Enumerating alternating matrix spaces over finite fields with explicit coordinates

Youming Qiao [*]

March 4, 2021

Abstract

We initiate the study of enumerating linear subspaces of alternating matrices over finite fields with explicit coordinates. We present q-analogues of Gilbert's formula for enumerating connected graphs (*Can. J. Math.*, 1956), and Read's formula for enumerating c-colored graphs (*Can. J. Math.*, 1960). We also develop an analogue of Riddell's formula relating the exponential generating function of graphs with that of connected graphs (Riddell's PhD thesis, 1951), building on Eulerian generating functions developed by Srinivasan (*Discrete Math.*, 2006).

Keywords: labelled graph enumeration; alternating matrix spaces; Eulerian generating functions; q-calculus; alternating bilinear maps.

1 Introduction

An $n \times n$ matrix A over a field $\mathbb{F}$ is *alternating*, if for any $v \in \mathbb{F}^n$, $v^t A v = 0$. Let $\Lambda(n, \mathbb{F})$ be the linear space of $n \times n$ alternating matrices over $\mathbb{F}$. A subspace of $\Lambda(n, \mathbb{F})$ is referred to as an *alternating matrix space*. When $\mathbb{F}$ is the finite field with q elements $\mathbb{F}_q$, we may also write $\Lambda(n, \mathbb{F}_q)$ as $\Lambda(n, q)$.

We study enumerating alternating matrix spaces over finite fields with explicit coordinates. This leads us to derive q-analogues of several classical graph enumeration formulas, including Read's formula for enumerating c-colored graphs [Rea60], Gilbert's formula for enumerating connected graphs [Gil56], and Riddell's formula relating the exponential generating function of graphs with that of connected graphs [Rid51].

In the following of this introduction, we will first present a q-analogue of Read's formula for alternating matrix spaces. We will then briefly introduce other results. We conclude the introduction by providing some general remarks on motivations and future directions. The rest of the article is devoted to prove our results.

A q-analogue of Read's formula. In [Rea60], generalising a result of Gilbert [Gil56], Read gave a formula for the number of labelled c-coloured graphs. As a graph could be c-coloured in several ways, that formula essentially enumerates (G, U), where $G = ([n], E)$ is a graph, and U is a partition of $[n]$ such that each subset in U is an independent set of G. Read's formula is then

$$\sum_{(n_1, \ldots, n_c)} \binom{n}{n_1, \ldots, n_c} \cdot 2^{\kappa(n, n_1, \ldots, n_c)}, \tag{1}$$

where $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n, and $\kappa(n, n_1, \ldots, n_c) := \binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}$.

---

[*]Centre for Quantum Software and Information, University of Technology Sydney. `jimmyqiao86@gmail.com`

Now let $\mathcal{A} \leq \Lambda(n, q)$ be an alternating matrix space. For $c \in \mathbb{N}$, we say that a direct sum decomposition $\mathbb{F}_q^n = U_1 \oplus \cdots \oplus U_c$ is a *totally-isotropic c-decomposition* of $\mathcal{A}$, if for any $i \in [c]$, any $u, v \in U_i$, and any $A \in \mathcal{A}$, we have $u^t A v = 0$. The following formula counts the number of alternating matrix spaces with totally-isotropic c-decompositions:

$$\sum_{(n_1, \ldots, n_c)} \binom{n}{n_1, \ldots, n_c}_q \cdot q^{\kappa(n, n_1, \ldots, n_c)} \cdot \mathrm{GalN}^q_{\kappa(n, n_1, \ldots, n_c)}, \tag{2}$$

where $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n, and $\kappa(n, n_1, \ldots, n_c) = \binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}$. Here $\binom{n}{n_1, \ldots, n_c}_q := \frac{[n]_q!}{[n_1]_q! \ldots [n_c]_q!}$ is the q-analogue of multimonomial coefficients, and GalN^q_N denotes the Nth Galois number over q [GR69]; see Section 2 for more details on these notations. In particular, when setting $q = 1$, Equation 2 becomes Equation 1.

Overview of other results. We now give an overview of other results in this paper.

For connected graphs, there is a classical formula as reviewed in Equation 5. Enumerating connected graphs is one of the first few questions studied in graph enumeration, tracing back to at least Riddell's thesis [Rid51], though it seems to the author that the exact formula as in Equation 5 first appeared in Gilbert's article [Gil56].

For alternating matrix spaces, there are two indecomposability notions, which, when restricted to alternating matrix spaces of the form $\mathcal{A}_G$ as in Equation 3, both coincide with the connectivity of G [LQ20].

The first indecomposability notion is with respect to the so-called direct decompositions (cf. Definition 4.1). This indecomposability has a property that makes it quite close to connectivity. That is, for non-degenerate alternating matrix spaces (cf. Section 2), there is a unique complete direct decomposition [Wil12]. In Section 4, we study enumerating directly-indecomposable alternating matrix spaces. Despite some minor subtleties caused by the non-degeneracy condition, we obtain a q-analogue of Gilbert's formula in Equation 7.

The second indecomposability notion is with respect to the so-called orthogonal decompositions (cf. Definition 4.1). This indecomposability is more flexible, meaning an alternating matrix space could have several complete orthogonal decompositions in several ways even under the automorphism group action [Wil09]. So we give a formula for alternating matrix spaces with orthogonal c-decompositions in Equation 4 in the spirit of Equation 2.

A basic tool in labelled graph enumeration is the exponential generating function, based on which we have the labelled counting lemma [HP73, pp. 8]. We demonstrate a q-analogue of this lemma for alternating matrix spaces, which we call the coordinate-explicit counting lemma, in Lemma 5.2. As an application of this lemma, we derive a q-analogue of Riddell's formula relating the exponential generating function of graphs with that of connected graphs [Rid51] in Equation 9. Here, we heavily rely on the Eulerian generating functions developed by Srinivasan [Sri06].

Motivations for this study. The results presented in this paper are motivated by a classical connection between graphs and alternating matrix spaces, going back to Tutte [Tut47] and Lovász [Lov79]. This connection recently lead to interesting structures for alternating matrix spaces, which in turn forms the basis of our investigation.

So let us review the classical construction of alternating matrix spaces from graphs [Tut47, Lov79]. Since we focus on labelled graphs, without loss of generality let us consider graphs with vertex sets being $[n] = \{1, \ldots, n\}$. Let $G = ([n], E)$ be an undirected simple graph, so $E \subseteq \binom{[n]}{2}$. For $\{i, j\} \in \binom{[n]}{2}$, $i < j$, an elementary alternating matrix $A_{i,j} \in \mathrm{M}(n, \mathbb{F})$ is the $n \times n$ matrix with the (i, j)th entry being 1, the (j, i)th entry being -1, and the rest entries being 0. We then define

$$\mathcal{A}_G = \langle A_{i,j} : \{i, j\} \in E \rangle \leq \Lambda(n, \mathbb{F}), \tag{3}$$

where $\langle \cdot \rangle$ denotes linear span. As G has a perfect matching if and only if $\mathcal{A}_G$ contains a full-rank matrix, Tutte used $\mathcal{A}_G$ to characterise graphs without perfect matchings [Tut47], and Lovász used $\mathcal{A}_G$ to obtain a simple efficient randomised algorithm for the perfect matching problem [Lov79].

Inspired by this classical example, several correspondences between graph-theoretic structures, and structures for alternating matrix spaces, have been discovered recently, including:

1. Independent sets vs totally-isotropic spaces, and vertex colourings vs totally-isotropic decompositions [BCG$^+$20];

2. Connectivity vs orthogonal indecomposability. As a consequence, correspondences of vertex and edge connectivities for alternating matrix spaces are also presented [LQ20];

3. Isomorphism notions for graphs and alternating matrix spaces [HQ20].

For example, let us review the one between independent sets and isotropic spaces in [BCG$^+$20]. Some other correspondences will be introduced later, when we come to the relevant enumeration problems.

Definition 1.1. Let $\mathcal{A} \le \Lambda(n, \mathbb{F})$ be an alternating matrix spaces. A subspace $U \le \mathbb{F}^n$ is called a *totally-isotropic space* of $\mathcal{A}$, if for any $u, u' \in U$, and any $A \in \mathcal{A}$, $u^t A u' = 0$.

The correspondence between independent sets and totally-isotropic spaces is supported by the following. Recall that $\alpha(G)$ denotes *independence number* of a graph G. Similarly, define the *totally-isotropic number* of $\mathcal{A}$, $\alpha(\mathcal{A})$, to be the maximum dimension over all totally-isotropic spaces of $\mathcal{A}$. Letting $\mathcal{A}_G$ be constructed from a graph G as in Equation 3, it is shown in [BCG$^+$20] that $\alpha(G) = \alpha(\mathcal{A}_G)$. Based on this correspondence, several classical questions for independent sets are found to have natural correspondences in the alternating matrix space setting, with applications to group theory and quantum information theory [BCG$^+$20].

Remark 1.2. It is interesting to study enumerating questions for other types of matrix spaces, such as symmetric matrix spaces over finite fields. We came to alternating matrix spaces mostly because of the connections between graphs and alternating matrix spaces as described above. For example, while it is natural to define totally-isotropic spaces for symmetric matrix spaces, it is not clear to us whether a result as $\alpha(G) = \alpha(\mathcal{A}_G)$ [BCG$^+$20] would hold in the symmetric setting.

Remarks for future research. The results presented in this paper are mostly straightforward, and the corresponding graph enumeration results were all known in the 1950's. It is our hope that more q-analogues of formulas from graph enumeration will be found in the near future.

For graph enumeration, the usefulness of the formulas is usually evidenced by the ability to calculate the exact numbers of graphs of order n satisfying certain properties (as seen in e.g. [HP73]). On the contrary, we do not expect our formulas could be used so, as the Galois numbers (see Section 2) are already difficult to be evaluated exactly [GR69].

In the future, we expect that, instead of exact recursive enumeration formulas, asymptotic enumerations could be more useful for e.g. algorithms and probabilistic analysis, as also in the case of graph enumeration. Previous works of the author with collaborators [LQ17] (improved later in [BLQW20]) support this possibility. Let c be a constant. In [LQ17], it is shown that the automorphism group of a random cn-dimensional alternating matrix space $\mathcal{A}$ in $\Lambda(n, q)$ is of order $q^{O(n)}$. Here, a random $\mathcal{A}$ means drawing uniformly random from the $\left[\binom{n}{2} \atop m \right]_q$-many m-dimensional subspaces of $\Lambda(n, q)$. This is a q-analogue of the well-known Erdős-Rényi model [ER59]. Therefore the result in [LQ17] can be viewed as the q-analogue of the celebrated result that when m is

asymptotically within $\frac{1}{2}n \log n$ and $\binom{n}{2} - \frac{1}{2}n \log n$, the automorphism group of a random graph with n vertices and m edges is trivial (i.e. of order 1) [ER63, Wri71].

We didn't touch the topic of enumerating coordinate-free alternating matrix spaces, which corresponds to enumerating unlabelled graphs. Enumerating coordinate-free alternating matrix spaces can be understood as enumerating the orbits of $\Lambda(n, q)$ under the natural action of $\mathrm{GL}(n, q)$ (see Section 2). We leave this topic to a future work.

Structure of the paper. After presenting some preliminaries in Section 2, we prove a q-analogue of Read's formula in Section 3, a q-analogue of Gilbert's formula in Section 4, and a q-analogue of Riddell's formula in Section 5.

2 Preliminaries

Some notions for alternating matrix spaces. A natural group action of $\mathrm{GL}(n, \mathbb{F})$ on $\Lambda(n, \mathbb{F})$ is as follows: for $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ and $T \in \mathrm{GL}(n, \mathbb{F})$, T sends $\mathcal{A}$ to $T^t \mathcal{A} T = \{T^t A T : A \in \mathcal{A}\}$. Then the *automorphism group* of $\mathcal{A}$, $\mathrm{Aut}(\mathcal{A}) = \{T \in \mathrm{GL}(n, \mathbb{F}) : \mathcal{A} = T^t \mathcal{A} T\}$. We say that $\mathcal{A}, \mathcal{B} \leq \Lambda(n, \mathbb{F})$ are isomorphic, if there exists $T \in \mathrm{GL}(n, \mathbb{F})$, such that $\mathcal{A} = T^t \mathcal{B} T$.

For $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, the *radical* of $\mathcal{A}$ is $\mathrm{rad}(\mathcal{A}) := \{v \in \mathbb{F}^n : \forall A \in \mathcal{A}, Av = 0\}$. We say that $\mathcal{A}$ is *degenerate*, if $\mathrm{rad}(\mathcal{A}) \neq 0$.

Given a d-dimensional $U \leq \mathbb{F}^n$, let T be the matrix of size $n \times d$ in column echelon form whose columns span U. The *restriction* of $\mathcal{A}$ on U is defined as $\mathcal{A}|_U := \{T^t A T : A \in \mathcal{A}\} \leq \Lambda(d, \mathbb{F})$.

Some basic q-calculus. We present some notation and basic facts from the so-called q-calculus [KC02]. For $n \in \mathbb{N}$ and a prime power q, let $[n]_q := \frac{q^n - 1}{q - 1} = q^{n-1} + \cdots + 1$. The q-factorial $[n]_q! = [n]_q \cdot [n-1]_q \cdot \ldots \cdot [1]_q$. The Gaussian binomial coefficient $\begin{bmatrix} n \\ d \end{bmatrix}_q$ can then be written as $\frac{[n]_q!}{[d]_q![n-d]_q!}$, which counts the number of d-dimensional subspaces of $\mathbb{F}_q^n$. The q-multimonomial coefficient is $\begin{pmatrix} n \\ n_1, \ldots, n_c \end{pmatrix}_q := \frac{[n]_q!}{[n_1]_q! \ldots [n_c]_q!}$.

Following Goldman and Rota [GR69] (see also [KC02]), define the nth Galois number over q GalN_n^q to be $\sum_{d=0}^n \begin{bmatrix} n \\ d \end{bmatrix}_q$, which is the total number of subspaces of $\mathbb{F}_q^n$.

Let $\mathrm{G}_n = 2^{\binom{n}{2}}$ be the number of labelled graphs of order n. Let $\mathrm{G}_{n,q} = \mathrm{GalN}_{\binom{n}{2}}^q$ be the number of subspaces of $\Lambda(n, q)$.

Eulerian generating functions. We recall the notions of Eulerian generating functions, which are q-analogues of exponential generating functions. There are actually two versions of Eulerian generating functions.

Let U be a vector space, and $V \leq U$ be a subspace. We can consider the quotient space U/V, or complement subspaces of V in U. Note that complement subspaces of V in U, i.e. those $W \leq U$, $W \cap V = 0$, and $\langle W, V \rangle = U$, are not unique. If V is a d-dimensional subspace of $U = \mathbb{F}_q^n$, then there are $q^{d(n-d)}$-many complement subspaces of V in U.

The distinction between quotient spaces and complement spaces leads to two types of Eulerian generating functions. The Eulerian generating function for quotient spaces was first studied by Goldman and Rota in [GR70]. To the best of our knowledge, the Eulerian generating function for complement spaces was first used explicitly by Srinivasan in [Sri06]. We won't go into a detailed comparison between these two notions, but only indicate a key here: the coefficient of the Gaussian convolution for the Eulerian generating function in [GR70] is $\begin{bmatrix} n \\ d \end{bmatrix}_q$, while that in [Sri06] is $\begin{bmatrix} n \\ d \end{bmatrix}_q \cdot q^{d(n-d)}$, where the extra $q^{d(n-d)}$ is to take care of multiple complement subspaces.

In this article we shall use the Eulerian generating function in [Sri06].

3   From vertex c-colourings to isotropic c-decompositions

In the introduction we have seen Read's formula and its q-analogue. In this section we present a detailed exposition and a proof.

Totally-isotropic spaces for an alternating matrix space $\mathcal{A} \leq \Lambda(n, \mathbb{F})$ were defined in Definition 1.1, and results in [BCG$^+$20] indicate that totally-isotropic spaces can be studied as a linear algebraic analogue of independent sets. In [BCG$^+$20], the following notion is also proposed.

Definition 3.1. Let $\mathcal{A} \leq \Lambda(n, \mathbb{F})$. A direct sum decomposition $\mathbb{F}^n = U_1 \oplus \cdots \oplus U_c$ is a *totally-isotropic c-decomposition* of $\mathcal{A}$, if each U_i is a totally-isotropic space of $\mathcal{A}$.

In the following we shall only consider totally-isotropic c-decompositions which are non-trivial, i.e. none of U_i's are the zero space. The totally-isotropic decomposition number of $\mathcal{A}$, $\chi(\mathcal{A})$, is the smallest $c \in \mathbb{N}$ such that $\mathcal{A}$ admits a totally-isotropic c-decomposition. Let G be a graph and let $\mathcal{A}_G$ be constructed from G as in Equation 3. It is shown in [BCG$^+$20] that $\chi(G) = \chi(\mathcal{A}_G)$. Therefore, totally-isotropic decompositions can be viewed as a linear algebraic analogue of vertex colorings.

Read gave a formula for the number of labelled c-coloured graphs [Rea60], generalising a result of Gilbert [Gil56]. In this section, we shall review Read's formula first, and then present the result on enumerating alternating matrix spaces with isotropic c-decompositions.

Review of enumerating c-colored labelled graphs. Following Read [Rea60], to enumerate c-colored labelled graphs with n vertices, we go through the following steps. It should be noted that a graph can be c-colored in several ways. So the following in fact enumerates pairs of the form (G, U) where $G = ([n], E)$ is a graph, and $U = (U_1, \ldots, U_c)$ is an ordered partition of $[n]$, such that each U_i is an independent set of G.

1. Enumerate ordered c-partition of n, i.e. $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, $\sum_{i \in [c]} n_i = n$.

2. Fix $(n_1, \ldots, n_c)$, an ordered partition of n. Enumerate the number of ways to allocate n_i vertices with color i. This is counted by the multinomial coefficient $\binom{n}{n_1, \ldots, n_c} = \frac{n!}{n_1! \cdot \ldots \cdot n_c!}$.

3. Fix an allocation of n_i vertices with color i. The number of graphs with this configuration is $2^{\binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}}$, as only edges from one color class to another are possibly present.

Summarising the above, Read's formula is

$$\sum_{(n_1, \ldots, n_c)} \binom{n}{n_1, \ldots, n_c} \cdot 2^{\kappa(n, n_1, \ldots, n_c)},$$

where $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n, and $\kappa(n, n_1, \ldots, n_c) := \binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}$. If the colors are not assume to have identity as in [HP73], then a multiplicative factor of $\frac{1}{c!}$ is required.

Enumerating alternating matrix spaces with totally-isotropic c-decompositions. Following Read's recipe, we can enumerate alternating matrix spaces with totally-isotropic c-decompositions.

1. Enumerate ordered c-partitions of n, i.e. $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, $\sum_{i \in [c]} n_i = n$.

2. Fix $(n_1, \ldots, n_c)$, an ordered partition of n. Enumerate the number of tuples of subspaces $(U_1, \ldots, U_c)$, $U_i \leq \mathbb{F}_q^n$, such that $\dim(U_i) = n_i$, and $\mathbb{F}_q^n = U_1 \oplus \cdots \oplus U_c$. We shall refer to

5

this tuple of subspaces an *ordered direct sum decomposition* of $\mathbb{F}_q^n$. This number is, by [Sri06, Lemma 4],

$$\frac{q^{\binom{n}{2}} \cdot [n]_q!}{(q^{\binom{n_1}{2}} \cdot [n_1]_q!) \dots (q^{\binom{n_c}{2}} \cdot [n_c]_q!)}.$$

3. Fix an ordered direct sum decomposition $(U_1, \dots, U_c)$ of $\mathbb{F}_q^n$. Requiring U_i's where $\dim(U_i) = n_i$ to be totally-isotropic spaces impose $\sum_{i \in [c]} \binom{n_i}{2}$ independent linear conditions on $\Lambda(n, q)$. So the number of alternating matrix spaces with U_i's being isotropic spaces is $\text{GalN}^q_{\binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}}$.

Summarising, we obtain a q-analogue of Read's formula which counts the number of alternating matrix spaces with totally-isotropic c-decompositions:

$$\sum_{(n_1, \dots, n_c)} \frac{q^{\binom{n}{2}} \cdot [n]_q!}{(q^{\binom{n_1}{2}} \cdot [n_1]_q!) \dots (q^{\binom{n_c}{2}} \cdot [n_c]_q!)} \cdot \text{GalN}^q_{\binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}}$$

$$= \sum_{(n_1, \dots, n_c)} \binom{n}{n_1, \dots, n_c}_q \cdot q^{\kappa(n, n_1, \dots, n_c)} \cdot \text{GalN}^q_{\kappa(n, n_1, \dots, n_c)},$$

where $(n_1, \dots, n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n, and $\kappa(n, n_1, \dots, n_c) = \binom{n}{2} - \sum_{i \in [c]} \binom{n_i}{2}$. If unordered direct sum decompositions rather than ordered direct sum decompositions are counted, then a multiplicative factor of $\frac{1}{c!}$ is required.

4 From connectivity to direct and orthogonal indecomposabilities

Let us first define the structures of alternating matrix spaces to be studied in this section. We say that a direct sum decomposition of $\mathbb{F}_q^n = U_1 \oplus \dots \oplus U_k$ is non-trivial, if none of U_i is the zero space.

Definition 4.1. For an alternating matrix space $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, a non-trivial direct sum decomposition $\mathbb{F}^n = U_1 \oplus \dots \oplus U_k$ is an *orthogonal decomposition* of $\mathcal{A}$, if for any $i \neq j$, $u_i \in U_i$, $u_j \in U_j$, and $A \in \mathcal{A}$, $u_i^t A u_j = 0$. An orthogonal decomposition is a *direct decomposition*, if $\dim(\mathcal{A}) = \sum_{i \in [k]} \dim(\mathcal{A}|_{U_i})$.

We say that $\mathcal{A}$ is *orthogonally decomposable*, if it admits an orthogonal decomposition into $k \geq 2$ subspaces. It is *directly decomposable*, if it admits a direct decomposition into $k \geq 2$ subspaces.

An orthogonal (resp. direct) decomposition $U = U_1 \oplus \dots \oplus U_k$ is *complete*, if for any U_i, $\mathcal{A}|_{U_i}$ is orthogonally (resp. directly) indecomposable.

Let G be a graph, and let $\mathcal{A}_G$ be constructed from G as in Equation 3. In [LQ20], it was shown that G is disconnected if and only if $\mathcal{A}_G$ is orthogonally decomposable. Actually, it is straightforward to see that orthogonally decomposable there can be strengthened to directly decomposable. Therefore, both orthogonal indecomposability and direct indecomposability can be viewed as linear algebraic analogues of connectivity.

Interestingly, orthogonal indecomposability and direct indecomposability behave quite differently. On one hand, by [Wil12, Lemma 6.9 (iii)], if $\mathcal{A}$ is non-degenerate, then $\mathcal{A}$ has a unique complete direct decomposition. On the other hand, by [Wil09, Theorem 1.1 (ii)], the number of complete orthogonal decompositions can be any positive integer even under the automorphism group of $\mathcal{A}$. Therefore it is not surprising that the same strategy for enumerating alternating matrix spaces with totally-isotropic c-decompositions can be applied to enumerating alternating

matrix spaces with orthogonal c-decompositions in a straightforward fashion. So we present the formula here without giving the details:

$$\sum_{(n_1,\ldots,n_c)} \frac{q^{\binom{n}{2}} \cdot [n]_q!}{(q^{\binom{n_1}{2}} \cdot [n_1]_q!)\ldots(q^{\binom{n_c}{2}} \cdot [n_c]_q!)} \cdot \mathrm{GalN}^q_{\sum_{i \in [c]} \binom{n_i}{2}}. \tag{4}$$

In the following, we focus on direct decompositions. We first review Gilbert's formula for enumerating connected graphs in Section 4.1. We then derive a q-analogue of this formula in the setting of enumerating directly indecomposable alternating matrix spaces in Section 4.2.

4.1 Review of enumerating connected graphs

Let us review the classical formula of Gilbert [Gil56] and its proof following Harary and Palmer [HP73, Eq. 1.2.], which uses the notion of rooted graphs. Recall that a *rooted graph* is a graph $G = ([n], E)$ with one of the vertices $v \in [n]$, called the root, distinguished from others.

Recall that $\mathrm{G}_n = 2^{\binom{n}{2}}$ denotes the number of labelled graphs of order n. Let RG_n be the number of rooted, labelled graphs of order n. Let CG_n be the number of connected labelled graphs of order n. On one hand, a graph of order n gives rise to n rooted graphs, so $\mathrm{RG}_n = n \cdot \mathrm{G}_n$. On the other hand, we count the number of rooted, labelled graphs depending on the size of the connected component containing the root, as follows.

1. Enumerate $k \in [n]$ as the size of the connected component containing the root.

2. Fix $k \in [n]$. Enumerate $S \subseteq [n]$, $|S| = k$. In the following, S will contain the root.

3. Fix $S \subseteq [n]$, $|S| = k$. Enumerate connected, labelled graphs with the vertex set being S. Enumerate $v \in S$, where v is chosen as the root.

4. Enumerate labelled graphs with the vertex set being $[n] \setminus S$.

The above recipe gives that $\mathrm{RG}_n = \sum_{k=1}^{n} k \cdot \binom{n}{k} \cdot \mathrm{CG}_k \cdot \mathrm{G}_{n-k}$. Therefore by $\mathrm{RG}_n = n \cdot \mathrm{G}_n$, we get

$$\mathrm{CG}_n = \mathrm{G}_n - \frac{1}{n} \cdot \sum_{k=1}^{n-1} k \cdot \binom{n}{k} \cdot \mathrm{CG}_k \cdot \mathrm{G}_{n-k}. \tag{5}$$

4.2 Enumerating directly indecomposable alternating matrix spaces

Following the recipe in Section 4.1, we can enumerate directly indecomposable alternating matrix spaces as follows. However, a little care will be needed to handle degenerate alternating matrix spaces.

The issue with degenerate alternating matrix spaces. Let us first formally cite a result of J. B. Wilson, which forms the basis for our enumeration formula. Recall the notion of complete direct decompositions in Definition 4.1.

Theorem 4.2 ([Wil12, Lemma 6.9 (iii)]). *Let $\mathcal{A} \leq \Lambda(n, q)$ be non-degenerate. Then there exists a unique complete direct decomposition for $\mathcal{A}$.*

If $\mathcal{A} \leq \Lambda(n, q)$ is degenerate, then it can have several complete direct decompositions, which leads to over-counting if we follow the recipe in Section 4.1 directly. Let us present an example to explain how this over-counting occurs. In analogy with rooted graphs, we define rooted alternating matrix spaces. That is, a *rooted alternating matrix space* is a pair $(\mathcal{A}, v)$ where $\mathcal{A} \leq \Lambda(n, \mathbb{F})$, and $v \neq 0 \in \mathbb{F}^n$ is called the root.

Example 4.3. Let us follow the recipe in Section 4.1 for $\Lambda(5, q)$. In Step 1, set $k = 2$. In Step 2, it is natural to enumerate direct sum decompositions $\mathbb{F}_q^5 = U_1 \oplus U_2$, where $\dim(U_1) = 2$ and $\dim(U_2) = 3$. Let e_i be the ith standard basis vector, and $C = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$.

1. Let $U_1 = \langle e_1, e_2 \rangle$, $U_3 = \langle e_3, e_4, e_5 \rangle$, and the root vector be e_2. For $\mathcal{A}|_{U_1}$ there is only one choice, namely $\Lambda(2, q)$. Then suppose $\mathcal{A}|_{U_2} = \langle C \rangle$.

2. Now consider $V_1 = \langle e_1 + e_5, e_2 \rangle$, $V_2 = \langle e_3, e_4, e_5 \rangle$, and the root vector be e_2. Let $\mathcal{B}|_{V_1} = \Lambda(2, q)$, and let $\mathcal{B}|_{V_2} = \langle C \rangle$.

Clearly, $\mathcal{A}$ and $\mathcal{B}$ are the same alternating matrix space namely

$$\left\langle \begin{bmatrix} 0 & 1 & & & \\ -1 & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & 1 & \\ & & -1 & 0 & \\ & & & & 0 \end{bmatrix} \right\rangle \leq \Lambda(5, q),$$

but it will be counted twice when enumerating the direct sum decompositions $U_1 \oplus U_2$ and $V_1 \oplus V_2$.

The above examples leads us to ponder on Gilbert's formula in Equation 5. The formula is correct because for any graph, there is a unique way to partition the vertex set into a disjoint union of connected components. In the alternating matrix space setting, since Theorem 4.2 ensures the uniqueness of complete direct decompositions only in the non-degenerate case, it will be natural to focus on non-degenerate alternating matrix spaces.

The number of non-degenerate alternating matrix spaces. The number of non-degenerate alternating matrix spaces is in complete analogy with the number of graphs without isolated vertices. Let us first recall a basic formula for graphs without isolated vertices. Let NDG_n be the number of labelled graphs on n vertices without isolated vertices. Set $\mathrm{NDG}_0 = 1$. We can relate NDG_n with G_n as follows. First, fix a size-k subset S of $[n]$ as isolated vertices. Second, put a graph with $n - k$ vertices without isolated vertices on $[n] \setminus S$. This gives that $\mathrm{G}_n = \sum_{i=0}^n \binom{n}{k} \mathrm{NDG}_{n-k} = \sum_{i=0}^n \binom{n}{k} \mathrm{NDG}_k$.

Analogously, let $\mathrm{NDS}_{n,q}$ be the number of non-degenerate spaces of $\Lambda(n, q)$. Set $\mathrm{NDS}_{0,q} = 1$. We can related $\mathrm{NDS}_{n,q}$ with $\mathrm{G}_{n,q}$ as follows. First fix a k-dimensional subspace U of $\mathbb{F}_q^n$ as the radical (defined in Section 2), and choose any complement subspace V of U in $\mathbb{F}_q^n$. Second, put a non-degenerate alternating matrix space in $\Lambda(n - k, q)$ with the *support space* being V. That is, first fix a linear isomorphism $T : \mathbb{F}_q^{n-k} \to V$, represented by a $(n - k) \times n$ matrix, and then send $\mathcal{A} \leq \Lambda(n - k, q)$ to $T^t \mathcal{A} T \leq \Lambda(n, q)$. This gives that

$$\mathrm{G}_{n,q} = \sum_{i=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q \mathrm{NDS}_{n-k,q} = \sum_{i=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q \mathrm{NDS}_{k,q}. \tag{6}$$

Because of Equation 6, we shall assume that $\mathrm{NDS}_{n,q}$ is known from $\mathrm{G}_{n,q}$.

A q-analogue of Gilbert's formula. Let $\mathrm{DIS}_{n,q}$ be the number of direct-indecomposable, non-degenerate alternating matrix spaces in $\Lambda(n, q)$. Let $\mathrm{RS}_{n,q}$ be the number of rooted, non-degenerate spaces of $\Lambda(n, q)$. Recall that $\mathrm{NDS}_{n,q}$ denotes the number of non-degenerate spaces of $\Lambda(n, q)$. On one hand, an alternating matrix space in $\Lambda(n, q)$ yields $(q^n - 1)$ rooted alternating matrix spaces, so $\mathrm{RS}_{n,q} = (q^n - 1) \cdot \mathrm{NDS}_{n,q}$. On the other hand, we count the number of rooted, non-degenerate alternating matrix spaces depending on the dimension of the subspace containing the root.

1. Enumerate $k \in \{2, \ldots, n\}$ as the dimension of the subspace containing the root.

2. Fix $k \in [n]$. Enumerate $U \leq \mathbb{F}^n$, $\dim(U) = k$, and enumerate complement subspaces of U. In the following, U will contain the root.

3. Fix $U \leq \mathbb{F}^n$, $\dim(U) = k$. Enumerate directly indecomposable non-degenerate alternating matrix spaces with the support space being U. Enumerate non-zero vectors in U as the root.

4. Fix a complement subspace of U in $\mathbb{F}^n$. Let it be V. Enumerate non-degenerate alternating matrix spaces with the support space being V.

The above recipe gives that $\text{RS}_{n,q} = \sum_{k=2}^{n}(q^k - 1) \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot q^{k(n-k)} \cdot \text{DIS}_{k,q} \cdot \text{NDS}_{n-k,q}$. Therefore using $\text{RS}_{n,q} = (q^n - 1) \cdot \text{NDS}_{n,q}$, we have

$$\text{DIS}_{n,q} = \text{NDS}_{n,q} - \frac{1}{[n]_q} \cdot \sum_{k=2}^{n-1} [k]_q \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot q^{k(n-k)} \cdot \text{DIS}_{k,q} \cdot \text{NDS}_{n-k,q}. \tag{7}$$

For graphs, we can derive a version of Gilbert's formula in Equation 5 for graphs without isolated vertices. That formula would be the same as setting $q = 1$ there in Equation 7.

5 From labelled counting lemma to coordinate-explicit counting lemma

The exponential generating function and the labelled counting lemma are basic tools in graph enumeration. We first review them below. We then present a corresponding lemma for enumerating alternating matrix spaces, building on the work of Srinivasan [Sri06].

Review of the labelled counting lemma. Given a function $f : \mathbb{Z}^+ \to \mathbb{N}$ and a variable x, the exponential generating function for f in x is $\exp(f, x) = \sum_{n \in \mathbb{Z}^+} f(n) \cdot \frac{x^n}{n!}$. When the variable x is understood from the context, we may simply write $\exp(f, x)$ as $\exp(f)$. Given $f_i : \mathbb{Z}^+ \to \mathbb{N}$, $i \in [c]$, suppose $\prod_{i \in [c]} \exp(f_i, x) = \sum_{n \in \mathbb{N}} f(n) \cdot \frac{x^n}{n!} = \exp(f, x)$, where $f : \mathbb{Z}^+ \to \mathbb{N}$. Then $f(n) = \sum_{(n_1, \ldots, n_c)} \binom{n}{n_1, \ldots, n_c} \cdot \prod_{i \in [c]} f_i(n_i)$, where $(n_1, \ldots, n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n. The above, when interpreting in the context of graphs, leads to the following.

Lemma 5.1 (Labelled counting lemma, see e.g. [HP73, pp. 8]). *Let $f_i, f : \mathbb{Z}^+ \to \mathbb{N}$ be from above. Suppose $f_i : \mathbb{Z}^+ \to \mathbb{N}$ is the exponential generating function for the number of labelled graphs satisfying property P_i. Then $f(n)$ counts the number of tuples of labelled graphs $(G_1, \ldots, G_c)$, such that G_i satisfies P_i, the sum of orders of G_i is n, and the union of the vertex sets of G_i is $[n]$.*

An immediate application of the labelled counting lemma is the following relation discovered by Riddell [Rid51] (cf. [HP73, pp. 8]). Recall that G_n counts the number of labelled graphs of order n, and CG_n counts the number of connected labelled graphs of order n. With a little manipulation, the labelled counting lemma gives that $\exp(\text{G}) = \sum_{c=1}^{\infty} \exp(\text{CG})^c / c!$, which can be recorded conveniently as

$$1 + \exp(\text{G}) = e^{\exp(\text{CG})}. \tag{8}$$

A coordinate-explicit counting lemma. Following Srinivasan [Sri06], we define the following. Given a function $f : \mathbb{Z}^+ \to \mathbb{N}$, a variable x, and a prime power q, the Eulerian generating function for f in x and q is

$$\exp_q(f, x) = \sum_{n \in \mathbb{Z}^+} f(n) \cdot \frac{x^n}{q^{\binom{n}{2}} \cdot [n]_q!}.$$

We may omit x and write $\exp_q(f,x)$ in the following.

Given $f_i : \mathbb{Z}^+ \to \mathbb{N}$, $i \in [c]$, suppose $\prod_{i\in[c]} \exp_q(f_i,x) = \sum_{n\in\mathbb{Z}^+} f(n) \cdot \frac{x^n}{q^{\binom{n}{2}} \cdot [n]_q!} = \exp_q(f,x)$. Then by [Sri06, Theorem 5],

$$f(n) = \sum_{(n_1,\ldots,n_c)} \frac{q^{\binom{n}{2}} \cdot [n]_q!}{(q^{\binom{n_1}{2}} \cdot [n_1]_q!)\ldots(q^{\binom{n_c}{2}} \cdot [n_c]_q!)} \cdot \prod_{i\in[c]} f_i(n_i),$$

where $(n_1,\ldots,n_c)$, $n_i \in \mathbb{Z}^+$, goes over all ordered c-partition of n.

The above, when interpreting in the context of alternating matrix spaces, leads to the following.

Lemma 5.2 (Coordinate-explicit counting lemma). *Let $f_i, f : \mathbb{Z}^+ \to \mathbb{N}$ be from above. Suppose $f_i : \mathbb{Z}^+ \to \mathbb{N}$ is the Eulerian generating function for the number of alternating matrix spaces satisfying property P_i. Then $f(n)$ counts the number of tuples of coordinate-explicit alternating matrix spaces $(\mathcal{A}_1,\ldots,\mathcal{A}_c)$, such that $\mathcal{A}_i$ satisfies P_i, $\mathcal{A}_i$ supported by $U_i \leq \mathbb{F}_q^n$ of dimension $n_i \in \mathbb{Z}^+$, $\sum_{i\in[c]} n_i = n$, and $\mathbb{F}^n = U_1 \oplus \cdots \oplus U_c$.*

(For the notion of $\mathcal{A}_i$ supported by U_i, see the discussion before Equation 6.)

Based on the above, we can derive a q-analogue of Riddell's formula. The following is essentially a consequence of [Sri06, Theorem 6]. Recall that $\mathrm{NDS}_{n,q}$ counts the number of non-degenerate spaces of $\Lambda(n,q)$, and $\mathrm{DIS}_{n,q}$ counts the number of directly indecomposable, non-degenerate spaces of $\Lambda(n,q)$. By Lemma 5.2, $\exp_q(\mathrm{DIS})^c$ is the Eulerian generating function of ordered c-tuples of directly indecomposable, non-degenerate alternating matrix spaces, whose support spaces form a direct sum decomposition of the underlying vector space. Then the coefficient of $x^n/(q^{\binom{n}{2}} \cdot [n]_q!)$ of $\exp_q(\mathrm{DIS})^c/c!$ is the number of non-degenerate spaces of $\Lambda(n,q)$ whose complete direct decompositions have c summands. It follows that $\exp_q(\mathrm{NDS}) = \sum_{c=1}^{\infty} \exp_q(\mathrm{DIS})^c/c!$, which can be convenient recorded as

$$1 + \exp_q(\mathrm{NDS}) = e^{\exp_q(\mathrm{DIS})}. \tag{9}$$

Let us also add that the correctness of the above reasoning follows from Theorem 4.2.

References

[BCG+20] 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. In *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*, pages 8:1–8:48, 2020. Journal version accepted to SIAM J. Comput.

[BLQW20] Peter A. Brooksbank, Yinan Li, Youming Qiao, and James B. Wilson. Improved algorithms for alternating matrix space isometry: From theory to practice. In Fabrizio Grandoni, Grzegorz Herman, and Peter Sanders, editors, *28th Annual European Symposium on Algorithms, ESA 2020, September 7-9, 2020, Pisa, Italy (Virtual Conference)*, volume 173 of *LIPIcs*, pages 26:1–26:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[ER59]   Paul Erdős and Alfréd Rényi. On random graphs I. *Publ. Math. Debrecen*, 6:290–297, 1959.

[ER63]   Paul Erdős and Alfréd Rényi. Asymmetric graphs. *Acta Mathematica Hungarica*, 14(3-4):295–315, 1963.

[Gil56]   E. N. Gilbert. Enumeration of labelled graphs. *Canadian Journal of Mathematics*, 8:405–411, 1956.

[GR69]   Jay Goldman and Gian-Carlo Rota. The number of subspaces of a vector space. In *Recent Progress in Combinatorics, Proc. Third Waterloo Conf. on Combinatorics, 1968*, pages 75–83. Academic Press, New York, 1969.

[GR70]   Jay Goldman and Gian-Carlo Rota. On the foundations of combinatorial theory IV finite vector spaces and eulerian generating functions. *Studies in Applied Mathematics*, 49(3):239–258, 1970.

[HP73]   Frank Harary and Edgar M. Palmer. *Graphical Enumeration*. Academic Press, 1973.

[HQ20]   Xiaoyu He and Youming Qiao. On the Baer-Lovász-Tutte construction of groups from graphs: isomorphism types and homomorphism notions, 2020. arXiv:2003.07200.

[KC02]   Victor Kac and Pokman Cheung. *Quantum calculus*. Universitext. Springer-Verlag, 2002.

[Lov79]   László Lovász. On determinants, matchings, and random algorithms. In *Fundamentals of Computation Theory, FCT 1979, Proceedings of the Conference on Algebraic, Arthmetic, and Categorial Methods in Computation Theory, Berlin/Wendisch-Rietz, Germany, September 17-21, 1979*, pages 565–574, 1979.

[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.

[LQ20]   Yinan Li and Youming Qiao. Group-theoretic generalisations of vertex and edge connectivities. *Proceedings of the American Mathematical Society*, 148(11):4679–4693, 2020.

[Rea60]   R. C. Read. The number of k-coloured graphs on labelled nodes. *Canadian Journal of Mathematics*, 12:410–414, 1960.

[Rid51]   R. J. Riddell. *Contributions to the theory of condensation*. PhD thesis, Univ. of Michigan, Ann Arbor, 1951.

[Sri06]   Murali K. Srinivasan. The Eulerian generating function of q-derangements. *Discrete mathematics*, 306(17):2134–2140, 2006.

[Tut47]   W. T. Tutte. The factorization of linear graphs. *Journal of the London Mathematical Society*, s1-22(2):107–111, 1947.

[Wil09]   James B. Wilson. Decomposing *p*-groups via Jordan algebras. *J. Algebra*, 322:2642–2679, 2009.

[Wil12]   James B. Wilson. Existence, algorithms, and asymptotics of direct product decompositions, I. *Groups Complexity Cryptology*, 4(1):33–72, 2012.

[Wri71]   Edward M. Wright. Graphs on unlabelled nodes with a given number of edges. *Acta Mathematica*, 126(1):1–9, 1971.