

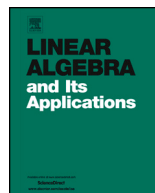


ELSEVIER

Contents lists available at ScienceDirect

# Linear Algebra and its Applications

journal homepage: [www.elsevier.com/locate/laa](http://www.elsevier.com/locate/laa)



## Testing isomorphism between tuples of subspaces

Emily J. King<sup>a,\*</sup>, Dustin G. Mixon<sup>b,c</sup>, Shayne Waldron<sup>d</sup>

<sup>a</sup> Department of Mathematics, Colorado State University, Fort Collins, CO, USA

<sup>b</sup> Department of Mathematics, The Ohio State University, Columbus, OH, USA

<sup>c</sup> Translational Data Analytics Institute, The Ohio State University, Columbus, OH, USA

<sup>d</sup> Department of Mathematics, The University of Auckland, Auckland, New Zealand

### ARTICLE INFO

#### Article history:

Received 29 May 2024

Received in revised form 24 December 2025

Accepted 29 December 2025

Available online 2 January 2026

Submitted by V. Mehrmann

#### MSC:

14M15

05C60

81R05

16G20

#### Keywords:

Subspace isomorphism

Grassmannian

Bargmann invariants

$H^*$ -algebras

Quivers

Graph isomorphism

### ABSTRACT

Given two tuples of subspaces, can you tell whether the tuples are isomorphic? We develop theory and algorithms to address this fundamental question. We focus on isomorphisms in which the ambient vector space is acted on by either a unitary group or general linear group. If isomorphism also allows permutations of the subspaces, then the problem is at least as hard as graph isomorphism. Otherwise, we provide a variety of polynomial-time algorithms with Matlab implementations to test for isomorphism.

© 2025 Elsevier Inc. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

\* Corresponding author.

E-mail address: [emily.king@colostate.edu](mailto:emily.king@colostate.edu) (E.J. King).

## 1. Introduction

The last decade has seen a surge of work to find arrangements of points in real and complex Grassmannian spaces that are well spaced in some sense; for example, one may seek **optimal codes**, which maximize the minimum distance between points, or **designs**, which offer an integration rule. While precursor work in this vein appeared between the '50s and '80s by Rankin [72,71], Grey [40], Seidel [74], Welch [88], and Levenshtein [62], the seminal paper by Conway, Hardin and Sloane [21] arrived later in 1996. The recent resurgence of interest in this problem has been largely stimulated by emerging applications in multiple description coding [80], digital fingerprinting [67], compressed sensing [7], and quantum state tomography [73].

There have been several fruitful approaches to studying arrangements of points in the Grassmannian. First, it is natural to consider highly symmetric arrangements of points. Such arrangements were extensively studied in [83,17,14,86,82,16] in the context of designs, and later, symmetry was used to facilitate the search for optimal codes [49–51, 60,12,57,52]. In many cases, the symmetries that underly optimal codes can be abstracted to weaker combinatorial structures that produce additional codes. For example, one may use strongly regular graphs to obtain optimal codes in  $\text{Gr}(1, \mathbf{R}^d)$  [87], or use Steiner systems to obtain optimal codes in  $\text{Gr}(1, \mathbf{C}^d)$  [37]. In this spirit, several infinite families of optimal codes have been constructed from combinatorial designs [54,59,36,33,34,32,29, 38,28]. In some cases, it is even possible to construct optimal codes from smaller codes [10, 84,11,58]. Researchers have also leveraged different computational techniques to find new arrangements [3,47,53] and to study various properties of known arrangements [19,31, 30,66,65]. See [8,35,85] for surveys of many of these results.

To date, the vast majority of this work has focused on the special case of projective spaces, and it is easy to explain this trend: it is harder to interact with points in general Grassmannian spaces. To illustrate this, suppose you are given two tuples  $A$  and  $B$  of  $r$ -dimensional subspaces of  $\mathbf{R}^d$ . You are told that the subspaces in  $A$  were drawn independently and uniformly at random from the Grassmannian  $\text{Gr}(r, \mathbf{R}^d)$ , and that  $B$  was drawn according to one of two processes: either there exists an orthogonal transformation  $g \in O(d)$  such that  $B = g \cdot A$ , or  $B$  was also drawn independently and uniformly at random. How can you tell which process was used to construct  $B$ ? In the special case where  $r = 1$ , the lines are almost surely not orthogonal, and one may leverage this feature to select vector representatives of the lines and then compute a canonical form of the Gramian (i.e., the reduced signature matrix discussed in [85]) that detects whether there exists  $g \in O(d)$  such that  $B = g \cdot A$ . However, if  $r > 1$ , it is not obvious how to find such an invariant. On the other hand, we benefit from the fact that many optimal configurations – like so-called *equiangular tight frames* – share certain properties – like not being pairwise orthogonal – with generic configurations, allowing results about generic configurations to be applied to certain optimal configurations.

This obstruction has had substantial ramifications on progress toward optimal codes in more general Grassmannian spaces. In particular, Sloane maintains an online cata-

$\log$  [77] of putatively optimal codes in  $\text{Gr}(r, \mathbf{R}^d)$  for  $r \in \{1, 2, 3\}$  and  $d \in \{3, \dots, 16\}$ . Suppose one were to find a code for  $r \in \{2, 3\}$  that is competitive with Sloane's corresponding putatively optimal code. Are these codes actually the same up to rotation? If researchers cannot easily answer this question, then they are less inclined to contribute to the hunt for optimal codes in these more general Grassmannian spaces. Alternatively, optimal packings that are different (even up to unitary transformations) might have different structures which may be exploited. For example, different structures that appear in distinct optimal configurations of 9 points in  $\text{Gr}(1, \mathbf{C}^3)$  [48] led to progress on Zauner's conjecture in quantum information theory [2,22], along with infinite classes of optimal packings with nice matroidal structures [12]. While there are several works in the literature that treat related problems [78,89,68,55,76,45,44], the particular problem we identify has yet to be treated. The primary purpose of this paper is to help close this gap with both theory and code.

Notationally, we let  $\mathbf{F}$  denote an arbitrary field. Every  $\Gamma \leq \text{GL}(d, \mathbf{F})$  has a natural action on  $\text{Gr}(r, \mathbf{F}^d)$ . Given an involutive automorphism  $\sigma$  of  $\mathbf{F}$ , we consider the Hermitian form defined by  $\langle x, y \rangle = \sum_i \sigma(x_i)y_i$ , and we let  $\text{U}(d, \mathbf{F}, \sigma)$  denote the subgroup of all  $g \in \text{GL}(d, \mathbf{F})$  such that  $\langle gx, gy \rangle = \langle x, y \rangle$  for all  $x, y \in \mathbf{F}^d$ . For example,  $\text{U}(d, \mathbf{F}, \sigma)$  contains all  $d \times d$  permutation matrices. Over any field, the identity is an involutive automorphism and over quadratic extensions one may choose the only nontrivial field automorphism as the involution (see, e.g., [41,42]). Specifically, we also adopt the standard notations for the orthogonal group  $\text{O}(d) = \text{U}(d, \mathbf{R}, \text{id})$  and the unitary group  $\text{U}(d) = \text{U}(d, \mathbf{C}, \bar{\cdot})$ . For  $\mathbf{F} \in \{\mathbf{R}, \mathbf{C}\}$ , we say that **generic** points in  $\text{Gr}(r, \mathbf{F}^d)$  satisfy property  $P$  if there exists an open and dense subset  $S \subseteq \mathbf{F}^{d \times r}$  such that for every  $A \in S$ , it holds that  $V := \text{im } A \in \text{Gr}(r, \mathbf{F}^d)$  and  $V$  has property  $P$ . Throughout this paper, this open and dense subset turns out to be the complement of the zero set of a nonzero real polynomial, and so one may think of genericity in terms of the associated Zariski topology.

Our problem can be viewed as an instance of a more general, fundamental problem:

**Problem 1** (*Common orbit*). Given a  $G$ -set  $X$  and two points  $x, y \in X$ , determine whether there exists  $g \in G$  such that  $g \cdot x = y$ .

One attractive approach to solving the common orbit problem is to construct an **invariant**, that is, a function  $f: X \rightarrow S$  for some set  $S$  such that  $f(x) = f(y)$  only if there exists  $g \in G$  such that  $g \cdot x = y$ . In particular,  $f(x)$  is determined by the orbit  $G \cdot x$ . If  $f$  always returns different values for different orbits, then we say  $f$  is a **complete invariant**. Observe that a *complete* invariant provides a complete solution to common orbit (hence the name), since one may simply compare  $f(x)$  with  $f(y)$ .

We will study three types of common orbit problems with  $X = (\text{Gr}(r, \mathbf{F}^d))^n$ . In particular, for  $\Gamma \in \{\text{U}(d, \mathbf{F}, \sigma), \text{GL}(d, \mathbf{F})\}$ , we consider the following actions on  $X$ :

$$G = \Gamma \times S_n, \quad (g, \pi) \cdot (x_i)_{i \in [n]} = (g \cdot x_{\pi^{-1}(i)})_{i \in [n]}; \quad G = \Gamma, \quad g \cdot (x_i)_{i \in [n]} = (g \cdot x_i)_{i \in [n]}.$$

Here,  $S_n$  denotes the symmetric group on  $n$  letters. In the following section, we show that any solution to common orbit in the case of  $G = \Gamma \times S_n$  can be used to solve graph isomorphism, thereby suggesting that this case is computationally hard. Next, Section 3 treats the case  $G = \Gamma \in \{O(d), U(d)\}$ . First, we show how to obtain a canonical choice of Gramian for generic real planes (i.e., points in  $\text{Gr}(2, \mathbf{R}^d)$ ), before finding injective invariants using ideas from the representation theory of  $H^*$ -algebras. We note that the remaining orbit problem with  $G = \Gamma = \text{GL}(d, \mathbf{F})$  has been completely solved, not only for  $\mathbf{F} \in \{\mathbf{R}, \mathbf{C}\}$  but also for other rings and fields [13,18,81,75,70]. Matlab implementations of Algorithm 1, Algorithm 2, and Lemma 11 may be downloaded from [56].

## 2. Isomorphism up to permutation

An important instance of common orbit is when  $G = S_m \times S_n$  acts on  $X = \{0, 1\}^{m \times n}$  by  $(g, h) \cdot x = gxh^{-1}$ . If we restrict  $X$  to only include matrices for which each column has exactly two 1s and no two columns are equal, then  $X$  corresponds to the set of incidence matrices of simple graphs on  $m$  vertices and  $n$  edges, and the common orbit problem corresponds to graph isomorphism:

**Problem 2** (*Graph isomorphism*). Given two simple graphs  $G$  and  $H$ , determine whether  $G \sim H$ , that is, there exists a bijection  $f: V(G) \rightarrow V(H)$  between the vertices that preserves the edges; i.e., for every  $u, v \in V(G)$ , it holds that  $\{u, v\} \in E(G)$  if and only if  $\{f(u), f(v)\} \in E(H)$ .

In general, a **decision problem** is a pair  $(P, M)$  where  $P$  maps problem instances to answers  $P: Q \rightarrow \{\text{yes}, \text{no}\}$  and  $M: Q \rightarrow \mathbf{N}$  measures the size of the problem instance. For example, for the graph isomorphism problem,  $Q$  is the set of all  $(G, H)$ , where  $G$  and  $H$  are both simple graphs,  $P(G, H)$  returns whether  $G$  and  $H$  are isomorphic, and if we represent  $G$  and  $H$  in terms of their incidence matrices, we are inclined to take  $M(G, H) = |V(G)||E(G)| + |V(H)||E(H)|$ . We say a decision problem  $(P, M)$  is **GI-hard** if, given a black box that computes  $P(x)$ , one may solve graph isomorphism by an algorithm that uses that black box, and that, outside of that black box, takes time that is at most polynomial in the number of vertices in the input graphs  $G$  and  $H$ . For example, if we restrict the input set of graph isomorphism to only consider  $(G, H)$  for which  $G$  and  $H$  are regular graphs, then the resulting subproblem is known to be GI-hard [90]. Today, the fastest known graph isomorphism algorithm in the worst case has quasipolynomial runtime [4], though faster algorithms are available in practice [64]. Graph isomorphism is one of a few problems that are believed to be NP-intermediate, meaning it is in NP, but not in P, and not NP-complete.

This section is concerned with two different isomorphism problems between tuples of subspaces. In both cases, we focus our attention on a discrete set of problem instances. Given a field  $\mathbf{F}$ , take  $0, 1 \in \mathbf{F}$  and let  $Q(r, d, n, \mathbf{F})$  denote the set of  $(A, B) \in (\{0, 1\}^{d \times r})^n \times (\{0, 1\}^{d \times r})^n$  such that  $\text{rank } A_i = \text{rank } B_i = r$  for every  $i \in [n]$ .

The standard representation of  $(A, B) \in Q(r, d, n, \mathbf{F})$  uses  $2rdn$  bits. With this, we may define our decision problems:

- $\mathcal{P}_U(r, \mathbf{F}, \sigma) = (P, M)$ , where  $\mathbf{F}$  is an arbitrary field with involutive automorphism  $\sigma$ ,  $Q = \bigcup_{d, n \geq 1} Q(r, d, n, \mathbf{F})$ ,  $P(A, B)$  returns whether there exists  $(g, \pi) \in U(d, \mathbf{F}, \sigma) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ , where  $d = d(A, B)$  and  $n = n(A, B)$ , and  $M(A, B) = 2 \cdot r \cdot d(A, B) \cdot n(A, B)$ .
- $\mathcal{P}_{GL}(\mathbf{F}) = (P, M)$ , where  $\mathbf{F}$  is an arbitrary field,  $Q = \bigcup_{r, d, n \geq 1} Q(r, d, n, \mathbf{F})$ ,  $P(A, B)$  returns whether there exists  $(g, \pi) \in GL(d, \mathbf{F}) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ , where  $d = d(A, B)$  and  $n = n(A, B)$ , and  $M(A, B) = 2 \cdot r(A, B) \cdot d(A, B) \cdot n(A, B)$ .

In words,  $\mathcal{P}_U(r, \mathbf{F}, \sigma)$  concerns isomorphism up to unitary and permutation for any fixed rank  $r$ , whereas  $\mathcal{P}_{GL}(\mathbf{F})$  concerns isomorphism up to linear automorphism and permutation, but with the rank no longer fixed. As we will see, both problems are hard. Prior work studied the special case where  $r = 1$ . For work relating to  $\mathcal{P}_U(1, \mathbf{R}, \sigma)$ , see [20]. The fact that  $r$  is fixed for one problem and not for the other is an artifact of our proof of hardness. In particular, by fixing  $r = 1$  rather than all  $r$ , one may consider a problem denoted as  $\mathcal{P}_{GL}(1, \mathbf{F})$  for arbitrary fields  $\mathbf{F}$ . This problem is known as monomial code equivalence and is related to permutational code equivalence, which are both known to be GI-hard [9, 43, 69]. This might suggest that  $\mathcal{P}_{GL}(r, \mathbf{F})$  is GI-hard for each  $r$ . However, our proof technique relies on a reduction to regular graph isomorphism in which  $r$  is determined by the graph degree; n.b. bounded degree GI is in P, while GI is not known to be [63].

**Theorem 3.** *The following problems are GI-hard:*

- $\mathcal{P}_U(r, \mathbf{F}, \sigma)$  for every  $r \in \mathbf{N}$  and every field  $\mathbf{F}$  with involutive automorphism  $\sigma$  and
- $\mathcal{P}_{GL}(\mathbf{F})$  for every field  $\mathbf{F}$ .

**Proof.** (a) Fix  $r$ ,  $\mathbf{F}$  and  $\sigma$ . We will use a  $\mathcal{P}_U(r, \mathbf{F}, \sigma)$  oracle to efficiently solve graph isomorphism. Given two simple graphs  $G$  and  $H$ , we return no if  $V(G)$  and  $V(H)$  are of different size, or if  $E(G)$  and  $E(H)$  are of different size. Otherwise, put  $n := |V(G)|$ ,  $e = |E(G)|$  and  $d := re$ , and for each graph, arbitrarily label the vertices and edges with members of  $[n]$  and  $[e]$ , respectively. We use this labeling of  $G$  to determine  $A$ . Specifically, for each  $j \in [n]$ , define  $A_j \in \mathbf{F}^{d \times r}$  to consist of  $e$  blocks of size  $r \times r$ , where for each  $i \in [e]$ , the  $i$ th block of  $A_j$  is  $I_r$  if  $j$  is a vertex in edge  $i$ , and otherwise the block is zero. Define  $B$  similarly in terms of our labeling of  $H$ . Given  $(A, B)$ , the  $\mathcal{P}_U(r, \mathbf{F}, \sigma)$  oracle returns whether there exists  $(g, \pi) \in U(d, \mathbf{F}, \sigma) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ , and we will output this answer as our solution to graph isomorphism. It remains to show that  $G \sim H$  if and only if there exists  $(g, \pi) \in U(d, \mathbf{F}, \sigma) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ . For  $(\Rightarrow)$ , observe that a graph isomorphism

determines a choice of  $\pi \in S_n$  as well as a permutation of edges. This permutation of edges can be implemented as a block permutation matrix  $g \in \mathbf{U}(d, \mathbf{F}, \sigma)$  so that  $gA_{\pi^{-1}(i)} = B_i$ , which then implies  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ . For  $(\Leftarrow)$ , we first define two additional graphs  $G'$  and  $H'$ , both on vertex set  $[n]$ . For  $G'$ , say  $i \leftrightarrow j$  if there exists  $x \in \text{im } A_i$  and  $y \in \text{im } A_j$  such that  $\langle x, y \rangle \neq 0$ . Define  $H'$  similarly in terms of  $B$ . By our construction of  $A$  and  $B$ , it holds that  $G' \sim G$  and  $H' \sim H$ . Furthermore, the existence of  $(g, \pi) \in \mathbf{U}(d, \mathbf{F}, \sigma) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$  implies that  $G' \sim H'$ , meaning  $G \sim H$ , as desired.

(b) Fix  $\mathbf{F}$ . We will use a  $\mathcal{P}_{\text{GL}}(\mathbf{F})$  oracle to efficiently solve graph isomorphism for regular graphs, which suffices by [90]. Without loss of generality, we may put  $n := |V(G)| = |V(H)|$ ,  $d := |E(G)| = |E(H)|$ , and let  $r$  denote the common degree of  $G$  and  $H$ . For each graph, arbitrarily label the vertices and edges with members of  $[n]$  and  $[d]$ , respectively, and let  $(e_i)_{i \in [d]}$  denote the identity basis in  $\mathbf{F}^d$ . For each  $j \in [n]$ , select  $A_j \in \mathbf{F}^{d \times r}$  so that its column vectors are the  $r$  members of  $(e_i)_{i \in [d]}$  that correspond to edges  $i$  incident to vertex  $j$ . Define  $B$  similarly in terms of our labeling of  $H$ . Given  $(A, B)$ , the  $\mathcal{P}_{\text{GL}}(\mathbf{F})$  oracle returns whether there exists  $(g, \pi) \in \text{GL}(d, \mathbf{F}) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ , and we will output this answer as our solution to graph isomorphism. It remains to show that  $G \sim H$  if and only if there exists  $(g, \pi) \in \text{GL}(d, \mathbf{F}) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ . For  $(\Rightarrow)$ , the isomorphism determines a permutation matrix  $g \in \text{GL}(d, \mathbf{F})$  and a permutation  $\pi \in S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$ . For  $(\Leftarrow)$ , we first define two additional graphs  $G'$  and  $H'$ , both on vertex set  $[n]$ . For  $G'$ , say  $i \leftrightarrow j$  if  $\text{im } A_i \cap \text{im } A_j \neq \{0\}$ , and define  $H'$  similarly in terms of  $B$ . By our construction of  $A$  and  $B$ , it holds that  $G' \sim G$  and  $H' \sim H$ . Furthermore, the existence of  $(g, \pi) \in \text{GL}(d, \mathbf{F}) \times S_n$  such that  $(g, \pi) \cdot (\text{im } A_i)_{i \in [n]} = (\text{im } B_i)_{i \in [n]}$  implies that  $G' \sim H'$ , meaning  $G \sim H$ , as desired.  $\square$

Of course, Theorem 3 does not mean that solving  $\mathcal{P}_{\text{U}}(r, \mathbf{F}, \sigma)$  or  $\mathcal{P}_{\text{GL}}(\mathbf{F})$  is always hopeless. (In particular, graph isomorphism is solvable in practice [64].) As an example, the Bargmann invariants computed in Section 3.1 are ordered lists of numbers; if the histograms of these numbers are not equal, then the lines cannot be isomorphic up to permutation.

### 3. Isomorphism up to linear isometry

While the previous section demonstrated that certain isomorphism problems are hard, this section will show that isomorphism up to linear isometry is relatively easy. This would have taken Halmos by surprise, as he considered this problem to be difficult even for triples of subspaces [46]. Throughout this section, we assume  $\mathbf{F} \in \{\mathbf{R}, \mathbf{C}\}$  without mention, meaning  $\mathbf{U}(d, \mathbf{F}, \sigma) \in \{\mathbf{O}(d), \mathbf{U}(d)\}$ .

### 3.1. Lines

Chien and Waldron [16] provide a complete invariant for tuples of lines in  $\mathbf{F}^d$  up to isometric isomorphism. Given a tuple  $(v_i)_{i \in [n]}$  of unit vectors in  $\mathbf{F}^d$  that span each line in the tuple  $\mathcal{L} = (\ell_i)_{i \in [n]}$ , define<sup>1</sup> the  $m$ -**vertex Bargmann invariants** or  $m$ -**products** by

$$\Delta(v_{i_1}, \dots, v_{i_m}) := \langle v_{i_1}, v_{i_2} \rangle \langle v_{i_2}, v_{i_3} \rangle \cdots \langle v_{i_m}, v_{i_1} \rangle, \quad i_1, \dots, i_m \in [n].$$

Denoting  $P_i := v_i v_i^*$ , we see that  $\Delta(v_{i_1}, \dots, v_{i_m}) = \text{tr}(P_{i_1} \cdots P_{i_m})$ , and so the choice of  $v_i \in \ell_i$  is irrelevant. Furthermore, as their name suggests, these quantities are invariant to isometric isomorphism, since for  $Q \in \text{U}(d, \mathbf{F}, \sigma)$ , the orthogonal projection onto  $Q \cdot \ell_i$  is  $Q P_i Q^*$ , and  $\text{tr}(Q P_{i_1} Q^* \cdots Q P_{i_m} Q^*) = \text{tr}(P_{i_1} \cdots P_{i_m})$ .

Let's take a moment to discuss the relationship to classical invariant theory. In the special case where  $\mathbf{F} = \mathbf{R}$ , we are interested in the orbit of  $(v_i)_{i \in [n]} \in (\mathbf{R}^d)^n$  under the action of  $\text{O}(d) \times \text{O}(1)^n$ . Any polynomial that is invariant to this group is invariant to the subgroup  $\text{O}(d)$ , and is therefore a polynomial of  $(x_{ij} := \langle v_i, v_j \rangle)_{1 \leq i \leq j \leq n}$  by the first fundamental theorem of invariant theory for the orthogonal group. Next, if we apply the Reynolds operator of  $\text{O}(1)^n$  to any monic monomial of the  $x_{ij}$ 's, the result is either zero or the same monomial, with the later case occurring precisely when the multiset of indices  $ij$  that appear in the monomial form the edges of a (not necessarily simple) graph with vertex set  $[n]$  in which every vertex has even degree. Since every such graph can be decomposed into cycles, it follows that the  $m$ -products with  $m \in [n]$  together generate the algebra of polynomial invariants, which in turn separates the orbits. As we discuss below, Chien and Waldron [16] identify a much smaller subset of  $m$ -products separate these orbits.

Given the 2-products, one may define the **frame graph**  $G(\mathcal{L})$  on  $[n]$  in which we draw an edge  $i \leftrightarrow j$  when  $\ell_i$  and  $\ell_j$  are not orthogonal; we note that the frame graph has also been referred to as the *correlation network* [79]. Letting  $E$  denote the edge set of the frame graph, then the indicator functions of the edge sets of Eulerian subgraphs of  $G(\mathcal{L})$  form a subspace  $\mathcal{E} \subseteq \mathbf{F}_2^E$ . Given a maximal spanning forest  $F$  of  $G(\mathcal{L})$ , then each edge in  $E \setminus E(F)$  completes a unique cycle with this forest, and the indicator functions of the edge sets of these cycles form a basis for  $\mathcal{E}$ . Let  $C(F)$  denote the set of these cycles. With these notions, we may enunciate the main result of [16] (for unweighted lines).

**Proposition 4** (Corollary 3.2 in [16], cf. Theorem 2 in [39]). *Given a tuple  $\mathcal{L}$  of lines in  $\mathbf{F}^d$ , select any maximal spanning forest  $F$  of the frame graph  $G(\mathcal{L})$ . Then  $\mathcal{L}$  is determined up to isometric isomorphism by its 2-products and each  $m$ -product corresponding to a cycle in  $C(F)$ .*

<sup>1</sup> Our definition differs slightly from [16] since our inner product is conjugate-linear in the first argument.

**Proof.** Let  $\mathcal{L}$  and  $\mathcal{L}'$  be  $n$ -tuples of lines in  $\mathbf{F}^d$ . As noted above, if  $\mathcal{L}$  and  $\mathcal{L}'$  are isometrically isomorphic, then all of their  $m$ -products must be equal.

For the other direction, select an  $n$ -tuple of unit vectors  $\{v_i\}_{i=1}^n$  in  $\mathbf{F}^d$  that span the lines in  $\mathcal{L}$ . Let  $\{u_i\}_{i=1}^n$  be another  $n$ -tuple of unit vectors in  $\mathbf{F}^d$  such that the 2-products and each  $m$ -product corresponding to a cycle in  $C(F)$  (corresponding to a spanning forest  $F$  of  $\mathcal{L}$ ) of each tuple of vectors are equal. We would like to show that  $\{v_i\}_{i=1}^n$  and  $\{u_i\}_{i=1}^n$  are the same modulo  $U(d, \mathbf{F}, \sigma)$  and choice of basis vectors. Since the spectral theorem implies tuples of vectors are the same modulo  $U(d, \mathbf{F}, \sigma)$  if and only if their Gramians are component-wise equal, it suffices to show that there exist unimodular  $\eta_i$  for  $i \in [n]$  such that for all  $i, j \in [n]$

$$\langle u_i, u_j \rangle = \overline{\eta_i} \eta_j \langle v_i, v_j \rangle. \quad (1)$$

If  $i$  and  $j$  are in different components of  $G(\mathcal{L})$  (where we are using  $i$  as shorthand for  $\ell_i$ ), then  $\langle v_i, v_j \rangle = 0$  and (1) yields no restriction on the values of  $\eta_i$  and  $\eta_j$ . Thus, we may assume without loss of generality that  $G(\mathcal{L})$  is connected and  $F$  is a spanning tree with root  $r$ . Since 2-products are equal,

$$|\langle u_i, u_j \rangle|^2 = \langle u_i, u_j \rangle \langle u_j, u_i \rangle = \langle v_i, v_j \rangle \langle v_j, v_i \rangle = |\langle v_i, v_j \rangle|^2$$

for all  $i, j \in [n]$ . For  $i \in [n]$  such that  $ri$  is an edge in  $F$ , let  $\eta_i$  be the necessarily unimodular scalar such that  $\langle u_r, u_i \rangle = \eta_i \langle v_r, v_i \rangle$ . Now for  $j \in [n]$  such that  $ri$  and  $ij$  are edges in  $F$  but not  $rj$  let  $\eta_j$  be the necessarily unimodular scalar such that (1) holds. Continue this process inductively, setting the  $\eta_k$  for vertices  $k$  at distance 3, 4, ... from  $r$ . Since  $F$  is spanning, we have uniquely defined  $\eta_i$  for each  $i \in [n]$ . However, we now need to verify that (1) holds for any  $ij$  that is an edge in  $G(\mathcal{L})$  but not  $F$ . Let  $ij$  be such an edge; it lies in a unique cycle in  $C(F)$ , say with vertex sequence  $i, j, k_3, k_4, \dots, k_m, i$ . Since each edge but  $ij$  lies in  $F$ ,

$$\begin{aligned} & \langle v_i, v_j \rangle \langle v_j, v_{k_3} \rangle \langle v_{k_3}, v_{k_4} \rangle \cdots \langle v_{k_m}, v_i \rangle \\ &= \langle u_i, u_j \rangle \langle u_j, u_{k_3} \rangle \langle u_{k_3}, u_{k_4} \rangle \cdots \langle u_{k_m}, u_i \rangle \\ &= \langle u_i, u_j \rangle \overline{\eta_j} \eta_{k_3} \langle v_j, v_{k_3} \rangle \overline{\eta_{k_3}} \eta_{k_4} \langle v_{k_3}, v_{k_4} \rangle \cdots \overline{\eta_{k_m}} \eta_i \langle v_{k_m}, v_i \rangle \\ &= \eta_i \overline{\eta_j} \langle u_i, u_j \rangle \langle v_j, v_{k_3} \rangle \langle v_{k_3}, v_{k_4} \rangle \cdots \langle v_{k_m}, v_i \rangle, \end{aligned}$$

implying that (1) holds for  $ij$ , as desired.  $\square$

Generically (or for equiangular tight frames and certain other optimal configurations), none of the inner products  $\langle v_i, v_j \rangle$  equal zero. In this case, the frame graph is complete, and so we may take  $F$  to be the star graph in which  $1 \leftrightarrow j$  for every  $j \neq 1$ . Then  $C(F)$  consists of all triangles in  $K_n$  that have 1 as a vertex. Alternatively, we can put the Gramian  $A = (\langle v_i, v_j \rangle)_{i,j \in [n]}$  in a canonical form by taking  $D = \text{diag}(\text{sgn}\langle v_1, v_1 \rangle, \dots, \text{sgn}\langle v_1, v_n \rangle)$  and  $G = DAD^*$ . Here,  $\text{sgn}(re^{i\theta}) = e^{i\theta}$ , and so  $DAD^*$  has all positive entries in its first



row and column. We refer to  $G$  as the **normalized Gramian** of  $A$ . Since the Gramian of  $(v_i)_{i \in [n]}$  is invariant to isometries acting on  $(v_i)_{i \in [n]}$ , normalizing the Gramian removes any ambiguity introduced by selecting  $v_i \in \ell_i$ , and so the normalized Gramian is a generically injective invariant for  $(\text{Gr}(1, \mathbf{F}^d))^n$  modulo  $U(d, \mathbf{F}, \sigma)$ . Notice that the entries of  $G$  are the triple products corresponding to  $C(F)$ , and so this conclusion may also be viewed in terms of Proposition 4.

At this point, we can treat the case of lines from two related but different perspectives: Generically (and for certain optimal configurations), it suffices to compute the normalized Gramian, but in general, we must appeal to more intricate Bargmann invariants. In what follows, we will see that a similar story holds for general subspaces.

### 3.2. Real, nowhere orthogonal planes

We say two subspaces  $U, V \subseteq \mathbf{F}^d$  are **nowhere orthogonal** if  $U \cap V^\perp = U^\perp \cap V = \{0\}$ . By counting dimensions, one may conclude that subspaces are nowhere orthogonal only if they have the same dimension. Given bases  $(u_i)_{i \in [r]}$  and  $(v_i)_{i \in [r]}$  for  $U$  and  $V$ , nowhere orthogonality is equivalent to the cross Gramian  $(\langle u_i, v_j \rangle)_{i,j \in [r]}$  being invertible. As one might expect, nowhere orthogonality is a generic property of subspaces of common dimension; we provide a short proof in the real case:

**Lemma 5.** *Two generic  $r$ -dimensional subspaces of  $\mathbf{R}^d$  are nowhere orthogonal.*

**Proof.** Given  $A_1, A_2 \in \mathbf{R}^{d \times r}$ , then  $\text{im } A_1$  and  $\text{im } A_2$  are nowhere orthogonal subspaces of dimension  $r$  if and only if  $f(A_1, A_2) := \det(A_1^* A_2) \neq 0$ . Since the polynomial  $f$  is nonzero at  $A_1 = A_2 = [I_r; 0]$ , it follows that  $f \neq 0$ , and so  $f^{-1}(\mathbf{R} \setminus \{0\})$  is a generic set, as desired.  $\square$

In this section, we consider the special case of nowhere orthogonal 2-dimensional subspaces of  $\mathbf{R}^d$ . This case is particularly relevant to the study of real equi-isoclinic planes, which have received some attention recently [24,26,25,27,58]. In general, subspaces are said to be **equi-isoclinic** if there exists  $\theta > 0$  such that every principal angle between any two of the subspaces equals  $\theta$ . (Note that equi-isoclinic subspaces with  $\theta < \frac{\pi}{2}$  are nowhere orthogonal.) Such subspaces were introduced by Lemmens and Seidel [61], and at times, they emerge as arrangements of points in the Grassmannian that maximize the minimum chordal distance [23]. In fact, most of Sloane's chordal-distance codes of real planes [77] are nowhere orthogonal, and well over half have the property that all cross Gramians have a minimum singular value greater than  $10^{-4}$ .

In what follows, we obtain a normalized Gramian for real, nowhere orthogonal planes, and to do so, we exploit several features of this special case. For example, the singular values of a cross Gramian between two planes are either all equal or all distinct. We will also leverage consequences of the fact that  $\text{SO}(2)$  is abelian:

**Lemma 6.** *If  $A \in \text{SO}(2)$  and  $B \in \text{O}(2)$ , then  $A^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} A \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$  and  $AB = BA^{\det B}$ .*

**Algorithm 1:** Canonical Gramian between real, nowhere orthogonal planes.**Data:** Gramian  $A \in (\mathbf{R}^{2 \times 2})^{n \times n}$  of orthobases of  $n$  nowhere orthogonal planes in  $\mathbf{R}^d$ **Result:** Gramian  $G \in (\mathbf{R}^{2 \times 2})^{n \times n}$  of another choice of orthobasesPut  $R = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$  and  $S = \text{diag}(R, \dots, R)$ **if** there exists  $(k, l)$  such that  $A_{kl}$  has distinct singular values **then**    Let  $(k, l)$  be the first such indices, lexicographically    Compute the singular value decomposition  $A_{kl} = W_k \Sigma V^*$  and put  $\widetilde{W}_k = W_k R$     For  $j \neq k$ , compute polar decompositions  $W_k^* A_{kj} = P_j W_j^*$  and  $\widetilde{W}_k^* A_{kj} = \widetilde{P}_j \widetilde{W}_j^*$     Put  $D = \text{diag}(W_1, \dots, W_n)$  and  $\widetilde{D} = \text{diag}(\widetilde{W}_1, \dots, \widetilde{W}_n)$     Put  $G = \min(D^* A D, \widetilde{D}^* A \widetilde{D})$ , lexicographically**else**    For each  $(i, j)$ , find  $\alpha_{ij} > 0$  such that  $H_{ij} := \alpha_{ij} A_{ij} \in \text{O}(2)$     Put  $H = (H_{ij})_{i,j \in [n]}$  and  $D = \text{diag}(H_{11}, \dots, H_{1n})$     **if** there exists  $(k, l)$  such that  $\det(D H D^*)_{kl} = -1$  **then**        Let  $(k, l)$  be the first such indices, lexicographically        Put  $Q = ((D H D^*)_{kl} R)^{-1/2}$ 

// either square root may be selected

        Put  $E = \text{diag}(Q H_{11}, \dots, Q H_{1n})$         Put  $G = \min(E A E^*, S E A E^* S)$ , lexicographically    **else**        Put  $G = \min(D A D^*, S D A D^* S)$ , lexicographically    **end****end**

**Proof.** The first claim follows from the fact that  $\begin{bmatrix} c & -s \\ s & c \end{bmatrix}^{-1} = \begin{bmatrix} c & s \\ -s & c \end{bmatrix}$  when  $c^2 + s^2 = 1$ . For the second claim, if  $\det B = 1$ , then since  $\text{SO}(2)$  is abelian, we have  $AB = BA$ . If  $\det B = -1$ , then put  $R = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$  and  $C = BR$ . Then  $C \in \text{SO}(2)$ , and so the first claim gives

$$AB = ABRR = ACR = CAR = CRRAR = CRA^{-1} = BA^{-1}. \quad \square$$

**Theorem 7.** The function implemented by Algorithm 1 is a complete invariant for nowhere orthogonal tuples in  $(\text{Gr}(2, \mathbf{R}^d))^n$  modulo  $\text{O}(d)$ .

We note that the Algorithm 1 takes as input (and gives as output) a Gramian of  $n$  orthonormal bases of nowhere orthogonal planes in  $\mathbf{R}^d$ . That is, given an element  $(\text{Gr}(2, \mathbf{R}^d))^n$ , one fixes an orthonormal basis (i.e., columns of a  $d \times 2$  matrix  $A_i$ ) for each of the points in  $\text{Gr}(2, \mathbf{R}^d)$  and then computes the Gramian of the  $2n$  vectors (i.e., columns of  $d \times 2n$  matrix  $(A_1, A_2, \dots, A_n)$ ). The Gramian output by the algorithm can then be factored using spectral methods to yield a  $d \times 2n$  matrix  $(B_1, B_2, \dots, B_n)$  with columns orthonormal bases of points in  $\text{Gr}(2, \mathbf{R}^d)$ . Thus, this theorem also means that the algorithm returns the same output regardless of choice of orthonormal bases for elements of  $(\text{Gr}(2, \mathbf{R}^d))^n$ .

**Proof.** First, if two different inputs  $A_1$  and  $A_2$  produce the same output  $G$ , then by the construction of  $G$  in both cases, there must exist block diagonal unitary matrices  $U_1$  and  $U_2$  such that  $G = U_1 A_1 U_1^* = U_2 A_2 U_2^*$ . It then follows that  $A_2 = (U_2^* U_1) A_1 (U_2^* U_1)^*$ ,

that is,  $A_1$  and  $A_2$  are equivalent. It remains to show that equivalent inputs produce identical outputs.

Take any tuple  $(U_i)_{i \in [n]}$  in  $O(2)$  and put  $U = \text{diag}(U_1, \dots, U_n)$ . We will first show that  $UAU^*$  produces the same output as  $A$ . Throughout, we use  $\sharp$  to denote the version of calculations that come from  $UAU^*$ , e.g.,  $A^\sharp = UAU^*$ . First,  $A_{kl}$  has the same singular values as  $A_{kl}^\sharp = U_k A_{kl} U_l^*$ , and so  $(k, l)^\sharp$  exists if and only if  $(k, l)$  exists for the first condition in Algorithm 1. Suppose  $(k, l)^\sharp = (k, l)$  does exist. Next, there are four choices of left singular vectors of  $U_k A_{kl} U_l^*$ , namely,  $W_k^\sharp \in \{\pm U_k W_k, \pm U_k W_k R\}$ . As such, there exists  $\epsilon \in \{\pm 1\}$  and  $t \in \{0, 1\}$  such that

$$W_k^\sharp = \epsilon U_k W_k R^t, \quad \widetilde{W}_k^\sharp = \epsilon U_k W_k R^{t+1}.$$

Since each  $A_{kj}$  is invertible, the polar decompositions are unique, and we have

$$(W_k^* A_{kj})^\sharp = \epsilon R^t W_k^* U_k^* U_k A_{kj} U_j^* = \epsilon R^t W_k^* A_{kj} U_j^* = \begin{cases} \epsilon P_j W_j^* U_j^* & \text{if } t = 0 \\ \epsilon \widetilde{P}_j \widetilde{W}_j^* U_j^* & \text{if } t = 1. \end{cases}$$

Either way, the polar decomposition gives  $W_j^\sharp = \epsilon U_j W_j R^t$ . Similarly,  $\widetilde{W}_j^\sharp = \epsilon U_j W_j R^{t+1}$ . With this we see that

$$(D^* AD)_{ij}^\sharp = (W_i^* A_{ij} W_j)^\sharp = R^t W_i^* U_i^* U_i A_{ij} U_j^* U_j W_j R^t = (W_i R^t)^* A_{ij} (W_j R^t),$$

and similarly  $(\widetilde{D}^* A \widetilde{D})_{ij}^\sharp = (W_i R^{t+1})^* A_{ij} (W_j R^{t+1})$ . It follows that  $\{(D^* AD)^\sharp, (\widetilde{D}^* A \widetilde{D})^\sharp\} = \{D^* AD, \widetilde{D}^* A \widetilde{D}\}$ , and so  $G^\sharp = G$ .

Next, we suppose that no such  $(k, l)$  exists. Since  $A_{ij}^\sharp = U_i A_{ij} U_j^*$  with  $U_i, U_j \in O(2)$ , then  $\alpha_{ij}^\sharp = \alpha_{ij}$  and so  $H_{ij}^\sharp = U_i H_{ij} U_j^*$ . Next,

$$(DHD^*)_{kl}^\sharp = (H_{1k} H_{kl} H_{1l}^*)^\sharp = U_1 H_{1k} U_k^* U_k H_{kl} U_l^* U_l H_{1l}^* U_1^* = U_1 (DHD^*)_{kl} U_1^*,$$

and so  $\det(DHD^*)_{kl}^\sharp = \det(DHD^*)_{kl}$ . For the remainder of the proof, put  $T = DHD^*$  and define  $t$  to be 1 if  $\det U_1 = -1$ , and otherwise 0.

Suppose there exists  $(k, l)^\sharp = (k, l)$  such that  $\det T_{kl} = -1$ . Then  $Q^\sharp = \pm (U_1 T_{kl} U_1^*)^{-1/2}$ , and since  $Q^\sharp \in SO(2)$ , Lemma 6 gives

$$(EAE^*)_{ij}^\sharp = \alpha_{ij}^{-1} (QT_{ij} Q^*)^\sharp = \alpha_{ij}^{-1} Q^\sharp U_1 T_{ij} U_1^* (Q^\sharp)^* = \alpha_{ij}^{-1} U_1 T_{ij} U_1^* (Q^\sharp)^{\det T_{ij}} (Q^\sharp)^*.$$

If  $\det T_{ij} = 1$ , then this reduces to

$$(EAE^*)_{ij}^\sharp = \alpha_{ij}^{-1} U_1 T_{ij} U_1^* (Q^\sharp)^{\det T_{ij}} (Q^\sharp)^* = \alpha_{ij}^{-1} U_1 T_{ij} U_1^* = \alpha_{ij}^{-1} T_{ij}^{\det U_1} = \alpha_{ij}^{-1} R^t T_{ij} R^t.$$

Otherwise,  $\det T_{ij} = -1$ , and so

$$(EAE^*)_{ij}^\sharp = \alpha_{ij}^{-1} U_1 T_{ij} U_1^* (Q^\sharp)^{-2} = \alpha_{ij}^{-1} U_1 T_{ij} U_1^* U_1 T_{kl} U_1^* R = \alpha_{ij}^{-1} U_1 T_{ij} T_{kl} U_1^* R.$$

Since  $\det(T_{ij}T_{kl}) = 1$ , Lemma 6 then gives

$$(EAE^*)_{ij}^\sharp = \alpha_{ij}^{-1} U_1 T_{ij} T_{kl} U_1^* R = \alpha_{ij}^{-1} (T_{ij} T_{kl})^{\det U_1} R = \alpha_{ij}^{-1} R^t T_{ij} T_{kl} R^{t+1}.$$

Similarly,

$$(EAE^*)_{ij} = \begin{cases} \alpha_{ij}^{-1} T_{ij} & \text{if } \det T_{ij} = 1 \\ \alpha_{ij}^{-1} T_{ij} T_{kl} R & \text{if } \det T_{ij} = -1, \end{cases}$$

meaning  $\{(EAE^*)^\sharp, S(EAE^*)^\sharp S\} = \{EAE^*, SEAE^* S\}$ , and so  $G^\sharp = G$ .

In the final case, we have  $\det(DHD^*)_{ij}^\sharp = \det(DHD^*)_{ij} = 1$  for every  $i, j \in [n]$ . Here, Lemma 6 gives

$$T_{ij}^\sharp = U_1 T_{ij} U_1^* = T_{ij}^{\det U_1} = R^t T_{ij} R^t,$$

meaning  $\{T^\sharp, ST^\sharp S\} = \{T, STS\}$ , and so  $G^\sharp = G$ .  $\square$

A Matlab implementation of Algorithm 1 may be downloaded from [56].

We note that another (uglier) algorithm produces a normalized Gramian for generic rank- $r$  subspaces, but the algorithm we found does not produce a Gramian if any two of the subspaces are isoclinic (for example). Due to this failure, we decided to not report the details of this algorithm.

### 3.3. $H^*$ -algebras and generalized Bargmann invariants

In pursuit of a complete invariant for  $(\text{Gr}(r, \mathbf{F}^d))^n$  modulo  $U(d, \mathbf{F}, \sigma)$ , we consider traces of products of matrices, generalizing Bargmann invariants and building on the approaches in [78, 89, 68, 55, 39, 76]. There are large upper bounds on the number of traces of products that must be computed to generate a complete invariant on a single (1-tuple)  $d \times d$  matrix, like  $4^{d^2}$  [68], and we prove in Lemma 8 that there is a lower bound on Bargmann invariants that must be computed in general to provide a complete invariant for tuples of lines. Thus, our goal of this section is to give (two different) algorithms to compute injective invariants that generalize Bargmann invariants and require a reasonable number of computations. Neither requires genericity of the subspaces.

First, we clarify how we must use these invariants with the help of a lemma:

**Lemma 8.** *Consider any function  $f: (\text{Gr}(1, \mathbf{F}^d))^d \rightarrow \mathbf{F}^m$  such that each coordinate function of  $f$  is a fixed Bargmann invariant. Then  $f$  is a complete invariant of  $(\text{Gr}(1, \mathbf{F}^d))^d$  modulo  $U(d, \mathbf{F}, \sigma)$  only if  $m \geq (d-1)!/2$ .*

**Proof.** Select  $\epsilon \in \{\pm\}$  and consider the lines  $\mathcal{L}_\epsilon$  spanned by the vectors

$$e_1 + e_2, \quad \dots, \quad e_{d-1} + e_d, \quad e_d + \epsilon e_1.$$

For both choices of  $\epsilon$ , the frame graph  $G(\mathcal{L}_\epsilon)$  is the cycle graph  $C_d$  of length  $d$ , and so the maximal spanning forest  $F$  is a path graph. The 2-products of  $\mathcal{L}_+$  equal those of  $\mathcal{L}_-$ , but the  $d$ -product corresponding to the lone cycle  $C_d \in C(F)$  has the same sign as  $\epsilon$ . As such,  $\mathcal{L}_+$  is not isomorphic to  $\mathcal{L}_-$  modulo  $U(d, \mathbf{F}, \sigma)$  by Proposition 4. The Bargmann invariants that do not vanish on  $\mathcal{L}_\epsilon$  are the ones that correspond to closed walks along  $C_d$ . Of these, the Bargmann invariants that distinguish  $\mathcal{L}_+$  from  $\mathcal{L}_-$  are closed walks with odd winding number around  $C_d$ . Overall, distinguishing  $\mathcal{L}_+$  from  $\mathcal{L}_-$  requires a Bargmann invariant whose closed walk is supported on all of  $C_d$ .

Now select  $\pi \in S_d$  and  $\epsilon \in \{\pm\}$  and consider the lines  $\pi \cdot \mathcal{L}_\epsilon$  obtained by permuting the tuple  $\mathcal{L}_\epsilon$  according to  $\pi$ . Distinguishing  $\pi \cdot \mathcal{L}_+$  from  $\pi \cdot \mathcal{L}_-$  for every  $\pi \in S_d$  requires Bargmann invariants whose closed walks are supported on each of the length- $d$  cycles in the complete graph  $K_d$ . The result follows from the fact that there are  $(d-1)!/2$  such cycles.  $\square$

Considering  $(d-1)!/2$  is far too large for efficient computation, we instead accept a different type of injective invariant: Given a tuple  $\mathcal{L}$  of  $n$  lines, return a collection  $W$  of walks on  $K_n$  as well as the Bargmann invariant of  $w$  evaluated at  $\mathcal{L}$  for each  $w \in W$ . Note that this is the form provided by Proposition 4, at least if  $F$  were selected canonically; this can be accomplished by iteratively growing  $F$  from edges in lexicographic order.

The remainder of this section considers two different generalizations of the Bargmann invariants, and we use these invariants to distinguish between tuples of subspaces modulo isometric isomorphism. Our results for both generalizations apply ideas from the representation theory of  $H^*$ -algebras. For what follows, we remind the reader that  $\mathbf{F} \in \{\mathbf{R}, \mathbf{C}\}$ .

**Definition 9.** We say  $\mathcal{A}$  is an  $H^*$ -algebra over  $(\mathbf{F}, \sigma)$  if

- (H1)  $(\mathcal{A}, +, \times, \mathbf{F})$  is a finite-dimensional associative algebra with unity,
- (H2)  $*$ :  $\mathcal{A} \rightarrow \mathcal{A}$  is a conjugate-linear involutory antiautomorphism, and
- (H3)  $(\cdot, \cdot)$ :  $\mathcal{A} \times \mathcal{A} \rightarrow \mathbf{F}$  is a Hermitian form on  $\mathcal{A}$  such that

$$(xy, z) = (y, x^*z) = (x, zy^*) \quad \forall x, y, z \in \mathcal{A}.$$

A **representation** of an  $H^*$ -algebra  $\mathcal{A}$  is a  $*$ -algebra homomorphism  $f: \mathcal{A} \rightarrow \mathbf{F}^{k \times k}$ . The corresponding **character**  $\chi_f: \mathcal{A} \rightarrow \mathbf{F}$  is given by  $\chi_f(x) = \text{tr } f(x)$ . Two representations  $f, g: \mathcal{A} \rightarrow \mathbf{F}^{k \times k}$  are **equivalent** if there exists  $U \in U(k, \mathbf{F})$  such that  $g(x) = Uf(x)U^*$ .

One example of an  $H^*$ -algebra over  $\mathbf{F}$  is  $\mathbf{F}^{k \times k}$ , with conjugate-linear involutory antiautomorphism  $*$  the adjoint and Hermitian form  $(\cdot, \cdot)$  the Hilbert–Schmidt inner product. The quaternions form an  $H^*$ -algebra over the reals (see, e.g., [5]), where  $q^* = \bar{q}$  and  $(q_1, q_2) = \text{Re } q_1 \bar{q}_2$ .  $H^*$ -algebras have also more recently arisen in infinite-dimensional quantum mechanics [1].

One might ask why the Hermitian form is not mentioned in the definition of a representation of an  $H^*$ -algebra, considering it is an important part of the structure.

Homomorphisms of Hilbert spaces are continuous linear operators, which also do not explicitly involve the Hermitian form, just the topology induced from it. Since we are dealing with finite-dimensional objects, this reduces to any linear map, e.g., an algebra homomorphism.

**Proposition 10** (Theorem 3 in [39]). *Two representations of an  $H^*$ -algebra are equivalent if and only if their characters are equal.*

Given  $S \subseteq \mathbf{F}^{k \times k}$ , let  $\mathcal{A}(S)$  denote the smallest algebra with unity containing  $S$ .

**Lemma 11.** *Consider tuples  $(A_i)_{i \in [n]}$  and  $(B_i)_{i \in [n]}$  over  $\mathbf{F}^{k \times k}$  for which there exists  $\pi \in S_n$  such that  $A_i^* = A_{\pi(i)}$  and  $B_i^* = B_{\pi(i)}$  for every  $i \in [n]$ . Select words  $(w_j(x_1, \dots, x_n))_{j \in [m]}$  in noncommuting variables  $x_i$  such that the evaluation  $(E_j := w_j(A_1, \dots, A_n))_{j \in [m]}$  is a basis for  $\mathcal{A}((A_i)_{i \in [n]})$ . (Here, evaluating the word of length zero produces the identity matrix.) There exists  $U \in \mathbf{U}(k, \mathbf{F}, \sigma)$  such that  $UA_iU^* = B_i$  for every  $i \in [n]$  if and only if*

- (i) *the evaluation  $(F_j := w_j(B_1, \dots, B_n))_{j \in [m]}$  is a basis for  $\mathcal{A}((B_i)_{i \in [n]})$ ,*
- (ii)  *$\text{tr}(E_i^* E_j) = \text{tr}(F_i^* F_j)$  for every  $i, j \in [m]$ ,*
- (iii)  *$\text{tr}(E_i^* E_j E_k) = \text{tr}(F_i^* F_j F_k)$  for every  $i, j, k \in [m]$ , and*
- (iv)  *$\text{tr}(E_i^* A_j) = \text{tr}(F_i^* B_j)$  for every  $i \in [m]$ ,  $j \in [n]$ .*

**Proof.** ( $\Rightarrow$ ) Suppose there exists  $U \in \mathbf{U}(k, \mathbf{F}, \sigma)$  such that  $UA_iU^* = B_i$  for every  $i \in [n]$ . Then  $UE_iU^* = F_i$  for every  $i \in [m]$ , and (i)–(iv) follow immediately.

( $\Leftarrow$ ) First, the assumed existence of  $\pi \in S_n$  implies that  $\mathcal{A}((A_i)_{i \in [n]})$  and  $\mathcal{A}((B_i)_{i \in [n]})$  are  $H^*$ -algebras. Indeed, both algebras inherit (H3) from  $\mathbf{F}^{k \times k}$  by taking  $(x, y) = \text{tr}(x^*y)$ . By (i), there is a unique linear  $f: \mathcal{A}((A_i)_{i \in [n]}) \rightarrow \mathcal{A}((B_i)_{i \in [n]})$  that maps  $E_i \mapsto F_i$  for every  $i \in [m]$ . Next, (ii) and the non-degeneracy of  $(A, B) \mapsto \text{tr}(A^*B)$  implies that for every  $x \in \mathcal{A}((A_i)_{i \in [n]})$ , it holds that  $f(x)$  is the unique  $y \in \mathcal{A}((B_i)_{i \in [n]})$  such that  $\text{tr}(E_i^*x) = \text{tr}(F_i^*y)$  for every  $i \in [m]$ . This combined with (iii) and (iv) then imply that  $f$  maps  $E_j E_k \mapsto F_j F_k$  for every  $j, k \in [m]$  and  $A_j \mapsto B_j$  for every  $j \in [n]$ . The former implies that  $f$  is an algebra isomorphism, since decomposing  $x = \sum_i a_i E_i$  and  $y = \sum_j b_j E_j$  gives  $xy = \sum_{i,j} a_i b_j E_i E_j$ , which  $f$  then maps to  $\sum_{i,j} a_i b_j F_i F_j = f(x)f(y)$ . Since  $f: A_i \mapsto B_i$  for every  $i \in [n]$ , the assumed existence of  $\pi \in S_n$  implies that  $f$  is a  $*$ -algebra isomorphism. Indeed, letting  $Rw$  denote the reversal of the word  $w$ , then since  $f$  is an algebra isomorphism,  $f$  maps

$$(w(A_1, \dots, A_n))^* = (Rw)(A_1^*, \dots, A_n^*) = (Rw)(A_{\pi(1)}, \dots, A_{\pi(n)})$$

to  $(Rw)(B_{\pi(1)}, \dots, B_{\pi(n)}) = (w(B_1, \dots, B_n))^*$ , and so  $f(x^*) = f(x)^*$  by linearity. At this point, we consider two representations of  $\mathcal{A}((A_i)_{i \in [n]})$ , namely, the identity map and  $f$ . Since the identity matrix resides in both  $\mathcal{A}((A_i)_{i \in [n]})$  and  $\mathcal{A}((B_i)_{i \in [n]})$  by definition,

---

**Algorithm 2:** Canonical basis for matrix algebra from finite generating set.
 

---

**Data:** Matrices  $(A_i)_{i \in [n]}$  in  $\mathbf{F}^{k \times k}$

**Result:** Words  $(w_j)_{j \in [m]}$  such that  $(w_j(A_1, \dots, A_n))_{j \in [m]}$  is a basis for  $\mathcal{A}((A_i)_{i \in [n]})$

Put  $w_1 = 1$  (the word of length zero)

Initialize  $m_{\text{old}} = 0$  and  $m_{\text{new}} = 1$

```

while  $m_{\text{new}} > m_{\text{old}}$  do
  Update  $m_{\text{old}} = m_{\text{new}}$ 
  for  $i \in [n]$  and  $j \in [m_{\text{old}}]$  do
    if  $A_i w_j(A_1, \dots, A_n)$  is linearly independent of  $(w_l(A_1, \dots, A_n))_{l \in [m_{\text{new}}]}$  then
      Put  $w_{m_{\text{new}}+1} = x_i w_j$  and update  $m_{\text{new}} = m_{\text{new}} + 1$ 
    end
  end
end
end

```

---

(ii) together with linearity gives that the characters of these representations are equal, and so Proposition 10 implies the existence of  $U \in \text{U}(k, \mathbf{F}, \sigma)$  such that  $f(x) = UxU^*$ . Since  $f: A_i \mapsto B_i$  for every  $i \in [n]$ , we are done.  $\square$

In [39], Proposition 10 is used to prove (Theorem 4 in [39]) that calculating the traces of the evaluations of every possible word on the generating matrices of length between one and  $4k^2$  (i.e., on the order of  $n^{4k^2}$ ) is a complete invariant. Our goal in what follows is to prune the list of necessary words to evaluate.

Overall, to determine a tuple of matrices in  $\mathbf{F}^{k \times k}$  up to unitary equivalence, it suffices to specify a collection of words  $(w_i)_{i \in [m]}$  that can be used to span the corresponding  $H^*$ -algebra, and then report traces of the form (ii)–(iv). In the following, we show that a certain (obvious) choice of words, i.e., the result of Algorithm 2, is invariant to conjugation by unitary matrices and computable in polynomial time.

**Lemma 12.** *Given  $(A_i)_{i \in [n]}$  in  $\mathbf{F}^{k \times k}$ , Algorithm 2 returns words  $(w_j)_{j \in [m]}$  such that the evaluation  $(w_j(A_1, \dots, A_n))_{j \in [m]}$  is a basis for  $\mathcal{A}((A_i)_{i \in [n]})$ . Given  $(UA_iU^*)_{i \in [n]}$  for some  $U \in \text{U}(k, \mathbf{F}, \sigma)$ , Algorithm 2 returns the same words  $(w_j)_{j \in [m]}$ . Algorithm 2 terminates after at most  $m \leq k^2$  iterations of the while loop, and each iteration can be implemented in a way that costs  $O(mnk^4)$  operations.*

**Proof.** First, consider the set of evaluations of all words at  $(A_i)_{i \in [n]}$ . This set spans  $\mathcal{A}((A_i)_{i \in [n]})$ , which is a subspace of  $\mathbf{F}^{k \times k}$ , and therefore has finite dimension. It follows that there exists a basis among these evaluations. Let  $L$  denote the smallest possible length of the longest word in a basis.

For the moment, let us remove the constraint  $m_{\text{new}} > m_{\text{old}}$  of the while loop. We claim that after the  $l$ th iteration of the unconstrained while loop,  $\text{span}(w_j(A_1, \dots, A_n))_{j \in [m_{\text{new}}]}$  contains all evaluations of words of length  $l$ . By our initialization  $w_1 = 1$ , this holds for  $l = 0$ . Assume it holds for  $l \geq 0$ . Then every word of length  $l + 1$  has the form  $x_i w$ , where  $w$  is a word of length  $l$ . Evaluating then produces  $A_i w(A_1, \dots, A_n)$ . By the induction hypothesis,  $w(A_1, \dots, A_n)$  can be expressed as a linear combination of  $(w_j(A_1, \dots, A_n))_{j \in [m_{\text{old}}]}$ . Since we test all of  $(A_i w_j(A_1, \dots, A_n))_{j \in [m_{\text{old}}]}$  for linear indepen-

dence in order to select  $(w_j)_{j \in [m_{\text{new}}]}$ , it follows that  $\text{span}(w_j(A_1, \dots, A_n))_{j \in [m_{\text{new}}]}$  contains  $A_i w(A_1, \dots, A_n)$ .

Now suppose that the  $l$ th iteration of the unconstrained while loop resulted in  $m_{\text{new}} = m_{\text{old}}$ . Then no new words were added to  $\{w_j\}$  in the  $l$ th iteration. In fact, for every  $i \in [n]$  and  $j \in [m_{\text{old}}]$ , it holds that  $A_i w_j(A_1, \dots, A_n)$  resides in  $\text{span}(w_l(A_1, \dots, A_n))_{l \in [m_{\text{old}}]}$ , and so no new words will also be added in any future iteration. Considering  $(w_l(A_1, \dots, A_n))_{l \in [m_{\text{new}}]}$  forms a basis for  $\mathcal{A}((A_i)_{i \in [n]})$  by the end of the  $L$ th iteration, it follows that the original while loop with constraint  $m_{\text{new}} > m_{\text{old}}$  terminates with a basis after  $L + 1$  iterations.

Now suppose we were instead given  $(UA_i U^*)_{i \in [n]}$  for some  $U \in \text{U}(k, \mathbf{F}, \sigma)$ . Since the map  $x \mapsto UxU^*$  is a linear isometry over  $\mathbf{F}^{k \times k}$ , it follows that  $UA_i U^* w_j(UA_1 U^*, \dots, UA_n U^*) = UA_i w_j(A_1, \dots, A_n) U^*$  is linearly independent of

$$(w_l(UA_1 U^*, \dots, UA_n U^*))_{l \in [m_{\text{new}}]} = (Uw_l(A_1, \dots, A_n)U^*)_{l \in [m_{\text{new}}]}$$

if and only if  $A_i w_j(A_1, \dots, A_n)$  is linearly independent of  $(w_l(A_1, \dots, A_n))_{l \in [m_{\text{new}}]}$ . As a consequence, Algorithm 2 returns the same words  $(w_j)_{j \in [m]}$ .

For the final claim, recall that the while loop terminates after  $L + 1$  iterations. To estimate this number of iterations, let  $m_l$  denote the dimension of  $\text{span}(w_l(A_1, \dots, A_n))_{l \in [m_{\text{new}}]}$  after the  $l$ th iteration of the while loop, i.e.,  $m_l = m_{\text{new}}$ . Then

$$1 = m_0 < m_1 < \dots < m_L = m_{L+1} = m.$$

It follows that  $L < m$ , and so the while loop terminates after at most  $m \leq k^2$  iterations, as claimed. One may implement each iteration of the while loop by first multiplying every matrix  $A_i$  by every matrix  $w_j(A_1, \dots, A_n)$ , costing  $nm_{\text{old}} \cdot O(k^3) = O(nk^5)$  operations, then vectorizing the matrices  $(w_l(A_1, \dots, A_n))_{l \in [m_{\text{new}}]}$  and the  $nm_{\text{old}}$  matrix products to form the columns of a  $k^2 \times (m_{\text{old}} + nm_{\text{old}})$  matrix, computing the row echelon form of this matrix in  $O(k^4(m_{\text{old}} + nm_{\text{old}})) = O(mnk^4)$  operations, and then finally using the pivot columns of the result to decide which words to add to  $\{w_j\}$ .  $\square$

Matlab implementations of Algorithm 2 and Lemma 11 may be downloaded from [56].

While the per-iteration cost of Algorithm 2 scales poorly with  $k$ , we will find that this cost can sometimes be improved dramatically. At the moment, the main takeaway should be that Algorithm 2 always returns the desired basis in polynomial time.

### 3.3.1. Projection algebras

Taking inspiration from [39], and in light of Lemma 11, there is a natural choice of invariant to determine tuples of subspaces up to isometric isomorphism.

**Theorem 13.** *There exists a complete invariant for  $(\text{Gr}(r, \mathbf{F}^d))^n$  modulo  $\text{U}(d, \mathbf{F}, \sigma)$  that, given a tuple of orthogonal projection matrices, can be computed in  $O(nd^8 + r^2 d^9)$  operations.*



**Proof.** Let  $A_i$  denote the orthogonal projection onto the  $i$ th subspace, run Algorithm 2 to determine words  $(w_j)_{j \in [m]}$  that produce a basis  $(E_j)_{j \in [m]}$  for the algebra  $\mathcal{A}((A_i)_{i \in [n]})$ , and then compute the traces prescribed in Lemma 11(ii)–(iv). By Lemmas 11 and 12, the words  $(w_j)_{j \in [m]}$  together with the traces (ii)–(iv) form a complete invariant for  $(\text{Gr}(r, \mathbf{F}^d))^n$  modulo  $\text{U}(d, \mathbf{F}, \sigma)$ . Since Algorithm 2 ensures that  $E_1 = I$ , then the traces in (ii) are already captured by the traces in (iii).

To compute these traces, it is helpful to perform some preprocessing. For each projection  $A_i$ , we find a decomposition of the form  $A_i = T_i T_i^*$  with  $T_i \in \mathbf{F}^{d \times r}$  in  $O(rd^2)$  operations. (It suffices to draw Gaussian vectors  $(g_j)_{j \in [r]}$  in  $O(rd)$  operations, then compute  $(A_i g_j)_{j \in [r]}$  in  $O(rd^2)$  operations, then perform Gram–Schmidt in  $O(dr^2)$  operations.) Every trace that we need to compute can be expressed as the trace of a product of  $A_i$ ’s. We will apply the cyclic property of the trace and compute matrix–vector products whenever possible. For example, the trace of  $A_1 A_2$  is given by

$$\text{tr}(A_1 A_2) = \text{tr}(T_1 T_1^* T_2 T_2^*) = \text{tr}(T_1^* T_2 T_2^* T_1) = \sum_{j \in [r]} e_j^* T_1^* T_2 T_2^* T_1 e_j,$$

where  $(e_j)_{j \in [r]}$  denotes the identity basis in  $\mathbf{F}^r$ . We compute the right-hand side by first computing  $T_1 e_j$  in  $O(rd)$  operations, then  $T_2^*(T_1 e_j)$  in  $O(rd)$  operations, etc. In our case, each word has length at most  $m$ , and so each term of the above sum can be computed in  $O(rdm)$  operations.

Overall, we compute the words in  $O(m^2 n d^4)$  operations (by Lemma 12), then we compute  $(T_i)_{i \in [n]}$  in  $O(n r d^2)$  operations, and then each of the  $m^3$  traces in (iii) and each of the  $mn$  traces in (iv) costs  $O(r^2 d m)$  operations. In total, this invariant costs  $O(m^2 n d^4 + n r d^2 + m^4 r^2 d + m^2 n r^2 d)$  operations. Since  $m \leq d^2$ , this operation count is  $O(n d^8 + r^2 d^9)$ .  $\square$

While this invariant can be computed in polynomial time, the runtime is sensitive to the ambient dimension  $d$ .

### 3.3.2. Quivers and cross Gramian algebras

Consider any sequence  $(A_i)_{i \in [n]}$ , where each  $A_i$  is an isometric embedding of some  $r$ -dimensional vector space  $V_i$  over  $\mathbf{F}$  into  $\mathbf{F}^d$ . That is,  $A_i: V_i \hookrightarrow \mathbf{F}^d$  and  $(\text{im } A_i)_{i \in [n]} \in (\text{Gr}(r, \mathbf{F}^d))^n$ . For every  $(i, j) \in [n]^2$ , we then have a mapping  $A_i^* A_j: V_j \rightarrow V_i$ . Together,  $((V_i)_{i \in [n]}, (A_i^* A_j)_{i, j \in [n]})$  forms a representation of a so-called *quiver*  $Q = (Q_0, Q_1, s, t)$  defined by  $Q_0 = [n]$ ,  $Q_1 = [n]^2$ ,  $s: (i, j) \mapsto j$ , and  $t: (i, j) \mapsto i$ . The corresponding quiver algebra  $\mathbf{F}Q$  enjoys a representation over  $V := \bigoplus_{i \in [n]} V_i$  with maps

$$f_{ij}: V \xrightarrow{\pi_j} V_j \xrightarrow{A_i^* A_j} V_i \xleftarrow{\pi_i^*} V,$$

where  $\pi_i$  denotes the coordinate projection from  $V$  to  $V_i$ . As we will see, these endomorphisms over  $V$  generate an  $H^*$ -algebra that provides more efficient invariants.

**Theorem 14.** *There exists a complete invariant for  $(\text{Gr}(r, \mathbf{F}^d))^n$  modulo  $\text{U}(d, \mathbf{F}, \sigma)$  that, given a Gramian of orthobases of subspaces, can be computed in  $O(r^8 n^5 + r^9 n^3)$  operations.*

**Proof.** Denote the subspaces by  $(\text{im } A_i)_{i \in [n]}$ , where each  $A_i \in \mathbf{F}^{d \times r}$  has orthonormal columns, and put  $A = [A_1 \cdots A_n]$ . By assumption, we are given the Gramian  $A^* A$ . Letting  $\Pi_i$  denote the  $rn \times rn$  orthogonal projection matrix onto the  $i$ th block of  $r$  coordinates in  $\mathbf{F}^{rn}$ , then the matrix representation of  $f_{ij}$  is  $A_{ij} := \Pi_i A^* A \Pi_j$ .

Given  $(A_{ij})_{i,j \in [n]}$  and  $(B_{ij})_{i,j \in [n]}$  of this form, suppose there exists  $U \in \text{U}(rn, \mathbf{F}, \sigma)$  such that  $U A_{ij} U^* = B_{ij}$  for every  $i, j \in [n]$ . Then since  $A_{ii} = B_{ii} = \Pi_i$ , it holds that  $U$  is necessarily block diagonal. Furthermore,

$$U A^* A U^* = U \left( \sum_{ij} \Pi_i A^* A \Pi_j \right) U^* = \sum_{ij} U A_{ij} U^* = \sum_{ij} B_{ij} = B^* B.$$

As such, unitary equivalence between  $(A_{ij})_{i,j \in [n]}$  and  $(B_{ij})_{i,j \in [n]}$  implies block unitary equivalence between the orthobasis Gramians  $A^* A$  and  $B^* B$ . The implication also goes in the other direction: Given a block diagonal  $U \in \text{U}(rn, \mathbf{F}, \sigma)$  such that  $U A^* A U^* = B^* B$ , then

$$U A_{ij} U^* = U \Pi_i A^* A \Pi_j U^* = \Pi_i U A^* A U^* \Pi_j = \Pi_i B^* B \Pi_j = B_{ij}.$$

It remains to test whether there exists  $U \in \text{U}(rn, \mathbf{F}, \sigma)$  such that  $U A_{ij} U^* = B_{ij}$  for every  $i, j \in [n]$ , which leads us to consider Lemma 11.

Note that  $A_{ij}^* = A_{ji}$  and similarly for  $B$ , and so  $(A_{ij})_{i,j \in [n]}$  and  $(B_{ij})_{i,j \in [n]}$  satisfy the hypothesis of Lemma 11 with  $\pi(i, j) = (j, i)$ . Since  $\sum_i A_{ii} = I$ , we may run a version of Algorithm 2 that instead initializes with all words  $x_{ij}$  of length 1 whose evaluations  $A_{ij}$  are nonzero; these evaluations are linearly independent since they have disjoint support. Since all words of positive length evaluate as a matrix in  $\mathbf{F}^{rn \times rn}$  that is supported on some  $r \times r$  block, it follows that the resulting basis can be indexed as  $(E_{ijk})_{i,j \in [n], k \in [m_{ij}]}$ , where  $E_{ijk}$  is the  $k$ th basis element that is supported in the  $(i, j)$ th  $r \times r$  block. For example, it holds that  $E_{ij1} = A_{ij}$  whenever  $A_{ij} \neq 0$ .

To see how efficient this choice of invariants is, we first describe how to reduce the per-iteration cost of Algorithm 2 to  $O(r^6 n^3)$ . First, we take all products between  $A_{ij}$ 's and evaluations of existing words. For each word, there are at most  $n$  different  $A_{ij}$ 's that will produce a nonzero product, and so the total number of products is at most  $r^2 n^3$ , each costing  $O(r^3)$  operations. Next, the evaluations of existing words and the resulting products can be partitioned according to their support before testing linear independence. For each  $i, j \in [n]$ , the total number of these matrices that are supported on the  $(i, j)$ th  $r \times r$  block is at most  $r^2 + nr^2$  (at most  $r^2$  from the existing words, and at most  $nr^2$  from the resulting products), and it costs  $O(r^6 n)$  operations to compute the corresponding row echelon form. We perform this for each of the  $n^2$  blocks to identify new words to add. All together, the per-iteration cost is  $O(r^2 n^3 \cdot r^3 + n^2 \cdot r^6 n) = O(r^6 n^3)$ . Our

bound on the total number of iterations is  $r^2 n^2$ , meaning we obtain the desired words after  $O(r^8 n^5)$  operations.

Next, we point out the complexity of computing the traces (ii)–(iv). First, since  $E_{ii1}E_{ijk} = E_{ijk}$ , the traces in (ii) are examples of traces in (iii). Next, for every  $(i, j) \in [n]$ , we either have  $E_{ij1} = A_{ij}$  or  $x_{ij}$  is not one of the words in  $(w_j)_{j \in [m]}$ . As such, the traces in (iv) are captured by both the words and the traces in (iii). Of the traces in (iii), the only ones that are possibly nonzero take the form

$$\text{tr}(E_{jia}^* E_{jkb} E_{kic})$$

for some  $i, j, k \in [n]$ ,  $a \in [m_{ji}]$ ,  $b \in [m_{jk}]$  and  $c \in [m_{ki}]$ . Since  $m_{ij} \leq r^2$  for every  $i, j \in [n]$ , we therefore have at total of at most  $n^3 r^6$  traces to compute, each costing  $O(r^3)$  operations. These  $O(r^9 n^3)$  operations contribute to the total of  $O(r^8 n^5 + r^9 n^3)$  operations it takes to compute this invariant.  $\square$

Interestingly, the cross Gramian algebra introduced in the above proof can be used to obtain a new (short) proof of Proposition 4:

**Proof of Proposition 4.** Consider  $A = [a_1 \cdots a_n]$ , where each  $a_i$  is a unit vector spanning the corresponding line in  $\mathcal{L}$ . Then the cross Gramian algebra is generated by  $A_{ij} = \langle a_i, a_j \rangle e_i e_j^*$ . Observe that every product of these matrices is either 0 or a multiple of  $e_i e_j^*$  for some  $(i, j) \in [n]^2$ . Furthermore,  $e_i e_j^*$  resides in the algebra precisely when  $i$  and  $j$  belong to a common component of the frame graph  $G(\mathcal{L})$ .

Given a maximal spanning forest  $F$  of the frame graph  $G(\mathcal{L})$ , we select the following words in noncommuting variables  $(x_{ij})_{i,j \in [n]}$ : For each  $(i, j) \in [n]^2$  such that  $i$  and  $j$  belong to a common component of  $G(\mathcal{L})$ , select the unique directed path in  $F$  from  $j$  to  $i$  with vertices denoted by  $j = i_0 \rightarrow i_1 \rightarrow \cdots \rightarrow i_l = i$ , and then put

$$w_{ij} := x_{i_l, i_{l-1}} x_{i_{l-1}, i_{l-2}} \cdots x_{i_2, i_1} x_{i_1, i_0}.$$

In particular,  $w_{ii} = x_{ii}$  for every  $i \in [n]$ . Then the evaluation of  $w_{ij}$  is a nonzero multiple of  $e_i e_j^*$ , and all of these evaluations together form a basis for the algebra.

Now consider the traces in Lemma 11(ii)–(iv). Every trace in (ii) and (iii) is either 0 or some product of 2-products. Indeed, the trace is nonzero only if the corresponding directed paths form a closed walk along the edges of  $F$ , in which case each edge of  $F$  is traversed as many times in one direction as it is in the other direction. Meanwhile, a trace in (iv) is nonzero only if the corresponding directed paths form a closed walk comprised of a directed path in  $F$  and a directed edge in  $G(\mathcal{L})$ . If the path has length 1, then the result is a 2-product, and otherwise the result is an  $m$ -product corresponding to a cycle in  $C(F)$ .  $\square$

## 4. Discussion

This paper studied the problem of testing isomorphism between tuples of subspaces with respect to various notions of isomorphism. Several open problems remain:

- Is there a canonical choice of Gramian for equi-isoclinic subspaces of dimension  $r > 2$ ? What about the complex case?
- How many (generalized) Bargmann invariants are required to solve isomorphism up to linear isometry?
- How should one compute the symmetry group of a given tuple of subspaces?

Some of the ideas in the paper may have interesting applications elsewhere. For example, there has been a lot of work to develop symmetric arrangements of points in the Grassmannian [83,17,14,86,82,16,49–51,60,12,57,52,38,28]. What are the projection and cross Gramian algebras of these arrangements? It would also be interesting to see if some of the techniques presented in this paper could be used to treat other emerging problems involving invariants to group actions, e.g. [6,15].

## Declaration of competing interest

There are no competing interests.

## Acknowledgements

The authors thank the anonymous referees who gave valuable feedback and also alerted us to the fact that the orbit problem with  $G = \Gamma = \text{GL}(d, \mathbf{F})$  had been solved. DGM was partially supported by AFOSR FA9550-18-1-0107, NSF DMS 1829955, and the 2019 Kalman Visiting Fellowship at the University of Auckland.

## Data availability

No data was used for the research described in the article.

## References

- [1] S. Abramsky, C. Heunen,  $H^*$ -algebras and nonunital Frobenius algebras: first steps in infinite-dimensional categorical quantum mechanics, mathematical foundations of information flow, Proc. Symp. Appl. Math. 71 (2012) 1–24.
- [2] M. Appleby, I. Bengtsson, I. Dumitru, S. Flammia, Dimension towers of SICs. I. Aligned SICs and embedded tight frames, J. Math. Phys. 58 (2017) 112201.
- [3] M. Appleby, T.-Y. Chien, S. Flammia, S. Waldron, Constructing exact symmetric informationally complete measurements from numerical solutions, J. Phys. A 51 (2018) 165302.
- [4] L. Babai, Graph isomorphism in quasipolynomial time, STOC (2016) 684–697.
- [5] V.K. Balachandran, N. Swaminathan, Real  $H^*$ -algebras, J. Funct. Anal. 65 (1986) 64–75.

- [6] A.S. Bandeira, B. Blum-Smith, J. Kileel, A. Perry, J. Weed, A.S. Wein, Estimation under group actions: recovering orbits from invariants, *Appl. Comput. Harmon. Anal.* 66 (2023) 236–319.
- [7] A.S. Bandeira, M. Fickus, D.G. Mixon, P. Wong, The road to deterministic matrices with the restricted isometry property, *J. Fourier Anal. Appl.* 19 (2013) 1123–1149.
- [8] E. Bannai, E. Bannai, A survey on spherical designs and algebraic combinatorics on spheres, *Eur. J. Comb.* 30 (2009) 1392–1425.
- [9] H. Bennett, K.M.H. Win, Relating code equivalence to other isomorphism problems, *Des. Codes Cryptogr.* 93 (2025) 701–723.
- [10] B.G. Bodmann, J. Haas, Achieving the orthoplex bound and constructing weighted complex projective 2-designs with Singer sets, *Linear Algebra Appl.* 511 (2016) 54–71.
- [11] B. Bodmann, J. Haas, Maximal orthoplectic fusion frames from mutually unbiased bases and block designs, *Proc. Am. Math. Soc.* 146 (2018) 2601–2616.
- [12] B. Bodmann, E.J. King, Optimal arrangements of classical and quantum states with limited purity, *J. Lond. Math. Soc.* 101 (2020) 393–431.
- [13] P.A. Brooksbank, E.M. Luks, Testing isomorphism of modules, *J. Algebra* 320 (2008) 4020–4029.
- [14] H. Broome, S. Waldron, On the construction of highly symmetric tight frames and complex polytopes, *Linear Algebra Appl.* 439 (2013) 4135–4151.
- [15] J. Cahill, A. Contreras, A. Contreras Hip, Complete set of translation invariant measurements with Lipschitz bounds, *Appl. Comput. Harmon. Anal.* 49 (2020) 521–539.
- [16] T.-Y. Chien, S. Waldron, A characterization of projective unitary equivalence of finite frames and applications, *SIAM J. Discrete Math.* 30 (2016) 976–994.
- [17] T.-Y. Chien, S. Waldron, A classification of the harmonic frames up to unitary equivalence, *Appl. Comput. Harmon. Anal.* 30 (2011) 307–318.
- [18] A. Chistov, G. Ivanyos, M. Karpinski, Polynomial time algorithms for modules over finite dimensional algebras, in: *ISSAC*, 1997, pp. 68–74.
- [19] H. Cohn, J. Woo, Three-point bounds for energy minimization, *J. Am. Math. Soc.* 25 (2012) 929–958.
- [20] C.J. Colbourn, D.G. Corneil, On deciding switching equivalence of graphs, *Discrete Appl. Math.* 2 (1980) 181–184.
- [21] J.H. Conway, R.H. Hardin, N.J.A. Sloane, Packing lines, planes, etc.: packings in Grassmannian spaces, *Exp. Math.* 5 (1996) 139–159.
- [22] H.B. Dang, K. Blanchfield, I. Bengtsson, D.M. Appleby, Linear dependencies in Weyl–Heisenberg orbits, *Quantum Inf. Process.* 12 (2013) 3449–3475.
- [23] I.S. Dhillon, R.W. Heath, T. Strohmer, J.A. Tropp, Constructing packings in Grassmannian manifolds via alternating projection, *Exp. Math.* 17 (2008) 9–35.
- [24] B. Et-Taoui, Equiangular lines in  $\mathbb{C}^7$ , *Indag. Math. (N. S.)* 11 (2000) 201–207.
- [25] B. Et-Taoui, Equi-isoclinic planes in Euclidean even dimensional spaces, *Adv. Geom.* 7 (2007) 379–384.
- [26] B. Et-Taoui, Equi-isoclinic planes in Euclidean spaces, *Indag. Math. (N. S.)* 17 (2006) 205–219.
- [27] B. Et-Taoui, Infinite family of equi-isoclinic planes in Euclidean odd dimensional spaces and of complex symmetric conference matrices of odd orders, *Linear Algebra Appl.* 556 (2018) 373–380.
- [28] M. Fickus, J.W. Iverson, J. Jasper, E.J. King, Grassmannian codes from paired difference sets, *Des. Codes Cryptogr.* 89 (2021) 2553–2576.
- [29] M. Fickus, J. Jasper, Equiangular tight frames from group divisible designs, *Des. Codes Cryptogr.* 87 (2019) 1673–1697.
- [30] M. Fickus, J. Jasper, E.J. King, D.G. Mixon, Equiangular tight frames that contain regular simplices, *Linear Algebra Appl.* 555 (2018) 98–138.
- [31] M. Fickus, J. Jasper, D.G. Mixon, Packings in real projective spaces, *SIAM J. Appl. Algebra Geom.* 2 (2018) 377–409.
- [32] M. Fickus, J. Jasper, D.G. Mixon, J.D. Peterson, Hadamard equiangular tight frames, *Appl. Comput. Harmon. Anal.* 50 (2021) 281–302.
- [33] M. Fickus, J. Jasper, D.G. Mixon, J. Peterson, Tremain equiangular tight frames, *J. Comb. Theory, Ser. A* 153 (2018) 54–66.
- [34] M. Fickus, J. Jasper, D.G. Mixon, J. Peterson, C.E. Watson, Polyphase equiangular tight frames and abelian generalized quadrangles, *Appl. Comput. Harmon. Anal.* 47 (2019) 628–661.
- [35] M. Fickus, D.G. Mixon, Tables of the existence of equiangular tight frames, *arXiv:1504.00253*.
- [36] M. Fickus, D.G. Mixon, J. Jasper, Equiangular tight frames from hyperovals, *IEEE Trans. Inf. Theory* 62 (2016) 5225–5236.
- [37] M. Fickus, D.G. Mixon, J.C. Tremain, Steiner equiangular tight frames, *Linear Algebra Appl.* 436 (2012) 1014–1027.

- [38] M. Fickus, C.A. Schmitt, Harmonic equiangular tight frames comprised of regular simplices, *Linear Algebra Appl.* 586 (2020) 130–169.
- [39] P.X. Gallagher, R.J. Proulx, Orthogonal and unitary invariants of families of subspaces, in: *Contributions to Algebra*, Academic Press, 1977, pp. 157–164.
- [40] L.D. Grey, Some bounds for error-correcting codes, *IRE Trans. Inf. Theory* 8 (1962) 200–202.
- [41] G.R.W. Greaves, J.W. Iverson, J. Jasper, D.G. Mixon, Frames over finite fields: equiangular lines in orthogonal geometry, *Linear Algebra Appl.* 639 (2022) 50–80.
- [42] G.R.W. Greaves, J.W. Iverson, J. Jasper, D.G. Mixon, Frames over finite fields: basic theory and equiangular lines in unitary geometry, *Finite Fields Appl.* 77 (2022) 101954.
- [43] J.A. Grochow, Matrix isomorphism of matrix Lie algebras, *CCC* (2012) 203–213.
- [44] J.A. Grochow, Y. Qiao, On  $p$ -group isomorphism: search-to-decision, counting-to-decision, and nilpotency class reductions via tensors, *ACM Trans. Comput. Theory* 16 (2024) 1–39.
- [45] J. Grochow, Y. Qiao, On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness, *SIAM J. Comput.* 52 (2023) 568–617.
- [46] P.R. Halmos, Finite-dimensional Hilbert spaces, *Am. Math. Mon.* 77 (1970) 457–464.
- [47] D. Hughes, S. Waldron, Spherical  $(t, t)$ -designs with a small number of vectors, *Linear Algebra Appl.* 608 (2021) 84–106.
- [48] L. Hughston,  $d = 3$  SIC-POVMs and elliptic curves, Perimeter Institute, October 2007, Seminar Talk, [pirsa.org/07100040](https://pirsa.org/07100040).
- [49] J.W. Iverson, J. Jasper, D.G. Mixon, Optimal line packings from nonabelian groups, *Discrete Comput. Geom.* 63 (2020) 731–763.
- [50] J.W. Iverson, J. Jasper, D.G. Mixon, Optimal line packings from finite group actions, *Forum Math. Sigma* 8 (2020) 1–40.
- [51] J.W. Iverson, D.G. Mixon, Doubly transitive lines I: higman pairs and roux, *J. Comb. Theory, Ser. A* 185 (2022) 105540.
- [52] J.W. Iverson, D.G. Mixon, Doubly transitive lines II: almost simple symmetries, *Algebr. Comb.* 7 (2024) 37–76.
- [53] J. Jasper, E.J. King, D.G. Mixon, Game of sloanes: best known packings in complex projective space, *Proc. SPIE* 11138 (2019) 111381E/1–10.
- [54] J. Jasper, D.G. Mixon, M. Fickus, Kirkman equiangular tight frames and codes, *IEEE Trans. Inf. Theory* 60 (2014) 170–181.
- [55] L.A. Kaluznin, H. Havidi, Geometric theory of the unitary equivalence of matrices, *Dokl. Akad. Nauk SSSR* 7 (1966) 1044–1047.
- [56] E.J. King, Software and code, [https://github.com/gnikylime/test\\_subsp\\_iso](https://github.com/gnikylime/test_subsp_iso).
- [57] E.J. King, 2- and 3-covariant equiangular tight frames, *Proc. Sampl. Theory Appl.* (2019) 1–4.
- [58] E.J. King, Constructing subspace packings from other packings, *Linear Algebra Appl.* 625 (2021) 68–80.
- [59] E.J. King, New constructions and characterizations of flat and almost flat Grassmannian fusion frames, *arXiv:1612.05784*.
- [60] G.S. Kopp, SIC-POVMs and the Stark conjectures, *Int. Math. Res. Not.* 2021 (2021) 13812–13838.
- [61] P.W.H. Lemmens, J.J. Seidel, Equi-isoclinic subspaces of Euclidean spaces, *Indag. Math.* 35 (1973) 98–107.
- [62] V.I. Levenstein, Bounds on the maximal cardinality of a code with bounded modules of the inner product, *Sov. Math. Dokl.* 25 (1982) 526–531.
- [63] E.M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. Syst. Sci.* 25 (1982) 42–65.
- [64] B.D. McKay, A. Piperno, Practical graph isomorphism, II, *J. Symb. Comput.* 60 (2014) 94–112.
- [65] D.G. Mixon, H. Parshall, Globally optimizing small codes in real projective spaces, *SIAM J. Discrete Math.* 35 (2021) 234–249.
- [66] D.G. Mixon, H. Parshall, The optimal packing of eight points in the real projective plane, *Exp. Math.* (2019) 1–12.
- [67] D.G. Mixon, C.J. Quinn, N. Kiyavash, M. Fickus, Fingerprinting with equiangular tight frames, *IEEE Trans. Inf. Theory* 59 (2013) 1855–1865.
- [68] C. Pearcy, A complete set of unitary invariants for operators generating finite  $W^*$ -algebras of type I, *Pac. J. Math.* 12 (1962) 1405–1416.
- [69] E. Petrank, R.M. Roth, Is code equivalence easy to decide?, *IEEE Trans. Inf. Theory* 43 (1997) 1602–1604.
- [70] Y. Qiao, X. Sun, Canonical Forms for Matrix Tuples in Polynomial Time, *FOCS*, 2024, pp. 780–789.

- [71] R.A. Rankin, On the minimal points of positive definite quadratic forms, *Mathematika* 3 (1956) 15–24.
- [72] R.A. Rankin, The Closest Packing of Spherical Caps in  $n$  Dimensions, *Proceedings of the Glasgow Mathematical Association*, vol. 2, Cambridge University Press, 1955, pp. 139–144.
- [73] J.M. Renes, R. Blume-Kohout, A.J. Scott, C.M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys.* 45 (2004) 2171–2180.
- [74] J.J. Seidel, A survey of two-graphs, in: *Proc. Intern. Coll. Theorie Combinatorie*, 1973, pp. 481–511.
- [75] V.V. Sergeichuk, Canonical matrices for linear matrix problems, *Linear Algebra Appl.* 317 (2000) 53–102.
- [76] H. Shapiro, A survey of canonical forms and invariants for unitary similarity, *Linear Algebra Appl.* 147 (1991) 101–167.
- [77] N.J.A. Sloane, Packings in Grassmannian spaces, [neilsloane.com/grass](http://neilsloane.com/grass).
- [78] W. Specht, Zur Theorie der Matrizen. II, *Jahresber. Dtsch. Math.-Ver.* 50 (1940) 19–23.
- [79] N. Strawn, Geometry and Constructions of Finite Frames, Master's Thesis, Department of Mathematics, Texas A&M University, College Station, TX, 2007.
- [80] T. Strohmer, R.W. Heath, Grassmannian frames with applications to coding and communication, *Appl. Comput. Harmon. Anal.* 14 (2003) 257–275.
- [81] I.C. Teodorescu, The module isomorphism problem for finite rings and related results, *ACM Commun. Comput. Algebra* 49 (2015) 14.
- [82] R. Vale, S. Waldron, The construction of  $G$ -invariant finite tight frames, *J. Fourier Anal. Appl.* 22 (2016) 1097–1120.
- [83] R. Vale, S. Waldron, Tight frames and their symmetries, *Constr. Approx.* 21 (2004) 83–112.
- [84] S. Waldron, A sharpening of the Welch bounds and the existence of real and complex spherical  $t$ -designs, *IEEE Trans. Inf. Theory* 63 (2017) 6849–6857.
- [85] S. Waldron, *An Introduction to Finite Tight Frames*, Applied and Numerical Harmonic Analysis, Birkhäuser, Basel, 2018.
- [86] S. Waldron, Group frames, in: P.G. Casazza, G. Kutyniok (Eds.), *Finite Frames: Theory and Applications*, in: *Applied and Numerical Harmonic Analysis*, Birkhäuser, 2013, pp. 171–191.
- [87] S. Waldron, On the construction of equiangular frames from graphs, *Linear Algebra Appl.* 431 (2009) 2228–2242.
- [88] L.R. Welch, Lower bounds on the maximum cross correlation of signals, *IEEE Trans. Inf. Theory* 20 (1974) 397–399.
- [89] N. Wiegmann, Necessary and sufficient conditions for unitary similarity, *J. Aust. Math. Soc.* 2 (1962) 122–126.
- [90] V.N. Zemlyachenko, N.M. Korneenko, R.I. Tyshkevich, Graph isomorphism problem, *J. Math. Sci.* 29 (1985) 1426–1481.