이학석사 학위논문

Matroid and Rainbow Matching

(매트로이드와 무지개 부합)

2019년 2월

서울대학교 대학원

수리과학부

정우석

Matroid and Rainbow Matching

지도교수 국 웅

이 논문을 이학석사 학위논문으로 제출함

2018년 4 월

서울대학교 대학원

수리과학부

정 우 석

정우석의 석사 학위논문을 인준함

2018년 6 월

위 원 장 김서령 (인)

부위원장 국웅 (인)

위 원 이승진 (인)

Abstract

A rainbow matching of an edge-colored graph is a matching which edges have all distinct colors. It is natural to ask about the maximum size of rainbow matching of a given edge-colored graph. This paper gives a survey on the problem, especially on the complete bipartite graphs $K_{n,n}$ which is equivalent to the Ryser-Brualdi-Stein conjecture on the Latin squares. An introduction to matroid theory and generalized versions of Ryser-Brualdi-Stein conjecture on the matroids are surveyed. The Ryser conjecture on the Cayley tables of groups is called the Hall-Paige conjecture which was solved by Wilcox, Bray, and Evan in 2009. We give applications of the theorem. One of the application gives a lower bound for the maximum size of a rainbow matching when the bipartite graph is induced by a group. Also, we showed that there is an $n-1$ partial transversal for the Cayley table of a dihedral group, which means that the Brualdi-Stein conjecture on the dihedral groups is true.

Keywords : Rainbow matching, Complete bipartite graph, Latin square, Group, Matroid
Student number : 2014-22351

Contents

1 Introduction

A *matching* of a graph $G = (V, E)$ is a set of pairwise non-adjacent edges. An *edge coloring of a graph* $G = (V, E)$ is a partition of the edge set E with pairwise disjoint matchings. A *rainbow matching* of an edge-colored graph G is a matching with all the edges have different colors.

In this paper, we mainly focus on when the graph is a complete bipartite graph. A complete bipartite graph $K_{n,n}$ can be decomposed into pairwise disjoint n-matchings of size n. Let $\{F_1, F_2, ..., F_n\}$ be the decomposition of the edge set of $K_{n,n}$ (an edge-colored $K_{n,n}$). By taking at most one edge from each F_i appropriately, one can construct a rainbow matching of given decomposition.

It is natural to ask what the maximum size of a rainbow matching is. There is a conjecture asserts that there exists a full rainbow matching of size n if n is odd, and there is a rainbow matching of size $n - 1$ if n is even. The exception when n is even is due to the counterexamples given by Euler (Section2).

The Latin square is an interesting mathematical object which has a long history. Though Latin square is interesting in its own right, our main focus is on the relationship between complete bipartite graphs. Section 2 introduces the definition of Latin square and its transversal and gives a conjecture (Ryser-Brualdi-Stein Conjecture) which is equivalent to the conjecture of above paragraph. In addition, Section 2 contains theorems on lower bounds for the maximum size of rainbow matchings of edge-colored $K_{n,n}$ graphs. [14, 29]

As the Cayley table of a group is a Latin square, one can restrict the problem to the Cayley table of a group. Section 3 deals with Hall's results, which solves Ryser-Brualdi-Stein conjecture on the finite abelian group. Furthermore, there is a theorem which gives an equivalent condition for the existence of a full transversal of a group. The theorem was conjectured to be true by Hall and Paige in 1955, and solved by Wilcox, Bray, and Evans in 2009. As an application of their theorem, we give a sufficient condition for the Cayley tables of groups have a transversal. Another application of the theorem gives a lower bound in the case of groups, which says that if a group G has order $2^n k$ and k is odd, then it has a partial transversal at least of length $(2^n - 1)k$.

In Section 4, we show that the Ryser conjecture on the Dihedral group is true. Section 5 shows an analog problem on complete graphs, which was solved by Woolbright and Fu.

Section 6 covers an introduction to the matroid theory. Matroid theory can extend some graph problems, and have other interesting features. Generalized conjectures of Brualdi-Stein conjecture, stated in [16] and [2], are surveyed in Section 7.

2 Latin Squares and Transversals

2.1 Ryser-Brualdi-Stein Conjecture

Bipartite graphs are closely related to the Latin squares.

Definition 1. *A Latin square of order n is a $n \times n$ matrix filled with n different symbols each occurring exactly once in each row and column. A partial transversal of length m of a Latin square is a set of entries from different rows and different columns and different symbols with size $m \leq n$. In particular, if the length of a partial transversal m is equal to n, then we call it a (full) transversal.*

Example 1. *A matrix* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}$ *is a latin square and the diagonal is a transversal.*

The question on the bipartite graph can be transformed into an equivalent question on the Latin square. Label the left vertices of $K_{n,n}$ from 1 to n and the right vertices from 1 to n. Given an edge-colored graph of $K_{n,n}$ with n-matchings of size n, index left vertices as columns and right vertices as symbols and each matching as rows, then we get a Latin square. This shows a one-to-one correspondence between the set of edge-colored $K_{n,n}$ with n color(with labelled vertices) and the set of Latin square of order n. In the correspondence, a rainbow matching of size m corresponds to a partial transversal of length m.

Cayley table (binary operation table) of any finite group is a typical example of a Latin square. In fact, G is a finite quasigroup (satisfy all group axioms except for the associativity axiom) if and only if the binary operation table is a Latin square. So the group can be thought of as a Latin square with the 'associativity condition' is added.

Not every Latin square has a full transversal.

Theorem 2.1 (Euler)**.** *A Cayley table of a cyclic group of even order has no transversal.*

Proof. Assume $G = (\{1, 2, .., 2n\}, +)$. Suppose there is a full transversal $\{a_1, a_2, ..., a_{2n}\}$ of the Cayley table. Then the sum of all a_i must be $1 + 2 + ... + 2n = (1 + 2n)(2n)/2 = (1 + 2n)n \equiv n(\bmod 2n)$, since they are all different elements.

However, each a_i is sum of two elements of G, thus the sum should be $(1+2+...+2n)+(1 + 2 + ... + 2n) \equiv 2n \equiv 0(\bmod 2n)$.

Since n is not equal to 0 in G, so there is no transversal. $\square$

No counterexample has been found when a Latin square has odd order. The following conjectures are posed by Ryser, Brualdi and Stein.

Conjecture 2.2 (Ryser). *Every odd order latin square has a full transversal.*

Conjecture 2.3 (Brualdi-Stein). *Every (even order) latin square has a partial transversal of length $n-1$.*

In the language of complete bipartite graph and rainbow matching,

Conjecture 2.4 (Ryser). *If n is odd, $K_{n,n}$ admits a full rainbow matching.*

Conjecture 2.5 (Brualdi-Stein). *$K_{n,n}$ always admits a partial rainbow matching of size $n-1$.*

The Ryser conjecture on cyclic groups is easily verified since the diagonal of the Cayley table of a cyclic group of odd order is a full transversal. Further researches on Cayley tables of groups are surveyed in Section 3.

2.2 Lower bounds for the maximum size of rainbow matchings

The conjectures are not yet solved. As progress to solve the conjectures, there are theorems on lower bound for the maximum size of a transversal. For a given Latin square L, let $t(L)$ be the maximal size of a partial transversal on L. Define $T(n)$ be the minimum number of $t(L)$ among the all Latin squares L of order n. Ryser-Brualdi-Stein conjecture suggests that,

$$T(n) = \begin{cases} n & \text{if } n \textit{ is odd} \\ n-1 & \text{if } n \textit{ is even} \end{cases}.$$

Though it is not yet solved, there are theorems on lower bounds on $T(n)$. Koksma proved that for $n \geq 3$, $T(n) \geq \lceil (2n+1)/3 \rceil$ in [15], which was improved by Drake to $T(n) \geq \lceil 3n/4 \rceil$ for $n > 7$ in [6]. De Veris-Wieringa improved that $T(n) \geq \lceil (4n-3)/5 \rceil$ for $n \geq 12$ in [5].

Instead of lower bounds of type $n - O(n)$, there are other types of bounds. Following theorem was proved by Woolbright and independently Brower-de Vries-Wieringa. The proof follows from the Woolbright's paper.

Theorem 2.6 (Woolbright [29] and Brouwer-de Vries-Wieringa [5], 1978). *A n-edge coloring on $K_{n,n}$ has a rainbow set of size bigger than $n - \sqrt{n}$. That is, $T(n) \geq \lceil n - \sqrt{n} \rceil$.*

Proof. Suppose an edge-coloring on $K_{n,n} = ((A,B),E)$ is given with color $c_1, c_2, ..., c_n$. Note that each vertex has c_i-colored edge for all i. Let R be a rainbow set with maximum size with size $|R| = t$ and $n - t := d$. We may assume that $c_1, .., c_d$ are not the colors of edges in R and $c_{d+1}, .., c_n$ are the colors in R.

Let $A_1(B_1)$ be the subset of $A(B)$ which is not adjacent with R. If any c_1-colored edges from a vertex in A_1 meets B_1, then we get a contradiction on the maximality of R, since we can replace R by one more edge rainbow set.

So all the c_1-colored edges from A_1 goes to the subset B_2 of $B \setminus B_1$ of size d. And B_2 correspond to the same size subset of A which are connected by R, say A_2'. Let $A_2 := A_1 \cup A_2'$. By the similar argument as above, c_2-colored edges from A_2 cannot meat B_1. So they meat $2d$-vertices in B, which means that the vertices in $B \setminus (B_2 \cup B_1)$ that meats the c_2-colored edges from A_2 has more than d. Take any such d vertices, say B_3. And define $A_3 := \{corresponding\ vertices\ of\ B_3\ in\ A\ connected\ by\ R\} \cup A_2$, which has size $3d$.

In the j-th step, c_j-colored edges from A_j cannot meat B_1, for $j \leq d$. (If not, R can be replaced by a more edged rainbow set, which contradicts the maximality.) Take any d vertices (meating c_j-colored edges from A_j) that is not in $B_1, ..., B_d$ and there are corresponding d vertices in A by R. A_{j+1} is defined by those d-vertices in A union A_j.

Therefore, the process can continue until the d-th step, then we get a set A_{d+1} set of size $d(d+1)$. Therefore,

$$n = |A| \geq |A_{d+1}| = d(d+1) \geq d^2 = (n-t)^2, \tag{1}$$

This implies $t \geq n - \sqrt{n}$. □

This gives a better bound on $T(n)$ than $n - O(n)$-types if n is sufficiently large. Further improvement was given by Hatami and Shor.

Theorem 2.7 (Hatami-Shor [14])**.** $T(n) \geq 5.53(\log^2 n)$.

3 Cayley tables of groups

The case when the Latin square is a Cayley table of a group, that is when the Latin square satisfies the associativity condition, has more progress on the conjectures. In 1952, Hall solved the whole Ryser-Brualdi-Stein conjecture when the Latin square is a Cayley table of an abelian group in [12]. In 1955, Hall and Paige gave a necessary condition for the existence of a full transversal of a Cayley table of a group and conjectured that it is also sufficient in [13]. The Hall-Paige conjecture were settled by Wilcox, Bray, and Evans in 2009, [9, 28]. Thus the Ryser conjecture (the conjecture on the odd order group Cayley table) is proved to be true when the Latin square is induced by a group.

3.1 Complete mapping

In this section, we use the notion of complete mapping instead of transversal.

Definition 2. *Let G be a group (or a quasigroup). G admits a complete mapping, if there exist a bijection $\theta : G \to G$ such that $g \mapsto g\theta(g)$ is again a bijection of G onto itself.*

Transversals of Cayley table of a group are complete mappings of the group. Moreover, complete mapping extends the concept of transversal to the infinite (quasi)group. In 1950, P.T.Bateman proved that every infinite quasigroup admits a complete mapping [3].

Theorem 3.1 (Bateman [3], 1950)**.** *For any infinite quasigroup G there is a bijection of G onto itself ϕ such that $x \mapsto x\phi(x)$ is bijective. Moreover, for any $a, b \in G$, ϕ can be chosen to be that $\phi(a) = b$.*

3.2 Finite abelian group

Back to the finite group case, in 1952, Hall proved following theorem.

Theorem 3.2 (Hall [12], 1952)**.** *Let $(G, +)$ be an abelian group of order n. $G = \{a_1, a_2, ..., a_n\}$. Given a function ϕ such that $\phi(i) = b_i$, $i = 1, 2, ..., n$ with $b_i \in G$ and $\sum_{i=1}^{n} b_i = 0$, there exist a permutation*

$$\begin{pmatrix} a_1, & ..., & a_n \\ c_1, & ..., & c_n \end{pmatrix} \tag{2}$$

of G such that $b_i = c_i - a_i$, for $i = 1, 2, ..., n$, the b's being appropriately renumbered.

A proof can be found in [12].

As an application, one can prove that the Ryser-Brualdi-Stein conjecture on every finite abelian group is true.

Consider the Cayley table of G,

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \tag{3}$$

, where $a_{ij} = a_i + a_j$. Suppose

$$\begin{pmatrix} a_1 & a_2 & ... & a_n \\ c_1 & c_2 & ... & c_n \end{pmatrix} \tag{4}$$

is a permutation of elements of G, then c_r (below a_r in the permutation and in the r-th column of the Cayley table (3)) is in the kth row of the Cayley table (3) iff $c_r = a_{kr} = a_k + a_r$, which means $b_r = a_k$ (when r is renumbered as $b_r = c_r - a_r$). Therefore,

Corollary 3.3. *Let $G = \{a_1, a_2, ..., a_n\}$ be a finite abelian group. Then there exists a permutation agreeing with the ith row k_i times in the Cayley table $a_{ij} = a_i + a_j$ of G if and only if $k_1 + k_2 + ... + k_n = n$ and $k_1a_1 + k_2a_2 + ... + k_na_n = 0$.*

In the above Corollary take $k_i = 1$ for all i, then G has a transversal if and only if

$$a_1 + a_2 + ... + a_n = 0 \tag{5}$$

where 0 is the identity element of G.

1) When G has odd order, the sum of all elements should be the identity, since there is no element of order 2 so the identity is the only self-inverse element. Thus Ryser's conjecture is true for finite abelian groups.

2) It is fact that if there is more than one element of order 2 in a finite abelian group, then the sum of all elements should be equal to the identity. Therefore, if G has even order then the sum is identity unless G contains a unique element of order 2. In this case, the sum is the unique element. Therefore an equivalent condition for the existence of a complete mapping is obtained.

Corollary 3.4. *A finite abelian group admits complete mapping if and only if it has no unique element of order 2.*

Following corollary shows that a stronger theorem than Brualdi-Stein conjecture is true for finite abelian groups.

Corollary 3.5. *Let G be a finite abelian group. For any subset of G with $n-1$ elements, there exists a partial transversal containing the $n-1$ subset.*

Proof. Let $G = \{a_1, a_2, ..., a_n\}$. Consider the $n-1$ element subset which contains all elements of G except for a_i.

Then if $\sum_{j\neq i} a_j = a_i$ then we get a full transversal by Cor3.3, so we are done.
If not, say $\sum_{j\neq i} a_j = a_r$ with $r \neq i$. Take $k_r = 2,\ k_j = 1$ for all $j \neq i,\ r$ in Cor3.3, then there is a permutation of G with 2-element in row r of the Cayley table, which gives a partial transversal consists of given $n-1$-subset. $\square$

Therefore the Ryser-Brualdi-Stein conjecture on the finite abelian group is valid.

3.3 Hall-Paige conjecture

As an extension of Cor3.4 to all the finite groups, Hall and Paige posed a conjecture in 1955. They expected that a finite group admits complete mapping if and only if it has a trivial or noncyclic Sylow 2-subgroup. (Note that all Sylow 2-subgroups are isomorphic.) The Hall-Paige conjecture was proven to be true in 2009 by Wilcox, Bray, and Evans.

Lemma 3.6. *Let G be a finite group and T be a Sylow 2-subgroup of G and cyclic. Then G has unique maximal normal subgroup $O(G)$ of odd order and T is complement of $O(G)$. (i.e. $G = T \cdot O(G)$)*

Proof. Let $|G| = 2^n m$. The left multiplication group action of G on itself induces a homomorphism

$$\phi : G \to Sym(G) = S_{|G|} \tag{6}$$

sending element g of G to ρ_g, which is defined by $\rho_g(x) = gx$ for all $x \in G$.

Consider the composition of homomorphisms

$$G \xrightarrow{\phi} S_{|G|} \xrightarrow{\epsilon} \pm 1 \tag{7}$$

where ϵ is the sign homomorphism which sends even permutation to $+1$ and odd permutation to -1.

Let a be a generator of T. Then ρ_a is product of m disjoint cycles of each length 2^n. Thus ρ_a is a odd permutation and above homomorphism is surjective, its kernel K is index 2 normal subgroup of G. K has order $2^{n-1}m$.

We use induction on n. For n=1, K is a normal subgroup order m.

To show the uniqueness, suppose H is another subgroup of G of order m. Then KH form a group since K is normal subgroup and $|KH| = |K|\,|H|\,/\,|K \cap H|$. Thus KH is also odd order subgroup and order must be bigger m since K and H is different, but which is impossible since the largest odd order dividing G is m. $K = O(G)$.

Now suppose the statement is true for n-1. Note the kernel K of $\phi(\epsilon)$ has order $2^{n-1}m$, and its Sylow 2-subgroup is $T \cap K$ is cyclic since it is subgroup of cyclic group T. Thus there is unique normal subgroup L of K with order m by induction hypothesis. We claim that $L = O(G)$.

If we show that L is a normal subgroup of G, then the uniqueness comes from the same argument in the case when n=1.

Since L is unique normal subgroup of K with order m, L is invariant under any automorphism of K. Such group is called characteristic subgroup. Since K is normal subgroup of G, any conjugation action of $g \in G$ on K is automorphism of K. Therefore any conjugation action of $g \in G$ will leave L invariant. Therefore, L is a normal subgroup of G. $\square$

Above Lemma and similar method used in the proof of Thm2.1 (Cyclic group of even order has no transversal), give a necessary condition for a finite group to admit complete mapping.

Theorem 3.7 (Hall-Paige [13], 1955)**.** *If a finite group has a nontrivial cyclic Sylow 2-subgroup, then it does not admit complete mapping.*

Proof. Suppose G has order nm, m is odd and n is power of 2. By above lemma, there exists an epimorphism of G to the cyclic group of order n.

$$\varphi : G \to T = C_n \tag{8}$$

where T is cyclic Sylow 2-subgroup and the kernel is $O(G)$.
Consider an element S of C_n defined by,

$$S = \sum_{g \in G} \varphi(g) = mn(n-1)/2 \tag{9}$$

which is not 0 since n does not divide $mn(n-1)/2$.

Suppose G admits a complete mapping θ.
Then,

$$S = \sum_{g \in G} \varphi(g\theta(g)) = \sum_{g \in G} \varphi(g) + \sum_{g \in G} \varphi(\theta(g)) = S + S = mn(n-1) \tag{10}$$

which is divisible by n. Therefore $S = 0$ which contradicts to the equation (9). $\square$

Hall and Paige conjectured that the condition in above theorem is also a sufficient condition for admitting a complete mapping of a group. The conjecture is true and proved by , Evans, and Bray in 2009. Wilcox reduced that minimal counterexample for the conjecture should appear among the 26 sporadic simple groups or the Tits group. Bray proved that a sporadic simple group J_4 cannot be a counterexample and Evans checked that non of other 26 groups(25 sporadic simple group+the Tits group) is a counterexample.

Theorem 3.8 (Wilcox, Bray, Evans, 2009)**.** *A finite group admits complete mapping if and only if its Sylow 2-subgroup is trivial or noncyclic.*

If a group has odd order, it has trivial Sylow 2-subgroup, so Brualdi-Stein conjecture for groups is true. Now the remaining part is to prove or disprove the Ryser conjecture for the non-abelian groups. (or for the groups which have a nontrivial cyclic 2-Sylow subgroup.)

3.4 First application

As an application of Theorem3.8, we give another sufficient condition for admitting a complete mapping.

Lemma 3.9. *Let G be a finite group and P be a p-Sylow subgroup of G. For any normal subgroup N of G, $P \cap N$ is a p-Sylow subgroup of N.*

Proof. Let $|G| = p^n m$ where $(p, m) = 1$.

Since $N \triangleleft G$, PN is a group. Note that $P \cap N$ has order p^k, $k \leq n$. By the second isomorphism theorem, $[N : P \cap N] = [PN : P]$.
Thus $[N : P \cap N]$ is not divisible by p, $P \cap N$ is a p-Sylow subgroup of N.

□

Theorem 3.10. *Let G be a finite group of order $2^n k$ where k is odd. Suppose $N \triangleleft G$ has a complete mapping.*
If one of the following conditions
(1) G/N does not contain a cyclic group of order 2^n
(2) $|G/N| < 2^n$
(3) $|G/N|$ is odd
holds, then G has a complete mapping.

Proof. We may assume that $n \geq 1$, since if $|G|$ is odd, then G has a complete mapping by Theorem3.8. Let H be a 2-Sylow subgroup of G. Since N has a complete mapping, $H \cap N$ is either non-cyclic or trivial by Lemma3.9.

Case1) $H \cap N$ is non-cyclic.

Since $H \cap N < H$, H is non-cyclic. Thus G has a complete mapping by Theorem3.8.

Case2) $H \cap N$ is trivial.

Suppose G has no complete mapping, then by Theorem3.8, $H \simeq C_{2^n}$ (Cyclic group of order 2^n).
By the second isomorphism theorem,

$$C_{2^n} \simeq H = H/(H \cap N) \simeq HN/N < G/N \tag{11}$$

which contradicts (1).
By above, $[HN : N] = 2^n$.
Thus $[G : N] = [G : HN][HN : N]$ contradicts to (2) and (3). $\square$

It is not difficult to prove the following theorem.

Theorem 3.11. *$N \triangleleft G$, G/N, N both have complete mapping then G has a complete mapping.*

Proof. A transversal of G/N (in its Cayley table) makes a block (of each size $|N|$) transversal in the Cayley table of G. Fill the blocks using transversal of N. It is not difficult to prove that all these elements are different. Thus we have a transversal of G. $\square$

Determining whether a group has a complete mapping or not, can be done by calculating its 2-Sylow subgroup. Above theorem reduces the work to smaller groups.

Since every odd order group has a complete mapping (the diagonal of the Cayley table of a odd order group is a transversal or by Theorem3.8), the result from the condition (3) in Theorem3.10 is contained in the above Theorem3.11. However, the results of the condition (1) or (2) might be helpful, since you don't have to calculate 2-Sylow subgroup of G/N if one of (1) or (2) is satisfied.

3.5 Second application : A lower bound

More general version of Theorem 3.11 also hold.

Theorem 3.12. *If $N \triangleleft G$, G/N has partial transversal of length a, N has a partial transversal of length b, then G has a partial transversal of length ab.*

Proof. Similar to the Theorem 3.11. $\square$

Now we have a new type of lower bound on the size of maximum transversal for the Cayley tables of the groups.

Theorem 3.13. *Write $|G| = 2^n k$, k is odd. Then G has a partial transversal of length $(2^n - 1)k$.*

Proof. We may assume that and G has a nontrivial cyclic Sylow 2-subgroup T, since otherwise it has a full transversal by Theorem 3.8. Then by Lemma 3.6, there is a normal subgroup $O(G) \triangleleft G$ of G with $|O(G)| = k$ and $G/O(G) \simeq T$. Since T is an abelian group, it has a partial transversal of length $|T| - 1 = 2^n - 1$ by Corollary 3.5. $O(G)$ has a full transversal since its order is odd. Therefore by Theorem 3.12, G has a transversal of length $(2^n - 1)k$. $\square$

4 On the Dihedral Groups

In this section, we prove the Brualdi-Stein conjecture on Cayley tables of dihedral groups. Let D_{2n} be the dihedral group of order $2n$. If n is odd, then a 2-Sylow subgroup of D_{2n} have order 2, therefore it is cyclic. By Theorem 3.7 (Hall-Paige theorem), its Cayley table has a full transversal.

Lemma 4.1. *2-Sylow subgroup of D_{2n} is not cyclic when n is even*

Proof. D_{2n} contains normal cyclic subgroup C_n of order n. Let H be the 2-Sylow subgroup of C_n. Let f be an element of order 2 which is outside C_n. (a reflection element) Then $< H, t >= H \bigcup Ht$ is a 2-Sylow subgroup of D_{2n}, which is not cyclic. Since every p-Sylow subgroup is isomorphic to each other (by conjugation isomorphism), none of 2-Sylow subgroup of D_{2n} are cyclic. $\square$

Corollary 4.2. *If n is even, there is no full transversal of the Cayley table of D_{2n}.*

Proof. Directly follows from Lemma 4.1 and Theorem 3.8. $\square$

The main purpose of this section to give an example of a maximal transversal for each D_{2n} to prove that the Brualdi-Stein conjecture is true on every dihedral group.

Theorem 4.3. *Every Cayley table of a dihedral group has a partial transversal of size $n-1$.*

Proof. It suffices to show when n is odd. We give a constructive proof by showing an example of $n-1$ partial transversal for each odd n. Let $n = 2k+1$ and $D_{2n} = \langle r, f \mid r^n = f^2 = e, rfr = f \rangle$.
Assign order on the elements of D_{2n} as $D_{2n} = \{e, r, r^2, ..., r^{n-1}, f, rf, r^2f, ..., r^{n-1}f\}$.
Consider the Cayley table with respect to the above order (i.e. $a_{ij} = (i-th\ element) + (j-th\ element)$). For the convenience of calculation, we divide the Cayley table by 4 parts of $n \times n$ matrix each.

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \tag{12}$$

(1) In A, choose k elements on the diagonal from top left:
(i.e. $(1,1), (2,2), ..., (k,k)$ entries of A)

$$\begin{aligned} &\left\{e, r \cdot r, r^2 \cdot r^2, ..., r^{k-1} \cdot r^{k-1}\right\} \\ &= \left\{e, r^2, r^4, ..., r^{2k-2}\right\} \end{aligned} \tag{13}$$

(2) In B, choose $(k+1,1),(k+2,2),...,(2k+1,k)$ entries.($k+1$-entries) :

$$\begin{aligned}&\left\{r^k\cdot f, r^{k+1}\cdot rf, r^{k+2}\cdot r^2f,...,r^{2k}\cdot r^kf\right\}\\&=\left\{r^kf, r^{k+2}f, r^{k+4}f,...,\right\}\end{aligned}\tag{14}$$

which is exactly, the elements of form $r^{k+i}f$ for all even integer i.

(3) In C, choose $(k,2k+1),(k+1,2k),...,(2k,k+1)$ entries.(k-entries) :

$$\begin{aligned}&\left\{r^kf\cdot r^{2k}, r^{k+1}f\cdot r^{2k-1},...,r^{2k-1}f\cdot r^k\right\}\\&=\left\{r^{k+1}f, r^{k+3}f,...,r^{k-1}f\right\}\end{aligned}\tag{15}$$

which is exactly, the elements of form $r^{k+i}f$ for all odd integer i.
Thus (2) and (3) counts all element of form r^ik.

(4) In D, choose first k anti-diagonal elements,
i.e. $(1,2k+1),(2,2k),...,(k,k+1)$ entries.(k-entries) :

$$\begin{aligned}&\left\{f\cdot r^{2k}f, rf\cdot r^{2k-1}f,...,r^{k-1}f\cdot r^kf\right\}\\&=\left\{r, r^3,...,r^{2k-1}\right\}\end{aligned}\tag{16}$$

It is easy to see that all chosen entries in (1),...,(4) have different row, column in the Cayley table $\begin{pmatrix}A & B\\ C & D\end{pmatrix}$. Since they are distinct the elements of D_{2n}(all the elements except for r^{2k}), we found a partial transversal of size $n-1$. $\square$

With the similar method, one can find a full transversal of D_{2n} when n is even. Say $n=2k$ and choose k-elements from each A,B,C,D in the divided Cayley table.

Example 2. *A transversal of Cayley table of D_8.*

$$\begin{bmatrix} e & . & . & . & . & . & . & . \\ . & r^2 & . & . & . & . & . & . \\ . & . & . & . & r^2f & . & . & . \\ . & . & . & . & . & f & . & . \\ . & . & . & . & . & . & . & r \\ . & . & . & . & . & . & r^3 & . \\ . & . & . & r^3f & . & . & . & . \\ . & . & rf & . & . & . & . & . \end{bmatrix}$$

5 Rainbow matchings in the Complete Graphs

Let K_n be a complete graph with n vertices. In the problem of complete bipartite graph $K_{n,n}$, we partitioned edges with matchings of size n so that each matching contains all the vertices of $K_{n,n}$. For a given graph $G = (V, E)$, a *1-factor* is a matching which contains all the vertices. A *1-factorization* of $G = (V, E)$ is a partition of the edge set with 1-factors. A *rainbow 1-factor* is a rainbow matching and 1-factor. The Ryser conjecture can be rewritten.

Conjecture 5.1. *For odd n and any 1-factorization of $K_{n,n}$, there exists a rainbow 1-factor.*

In this section we investigate K_n instead of $K_{n,n}$. If n is odd, 1-factor of K_n does not exist so there is no 1-factorization.

If n is even, 1-factor of K_n does exist but we must show that there exist at least one 1-factorization. Take a vertex a of K_{2n}. Remove a and all its adjacent $2n$ edges for a moment, then we get K_{2n-1}. Color each vertex of K_{2n-1} with different colors $F_1, F_2, ..., F_{2n-1}$. Color edges of K_{2n-1} by F_i if the edges are 'parallel' to the F_i-vertex (the vertex colored by F_i). An edge is 'parallel' to the F_i-vertex if the edge is of form (F_{i-1}, F_{i+1}) or (F_{i-2}, F_{i+2}) ... or (F_{i-n}, F_{i+n}) where subscripts are modulo $2n$. Then all edges of K_{2n-1} are colored. Now, recover the removed vertex a and its adjacent edges by coloring the edge (a, F_i) by F_i. Then F_i-colered edges form a 1-factor (matching) of K_{2n} for all i. Thus we have a 1-factorization $F_1, F_2, ..., F_{2n-1}$ of K_{2n}. Each 1-factor F_i contains n edges.
Thus it is valid to ask the following question :

For any 1-factorization of K_{2n}, does there exists a rainbow 1-factor?

The answer is positive except for n=2. It is easy to prove that there is no rainbow 1-factor for any 1-factorization of K_4.

The answer was first given [30] by Woolbright and Fu in 1998. The problem of 1-factorization on graphs can be extended to the hypergraphs and the analog question on the complete hypergraph was solved [8] by El-Zanati, Plantholt, Sissokho,and Spence in 2006. Moreover, they gave an easier proof on the complete bipartite graph problem. We follow their proof.

Lemma 5.2. *For any 1-factorization of K_{2n}, there is a rainbow 1-factor when $n = 3, 4$.*

Proof. For $n = 3$, in a 1-factorization of K_6, we assume that there are $1, 2, .., 5$ colors are used. Take any 1-colored edge (x, y). Note that the adjacent edges of x(and y) are colored by 2,3,4,5. The remaining graph K_4 has two 1-colored edge and one i-colored edge for all $i = 2, 3, 4, 5$. We can find two non adjacent edges of color not 1, to make a rainbow 1-factor.

For $n = 4$, in a 1-factorization of K_8, start from any triangle, one can find a rainbow K_4 (The graph is isomorphic to K_4 and all the edges have different colors), say R. Suppose color used in R is 1,2,3,4,5,6. The vertices not in R and edges not in R and not adjacent to R, form another graph isomorphic to K_4, say T. For each $i \in \{1, 2, .., 6\}$, there exists one i-colored edge in T. Therefore, T is another rainbow K_4 with same color used in R. We can choose two edges from R and T each, to make a rainbow 1-factor of K_8. □

Theorem 5.3. *For any 1-factorization of K_{2n}, there exists a rainbow 1-factor when $n \neq 2$*

Proof. It Suffices to show for $n \geq 5$. Suppose a 1-factorization of K_{2n} is given with color $1, 2, .., 2n - 1$ and let M be a maximal rainbow matching. Denote $V(M)$ and $E(M)$, the vertex set and edge set of M respectively. $c(e)$ denotes the color of edge e, $C(M)$ denotes color used in M, $F(M)$ denotes color not used in M.
Suppose $k < n$. (We will find a contradiction)
We may assume that $C(M) = \{1, 2, .., k\}$, $F(M) = \{k + 1, 2, .., 2n - 1\}$ Fix two vertices s and t not in M, may assume $c(st) = 1$.(st denotes the edge adjacent with s and t.) Note that any adjacent edge with s whose color is in $F(M)$ must adjacent to M by the maximality of M.

Consider 3-edge path set from s to t, whose first edge color is $a \in F(M)$ and second edge is in $E(M)$. Such 3-path is called the *candidate 3-path related to a pair* $(M, (s, t))$. There are total $2n - 1 - k$ (choice of a) number of candidate 3-path.

For any candidate 3-path, the third edge must have color either a again or in $C(M) - \{1\}$. (Otherwise, $M - \{2nd\ edge\} \cup \{1st\ edge, 3rd\ edge\}$ is a rainbow matching of size $> k$.)

A candidate 3-path which have the same first and third edge color($a \in F(M)$), is called a *M-Symmetric (s,t) path.* By above two paragraph, there are at least $(2n-1-k)-(k-1) = 2(n - k) \geq 2$ M-Symmetric (s,t) paths.

Consider the two edges adjacent with t and the 1-colored edge in M. At most 2 colors in $F(M)$ can be used in those two edges. Then we may assume that these color are $k+1$ and $k+2$. Let $L = \{K+3, K+4, ..., 2n-1\}$.

For each $i \in L$, take the i-colored edge incident with t, and denote it $e_t = tz_i$. And denote the edge in M which is adjacent with z_i as $e_i = z_i t_i \in E(M)$. Then $M_i := M - \{e_i\} \cup \{e_t\}$ form a rainbow matching, so we can generate a new pair $(M_i, (s, t_i))$ for each $i \in L$. Note that $c(e_i) \neq 1$ since $i \in L$. Note, $F(M_i) = (F(M) - \{i\}) \cup \{c(e_i)\}$

Let S be the collection of M-symmetric (s, t) paths and M_i-symmetric (s, t_i) paths for each $i \in L$. For each $i \in L$, there are at least two M_i-symmetric (s, t_i) paths(by the same argument of M-symmetric (s, t) paths), which means that $|S| \geq 2(2n-k-3) = 4n-2k-6$.

Claim : Each element of S is determined by its 1st edge(incident with s).
Let $p \in S$. Enough to show when p is a M_i-symmetric (s, t_i) path. Either p have the 2nd edge is in M(then the 1st edge determines the others) or p is of form sz_itt_i.(Otherwise,$p = stz_it_i$ which have the first edge color 1, not in $F(M_i)$) In the latter case, p has the same 1st and 3rd edge color with sz_it_it, which is a M-symmetric (s, t) path, so it is determined by its 1st edge. Therefore, the claim is valid.

In a M_i-symmetric (s, t_i) path, the 1st,3rd edge color $a \neq c(e_i)$. (Otherwise, the path should be of form stz_it_i which is not symmetric since $c(e_i) \neq 1$.) Thus any element of S should have the 1st and 3rd color $a \in F(M)$. Combining with above claim, there are $|F(M)| = 2n-1-k$ number of symmetric paths, which implies $2n-1-k \geq 4n-2k-6$. Therefore, $2n-5 \leq k < n \Rightarrow n < 5$ a contradiction. □

6 Matroid

Many questions on graph and edge can be extended to questions on Matroid. This section introduces the basic matroid theory.

Matroid was introduced by Hassler Whitney in 1935 in the paper 'On the abstract properties of linear dependence' [27]. His idea was to capture the abstract essence of dependence. The matroid is a concept that integrates graphs and matrices. Therefore matroid theory can convert some problems on graphs and their edges to problems in linear algebra. The context of this section follows mostly from 'What is a matroid [19]' by J. Oxley and 'Lectures on matroids and oriented matroids [21]' by V. Reiner. Since the main theme of this paper is on the rainbow matching, this section does not cover every important aspect of the matroid. Proofs omitted in this section can be found in the references.

6.1 Matroid

Definition 3. *A Matroid M is a pair (E,$\mathcal{I}$) where E is a finite set called ground set and $\mathcal{I}$ is a collection of subsets of E, called independant sets, satisfying the followings axioms:*
(1) $\mathcal{I}$ is non-empty.
(2) For any subsets $A' \subset A \subset E$, if $A \in \mathcal{I}$ then $A' \in \mathcal{I}$. (Hereditary property)
(3) For $A, B \in \mathcal{I}$ and $|A| < |B|$, there exists $x \in A \setminus B$ such that $A \cup x \in \mathcal{I}$. (Exchange property)

Note that exchange property makes $\mathcal{I}$ satisfy the 'dimensional property' which means that every maximal independent set have the same cardinality.

Exercise 1. *Let $\mathcal{I}$ be a non-empty and hereditary condition satisfied collection of finite set E.*
Then $(E,\mathcal{I})$ form a matroid $\Leftrightarrow$ $\mathcal{I}$ satisfy the dimensional property, that is for all $X \subseteq E$, all maximal members of $\{I : I \in \mathcal{I} \text{ and } I \subseteq X\}$ have the same number of elements.

Two matroids M_1, M_2 are called *isomorphic* if there is a bijection between their ground sets which sends independent sets to independent sets and dependent sets to dependant sets. Isomorphic matroids are denoted by $M_1 \simeq M_2$.

Example 3 (Vectors in a vector space)**.** *Consider a matrix*

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{17}$$

Let a, b, c, d be the columns of A from the first column to the last.
Let the ground set E be the columns of A and $\mathcal{I}$ be the set of all independant subset of E.
$E = \{a, b, c, d\}$
$\mathcal{I} = \{\varnothing, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, c, d\}, \{b, c, d\}\}$
Then M = (E, $\mathcal{I}$) satisfies the 3 axioms of matroid, denote it $M[A]$.

A matroid is called *vector matroid* if it is isomorphic to a matroid $M[A]$ induced by some matrix A. A matroid M is *representable over a field* $\mathbb{F}$ if $M \simeq M[A]$ for some matrix A over field $\mathbb{F}$.

Definition 4 (Uniform matroid $U_{r,n}$)**.** *For $0 \le r \le n$, let E be an n-element set and $\mathcal{I}$ be the collection of all subsets of E with at most r elements.*
Then (E,$\mathcal{I}$) form a matroid, denote it by $U_{r,n}$.

Definition 5 (Graphic matroid $M(G)$)**.** *Let $G = (V, E)$ be a graph and $\mathcal{I}$ be the collection of all subsets of E which do not contain any cycle. Then $M(G) = (E, \mathcal{I})$ form a matroid. $M(G)$ is called a graphic matroid(or a cycle matroid) induced by G.*

Remark 6.1. *If G and H is isomorphic as graph, then obviously $M(G) \simeq M(H)$. However, the converse is not true :*
Let T be a tree on n-vertices. Then any edge subset of T is not cycle, so it is a independent set of $M(T)$. Thus the graphic matroid induced by a matching in K_{2n}(which has n-edges, $2n$-vertices) is isomorphic to $M(T)$.

6.2 Alternative definitions

There are alternative axioms for matroid. By hereditary property, the independent set $\mathcal{I}$ is completely determined by its maximal members called bases or minimal dependent sets called circuits.

The collection of Bases $\mathcal{B}$ of M satisfy following properties, called base axioms :
(B1) $\mathcal{B}$ is non-empty
(B2) (exchange property) For any two member B_1, B_2 of $\mathcal{B}$ and $x \in B_1 - B_2$, there exist $y \in B_2 - B_1$ such that $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$.

And the collection of circuits $\mathcal{C}$ of M satisfy following properties, called circuit axioms :
(C1) $\emptyset \notin \mathcal{C}$
(C2) No members of $\mathcal{C}$ is a proper subset of another member of $\mathcal{C}$.
(C3) For two distinct member C_1, C_2 of $\mathcal{C}$ and $e \in C_1 \cap C_2$, $(C_1 \cup C_2) - \{e\}$ contains a member of $\mathcal{C}$.

Converses hold. Therefore, we have alternative definitions for matroid denoted by $(E, \mathcal{B})$ and $(E, \mathcal{C})$.

Theorem 6.2. *(1) Let $\mathcal{B}$ be a set of subsets of finite set E. Then $\mathcal{B}$ satisfy (B1), (B2) if and only if $\mathcal{B}$ is the collection of bases of a matroid on E.*
(2) Let $\mathcal{C}$ be a set of subsets of finite set E. Then $\mathcal{C}$ satisfy (C1), (C2), (C3) if and only if $\mathcal{C}$ is the collection of circuits of a matroid on E.

Let M be a matroid on E and $r(M)$ be the maximum size of an independent set in the matroid. For a subset A of E, one can define a matroid on A by considering a subset of A is independent if and only if it is independent in M. The matroid on a subset of E is called a submatroid of M. So the function $r(A)$ counts the maximum size of an independent subset of A and r is defined on every subset of E. r is called the rank function. The rank function has following properties, called rank axioms:

(R1) The value of r is non-negative integer.

(R2) For any subset A of E, $r(A) \leq |A|$.

(R3) For any two subsets A and B of E, $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.(i.e. a submodular function)

(R4) For any $A \subseteq B \subseteq E$, $r(A) \leq r(B) \leq r(E)$. (i.e a monotonic function)

These properties can be used as one of the alternative definitions of matroid (E, r).

Theorem 6.3. *Let E be a finite set, r be a function satisfy (R1)-(R4). Define I is independent set iff $r(I) = |I|$. Then $(M, \mathcal{I} = \{I\})$ form a matroid.*

Therefore a matroid is determined by ranks of its subsets. $M_1 = (E_1, r_1) \simeq M_2 = (E_2, r_2)$ if there is a bijection between E_1 and E_2 which preserve rank functions.

6.3 Dual

For any planner graph G, we can define the dual of G by drawing a vertex for each face of G, and an edge if two faces of G are divided by an edge. Unfortunately, dual cannot be defined on non-planner graphs. One of the advantages of introducing matroid is that we can extend the concept of dual to arbitrary graphs. Let M=(E,$\mathcal{B}$) be a matroid where $\mathcal{B}$ is the collection of base of M.

Definition 6 (Dual)**.** *Define $\mathcal{B}^*$:=$\{E - B : B \in \mathcal{B}\}$*
M^*:=(E, $\mathcal{B}^*$) also satisfy axiom of matroid($\mathcal{B}^*$ is the base set) and is called the dual of matroid M.

Note that $M^{**} = M$.

For a planner graph G, denote its dual by G^*. Then $M(G^*) = M(G)^*$ since there is a canonical 1-1 correspondence between complement of spanning trees of G and spanning trees of G^*.

Remark 6.4. *(1)* $(U_{r,n})^* = U_{n-r,n}$. *(2)* $r(M) + r(M^*) = n$ *if* M *has* n*-element of ground set.*

Following operations on matrix does not change its induced matroid.

Lemma 6.5. *Let* A *be a matrix with entries are from field element* $\mathbb{F}$. *Then under following matrix operations on* A*, induced vector matroid* $M[A]$ *remains unaltered(isomorphic).*

(1) Interchange two rows.
(2) Multiply a row by any non-zero number of field $\mathbb{F}$.
(3) Replace a row by the sum of that row and another.
(4) Delete a zero row unless it is the only row.
(5) Interchange two columns(moving the labels with the columns.
(6) Multiply a column by a non-zero member of $\mathbb{F}$.

If A has rank r, then by above operations, A can be changed into of form $[I_r|D]$. Thus $M[A] \simeq M[I_r|D]$. Taking dual of $M[A]$ involves D^T, indeed $M[I_r|D]^* = M[-D^T|I_{n-r}]$.

Theorem 6.6. *Let* M *be an* n*-element matroid which is representable over* $\mathbb{F}$. *Then* M^* *is also representable over* $\mathbb{F}$.

6.4 Deletion and Contraction

Consider a set of finite vectors $M = \{v_1, v_2, .., v_n\}$ in a vector space. Deleting any v_i from M also form a finite set of vectors in a vector space. Or if we project all the other $n-1$ vector to the subspace orthogonal to v_i except for v_i, then the result vectors form a finite set of vectors in the subspace. As matroid is a generalized concept of the finite set of vectors in a vector space, we can expect that there will be similar operations in matroid. These operations are called deletion and contraction.

Definition 7 (Deletion)**.** *Let* M=$(E,\mathcal{I})$, $e \in E$.
$\mathcal{I}' := \{I \subseteq E - e : I \in \mathcal{I}\}$.
Then $(E - \{e\}, \mathcal{I}')$ *form a matroid, denoted by* $M \setminus e$*, called the deletion of* e *from* M.

Definition 8 (Contraction)**.** *Let* M=$(E,\mathcal{I})$, $e \in E$.
If $\{e\}$ *is a circuit of* M*, then define* $M/e := M \setminus e$.
If $\{e\}$ *is not a circuit, then define* $\mathcal{I}'' := \{I \subseteq E - \{e\} : I \cup \{e\} \in \mathcal{I}\}$.
Then $\{E - \{e\}, \mathcal{I}''\}$ *form a matroid, denoted by* M/e.
M/e *is called the contraction of* e *from* M.

It is also a generalization of deletion and contraction of an edge of graph: $M(G/e) = M(G)/e$ and $M(G \setminus e) = M(G) \setminus e$.

Remark 6.7. *$M/e/f = M/f/e$, $M/e/f = M \setminus f \setminus e$, $M \setminus e/f = M/f \setminus e$.*

Thus we can extend deletion and contraction by replacing simple element e to any subset T of E. For $T = \{a_1, a_2, ..\}$, $M \setminus T := ((M \setminus a_1) \setminus a_2...))$ and $M/T := ((M/a_1)/a_2...))$.

Theorem 6.8. *Let M be a matroid on ground set E. $T \subseteq E$. $X \subseteq E \setminus T$.*

(1) X is $\begin{pmatrix} \text{independent} \\ \text{circuit} \\ \text{basis} \end{pmatrix}$ in $M \setminus T$

$\Leftrightarrow$

X is $\begin{pmatrix} \text{independent} \\ \text{circuit} \\ \text{maximal subset independent in } E - T \end{pmatrix}$ in M.

(2) X is $\begin{pmatrix} \text{independent} \\ \text{basis} \end{pmatrix}$ in $M/T \Leftrightarrow X \cup B_T$ is $\begin{pmatrix} \text{independent} \\ \text{basis} \end{pmatrix}$ in M for some maximal subset B_T of T in M.

(3) X is circuit in $M/T \Leftrightarrow X$ is minimal non-empty member of $\{C - T \mid C : \text{circuit of } M\}$.

Remark 6.9. *Deletion and contraction are reversed by duality: $(M \setminus T)^* \simeq M^*/T$ and $(M \setminus T)^* \simeq M^* \setminus T$*

Example 4. *If $M = U_{r,n}$ a uniform matroid then*

$$M \setminus e \simeq \begin{cases} U_{r,n-1} & \text{if } r < n \\ U_{r-1,n-1} & \text{if } r = n \end{cases}$$

$$M/e \simeq \begin{cases} U_{r-1,n-1} & \text{if } r > 0 \\ U_{r,n-1} & \text{if } r = 0 \end{cases}$$

for any ground set element e of M.

Definition 9 (Minor)**.** *A matroid N is called minor of M if we can obtain N form M by performing a finite sequence consists of deletions and contractions.*
i.e. $N = M \setminus S/T$

Minor is useful in characterizing families of matroids. The family of Graphic matroids, the family of vector matroids over a field $\mathbb{F}$, and so on. Characterizing some families of matroid using minor is given later.

6.5 Direct sum

Suppose $M_1 = \{v_1, v_2, .., v_n\}$ be a finite set of vectors in a vector space V_1 and $M_2 = \{w_1, w_2, .., w_m\}$ be a finite set of vectors in a vector space V_2. Then the set
$\{(v_1, 0), (v_2, 0), .., (v_n, 0), (0, w_1), (0, w_2), .., (0, w_m)\}$
is again a finite set of vectors in the direct sum of vector spaces $V_1 \bigoplus V_2$.

Definition 10 (Direct sum)**.** *Let M_1=(E_1,$\mathcal{I}_1$), M_2=(E_2,$\mathcal{I}_2$). The direct sum $M_1 \bigoplus M_2$=(E,$\mathcal{I}$) of matroids M_1 and M_2 is defined by,*
The ground set $E := E_1 \cup E_2$ and the independent set $\mathcal{I} := \{I_1 \cup I_2 \mid I_1 \in \mathcal{I}_1, I_2 \in \mathcal{I}_2\}$.

It is equivalent to define the base set of $M_1 \bigoplus M_2$ by $\mathcal{B} := \{B_1 \cup B_2 \mid B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}$ where $\mathcal{B}_i$ is the base set of M_i.

Definition 11. *A matroid that cannot be written as direct sum of two smaller matroids is called indecomposable or connected.*

For two graphs G_1 and G_2, $G_1 \vee_v G_1$ denotes a graph obtained by gluing two graphs at a common vertex v.

Remark 6.10. $M(G_1) \bigoplus M(G_2) = M(G_1 \vee_v G_1) = M(G_1 \sqcup G_1)$ *where $\sqcup$ denotes disjoint union. Vertex v can be chosen any two vertex of G_1, G_2*

Therefore, the family of graphic matroid is closed under $\bigoplus$.

Definition 12. *A cographic matroid is a matroid isomorphic to dual of a graphic matroid.($M(G)^*$)*

Remark 6.11. $(M(G_1) \bigoplus M(G_2))^* = M_1^* \bigoplus M_2^*$

Therefore, the family of cographic matroid is also closed under $\bigoplus$.
For any field $\mathbb{F}$, the family of matroid representable over $\mathbb{F}$ is also closed under $\bigoplus$.

Indeed, $M[A_1]\bigoplus M[A_2] = M[\left(\begin{smallmatrix} A_1 & 0 \\ 0 & A_2 \end{smallmatrix}\right)]$

However, the class of uniform matroid is not closed under $\bigoplus$.

Theorem 6.12. *$U_{0,1}\bigoplus U_{1,1}$ is not a uniform matroid.*

Proof. $E(U_{0,1}\bigoplus U_{1,1}) \simeq \{a,b\}$ with $\{a\}$ is a independent set and $\{a\}$ is a dependent set of the matroid. Therefore not every 1-element subset is all independent nor dependent, so not a uniform matroid. $\square$

Later, Theorem6.17, $U_{0,1}\bigoplus U_{1,1}$ characterizes the class of uniform matroids.

Definition 13 (Partition Matroid)**.** *Let B_i be a collection of disjoint sets, and d_i be integers with $0 \le d_i \le |B_i|$. Define the ground set $E := \cup_i B_i$ and define I be an independent set if $|I \cap B_i| \le d_i$, for each i. Then it is a matroid since it is isomorphic to the direct sum of uniform matroids $\bigoplus_i U_{d_i,|B_i|}$. This matroid is called a partition matroid.*

Remark 6.13. *The class of partition matroids is closed under $\bigoplus$, dual, deletion and contraction.*

6.6 Excluded minor

Let $\mathfrak{F}$ be a family of matroids. A family of matroids $\mathfrak{F}$ is called *minor-closed* if $\mathfrak{F}$ is closed under deletion and contraction.

Theorem 6.14. *The class of uniform matroids $\mathfrak{U}$ is minor-closed.*

Proof. Follows from Example 2. $\square$

Theorem 6.15. *The class of graphic matorids $\mathfrak{G}$ and cographic matroids $\mathfrak{C}$ are minor-closed.*

Proof. $M(G/e) = M(G)/e$ and $M(G \setminus e) = M(G) \setminus e$ implies $\mathfrak{G}$ is minor-closed. By remark 5.6 $\mathfrak{C}$ is minor-closed. $\square$

Theorem 6.16. *For any field $\mathbb{F}$, the family of $\mathbb{F}$-representable matroids is minor-closed.*

Proof. Deletion of a column e from $M[A]$ is obtained by deleting e form A. Since dual of $M[A] \simeq M[I_r|D]$ is $M[I_r|D]^* = M[-D^T|I_{n-r}]$, the dual is also $\mathbb{F}$-representable. Since contraction of e is a composition of deletion of e and dual, contraction of $\mathbb{F}$-representable a matroid is again $\mathbb{F}$-representable. $\square$

Definition 14 (Excluded Minor). *Let $\mathfrak{F}$ be a minor-closed class of matroids. The collection of minor-minimal matroids not in $\mathfrak{F}$ is called excluded minors denoted by $E(\mathfrak{F})$. That is, $M \in \mathfrak{F}$ iff $M \notin \mathfrak{F}$ and every proper minor of M is in $\mathfrak{F}$.*

Theorem 6.17. *Excluded minor of the class of uniform matroids, $E(\mathfrak{U}) = \{U_{0,1} \bigoplus U_{1,1}\}$*

Proof. $U_{0,1} \bigoplus U_{1,1} \notin \mathfrak{U}$ by Theorem 5.9.
Suppose $M \in E(\mathfrak{F})$. Since M is not a uniform matroid, there exist natural number k such that M has both a k-element independent set and a k-element dependent set. Choose k minimal number. Let C be a k-element dependent set, which is a circuit by minimality of k. Thus, for any $e \in C$, $C - \{e\}$ form an independent set of size $k-1$. Since there is a k-element independent set, there exist $f \in C - \{e\}$ such that $C - \{e\} \cup \{f\}$ is an independent set.
By Theorem 5.5, $\{e\}$ is a circuit and $\{f\}$ is an independent set of the matroid $M/(C - \{e\})$. Since M must be a deletion invariant, $M/(C - \{e\}) = M$. Thus, $(C - \{e\}$ must be empty set.
Deletion of all elements except for e, f from M must be M, thus $E(M) = \{e, f\}$. By above paragraph $\{f\}$ is independent and $\{e\}$ is a circuit (so dependent) of M. Therefore, $M \simeq U_{0,1} \bigoplus U_{1,1}$. □

6.7 Excluded minors of graphic matroid

A minor of graph G is a graph obtained by a finite sequence of deleting an edge, contracting an edge and deleting an isolated vertex. Following is a characterization of planner given by Kuratowski [17].

Theorem 6.18. *A graph is planner if and only if it has no minor isomorphic to K_5 or $K_{3,3}$.*

Tutte [26] generalized the theorem and gave a characterization of graphic and cographic matroid.

Theorem 6.19 (Tutte). *The excluded minor set of the family of graphic matroids is given by,*
$E(\mathfrak{G}) = \{U_{2,4}, F_7, F_7^*, M(K_5)^*, M(K_{3,3})^*\}$

Corollary 6.20. *The excluded minor set of the family of cographic matroids is given by,*
$E(\mathfrak{C}) = \{U_{2,4}, F_7, F_7^*, M(K_5), M(K_{3,3})\}$

F_7 is called the *Fano Matroid* defined by $\{(1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)\}$ vectors in the 3 dimensional vector space over $\mathbb{F}_2$.

6.8 Matroid representation

The matroid is an axiomatization of combinatorial properties of finite sets of vectors in a vector space, so determining a given matroid is whether $\mathbb{F}$-representable or not is a fundamental question.

Note that, the family of $\mathbb{F}$-representable matroid is minor-closed for any $\mathbb{F}$ by Theorem6.16. Therefore, the excluded minor set can be used in characterizing the class of $\mathbb{F}$-representable mantroids.

However, finding excluded minor set is tough problem in general, even determining whether it is finite or infinite. In 1970, Gian-Carlo Rota conjectured that if $\mathbb{F}$ is a finite field, then the excluded minor set of the family of $\mathbb{F}$-representable matroids is finite set. [23] A proof of the conjecture has been announced by Gleen, Geralds, and Whittle [11]. However, the set of excluded minor of $GF(n)$ when $n > 4$ is not yet completely characterized.

Remark 6.21. *M is $\mathbb{F}$-representalbe then M^* is also representable. Thus if N is an excluded minor of the family of $\mathbb{F}$-representable matroid then N^* should be an excluded minor.*

A matroid is called *binary* if it is $GF(2)$-representable and *ternary* if it is $GF(3)$-representable. A matroid is called *regular* if it is representable over all fields. Following theorems show the history of matroid representation and excluded minor.

Theorem 6.22 (Tutte [25], 1958)**.** *A matroid is binary if and only if it has no minor isomorphic to $U_{2,4}$.*

Theorem 6.23 (Bixby [4] and Seymour [24] , 1970's)**.** *A matroid is ternary if and only if it has no minor isomorphic to $U_{2,5}, U_{3,5}, F_7, F_7^*$.*

Theorem 6.24 (Tutte [25], 1958)**.** *A matroid is regular if and only if it is both binary and ternary.*
Moreover, M is regular if and only if it has no minor isomorphic to $U_{2,4}$, F_7 or F_7^*.

Theorem 6.25 (Geelen-Gerards-Kapoor [10], 1996)**.** *There are 8 excluded minors of the class of $GF(4)$-representable matroid.*

Theorem 6.26 (Geelen-Gerards-Whittle [11], 2013)**.** *For any finite field $\mathbb{F}$, the excluded minor set of the family of $\mathbb{F}$-representable matroid is finite.*

For the case of an infinite field, there are infinitely many excluded minors. Moreover,

Theorem 6.27 (Mayhew-Newman-Whittle [18])**.** *Let $\mathbb{F}$ be an infinite field and N be a matroid representable over $\mathbb{F}$. Then there exists a $\mathbb{F}$-representable matroid M which does not have N as its minor.*

6.9 Robertson-Seymour Theorem and Matroid

Seymour and Robertson proved following great theorem on graph theory.

Theorem 6.28 (Robertson-Seymour Graph Minors Theorem [22], 2004)**.** *Any minor-closed class of graphs have a finite number of excluded minor graphs.*

Combining Theorem6.19 (Tutte's characterization of graphic matroids) and above theorem,

Corollary 6.29. *Any minor-closed class of graphs has a finite excluded minor set.*

Though rota's conjecture on the finiteness of excluded minor of finite fields is settled, there is a stronger conjecture left which is parallel to above Corollary.

Conjecture 6.30 (Matroid Minors Conjecture)**.** *Let $\mathbb{F}$ be a finite field. Then any minor-closed class of $\mathbb{F}$-representable matroids has a finite excluded minor set.*

However, the problem is not yet solved even for $GF(2)$.

6.10 Transversal matroid

Let $S = \{a_j\}$ be a finite set. A set system is a multiset $A = (A_i : i \in I)$ of subsets of a set S. Regard the multiset $A = (A_i : i \in I)$ as the left vertices and $S = \{a_j\}$ as right vertices and connect edges if A_i contains a_j then we get a bipartite graph.

Example 5. $S = \{a, b, c\}$, $A = (A = \{a, b, c\}, B = \{a, b, c\}, C = \{a, b, c\})$.
The bipartite graph is $K_{3,3}$.

Definition 15. *A transversal (matching) of A is a subset T of S for which there is a bijection $\varphi : T \to J$ with $t \in A_{\varphi(t)}$ for all $t \in T$.*

Transversals of a set system are exactly matchings of the corresponding bipartite graph.

Theorem 6.31 (Edmonds and Fulkerson [7], 1965)**.** *The partial transversals of a set system A are the independent sets of a matroid.*

Theorem can be proved directly by partial transversal satisfy the independent axioms of matroid. But the theorem also can be proved by showing the partial transversal forms a $\mathbb{F}$-representable matroid.

Proof. Let $\mathbb{F}$ be a field and the corresponding bipartite graph be $((A,B),E)$. Let $\mathbb{F}(x_{a,b})$ be the field extension of $\mathbb{F}$ by the transcendentals $\{x_{a,b} : a \in A, b \in B\}$. Consider the vector space $\mathbb{F}(x_{a,b})^{|B|}$ and standard basis $\{e_b : b \in B\}$. For a vertex $a \in A$, replace a by a vector,

$$\sum_{b \in B : ab \in E} x_{a,b} e_b \tag{18}$$

Write the vectors replaced by a with respect to the standard basis as columns of a matrix, then we get a $|B| \times |A|$ matrix. Consider a square minor from $I \times J (I \subseteq A, J \subseteq B)$ of the matrix and its determinant. Each monomial of the determinant correspond to a matching between I and J and since non-zero entries are all different transcendental element, the minor has non-zero determinant iff there is a matching between I and J. Therefore, partial transversals of a set system form a vector matroid.

□

The matroid of above theorem is called *transversal matroid* of the set system.

Theorem 6.32 (Piff and Welsh [20], 1970)**.** *A transversal matroid is representable over all sufficiently large fields, in particular, over all infinite fields.*

Proof. (Sketch) By the proof of above theorem, a transversal matroid is representable by a matrix whose non-zero entries are indeterminants $x_{a,b}$. If a field $\mathbb{F}$ is sufficiently large, then we can replace $x_{a,b}$ by appropriate field members so that, the statement "a square minor determinant is non-zero iff there is a corresponding matching" is still true.

□

Theorem 6.33. *The class of transversal matroids is closed under direct sums.*

7 Matroid and Generalized Conjectures

Some problems on Graphs and their edges can be extended to problems in matroid. The Ryser-Brualdi-Stein conjecture has some generalized versions in matroid theory.

7.1 Matroidal Latin Square

In [16], Kotlar and Ziv generalized the conjecture using matroidal Latin square.

Definition 16 (Matroidal Latin square)**.** *Let M be a matroid with ground set E. A matroidal latin square L of degree n is a $n \times n$ array whose entries are elements of E, such that every* *row and column form a basis of M.*

A (partial) transversal of L is an independent subset of entries of A where no two of them lie in the same row or column of A.

Matroidal latin square is an extended concept of Latin square.

Example 6. *Consider a partition matroid $\bigoplus^n U_{1,n}$, which has ground set $[n]_1 \dot{\bigcup} [n]_2 ... \dot{\bigcup} [n]_n$ where $[n]_i = \{1, 2, .., n\}$ for all $i = 1, 2, ..., n$. Then a choice of distinct number from each $[n]_i$ by one element is a basis of $\bigoplus^n U_{1,n}$. A matroidal latin square of $\bigoplus^n U_{1,n}$ correspond to a latin square.*

However, extended version of Ryser conjecture in matroidal Latin squares is false by following theorem [16]:

Theorem 7.1. *For every n, there is a matroidal Latin squre which has no full transversal.*

Proof. Let $\{v_1, v_2, ..., v_n\}$ be a basis of $\mathbb{R}^n$. Consider a vector matroid M whose ground set is $E = \{v_k, v_i - v_j : k = 1, 2, .., n \text{ and } i \neq j\}$ and a subset of E is an independent set if it is an independent set of $\mathbb{R}^n$.
Let $A = (a_{ij})$ be a matrix defined by

$$a_{ij} = \begin{cases} v_1 & \text{if } i = j \\ v_i - v_j & \text{if } i \neq j \end{cases}$$

Then every column and row of A form base, so A is a matroidal Latin square of M. Suppose A has a full transversal $T = \{t_1, t_2, ..., t_n\}$

Case1) Suppose T does not contains any diagonal element of A. Then,

$$\sum_{i}^{n} t_i = \sum_{i,j=1}^{n} v_i - v_j = (v_1 + v_2 + ... + v_n) - (v_1 + v_2 + ... + v_n) = 0 \tag{19}$$

which means T is a dependent set. contradiction

Case2) Suppose T contains exactly one diagonal element.
If T contains a_{11}, then

$$\sum_{i}^{n} t_i - v_1 = 0 \tag{20}$$

which means that T is a dependent set.
If T contains a_{ii}, $i \neq 1$ then any element of T has no term of $\pm v_i$, which means $v_i \notin span(T)$. Thus T is a dependent set. Contradiction.

If T contains more than one diagonal element, then it contains a_1 more than one, which means T is a dependent set. Therefore A has no full transversal. $\square$

Still, an extended version of Brualdi-Stein conjecture can be stated.

Conjecture 7.2. *Every matroidal Latin square of order n has $n-1$ partial transversal.*

A lower bound $\lceil 2n/3 \rceil$ for the maximum size of transversal of matroidal Latin square of order n is given in [16]. Later, Corollary7.5 shows that $n - \sqrt{n}$ is another lower bound.

7.2 Intersection of two matroids

In 2009, Aharoni and Berger extended the conjecture of Brualdi-Stein [1]. Let a bipartite graph $((X,Y),E)$ is given, where X is left vertices and Y is right vertices. Define

$\mathcal{I}_X := \{T \subseteq E : T \textit{ has no same end points in } X\}$

$\mathcal{I}_Y := \{T \subseteq E : T \textit{ has no same end points in } Y\}$

Then $\mathcal{I}_X$ and $\mathcal{I}_Y$ satisfy axioms of independent set of matroid. Thus $M_X = (E, \mathcal{I}_X)$ and $M_Y = (E, \mathcal{I}_Y)$ are matroids.
Moreover, the set of matchings of bipartite graph is exactly $\mathcal{I}_X \cap \mathcal{I}_Y$, or denote it by $\mathcal{M}_X \cap \mathcal{M}_Y$. Therefore Brualdi-Stein conjecture can be extended as follow:

Conjecture 7.3 (Aharoni-Berger)**.** *Let M and N be matroids on the same ground set E, and a pairwise disjoint set system $F = \{F_1, F_2, ..., F_n\}$ satisfy $F_i \in \mathcal{M} \cap \mathcal{M}$, $|F_i| = n$ for all $i = 1, 2, ..n$. Then F has a partial rainbow of size $n-1$ belonging to $\mathcal{M} \cap \mathcal{M}$.*

The Aharoni-Berger conjecture is more general version of the conjecture of matroidal Latin square, see the proof of Corollary7.5.

There is some progress on the conjecture. Aharoni, Kotlar, and Ziv proved the parallel version of Theorem 2.6 which says $n - \sqrt{n}$ is also a lower bound in the problem of intersection of two matroids.

Theorem 7.4 (Aharoni-Kotlar-Ziv [2], 2015)**.** *With the same hypothesis as above conjecture, there is a rainbow set of size at least $n - \sqrt{n}$.*

Corollary 7.5. *Matroidal Latin square of order n has a partial transversal of size at least $n - \sqrt{n}$.*

Proof. Let A be a matroidal Latin square of order n on a matroid M with ground set S. We may assume that S is the set of all entries of A. Take N as the partition matroid induced by columns of A (which has the ground set S.), i.e. a subset of S is independent in N iff entries are in different columns of A. ($N \simeq \bigoplus^n U_{1,n}$). Applying Theorem7.3, on the rows of A, we get the result. $\square$

The parallel version of Hatami-Shor theorem ($n - O(log^2 n)$ is a lower bound) is not yet proved or disproved.

References

[1] Ron Aharoni and Eli Berger. Rainbow matchings in r-partite r-graphs. *the electronic journal of combinatorics*, 16(1):119, 2009.

[2] Ron Aharoni, Daniel Kotlar, and Ran Ziv. Rainbow sets in the intersection of two matroids. *Electronic Notes in Discrete Mathematics*, 43:39–42, 2013.

[3] Paul T Bateman. A remark on infinite groups. *The American Mathematical Monthly*, 57(9):623–624, 1950.

[4] Robert E Bixby. On reid's characterization of the ternary matroids. *Journal of Combinatorial Theory, Series B*, 26(2):174–204, 1979.

[5] Andries E Brouwer, AJ de Vries, and RMA Wieringa. A lower bound for the length of partial transversals in a latin square. *Nieuw Archief Voor Wiskunde*, 26(2):330, 1978.

[6] David A Drake. Maximal sets of latin squares and partial transversals. *Journal of Statistical Planning and Inference*, 1(2):143–149, 1977.

[7] Jack Edmonds and Delbert Ray Fulkerson. Transversals and matroid partition. Technical report, RAND CORP SANTA MONICA CA, 1965.

[8] SI El-Zanati, MJ Plantholt, PA Sissokho, and LE Spence. On the existence of a rainbow 1-factor in 1-factorizations of k rn (r). *Journal of Combinatorial Designs*, 15(6):487–490, 2007.

[9] Anthony B Evans. The admissibility of sporadic simple groups. *Journal of Algebra*, 321(1):105–116, 2009.

[10] James F Geelen, AMH Gerards, and Ajai Kapoor. The excluded minors for gf (4)-representable matroids. *Journal of Combinatorial Theory, Series B*, 79(2):247–299, 2000.

[11] Jim Geelen, Bert Gerards, and Geoff Whittle. Solving rotas conjecture. *Notices of the AMS*, 61(7):736–743, 2014.

[12] Marshall Hall. A combinatorial problem on abelian groups. *Proceedings of the American Mathematical Society*, 3(4):584–587, 1952.

[13] Marshall Hall and Lowell Paige. Complete mappings of finite groups. *Pacific Journal of Mathematics*, 5(4):541–549, 1955.

[14] Pooya Hatamia and Peter W Shorb. A lower bound for the length of a partial transversal in a latin square, revised version.

[15] Klaas K Koksma. A lower bound for the order of a partial transversal in a latin square. *Journal of Combinatorial Theory*, 7(1):94–95, 1969.

[16] Daniel Kotlar and Ran Ziv. On the length of a partial independent transversal in a matroidal latin square. *arXiv preprint arXiv:1204.5274*, 2012.

[17] Casimir Kuratowski. Sur le probleme des courbes gauches en topologie. *Fundamenta mathematicae*, 15(1):271–283, 1930.

[18] Dillon Mayhew, Mike Newman, and Geoff Whittle. On excluded minors for real-representability. *Journal of Combinatorial Theory, Series B*, 99(4):685–689, 2009.

[19] James G Oxley. *Matroid theory*, volume 3. Oxford University Press, USA, 2006.

[20] MJ Piff and DJA Welsh. On the vector representation of matroids. *Journal of the London Mathematical Society*, 2(2):284–288, 1970.

[21] Victor Reiner. Lectures on matroids and oriented matroids. *Lecture Notes for ACE Summer School in Geometric Combinatorics*, 2005.

[22] Neil Robertson and P.D. Seymour. Graph minors. xx. wagner's conjecture. *Journal of Combinatorial Theory, Series B*, 92(2):325 – 357, 2004. Special Issue Dedicated to Professor W.T. Tutte.

[23] Gian-Carlo Rota. Combinatorial theory, old and new. *Proc. Internat. Cong. Math.(Nice*, pages 229–233, 1970.

[24] Paul D Seymour. Matroid representation over gf (3). *Journal of Combinatorial Theory, Series B*, 26(2):159–173, 1979.

[25] William T Tutte. A homotopy theorem for matroids. i. *Transactions of the American Mathematical Society*, 88(1):144–160, 1958.

[26] William Thomas Tutte. Matroids and graphs. *Transactions of the American Mathematical Society*, 90(3):527–552, 1959.

[27] Hassler Whitney. On the abstract properties of linear dependence. *American Journal of Mathematics*, 57(3):509–533, 1935.

[28] Stewart Wilcox. Reduction of the hall–paige conjecture to sporadic simple groups. *Journal of Algebra*, 321(5):1407–1428, 2009.

[29] David E Woolbright. An n× n latin square has a transversal with at least n- n distinct symbols. *Journal of Combinatorial Theory, Series A*, 24(2):235–237, 1978.

[30] David E Woolbright, Hung-Lin Fu, et al. On the existence of rainbows in 1-factorizations of k-2n. *Journal of Combinatorial Designs*, 6(1):1–20, 1998.

국문초록

변이 색칠된 그래프가 주어져 있을 때 모두 다른 색을 가지는 부합(matching)을 rainbow matching이라고 한다. n개의 색으로 변이 색칠된 완전 이분 그래프의 rainbow matching의 최대 크기에 대한 추측이 Ryser, Brualdi, Stein에 의해 제기되었다. 최대 크기의 하한(lower bound)에 대해서 어디까지 연구되었는지 알아보고, 군(group)의 Cayley table으로 추측을 제한한 문제(Hall-Paige)와 2009년의 결과(Wilcox-Bray-Evan)에 대해서 알아보았다. 그 결과에 대한 응용으로 group으로 문제를 제한한 경우에서 rainbow matching의 최대 크기에 대한 하한을 얻었고, dihedral group에 대해서 Ryser-Brualdi-Stein 추측이 참인 것을 확인해 보았다. 또한 기본적인 Matroid이론과 Ryser-Brualdi 추측의 Matroid로의 확장에 대한 연구에 대해서 알아보았다.

주요어 : 무지개 부합, 완전 이분 그래프, 라틴 방진, 군, 매트로이드
학　번 : 2014-22351