Faster isomorphism testing of p-groups of Frattini class 2

Gábor Ivanyos* Euan J. Mendoza † Youming Qiao‡ Xiaorui Sun§
Chuanqi Zhang¶

Abstract

The finite group isomorphism problem asks to decide whether two finite groups of order N are isomorphic. Improving the classical $N^{O(\log N)}$-time algorithm for group isomorphism is a long-standing open problem. It is generally regarded that p-groups of class 2 and exponent p form a bottleneck case for group isomorphism in general. The recent breakthrough by Sun (*STOC* '23) presents an $N^{O((\log N)^{5/6})}$-time algorithm for this group class.

In this paper, we improve Sun's algorithm by presenting an $N^{\tilde{O}((\log N)^{1/2})}$-time algorithm for this group class. We also extend our result to the more general p-groups of Frattini class 2. Our algorithm is obtained by sharpening the key technical ingredients in Sun's algorithm and building connections with other research topics. One intriguing connection is with the maximal and non-commutative ranks of matrix spaces, which have recently received considerable attention in algebraic complexity and computational invariant theory. Results from the theory of Tensor Isomorphism complexity class (Grochow–Qiao, *SIAM J. Comput.* '23) are utilized to simplify the algorithm and achieve the extension to p-groups of Frattini class 2.

*Institute for Computer Science and Control, Hungarian Reserch Network, Budapest, Hungary (Gabor.Ivanyos@sztaki.hun-ren.hu).

†University of Technology Sydney, Australia (euan.j.mendoza@student.uts.edu.au).

‡Centre for Quantum Software and Information, University of Technology Sydney, Australia (Youming.Qiao@uts.edu.au).

§Computer Science Department, University of Illinois at Chicago, Chicago, USA (xiaorui@uic.edu)

¶Centre for Quantum Software and Information, University of Technology Sydney, Australia (Chuanqi.Zhang@uts.edu.au).

1 Introduction

1.1 Finite group isomorphism

The finite group isomorphism problem (GpI) asks to decide whether two finite groups of order N are isomorphic or not. Tarjan observed that GpI can be solved in time $N^{\log N+O(1)}$ [Mil78], and to now, only the constant before $\log N$ on the exponent has been improved [Ros13].

It has long been known that when the group order N is a power of prime p, namely when the groups are p-groups, GpI seems the most difficult. Even for p-groups that are "just above" abelian groups, namely p-groups of class 2 and exponent p,[1] no essential progress had not been made, until the recent breakthrough of Sun [Sun23].

Theorem 1.1 ([Sun23, Theorem 1.1]). *Given two p-groups of class 2 and exponent p of order N, there exists an algorithm in time $N^{O((\log N)^{5/6})}$ to decide whether they are isomorphic or not.*

Our first result is to improve the running time from [Sun23] as follows.

Theorem 1.2. *Let p be an odd prime. Given two p-groups of class 2 and exponent p of order N, there exists an algorithm in time $N^{\tilde{O}((\log N)^{1/2})}$ to decide whether they are isomorphic or not.*

In Theorem 1.2, $\tilde{O}$ on the exponent hides a polylogarithmic factor, i.e. $\tilde{O}((\log N)^{1/2}) = O((\log N)^{1/2} \cdot (\log\log N)^{O(1)})$.

We also broaden the group class for which this running time holds. That is, we extend from p-groups of class 2 and exponent p to p-groups of Frattini class 2.

A p-group G is of *Frattini class* 2, if there exists $H \leq G$, such that H is central, and both H and G/H are elementary abelian. p-groups of Frattini class 2 plays an important role in the enumeration of finite groups [BNV07], as it gives a lower bound on the number of p-groups by the celebrated work of Higman [Hig60].

Theorem 1.3. *Let p be an odd prime. Given two p-groups of Frattini class 2 of order N, there exists an algorithm in time $N^{\tilde{O}((\log N)^{1/2})}$ to decide whether they are isomorphic or not.*

1.2 From groups to matrix spaces

A key to several recent works on p-group isomorphism [LQ17, Sun23, GQ24], as well as to this work, is to examine the following linear algebraic problem.

Let $\mathrm{M}(n,q)$ be the linear space of $n\times n$ matrices over $\mathbb{F}_q$ the finite field of order q. Let $\mathrm{GL}(n,q)$ be the general linear group of degree n over $\mathbb{F}_q$. Recall that a matrix $A\in \mathrm{M}(n,q)$ is *alternating*, if for any $v\in\mathbb{F}_q^n$, we have $v^{\mathrm{t}}Av=0$. The linear space of $n\times n$ alternating matrices over $\mathbb{F}_q$ is denoted by $\Lambda(n,q)$.

Let $\mathcal{A},\mathcal{B}\leq\Lambda(n,q)$ be two alternating matrix spaces. We say that $\mathcal{A}$ and $\mathcal{B}$ are *congruent*[2], if there exists $T\in\mathrm{GL}(n,q)$ such that $\mathcal{A}=T^{\mathrm{t}}\mathcal{B}T := \{T^{\mathrm{t}}BT \mid B\in\mathcal{B}\}$. The *alternating matrix space congruence* problem (Alt-MSC) asks to decide $\mathcal{A}$ and $\mathcal{B}$, given by their linear bases, are congruent or not.

Alt-MSC is closely related to testing isomorphism of p-groups of class 2 and exponent p, because of Baer's correspondence [Bae38]. To make this explicit, it is convenient to introduce the following

[1] A p-group G is of class 2 and exponent p, if the centre $Z(G)$ contains the commutator subgroup $[G,G]$, and every $g\in G$ satisfies that $g^p=\mathrm{id}$.

[2] In [Sun23, LQ17], this was called "isometric". We choose to use "congruent" as this is in line with the classical notion of matrix congruence [Mal63].

notation. For an alternating matrix space $\mathcal{A} \leq \Lambda(n,q)$ of dimension m, we define its *length* to be $\ell = n + m$.

Our main technical result is then the following.

Theorem 1.4. *Let $\mathcal{A}, \mathcal{B} \leq \Lambda(n,q)$ be two alternating matrix spaces of dimension m, and let $\ell = n + m$ be their length. Then there exists an algorithm in time $q^{\tilde{O}(\ell^{1.5})}$ that decides whether $\mathcal{A}$ and $\mathcal{B}$ are congruent.*

Theorem 1.4 improves [Sun23, Theorem 1.2], where the running time was $q^{O(\ell^{1.8} \cdot \log q)}$. As solving GpI for p-groups of class 2 and exponent p in time polynomial in the group order is equivalent to solving Alt-MSC over $\mathbb{F}_p$ of length ℓ in time $p^{O(\ell)}$ (see [GQ17]), Theorem 1.2 follows from Theorem 1.4 immediately.

1.3 On the techniques

The overall strategy: reducing to matrix tuple congruence. The algorithm in [Sun23] for Alt-MSC is a reduction from Alt-MSC to the following problem. Let $\mathbf{A} = (A_1, \ldots, A_m)$ and $\mathbf{B} = (B_1, \ldots, B_m) \in \Lambda(n,q)^m$ be two tuples of alternating matrices. We shall call $\ell := n + m$ the *length* of $\mathbf{A}$. They are *congruent* if there exists $T \in \mathrm{GL}(n,q)$ such that for all $i \in [m]$, $A_i = T^{\mathrm{t}} B_i T$. The *alternating matrix tuple congruence* problem (Alt-MTC) asks to decide whether two alternating matrix tuples are congruent.

Roughly speaking, in [Sun23], the algorithm for Alt-MSC of length ℓ over $\mathbb{F}_q$ is obtained by reducing to $q^{O(\ell^{1.8} \cdot \log q)}$-many instances of Alt-MTC[3]of length poly(ℓ), and using that Alt-MTC over finite fields of characteristic $\neq 2$ can be solved in deterministic time poly(ℓ, q) in [IQ19].

In this work, we achieve Theorem 1.4 by following the same strategy as in [Sun23]. We devise a reduction from Alt-MSC of length ℓ over $\mathbb{F}_q$ to $q^{\tilde{O}(\ell^{1.5})}$-many instances of Alt-MTC of length poly(ℓ).

An outline of Sun's algorithm. We give an outline of Sun's algorithm in [Sun23]. Let $\mathcal{A}, \mathcal{B} \leq \Lambda(n,q)$ be two alternating matrix spaces of dimension m. Let $(A_1, \ldots, A_m) \in \Lambda(n,q)^m$ be an ordered basis for $\mathcal{A}$, and $(B_1, \ldots, B_m) \in \Lambda(n,q)^m$ be an ordered basis for $\mathcal{B}$. The question becomes to compute $T \in \mathrm{GL}(n,q)$ and $C = (c_{i,j}) \in \mathrm{GL}(m,q)$, such that $\forall i \in [m]$, $T^{\mathrm{t}} A_i T = \sum_{j \in [m]} c_{i,j} B_j$.

The first key idea, called matrix space individualisation, is the following. Let $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, and consider $L\mathcal{A}R = \{LAR \mid A \in \mathcal{A}\} \leq \mathrm{M}(s,q)$. If $\dim(L\mathcal{A}R) = \dim(\mathcal{A})$, then each $A \in \mathcal{A}$ gets a unique label, namely LAR. A consequence that there exists a canonical basis of $\mathcal{A}$ based on $L\mathcal{A}R$, so we will reduce to the matrix tuple congruence problem.

However, it is possible that $\dim(L\mathcal{A}R) < \dim(\mathcal{A})$, that is, $\mathcal{K} := \{A \in \mathcal{A} \mid LAR = 0\}$ is a non-trivial subspace of $\mathcal{A}$. Fortunately, it can be shown that, for appropriate choices of s, random L and R yield $\mathcal{K}$ that consists of matrices of low rank. This leads to the second key idea: as $\mathcal{K}$ is a low-rank matrix space, it can be arranged in a format that every $A \in \mathcal{K}$ has the last few rows and columns being non-zero. This is referred to as the low-rank matrix characterisation in [Sun23].

Given the above, Sun applied matrix space individualisation and low-rank matrix characterisation to three directions of the $n \times n \times m$ tensor $(A_1, \ldots, A_m)$. This gives a so-called semi-canonical tensors associated with $\mathcal{A}$. To decide isomorphism between semi-canonical tensors, the semi-canonicity ensures that the underlying transformation matrices must be of a certain format. Such structural restrictions lead to a special form of matrix tuple congruence problem, solvable by using the algorithm from [IQ19].

[3]Note that some technicality appears here, namely the Alt-MTC instances have some restrictions on the congruence matrices; see Section 4.3.

Sharpening some key techniques in [Sun23]. Our algorithm follows the strategy of Sun's algorithm, and it improve the two novel techniques proposed in [Sun23] to near optimal (up to a logarithmic factor).

The first one is the matrix space individualisation. Briefly speaking, for an alternating matrix space $\mathcal{A} \leq \Lambda(n, q)$, we use $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, and label each $A \in \mathcal{A}$ by the smaller matrix LAR. For the sake of the second technique, we also need that $\mathcal{K} = \{A \in \Lambda(n, q) \mid LAR = \mathbf{0}\}$ consists of matrices of rank $\leq r$, where r is a parameter and will be determined later. Here we need s, the size parameter of L and R, to be upper bounded by some function of r. We improve this upper bound over that in [Sun23, Lemma 3.2] (as seen in Lemmas 3.3 and 3.4), and the number of individualisations (the number of rows of L and the number of columns of R) is optimal, matching the random sampling lower bound (Remark 4.3).

The second one is the so-called low-rank matrix space characterisation. Recall that from the first step we obtained $\mathcal{K} \leq \Lambda(n, q)$ which consists of matrices of rank $\leq r$. The purpose of the second technique is to put every $A \in \mathcal{K}$ in the form of $\begin{bmatrix} \mathbf{0} & A_2 \\ A_3 & A_4 \end{bmatrix}$ where $\mathbf{0}$ is of size $c \times e$, such that $(n - c) + (n - e)$, the sum of the number of rows in A_3 and the number of columns in A_2, is upper bounded by some function of r. We improve this upper bound over from $O(r^2)$ in [Sun23, Lemma 4.6] to $\tilde{O}(r)$, which is optimal up to a logarithmic factor (Remark 4.6).

Connections with other problems. We realise some connections of the results and techniques in [Sun23] with some problems that have received considerable attention and utilising some recent powerful results.

First, we observe that the low-rank matrix space characterisation as in [Sun23] is closely related to non-commutative ranks of matrix spaces. Non-commutative ranks of matrix spaces has been studied since the 1970s [Coh75, FR04], and recently received considerable attention in computational complexity [HW15, Mul17]. Some recent works show that non-commutative ranks of matrix spaces can be computed in deterministic polynomial time [GGdOW20, IQS18, HH21]. The so-called low-rank matrix space characterisation in [Sun23] is in fact an upper bound of the non-commutative rank of a matrix space in terms of its maximum rank. This has been known over large enough fields [Fla62, FR04], while [Sun23, Lemma 4.6] works over any field.

Second, we note that the alternating matrix tuple congruence problem (Alt-MTC) obtained in [Sun23] has certain restrictions on the congruence matrix structure. This suggests a new family of "restricted" alternating matrix tuple congruence problems, and it is interesting to systematically examine current techniques in [IQ19] for these problems.

Simplifications of the algorithm in [Sun23]. Besides improving some key techniques in [Sun23], we also simplify the algorithm in several ways.

First, our improvement of [Sun23, Lemma 4.6] makes use some classical results about non-commutative ranks as in [Fla62, FR04, IQS18]. We also make use of the fact that non-commutative ranks can be computed in polynomial time to simplify the algorithm.

Second, we simplify the algorithm in [Sun23] by applying individualisation and refinement, and low-rank matrix space characterisation, in one direction, instead of applying these to three directions as in [Sun23]. As a result, the resulting semi-canonical tensors (Section 3.3) have a simpler structure. This is made possible by starting with the matrix space equivalence problem (MSE).

Definition 1.5 (Matrix space equivalence problem (MSE))**.** Given two matrix spaces $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n_1 \times n_2, q)$ of dimension n_3, decide if there exist $L \in \mathrm{GL}(n_1, q)$ and $R \in \mathrm{GL}(n_2, q)$, such that $\mathcal{A} = L^{\mathrm{t}}\mathcal{B}R = \{L^{\mathrm{t}}BR \mid B \in \mathcal{B}\}$.

For $\mathcal{A} \leq \mathrm{M}(n_1 \times n_2, q)$ of dimension n_3, $\ell = n_1 + n_2 + n_3$ is called the length of $\mathcal{A}$. It was recently shown in [GQ23b] that solving Alt-MSC of length ℓ over $\mathbb{F}_q$ reduces to solving MSE of length $O(\ell)$ over $\mathbb{F}_q$. This justifies working with MSE instead of Alt-MSC. The results and techniques in [GQ23b] also play an important role in Theorem 1.3. We remark that [GQ23b] falls into the Tensor Isomorphism complexity class framework initiated in [GQ23a].

Third, in [Sun23], some gadgets are designed to enforce these structural restriction on the congruence matrices of the Alt-MTC problem. Here, we show that one restricted Alt-MTC problem in this setting can be solved efficiently by a short reduction to the key technical problem, called the $*$-symmetric element decomposition problem, solved in [IQ19].

Structure of the paper. After presenting some preliminaries in Section 2, we prove Theorem 1.4 in Section 3, modulo some technical results that will be proved in Section 4. Finally we prove Theorem 1.3 in Section 5.

2 Preliminary

Notations. For $n \in \mathbb{N}$, $[n] := \{1, 2, \ldots, n\}$. Unless otherwise stated, the base of logarithm is 2.

Vector spaces. Let $\mathbb{F}$ be a field. Let $\mathbb{F}^n$ be the linear space of length-n *column* vectors over $\mathbb{F}$. We use $\mathbf{b}_i$ to denote the ith standard basis vector of $\mathbb{F}^n$. For a prime power q, we use $\mathbb{F}_q$ to denote the finite field of order q. Let $\mathrm{GL}(n, \mathbb{F})$ be the general linear group of degree n over $\mathbb{F}$.

Matrix spaces. We use $\mathrm{M}(n_1 \times n_2, \mathbb{F})$ for the linear space of $n_1 \times n_2$ matrices over $\mathbb{F}$, and let $\mathrm{M}(n, q) := \mathrm{M}(n \times n, \mathbb{F}_q)$. A *matrix space* $\mathcal{A}$ is a subspace of $\mathrm{M}(n_1 \times n_2, \mathbb{F})$, denoted by $\mathcal{A} \leq \mathrm{M}(n_1 \times n_2, \mathbb{F})$. A matrix $A \in \mathrm{M}(n, q)$ is *alternating*, if for any $v \in \mathbb{F}_q^n$, we have $v^{\mathrm{t}} A v = 0$. The linear space of $n \times n$ alternating matrices over $\mathbb{F}_q$ is denoted by $\Lambda(n, q)$.

Matrix space equivalence relations. Let $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n_1 \times n_2, \mathbb{F})$. Let $L \in \mathrm{M}(s \times n_1, \mathbb{F})$ and $R \in \mathrm{M}(n_2 \times t, \mathbb{F})$. Then $L\mathcal{A}R := \{LAR \mid A \in \mathcal{A}\} \leq \mathrm{M}(s \times t, \mathbb{F})$. We say that $\mathcal{A}, \mathcal{B}$ are *equivalent*, if there exist $P \in \mathrm{GL}(n_1, \mathbb{F})$ and $Q \in \mathrm{GL}(n_2, \mathbb{F})$, such that $\mathcal{A} = P^{\mathrm{t}} \mathcal{B} Q$. We say that $\mathcal{A}$ and $\mathcal{B}$ are *congruent*, if there exists $T \in \mathrm{GL}(n, \mathbb{F})$, such that $\mathcal{A} = T^{\mathrm{t}} \mathcal{B} T$.

Matrix tuples. We use $\mathrm{M}(n_1 \times n_2, \mathbb{F})^{n_3}$ to denote the linear space of n_3-tuples of $n_1 \times n_2$ matrices, and let $\mathrm{M}(n, q)^k := \mathrm{M}(n \times n, \mathbb{F}_q)^k$. Given a *matrix tuple* $\mathbf{A} = (A_1, \ldots, A_n) \in \mathrm{M}(n_1 \times n_2, \mathbb{F})^{n_3}$, and two matrices $P \in \mathrm{M}(s \times n_1, \mathbb{F})$ and $Q \in \mathrm{M}(n_2 \times t, \mathbb{F})$, $P\mathbf{A}Q := (PA_1Q, \ldots, PA_nQ) \in \mathrm{M}(s \times t, \mathbb{F})^n$. The definitions of matrix tuple equivalence, conjugacy and congruence are similar to those for matrix spaces as above.

Canonical ordered bases of vector and matrix spaces. Let $U \leq \mathbb{F}^n$ and $d = \dim(U)$. We say that an ordered basis $(u_1, \ldots, u_d) \in U^d$ is a canonical basis of U, if there exists a polynomial-time algorithm that, given any ordered basis $(u'_1, \ldots, u'_d)$ of U, outputs $(u_1, \ldots, u_d)$. Viewing $(u_1, \ldots, u_d)$ as an $n \times d$ matrix over $\mathbb{F}$, this is the canonical form problem for $\mathrm{GL}(d, \mathbb{F})$ acting on $\mathrm{M}(n \times d, \mathbb{F})$ from the right. For d-dimensional spaces in $\mathbb{F}^n$, this problem is efficiently solvable by performing Gaussian elimination on the columns of matrices $\mathrm{M}(n \times d, \mathbb{F})$, which gives the reduced column echelon form as a canonical basis.

Let $\mathcal{Q} \leq \mathrm{M}(s, \mathbb{F})$ be a matrix space. We can view $\mathrm{M}(s, \mathbb{F})$ as $\mathbb{F}^{s^2}$ by sending $A \in \mathrm{M}(s, \mathbb{F})$ to $v_A \in \mathbb{F}^{s^2}$ by concatenating the columns of A. A canonical linear basis of $\mathcal{Q} \leq \mathrm{M}(s, \mathbb{F})$ can then be obtained by using the canonical basis algorithm for $\mathbb{F}^{s^2}$ in the last paragraph.

Ranks of matrix spaces. Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F})$. The *maximum rank* of $\mathcal{A}$ is $\mathrm{mrk}(\mathcal{A}) := \max\{\mathrm{rk}(A) \mid A \in \mathcal{A}\}$. For $U \leq \mathbb{F}^n$, the image of U under $\mathcal{A}$ is $\mathcal{A}(U) := \mathrm{span}\{\cup_{A \in \mathcal{A}} A(U)\}$. For $g \in \mathbb{N}$, we say that U is a g-shrunk subspace of $\mathcal{A}$, if $\dim(U) - \dim(\mathcal{A}(U)) \geq g$. The *non-commutative corank* of $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F})$ is defined as $\text{co-ncrk}(\mathcal{A}) := \max\{g \in \mathbb{N} \mid \exists g\text{-shrunk subspace of } \mathcal{A}\}$. The *non-commutative rank* of $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F})$ is defined as $\mathrm{ncrk}(\mathcal{A}) := n - \text{co-ncrk}(\mathcal{A})$.

Canonical shrunk subspaces. Let $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$ with $\text{co-ncrk}(\mathcal{K}) = g$. Then there exists a unique g-shrunk subspace of $\mathcal{K}$ of the smallest dimension [IMQ22, Proposition 7]. This will be called the canonical g-shrunk subspace. The algorithm in [IQS18] computes this canonical g-shrunk subspace of $\mathcal{K}$ (see the paragraph after the proof of [IMQ22, Proposition 7]).

Tensors. A 3-*way array* or a *tensor* of size $n_1 \times n_2 \times n_3$ is $\mathtt{A} = (a_{i,j,k})$ where $i \in [n_1]$, $j \in [n_2]$, and $k \in [n_3]$, and $a_{i,j,k} \in \mathbb{F}$. Let $\mathrm{T}(n_1 \times n_2 \times n_3, \mathbb{F})$ be the linear space of $n_1 \times n_2 \times n_3$ tensors over $\mathbb{F}$. Let $\mathrm{T}(n, \mathbb{F}) := \mathrm{T}(n \times n \times n, \mathbb{F})$.

Let $\mathtt{A} = (a_{i,j,k}) \in \mathrm{T}(n_1 \times n_2 \times n_3, \mathbb{F})$ be a tensor. We can slice $\mathtt{A}$ along one direction and obtain a matrix tuple, and the matrices in this tuple are then called slices. For example, slicing along the first coordinate, we obtain its *horizontal matrix tuple* $(A_1, \ldots, A_{n_1}) \in \mathrm{M}(n_2 \times n_3, \mathbb{F})^{n_1}$, where $A_i(j,k) = \mathtt{A}(i,j,k)$ are called horizontal slices. Similarly, by slicing along the second coordinate, we obtain its *vertical matrix tuple* which is an n_2-tuple of $n_1 \times n_3$ matrices, and the matrices in this tuple are called vertical slices. By slicing along the third coordinate, we get its *frontal matrix tuple*, which is an n_3-tuple of $n_1 \times n_2$ matrices, and the matrices in this tuple are called frontal slices.

3 Algorithm for alternating matrix space congruence

In this section we prove Theorem 1.4, which is obtained by combining Theorem 3.2 with Theorem 3.1.

3.1 From matrix space congruence to matrix space equivalence

Let $\mathcal{A}, \mathcal{B} \leq \Lambda(n, q)$, and suppose $m = \dim(\mathcal{A}) = \dim(\mathcal{B})$. Let $\ell = n + m$ be their length. Our goal is to devise an algorithm to test whether $\mathcal{A}$ and $\mathcal{B}$ are congruent in time $q^{\tilde{O}(\ell^{1.5})}$.

To this end, as indicated in Section 1.3, we shall study the matrix space equivalence problem (MSE) as in Definition 1.5. Recall that for $\mathcal{A} \leq \mathrm{M}(n_1 \times n_2, q)$ of dimension n_3, the length of $\mathcal{A}$ is defined as $\ell = n_1 + n_2 + n_3$.

Our focus on MSE is justified by the following result from [GQ23b].

Theorem 3.1 ([GQ23b, Theorem 1.10])**.** *There is a reduction from* Alt-MSC *of length ℓ over $\mathbb{F}_q$ to* MSE *of length $O(\ell)$ over $\mathbb{F}_q$ in time* $\mathrm{poly}(\ell, \log q)$.

Theorem 3.1 implies that for any constant $1 \leq c \leq 2$, an algorithm solving MSE of length ℓ over $\mathbb{F}_q$ in time $q^{\tilde{O}(\ell^c)}$ implies an algorithm solving Alt-MSC of length ℓ over $\mathbb{F}_q$ in time $q^{\tilde{O}(\ell^c)}$.

We now state our result for matrix space equivalence.

Theorem 3.2. *There is a $q^{\tilde{O}(\ell^{1.5})}$-time algorithm for testing equivalence of matrix spaces of length ℓ over $\mathbb{F}_q$.*

A simplification: from cuboids to cubes. Recall that we want to test if two matrix spaces $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n_1 \times n_2, q)$ of dimension n_3 are equivalent. A minor simplification is to reduce to the case when $\mathcal{A}', \mathcal{B}' \leq \mathrm{M}(n, q)$ of dimension n where $n = \max\{n_1, n_2, n_3\}$ (Proposition 4.11 in Section 4.4). Note that the lengths of $\mathcal{A}'$ and $\mathcal{B}'$ are linear in the lengths of $\mathcal{A}$ and $\mathcal{B}$, so working with $\mathcal{A}'$ and $\mathcal{B}'$ is fine for proving Theorem 3.2.

In the following, we assume that we have $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n, q)$ of dimension n. We wish to test if there exist $P, Q \in \mathrm{GL}(n, q)$, such that $P^{\mathrm{t}} \mathcal{A} Q = \mathcal{B}$.

3.2 Sun's techniques and our improvements

We review two techniques from Sun's algorithm [Sun23] and introduce our improvements, and explain how they affect the final running time of the algorithm. Let $\mathcal{A} \leq \mathrm{M}(n, q)$ be a matrix space of dimension n.

Technique 1: Individualisation by left-right restrictions. The first is an individualisation-type technique. That is, for $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, define $\ker(\mathcal{A}, L, R) := \{A \in \mathcal{A} \mid LAR = 0\} \leq \mathcal{A}$ and $\mathrm{im}(\mathcal{A}, L, R) = \{LAR \mid A \in \mathcal{A}\} \leq \mathrm{M}(s, q)$. Once L and R are fixed, we compute a canonical linear basis of $\mathrm{im}(\mathcal{A}, L, R)$.

The purpose of a canonical linear basis is to assign the every element in the quotient space $\mathcal{A}/\ker(\mathcal{A}, L, R)$ a unique "label". This leaves the ambiguity caused by $\ker(\mathcal{A}, L, R)$, so we need the second technique, namely making use of low-rank matrices. For this purpose, we require L and R to satisfy that (1) $\ker(\mathcal{A}, L, R)$ consists of matrices of rank $\leq r$ where r is sufficiently smaller than n, and (2) the size s for $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$ is upper bounded by some function r. The existence of such L and R with these properties is ensured by a probabilistic argument in [Sun23].

Lemma 3.3 ([Sun23, Lemma 3.2])**.** *Let $\mathcal{A} \leq \mathrm{M}(n, q)$ be a matrix space of dimension n. Fix some $r \in [n]$, and let*

$$s = \lceil 32 \cdot \max\{\frac{n \log q}{\sqrt{r}}, \sqrt{r}\}\rceil. \tag{1}$$

Then there exist $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, such that $\ker(\mathcal{A}, L, R)$ consists of matrices of rank $\leq r$.

We improve the parameters in Lemma 3.3 and put it as a probabilistic statement as follows. The proof of the following lemma is in Section 4.1.

Lemma 3.4. *Let $\mathcal{A} \leq \mathrm{M}(n, q)$ be a matrix space of dimension n. Fix some $r \in [n]$, and let*

$$s = \lceil 3 \cdot \max\{\frac{n}{r}, r\}\rceil. \tag{2}$$

Then with at least probability of $1 - \frac{1}{q^r}$, uniformly randomly sampled $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$ satisfy that $\ker(\mathcal{A}, L, R)$ consists of matrices of rank $\leq r$.

Note that Lemma 3.4 allows us to choose $r = \lceil\sqrt{n}\rceil$ which gives $s = O(\sqrt{n})$. On the other hand, to achieve $s = O(\sqrt{n})$ in [Sun23, Lemma 3.2] requires $r = O(n)$ which is not useful for the next step. Lemma 3.4 also gets rid of the $\log q$ factor of $\frac{n}{\sqrt{r}}$ as in Equation 1, which in [Sun23] affects the final exponent on the $\log N$ as in Theorem 1.1.

Technique 2: Low-rank matrix space characterisation. From the above, we obtain $\mathcal{K} := \ker(\mathcal{A}, L, R) \leq \mathrm{M}(n, q)$ which consists of matrices of rank $\leq r$, where r is small compared with n. Then there exists $U \leq \mathbb{F}_q^n$ of dimension e, such that $\mathcal{K}(U)$ is of dimension d, and letting $g := \dim(U) - \dim(\mathcal{K}(U)) = e - d$, $h := n - g$ is a function in r. Non-commutative ranks (ncrk), non-commutative coranks (co-ncrk), and maximum ranks (mrk) for matrix spaces are defined in Section 2.

In [Fla62], Flanders showed that when the field order $q \geq r+1$, then $h = n-g \leq 2r$ (see [FR04]). When the field order can be small, the following was shown in [Sun23].

Lemma 3.5 ([Sun23, Lemma 4.6])**.** *Let $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$. Suppose $\mathrm{mrk}(\mathcal{K}) = r$. Then $\mathrm{ncrk}(\mathcal{K}) \leq O(r^2)$.*

We improve the parameters in Lemma 3.5 in the following lemma, whose proof is in Section 4.2.

Lemma 3.6. *Let* $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$*. Suppose* $\mathrm{mrk}(\mathcal{K}) = r$*. Then* $\mathrm{ncrk}(\mathcal{K}) \leq O(r \log r)$*.*

Summarising the improvements and the final running time. The two improvements in Lemmas 3.4 and 3.6 contribute to the reduction from $q^{O(\ell^{1.8} \cdot \log q)}$ in [Sun23, Theorem 1.2] to $q^{\tilde{O}(\ell^{1.5})}$ in Theorem 1.4 as follows. Recall that s is the size parameter of the individualising matrices, and $h = \mathrm{ncrk}(\mathcal{K})$ is the non-commutative rank of $\mathcal{K}$.

Briefly speaking, as shown in Section 3.5, the main factor in the running time is $q^{O((s+h)n)}$. In [Sun23], because of Lemmas 3.3 and 3.5, the relations between r, s and h lead to setting $r = \lceil n^{0.4} \rceil$, so $s = O(\max\{n \cdot \log q/\sqrt{r}, \sqrt{r}\}) = O(n^{0.8} \log q)$, and $h = O(r^2) = O(n^{0.8})$. This gives the running time $q^{O(n^{1.8} \cdot \log q)}$. Here, because of Lemmas 3.4 and 3.6, the relations between r, s and h lead to setting $r = \lceil \sqrt{n} \rceil$, so $s = O(\max\{n/r, r\}) = O(\sqrt{n})$, and $h = O(r \log r) = \tilde{O}(\sqrt{n})$. This gives the running time $q^{\tilde{O}(n^{1.5})}$.

3.3 Semi-canonical tensors of matrix spaces

We use the two techniques in Section 3.2 to associate $\mathcal{A} \leq \mathrm{M}(n, q)$ with certain tensors $\mathtt{A} \in \mathrm{T}(n, q)$ in a specific format, such that those $(P, Q, S) \in \mathrm{GL}(n, q) \times \mathrm{GL}(n, q) \times \mathrm{GL}(n, q)$ preserving this format needs to satisfy certain structural constraints.

In the following, we use a parameter r which is the target rank. It will be set as $\lceil \sqrt{n} \rceil$ based on the discussion at the end of Section 3.2.

Semi-canonical tensors. Let $\mathcal{A} \leq \mathrm{M}(n, q)$ be of dimension n. For $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, let $\mathcal{K} = \ker(\mathcal{A}, L, R) \leq \mathcal{A}$ and $\mathcal{Q} = \mathrm{im}(\mathcal{A}, L, R) \leq \mathrm{M}(s, q)$. Let $a = \dim(\mathcal{K})$ and $b = \dim(\mathcal{Q})$, so $a + b = n$. We can then arrange an ordered linear basis $(A_1, \ldots, A_n) \in \mathrm{M}(n, q)^n$ of $\mathcal{A}$, such that $\mathcal{K} = \mathrm{span}\{A_1, \ldots, A_a\}$.

Suppose $\mathrm{mrk}(\mathcal{K}) \leq r$. Let $g = \text{co-ncrk}(\mathcal{K})$, and $h = \mathrm{ncrk}(\mathcal{K}) = n - g$. Let $U \leq \mathbb{F}_q^n$ be the canonical shrunk subspace of $\mathcal{K}$ (Section 2). Let $e := \dim(U)$, $f := n - e$, $d := e - g = \dim(\mathcal{K}(U))$, and $c := n - d$. By left and right multiplying suitable change-of-basis matrices, we can assume $U = \mathrm{span}\{\mathbf{b}_1, \ldots, \mathbf{b}_e\}$, and $\mathcal{K}(U) = \{\mathbf{b}_{c+1}, \ldots, \mathbf{b}_n\}$, and get an $n \times n$ matrix tuple $\mathbf{A} = (A_1, \ldots, A_n)$. For $i \in [n]$, let $A_i = \begin{bmatrix} A_{i,1} & A_{i,2} \\ A_{i,3} & A_{i,4} \end{bmatrix}$, where $A_{i,1} \in \mathrm{M}(c \times e, \mathbb{F})$. Then for $i \in [a]$, $A_{i,1} = \mathbf{0}$.

Because of the canonical basis of $\mathrm{im}(\mathcal{A}, L, R)$ and the canonical shrunk subspace U of $\mathcal{K}$, following [Sun23], we call this $\mathtt{A}$ a *semi-canonical tensor* associated with $\mathcal{A}$, L, and R. The *shape* of $\mathtt{A}$ is then $(a, b, c, d, e, f) \in \mathbb{N}^6$ as above – that is, $a = \dim(\mathcal{K})$, $e = \dim(U)$ where U is the canonical shrunk subspace, and $d = \dim(\mathcal{K}(U))$, and $b = n - a$, $f = n - e$, and $c = n - d$. Figure 1 illustrates the form of a semi-canonical tensor with parameters in its shape.

Briefly speaking, $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$ satisfying $\mathrm{mrk}(\ker(\mathcal{A}, L, R)) \leq r$ will result in a semi-canonical tensor. This tensor is obtained by applying appropriate change-of-basis matrices along the three directions, so that $\mathcal{K} = \ker(\mathcal{A}, L, R)$ is spanned by the first few frontal slices, the canonical shrunk subspace U of $\mathcal{K}$ is spanned by the first few standard basis vectors, and the image of U under $\mathcal{K}$ is spanned by the last few standard basis vectors.

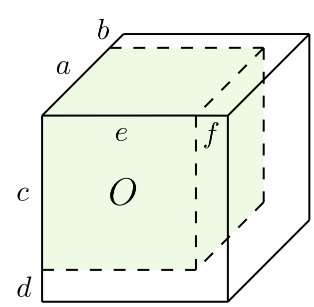

Figure 1: A semi-canonical tensor.

Structural restrictions on the equivalence matrices. Suppose $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$ give rise to two semi-canonical 3-way arrays $\mathtt{A}$ and $\mathtt{B}$ from

$\mathcal{A} \leq \mathrm{M}(n, q)$ as above. Suppose we wish to test equivalence between $\mathtt{A}$ and $\mathtt{B}$ respecting L and R. This means that the canonical objects associated with L and R need to be respected too. Therefore, the equivalence matrices $(P, Q, S) \in \mathrm{GL}(n, q) \times \mathrm{GL}(n, q) \times \mathrm{GL}(n, q)$ need to satisfy the following:

1. S preserves the canonical basis of $\mathrm{im}(\mathcal{A}, L, R)$,
2. Q preserves the canonical shrunk subspace U of $\mathcal{K}$, and
3. P preserves the image of the canonical shrunk subspace of $\mathcal{K}$.

As we have arranged that $\ker(\mathcal{A}, L, R) = \mathrm{span}\{A_1, \dots, A_a\}$ and $(LA_{a+1}R, \dots, LA_nR)$ is the canonical ordered basis of $\mathrm{im}(\mathcal{A}, L, R)$, S is of the form $\begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_b \end{bmatrix}$, where S_1 is of size $a \times a$. As we have arranged the canonical shrunk subspace U of $\mathcal{K}$ to be $\mathrm{span}\{\mathbf{b}_1, \dots, \mathbf{b}_e\}$, Q is of the form $\begin{bmatrix} Q_1 & Q_2 \\ \mathbf{0} & Q_4 \end{bmatrix}$, where Q_1 is of size $e \times e$. As we have arranged $\mathcal{K}(U)$ to be $\mathrm{span}\{\mathbf{b}_{c+1}, \dots, \mathbf{b}_n\}$, P is of the form $\begin{bmatrix} P_1 & \mathbf{0} \\ P_3 & P_4 \end{bmatrix}$, where P_1 is of size $c \times c$.

Observe that $\begin{bmatrix} Q_2 \\ Q_4 \end{bmatrix}$ is of size $n \times f$, and $\begin{bmatrix} P_3 & P_4 \end{bmatrix}$ is of size $d \times n$. And recall that $d + f = (n - e) + (e - g) = n - g = \mathrm{ncrk}(\mathcal{K})$.

3.4 Testing equivalences between semi-canonical tensors

Based on the discussions in Section 3.3, the following problem is crucial.

Problem 3.7. Suppose we are given two 3-way arrays $\mathtt{A}$ and $\mathtt{B}$ in $\mathrm{T}(n, q)$. Let $\mathbf{A} = (A_1, \dots, A_n)$ be the frontal matrix tuple of $\mathtt{A}$, and $\mathbf{B} = (B_1, \dots, B_n)$ be the frontal matrix tuple of $\mathtt{B}$. For $i \in [n]$, let $A_i = \begin{bmatrix} A_{i,1} & A_{i,2} \\ A_{i,3} & A_{i,4} \end{bmatrix}$, where $A_{i,1}$ is of size $c \times e$. Similarly, $i \in [n]$, let $B_i = \begin{bmatrix} B_{i,1} & B_{i,2} \\ B_{i,3} & B_{i,4} \end{bmatrix}$, where $B_{i,1}$ is of size $c \times e$. For $i \in [a]$, $A_{i,1} = B_{i,1} = \mathbf{0}$. Let $d = n - c$, $f = n - e$, and $b = n - a$.

The problem is to decide equivalence of $\mathtt{A}$ and $\mathtt{B}$ under the action of $(P, Q, S) \in \mathrm{GL}(n, q) \times \mathrm{GL}(n, q) \times \mathrm{GL}(n, q)$, where $P = \begin{bmatrix} P_1 & \mathbf{0} \\ P_3 & P_4 \end{bmatrix}$ with $P_1 \in \mathrm{GL}(c, q)$, $Q = \begin{bmatrix} Q_1 & Q_2 \\ \mathbf{0} & Q_4 \end{bmatrix}$ where $Q_1 \in \mathrm{GL}(e, q)$, and $S = \begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_b \end{bmatrix}$ where $S_1 \in \mathrm{GL}(a, q)$.

We will reduce Problem 3.7 to the following conditioned alternating matrix tuple congruence (Cond-Alt-MTC) problem. To introduce this problem, it is convenient to introduce the following. Let $n \in \mathbb{N}$. For $n_1, \dots, n_s \in \mathbb{Z}^+$ with $n_1 + \dots + n_s = n$, let $\mathrm{D}(n_1, \dots, n_s, \mathbb{F}) \leq \mathrm{GL}(n, \mathbb{F})$ be the group of invertible block-diagonal matrices with the block sizes being $n_1, \dots, n_s$. For $t \in \mathbb{N}$, let $\mathrm{I}(n : t, \mathbb{F}) \leq \mathrm{GL}(n, \mathbb{F})$ be the group consisting of invertible matrices of the form $\begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_t \end{bmatrix}$. Let $\mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$ be the group of invertible block-diagonal matrices with the block sizes being $n_1, \dots, n_s$, and each block consisting of matrices from $T(n_i : t_i, \mathbb{F})$.

Problem 3.8 (Conditioned alternating matrix tuple congruence (Cond-Alt-MTC))**.** Given the linear bases of $\mathtt{A}$ and $\mathtt{B} \in \Lambda(n, q)$, decide if they are congruent by a matrix from $\mathrm{I}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$.

In Section 4.3, we show the following.

Lemma 3.9. *There is a polynomial-time algorithm for the conditioned alternating matrix tuple congruence problem over finite fields.*

Based on the above, we can solve Problem 3.7.

Theorem 3.10. *There exists an algorithm solving Problem 3.7 in time* $q^{(d+f)n} \cdot \mathrm{poly}(n, \log q)$.

Proof. Note that $\begin{bmatrix} Q_2 \\ Q_4 \end{bmatrix}$ is of size $n \times f$, and $\begin{bmatrix} P_3 & P_4 \end{bmatrix}$ is of size $d \times n$. As we can accommodate a multiplicative factor of $q^{(d+f)n}$, we can enumerate all matrices of the form $\begin{bmatrix} Q_2 \\ Q_4 \end{bmatrix}$ where Q_4 is invertible, and $\begin{bmatrix} P_3 & P_4 \end{bmatrix}$ where P_4 is invertible. For each fixed $\begin{bmatrix} Q_2 \\ Q_4 \end{bmatrix}$ and $\begin{bmatrix} P_3 & P_4 \end{bmatrix}$, by applying appropriate change of basis matrices, we can assume that $P = \begin{bmatrix} P_1 & \mathbf{0} \\ \mathbf{0} & I_d \end{bmatrix}$ with $P_1 \in \mathrm{GL}(c, q)$, $Q = \begin{bmatrix} Q_1 & \mathbf{0} \\ \mathbf{0} & I_f \end{bmatrix}$ where $Q_1 \in \mathrm{GL}(e, q)$.

We now examine the action of $P = \begin{bmatrix} P_1 & \mathbf{0} \\ \mathbf{0} & I_d \end{bmatrix}$, $Q = \begin{bmatrix} Q_1 & \mathbf{0} \\ \mathbf{0} & I_f \end{bmatrix}$, and $S = \begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_b \end{bmatrix}$ on $\mathtt{A}$. Recall that the frontal matrix tuple of $\mathtt{A}$ is

$$\left(\begin{bmatrix} \mathbf{0} & A_{1,2} \\ A_{1,3} & A_{1,4} \end{bmatrix}, \ldots, \begin{bmatrix} \mathbf{0} & A_{a,2} \\ A_{a,3} & A_{a,4} \end{bmatrix}, \begin{bmatrix} A_{a+1,1} & A_{a+1,2} \\ A_{a+1,3} & A_{a+1,4} \end{bmatrix}, \ldots, \begin{bmatrix} A_{n,1} & A_{n,2} \\ A_{n,3} & A_{n,4} \end{bmatrix} \right).$$

We then consider the following three sub-arrays of $\mathtt{A}$.

The first one is $\mathtt{A}' \in \mathrm{T}(n \times f \times n, q)$, whose frontal slices are $\left(\begin{bmatrix} A_{1,2} \\ A_{1,4} \end{bmatrix}, \begin{bmatrix} A_{2,2} \\ A_{2,4} \end{bmatrix}, \ldots, \begin{bmatrix} A_{n,2} \\ A_{n,4} \end{bmatrix} \right)$. As $Q = \begin{bmatrix} Q_1 & \mathbf{0} \\ \mathbf{0} & I_f \end{bmatrix}$, the action of (P, Q, S) on its vertical slices is trivial. So let its vertical matrix tuple be $\mathbf{A}' = (A'_1, \ldots, A'_f) \in \mathrm{M}(n, q)^f$, with P acting on its left, and S acting on its right.

The second one is $\mathtt{A}'' \in \mathrm{T}(d \times e \times n, q)$, whose frontal slices are $(A_{1,3}, A_{2,3}, \ldots, A_{n,3})$. As $P = \begin{bmatrix} P_1 & \mathbf{0} \\ \mathbf{0} & I_d \end{bmatrix}$, the action of (P, Q, S) on its horizontal slices is trivial. So let its horizontal matrix tuple be $\mathbf{A}'' = (A''_1, \ldots, A''_d) \in \mathrm{M}(e \times n, q)^d$, with $Q_1 \in \mathrm{GL}(e, q)$ acting on its left, and S acting on its right.

The third one is $\mathtt{A}''' \in \mathrm{T}(c \times e \times b, q)$, whose frontal slices are $(A_{a+1,1}, A_{a+2,1}, \ldots, A_{n,1})$. As $S = \begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_b \end{bmatrix}$ and $A_{1,1} = \cdots = A_{a,1} = \mathbf{0}$, the action of (P, Q, S) on its frontal slices is trivial. So let its frontal matrix tuple be $\mathbf{A}''' = (A'''_1, \ldots, A'''_b) \in \mathrm{M}(c \times e, q)^b$, with $P_1 \in \mathrm{GL}(c, q)$ acting on its left and $Q_1 \in \mathrm{GL}(e, q)$ acting on its right.

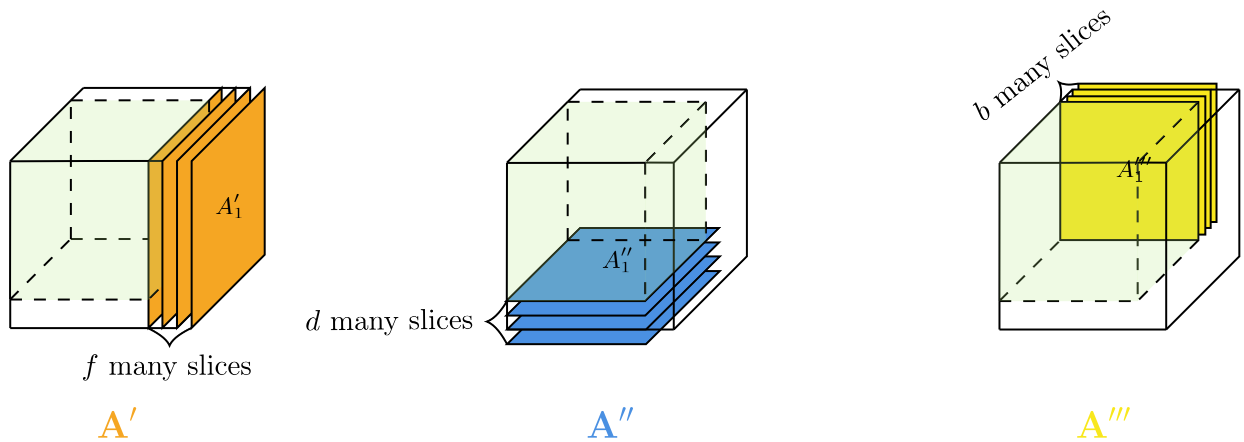

Figure 2: Construction of matrix tuples from semi-canonical tensors.

We perform the above array decomposition to $\mathtt{B}$ to obtain three matrix tuples $\mathbf{B}'$, $\mathbf{B}''$, and $\mathbf{B}'''$. This leads to three matrix *tuple* equivalence instances with correlated actions as follows.

- *Input:* Three pairs of matrix tuples: $\mathbf{A}', \mathbf{B}' \in \mathrm{M}(n,q)^f$, $\mathbf{A}'', \mathbf{B}'' \in \mathrm{M}(e \times n, q)^d$, and $\mathbf{A}''', \mathbf{B}''' \in \mathrm{M}(c \times e, q)^b$.
- *Output:* "Yes" if there exist $P_1 \in \mathrm{GL}(c,q)$, $Q_1 \in \mathrm{GL}(e,q)$, and $S = \begin{bmatrix} S_1 & S_2 \\ 0 & I_b \end{bmatrix} \in \mathrm{GL}(n,q)$, such that the following holds. Let $P = \begin{bmatrix} P_1 & \mathbf{0} \\ \mathbf{0} & I_d \end{bmatrix} \in \mathrm{GL}(n,q)$. Then $P^{\mathrm{t}}\mathbf{A}'S = \mathbf{B}'$, $Q_1^{\mathrm{t}}\mathbf{A}''S = \mathbf{B}''$, and $P_1^{\mathrm{t}}\mathbf{A}'''Q_1 = \mathbf{B}'''$. "No" if no such P_1, Q_1, and S exist.

We assemble the above three matrix tuple equivalence instances into one alternating matrix tuple congruence instance as follows. Let $\tilde{\mathbf{A}} = (\tilde{A}_1, \dots, \tilde{A}_{f+d+b}) \in \Lambda(2n+e,q)^{f+d+b}$ be as follows. For $i \in [f]$, $\tilde{A}_i = \begin{bmatrix} \mathbf{0} & \mathbf{0} & A'_i \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -A'^{\mathrm{t}}_i & \mathbf{0} & \mathbf{0} \end{bmatrix}$, where $A'_i \in \mathrm{M}(n,q)$. For $i \in [f+1, f+d]$, $\tilde{A}_i = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & A''_{i-f} \\ \mathbf{0} & -A''^{\mathrm{t}}_{i-f} & \mathbf{0} \end{bmatrix}$, where $A''_i \in \mathrm{M}(e \times n, q)$. For $i \in [f+d+1, f+d+b]$, $\tilde{A}_i = \begin{bmatrix} \mathbf{0} & A'''_{i-f-b} & \mathbf{0} \\ -A'''_{i-f-b} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$, where $A'''_i \in \mathrm{M}(c \times e, q)$. Do the same for $\mathbf{B}'$, $\mathbf{B}''$, and $\mathbf{B}'''$ to obtain $\tilde{\mathbf{B}} \in \Lambda(2n+e,q)^{f+d+b}$. We then need to test the congruence of alternating matrix tuples $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{B}}$ under the action of $T \in \mathrm{diag}(P_1, I_d, Q_1, S)$ where $S = \begin{bmatrix} S_1 & S_2 \\ \mathbf{0} & I_b \end{bmatrix}$. This is an instance of Cond-Alt-MTC, which can be solved in polynomial time by Lemma 3.9. This concludes the proof. □

3.5 Algorithm description

We now briefly summarise the contents from Section 3.2 to Section 3.4. Recall that we wish to test if $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n,q)$ of dimension n are equivalent or not. In Section 3.2, we introduced two key techniques (individualisation by left and right matrices, low-rank matrix space characterisation) from [Sun23] and our improvements. In Section 3.3, by utilising the two techniques, given appropriate left and right individualising matrices $L \in \mathrm{M}(t \times n, q)$ and $R \in \mathrm{M}(n \times t, q)$, we obtain a tensor called a semi-canonical tensor $\mathtt{A} \in \mathrm{T}(n,q)$ of $\mathcal{A}$ w.r.t. L and R. Because of the canonical objects in this procedure, we see that there are structural restrictions on the equivalence matrices of two semi-canonical tensors $\mathtt{A}, \mathtt{B} \in \mathrm{T}(n, q)$ of $\mathcal{A}$ from the same L and R. In Section 3.4, we study the tensor equivalence with structural restriction problem from the previous step. We show that this problem reduces to the conditioned alternating matrix *tuple* congruence problem, with some conditions on the congruence matrices. This problem can be solved in polynomial time (Section 4.3).

Based on the above, an algorithm for testing equivalence of $\mathcal{A}, \mathcal{B} \in \mathrm{M}(n, q)$ is as follows.

1. Compute a semi-canonical tensor $\mathtt{A}$ of $\mathcal{A}$ w.r.t. $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, with the target rank being r. Let the shape of $\mathtt{A}$ be (a, b, c, d, e, f).

2. Enumerate all $L' \in \mathrm{M}(s \times n, q)$ and $R' \in \mathrm{M}(n \times s, q)$ and compute a semi-canonical tensor $\mathtt{B}$ of $\mathcal{B}$ w.r.t. L' and R'. For each $\mathtt{B}$ of the same shape as $\mathtt{A}$, test if $\mathtt{A}$ and $\mathtt{B}$ are equivalent in the sense of Problem 3.7, which can be solved in time $q^{(d+f)n} \cdot \mathrm{poly}(n, \log q)$ by Theorem 3.10. If for some $\mathtt{B}$ the algorithm in Theorem 3.10 reports "Yes", then return "Yes".

3. Return "No".

To compute a semi-canonical tensor on the $\mathcal{A}$ side with the target rank r, we can do the following.

1. First, randomly sample $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$, where $s = \lceil 3 \cdot \max\{\frac{n}{r}, r\} \rceil$ by Lemma 3.4. Let $\mathcal{K} := \ker(\mathcal{A}, L, R)$. Set $a := \dim(\mathcal{K})$, and $b := n - a$. Test whether $\mathrm{mrk}(\mathcal{K}) \leq r$, by going over all the matrices in $\mathcal{K}$, in time $q^a \cdot \mathrm{poly}(n, \log q)$. By Lemma 3.4, the probability of $\mathrm{mrk}(\mathcal{K}) \leq r$ is lower bounded by $1 - \frac{1}{q^r}$

2. Second, we have $\mathcal{K} := \ker(\mathcal{A}, L, R)$ such that $a = \dim(\mathcal{K})$ and $\mathrm{mrk}(\mathcal{K}) \leq r$. By a basis change, we arrange a matrix tuple $(A_1, \dots, A_n)$, such that (1) $\mathcal{A} = \mathrm{span}\{A_1, \dots, A_n\}$, (2) $\mathcal{K} := \ker(\mathcal{A}, L, R) = \mathrm{span}\{A_1, \dots, A_a\}$, and (3) $(LA_{a+1}R, \dots, LA_nR)$ is the canonical ordered basis of $\mathrm{im}(\mathcal{A}, L, R)$. This canonical ordered basis of $\mathrm{im}(\mathcal{A}, L, R)$ can be computed efficiently as described in Section 2.

3. Third, let $g = \text{co-ncrk}(\mathcal{K})$, and $h = \mathrm{ncrk}(\mathcal{K}) = n - g$. Compute the canonical shrunk subspace U of $\mathcal{K}$ by the algorithm in [IQS18] (see Section 2). By Lemma 3.6, $h \leq O(r \log r)$. Let $e := \dim(U)$, $f := n - e$, $d := e - g = \dim(\mathcal{K}(U))$, and $c := n - d$. By applying suitable basis changes, we can set $U = \mathrm{span}\{\mathbf{b}_1, \dots, \mathbf{b}_e\}$, and $\mathcal{K}(U) = \{\mathbf{b}_{c+1}, \dots, \mathbf{b}_n\}$. This then gives us a semi-canonical tensor of $\mathcal{A}$ w.r.t. L and R.

To enumerate semi-canonical tensors on the $\mathcal{B}$ side follows the same steps, so we omit here.

Correctness. We need to argue that $\mathcal{A}$ and $\mathcal{B}$ are equivalent if and only if the above algorithm returns "Yes". First, if the algorithm returns "Yes", then this means that there is a series of matrices multiplying on the three directions of $\mathtt{A}$ to arrive at $\mathtt{B}$, so $\mathcal{A}$ and $\mathcal{B}$ are equivalent. Second, suppose $\mathcal{A}$ and $\mathcal{B}$ are equivalent, namely there exist $P, Q \in \mathrm{GL}(n, \mathbb{F})$ such that $\mathcal{A} = P^{\mathrm{t}} \mathcal{B} Q$. Recall that L and R are the left and right individualising matrices which we fixed on the $\mathcal{A}$ side. Then the left and right individualising matrices LP^{t} and QR on the $\mathcal{B}$ side will give rise to a semi-canonical tensor $\mathtt{B}$ that are related by the special equivalence matrices as defined in Problem 3.7. As Theorem 3.10 solves Problem 3.7, the algorithm will return "Yes".

Running time. To compute a semi-canonical tensor of $\mathcal{A}$ takes $\mathrm{poly}(n, \log q)$ time. To enumerate $L' \in \mathrm{M}(s \times n, q)$ and $R' \in \mathrm{M}(n \times s, q)$ takes q^{sn} time. To solve Problem 3.7 takes $q^{(d+f)n} \cdot \mathrm{poly}(n, \log q)$ time. Therefore the total running time is upper bounded by $q^{(s+d+f)n} \cdot \mathrm{poly}(n, \log q)$ time. Recall that $r = \lceil \sqrt{n} \rceil$. By Lemma 3.4, $s = O(r)$. By Lemma 4.5, $d + f = \mathrm{ncrk}(\mathcal{K}) \leq O(r \log r) = O(\sqrt{n} \log n)$. Therefore, the total running time is bounded by $q^{\tilde{O}(n^{1.5})}$.

4 Technical results to support Theorem 3.2

4.1 On the individualisation step

Lemma 4.1. *Suppose $A \in \mathrm{M}(m \times n, q)$ is of rank at least r. For uniformly randomly sampled $L \in \mathrm{M}(s \times m, q)$ and $R \in \mathrm{M}(n \times s, q)$,* $\Pr[LAR = \mathbf{0} \in \mathrm{M}(s, q)] \leq \frac{1}{q^{r(s-1)-(r+1)^2/4}}$.

Proof. First of all, we prove $\Pr[\mathrm{rk}(A) = r, LAR = \mathbf{0} \in \mathrm{M}(s, q)] \leq \frac{1}{q^{r(s-1)-(r+1)^2/4}}$. Without loss of generality, we may assume $A = \begin{bmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. Let $L = \begin{bmatrix} L_1 & L_2 \end{bmatrix}$, where $L_1 \in \mathrm{M}(s \times r, q)$, and $R = \begin{bmatrix} R_1 \\ R_2 \end{bmatrix}$, where $R_1 \in \mathrm{M}(r \times s, q)$. Then $\Pr[\mathrm{rk}(A) = r, LAR = \mathbf{0} \in \mathrm{M}(s, q)] = \Pr[L_1 R_1 = \mathbf{0} \in \mathrm{M}(s, q)]$. Observe that

$$\begin{aligned} \Pr[L_1 R_1 = \mathbf{0} \in \mathrm{M}(s, q)] &= \sum_{0 \leq k \leq \min\{r,s\}} \Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] \cdot \Pr[\mathrm{rk}(R_1) = k] \\ &\leq r \cdot \max_{0 \leq k \leq \min\{r,s\}} \left\{ \Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] \cdot \Pr[\mathrm{rk}(R_1) \leq k] \right\}. \end{aligned}$$

Now let us focus on $\Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] \cdot \Pr[\mathrm{rk}(R_1) \leq k]$, where $0 \leq k \leq \min\{r, s\}$.

First, we have $\Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] = \frac{q^{(r-k) \cdot s}}{q^{rs}} = \frac{1}{q^{ks}}$.

Second, to upper bound $\Pr[\mathrm{rk}(R_1) \leq k]$, we can equivalently consider when R_1 has a column space of dimension $\leq k$. Then it is straightforward to see that $\binom{r}{k}_q \cdot q^{ks}$ is an upper bound for the number of $r \times s$ matrices of rank $\leq k$. Here, $\binom{r}{k}_q$ is the Gaussian binomial coefficient which counts the number of k-dimensional subspaces of $\mathbb{F}_q^r$, and q^{ks} accounts for the possibilities of choosing s many column vectors from each k-dimensional subspace. Using the bound $\binom{r}{k}_q \leq q^{k(r-k)+k}$ [BNV07, Proposition 3.16], it follows that $\Pr[\mathrm{rk}(R_1) \leq k] \leq \frac{q^{k(r-k)+k}}{q^{rs}} \cdot q^{ks}$.

Based on the above, we have $\Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] \cdot \Pr[\mathrm{rk}(R_1) \leq k] \leq \frac{1}{q^{ks}} \cdot \frac{1}{q^{rs+k^2-kr-k}} \cdot q^{ks} = \frac{1}{q^{rs+k^2-kr-k}}$. Note that $\frac{1}{q^{rs+k^2-kr-k}}$ achieves maximum at $k = (r+1)/2$, with the value $\frac{1}{q^{rs-(r+1)^2/4}}$. It follows that

$$\begin{aligned} \Pr[\mathrm{rk}(A) = r, LAR = \mathbf{0} \in \mathrm{M}(s, q)] &\leq r \cdot \max_{0 \leq k \leq \min\{r,s\}} \left\{ \Pr[L_1 R_1 = \mathbf{0} \mid \mathrm{rk}(R_1) = k] \cdot \Pr[\mathrm{rk}(R_1) \leq k] \right\} \\ &\leq \frac{r}{q^{rs-(r+1)^2/4}} \\ &\leq \frac{q^r}{q^{rs-(r+1)^2/4}} = \frac{1}{q^{r(s-1)-(r+1)^2/4}}. \end{aligned}$$

To complete the proof, we claim that for uniformly randomly sampled $L \in \mathrm{M}(s \times m, q)$ and $R \in \mathrm{M}(n \times s, q)$, $\Pr[\mathrm{rk}(A') \geq r, LA'R = \mathbf{0} \in \mathrm{M}(s, q)] \leq \Pr[\mathrm{rk}(A) = r, LAR = \mathbf{0} \in \mathrm{M}(s, q)]$. Again, without loss of generality, we assume $A' = \begin{bmatrix} I_{r'} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$ where $r' \geq r$. Let $L = \begin{bmatrix} L'_1 & L'_2 \end{bmatrix}$, where $L'_1 \in \mathrm{M}(s \times r', q)$, and $R = \begin{bmatrix} R'_1 \\ R'_2 \end{bmatrix}$, where $R'_1 \in \mathrm{M}(r' \times s, q)$. Then $\Pr[\mathrm{rk}(A') = r', LA'R = \mathbf{0} \in \mathrm{M}(s, q)] = \Pr[L'_1 R'_1 = \mathbf{0} \in \mathrm{M}(s, q)]$. Now it suffices to show that for any $r' \geq r$, $\Pr[L'_1 R'_1 = \mathbf{0}] \leq \Pr[L_1 R_1 = \mathbf{0}]$ for uniformly randomly sampled $L_1 \in \mathrm{M}(s \times r, q)$, $R_1 \in \mathrm{M}(r \times s, q)$, $L'_1 \in \mathrm{M}(s \times r', q)$ and $R'_1 \in \mathrm{M}(r' \times s, q)$. This can be done by further partitioning $L'_1 \in \mathrm{M}(s \times r', q)$ and $R'_1 \in \mathrm{M}(r' \times s, q)$, i.e., letting $L'_1 = \begin{bmatrix} L''_1 & L''_2 \end{bmatrix}$ where $L''_1 \in \mathrm{M}(s \times r, q)$, and $R'_1 = \begin{bmatrix} R''_1 \\ R''_2 \end{bmatrix}$ where $R''_1 \in \mathrm{M}(r \times s, q)$. Thus,

$\Pr[L_1'R_1' = \mathbf{0}] = \Pr[L_1''R_1'' + L_2''R_2'' = \mathbf{0}] \leq \Pr[L_1''R_1'' = \mathbf{0}] = \Pr[L_1R_1 = \mathbf{0}]$. This concludes the proof. □

Proposition 4.2. *Let $\mathcal{A} \leq \mathrm{M}(m \times n, q)$ be a matrix space of dimension d. Let $s = 2 + \lceil \frac{d}{r} + \frac{(r+1)^2}{4r} \rceil$. Then with probability at least $1 - \frac{1}{q^r}$, uniformly randomly sampled $L \in \mathrm{M}(s \times m, q)$ and $R \in \mathrm{M}(n \times s, q)$ satisfy that for any $A \in \mathcal{A}$ of rank $\geq r$, LAR is not zero.*

Proof. Suppose L and R are uniformly randomly sampled matrices. By union bound and Lemma 4.1, $\Pr[\exists A \in \mathcal{A}, \mathrm{rk}(A) \geq r, LAR = \mathbf{0}] \leq q^d \cdot \Pr[\mathrm{rk}(A) \geq r, LAR = \mathbf{0}] \leq \frac{q^d}{q^{r(s-1)-(r+1)^2/4}}$. Therefore, when $s = 2 + \lceil \frac{d}{r} + \frac{(r+1)^2}{4r} \rceil$, $\Pr[\forall A \in \mathcal{A}, \mathrm{rk}(A) \geq r, LAR \neq \mathbf{0}] \geq 1 - \frac{q^d}{q^{r(s-1)-(r+1)^2/4}} \geq 1 - \frac{1}{q^r}$, which ensures such L and R with the desired probability. □

Lemma 3.4, restated. Let $\mathcal{A} \leq \mathrm{M}(n, q)$ be a matrix space of dimension n. Fix some $r \in [n]$, and let

$$s = \lceil 3 \cdot \max\{\frac{n}{r}, r\} \rceil. \tag{3}$$

Then with probability at least $1 - \frac{1}{q^r}$, uniformly randomly sampled $L \in \mathrm{M}(s \times n, q)$ and $R \in \mathrm{M}(n \times s, q)$ satisfy that $\ker(\mathcal{A}, L, R)$ consists of matrices of rank $\leq r$.

Proof of Lemma 3.4. By Proposition 4.2, it suffices to show that $3 \cdot \max\{\frac{n}{r}, r\} \geq 2 + \frac{n}{r} + \frac{(r+1)^2}{4r}$ for all $n \geq 2$.

If $\frac{n}{r} \geq r$, then $3 \cdot \frac{n}{r} - (2 + \frac{n}{r} + \frac{(r+1)^2}{4r}) \geq 2r - 2 - \frac{(r+1)^2}{4r}$, which is positive for all $r \geq 2$. When $r = 1$, $3 \cdot \max\{\frac{n}{r}, r\} - (2 + \frac{n}{r} + \frac{(r+1)^2}{4r}) = 3n - (n+3) \geq 0$ for all $n \geq 2$.

If $\frac{n}{r} \leq r$, then $3r - (2 + \frac{n}{r} + \frac{(r+1)^2}{4r}) \geq 2r - 2 - \frac{(r+1)^2}{4r}$, which is positive for all $r \geq 2$. □

Remark 4.3. The parameters in Lemma 3.4 are near optimal in the following sense. Consider an n-dimensional $\mathcal{A} \leq \mathrm{M}(n, q)$, such that every $A \in \mathcal{A}$ is of rank $r := \lceil \sqrt{n} \rceil$. By increasing by 1 if needed, assume that r is even. Then the number of $r/2$-dimensional subspaces contained in $\ker(A)$ for some $A \in \mathcal{A}$ could be as many as $q^n \cdot \binom{n-r/2}{r/2}_q = q^n \cdot q^{(n-r)r/2+\Theta(r)} = q^{(n-r/2)r/2+3n/4+\Theta(r)}$, which is much larger than $\binom{n}{r/2}_q = q^{(n-r/2)r/2+\Theta(r)}$, the number of $r/2$-dimensional subspaces in $\mathbb{F}_q^n$. From this perspective, the best we can hope for the size s in L and R is cr for some constant $c > 1$, and this is indeed achievable by Lemma 3.4.

4.2 Non-commutative and commutative ranks over small fields

Let $\mathcal{A} \leq \mathrm{M}(n, \mathbb{F})$ be a matrix space. Recall that the maximum rank and the non-commutative ranks of $\mathcal{A}$, $\mathrm{mrk}(\mathcal{A})$ and $\mathrm{ncrk}(\mathcal{A})$, were defined in Section 2. We recall some previous results. First observe that $\mathrm{mrk}(\mathcal{A}) \leq \mathrm{ncrk}(\mathcal{A})$. We are interested in upper bounding $\mathrm{ncrk}(\mathcal{A})$ by $\mathrm{mrk}(\mathcal{A})$.

When the field order is large, the following was known.

Theorem 4.4 ([Fla62, Lemma 1]; see [FR04, Corollary 2])**.** *Let $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$. Suppose $\mathrm{mrk}(\mathcal{K}) = r$ and $|\mathbb{F}| \geq r + 1$. Then $\mathrm{ncrk}(\mathcal{K}) \leq 2r$.*

Lemma 3.6, restated. Let $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$. Suppose $\mathrm{mrk}(\mathcal{K}) = r$. Then $\mathrm{ncrk}(\mathcal{K}) \leq O(r \log r)$.

Proof of Lemma 3.6. Because of Theorem 4.4, we only need to show this for the case of $|\mathbb{F}| \leq r$. Our strategy is to use extension fields of $\mathbb{F}$.

In the following, $\mathbb{F}$ is a finite field of order s.

Suppose $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$ is of dimension m, and $A_1, \ldots, A_m \in \mathrm{M}(n, \mathbb{F})$ form a linear basis of $\mathcal{K}$. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ of degree d. Let $\mathcal{K}_{\mathbb{E}} = \{\alpha_1 A_1 + \cdots + \alpha_m A_m \mid \forall i \in [m], \alpha_i \in \mathbb{E}\} \leq \mathrm{M}(n, \mathbb{E})$. To distinguish $\mathcal{K}$ and $\mathcal{K}_{\mathbb{E}}$, we shall write $\mathcal{K}$ as $\mathcal{K}_{\mathbb{F}}$ in the following.

Note that $|\mathbb{E}| = |\mathbb{F}|^d = s^d$. Let $d = \lceil \log(r) \rceil + 1$, so $|\mathbb{E}| = s^d \geq 2^{\lceil \log(r) \rceil + 1} \geq r + 1$. By Theorem 4.4, $\mathrm{ncrk}(\mathcal{K}_{\mathbb{E}}) \leq 2 \cdot \mathrm{mrk}(\mathcal{K}_{\mathbb{E}})$. As the non-commutative rank remains the same over field extensions (see [IQS18, Lemma 5.3]), we have

$$\mathrm{ncrk}(\mathcal{K}_{\mathbb{F}}) = \mathrm{ncrk}(\mathcal{K}_{\mathbb{E}}) \leq 2 \cdot \mathrm{mrk}(\mathcal{K}_{\mathbb{E}}). \tag{4}$$

Our goal is to upper bound $\mathrm{mrk}(\mathcal{K}_{\mathbb{E}})$ by $r = \mathrm{mrk}(\mathcal{K}_{\mathbb{F}})$. This is achieved by the following lemma, whose proof is put in Section 4.2.1.

Lemma 4.5. *Let $\mathbb{F}$ be a field and $\mathbb{E}$ be an extension field of $\mathbb{F}$ of degree d. Let $\mathcal{K} \leq \mathrm{M}(n, \mathbb{F})$, and $\mathcal{K}_{\mathbb{E}} = \mathcal{K} \otimes_{\mathbb{F}} \mathbb{E}$. Then $\mathrm{mrk}(\mathcal{K}_{\mathbb{E}}) \leq \mathrm{mrk}(\mathcal{K}) \cdot d$.*

Back to our setting, we combine Lemma 4.5, $d = \lceil \log(r) \rceil + 1$, and Equation 4 to obtain

$$\mathrm{ncrk}(\mathcal{K}_{\mathbb{F}}) = \mathrm{ncrk}(\mathcal{K}_{\mathbb{E}}) \leq 2 \cdot \mathrm{mrk}(\mathcal{K}_{\mathbb{E}}) \leq 2 \cdot \mathrm{mrk}(\mathcal{K}_{\mathbb{F}}) \cdot d = O(r \log r).$$

This concludes the proof. □

Remark 4.6. Note that Lemma 3.6 is optimal up to a logarithmic factor, because of the basic fact that $\mathrm{mrk}(\mathcal{K}_{\mathbb{F}}) \leq \mathrm{ncrk}(\mathcal{K}_{\mathbb{F}})$.

4.2.1 Proof of Lemma 4.5

Proof of Lemma 4.5. We may write $\mathcal{K}$ as $\mathcal{K}_{\mathbb{F}}$ for clarity in the following. Let $r = \mathrm{mrk}(\mathcal{K}_{\mathbb{F}})$ and $\tilde{r} = \mathrm{mrk}(\mathcal{K}_{\mathbb{E}})$. Our goal is to show that $\tilde{r} \leq r \cdot d$.

Suppose $A_1, \ldots, A_m \in \mathrm{M}(n, \mathbb{F})$ form a linear basis of $\mathcal{K}_{\mathbb{F}}$. So $\mathcal{K}_{\mathbb{F}} = \{c_1 A_1 + \cdots + c_m A_m \mid \forall i \in [m], c_i \in \mathbb{F}\}$, and $\mathcal{K}_{\mathbb{E}} = \{\gamma_1 A_1 + \cdots + \gamma_m A_m \mid \forall i \in [m], \gamma_i \in \mathbb{E}\}$. As $\tilde{r} = \mathrm{mrk}(\mathcal{K}_{\mathbb{E}})$, there exist $\beta_1, \ldots, \beta_m \in \mathbb{E}$, such that $B = \beta_1 A_1 + \cdots + \beta_m A_m$ is of rank $\tilde{r}$.

As $\mathbb{E}$ is an extension field of $\mathbb{F}$ of degree d, there exists $\{\alpha_1, \ldots, \alpha_d\} \subseteq \mathbb{E}$ as an $\mathbb{F}$-linear basis of $\mathbb{E}$. We can then write, for every $i \in [m]$, $\beta_i = \sum_{j \in [d]} a_{i,j} \alpha_j$, $a_{i,j} \in \mathbb{F}$. It follows that $B = \beta_1 A_1 + \cdots + \beta_m A_m = \sum_{i \in [m]} (\sum_{j \in [d]} a_{i,j} \alpha_j) A_i = \sum_{j \in [d]} (\sum_{i \in [m]} a_{i,j} A_i) \alpha_j$. For $j \in [d]$, let $C_j = \sum_{i \in [m]} a_{i,j} A_i$, which is in $\mathcal{K}_{\mathbb{F}}$. So $B = \sum_{j \in [d]} \alpha_j C_j$. By the subadditivity of matrix ranks, $\tilde{r} = \mathrm{rk}(B) \leq \sum_{j \in [d]} \mathrm{rk}(C_j \alpha_j)$. So there exists some $k \in [d]$, such that $\mathrm{rk}(C_k) = \mathrm{rk}(C_k \cdot \alpha_k) \geq \tilde{r}/d$. As $C_k \in \mathcal{K}_{\mathbb{F}}$, we have $r \geq \mathrm{rk}(C_k) \geq \tilde{r}/d$. This concludes the proof. □

4.3 Solving conditioned alternating matrix tuple congruence

In this section, we give an algorithm for the conditioned alternating matrix tuple congruence problem (Cond-Alt-MTC) to prove Lemma 3.9. We first reduce to the block-diagonal group setting (i.e. resolving $\mathrm{I}(n : t, q)$ components), using a technique from [Sun23]. We then solve the block-diagonal alternating matrix tuple congruence directly by a simple reduction to a problem solved in [IQ19].

4.3.1 Reducing the block-diagonal Alt-MTC problem

Our problem in this subsection is to test if $\mathbf{A}, \mathbf{B} \in \Lambda(n, q)^m$ are congruent under $\mathrm{DI}(n_1 : t_1, \ldots, n_s : t_s, q)$. We will construct $\mathbf{A}', \mathbf{B}' \in \Lambda(n + 3, q)^{m'}$, such that $\mathbf{A}$ and $\mathbf{B}$ are congruent by $\mathrm{DI}(n_1 : t_1, \ldots, n_s : t_s, q)$ if and only if $\mathbf{A}'$, $\mathbf{B}'$ are congruent by $\mathrm{D}(n_1, \ldots, n_s, 3, q)$. To achieve this, the following facts are useful.

Lemma 4.7. *1. Let $u_1, u_2, v_1, v_2 \in \mathbb{F}^n$. Then $u_1u_2^{\mathrm{t}} - u_2u_1^{\mathrm{t}}$ is a scalar multiple of $v_1v_2^{\mathrm{t}} - v_2v_1^{\mathrm{t}}$ if and only if* $\mathrm{span}\{u_1, u_2\} = \mathrm{span}\{v_1, v_2\}$.

2. *Let $u_1, u_2, u_3 \in \mathbb{F}^n$. Suppose $u_1u_2^{\mathrm{t}} - u_2u_1^{\mathrm{t}} = \mathbf{b}_1\mathbf{b}_2^{\mathrm{t}} - \mathbf{b}_2\mathbf{b}_1^{\mathrm{t}}$, $u_1u_3^{\mathrm{t}} - u_3u_1^{\mathrm{t}} = \mathbf{b}_1\mathbf{b}_3^{\mathrm{t}} - \mathbf{b}_3\mathbf{b}_1^{\mathrm{t}}$, and $u_2u_3^{\mathrm{t}} - u_3u_2^{\mathrm{t}} = \mathbf{b}_2\mathbf{b}_3^{\mathrm{t}} - \mathbf{b}_3\mathbf{b}_2^{\mathrm{t}}$. Then there exists $\lambda \in \{1, -1\} \subseteq \mathbb{F}$, such that $u_1 = \lambda\mathbf{b}_1$, $u_2 = \lambda\mathbf{b}_2$, and $u_3 = \lambda\mathbf{b}_3$.*

3. *Let $u \in \mathbb{F}^n$, and $i \in [3, n]$. Suppose $\mathbf{b}_1u^{\mathrm{t}} - u\mathbf{b}_1^{\mathrm{t}} = \mathbf{b}_1\mathbf{b}_i^{\mathrm{t}} - \mathbf{b}_i\mathbf{b}_1^{\mathrm{t}}$ and $\mathbf{b}_2u^{\mathrm{t}} - u\mathbf{b}_2^{\mathrm{t}} = \mathbf{b}_2\mathbf{b}_i^{\mathrm{t}} - \mathbf{b}_2\mathbf{b}_1^{\mathrm{t}}$. Then $u = \mathbf{b}_i$.*

Proof. (1) is classical and can be verified easily.

For (2), we have $\mathrm{span}\{u_1, u_2\} = \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_2\}$, $\mathrm{span}\{u_1, u_3\} = \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_3\}$, and $\mathrm{span}\{u_2, u_3\} = \mathrm{span}\{\mathbf{b}_2, \mathbf{b}_3\}$ by (1). Therefore, $u_1 \in \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_2\} \cap \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_3\}$, so $u_1 = \alpha\mathbf{b}_1$. Similarly, $u_2 = \beta\mathbf{b}_2$, and $u_3 = \gamma\mathbf{b}_3$. We further note that $\alpha\beta = \beta\gamma = \alpha\gamma = 1$, which gives $\alpha = \beta = \gamma = 1$ or $\alpha = \beta = \gamma = -1$.

For (3), we have $\mathrm{span}\{\mathbf{b}_1, u\} = \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_i\}$ and $\mathrm{span}\{\mathbf{b}_2, u\} = \mathrm{span}\{\mathbf{b}_2, \mathbf{b}_i\}$ by (1). Therefore, $u \in \mathrm{span}\{\mathbf{b}_1, \mathbf{b}_i\} \cap \mathrm{span}\{\mathbf{b}_2, \mathbf{b}_i\}$ by (1). It follows that $u = \alpha\mathbf{b}_i$. Comparing the coefficients of $\mathbf{b}_1u^{\mathrm{t}} - u\mathbf{b}_1^{\mathrm{t}} = \mathbf{b}_1\mathbf{b}_i^{\mathrm{t}} - \mathbf{b}_i\mathbf{b}_1^{\mathrm{t}}$, we further have $\alpha = 1$, so $u = \mathbf{b}_i$. □

Based on Lemma 4.7, we construct $\mathbf{A}' = (A'_1, \dots, A'_m) \in \Lambda(n+3, q)^{m'}$, where $m' = m + 3 + 2 \cdot (t_1 + \cdots + t_s)$, from $\mathbf{A} = (A_1, \dots, A_m) \in \Lambda(n, q)^m$ as follows.

- For $i \in [m]$, $A'_i = \begin{bmatrix} A_i & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$.
- $A'_{m+1} = \mathbf{b}_{n+1}\mathbf{b}_{n+2}^{\mathrm{t}} - \mathbf{b}_{n+2}\mathbf{b}_{n+1}^{\mathrm{t}}$, $A'_{m+2} = \mathbf{b}_{n+1}\mathbf{b}_{n+3}^{\mathrm{t}} - \mathbf{b}_{n+3}\mathbf{b}_{n+1}^{\mathrm{t}}$, and $A'_{m+3} = \mathbf{b}_{n+2}\mathbf{b}_{n+3}^{\mathrm{t}} - \mathbf{b}_{n+2}\mathbf{b}_{n+3}^{\mathrm{t}}$.
- Suppose $i \in [n]$ satisfies $\mathbf{b}_i^{\mathrm{t}}T = \mathbf{b}_i^{\mathrm{t}}$ for any $T \in \mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$. Note that such an i belongs to an identity component in the definition of $\mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$, and there are $t_1 + \cdots + t_s$ such i. For each such i, add $\mathbf{b}_1\mathbf{b}_i^{\mathrm{t}} - \mathbf{b}_i\mathbf{b}_1^{\mathrm{t}}$ and $\mathbf{b}_1\mathbf{b}_i^{\mathrm{t}} - \mathbf{b}_i\mathbf{b}_1^{\mathrm{t}}$ to the $\mathbf{A}'$ tuple.

Proposition 4.8. *Let $\mathbf{A} \in \Lambda(n, \mathbb{F})^m$ and $\mathbf{A}' \in \Lambda(n+3, \mathbb{F})^{m'}$ be as above. Similarly construct $\mathbf{B}' \in \Lambda(n+3, \mathbb{F})^{m'}$ from $\mathbf{B} \in \Lambda(n, \mathbb{F})^m$. Then $\mathbf{A}$ and $\mathbf{B}$ are congruent under* $\mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$ *if and only if $\mathbf{A}'$ and $\mathbf{B}'$ are congruent under* $\mathrm{D}(n_1, \dots, n_s, 3, \mathbb{F})$.

Proof. The only if direction is easy to verify. For the if direction, suppose $T \in \mathrm{D}(n_1, \dots, n_s, 3, \mathbb{F})$ satisfies that $T^{\mathrm{t}}\mathbf{A}'T = \mathbf{B}'$. By the constructions of A'_{m+i} and B'_{m+i} for $i = 1, 2, 3$ and Lemma 4.7 (2), the last three rows of T are $\lambda \cdot \begin{bmatrix} \mathbf{b}_{n+1}^{\mathrm{t}} \\ \mathbf{b}_{n+2}^{\mathrm{t}} \\ \mathbf{b}_{n+3}^{\mathrm{t}} \end{bmatrix}$ where $\lambda \in \{1, -1\}$. Then by the constructions of the last $2(t_1, \dots, t_s)$ matrices in $\mathtt{A}'$ and $\mathtt{B}'$ and Lemma 4.7. (3), for every $i \in [n]$ in an identity component in the definition of $\mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$, we have the ith row of T is $\lambda \cdot \mathbf{b}_i^{\mathrm{t}}$. By multiplying λ in case it is -1, we have that $T = \begin{bmatrix} T' & \mathbf{0} \\ \mathbf{0} & I_3 \end{bmatrix}$ for some $T' \in \mathrm{DI}(n_1 : t_1, \dots, n_s : t_s, \mathbb{F})$, and this T' is a congruence matrix from $\mathtt{A}$ to $\mathtt{B}$. This concludes the proof. □

4.3.2 Solving the block-diagonal Alt-MTC problem

Our problem in this subsection is to test if $\mathtt{A}, \mathtt{B} \in \Lambda(n, q)^m$ are congruent under $\mathrm{D}(n_1, \dots, n_s, q)$. We solve this by reducing to an algorithmic problem about $*$-algebras that was solved in [IQ19]. Here we give a concise and self-contained description.

To start with, instead of finding $T \in \mathrm{D}(n_1, \dots, n_s, q)$ such that $T^{\mathrm{t}}\mathtt{A}T = \mathtt{B}$, we first compute $T, S \in \mathrm{D}(n_1, \dots, n_s, q)$ such that $T^{\mathrm{t}}\mathtt{A} = \mathtt{B}S$, if such S and T exist. This is the matrix tuple equivalence problem under $\mathrm{D}(n_1, \dots, n_s, q)$.

Proposition 4.9. *Let q be an odd prime power. To test if $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, q)^m$ are equivalent under $\mathrm{D}(n_1, \dots, n_s, q)$ can be solved in deterministic polynomial time. If $\mathbf{A}$ and $\mathbf{B}$ are equivalent, then the algorithm returns $T, S \in \mathrm{D}(n_1, \dots, n_s, q)$ such that $T^{\mathrm{t}}\mathbf{A} = \mathbf{B}S$.*

Proof. Similar to [IQ19, Proposition 3.2]. For $A_i \in \mathrm{M}(n, \mathbb{F})$, construct $\tilde{A}_i = \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \in \mathrm{M}(2n, \mathbb{F})$. Similarly construct $\tilde{B}_i$.

Then set $\tilde{A}_0 = \tilde{B}_0 = \begin{bmatrix} I_n & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. For $i \in [s]$, let $C_{n+i} = \mathrm{diag}(\mathbf{0}_{n_1}, \dots, \mathbf{0}_{n_{i-1}}, I_i, \mathbf{0}_{n_{i+1}}, \dots, \mathbf{0}_{n_s})$. Then for $i \in [s]$, set $\tilde{A}'_i = \tilde{B}'_i = \begin{bmatrix} C_{n+i} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, and $\tilde{A}''_i = \tilde{B}''_i = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & C_{n+i} \end{bmatrix} \in \mathrm{M}(2n, \mathbb{F})$. Consider $\tilde{\mathbf{A}} = (\tilde{A}_0, \tilde{A}_1, \dots, \tilde{A}_m, \tilde{A}'_1, \dots, \tilde{A}'_s, \tilde{A}''_1, \dots, \tilde{A}''_s)$ and $\tilde{\mathbf{B}} = (\tilde{B}_0, \tilde{B}_1, \dots, \tilde{B}_m, \tilde{B}'_1, \dots, \tilde{B}'_s, \tilde{B}''_1, \dots, \tilde{B}''_s) \in \mathrm{M}(2n, \mathbb{F})^{1+m+2s}$. It can be verified that $\mathbf{A}, \mathbf{B}$ are diagonal equivalent if and only if $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{B}}$ are conjugate. The latter problem is called the module isomorphism problem and can be decided in deterministic polynomial time [BL08, IKS10]. □

Note that if $\mathtt{A}$ and $\mathtt{B}$ are congruent under $\mathrm{D}(n_1, \dots, n_s, q)$, then they must be equivalent under $\mathrm{D}(n_1, \dots, n_s, q)$. In this case, Proposition 4.9 gives us $T, S \in \mathrm{D}(n_1, \dots, n_s, q)$ such that $T^{\mathrm{t}}\mathbf{A} = \mathbf{B}S$. If $S = T^{-1}$ then we are done. If not, we need the following $*$-algebra machinery for $\mathrm{D}(n_1, \dots, n_s, q)$, following [BW12, IQ19].

Some $*$-algebra background. For $\mathbf{A} \in \Lambda(n, q)^m$, define

$$\mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s) = \{T, S \in \mathrm{diag}(n_1, \dots, n_s, q) \mid T^{\mathrm{t}}\mathbf{A} = \mathbf{A}S\},$$

called the *adjoint algebra* corresponding to $\mathrm{D}(n_1, \dots, n_s, q)$. It can be verified that this is a subalgebra of $\mathrm{M}(n, q) \oplus \mathrm{M}(n, q)^{op}$.[4] Because $\mathbf{A}$ consists of alternating matrices, $\mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$ comes with an involutive anti-automorphism $*$ as follows: for $(T, S) \in \mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$, $(T, S)^* = (S, T)$.

For $\mathbf{A} \in \Lambda(n, q)^m$, let $\mathrm{RKer}(\mathbf{A}) = \{u \in \mathbb{F}^n \mid \forall A \in \mathbf{A}, Au = 0\}$. For $i \in [s]$, let $U_i = \mathrm{span}\{\mathbf{b}_i \mid i \in [n_1 + \dots + n_i + 1, n_1 + \dots + n_{i+1}]$. If for every $i \in [s]$, $\mathrm{RKer}(\mathbf{A}) \cap U_i = \mathbf{0}$, we say that $\mathbf{A}$ is diagonally non-degenerate. If $\mathbf{A}$ is diagonally degenerate, then we can obtain its non-degenerate part $\mathbf{A}' \leq \Lambda(n', q)^m$ by restricting to complement subspaces of $\mathrm{RKer}(\mathbf{A}) \cap U_i$. It is easy to show the following.

Proposition 4.10.
1. *$\mathbf{A}$ and $\mathbf{B}$ are diagonally congruent if and only if their non-degenerate parts $\mathbf{A}'$ and $\mathbf{B}'$ are diagonally congruent.*
2. *$\mathbf{A}$ is diagonally non-degenerate if and only if the projection of $\mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$ to the first component is surjective.*

Proposition 4.10 (1) allows us to focus on the non-degenerate setting, and Proposition 4.10 (2) allows us to view $\mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s) \subseteq \mathrm{M}(n, q)$ (instead of $\mathrm{M}(n, q) \oplus \mathrm{M}(n, q)^{op}$), and the $*$ operation is defined as: for $T \in \mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$, T^* is the unique $S \in \mathrm{M}(n, q)$ such that $T^{\mathrm{t}}\mathbf{A} = \mathbf{A}S$.

[4] $\mathrm{M}(n, q)^{op}$ is the opposite matrix algebra where the multiplication $\circ$ is defined as $A \circ B = BA$ where BA denotes the normal matrix multiplication.

Getting back from $*$-algebras. Recall that we obtained $T, S \in \mathrm{D}(n_1, \dots, n_s, q)$ such that $T^{\mathrm{t}}\mathbf{A} = \mathbf{B}S$. We then utilise $\mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$ as follows. Let $E = T^{-1}S^{-1}$. By the same proof of [IQ19, Claim 3.3], $E \in \mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$, and $E^* = E$. By the same proof of [IQ19, Proposition 3.4], $\mathbf{A}$ and $\mathbf{B}$ are diagonally congruent if and only if there exists $X \in \mathrm{DAdj}(\mathbf{A}, n_1, \dots, n_s)$ such that there exists $X^*X = E$. This $*$-symmetric decomposition problem admits a deterministic $\mathrm{poly}(n, m, \log q)$-time or a randomised $\mathrm{poly}(n, m, q)$-time solution over finite fields of odd characteristics [IQ19]. This then give a solution to the diagonal alternating matrix tuple congruence problem as desired.

4.4 From cuboids to cubes

Proposition 4.11. *There is a polynomial-time reduction from matrix space equivalence for n_3-dimensional matrix spaces in $\mathrm{M}(n_1 \times n_2, \mathbb{F})$ to that for n-dimensional matrix spaces in $\mathrm{M}(n, \mathbb{F})$ with $n \le \max\{n_1, n_2, n_3\}$.*

Proof. Let $\mathcal{A} \le \mathrm{M}(n_1 \times n_2, \mathbb{F})$. The left common kernel of $\mathcal{A}$ is $\mathrm{LKer}(\mathcal{A}) = \{u \in \mathbb{F}^{n_1} \mid \forall A \in \mathcal{A}, u^{\mathrm{t}}A = 0\}$. The right common kernel of $\mathcal{A}$ is $\mathrm{RKer}(\mathcal{A}) = \{u \in \mathbb{F}^{n_2} \mid \forall A \in \mathcal{A}, Au = 0\}$. We say that $\mathcal{A}$ is degenerate, if its left or right common kernel is non-trivial. Suppose $\mathcal{A} = \mathrm{span}\{A_1, \dots, A_m\}$ where $A_i \in \mathrm{M}(n_1 \times n_2, \mathbb{F})$. If $\dim(\mathrm{LKer}(\mathcal{A})) = d$ and $\dim(\mathrm{RKer}(\mathcal{A})) = e$, then let $n_1' = n_1 - d$ and $n_2' = n_2 - e$. Then there exist $L \in \mathrm{GL}(n_1, \mathbb{F})$ and $R \in \mathrm{GL}(n_2, \mathbb{F})$, such that for every $i \in [m]$, $LA_iR = \begin{bmatrix} A_i' & 0 \\ 0 & 0 \end{bmatrix}$ where $A_i' \in \mathrm{M}(n_1' \times n_2', \mathbb{F})$. We call $\mathcal{A}' = \mathrm{span}\{A_1', \dots, A_m'\} \le \mathrm{M}(n_1' \times n_2', \mathbb{F})$ the non-degenerate part of $\mathcal{A}$.

Let $\mathcal{A}, \mathcal{B}$ be two n_3-dimensional spaces in $\mathrm{M}(n_1 \times n_2, \mathbb{F})$. Clearly, for $\mathcal{A}$ and $\mathcal{B}$ to be equivalent, their left (resp. right) kernels must be of the same dimension. Therefore, if they are degenerate, we compute their non-degenerate parts $\mathcal{A}', \mathcal{B}' \le \mathrm{M}(n_1' \times n_2', \mathbb{F})$. It is easy to show that $\mathcal{A}$ and $\mathcal{B}$ are equivalent if and only if $\mathcal{A}'$ and $\mathcal{B}'$ are equivalent. We therefore assume that $\mathcal{A}$ and $\mathcal{B}$ are non-degenerate in the following.

Now let $\mathcal{A} = \mathrm{span}\{A_1, \dots, A_{n_3}\} \le \mathrm{M}(n_1 \times n_2, \mathbb{F})$. Let $\mathtt{A}$ be an $n_1 \times n_2 \times n_3$ tensor, whose frontal matrix tuple is $(A_1, \dots, A_{n_3})$. Similarly, let $\mathcal{B} = \mathrm{span}\{B_1, \dots, B_{n_3}\}$, and let $\mathtt{B}$ be an $n_1 \times n_2 \times n_3$ tensor, whose frontal matrix tuple is $(B_1, \dots, B_{n_3})$.

Suppose $n_3 = \max\{n_1, n_2, n_3\}$. Then we set $n = n_3$, set $n \times n$ matrices $A_i' = \begin{bmatrix} A_i & 0 \\ 0 & 0 \end{bmatrix}$, and consider $\mathcal{A}' = \mathrm{span}\{A_1', \dots, A_n'\}$. So $\mathcal{A}'$ is an n-dimensional matrix space in $\mathrm{M}(n, \mathbb{F})$. Similarly, do this for $\mathcal{B}$ to obtain an n-dimensional matrix space $\mathcal{B}'$ in $\mathrm{M}(n, \mathbb{F})$. Then we have that $\mathcal{A}$ and $\mathcal{B}$ are equivalent if and only if $\mathcal{A}'$ and $\mathcal{B}'$ are equivalent.

Suppose $n_1 = \max\{n_1, n_2, n_3\}$. Then we set $n = n_1$, and slice $\mathtt{A}$ along the first coordinate to get its horizontal tuple $(A_1', \dots, A_n') \in \mathrm{M}(n_2 \times n_3, \mathbb{F})^n$. Let $\mathcal{A}' = \mathrm{span}\{A_1', \dots, A_n'\} \le \mathrm{M}(n_2 \times n_3, \mathbb{F})$, and do the same for $\mathtt{B}$ to get $\mathcal{B}' \le \mathrm{M}(n_2 \times n_3, \mathbb{F})$. It is clear that $\mathcal{A}$ and $\mathcal{B}$ are equivalent if and only if $\mathcal{A}'$ and $\mathcal{B}'$ are equivalent. We can then pad 0's to make $\mathcal{A}'' \le \mathrm{M}(n, \mathbb{F})$ and $\mathcal{B}'' \le \mathrm{M}(n, \mathbb{F})$ as in the last paragraph so that $\mathcal{A}'$ and $\mathcal{B}'$ are equivalent if and only if $\mathcal{A}''$ and $\mathcal{B}''$ are equivalent.

The case of $n_2 = \max\{n_1, n_2, n_3\}$ is the same as n_1, by replacing horizontal slices with vertical slices. This concludes the proof. □

4.5 Strengthening to computing the coset of isomorphisms

Let $\mathcal{A}, \mathcal{B} \le \mathrm{M}(n, q)$. The algorithm in Section 3.5 decides whether $\mathcal{A}$ and $\mathcal{B}$ are equivalent in time $q^{\tilde{O}(n^{1.5})}$. In this section, we explain that this algorithm can be combined with results in [BW12] to compute the coset of equivalences in the same running time.

For this we need some notations. For $\mathcal{A}, \mathcal{B} \leq \mathrm{M}(n, q)$, let $\mathrm{Iso}(\mathcal{A}, \mathcal{B}) = \{(P, Q) \in \mathrm{GL}(n, q) \times \mathrm{GL}(n, q) \mid P^{\mathrm{t}}\mathcal{A}Q = \mathcal{B}\}$. Let $\mathrm{Aut}(\mathcal{A}) = \{(P, Q) \in \mathrm{GL}(n, q) \times \mathrm{GL}(n, q) \mid P^{\mathrm{t}}\mathcal{A}Q = \mathcal{A}\}$. Note that $\mathrm{Aut}(\mathcal{A})$ is a subgroup of $\mathrm{GL}(n, q) \times \mathrm{GL}(n, q)$, and $\mathrm{Iso}(\mathcal{A}, \mathcal{B})$ is a coset of $\mathrm{Aut}(\mathcal{A})$.

As customary in computing with groups, a coset C of a subgroup $H \leq G$ is represented by a coset representative and a generating set of H. The algorithm in Section 3.5 returns an equivalence in $\mathrm{Iso}(\mathcal{A}, \mathcal{B})$. To see this, we start with the fact that the algorithms for Alt-MTC [IQ19] returns an explicit congruence matrix (see [IQ19, Theorem 1.7]). Then it is routine to check that this congruence matrix as a solution to the block-diagonal Alt-MTC can be transformed to an equivalence from $\mathcal{A}$ to $\mathcal{B}$.

Therefore, the remaining task is to compute a generating set for $\mathrm{Aut}(\mathcal{A})$. This can also be done similarly as above, by running the algorithm in Section 3.5 for $\mathcal{A}$ and $\mathcal{A}$. At the bottom, we need the polynomial-time algorithms for computing a generating set of the group of congruence matrices for alternating matrix tuples in [BW12]. We then collect these at most $q^{\tilde{O}(n^{1.5})}$-many cosets, and transform them into a generating set of size at most $q^{O(n)}$ using Sims' algorithm (cf. [Ser03]). Much smaller generating sets can be obtained by e.g. more advanced algorithms dealing with matrix groups [BBS09], but this is not necessary for the purpose of this article.

5 On Frattini class 2 group isomorphism

We will first introduce the linear algebraic problem underlying testing isomorphism of p-groups of Frattini class 2, and show that this problem can be reduced to Alternating Matrix Space Isometry. We will then review the reduction from Frattini class 2 group isomorphism to this linear algebraic problem.

5.1 Inhomogeneous alternating matrix space congruence

Recall the definition of alternating matrix space congruence (Alt-MSC): given $\mathcal{A}, \mathcal{B} \leq \Lambda(n, q)$, decide if there exists $T \in \mathrm{GL}(n, q)$, such that $\mathcal{A} = T^{\mathrm{t}}\mathcal{B}T$.

We now introduce the following inhomogeneous version of Alt-MSC, called Inhomogeneous Alternating Matrix Space Congruence (Inhom-Alt-MSC), as follows. Consider $\Lambda^*(n, q) := \mathbb{F}_q^n \oplus \Lambda(n, q) = \{(v, A) \mid v \in \mathbb{F}_q^n, A \in \Lambda(n, q)\}$. Note that $\Lambda^*(n, q)$ is a linear space over $\mathbb{F}_q$ of dimension $n + \binom{n}{2}$. Then $T \in \mathrm{GL}(n, q)$ has a natural action $\circ$ on $\Lambda^*(n, q)$ by sending $(v, A) \in \Lambda^*(n, q)$ to $T \circ (v, A) := (Tv, T^{\mathrm{t}}AT)$.

Subspaces of $\Lambda^*(n, q)$ are called inhomogeneous alternating matrix spaces. For $T \in \mathrm{GL}(n, q)$ and $\mathcal{A} \leq \Lambda^*(n, q)$, let $T \circ \mathcal{A} := \{T \circ (v, A) \mid (v, A) \in \mathcal{A}\}$. Then Inhom-Alt-MSC is the problem of deciding, given $\mathcal{A}, \mathcal{B} \leq \Lambda^*(n, q)$, whether there exists $T \in \mathrm{GL}(n, q)$ such that $\mathcal{A} = T \circ \mathcal{B}$. Such such T exists, then $\mathcal{A}$ and $\mathcal{B}$ are said to be *congruent*.

We show that Inhom-Alt-MSC reduces to Alt-MSC. For this we use the following definition and result from [GQ23b].

Definition 5.1 (Block-diagonal alternating matrix space congruence, BDiag-Alt-MSC)**.** Given $\mathcal{A}, \mathcal{B} \leq \Lambda(n, q)$ and $n = n_1 + n_2$, decide if there exists $T = \mathrm{diag}(T_1, T_2) \in \mathrm{D}(n_1, n_2, q)$, such that $\mathcal{A} = T^{\mathrm{t}}\mathcal{B}T$.

Theorem 5.2 ([GQ23b])**.** *There exists a polynomial-time algorithm that, given m-dimensional $\mathcal{A}, \mathcal{B} \leq \Lambda(n, q)$ and $n = n_1 + n_2$, outputs $(m+1)$-dimensional $\mathcal{A}'$ and $\mathcal{B}' \leq \Lambda(n', q)$ with $n' = O(n)$, such that $\mathcal{A}$ and $\mathcal{B}$ are congruent by $\mathrm{D}(n_1, n_2, q)$ if and only if $\mathcal{A}'$ and $\mathcal{B}'$ are congruent by $\mathrm{GL}(n', q)$.*

Note that Theorem 5.2 is about matrix space congruence, not the matrix tuple congruence as discussed in Section 4.3.

We can then formulate Inhom-Alt-MSC as an instance of BDiag-Alt-MSC but with a further restriction. Let $\mathcal{A} \leq \Lambda^*(n, q)$, and suppose $(v_1, A_1), \ldots, (v_m, A_m)$ form a linear basis of $\mathcal{A}$. Then for $i \in [m]$, construct $\tilde{A}_i = \begin{bmatrix} A_i & v_i \\ -v_i^t & 0 \end{bmatrix}$, and let $\tilde{\mathcal{A}} = \text{span}\{\tilde{A}_1, \ldots, \tilde{A}_m\} \leq \Lambda(n+1, q)$. Similarly, starting from $\mathcal{B} \leq \Lambda^*(n, q)$, construct $\tilde{\mathcal{B}} \leq \Lambda(n+1, q)$ in the same way. The following lemma is easy, so we omit its proof.

Lemma 5.3. *Let $\mathcal{A}, \mathcal{B} \leq \Lambda^*(n, q)$ and $\tilde{\mathcal{A}}, \tilde{\mathcal{B}} \leq \Lambda(n+1, q)$ be as above. Then $\mathcal{A}$ and $\mathcal{B}$ are congruent if and only if $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ are congruent by some $T = \begin{bmatrix} T' & 0 \\ 0 & 1 \end{bmatrix} \in \text{GL}(n+1, q)$ where $T' \in \text{GL}(n, q)$.*

We can state the main result in this subsection as follows.

Proposition 5.4. Inhom-Alt-MSC *for m-dimensional $\mathcal{A}, \mathcal{B} \leq \Lambda^*(n, q)$ can be solved in time $q^{\tilde{O}((n+m)^{1.5})}$.*

Proof. Given $\mathcal{A}, \mathcal{B} \leq \Lambda^*(n, q)$, construct m-dimensional $\tilde{\mathcal{A}}, \tilde{\mathcal{B}} \leq \Lambda(n+1, q)$ as in Lemma 5.3. Then construct $(m+1)$-dimensional $\tilde{\mathcal{A}}', \tilde{\mathcal{B}}' \leq \Lambda(n', q)$ using Theorem 5.2, with the block sizes being $n_1 = n$ and $n_2 = 1$.

By Lemma 5.3, $\mathcal{A}$ and $\mathcal{B}$ are congruent if and only if $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ are congruent by

$$T = \begin{bmatrix} T' & 0 \\ 0 & 1 \end{bmatrix} \in \text{GL}(n+1, q) \tag{5}$$

where $T' \in \text{GL}(n, q)$.

By Theorem 5.2, we have $\tilde{\mathcal{A}}'$ and $\tilde{\mathcal{B}}'$ are congruent if and only if $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ are congruent by $S = \begin{bmatrix} S' & 0 \\ 0 & \lambda \end{bmatrix} \in \text{GL}(n+1, q)$ where $S' \in \text{GL}(n, q)$.

The difference between λ in the lower-right corner of S, and 1 in the lower-right corner of T, is what we need to overcome now. For this, we use the observation that the coset of congruence matrices can be computed for $\tilde{\mathcal{A}}'$ and $\tilde{\mathcal{B}}'$ (see Section 4.5). As the reduction in Theorem 5.2 also allows for translating cosets from one solution to another [GQ23b], this then gives us a congruence matrix $S = \begin{bmatrix} S' & 0 \\ 0 & \lambda \end{bmatrix}$ from $\tilde{\mathcal{A}}$ to $\tilde{\mathcal{B}}$, and a generate set for the group $\text{Aut}(\tilde{\mathcal{A}}) := \{R = \begin{bmatrix} R' & 0 \\ 0 & \gamma \end{bmatrix} \mid R^{\text{t}} \tilde{\mathcal{A}} R = \mathcal{A}\}$. Let $\text{Aut}_1(\tilde{\mathcal{A}}) = \{\gamma \mid \exists R' \in \text{GL}(n, q), \text{diag}(R', \gamma) \in \text{Aut}(\tilde{\mathcal{A}})\}$, which is a subgroup of $\mathbb{F}_q^\times$, the multiplicative group of $\mathbb{F}_q$. Note that a generating set for $\text{Aut}_1(\tilde{\mathcal{A}})$ can be easily obtained from a generating set for $\text{Aut}(\tilde{\mathcal{A}})$ by restricting to the lower-right corner entries. The question of the existence of T as in Equation 5 becomes to decide if λ^{-1} is in $\text{Aut}_1(\tilde{\mathcal{A}})$. This is solvable easily in time $O(q)$ as we can list elements in $\text{Aut}_1(\tilde{\mathcal{A}})$ in this time bound.

This concludes the proof. □

5.2 Testing isomorphism of p-groups of Frattini class 2

We collect some basic facts about p-groups of Frattini class 2, which are mostly from [BNV07].

Let G be a group. The Frattini subgroup $\Phi(G)$ of G is the characteristic subgroup defined as the intersection of maximal subgroups of G.

If G is a p-group, then $G/\Phi(G)$ is elementary abelian, and $\Phi(G) = G^p[G, G]$ where G^p is the subgroup generated by $\{x^p \mid x \in G\}$ [BNV07, Lemma 3.12]. In particular, $\Phi(G)$ is generated by x^p and $[x, y]$ for $x, y \in G$. These lead to the following.

Proposition 5.5. *Let G be a p-group given by its Cayley table. Then there exist a polynomial-time algorithm to compute $\Phi(G)$.*

A p-group G is of Frattini class 2 (or Φ class 2 for short), if there exists $H \le G$, such that H is central, and both H and G/H are elementary abelian, or equivalently, if $\Phi(G)$ is elementary abelian and is contained in $Z(G)$. These lead to the following.

Proposition 5.6. *Let G be a p-group given by its Cayley table. Then there exist a polynomial-time algorithm to decide if G is of Frattini class 2.*

The free p-group of Φ class 2 with n generators, denoted by $F_{\Phi\text{-}2,p,n}$, is the quotient of the free group F_n with n generators by the relations x^{p^2}, $[x,y]^p$, and $[x,y,z]$.

Let G be a p-group of Frattini class 2. Suppose $G/\Phi(G) \cong \mathbb{Z}_p^n$. As $\Phi(G) = G^p[G,G]$ and it is elementary abelian, $\Phi(G) \le \mathbb{Z}_p^n \oplus \Lambda(n,p)$.

Proposition 5.7. *Let G be a p-group of Frattini class 2, given by its Cayley table. Then there exist a polynomial-time algorithm to compute an isomorphism from $\Phi(G)$ to a subgroup of $\mathbb{Z}_p^n \oplus \Lambda(n,p)$.*

Proof. First, compute $\Phi(G)$ via Proposition 5.5. Suppose that $G/\Phi(G) \cong \mathbb{Z}_p^n$ and $\Phi(G) \cong \mathbb{Z}_p^m$. Let $g_1, \dots, g_n$ be a set of group elements such that g_iG generate $G/\Phi(G)$. Let $h_1, \dots, h_m$ be a set of generators of $\Phi(G)$. View h_i as a linear basis of $\mathbb{Z}_p^m$, we can compute g_i^p, $[g_i, g_j]$ as vectors in $\mathbb{Z}_p^m$. This gives us an $m \times (n + \binom{n}{2})$ matrix S over $\mathbb{F}_p$. It can be seen that the rows of S gives a subgroup of $\mathbb{Z}_p^n \oplus \Lambda(n,p)$, to which $\Phi(G)$ is naturally isomorphic. □

Let $T \in \mathrm{Aut}(G/\Phi(G)) \cong \mathrm{GL}(n,p)$. Then the induced action of T on $\Phi(G)$ sends $(v, A) \in \mathbb{Z}_p^n \oplus \Lambda(n,p)$ to $(Tv, T^{\mathrm{t}}AT)$.

Suppose G_1, G_2 are two p-groups of Frattini class 2, with $G_i/\Phi(G_i) \cong \mathbb{Z}_p^n$ for $i = 1, 2$. Furthermore, suppose $\Phi(G_1)$ and $\Phi(G_2)$ are identified as subspaces of $\mathbb{Z}_p^n \oplus \Lambda(n,p)$ by Proposition 5.7. Then G_1 and G_2 are isomorphic, if and only if there exists $T \in \mathrm{GL}(n,p)$ such that T sends $\Phi(G_1)$ to $\Phi(G_2)$ as subspaces. This follows from [BNV07, Lemma 4.3], viewing $\Phi(G_i)$ as the dual space of the subspace in the quotient of the free p-group of Φ class 2 with n generators.

Based on the above, we have the following.

Lemma 5.8. *Suppose G_1, G_2 are two p-groups of Frattini class 2 of order p^ℓ, given by their Cayley tables. Then we can construct two inhomogeneous alternating matrix spaces $\mathcal{A}_1, \mathcal{A}_2$ of length ℓ, such that $G_1 \cong G_2$ if and only if $\mathcal{A}_1$ and $\mathcal{A}_2$ are congruent as inhomogeneous alternating matrix spaces.*

Theorem 1.3 is then obtained by combining Lemma 5.8 with Proposition 5.4.

Acknowledgement. G. I. is supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Artificial Intelligence National Laboratory Program. E. M. is supported by SQA/CSIRO scholarship stipend and training allowance. Y. Q. is partly supported by Australian Research Council DP200100950 and LP220100332. X. S. is supported by the National Science Foundation (NSF) under Grant No. 2240024. C. Z. is supported by by the Australian Research Council DP200100950 and LP220100332 and the Sydney Quantum Academy, Sydney, NSW, Australia.

References

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

[BBS09] László Babai, Robert Beals, and Ákos Seress. Polynomial-time theory of matrix groups. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 55–64, 2009. doi:10.1145/1536414.1536425.

[BKW24] Peter A. Brooksbank, Martin Kassabov, and James B. Wilson. Intersecting classical groups in polynomial time, 2024. In preparation.

[BL08] Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020 – 4029, 2008. URL: http://www.sciencedirect.com/science/article/pii/S0021869308003748, doi:10.1016/j.jalgebra.2008.07.014.

[BNV07] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman. *Enumeration of finite groups*. Cambridge Univ. Press, 2007.

[BW12] Peter A. Brooksbank and James B. Wilson. Computing isometry groups of Hermitian maps. *Trans. Amer. Math. Soc.*, 364:1975–1996, 2012. doi:10.1090/S0002-9947-2011-05388-2.

[Coh75] P. M. Cohn. The word problem for free fields: A correction and an addendum. *J. Symbolic Logic*, 40(1):69–74, 03 1975. URL: http://projecteuclid.org/euclid.jsl/1183739310.

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

[FR04] M. Fortin and C. Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Séminaire Lotharingien de Combinatoire*, 52:B52f, 2004.

[GGdOW20] Ankit Garg, Leonid Gurvits, Rafael Mendes de Oliveira, and Avi Wigderson. Operator scaling: Theory and applications. *Found. Comput. Math.*, 20(2):223–290, 2020. URL: https://doi.org/10.1007/s10208-019-09417-z, doi:10.1007/s10208-019-09417-z.

[GQ17] Joshua A. Grochow and Youming Qiao. Algorithms for group isomorphism via group extensions and cohomology. *SIAM J. Comput.*, 46(4):1153–1216, 2017. Preliminary version in IEEE Conference on Computational Complexity (CCC) 2014 (DOI:10.1109/CCC.2014.19). Also available as arXiv:1309.1776 [cs.DS] and ECCC Technical Report TR13-123. doi:10.1137/15M1009767.

[GQ23a] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. *SIAM J. Comput.*, 52(2):568–617, 2023. Extended abstract appeared in ITCS '21. URL: https://doi.org/10.1137/21m1441110, doi:10.1137/21M1441110.

[GQ23b] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials IV: linear-length reductions and their applications. *CoRR*, abs/2306.16317, 2023. Version 2. arXiv:2306.16317.

[GQ24] Joshua A. Grochow and Youming Qiao. On p-group isomorphism: Search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. *ACM Trans. Comput. Theory*, 16(1):2:1–2:39, 2024. doi:10.1145/3625308.

[HH21] Masaki Hamada and Hiroshi Hirai. Computing the nc-rank via discrete convex optimization on cat (0) spaces. *SIAM Journal on Applied Algebra and Geometry*, 5(3):455–478, 2021.

[Hig60] Graham Higman. Enumerating p-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960. doi:10.1112/plms/s3-10.1.24.

[HW15] Pavel Hrubeš and Avi Wigderson. Non-commutative arithmetic circuits with division. *Theory of Computing*, 11:357–393, 2015. URL: http://dx.doi.org/10.4086/toc.2015.v011a014, doi:10.4086/toc.2015.v011a014.

[IKS10] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010. URL: http://dx.doi.org/10.1137/090781231, doi:10.1137/090781231.

[IMQ22] Gábor Ivanyos, Tushant Mittal, and Youming Qiao. Symbolic determinant identity testing and non-commutative ranks of matrix lie algebras. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 87:1–87:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. URL: https://doi.org/10.4230/LIPIcs.ITCS.2022.87, doi:10.4230/LIPICS.ITCS.2022.87.

[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. doi:10.1137/18M1165682.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complex.*, 27(4):561–593, 2018. URL: https://doi.org/10.1007/s00037-018-0165-7, doi:10.1007/S00037-018-0165-7.

[LQ17] Yinan Li and Youming Qiao. Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 463–474. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.49.

[Mal63] Anatolii Ivanovich Mal'tsev. *Foundations of linear algebra.* WH Freeman, 1963.

[Mil78] Gary L. Miller. On the $n^{\log n}$ isomorphism technique (a preliminary report). In *STOC*, pages 51–58, New York, NY, USA, 1978. ACM. doi:http://doi.acm.org/10.1145/800133.804331.

[Mul17] Ketan Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *Journal of the American Mathematical Society*, 30(1):225–309, 2017.

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

[Ser03] Ákos Seress. *Permutation group algorithms*, volume 152. Cambridge University Press, 2003.

[Sun23] Xiaorui Sun. Faster isomorphism for p-groups of class 2 and exponent p. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 433–440. ACM, 2023. `doi:10.1145/3564246.3585250`.