Diagonal Forms, Linear Algebraic Methods and Ramsey-Type Problems

Thesis by

Wing Hong Tony Wong

In Partial Fulfillment of the Requirements
for the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California

2013
(Defended May 28, 2013)

To my wife, Jane, who offers me unconditional love, care and support throughout the course of this thesis.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my advisor, Prof. Richard M. Wilson, for his guidance, teaching, patience and support. His extensive knowledge in combinatorics and unparalleled skills in teaching inspire and sparkle me tremendously. I am very fortunate to be able to work closely with him for four years on numerous projects, and our collaboration work lays down the most important foundation for my thesis and beyond.

I would also like to thank my friends and collaborators, Mr. Edward S. C. Fan, with whom I always enjoy discussing about mathematics, and Mr. Michel van Garrel, who is always giving me useful advices and supportive comments.

A very special thank goes to Dr. Cheng Yeaw Ku, my mentor in the Summer Undergraduate Research Fellowship at California Institute of Technology in 2006, when I was a sophomore in the Chinese University of Hong Kong. He is the one who introduces me to frontier research in combinatorics.

Another special thank goes to the Sir Edward Youde Memorial Fund for providing a three-year Overseas Fellowship to support my graduate studies.

Lastly, I would like to thank my parents, for their constant care and love, as well as being the perfect role models and moral exemplars for me, and my elder brother, the very first mathematics teacher in my life.

Abstract

This thesis focuses mainly on linear algebraic aspects of combinatorics. Let $N_t(H)$ be an incidence matrix with edges versus all subhypergraphs of a complete hypergraph that are isomorphic to H. Richard M. Wilson and the author find the general formula for the Smith normal form or diagonal form of $N_t(H)$ for all simple graphs H and for a very general class of t-uniform hypergraphs H.

As a continuation, the author determines the formula for diagonal forms of integer matrices obtained from other combinatorial structures, including incidence matrices for subgraphs of a complete bipartite graph and inclusion matrices for multisets.

One major application of diagonal forms is in zero-sum Ramsey theory. For instance, Caro's results in zero-sum Ramsey numbers for graphs and Caro and Yuster's results in zero-sum bipartite Ramsey numbers can be reproduced. These results are further generalized to t-uniform hypergraphs. Other applications include signed bipartite graph designs.

Research results on some other problems are also included in this thesis, such as a Ramsey-type problem on equipartitions, Hartman's conjecture on large sets of designs and a matroid theory problem proposed by Welsh.

Contents

Chapter 1

Introduction

1.1 Integer matrices and Smith normal form

Understanding integer matrices is essential in the studies of many combinatorial problems. For instance, it was the study of a hypothetical self-dual binary code arising from a putative projective plane of order 10 that led to the proof of the nonexistence of such a plane [16], while the p-rank for primes p of the inclusion matrices was used to prove the Frankl-Wilson inequalities [10] that have geometric consequences.

To understand the p-rank of an integer matrix or the structure of its row module over $\mathbb{Z}$, one of the most important techniques is to find the Smith normal form or a diagonal form of that matrix. This thesis is partly motivated by Wilson [27] and Brouwer and Van Eijl [5]. Both works determine the diagonal forms and Smith normal forms of matrices arising from special graphs and hypergraphs.

For any integer matrix A, there always exist two square integer matrices E and F, each with determinant ± 1, such that $EAF = D$ is a diagonal matrix. D is called a *diagonal form* of A, and E and F are called a *front* and a *back* of A respectively. If D has diagonal entries d_i dividing d_{i+1} for all i, then D is called the *Smith normal form*, or *Smith form*, of A.

There are numerous applications of Smith forms in combinatorics. In design theory, for example, Smith forms help with distinguishing nonisomorphic designs. In particular, Brouwer and Van Eijl [5] used Smith forms to identify nonisomorphic strongly regular graphs with the same parameters, and Chandler and Xiang [8] showed that certain difference sets (the HKM and Lin difference sets) and their associated designs are nonisomorphic by computing the Smith forms of their incidence matrices.

While it is easy to convert between the Smith form and a diagonal form of an integer matrix, the expression of a diagonal form is often much cleaner. Besides, a diagonal form is sometimes more natural to obtain by constructing a front explicitly. With a front, not only can we determine the corresponding diagonal form, the front also helps with determining whether a particular vector is in the row module of A. This technique is essential in the research on zero-sum Ramsey problems, discussed in chapter 5.

1.2 Incidence matrices for hypergraphs

Let X be a set of size v, and $\mathcal{T}$ be the set of all t-subsets of X, with $0 \le t \le v$. By a *t-vector* based on X, we refer to an integer vector $\mathbf{h}$ whose $\binom{v}{t}$ coordinates are indexed by $\mathcal{T}$.

Given a column t-vector $\mathbf{h}$, for each permutation σ in the symmetric group S_v, let $\sigma(\mathbf{h})$ be the t-vector such that for each $T \in \mathcal{T}$, $\sigma(\mathbf{h})(T) = \mathbf{h}(\sigma^{-1}(T))$. Let $N_t(\mathbf{h})$ be the matrix whose columns are all the images of $\mathbf{h}$ under the symmetric group S_v, i.e., $N_t(\mathbf{h}) = [\sigma(\mathbf{h})]_{\sigma \in S_v}$. In particular, if $\mathbf{h}$ is a zero-one vector, then we can view $\mathbf{h}$ as a characteristic vector of a simple t-uniform hypergraph H, and the corresponding incidence matrix can be written as $N_t(H)$.

The matrix $N_t(\mathbf{h})$ is a generalization of many integer matrices arising from set systems. Examples include integer matrices in the association algebras of Johnson schemes $J(n,t)$, as well as the inclusion matrices W_{tk}^{v} introduced in section 2.2.

Let $\mathbf{h}(T)$ denote the entry of $\mathbf{h}$ at coordinate $T \in \mathcal{T}$. $x \in X$ is an "isolated vertex" of $\mathbf{h}$ if $\mathbf{h}(T) = 0$ for all T containing x. Wilson [27] described a diagonal form for $N_t(\mathbf{h})$ when $\mathbf{h}$ has at least t isolated vertices. In chapter 2, this result is extended to a very general class of $\mathbf{h}$, namely all "primitive" $\mathbf{h}$ whose "shadows" are primitive or "multiples of primitive vectors", defined in section 2.3 (see theorem 2.3.3). It is further shown in section 2.4 that most t-vectors $\mathbf{h}$ satisfies this property, including those $\mathbf{h}$ with t isolated vertices.

Diagonal forms for $N_2(G)$, where G is a simple graph, are studied in greater details. The family of primitive graphs is treated in section 2.5, while the remaining nonprimitive graphs are tackled one by one in section 2.6. This work generalizes the results by some mathematicians interested in Smith forms. For example, $N_2(K_{2,k-2})$ is the adjacency matrix of the complement of the line graph of K_n, whose Smith form was given by Brouwer and Van Eijl [5].

1.3 Matrices for bipartite graphs and multisets

In the previous project, simple t-uniform hypergraphs, or simple graphs in particular, are embedded into a complete one. As a continuation, the author considers embeddings of simple bipartite graphs into complete bipartite ones.

Let G be a nonempty spanning subgraph of the complete bipartite graph $K_{n,n}$, i.e., G has $2n$ vertices, some of which may be isolated. As an analogue of the setting in chapter 2, let $\mathbf{h}$ be the characteristic vector of G. This means that $\mathbf{h}$ is a column vector indexed by the edge set of $K_{n,n}$ such that for each edge E in $K_{n,n}$, $\mathbf{h}(E) = 1$ if E is an edge of G and 0 otherwise. Let $\mathcal{P}$ be the graph automorphism group on $K_{n,n}$, and let $N = N(G)$ be the matrix whose columns are all the images of $\mathbf{h}$ under the action of $\mathcal{P}$.

The main results in chapter 3 are the expressions for a diagonal form of $N(G)$ for every nonempty spanning subgraph G in $K_{n,n}$ (see theorems 3.2.2 and 3.3.2).

This work on bipartite cases again leads to applications in zero-sum Ramsey theory, and Caro and Yuster's results on zero-sum bipartite Ramsey numbers [7] can be deduced as a corollary (see section 5.3). Besides, it gives the necessary and sufficient conditions for the existence of a signed bipartite graph design, which are previously unknown (see section 6.2).

Another direction is to consider a multiset system. Motivated by Ray-Chaudhuri and Singhi's ideas on studying designs via multisets [19], the author derives the diagonal forms and discover other properties for the inclusion matrices of multisets (see chapter 4).

1.4 Ramsey-type problems

The Ramsey problem is a classical graph coloring problem. One version of the Ramsey problem for hypergraphs can be stated as follows: Given a t-uniform hypergraph H and m colors, determine the minimum integer $R_m(H)$ such that for all $v \geq R_m(H)$, for all edge-coloring of $K_v^{(t)}$ with m colors, there exists a monochromatic H in $K_v^{(t)}$. Note that $K_v^{(t)}$ denotes the complete t-uniform hypergraph on v vertices.

The classical Ramsey problem is notoriously difficult. In fact, $R_2(K_5)$ is still unknown. Besides, the classical Ramsey numbers $R_m(H)$ grows exponentially with k in general, where k is the number of vertices of H. Many mathematicians thus start to look for variations of the Ramsey problem and try to make progress on those problems.

Zero-sum Ramsey problems are first studied by Bialostocki and Dierker [4] and Alon and Caro [3] in the 1990s. Let H be a t-uniform hypergraph with e edges and let $\mathbb{Z}_m$ be the set of colors such that $m \mid e$. The objective of the zero-sum Ramsey problem is to determine the minimum integer $ZR_m(H)$ such that for all $v \geq ZR_m(H)$, for all edge-coloring $c : E(K_v^{(t)}) \to \mathbb{Z}_m$, there exists a subgraph H' in $K_v^{(t)}$, H' isomorphic to H, such that the sum of the colors on $E(H')$ is 0 in $\mathbb{Z}_m$.

Using the notation in chapter 2, the zero-sum Ramsey problem is looking for the minimum integer $ZR_m(H)$ such that for all $v \geq ZR_m(H)$, the row module of $N_t(H^{\uparrow v})$ over $\mathbb{Z}_m$ does not contain a nowhere-zero vector. Here, $H^{\uparrow v}$ denotes the hypergraph obtained by adjoining isolated vertices to H so that the total number of vertices is v. Note that $ZR_m(H)$ is well-defined since $R_m(H)$ exists by classical Ramsey theorem. In particular, if $p = 2$, then the zero-sum Ramsey number $ZR_2(H)$ is the smallest integer such that for all $v \geq ZR_2(H)$, the binary code generated by $N_t(H^{\uparrow v})$ does not contain the vector $\mathbf{1}$ of all 1's.

Based on the formula for the diagonal forms and fronts of $N_t(H)$ given in theorem 2.3.3, it is shown in section 5.1 that vector $\mathbf{1}$ does not lie in the row module of $N_t(H)$ over $\mathbb{Z}_m$ if H is primitive and all its shadows are multiples of primitive. Together with the result in section 2.4, we conclude that $ZR_2(H) = k$ for almost all H, where k is the number of vertices of H (see theorem 5.1.4). This extends earlier results by Wilson [29], which gives $ZR_2(H) \leq k + t$

for all t-uniform hypergraph H.

As an analogue to the zero-sum Ramsey number, for each simple bipartite graph G, we define the zero-sum bipartite Ramsey number $ZB_m(G)$ as the smallest integer such that for all $n \geq ZB_m(G)$, for all edge-coloring $c : E(K_{n,n}) \to \mathbb{Z}_m$, there exists a subgraph G' in $K_{n,n}$, G' isomorphic to G, such that the sum of the colors on $E(G')$ is 0 in $\mathbb{Z}_m$. A complete characterization of $ZR_2(G)$ and $ZB_2(G)$ are given in [6] and [7] respectively, and these results are reproduced through the studies of the diagonal forms (see sections 5.2 and 5.3).

Another Ramsey-type problem that the author has studied is on hypergraphs induced by equipartitions on sets. Given a set X of v elements, consider the set $\mathcal{V}$ of all s-equipartitions, and the set $\mathcal{E}$ of all t-equipartitions, where $s \mid t \mid v$. Consider the hypergraph $H = H(s, t, v)$ with $\mathcal{V}$ as its vertex set, and an edge E of H is the set of s-equipartitions in $\mathcal{V}$ that has a common t-equipartition in $\mathcal{E}$ as a refinement.

It is conjectured that the Ramsey property holds for these hypergraphs on equipartitions, i.e., there exists v_0 such that for all $v \geq v_0$, for all 2-colorings of the vertices in $H(v, s, t)$, there exists a monochromatic edge in H. This conjecture is proved to be true for $s = 2$ and $t = 4$ (see section 5.4).

1.5 Some problems in design theory

Apart from the zero-sum Ramsey theory, the studies of incidence matrices have applications in design theory as well. In chapter 6, two of such applications are introduced. One of them is Hartman's conjecture about large sets of t-designs.

Hartman's conjecture is one of the most important problems in design theory. Translating back to the language of inclusion matrix, this conjecture is related to the existence of a vector consisting of only 1's and -1's in the null space of W_{tk}^{v}. This conjecture is solved in [1] for $t = 2$ as well as for some other cases (see [15] for more details). The author solved the case independently for $t = 2$ and $k = 3$, using some results from his studies of the inclusion matrix W_{tk}^{v}.

Another application is on signed graph design. This is a generalization of graph decomposition, studied by Wilson [25], Ushio [22] and many others. In section 6.2, the necessary and sufficient conditions for the existence of a signed bipartite graph design are given.

1.6 Number of bases in a matroid of fixed size and rank

One of the problems in matroid theory that Dominic Welsh [24] proposed is to determine all triples of integers (n, r, b), $0 < r \leq n$ and $1 \leq b \leq \binom{n}{r}$, for which there exists a matroid of rank r on n elements with exactly b bases. Mayhew and Royle [17] conjectured that there exists such a matroid for all triples except the case where $(n, r, b) = (6, 3, 11)$. Sivaraman [21] used computer program SAGE to verify the conjecture up to $n = 12$.

Given an $r \times n$ matrix A with full row rank over a field, the set of columns of A will form a linear matroid or column matroid with n elements and rank r, and a basis of this matroid is given by an invertible $r \times r$ submatrix. Edward S. T. Fan and the author [9] prove the conjecture for $1 \leq b \leq \binom{r+2}{r}$ by constructing these matrices explicitly (see chapter 7).

Chapter 2

Diagonal forms of incidence matrices arising from subhypergraphs of complete t-uniform hypergraphs

2.1 Diagonal forms of integer matrices

Two integer matrices A and B of the same size are $\mathbb{Z}$-*equivalent* if B can be obtained from A by a sequence of integral row and column operations (adding an integer multiple of one row or column to another row or column, or multiplying a row or column by -1). Alternatively, A and B are $\mathbb{Z}$-equivalent if there exist integer square matrices E and F with determinants ± 1 such that $EAF = B$.

If integer matrix A is $\mathbb{Z}$-equivalent to a diagonal matrix D, then D is called a *diagonal form of* A, and the list of diagonal entries of D are called *a list of diagonal factors of* A. Here, diagonal means that the (i, j)-entry of D is nonzero only if $i = j$. In the $\mathbb{Z}$-equivalence relation, if $EAF = D$ where E and F are integer square matrices with determinants ± 1, we call E a *front* and F a *back* of A. One remark is that for a fixed A and a diagonal form D, the choice of E and F is not unique.

Given A, if a list of diagonal factors $d_1, d_2, \ldots$ of A are nonnegative such that $d_i \mid d_{i+1}$ for all i, then D is the *Smith normal form of* A, and this list of diagonal factors is called the *invariant factors* or the *elementary divisors* of A. Note that the Smith normal form is unique for each A, while diagonal forms are not. Readers are referred to [18] for more background on Smith normal form.

It is clear that the rank of an integer matrix A is the number of nonzero entries in any list of diagonal factors. As an extension, for any prime p, the *p-rank*, or p^α*-rank* with $\alpha \in \mathbb{N}$, is the number of entries in any list of diagonal factors that are indivisible by p^α.

The number of diagonal factors of an $r \times s$ matrix A is the minimum of r and s, but sometimes it will be convenient to speak of diagonal factors $d_1, d_2, \ldots, d_r$ of an $r \times s$ matrix even when $r > s$, in which case it is to be understood that $d_i = 0$ for $s < i \leq r$, as if we have appended $r - s$ columns of all 0's to A. Notice that diagonal factors of A are also diagonal factors for $A^\top$, if we consider $\min\{r, s\}$ as the number of diagonal factors.

Integers $d_1, d_2, \ldots, d_r$ are diagonal factors for an $r \times s$ matrix A if and only if

$$\mathbb{Z}^r/\mathrm{col}_{\mathbb{Z}}(A) \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}, \tag{2.1}$$

where $\mathrm{col}_{\mathbb{Z}}(A)$ is the $\mathbb{Z}$-module (abelian group) generated by the columns of A. Here, we take the convention that $\mathbb{Z}_1 = \{0\}$ and $\mathbb{Z}_0 = \mathbb{Z}$. As we mentioned above, it is to be understood that $d_i = 0$ for $s < i \leq r$.

The group in (2.1) may be called the (column) *Smith group* $S(A)$ of A. The dimension of $S(A)$ as a finitely generated abelian group is the number of diagonal factors $d_1, \ldots, d_r$ that are equal to 0 and this is $r - \mathrm{rank}(A)$. We use $\tau(A)$ to denote the order of the torsion subgroup of $S(A)$, which is simply the product of the nonzero diagonal factors.

An integer matrix A is said to be *unimodular* if A is of square size and is $\mathbb{Z}$-equivalent to an identity matrix. In fact, it is easy to see that A is unimodular if and only if its determinant is ± 1. If A is rectangular of dimension $r \times s$ and has a unimodular submatrix of size r, then A is said to be *row-unimodular*. Equivalently, A is row-unimodular if a list of diagonal factors of A has r 1's, or if the Smith group $S(A)$ is trivial.

A significant property of a row-unimodular matrix is that all its rows are linearly independent over any field. Besides, every row-unimodular A has *unimodular extensions*, i.e., there are unimodular matrices B whose row set contains that of A. We remark that if A' has the same size and the same row module over $\mathbb{Z}$ as A, then any unimodular extension of

A will also give a unimodular extension of A' by appending the same rows.

2.2 Inclusion matrices for hypergraphs and primitivity

Let X be a set of size v, $\mathcal{T}$ be the set of all t-subsets of X and $\mathcal{S}$ the set of all k-subsets, with $0 \le t \le k \le t + k \le v$. Let W_{tk}^v, or simply W_{tk} if the underlying set X is understood, be the $\binom{v}{t} \times \binom{v}{k}$ inclusion matrix, rows indexed by $\mathcal{T}$ and columns by $\mathcal{S}$, such that for each $T \in \mathcal{T}$ and $S \in \mathcal{S}$,

$$W_{tk}^v(T, S) = \begin{cases} 1 & \text{if } T \subseteq S, \\ 0 & \text{otherwise.} \end{cases}$$

A diagonal form of this matrix is given by [26].

Let $\mathrm{null}_R(A)$ denote the null module to the row module of A over the ring R. Integer vectors in the null space $\mathrm{null}_{\mathbb{Q}}(W_{tk})$ are called *null t-designs* or *trades*. A survey and comparison of explicit constructions of $\mathbb{Z}$-bases for $\mathrm{null}_{\mathbb{Z}}(W_{tk})$ may be found in [14].

The elements of all $\mathbb{Z}$-bases in $\mathrm{null}_{\mathbb{Z}}(W_{tk})$ are of a certain type that were called (t, k)-pods by Graver and Jurkat [12], cross-polytopes by Graham, Li, and Li in [11], and minimal trades in [14]. For our purpose, we only need to know a generating set for $\mathrm{null}_{\mathbb{Z}}(W_{t-1,t})$, and we restrict our attention to this case. We use the term *t-pods* for what are called $(t-1, t)$-pods in [12].

Let P be a *pairing*, a set of t disjoint ordered pairs

$$\{(a_1, b_1), (a_2, b_2), \dots, (a_t, b_t)\}$$

of elements of X. To each pairing P, we associate a row t-vector $\mathbf{f}_P$, indexed by $T \in \mathcal{T}$ such that for each $T = \{c_1, c_2, \dots, c_t\} \in \mathcal{T}$, $\mathbf{f}_P(T)$ is the coefficient of the monomial $c_1 c_2 \cdots c_t$ in the expansion of the polynomial

$$(a_1 - b_1)(a_2 - b_2) \cdots (a_t - b_t).$$

Thus $\mathbf{f}_P(T) = 0$ unless T is *transverse* to P, i.e., contains exactly one member of each pair $\{a_i, b_i\}$, in which case

$$\mathbf{f}_P(T) = (-1)^{|T\cap\{b_1,b_2,\ldots,b_t\}|}.$$

These $\mathbf{f}_P$ are called t-pods, and the following theorem 2.2.1 about t-pods is proved in [11] and [12].

Theorem 2.2.1. *Every t-pod is in $\mathrm{null}_{\mathbb{Q}}(W^v_{t-1,t})$ and every integer t-vector in the null space $\mathrm{null}_{\mathbb{Q}}(W^v_{tk})$ is an integer linear combination of the t-pods.*

We remark that there are no t-pods if $v < 2t$, but in that case, $\mathrm{null}_{\mathbb{Q}}(W_{t-1,t})$ is trivial, see, e.g., [12], so the theorem remains valid.

Let $\mathbf{h}$ be a t-vector based on X, a set of size $v \geq 2t$. We say that $\mathbf{h}$ is *primitive* if the GCD of $\langle \mathbf{f}, \mathbf{h}\rangle$ over all integer t-vectors $\mathbf{f} \in \mathrm{null}_{\mathbb{Q}}(W_{t-1,t})$ is equal to 1. Equivalently, $\mathbf{h}$ is primitive if the GCD of the entries in $\mathbf{f}_P N_t(\mathbf{h})$ is 1 for any t-pod $\mathbf{f}_P$. This is because of theorem 2.2.1 and the fact that $\{\sigma(\mathbf{f}_P)\}_{\sigma\in S_v}$, the set of images of $\mathbf{f}_P$ under the symmetric group S_v, is the collection of all t-pods.

In general, we say that the GCD γ of the entries in $\mathbf{f}_P N_t(\mathbf{h})$ is the *index of primitivity* of $\mathbf{h}$. In the sequel, when we speak of a "multiple of a primitive vector", we refer to a nonzero integer multiple of a primitive vector.

Lemma 2.2.2. *Let $\mathbf{h}$ be a t-vector based on a set X of size $v \geq 2t$ with the index of primitivity γ, and let c be the* GCD *of the entries of $\mathbf{h}$. Then $\mathbf{h}$ is a multiple of a primitive vector if and only if $\gamma = c$.*

Proof. If $\mathbf{h} = c\mathbf{p}$ is a multiple of primitive vector $\mathbf{p}$, then $\mathbf{f}_P N_t(\mathbf{h}) = c\mathbf{f}_P N_t(\mathbf{p})$ whose GCD is $c \cdot 1$, so c is the index of primitivity of $\mathbf{h}$. On the other hand, if $\gamma = c$, we write $\mathbf{h} = c\mathbf{h}'$. Then $\mathbf{f}_P N_t(\mathbf{h}') = \mathbf{f}_P N_t((1/c)\mathbf{h}) = (1/\gamma)\mathbf{f}_P N_t(\mathbf{h})$ which has GCD 1. □

Proposition 2.2.3. *Let $\mathbf{h}$ be a t-vector based on a set X of size $v \geq 2t$ such that $\mathbf{h}$ has at least t isolated vertices. Then $\mathbf{h}$ is a multiple of a primitive vector.*

We recall that x is an isolated vertex of $\mathbf{h}$ if $\mathbf{h}(T) = 0$ for all T containing x.

Proof. Let $b_1, \ldots, b_t$ be t isolated vertices of $\mathbf{h}$. For each $T \in \mathcal{T}$, if $T\cap\{b_1, \ldots, b_t\}$ is nonempty, then $\mathbf{h}(T) = 0$. Otherwise, let $T = \{a_1, \ldots, a_t\}$, and let $P = \{(a_1, b_1), \ldots, (a_t, b_t)\}$ be a pairing. Now, $\langle \mathbf{f}_P, \mathbf{h} \rangle = \mathbf{h}(T)$, implying that the index of primitivity γ divides the GCD of $\mathbf{h}$. Since the GCD of $\mathbf{h}$ always divides γ, we are done by lemma 2.2.2. $\square$

Proposition 2.2.4. *Let* $\mathbf{h}$ *be a* t*-vector with* $t-1$ *isolated vertices* $b_1, \ldots, b_{t-1}$*, and let* γ *be the index of primitivity of* $\mathbf{h}$*. Then* $\mathbf{h}(T)$ *is constant modulo* γ *for all* t*-subsets* $T \subset X \backslash \{b_1, \ldots, b_{t-1}\}$*.*

Proof. Consider two t-subsets $T_1 = \{a_1, \ldots, a_{t-1}, c\}$ and $T_2 = \{a_1, \ldots, a_{t-1}, d\}$, both disjoint from $B = \{b_1, \ldots, b_{t-1}\}$. Let P be the pairing $\{(a_1, b_1), \ldots, (a_{t-1}, b_{t-1}), (c, d)\}$. Then γ divides $\langle \mathbf{f}_P, \mathbf{h} \rangle = \mathbf{h}(T_1) - \mathbf{h}(T_2)$, i.e., $\mathbf{h}(T_1) \equiv \mathbf{h}(T_2) \pmod{\gamma}$.

Given any two t-subsets T, T' disjoint from B, there exists a sequence $T = T_1, T_2, \ldots, T_m = T'$ of t-subsets disjoint from B such that $|T_i \cap T_{i+1}| = t-1$, so $\mathbf{h}(T) \equiv \mathbf{h}(T') \pmod{\gamma}$. $\square$

Theorem 2.2.5. *Let* $\mathbf{h}$ *be a* t*-vector with the index of primitivity* γ*. Then* $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ *contains* $\gamma \mathbf{f}$ *for every integer vector* $\mathbf{f}$ *in the* $\mathrm{null}_{\mathbb{Q}}(W_{t-1,t})$*.*

Proof. It suffices to show that for each pairing $P = \{(a_1, b_1), \ldots, (a_t, b_t)\}$, $\gamma \mathbf{f}_P$ is contained in $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$.

For a subset $I \subseteq \{1, 2, \ldots, t\}$, let σ_I be the product of the transpositions (a_i, b_i), $i \in I$. Let $\mathbf{h}'$ be a column in $N_t(\mathbf{h})$. We claim that for each $T \in \mathcal{T}$,

$$\sum_{I \subseteq \{1,2,\ldots,t\}} \mathrm{sign}(\sigma_I) \cdot \sigma_I(\mathbf{h}')(T) = \langle \mathbf{f}_P, \mathbf{h}' \rangle \cdot \mathbf{f}_P(T). \tag{2.2}$$

If T is not transverse to the pairing P, then the R.H.S. of (2.2) is 0, while there exists $i \in \{1, 2, \ldots, t\}$ such that $\sigma_I(\mathbf{h}')(T) = ((a_i, b_i)\sigma_I)(\mathbf{h}')(T)$ for all $I \subseteq \{1, 2, \ldots, t\}$, meaning that the terms on the L.H.S of (2.2) can be paired up with terms of the opposite signs but the same magnitude, yielding 0 when we take the sum.

If T is transverse to the pairing P, then there is a bijection between subsets $I \subseteq \{1, 2, \ldots, t\}$ and transversals T_I to P such that $\sigma_I(T) = T_I$, and

$$\mathrm{sign}(\sigma_I) \cdot \sigma_I(\mathbf{h}')(T) = (-1)^{|T \cap B|}(-1)^{|T_I \cap B|} \cdot \mathbf{h}'(T_I) = \mathbf{f}_P(T)\mathbf{f}_P(T_I)\mathbf{h}'(T_I),$$

where $B = \{b_1, b_2, \ldots, b_t\}$. Summing over $I \subseteq \{1, 2, \ldots, t\}$, we get (2.2). Now, $\langle \mathbf{f}_p, \mathbf{h}' \rangle \cdot \mathbf{f}_P$ is in $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ for every column $\mathbf{h}'$ in $N_t(\mathbf{h})$, then so is $\gamma \mathbf{f}_P$. $\square$

2.3 Shadows and fronts

Let X be a fixed v set. We are going to define a family of matrices, written as Y_{it}^v. Let $Y_{0t}^v = W_{0t}^v$, a $1 \times \binom{v}{t}$ matrix of all 1's. For $i = 1, 2, \ldots, t$, let Y_{it}^v be the $\binom{v}{i} - \binom{v}{i-1}$ by $\binom{v}{t}$ matrix obtained from W_{it}^v by deleting those rows corresponding to an $(i-1, i)$-basis on X. Here, an $(i-1, i)$-basis on X is a set of i-subsets of X such that the corresponding columns of $W_{i-1,i}^v$ form a $\mathbb{Z}$-basis for $\mathrm{col}_{\mathbb{Z}}(W_{i-1,i}^v)$. Such bases exist by proposition 1 of [27] and here we choose and fix one for each i.

If A and B are two matrices with the same number of columns, let $A \sqcup B$ denote the matrix obtained by placing A on top of B. The following lemma is proved in [27] for $v \geq 2t$ but is easily extended to $v \geq t + i$; see [28].

Lemma 2.3.1. *Let $i \leq t \leq v - i$.*

(a) The matrix

$$\bigsqcup_{i=0}^{j} Y_{it}^v = \begin{array}{|c|}\hline Y_{0t}^v \\ \hline Y_{1t}^v \\ \hline Y_{2t}^v \\ \hline \vdots \\ \hline Y_{jt}^v \\ \hline \end{array}$$

is a $\binom{v}{j} \times \binom{v}{t}$ row-unimodular matrix whose rows form a $\mathbb{Z}$-basis for the integer vectors in $\mathrm{row}_{\mathbb{Q}}(W_{jt}^v)$. *In particular, if $v \geq 2t$, then $\bigsqcup_{i=0}^{t} Y_{it}^v$ is a $\binom{v}{t} \times \binom{v}{t}$ unimodular matrix.*

(b) *For each* $j = 0, 1, 2, \ldots, t$, *the module* $\mathrm{row}_{\mathbb{Z}}(W^v_{jt})$ *is equal to that generated by the rows of*

$$\bigsqcup_{i=0}^{j} \binom{t-i}{j-i} Y^v_{it}.$$

A fundamental relation for inclusion matrices W^v_{it} is given by

$$W^v_{ij} W^v_{jt} = \binom{t-i}{j-i} W^v_{it}, \tag{2.3}$$

and when we delete the rows corresponding to an $(i-1, i)$-basis from both sides of (2.3), we obtain

$$Y^v_{ij} W^v_{jt} = \binom{t-i}{j-i} Y^v_{it}. \tag{2.4}$$

Theorem 2.3.2. *Let* $\mathbf{h}$ *be a* t*-vector based on a* v*-set* X, *and let* γ *be the primitivity of* $\mathbf{h}$. *Let* $U^v_{t-1,t}$ *be an integer matrix whose rows form a* $\mathbb{Z}$*-basis for the module of integer vectors in* $\mathrm{row}_{\mathbb{Q}}(W^v_{t-1,t})$.

(a) *If* $\gamma \neq 0$, *then*

$$\mathrm{rank}\big(N_t(\mathbf{h})\big) = \mathrm{rank}\big(U^v_{t-1,t} N_t(\mathbf{h})\big) + \left(\tbinom{v}{t} - \tbinom{v}{t-1}\right),$$

and

$$\tau\big(N_t(\mathbf{h})\big) \qquad \textit{divides} \qquad \gamma^{\binom{v}{t} - \binom{v}{t-1}} \tau\big(U^v_{t-1,t} N_t(\mathbf{h})\big). \tag{2.5}$$

(b) *If* $\mathbf{h}$ *is a multiple of a primitive* t*-vector, then equality holds in* (2.5). *Moreover, a front for* $N_t(\mathbf{h})$ *can be any unimodular extension of* $E U^v_{t-1,t}$, *where* E *is a front of* $U^v_{t-1,t} N_t(\mathbf{h})$, *and the corresponding list of diagonal factors of* $N_t(\mathbf{h})$ *is obtained by adjoining* $\binom{v}{t} - \binom{v}{t-1}$ *copies of* γ *to the list of diagonal factors of* $U^v_{t-1,t} N_t(\mathbf{h})$.

Proof. (a) By theorem 2.2.5, $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ contains $\gamma \mathbf{f}$ for any t-pod $\mathbf{f}$, so the column module

$\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ is equal to the column module of the matrix

$$\overline{N_t}(\mathbf{h}) = \begin{array}{|c|c|}\hline & \\ \quad N_t(\mathbf{h}) \quad & \gamma(M^v_{t-1,t})^\top \\ & \\ \hline \end{array},$$

where $M^v_{t-1,t}$ is a $\binom{v}{t} - \binom{v}{t-1}$ by $\binom{v}{t}$ matrix whose rows are selected t-pods $\mathbf{f}$ such that the rows of $M^v_{t-1,t}$ form a $\mathbb{Z}$-basis for the integer vectors in $\mathrm{null}_{\mathbb{Q}}(W^v_{t-1,t})$. Let

$$U = \begin{array}{|c|}\hline U^v_{t-1,t} \\ \hline \\ V \\ \\ \hline \end{array}$$

be a unimodular extension of $U^v_{t-1,t}$. Then

$$U(M^v_{t-1,t})^\top = \begin{array}{|c|}\hline U^v_{t-1,t} \\ \hline \\ V \\ \\ \hline \end{array} \; \begin{array}{|c|}\hline \\ (M^v_{t-1,t})^\top \\ \\ \hline \end{array} = \begin{array}{|c|}\hline O \\ \hline \\ B \\ \\ \hline \end{array},$$

since $\mathrm{row}_{\mathbb{Q}}(U^v_{t-1,t}) = \mathrm{row}_{\mathbb{Q}}(W^v_{t-1,t})$ while all the rows in $M^v_{t-1,t}$ are in $\mathrm{null}_{\mathbb{Q}}(W^v_{t-1,t})$. So

$$U\overline{N_t}(\mathbf{h}) = \begin{array}{|c|c|}\hline U^v_{t-1,t}N_t(\mathbf{h}) & O \\ \hline & \\ VN_t(\mathbf{h}) & \gamma B \\ & \\ \hline \end{array}. \tag{2.6}$$

As $M^v_{t-1,t}$ is row-unimodular, B is unimodular and $\det(B) = \pm 1$. It is now clear that the rank of $N_t(\mathbf{h})$ is the rank of $U^v_{t-1,t}N_t(\mathbf{h})$ plus $\binom{v}{t} - \binom{v}{t-1}$.

For any square submatrix A of $U^v_{t-1,t}N_t(\mathbf{h})$ of order equal to $\mathrm{rank}\big(U^v_{t-1,t}N_t(\mathbf{h})\big)$, the determinant of the square submatrix

$$\begin{array}{|c|c|}\hline A & O \\ \hline C & \gamma B \\ \hline \end{array}$$

of $U\overline{N_t}(\mathbf{h})$ is a multiple of $\tau(U\overline{N}_t(\mathbf{h})) = \tau(N_t(\mathbf{h}))$, i.e., $\gamma^{\binom{v}{t}-\binom{v}{t-1}}\det(A)$ is a multiple of $\tau(N_t(\mathbf{h}))$, which implies (2.5).

(b) As $\mathbf{h}$ is a multiple of a primitive vector, by lemma 2.2.2, the GCD of the entries of $\mathbf{h}$ is γ. In this case, column operations can be used to transform the matrix $U\overline{N_t}(\mathbf{h})$ in (2.6) to

$$U\overline{N_t}(\mathbf{h})U' = \begin{array}{|c|c|}\hline U^v_{t-1,t}N_t(\mathbf{h}) & O \\ \hline O & \gamma I \\ \hline \end{array},$$

where U' is an appropriate unimodular matrix. If E is a front for $U^v_{t-1,t}N_t(\mathbf{h})$ with D and F the corresponding diagonal form and back such that $EU^v_{t-1,t}N_t(\mathbf{h})F = D$, then

$$\begin{array}{|c|}\hline EU^v_{t-1,t} \\ \hline V \\ \hline \end{array}\;\overline{N_t}(\mathbf{h})U'\;\begin{array}{|c|c|}\hline F & O \\ \hline O & I \\ \hline \end{array} = \begin{array}{|c|c|}\hline D & O \\ \hline O & \gamma I \\ \hline \end{array}.$$

As $EU^v_{t-1,t}$ and $U^v_{t-1,t}$ have the same size and the same row module over $\mathbb{Z}$, appending V to $EU^v_{t-1,t}$ is also a unimodular extension. Hence, $EU^v_{t-1,t} \sqcup V$ is a front for $\overline{N_t}(\mathbf{h})$ or $N_t(\mathbf{h})$. $\square$

Remarks. One choice for the matrix $U^v_{t-1,t}$ in the above theorem is $\bigsqcup_{i=0}^{t-1} Y^v_{it}$, and in the proof, one may take $V = Y^v_{tt}$ regardless of the choice of $U^v_{t-1,t}$.

For an integer j, $0 \le j \le t$, the *j-th shadow* $\mathbf{h}^{(j)}$ of a t-vector $\mathbf{h}$ is the $(t-j)$-vector $W^v_{t-j,t}\mathbf{h}$. For example, if $\mathbf{g}$ is the characteristic 2-vector of a multigraph G, then the first shadow $\mathbf{g}^{(1)}$ is the 1-vector whose coordinates give the degrees of the vertices of G, and the second shadow $\mathbf{g}^{(2)}$ is the scalar e, the number of edges of G. Note that by (2.3), a shadow of a shadow is an integer multiple of a shadow. For instance, the first shadow of $\mathbf{g}^{(1)}$ is the scalar $2e$.

Theorem 2.3.3. *If a t-vector $\mathbf{h}$ and all of its shadows are primitive or multiples of primitive vectors, then a front for $N_t(\mathbf{h})$ is given by*

$$E = \bigsqcup_{i=0}^{t} Y^v_{it},$$

and the corresponding list of diagonal factors are

$$(g_0)^1,\ (g_1)^{v-1},\ (g_2)^{\binom{v}{2}-v}, \dots,\ (g_t)^{\binom{v}{t}-\binom{v}{t-1}},$$

where g_i is the GCD *of all entries of $W^v_{it}\mathbf{h}$. Here, the exponents denote the multiplicities.*

Proof. We proceed by induction on t. When $t = 0$, a 0-vector $\mathbf{h}$ is a scalar. Then a front for $N_0(\mathbf{h})$ can be $Y^v_{00} = 1$, and the corresponding diagonal form is $\mathbf{h}$, which is equal to g_0, the GCD of the entries of $W^v_{00}\mathbf{h}$. Now fix $t \ge 1$.

Given $\mathbf{h}$, let $\mathbf{h}' = W^v_{t-1,t}\mathbf{h}$ be the first shadow of $\mathbf{h}$. Then $N_{t-1}(\mathbf{h}') = W^v_{t-1,t}N_t(\mathbf{h})$. Let g'_i be the GCD of the entries of $W^v_{i,t-1}\mathbf{h}'$ for $i = 0, 1, \dots, t-1$. By (2.3),

$$g'_i = (t-i)g_i, \qquad i = 0, 1, \dots, t-1. \tag{2.7}$$

Applying the induction hypothesis to $\mathbf{h}'$, $\bigsqcup_{i=0}^{t-1} Y^v_{i,t-1}$ is a front for $N_{t-1}(\mathbf{h}')$, and the corresponding diagonal form is

$$D = \operatorname{diag}\big((g'_i)^{\binom{v}{i}-\binom{v}{i-1}},\ i = 0, 1, \dots, t-1\big). \tag{2.8}$$

By (2.4),

$$\Big(\bigsqcup_{i=0}^{t-1} Y_{i,t-1}^v\Big) W_{t-1,t}^v N_t(\mathbf{h}) = \Big(\bigsqcup_{i=0}^{t-1} (t-i) Y_{it}^v\Big) N_t(\mathbf{h}) = D'\Big(\bigsqcup_{i=0}^{t-1} Y_{it}^v\Big) N_t(\mathbf{h}),$$

where D' is the square diagonal matrix with diagonal entries

$$(t-i)^{\binom{v}{i}-\binom{v}{i-1}},\ i = 0, 1, \ldots, t-1. \tag{2.9}$$

By (2.7), (2.8) and (2.9), a diagonal form for $\Big(\bigsqcup_{i=0}^{t-1} Y_{it}^v\Big) N_t(\mathbf{h})$ is

$$\operatorname{diag}\Big((g_i)^{\binom{v}{i}-\binom{v}{i-1}},\ i = 0, 1, \ldots, t-1\Big).$$

The index of primitivity γ of $\mathbf{h}$ is the GCD of the entries of $\mathbf{h}$, and this is g_t. By theorem 2.3.2(b), $\bigsqcup_{i=0}^{t} Y_{it}^v$ is a front for $N_t(\mathbf{h})$ with the corresponding diagonal form

$$\operatorname{diag}\Big((g_i)^{\binom{v}{i}-\binom{v}{i-1}},\ i = 0, 1, \ldots, t\Big).$$

□

2.4 Primitivity of random hypergraphs

We consider the following model for a random t-uniform multihypergraph on k vertices. Let X_T be i.i.d random variables associated with each edge T of $K_k^{(t)}$, uniformly distributed on $\{0, 1, \ldots, M-1\}$ for some $M \geq 2$. Let H be the "random multihypergraph" where the multiplicity of each edge T is given by X_T.

Let $P = \{(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)\}$ be a pairing and σ_I the product of the transpositions (a_i, b_i), $i \in I \subseteq \{1, 2, \ldots, t\}$. Let $T = \{a_1, a_2, \ldots, a_t\}$. By definition, H is primitive if and only if the GCD of

$$\sum_{I \subseteq \{1,2,\ldots,t\}} (-1)^{|I|} X_{\sigma_I(T)}$$

with P running over all pairings in the k-set is 1. Note that if we fix a pairing P, for any prime p,

$$\mathbb{P}\left(\sum_{I\subseteq\{1,2,\ldots,t\}}(-1)^{|I|}X_{\sigma_I(T)}\equiv_p 0\right) = \mathbb{P}\left(\sum_{i=1}^{2^{t-1}}X_{T_i}-\sum_{i=1}^{2^{t-1}}X_{T_i'}\equiv_p 0\right)$$
$$= \sum_{r=-(M-1)(2^{t-1}-1)}^{(M-1)2^{t-1}}\mathbb{P}\left(\sum_{i=1}^{2^{t-1}}X_{T_i}-\sum_{i=2}^{2^{t-1}}X_{T_i'}=r\right)\cdot\mathbb{P}\left(X_{T_1'}\equiv_p r\right)\le\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil,$$

since $\mathbb{P}\left(X_{T_1'}\equiv_p r\right)=\frac{1}{M}\left\lfloor\frac{M}{p}\right\rfloor$ or $\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil$ for all $r\in\mathbb{Z}$.

If we form $\lfloor k/2t\rfloor$ disjoint subsets of $2t$ vertices out of the set of k vertices, and from each subset of $2t$ vertices we choose a pairing, then

$$\mathbb{P}(H\text{ is nonprimitive})\le\sum_{p\text{ prime}\le(M-1)2^{t-1}}\left(\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil\right)^{\lfloor k/2t\rfloor}$$
$$\le(M-1)2^{t-1}\left(\frac{2}{3}\right)^{\lfloor k/2t\rfloor}\xrightarrow{k\to\infty}0,$$

which proves the following theorem.

Theorem 2.4.1. *A random t-uniform multihypergraph H on k vertices is almost surely primitive as $k\to\infty$.*

We remark that the i-th shadow of a random t-uniform hypergraph is not necessarily a random $(t-i)$-uniform hypergraph, yet we show that it, too, is almost surely primitive.

Consider the i-th shadow $H^{(i)}$ of H. For each edge $R=\{a_1,\ldots,a_{t-i}\}$ in $H^{(i)}$, let $Z_R=\sum_{T\in E(H)\text{ s.t. }R\subset T}X_T$, which represents the multiplicity of each edge R in $H^{(i)}$. Then $H^{(i)}$ is primitive if and only if the GCD of

$$\omega(P^{(i)}):=\sum_{I\subseteq\{1,2,\ldots,t-i\}}(-1)^{|I|}Z_{\sigma_I(\{a_1,a_2\ldots,a_{t-i}\})}$$

with $P^{(i)}=\{(a_1,b_1),(a_2,b_2),\ldots,(a_{t-i},b_{t-i})\}$ running over all pairings in the k-set is 1.

We form $\lfloor k/2(t-i)\rfloor$ disjoint subsets of $2(t-i)$ vertices out of the set of k vertices, and from each subset of $2(t-i)$ vertices we choose a pairing, labeled by $P_1^{(i)}, P_2^{(i)}, \dots, P_{\lfloor k/2(t-i)\rfloor}^{(i)}$. For each pairing $P_j^{(i)}$, since $k \to \infty$, there always exists at least one t-subset T such that X_T occurs only once in $\omega(P_j^{(i)})$ but not in any other $\omega(P_\ell^{(i)})$. Hence, the independence of the X_T's gives

$$\mathbb{P}(H^{(i)} \text{ is nonprimitive}) \leq \sum_{p \text{ prime} \leq (M-1)2^{t-i-1}\binom{k-2(t-i)}{i}} \left(\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil\right)^{\lfloor k/2(t-i)\rfloor},$$

which also goes to 0 when $k \to \infty$, and so we obtain the following theorem.

Theorem 2.4.2. *The i-th shadow $H^{(i)}$ of a random multihypergraph H on k vertices is almost surely primitive as $k \to \infty$.*

In fact, both theorems hold for any distribution of i.i.d. random variables X_T as long as $\mathbb{P}(X_T \equiv_p r) < 1$ for all primes p and $r \in \mathbb{Z}$. Finally, note that when $M = 2$, our original setting coincides with one of the most classical definition of random simple hypergraph.

2.5 Fronts and diagonal forms for primitive 2-vectors and graphs

For a column 1-vector $\mathbf{a} = [a_1, \dots, a_v]^\top$, the columns of $N_1(\mathbf{a})$ are simply all the permutations of $\mathbf{a}$. Let $B = B(b; a_1, \dots, a_v)$ be the matrix derived from $N_1(\mathbf{a})$ by replacing the top row with the row vector $b\mathbf{1}_{v!}$ for some integer b. Here, and throughout this thesis, we use $\mathbf{1}_i$ and $\mathbf{0}_i$ to denote row vectors of all 1's and all 0's respectively of length i, and $O_{i\times j}$ the matrix of all 0's of size i by j, unless otherwise specified.

Before we proceed, we will prove the following lemma in elementary number theory.

Lemma 2.5.1. *For any $x, y \in \mathbb{Z}$, there exists $a, b \in \mathbb{Z}$ such that* $\mathrm{GCD}\{a, x, y\} = 1$ *and* $ax + by = \mathrm{GCD}\{x, y\}$.

Proof. Let $\mathrm{GCD}\{x, y\} = d$, $x = x'd$ and $y = y'd$. Let $a_0, b_0 \in \mathbb{Z}$ be such that $a_0x' + b_0y' = 1$. Note that $\mathrm{GCD}\{a_0, y'\} = 1$. Our goal is to find a such that $a \equiv a_0 \pmod{y'}$ and

$\mathrm{GCD}\{a,d\}=1$.

Without loss of generality, we can assume that all prime factors of d are of degree 1. Let $d=d_1d_2$ such that $d_1 \mid y'$ and $\mathrm{GCD}\{d_2,y'\}=1$. As $\mathrm{GCD}\{a_0,y'\}=1$, it suffices to find a such that $a\equiv a_0 \pmod{y'}$ and $a \equiv 1 \pmod{d_2}$, which is possible by the Chinese remainder theorem. $\square$

Theorem 2.5.2. *Given integers $a_1,\ldots,a_v$ and b, not all zero, let*

$$h=\mathrm{GCD}\{a_1,\ldots,a_v,b\} \qquad \textit{and} \qquad g=\mathrm{GCD}\{a_i-a_j : 1\le i,j\le v\}.$$

A front for $B(b;a_1,\ldots,a_v)$ can be given by the matrix

$$E=\left[\begin{array}{c|c|c} (a_1,g)/h & \ell b/h & \\ \cline{1-2} \alpha & \beta & O_{2\times(v-2)} \\ \hline \mathbf{0}_{v-2}^{\top} & -\mathbf{1}_{v-2}^{\top} & I_{(v-2)\times(v-2)} \end{array}\right],$$

and the corresponding list of diagonal factors is

$$(bg/h)^1,\ (h)^1,\ (g)^{v-2}.$$

Here, ℓ is any nonzero integer such that $\mathrm{GCD}\{\ell,a_1,g\}=1$ and $(a_1,g)+\ell a_1\equiv 0 \pmod{g}$, which exists by lemma 2.5.1, and α,β are chosen to satisfy

$$\det\begin{pmatrix}(a_1,g)/h & \ell b/h\\ \alpha & \beta\end{pmatrix}=1.$$

Proof. For each $2\le r\le v$ and $1\le i,j\le v$, there are two columns of B that are identical except the r-th coordinate, where one contains a_i and the other a_j. For example, if $i=1$,

$j = 2$, $r = 3$, the columns could be

$$[b, a_3, a_1, a_4, a_5, \ldots, a_v]^\top \qquad \text{and} \qquad [b, a_3, a_2, a_4, a_5, \ldots, a_v]^\top.$$

By taking the difference between these two vectors, we show that $\mathrm{col}_{\mathbb{Z}}(B)$ contains the vector $(a_i - a_j)\mathbf{e}_r$, where $\mathbf{e}_r$ is the r-th standard basis vector. As this is true for every pair of i and j, $\mathrm{col}_{\mathbb{Z}}(B)$ has to contain the vector $g\mathbf{e}_r$ for each $r \geq 2$. It is now obvious that the matrix

$$C = \left[\begin{array}{c|c} b & \mathbf{0}_{v-1} \\ \hline a_1 \mathbf{1}_{v-1}^\top & gI_{(v-1)\times(v-1)} \end{array}\right]$$

shares the same column module as B, thus the same fronts and diagonal factors as well. For the rest of the proof, we will try to show that E is a front for C.

The matrix E is defined such that it has determinant 1, so it is unimodular. It then suffices to find a unimodular matrix F such that $EC = DF$, where D is the diagonal form in the statement of the theorem. Now, let

$$F = \left[\begin{array}{c|c|c} \ell' & \ell & \\ (\alpha b + \beta a_1)/h & \beta g/h & O_{2\times(v-2)} \\ \hline \mathbf{0}_{v-2}^\top & -\mathbf{1}_{v-2}^\top & I_{(v-2)\times(v-2)} \end{array}\right],$$

where ℓ' is an integer defined such that $(a_1, g) + \ell a_1 = \ell' g$. By the definition of α and β, $\big((a_1, g)\beta - \ell\alpha b\big)/h = 1$, or $(a_1, g)\beta - \ell\alpha b = h$. From these two equations, we get $\ell(\alpha b + \beta a_1) = \ell'\beta g - h$. As $\mathrm{GCD}\{\ell, a_1, g\} = 1$, we have ℓ and h are relatively prime. Hence, $\alpha b + \beta a_1 = (\ell'\beta g - h)/\ell$ is divisible by h, and we have shown that F is an integer matrix.

The determinant of F is $\ell'\beta g/h - \ell(\alpha b + \beta a_1)/h = \ell'\beta g/h - (\ell'\beta g - h)/h$ which is 1, meaning that F is unimodular. Finally, it is routine to check that $EC = DF$. □

Corollary 2.5.3. *For any nonzero* $\mathbf{a}$*, a list of diagonal factors of* $N_1(\mathbf{a})$ *is*

$$(bg/h)^1,\ (h)^1,\ (g)^{v-2},$$

where $b = a_1 + a_2 + \cdots + a_v$*,* $h = \mathrm{GCD}\{a_1, \ldots, a_v\}$ *and* $g = \mathrm{GCD}\{a_i - a_j : 1 \leq i, j \leq v\}$*.*

Proof. This is a direct application of theorem 2.5.2, since $B(b; a_1, \ldots, a_v)$ is obtained by adding all the other rows to the top row of $N_1(\mathbf{a})$. □

We now describe a front and the corresponding list of diagonal factors for $N_2(\mathbf{h})$ for any primitive 2-vector $\mathbf{h}$.

Theorem 2.5.4. *Let* $\mathbf{h}$ *be a primitive* 2*-vector based on a* v*-set with the first shadow* $\mathbf{a} = [a_1, \ldots, a_v]^\top$*. Let* $b = (a_1 + \cdots + a_v)/2$ *and let* g, h, E *be described as in the statement of theorem* 2.5.2*. Then a front for* $N_2(\mathbf{h})$ *can be* $(E(Y_{02} \sqcup Y_{12})) \sqcup Y_{22}$*, and the corresponding list of diagonal factors is*

$$(bg/h)^1,\ (h)^1,\ (g)^{v-2},\ (1)^{\binom{v}{2}-v}.$$

Proof. Note that $W_{02}N_2(\mathbf{h}) = b\mathbf{1}_{v!}$ and $W_{12}N_2(\mathbf{h}) = N_1(\mathbf{a})$, so if we take $U_{12} = Y_{02} \sqcup Y_{12}$, where Y_{12} is W_{12} with the top row deleted, we will have $U_{12}N_2(\mathbf{h}) = B(b; a_1, \ldots, a_v)$. As E is a front for $U_{12}N_2(\mathbf{h})$ by theorem 2.5.2, we can apply theorem 2.3.2(b), which says any unimodular extension of EU_{12} is a front for $N_2(\mathbf{h})$, and the list of corresponding diagonal factors is obtained by adjoining $\binom{v}{2} - v$ copies of 1's to $(bg/h)^1,\ (h)^1,\ (g)^{v-2}$. We finish by noticing that $EU_{12} \sqcup Y_{22}$ is a unimodular extension of EU_{12}, since U_{12} and EU_{12} have the same row module over $\mathbb{Z}$, and Y_{22} is a unimodular extension of U_{12} by lemma 2.3.1. □

Remarks. If $\mathbf{h}$ is the characteristic 2-vector of a multigraph G (graphs with multiple edges but no loops), then the shadow $\mathbf{a} = W_{12}\mathbf{h}$ is the degree sequence and b the number of edges of G. Theorem 2.5.4 gives a list of diagonal factors of $N_2(G)$ if G is primitive, determined only by the degree sequence of G. As simple examples, if G is the Petersen graph, then a list of diagonal factors of $N_2(G)$ is $(3)^1,\ (0)^9,\ (1)^{35}$ ($g = 0$ since G is a regular graph), while for the graph G' consisting of the Petersen graph plus an isolated vertex, a list of diagonal factors for $N_2(G')$ is $(15)^1,\ (3)^{10},\ (1)^{44}$. This is because both graphs G and G' (and almost all simple graphs) are primitive by theorem 2.6.1 in the next section.

2.6 Fronts and diagonal forms for nonprimitive simple graphs

Let X be a set of size k. We use $\mathbb{1}_{\{x,y\}}$ to denote a row 2-vector of length $\binom{k}{2}$, indexed by the 2-subsets of X, such that the entry corresponding to $\{x,y\}$ is 1 and 0 elsewhere. Then the 2-pod corresponding to the pairing $P = \{(a_1,b_1),(a_2,b_2)\}$ can be written as

$$\mathbf{f}_P = \mathbb{1}_{\{a_1,a_2\}} + \mathbb{1}_{\{b_1,b_2\}} - \mathbb{1}_{\{a_1,b_2\}} - \mathbb{1}_{\{a_2,b_1\}}.$$

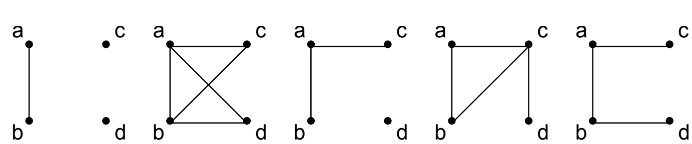
If G is a simple graph with characteristic 2-vector $\mathbf{g}$, i.e., $\mathbf{g}(\{x,y\}) = 1$ if $\{x,y\}$ is an edge of G and 0 otherwise, then

$$\langle \mathbf{f}_P, \mathbf{g} \rangle = \mathbf{g}(\{a_1,a_2\}) + \mathbf{g}(\{b_1,b_2\}) - \mathbf{g}(\{a_1,b_2\}) - \mathbf{g}(\{a_2,b_1\}).$$

In particular, we always have $\langle \mathbf{f}_p, \mathbf{g} \rangle \in \{-2,-1,0,1,2\}$.

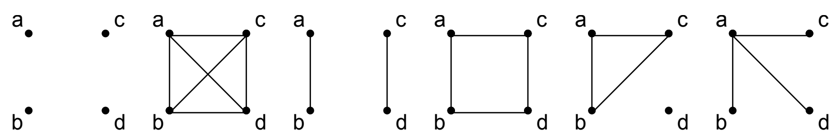
Theorem 2.6.1. *A simple graph G with at least four vertices is primitive unless G is isomorphic to a complete graph, an empty graph, a complete bipartite graph, or a disjoint union of two cliques.*

Proof. It is easy to check which simple graphs on four vertices are primitive, since there are only three possible 2-pods, up to signs, on four vertices. Up to isomorphism, here are all the primitive simple graphs on four vertices.



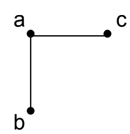
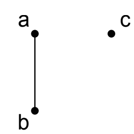
(2.10)

As a result, a simple graph G is nonprimitive if and only if every subgraph induced by any four vertices of G is isomorphic to one of the following.

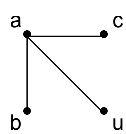
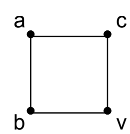


Note that a simple graph is primitive if and only if its complement is primitive.

Let G be a nonprimitive simple graph. If G is neither a complete graph nor an empty graph, then there exist three vertices a, b, c such that the subgraph they induce is isomorphic to

Case (i)  or *Case* (ii)  .

Case (i). For every vertex $x \neq a, b, c$ in G, the induced subgraph on $\{a, b, c, x\}$ is isomorphic to

 or  .

Let U and V be, respectively, the sets of vertices other than a, b, c that are adjacent to a, and are adjacent to b and c. Observe that two vertices $u_1, u_2 \in U$ cannot be adjacent in G, or else the subgraph induced by $\{a, b, u_1, u_2\}$ is on the list (2.10); two vertices $v_1, v_2 \in V$ cannot be adjacent in G, or else the subgraph induced by $\{a, b, v_1, v_2\}$ is on the list (2.10); and vertices $u \in U$, $v \in V$ must be adjacent in G, or else the subgraph induced by $\{a, b, u, v\}$ is on the list (2.10). Therefore, G is a complete bipartite graph with partite sets $\{b, c\} \cup U$ and $\{a\} \cup V$.

Case (ii). We simply take the complement of the graph G and it will return to case (i). Hence, G is a disjoint union of two cliques. $\square$

Theorem 2.6.2. *Let G be a simple nonprimitive graph with k vertices, $k \geq 4$. Then diagonal forms of G can be given by the following table.*

	G	*a list of diagonal factors of* $N_2(G)$
(a)	K_k	$(1)^1,\ (0)^{\binom{k}{2}-1}$
(b)	*empty*	$(0)^{\binom{k}{2}}$
(c)	$K_{1,k-1}$	$(2)^1,\ (1)^{k-1},\ (0)^{\binom{k}{2}-k}$
(d)	$K_1\dot{\cup}K_{k-1}$	$(k-2)^1,\ (1)^{k-1},\ (0)^{\binom{k}{2}-k}$
(e)	$K_{r,k-r}$ $2\le r\le \frac{k}{2}$	$\left(\frac{eg}{h}\right)^1,\ (h)^1,\ (2g)^{k-2},\ (2)^{\binom{k}{2}-(2k-2)},\ (1)^{k-2}$ $e=r(k-r),\ g=k-2r,\ h=\mathrm{GCD}\{r,k\}$
(f)	$K_r\dot{\cup}K_{k-r}$ $2\le r\le \frac{k}{2}$	$\left(\frac{2eg}{\epsilon h}\right)^1,\ (\epsilon h)^1,\ (2g)^{k-2},\ (2)^{\binom{k}{2}-(2k-1)},\ (1)^{k-1}$ $e=\binom{r}{2}+\binom{k-r}{2},\ g=k-2r,$ $h=\mathrm{GCD}\{r-1,g,e\},\ \epsilon=\mathrm{GCD}\{k,2\}$

Parts (a) and (b) are trivial, so we will omit the proof.

Proof of (c). Let $X=\{v_1,v_2,\ldots,v_k\}$ be the vertex set of G. Let E be the $\binom{k}{2}\times\binom{k}{2}$ matrix given in (2.11) below.

By elementary row operations, we can clear the two -1's in the top row of E without changing its determinant, and the resultant matrix is lower-triangular with only 1's on the diagonal, so E is unimodular.

Note that the bottom $\binom{k}{2}-k$ rows of E are 2-pods, so we get 0's for these rows of $EN_2(G)$ since all the columns in $N_2(G)$ are columns in $(W_{12}^k)^\top$. The top k rows of $EN_2(G)$ are given by

$$\left[\begin{array}{c|c|c|c} 1 & -1 & \mathbf{0}_{k-3} & -1 \\ \hline \mathbf{0}_{k-1}^\top & \multicolumn{3}{c}{I_{(k-1)\times(k-1)}} \end{array}\right] \cdot \left[\begin{array}{c|c|c|c} \mathbf{1}_{k-1}^\top & \multicolumn{3}{c}{I_{(k-1)\times(k-1)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \end{array}\right] \cdots \left[\begin{array}{c|c|c|c} \mathbf{1}_{k-1}^\top & \multicolumn{3}{c}{I_{(k-1)\times(k-1)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \end{array}\right] =$$

$$\left[\begin{array}{c|c} 2 & \mathbf{0}_{k-1} \\ \hline \mathbf{0}_{k-1}^\top & I_{(k-1)\times(k-1)} \end{array}\right] \cdot \left[\begin{array}{c|c|c|c} 0 & 0 & -1 & \mathbf{0}_{k-3} \\ \hline \mathbf{1}_{k-2}^\top & \mathbf{0}_{k-2}^\top & \multicolumn{2}{c}{I_{(k-2)\times(k-2)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \end{array}\right] \cdots \left[\begin{array}{c|c|c|c} 0 & 0 & -1 & \mathbf{0}_{k-3} \\ \hline \mathbf{1}_{k-2}^\top & \mathbf{0}_{k-2}^\top & \multicolumn{2}{c}{I_{(k-2)\times(k-2)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \end{array}\right].$$

It is easy to see that the last matrix is row-unimodular, and can be extended to a unimodular matrix F such that $EN_2(G) = DF$, where $D = \operatorname{diag}\big((2)^1, (1)^{k-1}, (0)^{\binom{k}{2}-k}\big)$.

$$\begin{array}{|c|c|c|c|c|l} \hline 1 & -1 & \mathbf{0}_{k-3} & -1 & & \\ \cline{1-4} \mathbf{0}_{k-1}^\top & \multicolumn{3}{c|}{I_{(k-1)\times(k-1)}} & O_{k\times\left(\binom{k}{2}-k\right)} & \Big\}\ k \text{ rows} \\ \hline \multicolumn{5}{|c|}{\mathbb{1}_{\{v_1,v_3\}} + \mathbb{1}_{\{v_2,x\}} - \mathbb{1}_{\{v_1,x\}} - \mathbb{1}_{\{v_2,v_3\}},\ x \in \{v_4,\dots,v_k\}} & \Big\}\ k-3 \text{ rows} \\ \hline \multicolumn{5}{|c|}{\mathbb{1}_{\{v_1,v_2\}} + \mathbb{1}_{\{x,y\}} - \mathbb{1}_{\{v_1,y\}} - \mathbb{1}_{\{v_2,x\}},\ \{x,y\} \subseteq \{v_3,\dots,v_k\}} & \Big\}\ \binom{k-2}{2} \text{ rows} \\ \hline \end{array} \tag{2.11}$$

□

Proof of (d). Let E be the same $\binom{k}{2} \times \binom{k}{2}$ matrix given in (2.11) except that the first k rows are replaced by the matrix in (2.12).

$$
\left[\begin{array}{c|c|c|c}
1 & \mathbf{1}_{k-2} & 0 & \\
\cline{1-3}
\mathbf{0}_{k-1}^{\top} & \multicolumn{2}{c|}{I_{(k-1)\times(k-1)}} & O_{k\times(\binom{k}{2}-k)}
\end{array}\right]
\tag{2.12}
$$

By elementary row operations, we can clear the vector $\mathbf{1}_{k-2}$ in the top row of E without changing its determinant, and the resultant matrix is lower-triangular with only 1's on the diagonal, so E is unimodular.

Note that all the columns in $N_2(G)$ are columns in $J-(W_{12}^k)^{\top}$, where J denotes the matrix of all 1's. Since a 2-pod is orthogonal to a vector of all 1's, it is orthogonal to all the columns in $J-(W_{12}^k)^{\top}$. As a result, the bottom $\binom{k}{2}-k$ rows of $EN_2(G)$ are again all 0's. The top k rows of $EN_2(G)$ are given by

$$
\left[\begin{array}{c|c|c}
1 & \mathbf{1}_{k-2} & 0 \\
\hline
\mathbf{0}_{k-1}^{\top} & \multicolumn{2}{c}{I_{(k-1)\times(k-1)}}
\end{array}\right]
\cdot
\left[\begin{array}{c|c|c|c|c|c|c|c|c|c}
\mathbf{0}_{k-1}^{\top} & \multicolumn{3}{c|}{(J-I)_{(k-1)\times(k-1)}} & & \mathbf{0}_{k-1}^{\top} & \multicolumn{3}{c}{(J-I)_{(k-1)\times(k-1)}} \\
\cline{1-4}\cline{6-9}
1 & 0 & 0 & \mathbf{1}_{k-3} & \cdots & 1 & 0 & 0 & \mathbf{1}_{k-3}
\end{array}\right]
=
$$

$$
\left[\begin{array}{c|c}
k-2 & \mathbf{0}_{k-1} \\
\hline
\mathbf{0}_{k-1}^{\top} & I_{(k-1)\times(k-1)}
\end{array}\right]
\cdot
\left[\begin{array}{c|c|c|c|c|c|c|c|c|c}
0 & 1 & \multicolumn{2}{c|}{\mathbf{1}_{k-2}} & & 0 & 1 & \multicolumn{2}{c}{\mathbf{1}_{k-2}} \\
\cline{1-4}\cline{6-9}
\mathbf{0}_{k-2}^{\top} & \mathbf{1}_{k-2}^{\top} & \multicolumn{2}{c|}{(J-I)_{k-2}} & \cdots & \mathbf{0}_{k-2}^{\top} & \mathbf{1}_{k-2}^{\top} & \multicolumn{2}{c}{(J-I)_{k-2}} \\
\cline{1-4}\cline{6-9}
1 & 0 & 0 & \mathbf{1}_{k-3} & & 1 & 0 & 0 & \mathbf{1}_{k-3}
\end{array}\right].
$$

It is easy to see that the last matrix is row-unimodular, and can be extended to a unimodular matrix F such that $EN_2(G)=DF$, where $D=\operatorname{diag}\big((k-2)^1,(1)^{k-1},(0)^{\binom{k}{2}-k}\big)$. $\square$

To prove theorem 2.6.2(e) and (f), we need the following two lemmas.

Lemma 2.6.3. *Let A be an $r\times s$ integer matrix, $r\le s$, and D a square diagonal integer matrix of order r. If both A and D are of rank r, then $\tau(DA)=\det(D)\tau(A)$.*

Proof. As DA is of rank r, $\tau(DA)$ is simply the product of its invariant factors. On the other hand, from the notion of determinantal divisors (see [23] for details), the product of the invariant factors of DA is $\mathrm{GCD}\big\{ \det((DA)_L) : L \subseteq \{1,\dots,s\}, |L| = r\big\}$, where $(DA)_L$ denotes the submatrix of DA by picking columns in L. Since $\det((DA)_L) = \det(D)\det(A_L)$, we have $\tau(DA) = \det(D)\cdot \mathrm{GCD}\big\{ \det(A_L) : L \subseteq \{1,\dots,s\}, |L| = r\big\}$, which is $\det(D)\tau(A)$. □

Lemma 2.6.4. *Let A be an $r\times s$ integer matrix, $r \le s$, and E a unimodular matrix with rows $E_1,\dots,E_r$. Suppose $d_i \mid E_iA$ for all $i = 1,2,\dots r$. Let D be a diagonal matrix of size $r\times s$ with diagonal entries d_i's. If* $\mathrm{rank}(A) = \mathrm{rank}(D)$ *and* $\tau(A) \mid \tau(D)$*, then E is a front and D a diagonal form of A.*

Proof. Let $\ell = \mathrm{rank}(D)$. Without loss of generality, assume that $d_{\ell+1} = \cdots = d_r = 0$. Let B be a square integer matrix of order s such that $EA = DB$. Let D' be the submatrix of D by taking the first ℓ rows and first ℓ columns, and let B' be the submatrix of B by taking the first ℓ rows. Note that $DB = D'B' \sqcup O_{(r-\ell)\times s}$, and hence $\tau(DB) = \tau(D'B') = \det(D')\tau(B')$, where the last equality is due to lemma 2.6.3.

Now, since A and EA share the same row module over $\mathbb{Z}$, we have $\tau(A) = \tau(EA) = \tau(DB) = \det(D')\tau(B')$. On the other hand, it is given that $\tau(A) \mid \tau(D) = \det(D')$, which forces $\tau(A) = \det(D')$ and $\tau(B') = 1$, i.e., B' is row-unimodular. Hence, there is a unimodular extension of B' to F'. By letting $F = (F')^{-1}$, we get $EAF = D$, where both E and F are unimodular. □

Proof of (e). Let $U^k_{12} = Y^k_{02} \sqcup Y^k_{12}$, where Y^k_{it} are defined in section 2.3. Then by the notation of theorem 2.5.2, $U^k_{12}N_2(G) = B(e;(r)^{k-r},(k-r)^r)$, where $e = r(k-r)$. By theorem 2.5.2, a list of diagonal factors of $U^k_{12}N_2(G)$ is $(eg/h)^1,(h)^1,(g)^{k-2}$, where $g = k-2r$, $h = \mathrm{GCD}\{r,k\}$.

If $k \neq 2r$, then $\mathrm{rank}(U^k_{12}N_2(G)) = k$ and $\tau(U^k_{12}N_2(G)) = eg^{k-1}$. Since the index of primitivity of $K_{r,k-r}$ is 2 when $2 \le r \le k-2$, by theorem 2.3.2(a), $\mathrm{rank}(N_2(G)) = \binom{k}{2}$ and $\tau(N_2(G)) \mid 2^{\binom{k}{2}-k}eg^{k-1}$.

Let

$$D = \mathrm{diag}\big((\tfrac{eg}{h})^1,(h)^1,(2g)^{k-2},(2)^{\binom{k}{2}-(2k-2)},(1)^{k-2}\big).$$

If we can find a unimodular matrix E such that $EN_2(G) = DB$ for some integer matrix B, then we are done by lemma 2.6.4 since $\operatorname{rank}(D) = \binom{k}{2}$ and $\tau(D) = 2^{\binom{k}{2}-k} e g^{k-1}$.

Let E be the $\binom{k}{2} \times \binom{k}{2}$ matrix

$$
\left[\begin{array}{l|l}
\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^k & \big\} \; 1 \text{ row} \\
\hline
\text{second row of } W_{12}^k & \big\} \; 1 \text{ row} \\
\hline
\begin{array}{l}
\displaystyle\sum_{i=1}^{k-3} \left(\mathbb{1}_{\{w_i,x\}} - \mathbb{1}_{\{w_i,y\}}\right) - (k-2r-1)\left(\mathbb{1}_{\{x,z\}} - \mathbb{1}_{\{y,z\}}\right), \\
\begin{array}{c|c|c}
x & y & z \\
\hline
v_2 & v_{k-1} & v_k \\
v_3 & v_{k-1} & v_k \\
\vdots & \vdots & \vdots \\
v_{k-2} & v_{k-1} & v_k \\
v_{k-2} & v_k & v_{k-1}
\end{array}
\quad \text{and } \{w_i\}_{i=1}^{k-3} = X \backslash \{x,y,z\}
\end{array} & \Bigg\} \; k-2 \text{ rows} \\
\hline
\begin{array}{c}
\mathbb{1}_{\{x,y\}} + \mathbb{1}_{\{x,v_k\}} + \mathbb{1}_{\{y,v_k\}}, \\
\{x,y\} \subseteq \{v_2, \ldots, v_{k-1}\} \text{ except } \{x,y\} = \{v_2, v_3\}
\end{array} & \Bigg\} \; \binom{k-2}{2} - 1 \text{ rows} \\
\hline
\mathbb{1}_{\{x,v_k\}},\ x \in \{v_2, \ldots, v_{k-1}\} & \Bigg\} \; k-2 \text{ rows}
\end{array}\right],
$$

where ℓ is an integer such that $1 + \ell r/h \equiv 0 \pmod{g/h}$. Here, we assume the edges that index the columns of E are ordered lexicographically.

The bottom left $\left(\binom{k}{2} - k\right) \times k$ submatrix of E is a zero matrix. By a suitable permutation of the bottom $\binom{k}{2} - k$ rows, the bottom right $\left(\binom{k}{2} - k\right) \times \left(\binom{k}{2} - k\right)$ submatrix will become upper-trianglar with only 1's on the diagonal. The top left $k \times k$ submatrix is

<table>
<tr><td>$1+\ell e/h$</td><td colspan="4">$\mathbf{1}_{\binom{k}{2}-2}$</td><td>$1+\ell e/h$</td></tr>
<tr><td>1</td><td colspan="4"></td><td>1</td></tr>
<tr><td colspan="3" rowspan="3">$I_{(\binom{k}{2}-3)\times(\binom{k}{2}-3)}$</td><td rowspan="3">$-\mathbf{1}^{\top}_{\binom{k}{2}-3}$</td><td rowspan="3"></td><td>1</td></tr>
<tr><td>1</td></tr>
<tr><td rowspan="2"></td></tr>
<tr><td colspan="2">$\mathbf{0}_{\binom{k}{2}-4}$</td><td>$1$</td><td>$0$</td><td>$-1$</td></tr>
</table>

.

By some elementary row operations, we can see that this matrix has determinant ± 1. Hence, E is unimodular, and it remains to show that $EN_2(G)$ gives the correct factors.

Let E_i denote the i-th row of E. Then

$$\begin{aligned} E_1 N_2(G) &= \big(\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^{k}\big) N_2(G) \\ &= e\mathbf{1}_{k!} + \ell e/h \times \text{vector with entries } r \text{ or } k-r \\ &= e \times \text{vector with entries } 1+\ell r/h \text{ or } 1+\ell(k-r)/h \end{aligned}$$

which are all divisible by eg/h by the definition of ℓ.

$$E_2 N_2(G) = \big(\text{second row of } W_{12}^{k}\big) \times N_2(G) = \text{vector with entries } r \text{ or } k-r$$

which are all divisible by h.

For $3 \leq i \leq k$, note that each column of $N_2(G)$ corresponds to a $G' \cong K_{r,k-r}$. Let P_1 and P_2 be the two partite sets of G' with $|P_1| = r$ and $|P_2| = k-r$. If $x, y \in P_1$ or $x, y \in P_2$, then the product of E_i with this column is 0. If $x \in P_1$ and $y \in P_2$, then if $z \in P_1$, the product of E_i with this column is $1 \times |P_2 \backslash \{y\}| + (-1) \times |P_1 \backslash \{x, z\}| + (k-2r-1) = (k-r-1) - (r-2) + (k-2r-1) = 2(k-2r) = 2g$; if $z \in P_2$, the product of E_i with this column is $1 \times |P_2 \backslash \{y, z\}| + (-1) \times |P_1 \backslash \{x\}| - (k-2r-1) = 0$. Similar results hold if $x \in P_2$ and $y \in P_1$. Hence, all the entries in $E_i N_2(G)$ are divisible by $2g$.

For $k+1 \leq i \leq \binom{k}{2} - (k-2)$, any triangle has 2 or 0 edges incident with any complete bipartite graph. Hence, all the entries in $E_i N_2(G)$ are divisible by 2.

If $k = 2r$, then by deleting repeated columns from $N_2(G)$, we get the matrix

$$\dot{N} = \begin{array}{|c|} \hline W_{21}^{k-1} W_{1,r-1}^{k-1} - 2W_{2,r-1}^{k-1} \\ \hline J - W_{1,r-1}^{k-1} \\ \hline \end{array},$$

where J is the matrix of all 1's. This is because there is a bijection between graphs G' isomorphic to $K_{r,r}$ and $r-1$ subsets R not containing v_1, and for each edge $\{x, y\}$, we can easily check that $N_2(G)(\{x, y\}, G') = \dot{N}(\{x, y\}, R)$.

Multiplying the bottom layer of $\dot{N}$ by W_{21}^{k-1} and adding this to the top layer yield

$$\ddot{N} = \begin{array}{|c|} \hline 2J - 2W_{2,r-1}^{k-1} \\ \hline J - W_{1,r-1}^{k-1} \\ \hline \end{array}.$$

By lemma 2.3.1(a), $\bigsqcup_{i=0}^{2} Y_{i2}^{k-1}$ and $\bigsqcup_{i=0}^{1} Y_{i1}^{k-1}$ are unimodular matrices of order $\binom{k-1}{2}$ and $k-1$ respectively, so if we multiply them to the top and bottom layers respectively, the new matrix $\dddot{N}$ shares the same row module as $\ddot{N}$.

$$\dddot{N} = \begin{array}{|c|} \hline 2\binom{k-1}{2}J - 2\binom{r-1}{2}Y_{0,r-1}^{k-1} \\ \hline 2(k-2)J - 2\binom{r-2}{1}Y_{1,r-1}^{k-1} \\ \hline 2J - 2Y_{2,r-1}^{k-1} \\ \hline (k-1)J - \binom{r-1}{1}Y_{0,r-1}^{k-1} \\ \hline J - Y_{1,r-1}^{k-1} \\ \hline \end{array} = \begin{array}{|c|} \hline 3r(r-1)\mathbf{1} \\ \hline 2(k-2)J - 2(r-2)Y_{1,r-1}^{k-1} \\ \hline 2J - 2Y_{2,r-1}^{k-1} \\ \hline r\mathbf{1} \\ \hline J - Y_{1,r-1}^{k-1} \\ \hline \end{array}.$$

By doing simple row operations, we can clear the top two layers of $\ddot{N}$ to get

$$\widetilde{N} = \begin{array}{|c|}\hline \mathbf{0} \\ \hline O_{(k-2)\times\binom{k-1}{r-1}} \\ \hline 2J - 2Y^{k-1}_{2,r-1} \\ \hline r\mathbf{1} \\ \hline J - Y^{k-1}_{1,r-1} \\ \hline \end{array}.$$

Let $\widehat{N}$ be the bottom three layers of $\widetilde{N}$, $\widehat{D} = \operatorname{diag}\big((2)^{\binom{k-1}{2}-(k-1)}, (r)^1, (1)^{k-2}\big)$ and B an integer matrix such that $\widehat{N} = \widehat{D}B$. Lemma 2.6.3 then implies that $\tau(\widehat{N}) = \det(\widehat{D})\tau(B) = r2^{\binom{k-1}{2}-(k-1)}$ since $\tau(B) = 1$ because B has the same row module as $\bigsqcup\limits_{i=0}^{2} Y^{k-1}_{i,r-1}$ which is row-unimodular.

Now, if we let

$$D = \operatorname{diag}\big((\tfrac{eg}{h})^1, (h)^1, (2g)^{k-2}, (2)^{\binom{k}{2}-(2k-2)}, (1)^{k-2}\big),$$

then $\operatorname{rank}(D) = \binom{k}{2} - (k-1) = \operatorname{rank}(\widehat{N}) = \operatorname{rank}(N_2(G))$ since $g = 0$, and $\tau(D) = \tau(\widehat{N}) = \tau(N_2(G))$. By lemma 2.6.4, E is a front and D the corresponding diagonal form of $N_2(G)$. $\square$

Proof of (f). Similar to the proof of (e), $U^k_{12}N_2(G) = B(e; (r-1)^r, (k-r-1)^{k-r})$, where $e = \binom{r}{2} + \binom{k-r}{2}$ since $h = r$. By theorem 2.5.2, a list of diagonal factors of $U^k_{12}N_2(G)$ is $(eg/h)^1, (h)^1, (g)^{k-2}$, where $g = k - 2r$, $h = \operatorname{GCD}\{r-1, g, e\}$.

If $k \neq 2r$, since the index of primitivity of $K_r \dot\cup K_{k-r}$ is 2 when $2 \leq r \leq k-2$, by theorem 2.3.2(a), $\operatorname{rank}(N_2(G)) = \binom{k}{2}$ and $\tau(N_2(G)) \mid 2^{\binom{k}{2}-k}eg^{k-1}$. Let

$$D = \operatorname{diag}\big((\tfrac{2eg}{\epsilon h})^1, (\epsilon h)^1, (2g)^{k-2}, (2)^{\binom{k}{2}-(2k-1)}, (1)^{k-1}\big),$$

where $\epsilon = \operatorname{GCD}\{k, 2\}$. It suffices to determine a unimodular E such that $EN_2(G) = DB$ for some integer matrix B.

When k is odd, let E be the $\binom{k}{2} \times \binom{k}{2}$ matrix

$$
\left.\begin{array}{c}
\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^k \\
+eg/h \times [\mathbf{0}_{\binom{k}{2}-3}, 1, 1, 1]
\end{array}\right\} \text{1 row}
$$

$$
\left.\text{second row of } W_{12}^k\right\} \text{1 row}
$$

$$
\left.\begin{array}{l}
\displaystyle\sum_{i=1}^{k-3} \left(\mathbb{1}_{\{w_i,x\}} - \mathbb{1}_{\{w_i,y\}}\right) - (k-2r-1)\left(\mathbb{1}_{\{x,z\}} - \mathbb{1}_{\{y,z\}}\right), \\
\quad \begin{array}{c|c|c}
x & y & z \\
\hline
v_2 & v_{k-1} & v_k \\
v_3 & v_{k-1} & v_k \\
\vdots & \vdots & \vdots \\
v_{k-2} & v_{k-1} & v_k \\
v_{k-2} & v_k & v_{k-1}
\end{array} \quad \text{and } \{w_i\}_{i=1}^{k-3} = X \backslash \{x,y,z\}
\end{array}\right\} k-2 \text{ rows}
$$

$$
\left.\begin{array}{c}
\mathbb{1}_{\{w,x\}} + \mathbb{1}_{\{w,y\}} + \mathbb{1}_{\{x,z\}} + \mathbb{1}_{\{y,z\}}, \\
\begin{array}{c|c|c|c}
w & x & y & z \\
\hline
v_2 & v_4 & v_{k-1} & v_k \\
\vdots & \vdots & \vdots & \vdots \\
v_2 & v_{k-2} & v_{k-1} & v_k \\
v_2 & v_{k-1} & v_k & v_3 \\
v_3 & v_4 & v_{k-1} & v_k \\
\vdots & \vdots & \vdots & \vdots \\
v_3 & v_{k-2} & v_{k-1} & v_k \\
v_3 & v_{k-1} & v_k & v_4 \\
\vdots & \vdots & \vdots & \vdots \\
v_{k-4} & v_{k-3} & v_{k-1} & v_k \\
v_{k-4} & v_{k-2} & v_{k-1} & v_k \\
v_{k-4} & v_{k-1} & v_k & v_{k-3} \\
v_{k-3} & v_{k-2} & v_{k-1} & v_k \\
v_{k-3} & v_{k-1} & v_k & v_{k-2}
\end{array}
\end{array}\right\} \binom{k-2}{2} - 2 \text{ rows}
$$

$$
\left.\begin{array}{c}
\mathbb{1}_{\{x,y\}}, \\
\{x,y\} = \{v_2, v_k\}, \{v_3, v_k\}, \ldots, \{v_{k-1}, v_k\}, \{v_{k-2}, v_{k-1}\}
\end{array}\right\} k-1 \text{ rows}
$$

,

where ℓ is an even integer such that $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$. This is possible since $g = k - 2r$ is odd. Here, we assume the edges that index the columns of E are ordered lexicographically. By the exact same argument as in (e), this matrix E is unimodular.

To show that $EN_2(G)$ gives the correct factors, let E_i be the i-th row of E. As ℓ is even, we have $1 + \ell(r-1)/h \equiv 1 + \ell(k-r-1)/h \equiv g/h \pmod{2g/h}$. So

$$\begin{aligned} E_1 N_2(G) &= \big(\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^k + eg/h \times [\mathbf{0}_{\binom{k}{2}-3}, 1, 1, 1]\big) N_2(G) \\ &= e\mathbf{1}_{k!} + \ell e/h \times \text{vector with entries } r-1 \text{ or } k-r-1 \\ &\quad + eg/h \times \text{vector with entries 1 or 3} \\ &= e \times \text{vector with entries } 1 + \ell(r-1)/h \text{ or } 1 + \ell(k-r-1)/h \\ &\quad + eg/h \times \text{vector with entries 1 or 3} \\ &\equiv (eg/h)\mathbf{1}_{k!} + (eg/h)\mathbf{1}_{k!} \equiv \mathbf{0}_{k!} \pmod{2eg/h}. \end{aligned}$$

$$E_2 N_2(G) = \big(\text{second row of } W_{12}^k\big) \times N_2(G) = \text{vector with entries } r-1 \text{ or } k-r-1$$

which are all divisible by h.

For $3 \le i \le k$, note that each column of $N_2(G)$ corresponds to a $G' \cong K_r \dot\cup K_{k-r}$. If x and y are in the same clique of G', then the product of E_i with this column is 0. If $x \in K_r$ and $y \in K_{k-r}$, then if $z \in K_r$, the product of E_i with this column is $1 \times (r-2) + (-1) \times (k-r-1) - (k-2r-1) = -2(k-2r) = -2g$; if $z \in K_{k-r}$, the product of E_i with this column is $1 \times (r-1) + (-1) \times (k-r-2) + (k-2r-1) = 0$. Similar results hold if $x \in K_{k-r}$ and $y \in K_r$. Hence, all the entries in $E_i N_2(G)$ are divisible by $2g$.

For $k+1 \le i \le \binom{k}{2} - (k-2)$, any 4-cycle has 4, 2 or 0 edges incident with $K_r \dot\cup K_{k-r}$. Hence, all the entries in $E_i N_2(G)$ are divisible by 2.

When k is even and $r - 1 \equiv \lambda \pmod{2h}$, where $\lambda = 0$ or h, we use the matrix E almost the same as in the case when k is odd, except that the first two rows are replaced by

$\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^k$	$\}$ 1 row
$\text{second row of } W_{12}^k + \lambda \times [\mathbf{0}_{\binom{k}{2}-3}, 1, 1, 1]$	$\}$ 1 row

where ℓ is an integer, not necessarily even, such that $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$. This change does not affect the unimodularity of E, and we only need to verify whether the product of these two rows with $N_2(G)$ gives the correct factors.

Let E_1 and E_2 be the first and second row respectively. Then

$$\begin{aligned} E_1 N_2(G) &= \big(\mathbf{1}_{\binom{k}{2}} + \ell e/h \times \text{second row of } W_{12}^k\big) N_2(G) \\ &= e\mathbf{1}_{k!} + \ell e/h \times \text{vector with entries } r-1 \text{ or } k-r-1 \\ &= e \times \text{vector with entries } 1+\ell(r-1)/h \text{ or } 1+\ell(k-r-1)/h \end{aligned}$$

which are all divisible by eg/h by the definition of ℓ.

Before we work on $E_2N_2(G)$, we claim that $k-r-1 \equiv r-1 \pmod{2h}$. If $r-1$ is odd, then $k-r-1$ is also odd since k is even and we are done. If $r-1$ is even, then r and $k-r$ are both odd. Since $h \mid e = r(r-1)/2+(k-r)(k-r-1)/2$, i.e., $r(r-1)+(k-r)(k-r-1) \equiv 0 \pmod{2h}$, we have $r-1 \equiv r(r-1) \equiv -(k-r)(k-r-1) \equiv k-r-1 \pmod{2h}$. Now,

$$\begin{aligned} E_2 N_2(G) &= \big(\text{second row of } W_{12}^k + \lambda \times [\mathbf{0}_{\binom{k}{2}-3}, 1, 1, 1]\big) N_2(G) \\ &= \text{vector with entries } r-1 \text{ or } k-r-1 \;+\; \lambda \times \text{vector with entries } 1 \text{ or } 3 \\ &\equiv \lambda\mathbf{1}_{k!} + \lambda\mathbf{1}_{k!} \equiv \mathbf{0}_{k!} \pmod{2h}. \end{aligned}$$

If $k = 2r$, we proceed in a similar manner as in (e). First, by taking the complement of the matrix in (e), we get the matrix

$$\dot{N} = \begin{array}{|c|} \hline \\ J - W_{21}^{k-1} W_{1,r-1}^{k-1} + 2W_{2,r-1}^{k-1} \\ \\ \hline W_{1,r-1}^{k-1} \\ \hline \end{array}$$

which has the same column module as $N_2(G)$.

Multiplying the bottom layer of $\dot{N}$ by W_{21}^{k-1} and adding this to the top layer yield

$$\ddot{N} = \begin{array}{|c|}\hline J + 2W_{2,r-1}^{k-1} \\ \hline W_{1,r-1}^{k-1} \\ \hline \end{array}.$$

By multiplying $\bigsqcup_{i=0}^{2} Y_{i2}^{k-1}$ and $\bigsqcup_{i=0}^{1} Y_{i1}^{k-1}$ to the top and bottom layers respectively, the new matrix $\dddot{N}$ becomes

$$\dddot{N} = \begin{array}{|c|}\hline \binom{k-1}{2}J + 2\binom{r-1}{2}Y_{0,r-1}^{k-1} \\ \hline (k-2)J + 2\binom{r-2}{1}Y_{1,r-1}^{k-1} \\ \hline J + 2Y_{2,r-1}^{k-1} \\ \hline \binom{r-1}{1}Y_{0,r-1}^{k-1} \\ \hline Y_{1,r-1}^{k-1} \\ \hline \end{array} = \begin{array}{|c|}\hline 3(r-1)^2\mathbf{1} \\ \hline (k-2)J + 2(r-2)Y_{1,r-1}^{k-1} \\ \hline J + 2Y_{2,r-1}^{k-1} \\ \hline (r-1)\mathbf{1} \\ \hline Y_{1,r-1}^{k-1} \\ \hline \end{array}.$$

By doing simple row operations, we can clear the top two layers of $\dddot{N}$ to get

$$\widetilde{N} = \begin{array}{|c|}\hline \mathbf{0} \\ \hline O_{(k-2)\times\binom{k-1}{r-1}} \\ \hline J + 2Y_{2,r-1}^{k-1} \\ \hline (r-1)\mathbf{1} \\ \hline Y_{1,r-1}^{k-1} \\ \hline \end{array}.$$

Let $\widehat{N}$ be the bottom three layers of $\widetilde{N}$, $\widehat{D} = \operatorname{diag}\big((1)^{\binom{k-1}{2}-(k-1)}, (r-1)^1, (1)^{k-2}\big)$ and B an integer matrix such that $\widehat{N} = \widehat{D}B$. Lemma 2.6.3 then implies that $\tau(\widehat{N}) = \det(\widehat{D})\tau(B) = (r-1)2^{\binom{k-1}{2}-(k-1)}$ since $\tau(B) = 2^{\binom{k-1}{2}-(k-1)}$ because B has the same row module as $Y_{0,r-1}^{k-1} \sqcup Y_{1,r-1}^{k-1} \sqcup 2Y_{2,r-1}^{k-1}$.

Now, if we let

$$D = \operatorname{diag}\big((\tfrac{2eg}{\epsilon h})^1, (\epsilon h)^1, (2g)^{k-2}, (2)^{\binom{k}{2}-(2k-1)}, (1)^{k-1}\big),$$

where $\epsilon = \mathrm{GCD}\{k, 2\}$. However, since $k = 2r$, we automatically have k being even, so $\epsilon = 2$ in this situation. So $\operatorname{rank}(D) = \binom{k}{2} - (k-1) = \operatorname{rank}(\widehat{N}) = \operatorname{rank}(N_2(G))$ since $g = 0$, and $\tau(D) = \epsilon h 2^{\binom{k}{2}-(2k-1)} = \tau(\widehat{N}) = \tau(N_2(G))$ since $h = r - 1$. By lemma 2.6.4, E is a front and D the corresponding diagonal form of $N_2(G)$. $\square$

Chapter 3

Diagonal forms of incidence matrices arising from subgraphs of complete bipartite graphs

3.1 Diagonal forms of $U \cdot N(G)$

In this chapter, we let W be a $2n \times n^2$ incidence matrix of $K_{n,n}$ with vertices against edges, and let U be a $(2n-1) \times n^2$ matrix obtained from W with the first row replaced by $\mathbf{1}$, the vector of all ones, and the last row deleted. The matrix U is row-unimodular since U has a submatrix

$$\left[\begin{array}{c|c|c} \mathbf{1}_{n-1} & 1 & \mathbf{1}_{n-1} \\ \hline O_{(n-1)\times(n-1)} & \mathbf{0}_{n-1}^{\top} & I_{(n-1)\times(n-1)} \\ \hline I_{(n-1)\times(n-1)} & \mathbf{0}_{n-1}^{\top} & \begin{array}{c} \mathbf{1}_{n-1} \\ \hline O_{(n-2)\times(n-1)} \end{array} \end{array}\right],$$

which is $\mathbb{Z}$-equivalent to $I_{(2n-1)\times(2n-1)}$. Once again, $\mathbf{1}_i$ and $\mathbf{0}_i$ denote row vectors of all ones and all zeros respectively of length i, and $O_{i\times j}$ denotes a zero matrix of dimensions i by j.

Let G be a nonempty subgraph of the complete bipartite graph $K_{n,n}$ with degrees $a_1, \ldots, a_n, b_1, \ldots, b_n$, where a_i's are the degrees of the vertices in one partite set and b_i's in the other one, and some of these are possibly zeroes. Let $\mathbf{h}$ be the characteristic vector of G, i.e., $\mathbf{h}$ is a column vector of length n^2 indexed by the edges of $K_{n,n}$, with 1 if the edge is in G and 0 otherwise. Let $\mathcal{P} \cong S_n \wr_{\{a,b\}} S_2$ be the permutation group on the vertices of $K_{n,n}$ which can permute vertices within each partite set and interchange the two partite sets. Let $N = N(G)$ be the matrix with $2(n!)^2$ columns, each column representing an image of $\mathbf{h}$ under the action of $\mathcal{P}$ on the vertices.

In the following, we try to find a diagonal form for $U \cdot N(G)$. We proceed in a similar manner as in the proof of theorem 2.5.2. In $U \cdot N(G)$, each column is either $[e, a_{i_2}, a_{i_3} \ldots, a_{i_n}, b_{j_2}, b_{j_3}, \ldots, b_{j_n}]^\top$ or $[e, b_{i_2}, b_{i_3} \ldots, b_{i_n}, a_{j_2}, a_{j_3}, \ldots, a_{j_n}]^\top$, where e is the number of edges of G and $\{i_1, i_2, \ldots, i_n\} = \{j_1, j_2, \ldots, j_n\} = \{1, 2, \ldots, n\}$. Pick two columns in UN that are identical except one entry, e.g. $[e, a_1, a_3 \ldots, a_n, b_1, \ldots, b_{n-1}]^\top$ and $[e, a_2, a_3, \ldots, a_n, b_1, \ldots, b_{n-1}]^\top$. Taking the difference of these two columns, we get $[0, a_1 - a_2, 0, \ldots, 0]^\top$ in the column module of UN over $\mathbb{Z}$. Hence, the column module of UN contains $g\mathbf{e}_k^\top$, $k = 2, \ldots, 2n-1$, where $g = \mathrm{GCD}\{a_i - a_j, b_i - b_j\}$ over $1 \le i, j \le n$ and $\mathbf{e}_k$ denotes the k-th standard unit vector of length $2n-1$. So the matrix

$$
\begin{array}{|c|c|c|}
\hline
e & e & \mathbf{0}_{2n-2} \\
\hline
a_1 \mathbf{1}_{n-1}^\top & b_1 \mathbf{1}_{n-1}^\top & \\
\cline{1-2}
b_1 \mathbf{1}_{n-1}^\top & a_1 \mathbf{1}_{n-1}^\top & \raisebox{1.5ex}{$gI_{(2n-2)\times(2n-2)}$} \\
\hline
\end{array}
$$

has the same column module as UN. After some integral row and column operations, we can see that the matrix

$$\begin{array}{|c|c|c|}
\hline
e & 0 & \mathbf{0}_{2n-3} \\
\hline
a_1 & \tilde{g} & \mathbf{0}_{2n-3} \\
\hline
\mathbf{0}_{n-2}^{\top} & \mathbf{0}_{n-2}^{\top} & \\
\cline{1-2}
 & & gI_{(2n-3)\times(2n-3)} \\
(a_1+b_1)\mathbf{1}_{n-1}^{\top} & \mathbf{0}_{n-1}^{\top} & \\
\hline
\end{array} \tag{3.1}$$

has the same diagonal form as UN, where

$$\tilde{g} = \mathrm{GCD}\{a_i - b_j, a_i - a_j, b_i - b_j\} = \mathrm{GCD}\{a_1 - b_1, g\}.$$

By computing the determinantal divisors (see [23] for details), we have the following theorem.

Theorem 3.1.1. *A list of diagonal factors of UN is*

$$(\tfrac{eg}{hc})^1, (\tilde{g}c)^1, (h)^1, (g)^{2n-4},$$

where $h = \mathrm{GCD}\{a_i, b_j\} = \mathrm{GCD}\{a_1, \tilde{g}\}$ and $c = \mathrm{GCD}\{\frac{e}{h}, \frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\}$. (Note that $h \neq 0$ since G is nonempty. Note also that $\tilde{g} = 0$ if and only if $g = 0$, and in this case, we define $\frac{g}{\tilde{g}} = 1$.)

Proof. The GCD of the determinants of 1×1 submatrices in (3.1) is $\mathrm{GCD}\{a_1, \tilde{g}\} = h$.
The GCD of the determinants of $i \times i$ submatrices in (3.1), $2 \leq i \leq 2n-2$, is $\mathrm{GCD}\{e\tilde{g}g^{i-2}, \tilde{g}g^{i-1}, a_1 g^{i-1}, \tilde{g}g^{i-2}(a_1+b_1)\} = \tilde{g}g^{i-2}hc$.
The determinant of the full matrix in (3.1) is $e\tilde{g}g^{2n-3}$. □

Theorem 3.1.2. *By lemma 2.5.1, let $\alpha, \sigma \in \mathbb{Z}$ be such that $\mathrm{GCD}\{\alpha, \frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\} = 1$ and $-\alpha\,\frac{a_1+b_1}{h} + \sigma\,\frac{g}{\tilde{g}} = \mathrm{GCD}\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\}$. Then there exist $\ell, \ell' \in \mathbb{Z}$ such that $\frac{\ell'}{c}\mathrm{GCD}\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\} - \ell\alpha\frac{e}{hc} = 1$. Let $\beta, \tau \in \mathbb{Z}$ be such that $-\beta a_1 + \tau\tilde{g} = h$. Let $\ell'' = \beta\,\frac{\ell e + \ell'(a_1+b_1)}{h}$. A front E of UN is*

$$\begin{array}{|c|c|c|c|c|}
\hline
\frac{1}{c}\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} & \alpha\frac{e}{hc}+\sigma\beta\frac{eg}{hc\tilde{g}} & \mathbf{0}_{n-2} & \alpha\frac{e}{hc} & \mathbf{0}_{n-2} \\
\hline
\ell & \ell'+\ell'' & \mathbf{0}_{n-2} & \ell' & \mathbf{0}_{n-2} \\
\hline
0 & 1 & \mathbf{0}_{n-2} & 0 & \mathbf{0}_{n-2} \\
\hline
\mathbf{0}_{n-2}^{\top} & -\mathbf{1}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & \mathbf{0}_{n-2}^{\top} & O_{(n-2)\times(n-2)} \\
\hline
\mathbf{0}_{n-2}^{\top} & \mathbf{0}_{n-2}^{\top} & O_{(n-2)\times(n-2)} & -\mathbf{1}_{n-2}^{\top} & I_{(n-2)\times(n-2)} \\
\hline
\end{array},$$

where the first three rows correspond to the diagonal factors $\frac{eg}{hc}$, $\tilde{g}c$ and h respectively, and the other rows correspond to the diagonal factors g.

Proof. We first show that E is unimodular. Given that $\mathrm{GCD}\left\{\alpha, \frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} = 1$, we have $\mathrm{GCD}\left\{\alpha\frac{e}{h}, \frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} = c$, or $\mathrm{GCD}\left\{\alpha\frac{e}{hc}, \frac{1}{c}\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\}\right\} = 1$. Hence, there exist $\ell, \ell' \in \mathbb{Z}$, $\mathrm{GCD}\{\ell, \ell'\} = 1$, such that $\frac{\ell'}{c}\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} - \ell\alpha\frac{e}{hc} = 1$. So the submatrix

$$\begin{array}{|c|c|c|}
\hline
\frac{1}{c}\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} & \alpha\frac{e}{hc}+\sigma\beta\frac{eg}{hc\tilde{g}} & \alpha\frac{e}{hc} \\
\hline
\ell & \ell'+\ell'' & \ell' \\
\hline
0 & 1 & 0 \\
\hline
\end{array}$$

has determinant -1, thus E is unimodular.

From (3.1), we note that the column module of UN is the same as that of

$$M = \begin{array}{|c|c|c|}
\hline
e & 0 & \mathbf{0}_{2n-3} \\
\hline
 & & \mathbf{0}_{2n-3} \\
\cline{3-3}
a_1\mathbf{1}_{n-1}^{\top} & \tilde{g}\mathbf{1}_{n-1}^{\top} & \\
\cline{1-2}
 & & gI_{(2n-3)\times(2n-3)} \\
b_1\mathbf{1}_{n-1}^{\top} & -\tilde{g}\mathbf{1}_{n-1}^{\top} & \\
\hline
\end{array}.$$

Let E_i denote the i-th row of E. The product of the E_1 with the first column of M is

$$\tfrac{e}{c}\big(\mathrm{GCD}\{\tfrac{a_1+b_1}{h}, \tfrac{g}{\tilde{g}}\} + \alpha\tfrac{a_1+b_1}{h} + \sigma\beta\tfrac{a_1 g}{h\tilde{g}}\big) = \tfrac{e}{c}\big(- \alpha\tfrac{a_1+b_1}{h} + \sigma\tfrac{g}{\tilde{g}} + \alpha\tfrac{a_1+b_1}{h} + \sigma\beta\tfrac{a_1 g}{h\tilde{g}}\big)$$
$$= \sigma\tfrac{eg}{hc\tilde{g}}(h + \beta a_1) = \sigma\tfrac{eg}{hc\tilde{g}}(-\beta a_1 + \tau\tilde{g} + \beta a_1) = \sigma\tau\tfrac{eg}{hc}.$$

The product of E_1 with the second column of M is $\sigma\beta\frac{eg}{hc}$, and the product of E_1 with the $(n+1)$-th column of M is $\alpha\frac{eg}{hc}$. From the definition, it is clear that $\mathrm{GCD}\{\beta,\tau\} = \mathrm{GCD}\{\alpha,\sigma\} = 1$, so $\mathrm{GCD}\{\sigma\tau, \sigma\beta, \alpha\} = 1$. Hence, the GCD of the entries in $E_1(UN)$ is $\frac{eg}{hc}$.

The product of E_2 with the first column of M is

$$\ell e + \ell'(a_1+b_1) + \ell'' a_1 = \tfrac{\ell e+\ell'(a_1+b_1)}{h}(h+\beta a_1) = \tfrac{\ell e+\ell'(a_1+b_1)}{hc}\tau\widetilde{gc}.$$

The product of E_2 with the second column of M is $\ell''\tilde{g} = \beta\frac{\ell e+\ell'(a_1+b_1)}{hc}\tilde{g}c$, and the product of E_2 with the $(n+1)$-th column of M is $\ell' g = \ell'\frac{g}{\tilde{g}c}\tilde{g}c$. Recall that $\mathrm{GCD}\{\tau,\beta\} = 1$. Note that $\mathrm{GCD}\{\frac{\ell e+\ell'(a_1+b_1)}{h}, \ell'\frac{g}{\tilde{g}}\}$ divides

$$-\ell\alpha\tfrac{e}{h} + \ell'\big(- \alpha\tfrac{a_1+b_1}{h} + \sigma\tfrac{g}{\tilde{g}}\big) = -\ell\alpha\tfrac{e}{h} + \ell'\mathrm{GCD}\{\tfrac{a_1+b_1}{h}, \tfrac{g}{\tilde{g}}\} = c,$$

so $\mathrm{GCD}\{\tau\frac{\ell e+\ell'(a_1+b_1)}{hc}, \beta\frac{\ell e+\ell'(a_1+b_1)}{hc}, \ell'\frac{g}{\tilde{g}c}\} = 1$. Hence, the GCD of the entries in $E_2(UN)$ is $\tilde{g}c$.

Finally, it is obvious that the GCD of the entries in $E_3(UN)$ is h, and the GCD of $E_i(UN)$ is g for all $i \geq 4$. Since the factors of each row in $E(UN)$ agree with the list of diagonal factors given in theorem 3.1.1, E is a front for UN. $\square$

3.2 Primitivity

Let u, u', v, v' be four distinct vertices of $K_{n,n}$ such that u and u' are in the same partite set while v and v' are in the other one. Let $\mathbb{1}_{\{u,v\}}$ be a row vector of length n^2, indexed by the edges of $K_{n,n}$, such that the entry corresponding to the edge $\{u,v\}$ is 1 and all other entries are 0. Let $\mathbf{f}_{u,u',v,v'} = \mathbb{1}_{\{u,v\}} + \mathbb{1}_{\{u',v'\}} - \mathbb{1}_{\{u,v'\}} - \mathbb{1}_{\{u',v\}}$. Such a vector is called a 2-*pod* over the tuple (u,u',v,v'), which is an analogue of the t-pods in section 2.2. If $\mathbf{h}$ is a characteristic vector of a nonempty subgraph G of $K_{n,n}$, then we say G or $\mathbf{h}$ is *primitive* if $\mathrm{GCD}(\mathbf{f}N(G)) = 1$, where $\mathbf{f}$ is any 2-pod.

Proposition 3.2.1. *The collection of* 2*-pods* $\mathbf{f}_{u,u',v,v'}$ *over all tuples* (u,u',v,v') *spans over* $\mathbb{Z}$ *all the integer vectors in* $\mathrm{null}_{\mathbb{Q}}(U)$*, the null space of* U*.*

Proof. Let $\{u_1,\ldots,u_n\}$ and $\{v_1,\ldots,v_n\}$ be the two partite sets of $K_{n,n}$. Let $\mathbf{g}$ be an integer row vector indexed by $\{u_i,v_j\}$. As $\mathrm{null}_{\mathbb{Q}}(U)=\mathrm{null}_{\mathbb{Q}}(W)$, $\mathbf{g}$ is in $\mathrm{null}_{\mathbb{Q}}(U)$ if and only if $\sum_{j=1}^{n}\mathbf{g}(\{u_i,v_j\})=0$ for all u_i and $\sum_{i=1}^{n}\mathbf{g}(\{u_i,v_j\})=0$ for all v_j, so all 2-pods are contained in $\mathrm{null}_{\mathbb{Q}}(U)$. We say that u_i is an isolated vertex of $\mathbf{g}$ if $\mathbf{g}(\{u_i,v_j\})=0$ for all $j=1,\ldots,n$.

Let $\mathbf{g}$ be an integer vector in $\mathrm{null}_{\mathbb{Q}}(U)$. If i is the maximum such that u_i is not an isolated vertex of $\mathbf{g}$ and $i\geq 2$, then consider $\mathbf{g}'=\mathbf{g}-\sum_{j=2}^{n}\mathbf{g}(\{u_i,v_j\})\mathbf{f}_{u_1,u_i,v_1,v_j}$, which is in $\mathrm{null}_{\mathbb{Q}}(U)$ since it is a linear combination of vectors inside $\mathrm{null}_{\mathbb{Q}}(U)$. Note then that u_i is an isolated vertex of $\mathbf{g}'$ since $\mathbf{g}'(\{u_i,v_j\})=0$ for all $j=2,\ldots,n$, and $\mathbf{g}'$ being inside $\mathrm{null}_{\mathbb{Q}}(U)$ means that $\sum_{j=1}^{n}\mathbf{g}'(\{u_i,v_j\})=0$, implying that $\mathbf{g}'(\{u_i,v_1\})=0$.

In this way, we have expressed $\mathbf{g}$ as a linear combination of $\mathbf{g}'$ and 2-pods, and if i' is the maximum such that $u_{i'}$ is not an isolated vertex of $\mathbf{g}'$, we have $i'<i$. By iterating this process, we can express $\mathbf{g}$ as a linear combination of $\widetilde{\mathbf{g}}$ and 2-pods, where $\widetilde{\mathbf{g}}$ is in $\mathrm{null}_{\mathbb{Q}}(U)$, and the maximum $\widetilde{i}$ such that $u_{\widetilde{i}}$ is not an isolated vertex of $\widetilde{\mathbf{g}}$ satisfies $\widetilde{i}\leq 1$. However, $\widetilde{\mathbf{g}}$ being in $\mathrm{null}_{\mathbb{Q}}(U)$ implies that u_1 is also an isolated vertex of $\widetilde{\mathbf{g}}$, meaning that $\widetilde{\mathbf{g}}$ is a vector of all 0's. Hence, $\mathbf{g}$ is a linear combination of 2-pods. $\square$

Theorem 3.2.2. *If* $\mathbf{h}$ *is primitive, a list of diagonal factors of* N *is*

$$(\tfrac{eg}{hc})^1,(\tilde{g}c)^1,(h)^1,(g)^{2n-4},(1)^{(n-1)^2},$$

and a corresponding front can be any unimodular extension $\widetilde{E}$ *of* EU*, where* E *is defined in theorem* 3.1.2*.*

We proceed to prove theorem 3.2.2 by first introducing a number of lemmas. The proofs of lemmas 3.2.3 and 3.2.4 can be found in [27] and [20] respectively.

Lemma 3.2.3. *Let* A *be an* $r\times s$ *integer matrix. Suppose* $EA=DA'$ *for some unimodular* E*, diagonal* D *and integer matrix* A'*. Let* E_i *be the* i*-th row of* E *and* d_i *the* i*-th diagonal entry of* D*. If the conditions* $E_i\mathbf{b}\equiv 0 \pmod{d_i}$ *for* $i=1,\ldots,r$ *are sufficient for the existence of an* *integer vector solution* $\mathbf{x}$ *of* $A\mathbf{x} = \mathbf{b}$*, then* D *is a diagonal form for* A *and* E *a corresponding front.*

Lemma 3.2.4. *Given a rational matrix* A *and a column vector* $\mathbf{b}$*, the system* $A\mathbf{x} = \mathbf{b}$ *has an integer vector solution* $\mathbf{x}$ *if and only if for every rational row vector* $\mathbf{y}$*,*

$$\mathbf{y}A \equiv \mathbf{0} \pmod 1 \textit{ implies } \mathbf{y}\mathbf{b} \equiv 0 \pmod 1.$$

Lemma 3.2.5. *If* $\mathbf{h}$ *is primitive, then any rational row vector* $\mathbf{y}$ *such that* $\mathbf{y}N \equiv \mathbf{0} \pmod 1$ *implies* $\mathbf{y} \equiv \mathbf{z}U \pmod 1$ *for some rational vector* $\mathbf{z}$*.*

Proof. Let $\mathbf{f} = \mathbf{f}_{u,u',v,v'}$ be a 2-pod. Let $\mathbf{h}_{(u,v)}$, $\mathbf{h}_{(u',v')}$ and $\mathbf{h}_{(u,v)(u',v')}$ be the image of $\mathbf{h}$ under the permutations (u, v), (u', v') and $(u, v)(u', v')$ respectively. By direct computation, $\langle \mathbf{f}, \mathbf{h} \rangle\, \mathbf{f}^\top = \mathbf{h} + \mathbf{h}_{(u,v)(u',v')} - \mathbf{h}_{(u,v)} - \mathbf{h}_{(u',v')}$. As $\mathbf{h}$ is primitive, $\mathbf{f}^\top$ will be in the column module of N over $\mathbb{Z}$.

Now, $\mathbf{f}\mathbf{y}^\top = \mathbf{y}\mathbf{f}^\top \equiv 0 \pmod 1$ since $\mathbf{y}N \equiv \mathbf{0} \pmod 1$. Note that $\mathbf{f}$ can run through all 2-pods, so $\mathcal{F}\mathbf{y}^\top \equiv \mathbf{0} \pmod 1$, where $\mathcal{F}$ is a matrix whose rows are all the 2-pods $\mathbf{f}$. We claim that there is an integer vector solution $\mathbf{x}$ to $\mathcal{F}\mathbf{x} = \mathcal{F}\mathbf{y}^\top$. For every rational row vector $\mathbf{w}$ such that $\mathbf{w}\mathcal{F} \equiv \mathbf{0} \pmod 1$, $\mathbf{w}\mathcal{F}$ is an integer vector in the null space of U. By proposition 3.2.1, $\mathbf{w}\mathcal{F} = \mathbf{w}'\mathcal{F}$ for some integer vector $\mathbf{w}'$, so $\mathbf{w}\mathcal{F}\mathbf{y}^\top = (\mathbf{w}'\mathcal{F})\mathbf{y}^\top \equiv \mathbf{w}'(\mathcal{F}\mathbf{y}^\top) \equiv 0 \pmod 1$. Our claim then follows from lemma 3.2.4.

Let $\mathbf{x}$ be our integer vector solution to $\mathcal{F}\mathbf{x} = \mathcal{F}\mathbf{y}^\top$, or $\mathcal{F}(\mathbf{y}^\top - \mathbf{x}) = \mathbf{0}$. This implies that $\mathbf{y} - \mathbf{x}^\top$ is in the row space of U, so $\mathbf{y} = \mathbf{z}U + \mathbf{x}^\top$ for some rational vector $\mathbf{z}$, i.e., $\mathbf{y} \equiv \mathbf{z}U \pmod 1$. □

Lemma 3.2.6. *If* $\mathbf{h}$ *is primitive,* $N\mathbf{x} = \mathbf{b}$ *has an integer vector solution* $\mathbf{x}$ *if and only if* $UN\mathbf{x}' = U\mathbf{b}$ *has an integer vector solution* $\mathbf{x}'$*.*

Proof. The direction "only if" is trivial. Assume that $\mathbf{x}'$ is an integer vector solution of $UN\mathbf{x}' = U\mathbf{b}$. Let $\mathbf{y}$ be a rational row vector such that $\mathbf{y}N \equiv \mathbf{0} \pmod 1$. By lemma 3.2.5, $\mathbf{y} \equiv \mathbf{z}U \pmod 1$ for some rational $\mathbf{z}$. Then $\mathbf{y}\mathbf{b} \equiv \mathbf{z}U\mathbf{b} = \mathbf{z}UN\mathbf{x}' \equiv \mathbf{y}N\mathbf{x}' \equiv 0 \pmod 1$. By lemma 3.2.4, we are done. □

Proof of theorem 3.2.2. Let $d_1 = \frac{eg}{hc}$, $d_2 = \tilde{g}c$, $d_3 = h$ and $d_i = g$ for $i = 4, 5, \ldots, 2n-1$. As E is a front of UN, there exists a back F such that $EUNF = D$ where D is a diagonal matrix with diagonal entries d_i's.

Let $\widetilde{E}$ be a unimodular extension of EU with rows $\widetilde{E}_i$, $i = 1, \ldots, n^2$. Suppose $\widetilde{E}_i\mathbf{b} \equiv 0 \pmod{d_i}$ for $i = 1, \ldots, 2n-1$ and $\widetilde{E}_i\mathbf{b} \equiv 0 \pmod{1}$ for $i = 2n \ldots, n^2$. Note that the first $2n-1$ congruences are equivalent to $E_iU\mathbf{b} \equiv 0 \pmod{d_i}$ for $i = 1, \ldots, 2n-1$, which implies $EU\mathbf{b} = D\mathbf{x}'' = EUNF\mathbf{x}''$ for some integer vector $\mathbf{x}''$. Hence, $UN\mathbf{x}' = U\mathbf{b}$ has an integer vector solution $\mathbf{x}' = F\mathbf{x}''$. By lemma 3.2.6, $N\mathbf{x} = \mathbf{b}$ has an integer vector solution $\mathbf{x}$. By lemma 3.2.3, $\widetilde{E}$ is a front of N and $d_1, \ldots, d_{2n-1}, (1)^{(n-1)^2}$ is the corresponding list of diagonal factors. $\square$

3.3 The nonprimitive case

Proposition 3.3.1. *Let G be a nonempty subgraph of the complete bipartite graph $K_{n,n}$ with $2n$ vertices. Then G is nonprimitive if and only if G is $K_{n,n}$, $K_{s,n} \dot\cup \{n-s$ isolated vertices$\}$ or $K_{s,t} \dot\cup K_{n-s,n-t}$ for some $1 \le s, t \le n-1$.*

Proof. Let $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ be the two partite sets of G. Let $u \leftrightarrow v$ represent that $\{u, v\}$ is an edge in G while $u \not\leftrightarrow v$ represent that $\{u, v\}$ is not.

If G is $K_{n,n}$, then it is obviously nonprimitive. If G is nonprimitive but not $K_{n,n}$, then without loss of generality, u_1, u_2, v_1, v_2 satisfy one of the following two cases:

(i) $u_1 \leftrightarrow v_1$ and $u_1 \leftrightarrow v_2$, while $u_2 \not\leftrightarrow v_1$ and $u_2 \not\leftrightarrow v_2$;

(ii) $u_1 \leftrightarrow v_1$ and $u_2 \leftrightarrow v_2$, while $u_1 \not\leftrightarrow v_2$ and $u_2 \not\leftrightarrow v_1$.

Case (i). For any $u \neq u_1, u_2$, either $u \leftrightarrow v_i$ for both $i \in \{1, 2\}$ or $u \not\leftrightarrow v_i$ for both $i \in \{1, 2\}$, so $\Gamma(v_1) = \Gamma(v_2)$, where $\Gamma(x)$ denotes all the neighbors of vertex x. Now, for any $v \neq v_1, v_2$, either $v \leftrightarrow u$ for all $u \in \Gamma(v_1)$ and $v \not\leftrightarrow u'$ for all $u' \notin \Gamma(v_1)$, or $v \not\leftrightarrow u$ for all $u \in \Gamma(v_1)$ and $v \leftrightarrow u'$ for all $u' \notin \Gamma(v_1)$. Hence, G is either $K_{s,n} \dot\cup \{n-s$ isolated vertices$\}$ or $K_{s,t} \dot\cup K_{n-s,n-t}$ for some $1 \le s, t \le n$.

Case (ii). For any $u \neq u_1, u_2$, exactly one of $u \leftrightarrow v_1$ and $u \leftrightarrow v_2$ occurs. Note that $\Gamma(v_1)$

and $\Gamma(v_2)$ form a partition of $\{u_1, \ldots, u_n\}$. Now, for any $v \neq v_1, v_2$, either $v \leftrightarrow u$ for all $u \in \Gamma(v_1)$ and $v \not\leftrightarrow u'$ for all $u' \in \Gamma(v_2)$, or $v \not\leftrightarrow u$ for all $u \in \Gamma(v_1)$ and $v \leftrightarrow u'$ for all $u' \in \Gamma(v_2)$. Hence, G is $K_{s,t} \dot\cup K_{n-s,n-t}$ for some $1 \leq s, t \leq n$. $\square$

Theorem 3.3.2. *If G is nonprimitive, then diagonal forms of $N(G)$ can be given by the following.*

	G	*a list of diagonal factors of* $N(G)$
(a)	$K_{n,n}$	$(1)^1,\ (0)^{n^2-1}$
(b)	$K_{s,n} \dot\cup \{n-s$ *isolated vertices*$\}$ $1 \leq s \leq n-1$	$(s)^1,\ (h)^1,\ (1)^{2n-3},\ (0)^{(n-1)^2}$ $h = \text{GCD}\{n, s\}$
(c)	$K_{s,t} \dot\cup K_{n-s,n-t}$ $1 \leq s \leq t \leq n-1$	$\left(\frac{2((n-s)(n-t)+st)\tilde{g}}{h\delta}\right)^1, (h)^1, (\delta\tilde{g})^1, (2\tilde{g})^{2n-4}, (2)^{(n-2)^2}, (1)^{2n-3}$ $\tilde{g} = \text{GCD}\{n-2s, t-s\}$, $h = \text{GCD}\{n, s, t\}$, $\delta = \text{GCD}\{\frac{n-t+s}{h}, 2\}$

(a) is trivial, so we will omit its proof.

Proof of (b). By dropping the repetitive columns and applying integral elementary column operations on N, the matrix becomes

$$\begin{array}{|c|c|} \hline A & B \\ \hline A & C_1 - C_2 \\ \hline \vdots & \vdots \\ \hline A & C_1 - C_s \\ \hline \hline A & -C_{s+1} \\ \hline \vdots & \vdots \\ \hline A & -C_n \\ \hline \end{array}\ , \text{ where } A = \begin{array}{|c|c|} \hline 1 & \mathbf{1}_{n-1} \\ \hline \begin{array}{c} \mathbf{1}^\top_{s-1} \\ \hline \mathbf{0}^\top_{n-s} \end{array} & -I_{(n-1)\times(n-1)} \\ \hline \end{array}\ ,$$

B is an $n \times n$ matrix of all 1's, and C_i is an $n \times n$ matrix with 1's in the i-th column and 0's elsewhere.

Take the sum of the second to the s-th column and add it to the first column, and take the sum of the $(n+2)$-th to the $(n+s)$-th column and add it to the $(n+1)$-th column. After that, in each section of n rows, subtract the last row from each of the other rows. Then add each of the in-th row, $2 \leq i \leq n$, to the n-th row. Finally, take the sum of the $(n+2)$-th to the $2n$-th column and add it to the n-th column. The resultant matrix will have the first to the $(n-1)$-th row occurring once in every section of n rows. By deleting the repeated rows, the matrix becomes

$$\left[\begin{array}{c|c|c||c|c}
s & \mathbf{1}_{n-2} & 2 & & \\
\hline
 & -I_{(n-2)\times(n-2)} & \mathbf{1}_{n-2}^{\top} & & \\
\hline
 & & -n & s & \\
\hline
 & & & & -I_{(n-1)\times(n-1)}
\end{array}\right].$$

Take the sum of the second to the $(n-1)$-th row and add it to the first row. Then take the sum of the second to the $(n-1)$-th column and add it to the n-th column. By rearranging the rows and columns, we have

$$\left[\begin{array}{ccc|c}
s & n & 0 & \multirow{2}{*}{$O_{2\times(2n-3)}$} \\
0 & -n & s & \\
\hline
\multicolumn{3}{c|}{O_{(2n-3)\times 3}} & -I_{(2n-3)\times(2n-3)}
\end{array}\right].$$

Adding the second row to the first row, subtracting the third column from the first column, and applying the Euclidean algorithm to $-n$ and s, we obtain the desired diagonal form. $\square$

Proof of (c). We will separate the proof into two cases: *Case* (i) $s=t$ and *Case* (ii) $s<t$. *Case* (i). In this case, diagonal factors of $N(G)$ can be simplified as

$$\left(\tfrac{2((n-s)^2+s^2)(n-2s)}{h\delta}\right)^1, (h)^1, (\delta(n-2s))^1, (2(n-2s))^{2n-4}, (2)^{(n-2)^2}, (1)^{2n-3},$$

where $h=\mathrm{GCD}\{n,s\}$ and $\delta=\mathrm{GCD}\{\frac{n}{h},2\}$.

By dropping the repetitive columns and applying integral elementary column operations on N, the matrix becomes

$$
\left[\begin{array}{c|c|ccccccc}
A_1 + \cdots + A_n - (B_2 + \cdots + B_n) & C & 2C & \cdots & 2C & 2C & \cdots & 2C \\
\hline
A_1 - A_2 + B_2 & C & -2C & & & & & \\
\vdots & \vdots & & \ddots & & & & \\
A_1 - A_s + B_s & C & & & -2C & & & \\
\hline
B_1 - A_{s+1} + B_{s+1} & -C & & & & -2C & & \\
\vdots & \vdots & & & & & \ddots & \\
B_1 - A_n + B_n & -C & & & & & & -2C
\end{array}\right],
$$

where A_i is an $n \times n$ matrix with the i-th column $\begin{bmatrix} \mathbf{1}_t & \mathbf{0}_{n-t} \end{bmatrix}^\top$ and 0's elsewhere, B_i is an $n \times n$ matrix with the i-th column $\begin{bmatrix} \mathbf{0}_t & \mathbf{1}_{n-t} \end{bmatrix}^\top$ and 0's elsewhere, and

$$
C = \left[\begin{array}{c}
\mathbf{1}_{n-1} \\
\hline
-I_{(n-1)\times(n-1)}
\end{array}\right].
$$

In each section of n rows, take the sum of the second to the n-th row and add it to the first row. For each $1 \leq i \leq n$, add the $(i + (n-1)n)$-th row to the $(i + jn)$-th row for each $0 \leq j \leq s - 1$, and subtract the $(i + (n-1)n)$-th row from the $(i + jn)$-th row for each $s \leq j \leq n - 1$. At this moment, from the $(n + 1)$-th column to the $(2n - 1)$-th column, there is only one 1 in each of them, and we can use them to clear all other entries in their corresponding $(2+(n-1)n)$-th row to the last row. This gives $(1)^{n-1}$ in a diagonal form of N.

Dropping the $(n+1)$-th column to the $(2n-1)$-th column and the $(2+(n-1)n)$-th row to the last row, the matrix becomes

$$
\begin{array}{|c|c|c||c|c|c|c|c|c|c|}
\hline
\multicolumn{3}{|c||}{A' - (B'_2 + \cdots + B'_{n-1})} & -C' & \cdots & -C' & -C' & \cdots & -C' & \\
\hline
\multicolumn{3}{|c||}{A' + B'_2 + B'_n} & C' & & & & & & C' \\
\hline
\multicolumn{3}{|c||}{\vdots} & & \ddots & & & & & \vdots \\
\hline
\multicolumn{3}{|c||}{A' + B'_s + B'_n} & & & C' & & & & C' \\
\hline\hline
\multicolumn{3}{|c||}{B'_{s+1} - B'_n} & & & & C' & & & -C' \\
\hline
\multicolumn{3}{|c||}{\vdots} & & & & & \ddots & & \vdots \\
\hline
\multicolumn{3}{|c||}{B'_{n-1} - B'_n} & & & & & & C' & -C' \\
\hline
n-t & \mathbf{0}_{n-2} & n-2t & \multicolumn{7}{c|}{\mathbf{0}_{(n-1)^2}} \\
\hline
\end{array},
$$

where A' is an $n \times n$ matrix with the first column $\begin{array}{|c|c|}\hline n & \mathbf{1}_{n-1} \\ \hline \end{array}^\top$ and 0's elsewhere, B'_i is an $n \times n$ matrix with the i-th column $\begin{array}{|c|c|c|}\hline n-2t & -\mathbf{1}_{s-1} & \mathbf{1}_{n-s} \\ \hline \end{array}^\top$ and 0's elsewhere, and

$$C' = \begin{array}{|c|} \hline \mathbf{0}_{n-1} \\ \hline \\ 2I_{(n-1)\times(n-1)} \\ \\ \hline \end{array} .$$

In each section of n rows, subtract $n-2t$ times the last row from the first row, add the last row to each of the second to the t-th row, and subtract the last row from each of the $(t+1)$-th to the $(n-1)$-th row. Subtract twice the n-th column from the last column. Take the sum of the second to the s-th column and subtract it from the n-th column, and take the sum of the $(s+1)$-th to the $(n-1)$-th column and add it to the n-th column. For each $2 \le i \le n-1$, subtract twice the i-th column from the $n+(i-1)(n-1)$-th column. For each $2 \le i \le n-1$, add the in-th row to the n-th row. At this moment, from the second column to the n-th column, there is only one 1 in each of them, and and we can use them to clear all other entries in their corresponding rows. This gives another $(1)^{n-2}$ in a diagonal form of N.

Dropping the second to the n-th column and the corresponding rows, the matrix becomes

$$
\left[\begin{array}{cc|ccccccc c}
\multicolumn{2}{c|}{A''} & -B'' & \cdots & -B'' & -B'' & \cdots & -B'' & \multicolumn{2}{c}{} \\
\hline
s & -(n-2s) & \multicolumn{8}{c}{\mathbf{0}_{(n-1)^2}} \\
\hline
\multicolumn{2}{c|}{A''} & B'' & & & & & & \multicolumn{2}{c}{B''} \\
\multicolumn{2}{c|}{\vdots} & & \ddots & & & & & \multicolumn{2}{c}{\vdots} \\
\multicolumn{2}{c|}{A''} & & & B'' & & & & \multicolumn{2}{c}{B''} \\
\hline
\multicolumn{2}{c|}{} & & & & B'' & & & \multicolumn{2}{c}{-B''} \\
\multicolumn{2}{c|}{} & & & & & \ddots & & \multicolumn{2}{c}{\vdots} \\
\multicolumn{2}{c|}{} & & & & & & B'' & \multicolumn{2}{c}{-B''} \\
\hline
n-t & n-2t & \multicolumn{6}{c}{\mathbf{0}_{(n-1)(n-2)}} & \mathbf{0}_{n-2} & -2(n-2t)
\end{array}\right],
$$

where

$$
A'' = \left[\begin{array}{c|c}
2t & \\
2\mathbf{1}_{t-1}^\top & \mathbf{0}_{n-1}^\top \\
\mathbf{0}_{n-t-1}^\top &
\end{array}\right], \quad
B'' = \left[\begin{array}{c|c}
\mathbf{0}_{n-2} & -2(n-2t) \\
\hline
 & 2\mathbf{1}_{t-1}^\top \\
2I_{(n-2)\times(n-2)} & \\
 & -2\mathbf{1}_{n-t-1}^\top
\end{array}\right],
$$

and there are s sections of A'' above the thick horizontal line.

For each $1 \le i \le n-2$, for each $1 \le j \le n-1$, add the $(1+i(n-1)+j)$-th row to the j-th row. At this moment, from the third column to the $(2+(n-2)(n-1))$-th column, except the $(2+in)$-th column for $1 \le i \le n-2$, there is only one 2 in each of them, and we can use them to clear all other entries in their corresponding rows. This gives $(2)^{(n-2)^2}$ in a diagonal form of N.

Dropping the third to the $(2+(n-2)(n-1))$-th column, except the $(2+in)$-th column for $1 \le i \le n-2$ and the corresponding rows, the matrix becomes $N' =$

$$\begin{array}{|c|c|c|c|c|}
\hline
2st & \mathbf{0}_{n-1}^\top & O_{(n-1)\times(n-2)} & \mathbf{0}_{n-2} & 2(n-2s)(n-2t) \\
\hline
2s\mathbf{1}_{t-1}^\top & & & -2(n-2s)I_{(n-2)\times(n-2)} & -2(n-2s)\mathbf{1}_{t-1}^\top \\
\hline
\mathbf{0}_{n-t-1}^\top & & & & 2(n-2s)\mathbf{1}_{n-t-1}^\top \\
\hline
s & -(n-2s) & \multicolumn{3}{c|}{\mathbf{0}_{2n-3}} \\
\hline
2t\mathbf{1}_{s-1}^\top & \mathbf{0}_{n-2}^\top & -2(n-2t)I_{(n-2)\times(n-2)} & O_{(n-2)\times(n-2)} & -2(n-2t)\mathbf{1}_{s-1}^\top \\
\hline
\mathbf{0}_{n-s-1}^\top & & & & 2(n-2t)\mathbf{1}_{n-s-1}^\top \\
\hline
n-t & n-2t & \multicolumn{2}{c|}{\mathbf{0}_{2n-4}} & -2(n-2t) \\
\hline
\end{array}.$$

For each $2 \le i \le t$, subtract twice the n-th row from the i-th row. For each $2 \le i \le s$, subtract twice the n-th row from the $(n+i-1)$-th row. At this moment, from the third to the $(2+2(n-2))$-th column, there is only one $-2(n-2s)$ in each of them, and we can use them to clear all other entries in their corresponding rows. This gives $(2(n-2s))^{2n-4}$ in a diagonal form of N.

Dropping the third to the $(2+2(n-2))$-th column and the corresponding rows, the matrix becomes

$$\begin{pmatrix} 2st & 0 & 2(n-2s)(n-2t) \\ s & -(n-2s) & 0 \\ n-t & n-2t & -2(n-2t) \end{pmatrix}.$$

Let $\theta, \phi \in \mathbb{Z}$ be such that ϕ is odd and $\theta n + \phi s = h = \mathrm{GCD}\{n, s\}$. This is possible since if one choice of ϕ is even, then $\frac{n}{h}$ is odd, and we can pick $\phi - \frac{n}{h}$ as our new ϕ. Using $s = t$, and applying a series of integral elementary row and column operations to this matrix, we get

$$\begin{pmatrix} 2s^2 & 0 & 2(n-2s)^2 \\ s & -(n-2s) & 0 \\ n-s & n-2s & -2(n-2s) \end{pmatrix} \sim \begin{pmatrix} 2s^2 & 0 & 2(n-2s)^2 \\ s & -(n-2s) & 0 \\ n & 0 & -2(n-2s) \end{pmatrix} \sim$$
$$\begin{pmatrix} (n-s)^2+s^2 & 0 & 0 \\ s & -(n-2s) & 0 \\ n & 0 & -2(n-2s) \end{pmatrix} \sim \begin{pmatrix} (n-s)^2+s^2 & 0 & 0 \\ -\frac{\phi-1}{2}n+\phi s & -(n-2s) & 0 \\ n & 0 & -2(n-2s) \end{pmatrix} \sim$$
$$\begin{pmatrix} (n-s)^2+s^2 & 0 & 0 \\ \theta n+\phi s & -(n-2s) & -(2\theta+\phi-1)(n-2s) \\ n & 0 & -2(n-2s) \end{pmatrix} \sim \begin{pmatrix} (n-s)^2+s^2 & 0 & 0 \\ h & -(n-2s) & 0 \\ n & 0 & -2(n-2s) \end{pmatrix} \sim$$
$$\begin{pmatrix} 0 & \frac{((n-s)^2+s^2)(n-2s)}{h} & 0 \\ h & -(n-2s) & 0 \\ 0 & \frac{n(n-2s)}{h} & -2(n-2s) \end{pmatrix} \sim \begin{pmatrix} 0 & \frac{((n-s)^2+s^2)(n-2s)}{h} & 0 \\ h & 0 & 0 \\ 0 & \frac{n(n-2s)}{h} & -2(n-2s) \end{pmatrix}.$$

If $\frac{n}{h}$ is even, then the last matrix is equivalent to

$$\begin{pmatrix} 0 & \frac{((n-s)^2+s^2)(n-2s)}{h} & 0 \\ h & 0 & 0 \\ 0 & 0 & -2(n-2s) \end{pmatrix}.$$

If $\frac{n}{h}$ is odd, then the last matrix is equivalent to

$$\begin{pmatrix} 0 & \frac{((n-s)^2+s^2)(n-2s)}{h} & 0 \\ h & 0 & 0 \\ 0 & n-2s & -2(n-2s) \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & \frac{2((n-s)^2+s^2)(n-2s)}{h} \\ h & 0 & 0 \\ 0 & n-2s & 0 \end{pmatrix}.$$

Case (ii). In a manner similar to case (i), by dropping the repetitive columns and applying integral elementary column operations on N, the first n^2 columns of the matrix are identical to those in case (i). However, there are an additional $2n-1$ columns, which are

$$\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\mathbf{p}^\top & \mathbf{r}^\top & \cdots & \mathbf{r}^\top & \mathbf{r}^\top & \cdots & \mathbf{r}^\top & \mathbf{r}^\top & \cdots & \mathbf{r}^\top & 2(t-s)C \\
\hline
\mathbf{p}^\top & -\mathbf{r}^\top & & & & & & & & & \\
\hline
\vdots & & \ddots & & & & & & & & \\
\hline
\mathbf{p}^\top & & & -\mathbf{r}^\top & & & & & & & \\
\hline\hline
\mathbf{p}^\top & & & & -\mathbf{r}^\top & & & & & & \\
\hline
\vdots & & & & & \ddots & & & & & \\
\hline
\mathbf{p}^\top & & & & & & -\mathbf{r}^\top & & & & \\
\hline\hline
\mathbf{q}^\top & & & & & & & -\mathbf{r}^\top & & & \\
\hline
\vdots & & & & & & & & \ddots & & \\
\hline
\mathbf{q}^\top & & & & & & & & & -\mathbf{r}^\top & \\
\hline
\end{array},$$

where $\mathbf{p} = \begin{array}{|c|c|}\hline \mathbf{1}_s & \mathbf{0}_{n-s} \\ \hline\end{array}$, $\mathbf{q} = \begin{array}{|c|c|}\hline \mathbf{0}_s & \mathbf{1}_{n-s} \\ \hline\end{array}$, $\mathbf{r} = \begin{array}{|c|c|}\hline 2(t-s) & \mathbf{0}_{n-1} \\ \hline\end{array}$,

$$C = \begin{array}{|c|}
\hline
\mathbf{1}_{n-1} \\
\hline
\\
-I_{(n-1)\times(n-1)} \\
\\
\hline
\end{array}\,,$$

and there are s sections above the first thick horizontal line, $t-s$ sections between the two thick horizontal lines and $n-t$ sections below the second thick horizontal lines.

Now, together with the first n^2 columns, apply the same row and column operations as in case (i) to get rid of the last $n-1$ rows, the n-th row in each of the i-th section, $2 \le i \le n-1$, as well as the j-th row, $2 \le j \le n-1$, in each of the i-th section, $2 \le i \le n-1$. The remaining rows in these extra $2n-1$ columns are $N'' =$

$$\begin{array}{|c|c|c|c|c|}
\hline
2st-2(t-s)^2 & & 2(t-s)(n-2s) & \mathbf{0}_{n-2} & 2(t-s)(n-2t) \\
\cline{1-1}\cline{3-5}
2s\mathbf{1}_{s-1}^{\top} & & & & -2(t-s)\mathbf{1}_{s-1}^{\top} \\
\cline{1-1}\cline{5-5}
2(2s-t)\mathbf{1}_{t-s}^{\top} & O_{n\times(n-2)} & \mathbf{0}_{n-1}^{\top} & -2(t-s)I_{(n-2)\times(n-2)} & -2(t-s)\mathbf{1}_{t-s}^{\top} \\
\cline{1-1}\cline{5-5}
\mathbf{0}_{n-t-1}^{\top} & & & & 2(t-s)\mathbf{1}_{s-1}^{\top} \\
\cline{1-1}\cline{4-5}
2s-t & & & \mathbf{0}_{n-2} & -2(t-s) \\
\hline
2t\mathbf{1}_{s-1}^{\top} & & -2(t-s)\mathbf{1}_{s-1}^{\top} & & \\
\cline{1-1}\cline{3-3}
-2(t-s)\mathbf{1}_{t-s}^{\top} & -2(t-s)I_{(n-2)\times(n-2)} & 2(t-s)\mathbf{1}_{t-s}^{\top} & O_{(n-1)\times(n-1)} & \\
\cline{1-1}\cline{3-3}
\mathbf{0}_{n-t-1}^{\top} & & 2(t-s)\mathbf{1}_{n-t-1}^{\top} & & \\
\cline{1-3}
n-s & \mathbf{0}_{n-2} & -2(t-s) & & \\
\hline
\end{array}\,.$$

Take the first column in N' in case (i) and subtract it from the first column in N''. For each $2 \le i \le t$, subtract twice the n-th row from the i-th row. For each $2 \le i \le s$, subtract twice the n-th row from the $(n+i-1)$-th row. At this moment, from the third to the $(2+2(n-2))$-th column in N', there is only one $-2(n-2s)$ or $-2(n-2t)$ in each of them, and from the second to the $(n-1)$-th column and from the $(n+1)$-th to the $(2n-2)$-th column in N'', there is only one $-2(t-s)$ in each of them. We can use them to clear all other entries in their corresponding rows. This gives $(2\mathrm{GCD}\{n-2s, t-s\})^{2n-4}$ in a diagonal form of N.

Dropping the second to the $(n-1)$-th row and the $(n+1)$-th to the $(2n-2)$-th row and the corresponding columns in both N' and N'', the combined matrix becomes

$$\begin{pmatrix} 2st & 0 & 2(n-2s)(n-2t) & -2(t-s)^2 & 2(t-s)(n-2s) & 2(t-s)(n-2t) \\ s & -(n-2s) & 0 & -(t-s) & 0 & -2(t-s) \\ n-t & n-2t & -2(n-2t) & t-s & -2(t-s) & 0 \end{pmatrix}.$$

Note that adding twice the fourth column with the fifth column gives the last, so we can eliminate the last column. Add $n-2t$ times the second row and $n-2s$ times the last row to the first row. Add the second row to the last row. Subtract the fifth column from the second column. Then the matrix becomes

$$\begin{pmatrix} (n-s)(n-t)+st & 0 & 0 & 0 & 0 \\ s & -(n-2s) & 0 & -(t-s) & 0 \\ n-t+s & 0 & -2(n-2t) & 0 & -2(t-s) \end{pmatrix},$$

which is equivalent to

$$\begin{pmatrix} (n-s)(n-t)+st & 0 & 0 \\ s & \tilde{g} & 0 \\ n-t+s & 0 & 2\tilde{g} \end{pmatrix},$$

where $\tilde{g} = \mathrm{GCD}\{n-2s, t-s\}$.

Let $\theta, \phi, \xi \in \mathbb{Z}$ be such that $\theta n + \phi s + \xi t = h = \mathrm{GCD}\{n, s, t\}$. Applying a series of integral elementary row and column operations to this matrix, we get

$$\begin{pmatrix} (n-s)(n-t)+st & 0 & 0 \\ s & \tilde{g} & 0 \\ n-t+s & 0 & 2\tilde{g} \end{pmatrix} \sim \begin{pmatrix} (n-s)(n-t)+st & 0 & 0 \\ s+\frac{-\phi-\xi+1}{2}(n-2s)+\frac{2\theta+\phi+3\xi-1}{2}(t-s) & \tilde{g} & 0 \\ n-t+s & 0 & 2\tilde{g} \end{pmatrix} \sim$$

$$\begin{pmatrix} (n-s)(n-t)+st & 0 & 0 \\ \theta n+\phi s+\xi t & \tilde{g} & (2\theta+\phi+\xi-1)\tilde{g} \\ n-t+s & 0 & 2\tilde{g} \end{pmatrix} \sim \begin{pmatrix} (n-s)(n-t)+st & 0 & 0 \\ h & -\tilde{g} & 0 \\ n-t+s & 0 & 2\tilde{g} \end{pmatrix} \sim$$

$$\begin{pmatrix} 0 & \frac{((n-s)(n-t)+st)\tilde{g}}{h} & 0 \\ h & -\tilde{g} & 0 \\ 0 & \frac{(n-t+s)\tilde{g}}{h} & 2\tilde{g} \end{pmatrix} \sim \begin{pmatrix} 0 & \frac{((n-s)(n-t)+st)\tilde{g}}{h} & 0 \\ h & 0 & 0 \\ 0 & \frac{(n-t+s)\tilde{g}}{h} & 2\tilde{g} \end{pmatrix}.$$

If $\frac{n-t+s}{h}$ is even, then the last matrix is equivalent to

$$\begin{pmatrix} 0 & \frac{((n-s)(n-t)+st)\tilde{g}}{h} & 0 \\ h & 0 & 0 \\ 0 & 0 & 2\tilde{g} \end{pmatrix}.$$

If $\frac{n-t+s}{h}$ is odd, then the last matrix is equivalent to

$$\begin{pmatrix} 0 & \frac{((n-s)(n-t)+st)\tilde{g}}{h} & 0 \\ h & 0 & 0 \\ 0 & \tilde{g} & -2\tilde{g} \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & \frac{2((n-s)(n-t)+st)\tilde{g}}{h} \\ h & 0 & 0 \\ 0 & \tilde{g} & 0 \end{pmatrix}.$$

$\square$

Chapter 4

Inclusion matrices arising from multisets

4.1 Inclusion matrix C_{tk}^v for multisets

Let $X = \{x_1, x_2, \ldots, x_v\}$ be a set of size v, and let $S = [a_1, a_2, \ldots, a_k]$ be a submultiset of X of size k, where every a_i is from X and they are not necessarily distinct. Also, the order of the elements does not matter. For example, $[1, 1, 1, 2, 2]$ is a submultiset of $\{1, 2, 3\}$ of size 5, and $[1, 1, 1, 2, 2] = [2, 1, 1, 2, 1]$.

For each element $x_i \in X$, let s_i denote the number of occurences of x_i in S, and we write $S = [x_1^{(s_1)}, x_2^{(s_2)}, \ldots, x_v^{(s_v)}]$. Hence, each submultiset S of size k corresponds to a tuple $(s_1, \ldots, s_v)$ of nonnegative integers such that $\sum s_i = k$. We denote it as $S \sim (s_i)_{i=1}^v$.

Let $0 \leq t \leq k$. Denote the set of k-submultisets of X by $\mathfrak{S}$ and the set of t-submultisets by $\mathfrak{T}$. Let C_{tk}^v be a $\binom{v+t-1}{t} \times \binom{v+k-1}{k}$ matrix with rows indexed by $T \in \mathfrak{T}$ and columns by $S \in \mathfrak{S}$ such that for each $T \sim (t_i)_{i=1}^v$ and $S \sim (s_i)_{i=1}^v$, $C_{tk}^v(T, S) = \prod \binom{s_i}{t_i}$, which calculates the number of ways to extract T from S. It is worth noting that W_{tk}^v is a submatrix of C_{tk}^v when $v \geq t + k$, since if both S and T are sets, then $C_{tk}^v(T, S) = 1$ if $T \subseteq S$ and 0 otherwise.

A fundamental relation for inclusion matrices C_{tk}^v is given by the following lemma.

Lemma 4.1.1 ([19]). *For $0 \leq i \leq t \leq k$, $C_{it}^v C_{tk}^v = \binom{k-i}{t-i} C_{ik}^v$.*

This chapter is going to study the row, column and null module of C_{tk}^v, and give the diagonal forms of C_{tk}^v for all parameters t, k and v.

4.2 Row, column and null module

Let $\mathbf{c}_S$ denote the column of C^v_{tk} corresponding to $S \in \mathfrak{S}$. For each $T = [a_1, \ldots, a_t] \in \mathfrak{T}$, let $S_T = [x_1^{(k-t)}, a_1, \ldots, a_t] \in \mathfrak{S}$ be an extension of T, the k-submultiset containing T and $k-t$ extra copies of x_1. So if $T \sim (t_i)_{i=1}^v$, then $S_T \sim (t_1 + k - t, t_2, \ldots, t_v)$. Let D^v_{tk} be the square submatrix of C^v_{tk} consisting of all the columns $\mathfrak{S}_0 := \{\mathbf{c}_{S_T}\}_{T \in \mathfrak{T}}$.

Let $A = (a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_t) \in X^{2t}$ be an ordered $2t$-tuple. Let $P_A = \prod(a_i - b_i) \in \mathbb{Z}[X]$ be a polynomial, and $\mathbf{p}_A$ be a column vector indexed by $\mathfrak{T}$ such that $\mathbf{p}_A(T)$ denotes the coefficient of T in the expansion of P_A, so

$$\mathbf{p}_A(T) = \sum_{\substack{(\theta_1, \ldots, \theta_t) \in \prod\{a_i, b_i\}: \\ T = [\theta_1, \ldots, \theta_t]}} (-1)^{|\{\theta_i : \theta_i = b_i\}|}.$$

This is analogous to the t-pods in chapter 2 and 2-pods in chapter 3. In fact, it is proved in [19] that $\{\mathbf{p}_A\}_{A \in X^{2t}}$ spans over $\mathbb{Z}$ all the integer vectors in $\mathrm{null}_{\mathbb{Q}}(C^v_{t-1,t})$.

Lemma 4.2.1. $D^v_{tk}\mathbf{p}_A = \mathbf{p}_A$.

Proof. Fix $A = (a_1, \ldots, a_t, b_1, \ldots, b_t) \in X^{2t}$. We will show that for each $T \in \mathfrak{T}$,

$$\sum_{T' \in \mathfrak{T}} D^v_{tk}(T, S_{T'})\mathbf{p}_A(T') = \mathbf{p}_A(T).$$

Fix $T \sim (t_i)_{i=1}^v$. Each term $D^v_{tk}(T, S_{T'})\mathbf{p}_A(T') \neq 0$ only if $T' = [\theta_1, \theta_2, \ldots, \theta_t]$ for some $\Theta = (\theta_1, \ldots, \theta_t) \in \prod\{a_i, b_i\}$ and T can be extracted from $S_{T'} = [x_1^{(k-t)}, \theta_1, \theta_2, \ldots, \theta_t]$. For each $0 \le r \le t_1$, let $\Gamma_{\Theta,r}$ be the set of $(t-r)$-subsets $\{i_1, i_2, \ldots, i_{t-r}\}$ of $\{1, 2, \ldots, t\}$ such that T can be written as $[x_1^{(r)}, \theta_{i_1}, \theta_{i_2}, \ldots, \theta_{i_{t-r}}]$. As $D^v_{tk}(T, S_{T'})$ calculates the number of ways to extract T from $S_{T'}$, we split the term in the following way: for each Θ, r and $\{i_1, \ldots, i_{t-r}\} \in \Gamma_{\Theta,r}$, we extract $x_1^{(r)}$ in T from $x_1^{(k-t)}$ in $S_{T'}$ and $\theta_{i_1}, \ldots, \theta_{i_{t-r}}$ in T from $\theta_{i_1}, \ldots, \theta_{i_{t-r}}$ in $S_{T'}$. Then the summation becomes

$$\begin{aligned}
\sum_{T' \in \mathfrak{T}} D^v_{tk}(T, S_{T'})\mathbf{p}_A(T') &= \sum_{\substack{T' = [\theta_1, \ldots, \theta_t]: \\ (\theta_1, \ldots, \theta_t) \in \prod\{a_i, b_i\}}} D^v_{tk}(T, S_{T'})(-1)^{|\{\theta_i : \theta_i = b_i\}|} \\
&= \sum_{0 \le r \le t_1} \sum_{\Theta \in \prod\{a_i, b_i\}} \sum_{\{i_1, \ldots, i_{t-r}\} \in \Gamma_{\Theta,r}} \binom{k-t}{r} (-1)^{|\{\theta_i : \theta_i = b_i\}|}.
\end{aligned}$$

In this summation, for each $r > 0$, for each $\{i_1, \ldots, i_{t-r}\} \in \Gamma_{\Theta,r}$, if we fix $(\theta_{i_1}, \ldots, \theta_{i_{t-r}})$, then there are 2^r choices of $\{\theta_1, \ldots, \theta_t\} \backslash \{\theta_{i_1}, \ldots, \theta_{i_{t-r}}\}$ to extend it to Θ. Among all these choices, exactly half of the extensions have $|\{\theta_i : \theta_i = b_i\}|$ being an odd number and the other half even, so these terms will cancel in the summation. This leaves the terms corresponding to $r = 0$. In this case, $T = T'$, and $\binom{k-t}{0} = 1$, so the summation is simply

$$\sum_{\substack{(\theta_1,\ldots,\theta_t)\in\prod\{a_i,b_i\}:\\ T=[\theta_1,\ldots,\theta_t]}} (-1)^{|\{\theta_i:\theta_i=b_i\}|} = \mathbf{p}_A(T).$$

□

Using the same notation introduced in section 2.3, we use $\sqcup M_i$ to denote the matrix composed by stacking the rows of the matrices M_i.

Lemma 4.2.2. *Let E^v_{jt} be the submatrix of C^v_{jt} consisting of the rows corresponding to those j-submultisets containing no x_1. Then if $i \leq t$, the row module of $\bigsqcup_{0\leq j\leq i} \binom{t-j}{i-j} E^v_{jt}$ over $\mathbb{Z}$ is the same as that of C^v_{it}.*

Proof. As $\binom{t-j}{i-j} E^v_{jt} = E^v_{ji} C^v_{it}$, $\bigsqcup_{0\leq j\leq i} \binom{t-j}{i-j} E^v_{jt} = \big(\bigsqcup_{0\leq j\leq i} E^v_{ji}\big) C^v_{it}$. It suffices to show that $E_i = \bigsqcup_{0\leq j\leq i} E^v_{ji}$ has determinant 1.

Assume that the rows and columns of E_i are arranged in lexicographical order. Let J_m denote the submultiset corresponding to the m-th row and H_n the i-submultiset corresponding to the n-th column of E_i. If $J_m \sim (0, j_2, \ldots, j_v)$ is of size j, then $H_m \sim (i-j, j_2, \ldots, j_v)$, so $E_i(J_m, H_m) = 1$. If $n < m$, then $H_n \sim (h_1, h_2, \ldots, h_v)$ has $h_1 \geq i - j$, so there is one ℓ, $2 \leq \ell \leq v$, such that $h_\ell < j_\ell$, and $E_i(J_m, H_n) = 0$. Therefore, E_i is upper-triangular with only 1's on the diagonal. □

Theorem 4.2.3. *The columns of D^v_{tk} form a basis in the column module of C^v_{tk} over $\mathbb{Z}$.*

Proof. Let $S = [a_1, \ldots, a_k] \in \mathfrak{S}$. We start by assuming that $a_1, \ldots, a_k \in X \backslash \{x_1\}$ are distinct, i.e., we also assume $v \geq k + 1$. It suffices to show that

$$\mathbf{c}_S = \sum_{0\leq i\leq t} r_i \sum_{\substack{\delta\subseteq\{1,\ldots,k\}\\ |\delta|=t-i}} \mathbf{c}_{[x_1^{(k-t+i)}, a_{\delta_1}, \ldots, a_{\delta_{t-i}}]}$$

for some integers r_i, $i = 0, \ldots, t$.

Take $r_0 = 1$. Then the entries corresponding to $[a_{\delta_1}, \ldots, a_{\delta_t}]$, $\delta \subseteq \{1, \ldots, k\}$ and $|\delta| = t$, are 1's on both sides. In summand i, the entries corresponding to $[x_1^{(j)}, a_{\delta_1}, \ldots, a_{\delta_{t-j}}]$ is $\binom{k-t+i}{j}\binom{k-t+j}{j-i}$, since there are $\binom{k-t+i}{j}$ ways to extract $x_1^{(j)}$ from $x_1^{(k-t+i)}$ and $\binom{k-t+j}{j-i}$ choices for $\delta_{t-j+1}, \ldots, \delta_{t-i}$. As $\binom{k-t+j}{j-i} = 0$ when $i > j$, in order to choose integers r_i such that all the entries corresponding to $[x_1^{(j)}, a_{\delta_1}, \ldots, a_{\delta_{t-j}}]$ are cancelled for $j > 0$, we only need to check that $\binom{k-t+i}{j}\binom{k-t+j}{j-i}$ is divisible by $\binom{k-t+j}{j}$ for all $i < j$, which is true since $\binom{k-t+i}{j}\binom{k-t+j}{j-i} = \binom{k-t}{j-i}\binom{k-t+j}{j}$.

Next, we remove all assumptions on S, but realize that $\mathbf{c}_S = \sum_{\substack{\delta \subseteq \{1, \ldots, k\} \\ |\delta| = t}} \mathbb{1}_{[a_{\delta_1}, \ldots, a_{\delta_t}]}$, where $\mathbb{1}_T$ is the characteristic column vector of length $\binom{v+t-1}{t}$ with 1 at the entry corresponding to T and 0 elsewhere. Hence, our proof above works for all $S \in \mathfrak{S}$. $\square$

The next theorem is motivated by the work in [2], which attempts to study Hartman's conjecture on large sets of t-designs [13, 15] through understanding the row module of the inclusion matrix W_{tk}^v for sets. More details will be introduced in section 6.1. A conjecture in [2] is that the signs are constant in each row of the reduced row echelon form of W_{tk}^v. They believe that there are certain relationships between this property and the property that there is a vector of 1's and -1's in the null space of W_{tk}^v. Although the author cannot prove this sign property for W_{tk}^v, he manages to prove it for C_{tk}^v instead.

Theorem 4.2.4. *Let the columns of C_{tk}^v be arranged in lexicographical order, and let $\widetilde{C}_{tk}^v$ be the reduced row echelon form of C_{tk}^v. Then all entries of $\widetilde{C}_{tk}^v$ are integers, and the signs of each row are constant, i.e., either all entries are nonnegative or all entries are nonpositive except the leading* 1.

Proof. The fact that all entries of $\widetilde{C}_{tk}^v$ are integers follows from theorem 4.2.3 since D_{tk}^v are the leading columns of C_{tk}^v. We will finish by showing that when $\{\mathbf{c}_S : S \in \mathfrak{S}\}$ are expressed as a linear combination of $\{\mathbf{c}_{S_T} : T \in \mathfrak{T}\}$, the signs of the coefficients of $\mathbf{c}_{S_T}$ always stay unchanged. To do that, we first determine r_j's in theorem 4.2.3.

Claim. $r_j = (-1)^j \binom{k-t+j-1}{j}$.

Proof of claim. The claim holds for $j = 0$. When $j > 0$, there is a recurrence relation for r_j, namely $r_j = -\sum_{i=0}^{j-1} \binom{k-t}{j-i} r_i$. By induction, we have $r_j = -\sum_{i=0}^{j-1} (-1)^i \binom{k-t}{j-i}\binom{k-t+i-1}{i}$, so we would like to show that $\sum_{i=0}^{j} (-1)^i \binom{k-t}{j-i}\binom{k-t+i-1}{i} = 0$. Note that $(-1)^i \binom{k-t+i-1}{i} = \binom{-(k-t)}{i}$, so the identity becomes $\sum_{i=0}^{j} \binom{k-t}{j-i}\binom{-(k-t)}{i} = 0$, which is true as a special case of $\sum_{i=0}^{j} \binom{x}{j-i}\binom{y}{i} = \binom{x+y}{j}$. □

This claim shows that if $S = [a_1, \dots, a_k]$ has $a_1, \dots, a_k \in X \backslash \{x_1\}$ all distinct, then when $\mathbf{c}_S$ is expressed as a linear combination of $\{\mathbf{c}_{S_T} : T \in \mathfrak{T}\}$, the sign of the coefficient of $\mathbf{c}_{S_T}$ is always $(-1)^j$ if $T \sim (j, t_2, \dots, t_v)$.

Next, notice if $a_1, \dots, a_\ell = x_1$, $\ell < k - t$, and $a_{\ell+1}, \dots, a_k \in X \backslash \{x_1\}$ are all distinct, then the coefficient of $\mathbf{c}_{[x_1^{(k-t+j)}, a_{\delta_1}, \dots, a_{\delta_{t-i}}]}$ is $\sum_{i=0}^{j} \binom{\ell}{j-i} r_i = \sum_{i=0}^{j} \binom{\ell}{j-i}\binom{-(k-t)}{i} = \binom{\ell-(k-t)}{j} = (-1)^j \binom{k-t-\ell+j-1}{j}$, so the sign is still $(-1)^j$.

Finally, if $a_{\ell+1}, \dots, a_k \in X \backslash \{x_1\}$ are not distinct, then the coefficient of $\mathbf{c}_{S_T}$, $T \sim (j, t_2, \dots, t_v)$, is a positive integral multiple of $(-1)^j \binom{k-t-\ell+j-1}{j}$. Hence, the sign of the coefficient of $\mathbf{c}_{S_T}$ is always $(-1)^j$. □

4.3 Integer solutions and diagonal forms of C_{tk}^v

Theorem 4.3.1. *There exists an integer vector solution* $\mathbf{x}$*for* $C_{tk}^v \mathbf{x} = \mathbf{a}$ *if and only if*

$$C_{it}^v \mathbf{a} \equiv \mathbf{0} \pmod{\tbinom{k-i}{t-i}} \text{ for } i = 0, 1, \dots, t. \tag{4.1}$$

Proof. The "only if" statement is trivial since $C_{tk}^v \mathbf{x} = \mathbf{a}$ for some integer vector $\mathbf{x}$ implies $C_{it}^v \mathbf{a} = C_{it}^v C_{tk}^v \mathbf{x} \equiv \mathbf{0} \pmod{\binom{k-i}{t-i}}$ for $i = 0, 1, \dots, t$ by lemma 4.1.1.

To prove the "if" statement, we proceed by induction on t. When $t = 0$, C_{tk}^v is a row vector of all 1's, so if $C_{00}^v \mathbf{a} \equiv 0 \pmod{\binom{k-0}{0-0}}$, i.e., $\mathbf{a}$ is an integer, then there always exists an integer vector $\mathbf{x}$ such that $C_{tk}^v \mathbf{x} = \mathbf{a}$. When $t > 0$, by lemma 3.2.4, it suffices to show that if condition (4.1) holds, then for any rational vector $\mathbf{y}$, $\mathbf{y} C_{tk}^v$ is an integer vector implies $\mathbf{y}\mathbf{a} \in \mathbb{Z}$.

Let $\mathbf{a}' = C^v_{t-1,t}\mathbf{a}$. For $i = 0, 1, \ldots, t-1$, by lemma 4.1.1,

$$C^v_{i,t-1}\mathbf{a}' = C^v_{i,t-1}C^v_{t-1,t}\mathbf{a} = (t-i)C^v_{it}\mathbf{a} \equiv \mathbf{0} \pmod{(t-i)\tbinom{k-i}{t-i}},$$

so $C^v_{i,t-1}(\frac{1}{k-t+1}\mathbf{a}') \equiv \mathbf{0} \pmod{\binom{k-i}{t-1-i}}$.

Claim. There exists an integer vector $\mathbf{z}$ indexed by t-submultisets and a rational vector $\mathbf{y}'$ indexed by $(t-1)$-submultisets such that $\mathbf{y} = \mathbf{z} + \mathbf{y}'C^v_{t-1,t}$.

If the claim holds,

$$((k-t+1)\mathbf{y}')C^v_{t-1,k} = \mathbf{y}'C^v_{t-1,t}C^v_{tk} = \mathbf{y}C^v_{tk} - \mathbf{z}C^v_{tk},$$

which is an integer vector. By induction hypothesis, $(k-t+1)\mathbf{y}'(\frac{1}{k-t+1}\mathbf{a}') = \mathbf{y}'\mathbf{a}' \in \mathbb{Z}$. As a result, $\mathbf{y}\mathbf{a} = \mathbf{z}\mathbf{a} + \mathbf{y}'\mathbf{a}' \in \mathbb{Z}$ and we are done.

Proof of claim. By lemma 4.2.1, $\mathbf{p}_A$ is in the column module of C^v_{tk} over $\mathbb{Z}$, so $\mathbf{y} \cdot \mathbf{p}_A$ is an integer since $\mathbf{y}C^v_{tk}$ is an integer vector. If P denotes the matrix with all $\mathbf{p}_A$ as its columns, then $\mathbf{y}P$ is an integer vector. As $\{\mathbf{p}_A\}_{A\in X^{2t}}$ spans over $\mathbb{Z}$ all the integer vectors in the null space to the row space of $C^v_{t-1,t}$ over $\mathbb{Q}$, we can select columns of P to obtain a unimodular matrix. Then P is row-unimodular by definition, so there exists an integer vector $\mathbf{z}$ such that $\mathbf{y}P = \mathbf{z}P$. This implies $\mathbf{y} - \mathbf{z}$ is in the null space to the column space of P, or equivalently, it is in the row space of $C^v_{t-1,t}$. Hence, there exists a rational vector $\mathbf{y}'$ such that $\mathbf{y} - \mathbf{z} = \mathbf{y}'C^v_{t-1,t}$. □

Theorem 4.3.2. *A diagonal form for C^v_{tk} is given by diagonal entries $\binom{k-i}{t-i}$ with multiplicities $\binom{v+i-1}{i} - \binom{v+i-2}{i-1}$, $i = 0, 1, \ldots, t$.*

Proof. Let D be a diagonal matrix with entries $\binom{k-i}{t-i}$ of multiplicities $\binom{v+i-1}{i} - \binom{v+i-2}{i-1}$, $i = 0, 1, \ldots, t$. From the proof in lemma 4.2.2, $E_t = \bigsqcup_{0\le i\le t} E^v_{it}$ is a unimodular matrix, and $E^v_{it}C^v_{tk} \equiv O \pmod{\binom{k-i}{t-i}}$, so $E_tC^v_{tk} = DA'$ for some integral matrix A'.

Assume that $E^v_{it}\mathbf{a} \equiv \mathbf{0} \pmod{\binom{k-i}{t-i}}$ for $i = 0, 1, \ldots, t$. By lemma 4.2.2, there exists a unimodular matrix U_i such that $C^v_{it} = U_i\big(\bigsqcup_{0\le j\le i} \binom{t-j}{i-j}E^v_{jt}\big)$. Then

$$C^v_{it}\mathbf{a} = U_i\Big(\bigsqcup_{0\le j\le i} \binom{t-j}{i-j}E^v_{jt}\Big)\mathbf{a} \equiv \mathbf{0} \pmod{\tbinom{k-i}{t-i}},$$

since $\binom{t-j}{i-j}\binom{k-j}{t-j} = \binom{k-j}{i-j}\binom{k-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}$. By theorem 4.3.1, there exists an integer vector solution $\mathbf{x}$ for $C_{tk}^{v}\mathbf{x} = \mathbf{a}$, and by lemma 3.2.3, D is a diagonal form of C_{tk}^{v}. $\square$

Chapter 5

Ramsey-type problems

5.1 Zero-sum (mod 2) Ramsey numbers for hypergraphs

Let H be a given t-uniform hypergraph on k vertices with e edges, and let m be a positive integer which divides e. Let $K_v^{(t)}$ denote the complete t-uniform hypergraph on v vertices, and let $\mathcal{T}$ denote the set of all edges of $K_v^{(t)}$. In the zero-sum Ramsey problem, we want to determine the smallest integer $v \geq k$, called $ZR_m(H)$, such that for any coloring $c : \mathcal{T} \to \mathbb{Z}_m$, there exists an isomorphic copy of H in $K_v^{(t)}$ so that the sum of the colors on its edges is 0 in $\mathbb{Z}_m$.

The zero-sum (mod 2) Ramsey numbers for graphs are completely characterized by Caro [6], and a bound on the $ZR_2(H)$ for t-uniform hypergraphs is given by Wilson [29]. In this section, we will show that $ZR_2(H) = k$ for almost all H, and reproduce Caro's results on $ZR_2(G)$ in the next section.

Let $c : \mathcal{T} \to \mathbb{Z}_m$ be a coloring of $K_v^{(t)}$ and let $\mathbf{c}$ be the t-vector over $\mathbb{Z}_m$ such that $\mathbf{c}(T) = c(T)$. Let $H^{\uparrow v}$ be the hypergraph obtained by adjoining isolated vertices to H so that the total number of vertices is v. If $\mathbf{h}$ is the characteristic vector of a spanning subgraph H' of $K_v^{(t)}$ which is isomorphic to $H^{\uparrow v}$, then $\langle \mathbf{c}, \mathbf{h} \rangle$ gives the sum of the colors on the edges of H'. Hence, $ZR_m(H)$ is the smallest integer $v \geq k$ such that $\mathrm{row}_{\mathbb{Z}_m}(N_t(H^{\uparrow v}))$ does not contain a nowhere zero vector. In particular, if $m = 2$, then $ZR_m(H)$ is the smallest integer $v \geq k$ such that the vector $\mathbf{1}$ of all ones is not in $\mathrm{row}_{\mathbb{Z}_m}(N_t(H^{\uparrow v}))$.

Lemma 5.1.1. *Let A be an $r \times s$ integer matrix, D, E and F be its diagonal form, front and back respectively, i.e., $EAF = D$. Let $d_1, d_2, \ldots, d_s$ be the diagonal entries of D, with the understanding that $d_i = 0$ if $r < i \leq s$. Let $\mathbf{s}$ be an integer row vector of length s. Then $\mathbf{s}$ is in $\mathrm{row}_{\mathbb{Z}_m}(A)$ if and only if the i-th entry of $\mathbf{s}F$ is divisible by $\mathrm{GCD}\{d_i, m\}$ for $i = 1, 2, \ldots, s$.*

Proof. The vector $\mathbf{s}$ is in $\mathrm{row}_{\mathbb{Z}_m}(A)$ if and only if there exists an integer vector $\mathbf{x}$ such that $\mathbf{x}A \equiv \mathbf{s} \pmod m$, which is equivalent to $(\mathbf{x}E^{-1})EA \equiv \mathbf{s} \pmod m$. This equation has an integer vector solution $\mathbf{x}$ if and only if $\mathbf{y}D \equiv \mathbf{s}F \pmod m$ has an integer vector solution $\mathbf{y}$, and the necessary and sufficient conditions for the existence of an integer vector solution $\mathbf{y}$ are those given in the statement of the lemma. □

Theorem 5.1.2. *Let $\mathbf{h}$ be a t-vector based on a k-set X, $k \geq 2t$, and suppose that $\mathbf{h}$ and all of its shadows are multiples of primitive vectors. Let e be the sum of all entries of $\mathbf{h}$. Then $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_m}(N_t(\mathbf{h}))$ if and only if $\mathrm{GCD}\{e, m\} = 1$.*

Proof. Let E and D be defined as in the statement of theorem 2.3.3, and let F be the corresponding back such that such that $EN_tF = D$.

The first row of E is $\mathbf{1}_{\binom{k}{2}}$, so the first row of EN_t is $e\mathbf{1}_{k!}$. As the first row of D is $[e, \mathbf{0}_{k!-1}]$, we have $e\mathbf{1}_{k!}F = [e, \mathbf{0}_{k!-1}]$, or $\mathbf{1}_{k!}F = [1, \mathbf{0}_{k!-1}]$. By lemma 5.1.1, $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_m}(N_t(\mathbf{h}))$ if and only if 1 is divisible by $\mathrm{GCD}\{e, m\}$, or equivalently, $\mathrm{GCD}\{e, m\} = 1$. □

By taking $m = 2$, we obtain the following theorems as corollaries.

Theorem 5.1.3. *If H is a simple t-uniform hypergraph on $k \geq 2t$ vertices with even number of edges such that H and all of its shadows are primitive, then $ZR_2(H) = k$.*

A slightly weaker but probably more remarkable version is stated in the following theorem.

Theorem 5.1.4. *Let H be a simple random t-uniform hypergraph on k vertices with even number of edges. Then $ZR_2(H) = k$ almost surely as $k \to \infty$.*

Proof. This follows from theorems 2.4.1, 2.4.2, and 5.1.3. □

The following theorem gives sharp upper bounds on $ZR_2(H)$.

Theorem 5.1.5. *Let H be a simple t-uniform hypergraph on $k \geq 2t$ vertices with even number of edges. Then*
(a) $ZR_2(H) \leq k + t$;
(b) if H is neither empty nor complete, then $ZR_2(H) \leq k + t - 1$.

Proof. (a) When $v \geq k+t$, the hypergraph $H^{\uparrow v}$ and all of its shadows have at least t isolated vertices. By proposition 2.2.3, $H^{\uparrow v}$ and all of its shadows are primitive, so the result follows from theorem 5.1.3.
(b) When $v \geq k + t - 1$, $H^{\uparrow v}$ has at least $t - 1$ isolated vertices. By proposition 2.2.4, if the primitivity γ of $H^{\uparrow v}$ is greater than 1, then either all edges of H are present or all are absent. In other words, if H is neither empty nor complete, then $\gamma = 1$, or H is primitive. The j-th shadow of $H^{\uparrow v}$, $j \geq 1$, has at least $t - 1$ isolated vertices, so they are all primitive by proposition 2.2.3. Theorem 5.1.3 completes the proof. □

We remark that Caro [6] proves the special case of theorem 5.1.5(a) for $H = K_k^{(t)}$, while Wilson [29] proves the full statement of theorem 5.1.5(a). Also, it is proved in [29] that if $H = K_k^{(t)}$ and $\binom{k}{t}$ is even, then $ZR_2(H) = k + 2^q$, where 2^q is the smallest power of 2 that appears in the base 2 representation of t but not in the base 2 representation of k. So even when H is complete, $ZR_2(H) \leq k + t - 1$ holds except when t is a power of 2, in which case $ZR_2(H) = k + t$.

5.2 When is $\mathbf{1} \in \mathbf{row}_{\mathbb{Z}_p}(N_2(G))$ for graphs G?

The following theorem on zero-sum (mod 2) Ramsey numbers for graphs is from [6].

Theorem 5.2.1 (Y. Caro)**.** *Let G be a simple graph on k vertices with even number of edges. Then*

$$ZR_2(G) = \begin{cases} k+2 & \textit{if } G = K_k, \\ k+1 & \textit{if } G = K_r \mathbin{\dot\cup} K_{k-r} \textit{ or } G \neq K_k \textit{ has all vertices of odd degree,} \\ k & \textit{otherwise.} \end{cases}$$

This theorem is a corollary of theorem 5.2.2 below. Caro's proof of theorem 5.2.1 is significantly shorter than that obtained from our viewpoint, but our theorem makes assertions for all primes p. It is interesting to note that $p = 2$ is often a special case in the statement of theorem 5.2.2. In theorem 5.2.2, we opt to restrict our results for primes p rather than general m, because the statements become more complex in the general case.

Theorem 5.2.2. *Let G be a simple graph with $k \geq 4$ vertices with e edges and let p be a prime divisor of e. Let $\delta_1, \ldots, \delta_k$ be the degree sequence of G, $g = \mathrm{GCD}_{1 \leq i,j \leq v}(\delta_i - \delta_j)$, and $h = \mathrm{GCD}\{\delta_1, \ldots, \delta_k, e\}$. Then $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2(G))$ if and only if one of the following holds:*

(i) G is primitive with $p \mid g$ but $p \nmid h$,

(ii) $G = K_k$,

(iii) $G = K_{1,k-1}$ and $p > 2$,

(iv) $G = K_1 \mathbin{\dot\cup} K_{k-1}$ and $(p = 2$ or $p \nmid k-2)$,

(v) $G = K_r \mathbin{\dot\cup} K_{k-r}$, $2 \leq r \leq k-2$, and $(p = 2$ or $(p \mid g$ but $p \nmid h))$.

Proof of theorem 5.2.2 *implying theorem* 5.2.1. A graph G which satisfies condition (i) is a graph which is not complete but all the degrees are odd, so for this type of G, $ZR_2(G) \geq k+1$. However, the graph $G^{\uparrow k+1}$ does not satisfy any of the above five conditions, since it has an isolated vertex whose degree is even. Hence, $ZR_2(G^{\uparrow k+1}) = k+1$, implying $ZR_2(G) = k+1$.

If $G = K_k$, then $ZR_2(G) \geq k+1$ by (ii). However, $G^{\uparrow k+1} = K_1 \mathbin{\dot\cup} K_{k-1}$, so $ZR_2(G^{\uparrow k+1}) \geq k+2$ by (iv). As $ZR_2(G) \leq k+2$ by theorem 5.1.5(a), we have $ZR_2(G) = k+2$.

If $G = K_r \mathbin{\dot\cup} K_{k-r}$, $1 \leq r \leq k-1$, then (iv) and (v) implies that $ZR_2(G) \geq k+1$. Therefore, $ZR_2(G) = k+1$ since $ZR_2(G) \leq k+1$ by theorem 5.1.5(b). $\square$

To prove theorem 5.2.2, we restate lemma 5.1.1 for primes.

Lemma 5.2.3. *Let A be an $r \times s$ integer matrix, D, E and F be its diagonal form, front and back respectively, i.e., $EAF = D$. Let $d_1, d_2, \ldots, d_s$ be the diagonal entries of D, with the understanding that $d_i = 0$ if $r < i \leq s$. Let $\mathbf{s}$ be an integer row vector of length s. If p is a prime, then $\mathbf{s}$ is in $\mathrm{row}_{\mathbb{Z}_p}(A)$ if and only if*

$$p \mid d_i \qquad \textit{implies} \qquad p \textit{ divides the } i\textit{-th entry of } \mathbf{s}F$$

for $i = 1, 2, \ldots, s$.

Proof of theorem 5.2.2 when G is primitive. Recall from theorem 2.5.4 that the front E can be taken as

$$\left[\begin{array}{c|c|c|c}
\frac{(a_1,g)}{h} & \ell\frac{e}{h} & \multicolumn{1}{c|}{\multirow{2}{*}{$O_{2\times(k-2)}$}} & \multirow{3}{*}{$O_{k\times(\binom{k}{2}-k)}$} \\
\alpha & \beta & & \\
\mathbf{0}_{k-2}^{\top} & -\mathbf{1}_{k-2}^{\top} & I_{(k-2)\times(k-2)} & \\
\hline
\multicolumn{3}{c|}{O_{(\binom{k}{2}-k)\times k}} & I_{(\binom{k}{2}-k)\times(\binom{k}{2}-k)}
\end{array}\right]
\cdot
\left[\begin{array}{c|c}
\multicolumn{2}{c}{Y_{02}} \\
\hline
\multicolumn{2}{c}{Y_{12}} \\
\hline
O_{(\binom{k}{2}-k)\times k} & I_{(\binom{k}{2}-k)\times(\binom{k}{2}-k)}
\end{array}\right],$$

and the corresponding diagonal form is $D = \mathrm{diag}\big((eg/h)^1, (h)^1, (g)^{k-2}, (1)^{\binom{k}{2}-k}\big)$.

If we multiply the vector $[\beta, -\ell e/h, \mathbf{0}_{\binom{k}{2}-2}]$ to both sides of $EN_2F = D$, then L.H.S. $=$ $Y_{02}N_2F = e\mathbf{1}_{n!}F$, and R.H.S. $= [\beta eg/h, -\ell e, \mathbf{0}_{k!-2}]$, so we get

$$\mathbf{1}F = [\beta g/h, -\ell, \mathbf{0}_{k!-2}].$$

If $p \nmid g$, then $p \nmid h$ and $p \nmid \beta$ since $\beta(a_1, g)/h - \alpha\ell e/h = 1$ by the definition of α and β, so $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N_2)$ since $p \mid eg/h$ but $p \nmid \beta g/h$. If $p \mid h$, then $p \nmid \ell$ since $\mathrm{GCD}\{\ell, a_1, g\} = 1$ by definition, while $h \mid (a_1, g)$, so we also have $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N_2)$. Finally, if $p \mid g$ but $p \nmid h$, then $p \mid eg/h$ and $p \mid \beta g/h$, so $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$. $\square$

If G is nonprimitive, we study case by case, following theorem 2.6.2. It is trivial that $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2(G))$ if $G = K_k$ and $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N_2)$ if G is empty.

Proof of theorem 5.2.2 *when* $G = K_{1,k-1}$. Note that N_2 and EN_2 share the same row module, so $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ if and only if $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(EN_2)$. Recall from the proof of theorem 2.6.2(c) that the bottom $\binom{k}{2} - k$ rows of EN_2 are 0's, and the top k rows can be given by

$$\begin{array}{|c|c|}\hline 2 & \mathbf{0}_{k-1} \\ \hline \mathbf{0}_{k-1}^\top & I_{(k-1)\times(k-1)} \\ \hline \end{array} \cdot \begin{array}{|c|c|c|c|}\hline 0 & 0 & -1 & \mathbf{0}_{k-3} \\ \hline \mathbf{1}_{k-2}^\top & \mathbf{0}_{k-2}^\top & \multicolumn{2}{c|}{I_{(k-2)\times(k-2)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \\ \hline \end{array} \cdots \begin{array}{|c|c|c|c|}\hline 0 & 0 & -1 & \mathbf{0}_{k-3} \\ \hline \mathbf{1}_{k-2}^\top & \mathbf{0}_{k-2}^\top & \multicolumn{2}{c|}{I_{(k-2)\times(k-2)}} \\ \hline 0 & 1 & 1 & \mathbf{0}_{k-3} \\ \hline \end{array} .$$

Let us denote the first matrix in this product as D' and the second as F'. If we multiply the vector $[-(k-4), -(k-4), \mathbf{1}_{k-2}]$ to F', we get $\mathbf{1}_{k!}$. As F' is row-unimodular, this is the unique way to obtain $\mathbf{1}$ in $\mathrm{row}_{\mathbb{Z}_p}(F')$ for all primes p. Hence, $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(EN_2)$ if and only if $[-(k-4), -(k-4), \mathbf{1}_{k-2}] \in \mathrm{row}_{\mathbb{Z}_p}(D')$, which obviously holds true if $p > 2$, and fails if $p = 2$ since $2 = p \mid e = k-1$ implies k is odd, meaning that $k-4$ is also odd. $\square$

Proof of theorem 5.2.2 *when* $G = K_1 \dot\cup K_{k-1}$. Similar to the above proof for the case $G = K_{1,k-1}$, we recall from the proof of theorem 2.6.2(d) that the bottom $\binom{k}{2} - k$ rows of EN_2 are 0's, and the top k rows can be given by

$$\begin{array}{|c|c|}\hline k-2 & \mathbf{0}_{k-1} \\ \hline \mathbf{0}_{k-1}^\top & I_{(k-1)\times(k-1)} \\ \hline \end{array} \cdot \begin{array}{|c|c|c|c|}\hline 0 & 1 & \multicolumn{2}{c|}{\mathbf{1}_{k-2}} \\ \hline \mathbf{0}_{k-2}^\top & \mathbf{1}_{k-2}^\top & \multicolumn{2}{c|}{(J-I)_{k-2}} \\ \hline 1 & 0 & 0 & \mathbf{1}_{k-3} \\ \hline \end{array} \cdots \begin{array}{|c|c|c|c|}\hline 0 & 1 & \multicolumn{2}{c|}{\mathbf{1}_{k-2}} \\ \hline \mathbf{0}_{k-2}^\top & \mathbf{1}_{k-2}^\top & \multicolumn{2}{c|}{(J-I)_{k-2}} \\ \hline 1 & 0 & 0 & \mathbf{1}_{k-3} \\ \hline \end{array} .$$

Again, we denote the first matrix in the product as D' and the second as F'. Multiplying $[-(k-4), 0, \mathbf{1}_{k-2}]$ to F', we get $\mathbf{1}_{k!}$. As F' is row-unimodular, $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(EN_2)$ if and only if $[-(k-4), 0, \mathbf{1}_{k-2}] \in \mathrm{row}_{\mathbb{Z}_p}(D')$. This obviously holds true if and only if $p \nmid k-2$, or $p \mid k-2$ and $p \mid k-4$, which forces $p = 2$. $\square$

Proof of theorem 5.2.2 *when* $G = K_{r,k-r}$, $2 \le r \le k-2$. Recall from theorem 2.6.2(e) that a diagonal form of N_2 is $D = \mathrm{diag}\big((eg/h)^1, (h)^1, (2g)^{k-2}, (2)^{\binom{k}{2}-(2k-2)}, (1)^{k-2}\big)$, and a corresponding front E is given in the proof of theorem 2.6.2(e). If we multiply $[1, -\ell e/h, \mathbf{0}_{\binom{k}{2}-k}]$ to both sides of $EN_2F = D$, then L.H.S. $= Y_{02}N_2F = e\mathbf{1}F$, and R.H.S. $= [eg/h, -\ell e, \mathbf{0}_{k!-2}]$, so we get

$$\mathbf{1}F = [g/h, -\ell, \mathbf{0}_{k!-2}].$$

If $p \nmid g$, then by lemma 5.2.3, $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N_2)$; if $p \mid g = k-2r$, then together with $p \mid e = r(k-r)$, we have $p \mid h = \mathrm{GCD}\{r,k\}$. However, g/h and ℓ cannot be 0 in $\mathbb{Z}_p$ simultaneously, otherwise we have $\mathbf{1}F = \mathbf{0}$ in $\mathbb{Z}_p$, contradicting that the rows of F are linearly independent over all fields. Hence, $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N_2)$. □

Proof of theorem 5.2.2 *when* $G = K_r \dot\cup K_{k-r}$, $2 \le r \le k-2$. Recall from theorem 2.6.2(f) that a diagonal form of N_2 is $D = \big((2eg/\epsilon h)^1, (\epsilon h)^1, (2g)^{k-2}, (2)^{\binom{k}{2}-(2k-1)}, (1)^{k-1}\big)$, where $\epsilon = \mathrm{GCD}\{k, 2\}$.

When k is odd, if E is the corresponding front such that $EN_2F = D$, we multiply the vector $[1, -\ell e/h, \mathbf{0}_{\binom{k}{2}-5}, -eg/h, -eg/h, -eg/h]$ to both sides of the equation. Then L.H.S. $= e\mathbf{1}F$, and R.H.S $= [2eg/h, -\ell e, \mathbf{0}_{\binom{k}{2}-5}, -eg/h, -eg/h, -eg/h, \mathbf{0}_{k!-\binom{k}{2}}]$, so we get

$$\mathbf{1}F = [2g/h, -\ell, \mathbf{0}_{\binom{k}{2}-5}, -g/h, -g/h, -g/h, \mathbf{0}_{k!-\binom{k}{2}}].$$

Note that $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ only if $p \mid 2g/h$. If $p \mid 2$, i.e., $p = 2$, then since ℓ is defined to be even, we have $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ by lemma 5.2.3. If $p \mid g/h$, then since $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$ by definition of ℓ, $p \nmid \ell$, so $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ if and only if $p \nmid h$.

When k is even and $r - 1 \equiv h \pmod{2h}$, if E is the corresponding front, we multiply the vector $[1, -\ell e/h, \mathbf{0}_{\binom{k}{2}-5}, \ell e, \ell e, \ell e]$ to both sides of $EN_2F = D$. Then L.H.S. $= e\mathbf{1}F$, and R.H.S. $= [eg/h, -2\ell e, \mathbf{0}_{\binom{k}{2}-5}, \ell e, \ell e, \ell e, \mathbf{0}_{k!-\binom{k}{2}}]$, so we get

$$\mathbf{1}F = [g/h, -2\ell, \mathbf{0}_{\binom{k}{2}-5}, \ell, \ell, \ell, \mathbf{0}_{k!-\binom{k}{2}}].$$

Note that $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ only if $p \mid g/h$. Recall from the proof of theorem 2.6.2(f) that $k - r - 1 \equiv r - 1 \pmod{2h}$, so $g = k - 2r \equiv 0 \pmod{2h}$, implying that g/h is even. Hence, if $p = 2$, $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$. If $p \mid g/h$, we again have $p \nmid \ell$ for the same reason above, so $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N_2)$ if and only if $p \nmid h$.

Finally, when k is even and $r - 1 \equiv 0 \pmod{2h}$, if E is the corresponding front, we multiply the vector $[1, -\ell/h, \mathbf{0}_{\binom{k}{2}-2}]$ to both sides of $EN_2F = D$. Then we have

$$\mathbf{1}F = [g/h, -2\ell, \mathbf{0}_{k!-2}],$$

and the rest of the proof is the same as the case when $r - 1 \equiv h \pmod{2h}$. □

5.3 Zero-sum (mod 2) bipartite Ramsey numbers

In sections 5.1 and 5.2, we use results from chapter 2. In this section, however, we use results from chapter 3.

Let G be a nonempty subgraph of the complete bipartite graph $K_{n,n}$, and let $\mathbf{h}$ be its characteristic vector. Let e be the number of edges in G, and let p be a prime that divides e. Let $N = N(G)$ be the matrix whose columns are all the images of $\mathbf{h}$ under the automorphism group on $K_{n,n}$. The objective of this section is to investigate when $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$, and reproduce Caro and Yuster's results [7] on zero-sum bipartite Ramsey numbers.

Theorem 5.3.1. *If $\mathbf{h}$ is primitive and p is a prime such that $p \mid e$, where e is the number of edges in G, then $\mathbf{1}$ is in $\mathrm{row}_{\mathbb{Z}_p}(N)$ if and only if either of the following holds:*
(i) $p \nmid h$ and $p \mid \tilde{g}$,
(ii) $p = 2$, $p \nmid \tilde{g}$ and $p \mid g$,
(iii) $p \neq 2$, $p \nmid \tilde{g}$, $p \mid g$ and $p \nmid a_1 + b_1$.

Proof. Let $\widetilde{E}NF = D$, where $D = \mathrm{diag}\big((\frac{eg}{hc})^1, (\tilde{g}c)^1, (h)^1, (g)^{2n-4}, (1)^{(n-1)^2}\big)$ is the diagonal form of N and $\widetilde{E}$ is the corresponding front given in theorem 3.2.2. If we multiply the vector $[\ell', -\alpha\frac{e}{hc}, \ell''\alpha\frac{e}{hc} - \ell'\sigma\beta\frac{eg}{hc\tilde{g}}, \mathbf{0}_{n^2-3}]$ to both sides of $\widetilde{E}NF = D$, then L.H.S. $= [1, \mathbf{0}_{n^2-1}]UNF =$

$\mathbf{1}_{n^2}NF = e\mathbf{1}F$, and R.H.S. $= [\ell'\frac{eg}{hc}, -\alpha\frac{e\tilde{g}}{h}, \ell''\alpha\frac{e}{c} - \ell'\sigma\beta\frac{eg}{\tilde{g}c}, \mathbf{0}_{n^2-3}] = [\ell'\frac{eg}{hc}, -\alpha\frac{e\tilde{g}}{h}, -\beta e, \mathbf{0}_{n^2-3}]$ since $\ell''\alpha\frac{e}{c} - \ell'\sigma\beta\frac{eg}{\tilde{g}c} = \beta\frac{e}{c}\left(\frac{\ell e+\ell'(a_1+b_1)}{h}\alpha - \ell'\sigma\frac{g}{\tilde{g}}\right) = \beta\frac{e}{c}\left(\ell\alpha\frac{e}{h} - \ell'\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\}\right) = -\beta e$. Therefore, we have

$$\mathbf{1}F = [\ell'\tfrac{g}{hc}, -\alpha\tfrac{\tilde{g}}{h}, -\beta, \mathbf{0}_{n^2-3}].$$

To determine whether $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$, we will apply lemma 5.2.3 and do the following analysis.

If $p \mid h$, then by lemma 2.5.1, β can be chosen in theorem 3.1.2 such that $\mathrm{GCD}\{\beta, h\} = 1$, so $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N)$. If $p \nmid h$ but $p \mid \tilde{g}$, then since $\frac{\tilde{g}}{h} = \frac{g}{h\,(g/\tilde{g})}$ which divides $\frac{g}{hc}$, we have p divides both $\ell'\frac{g}{hc}$ and $-\alpha\frac{\tilde{g}}{h}$, implying that $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$.

If $p \nmid \tilde{g}$ but $p \mid g$, then since $\tilde{g} = \mathrm{GCD}\{a_1 - b_1, g\}$, we have $p \nmid a_1 - b_1$. If $p = 2$, then $p \nmid a_1 + b_1$, implying that $p \nmid c$, so $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$. If $p \neq 2$ and $p \nmid a_1 + b_1$, then $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$ by the same argument. If $p \mid a_1 + b_1$, then $p \mid c$. However, $p \nmid \alpha$ since $\mathrm{GCD}\left\{\alpha, \frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} = 1$, so $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N)$.

Lastly, if $p \nmid g$, then $p \nmid c$, and $\ell'\mathrm{GCD}\left\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\right\} - \ell\alpha\frac{e}{h} = c$ implies $p \nmid \ell'$, so $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N)$. □

Theorem 5.3.2. *If* $\mathbf{h}$ *is nonprimitive and* p *is a prime such that* $p \mid e$, $\mathbf{1}$ *is in* $\mathrm{row}_{\mathbb{Z}_p}(N)$ *if and only if either of the following holds:*

(i) G *is* $K_{n,n}$*,*

(ii) G *is* $K_{s,n} \sqcup \{n - s$ *isolated vertices*$\}$ *with* $p \nmid s$*,*

(iii) G *is* $K_{s,t} \sqcup K_{n-s,n-t}$ *with* $p \nmid h$ *and* $p \mid \frac{2\tilde{g}}{\delta}$*, where* $h = \mathrm{GCD}\{n, s, t\}$*,* $\tilde{g} = \mathrm{GCD}\{n-2s, t-s\}$*,* $\delta = \mathrm{GCD}\left\{\frac{n-t+s}{h}, 2\right\}$

Proof. (i) Every row of N is $\mathbf{1}$, so $\mathbf{1}$ is in $\mathrm{row}_{\mathbb{Z}_p}(N)$.

(ii) The list of diagonal factors of N given in theorem 3.3.2(b) is $(s)^1, (h)^1, (1)^{2n-3}, (0)^{(n-1)^2}$. By keeping track of the row operations in the proof of theorem 3.3.2(b), the corresponding front E of N is

$$\begin{array}{|c|c|c|c|}
\hline
P & Q & \cdots & Q \\
\hline
R & S & & \\
\hline
\vdots & & \ddots & \\
\hline
R & & & S \\
\hline
\end{array},$$

where

$$P = \begin{array}{|c|c|c|}
\hline
1 & \mathbf{1}_{n-2} & -(n-2) \\
\hline
\mathbf{0}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & -\mathbf{1}_{n-2}^{\top} \\
\hline
0 & \mathbf{0}_{n-2} & 1 \\
\hline
\end{array}, \quad Q = \begin{array}{|c|c|}
\hline
 & 1 \\
\cline{2-2}
O_{n\times(n-1)} & \mathbf{0}_{n-2}^{\top} \\
\cline{2-2}
 & 1 \\
\hline
\end{array},$$

$$R = \begin{array}{|c|c|}
\hline
-I_{(n-1)\times(n-1)} & \mathbf{1}_{n-1}^{\top} \\
\hline
\mathbf{0}_{n-1} & 0 \\
\hline
\end{array}, \quad S = \begin{array}{|c|c|}
\hline
I_{(n-1)\times(n-1)} & -\mathbf{1}_{n-1}^{\top} \\
\hline
\mathbf{0}_{n-1} & 1 \\
\hline
\end{array},$$

and there are n horizontal sections. The first row of E corresponds to the diagonal factor s, the n-th row corresponds to the diagonal factor h, the second to the $(n-1)$-th row and the (in)-th row, $2 \le i \le n$, correspond to the diagonal factor 1, and the rest corresponds to 0.

Let $ENF = D$. From the structure of $K_{s,n}$, we see that the first row of EN is $s\mathbf{1}$, so $s\mathbf{1}F = [s, \mathbf{0}_{2(n!)^2-1}]$, the first row of D. Hence,

$$\mathbf{1}F = [1, \mathbf{0}_{2(n!)^2-1}],$$

and $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$ if and only if $p \nmid s$.

(iii) The list of diagonal factors of N given in theorem 3.3.2(c) is $(\frac{2((n-s)(n-t)+st)\tilde{g}}{h\delta})^1, (h)^1, (\delta\tilde{g})^1, (2\tilde{g})^{2n-4}, (2)^{(n-2)^2}, (1)^{2n-3}$, and a corresponding front E of N is

$$\begin{array}{|c|c|c|c|c|}
\hline
P' & P' & \cdots & P' & Q' \\
\hline
 & R' & & & S' \\
\hline
 & & \ddots & & \vdots \\
\hline
 & & & R' & S' \\
\hline
T' & T' & \cdots & T' & U' \\
\hline
\end{array},$$

where

$$P' = \begin{array}{|c|c|c|}
\hline
1 & \mathbf{1}_{n-2} & \omega_1 \\
\hline
\mathbf{0}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & -\mathbf{1}_{n-2}^{\top} \\
\hline
0 & \mathbf{0}_{n-2} & 1+\mu \\
\hline
\end{array},$$

$$Q' = \begin{array}{|c|c|c|}
\hline
\omega_2 & \omega_2\mathbf{1}_{n-2} & \omega_3 \\
\hline
\mathbf{0}_{n-2}^{\top} & (1-(n-2s))I_{(n-2)\times(n-2)} & ((n-2s)-1)\mathbf{1}_{n-2}^{\top} \\
\hline
\mu & \mu\mathbf{1}_{n-2} & \omega_4 \\
\hline
\end{array},$$

$$R' = \left|\begin{array}{c|c|c} 1 & \mathbf{1}_{n-2} & 1-(n-2s) \\ \hline \mathbf{0}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & \mathbf{1}_{n-2}^{\top} \\ \hline 0 & \mathbf{0}_{n-2} & 1 \end{array}\right|,$$

$$S' = \left|\begin{array}{c|c|c} -1 & -\mathbf{1}_{n-2} & (n-2s)-1 \\ \hline \mathbf{0}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & \mathbf{1}_{n-2}^{\top} \\ \hline 0 & \mathbf{0}_{n-2} & 1 \end{array}\right|,$$

$$T' = \left|\begin{array}{c|c} O_{n\times(n-1)} & \begin{array}{c} 1-\frac{\nu}{h}(1+\mu) \\ \hline \mathbf{0}_{n-1}^{\top} \end{array} \end{array}\right|, \quad U' = \left|\begin{array}{c|c|c} 1-\frac{\nu}{h}\mu & (1-\frac{\nu}{h}\mu)\mathbf{1}_{n-2} & \omega_5 \\ \hline \mathbf{0}_{n-2}^{\top} & I_{(n-2)\times(n-2)} & \mathbf{1}_{n-2}^{\top} \\ \hline 0 & \mathbf{0}_{n-2} & 1 \end{array}\right|$$

and $e = (n-s)(n-t) + st$, $\mu = \frac{2\theta+\phi+\xi-1}{2}$, $\nu = n - t + s$, $\omega_1 = 1 - \frac{e}{h}\big[1 + \big(1 - \frac{\nu}{h}\big)(1+\mu)\big]$, $\omega_2 = 1 - \frac{e}{h}\big[1 + \big(1 - \frac{\nu}{h}\big)\mu\big]$, $\omega_3 = 1 - \frac{e}{h}\big(\omega_4 + \omega_5\big)$, $\omega_4 = 1 - (n-2s) + (2-(n-2s))\mu$, $\omega_5 = 2 - (n-2s) - \frac{\nu}{h}\omega_4$. The first row of E corresponds to the diagonal factor $\frac{2e\tilde{g}}{h\delta}$, the n-th row corresponds to the diagonal factor h, the $(n(n-1)+1)$-th row corresponds to the diagonal factor $\delta\tilde{g}$, the second to the $(n-1)$-th row and the $(1+in)$-th row, $1 \le i \le n-2$, correspond to the diagonal factor $2\tilde{g}$, the $(i+jn)$-th row, $2 \le i \le n-1$, $1 \le j \le n-2$, correspond to the diagonal factor 2, while the (in)-th row, $2 \le i \le n-1$, and the $((n-1)n+2)$-th to the last row correspond to the diagonal factor 1.

This matrix works as a front since the first, n-th and $(n(n-1)+1)$-th rows come from the row operations in the proof of theorem 3.3.2(c). As for the other rows, we can multiply to N directly to check.

Now, if we multiply $[1, \mathbf{0}_{n-2}, \frac{e}{h}, \mathbf{0}_{n(n-1)}, \frac{e}{h}, \mathbf{0}_{n-1}]$ to both sides of $ENF = D$, then L.H.S. $= e\mathbf{1}F$, and R.H.S. $= [\frac{2e\tilde{g}}{h\delta}, \mathbf{0}_{n-2}, e, \mathbf{0}_{n(n-1)}, \frac{e}{h}\delta\tilde{g}, \mathbf{0}_{n-1}]$, so we have

$$\mathbf{1}F = [\tfrac{2\tilde{g}}{h\delta}, \mathbf{0}_{n-2}, 1, \mathbf{0}_{n(n-1)}, \tfrac{\delta\tilde{g}}{h}, \mathbf{0}_{n-1}].$$

If $p \mid h$, then $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N)$ by lemma 5.2.3. If $p \nmid h$ and $p \nmid \frac{2\tilde{g}}{\delta}$, then $\mathbf{1} \notin \mathrm{row}_{\mathbb{Z}_p}(N)$ either. If $p \nmid h$ but $p \mid \frac{2\tilde{g}}{\delta}$, then regardless whether $p \mid \delta\tilde{g}$, we still have $\mathbf{1} \in \mathrm{row}_{\mathbb{Z}_p}(N)$. □

Next, we apply these results to the zero-sum bipartite Ramsey problem. Let G be a simple nonempty bipartite graph with e edges. A p-coloring on the edges of G is a function $c : E(G) \to \mathbb{Z}_p$. If $\sum_{T \in E(G)} c(T) = 0$ over $\mathbb{Z}_p$, then we say that G is a *zero-sum* (mod p) graph with respect to c. If $p \mid e$, then the *zero-sum bipartite Ramsey number* $ZB_p(G)$ is the smallest integer n such that for every p-coloring of $K_{n,n}$, there exists a zero-sum (mod p) copy of G in $K_{n,n}$.

The zero-sum (mod 2) bipartite Ramsey numbers are fully characterized by Caro and Yuster [7] in the following theorem, and we are going to provide our own proof here.

Theorem 5.3.3 (Y. Caro and R. Yuster)**.** *Let G be a simple nonempty bipartite graph with even number of edges. Let n be the minimum number such that the vertices of G can be divided into two partite sets, each of size not exceeding n. Then isolated vertices are added to G if necessary to make each partite set of G have size n, and by abuse of notation, we call this new graph G instead. Let $ZB_2(G)$ denote the zero-sum bipartite Ramsey number of G modulo 2. Then $ZB_2(G) = n + 1$ if and only if one of the following holds:*
(i) G is primitive with all degrees odd,
(ii) G is primitive such that for any partition of the vertices of G into two partite sets, each of size n, all degrees in one partite set are odd and all degrees in the other partite set even,
(iii) $G = K_{n,n}$,
(iv) $G = K_{s,n} \sqcup \{n - s$ isolated vertices$\}$ with s odd,
(v) $G = K_{s,t} \sqcup K_{n-s,n-t}$ with n even and at least one of s and t is odd.
Otherwise, $ZB_2(G) = n$.

Proof. Let $p = 2$. It is easy to see that theorems 5.3.1(i), 5.3.1(ii), 5.3.2(i) and 5.3.2(ii) are respectively equivalent to (i), (ii), (iii) and (iv) of this theorem. This leaves the only unobvious case, which is theorem 5.3.2(iii) is equivalent to (v) of this theorem.

If n is odd, then $\tilde{g}$ is also odd. As $p \nmid h$ and $p \mid \frac{2\tilde{g}}{\delta}$, we must have $\delta = 1$, implying s and t are of the same parity, which contradicts that p divides $e = st + (n-s)(n-t)$. If n is even, then p always divides e. Since $p \nmid h$, at least one of s and t is odd. If s and t are of opposite parity, then δ is odd and $p \mid \frac{2\tilde{g}}{\delta}$. If both s and t are odd, then $\tilde{g}$ is even and again $p \mid \frac{2\tilde{g}}{\delta}$.

$ZB_2(G) \geq n+1$ if and only if there exists a 2-coloring on the edges of $K_{n,n}$ such that all isomorphic copies of G in $K_{n,n}$ have color sum equal to 1 (mod 2). In other words, $\mathbf{1}$ is in $\text{row}_{\mathbb{Z}_2}(N)$, which happens if and only if one of the conditions in theorems 5.3.1 and 5.3.2 hold. Note that when two more isolated vertices are added to G so that G is embedded in $K_{n+1,n+1}$, none of these conditions are satisfied, so we always have $ZB_2(G) \leq n+1$. Combining these two directions, this theorem is proved. □

5.4 Ramsey problem on hypergraphs induced by equipartitions

Let s, t, v be positive integers such that $s \mid t \mid v$. Let X be a set of size v. An *s-equipartition* or *t-equipartition* of X is a partition of X into s or t equal parts. Let $\mathcal{V}$ and $\mathcal{E}$ be the set of s-equipartitions and t-equipartitions of X respectively.

Let $H = H(s,t,v)$ be a hypergraph induced by the equipartitions of X, where the vertex set of H is $\mathcal{V}$, and an edge of H is the collection of all s-equipartitions that share a common refinement $E \in \mathcal{E}$.

Conjecture 5.4.1. *For all $s, t \in \mathbb{N}$, there exists $v_0 \in \mathbb{N}$ such that for all $v \geq v_0$, if $s \mid t \mid v$, then for all 2-colorings of the vertices of $H = H(s,t,v)$, there exists a monochromatic edge, i.e., all the vertices in that edge have the same color.*

Unlike the classical Ramsey problem, where $K_{v_0}^{(t)}$ is a subgraph of $K_v^{(t)}$ for all $v \geq v_0$, it is not true that $H(s,t,v_0)$ is always a subgraph of $H(s,t,v)$ for $v \geq v_0$, $t \mid v$. Hence, it is more difficult to show that hypergraphs $H(s,t,v)$ arising from equipartitions has the Ramsey property. This conjecture originates as a problem from the logician point of view, but the author attempts to solve it from the combinatorial perspective, and is able to verify the conjecture for the case $s = 2$ and $t = 4$ by explicit constructions.

Lemma 5.4.2. *If $s = 2$, $t = 4$ and $8 \mid v$, then for all 2-colorings of the vertices of $H(s,t,v)$, there exists a monochromatic edge.*

Proof. Let $\{X_1, X_2, \dots, X_8\}$ be an 8-equipartition of a v-set X. Label some 2-equipartitions of X as follows:

$$\begin{aligned}
a:&\quad \{X_1 \cup X_2 \cup X_3 \cup X_4, X_5 \cup X_6 \cup X_7 \cup X_8\},\\
b:&\quad \{X_1 \cup X_2 \cup X_7 \cup X_8, X_3 \cup X_4 \cup X_5 \cup X_6\},\\
c:&\quad \{X_1 \cup X_2 \cup X_5 \cup X_6, X_3 \cup X_4 \cup X_7 \cup X_8\},\\
d:&\quad \{X_2 \cup X_3 \cup X_5 \cup X_8, X_1 \cup X_4 \cup X_6 \cup X_7\},\\
e:&\quad \{X_2 \cup X_3 \cup X_6 \cup X_7, X_1 \cup X_4 \cup X_5 \cup X_8\},\\
f:&\quad \{X_2 \cup X_4 \cup X_6 \cup X_8, X_1 \cup X_3 \cup X_5 \cup X_7\},\\
g:&\quad \{X_2 \cup X_4 \cup X_5 \cup X_7, X_1 \cup X_3 \cup X_6 \cup X_8\}.
\end{aligned}$$

Then

$$\{a,b,c\}, \{a,d,e\}, \{a,f,g\}, \{b,d,f\}, \{b,e,g\}, \{c,d,g\}, \{c,e,f\}$$

are edges in H. In fact, these seven edges form a subhypergraph isomorphic to the Fano plane, which is not 2-vertex-colorable, i.e., for all 2-vertex-colorings of H, there always exists a monochromatic edge in H. □

Lemma 5.4.3. *If $s = 2$, $t = 4$ and $12 \mid v$, then for all 2-colorings of the vertices of $H(s,t,v)$, there exists a monochromatic edge.*

Proof. Let $\{X_1, X_2, \dots, X_{12}\}$ be a 12-equipartition of a v-set X. Label some 2-equipartitions of X as follows:

$$
\begin{aligned}
A: &\quad \{X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5 \cup X_6, X_7 \cup X_8 \cup X_9 \cup X_{10} \cup X_{11} \cup X_{12}\},\\
B: &\quad \{X_1 \cup X_2 \cup X_3 \cup X_{10} \cup X_{11} \cup X_{12}, X_4 \cup X_5 \cup X_6 \cup X_7 \cup X_8 \cup X_9\},\\
C: &\quad \{X_1 \cup X_2 \cup X_3 \cup X_7 \cup X_8 \cup X_9, X_4 \cup X_5 \cup X_6 \cup X_{10} \cup X_{11} \cup X_{12}\},\\
D: &\quad \{X_1 \cup X_3 \cup X_5 \cup X_7 \cup X_9 \cup X_{11}, X_2 \cup X_4 \cup X_6 \cup X_8 \cup X_{10} \cup X_{12}\},\\
E: &\quad \{X_1 \cup X_3 \cup X_5 \cup X_8 \cup X_{10} \cup X_{12}, X_2 \cup X_4 \cup X_6 \cup X_7 \cup X_9 \cup X_{11}\},\\
F: &\quad \{X_1 \cup X_3 \cup X_4 \cup X_6 \cup X_8 \cup X_{11}, X_2 \cup X_5 \cup X_7 \cup X_9 \cup X_{10} \cup X_{12}\},\\
G: &\quad \{X_1 \cup X_2 \cup X_6 \cup X_7 \cup X_9 \cup X_{10}, X_3 \cup X_4 \cup X_5 \cup X_8 \cup X_{11} \cup X_{12}\},\\
H: &\quad \{X_1 \cup X_2 \cup X_6 \cup X_8 \cup X_{11} \cup X_{12}, X_3 \cup X_4 \cup X_5 \cup X_7 \cup X_9 \cup X_{10}\},\\
I: &\quad \{X_1 \cup X_2 \cup X_4 \cup X_5 \cup X_8 \cup X_{10}, X_3 \cup X_6 \cup X_7 \cup X_9 \cup X_{11} \cup X_{12}\},\\
J: &\quad \{X_1 \cup X_4 \cup X_7 \cup X_8 \cup X_9 \cup X_{12}, X_2 \cup X_3 \cup X_5 \cup X_6 \cup X_{10} \cup X_{11}\},\\
K: &\quad \{X_2 \cup X_3 \cup X_5 \cup X_8 \cup X_9 \cup X_{10}, X_1 \cup X_4 \cup X_6 \cup X_7 \cup X_{11} \cup X_{12}\},\\
L: &\quad \{X_2 \cup X_3 \cup X_5 \cup X_7 \cup X_{11} \cup X_{12}, X_1 \cup X_4 \cup X_6 \cup X_8 \cup X_9 \cup X_{10}\},\\
M: &\quad \{X_2 \cup X_3 \cup X_4 \cup X_6 \cup X_7 \cup X_{10}, X_1 \cup X_5 \cup X_8 \cup X_9 \cup X_{11} \cup X_{12}\},\\
N: &\quad \{X_3 \cup X_4 \cup X_5 \cup X_6 \cup X_9 \cup X_{12}, X_1 \cup X_2 \cup X_7 \cup X_8 \cup X_{10} \cup X_{11}\},\\
O: &\quad \{X_2 \cup X_4 \cup X_9 \cup X_{10} \cup X_{11} \cup X_{12}, X_1 \cup X_3 \cup X_5 \cup X_6 \cup X_7 \cup X_8\}.
\end{aligned}
$$

Then

$$
\begin{gathered}
\{A, B, C\}, \{A, D, E\}, \{B, D, F\}, \{C, E, F\}, \{A, G, H\},\\
\{B, G, I\}, \{D, G, J\}, \{C, H, I\}, \{E, H, J\}, \{F, I, J\},\\
\{A, K, L\}, \{B, K, M\}, \{D, K, N\}, \{G, K, O\}, \{C, L, M\},\\
\{E, L, N\}, \{H, L, O\}, \{F, M, N\}, \{I, M, O\}, \{J, N, O\}
\end{gathered}
$$

are edges in H. The subgraph of H on these fifteen vertices with these twenty edges is not 2-vertex-colorable by some checking on Mathematica. $\square$

Theorem 5.4.4. *If $s = 2$ and $t = 4$, then for all $v \geq 8$ such that $4 \mid v$, for all 2-colorings of the vertices of $H = H(s, t, v)$, there exists a monochromatic edge. In other words, conjecture* 5.4.1 *is true for the case $s = 2$ and $t = 4$, with $v_0 = 8$.*

Proof. If $8 \mid v$ or $12 \mid v$, then it is done by lemmas 5.4.2 and 5.4.3. For all $v = 4k$ with $k \geq 2$ such that $8 \nmid v$ and $12 \nmid v$, there exists $\alpha, \beta \in \mathbb{N}$ such that $8\alpha + 12\beta = v$. Partition X

into $X' \cup X''$ such that $|X'| = 8\alpha$ and $|X''| = 12\beta$. Let aA denote the 2-equipartition of X such that the 2-equipartition on X' is a in lemma 5.4.2 and the 2-equipartition on X'' is A in lemma 5.4.3. We define other 2-equipartitions of X in the similar manner.

Consider the following fifteen 2-equiparitions of X: aA, bB, cC, dD, eE, fF, fG, gH, dI, bJ, eK, dL, gM, aN, cO, which are some of the vertices of H. By lemmas 5.4.2 and 5.4.3,

$$\{aA, bB, cC\}, \{aA, dD, eE\}, \{bB, dD, fF\}, \{cC, eE, fF\}, \{aA, fG, gH\},$$
$$\{bB, fG, dI\}, \{dD, fG, bJ\}, \{cC, gH, dI\}, \{eE, gH, bJ\}, \{fF, dI, bJ\},$$
$$\{aA, eK, dL\}, \{bB, eK, gM\}, \{dD, eK, aN\}, \{fG, eK, cO\}, \{cC, dL, gM\},$$
$$\{eE, dL, aN\}, \{gH, dL, cO\}, \{fF, gM, aN\}, \{dI, gM, cO\}, \{bJ, aN, cO\}$$

are edges in H. This subgraph of H is isomorphic to the one in lemma 5.4.3, so it is not 2-vertex-colorable. $\square$

Chapter 6

Problems in design theory

6.1 Hartman's conjecture on large sets of designs of size 2

A t-(v,k,λ) design is a collection $\mathcal{B}$ of k-subsets (often referred to as blocks) of a v-set X, such that every t-subset of X is contained in exactly λ blocks in $\mathcal{B}$. A large set of t-(v,k,λ) designs of size N, denoted by $\mathrm{LS}[N](t,k,v)$, is a partition of the set of all k-subsets of X into N disjoint t-(v,k,λ) designs, where $N = \binom{v-t}{k-t}/\lambda$. A set of trivial necessary conditions for the existence of a $\mathrm{LS}[N](t,k,v)$ is that $N \mid \binom{v-i}{k-i}$ for $i = 0,1,\ldots,t$. Hartman [13] conjectured that the trivial necessary conditions are sufficient for the existence of large sets of size $N = 2$.

When $N = 2$, the existence of a large set of t designs is equivalent to the existence of a vector of all 1's and -1's in $\mathrm{null}_{\mathbb{Q}}(W_{tk}^{v})$. Hartman's conjecture is proved in [1] to be true for $t = 2$ as well as for some other cases (see [15] for more details). Here, we will give an explicit construction for $t = 2$ and $k = 3$, which is independent of the results from the literature.

The set of trivial necessary conditions are $\binom{v-0}{3-0}$, $\binom{v-1}{3-1}$ and $\binom{v-2}{3-2}$ being even, which is equivalent to $v \equiv 2 \pmod 4$, so $v = 2(2w+1)$ for some $w \in \mathbb{N}$. Let the v vertices be $\{a_1,\ldots,a_{2w+1},b_1,\ldots,b_{2w+1}\}$. Let

$$\begin{bmatrix} a_{\sigma_1} & b_{\sigma_1} \\ a_{\sigma_2} & b_{\sigma_2} \\ a_{\sigma_3} & b_{\sigma_3} \end{bmatrix}$$

denote the 3-pod $\mathbb{1}_{\{a_{\sigma_1},a_{\sigma_2},a_{\sigma_3}\}} + \mathbb{1}_{\{a_{\sigma_1},b_{\sigma_2},b_{\sigma_3}\}} + \mathbb{1}_{\{b_{\sigma_1},a_{\sigma_2},b_{\sigma_3}\}} + \mathbb{1}_{\{b_{\sigma_1},b_{\sigma_2},a_{\sigma_3}\}} - \big(\mathbb{1}_{\{a_{\sigma_1},a_{\sigma_2},b_{\sigma_3}\}} + \mathbb{1}_{\{a_{\sigma_1},b_{\sigma_2},a_{\sigma_3}\}} + \mathbb{1}_{\{a_{\sigma_1},a_{\sigma_2},b_{\sigma_3}\}} + \mathbb{1}_{\{b_{\sigma_1},b_{\sigma_2},b_{\sigma_3}\}}\big)$ in the $\mathrm{null}_{\mathbb{Q}}(W^v_{23})$.

If $v = 6$, then

$$\begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{bmatrix} + \begin{bmatrix} a_1 & b_2 \\ a_2 & b_3 \\ a_3 & b_1 \end{bmatrix} - \begin{bmatrix} a_1 & b_3 \\ a_2 & b_1 \\ a_3 & b_2 \end{bmatrix}$$

is a vector of all ± 1's. In general, if $v = 2(2w+1)$, consider the vector

$$\mathbf{f} = \sum_{\substack{\{\sigma_1,\sigma_2,\sigma_3\}\subseteq[2w+1] \\ \sigma_1<\sigma_2<\sigma_3}} \left(\begin{bmatrix} a_{\sigma_1} & b_{\sigma_1} \\ a_{\sigma_2} & b_{\sigma_2} \\ a_{\sigma_3} & b_{\sigma_3} \end{bmatrix} + \begin{bmatrix} a_{\sigma_1} & b_{\sigma_2} \\ a_{\sigma_2} & b_{\sigma_3} \\ a_{\sigma_3} & b_{\sigma_1} \end{bmatrix} - \begin{bmatrix} a_{\sigma_1} & b_{\sigma_3} \\ a_{\sigma_2} & b_{\sigma_1} \\ a_{\sigma_3} & b_{\sigma_2} \end{bmatrix} \right) \times (-1)^{\sigma_1+\sigma_2+\sigma_3}. \tag{6.1}$$

Here, $[2w+1] = \{1, 2, \ldots, 2w+1\}$. We are going to show that $\mathbf{f}$ is a vector of $\pm 1'$s.

For all $\sigma_1 < \sigma_2 < \sigma_3$, each of $\mathbb{1}_{\{a_{\sigma_1},a_{\sigma_2},b_{\sigma_3}\}}$, $\mathbb{1}_{\{a_{\sigma_1},b_{\sigma_2},a_{\sigma_3}\}}$, $\mathbb{1}_{\{b_{\sigma_1},a_{\sigma_2},a_{\sigma_3}\}}$, $\mathbb{1}_{\{a_{\sigma_1},b_{\sigma_2},b_{\sigma_3}\}}$, $\mathbb{1}_{\{b_{\sigma_1},a_{\sigma_2},b_{\sigma_3}\}}$, $\mathbb{1}_{\{b_{\sigma_1},b_{\sigma_2},a_{\sigma_3}\}}$ only occurs once in the summation, so $\mathbf{f}$ has ± 1's in those entries. As for $\mathbb{1}_{\{a_{\sigma_1},a_{\sigma_2},a_{\sigma_3}\}}$ and $\mathbb{1}_{\{b_{\sigma_1},b_{\sigma_2},b_{\sigma_3}\}}$, the coefficients are $\pm(1+1-1)(-1)^{\sigma_1+\sigma_2+\sigma_3} = \pm 1$.

It remains to determine the coefficients of $\mathbb{1}_{\{a_{\sigma_i},a_{\sigma_j},b_{\sigma_i}\}}$ and $\mathbb{1}_{\{a_{\sigma_i},b_{\sigma_i},b_{\sigma_j}\}}$, where $\{i,j,k\} = \{1,2,3\}$. We will calculate the coefficient of $\mathbb{1}_{\{a_{\sigma_i},a_{\sigma_j},b_{\sigma_i}\}}$ for the case where $\sigma_i < \sigma_j$, and the computation for the other terms is similar.

We see that $\mathbb{1}_{\{a_{\sigma_i},a_{\sigma_j},b_{\sigma_i}\}}$ occurs $2w-1$ times in the summation in (6.1), falling into one of the following three categories.

(1) $\begin{bmatrix} a_{\sigma_k} & b_{\sigma_i} \\ a_{\sigma_i} & b_{\sigma_j} \\ a_{\sigma_j} & b_{\sigma_k} \end{bmatrix} \times 1 \times (-1)^{\sigma_i+\sigma_j+\sigma_k}$ for $1 \le \sigma_k < \sigma_i$,

(2) $\begin{bmatrix} a_{\sigma_i} & b_{\sigma_j} \\ a_{\sigma_k} & b_{\sigma_i} \\ a_{\sigma_j} & b_{\sigma_k} \end{bmatrix} \times (-1) \times (-1)^{\sigma_i+\sigma_j+\sigma_k}$ for $\sigma_i < \sigma_k < \sigma_j$,

$$(3)\ \begin{bmatrix} a_{\sigma_i} & b_{\sigma_j} \\ a_{\sigma_j} & b_{\sigma_k} \\ a_{\sigma_k} & b_{\sigma_i} \end{bmatrix} \times 1 \times (-1)^{\sigma_i+\sigma_j+\sigma_k} \text{ for } \sigma_j < \sigma_k \leq 2w+1.$$

If σ_i and σ_j are odd, the coefficient from (1) is 0, the coefficient from (2) is 1 and the coefficient from (3) is 0, so the total is 1; if σ_i is odd and σ_j is even, the coefficient from (1) is 0, the coefficient from (2) is 0, and the coefficient from (3) is -1, so the total is -1; if σ_i is even and σ_j is odd, the coefficient from (1) is -1, the coefficient from (2) is 0, and the coefficient from (3) is 0, so the total is -1; if σ_i and σ_j are even, the coefficient from (1) is 1, the coefficient from (2) is -1, and the coefficient from (3) is 1, so the total is 1. In any case, the coefficient of $\mathbb{1}_{\{a_{\sigma_i}, a_{\sigma_j}, b_{\sigma_i}\}}$ for $\sigma_i < \sigma_j$ is always ± 1.

6.2 Signed bipartite graph designs

Let G be a nonempty proper subgraph of the complete bipartite graph $K_{n,n}$ with $2n$ vertices, some of which are possibly isolated. Let $\mathcal{G}$ be the collection of subgraphs G' of $K_{n,n}$ which are isomorphic to G. We say that there exists a (n, G, λ)-*signed bipartite graph design* if there exists $z : \mathcal{G} \to \mathbb{Z}$ such that for each edge $e \in E(K_{n,n})$,

$$\sum_{\substack{G' \in \mathcal{G}: \\ E(G') \ni e}} z(G') = \lambda.$$

If $\lambda = 1$ and $z : \mathcal{G} \to \{0, 1\}$, then such a design becomes a graph decomposition, which is studied by Wilson [25] and many others. Ushio [22] gives the necessary and sufficient conditions for a complete bipartite graph to be decomposed into smaller complete bipartite graphs. Here, the necessary and sufficient conditions for the existence of a (n, G, λ)-signed bipartite graph design are given.

Theorem 6.2.1. *Let G be a nonempty proper spanning subgraph of the complete bipartite graph $K_{n,n}$. If G has only one connected component of size greater than 1, then there exists a (n, G, λ)-signed bipartite graph design if and only if all the following three conditions hold:*
(i) $h \mid \lambda n$,

(ii) $\tilde{g}c \mid \lambda n(\ell n + 2\ell' + \ell'')$,

(iii) $\frac{eg}{h} \mid \lambda n(n\text{GCD}\{\frac{a_1+b_1}{h}, \frac{g}{\tilde{g}}\} + \alpha\frac{2e}{h} + \sigma\beta\frac{eg}{h\tilde{g}})$,

where g, $\tilde{g}$, h, *are defined in section* 3.1, *and* α, β, σ, ℓ, ℓ' *and* ℓ'' *are defined in theorem* 3.1.2.

Proof. Note that there exists a (n, G, λ)-signed bipartite graph design if and only if there exists an integer vector solution $\mathbf{z}$ to $N(G)\mathbf{z} = \lambda\mathbf{1}^\top$. If G is primitive, then by theorem 3.2.2, $\widetilde{E}NF = D$ for some unimodular matrix F, where D contains the list of diagonal factors given in theorem 3.2.2. So $\widetilde{E}^{-1}DF^{-1}\mathbf{z} = \lambda\mathbf{1}^\top$, or $D\mathbf{z}' = \lambda\widetilde{E}\mathbf{1}^\top$ for some integer vector solution $\mathbf{z}'$, which exists if and only if $d_i \mid \lambda E_i U\mathbf{1}^\top$ for $i = 1, 2, \ldots, 2n-1$, where E_i is the i-th row of E given in theorem 3.1.2.

By definition, $U\mathbf{1}^\top = (n^2, n, \ldots, n)^\top$, so $\lambda E_i U\mathbf{1}^\top = 0$ which is divisible by d_i for $i \geq 4$. When $i = 3$, 2 and 1, they correspond to the conditions (i), (ii) and (iii) respectively.

If G is nonprimitive, then $G = K_{s,n} \dot{\cup} \{n-s \text{ isolated vertices}\}$. The conditions (i) to (iii) combine to be $\frac{s}{h} \mid \lambda$, which is equivalent to $s \mid \lambda n$ since $h = \text{GCD}\{n, s\}$. Let E be the front given in the proof of theorem 5.3.2(ii), and let D be the corresponding diagonal form, given in theorem 3.3.2. Again, there exists a (n, G, λ)-signed bipartite graph design if and only if there exists an integer vector solution to $D\mathbf{z}' = \lambda E\mathbf{1}$. Note that $\lambda E\mathbf{1}^\top$ is a vector with λn in the first and the n-th entries, λ's in the in-th entries, $2 \leq i \leq n$, and 0's elsewhere. As a result, $D\mathbf{z}' = \lambda E\mathbf{1}^\top$ has an integer vector solution if and only if $s \mid \lambda n$, since other congruent conditions are trivial. $\square$

Corollary 6.2.2. *If* $G = K_{s,t}$, $1 \leq s \leq t \leq n$, *then there exists a* (n, G, λ)*-signed bipartite graph design if and only if* $st \mid \lambda n^2$.

Chapter 7

A problem in matroid theory by Dominic Welsh

7.1 A brief introduction to matroids

A *matroid* $\mathcal{M} = (X, \mathcal{I})$ is a combinatorial structure defined on a finite ground set X of n elements, together with a family $\mathcal{I}$ of subsets of X called *independent sets*, satisfying the following three properties:

1. $\emptyset \in \mathcal{I}$, or $\mathcal{I}$ is nonempty.

2. If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$. This is sometimes known as *hereditary property.*

3. If $I, J \in \mathcal{I}$ and $|J| < |I|$, then there exists $x \in I \backslash J$ such that $J \cup \{x\} \in \mathcal{I}$. This is known as *augmentation property* or *exchange property.*

A maximal independent set is called a *basis* of the matroid. A direct consequence of the augmentation property is that all bases have the same cardinality, and this cardinality is defined as the *rank* of $\mathcal{M}$.

One of the most important examples of matroids is a *linear matroid.* A linear matroid is defined from a matrix A over a field $\mathbb{F}$, where X is the set of columns of A, and an independent set $I \in \mathcal{I}$ is a collection of columns which is linearly independent over $\mathbb{F}$. For a linear matroid, the rank is exactly the rank of the matrix A. Since the elements of a linear matroid are the columns of a matrix, it is also called a *column matroid.*

Given a triple of integers (n, r, b), $0 < r \leq n$ and $1 \leq b \leq \binom{n}{r}$, Welsh [24] asked if there exists a matroid of n elements, rank r, and has exactly b bases. It was conjectured that a matroid exists for every such triple, until Mayhew and Royle [17] found the lone counterexample to date, namely $(n, r, b) = (6, 3, 11)$. However, they suggested that this is the only triple where the conjecture fails.

In this chapter, we will show that if $1 \leq b \leq \binom{r+2}{r}$, there always exists a matroid satisfying the given parameters (n, r, b). We proceed by constructing the matrix, or the linear matroid, explicitly for all triples (n, r, b) such that $n \leq r + 2$. Then if $1 \leq b \leq \binom{r+2}{r}$ and $n > r + 2$, we simply put zeros in the last $n - (r + 2)$ columns.

7.2 The case $1 \leq b \leq \binom{r+2}{r}$

Let A be an $r \times n$ matrix over $\mathbb{Q}$ of rank r, and let b be the number of invertible $r \times r$ submatrices of A. Note that b is an invariant if we perform row operations or permute the columns of A, so we can always assume that $A = (I_r|M)$, where M is an $r \times (n - r)$ matrix.

Proposition 7.2.1. *The number of invertible square submatrices of M is $b - 1$, and the number of invertible $(n - r) \times (n - r)$ submatrices of $(I_{n-r}|M^\top)$ is b.*

Proof. Let $\mathcal{S}$ be the set of all invertible $r \times r$ submatrices of A except the identity matrix in the first r columns, and let $\mathcal{T}$ be the set of all invertible square submatrices of M.

Let S be a matrix in $\mathcal{S}$ with columns $i_1, i_2, \ldots, i_r$, where $i_1, \ldots, i_j \leq r$ and $i_{j+1}, \ldots, i_r > r$. Then there is a bijection between $\mathcal{S}$ and $\mathcal{T}$ which sends S to the square submatrix of M with rows $\{1, 2, \ldots, r\} \backslash \{i_1, i_2, \ldots, i_j\}$ and columns $i_{j+1}, i_{j+2}, \ldots, i_r$. Hence, the number of invertible square submatrices of M is $b - 1$.

It is obvious then that the number of invertible square submatrices of $M^\top$ is $b-1$, which implies that the number of invertible $(n - r) \times (n - r)$ submatrices of $(I_{n-r}|M^\top)$ is b. $\square$

In view of this proposition, it suffices to consider only $n \leq 2r$ when we study this Welsh's problem for matrices, since if $r < n - r$, then we can construct matrices of dimension

$(n-r)\times n$ instead. In theorem 7.2.3, we prove the conjecture for $n \le r+2$, so what remains unknown is when $r+3 \le n \le 2r$.

The following lemma in number theory will help us to show the existence of matrices satisfying the parameters (n, r, b).

Lemma 7.2.2. *Let $s \ge 5$ be a positive integer, and let k be a nonnegative integer such that $k \le \frac{s^2-5s}{4}$. Then there exist nonnegative integers $a_1, a_2, \dots, a_s$ such that $a_1 + a_2 + \cdots + a_s = s$ and $a_1^2 + a_2^2 + \cdots + a_s^2 = s + 2k$.*

Proof. For $5 \le s \le 32$, we verified the lemma by Mathematica; for $s \ge 33$, we will use strong induction on s.

Suppose the statement is true for all integers u such that $5 \le u < s$ for some $s \ge 33$, i.e., for all nonnegative integers $k' \le \frac{u^2-5u}{4}$, there exist nonnegative integers $a_1, \dots, a_u$ such that $a_1 + \cdots + a_u = u$ and $a_1^2 + \cdots + a_u^2 = u + 2k'$.

Let t and k be integers such that $0 < t \le s-5$ and $0 \le k - \frac{t^2-t}{2} \le \frac{(s-t)^2-5(s-t)}{4}$. Then $u := s-t$ falls in the range $5 \le u < s$, and $k' := k - \frac{t^2-t}{2} \le \frac{u^2-5u}{4}$. By the induction hypothesis, there are nonnegative integers $a_1, \dots, a_{s-t}$ such that $a_1 + \cdots + a_{s-t} = s-t$ and $a_1^2 + \cdots + a_{s-t}^2 = s - t + 2\bigl(k - \frac{t^2-t}{2}\bigr) = s + 2k - t^2$. If we set $a_{s-t+1} = t$ and $a_{s-t+2} = \cdots = a_s = 0$, then $a_1 + \cdots + a_s = s$ and $a_1^2 + \cdots + a_s^2 = s + 2k$, implying that the statement holds true for k satisfying $0 \le k - \frac{t^2-t}{2} \le \frac{(s-t)^2-5(s-t)}{4}$, or equivalently, $\frac{t^2-t}{2} \le k \le \frac{3t^2-2st+3t+s^2-5s}{4}$.

It now suffices to show that the union of the intervals $I(t) := \left[\frac{t^2-t}{2}, \frac{3t^2-2st+3t+s^2-5s}{4}\right]$ for $0 < t \le s-5$ covers $\left[0, \frac{s^2-5s}{4}\right]$ when $s \ge 33$. Let $\alpha(t) = \frac{t^2-t}{2}$ and $\beta(t) = \frac{3t^2-2st+3t+s^2-5s}{4}$.

Claim 1. $\frac{s^2-5s}{4} \le \beta(t)$ if and only if $t \ge \frac{2}{3}s - 1$, which is attainable for some t in the range $0 < t \le s-5$ if $s \ge 12$.

Proof of claim 1. This inequality holds if and only if $3t^2 - 2st + 3t \ge 0$, which is equivalent to $t \ge \frac{2}{3}s - 1$ since t is positive. We finish by noticing that when $s \ge 12$, $s - 5 \ge \frac{2}{3}s - 1$. □

Claim 2. $\alpha(t-1) \le \alpha(t) \le \beta(t)$.

Proof of claim 2. The first inequality holds since $\alpha(t)$ is an increasing function for $t \ge 1$, since $\alpha'(t) = \frac{2t-1}{2} > 0$ when $t \geq 1$, considering α as a continuous function on $\mathbb{R}$. The second inequality holds if and only if $5(s-t) \leq (s-t)^2$, which is always true since $t \leq s-5$. $\square$

Claim 3. $\alpha(t) \leq \beta(t-1)$ if and only if $t \leq \frac{2s+1-\sqrt{16s+1}}{2}$.

Proof of claim 3. This inequality holds if and only if $t^2 - (2s+1)t + s^2 - 3s \geq 0$, which occurs if and only if $t \leq \frac{2s+1-\sqrt{16s+1}}{2}$ or $t \geq \frac{2s+1+\sqrt{16s+1}}{2}$. However, $t \geq \frac{2s+1+\sqrt{16s+1}}{2}$ is rejected since $t < s$. $\square$

By claims 2 and 3, if $t \leq \frac{2s+1-\sqrt{16s+1}}{2}$, then $I(1) \cup \cdots \cup I(t-1) \cup I(t)$ forms one closed interval. If $\left\lceil \frac{2}{3}s - 1 \right\rceil \leq \frac{2s+1-\sqrt{16s+1}}{2}$, then claim 1 implies that $\left[0, \frac{s^2-5s}{4}\right] \subseteq \bigcup_{t=1}^{\left\lceil \frac{2}{3}s-1 \right\rceil} I(t)$.

To obtain $\left\lceil \frac{2}{3}s - 1 \right\rceil \leq \frac{2s+1-\sqrt{16s+1}}{2}$, we look for integers s satisfying $\frac{2}{3}s \leq \frac{2s+1-\sqrt{16s+1}}{2}$, or equivalently, $3\sqrt{16s+1} \leq 2s+3$. This inequality holds if $33s \leq s^2$, or $s \geq 33$. $\square$

Theorem 7.2.3. *If $n \leq r+2$, then for all b such that $1 \leq b \leq \binom{n}{r}$, there exists a matrix $A = (I_r|M)$ over $\mathbb{Q}$ such that the number of invertible $r \times r$ submatrices of A is exactly b.*

Proof. It is trivial for $n = r$. If $n = r+1$, then $A = (I_r|M)$ where M is a column vector with the first $b-1$ entries 1's and the rest 0's.

If $n = r+2$, let the first column of M have the first s entries 1's, the second column have the first s entries nonzero, and the rest be all 0's. Furthermore, assume that there are a_i i's in the second column, $1 \leq i \leq s$, where $a_1 + a_2 + \cdots + a_s = s$. Then the number of invertible $r \times r$ submatrices of A is

$$\begin{aligned} 1 + 2s + \textstyle\sum_{i<j} a_i a_j &= 1 + 2s + \tfrac{1}{2}(\textstyle\sum_i a_i)^2 - \tfrac{1}{2}(\textstyle\sum_i a_i^2) \\ &= 1 + 2s + \tfrac{1}{2}s^2 - \tfrac{1}{2}(\textstyle\sum_i a_i^2), \end{aligned}$$

and we would like to set it to be b, which gives $s + 2(\binom{s+2}{2} - b) = \sum_i a_i^2$.

By lemma 7.2.2, if $0 \leq \binom{s+2}{2} - b \leq \frac{s^2-5s}{4}$, or equivalently $\frac{s^2+11s+4}{4} \leq b \leq \frac{s^2+3s+2}{2}$, there is a solution for a_i's. It is easy to check that the intervals $[\frac{s^2+11s+4}{4}, \frac{s^2+3s+2}{2}]$ cover all integers $b \geq 39$, and the only missing integers are in $[1,20] \cup [22,26] \cup [29,32] \cup [37,38]$. Here, we finish the proof by constructing M explicitly for each of these b's.

In the following table, **0** represents a column vector of all 0's (possibly of length 0), which fills up the column so that M has r rows.

$b =$	1	2	3	4	5	6	7	8
$M =$	$\begin{array}{\|c\|c\|}\hline \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 0 \\ 0 & 1 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$

$b =$	9	10	11	12	13	14	15	16
$M =$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$	$\begin{array}{\|c\|c\|}\hline 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ \mathbf{0} & \mathbf{0} \\ \hline\end{array}$

$b =$	17	18	19	20	22	23	24	25
$M =$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 2 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$

$b =$	26	29	30	31	32	37	38
$M =$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 2 \\ 1 & 3 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$	$\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ \mathbf{0} & \mathbf{0} \end{array}$

$\square$

Bibliography

[1] S. Ajoodani-Namini, All block designs with $b = \binom{v}{k}/2$ exist, *Disc. Math.* **179** (1998), 27–35.

[2] M. H. Ahmadi, N. Akhlaghinia, G. B. Khosrovshahi, Ch. Maysoori, On the inclusion matrix $W_{23}(v)$, *preprint.*

[3] N. Alon and Y. Caro, On three zero-sum Ramsey-type problems, *J. Graph Thy.* **17** (1993), 177–192.

[4] A. Bialostocki and P. Dierker, Zero-sum Ramsey theorems, *Congressus Numerantium* **70** (1990), 119–130.

[5] A. E. Brouwer and C. A. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, *J. Alg. Combinatorics* **1** (1992), 329–346.

[6] Y. Caro, A complete characterization of the zero-sum (mod 2) Ramsey numbers, *J. Combinatorial Thy. Ser. A* **68** (1994), 205–211.

[7] Y. Caro and R. Yuster, The characterization of zero-sum (mod 2) bipartite Ramsey numbers, *J. Graph Thy.* **29** (1998), 151–166.

[8] D. B. Chandler and Q. Xiang, The invariant factors of some cyclic difference sets, *J. Combinatorial Thy. Ser. A* **101** (2003) 131–146.

[9] E. S. T. Fan and T. W. H. Wong, Welsh's problem on the number of bases of matroids, *in preparation.*

[10] P. Frankl and R. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

[11] R. L. Graham, S.-Y. R. Li, and W.-C. W. Li, On the structure of t-designs, *SIAM J. Alg. Disc. Math.* **1** (1980), 8–14.

[12] J. E. Graver and W. B. Jurkat, The module structure of integral designs, *J. Combinatorial Thy.* **15** (1973), 75–90.

[13] A. Hartman, Halving the complete design, *Ann. Disc. Math.* **34** (1987), 207–224.

[14] G. B. Khosrovshahi and Ch. Maysoori, On the bases for trades, *Lin. Alg. and its Appl.* **226–228** (1995), 731–748.

[15] G. B. Khosrovshahi, B. Tayfeh-Rezaie, Large sets of t-designs through partitionable sets, a Review, *Disc. Math.* **306** (2006), 2993–3004.

[16] C. W. H. Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly* **98** (1991), 305–318.

[17] D. Mayhew and G. F. Royle, Matroids with nine elements, *J. Combinatorial Thy. Ser. B* **98** (2008), 415–431.

[18] M. Newman, The Smith normal form, Proceedings of the Fifth Conference of the International Linear Algebra Society (Atlanta, GA, 1995), *Lin. Alg. and its Appl.* **254** (1997), 367–381.

[19] D. K. Ray-Chaudhuri, N. Singhi, Studying designs via multisets, *Des. Codes Cryptogr.* **65** (2012), 365–381.

[20] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, New York, 1986.

[21] V. Sivaraman, On a conjecture of Welsh, *preprint.*

[22] K. Ushio, Bipartite decomposition of complete multipartite graphs, *Hiroshima Math. J.* **11** (1981), 321–345.

[23] B. L. van der Waerden, *Algebra, Vol.* 2, Springer, 2003.

[24] D. Welsh, Combinatorial problems in matroid theory, *Combinatorial Math. and its Appl. (Proc. Conf. Oxford* 1969*)*, Academic Press, London, 1971.

[25] R. M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, *Proc. 5th Brit. Combinatorial Conf.* (1975), 647–659.

[26] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combinatorics* **11** (1990), 609–615.

[27] R. M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices, *Des. Codes Cryptogr.* **17** (1999), 289–297.

[28] R. M. Wilson, On set systems with restricted intersections modulo p and p-ary t-designs, *Disc. Math.* **309** (2009), 606–612.

[29] R. M. Wilson, Some applications of incidence matrices of t-subsets and hypergraphs, Proceedings of the Third Shanghai Conference on Combinatorics, *Disc. Math.*, to appear.

[30] R. M. Wilson and T. W. H. Wong, Diagonal forms of incidence matrices associated with t-uniform hypergraphs, *accepted by Europ. J. Combinatorics.*

[31] T. W. H. Wong, Diagonal forms and zero-sum (mod 2) bipartite Ramsey numbers, *submitted to J. Combinatorial Thy. Ser. A.*

[32] T. W. H. Wong, Inclusion matrices of multisets, *in preparation.*