for the input matrix space. Suppose we apply left and right individualization matrices L and R to a matrix space $\mathfrak{A}$ of dimension d and compute a linear basis $(A_1, \ldots, A_d)$ of $\mathfrak{A}$ such that $(LA_1R, LA_2R, \ldots, LA_dR)$ is lexically minimized among all the linear basis of $\mathfrak{A}$. Because the zero matrix is lexically the smallest among all the matrices, the first few matrices in the semi-canonical basis correspond to a linear basis of $\mathfrak{C}$, which is the linear span of all the matrices $A \in \mathfrak{A}$ such that LAR is a zero matrix.

We further apply formatting matrices P and Q for $\mathfrak{C}$ to each matrix in the semi-canonical basis of $\mathfrak{A}$ (every matrix A in the semi-canonical basis becomes PAQ). Then by our low rank matrix space characterization, the matrices that form a linear basis of $\mathfrak{C}$ have non-zero entries only in the last few rows or columns. See Figure 1 for an illustration.

The semi-canonical basis is not canonical because, for fixed individualization matrices, there can be different semi-canonical bases. But the semi-canonical bases can provide a partial correspondence between two isometric skew-symmetric matrix spaces. Suppose two skew-symmetric matrix spaces $\mathfrak{A}$ and $\mathfrak{B}$ are isometric and let S be an isometry from $\mathfrak{A}$ to $\mathfrak{B}$. For individualization matrices L and R of $\mathfrak{A}$, let $(A_1, \ldots, A_d)$ be a semi-canonical basis of $\mathfrak{A}$ with L and R as individualization matrices, and $(B_1, \ldots, B_d)$ be a semi-canonical basis of $\mathfrak{B}$ with LS^{-1} and $(S^T)^{-1}R$ as individualization

4

Figure 1: The semi-canonical basis of a matrix space after applying matrix space individualization-refinement and the low rank matrix space characterization. The three black matrices in the front form a basis of the space spanned by all the matrices $A \in \mathfrak{A}$ such that LAR is a zero matrix. The transparent rectangles enclosed by the dashed black lines are zero matrices. The four light brown matrices in the back are the rest matrices in the basis.

matrices. Then for each $1 \leq i \leq d$, $SA_iS^T = B_i + B_i'$ for some B_i' satisfying the condition that $LS^{-1}B_i'(S^T)^{-1}R$ is a zero matrix. The partial correspondence also holds for two equivalent matrix spaces. Two matrix spaces $\mathfrak{A}$ and $\mathfrak{B}$, in which matrices are not necessarily square matrices, are equivalent if there are invertible matrices X and Y such that $X\mathfrak{A}Y = \mathfrak{B}$, i.e., $\mathfrak{B}$ equals the space spanned by XAY for all the matrices $A \in \mathfrak{A}$.

Tensor representation of skew-symmetric matrix spaces   Next, we combine the matrix space individualization-refinement and the low rank matrix space characterization to analyze skew-symmetric matrix spaces. For convenience, let us define a three-tensor representation for skew-symmetric matrix spaces following [LQ17]. For a skew-symmetric matrix space $\mathfrak{A}$ of dimension m such that every matrix in the space is an $n \times n$ matrix, a three-tensor $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$ is a skew-symmetric matrix space tensor of $\mathfrak{A}$ if $\mathbf{G}[i,j,k] = A_i[j,k]$ for a linear basis $(A_1, \ldots, A_m)$ of $\mathfrak{A}$, where $A_i[j,k]$ is the (j,k)-th entry of A_i, and $\mathbf{G}[i,j,k]$ is the (i,j,k)-th entry of $\mathbf{G}$.

Given a skew-symmetric matrix space tensor $\mathbf{G}$, we use $\mathfrak{X}_{\mathbf{G},i}$ to denote the $n \times n$ skew-symmetric matrix such that $\mathfrak{X}_{\mathbf{G},i}[j,k] = \mathbf{G}[i,j,k]$, use $\mathfrak{Y}_{\mathbf{G},j}$ to denote the $m \times n$ matrix such that $\mathfrak{Y}_{\mathbf{G},j}[i,k] = \mathbf{G}[i,j,k]$, and use $\mathfrak{Z}_{\mathbf{G},k}$ to denote the $m \times n$ matrix such that $\mathfrak{Z}_{\mathbf{G},k}[i,j] = \mathbf{G}[i,j,k]$. We also use $\mathfrak{X}_{\mathbf{G}}$ to denote the matrix space $\langle \mathfrak{X}_{\mathbf{G},1}, \ldots \mathfrak{X}_{\mathbf{G},m} \rangle$, use $\mathfrak{Y}_{\mathbf{G}}$ to denote the matrix space $\langle \mathfrak{Y}_{\mathbf{G},1}, \ldots \mathfrak{Y}_{\mathbf{G},n} \rangle$, and use $\mathfrak{Z}_{\mathbf{G}}$ to denote the matrix space $\langle \mathfrak{Z}_{\mathbf{G},1}, \ldots \mathfrak{Z}_{\mathbf{G},n} \rangle$, where $\langle \cdot \rangle$ is the linear span. We remark that $\mathfrak{X}_{\mathbf{G}}$ is a skew-symmetric matrix space, but $\mathfrak{Y}_{\mathbf{G}}$ and $\mathfrak{Z}_{\mathbf{G}}$ are not.

One can verify that two skew-symmetric matrix spaces are isometric if and only if their tensors (denoted as $\mathbf{G}$ and $\mathbf{H}$) are isometric, i.e., there is an $n \times n$ invertible matrix N and an $m \times m$ invertible matrix M such that the transform of $\mathbf{G}$ by N and M, denoted as $\mathrm{Trans}_{N,M}(\mathbf{G})$, equals $\mathbf{H}$, where

$$\mathfrak{X}_{\mathrm{Trans}_{N,M}(\mathbf{G}),i} = \sum_{i'=1}^{m} M[i,i'] \cdot \left(N \cdot \mathfrak{X}_{\mathbf{G},i'} \cdot N^T \right).$$

Semi-canonical form of skew-symmetric matrix space tensors   In this work, the purpose of the tensor representation of a skew-symmetric matrix space is to incorporate the matrix space

5

individualization-refinement and the low rank matrix space characterization techniques so the tensor is transformed into a more structured form, called the "semi-canonical form" of the tensor.

For a skew-symmetric matrix space tensor $\mathbf{G}$, the semi-canonical form of $\mathbf{G}$, denoted as $\mathbf{SC}(\mathbf{G})$, is obtained by applying the two techniques to the three matrix spaces $\mathfrak{X}_{\mathbf{G}}$, $\mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$ so matrices in each of the three matrix spaces have the structure shown in Figure 1. To achieve this, we need to carefully choose the individualization and formatting matrices in a coordinated fashion. In particular, if the individualization and formatting matrices are chosen such that, for the left formatting matrix P used for $\mathfrak{X}_{\mathbf{G}}$, P^T can also be used as the right formatting matrix for $\mathfrak{Y}_{\mathbf{G}}$ and $\mathfrak{Z}_{\mathbf{G}}$, then the tensor semi-canonical form has the structure shown in Figure 2(a). The tensor values in the transparent region are all zero. The union of the transparent region and the red cube is called the kernel of the tensor semi-canonical form. The blue region is called the surface of the tensor semi-canonical form.

Figure 2: (a). Semi-canonical form of a skew-symmetric matrix space tensor. (b) Matrices in the surfaces of $\mathfrak{X}_{\mathbf{G}}, \mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$.

For fixed individualization and formatting matrices, the tensor semi-canonical form is also fixed. However, for an efficient tensor isometry testing algorithm, it is unacceptable to enumerate all possible formatting matrices, though it is affordable to enumerate all possible individualization matrices. To address this issue, we show that if the individualization matrices are fixed, and the formatting matrices are partially fixed (i.e., only a few key rows are fixed, and all the other rows satisfy certain conditions), then the kernel is fixed (Lemma 5.10). This is also the reason for the term "semi-canonical form": the semi-canonical form is not unique for fixed individualization matrices and partially fixed formatting matrices, but the kernel is unique.

In other words, if two tensors are isometric, and one constructs the semi-canonical forms of the two tensors using individualization matrices and partially fixed formatting matrices that are the same up to some isometry, then the kernels of the two semi-canonical forms are identical. Therefore, to determine whether the two tensors are isometric, one only needs to check further if there are formatting matrices that make the surface identical for the two tensors while keeping the kernel unchanged.

In addition, based on the results from the matrix space individualization-refinement and the low rank matrix space characterization, there are always semi-canonical forms such that the numbers of matrices in the surfaces of $\mathfrak{X}_{\mathbf{G}}$, $\mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$ (Figure 2(b)) are small. Hence, in the partially fixed formatting matrices, we also fix the rows related to the surfaces of $\mathfrak{X}_{\mathbf{G}}$, $\mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$. Then

matrices in the surfaces from the three matrix spaces are fixed up to some formatting matrices satisfying the partially fixed constraint.

Hence, the isometry testing of skew-symmetric matrix space tensors reduces to the isometry testing of their semi-canonical forms by enumerating individualization matrices and partially fixed formatting matrices for both tensors. Due to the fixed kernel for all the semi-canonical forms, the isometry testing of semi-canonical forms further reduces to deciding whether the surfaces are identical between semi-canonical forms up to some formatting matrices satisfying the partially fixed constraint.

Reduction to skew-symmetric matrix tuple isometry testing Finally, we reduce the isometry testing of semi-canonical forms of skew-symmetric matrix spaces to the aforementioned skew-symmetric matrix tuple isometry problem. The high-level idea is to construct a skew-symmetric matrix tuple to encode the surface of the tensor semi-canonical form. Because the matrices in the surfaces of $\mathfrak{X}_{\mathbf{G}}$, $\mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$ are fixed, we can use different matrices in the matrix tuple to encode the matrices in the surface.

Suppose the kernel is of dimension $m' \times n' \times n'$ for some $1 \leq m' \leq m$ and $1 \leq n' \leq n$. In our skew-symmetric matrix tuple of $\mathbf{SC(G)}$, denoted as $\mathcal{F}_{\mathbf{SC(G)}}$, each matrix is of dimension $(3 + n + m') \times (3 + n + m')$. The rows from the fourth to the $(3 + n)$-th of matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ correspond to the rows of matrices in $\mathfrak{X}_{\mathbf{G}}$. The last m' rows of matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ correspond to the first m' rows of matrices in $\mathfrak{Y}_{\mathbf{G}}$ (or equivalently $\mathfrak{Z}_{\mathbf{G}}$). The first three rows of matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ are auxiliary rows used to ensure that the other rows satisfy the constraints of the partially fixed formatting matrices. See Figure 3 for an illustration.

Figure 3: The matrices in $\mathcal{F}_{\mathbf{SC(G)}}$.

We use the submatrices on R_1 (as Figure 3) for all the matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ to encode the skew-symmetric matrices in the surface of $\mathfrak{X}_{\mathbf{G}}$. We also use the submatrices on R_2 for all the matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ to encode the matrices in the surface of $\mathfrak{Y}_{\mathbf{G}}$ (excluding the intersection with the surface of $\mathfrak{X}_{\mathbf{G}}$). Consequently, the submatrices on R_3 for all the matrices in $\mathcal{F}_{\mathbf{SC(G)}}$, which is the negative transpose of submatrices on R_2 by the skew-symmetric condition, encode the matrices in the surface of $\mathfrak{Z}_{\mathbf{G}}$ (excluding the intersection with the surface of $\mathfrak{X}_{\mathbf{G}}$). We use the other submatrices to ensure constraints given by the partially fixed formatting matrices.

By carefully designing matrix tuples constructed from tensor semi-canonical forms, we show that the semi-canonical forms of two skew-symmetric matrix space tensors are isometric if and only

7

if there is an isometry S between the skew-symmetric matrix tuples such that S is a block diagonal matrix

$$S = \begin{pmatrix} Q & 0 \\ 0 & W \end{pmatrix}$$

for some $(3 + n) \times (3 + n)$ matrix Q and $m' \times m'$ matrix W (Lemma 6.2).

Naturally, we want to determine the isometry of the two tensors by running the skew-symmetric matrix tuple isometry algorithm (Theorem 1.3) on the matrix tuples constructed from the semi-canonical forms. However, the requirement of S being block diagonal makes things more complex.

Suppose we run the algorithm for skew-symmetric matrix tuple isometry on the matrix tuples constructed. If the algorithm returns no, then the two semi-canonical forms are not isometric. If the algorithm returns yes and an isometry that is block diagonal, then the two semi-canonical forms are isometric. The difficult case is when the algorithm returns yes and an isometry that is not block diagonal. For this case, we can neither certify that the two semi-canonical forms are isometric, nor show that the two semi-canonical forms are not isometric.

Let us consider an easier scenario: Suppose for each non-zero row vector $v \in \mathbb{F}_p^n$, there is a matrix X in the surface of $\mathfrak{X}_{\mathbf{G}}$ such that vX is a non-zero vector. With this condition, together with our construction of matrix tuples, we can show that the isometry returned is of the form

$$\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix}.$$

After carefully analyzing the matrix tuples constructed, we show that

$$\begin{pmatrix} X & 0 \\ 0 & Z \end{pmatrix}$$

is also an isometry, and thus the two semi-canonical forms are isometric.

The general case is more complex because the left bottom submatrix of the isometry returned can be non-zero. However, we show that either we can certify that there exists another block diagonal isometry for the skew-symmetric matrix tuples, or we can reduce the problem to a matrix tuple equivalence problem, i.e., the problem of determining whether two matrix tuples $\mathcal{A}$ and $\mathcal{B}$ have invertible matrices P and Q such that $P\mathcal{A}Q = \mathcal{B}$. According to [IQ19], the matrix tuple equivalence problem can be solved efficiently.

Paper organization   In Section 2, we define the notations and provide the preliminaries. In Section 3, we present our results on matrix space individualization-refinement. In Section 4, we present our results on low rank matrix space characterization. Section 5 defines skew-symmetric matrix space tensor and its semi-canonical form. In Section 6, we present the reduction to the skew-symmetric matrix tuple isometry problem. Section 7 proves Theorem 1.1 and Theorem 1.2.

2   Notations and preliminaries

Throughout the paper, the vectors and matrices are over $\mathbb{F}_p$ for a prime number $p > 2$. We use $\langle \cdot \rangle$ to denote the linear span. The base of the logarithm is two unless specified. Let $\mathbb{F}_p^n$ be the linear space of row vectors of length n over $\mathbb{F}_p$. Unless specified, the vectors are row vectors. For a vector $v \in \mathbb{F}_p^n$, we use $v[i]$ to denote the i-th entry of v for any $1 \le i \le n$.

8

Matrices   Let $M(n, \mathbb{F}_p)$ (and respectively $M(m, n, \mathbb{F}_p)$) be the linear space of $n \times n$ (and respectively $m \times n$) matrices over $\mathbb{F}_p$. Let $\mathrm{GL}(n, \mathbb{F}_p)$ be the group of $n \times n$ invertible matrices over $\mathbb{F}_p$.

For a matrix $A \in M(m, n, \mathbb{F}_p)$, let $\mathrm{rank}\,(A)$ be the rank of A, and A^T be the transpose of A. A square matrix $A \in M(n, \mathbb{F}_p)$ is a skew-symmetric matrix if and only if $A = -A^T$. For any $1 \le i \le m, 1 \le j \le n$, let $A[i, j]$ be the entry of A in the i-th row and j-th column. For $1 \le i \le i' \le m, 1 \le j \le j' \le n$, let $A[i, i'; j, j']$ be the submatrix of A on the rows between i and i' and the columns between j and j'.

For two matrices $A, B \in M(m \times n, \mathbb{F}_p)$, A is lexically smaller than B, denoted as $A \prec B$, if there exist $1 \le q \le m$ and $1 \le r \le n$ such that the following conditions hold:

- $A[i, j] = B[i, j]$ for any $1 \le i \le q - 1, 1 \le j \le n$ or any $i = q, 1 \le j < r$;

- $A[q, r] < B[q, r]$.

We denote $A \preceq B$ if $A \prec B$ or $A = B$.

We use I_n to denote the $n \times n$ identity matrix.

Matrix tuples and matrix spaces   An $m \times n$ matrix tuple $\mathcal{A}$ of length k, denoted as $\mathcal{A} = (A_1, \ldots, A_k)$, is an element in $M(m, n, \mathbb{F}_p)^k$. For any $P \in M(\alpha, m, \mathbb{F}_p)$ and $Q \in M(n, \beta, \mathbb{F}_p)$ with some positive integers α and β, let $P\mathcal{A}Q$ be the matrix tuple $(PA_1Q, PA_2, Q, \ldots, PA_kQ)$.

An $m \times n$ matrix space $\mathfrak{A}$ is a linear subspace of $M(m, n, \mathbb{F}_p)$. For any $P \in M(\alpha, m, \mathbb{F}_p)$ and $Q \in M(n, \beta, \mathbb{F}_p)$ with some positive integers α and β, let $P\mathfrak{A}Q$ be the linear space spanned by PAQ for all the $A \in \mathfrak{A}$. For any row vector $v \in \mathbb{F}_p^m$, we use $\langle v\mathfrak{A} \rangle$ to denote the row vector space spanned by vA for all the $A \in \mathfrak{A}$. For two matrix spaces $\mathfrak{A}$ and $\mathfrak{B}$, we denote $\mathfrak{A} \le \mathfrak{B}$ if $\mathfrak{A}$ is a subspace of $\mathfrak{B}$.

Since any linear combination of skew-symmetric matrices of the same dimension is also a skew-symmetric matrix, we use $\mathrm{SS}(n, \mathbb{F}_p)$ to denote the linear space of all the $n \times n$ skew-symmetric matrices.

Isometry and equivalence for matrix tuples and spaces   We define equivalence relations for matrix tuples.

Definition 2.1 (Matrix tuple equivalence). Let $\mathcal{A} = (A_1, \ldots, A_k), \mathcal{B} = (B_1, \ldots, B_k)$ be two matrix tuples in $M(m, n, \mathbb{F}_p)^k$. $\mathcal{A}$ and $\mathcal{B}$ are equivalent if there exist two matrices $P \in \mathrm{GL}(m, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $P\mathcal{A}Q = \mathcal{B}$.

Definition 2.2 (Skew-symmetric matrix tuple isometry). Let $\mathcal{A} = (A_1, \ldots, A_k)$ and $\mathcal{B} = (B_1, \ldots, B_k)$ be two skew-symmetric matrix tuples in $\mathrm{SS}(n, \mathbb{F}_p)^k$. $\mathcal{A}$ and $\mathcal{B}$ are isometric if there exists a matrix $P \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $P\mathcal{A}P^T = \mathcal{B}$. P is called an isometry from $\mathcal{A}$ to $\mathcal{B}$ if P exists.

In this paper, we use the algorithm for the isometry testing of two skew-symmetric matrix tuples (Theorem 1.3) and the algorithm for the equivalence testing of two matrix tuples (Theorem 2.3), both proposed by Ivanyos and Qiao in [IQ19].

Theorem 2.3 (Proposition 3.2 of [IQ19]). *Given two matrix tuples $\mathcal{A} = (A_1, \ldots, A_k)$ and $\mathcal{B} = (B_1, \ldots, B_k)$ in $M(m, n, \mathbb{F}_p)^k$ for some prime $p > 2$ and positive integers k, m and n, there is an algorithm with running time $\mathrm{poly}(k, n, m, p)$ to determine whether $\mathcal{A}$ and $\mathcal{B}$ are equivalent.*

Following the definitions for matrix tuples, we also define the equivalence of matrix spaces and the isometry of skew-symmetric matrix spaces.

9

Definition 2.4 (Matrix space equivalence)**.** Let $\mathfrak{A}, \mathfrak{B} \leq M(m, n, \mathbb{F}_p)$ be two matrix spaces for some positive integers m and n. $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent if there exist two matrices $P \in \mathrm{GL}(m, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $P\mathfrak{A}Q = \mathfrak{B}$.

Definition 2.5 (Skew-symmetric matrix space isometry)**.** Let $\mathfrak{A}, \mathfrak{B} \leq \mathrm{SS}(n, \mathbb{F}_p)$ be two skew-symmetric matrix spaces. $\mathfrak{A}$ and $\mathfrak{B}$ are isometric if there exists a matrix $P \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $P\mathfrak{A}P^T = \mathfrak{B}$. P is called an isometry from $\mathfrak{A}$ to $\mathfrak{B}$ if P exists.

Baer's correspondence   For a p-group of nilpotent class 2 and exponent p, let p^k denote the order of the group. Because of the class two and exponent p condition, $G/Z(G)$ is isomorphic to $\mathbb{Z}_p^n$, and $[G, G]$ is isomorphic to $\mathbb{Z}_p^m$ for some positive integers n and m such that $m + n \leq k$, where $Z(G)$ denotes the center of G and $[G, G]$ denotes the group generated by $xyx^{-1}y^{-1}$ for all $x, y \in G$. Taking an arbitrary basis of $G/Z(G)$, an arbitrary basis of $[G, G]$, and taking the commutator bracket, we obtain a skew-symmetric bilinear map $b_G : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$, which can be represented by a skew-symmetric matrix tuple $\mathcal{G} = (G_1, \ldots, G_m)$ such that every G_i is a matrix in $\mathrm{SS}(n, \mathbb{F}_p)$. Such a skew-symmetric matrix tuple is called a skew-symmetric matrix tuple of G.

For two p-groups G and H of nilpotent class 2 and exponent p, it is necessary for H to be isomorphic to G that $\dim_{\mathbb{Z}_p}(G/Z(G)) = \dim_{\mathbb{Z}_p}(H/Z(H))$ and $\dim_{\mathbb{Z}_p}([G, G]) = \dim_{\mathbb{Z}_p}([H, H])$. The following theorem, also called Baer's correspondence, was proved by Baer in [Bae38].

Theorem 2.6 (Baer's correspondence [Bae38], rephrased)**.** *Let G and H be two p-groups of class two and exponent p for some prime number p with the same order. Let $\mathcal{G}$ and $\mathcal{H}$ be the skew-symmetric matrix tuples of G and H, respectively. If both $\mathcal{G}$ and $\mathcal{H}$ are $n \times n$ skew-symmetric matrix tuples of length m, then G and H are isomorphic if and only if there are matrices $P \in \mathrm{GL}(n, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(m, \mathbb{F}_p)$ such that $G_i = \sum_{j=1}^m Q[i, j](P \cdot H_j \cdot P^T)$.*

Furthermore, we can also represent skew-symmetric matrix tuples of groups by skew-symmetric matrix spaces. Given an arbitrary skew-symmetric matrix tuple $\mathcal{G}$ of group G, the skew-symmetric matrix space $\mathfrak{G}$ of G is the linear matrix space spanned by matrices in $\mathcal{G}$. Hence, Baer's correspondence can be rephrased as follows.

Corollary 2.7. *Let G and H be two p-groups of class two and exponent p for some prime number p with the same order. Let $\mathfrak{G}$ and $\mathfrak{H}$ be the skew-symmetric matrix spaces of G and H, respectively. G and H are isomorphic if and only if $\mathfrak{G}$ and $\mathfrak{H}$ are isometric.*

In this paper, we will use the following fact from Baer's correspondence.

Fact 2.8. *Let $\mathfrak{G} \leq \mathrm{SS}(n, \mathbb{F}_p)$ be a skew-symmetric matrix space of a p-group of class two and exponent p for some prime number p. Then for any non-zero row vector $v \in \mathbb{F}_p^n$, there is a matrix $A \in \mathfrak{G}$ such that vA is a non-zero vector.*

3   Matrix space individualization-refinement

In this paper, the individualization-refinement to a matrix space $\mathfrak{A} \leq M(m, n, \mathbb{F}_p)$ is defined by a left individualization matrix $L \in M(\alpha, m, \mathbb{F}_p)$ and a right individualization matrix $R \in M(n, \beta, \mathbb{F}_p)$ for some positive integers α and β. We aim to distinguish matrices in $\mathfrak{A}$ by comparing LAR for matrices $A \in \mathfrak{A}$.

Ideally, if for any two different matrices $A, A' \in \mathfrak{A}$, $LAR \neq LA'R$, then each matrix $A \in \mathfrak{A}$ has its unique LAR. And thus, all the matrices in $\mathfrak{A}$ are distinguished. But if there is a matrix $A \in \mathfrak{A}$

such that LAR is a zero matrix, then for each $A' \in \mathfrak{A}$, $LA'R = L(A' + A)R$. Let $\text{zero}_{L,R}(\mathfrak{A})$ be the space spanned by matrices $A \in \mathfrak{A}$ such that LAR is a zero matrix.

We show that in order to distinguish matrices in a matrix space, the dimensions of the left and right individualization matrices are related to the rank of the matrices in the matrix space (Lemma 3.2).

Lemma 3.1. *Let A be a matrix in $M(m, n, \mathbb{F}_p)$ of rank at least k for a prime p and some positive integers m, n, k. Given an integer $1 \le k' \le k/2$ and a parameter $0 < \delta < 1$ satisfying $\log(1/\delta) \ge k$, let Q be a matrix in*

$$M\left(\left\lceil \frac{8k'\log(1/\delta)}{k}\right\rceil, m, \mathbb{F}_p\right)$$

such that the entries of Q are independently and uniformly sampled from $\{0, 1, \ldots, p - 1\}$. With probability $1 - \delta$, QA is a matrix of rank at least k'.

Proof. Since the entries of Q are independently and uniformly sampled, without loss of generality, we assume the matrix Q is sampled sequentially by rows $q_1, \ldots, q_\alpha$, where q_i is the i-th row of Q.

Suppose that after sampling the first α rows for some positive integer α, $\langle q_1 A, \ldots, q_\alpha A\rangle$ is a β dimensional space for some $\beta < k'$. The probability that $q_{\alpha+1}A$ is a vector in $\langle q_1 A, \ldots, q_\alpha A\rangle$ is $(1/p)^{k-\beta}$. Thus, by sampling $\lceil \log(k'/\delta)/(k - k')\rceil$ new rows of Q, the rank of Q increases by at least one with probability

$$1 - \left(\frac{1}{p}\right)^{(k-\beta)\cdot\lceil\log(k'/\delta)/(k-k')\rceil} \ge 1 - \left(\frac{1}{p}\right)^{\log(k'/\delta)} \ge 1 - \left(\frac{1}{2}\right)^{\log(k'/\delta)} = 1 - \frac{\delta}{k'}.$$

On the other hand, observe that

$$k'\left\lceil\frac{\log(k'/\delta)}{(k - k')}\right\rceil \le \frac{2k'\log(k'/\delta)}{k - k'} \le \frac{4k'\log(1/\delta)}{k - k'} \le \frac{8k'\log(1/\delta)}{k},$$

where the first inequality uses the condition that $\log(k'/\delta) \ge \log(1/\delta) \ge k \ge k - k'$, the second inequality uses the condition that $1/\delta \ge \log(1/\delta) \ge k > k'$, and the third inequality uses the condition that $k - k' \ge k/2$.

By union bound, with probability at least $1 - \delta$, if Q contains at least $\lceil 8k'\log(1/\delta)/k\rceil$ rows, then the rank of Q is at least k'. $\square$

Lemma 3.2. *Let $\mathfrak{A}$ be a d-dimensional matrix subspace of $M(m, n, \mathbb{F}_p)$ for a prime p and some positive integers d, m, n. For any $k \ge 4$, denote*

$$t := \left\lceil 32\max\{d\log(p), k\}/\sqrt{k}\right\rceil.$$

There is a left individualization matrix $L \in M(t, m, \mathbb{F}_p)$ and a right individualization matrix $R \in M(n, t, \mathbb{F}_p)$ such that for any $A \in \mathfrak{A}$ of rank at least k, LAR is a non-zero matrix.

Proof. Let A be an arbitrary matrix in $\mathfrak{A}$ of rank at least k. By Lemma 3.1 with $k' = \lfloor\sqrt{k}\rfloor$ and $\delta = \min\{1/(4p^d), 1/2^k\}$, if every entry of L is independently and uniformly sampled from $\{0, \ldots, p - 1\}$, then with probability at least $1 - 1/(4p^d)$, LA is of rank at least $\lfloor\sqrt{k}\rfloor$. If this case happens, then by Lemma 3.1 with $k' = 1$ and $\delta = \min\{1/(4p^d), 1/2^k\}$, if every entry of R is independently and uniformly sampled from $\mathbb{F}_p$, then with probability at least $1 - 1/(4p^d)$, LAR is of rank at least 1. By union bound, for random Q and R, with probability at least $1 - 1/(2p^d)$, LAR is a non-zero matrix.

By union bound, with constant probability, for random Q and R, QAR is a non-zero matrix for all the $A \in \mathfrak{A}$ of rank at least k. $\square$

We define the semi-canonical basis for a matrix space with respect to left and right individualization matrices.

Definition 3.3. Let $\mathfrak{A}$ be a matrix space of dimension d for some positive integer d. Let L be a left individualization matrix for $\mathfrak{A}$ and R be a right individualization matrix for $\mathfrak{A}$. A matrix tuple $\mathcal{A} = (A_1, \ldots, A_d)$ is a semi-canonical basis of $\mathfrak{A}$ with respect to L and R if the following two conditions hold:

1. $\langle A_1, \ldots, A_d \rangle = \mathfrak{A}$.

2. For each $1 \leq i \leq d$, $LA_iR \preceq LAR$ for all the A in $\mathfrak{A}$ but not in $\langle A_1, \ldots, A_{i-1} \rangle$.

We prove some basic properties for a semi-canonical basis of a matrix space.

Lemma 3.4. *Let $\mathfrak{A}$ be a matrix space of dimension d for some positive integer d. Let L be a left individualization matrix for $\mathfrak{A}$ and R be a right individualization matrix for $\mathfrak{A}$. If $\mathrm{zero}_{L,R}(\mathfrak{A})$ only contains the zero matrix, then there is a unique semi-canonical basis of $\mathfrak{A}$ with respect to L and R.*
If $\dim(\mathrm{zero}_{L,R}(\mathfrak{A})) > 0$, then for any semi-canonical basis $(A_1, \ldots, A_d)$ of $\mathfrak{A}$, LA_iR is a zero matrix for all the $1 \leq i \leq \dim(\mathrm{zero}_{L,R}(\mathfrak{A}))$, and LA_iR is a non-zero matrix for all the $\dim(\mathrm{zero}_{L,R}(\mathfrak{A}))+1 \leq i \leq d$. Furthermore, let $(A_1, \ldots, A_d)$ and $(A'_1, \ldots, A'_d)$ be two semi-canonical bases of $\mathfrak{A}$ with respect to L and R. For any $1 \leq i \leq d$, $A_i = A'_i + A''_i$ for some $A''_i \in \mathrm{zero}_{L,R}(\mathfrak{A})$.

Proof. If $\mathrm{zero}_{L,R}(\mathfrak{A})$ only contains the zero matrix, then for every non-zero matrix $A \in \mathfrak{A}$, LAR is a non-zero matrix. Let $\mathfrak{A}'$ be a subspace of $\mathfrak{A}$ such that $LA'R \prec LAR$ for any $A' \in \mathfrak{A}'$ and $A \notin \mathfrak{A}'$. There is a unique $A \in \mathfrak{A}$ such that $A \notin \mathfrak{A}'$, and $LAR \preceq LA''R$ for all the $A'' \notin \mathfrak{A}'$. Hence, the semi-canonical base is unique.

If $\dim(\mathrm{zero}_{L,R}(\mathfrak{A})) > 0$, since the zero matrix is lexically smallest among all the matrices, for any semi-canonical basis $(A_1, \ldots, A_d)$ of $\mathfrak{A}$, LA_iR is a zero matrix for all the $1 \leq i \leq \dim(\mathrm{zero}_{L,R}(\mathfrak{A}))$. By Definition 3.3, the lemma holds. $\square$

The following lemma shows that for a subspace of $M(m, n, \mathbb{F}_p)$ with dimension d, given left and right individualization matrices, a semi-canonical basis can be constructed in $p^d \cdot \mathrm{poly}(n, m, p, d)$ time.

Lemma 3.5. *Given an arbitrary basis of a matrix space $\mathfrak{A} \leq M(m, n, \mathbb{F}_p)$ of dimension d, a left individualization matrix L, and a right individualization matrix R for $\mathfrak{A}$, there is an algorithm to compute a semi-canonical basis of $\mathfrak{A}$ with respect to L and R in time $p^d \cdot \mathrm{poly}(n, m, p, d)$ if both L and R contain at most $\mathrm{poly}(n, m)$ rows and columns.*

Proof. Consider the following algorithm:

1. For $i = 1$ to d, find a non-zero matrix A_i in $\mathfrak{A}$ but not in $\langle A_1, \ldots, A_{i-1} \rangle$ such that $LA_iR \preceq LAR$ for all the matrices A in $\mathfrak{A}$ but not in $\langle A_1, \ldots, A_{i-1} \rangle$.

2. Return $(A_1, \ldots, A_d)$.

The correctness of the algorithm is by Definition 3.3. Since the algorithm has d iterations, and in each iteration, the algorithm enumerates all the matrices in $\mathfrak{A}$, the running time of the algorithm is $p^d \cdot \mathrm{poly}(n, m, d, p)$. $\square$

4 Low rank matrix space characterization

If all the matrices in a skew-symmetric matrix space, except the zero matrix, are of high rank, then with proper left and right individualization matrices, the semi-canonical basis is unique (Lemma 3.4). Furthermore, if two skew-symmetric matrix spaces are isometric and the two matrix spaces only contain high rank matrices (excluding the zero matrix in each space), then one can fix left and right individualization matrices for one space such that the semi-canonical basis is unique and enumerate all the possible images of the left and right individualization matrices for the other space. With left and right individualization matrices for both spaces, we compute the unique semi-canonical bases for both matrices spaces. Then the skew-symmetric matrix space isometry problem reduces to the skew-symmetric matrix tuple isometry problem, which can be solved efficiently (Theorem 1.3).

So, the hard case for the skew-symmetric matrix space isometry problem is that the matrix space contains some matrices of low rank. After applying the left and right individualization matrices, the resulting zero matrices correspond to a subspace of the skew-symmetric matrix space such that all the matrices in the subspace are of low rank.

In this section, we investigate the structure of low rank matrix spaces, i.e., matrix spaces in which every matrix is of low rank, to characterize some useful properties. In Section 5, we will use these properties to construct semi-canonical forms for tensors obtained from skew-symmetric matrix spaces so that the skew-symmetric matrix space isometry problem reduces to the skew-symmetric matrix tuple isometry problem.

In particular, we show that for a low rank matrix space $\mathfrak{A} \leq M(m, n, \mathbb{F}_p)$ such that every matrix in the space is of rank at most r, there are matrices $P \in \mathrm{GL}(m, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(n, \mathbb{F}_p)$ such that for each $A \in \mathfrak{A}$, PAQ has non-zero entries only in the last $O(r^2)$ rows or in the last $O(r^2)$ columns. Furthermore, if $\mathfrak{A}$ is a skew-symmetric matrix space, then $Q = P^T$. Similar characterizations were studied in [Fla62, AL81]. But to the author's knowledge, all the previous results require that the underlying field has at least $r + 1$ elements.

We first define the attribute set for a matrix space, as well as the kernel, complementary matrix, and formatting matrix for a matrix space and an attribute set. Since we require the property of $Q = P^T$ for the skew-symmetric matrix space, we give the definition for skew-symmetric matrix space and the definition for general (non-square) matrix space separately.

Take the general matrix space as an example. Suppose $\mathfrak{A} \leq M(m, n, \mathbb{F}_p)$ is matrix space, and there are matrices $P \in \mathrm{GL}(m, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(n, \mathbb{F}_p)$ such that for each $A \in \mathfrak{A}$, PAQ has non-zero entries only in the last α rows or in the last α columns for some integer α. Roughly speaking, P and Q are left and right formatting matrices of $\mathfrak{A}$. The row vector space S spanned by the first $m - \alpha$ rows of PA for all the $A \in \mathfrak{A}$ is a space of dimension α. To define P and Q, the attribute set corresponds to a linear basis of the row vector space S, and the complementary matrix corresponds to the submatrix of P on the last α rows.

Definition 4.1 (kernel, complementary matrix, and formatting matrix for skew-symmetric matrix spaces). Let $\mathfrak{A}$ be an $n \times n$ skew-symmetric matrix space over $\mathbb{F}_p$ for some prime $p > 2$ and positive integer n. An attribute set Λ for $\mathfrak{A}$ is a set of linearly independent row vectors in $\mathbb{F}_p^n$. The kernel for $\mathfrak{A}$ and Λ, denoted as $\ker_{\mathrm{skew}}(\mathfrak{A}, \Lambda)$, is the space spanned by all row vectors $v \in \mathbb{F}_p^n$ satisfying the following two conditions:

1. $x \cdot v^T = 0$ for each $x \in \Lambda$.

2. $\langle v\mathfrak{A} \rangle$ is a subspace of $\langle \Lambda \rangle$.

A matrix C_{skew} is a complementary matrix for skew-symmetric matrix space $\mathfrak{A}$ and attribute set Λ if

1. C_{skew} is a full rank matrix in $M(n - \dim(\ker_{\text{skew}}(\mathfrak{A}, \lambda)), n, \mathbb{F}_p)$.

2. The intersection of $\ker_{\text{skew}}(\mathfrak{A}, \Lambda)$ and the row vector space spanned by the rows of C_{skew} only contains the zero vector.

3. Let c_i be the i-th row of C_{skew}. $x \cdot c_i^T = 0$ for all the $x \in \Lambda$ and $1 \leq i \leq n - \dim(\ker_{\text{skew}}(\mathfrak{A}, \lambda)) - |\Lambda|$.

A matrix $P_{\text{skew}} \in \text{GL}(n, \mathbb{F}_p)$ is called a formatting matrix for attribute set Λ and complementary matrix C_{skew} with respect to skew-symmetric matrix space $\mathfrak{A}$, where C_{skew} is a complementary matrix for $\mathfrak{A}$ and Λ, if the following conditions hold:

1. P_{skew} is a full rank matrix.

2. The first $\dim(\ker_{\text{skew}}(\mathfrak{A}, \Lambda))$ rows of P_{skew} form a linear basis of $\ker_{\text{skew}}(\mathfrak{A}, \Lambda)$.

3. The submatrix of P_{skew} on the last $n - \dim(\ker_{\text{skew}}(\mathfrak{A}, \Lambda))$ rows equals C_{skew}.

Lemma 4.2. *Let $\mathfrak{A}$ be an $n \times n$ skew-symmetric matrix space over $\mathbb{F}_p$, Λ be an attribute set for $\mathfrak{A}$, and C_{skew} be a complementary matrix for $\mathfrak{A}$ and Λ. If P_{skew} is a formatting matrix for Λ and C_{skew} with respect to $\mathfrak{A}$, then for any $A \in \mathfrak{A}$,*

$$\left(P_{\text{skew}} A P_{\text{skew}}^T\right)[1, \dim(\ker_{\text{skew}}(\mathfrak{A}, \Lambda)); 1, \dim(\ker_{\text{skew}}(\mathfrak{A}, \Lambda))]$$

is a zero matrix.

Proof. Let v, v' be two arbitrary rows of the first $\dim(\ker_{\text{skew}}(\mathfrak{A}, \Lambda))$ rows of P_{skew}. By Definition 4.1, vA is a linear combination of vectors in Λ. Since $x \cdot v'^T = 0$ for each $x \in \Lambda$, $vAv'^T = 0$. $\square$

Definition 4.3 (kernel, complementary matrix, and formatting matrix for general matrix spaces)**.** Let $\mathfrak{A}$ be a matrix subspace of $M(m, n, \mathbb{F}_p)$. An attribute set Λ for $\mathfrak{A}$ is a set of linearly independent row vectors in $\mathbb{F}_p^n$. The kernel for $\mathfrak{A}$ and Λ, denoted as $\ker(\mathfrak{A}, \Lambda)$, is the space spanned by all row vectors $v \in \mathbb{F}_p^m$ such that $\langle v\mathfrak{A} \rangle$ is a subspace of $\langle \Lambda \rangle$.

A matrix C is a complementary matrix for $\mathfrak{A}$ and Λ if the following conditions hold:

1. C is a full rank matrix in $M(m - \dim(\ker(\mathfrak{A}, \lambda)), m, \mathbb{F}_p)$.

2. The intersection of $\ker(\mathfrak{A}, \Lambda)$ and the row vector space spanned by all the rows of C contains only the zero vector.

Given a complementary matrix C of Λ with respect to $\mathfrak{A}$, a matrix P is a left formatting matrix for Λ and C with respect to $\mathfrak{A}$ if the following conditions hold:

1. P is a matrix in $\text{GL}(m, \mathbb{F}_p)$.

2. The first $\dim(\ker(\mathfrak{A}, \Lambda))$ rows of P form a linear basis of $\ker(\mathfrak{A}, \Lambda)$.

3. The submatrix of P on the last $m - \dim(\ker(\mathfrak{A}, \Lambda))$ rows equal to C.

A matrix Q is a right formatting matrix for Λ with respect to $\mathfrak{A}$ if the following conditions hold:

1. Q is a matrix in $\text{GL}(n, \mathbb{F}_p)$.

2. Let q_i be the i-th column vector of Q. For any $1 \leq i \leq n - |\Lambda|$, $x \cdot q_i = 0$ for any $x \in \Lambda$.

Lemma 4.4. *Let $\mathfrak{A}$ be an $m \times n$ matrix space, Λ be an attribute set for $\mathfrak{A}$, and C be a complementary matrix for $\mathfrak{A}$ and Λ. If P is a left formatting matrix for Λ and C with respect to $\mathfrak{A}$, and Q is a right formatting matrix for Λ with respect to $\mathfrak{A}$, then for any $A \in \mathfrak{A}$,*

$$(PAQ)[1, \dim(\ker(\mathfrak{A}, \Lambda)); 1, n - |\Lambda|]$$

is a zero matrix.

Proof. Let v be an arbitrary row vector of the first $\dim(\ker(\mathfrak{A}, \Lambda))$ rows of P, and v' be an arbitrary column vector of the first $n - |\Lambda|$ columns of Q. For any $A \in \mathfrak{A}$, by Definition 4.3, vA is a linear combination of the row vectors in Λ. Since $x \cdot v' = 0$ for each $x \in \Lambda$ by Definition 4.3, $vAv' = 0$. $\square$

As the main observation for the structure of low rank matrix spaces (Lemma 4.6), we show that for any low rank matrix space $\mathfrak{A}$, there always exists a small attribute set such that the dimension of $\ker(\mathfrak{A}, \Lambda)$ (or $\ker_{\mathrm{skew}}(\mathfrak{A}, \Lambda)$ if $\mathfrak{A}$ is a skew-symmetric matrix space) is large.

Lemma 4.5. *Let $A_1, A_2, \ldots, A_k$ be k matrices in $M(m, n, \mathbb{F}_p)$ for some prime p and positive integers k, m, n. If there exist d row vectors $x_1, x_2, \ldots, x_d \in \mathbb{F}_p^m$ such that for every $1 \leq i < d$, the following condition holds*

$$\langle \{x_j A_\ell : 1 \leq j \leq i, 1 \leq \ell \leq k\} \rangle \neq \langle \{x_j A_\ell : 1 \leq j \leq i+1, 1 \leq \ell \leq k\} \rangle, \tag{1}$$

then there is a linear combination of $A_1, A_2, \ldots, A_k$ with rank at least $(1 - 1/p)d$.

Proof. Let X be the $d \times n$ matrix such that x_i is the i-th row of X. To prove the lemma, it is sufficient to show that if $\alpha_1, \ldots, \alpha_k$ are uniformly and independently sampled from $\{0, \ldots, p-1\}$, then we have the following expectation estimation.

$$E_{\alpha_1, \ldots, \alpha_k}\left[\mathrm{rank}\left(X\left(\sum_{\ell=1}^{k} \alpha_\ell A_\ell\right)\right)\right] \geq \left(1 - \frac{1}{p}\right)d.$$

If this is the case, then there exist $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_p$ such that

$$\mathrm{rank}\left(\sum_{\ell=1}^{k} \alpha_\ell A_\ell\right) \geq \mathrm{rank}\left(X\left(\sum_{\ell=1}^{k} \alpha_\ell A_\ell\right)\right) \geq \left(1 - \frac{1}{p}\right)d,$$

and then the lemma follows.

For any $1 \leq i \leq d$, let S_i be the set of row vectors

$$\left\{(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_p^k : x_i\left(\sum_{\ell=1}^{k} \alpha_\ell A_\ell\right) \in \langle \{x_j A_\ell : 1 \leq j \leq i-1, 1 \leq \ell \leq k\} \rangle\right\}.$$

Since $\langle \{x_j A_\ell : 1 \leq j \leq i-1, 1 \leq \ell \leq k\} \rangle$ is a row vector space, if both $(\alpha_1, \ldots, \alpha_k)$ and $(\beta_1, \ldots, \beta_k)$ are in S_i, then $(\alpha_1 + \beta_1, \ldots, \alpha_k + \beta_k)$ is also in S_i. Hence, the row vectors in S_i form a subspace of $\mathbb{F}_p^k$. By Inequality (1), S_i does not contain all the vectors in $\mathbb{F}_p^k$. Hence $|S_i| \leq p^{k-1}$. We have for each $1 \leq i \leq d$,

$$\Pr_{\alpha_1, \ldots, \alpha_k}\left[x_i\left(\sum_{\ell=1}^{k} \alpha_\ell A_\ell\right) \notin \langle \{x_j A_\ell : 1 \leq j \leq i-1, 1 \leq \ell \leq k\} \rangle\right] = \frac{p^k - |S_i|}{p^k} \geq 1 - \frac{1}{p}.$$

15

If $x_i \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right)$ is not in $\langle \{ x_j A_\ell : 1 \leq j < i, 1 \leq \ell \leq k \} \rangle$, then $x_i \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right)$ is not a linear combination of $x_1 \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right), \ldots, x_{i-1} \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right)$. Thus, we have

$$
E_{\alpha_1,\ldots,\alpha_k} \left[\mathrm{rank} \left(X \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right) \right) \right]
$$

$$
\geq \sum_{i=1}^d \mathrm{Pr}_{\alpha_1,\ldots,\alpha_k} \left[x_i \left(\sum_{\ell=1}^k \alpha_\ell A_\ell \right) \notin \langle \{ x_j A_\ell : 1 \leq j < i, 1 \leq \ell \leq k \} \rangle \right]
$$

$$
\geq \left(1 - \frac{1}{p} \right) d.
$$

$\square$

Lemma 4.6. *Let $\mathfrak{A}$ be a matrix subspace of $M(m, n, \mathbb{F}_p)$ or a skew-symmetric matrix subspace of $\mathrm{SS}(n, \mathbb{F}_p)$ such that for each $A \in \mathfrak{A}$, $\mathrm{rank}\,(A) \leq r$ for some positive integer r. There is an attribute set Λ of size $O(r^2)$ for $\mathfrak{A}$ such that*

1. *$\dim(\ker(\mathfrak{A}, \Lambda)) \geq m - O(r)$ if $\mathfrak{A}$ is a matrix subspace of $M(m, n, \mathbb{F}_p)$, or*

2. *$\dim(\ker_{\mathrm{skew}}(\mathfrak{A}, \Lambda)) \geq n - O(r^2)$ if $\mathfrak{A}$ is a skew-symmetric matrix subspace of $\mathrm{SS}(n, \mathbb{F}_p)$.*

Proof. We first consider the case that $\mathfrak{A}$ is a matrix subspace of $M(m, n, \mathbb{F}_p)$. Let $A_1, \ldots, A_k$ be a linear basis for $\mathfrak{A}$. Let $x_1, x_2, \ldots, x_d \in \mathbb{F}_p^m$ be d row vectors for some positive integer d such that for any $1 \leq i \leq d$, there are at least $p^k/2$ different $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_p$ satisfying

$$
\mathrm{rank} \left(X_i \left(\sum_{j=1}^k \alpha_j A_j \right) \right) > \mathrm{rank} \left(X_{i-1} \left(\sum_{j=1}^k \alpha_j A_j \right) \right),
$$

where for each $1 \leq i \leq d$, X_i is the $i \times m$ matrix with x_j as the j-th row of X_i for all $1 \leq j \leq i$. Since every linear combination of $A_1, \ldots, A_k$ is of rank at most r, we have

$$
d \cdot \frac{p^k}{2} \leq r \cdot p^k,
$$

which implies $d \leq 2r$. Suppose there does not exist a vector $x_{d+1} \in \mathbb{F}_p^m$ such that there are at least $p^k/2$ different $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_p$ satisfying

$$
\mathrm{rank} \left(X_{d+1} \left(\sum_{j=1}^k \alpha_j A_j \right) \right) > \mathrm{rank} \left(X_d \left(\sum_{j=1}^k \alpha_j A_j \right) \right).
$$

For each row vector $v \in \mathbb{F}_p^m$ such that $v \notin \langle x_1, \ldots, x_d \rangle$, there exist $\beta_1, \ldots, \beta_d \in \mathbb{F}_p$ such that the following condition holds for at least $\frac{p^k}{2p^d}$ different $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_p$

$$
v \cdot \left(\sum_{i=1}^k \alpha_k A_k \right) = \left(\sum_{i=1}^d \beta_i x_i \right) \left(\sum_{i=1}^k \alpha_k A_k \right).
$$

Thus, $\langle (v - \sum_{i=1}^d \beta_i x_i) \mathfrak{A} \rangle$ is a space of dimension at most $d + 1 = O(r)$. Hence, one can construct a matrix $P \in \mathrm{GL}(m, \mathbb{F}_p)$ satisfying the following properties: Let p_i denote the row vector of the i-th row of P,

1. $p_i = x_i$ for any $1 \leq i \leq d$.

2. $\langle p_i \mathfrak{A} \rangle$ is of dimension at most $O(r)$ for any $d+1 \leq i \leq m$.

Let $i_1, \ldots, i_t \in \{d+1, \ldots, m\}$ be a sequence of integers such that for each $1 \leq j \leq t$

$$\left\langle \bigcup_{\ell=1}^{j-1} \langle p_{i_\ell} \mathfrak{A} \rangle \right\rangle \neq \left\langle \bigcup_{\ell=1}^{j} \langle p_{i_\ell} \mathfrak{A} \rangle \right\rangle.$$

By Lemma 4.5, $t \leq r/(1 - 1/p) \leq 2r$. Hence, the dimension of

$$\mathfrak{S} = \left\langle \bigcup_{i=d+1}^{n} \langle p_i \mathfrak{A} \rangle \right\rangle$$

is at most $2r \cdot O(r) = O(r^2)$. Let Λ be an arbitrary linear basis of $\mathfrak{S}$. We have $|\Lambda| = O(r^2)$. Since $\langle p_i \mathfrak{A} \rangle$ is a subspace of $\langle \Lambda \rangle$ for each $d+1 \leq i \leq m$, $\langle p_{d+1}, \ldots, p_m \rangle$ is a subspace of $\ker(\mathfrak{A}, \Lambda)$. Hence, $\dim(\ker(\mathfrak{A}, \Lambda)) \geq m - d = m - O(r)$.

Now we consider the case that $\mathfrak{A}$ is a skew-symmetric matrix subspace of $\mathrm{SS}(n, \mathbb{F}_p)$. With a similar argument above, there is a set Λ of linearly independent row vectors over $\mathbb{F}_p^n$ satisfying the following conditions:

1. $|\Lambda| = O(r^2)$.

2. Let $\mathfrak{S}$ be the space spanned by row vectors $v \in \mathbb{F}_p^n$ such that $\langle v \mathfrak{A} \rangle$ is a subspace of $\langle \Lambda \rangle$. $\dim(\mathfrak{S}) \geq n - O(r)$.

Let $\mathfrak{T}$ be the space spanned by row vectors $v \in \mathbb{F}_p^n$ such that $x \cdot v^T = 0$ for all the $x \in \Lambda$. We have $\dim(\mathfrak{T}) = n - |\Lambda|$. Hence,

$$\begin{aligned}
\dim(\ker_{\mathrm{skew}}(\mathfrak{A}, \Lambda)) &= \dim(\mathfrak{S} \cap \mathfrak{T}) \\
&\geq \dim(\mathfrak{S}) + \dim(\mathfrak{T}) - n \\
&= n - O(r) + n - |\Lambda| - n \\
&= n - O(r^2).
\end{aligned}$$

$\square$

We also prove some useful properties for kernels with respect to a matrix space and an attribute set.

Lemma 4.7. *Let $\mathfrak{A}$ be a matrix space. Let Λ and Λ' be two attribute sets of $\mathfrak{A}$ such that Λ is a subset of Λ'. Then $\ker(\mathfrak{A}, \Lambda)$ is a subspace of $\ker(\mathfrak{A}, \Lambda')$.*

Let $\mathfrak{B}$ be a skew-symmetric subspace such that each matrix in $\mathfrak{B}$ is of dimension $n \times n$. Let Δ and Δ' be two attribute sets of $\mathfrak{B}$ such that Δ is a subset of Δ'. Then $\dim(\ker_{\mathrm{skew}}(\mathfrak{A}, \Delta')) \geq \dim(\ker_{\mathrm{skew}}(\mathfrak{A}, \Delta)) - |\Delta'| + |\Delta|$.

Proof. By Definition 4.3, every row vector $x \in \ker(\mathfrak{A}, \Lambda)$ is also a vector in $\ker(\mathfrak{A}, \Lambda')$. Hence, $\ker(\mathfrak{A}, \Lambda)$ is a subspace of $\ker(\mathfrak{A}, \Lambda')$.

For $\mathfrak{B}$, every row vector $v \in \ker_{\mathrm{skew}}(\mathfrak{B}, \Delta)$ satisfies the condition that $\langle v \mathfrak{B} \rangle$ is a subspace of $\langle \Delta' \rangle$. Let $\Delta'' = \Delta' \setminus \Delta$, and S denote the space

$$\langle \{v \in \mathbb{F}_p^n : x \cdot v^T = 0 \text{ for all } x \in \Delta''\} \rangle.$$

17

Hence, $\ker_{\text{skew}}(\mathfrak{B}, \Delta) \cap S$ is a subspace of $\ker_{\text{skew}}(\mathfrak{B}, \Delta')$. Since $\dim(S) = n - |\Delta''|$,

$$\begin{aligned}
\dim(\ker_{\text{skew}}(\mathfrak{B}, \Delta')) &\geq \dim(\ker_{\text{skew}}(\mathfrak{B}, \Delta)) + \dim(S) - n \\
&= \dim(\ker_{\text{skew}}(\mathfrak{B}, \Delta)) + n - |\Delta''| - n \\
&= \dim(\ker_{\text{skew}}(\mathfrak{B}, \Delta)) - |\Delta'| + |\Delta|.
\end{aligned}$$

$\square$

Lemma 4.8. *Let $\mathfrak{A}$ be a matrix subspace of $M(m, n, \mathbb{F}_p)$, X be a matrix in $\text{GL}(m, \mathbb{F}_p)$, and Y be a matrix in $\text{GL}(n, \mathbb{F}_p)$. For any attribute set Λ of $\mathfrak{A}$, let $\Lambda' = \{xY : x \in \Lambda\}$. Then $\ker(\mathfrak{A}, \Lambda)X^{-1} = \ker(X\mathfrak{B}Y, \Lambda')$.*

Let $\mathfrak{B}$ be a skew-symmetric matrix subspace such that each matrix in $\mathfrak{B}$ is of dimension $n \times n$, and S be a matrix in $\text{GL}(n, \mathbb{F}_p)$. For any attribute set Δ of $\mathfrak{B}$, let $\Delta' = \{xS^T : x \in \Delta\}$. Then $\ker_{\text{skew}}(\mathfrak{A}, \Delta)S^{-1} = \ker_{\text{skew}}(S\mathfrak{B}S^T, \Delta')$.

Proof. Let v be an arbitrary row vector in $\ker(\mathfrak{A}, \Lambda)$. By Definition 4.3, $\langle vA \rangle$ is a subspace of $\langle \Lambda \rangle$ for any $A \in \mathfrak{A}$. Hence, $\langle vX^{-1}XA \rangle$ is a subspace of $\langle \Lambda \rangle$, and thus $\langle vX^{-1}XAY \rangle$ is a subspace of $\langle \Lambda' \rangle$. By Definition 4.3, vX^{-1} is a row vector in $\ker(X\mathfrak{B}Y, \Lambda')$.

Similarly, let v' be an arbitrary row vector in $\ker(X\mathfrak{A}Y, \Lambda')$. By Definition 4.3, $\langle v'XAY \rangle$ is a subspace of $\langle \Lambda' \rangle$ for any $A \in \mathfrak{A}$. Hence, $\langle v'XA \rangle$ is a subspace of $\langle \Lambda \rangle$. By Definition 4.3, $v'X$ is a row vector in $\ker(\mathfrak{B}, \Lambda)$. Hence, $\ker(\mathfrak{A}, \Lambda)X^{-1} = \ker(X\mathfrak{B}Y, \Lambda')$.

Now we consider $\mathfrak{B}$. Let v be an arbitrary row vector in $\ker_{\text{skew}}(\mathfrak{B}, \Delta)$. By Definition 4.1, we have

1. $\langle vB \rangle$ is a subspace of $\langle \Delta \rangle$ for any $B \in \mathfrak{A}$.

2. $x \cdot v^T = 0$ for any $x \in \Delta$.

Hence, $\langle vS^{-1}SB \rangle$ is a subspace of $\langle \Delta \rangle$, and thus $\langle vS^{-1}SBS^T \rangle$ is a subspace of $\langle \Delta' \rangle$. In addition, for any $x' \in \Delta'$, $x'(S^T)^{-1}$ is a vector in Δ, and thus we have

$$x' \cdot (vS^{-1})^T = x'(S^{-1})^T \cdot v^T = x'(S^T)^{-1} \cdot v^T = 0.$$

Hence vS^{-1} is a vector in $\ker_{\text{skew}}(S\mathfrak{B}S^T, \Delta')$.

Similarly, let v' be an arbitrary row vector in $\ker_{\text{skew}}(S\mathfrak{B}S^T, \Delta')$. By Definition 4.1, we have

1. $\langle v'SBS^T \rangle$ is a subspace of $\langle \Delta' \rangle$ for any $B \in \mathfrak{A}$.

2. $x' \cdot v'^T = 0$ for any $x' \in \Delta'$.

Hence, $\langle v'SB \rangle$ is a subspace of $\langle \Delta \rangle$. In addition, for any $x \in \Delta$, xS^T is a vector in Δ', and thus we have

$$x \cdot (v'S)^T = x \cdot S^T v'^T = xS^T \cdot v'^T = 0.$$

Hence $v'S$ is a vector in $\ker_{\text{skew}}(\mathfrak{B}, \Delta)$. Hence, $\ker_{\text{skew}}(\mathfrak{B}, \Delta)S^{-1} = \ker_{\text{skew}}(S\mathfrak{B}S^T, \Delta')$. $\square$

Lemma 4.9. *Let $\mathfrak{A}$ be a matrix subspace of $M(m, n, \mathbb{F}_p)$ and $\mathfrak{B}$ be a skew-symmetric matrix subspace of $\text{SS}(n, \mathbb{F}_p)$. Let Λ be a set of linearly independent row vectors in $\mathbb{F}_p^n$, and C_{skew} be a complementary matrix for $\mathfrak{B}$ and Λ. Then for any formatting matrix P_{skew} for Λ and C_{skew} with respect to $\mathfrak{B}$, P_{skew}^T is a right formatting matrix for $\mathfrak{A}$ and Λ.*

Proof. By Definition 4.1, for any row vector v that corresponds to one of the first $n - |\Lambda|$ rows of P_{skew}, $x \cdot v^T = 0$ for any $x \in \Lambda$. By Definition 4.3, P_{skew}^T is a right formatting matrix for $\mathfrak{A}$ and Λ. $\square$

5 Semi-canonical form of skew-symmetric matrix space tensors

In this section, we combine the matrix space individualization-refinement developed in Section 3 and the low rank matrix space characterization developed in Section 4 to analyze the skew-symmetric matrix spaces.

The main result of this section is a structure that accommodates the matrix space individualization-refinement and the low rank matrix space characterization. The purpose of such a structure is to establish a partial correspondence between matrices from two skew-symmetric matrix spaces after applying the two techniques to the skew-symmetric matrix spaces.

For convenience, we use a 3-tensor representation of skew-symmetric matrix spaces and define the semi-canonical form of skew-symmetric matrix space tensors.

5.1 Skew-symmetric matrix space tensors

Following [LQ17], we define the tensor representation of a skew-symmetric matrix space.

Definition 5.1. Let $\mathfrak{G}$ be a skew-symmetric matrix subspace of $\mathrm{SS}(n, \mathbb{F}_p)$ with dimension m. A 3-tensor $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$ is a tensor of $\mathfrak{G}$ if $\mathfrak{G}$ is equal to the space spanned by $A_1, \ldots, A_m$, where $A_i[j, k] = \mathbf{G}[i, j, k]$ for all the $1 \le i \le m$ and $1 \le j, k \le n$, and $\mathbf{G}[i, j, k]$ is the (i, j, k)-th entry of $\mathbf{G}$.

Given a skew-symmetric matrix space tensor $\mathbf{G}$, we use $\mathfrak{X}_{\mathbf{G},i}$ to denote the $n \times n$ matrix such that $\mathfrak{X}_{\mathbf{G},i}[j, k] = \mathbf{G}[i, j, k]$, use $\mathfrak{Y}_{\mathbf{G},j}$ to denote the $m \times n$ matrix such that $\mathfrak{Y}_{\mathbf{G},j}[i, k] = \mathbf{G}[i, j, k]$, and use $\mathfrak{Z}_{\mathbf{G},k}$ to denote the $m \times n$ matrix such that $\mathfrak{Z}_{\mathbf{G},k}[i, j] = \mathbf{G}[i, j, k]$ for all the $1 \le i \le m, 1 \le j, k \le n$. We also use $\mathfrak{X}_{\mathbf{G}}$ to denote the space $\langle \mathfrak{X}_{\mathbf{G},1}, \ldots \mathfrak{X}_{\mathbf{G},m} \rangle$, use $\mathfrak{Y}_{\mathbf{G}}$ to denote the space $\langle \mathfrak{Y}_{\mathbf{G},1}, \ldots \mathfrak{Y}_{\mathbf{G},n} \rangle$, and use $\mathfrak{Z}_{\mathbf{G}}$ to denote the space $\langle \mathfrak{Z}_{\mathbf{G},1}, \ldots \mathfrak{Z}_{\mathbf{G},n} \rangle$.

Fact 5.2. *Let $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$ be the tensor for a skew-symmetric matrix space. Then the following properties hold:*

1. *$\mathfrak{X}_{\mathbf{G}}$ is a skew-symmetric matrix space of dimension m.*

2. *$\mathfrak{Y}_{\mathbf{G}}$ and $\mathfrak{Z}_{\mathbf{G}}$ are matrix spaces of dimension n.*

3. *$\mathfrak{Y}_{\mathbf{G},j} = -\mathfrak{Z}_{\mathbf{G},j}$ for all the $1 \le j \le n$.*

Proof. The first and second properties are obtained by the definition of $\mathbf{G}$ and Fact 2.8. For the third property, since $\mathbf{G}[i, j, k] = -\mathbf{G}[i, k, j]$ holds for any $1 \le i \le m, 1 \le j, k \le n$, we have

$$\mathfrak{Y}_{\mathbf{G},j}[i, k] = \mathbf{G}[i, j, k] = -\mathbf{G}[i, k, j] = -\mathfrak{Z}_{\mathbf{G},j}[i, k]$$

for any $1 \le i \le m, 1 \le j, k \le n$. $\qquad\square$

Let N be a matrix in $\mathrm{GL}(n, \mathbb{F}_p)$ and M be a matrix in $\mathrm{GL}(m, \mathbb{F}_p)$. The transform of $\mathbf{G}$ by N and M, denoted as $\mathrm{Trans}_{N,M}(\mathbf{G})$, is the tensor $\mathbf{H} \in \mathbb{F}_p^{m \times n \times n}$ such that

$$\mathfrak{X}_{\mathbf{H},i} = \sum_{i'=1}^{m} M[i, i'] \cdot \left(N \cdot \mathfrak{X}_{\mathbf{G},i'} \cdot N^T \right).$$

We define the isometry of two tensors.

Definition 5.3. Let $\mathbf{G}, \mathbf{H} \in \mathbb{F}_p^{m \times n \times n}$ be tensors of two skew-symmetric matrix spaces. $\mathbf{G}$ and $\mathbf{H}$ are isometric if there are two matrices $N \in \mathrm{GL}(n, \mathbb{F}_p)$ and $M \in \mathrm{GL}(m, \mathbb{F}_p)$ such that $\mathrm{Trans}_{N,M}(\mathbf{G}) = \mathbf{H}$.

Lemma 5.4. *Let $\mathfrak{G}$ and $\mathfrak{H}$ be two skew-symmetric matrix spaces. $\mathfrak{G}$ and $\mathfrak{H}$ are isometric if and only if their tensors are isometric.*

Proof. Let $\mathbf{G}$ and $\mathbf{H}$ be the tensors of $\mathfrak{G}$ and $\mathfrak{H}$, respectively. Let $(G_1, \ldots, G_m)$ be the linear basis of $\mathfrak{G}$ such that $\mathbf{G}[i, j, k] = G_i[j, k]$ for all the $1 \leq i \leq m$ and $1 \leq j, k \leq n$. Let $(H_1, \ldots, H_m)$ be the linear basis of $\mathfrak{H}$ such that $\mathbf{H}[i, j, k] = H_i[j, k]$ for all the $1 \leq i \leq m$ and $1 \leq j, k \leq n$.

If $\mathfrak{G}$ and $\mathfrak{H}$ are isometric, then by Definition 2.5, there is a matrix $N \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $N\mathfrak{G}N^T = \mathfrak{H}$. Hence, there is a matrix $M \in \mathrm{GL}(m, \mathbb{F}_p)$ such that

$$H_i = \sum_{i'=1}^{m} M[i, i'] \cdot \left(N \cdot G_i \cdot N^T \right)$$

for all the $1 \leq i \leq m$. By the definition of tensor transform, we have $\mathrm{Trans}_{N,M}(\mathbf{G}) = \mathbf{H}$.

If $\mathbf{G}$ and $\mathbf{H}$ are isometric, then by Definition 5.3, there are matrices $N \in \mathrm{GL}(n, \mathbb{F}_p)$ and $M \in \mathrm{GL}(m, \mathbb{F}_p)$ such that $\mathrm{Trans}_{N,M}(\mathbf{G}) = \mathbf{H}$. Hence, we have $H_i = \sum_{i'=1}^{m} M[i, i'] \cdot N \cdot G_i \cdot N^T$ for all the $1 \leq i \leq m$. Thus, $\mathfrak{G}$ and $\mathfrak{H}$ are isometric. $\qquad\square$

Fact 5.5. *Let $\mathbf{G}$ be a skew symmetric matrix space tensor in $\mathbb{F}_p^{m \times n \times n}$. Let L_1 and L_2 be two matrices in $\mathrm{GL}(n, \mathbb{F}_p)$, and R_1 and R_2 be two matrices in $\mathrm{GL}(m, \mathbb{F}_p)$. Then*

$$\mathrm{Trans}_{L_1 \cdot L_2, R_1 \cdot R_2}(\mathbf{G}) = \mathrm{Trans}_{L_1, R_1}\left(\mathrm{Trans}_{L_2, R_2}(\mathbf{G}) \right).$$

Proof. By the definition of $\mathrm{Trans}_{L_1 \cdot L_2, R_1 \cdot R_2}(\mathbf{G})$, we have

$$
\begin{aligned}
\mathfrak{X}_{\mathrm{Trans}_{L_1 \cdot L_2, R_1 \cdot R_2}(\mathbf{G}), i} &= \sum_{i'=1}^{m} (R_1 \cdot R_2)[i, i'] \cdot \left((L_1 \cdot L_2) \cdot \mathfrak{X}_{\mathbf{G}, i'} \cdot (L_1 \cdot L_2)^T \right) \\
&= \sum_{i'=1}^{m} \sum_{i''=1}^{m} R_1[i, i''] \cdot R_2[i'', i'] \cdot \left(L_1 \left(L_2 \cdot \mathfrak{X}_{\mathbf{G}, i'} \cdot L_2^T \right) L_1^T \right) \\
&= \sum_{i''=1}^{m} R_1[i, i''] \left(L_1 \left(\sum_{i'=1}^{m} \cdot R_2[i'', i'] \cdot L_2 \cdot \mathfrak{X}_{\mathbf{G}, i'} \cdot L_2^T \right) L_1^T \right) \\
&= \sum_{i''=1}^{m} R_1[i, i''] \left(L_1 \cdot \mathfrak{X}_{\mathrm{Trans}_{L_2, R_2}(\mathbf{G}), i''} \cdot L_1^T \right) \\
&= \mathfrak{X}_{\mathrm{Trans}_{L_1, R_1}\left(\mathrm{Trans}_{L_2, R_2}(\mathbf{G}) \right), i}.
\end{aligned}
$$

$\qquad\square$

5.2 Semi-canonical form of skew-symmetric matrix space tensors

We first give the intuition behind the semi-canonical form of a skew-symmetric tensor. Consider a skew-symmetric matrix space tensor $\mathbf{G}$. Suppose we apply left and right individualization matrices L_{skew} and R_{skew} for space $\mathfrak{X}_{\mathbf{G}}$, and reorder matrices of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$ such that $(\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m})$ becomes a semi-canonical basis of $\mathfrak{X}_{\mathbf{G}}$ with respect to L_{skew} and R_{skew}. Let P_{skew} be a formatting matrix for $\mathrm{zero}_{L_{\mathrm{skew}}, R_{\mathrm{skew}}}(\mathfrak{X}_{\mathbf{G}})$ and an attribute set. If we apply the formatting matrix P_{skew} to each of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$ in a way that $\mathfrak{X}_{\mathbf{G},i}$ becomes $P_{\mathrm{skew}} \mathfrak{X}_{\mathbf{G},i} P_{\mathrm{skew}}^T$, then the first $\dim(\mathrm{zero}_{L_{\mathrm{skew}}, R_{\mathrm{skew}}}(\mathfrak{X}_{\mathbf{G}}))$ matrices of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$ have non-zero entries only in the last few rows or columns. See Figure 4(a) for an illustration: The black layers correspond to the first

Figure 4: (a) The matrix space individualization-refinement and the low rank matrix characterization of $\mathfrak{X}_{\mathbf{G}}$, and (b) the matrix space individualization-refinement and the low rank matrix characterization of $\mathfrak{Y}_{\mathbf{G}}$

$\dim(\text{zero}_{L_{\text{skew}}, R_{\text{skew}}}(\mathfrak{X}_{\mathbf{G}}))$ matrices of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$, and the red layers correspond to the remaining matrices of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$. The rectangles enclosed by black dashed lines are zero submatrices in the first $\dim(\text{zero}_{L_{\text{skew}}, R_{\text{skew}}}(\mathfrak{X}_{\mathbf{G}}))$ matrices of $\mathfrak{X}_{\mathbf{G},1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$.

We apply the same operation for the matrix space $\mathfrak{Y}_{\mathbf{G}}$. Suppose we apply left and right individualization matrices L and R for space $\mathfrak{Y}_{G}$, and reorder matrices of $\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n}$ such that $(\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n})$ becomes a semi-canonical basis of $\mathfrak{Y}_{\mathbf{G}}$ with respect to L and R. If we further apply left formatting matrix P and right formatting matrix Q to each of $\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n}$ in a way that $\mathfrak{Y}_{\mathbf{G},i}$ becomes $P \cdot \mathfrak{Y}_{\mathbf{G},i} \cdot Q$, then the first $\dim(\text{zero}_{L,R}(\mathfrak{Y}_{\mathbf{G}}))$ matrices of $\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n}$ have non-zero entries only in the last few rows or columns.

To maintain the skew-symmetric property, we also apply the same operation on $\mathfrak{Z}_{\mathbf{G}}$ using $\mathfrak{Z}_{\mathbf{G},j} = -\mathfrak{Y}_{\mathbf{G},j}$ for any $1 \leq j \leq n$. Then the first $\dim(\text{zero}_{L,R}(\mathfrak{Z}_{\mathbf{G}}))$ matrices of $\mathfrak{Z}_{\mathbf{G},1}, \ldots, \mathfrak{Z}_{\mathbf{G},n}$ have non-zero entries only in the last few rows or columns. See Figure 4(b) for an illustration: The black layers correspond to the first $\dim(\text{zero}_{L,R}(\mathfrak{Y}_{\mathbf{G}}))$ matrices of $\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n}$. The blue layers correspond to the matrices affected by the operation on $\mathfrak{Z}_{\mathbf{G}}$ so that the last few columns have zero entries in the first few rows. The red layers are the remaining matrices of $\mathfrak{Y}_{\mathbf{G},1}, \ldots, \mathfrak{Y}_{\mathbf{G},n}$.

We show that if the attribute sets used for $\mathfrak{X}_{\mathbf{G}}$ and $\mathfrak{Y}_{\mathbf{H}}$ are the same, then with fixed individualization matrices and complementary matrices, by carefully combining the matrix space individualization-refinement and low rank space characterization for $\mathfrak{X}_{\mathbf{G}}, \mathfrak{Y}_{\mathbf{G}}$, and $\mathfrak{Z}_{\mathbf{G}}$ together, we obtain the semi-canonical form of the tensor as shown in Figure 2(a). The blue region is called the surface of the semi-canonical form of the tensor. The other region (the union of the red cube and the transparent region) is called the kernel of the semi-canonical form of the tensor. This is also the underlying reason for the term "semi-canonical form": The semi-canonical forms can be different with respect to the fixed attribute set, individualization matrices, and complementary matrices, as the formatting matrices used can be different. But the kernels of different semi-canonical forms are the same (Lemma 5.10).

If two tensors are isometric, and semi-canonical forms of the two tensors are obtained by the same individualization matrices, complementary matrices, and attribute sets (up to an isometry between the two tensors), then the kernels of the two semi-canonical forms are the same. So, to determine whether the two tensors are isometric, one only needs to check further if there are formatting matrices to make the surfaces of the two tensors to be identical.

21

Before formally defining the semi-canonical form of a tensor, we first define the characterization tuple, which consists of the individualization matrices, the attribute set, and the complementary matrices used to define the semi-canonical form.

Definition 5.6. Let $\mathbf{G} \in \mathbb{F}_p^{n \times n \times m}$ be a tensor for a skew-symmetric matrix space. A characterization tuple for a skew-symmetric matrix space tensor $\mathbf{G}$ is a 5-tuple

$$(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$$

satisfying the following conditions:

1. L_{skew} is a matrix with n columns such that L_{skew} and L_{skew}^T are left and right individualization matrices for the skew-symmetric matrix space $\mathfrak{X}_{\mathbf{G}}$.

2. L is a matrix with m columns such that L and L_{skew}^T are left and right individualization matrices for the matrix space $\mathfrak{Y}_{\mathbf{G}}$.

3. Λ is is an attribute set for both $\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_{\mathbf{G}})$ and $\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_{\mathbf{G}})$.

4. C_{skew} is a complementary matrix for $\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_{\mathbf{G}})$ and Λ.

5. C is a complementary matrix for $\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_{\mathbf{G}})$ and Λ.

Remark 5.7. We remark that in the 5-tuple $(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$, L_{skew}, L and Λ can be arbitrary, but C_{skew} and C are not arbitrary. C_{skew} needs to be a complementary matrix for $\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_{\mathbf{G}})$ and Λ, and C needs to be a complementary matrix for $\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_{\mathbf{G}})$ and Λ.

We further define a few notations for convenience. Let

$$\mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)}$$

be the space spanned by $\sum_{i=1}^m v[i] \cdot \mathfrak{X}_{\mathbf{G}, i}$ for all the $v \in \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)$, and

$$\mathfrak{Y}_{\mathbf{G}, \ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)}$$

be the space spanned by $\sum_{j=1}^n v[j] \cdot \mathfrak{Y}_{\mathbf{G}, j}$ for all the $v \in \ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)$. Let

$$\alpha_{\mathfrak{X}, \mathbf{G}, L_{\mathrm{skew}}} := \dim\left(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}\left(\mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)}\right)\right),$$

$$\beta_{\mathfrak{X}, \mathbf{G}, L_{\mathrm{skew}}} := \dim\left(L_{\mathrm{skew}} \cdot \mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)} \cdot L_{\mathrm{skew}}^T\right),$$

$$\alpha_{\mathfrak{Y}, \mathbf{G}, L_{\mathrm{skew}}, L} := \dim\left(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}\left(\mathfrak{Y}_{\mathbf{G}, \ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)}\right)\right),$$

and

$$\beta_{\mathfrak{Y}, \mathbf{G}, L_{\mathrm{skew}}, L} := L \cdot \mathfrak{Y}_{\mathbf{G}, \ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)} \cdot L_{\mathrm{skew}}^T.$$

If $\mathbf{G}, L_{\mathrm{skew}}$ and L are fixed and there is no confusion, we use $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$ to denote $\alpha_{\mathfrak{X}, \mathbf{G}, L_{\mathrm{skew}}}$, $\beta_{\mathfrak{X}, \mathbf{G}, L_{\mathrm{skew}}}$, $\alpha_{\mathfrak{Y}, \mathbf{G}, L_{\mathrm{skew}}, L}$ and $\beta_{\mathfrak{Y}, \mathbf{G}, L_{\mathrm{skew}}, L}$, respectively. We define the semi-canonical form for a skew-symmetric tensor space tensor as follows.

Definition 5.8. A semi-canonical form of $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$ with respect to $(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$, denoted as $\mathbf{SC}_{L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C}(\mathbf{G})$ (or $\mathbf{SC}(\mathbf{G})$ if there is no confusion), is a tensor with the same dimension as $\mathbf{G}$ such that $\mathbf{SC}_{L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C}(\mathbf{G}) = \mathrm{Trans}_{N, M}(\mathbf{G})$ for some $N \in \mathrm{GL}(n, \mathbb{F}_p)$ and $M \in \mathrm{GL}(m, \mathbb{F}_p)$ satisfying the following two conditions:

1. N is a formatting matrix for Λ and C_{skew} with respect to the skew-symmetric matrix space $\text{zero}_{L_{\text{skew}}, L_{\text{skew}}^T}(\mathfrak{X}_{\mathbf{G}})$ such that for $\text{Trans}_{N, I_m}(\mathbf{G})$,

$$\left(\mathfrak{Y}_{\text{Trans}_{N, I_m}(\mathbf{G}), 1} \cdot (N^T)^{-1}, \ldots, \mathfrak{Y}_{\text{Trans}_{N, I_m}(\mathbf{G}), \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}} \cdot (N^T)^{-1} \right)$$

is a semi-canonical basis of the matrix space $\mathfrak{Y}_{\mathbf{G}, \ker_{\text{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)}$ with respect to L and L_{skew}^T.

2. M is a left formatting matrix for Λ and C with respect to matrix space $\text{zero}_{L, L_{\text{skew}}^T}(\mathfrak{Y}_{\mathbf{G}})$ such that for $\text{Trans}_{I_n, M}(\mathbf{G})$,

$$\left(\mathfrak{X}_{\text{Trans}_{I_n, M}(\mathbf{G}), 1}, \ldots, \mathfrak{X}_{\text{Trans}_{I_n, M}(\mathbf{G}), \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}} \right)$$

is a semi-canonical basis of matrix space $\mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)}$ with respect to L_{skew} and L_{skew}^T.

In addition, $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$ and $\beta_{\mathfrak{Y}}$ are the parameters of the semi-canonical form.

We remark that the semi-canonical form, with respect to fixed $(L_{\text{skew}}, L, \Lambda, C_{\text{skew}}, C)$, might not be unique using different transforming matrices M and N. But we show that the kernels of the semi-canonical forms with a fixed characterization tuple are identical (Lemma 5.10).

Lemma 5.9. *Let* $\mathbf{SC}(\mathbf{G})$ *be a semi-canonical form of* $\mathbf{G}$ *with parameters* $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, *and* $\beta_{\mathfrak{Y}}$. *Then* $\mathbf{SC}(\mathbf{G})[i, j, k] = 0$ *if at least one of the following conditions holds:*

1. $1 \le i \le \alpha_{\mathfrak{X}}$, $1 \le j, k \le \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$;

2. $1 \le i \le \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}$, $1 \le j \le \alpha_{\mathfrak{Y}}$, $1 \le k \le \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$;

3. $1 \le i \le \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}$, $1 \le j \le \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$, $1 \le k \le \alpha_{\mathfrak{Y}}$.

Proof. By Definition 5.8, there are two matrices M and N such that $\mathbf{SC}(\mathbf{G}) = \text{Trans}_{N, M}(\mathbf{G})$. Recall that N is a formatting matrix for Λ and C_{skew} with respect to

$$\text{zero}_{L_{\text{skew}}, L_{\text{skew}}^T}(\mathfrak{X}_{\mathbf{G}}).$$

By Definition 5.8, for any $1 \le i \le \alpha_{\mathfrak{X}}$, $\mathfrak{X}_{\text{Trans}_{I_n, M}(\mathbf{G}), i}$ is a matrix in

$$\text{zero}_{L_{\text{skew}}, L_{\text{skew}}^T}\left(\mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)} \right),$$

which is a subspace of $\text{zero}_{L_{\text{skew}}, L_{\text{skew}}^T}(\mathfrak{X}_{\mathbf{G}})$. Since

$$\mathfrak{X}_{\mathbf{SC}(\mathbf{G}), i} = N \cdot \mathfrak{X}_{\text{Trans}_{I_n, M}(\mathbf{G}), i} \cdot N^T,$$

$\mathfrak{X}_{\mathbf{SC}(\mathbf{G}), i}[1, \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}; 1, \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}]$ is a zero matrix. Hence, if the first condition holds, then $\mathbf{SC}(\mathbf{G})[i, j, k] = 0$.

Notice that M is a left formatting matrix for Λ and C with respect to

$$\text{zero}_{L, L_{\text{skew}}^T}(\mathfrak{Y}_{\mathbf{G}}),$$

and N^T is a right formatting matrix for Λ and C with respect to

$$\text{zero}_{L, L_{\text{skew}}^T}(\mathfrak{Y}_{\mathbf{G}})$$

by Lemma 4.9. Since for any $1 \leq j \leq \alpha_{\mathfrak{Y}}$

$$\mathfrak{Y}_{\mathbf{SC}(\mathbf{G}),j} = M \cdot \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),i} = M \cdot Y_i \cdot N^T$$

for some $Y_i \in \mathfrak{Y}_{\mathbf{G},\ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}},\Lambda)}$ by Definition 5.8, $\mathfrak{Y}_{\mathbf{SC}(\mathbf{G}),j}[1,\alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}; 1, \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}]$ is a zero matrix. Hence, if the second condition holds, then $\mathbf{SC}(\mathbf{G})[i,j,k] = 0$.

Since $\mathfrak{Z}_{\mathbf{SC}(\mathbf{G}),j} = -\mathfrak{Y}_{\mathbf{SC}(\mathbf{G}),j}$ for all the $1 \leq j \leq n$, if the third condition holds, then $\mathbf{SC}(\mathbf{G})[i,j,k] = 0$. $\qquad \square$

Lemma 5.10. *Let* $\mathbf{G} \in \mathbb{F}_p^{n \times n \times m}$ *be a tensor for a skew-symmetric matrix space. If* $\mathbf{SC}(\mathbf{G})$ *and* $\mathbf{SC}(\mathbf{G})'$ *are two semi-canonical forms of* $\mathbf{G}$ *with respect to the same characterization tuple with parameters* $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, *and* $\beta_{\mathfrak{Y}}$, *then we have the following properties.*

1. *There are two matrices*

$$M^{\dagger} = \begin{pmatrix} X & 0 & 0 \\ Y & I_{\beta_{\mathfrak{X}}} & 0 \\ 0 & 0 & I_{m-\alpha_{\mathfrak{X}}-\beta_{\mathfrak{X}}} \end{pmatrix} \text{ and } N^{\dagger} = \begin{pmatrix} X' & 0 & 0 \\ Y' & I_{\beta_{\mathfrak{Y}}} & 0 \\ 0 & 0 & I_{n-\alpha_{\mathfrak{Y}}-\beta_{\mathfrak{Y}}} \end{pmatrix} \qquad (2)$$

for some $X \in \mathrm{GL}(\alpha_{\mathfrak{X}}, \mathbb{F}_p)$, $X' \in \mathrm{GL}(\alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, $Y \in M(\beta_{\mathfrak{X}}, \alpha_{\mathfrak{X}}, \mathbb{F}_p)$, *and* $Y' \in M(\beta_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$ *such that* $\mathrm{Trans}_{N^{\dagger},M^{\dagger}}(\mathbf{SC}(\mathbf{G})) = \mathbf{SC}(\mathbf{G})'$.

2. $\mathbf{SC}(\mathbf{G})[i,j,k] = \mathbf{SC}(\mathbf{G})'[i,j,k]$ *for any* $1 \leq i \leq \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}, 1 \leq j, k \leq \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$.

Proof. Let N and M be two matrices such that $\mathbf{SC}(\mathbf{G}) = \mathrm{Trans}_{N,M}(\mathbf{G})$. Let N' and M' be two matrices such that $\mathbf{SC}(\mathbf{G})' = \mathrm{Trans}_{N',M'}(\mathbf{G})$. We prove the first property with $N^{\dagger} = N' \cdot N^{-1}$ and $M^{\dagger} = M' \cdot M^{-1}$. By Fact 5.5, we have $\mathrm{Trans}_{N^{\dagger},M^{\dagger}}(\mathbf{SC}(\mathbf{G})) = \mathbf{SC}(\mathbf{G})'$. So we only need to prove that $M^{\dagger}$ and $N^{\dagger}$ satisfy Equation (2).

By Definition 5.8 and Lemma 3.4, we have the following properties for the matrix space $\mathfrak{X}_{\mathbf{G}}$:

(a). For the $\mathfrak{X}_{\mathbf{G},\ker(\mathfrak{Y},\Lambda)}$ we have

$$\mathrm{zero}_{L_{\mathrm{skew}},L_{\mathrm{skew}}^T}\left(\mathfrak{X}_{\mathbf{G},\ker(\mathfrak{Y},\Lambda)}\right) = \left\langle \mathfrak{X}_{\mathrm{Trans}_{I_n,M}(\mathbf{G}),1}, \ldots, \mathfrak{X}_{\mathrm{Trans}_{I_n,M}(\mathbf{G}),\alpha_{\mathfrak{X}}} \right\rangle$$
$$= \left\langle \mathfrak{X}_{\mathrm{Trans}_{I_n,M'}(\mathbf{G}),1}, \ldots, \mathfrak{X}_{\mathrm{Trans}_{I_n,M'}(\mathbf{G}),\alpha_{\mathfrak{X}}} \right\rangle.$$

(b). For all the $\alpha_{\mathfrak{X}} + 1 \leq i \leq \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}$,

$$\mathfrak{X}_{\mathrm{Trans}_{I_n,M'}(\mathbf{G}),i} = \mathfrak{X}_{\mathrm{Trans}_{I_n,M}(\mathbf{G}),i} + X_i$$

for some $X_i \in \mathrm{zero}_{L_{\mathrm{skew}},L_{\mathrm{skew}}^T}\left(\mathfrak{X}_{\mathbf{G},\ker(\mathfrak{Y},\Lambda)}\right)$

(c). For all the $\alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}} + 1 \leq i \leq m$,

$$\mathfrak{X}_{\mathrm{Trans}_{I_n,M}(\mathbf{G}),i} = \mathfrak{X}_{\mathrm{Trans}_{I_n,M'}(\mathbf{G}),i}$$

The property (a) implies that each of the first $\alpha_{\mathfrak{X}}$ rows of M' is a linear combination of the first $\alpha_{\mathfrak{X}}$ rows of M. The property (b) implies that for all the $\alpha_{\mathfrak{X}} + 1 \leq i \leq \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}$, the i-th row of M' is the i-th row of M plus a linear combination of the first $\alpha_{\mathfrak{X}}$ rows of M. The property (c) implies that for all the $\alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}} \leq i \leq m$, i-th row of M' is the same as the i-th row of M. Hence, $M^{\dagger}$ satisfies Equation (2).

Also, by Definition 5.8 and Lemma 3.4, we have the following properties for the matrix space $\mathfrak{Y}$:

(d). For the $\mathfrak{Y}_{\mathbf{G},\ker_{\mathrm{skew}}(\mathfrak{X},\Lambda)}$ we have

$$\mathrm{zero}_{L,L^T_{\mathrm{skew}}}\left(\mathfrak{Y}_{\mathbf{G},\ker_{\mathrm{skew}}(\mathfrak{X},\Lambda)}\right)$$
$$= \left\langle \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),1} \cdot \left(N^T\right)^{-1}, \ldots, \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),\alpha_{\mathfrak{Y}}} \cdot \left(N^T\right)^{-1}\right\rangle$$
$$= \left\langle \mathfrak{Y}_{\mathrm{Trans}_{N',I_m}(\mathbf{G}),1} \cdot \left(N'^T\right)^{-1}, \ldots, \mathfrak{Y}_{\mathrm{Trans}_{N',I_m}(\mathbf{G}),\alpha_{\mathfrak{Y}}} \cdot \left(N'^T\right)^{-1}\right\rangle.$$

(e). For all the $\alpha_{\mathfrak{Y}} + 1 \le j \le \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$,

$$\mathfrak{Y}_{\mathrm{Trans}_{N',I_m}(\mathbf{G}),i} \cdot \left(N'^T\right)^{-1} = \left(\mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),i} + Y_i\right) \cdot \left(N^T\right)^{-1}$$

for some $Y_i \in \left\langle \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),1} \cdots, \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}(\mathbf{G}),\alpha_{\mathfrak{Y}}}\right\rangle$

(d). For all the $\alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}} + 1 \le j \le n$,

$$\mathfrak{Y}_{\mathrm{Trans}_{N',I_m}(\mathbf{G}),j} \cdot \left(N'^T\right)^{-1} = \mathfrak{Y}_{\mathrm{Trans}_{N,I_m}\mathbf{G}),j} \cdot \left(N^T\right)^{-1}$$

The property (d) implies that each of the first $\alpha_{\mathfrak{Y}}$ rows of N' is a linear combination of the first $\alpha_{\mathfrak{Y}}$ rows of N. The property (e) implies that for all $\alpha_{\mathfrak{Y}} + 1 \le j \le \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$, the j-th row of N' is the j-th row of N plus a linear combination of the first $\alpha_{\mathfrak{Y}}$ rows of N. The property (f) implies that for all $\alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}} + 1 \le j \le n$, the j-th row of N' is the same as the j-th row of N. Hence, $N^\dagger$ satisfies Equation (2). Hence, the first property of the current lemma holds.

The second property of the lemma is obtained by the first property and Lemma 5.9. $\square$

By the results from Section 3 and Section 4, we show that there is always a characterization tuple such that the attribute set contains a small number of row vectors, and each of the individualization and complementary matrices contains a small number of rows. This means that for the isometry testing of two skew-symmetric matrix space tensors, one can enumerate the characterization tuples so that the isometry testing of two tensors reduces to isometry testing of the semi-canonical forms of the two tensors.

Lemma 5.11. *For every skew-symmetric matrix space tensor* $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$, *there exists a characterization tuple* $(L_{\mathrm{skew}}, L, \Lambda, B_{\mathrm{skew}}, B)$ *satisfying the following conditions:*

1. L_{skew} *is a matrix in* $M(O(\max\{m,n\}\log(p)/n^{0.2}), n, \mathbb{F}_p)$.

2. L *is a matrix in* $M(O(n\log(p)/n^{0.2}), m, \mathbb{F}_p)$.

3. $|\Lambda| = O(n^{0.4})$.

4. C_{skew} *is a matrix in* $M(O(n^{0.8}), n, \mathbb{F}_p)$.

5. C *is a matrix in* $M(O(n^{0.8}), m, \mathbb{F}_p)$.

Proof. Let $r = n^{0.4}$. By Lemma 3.2, there exist two matrices

$$L_1 \in M(O(\max\{m\log(p),r\}/\sqrt{r}), n, \mathbb{F}_p) \text{ and } R_1 \in M(n, O(\max\{m\log(p),r\}/\sqrt{r}), \mathbb{F}_p)$$

such that $L_1 X R_1$ is a non-zero matrix for each $X \in \mathfrak{X}_{\mathbf{G}}$ of rank at least r. By Lemma 3.2, there exist two matrices

$$L_2 \in M(O(\max\{n\log(p),r\}/\sqrt{r}), m, \mathbb{F}_p) \text{ and } R_2 \in M(n, O(\max\{n\log(p),r\}/\sqrt{r}), \mathbb{F}_p)$$

such that $L_2 Y R_2$ is a non-zero matrix for each $Y \in \mathfrak{Y}_\mathbf{G}$ of rank at least r. Let L_{skew} be a matrix such that every row vector of L_1, R_1^T, and R_2^T is a linear combination of the row vectors of L_{skew}, and L be L_2. Thus L_{skew} has

$$O(\max\{m\log(p), n\log(p), r\}/\sqrt{r}) = O(\max\{m,n\}\log(p)/\sqrt{r}) = O(\max\{m,n\}\log(p)/n^{0.2})$$

rows, and L has $O(n\log(p)/n^{0.2})$ rows. We have that $L_{\mathrm{skew}} X L_{\mathrm{skew}}^T$ is a non-zero matrix for each $X \in \mathfrak{X}_\mathbf{G}$ of rank at least r, and $L Y L_{\mathrm{skew}}^T$ is a non-zero matrix for each $Y \in \mathfrak{Y}_\mathbf{G}$ of rank at least r.

By Lemma 4.6, there is a set of linearly independent row vectors in $\mathbb{F}_p^n$, denoted as Λ', such that the following two conditions hold

1. $|\Lambda'| \leq O(r^2)$.

2. $\dim(\ker_{\mathrm{skew}}(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G})), \Lambda') \geq n - O(r^2)$.

Also, by Lemma 4.6, there is a set of linearly independent row vectors in $\mathbb{F}_p^n$, denoted as Λ'', such that the following two conditions hold

1. $|\Lambda''| \leq O(r^2)$.

2. $\dim(\ker(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G}), \Lambda'')) \geq m - O(r)$.

Let Λ be a set of linear independent row vectors of size at most $|\Lambda'| + |\Lambda''| = O(r^2)$ such that $\langle \Lambda \rangle = \langle \Lambda' \cup \Lambda'' \rangle$. By Lemma 4.7, we have

$$\ker\left(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G}), \Lambda''\right) \leq \ker\left(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G}), \Lambda\right)$$

and

$$\dim\left(\ker_{\mathrm{skew}}\left(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G}), \Lambda\right)\right) \geq \dim\left(\ker_{\mathrm{skew}}\left(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G}), \Lambda'\right)\right) - |\Lambda|.$$

Thus, we have

$$\dim\left(\ker_{\mathrm{skew}}\left(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G}), \Lambda\right)\right) \geq n - O(r^2) - |\Lambda| \geq n - O(n^2)$$

and

$$\dim\left(\ker\left(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G}), \Lambda\right)\right) \geq m - O(r) \geq m - O(r^2).$$

Finally, any complementary matrix for the matrix space $\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G})$ and Λ has

$$n - \dim\left(\ker_{\mathrm{skew}}\left(\mathrm{zero}_{L_{\mathrm{skew}}, L_{\mathrm{skew}}^T}(\mathfrak{X}_\mathbf{G}), \Lambda\right)\right) = O(r^2)$$

rows, and any complementary matrix for the matrix space $\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G})$ and Λ has

$$m - \dim\left(\ker(\mathrm{zero}_{L, L_{\mathrm{skew}}^T}(\mathfrak{Y}_\mathbf{G}), \Lambda)\right) = O(r^2)$$

rows. $\qquad\square$

We present an algorithm to compute a semi-canonical form of a given skew-symmetric matrix space tensor based on a given characterization tuple.

Tensor Semi-Canonical Form Construction Algorithm

Input: A skew-symmetric tensor $\mathbf{G}$ and a characterization tuple $(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$

Output: $\mathbf{SC}_{L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C}(\mathbf{G})$

1. Compute a linear basis of $\ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)$ and a linear basis of $\ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)$.

2. Compute a semi-canonical basis $(X_1, \ldots, X_{\alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}})$ of $\mathfrak{X}_{\mathbf{G}, \ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)}$ with respect to L_{skew} and L_{skew}^T, and a semi-canonical basis $(Y_1, \ldots, Y_{\alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}})$ of $\mathfrak{Y}_{\mathbf{G}, \ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)}$ with respect to L and L_{skew}^T.

3. Compute a matrix $M \in \mathrm{GL}(m, \mathbb{F}_p)$ satisfying the following two conditions

   - Let m_i be the i-th row of M. $\sum_{i'=1}^m m_i[i'] \cdot \mathfrak{X}_{\mathbf{G}, i'} = X_i$ for all the $1 \leq i \leq \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}$.
   - The i-th row M is the same as the $(i - \alpha_{\mathfrak{X}} - \beta_{\mathfrak{X}})$-th row of C for all the $\alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}} + 1 \leq i \leq m$.

4. Compute a matrix $N \in \mathrm{GL}(n, \mathbb{F}_p)$ satisfying the following two conditions

   - Let n_i be the i-th row of N. $\sum_{i'=1}^n n_i[i'] \cdot \mathfrak{Y}_{\mathbf{G}, i'} = Y_i$ for all the $1 \leq i \leq \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}}$.
   - The i-th row N is the same as the $(i - \alpha_{\mathfrak{Y}} - \beta_{\mathfrak{Y}})$-th row of C_{skew} for all the $\alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}} + 1 \leq i \leq n$.

5. Return $\mathrm{Trans}_{N,M}(\mathbf{G})$.

Lemma 5.12. *Given a skew-symmetric matrix space tensor $\mathbf{G} \in \mathbb{F}_p^{m \times n \times n}$ and a characterization tuple $(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$, there is an algorithm to construct a semi-canonical form of $\mathbf{G}$ with respect to $(L_{\mathrm{skew}}, L, \Lambda, C_{\mathrm{skew}}, C)$ in time $p^{O(n+m)} \cdot \mathrm{poly}(n, m, p)$.*

Proof. The correctness of the algorithm is obtained by Definition 5.8. Now we bound the running time. For the first step of the algorithm, to compute a linear basis of $\ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)$, one can compute all the vectors in $\ker_{\mathrm{skew}}(\mathfrak{X}_{\mathbf{G}}, \Lambda)$ by enumerating all the possible vectors and then compute a linear basis. $\ker(\mathfrak{Y}_{\mathbf{G}}, \Lambda)$ can be computed similarly. Hence, the first step takes $p^{O(n+m)} \cdot \mathrm{poly}(n, m, p)$ time. By Lemma 3.5, the second step of the algorithm takes $p^{O(n+m)} \cdot \mathrm{poly}(n, m, p)$ time. For the third and fourth steps, computing a row of N (or M) can be done by enumerating all the row vectors of dimension n (or m). Hence, the third and fourth steps take $p^{O(n+m)} \cdot \mathrm{poly}(n, m, p)$ time. $\qquad\square$

5.3 Isometry of skew-symmetric matrix space tensor semi-canonical forms

We define the isometry between semi-canonical forms of two tensors and give an algorithm for the isometry testing of two skew-symmetric matrix space tensors assuming there is an algorithm for the isometry testing of tensor semi-canonical forms.

Definition 5.13 (Tensor semi-canonical form isometry)**.** Two skew-symmetric matrix space tensor semi-canonical forms $\mathbf{SC}(\mathbf{G})$ and $\mathbf{SC}(\mathbf{H})$ in $\mathbb{F}_p^{m \times n \times n}$ are isometric if the following two conditions hold:

1. The parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$ and $\beta_{\mathfrak{Y}}$ of the two semi-canonical forms are the same.

2. There exist matrices

$$M = \begin{pmatrix} X & 0 & 0 \\ Y & I_{\beta_{\mathfrak{X}}} & 0 \\ 0 & 0 & I_{m-\alpha_{\mathfrak{X}}-\beta_{\mathfrak{X}}} \end{pmatrix} \text{ and } N = \begin{pmatrix} X' & 0 & 0 \\ Y' & I_{\beta_{\mathfrak{Y}}} & 0 \\ 0 & 0 & I_{n-\alpha_{\mathfrak{Y}}-\beta_{\mathfrak{Y}}} \end{pmatrix} \tag{3}$$

for some $X \in \mathrm{GL}(\alpha_{\mathfrak{X}}, \mathbb{F}_p)$, $X' \in \mathrm{GL}(\alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, $Y \in M(\beta_{\mathfrak{X}}, \alpha_{\mathfrak{X}}, \mathbb{F}_p)$, and $Y' \in M(\beta_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$ such that $\mathrm{Trans}_{N,M}(\mathbf{SC}(\mathbf{G})) = \mathbf{SC}(\mathbf{H})$.

We give an algorithm for the isometry testing of two skew-symmetric matrix space tensors assuming there is an algorithm for the isomorphism testing of tensor semi-canonical forms.

Skew-Symmetric Matrix Space Tensor Isometry Testing Algorithm
Input: Two skew-symmetric matrix space tensors $\mathbf{G}, \mathbf{H} \in \mathbb{F}_p^{m \times n \times n}$ for some prime $p > 2$ and positive integers n, m.
Output: Yes or no.

1. Let $\ell_1 = O((m+n)\log(p)/n^{0.2})$, $\ell_2 = O(n\log(p)/n^{0.2})$, and $\ell_3 = O(n^{0.4})$ and $\ell_4 = O(n^{0.8})$.

2. For each $(L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G}}, \Lambda_{\mathbf{G}}, C_{\mathbf{G},\mathrm{skew}}, C_{\mathbf{G}})$ and $(L_{\mathbf{H},\mathrm{skew}}, L_{\mathbf{H}}, \Lambda_{\mathbf{H}}, C_{\mathbf{H},\mathrm{skew}}, C_{\mathbf{H}})$ satisfying the following conditions:

   - $L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{H},\mathrm{skew}} \in M(\ell_1, n, \mathbb{F}_p), L_{\mathbf{G}}, L_{\mathbf{H}} \in M(\ell_2, m, \mathbb{F}_p)$;
   - $|\Lambda_{\mathbf{G}}| = |\Lambda_{\mathbf{H}}| = \ell_3$;
   - $\dim(\ker(\mathrm{zero}_{L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G},\mathrm{skew}}^T}(\mathfrak{X}_{\mathbf{G}}), \Lambda_{\mathbf{G}})) \geq n - \ell_4$;
   - $\dim(\ker(\mathrm{zero}_{L_{\mathbf{G}}, L_{\mathbf{G},\mathrm{skew}}^T}(\mathfrak{Y}_{\mathbf{G}}), \Lambda_{\mathbf{G}})) \geq m - \ell_4$;
   - $\dim(\ker(\mathrm{zero}_{L_{\mathbf{H},\mathrm{skew}}, L_{\mathbf{H},\mathrm{skew}}^T}(\mathfrak{X}_{\mathbf{H}}), \Lambda_{\mathbf{H}})) \geq n - \ell_4$;
   - $\dim(\ker(\mathrm{zero}_{L_{\mathbf{H}}, L_{\mathbf{H},\mathrm{skew}}^T}(\mathfrak{Y}_{\mathbf{H}}), \Lambda_{\mathbf{H}})) \geq m - \ell_4$,

   run the following algorithm

   (a) Construct $\mathbf{SC}_{L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G}}, \Lambda_{\mathbf{G}}, C_{\mathbf{G},\mathrm{skew}}, C_{\mathbf{G}}}(\mathbf{G})$ and $\mathbf{SC}_{L_{\mathbf{H},\mathrm{skew}}, L_{\mathbf{H}}, \Lambda_{\mathbf{H}}, C_{\mathbf{H},\mathrm{skew}}, C_{\mathbf{H}}}(\mathbf{H})$, and denote the resulting semi-canonical forms as $\mathbf{SC}_1$ and $\mathbf{SC}_2$, respectively.

   (b) If $\mathbf{SC}_1$ and $\mathbf{SC}_2$ have different parameters, then continue.

   (c) Run the algorithm for the isometry testing of semi-canonical forms for two skew-symmetric matrix tensors with $\mathbf{SC}_1$ and $\mathbf{SC}_2$. If the algorithm returns yes, then return yes.

3. Return no.

Lemma 5.14. *If there is an algorithm to determine whether the semi-canonical forms of two skew-symmetric matrix space tensors in $\mathbb{F}_p^{m \times n \times n}$ are isometric with running time $T(p, n, m)$, then there is an algorithm for isometry testing of two skew-symmetric matrix space tensors in time*

$$p^{O((m+n)n^{0.8}\log(p))} \cdot T(p, n, m) \cdot \mathrm{poly}(p, n, m).$$

Proof. Let **G** and **H** be the two input tensors. We first prove the correctness of the algorithm. If **G** and **H** are isometric, then there are $M \in \mathrm{GL}(m, \mathbb{F}_p)$ and $N \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $\mathrm{Trans}_{N,M}(\mathbf{G}) = \mathbf{H}$. By Lemma 5.11, there is a characterization tuple

$$(L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G}}, \Lambda_{\mathbf{G}}, C_{\mathbf{G},\mathrm{skew}}, C_{\mathbf{G}})$$

for tensor **G** enumerated by the algorithm satisfying the conditions of Lemma 5.11. Let $\Lambda_{\mathbf{H}} = \{x \cdot N^T : x \in \Lambda_{\mathbf{G}}\}$. Then the tuple

$$(L_{\mathbf{G},\mathrm{skew}} \cdot N^{-1}, L_{\mathbf{G}} \cdot M^{-1}, \Lambda_{\mathbf{H}}, C_{\mathbf{G},\mathrm{skew}} \cdot N^{-1}, C_{\mathbf{G}} \cdot M^{-1})$$

is a characterization tuple for **H**, and is enumerated in the algorithm. Hence, the algorithm returns yes after running the algorithm for skew-symmetric tensor semi-canonical form isometry testing on the semi-canonical forms of **G** and **H** with respect to the above two characterization tuples, respectively.

On the other hand, if the algorithm for skew-symmetric tensor semi-canonical form isometry testing returns yes on two semi-canonical forms, then there is a transform to make the two tensors equal. Hence, the algorithm returns yes if and only if **G** and **H** are isometric.

Now we bound the running time of the algorithm. Since $L_{\mathbf{G},\mathrm{skew}}$ and $L_{\mathbf{H},\mathrm{skew}}$ are of dimension $O(\max\{m,n\}\log(p)/n^{0.2}) \times n$, $L_{\mathbf{G}}$ and $L_{\mathbf{H}}$ are of dimension $O(n\log(p)/n^{0.2}) \times m$, $\Lambda_{\mathbf{G}}$ and $\Lambda_{\mathbf{H}}$ contain at most $O(n^{0.4})$ vectors, each of $C_{\mathbf{G},\mathrm{skew}}$ $C_{\mathbf{H},\mathrm{skew}}$, $C_{\mathbf{G}}$ and $C_{\mathbf{H}}$ contains at most $O(n^{0.8})$ rows, there are at most

$$p^{O((m+n)n^{0.8}\log(p))} \cdot p^{O(n^{0.4} \cdot n)} \cdot p^{O(n^{0.8}(n+m))} = p^{O((n+m)n^{0.8}\log(p))}$$

different pairs of $(L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G}}, \Lambda_{\mathbf{G}}, C_{\mathbf{G},\mathrm{skew}}, C_{\mathbf{G}})$ and $(L_{\mathbf{H},\mathrm{skew}}, L_{\mathbf{H}}, \Lambda_{\mathbf{H}}, C_{\mathbf{H},\mathrm{skew}}, C_{\mathbf{H}})$ enumerated in step 2 of the algorithm. By Lemma 5.12, for each enumerated pair of

$$(L_{\mathbf{G},\mathrm{skew}}, L_{\mathbf{G}}, \Lambda_{\mathbf{G}}, C_{\mathbf{G},\mathrm{skew}}, C_{\mathbf{G}}) \text{ and } (L_{\mathbf{H},\mathrm{skew}}, L_{\mathbf{H}}, \Lambda_{\mathbf{H}}, C_{\mathbf{H},\mathrm{skew}}, C_{\mathbf{H}}),$$

the running time of step 2(a) to step 2(c) is

$$p^{O(n+m)} \cdot \mathrm{poly}(n,m,p) + T(p,n,m).$$

Then we obtain the desired overall running time. $\qquad\square$

6 Isometry testing for skew-symmetric matrix space tensor semi-canonical forms

In this section, we present an algorithm to determine whether the semi-canonical forms of two skew-symmetric tensors in $\mathbb{F}_p^{m \times n \times n}$ are isometric in $\mathrm{poly}(p, n, m)$ time for any prime $p > 2$.

Our approach constructs a skew matrix tuple for each semi-canonical form so that the isometry testing of tensor semi-canonical forms reduces to deciding whether the two skew-symmetric matrix tuples have a block diagonal isometry (Lemma 6.2). Making use of the properties of the skew matrix tuples constructed, we further show that the problem of deciding whether the two skew-symmetric tuples have a block diagonal isometry reduces to the skew-symmetric tuple isometry problem and the matrix tuple equivalence problem (Lemma 6.8).

6.1 Matrix tuple for skew-symmetric matrix space tensor semi-canonical forms

We present our skew-symmetric matrix tuple construction for a skew-symmetric matrix space tensor semi-canonical form in this subsection.

Before formally defining our matrix tuple, we first give a high level overview of our construction. Given a semi-canonical form $\mathbf{SC}(\mathbf{G})$ of a skew-symmetric matrix space tensor $\mathbf{G}$ with parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$, we let

$$n' := \alpha_{\mathfrak{Y}} + \beta_{\mathfrak{Y}} \text{ and } m' := \alpha_{\mathfrak{X}} + \beta_{\mathfrak{X}}.$$

In the skew matrix tuple of $\mathbf{SC}(\mathbf{G})$, denoted as $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$, all the matrices are in $\mathrm{SS}(3+n+m', \mathbb{F}_p)$. The fourth row to the $(3+n)$-th row of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ correspond to the rows of matrices in the matrix space $\mathfrak{X}_{\mathbf{G}}$. The last m' rows of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ correspond to the first m' rows of matrices in $\mathfrak{Y}_{\mathbf{G}}$ (or equivalently $\mathfrak{Z}_{\mathbf{G}}$). The first three rows of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are auxiliary rows used to fix the correspondence between the $(4+\alpha_{\mathfrak{Y}})$ to $(3+n)$-th rows of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ and the $(\alpha_{\mathfrak{Y}}+1)$-th row to n-th row of matrices in $\mathfrak{X}_{\mathbf{G}}$, as well as the correspondence between the $(4+n+\alpha_{\mathfrak{X}})$-th row to the $(3+n+m')$-th row of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ and the $(\alpha_{\mathfrak{X}}+1)$-th row to m'-th row of matrices in $\mathfrak{Y}_{\mathbf{G}}$.

Figure 5: (a) The matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$. (b) A_ℓ and B_ℓ.

See Figure 5(a) for an illustration. The submatrices on R_1 for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are used to encode the matrices of the kernel (the second step in the construction of $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$), as well as the skew-symmetric matrices in the surface for $\mathfrak{X}_{\mathbf{G}}$, i.e., $\mathfrak{X}_{\mathbf{G},m'+1}, \ldots, \mathfrak{X}_{\mathbf{G},m}$ (the second, third, and fourth step in the construction of $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$). The submatrices on R_2 for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are used to encode the matrices in the surface of $\mathfrak{Y}_{\mathbf{G}}$, excluding the intersection with the surface of $\mathfrak{X}_{\mathbf{G}}$ (the sixth and seventh step in the construction of $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$). Consequently, submatrices on the last m' rows and columns from the 4-th to the $(3+n)$-th ($-R_2^T$ in Figure 5(a)) for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ encode the matrices in the surface of $\mathfrak{Z}_{\mathbf{G}}$, excluding the intersection with the surface of $\mathfrak{X}_{\mathbf{G}}$. The submatrices on R_3 for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are used to fix the correspondence between some rows of matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ and some rows in the matrices of $\mathfrak{X}_{\mathbf{G}}$ and $\mathfrak{Y}_{\mathbf{G}}$ (the fifth and eighth steps in the construction of $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$). The submatrices on R_4 for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are used to fix the first three rows (the first step in the construction of $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$). The submatrices on the last m' rows and the last m' columns for all the matrices in $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ are always zero matrices.

30

The construction of the skew-symmetric matrix tuple for $\mathbf{SC(G)}$ is defined in Figure 6. The matrix tuple contains t matrices for some $t = \mathrm{poly}(n, m)$.

$\mathcal{F}_{\mathbf{SC(G)}} = (F_1, \ldots, F_t)$ **Construction**

(For each matrix, the undefined entries are zeros.)

1. Let $t_1 = 3$. $F_1(1,2) = 1, F_1(2,1) = -1, F_2(1,3) = 1, F_2(3,1) = -1, F_3(2,3) = 1$, and $F_3(3,2) = -1$.

2. Let $t_2 = t_1 + m - \alpha_{\mathfrak{x}}$. For each $t_1 + 1 \leq \ell \leq t_2$, the submatrix $F_\ell[4, n'+3; 4, n'+3]$ equals $\mathfrak{X}_{\mathbf{SC(G)}, \alpha_{\mathfrak{x}}+(\ell-t_1)}[1, n'; 1, n']$.

3. Let $t_3 = t_2 + m - m'$. For each $t_2 + 1 \leq \ell \leq t_3$, the submatrix $F_\ell[n'+4, n+3; n'+4, n+3]$ equals $\mathfrak{X}_{\mathbf{SC(G)}, m'+(\ell-t_2)}[n'+1, n; n'+1, n]$.

4. Let $t_4 = t_3 + m - m'$. For each $t_3 + 1 \leq \ell \leq t_4$, the submatrix $F_\ell[4, n'+3; n'+4, n+3]$ equals $\mathfrak{X}_{\mathbf{SC(G)}, m'+(\ell-t_3)}[1, n'; n'+1, n]$, and the submatrix of $F_\ell[n'+4, n+3; 4, n'+3]$ equals $\mathfrak{X}_{\mathbf{SC(G)}, m'+(\ell-t_3)}[n'+1, n; 1, n']$.

5. Let $t_5 = t_4 + 2(n - \alpha_{\mathfrak{y}})$. For each $1 \leq \ell \leq (n - \alpha_{\mathfrak{y}})$, $F_{t_4+2\ell-1}(1, 3+\alpha_{\mathfrak{y}}+\ell) = 1, F_{t_4+2\ell-1}(3+\alpha_{\mathfrak{y}}+\ell, 1) = -1, F_{t_4+2\ell}(2, 3+\alpha_{\mathfrak{y}}+\ell) = 1$, and $F_{t_4+2\ell}(3+\alpha_{\mathfrak{y}}+\ell, 2) = -1$.

6. Let $t_6 = t_5 + n - \alpha_{\mathfrak{y}}$. For each $t_5 + 1 \leq \ell \leq t_6$, the submatrix $F_\ell[3+n+1, 3+n+m'; 4, n'+3]$ equals $\mathfrak{Y}_{\mathbf{SC(G)}, \ell-t_5+\alpha_{\mathfrak{y}}}[1, m'; 1, n']$, and the submatrix $F_\ell[4, n'+3; 3+n+1, 3+n+m']$ equals $-(\mathfrak{Y}_{\mathbf{SC(G)}, \ell-t_5+\alpha_{\mathfrak{y}}}[1, m'; 1, n'])^T$.

7. Let $t_7 = t_6 + n - n'$. For each $t_6 + 1 \leq \ell \leq t_7$, $F_\ell[3+n+1, 3+n+m'; n'+4, n+3]$ equals $\mathfrak{Y}_{\mathbf{SC(G)}, \ell-t_6+n'}[1, m'; n'+1, n]$. $F_\ell[n'+4, n+3; 3+n+1, 3+n+m']$ equals $-(\mathfrak{Y}_{\mathbf{SC(G)}, \ell-t_6+n'}[n'+1, n; 1, m'])^T$.

8. Let $t = t_7 + 2\beta_{\mathfrak{x}}$. For each $1 \leq \ell \leq \beta_{\mathfrak{x}}$, $F_{t_7+2\ell-1}(1, 3+n+\alpha_{\mathfrak{x}}+\ell) = 1, F_{t_7+\ell}(3+n+\alpha_{\mathfrak{x}}+\ell, 1) = -1, F_{t_7+2\ell}(2, 3+n+\alpha_{\mathfrak{x}}+\ell) = 1$, and $F_{t_7+2\ell}(3+n+\alpha_{\mathfrak{x}}+\ell, 2) = -1$.

Figure 6: $\mathcal{F}_{\mathbf{SC(G)}}$ construction

As illustrated in Figure 5(b), for a matrix $F_\ell \in \mathcal{F}_{\mathbf{SC(G)}}$, we use A_ℓ to denote the submatrix on the first $3 + n$ rows and the first $3 + n$ columns (i.e., $F_\ell[1, 3+n; 1, 3+n]$), and use B_ℓ to denote the submatrix on the first $3 + n$ rows and the last m' columns (i.e., $F_\ell[1, 3+n; 4+n, 3+n+m']$). By the skew-symmetric condition, the submatrix on the last m' rows and the first $3 + n$ columns is $-B_\ell^T$.

All the matrices in $\mathcal{F}_{\mathbf{SC(G)}}$ have two types. If B_ℓ is a zero matrix, then F_ℓ is a type 1 matrix. If A_ℓ is a zero matrix, then F_ℓ is a type 2 matrix. By the construction of $\mathcal{F}_{\mathbf{SC(G)}}$, F_ℓ is either a type 1 matrix or a type 2 matrix.

We prove some useful properties for our construction of $\mathcal{F}_{\mathbf{SC(G)}}$.

Lemma 6.1. *We have the following properties for $\mathcal{F}_{\mathbf{SC(G)}} = (F_1, \ldots, F_t)$:*

1. *t is upper bounded by a polynomial of n and m.*

31

2. For $1 \leq \ell \leq t_5$, F_ℓ is a type 1 matrix, where t_5 is defined in the construction of $\mathcal{F}_{\mathbf{SC(G)}}$.

3. For $t_5 + 1 \leq \ell \leq t$, F_ℓ is a type 2 matrix.

4. For every non-zero row vector $v \in \mathbb{F}_p^{3+n+m'}$ such that $v[k] = 0$ for $k = 1, 2, 3$, there is an $1 \leq \ell \leq t$ such that vF_ℓ is a non-zero vector, and the first three rows of F_ℓ are all zero.

5. The linear span of the rows of B_ℓ for all the $1 \leq \ell \leq t$ is a row vector space of dimension m'.

Proof. The first three properties are by the construction of $\mathcal{F}_{\mathbf{SC(G)}}$. For the fourth property, let $x \in \mathbb{F}_p^{3+n+m'}$ be a non-zero row vector such that $x[k] = 0$ for all the $k = 1, 2, 3$, and $k > 3 + n$. By the construction of $\mathcal{F}_{\mathbf{SC(G)}}$, the row vectors of xF_ℓ for all the $4 \leq \ell \leq t_4$ and $t_5 + 1 \leq \ell \leq t_7$ encode the matrix $\sum_{j=1}^n x[j+3] \cdot \mathfrak{Y}_{\mathbf{G},j}$. By Fact 5.2, the matrix is a non-zero matrix. Hence, xF_ℓ is a non-zero vector for some $4 \leq \ell \leq t_4$ or $t_5 + 1 \leq \ell \leq t_7$.

Similarly, let y be a row vector such that $y[k] = 0$ for all the $k \leq 3 + n$. The row vectors of yF_ℓ for all the $t_5 + 1 \leq \ell \leq t_7$ encode the matrix $\sum_{i=1}^{m'} y[i+3+n] \cdot \mathfrak{X}_{\mathbf{G},i}$. By Fact 5.2, $\sum_{i=1}^{m'} y[i+3+n]\mathfrak{X}_{\mathbf{G},i}$ is a non-zero matrix, yF_ℓ is a non-zero vector for some $t_5 + 1 \leq \ell \leq t_7$.

For arbitrary row vectors x and y defined above, by the second and third properties, at most one of $(xF_\ell)[k]$ and $(yF_\ell)[k]$ is non-zero for any $1 \leq \ell \leq t$ and $1 \leq k \leq 3 + n + m'$. Hence, for any row vector $v \in \mathbb{F}_p^{3+n+m'}$ such that $v[k] = 0$ for $k = 1, 2, 3$, there is a non-zero vector vF_ℓ for some $4 \leq \ell \leq t_4$ or $t_5 + 1 \leq \ell \leq t_7$. Since the first three rows of F_ℓ are zero rows for all the $4 \leq \ell \leq t_4$ and $t_5 + 1 \leq \ell \leq t_7$, the fourth property holds.

For the last property, if linear span by the rows of B_ℓ for all the $1 \leq \ell \leq t$ is of dimension smaller than m', then there is a non-zero vector $(t_1, \ldots, t_{m'}) \in \mathbb{F}_p^{m'}$ such that $\sum_{i=1}^{m'} t_i \cdot \mathfrak{X}_{\mathbf{SC(G)},i}$ is a zero matrix, which contradicts to Fact 5.2. Hence, the last property holds. $\qquad \square$

6.2 Reduction to the restricted skew-symmetric matrix tuple isometry

In this section, we show that two semi-canonical forms $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ are isometric if and only if there is a block diagonal matrix S such that $S\mathcal{F}_{\mathbf{SC(G)}}S^T = \mathcal{F}_{\mathbf{SC(H)}}$.

Lemma 6.2. *Let $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ be the semi-canonical forms of two tensors with the same parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$. Then $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ are isometric if and only if there is a matrix S of form*

$$S = \begin{pmatrix} Q & 0 \\ 0 & W \end{pmatrix} \tag{4}$$

such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$, where Q is a $(3+n) \times (3+n)$ matrix and W is an $m' \times m'$ matrix.

We first prove some useful properties for the case that there is a matrix S such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$.

Lemma 6.3. *Let $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ be semi-canonical forms for two tensors with the same parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$. Let $\mathcal{F}_{\mathbf{SC(G)}} = (F_1, \ldots, F_t)$ and $\mathcal{F}_{\mathbf{SC(H)}} = (F'_1, \ldots, F'_t)$ be the skew-symmetric matrix tuples for $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ respectively. If there is a matrix $S \in M(3 + n + m', \mathbb{F}_p)$ such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$, then S satisfies the following properties:*

1. *S is a full rank matrix.*

2. *For any $1 \leq \ell \leq t$, if F_ℓ is a type 1 matrix, then F'_ℓ is a type 1 matrix. If F_ℓ is a type 2 matrix, then F'_ℓ is a type 2 matrix.*

3. Let Φ be the set

$$\{1,2,3\} \cup \{3+\alpha_{\mathfrak{Y}}+1,\ldots,3+n\} \cup \{4+n+\alpha_{\mathfrak{X}},\ldots,3+n+m'\}.$$

There is a $\gamma \in \mathbb{F}_p$ satisfying $\gamma^2 = 1$ such that the following conditions hold:

(a) $S[k,k] = \gamma$ for any $k \in \Phi$.

(b) $S[i,k] = 0$ for any $k \in \Phi$ and $i \neq k$.

4. $S[1,3;4,3+n+m']$ is a zero matrix.

5. For each row v of $S[3+n+1,3+n+m';1,3+n]$, vA_ℓ is a zero row vector for all the $1 \leq \ell \leq t$.

6. $S[4,3+n,4,3+n]$ is of form

$$S[4,3+n,4,3+n] = \begin{pmatrix} A & 0 & 0 \\ B & \gamma \cdot I_{\beta_{\mathfrak{Y}}} & 0 \\ C & 0 & \gamma \cdot I_{n-n'} \end{pmatrix} \tag{5}$$

for some $A \in M(\alpha_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, $B \in M(\beta_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, and $C \in M(n-n', \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$ satisfying the following conditions

(a) $C \cdot (\mathfrak{X}_{\mathbf{SC(G)},i}[1,\alpha_{\mathfrak{Y}};1,n'])$ is a zero matrix for each $1 \leq i \leq m$.

(b) $C \cdot (\mathfrak{X}_{\mathbf{SC(G)},i}[1,\alpha_{\mathfrak{Y}};n'+1,n])$ is a zero matrix for each $1 \leq i \leq m'$.

(c) $C \cdot (\mathfrak{X}_{\mathbf{SC(G)},i}[1,\alpha_{\mathfrak{Y}};n'+1,n]) + (\mathfrak{X}_{\mathbf{SC(G)},i}[1,\alpha_{\mathfrak{Y}};n'+1,n])^T \cdot C^T$ is a zero matrix for each $m'+1 \leq i \leq m$.

Proof. To prove the first property, we show that for each row vector $v \in \mathbb{F}_p^{3+n+m'}$, there is a matrix $F_\ell \in \mathcal{F}_{\mathbf{SC(G)}}$ such that vF_ℓ is a non-zero vector. By the construction of F_1, F_2 and F_3, if at least one of $v[1]$, $v[2]$ and $v[3]$ is not equal to zero, then at least one of vF_1, vF_2 and vF_3 is a non-zero vector. For the case of $v[1] = v[2] = v[3] = 0$, by the third property of Lemma 6.1, if v is a non-zero vector, vF_ℓ is a non-zero vector for some $F_\ell \in \mathcal{F}_{\mathbf{SC(G)}}$. Hence, the first property of the lemma holds.

The second property is obtained by $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$.

For the third property of the lemma, by the definition of $\mathcal{F}_{\mathbf{SC(G)}}$, if $S[1,2] \neq 0$, then the first row of SF_3 is not a zero matrix. Since S is invertible, the first row of SF_3S^T is a non-zero row. However, the first row of F_3' is a zero row, contradiction. Hence, $S[1,2] = 0$. Similarly, we have

$$S[1,3] = S[2,1] = S[2,3] = S[3,1] = S[3,2] = 0.$$

Since F_1 are all zero from the 4-th row to the $(3+n+m')$-th row, we have

$$
\begin{aligned}
\left(SF_1S^T\right)[1,3;1,3] &= \begin{pmatrix} S[1,1] & 0 & 0 \\ 0 & S[2,2] & 0 \\ 0 & 0 & S[3,3] \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} S[1,1] & 0 & 0 \\ 0 & S[2,2] & 0 \\ 0 & 0 & S[3,3] \end{pmatrix} \\
&= \begin{pmatrix} 0 & S[1,1] \cdot S[2,2] & 0 \\ -S[1,1] \cdot S[2,2] & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\
&= F_1'[1,3;1,3].
\end{aligned}
$$

33

Hence, $S[1,1] \cdot S[2,2] = 1$. Similarly, we have $S[1,1] \cdot S[3,3] = S[2,2] \cdot S[3,3] = 1$. Because $S[1,1], S[2,2], S[3,3] \in \mathbb{F}_p$ for some prime p, $S[1,1] = S[2,2] = S[3,3]$, and thus $S[1,1]^2 = 1$. So we have $S[1,1] = \gamma$ for some $\gamma^2 = 1$, and consequently

$$S[1,3;1,3] = \begin{pmatrix} \gamma & 0 & 0 \\ 0 & \gamma & 0 \\ 0 & 0 & \gamma \end{pmatrix}.$$

We prove $S[j,k] = 0$ for all the $j > 3$ and $k \in \{1,2,3\}$ by contraction. If $S[j,k] \neq 0$ for some $j > 3$ and $k \in \{1,2,3\}$, the j-th row of SF_iS^T is not a zero row for some $i \in \{1,2,3\}$, which contradicts to the fact that the j-th row of F_i' is a zero row for all the $1 \leq i \leq 3$ and $j > 3$. Hence, $S[j,k] = 0$ for all the $j > 3$ and $k \in \{1,2,3\}$.

Now we prove the third property for $\Phi \setminus \{1,2,3\}$. Let k be an arbitrary number in $\Phi \setminus \{1,2,3\}$. Since there is an $\ell \in \{1,\ldots,t\}$ such that $F_\ell[1,k] = F_\ell'[1,k] = 1$, $F_\ell[k,1] = F_\ell'[k,1] = -1$, and all the other entries of F_ℓ and F_ℓ' are zero. Hence, for all the $j \neq 1$ and $j \neq k$, $S[j,k] = 0$. Since $F_{\ell+1}[2,k] = F_{\ell+1}'[2,k] = 1$, $F_{\ell+1}[k,2] = F_{\ell+1}'[k,2] = -1$, and all the other entries of $F_{\ell+1}$ and $F_{\ell+1}'$ are zero, $S[1,k] = 0$. Thus, we have

$$
\begin{aligned}
(S \cdot F_\ell \cdot S^T)[1,k] &= \sum_{i=1}^{3+n+m'} \sum_{j=1}^{3+n+m'} S[1,i] \cdot F_\ell[i,j] \cdot S^T[j,k] \\
&= S[1,1] \cdot S^T[k,k] - S[1,k] \cdot S^T[1,k] \\
&= S[1,1] \cdot S^T[k,k] \\
&= 1,
\end{aligned}
$$

where the third inequality uses the fact that $S[1,k] = 0$ for all the $k > 3$. Thus, $S[k,k] = \gamma$. Then the third property of the lemma holds.

For the fourth property, if $S[1,3;4,3+n+m']$ is a non-zero matrix, then by Lemma 6.1, there exists an $\ell \in \{1,\ldots,t\}$ such that the first three rows of F_ℓ and F_ℓ' are zero rows, but $SF_\ell S^T$ has a non-zero row in one of the first three rows. This contradicts to $SF_\ell S^T = F_\ell'$. Hence, the fourth property holds.

For the fifth property, since $S \cdot F_\ell \cdot S^T = F_\ell'$ for each type 1 matrix F_ℓ and F_ℓ', and S^T is an invertible matrix, the last m' rows of $S \cdot F_\ell$ are zero rows. Since the last m' rows of F_ℓ are zero rows, for each row v of $S[3+n+1, 3+n+m'; 1, 3+n]$, vA_ℓ is a zero row vector.

Now we prove the last property of the lemma. Equation (5) is obtained by the third property of the current lemma. For each $t_1+1 \leq \ell \leq t_2$, F_ℓ and F_ℓ' have non-zero entries only in the submatrices $F_\ell[4, 3+n'; 4, 3+n']$ and $F_\ell'[4, 3+n'; 4, 3+n']$, respectively. Hence, $C \cdot F_\ell[4, 3+\alpha_{\mathfrak{Y}}; 4, 3+n']$ must be a zero matrix because $SF_\ell S^T[4+n', 3+n; 1, 3+n+m']$ is a zero matrix. Since $F_\ell[4, 3+\alpha_{\mathfrak{Y}}; 4, n'+3]$ equals

$$\mathfrak{X}_{\mathbf{SC(G)},\alpha_{\mathfrak{X}}+(\ell-t_1)}[1,\alpha_{\mathfrak{Y}}; 1, n']$$

for each $t_1 + 1 \leq \ell \leq t_2$, the property 6(a) holds.

For each $t_5 + 1 \leq \ell \leq t_6$, the rows between the 4-th row and the $(3 + n')$-th row of F_ℓ and F_ℓ' are non-zero only in the last m' columns, and the rows between the $(4 + n')$-th row and the $(3 + n)$-th row of F_ℓ and F_ℓ' are zero rows. Since $SF_\ell S^T = F_\ell'$, $C \cdot S[4, 3 + \alpha_{\mathfrak{Y}}; 4 + n, 3 + n + m']$ is a zero matrix. Since $F_\ell[4, n' + 3; 4 + n, 3 + n + m']$ equals $-(\mathfrak{Y}_{\mathbf{SC(G)},\ell-t_5+\alpha_{\mathfrak{Y}}}[1, m'; 1, n'])^T$, we have that $C \cdot (\mathfrak{Y}_{\mathbf{SC(G)},q}[1, m'; 1, \alpha_{\mathfrak{X}}])^T$ is a zero matrix for all the $n' + 1 \leq q \leq n$, and thus $C \cdot (\mathfrak{Y}_{\mathbf{SC(G)},q}[r, r; 1, \alpha_{\mathfrak{X}}])^T$ is a zero column vector for each $n' + 1 \leq q \leq n$ and $1 \leq r \leq m'$. Since $\mathfrak{X}_{\mathbf{SC(G)},i}[j,k] = \mathfrak{Y}_{\mathbf{SC(G)},j}[i,k]$, $C \cdot (\mathfrak{X}_{\mathbf{SC(G)},r}[q, q; 1, \alpha_{\mathfrak{Y}}])^T$ is a zero column vector for each

34

$n' + 1 \leq q \leq n$ and $1 \leq r \leq m'$. Using the fact that $\mathfrak{X}_{\mathbf{SC(G)}}$ is a skew-symmetric matrix space, $C \cdot \mathfrak{X}_{\mathbf{SC(G)},r}[1, \alpha_{\mathfrak{Y}}; q, q]$ is a zero column vector for each $n' + 1 \leq q \leq n$ and $1 \leq r \leq m'$. Then the property 6(b) holds.

To prove the property 6(c), we consider F_ℓ and F_ℓ' for $t_3 + 1 \leq \ell \leq t_4$. Since F_ℓ is non-zero only in the submatrices $F_\ell[4, n' + 3; n' + 4, n + 3]$ and $F_\ell[n' + 4, n + 3; 4, n' + 3]$ for $t_3 + 1 \leq \ell \leq t_4$, by Equation (5), we have

$$(SF_\ell)[4 + n', 3 + n; 4 + n', 3 + n] = C \cdot F_\ell[4, 3 + \alpha_{\mathfrak{Y}}; 4 + n', n + 3]$$

and

$$(SF_\ell)[4 + n', 3 + n; 4, 3 + n'] = F_\ell[4 + n', 3 + n; 4, 3 + n'].$$

All the other entries of $(SF_\ell)[4 + n', 3 + n; 1, 3 + n + m']$ are zero. Hence, by Equation (5),

$$
\begin{aligned}
&(SF_\ell S^T)[4 + n', 3 + n; 4 + n', 3 + n]\\
&= C \cdot F_\ell[4, 3 + \alpha_{\mathfrak{Y}}; 4 + n', n + 3] + (F_\ell[4, 3 + \alpha_{\mathfrak{Y}}; 4 + n', n + 3])^T \cdot C^T\\
&= F_\ell'[4 + n', 3 + n; 4 + n', 3 + n]
\end{aligned}
$$

is a zero matrix by the construction of $\mathcal{F}_{\mathbf{SC(G)}}$. Since for each $t_3 + 1 \leq \ell \leq t_4$, $F_\ell[4, 3 + \alpha_{\mathfrak{Y}}; 4 + n', n + 3]$ corresponds to $\mathfrak{X}_{\mathbf{SC(G)}, \ell - t_3 + m'}[1 + \alpha_{\mathfrak{Y}}; n' + 1, n]$. The property 4(c) holds. $\square$

Proof of Lemma 6.2. If two tensor semi-canonical forms are isometric, then by Definition 5.13, there exist two matrices M and N satisfying Equation (3) such that $\mathrm{Trans}_{N,M}(\mathbf{SC(G)}) = \mathbf{SC(H)}$. By Lemma 5.9 and Equation (3), $\mathbf{SC(G)}[i, j, k] = \mathbf{SC(H)}[i, j, k]$ for any $1 \leq i \leq m'$ and $1 \leq j, k \leq n'$. In addition, let

$$S' = \begin{pmatrix} I_3 & 0 & 0 \\ 0 & N & 0 \\ 0 & 0 & M' \end{pmatrix},$$

where M' is obtained by removing the last $m - m'$ rows and the last $m - m'$ columns of M. By our construction of $\mathcal{F}_{\mathbf{SC(G)}}$ and $\mathcal{F}_{\mathbf{SC(H)}}$, we have $S' \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S'^T = \mathcal{F}_{\mathbf{SC(H)}}$.

Now we show that $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ are isometric if there is a matrix S satisfying the form of Equation (4) such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$. By Lemma 6.3, we have

$$Q = \gamma \cdot \begin{pmatrix} I_3 & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & B & I_{\beta_{\mathfrak{Y}}} & 0 \\ 0 & C & 0 & I_{n-n'} \end{pmatrix}$$

for some some $\gamma \in \mathbb{F}_p$ satisfying $\gamma^2 = 1$, $A \in M(\alpha_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, $B \in M(\beta_{\mathfrak{Y}}, \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, $C \in M(n - n', \alpha_{\mathfrak{Y}}, \mathbb{F}_p)$, and

$$W = \gamma \cdot \begin{pmatrix} D & 0 \\ E & I_{\beta_{\mathfrak{X}}} \end{pmatrix}$$

for some $D \in M(\alpha_{\mathfrak{X}}, \alpha_{\mathfrak{X}}, \mathbb{F}_p)$, $E \in M(\beta_{\mathfrak{X}}, \alpha_{\mathfrak{X}}, \mathbb{F}_p)$. Let

$$N = \begin{pmatrix} A & 0 & 0 \\ B & I_{\beta_{\mathfrak{Y}}} & 0 \\ 0 & 0 & I_{n-n'} \end{pmatrix} \text{ and } M = \begin{pmatrix} D & 0 & 0 \\ E & I_{\beta_{\mathfrak{X}}} & 0 \\ 0 & 0 & I_{m-m'} \end{pmatrix}.$$

In the rest of this proof, we show that $\text{Trans}_{N,M}(\mathbf{SC(G)}) = \mathbf{SC(H)}$. Let

$$N' = \begin{pmatrix} A & 0 & 0 \\ B & I_{\beta_{\mathfrak{X}}} & 0 \\ C & 0 & I_{n-n'} \end{pmatrix}.$$

Since $N' - N$ has non-zero entries only in the submatrix of $(N' - N)[n' + 1, n; 1, \alpha_{\mathfrak{Y}}]$, by the last property of Lemma 6.3, the construction of $\mathcal{F}_{\mathbf{SC(G)}}$ and $\mathcal{F}_{\mathbf{SC(H)}}$, and the condition that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$, we have

$$\begin{aligned} N\mathfrak{X}_{\mathbf{SC(G)},i}N^T =& N'\mathfrak{X}_{\mathbf{SC(G)},i}N'^T + N'\mathfrak{X}_{\mathbf{SC(G)},i}(N - N')^T \\ &+ (N - N')\mathfrak{X}_{\mathbf{SC(G)},i}N'^T + (N - N')\mathfrak{X}_{\mathbf{SC(G)},i}(N - N')^T \\ =& N'\mathfrak{X}_{\mathbf{SC(G)},i}N'^T \\ =& \mathfrak{X}_{\mathbf{SC(H)},i} \end{aligned}$$

for all the $m' \leq i \leq m$. By the definition of M, we have $\text{Trans}_{N,M}(\mathbf{SC(G)})[i,j,k] = \mathbf{SC(H)}[i,j,k]$ for all the $m' + 1 \leq i \leq m, 1 \leq j, k \leq n$.

By Lemma 5.9 and the construction of $\mathcal{F}_{\mathbf{SC(G)}}$ and $\mathcal{F}_{\mathbf{SC(H)}}$, for all the $1 \leq i \leq m'$ and $1 \leq j, k \leq n'$,
$$\text{Trans}_{N,M}(\mathbf{SC(G)})[i,j,k] = \text{Trans}_{N',M}(\mathbf{SC(G)})[i,j,k] = \mathbf{SC(H)}[i,j,k].$$

Furthermore, by the construction of $\mathcal{F}_{\mathbf{SC(G)}}$, we have

$$\mathfrak{X}_{\text{Trans}_{N',M}(\mathbf{SC(G)}),i}[j,k] = \mathfrak{X}_{\mathbf{SC(H)},i}[j,k]$$

for all the $1 \leq i \leq m'$, $n' + 1 \leq j \leq n$ and $1 \leq k \leq n$. By the last property of Lemma 6.3, we have

$$\mathfrak{X}_{\text{Trans}_{N,M}(\mathbf{SC(G)}),i}[j,k] = \mathfrak{X}_{\text{Trans}_{N',M}(\mathbf{SC(G)}),i}[j,k]$$

for all the $1 \leq i \leq m'$, $n' + 1 \leq j \leq n$ and $1 \leq k \leq n$. Together with the skew-symmetric condition of matrices in $\mathfrak{X}_{\mathbf{SC(H)}}$, we have $\text{Trans}_{N,M}(\mathbf{SC(G)})[i,j,k] = \mathbf{SC(H)}[i,j,k]$ for all the $1 \leq i \leq m', 1 \leq j, k \leq n$. Hence, $\text{Trans}_{N,M}(\mathbf{SC(G)}) = \mathbf{SC(H)}$. $\qquad\square$

6.3 Isometry testing of tensor semi-canonical forms

We present the algorithm for deciding whether the semi-canonical forms of two skew-symmetric matrix spaces are isometric.

Suppose we run the algorithm for skew-symmetric matrix tuple isometry on $\mathcal{F}_{\mathbf{SC(G)}}$ and $\mathcal{F}_{\mathbf{SC(H)}}$. If the algorithm returns no, then by Lemma 6.2, the two semi-canonical forms are not isometric. If the algorithm returns yes and a block diagonal S, then by Lemma 6.2, the two semi-canonical forms are isometric. The difficult case is that the algorithm returns yes and a matrix S not satisfying Equation (4). For this case, we neither certify that the two semi-canonical forms are isometric by Lemma 6.2 nor rule out the possibility that the two semi-canonical forms are not isometric.

We characterize the matrix S in the difficult case by Lemma 6.4 and Lemma 6.6. We further show that the isometry between the two semi-canonical forms can be determined by running the matrix tuple equivalence algorithm for two matrix tuples constructed based on $\mathbf{SC(G)}, \mathbf{SC(H)}$, and S.

Lemma 6.4. *Let* $\mathbf{SC(G)}$ *and* $\mathbf{SC(H)}$ *be semi-canonical forms of two tensors in* $\mathbb{F}_p^{m \times n \times n}$ *with the same parameters for some prime* $p > 2$ *and integers* n, m. *Let* $\mathcal{F}_{\mathbf{SC(G)}} = (F_1, \ldots, F_t)$ *and* $\mathcal{F}_{\mathbf{SC(H)}} = (F'_1, \ldots, F'_t)$ *be the skew-symmetric matrix tuples for* $\mathbf{SC(G)}$ *and* $\mathbf{SC(H)}$ *respectively. Suppose there is a matrix* S *such that* $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$. *Denote* S *as*

$$S = \begin{pmatrix} Q & R \\ V & W \end{pmatrix},$$

where Q, R, V, *and* W *are matrices of dimensions* $(n+3) \times (n+3)$, $(n+3) \times m'$, $m' \times (n+3)$, *and* $m' \times m'$, *respectively. If at least one of* Q *and* W *is full rank, then there are* $(n+3) \times (n+3)$ *matrix* Q' *and* $m' \times m'$ *matrix* W' *such that*

$$\begin{pmatrix} Q' & 0 \\ 0 & W' \end{pmatrix} \mathcal{F}_{\mathbf{SC(G)}} \begin{pmatrix} Q'^T & 0 \\ 0 & W'^T \end{pmatrix} = \mathcal{F}_{\mathbf{SC(H)}}.$$

Furthermore, Q' *and* W' *can be computed in time* $\mathrm{poly}(n, m, p)$.

Proof. If Q is full rank, let

$$S' = \begin{pmatrix} Q & 0 \\ 0 & W - VQ^{-1}R \end{pmatrix}. \tag{6}$$

Let F_ℓ be a matrix in $\mathcal{F}_{\mathbf{SC(G)}}$ for some $1 \le \ell \le t$. If F_ℓ is a type 1 matrix, we have

$$
\begin{aligned}
SF_\ell S^T &= \begin{pmatrix} Q & R \\ V & W \end{pmatrix} \begin{pmatrix} A_\ell & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Q^T & V^T \\ R^T & W^T \end{pmatrix} \\
&= \begin{pmatrix} QA_\ell Q^T & QA_\ell V^T \\ VA_\ell Q^T & VA_\ell V^T \end{pmatrix} \\
&= F'_\ell \\
&= \begin{pmatrix} QA_\ell Q^T & 0 \\ 0 & 0 \end{pmatrix},
\end{aligned} \tag{7}
$$

where the last equality uses the fact that F'_ℓ is a type 1 matrix by Lemma 6.3. We also have

$$
\begin{aligned}
S'F_\ell S'^T &= \begin{pmatrix} Q & 0 \\ 0 & W - VQ^{-1}R \end{pmatrix} \begin{pmatrix} A_\ell & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Q^T & 0 \\ 0 & W^T - R^T (Q^{-1})^T V^T \end{pmatrix} \\
&= \begin{pmatrix} QA_\ell Q^T & 0 \\ 0 & 0 \end{pmatrix} \\
&= F'_\ell.
\end{aligned}
$$

Hence, $S'F_\ell S'^T = SF_\ell S^T$ for all the type 1 F_ℓ.

If F_ℓ is a type 2 matrix, since $SF_\ell S^T = F'_\ell$ is also a type 2 matrix, we have

$$
\begin{aligned}
SF_\ell S^T &= S \begin{pmatrix} 0 & B_\ell \\ -B_\ell^T & 0 \end{pmatrix} S^T \\
&= \begin{pmatrix} -RB_\ell^T Q^T + QB_\ell R^T = 0 & -RB_\ell^T V^T + QB_\ell W^T \\ -WB_\ell^T Q^T + VB_\ell R^T & -WB_\ell^T V^T + VB_\ell W^T = 0 \end{pmatrix}.
\end{aligned} \tag{8}
$$

Since $RB_\ell^T = RB_\ell^T Q^T (Q^T)^{-1} = QB_\ell R^T (Q^T)^{-1}$, we have

$$SF_\ell S^T = \begin{pmatrix} 0 & QB_\ell(W^T - R^T(Q^T)^{-1}V^T) \\ (-W + VQ^{-1}R)^T B_\ell^T Q^T & 0 \end{pmatrix}.$$

Hence,

$$S'F_\ell S'^T = \begin{pmatrix} Q & 0 \\ 0 & W - VQ^{-1}R \end{pmatrix} \begin{pmatrix} 0 & B_\ell \\ -B_\ell^T & 0 \end{pmatrix} \begin{pmatrix} Q^T & 0 \\ 0 & W^T - R^T(Q^{-1})^T V^T \end{pmatrix}$$

$$=SF_\ell S^T$$

$$=F'_\ell.$$

Then the lemma holds if Q is full rank.

Now we consider the case that W is full rank. Let

$$S' = \begin{pmatrix} Q - RW^{-1}V & 0 \\ 0 & W \end{pmatrix}. \tag{9}$$

We have for each type 1 matrix $F_\ell \in \mathcal{F}_{\mathbf{SC(G)}}$,

$$S'F_\ell S'^T = \begin{pmatrix} Q - RW^{-1}V & 0 \\ 0 & W \end{pmatrix} \begin{pmatrix} A_\ell & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Q^T - V^T(W^{-1})^T R^T & 0 \\ 0 & W^T \end{pmatrix}$$

$$= \begin{pmatrix} (Q - RW^{-1}V)A_\ell(Q - RW^{-1}V)^T & 0 \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} QA_\ell Q^T & 0 \\ 0 & 0 \end{pmatrix}$$

$$=SF_\ell S^T$$

$$=F'_\ell,$$

where the third equality uses the fact that $VA_\ell Q^T = 0$, $QA_\ell V^T = 0$ and $VA_\ell V^T = 0$ by Equation (7).

For each type 2 matrix F_ℓ, by Equation (8), we have

$$VB_\ell = VB_\ell W^T(W^T)^{-1} = WB_\ell^T V^T(W^T)^{-1},$$

and thus

$$SF_\ell S^T = \begin{pmatrix} 0 & (RW^{-1}V - Q)B_\ell W^T \\ WB_\ell^T(-V^T(W^T)^{-1}R^T + Q^T) & 0 \end{pmatrix}.$$

Hence,

$$S'F_\ell S'^T = \begin{pmatrix} Q - RW^{-1}V & 0 \\ 0 & W \end{pmatrix} \begin{pmatrix} 0 & B_\ell \\ -B_\ell^T & 0 \end{pmatrix} \begin{pmatrix} Q - RW^{-1}V & 0 \\ 0 & W \end{pmatrix}^T$$

$$=SF_\ell S^T$$

$$=F'_\ell.$$

Then the lemma holds if W is full rank. By Equation (6) and Equation (9), Q' and W' can be computed in $\text{poly}(n, m, p)$ time. $\square$

Lemma 6.5. *Let* $\mathbf{SC(G)}$ *and* $\mathbf{SC(H)}$ *be semi-canonical forms of two tensors with the same parameters. Let* $\mathcal{F}_{\mathbf{SC(G)}} = (F_1, \ldots, F_t)$ *and* $\mathcal{F}_{\mathbf{SC(H)}} = (F'_1, \ldots, F'_t)$ *be the skew-symmetric matrix tuples for* $\mathbf{SC(G)}$ *and* $\mathbf{SC(H)}$ *respectively. If the following two conditions hold:*

1. There is an invertible matrix S such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$.

2. *There is a matrix*

$$P = \begin{pmatrix} I_{3+n} & U \\ 0 & I_{m'} \end{pmatrix}$$

for some $U \in M(3+n, m', \mathbb{F}_p)$ such that for each type 2 matrix $F_\ell \in \mathcal{F}_{\mathbf{SC(G)}}$, $PSF_\ell S^T P^T[1, 3 + n; 1, 3 + n]$ is a zero matrix.

Then $PS \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T P^T = \mathcal{F}_{\mathbf{SC(H)}}$.

Proof. For each type 1 matrix $F_\ell \in \mathbf{F}_{\mathbf{SC(G)}}$, since $SF_\ell S^T = F'_\ell$, the submatrix $(SF_\ell S^T)[4 + n, 3 + n + m'; 1, 3 + n + m']$ is a zero matrix because F'_ℓ is also a type 1 matrix, we have

$$PSF_\ell S^T P^T$$
$$= (PSF_\ell S^T)P^T$$
$$= \left(\begin{pmatrix} I_{3+n} & U \\ 0 & I_{m'} \end{pmatrix} SF_\ell S^T \right) P^T$$
$$= \left(\begin{pmatrix} I_{3+n} & 0 \\ 0 & I_{m'} \end{pmatrix} SF_\ell S^T \right) P^T$$
$$= SF_\ell S^T \begin{pmatrix} I_{3+n} & 0 \\ U^T & I_{m'} \end{pmatrix}$$
$$= SF_\ell S^T$$
$$= F'_\ell,$$

where the fifth equality is obtained by the skew symmetric condition of $SF_\ell S^T$. For each type 2 matrix $F_\ell \in \mathbf{F}_{\mathbf{SC(G)}}$, we have

$$PSF_\ell S^T P^T$$
$$= \begin{pmatrix} I_{3+n} & U \\ 0 & I_{m'} \end{pmatrix} SF_\ell S^T \begin{pmatrix} I_{3+n} & U \\ 0 & I_{m'} \end{pmatrix}^T$$
$$= SF_\ell S^T + \begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix} SF_\ell S^T + SF_\ell S^T \begin{pmatrix} 0 & 0 \\ U^T & 0 \end{pmatrix} + \begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix} SF_\ell S^T \begin{pmatrix} 0 & 0 \\ U^T & 0 \end{pmatrix}.$$

Let V be the matrix

$$\begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix} SF_\ell S^T + SF_\ell S^T \begin{pmatrix} 0 & 0 \\ U^T & 0 \end{pmatrix} + \begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix} SF_\ell S^T \begin{pmatrix} 0 & 0 \\ U^T & 0 \end{pmatrix}.$$

Since the submatrix $F_\ell[4 + n, 3 + n + m'; 4 + n, 3 + n + m']$ is a zero matrix, V is a matrix such that the last m' rows are all zero, and the last m' columns are all zero. On the other hand, since both $SF_\ell S^T[1, 3 + n; 1, 3 + n]$ and $(PSF_\ell SP^T)[1, 3 + n; 1, 3 + n]$ are a zero matrices, $V[1, 3 + n; 1, 3 + n]$ is a zero matrix. Hence, V is a zero matrix. So we have $PSF_\ell S^T P^T = SF_\ell S^T = F'_\ell$. $\quad\square$

Lemma 6.6. *Let $\mathbf{SC(G)}$ and $\mathbf{SC(H)}$ be semi-canonical forms of two skew-symmetric matrix space tensors with the same parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}},$ and $\beta_{\mathfrak{Y}}$. If there is a matrix S such that $S \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S^T = \mathcal{F}_{\mathbf{SC(H)}}$. Denote S as*

$$S = \begin{pmatrix} Q & R \\ V & W \end{pmatrix},$$

where $Q, R, V,$ and W are of dimensions $(n + 3) \times (n + 3)$, $(n + 3) \times m'$, $m' \times (n + 3)$, and $m' \times m'$, respectively. If both Q and W are not full rank, then there is a matrix $J \in \mathrm{GL}(3 + n, \mathbb{F}_p)$, a matrix $K \in \mathrm{GL}(m', \mathbb{F}_p)$, a positive integer q, and a matrix S' satisfying the following conditions:

1. S' can be represented as

$$
\begin{pmatrix}
Q' & 0 \\
0 & R' \\
0 & W' \\
V' & 0
\end{pmatrix},
$$

where Q' is of dimension $q \times (3+n)$, R' is of dimension $(3+n-q) \times m'$, W' is of dimension $(m' - (3+n-q)) \times m'$, and V' is of dimension $(3+n-q) \times (3+n)$.

2. For each type 1 matrix F_ℓ in $\mathcal{F}_{\mathbf{SC(G)}}$,

$$
S' F_\ell S'^T = \begin{pmatrix} Q' A_\ell Q'^T & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} J & 0 \\ 0 & K \end{pmatrix} F'_\ell \begin{pmatrix} J^T & 0 \\ 0 & K^T \end{pmatrix}.
$$

3. For each type 2 matrix F_ℓ in $\mathcal{F}_{\mathbf{SC(G)}}$,

$$
S' F_\ell S'^T = \begin{pmatrix} 0 & D_\ell \\ -D_\ell^T & 0 \end{pmatrix} = \begin{pmatrix} J & 0 \\ 0 & K \end{pmatrix} F'_\ell \begin{pmatrix} J^T & 0 \\ 0 & K^T \end{pmatrix}
$$

for some $D_\ell = \begin{pmatrix} D'_\ell & 0 \\ 0 & D''_\ell \end{pmatrix}$ such that D'_ℓ is of dimension $q \times (m' - (3+n-q))$ and D''_ℓ is of dimension $(3+n-q) \times (3+n-q)$.

Proof. Denote

$$
\tau_S := \dim\left(\langle\{vQB_\ell R^T : v \in \mathbb{F}_p^{3+n}, 1 \le \ell \le t\}\rangle\right).
$$

By Equation (8), $QB_\ell R^T$ is a skew-symmetric matrix for all the $1 \le \ell \le t$. Hence, there is a matrix $J'_0 \in \mathrm{GL}(3+n, \mathbb{F}_p)$ such that for any $\tau_S + 1 \le 1 \le i \le 3+n$, the i-th row of $J_0 Q B_\ell R^T$ is a zero row for all the $1 \le \ell \le t$. Thus, the multiplication of J_0 and the submatrix on the first $3+n$ rows of S can be represented as

$$
J'_0 \cdot \begin{pmatrix} Q & R \end{pmatrix} = \begin{pmatrix} Q_1 & R_1 \\ Q_0 & R_0 \end{pmatrix}, \tag{10}
$$

where Q_1 is of dimension $\tau_S \times (3+n)$, R_1 is of dimension $\tau_S \times m'$, Q_0 is of dimension $(3+n-\tau_S) \times (3+n)$, and R_0 is of dimension $(3+n-\tau_S) \times m'$, such that $J'_0 Q B_\ell R^T$ is non-zero only in the first τ_S rows for all the $1 \le \ell \le t$. By Equation (8), $J'_0 Q B_\ell R^T J'^T_0$ is non-zero only in the submatrix on the first τ_S rows and the first τ_S columns. Hence, $Q_0 B_\ell R^T$ and $Q B_\ell R_0^T$ are zero matrices for all the B_ℓ. Furthermore, each non-zero linear combination of the rows of R_0 is not a linear combination of the rows of R_1. Otherwise, it contradicts the definition of τ_S. Thus

$$
\mathrm{rank}\,(R) = \mathrm{rank}\,(R_0) + \mathrm{rank}\,(R_1). \tag{11}
$$

On the other hand, by Lemma 6.3, S is an invertible matrix. So we have

$$
\mathrm{rank}\,(R_0) \ge n + 3 - \mathrm{rank}\,(Q). \tag{12}
$$

Furthermore, we can decompose V and W as follows:

1. $V = V_0 + Z_{Q,V}Q$ for some $Z_{Q,V} \in M(m', 3+n, \mathbb{F}_p)$ such that $\mathrm{rank}\,(V_0) = 3 + n - \mathrm{rank}\,(Q)$.

2. $W = W_0 + Z_{R,W}R$ for some $Z_{R,W} \in M(m', m', \mathbb{F}_p)$ such that $\mathrm{rank}\,(W_0) = m' - \mathrm{rank}\,(R)$.

Consider all the type 2 matrices F_ℓ. For each type 2 matrix F_ℓ, we have

$$
\begin{aligned}
-RB_\ell^T V^T + QB_\ell W^T &= -RB_\ell^T (V_0 + Z_{Q,V}Q)^T + QB_\ell(W_0 + Z_{R,W}R)^T \\
&= QB_\ell R^T(-Z_{Q,V}^T + Z_{R,W}^T) - RB_\ell^T V_0^T + QB_\ell W_0^T \\
&= QB_\ell R_1^T(-Z_{Q,V}^T + Z_{R,W}^T) - RB_\ell^T V_0^T + QB_\ell W_0^T,
\end{aligned}
$$

where the second equality is by Equation (8), and the third equality uses the fact that $QB_\ell R_0$ is a zero matrix for all the B_ℓ.

Since S is an invertible matrix, the span of row vectors of $-RB_\ell^T V^T + QB_\ell W^T$ for all the B_ℓ is of dimension m' by Lemma 6.1. Hence, we have

$$
\begin{aligned}
&\operatorname{rank}(R_1) + \operatorname{rank}(V_0) + \operatorname{rank}(W_0) \\
=&(\operatorname{rank}(R) - \operatorname{rank}(R_0)) + (3 + n - \operatorname{rank}(Q)) + (m' - \operatorname{rank}(R)) \\
\geq& m'
\end{aligned}
$$

which implies $3 + n - \operatorname{rank}(Q) \geq \operatorname{rank}(R_0)$. By Equation (12), we have $\operatorname{rank}(R_0) = 3 + n - \operatorname{rank}(Q)$. By Equation (10) and the fact that S is invertible, there is a matrix $J_0 \in \mathrm{GL}(n + 3, \mathbb{F}_p)$ such that

$$
J_0 \cdot \begin{pmatrix} Q & R \end{pmatrix} = \begin{pmatrix} Q_1 & R_1 \\ Q_0 & 0 \\ 0 & R_0 \end{pmatrix} \tag{13}
$$

where Q_1 is of dimension $\tau_S \times (3 + n)$, R_1 is of dimension $\tau_S \times m'$, Q_0 is of dimension $(\operatorname{rank}(Q) - \tau_S) \times (3 + n)$, and R_0 is of dimension $(\operatorname{rank}(R) - \tau_S) \times m'$.

Notice that the intersection of any two spaces among the space spanned by the row vectors of V_0, the space spanned by the row vectors of W_0, and the space spanned by the row vectors of $R_1^T(-Z_{Q,V}^T + Z_{R,W}^T)$ only contains the zero row vector. There is a matrix $K_0 \in \mathrm{GL}(m', \mathbb{F}_p)$ such that the multiplication of K_0 and the submatrix on V and W (i.e., $S[4+n, 3+n+m', 1, 3+n+m']$) can be written as (by slightly abusing the notations of W_0 and V_0)

$$
\begin{aligned}
&K_0 \cdot \left(S[4 + n, 3 + n + m', 1, 3 + n + m']\right) \\
&= \begin{pmatrix} Z_{Q_1,V}Q_1 + Z_{Q_0,V}Q_0 & Z_{R_1,W}R_1 + Z_{R_0,W}R_0 \\ Z'_{Q_1,V}Q_1 + Z'_{Q_0,V}Q_0 & W_0 \\ V_0 & Z'_{R_1,V}R_1 + Z'_{R_0,V}R_0 \end{pmatrix}
\end{aligned} \tag{14}
$$

for some $\tau_S \times \tau_S$ dimensional $Z_{Q_1,V}, Z_{R_1,W}$, $\tau_S \times \operatorname{rank}(Q_0)$ dimensional $Z_{Q_0,V}$, $\tau_S \times \operatorname{rank}(R_0)$ dimensional $Z_{R_0,W}$, $(m' - \operatorname{rank}(R)) \times \tau_S$ dimensional $Z'_{Q_1,V}$, $(m' - \operatorname{rank}(R)) \times \operatorname{rank}(Q_0)$ dimensional $Z'_{Q_0,V}$, $(3 + n - \operatorname{rank}(Q)) \times \tau_S$ dimensional $Z'_{R_1,W}$, and $(3 + n - \operatorname{rank}(Q)) \times \operatorname{rank}(R_0)$ dimensional $Z'_{R_0,W}$. In the rest of this proof, we consider three cases.

Case 1. $\tau_S = 0$. Since Q_1 and R_1 do not exist by the condition of $\tau_S = 0$,

$$
K_0 \cdot (S[4 + n, 3 + n + m', 1, 3 + n + m']) = \begin{pmatrix} Z'_{Q_0,V}Q_0 & W_0 \\ V_0 & Z'_{R_0,W}R_0 \end{pmatrix}.
$$

Since

$$
-K_0 W B_\ell^T V^T K_0^T + K_0 V B_\ell W^T K_0^T = K_0(-W B_\ell^T V^T + V B_\ell W^T)K_0^T
$$

is a zero matrix,

$$
-Z'_{Q_0,V}Q_0 B_\ell R_0^T Z'^T_{R_0,W} + W_0 B_\ell^T V_0^T = W_0 B_\ell^T V_0^T
$$

41

is a zero matrix based on the fact that $QB_\ell R^T = 0$ for all the B_ℓ. Let q be the number of rows of Q_0. Let

$$S' = \begin{pmatrix} Q_0 & 0 \\ 0 & R_0 \\ 0 & W_0 \\ V_0 & 0 \end{pmatrix},$$

$J = J_0$, and $K = K_0$. Let $Q' = Q_0, R' = R_0, V' = V_0$, and $W' = W_0$.

By the fifth property of Lemma 6.3, each row vector v that is a row of V satisfies $vA_\ell = 0$ for each type 1 matrix F_ℓ, and thus the second condition of the current lemma holds.

For each type 2 matrix F_ℓ, by the fact that $Q_0 B_\ell R_0^T$ is a zero matrix, $S'F_\ell S'^T$ is also a type 2 matrix. Furthermore, we have

$$(S'F_\ell S'^T)[1, 3+n; 4+n, 3+n+m']$$
$$= \begin{pmatrix} Q_0 \\ 0 \end{pmatrix} B_\ell \begin{pmatrix} W_0 \\ 0 \end{pmatrix}^T - \begin{pmatrix} 0 \\ R_0 \end{pmatrix} B_\ell^T \begin{pmatrix} 0 \\ V_0 \end{pmatrix}^T$$
$$= J \left(SF_\ell S^T[1, 3+n; 4+n, 3+n+m'] \right) K^T.$$

Thus, the third condition of the current lemma also holds. Thus, the current lemma holds for this case.

Case 2. $\tau_S > 0$ and at least one of $Z_{Q_1,V}$ and $Z_{R_1,W}$ is full rank. We show that if $Z_{Q_1,V}$ is full rank, then the current lemma holds. The case that $Z_{R_1,W}$ is full rank is similar. Let $S^\dagger$ be the matrix of

$$S^\dagger = \begin{pmatrix} Q^\dagger & R^\dagger \\ K_0 \cdot V & K_0 \cdot W \end{pmatrix}$$

where

$$Q^\dagger = \begin{pmatrix} 0 \\ Q_0 \\ 0 \end{pmatrix} \text{ and } R^\dagger = \begin{pmatrix} R_1' \\ 0 \\ R_0 \end{pmatrix}$$

with $R_1' = R_1 - (Z_{Q_1,V})^{-1}(Z_{R_1,W}R_1 + Z_{R_0,W}R_0)$. Since $Q_0 B_\ell R^T$ is a zero matrix for every type 2 matrix F_ℓ, $Q^\dagger B_\ell (R^\dagger)^T$ is a zero matrix for every type 2 matrix F_ℓ. And thus, $(S^\dagger F_\ell (S^\dagger)^T)[1, 3+n; 1, 3+n]$ is a zero matrix for every type 2 matrix F_ℓ.

On the other hand, notice that

$$S^\dagger = \begin{pmatrix} X & U \\ 0 & I_{m'} \end{pmatrix} \begin{pmatrix} J_0 & 0 \\ 0 & K_0 \end{pmatrix} S$$

for some $X \in \mathrm{GL}(3+n, \mathbb{F}_p)$ and $U \in M(3+n, m', \mathbb{F}_p)$. We have

$$\begin{pmatrix} X & U \\ 0 & I_{m'} \end{pmatrix} \begin{pmatrix} J_0 & 0 \\ 0 & K_0 \end{pmatrix} = \begin{pmatrix} XJ_0 & UK_0 \\ 0 & K_0 \end{pmatrix} = \begin{pmatrix} XJ_0 & 0 \\ 0 & K_0 \end{pmatrix} \begin{pmatrix} I_{3+n} & J_0^{-1}X^{-1}UK_0 \\ 0 & I_{m'} \end{pmatrix}$$

using the fact that J_0 is an invertible matrix. Let

$$S' = \begin{pmatrix} (XJ_0)^{-1} & 0 \\ 0 & K_0^{-1} \end{pmatrix} S^\dagger = \begin{pmatrix} (XJ_0)^{-1}Q^\dagger & (XJ_0)^{-1}R^\dagger \\ V & W \end{pmatrix} \text{ and } P = \begin{pmatrix} I_{3+n} & J^{-1}UK \\ 0 & I_{m'} \end{pmatrix}.$$

We have $S' = PS$. Using the fact that $(S^\dagger F_\ell (S^\dagger)^T)[1, 3+n; 1, 3+n]$ is a zero matrix for every type 2 matrix F_ℓ, $(S'F_\ell S'^T)[1, 3+n; 1, 3+n]$ is a zero matrix for every type 2 matrix F_ℓ. Hence,

42

$PSF_\ell S^T P^T[1, 3+n; 1, 3+n]$ is a zero matrix for every type 2 matrix F_ℓ. By Lemma 6.5, $S'F_\ell S'^T = SF_\ell S^T$ for all the F_ℓ in $\mathcal{F}_{\mathbf{SC(G)}}$. In addition, since $Q^\dagger B_\ell (R^\dagger)^T$ is a zero matrix for each B_ℓ, we have $\tau_{S'} = 0$, where

$$\tau_{S'} := \dim\left(\left\langle\left\{v(XJ_0)^{-1}Q^\dagger B_\ell((XJ_0)^{-1}R^\dagger)^T : v \in \mathbb{F}_p^{3+n}, 1 \le \ell \le t\right\}\right\rangle\right).$$

By Case 1, the current lemma holds for this case.

Case 3. Both $Z_{Q_1,V}$ and $Z_{R_1,W}$ are not full rank. Let S'' be the matrix of

$$\begin{pmatrix} Q'' & R'' \\ V & W \end{pmatrix}$$

where

$$Q'' = \begin{pmatrix} Q_1'' \\ Q_0 \\ 0 \end{pmatrix} \text{ and } R'' = \begin{pmatrix} R_1'' \\ 0 \\ R_0 \end{pmatrix}$$

with $Q_1'' = Z_{R_1,W}Q_1$ and $R_1'' = (2Z_{R_1,W} - Z_{Q_1,V})R_1$. We prove some useful properties of S''

(a). S'' is a full rank matrix, and there is a full rank matrix $P'' = \begin{pmatrix} Z'' & U'' \\ 0 & I_{m'} \end{pmatrix}$ such that $S'' = P''S$.

(b). $S''F_\ell S''^T[1, 3+n; 1, 3+n]$ is a zero matrix for each type 2 matrix F_ℓ.

(c). $\tau_{S''} < \tau_S$, where

$$\tau_{S'} := \dim\left(\left\langle\left\{vQ''B_\ell(R'')^T : v \in \mathbb{F}_p^{3+n}, 1 \le \ell \le t\right\}\right\rangle\right).$$

To prove the property (a), we first show that $Z_{Q_1,V} - Z_{R_1,W}$ is a full rank matrix, i.e.,

$$\operatorname{rank}\left(Z_{Q_1,V} - Z_{R_1,W}\right) = \tau_S.$$

Suppose it is not. Then there is a row vector $v \in \mathbb{F}_p^{\tau_S}$ such that $v(Z_{Q_1,V} - Z_{R_1,W})$ is a zero row vector, which means that there is a non-zero linear combination of the first $3+n$ rows of S equals a non-zero linear combination of the last m' rows of S, which contradicts to the fact that S is a full rank matrix. Hence, $Z_{Q_1,V} - Z_{R_1,W}$ is a full rank matrix. Since there is an invertible matrix Z' such that

$$Z' \cdot S[1, 3+n; 1, 3+m] = \begin{pmatrix} (Z_{R_1,W} - Z_{Q_1,V})Q_1 & (Z_{R_1,W} - Z_{Q_1,V})R_1 \\ Q_0 & 0 \\ 0 & R_0 \end{pmatrix},$$

the property (a) holds.

To prove the property (b), we show that for each type 2 matrix F_ℓ, $Q''B_\ell R''^T - R''B_\ell^T Q''^T$ is a zero matrix. We have

$$\begin{aligned} Q_1''B_\ell R_1''^T &= Z_{R_1,W}Q_1 B_\ell R_1^T (2Z_{R_1,W} - Z_{Q_1,V})^T \\ &= 2Z_{R_1,W}Q_1 B_\ell R_1^T Z_{R_1,W}^T - Z_{R_1,W}Q_1 B_\ell R_1^T Z_{Q_1,V}^T \end{aligned}$$

$Z_{R_1,W}Q_1 B_\ell R_1^T Z_{R_1,W}^T$ is a skew-symmetric matrix by the fact that $Q_1 B_\ell R_1^T$ is a skew-symmetric matrix for all the $1 \le \ell \le t$. $Z_{R_1,W}Q_1 B_\ell R_1^T Z_{Q_1,V}^T$ is also a skew-symmetric matrix by the fact that $WB_\ell V^T$ is a zero matrix and Equation (14). Hence, $Q''B_\ell R''^T - R''B_\ell^T Q''^T$ is a zero matrix.

43

For the property (c), since $Z_{R_1, W}$ is not full rank, we have $\tau_{S''} < \tau_S$.
Let

$$S' = \begin{pmatrix} (Z'')^{-1} & 0 \\ 0 & I_{m'} \end{pmatrix} \quad S'' = \begin{pmatrix} (Z'')^{-1} & 0 \\ 0 & I_{m'} \end{pmatrix} \begin{pmatrix} Z'' & U'' \\ 0 & I_{m'} \end{pmatrix} \quad S = \begin{pmatrix} I_{3+n} & (Z'')^{-1}U'' \\ 0 & I_{m'} \end{pmatrix} S.$$

Based on the properties of S'', $S'' F_\ell S''^T [1, 3 + n; 1, 3 + n]$ is a zero matrix for each type 2 matrix F_ℓ, and $\tau_{S'} = \tau_{S''} < \tau_S$. By Lemma 6.5, we have $S' F_\ell S'^T = F'_\ell$ for each F_ℓ. Repeating the process for at most $3 + n$ times, we obtain a matrix of either Case 1 or Case 2. Then the current lemma follows. $\qquad\square$

The following lemma was proved in the proof of Lemma 2.2 in [FGS19].

Lemma 6.7. *Let $\mathcal{A} = (A_1, \ldots A_k)$ and $\mathcal{B} = (B_1, \ldots, B_k)$ be two matrix tuples in $M(m, n, \mathbb{F}_p)^k$. Suppose there are $1 \le q < m$ and $1 \le r < n$ such that each A_i equals*

$$\begin{pmatrix} A'_i & 0 \\ 0 & A''_i \end{pmatrix}$$

for some $A'_i \in M(q, r, \mathbb{F}_p)$ and $A''_i \in M(m - q, n - r, \mathbb{F}_p)$, and each B_i equals

$$\begin{pmatrix} A'_i & 0 \\ 0 & B''_i \end{pmatrix}$$

for some $B''_i \in M(m - q, n - r, \mathbb{F}_p)$. There are $P \in \mathrm{GL}(m, \mathbb{F}_p)$ and $Q \in \mathrm{GL}(n, \mathbb{F}_p)$ such that $PA_iQ = B_i$ for each $1 \le i \le k$ if and only if there are $P'' \in \mathrm{GL}(m - q, \mathbb{F}_p)$ and $Q'' \in \mathrm{GL}(n - r, \mathbb{F}_p)$ such that $P'' A''_i Q'' = B''_i$ for all the $1 \le i \le k$.

Now we give our algorithm for isometry testing of semi-canonical forms of two skew-symmetric matrix space tensors.

Isometry Testing of Tensor Semi-Canonical Forms Algorithm
Input: Semi-canonical forms $\mathbf{SC}(\mathbf{G})$ and $\mathbf{SC}(\mathbf{H})$ of two skew-symmetric matrix space tensors.
Output: Yes or no.

1. Return no if the parameters of the two semi-canonical forms are different. Otherwise, let $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$ be the parameters of the two semi-canonical forms.

2. Construct $\mathcal{F}_{\mathbf{SC}(\mathbf{G})} = (F_1, \ldots, F_t)$ and $\mathcal{F}_{\mathbf{SC}(\mathbf{H})} = (F'_1, \ldots, F'_t)$.

3. Run the skew-symmetric matrix tuple isometry algorithm on $\mathcal{F}_{\mathbf{SC}(\mathbf{G})}$ and $\mathcal{F}_{\mathbf{SC}(\mathbf{H})}$. If the algorithm returns no, then return no. Otherwise, the algorithm returns a matrix S of form

$$\begin{pmatrix} Q & R \\ V & W \end{pmatrix}$$

   for some P, Q, R, and S of dimensions $(n + 3) \times (n + 3)$, $(n + 3) \times m'$, $m' \times (n + 3)$, and $m' \times m'$ respectively.

4. If either Q or W is a full rank matrix, return yes.

---

5. Construct matrices $J \in \mathrm{GL}(3+n, \mathbb{F}_p)$, $K \in \mathrm{GL}(m', \mathbb{F}_p)$ and matrix $S' \in \mathrm{GL}(3+n+m', \mathbb{F}_p)$ of form

$$
S' = \begin{pmatrix} Q' & 0 \\ 0 & R' \\ 0 & W' \\ V' & 0 \end{pmatrix}
$$

for some positive integer q, Q' of dimension $q \times (3+n)$, V' of dimension $(3+n-q) \times (3+n)$, R' of dimension $(3+n-q) \times m'$, and W' of dimension $(m'-3-n+q) \times m'$ such that Lemma 6.6 is satisfied.

6. Return the output of the matrix tuple equivalence algorithm with matrix tuples $(V'B_1R'^T, \ldots, V'B_tR'^T)$ and $(R'B_1^TV'^T, \ldots, R'B_t^TV'^T)$.

Lemma 6.8. *There is an algorithm for the isometry testing of the semi-canonical forms of two skew-symmetric matrix space tensors in $\mathbb{F}_p^{m \times n \times n}$ for some prime $p > 2$ and positive integers n, m with running time* $\mathrm{poly}(n, m, p)$.

Proof. We first prove the correctness of the algorithm. By Definition 5.13 and Lemma 6.2, the two semi-canonical forms are isometric if and only if the following two conditions hold

(a) The two semi-canonical forms have the same parameters $\alpha_{\mathfrak{X}}, \beta_{\mathfrak{X}}, \alpha_{\mathfrak{Y}}$, and $\beta_{\mathfrak{Y}}$.

(b) There is a matrix S_0 of form

$$
\begin{pmatrix} Q_0 & 0 \\ 0 & W_0 \end{pmatrix}
$$

such that $S_0 \cdot \mathcal{F}_{\mathbf{SC(G)}} \cdot S_0^T = \mathcal{F}_{\mathbf{SC(H)}}$, where Q_0 is a $(3+n) \times (3+n)$ matrix and W_0 is an $m' \times m'$ matrix.

If the two input semi-canonical forms are isometric, then the first step of the algorithm does not return no by Definition 5.13. Hence, step 4 of the algorithm returns yes and a matrix S of form

$$
\begin{pmatrix} Q & R \\ V & W \end{pmatrix}.
$$

If at least one of Q and W is full rank, then the algorithm returns yes. Otherwise, step 6 of the algorithm constructs matrices J, K, and S' satisfying Lemma 6.6. Let Q'' be the $(3+n) \times (3+n)$ matrix such that

$$
Q''[1, q; 1, 3+n] = Q' \text{ and } Q''[q+1, 3+n; 1, 3+n] = V',
$$

and W'' be the $m' \times m'$ matrix such that

$$
W''[1, m'-3-n+q; 1, m'] = W' \text{ and } W''[m'-2-n+q, m'; 1, m'] = R'.
$$

By Lemma 6.6, for each type 2 matrix F_ℓ, we have

$$
Q'' B_\ell W''^T = \begin{pmatrix} Q' B_\ell W'^T & 0 \\ 0 & V' B_\ell R'^T \end{pmatrix},
$$

45

and

$$JB'_\ell K^T = \begin{pmatrix} Q'B_\ell W'^T & 0 \\ 0 & R'B_\ell^T V'^T \end{pmatrix}.$$

Since one necessary condition for two semi-canonical forms being isometric is that there are $Q^\dagger \in \mathrm{GL}(3+n, \mathbb{F}_p)$ and $W^\dagger \in \mathrm{GL}(m', \mathbb{F}_p)$ such that $Q^\dagger B_\ell (W^\dagger)^T = B'_\ell$ for all the type 2 matrices F_ℓ, by Lemma 6.7, the matrix tuples $(V'B_1 R'^T, \ldots, V'B_t R'^T)$ and $(R'B_1^T V'^T, \ldots, R'B_t V'^T)$ are isometric. Hence, the algorithm returns yes.

If the input two semi-canonical forms are not isometric, then at least one of condition (a) and condition (b) does not hold. If condition (a) does not hold, then the algorithm returns no at step 1. If condition (b) does not hold and the algorithm does not return no at step 3, then by Theorem 1.3, step 3 returns a matrix S of form

$$\begin{pmatrix} Q & R \\ V & W \end{pmatrix}$$

such that $S\mathcal{F}_{\mathbf{SC(G)}} S^T = \mathcal{F}_{\mathbf{SC(H)}}$. Both Q and W are not full rank because otherwise, by Lemma 6.4, Lemma 6.2 does not hold. Hence, step 5 of the algorithm constructs matrices J, K, and S' satisfying Lemma 6.6. Let Q'' be the $(3+n) \times (3+n)$ matrix such that $Q''[1, q; 1, 3+n] = Q'$ and $Q''[q+1, 3+n; 1, 3+n] = V'$. Let W'' be the $m' \times m'$ matrix such that $W''[1, m'-3-n+q; 1, m'] = W'$ and $W''[m'-2-n+q, m'; 1, m'] = R'$. By Lemma 6.6, for each type 2 matrix F_ℓ, we have

$$Q''B_\ell W''^T = \begin{pmatrix} Q'B_\ell W'^T & 0 \\ 0 & V'B_\ell R'^T \end{pmatrix},$$

and

$$JB'_\ell K^T = \begin{pmatrix} Q'B_\ell W'^T & 0 \\ 0 & R'B_\ell^T V'^T \end{pmatrix}.$$

The matrix tuples $(V'B_1 R'^T, \ldots, V'B_t R'^T)$ and $(R'B_1^T V'^T, \ldots, R'B_t V'^T)$ are not isometric because otherwise, it contradicts Lemma 6.2. By Theorem 2.3 the algorithm returns no.

The running time of the algorithm is obtained by Theorem 1.3, Theorem 2.3, and Lemma 6.6. $\qquad \square$

7   Proof of Theorem 1.1 and Theorem 1.2

We first present our algorithm for the isometry testing of skew-symmetric matrix spaces.

Isometry Testing of Skew-Symmetric Matrix Spaces Algorithm
Input: Linear bases for two skew-symmetric matrix spaces $\mathfrak{G}, \mathfrak{H} \leq SS(n, \mathbb{F}_p)$, both of dimension m, for some prime $p > 2$ and positive integers n, m.
Output: Yes or no.

1. Construct skew-symmetric matrix space tensors $\mathbf{G}$ and $\mathbf{H}$ for $\mathfrak{G}$ and $\mathfrak{H}$, respectively.

2. Return the output of the algorithm for the isometry testing of skew-symmetric matrix space tensors with $\mathbf{G}$ and $\mathbf{H}$.

Proof of Theorem 1.2. The correctness of the algorithm is by Lemma 5.4 and Lemma 5.14. Now we bound the running time. By Definition 5.1, $\mathfrak{G}$ and $\mathfrak{H}$ can be constructed in time poly(n, m, p). The running time of the second step of the algorithm is obtained by Lemma 5.14 and Lemma 6.8. $\qquad \square$

> **Isomorphism Testing for p-Groups of Class 2 and Exponent p Algorithm**
> **Input:** Two p-groups G and H of class 2 and exponent p for some prime $p > 2$.
> **Output:** Yes or no.
>
> 1. If the orders of the two groups are different, then return no. Otherwise, let n denote the order of group G, and k be $\log_p(n)$.
>
> 2. If $k \leq (\log_2(p))^5$, then
>
>   (a) Enumerate all the possible $g_1, \ldots, g_k \in G$ and $h_1, \ldots, h_k \in H$ such that $\{g_1, \ldots, g_k\}$ is a generating set of G and $\{h_1, \ldots, h_k\}$ is a generating set of H.
>
>   (b) For each enumeration, if $f(g_i) = h_i$ gives an isomorphism from G to H, then return yes.
>
>   (c) Return no.
>
> 3. Construct skew-symmetric matrix spaces $\mathfrak{G}$ and $\mathfrak{H}$ for groups G and H, respectively, via Baer's correspondence.
>
> 4. Return the output of the algorithm for the isometry testing of skew-symmetric matrix spaces with $\mathfrak{G}$ and $\mathfrak{H}$.

Proof of Theorem 1.1. The correctness of the algorithm is obtained by Theorem 2.6 and Theorem 1.2. Now we bound the running time of the algorithm. If $k \leq (\log_2(p))^5$, then the running time of the algorithm is $p^{O(k^2)}$ because there are p^k elements in each group, and there are $2k$ elements need to enumerate, k elements for G and k elements for H. Since

$$k = k^{5/6} \cdot k^{1/6} \leq k^{5/6} \cdot (\log_2(p))^{5/6} = (k \cdot \log_2(p))^{5/6},$$

we have $p^{O(k^2)} \leq p^{O(k \cdot (k \cdot \log_2(p))^{5/6})} = n^{O((\log n)^{5/6})}$. Hence, the running time for this case is $n^{O((\log n)^{5/6})}$.

If $k > (\log_2(p))^5$, then by Theorem 1.2, the running time of the algorithm is $p^{O(k^{1.8} \cdot \log_2(p))}$. Since

$$k^{0.8} \cdot \log_2(p) = k^{0.8} \cdot (\log_2(p))^{1/6} \cdot (\log_2(p))^{5/6} < k^{0.8} \cdot k^{1/30} \cdot (\log_2(p))^{5/6} = (k \cdot \log_2(p))^{5/6},$$

we have $p^{O(k^{1.8} \cdot \log_2(p))} \leq p^{O(k \cdot (k \cdot \log_2(p))^{5/6})} = n^{O((\log n)^{5/6})}$. Hence, the running time for this case is also $n^{O((\log n)^{5/6})}$. $\square$

References

[AL81]   MD Atkinson and S Lloyd. Primitive spaces of matrices of bounded rank. *Journal of the Australian Mathematical Society*, 30(4):473–482, 1981.

[Bab80]   László Babai. On the complexity of canonical labeling of strongly regular graphs. *SIAM J. Comput.*, 9(1):212–216, 1980.

[Bab81]   László Babai. On the order of uniprimitive permutation groups. *Annals of Mathematics*, 113(3):553—568, 1981.

[Bab16]   László Babai. Graph isomorphism in quasipolynomial time. In *ACM Symposium on Theory of Computing (STOC)*, pages 684–697, 2016.

[Bab19]   László Babai. Canonical form for graphs in quasipolynomial time: preliminary report. In *ACM Symposium on Theory of Computing (STOC)*, pages 1237–1246, 2019.

[Bae38]   Reinhold Baer. Groups with abelian central quotient group. *Transactions of the American Mathematical Society*, 44(3):357–386, 1938.

[BCGQ11] László Babai, Paolo Codenotti, Joshua A Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1395–1408, 2011.

[BCQ12]   László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups. In *International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 51–62. Springer, 2012.

[BCS⁺13]   László Babai, Xi Chen, Xiaorui Sun, Shang-Hua Teng, and John Wilmes. Faster canonical forms for strongly regular graphs. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 157–166, 2013.

[BES80]   László Babai, Paul Erdós, and Stanley M Selkow. Random graph isomorphism. *SIAM Journal on computing*, 9(3):628–635, 1980.

[BGL⁺19]   Peter A Brooksbank, Joshua A Grochow, Yinan Li, Youming Qiao, and James B Wilson. Incorporating weisfeiler-leman into algorithms for group isomorphism. *arXiv preprint arXiv:1905.02518*, 2019.

[BL83]   László Babai and Eugene M Luks. Canonical labeling of graphs. In *ACM Symposium on Theory of computing (STOC)*, pages 171–183, 1983.

[BLQW20] Peter A Brooksbank, Yinan Li, Youming Qiao, and James B Wilson. Improved algorithms for alternating matrix space isometry: From theory to practice. In *European Symposium on Algorithms (ESA)*, 2020.

[BMW15]   Peter A Brooksbank, Joshua Maglione, and James B Wilson. A fast isomorphism test for groups of genus 2. *arXiv preprint arXiv:1508.03033*, 2015.

[BQ12]   László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with abelian sylow towers. In *International Symposium on Theoretical Aspects of Computer Science (STACS)*, page 453, 2012.

[BS20]   Jendrik Brachter and Pascal Schweitzer. On the weisfeiler-leman dimension of finite groups. In *ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 287–300, 2020.

[BW12]   Peter Brooksbank and James Wilson. Computing isometry groups of hermitian maps. *Transactions of the American Mathematical Society*, 364(4):1975–1996, 2012.

[BW13]   László Babai and John Wilmes. Quasipolynomial-time canonical form for steiner designs. In *ACM Symposium on Theory of Computing (STOC)*, 2013.

[CST13] Xi Chen, Xiaorui Sun, and Shang-Hua Teng. Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems. In *ACM Symposium on Theory of Computing (STOC)*, 2013.

[DLN$^+$09] Samir Datta, Nutan Limaye, Prajakta Nimbhorkar, Thomas Thierauf, and Fabian Wagner. Planar graph isomorphism is in log-space. In *IEEE Conference on Computational Complexity (CCC)*, pages 203–214, 2009.

[DW22] Heiko Dietrich and James B Wilson. Group isomorphism is nearly-linear time for most orders. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 457–467. IEEE, 2022.

[FGS19] Vyacheslav Futorny, Joshua A Grochow, and Vladimir V Sergeichuk. Wildness for tensors. *Linear Algebra and its Applications*, 566:212–244, 2019.

[Fla62] Harley Flanders. On spaces of linear transformations with bounded rank. *Journal of the London Mathematical Society*, 1(1):10–16, 1962.

[FN70] Volkmar Felsch and Joachim Neubüser. On a programme for the determination of the automorphism group of a finite group. In *Computational Problems in Abstract Algebra*, pages 59–60, 1970.

[GJ79] Michael R Garey and David S Johnson. Computers and intractability. *A Guide to the*, 1979.

[GN19] Martin Grohe and Daniel Neuen. Canonisation and definability for graphs of bounded rank width. In *ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–13, 2019.

[GNS20] Martin Grohe, Daniel Neuen, and Pascal Schweitzer. A faster isomorphism test for graphs of small degree. *SIAM Journal on Computing*, 2020.

[GQ21a] Joshua A Grochow and Youming Qiao. On p-group isomorphism: search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. In *36th Computational Complexity Conference (CCC)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021.

[GQ21b] Joshua A Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials i: Tensor isomorphism-completeness. In *Innovations in Theoretical Computer Science Conference (ITCS)*, 2021.

[GWN20] Martin Grohe, Daniel Wiebking, and Daniel Neuen. Isomorphism testing for graphs excluding small minors. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 625–636, 2020.

[IQ19] Gábor Ivanyos and Youming Qiao. Algorithms based on*-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing. *SIAM Journal on Computing*, 48(3):926–963, 2019.

[JQSY19] Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: a candidate for post-quantum cryptography. In *Theory of Cryptography Conference*, pages 251–281. Springer, 2019.

[Kav07] Telikepalli Kavitha. Linear time algorithms for abelian group isomorphism and related problems. *Journal of Computer and System Sciences*, 73(6):986–996, 2007.

[KPS19] Sandra Kiefer, Ilia Ponomarenko, and Pascal Schweitzer. The weisfeiler–leman dimension of planar graphs is at most 3. *Journal of the ACM (JACM)*, 66(6):1–31, 2019.

[LG09] François Le Gall. Efficient isomorphism testing for a class of group extensions. In *International Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 625–636, 2009.

[LPPS17] Daniel Lokshtanov, Marcin Pilipczuk, Michał Pilipczuk, and Saket Saurabh. Fixed-parameter tractable canonization and isomorphism test for graphs of bounded treewidth. *SIAM Journal on Computing*, 46(1):161–189, 2017.

[LQ17] Yinan Li and Youming Qiao. Linear algebraic analogues of the graph isomorphism problem and the erdős-rényi model. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 463–474, 2017.

[Luk15] Eugene M Luks. Group isomorphism with fixed subnormal chains. *arXiv preprint arXiv:1511.00151*, 2015.

[LW10] Mark L Lewis and James B Wilson. Isomorphism in expanding families of indistinguishable groups. *arXiv preprint arXiv:1010.5466*, 2010.

[Mil78] Gary L. Miller. On the $n^{\log n}$ isomorphism technique: A preliminary report. In *ACM Symposium on Theory of Computing (STOC)*, pages 51–58, 1978.

[Neu22] Daniel Neuen. Isomorphism testing for graphs excluding small topological subgraphs. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1411–1434, 2022.

[O'B94] Eamonn A O'Brien. Isomorphism testing for p-groups. *Journal of Symbolic Computation*, 17(2):133–147, 1994.

[QST12] You-Ming Qiao, Jayalal Sarma, and Bang-Sheng Tang. On isomorphism testing of groups with normal hall subgroups. *Journal of Computer Science and Technology*, 27(4):687–701, 2012.

[Ros13] David J. Rosenbaum. Bidirectional collision detection and faster deterministic isomorphism testing. *arXiv preprint arXiv:1304.3935*, 2013.

[RW15] David J. Rosenbaum and Fabian Wagner. Beating the generator-enumeration bound for p-group isomorphism. *Theoretical Computer Science*, 593:16–25, 2015.

[Sav80] Carla Diane Savage. *An $O(n^2)$ algorithm for abelian group isomorphism*. North Carolina State University, 1980.

[Sch19] Tyler Schrock. *On the complexity of isomorphism in finite group theory and symbolic dynamics*. PhD thesis, University of Colorado at Boulder, 2019.

[Spi96] Daniel A. Spielman. Faster isomorphism testing of strongly regular graphs. In *ACM Symposium on Theory of Computing (STOC)*, pages 576–584, 1996.

[SW15] Xiaorui Sun and John Wilmes. Faster canonical forms for primitive coherent configurations. In *ACM Symposium on Theory of Computing (STOC)*, 2015.

[TDJ+22]   Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 582–612, 2022.

[Vik96]   Narayan Vikas. An $O(n)$ algorithm for abelian p-group isomorphism and an $O(n \log n)$ algorithm for abelian group isomorphism. *Journal of Computer and System Sciences*, 53(1):1–9, 1996.

[Web83]   UHM Webb. On the rank of a p-group of class 2. *Canadian Mathematical Bulletin*, 26(1):101–105, 1983.

[Wie20]   Daniel Wiebking. Graph isomorphism in quasipolynomial time parameterized by treewidth. In *International Colloquium on Automata, Languages, and Programming (ICALP)*, 2020.

[Wil09a]   James B Wilson. Decomposing p-groups via jordan algebras. *Journal of Algebra*, 322(8):2642–2679, 2009.

[Wil09b]   James B Wilson. Finding central decompositions of p-groups. *Journal of Group Theory*, 12(6):813–830, 2009.

[WL68]   Boris Weisfeiler and A. A. Lehman. A reduction of a graph to a canonical form and an algebra arising during this reduction. *Nauchno-Technicheskaya Informatsiya*, 9:12–16, 1968.

[ZKT85]   Viktor N Zemlyachenko, Nickolay M Korneenko, and Regina I Tyshkevich. Graph isomorphism problem. *Journal of Soviet Mathematics*, 29(4):1426–1481, 1985.