PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

GROUP-THEORETIC GENERALISATIONS OF VERTEX AND EDGE CONNECTIVITIES

YINAN LI AND YOUMING QIAO

ABSTRACT. Let p be an odd prime. Let P be a finite p-group of class 2 and exponent p, whose commutator quotient $P/[P,P]$ is of order p^n. We define two parameters for P related to central decompositions. The first parameter, $\kappa(P)$, is the smallest integer s for the existence of a subgroup S of P satisfying (1) $S\cap[P,P]=[S,S]$, (2) $|S/[S,S]|=p^{n-s}$, and (3) S is centrally decomposable. The second parameter, $\lambda(P)$, is the smallest integer s for the existence of a central subgroup N of order p^s, such that P/N is centrally decomposable.

While defined in purely group-theoretic terms, these two parameters generalise respectively the vertex and edge connectivities of graphs: For a simple undirected graph G, through the classical procedures of Baer (Trans. Am. Math. Soc., 1938), Tutte (J. Lond. Math. Soc., 1947) and Lovász (B. Braz. Math. Soc., 1989), there is a p-group P_G of class 2 and exponent p that is naturally associated with G. Our main results show that the vertex connectivity $\kappa(G)$ equals $\kappa(P_G)$, and the edge connectivity $\lambda(G)$ equals $\lambda(P_G)$.

We also discuss the relation between $\kappa(P)$ and $\lambda(P)$ for a general p-group P of class 2 and exponent p, as well as the computational aspects of these parameters. In particular, our main results imply that the p-group central decomposition algorithm of Wilson (J. Algebra & J. of Group Theory, 2009) can be used to solve the graph connectivity problem.

Keywords: p-groups of class 2, graph connectivity, matrix spaces, bilinear maps

1. INTRODUCTION

The main purpose of this paper is to define and explore two natural group-theoretic parameters, which are closely related to vertex and edge connectivities in graphs. Since vertex and edge connectivities have been classical and central notions in graph theory [23], we expect that this connection can serve as another opportunity for a fruitful interaction between graph theory and group theory.

We first introduce a method to relate graphs with p-groups of class 2 and exponent p through Baer's correspondence [3] and the works of Tutte [22] and Lovász [16]. We then define two group-theoretic parameters. Our main result shows that the vertex and edge connectivities of a graph are equal to the two parameters we defined on the corresponding group respectively. We then compare the two parameters and discuss their computational feasibility.

2010 *Mathematics Subject Classification.* Primary 20D15, 05C40, 15A69.

Key words and phrases. p-groups of class 2, graph connectivity, matrix spaces, bilinear maps.

The authors thank the anonymous reviewers for their thoughtful feedback and useful references. Yinan Li is partially supported by ERC Consolidator Grant 615307-QPROGRESS. Youming Qiao is partially supported by the Australian Research Council DP200100950.

Since our main goal is to set up a link between graph theory and group theory, we shall include certain background information, despite that it is well-known to researchers in the respective areas.

1.1. **From graphs to groups: the Baer-Lovász-Tutte procedure.** One route from graphs to groups, following Baer [3], Tutte [22], and Lovász [16], goes via linear spaces of alternating matrices and alternating bilinear maps. While there are other related methods of constructing groups from graphs [9, 18], we follow this one here, as the perspectives from [3, 16, 22] are most relevant to our work (see Section 1.3 for details).

We set up some notation. For $n \in \mathbb{N}$, let $[n] := \{1, \dots, n\}$. Let $\binom{[n]}{2}$ be the set of size-2 subsets of $[n]$. We use $\mathbb{F}$ to denote a field, and $\mathbb{F}_q$ to denote the finite field with q elements. Vectors in $\mathbb{F}^n$ are column vectors, and $\langle \cdot \rangle$ denotes the linear span over $\mathbb{F}$. Let $\Lambda(n, \mathbb{F})$ be the linear space of $n \times n$ alternating matrices over $\mathbb{F}$. Recall that an $n \times n$ matrix A over $\mathbb{F}$ is alternating if for any $v \in \mathbb{F}^n$, $v^t A v = 0$. That is, A represents an alternating bilinear form. Subspaces $\mathcal{A}$ of $\Lambda(n, \mathbb{F})$, denoted by $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, are called alternating matrix spaces. Fix a field $\mathbb{F}$. For $\{i, j\} \in \binom{[n]}{2}$ with $i < j$, the elementary alternating matrix $A_{i,j}$ over $\mathbb{F}$ is the matrix with the (i, j)th entry being 1, the (j, i)th entry being -1, and the rest entries being 0.

In this paper, we only consider non-empty, simple, and undirected graphs with the vertex set being $[n]$. That is, a graph is $G = ([n], E)$ where $E \subseteq \binom{[n]}{2}$. Let $|E| = m$. Note that the non-empty condition implies that $n \geq 2$ and $m \geq 1$.

Let p be an odd prime. We use $\mathfrak{B}_{p,2}$ to denote the class of non-abelian p-groups of class 2 and exponent p. That is, a non-abelian group P is in $\mathfrak{B}_{p,2}$, if for any $g \in P$, $g^p = 1$, and the commutator subgroup $[P, P]$ is contained in the centre $\mathrm{Z}(P)$. For $P \in \mathfrak{B}_{p,2}$, $[P, P]$ is elementary abelian and also the Frattini subgroup. For $n, m \in \mathbb{N}$, we further define $\mathfrak{B}_{p,2}(n, m) \subseteq \mathfrak{B}_{p,2}$, which consists of those $P \in \mathfrak{B}_{p,2}$ with $|P/[P, P]| = p^n$ and $|[P, P]| = p^m$. Note that the non-abelian condition implies that $n \geq 2$ and $m \geq 1$ are required for $\mathfrak{B}_{p,2}(n, m)$ to be non-empty.

We then explain the procedure from graphs to groups in $\mathfrak{B}_{p,2}$ following Baer, Tutte and Lovász.

(1) Let $G = ([n], E)$ be a simple and undirected graph with m edges. Following Tutte [22] and Lovász [16], we construct from G an m-dimensional alternating matrix space

$$\mathcal{A}_G = \langle A_{i,j} : \{i, j\} \in E \rangle \leq \Lambda(n, \mathbb{F}). \tag{1.1}$$

(2) Given an m-dimensional $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, let $\mathbf{A} = (A_1, \dots, A_m) \in \Lambda(n, \mathbb{F})^m$ be an ordered basis of $\mathcal{A}$. The alternating bilinear map defined by $\mathbf{A}$, $\phi_{\mathbf{A}} : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$, is

$$\phi_{\mathbf{A}}(v, u) = (v^t A_1 u, \dots, v^t A_m u)^t. \tag{1.2}$$

Since $\mathcal{A}$ is of dimension m, we have that $\phi_{\mathbf{A}}(\mathbb{F}^n, \mathbb{F}^n) = \mathbb{F}^m$.

(3) Let p be an odd prime. Let $\phi : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ be an alternating bilinear map, such that $\phi(\mathbb{F}_p^n, \mathbb{F}_p^n) = \mathbb{F}_p^m$. Following Baer [3], we define a p-group, $P_\phi \in \mathfrak{B}_{p,2}(n, m)$, as follows. The group elements are from the set $\mathbb{F}_p^n \times \mathbb{F}_p^m$. For $(v_i, u_i) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$, $i = 1, 2$, the group product $\circ$ is defined as

$$(v_1, u_1) \circ (v_2, u_2) := (v_1 + v_2, u_1 + u_2 + \frac{1}{2} \cdot \phi(v_1, v_2)). \tag{1.3}$$

It can be verified that $P_\phi \in \mathfrak{B}_{p,2}(n,m)$, because of the condition that $\phi(\mathbb{F}_p^n, \mathbb{F}_p^n) = \mathbb{F}_p^m$.

Definition 1.1 (The Baer-Lovász-Tutte procedure)**.** Let $G = ([n], E)$ be an undirected simple graph with $|E| = m > 0$. The Baer-Lovász-Tutte procedure, as specified in the above three steps, takes G and a prime $p > 2$, and produces a p-group of class 2 and exponent p, $P_G \in \mathfrak{B}_{p,2}(n,m)$.

The above construction can be easily adjusted to accommodate graphs with arbitrary vertex sets and without imposing certain total orders on the vertex set. We can actually go from a graph to an alternating bilinear map directly, without going through alternating matrix spaces. We can also generalise the above construction to be over a ring R (in which 2 is a unit) instead over a field $\mathbb{F}$, so when $R = \mathbb{Z}$, it gives a finitely generated torsion-free nilpotent group. See [20, Sec. 3.4] and [8, Sec. 3] for descriptions covering some of the points above.

We adopt the current description to ease the presentation, and to make the links more transparent. Indeed, as reflected in the literature (see Section 1.3), graphs are naturally related to alternating matrix spaces, and p-groups of class 2 and exponent p are naturally associated with alternating bilinear maps. So we think it helpful to describe these two intermediate objects explicitly, despite that the link between alternating matrix spaces and alternating bilinear maps is routine.

The Baer-Lovász-Tutte construction also has the following intriguing property. If two graphs G_1 and G_2 are isomorphic, then the corresponding p-groups P_{G_1} and P_{G_2} are easily seen to be isomorphic. Interestingly, in [8] it is shown that the converse direction also holds. The authors of [8] further define a homomorphism notion of graphs, so that the Baer-Lovász-Tutte procedure leads to a functor from this category of graphs to the category of groups.

1.2. **Our results.** Let H be a finite group. We use $J \leq H$ to denote that J is a subgroup of H, and $J < H$ to denote that J is a proper subgroup of H. For $S, T \subseteq H$, $ST = \{st : s \in S, t \in T\}$. If $J, K \leq H$ satisfy that $JK = KJ$, then JK is a subgroup of H.

Recall that H is a central product of two subgroups J and K, if (1) every element of J commutes with every element of K, i.e. $[J, K] = 1$, (2) H is generated by J and K, i.e. $H = JK$, and (3) $H \neq J$ and $H \neq K$; cf. [21, pp. 137] and [25, Sec. 2.1]. If such J and K exist, then we say that H is centrally decomposable.

Definition 1.2 (κ and λ for p-groups of class 2 and exponent p)**.** Let $P \in \mathfrak{B}_{p,2}(n,m)$. A subgroup $S \leq P$ is regular with respect to commutation, or simply regular for short, if $[S, S] = S \cap [P, P]$.

The regular-subgroup central-decomposition number of P, denoted by $\kappa(P)$, is the smallest $s \in \mathbb{N}$ for the existence of a regular subgroup S with $|S/[S, S]| = p^{n-s}$, such that S is centrally decomposable.

The central-quotient central-decomposition number of P, denoted as $\lambda(P)$, is the smallest $s \in \mathbb{N}$ for the existence of a central subgroup N of order p^s, such that P/N is centrally decomposable.

Note that we use the letters κ and λ to follow the conventions in graph theory, as the reader will see below soon. An explanation for imposing the regularity condition in the definition of $\kappa(P)$ can be found in Remark 2.10. In the definition of $\lambda(P)$, we can actually restrict N to be from those central subgroups contained in $[P, P]$ (cf. Observation 2.8 (2)).

Recall that for a graph G, the vertex connectivity $\kappa(G)$ denotes the smallest number of vertices needed to remove in order that G becomes disconnected, and the edge connectivity $\lambda(G)$ denotes the smallest number of edges needed to remove in order that G becomes disconnected [7]. These are classical notions in graph theory (cf. e.g. [23]).

Let $P \in \mathfrak{B}_{p,2}(n,m)$, and let G be a graph with n vertices and m edges. We defined λ and κ for P and G. On the one hand, $\lambda(P)$ is defined with respect to all regular subgroups of P, the number of which is at least $p^{\frac{1}{4}n^2+\Omega(n)}$, the number of subgroups of $\mathbb{Z}_p^n$. On the other hand, $\lambda(G)$ is defined with respect to all subsets of vertices, the number of which is at most 2^n. Similarly, there is also a large gap between the numbers of those objects supporting the definitions of κ for P and G. Such differences may prompt one to think that $\lambda(P)$ and $\lambda(G)$, as well as $\kappa(P)$ and $\kappa(G)$, could behave quite differently. Surprisingly, our main result suggests that when restricting to those groups constructed from graphs via the Baer-Lovász-Tutte procedure, these parameters are actually the same.

Theorem 1.3. *For an n-vertex and m-edge graph G, let $P_G \in \mathfrak{B}_{p,2}(n,m)$ be the result of applying the Baer-Lovász-Tutte procedure to G and a prime $p > 2$. Then $\kappa(G) = \kappa(P_G)$, and $\lambda(G) = \lambda(P_G)$.*

Theorem 1.3 then sets up a surprising link between group theory and graph theory. For example, as a consequence of Theorem 1.3 in the case of $\kappa(P_G) = \lambda(P_G) = 0$, we note that Wilson's central decomposition algorithm for p-groups of class 2 [25, 26] can be used to solve the connectivity problem of graphs. While an overkill for such a basic problem on graphs, we believe it is an interesting instance of using algorithms developed for groups to solve graph-theoretic problems.

To understand these two parameters and their relation better, we consider the following question. Recall that for a graph G, it is well-known that $\kappa(G) \leq \lambda(G) \leq \delta(G)$, where $\delta(G)$ denotes the minimum degree of vertices in G (cf. e.g. [7, Proposition 1.4.2]). We study a question of the same type in the context of p-groups of class 2 and exponent p. For this we need the following definition.

Definition 1.4 (Degrees and δ for p-groups of class 2 and exponent p)**.** For $P \in \mathfrak{B}_{p,2}(n,m)$ and $g \in P$, suppose $C_P(g) = \{h \in P : [h,g] = 1\}$ is of order p^d. Then the degree of g is $\deg(g) = n + m - d$. The minimum degree of P, $\delta(P)$, is the minimum degree over $g \in P \setminus [P,P]$.

The degrees of elements of P are not to be confused with the degrees of the characters of P. This notion is closely related to the breadth notion defined for Lie algebras (cf. e.g. [17, 24]): for an element in a finite dimensional Lie algebra, its breadth is defined as the codimension of its centraliser. In particular, $\deg(g)$ is exactly the breadth of g in the associated graded Lie algebra of P.

It is easy to see that for any $g \in P$, $\deg(g) \leq n - 1$ (cf. Observation 2.8 (3)). Therefore $\delta(P) \leq n - 1$. We then have the following.

Proposition 1.5.
(1) *For any $P \in \mathfrak{B}_{p,2}$, $\kappa(P) \leq \delta(P)$, and $\lambda(P) \leq \delta(P)$.*
(2) *There exists $P \in \mathfrak{B}_{p,2}$, such that $\kappa(P) > \lambda(P)$.*

That is, while we can still upper bound $\kappa(P)$ and $\delta(P)$ using a certain minimum degree notion, the inequality $\kappa \leq \lambda$ does not hold in general in the p-group setting.

1.3. **Related works and open ends.** There are at least two known constructions of p-groups of class 2 from graphs. In [9], Heineken and Liebeck constructed p-groups of class 2 and exponent p^2 from directed graphs. Another natural construction, known as Mekler's construction [18] in model theory (cf. e.g. [11]), is as follows. Take a graph G on a vertex set V, and construct the p-group of class 2 and exponent p generated by V, with the relations $[v, v']$ added for edges $\{v, v'\}$ in G. Mekler's construction is essentially the same as the Baer-Lovász-Tutte construction applied to the complement graph of G, and is indeed easier to describe. We stick to the Baer-Lovász-Tutte construction, because it is the perspectives in their works [3, 15, 22] that lead to the present note, as we explain now.

1.3.1. *Related works: graphs and alternating matrix spaces.* The link between graphs and alternating matrix spaces dates back to the works of Tutte and Lovász [16,22] in the context of perfect matchings. Let $G = ([n], E)$ be a graph, and let $\mathcal{A}_G \leq \Lambda(n, \mathbb{F})$ be the alternating matrix space associated with G as in Step (1). Tutte and Lovász realised that the matching number of G, $\mu(G)$, is equal to one half of the maximum rank over matrices in $\mathcal{A}_G$.[1] More specifically, Tutte represented G as a symbolic matrix: A matrix whose entries are either variables or 0 [22]. It can be naturally interpreted as a linear space of matrices, and Lovász then more systematically studied Tutte's construction from this perspective [16].

Recently in [4], the second author and collaborators showed that the independence number of G equals the maximum dimension over the totally isotropic spaces[2] of $\mathcal{A}_G$. They also showed that the chromatic number of G equals the minimum c such that there exists a direct-sum decomposition of $\mathbb{F}^n$ into c non-trivial totally isotropic spaces of $\mathcal{A}_G$. As the reader will see below, the proof of Theorem 1.3 also goes by defining appropriate parameters κ and λ for alternating matrix spaces, and proving that $\kappa(\mathcal{A}_G) = \kappa(G)$ and $\lambda(\mathcal{A}_G) = \lambda(G)$. This translates another two graph-theoretic parameters to the alternating matrix space setting.

The work most relevant to the current note in this direction is [14] by the present authors. In that work, we adapted a combinatorial technique for the graph isomorphism problem by Babai, Erdős, and Selkow [2], to tackle isomorphism testing of groups from $\mathfrak{B}_{p,2}$, via alternating matrix spaces. This leads to the definition of a "cut" for alternating matrix spaces, which in turn naturally leads to the edge connectivity notion; cf. the proof of Proposition 2.5.

1.3.2. *Related works: alternating bilinear maps and p-groups of class 2 and exponent p.* The link between alternating bilinear maps and $\mathfrak{B}_{p,2}$ dates back to the work of Baer [3]. That is, from an alternating bilinear map ϕ, we can construct a group P_ϕ in $\mathfrak{B}_{p,2}$ as in Step (3). On the other hand, given $P \in \mathfrak{B}_{p,2}(n, m)$, by taking the commutator bracket we obtain an alternating bilinear map ϕ_P. A generalisation of this link to p-groups of Frattini class 2 was crucial in Higman's enumeration of p-groups [10]. Alperin [1], Ol'shanskii [19] and Buhler, Gupta, and Harris [5] used this link to study large abelian subgroups of p-groups, a question first considered by Burnside [6]. This is because abelian subgroups of P containing $[P, P]$ correspond to totally isotropic spaces of ϕ_P.

[1] This is straightforward if the underlying field $\mathbb{F}$ is large enough. If $|\mathbb{F}|$ is small, it follows e.g. as a consequence of the linear matroid parity theorem; cf. the discussion after [16, Theorem 4].

[2] A subspace $U \leq \mathbb{F}^n$ is totally isotropic for $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, if $\forall u, u' \in U$, and $\forall A \in \mathcal{A}$, $u^t A u' = 0$.

The work most relevant to the current note in this direction are [25,26] by James B. Wilson. He studied central decompositions of P via the link between alternating bilinear maps and $\mathfrak{B}_{p,2}$. In particular, he utilised that central decompositions of P correspond to orthogonal decompositions of ϕ_P.

Finally, we recently learnt of the work [20] of Rossmann and Voll, who study those p-groups of class 2 and exponent p obtained from graphs through the Baer-Lovász-Tutte procedure in the context of zeta functions of groups.

1.3.3. *Open ends.* The most interesting questions to us are the computational aspects of these parameters. That is, given the linear basis of an alternating matrix space $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, compute $\kappa(\mathcal{A})$ and $\lambda(\mathcal{A})$ (see Definition 2.1). When $\mathbb{F} = \mathbb{F}_q$ with q odd, there is a randomised polynomial-time algorithm to decide whether $\kappa(\mathcal{A}) = \lambda(\mathcal{A}) = 0$ by Wilson [26]. When $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$, by utilising certain machineries from [12], Wilson's algorithm can be adapted to yield a deterministic polynomial-time algorithm to decide whether $\kappa(\mathcal{A}) = \lambda(\mathcal{A}) = 0$. However, to directly use Wilson's algorithm to compute $\kappa(\mathcal{A})$ or $\lambda(\mathcal{A})$ seems difficult, as when $\kappa(\mathcal{A}) = \lambda(\mathcal{A}) = 0$, a non-trivial orthogonal decomposition can be nicely translated to a certain idempotent in an involutive algebra associated with any linear basis of $\mathcal{A}$; for details, see [26].

2. Proofs

2.1. **Preparations.** Some notation has been introduced at the beginning of sections 1.1 and 1.2. We add some more here. For a field $\mathbb{F}$ and $d_1, d_2 \in \mathbb{N}$, we use $\mathrm{M}(d_1 \times d_2, \mathbb{F})$ to denote the linear space of $d_1 \times d_2$ matrices over $\mathbb{F}$, and $\mathrm{M}(d, \mathbb{F}) := \mathrm{M}(d \times d, \mathbb{F})$. The ith standard basis vector of $\mathbb{F}^n$ is denoted by e_i.

2.1.1. *Some notions for alternating matrix spaces.* We introduce some basic concepts, and then define κ and λ, for alternating matrix spaces. Let $\mathcal{A}, \mathcal{B} \leq \Lambda(n, \mathbb{F})$. We say that $\mathcal{A}$ and $\mathcal{B}$ are isometric, if there exists $T \in \mathrm{GL}(n, \mathbb{F})$, such that $\mathcal{A} = T^t \mathcal{B} T := \{T^t B T : B \in \mathcal{B}\}$. For a d-dimensional $W \leq \mathbb{F}^n$, let T be an $n \times d$ matrix whose columns span W. Then the restriction of $\mathcal{A}$ to W via T is $\mathcal{A}|_{W,T} := \{T^t A T : A \in \mathcal{A}\} \leq \Lambda(d, \mathbb{F})$. For a different $n \times d$ matrix T' whose columns also span W, $\mathcal{A}|_{W,T'}$ is isometric to $\mathcal{A}|_{W,T}$. So we can write $\mathcal{A}|_W$ to indicate a restriction of $\mathcal{A}$ to W via some such T.

Let $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ be of dimension m. We define an orthogonal decomposition of $\mathcal{A}$ to be a direct-sum decomposition of $\mathbb{F}^n$ into $U \oplus V$, such that (1) for any $u \in U$, $v \in V$, and $A \in \mathcal{A}$, $u^t A v = 0$, and (2) neither U nor V equals $\mathbb{F}^n$. If $\mathcal{A}$ has such an orthogonal decomposition, then $\mathcal{A}$ is called orthogonally decomposable.

When $n = 1$, we define $\Lambda(1, \mathbb{F})$ to be orthogonally decomposable. Indeed, a graph with a single vertex is sometimes regarded as disconnected according to [7, pp. 12].

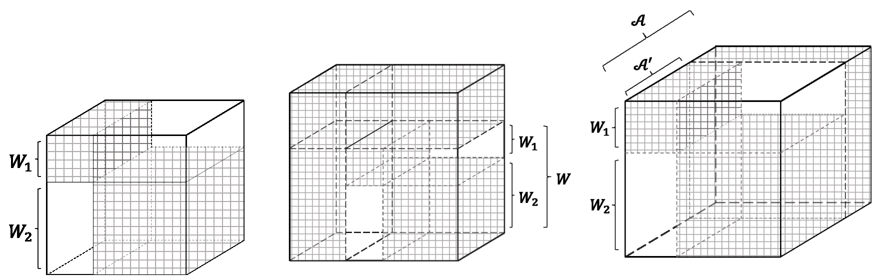
When $n > 2$ and $\mathcal{A} = \langle A \rangle \leq \Lambda(n, \mathbb{F})$ is of dimension 1, $\mathcal{A}$ is always orthogonally decomposable. This can be seen easily from the canonical forms of alternating matrices [13, Chap. XV, Sec. 8].

Definition 2.1 (κ and λ for alternating matrix spaces)**.** Let $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ be of dimension m. We define the restriction-orthogonal number of $\mathcal{A}$, $\kappa(\mathcal{A})$, as the minimum $c \in \mathbb{N}$ for the existence of a dimension-$(n-c)$ subspace $W \leq \mathbb{F}^n$, such that $\mathcal{A}|_W$ is orthogonally decomposable.

We define the subspace-orthogonal number of $\mathcal{A}$, $\lambda(\mathcal{A})$, as the minimum $c \in \mathbb{N}$ for the existence of a dimension-$(m-c)$ subspace $\mathcal{A}' \leq \mathcal{A}$, such that $\mathcal{A}'$ is orthogonally decomposable.

Clearly, $\mathcal{A}$ is orthogonally decomposable if and only if $\kappa(\mathcal{A}) = \lambda(\mathcal{A}) = 0$. Note that $\kappa(\mathcal{A}) \leq n-1$, as we defined $\Lambda(1, \mathbb{F})$ to be orthogonally decomposable. Also note that $\lambda(\mathcal{A}) \leq m$, as any non-trivial direct-sum decomposition is an orthogonal decomposition of the zero space in $\Lambda(n, \mathbb{F})$ when $n \geq 2$.

Suppose we are given a dimension-m $\mathcal{A} = \langle A_1, \ldots, A_m \rangle \leq \Lambda(n, \mathbb{F})$. We form a 3-tensor $\mathtt{A} \in \mathbb{F}^{n \times n \times m}$ such that $\mathtt{A}(i,j,k) = A_k(i,j)$. We illustrate the existence of an orthogonal decomposition for $\mathcal{A}$, the existence of W such that $\mathcal{A}|_W$ has an orthogonal decomposition, and the existence of $\mathcal{A}' \leq \mathcal{A}$ with an orthogonal decomposition, up to appropriate basis changes, in Figure 1.



(A) $\kappa(\mathcal{A}) = \lambda(\mathcal{A}) = 0$ (B) $\kappa(\mathcal{A}) \leq n - \dim(W)$ (C) $\lambda(\mathcal{A}) \leq m - \dim(\mathcal{A}')$

FIGURE 1. Pictorial descriptions of the alternating matrix space parameters. The unmarked regions indicate that the entries there are all zero, W, W_1 and W_2 denote subspaces of $\mathbb{F}^n$, and $\mathcal{A}$ and $\mathcal{A}'$ denote subspaces of $\Lambda(n, \mathbb{F})$. For example, in (a), suppose $W_1 \oplus W_2$ is an orthogonal decomposition for $\mathcal{A}$ spanned by corresponding alternating matrices. Then up to a change of basis, the upper-right and the lower-left corners of $\mathtt{A}$ have all-zero entries. (b) and (c) also indicate the situations with appropriate changes of bases.

2.1.2. *Some notions for alternating bilinear maps.* We introduce basic concepts, and then define κ and λ, for alternating bilinear maps. Let $\phi, \psi : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ be two alternating bilinear maps. Following [25], we say that ϕ and ψ are pseudo-isometric, if they are the same under the natural action of $\mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$. For $W \leq \mathbb{F}^n$, ϕ naturally restricts to W to give $\phi|_W : W \times W \to \mathbb{F}^m$. For $X \leq \mathbb{F}^m$, ϕ naturally induces $\phi/_X : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m/X$ by composing ϕ with the projection from $\mathbb{F}^m$ to $\mathbb{F}^m/X$.

Let $\phi : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ be an alternating bilinear map. Following [25, Definition 3.4], an orthogonal decomposition of ϕ is a direct-sum decomposition of $\mathbb{F}^n = W_1 \oplus W_2$, such that (1) for any $u \in W_1$, $v \in W_2$, we have $\phi(u,v) = 0$, and (2) neither W_1 nor W_2 equals $\mathbb{F}^n$. If ϕ has such an orthogonal decomposition, then ϕ is called orthogonally decomposable.

Definition 2.2 (κ and λ for alternating bilinear maps)**.** Let $\phi : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ be an alternating bilinear map. The restriction-orthogonal number of ϕ, $\kappa(\phi)$, is the minimum $c \in \mathbb{N}$ for the existence of a dimension-$(n-c)$ subspace $W \leq \mathbb{F}^n$, such that $\phi|_U$ is orthogonally decomposable.

The quotient-orthogonal number of ϕ, $\lambda(\phi)$, is the minimum $c \in \mathbb{N}$ for the existence of a dimension-c $X \leq \mathbb{F}^m$, such that $\phi/_X$ is orthogonally decomposable.

Remark 2.3 (From alternating matrix spaces to bilinear maps). This connection is simple but may deserve some discussion. Recall that, given an m-dimensional alternating matrix space $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, we can fix an ordered basis of $\mathcal{A}$ as $\mathbf{A} = (A_1, \dots, A_m) \in \Lambda(n, \mathbb{F})^m$, and construct an alternating bilinear map $\phi_{\mathbf{A}} : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ as in Equation (1.2). Furthermore, $\phi_{\mathbf{A}}$ is surjective since $\mathcal{A}$ is of dimension m. In the above transformation, we shall need $\mathbf{A} \in \Lambda(n, \mathbb{F})^m$ as an intermediate object. For a different ordered basis $\mathbf{A}'$, $\phi_{\mathbf{A}'}$ is pseudo-isometric to $\phi_{\mathbf{A}}$. Because of this, we shall write $\phi_{\mathcal{A}}$ to indicate $\phi_{\mathbf{A}}$ with some ordered basis $\mathbf{A}$ of $\mathcal{A}$. Furthermore, if $\mathcal{A}$ and $\mathcal{B}$ are isometric and $\mathbf{A}$ (resp. $\mathbf{B}$) is an ordered basis for $\mathcal{A}$ (resp. $\mathcal{B}$), then $\phi_{\mathcal{A}}$ and $\phi_{\mathcal{B}}$ are pseudo-isometric.

2.2. **Proof of Theorem 1.3.** The proof of Theorem 1.3 goes by showing that the parameters κ and λ defined for graphs, alternating matrix spaces, alternating bilinear maps, and groups from $\mathfrak{B}_{p,2}$, are preserved in the three steps of the Baer-Lovász-Tutte procedure. The first step, from graphs to alternating matrix spaces, is the tricky one, at least for λ. The other two steps are rather straightforward.

2.2.1. *From graphs to alternating matrix spaces.* Recall that for $\{i,j\} \in \binom{[n]}{2}$, $A_{i,j}$ denotes the elementary alternating matrix with the (i,j)th entry being 1, the (j,i)th entry being -1, and other entries being 0.

Proposition 2.4. *Let $G = ([n], E)$ be a graph, and let $\mathcal{A}_G = \langle A_{i,j} : \{i,j\} \in E\rangle \leq \Lambda(n, \mathbb{F})$ as defined in Step (1). Then $\kappa(G) = \kappa(\mathcal{A}_G)$.*

Proof. We first show $\kappa(\mathcal{A}_G) \leq \kappa(G)$. Let $I \subseteq [n]$ be a subset of vertices of size $d = n - \kappa(G)$, such that the induced subgraph of G on I is disconnected. Let $W = \langle e_i : i \in I\rangle$, and T be the $n \times d$ matrix over $\mathbb{F}$ whose columns are $e_i \in \mathbb{F}^n$, $i \in I$. It is straightforward to verify that $\mathcal{A}_G|_{W,T}$ is orthogonally decomposable.

We then show $\kappa(\mathcal{A}_G) \geq \kappa(G)$. Let $W \leq \mathbb{F}^n$ be a subspace of dimension $d = n - \kappa(\mathcal{A}_G)$, such that $\mathcal{A}|_W$ is orthogonally decomposable. That is, there exists $W = W_1 \oplus W_2$ such that

$$\forall w_1 \in W_1, w_2 \in W_2, \forall A \in \mathcal{A}, w_1^t A w_2 = 0. \tag{2.1}$$

Suppose $\dim(W_1) = b$ and $\dim(W_2) = c$, so $d = b + c$.

Construct an $n \times d$ matrix $T = \begin{bmatrix} T_1 & T_2 \end{bmatrix}$ where T_1 (resp. T_2) is of size $n \times b$ (resp. $n \times c$) and its columns form a basis of W_1 (resp. W_2). Let the ith row of T_1 be u_i^t where $u_i \in \mathbb{F}^b$, and let the jth row of T_2 be v_j^t where $v_j \in \mathbb{F}^c$, for $i, j \in [n]$. Observe that the elementary alternating matrix $A_{i,j} \in \Lambda(n, \mathbb{F})$ can be expressed as $e_i e_j^t - e_j e_i^t$. Then by Equation (2.1), for any $\{i,j\} \in E$,

$$T_1^t(e_i e_j^t - e_j e_i^t)T_2 = u_i v_j^t - u_j v_i^t \in \mathrm{M}(b \times c, \mathbb{F}) \tag{2.2}$$

is the all-zero matrix.

Because T is of rank d, there exists a $d \times d$ submatrix R of T of rank d. Let $I \subseteq [n]$ be the set of row indices of this submatrix R. The key to the proof is the following claim: the induced subgraph of G on I, $G[I]$, is disconnected. To show this, we shall exhibit a partition of $I = I_1 \uplus I_2$ such that no edges in $G[I]$ go across I_1 and I_2.

As R is of rank d, there exists a partition of I, $I = I_1 \uplus I_2$ with $|I_1| = b$, $|I_2| = d - b = c$, such that the following holds. Let R_1 be the $b \times b$ submatrix of R with row indices from I_1 and column indices from $[b]$, and R_2 the $c \times c$ submatrix of R with row indices from I_2 and column indices from $[d] \setminus [b]$. Then R_1 and R_2 are both full-rank. Note that $\{u_i^t : i \in I_1\}$ is the set of rows of R_1 and $\{v_j^t : j \in I_2\}$ is the set of rows of R_2. Up to a permutation of rows, R is of the form $\begin{bmatrix} R_1 & R_2' \\ R_1' & R_2 \\ * & * \end{bmatrix}$.

We then claim that no edges in $G[I]$ go across I_1 and I_2. By contradiction, suppose there is an edge $\{i, j\}$, $i \in I_1$ and $j \in I_2$, in $G[I]$. Then the same edge $\{i, j\}$ is also in G. By Equation (2.2), we have $u_i v_j^t - u_j v_i^t$ is the all-zero matrix, that is $u_i v_j^t = u_j v_i^t$. Note that, up to a permutation of rows as in the last paragraph, u_i is a row in R_1 and v_j is a row in R_2, while u_j is a row in R_1' and v_j is a row in R_2'. Since R_1 and R_2 are full-rank, u_i and v_j are nonzero vectors. This implies that $u_j = \alpha u_i$ and $v_i = (1/\alpha) v_j$ for some nonzero $\alpha \in \mathbb{F}$. But this gives that $\begin{bmatrix} u_j^t & v_j^t \end{bmatrix} = \alpha \begin{bmatrix} u_i^t & v_i^t \end{bmatrix}$, that is, the ith and jth rows of T are linearly dependent. Noting that these rows are in R which is full-rank, we arrive at the desired contradiction. This concludes the proof. □

Proposition 2.5. *Let $G = ([n], E)$ be a graph, and let $\mathcal{A}_G = \langle A_{i,j} : \{i, j\} \in E \rangle \leq \Lambda(n, \mathbb{F})$ be defined in Step (1). Then $\lambda(G) = \lambda(\mathcal{A}_G)$.*

Proof. We first show $\lambda(\mathcal{A}_G) \leq \lambda(G)$. Let D be a size-$\lambda(G)$ subset of E such that $G' = ([n], E \setminus D)$ is disconnected. Let $\mathcal{A}_{G'} = \langle A_{i,j} : \{i, j\} \in E \setminus D \rangle \leq \mathcal{A}_G$. It is straightforward to verify that $\mathcal{A}_{G'}$ is orthogonally decomposable.

We then show $\lambda(\mathcal{A}_G) \geq \lambda(G)$. For this, it is convenient to introduce an equivalent formulation of λ for alternating matrix spaces, which is originated from [14].

Given a direct-sum decomposition $\mathbb{F}^n = W_1 \oplus W_2$ with $\dim(W_1) = b$ and $\dim(W_2) = c = n - b$, let T_1 (resp. T_2) be a $n \times b$ (resp. $n \times c$) matrix whose columns form a basis of W_1 (resp. W_2). Given an m-dimensional $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, let $\mathcal{C}_{W_1,W_2,T_1,T_2}(\mathcal{A}) = \{T_1^t A T_2 : A \in \mathcal{A}\} \leq \mathrm{M}(b \times c, \mathbb{F})$. Note that different choices of T_1 and T_2 result in a subspace of $\mathrm{M}(b \times c, \mathbb{F})$ which can be transformed to $\mathcal{C}_{W_1,W_2,T_1,T_2}(\mathcal{A})$ by left-multiplying some matrix in $\mathrm{GL}(b, \mathbb{F})$ and right-multiplying some matrix in $\mathrm{GL}(c, \mathbb{F})$. So we can write $\mathcal{C}_{W_1,W_2}$ to indicate $\mathcal{C}_{W_1,W_2,T_1,T_2}$ via some such T_1 and T_2. Up to an appropriate basis change as illustrated in Figure 1c, $\mathcal{C}_{W_1,W_2}(\mathcal{A})$ can be seen intuitively as spanned by those submatrices in the upper-right block.

Now we claim that

$$\lambda(\mathcal{A}) = \min\{\dim(\mathcal{C}_{W_1,W_2}(\mathcal{A})) : \forall \text{ non-trivial } \mathbb{F}^n = W_1 \oplus W_2\}. \tag{2.3}$$

To see this, let $\mathcal{A}' \leq \mathcal{A}$ be of dimension $m - \lambda(\mathcal{A})$ which admits an orthogonal decomposition $\mathbb{F}^n = W_1 \oplus W_2$. It is easy to verify that $\dim(\mathcal{C}_{W_1,W_2}(\mathcal{A})) \leq m - (m - \lambda(\mathcal{A})) = \lambda(\mathcal{A})$. On the other hand, let $\mathbb{F}^n = W_1 \oplus W_2$ be a direct-sum decomposition such that $\dim(\mathcal{C}_{W_1,W_2}(\mathcal{A}))$ is minimal. Let T_1 (resp. T_2) be a matrix whose columns form a basis of W_1 (resp. W_2). Let $\mathcal{A}' = \{A \in \mathcal{A} : T_1^t A T_2 = 0\}$. We then have $\dim(\mathcal{A}') = m - \dim(\mathcal{C}_{W_1,W_2}(\mathcal{A}))$, and clearly $\mathcal{A}'$ is orthogonally decomposable. This gives $\lambda(\mathcal{A}) \leq m - \dim(\mathcal{A}') = \dim(\mathcal{C}_{W_1,W_2}(\mathcal{A}))$.

After introducing this formulation, let $\mathbb{F}^n = W_1 \oplus W_2$ be a direct-sum decomposition with $\dim(W_1) = b$ and $\dim(W_2) = c = n - b$, such that $\dim(\mathcal{C}_{W_1,W_2}(\mathcal{A}_G)) =$

$\lambda(\mathcal{A}_G) = d$. Construct an $n \times n$ full-rank matrix $T = \begin{bmatrix} T_1 & T_2 \end{bmatrix}$ where T_1 (resp. T_2) is a $n \times b$ (resp. $n \times c$) matrix whose columns form a basis of W_1 (resp. W_2). Let the ith row of T_1 be u_i^t where $u_i \in \mathbb{F}^b$, and let the jth row of T_2 be v_j^t where $v_j \in \mathbb{F}^c$. We distinguish between the following two cases. Recall that $\mathcal{A}_G = \langle A_{i,j} : \{i,j\} \in E \rangle$, where $A_{i,j} = e_i e_j^t - e_j e_i^t$ is the elementary alternating matrix.

(1) Suppose for any $i \in [n]$, $u_i \neq 0$ if and only if $v_i = 0$. Then there exists $[n] = I_1 \uplus I_2$ with $|I_1| = b$ and $|I_2| = c$, such that $i \in I_1$ if and only if $u_i \neq 0$, and $j \in I_2$ if and only if $v_j \neq 0$. Furthermore, vectors in $\{u_i : i \in I_1\}$ are linearly independent, and vectors in $\{v_j : j \in I_2\}$ are linearly independent. That is, up to a permutation of rows, T is of the form $\begin{bmatrix} T_{11} & 0 \\ 0 & T_{22} \end{bmatrix}$, where $T_{11} \in \mathrm{GL}(b, \mathbb{F})$ and $T_{22} \in \mathrm{GL}(c, \mathbb{F})$. We claim that there are no more than d edges of G crossing I_1 and I_2. Suppose not, then there exists $\{\{i_1, j_1\}, \dots, \{i_{d+1}, j_{d+1}\}\} \subseteq E$, such that $i_k \in I_1$, and $j_k \in I_2$ for $k \in [d+1]$. We then have for any $k \in [d+1]$

$$T_1^t(e_{i_k} e_{j_k}^t - e_{j_k} e_{i_k}^t) T_2 = u_{i_k} v_{j_k}^t - u_{j_k} v_{i_k}^t = u_{i_k} v_{j_k}^t \in \mathcal{C}_{W_1,W_2}(\mathcal{A}_G). \tag{2.4}$$

It is straightforward to verify that the rank-1 matrices $u_{i_k} v_{j_k}^t$, $k \in [d+1]$, are linearly independent, contradicting that $\mathcal{C}_{W_1,W_2}(\mathcal{A}_G)$ is of dimension d.

(2) Suppose there exists $i \in [n]$ such that both u_i and v_i are nonzero. Suppose by contradiction that $\lambda(G) > d$. Up to a permutation of vertices, we may assume $i = n$, and the vertex n is adjacent to vertices $1, \dots, d+1$. By Equation (2.4), we have $u_n v_k^t - u_k v_n^t \in \mathcal{C}_{W_1,W_2}(\mathcal{A}_G)$ for $k \in [d+1]$. Since $\dim(\mathcal{C}_{W_1,W_2}(\mathcal{A}_G)) = d$, the matrices $u_n v_k^t - u_k v_n^t$, $k \in [d+1]$, are linearly dependent. It follows that there exist $\alpha_k \in \mathbb{F}$ for $k \in [d+1]$, at least one of which is nonzero, such that $\sum_{k=1}^{d+1} \alpha_k (u_n v_k^t - u_k v_n^t) = 0$. This implies that $u_n (\sum_{k=1}^{d+1} \alpha_k v_k^t) = (\sum_{k=1}^{d+1} \alpha_k u_k) v_n^t$ as two rank-1 matrices.

From the above, and by the assumption that u_n and v_n are nonzero, we have that $\beta u_n = \sum_{k=1}^{d+1} \alpha_k u_k$ and $\beta v_n = \sum_{k=1}^{d+1} \alpha_k v_k$ for some $\beta \in \mathbb{F}$. Since at least one of α_k's is nonzero, this means that the rows in T with indices $\{1, \dots, d+1, n\}$ are linearly dependent, which contradicts that T is full-rank.

These conclude the proof that $\lambda(\mathcal{A}_G) \geq \lambda(G)$. □

Remark 2.6 (Cuts in alternating matrix spaces). The alternative formulation of λ as in Equation (2.3) rests on a natural generalisation of the notion of cuts in graphs. Proposition 2.5 then indicates that for an alternating matrix space $\mathcal{A}_G$ constructed from a graph G, the minimum cut sizes of $\mathcal{A}_G$ and G are equal.

2.2.2. *From alternating matrix spaces to alternating bilinear maps.* We now relate the parameters κ and λ for alternating matrix spaces and alternating bilinear maps in the following easy proposition. Note that we use the notation $\phi_{\mathcal{A}}$ due to the discussions in Remark 2.3.

Proposition 2.7. *For an m-dimensional $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, let an alternating bilinear map $\phi_{\mathcal{A}} : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$ be defined in Step (2). Then we have $\kappa(\mathcal{A}) = \kappa(\phi_{\mathcal{A}})$, and $\lambda(\mathcal{A}) = \lambda(\phi_{\mathcal{A}})$.*

Proof. The equality $\kappa(\mathcal{A}) = \kappa(\phi_{\mathcal{A}})$ is straightforward to verify.

To show that $\lambda(\mathcal{A}) \geq \lambda(\phi_{\mathcal{A}})$, let $\mathcal{A}' \leq \mathcal{A}$ be a dimension-$(n - \lambda(\mathcal{A}))$ subspace of $\mathcal{A}$ admitting an orthogonal decomposition. Let $c = \lambda(\mathcal{A})$. We fix an ordered basis of $\mathcal{A}$, $\mathbf{A} = (A_1, \dots, A_m)$, such that $\{A_1, \dots, A_{m-c}\}$ spans $\mathcal{A}'$. Let $X \leq \mathbb{F}^m$ be the linear span of the last c standard basis vectors. We claim that $\phi_{\mathbf{A}}/_X$ is orthogonally decomposable. Indeed, let $U \oplus V$ be an orthogonal decomposition of $\mathcal{A}'$. Then for any $u \in U, v \in V$, we have $\phi_{\mathbf{A}}(u, v) \in X$, which means that $U \oplus V$ is also an orthogonal decomposition for $\phi_{\mathbf{A}}/_X$.

To show that $\lambda(\mathcal{A}) \leq \lambda(\phi_{\mathcal{A}})$, let $\mathbf{A} = (A_1, \dots, A_m)$ be an ordered basis of $\mathcal{A}$, and let $c = \lambda(\phi_{\mathcal{A}})$. Let X be a dimension-c subspace of $\mathbb{F}^m$, such that $\phi_{\mathbf{A}}/_X$ admits an orthogonal decomposition $\mathbb{F}^n = U \oplus V$. That is, for any $u \in U$ and $v \in V$, $\phi_{\mathbf{A}}(u, v) \in X$. Form an ordered basis of $\mathbb{F}^m$, $(w_1, \dots, w_m)$, where $w_i = (w_{i,1}, \dots, w_{i,m})^t \in \mathbb{F}^m$, such that the last c vectors form a basis of X. Let $A_i' = \sum_{j \in [m]} w_{i,j} A_j$ be another ordered basis of $\mathcal{A}$, and $\mathbf{A}' = (A_1', \dots, A_m')$. Then for any $u \in U$ and $v \in V$, since $\phi_{\mathbf{A}}(u, v) \in X$, the first $m - c$ entries of $\phi_{\mathbf{A}'}(u, v)$ are zero. In particular, this implies that $\mathbb{F}^n = U \oplus V$ is an orthogonal decomposition for $\mathcal{A}' = \langle A_1', \dots, A_{m-c}' \rangle$, where $\mathcal{A}'$ is of dimension $m - c$. $\square$

2.2.3. *From alternating bilinear maps to groups from $\mathfrak{B}_{p,2}$.* To start with, we observe the following basic properties of κ, λ, and δ for groups from $\mathfrak{B}_{p,2}(n, m)$.

Observation 2.8. *Let $P \in \mathfrak{B}_{p,2}(n, m)$. Then we have the following.*

1. *Suppose $P = JK$ is a central decomposition. Let $J_0 = J[P, P]$, and $K_0 = K[P, P]$. Then J_0 and K_0 form a central decomposition of P, and both of them properly contain $[P, P]$.*
2. *If for a central subgroup N, P/N is orthogonally decomposable, then $P/(N \cap [P, P])$ is orthogonally decomposable.*
3. *For any $g \in P$, $\deg(g) \leq n - 1$.*

Proof. (1): To show that J_0 and K_0 form a central decomposition of P, we only need to verify that J_0 and K_0 are proper. For the sake of contradiction, suppose $P = J_0 = J[P, P]$. Since $[P, P]$ is the Frattini subgroup of P, it follows that $J = P$, contradicting that J is proper.

To show that J_0 properly contains $[P, P]$, again for the sake of contradiction suppose $J_0 \leq [P, P]$. Then $P = J_0 K_0 \leq [P, P] K_0 = K_0$, a contradiction to K_0 being a proper subgroup of P.

(2): If $N \leq [P, P]$, the conclusion holds trivially. Suppose otherwise. Let J/N and K/N be a central product of P/N for $J, K \leq P$. That is, for any $j \in J$ and $k \in K$, $jkj^{-1}k^{-1} \in N$, so in fact $jkj^{-1}k^{-1} = [j, k] \in N \cap [P, P]$. It then follows easily that $J/(N \cap [P, P])$ and $K/(N \cap [P, P])$ form a central product of $P/(N \cap [P, P])$.

(3): If $g \in \mathrm{Z}(P)$, $\deg(g) = 0$. If $g \notin \mathrm{Z}(P)$, then $C_P(g)$ contains the subgroup generated by g and $[P, P]$, which is of order at least p^{m+1}. $\square$

Recall that in Step (3), we start from an alternating bilinear map $\phi : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ satisfying $\phi(\mathbb{F}_p^n, \mathbb{F}_p^n) = \mathbb{F}_p^m$, and construct P_ϕ, a p-group of class 2 and exponent p. Then $[P_\phi, P_\phi] \cong \mathbb{Z}_p^m$, and $P_\phi/[P_\phi, P_\phi] \cong \mathbb{Z}_p^n$.

It is easily checked that, by Equation (1.3), subspaces of $\mathbb{F}_p^m$ correspond to subgroups of $[P_\phi, P_\phi]$, and subspaces of $\mathbb{F}_p^n$ correspond to subgroups of $P_\phi/[P_\phi, P_\phi]$. We then set up the following notation. For $U \leq \mathbb{F}_p^n$, let Q_U be the subgroup of $P_\phi/[P_\phi, P_\phi]$ corresponding to U, and let S_U be a subgroup of P_ϕ of the smallest order satisfying $S_U[P_\phi, P_\phi]/[P_\phi, P_\phi] = Q_U$. It is easy to show, by following the proof of [25, Lemma 2.3 (i)], that S_U is regular with respect to commutation, i.e. $S_U \cap [P_\phi, P_\phi] = [S_U, S_U]$. For $X \leq \mathbb{F}_p^m$, let N_X be the subgroup of $[P_\phi, P_\phi]$ corresponding to X.

Proposition 2.9. *Let $\phi : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ and $P_\phi \in \mathfrak{B}_{p,2}(n, m)$ be as above. Then $\kappa(\phi) = \kappa(P_\phi)$, and $\lambda(\phi) = \lambda(P_\phi)$.*

Proof. To show that $\kappa(\phi) \geq \kappa(P_\phi)$, suppose there exists a $(n - \kappa(\phi))$-dimensional $U \leq \mathbb{F}_p^n$ such that $\phi|_U$ is orthogonally decomposable. It can be verified easily that this induces a central decomposition for the regular subgroup $S_U \leq P_\phi$. Furthermore, by Noether's isomorphism theorems, $S_U/[S_U, S_U] = S_U/(S_U \cap [P_\phi, P_\phi]) \cong S_U[P_\phi, P_\phi]/[P_\phi, P_\phi] = Q_U$, which is of order $p^{n-\kappa(\phi)}$.

To show that $\kappa(\phi) \leq \kappa(P_\phi)$, suppose that a regular $S \leq P_\phi$ satisfying $|S/[S, S]| = p^{n-\kappa(P_\phi)}$ admits a central decomposition $S = JK$. Applying Observation 2.8 (1) to S, we can assume that J and K both properly contain $[S, S]$. Let U_S (resp. U_J, U_K) be the subspace of $\mathbb{F}_p^n$ corresponding to $S[P_\phi, P_\phi]/[P_\phi, P_\phi]$ (resp. $J[P_\phi, P_\phi]/[P_\phi, P_\phi]$, $K[P_\phi, P_\phi]/[P_\phi, P_\phi]$). Then it can be verified, using Equation (1.3), that U_J and U_K form an orthogonal decomposition for $\phi|_{U_S}$. Furthermore, by Noether's isomorphism theorems, $S[P_\phi, P_\phi]/[P_\phi, P_\phi] \cong S/[S, S]$, which holds with S replaced by J or K as well. In particular we have $\dim(U_S) = n - \kappa(P_\phi)$.

To show that $\lambda(\phi) \geq \lambda(P_\phi)$, we translate a subspace $X \leq \mathbb{F}_p^m$ with $\phi/_X$ orthogonally decomposable to a subgroup $N_X \leq [P_\phi, P_\phi]$. It can be verified easily that the orthogonal decomposition of $\phi/_X$ yields a central decomposition of P_ϕ/N_X.

To show that $\lambda(\phi) \leq \lambda(P_\phi)$, suppose $N \leq P_\phi$ is a central subgroup of order $p^{\lambda(P_\phi)}$ such that P_ϕ/N is centrally decomposable. By Observation 2.8 (2), we can assume that $N \leq [P_\phi, P_\phi]$. Let X be the subspace of $\mathbb{F}_p^m$ corresponding to N. Let $J/N, K/N \leq P_\phi/N$ be a central decomposition of P_ϕ/N for $J, K \leq P_\phi$. Applying Observation 2.8 (1) to P_ϕ/N, we can assume that J/N and K/N both properly contain $[P_\phi/N, P_\phi/N] = [P_\phi, P_\phi]/N$. In particular, J and K properly contain $[P_\phi, P_\phi]$, so $J/[P_\phi, P_\phi]$ (resp. $K/[P_\phi, P_\phi]$) corresponds to a non-trivial proper subspace $U_J \leq \mathbb{F}_p^n$ (resp. $U_K \leq \mathbb{F}_p^n$). Then it can be verified that U_J and U_K span $\mathbb{F}_p^n$, and for any $u \in U_J$ and $u' \in U_K$, we have $\phi(u, u') \in X$. Therefore U_J and U_K form an orthogonal decomposition for $\phi/_X$. □

Remark 2.10 (On the regular condition). The reason for imposing the regular condition is to rule out the following central decompositions, which is not well-behaved regarding the correspondence between ϕ and P_ϕ. Suppose that $S \leq P_\phi$ satisfies $[S, S] < [P_\phi, P_\phi]$. Then S and $[P_\phi, P_\phi]$ form a central decomposition of $S[P_\phi, P_\phi]$. Translating back to ϕ, $[S, S] < [P_\phi, P_\phi]$ just says that $\phi(U_S, U_S)$ is a proper subspace of $\mathbb{F}^m$, which is not related to whether $\phi|_{U_S}$ is orthogonally decomposable.

2.3. **Proof of Proposition 1.5.** We shall work in the setting of alternating matrix spaces. So we state the correspondence of Definition 1.4 in this setting, which was already used in [4].

Definition 2.11 (Degrees and δ for alternating matrix spaces)**.** Let $\mathcal{A} \leq \Lambda(n, \mathbb{F})$. For $v \in \mathbb{F}^n$, the degree of v in $\mathcal{A}$ is the dimension of $\mathcal{A}v := \{Av : A \in \mathcal{A}\}$. The minimum degree of $\mathcal{A}$, denoted as $\delta(\mathcal{A})$, is the minimum degree over all $0 \neq v \in \mathbb{F}^n$.

To translate from groups in $\mathfrak{B}_{p,2}(n,m)$ to alternating matrix spaces, we recall the following procedure which consists of inverses of the last two steps of the Baer-Lovász-Tutte procedure.

For any $P \in \mathfrak{B}_{p,2}(n,m)$, let $V = P/[P,P] \cong \mathbb{Z}_p^n$ and $U = [P,P] \cong \mathbb{Z}_p^m$. The commutator map $\phi_P : V \times V \to U$ is alternating and bilinear. After fixing bases of V and U as $\mathbb{F}_p$-vector spaces, we can represent $\phi_P : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m$ as $(A_1, \dots, A_m) \in \Lambda(n, \mathbb{F}_p)^m$, which spans an m-dimensional $\mathcal{A}_P \leq \Lambda(n, \mathbb{F}_p)$. It is easy to check that isomorphic groups yield isometric alternating matrix spaces. Furthermore, this procedure preserves κ and λ, by essentially the same proof for Proposition 2.7 and 2.9, and δ, by a straightforward calculation.

The following proposition then implies Proposition 1.5 (1).

Proposition 2.12. *Given $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, we have $\kappa(\mathcal{A}) \leq \delta(\mathcal{A})$ and $\lambda(\mathcal{A}) \leq \delta(\mathcal{A})$.*

Proof. We first show that $\kappa(\mathcal{A}) \leq \delta(\mathcal{A})$. Take some $v \in \mathbb{F}^n$ such that $\deg(v) = \delta(\mathcal{A})$. If $\delta(\mathcal{A}) = n-1$, then the inequality holds trivially. Otherwise, let $U = \{u \in \mathbb{F}^n : \forall\, A \in \mathcal{A}, u^t A v = 0\}$. Note that $\dim(U) = n - \deg(v) \geq 2$, and $v \in U$. Let V be any complement space of $\langle v \rangle$ in U. Then $\langle v \rangle \oplus V$ is an orthogonal decomposition of $\mathcal{A}|_U$. It follows that $\kappa(\mathcal{A}) \leq n - \dim(U) = \deg(v) = \delta(\mathcal{A})$.

We then show that $\lambda(\mathcal{A}) \leq \delta(\mathcal{A})$. Take some $v \in \mathbb{F}^n$ such that $\deg(v) = \delta(\mathcal{A})$. Let W be any complement subspace of $\langle v \rangle$ in $\mathbb{F}^n$, and let T_W be an $n \times (n-1)$ matrix whose columns form a basis of W. The space $v^t \mathcal{A} T_W = \{v^t A T_W : A \in \mathcal{A}\} \leq \mathrm{M}(1 \times (n-1), \mathbb{F})$ is of dimension $\deg(v)$. By Equation (2.3), we then have $\lambda(\mathcal{A}) \leq \dim(v^t \mathcal{A} T_W) = \deg(v) = \delta(\mathcal{A})$. □

In contrast to the graph setting, we show that it is possible that $\kappa(\mathcal{A}) > \lambda(\mathcal{A})$ over $\mathbb{Q}$ and $\mathbb{F}_q$, therefore proving Proposition 1.5 (2). For this we need the following:

Definition 2.13. We say that $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ is fully connected, if for any linearly independent $u, v \in \mathbb{F}^n$, there exists $A \in \mathcal{A}$, such that $u^t A v \neq 0$.

An observation on fully connected $\mathcal{A}$ follows from the definition easily.

Observation 2.14. *A fully connected $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ satisfies $\kappa(\mathcal{A}) = n - 1$.*

We shall construct a fully connected $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ with $\lambda(\mathcal{A}) < n - 1 = \kappa(\mathcal{A})$. To do this we need the fully connected notion in the (not necessarily alternating) matrix space setting. That is, $\mathcal{B} \leq \mathrm{M}(s \times t, \mathbb{F})$ is fully connected, if for any nonzero $u \in \mathbb{F}^s$ and nonzero $v \in \mathbb{F}^t$, there exists $B \in \mathcal{B}$, such that $u^t B v \neq 0$. The following fact is well-known.

Fact 2.15. *Let $\mathbb{F}$ be a finite field or $\mathbb{Q}$. Then over $\mathbb{F}$, there exists a fully connected matrix space in $\mathrm{M}(s, \mathbb{F})$ of dimension s.*

Proof. Let $\mathbb{K}$ be a degree-s field extension of $\mathbb{F}$. The regular representation of $\mathbb{K}$ on $\mathbb{F}^s$ gives an s-dimensional $\mathcal{C} \leq \mathrm{M}(s, \mathbb{F})$, such that each nonzero $C \in \mathcal{C}$ is of full rank. Let $(C_1, \dots, C_s)$ be an ordered basis of $\mathcal{B}$. Let $B_i \in \mathrm{M}(s, \mathbb{F})$, $i \in [s]$, be defined by $B_i = \begin{bmatrix} C_1 e_i & C_2 e_i & \dots & C_s e_i \end{bmatrix}$. That is, the jth column of B_i is the ith column of C_j. Then $\mathcal{B} = \langle B_1, \dots, B_s \rangle \leq \mathrm{M}(s, \mathbb{F})$ is of dimension s and fully connected. Indeed, if $\mathcal{B}$ is not fully connected, then there exist nonzero $v \in \mathbb{F}^s$ and nonzero $u = (u_1, u_2, \dots, u_s)^t \in \mathbb{F}^s$ such that $v^t B_i u = 0$ for any $i \in [s]$. But this just means that v is in the left kernel of $C' = u_1 C_1 + \dots + u_s C_s$, contradicting that C' is of full rank. □

Let $s, t \in \mathbb{N}$ and $n = s+t$. Let $\mathcal{B} \leq \mathrm{M}(s\times t, \mathbb{F})$ be a fully connected matrix space of dimension $d < n-1$. We shall use $\mathcal{B}$ to construct a fully connected $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ such that $\lambda(\mathcal{A}) \leq d < n-1 = \kappa(\mathcal{A})$.

Suppose $\mathcal{B}$ is spanned by $B_1, \dots, B_d \in \mathrm{M}(s\times t, \mathbb{F})$. Let $A_i = \begin{bmatrix} 0 & B_i \\ -B_i^t & 0 \end{bmatrix}$ for $i \in [d]$. For $1 \leq i < j \leq s$, let $C_{i,j} = \begin{bmatrix} E_{i,j} & 0 \\ 0 & 0 \end{bmatrix} \in \Lambda(n, \mathbb{F})$, where $E_{i,j} = e_i e_j^t - e_j e_i^t \in \Lambda(s, \mathbb{F})$ is an elementary alternating matrix. For $1 \leq i < j \leq t$, let $D_{i,j} = \begin{bmatrix} 0 & 0 \\ 0 & F_{i,j} \end{bmatrix} \in \Lambda(n, \mathbb{F})$, where $F_{i,j} = e_i e_j^t - e_j e_i^t \in \Lambda(t, \mathbb{F})$ is an elementary alternating matrix. Let $\mathcal{A}$ be spanned by $\{A_i : i \in [d]\} \cup \{C_{i,j} : 1 \leq i < j \leq s\} \cup \{D_{i,j} : 1 \leq i < j \leq t\}$.

Proposition 2.16. *Let $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ be as above. Then $\mathcal{A}$ is fully connected.*

Proof. Assume there exist linearly independent $u, v \in \mathbb{F}^n$ such that for any $A \in \mathcal{A}$, $u^t A v = 0$. Take $u = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$ and $v = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$, where $u_1, v_1 \in \mathbb{F}^s$ and $u_2, v_2 \in \mathbb{F}^t$. Note that for any $1 \leq i < j \leq s$, $\begin{bmatrix} u_1^t & u_2^t \end{bmatrix} \begin{bmatrix} E_{i,j} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = u_1^t E_{i,j} v_1 = 0$. Similarly, we have $u_2^t F_{i,j} v_2 = 0$ for all $1 \leq i < j \leq t$.

We then distinguish among the following cases.

(1) v_1 and v_2 are both nonzero. In this case we have $u_1 = \lambda v_1$ and $u_2 = \mu v_2$ for some $\lambda \neq \mu \in \mathbb{F}$. Therefore, we have

$$\begin{bmatrix} u_1^t & u_2^t \end{bmatrix} \begin{bmatrix} 0 & B_i \\ -B_i^t & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = -u_2^t B_i^t v_1 + u_1^t B_i v_2 = -\mu v_2^t B_i^t v_1 + \lambda v_1^t B_i v_2 = (\lambda - \mu) v_1^t B_i v_2.$$

Since $\mathcal{B}$ is fully connected, this implies that $v_1 = 0$ or $v_2 = 0$, a contradiction to the assumption of this case.

(2) v_1 is zero and v_2 is nonzero. Then $u_2 = \lambda v_2$, and u_1 cannot be zero. Therefore, we have

$$\begin{bmatrix} u_1^t & u_2^t \end{bmatrix} \begin{bmatrix} 0 & B_i \\ -B_i^t & 0 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = -u_2^t B_i^t v_1 + u_1^t B_i v_2 = u_1^t B_i v_2 = 0,$$

which is a contradiction to the full connectivity of $\mathcal{B}$.

(3) v_1 is nonzero and v_2 is zero. This case is in complete analogy with the previous case.

This concludes the proof that $\mathcal{A}$ is fully connected. $\square$

We then have $\kappa(\mathcal{A}) = n-1$ by Observation 2.14. Now observe that the subspace of $\mathcal{A}$ spanned by $C_{i,j}$ and $D_{i,j}$ is centrally decomposable. This gives that $\lambda(\mathcal{A}) \leq d < n-1 = \kappa(\mathcal{A})$. Over $\mathbb{F}_q$ and $\mathbb{Q}$, such $\mathcal{B}$ exists for $s > 1$ by Fact 2.15. This concludes the proof of Proposition 1.5 (2).

References

1. J. L. Alperin, *Large abelian subgroups of p-groups*, Transactions of the American Mathematical Society **117** (1965), 10–20.
2. László Babai, Paul Erdős, and Stanley M. Selkow, *Random graph isomorphism*, SIAM Journal on Computing **9** (1980), no. 3, 628–635.
3. Reinhold Baer, *Groups with abelian central quotient group*, Transactions of the American Mathematical Society **44** (1938), no. 3, 357–386.

4. Xiaohui Bei, Shiteng Chen, Ji Guan, Youming Qiao, and Xiaoming Sun, *From independent sets and vertex colorings to isotropic spaces and isotropic decompositions: Another bridge between graphs and alternating matrix spaces*, 11th Innovations in Theoretical Computer Science Conference, ITCS, 2020, pp. 8:1–8:48.
5. Joe Buhler, Ranee Gupta, and Joe Harris, *Isotropic subspaces for skewforms and maximal abelian subgroups of p-groups*, Journal of Algebra **108** (1987), no. 1, 269–279.
6. W. Burnside, *On some properties of groups whose orders are powers of primes*, Proceedings of the London Mathematical Society **2** (1913), no. 1, 225–245.
7. Reinhard Diestel, *Graph theory*, 5th ed., Springer Graduate Texts in Mathematics, no. 173, Springer, 2017.
8. Xiaoyu He and Youming Qiao, *On the Baer-Lovász-Tutte construction of groups from graphs: isomorphism types and homomorphism notions*, 2020, arXiv:2003.07200.
9. Hermann Heineken and Hans Liebeck, *The occurrence of finite groups in the automorphism group of nilpotent groups of class 2*, Archiv der Mathematik **25** (1974), no. 1, 8–16.
10. Graham Higman, *Enumerating p-groups. I: Inequalities*, Proceedings of the London Mathematical Society **3** (1960), no. 1, 24–30.
11. Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications **42** (1993).
12. 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** (2019), no. 3, 926–963.
13. Serge Lang, *Algebra*, third enlarged ed., Graduate Texts in Mathematics, no. 211, Springer-Verlag, New York, 2002.
14. Yinan Li and Youming Qiao, *Linear algebraic analogues of the graph isomorphism problem and the Erdős-Rényi model*, 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS (Chris Umans, ed.), IEEE Computer Society, 2017, pp. 463–474.
15. László Lovász, *On determinants, matchings and random algorithms*, Fundamentals of Computation Theory, 1979, pp. 565–574.
16. ———, *Singular spaces of matrices and their application in combinatorics*, Boletim da Sociedade Brasileira de Matemática **20** (1989), no. 1, 87–99.
17. Avinoam Mann, *Elements of minimal breadth in finite p-groups and Lie algebras*, Journal of the Australian Mathematical Society **81** (2006), no. 2, 209–214.
18. Alan H. Mekler, *Stability of nilpotent groups of class 2 and prime exponent*, The Journal of Symbolic Logic **46** (1981), no. 4, 781–788.
19. A. Yu. Ol'shanskii, *The number of generators and orders of abelian subgroups of finite p-groups*, Mathematical notes of the Academy of Sciences of the USSR **23** (1978), no. 3, 183–185.
20. Tobias Rossmann and Christopher Voll, *Groups, graphs, and hypergraphs: average sizes of kernels of generic matrices with support constraints*, 2019, arXiv:1908.09589.
21. M. Suzuki, *Group theory I*, Springer, 1982.
22. W. T. Tutte, *The factorization of linear graphs*, Journal of the London Mathematical Society **s1-22** (1947), no. 2, 107–111.
23. ———, *Connectivity in graphs*, University of Toronto Press, 1966.
24. Michael Vaughan-Lee, *Groups of order p^8 and exponent p*, International Journal of Group Theory **4** (2015), no. 4, 25–42.
25. James B. Wilson, *Decomposing p-groups via Jordan algebras*, Journal of Algebra **322** (2009), no. 8, 2642–2679.
26. ———, *Finding central decompositions of p-groups*, Journal of Group Theory **12** (2009), no. 6, 813–830.

Centrum Wiskunde & Informatica and QuSoft, Science Park 123, 1098XG Amsterdam, Netherlands
Email address: Yinan.Li@cwi.nl

Center for Quantum Software and Information, University of Technology Sydney, Ultimo NSW 2007, Australia
Email address: Youming.Qiao@uts.edu.au