

# From coordinate subspaces over finite fields to ideal multipartite uniform clutters

Ahmad Abdi <sup>1</sup>

Dabeen Lee <sup>2,\*</sup>

June 6, 2023

## Abstract

Take a prime power  $q$ , an integer  $n \geq 2$ , and a coordinate subspace  $S \subseteq GF(q)^n$  over the Galois field  $GF(q)$ . One can associate with  $S$  an  $n$ -partite  $n$ -uniform clutter  $\mathcal{C}$ , where every part has size  $q$  and there is a bijection between the vectors in  $S$  and the members of  $\mathcal{C}$ .

In this paper, we determine when the clutter  $\mathcal{C}$  is *ideal*, a property developed in connection to Packing and Covering problems in the areas of Integer Programming and Combinatorial Optimization. Interestingly, the characterization differs depending on whether  $q$  is 2, 4, a higher power of 2, or otherwise. Each characterization uses crucially that idealness is a *minor-closed property*: first the list of excluded minors is identified, and only then is the global structure determined. A key insight is that idealness of  $\mathcal{C}$  depends solely on the underlying matroid of  $S$ .

Our theorems also extend from idealness to the stronger *max-flow min-cut* property. As a consequence, we prove the Replication and  $\tau = 2$  Conjectures for this class of clutters.

**Keywords.** Vector space over finite field, multipartite uniform clutter, ideal clutter, the max-flow min-cut property, minor-closed property, matroid.

## 1 Introduction

Let  $V$  be a finite set of *elements*, and let  $\mathcal{C}$  be a family of subsets of  $V$  called *members*. A *cover* is defined as a subset of  $V$  that intersects every member in  $\mathcal{C}$ . Given weights  $w \in \mathbb{Z}_+^V$ , a minimum weight cover can be computed by solving the integer program  $\min\{w^\top x : M(\mathcal{C})x \geq \mathbf{1}, x \in \mathbb{Z}_+^V\}$ , where  $M(\mathcal{C})$  is the incidence matrix of  $\mathcal{C}$  whose columns are labeled by the elements and whose rows are the incidence vectors of the members. The linear programming relaxation of this integer program is the problem of minimizing  $w^\top x$  over the *associated set covering polyhedron* given by  $Q(\mathcal{C}) := \{x \in \mathbb{R}^V : M(\mathcal{C})x \geq \mathbf{1}, x \geq \mathbf{0}\}$ . For the purpose of finding a minimum

---

<sup>1</sup>Department of Mathematics, London School of Economics and Political Science, London WC2A 2AE, UK, [a.abdi1@lse.ac.uk](mailto:a.abdi1@lse.ac.uk)

<sup>2</sup>Department of Industrial and Systems Engineering, KAIST, Daejeon 34126, Republic of Korea, [dabeen1@kaist.ac.kr](mailto:dabeen1@kaist.ac.kr)

\*Corresponding author

weight cover, we may assume without loss of generality that no member properly contains another, in which case we call  $\mathcal{C}$  a *clutter* over ground set  $V$  [15]. A necessary and sufficient condition for the relaxation to return an integer solution for any  $w \in \mathbb{Z}_+^V$ , thereby giving a minimum weight cover, is that every extreme point of  $Q(\mathcal{C})$  is an integral vector, in which case we say that  $\mathcal{C}$  is *ideal* [12].

Every clutter whose members are pairwise disjoint is obviously ideal. Many non-trivial examples of ideal clutters can be found in Combinatorial Optimization – let us mention a few here: the clutter of  $st$ -paths of a graph [26], (inclusionwise) minimal  $st$ -cuts of a graph [14], minimal  $T$ -joins of a graph [17], minimal  $T$ -cuts of a graph [17], and odd circuits of a signed graph that has no odd- $K_5$  minor [18]. Each of these examples has as ground set the edge set of the associated graph. In general, it is co-NP-complete to decide whether a clutter is ideal [13], and understanding the various aspects of the theory of ideal clutters is one of the long-standing open research directions in the area: 11 of the 18 conjectures in the book *Combinatorial Optimization. Packing and Covering* [10] are directly about general or special instances of ideal clutters.

**Multipartite uniform clutters.** In this paper we introduce a novel approach to discover and understand ideal clutters, by studying the notion of *multipartite uniform clutters* defined as follows. A multipartite uniform clutter  $\mathcal{C}$  is obtained as a family of hyperedges of an  $n$ -partite hypergraph whose vertices are partitioned into  $n$  nonempty disjoint subsets  $V_1, \dots, V_n$  for some  $n \geq 1$ , and every hyperedge intersects each of the subsets exactly once. Then all members of  $\mathcal{C}$  have an equal size  $n$ , and therefore,  $\mathcal{C}$  is *uniform* and a *clutter*. In particular, in a multipartite uniform clutter, the size of a member is equal to the number of partitions. For example,  $Q_6$ , the clutter of triangles in  $K_4$  given by  $Q_6 := \{\{1, 3, 5\}, \{1, 4, 6\}, \{2, 3, 6\}, \{2, 4, 5\}\}$ , is a 3-partite 3-uniform clutter over ground set  $\{1, \dots, 6\}$  partitioned into  $\{1, 2\} \cup \{3, 4\} \cup \{5, 6\}$ . The class of multipartite uniform clutters looks restricted, but in fact, it is general enough to understand the entire class of ideal clutters. More precisely, it was shown in [4] that if we had a characterization of when a multipartite uniform clutter is ideal, then this would in turn completely characterize ideal clutters. This is because any given clutter can be “locally embedded” in a multipartite uniform clutter [4], and we will discuss related ideas in Section 2. This connection allows us to take a different angle on understanding idealness by studying multipartite uniform clutters.

**Vector spaces over  $GF(q)$ .** Thanks to their special structure, one may take advantage of a geometric framework for constructing multipartite uniform clutters. To explain it, take a prime power  $q$  and  $GF(q)$ , the *Galois field of order  $q$* . For convention, we denote by 0 and 1 the additive and multiplicative identities of  $GF(q)$ , respectively. When  $q$  is a power of a prime number  $p$ , we call  $p$  the *characteristic* of  $GF(q)$ .  $GF(q)^n$  for some  $n \geq 1$  is the set of  $n$ -dimensional vectors whose coordinates are in  $GF(q)$  and is called a *coordinate space*. We say that any vector subspace of the coordinate space over  $GF(q)$  is a *coordinate subspace*. Throughout the paper, we refer to a coordinate subspace over  $GF(q)$  as a *vector space over  $GF(q)$*  or simply as a coordinate subspace. For any vector space  $S \subseteq GF(q)^n$  over  $GF(q)$ , there exists a matrix  $A$  whose entries are in  $GF(q)$  such that  $S = \{x \in GF(q)^n : Ax = \mathbf{0}\}$  where  $\mathbf{0}$  denotes the vector of all zeros of appropriate dimension and all equalities in the system  $Ax = \mathbf{0}$  are over  $GF(q)$ . Given the coordinate subspace  $S$ , we construct a multipartite uniform clutter in the following way. Taking  $n$  disjoint copies  $V_1, \dots, V_n$  of  $GF(q)$ , we can view  $GF(q)^n$  as  $V_1 \times \dots \times V_n$  so that  $S$  is a subset of  $V_1 \times \dots \times V_n$ . The *multipartite uniform clutter of  $S$*  is the clutter over ground set  $V_1 \cup \dots \cup V_n$

defined by

$$\text{mult}(S) := \{\{x_1, \dots, x_n\} : (x_1, \dots, x_n) \in S, x_i \in V_i \text{ for } i \in [n]\}.$$

Here, the size of a member equals the number of partitions  $n$ , and  $\text{mult}(S)$  is an  $n$ -partite  $n$ -uniform clutter. For example,  $R_{1,1} := \{(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)\}$  is a vector space over  $GF(2)$ , and  $R_{1,1}$  is equivalent to  $\{(1, 3, 5), (1, 4, 6), (2, 3, 6), (2, 4, 5)\} \subseteq \{1, 2\} \times \{3, 4\} \times \{5, 6\}$ . So,  $\text{mult}(R_{1,1})$  is isomorphic<sup>1</sup> to  $Q_6$ . There is a one-to-one correspondence between the members of  $\text{mult}(S)$  and the vectors in  $S$ . Although we focus on vector spaces over a finite field, we remark that the definition of multipartite uniform clutters extends to any subset of the direct product of finite groups. We discuss this further in Section 2.

**Binary spaces.** Abdi, Cornuéjols, Guričanová, and Lee [4] considered vector spaces over  $GF(2)$ , often referred to as *binary spaces*, and provided a characterization of when their multipartite uniform clutters are ideal. For example,  $\text{mult}(R_{1,1}) = Q_6$  is ideal [33]. The characterization is in terms of *clutter minors*, or simply *minors*. Given a clutter  $\mathcal{C}$  over ground set  $V$  and disjoint subsets  $I, J$  of  $V$ , we define  $\mathcal{C} \setminus I/J$  as the clutter over  $V - (I \cup J)$  that consists of the minimal sets of  $\{C - J : C \in \mathcal{C}, C \cap I = \emptyset\}$ , and we say that  $\mathcal{C} \setminus I/J$  is *the minor of  $\mathcal{C}$  obtained after deleting  $I$  and contracting  $J$* . We call it a *proper minor* if  $I \cup J \neq \emptyset$ . It is well-known that if a clutter is ideal, then so is every minor [33]. It was proved in [4] that for a vector space  $S$  over  $GF(2)$ ,  $\text{mult}(S)$  is ideal if and only if  $\text{mult}(S)$  has none of three special clutters as a minor if and only if the binary matroid corresponding to  $S$  has the so-called sums of circuits property.

**Our results I.** Motivated by the result of [4] mentioned above, given a vector space  $S$  over an arbitrary finite field  $GF(q)$ , when is  $\text{mult}(S)$  ideal? In this paper, we completely answer this question. We divide our analysis into three cases. First, we consider prime powers that are odd, secondly the  $q = 4$  case, and thirdly powers of 2 greater than 4. What follows is a summary of our main results for the three cases.

For our first result, we need two more definitions. The *support* of a vector  $x \in GF(q)^n$  is defined as  $\text{support}(x) := \{i \in [n] : x_i \neq 0\}$ . Moreover, denote by  $\Delta_3$  the clutter over ground set  $\{1, 2, 3\}$  whose members are  $\{1, 2\}, \{2, 3\}, \{3, 1\}$ . Notice that  $\Delta_3$  is the clutter of edges in a triangle and that  $\Delta_3$  is non-ideal because  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  is a fractional extreme point of the associated set covering polyhedron  $Q(\Delta_3)$ .

**Theorem 1.1** (proved in Section 4). *Take an odd prime power  $q$ , and let  $S$  be a vector space over  $GF(q)$ . Then the following statements are equivalent:*

- (i)  $\text{mult}(S)$  is ideal,
- (ii)  $S$  admits a basis with vectors of pairwise disjoint supports,
- (iii)  $\text{mult}(S)$  contains no  $\Delta_3$  as a minor.

The case of  $GF(4)$  allows more general structures in the vector space. We say that row vectors  $v^1, \dots, v^r$  with

---

<sup>1</sup>Given clutters  $\mathcal{C}, \mathcal{C}'$ , we say that  $\mathcal{C}$  is *isomorphic* to  $\mathcal{C}'$  and write  $\mathcal{C} \cong \mathcal{C}'$  if  $\mathcal{C}'$  can be obtained from  $\mathcal{C}$  after relabeling the elements of  $\mathcal{C}$ .

$r \geq 2$  form a *sunflower* if, after permuting the coordinates, the vectors are of the form

$$\begin{array}{c} v^1 \\ v^2 \\ \vdots \\ v^r \end{array} \left[ \begin{array}{c|c|c|c|c} u^0 & u^1 & \mathbf{0} & \cdots & \mathbf{0} \\ u^0 & \mathbf{0} & u^2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u^0 & \mathbf{0} & \mathbf{0} & \cdots & u^r \end{array} \right]$$

where  $u^0, u^1, \dots, u^r$  are some row vectors with nonzero entries and  $\mathbf{0}$  denotes a row vector of all zeros of appropriate length.

**Theorem 1.2** (proved in Section 7). *Let  $S$  be a vector space over  $GF(4)$ . Then the following statements are equivalent:*

- (i)  $\text{mult}(S)$  is ideal,
- (ii)  $S = S_1 \times \cdots \times S_k$  where each  $S_i$  has dimension at most 1 or admits a sunflower basis,
- (iii)  $\text{mult}(S)$  contains no  $\Delta_3$  as a minor.

Lastly, for the case when  $q$  is a power of 2 greater than 4, we define another small non-ideal clutter.  $C_5^2$  is the clutter over ground set  $\{1, \dots, 5\}$  whose members are  $\{1, 2\}, \{2, 3\}, \{3, 4\}, \{4, 5\}, \{5, 1\}$ .  $C_5^2$  is the clutter of edges in a cycle of length 5, and notice that  $C_5^2$  is non-ideal because  $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$  is a fractional extreme point of the associated polyhedron  $Q(C_5^2)$ .

**Theorem 1.3** (proved in Section 8). *Let  $q$  be a power of 2 such that  $q > 4$ , and let  $S$  be a vector space over  $GF(q)$ . Then the following statements are equivalent:*

- (i)  $\text{mult}(S)$  is ideal,
- (ii)  $S$  admits a basis with vectors of pairwise disjoint supports,
- (iii)  $\text{mult}(S)$  contains no  $C_5^2$  as a minor.

Theorem 1.1, Theorem 1.2, and Theorem 1.3 lead to the conclusion that when  $q$  is a prime power other than 2, the class of coordinate subspaces whose multipartite uniform clutter is ideal has restricted structures. Nevertheless, the main takeaway of this paper is that we propose a novel framework to study and generate idealness by multipartite uniform clutters and complete the analysis of the natural class of multipartite uniform clutters obtained from coordinate subspaces. Our analysis is based on sophisticated interplays between clutters and underlying matroids.

**Our results II.** We take one step further to understand the *max-flow min-cut (MFMC) property* [33] for the multipartite uniform clutters from coordinate subspaces. While the idealness of a clutter corresponds to the integrality of the associated set covering polyhedron, the MFMC property is the analogue of *total dual integrality* [16, 19]. To formalize this, given a clutter  $\mathcal{C}$  over ground set  $V$  with weights  $w \in \mathbb{Z}_+^V$ , we consider  $\tau(\mathcal{C}, w) := \min\{w^\top x : M(\mathcal{C})x \geq \mathbf{1}, x \in \mathbb{Z}_+^V\}$  and  $\nu(\mathcal{C}, w) := \max\{\mathbf{1}^\top y : M(\mathcal{C})^\top y \leq w, y \in \mathbb{Z}_+^{\mathcal{C}}\}$ . Note that  $\tau(\mathcal{C}, w)$  computes the minimum weight of a cover of  $\mathcal{C}$ , whereas  $\nu(\mathcal{C}, w)$  computes the maximum size of a *packing* of members of  $\mathcal{C}$  such that each element  $v$  appears in at most  $w_v$  members in the packing. Here, we say that  $\mathcal{C}$  has

the MFMC property if  $\tau(\mathcal{C}, w) = \nu(\mathcal{C}, w)$  holds for every  $w \in \mathbb{Z}_+^V$ . Hence, the MFMC property of  $\mathcal{C}$  is equivalent to the total dual integrality of the linear system  $M(\mathcal{C})x \geq \mathbf{1}, x \geq \mathbf{0}$ , and therefore it follows that the MFMC property implies idealness. The following result provides a complete characterization of the MFMC property for the multipartite uniform clutters from vector spaces.

**Theorem 1.4** (proved in Section 4). *Take any prime power  $q$ , and let  $S$  be a vector space over  $GF(q)$ . Then the following statements are equivalent:*

- (i) *mult( $S$ ) has the max-flow min-cut property,*
- (ii)  *$S$  admits a basis with vectors of pairwise disjoint supports,*
- (iii) *mult( $S$ ) has none of  $\Delta_3, Q_6$  as a minor.*

As a corollary, idealness and the MFMC property coincide when  $q$  is an odd prime power or  $q$  is a power of 2 greater than 4. In contrast, there is an example of a vector space over  $GF(4)$  whose multipartite uniform clutter is ideal but does not have the MFMC property. We demonstrate this example in Section 9. Theorem 1.4 also has a consequence on the *Replication Conjecture*, proposed by Conforti and Cornuéjols [9]. In particular, the Replication Conjecture is a set covering analogue of the Duplication Lemma for perfect graphs [24].

**Corollary 1.5** (proved in Section 9). *The Replication Conjecture holds true for the class of multipartite uniform clutters from coordinate subspaces.*

Another corollary of Theorem 1.4 is on the  $\tau = 2$  Conjecture, proposed by Cornuéjols, Guenin, and Margot [11]. They showed that if the  $\tau = 2$  Conjecture holds, then so does the Replication Conjecture [11], providing a way of tackling the Replication Conjecture.

**Corollary 1.6** (proved in Section 9). *The  $\tau = 2$  Conjecture holds true for the class of multipartite uniform clutters from coordinate subspaces.*

We will formally state the Replication Conjecture and the  $\tau = 2$  Conjecture along with the proofs of Corollary 1.5 and Corollary 1.6 in Section 9.

**Summary and organizations of the paper.** This paper provides a complete characterization of when the multipartite uniform clutter of a coordinate subspace is ideal and when it has the MFMC property. The proofs of our main results are based on applications of the theory of ideal clutters and matroid theory. Tools from ideal clutters and matroid theory are presented in Section 2 and Section 3, respectively.

The first result we prove in this paper is Theorem 1.4 which characterizes the MFMC property of the multipartite uniform clutter of a vector space over  $GF(q)$  for any prime power  $q$ . In fact, Theorem 1.1 for the idealness under an odd prime power  $q$  shares much of the proof with Theorem 1.4. Hence, we prove the two theorems in Section 4.

For the idealness under the case of powers of 2, we need more techniques. In Section 5, we provide some properties of the underlying matroid of a vector space over  $GF(2^k)$  for  $k \geq 2$ . In Section 6, we develop some tools for understanding vector spaces of a certain structure that appear for the case of powers of 2. We divide



Then  $S \cong g(S)$  and  $\text{mult}(S) \cong \text{mult}(g(S))$ .

**Products of set systems and clutters.** Take two integers  $n_1, n_2 \geq 1$ . Let  $V_1, \dots, V_{n_1}$  be  $n_1$  nonempty sets, and let  $S_1$  be a subset of  $V_1 \times \dots \times V_{n_1}$ . Let  $U_1, \dots, U_{n_2}$  be  $n_2$  nonempty sets, and let  $S_2$  be a subset of  $U_1 \times \dots \times U_{n_2}$ . Recall that the product of  $S_1$  and  $S_2$  is defined as  $S_1 \times S_2 = \{(x_1, x_2) : x_1 \in S_1, x_2 \in S_2\}$ . We also define products of clutters. Let  $\mathcal{C}_1, \mathcal{C}_2$  be two clutters over disjoint ground sets  $E_1, E_2$ . The *product of  $\mathcal{C}_1$  and  $\mathcal{C}_2$* , denoted  $\mathcal{C}_1 \times \mathcal{C}_2$ , is defined as the clutter over ground set  $E_1 \cup E_2$  whose members are  $\mathcal{C}_1 \times \mathcal{C}_2 = \{C_1 \cup C_2 : C_1 \in \mathcal{C}_1, C_2 \in \mathcal{C}_2\}$ . Having defined the product of two clutters, we define the product of two multipartite uniform clutters  $\text{mult}(S_1)$  and  $\text{mult}(S_2)$ . In fact, we can show the following:

**Lemma 2.3.** *The following statements hold:*

1.  $\text{mult}(S_1) \times \text{mult}(S_2) = \text{mult}(S_1 \times S_2)$ .
2. Let  $\mathcal{C}_1, \mathcal{C}_2$  be clutters over disjoint ground sets. If  $\mathcal{C}_1, \mathcal{C}_2$  have the idealness (resp. MFMC) property, then so does  $\mathcal{C}_1 \times \mathcal{C}_2$ .
3. Take two integers  $n_1, n_2 \geq 1$ . Let  $V_1, \dots, V_{n_1}$  be  $n_1$  nonempty sets, and let  $S_1$  be a subset of  $V_1 \times \dots \times V_{n_1}$ . Let  $U_1, \dots, U_{n_2}$  be  $n_2$  nonempty sets, and let  $S_2$  be a subset of  $U_1 \times \dots \times U_{n_2}$ . If  $\text{mult}(S_1), \text{mult}(S_2)$  are ideal, then so is  $\text{mult}(S_1 \times S_2)$ .

*Proof.* **(1)** Let  $C_1 \in \text{mult}(S_1)$  and  $C_2 \in \text{mult}(S_2)$ . Then  $C_1 = \{x_1, \dots, x_{n_1}\}$  for some  $x = (x_1, \dots, x_{n_1}) \in S_1$  and  $C_2 = \{y_1, \dots, y_{n_2}\}$  for some  $y = (y_1, \dots, y_{n_2}) \in S_2$ . Moreover,  $(x, y) \in S_1 \times S_2$  and  $C_1 \cup C_2 \in \text{mult}(S_1 \times S_2)$ . Similarly, we can show that if  $C \in \text{mult}(S_1 \times S_2)$ , then  $C = C_1 \cup C_2$  for some  $C_1 \in \text{mult}(S_1)$  and  $C_2 \in \text{mult}(S_2)$ . Therefore, we obtain  $\text{mult}(S_1) \times \text{mult}(S_2) = \text{mult}(S_1 \times S_2)$ . **(2)** is routine and an argument can be found in ([4], §5). **(3)** follows from (1) and (2).  $\square$

So, if a set can be represented as the product of some smaller sets, we can check if its multipartite uniform clutter is ideal by studying the smaller sets and their multipartite uniform clutters. In particular, we will use this proposition to show implication **(iii)**→**(i)** in Theorem 1.1, Theorem 1.2, and Theorem 1.3.

**Projection and restriction of set systems.** Take an integer  $n \geq 1$ . Let  $V_1, \dots, V_n$  be  $n$  nonempty sets, and let  $S$  be a subset of  $V_1 \times \dots \times V_n$ . Given  $J \subseteq [n]$  and  $x \in S$ ,  $x/J$  denote the subvector of  $x$  that consists of the coordinates not in  $J$ . For  $J \subseteq [n]$ , the set obtained from  $S$  after *dropping* the coordinates in  $J$  is  $\{x/J : x \in S\}$ . We will refer to a set obtained from  $S$  after dropping some coordinates as a *projection* of  $S$ . Next, let  $U_i$  be a nonempty subset of  $V_i$  for  $i \in [n]$ . Here,  $U_i$  need not be a proper subset of  $V_i$ . Then the set obtained from  $S$  after *restricting* to  $U_1 \times \dots \times U_n$  is what is obtained from  $S \cap (U_1 \times \dots \times U_n)$  after dropping the coordinates where the points in  $S \cap (U_1 \times \dots \times U_n)$  agree on. We will refer to a set obtained from  $S$  after restricting  $S$  to some subset of  $V_1 \times \dots \times V_n$  as a *restriction* of  $S$ .

**Lemma 2.4.** *Let  $S'$  be a set that is either a projection or a restriction of  $S$ . Then  $\text{mult}(S')$  is a minor of  $\text{mult}(S)$ .*

*Proof.* Suppose first that  $S'$  is a projection, say for some  $J \subseteq [n]$ ,  $S'$  is obtained from  $S$  after dropping the

coordinates of  $J$ . Then  $\text{mult}(S')$  is the minor of  $\text{mult}(S)$  obtained after contracting the elements in  $V_j$  for  $j \in J$ .

Suppose next that  $S'$  is a restriction, say for some nonempty subset  $U_1 \times \cdots \times U_n$  of  $V_1 \times \cdots \times V_n$ ,  $S'$  is obtained after restricting  $S$  to  $U_1 \times \cdots \times U_n$ . Then  $\text{mult}(S')$  is the minor of  $\text{mult}(S)$  obtained after deleting the elements in  $(V_i \setminus U_i)$  for  $i \in [n]$  and contracting the elements in  $V_j$  for  $j \in J$  where  $J$  is the set of coordinates where the points in  $S \cap (U_1 \times \cdots \times U_n)$  agree on.  $\square$

**Localizations.** We mentioned before that a clutter is ideal if and only if every minor of it is ideal. In this section, we will define and study *localizations* that appear as a minor of a multipartite uniform clutter.

**Definition 2.5.** *Given a multipartite uniform clutter  $\mathcal{C}$  whose ground set is partitioned into non-empty parts  $V_1, \dots, V_n$ , a localization of  $\mathcal{C}$  is any minor obtained from  $\mathcal{C}$  after contracting precisely one element from each  $V_i$ .*

Thus, a localization of  $\mathcal{C}$  is obtained after contracting  $v_1, \dots, v_n$  for some  $v = (v_1, \dots, v_n) \in V_1 \times \cdots \times V_n$ . As  $\mathcal{C} = \text{mult}(S)$  for some  $S \subseteq V_1 \times \cdots \times V_n$  by Remark 2.1, the localization is equal to

$$\begin{aligned} \text{local}(S, v) &:= \text{mult}(S) / \{v_1, \dots, v_n\} \\ &= \{\text{the minimal sets of } \{\{x_1, \dots, x_n\} - \{v_1, \dots, v_n\} : (x_1, \dots, x_n) \in S\}\}. \end{aligned}$$

We call  $\text{local}(S, v)$  the *localization of  $\text{mult}(S)$  with respect to  $v$* . So, every localization of  $\mathcal{C}$  is equal to  $\text{local}(S, v)$  for some  $v$  and that  $\text{local}(S, v) = \{\emptyset\}$  if  $v \in S$ . In [4], localizations of a cuboid are referred to as *induced clutters*.

It turns out that a multipartite uniform clutter is ideal if and only if all localizations are ideal; let us prove this in the remainder of this section. We say that a clutter is *minimally non-ideal* if it is non-ideal but every proper minor of it is ideal. We need the following lemma.

**Lemma 2.6.** *Let  $\mathcal{C}$  be a minimally non-ideal clutter, and let  $V$  denote the ground set of  $\mathcal{C}$ . Then there is no subset  $U$  of  $V$  satisfying  $|C \cap U| = 1$  for every member  $C$  of  $\mathcal{C}$ .*

*Proof.* Since  $\mathcal{C}$  is non-ideal,  $P(\mathcal{C}) = \{\mathbf{1} \geq x \geq \mathbf{0} : M(\mathcal{C})x \geq \mathbf{1}\}$  has a fractional extreme point  $x^*$ . Let  $v \in V$ . Notice that  $P(\mathcal{C}/v)$  and  $P(\mathcal{C} \setminus v)$  are obtained from  $P(\mathcal{C}) \cap \{x : x_v = 0\}$  and  $P(\mathcal{C}) \cap \{x : x_v = 1\}$  after projecting out the variable  $x_v$ . As  $\mathcal{C}/v$  and  $\mathcal{C} \setminus v$  are ideal,  $P(\mathcal{C}/v)$  and  $P(\mathcal{C} \setminus v)$  are integral. Then both  $P(\mathcal{C}) \cap \{x : x_v = 0\}$  and  $P(\mathcal{C}) \cap \{x : x_v = 1\}$  are integral, implying in turn that  $x^*$  does not belong to any of these two. So, it follows that  $0 < x_v^* < 1$  for each  $v \in V$ . Now, consider a nonsingular row submatrix  $A$  of  $M(\mathcal{C})$  such that  $Ax^* = \mathbf{1}$ . Suppose that  $V$  has a subset  $U$  such that  $|C \cap U| = 1$  for every member  $C$  of  $\mathcal{C}$ . Let  $\chi_U$  denote the characteristic vector of  $U$  in  $\{0, 1\}^V$ . Since  $|C \cap U| = 1$  for every member  $C$  of  $\mathcal{C}$ , we have that  $M(\mathcal{C})\chi_U = \mathbf{1}$  and thus  $A\chi_U = \mathbf{1}$ . Since  $A$  is nonsingular,  $Ax = \mathbf{1}$  has a unique solution, so it follows that  $x^* = \chi_U$ , a contradiction. Therefore, there is no such subset  $U$  of  $V$ , as required.  $\square$

**Theorem 2.7.** *A multipartite uniform clutter is ideal if and only if all of its localizations are ideal.*

*Proof.* Let  $\mathcal{C}$  be a multipartite uniform clutter whose ground set is partitioned into nonempty parts  $V_1, \dots, V_n$ . ( $\Rightarrow$ ) If  $\mathcal{C}$  is ideal, every minor of  $\mathcal{C}$  is ideal, and so are all of its localizations. ( $\Leftarrow$ ) Assume that  $\mathcal{C}$  is non-ideal. Then it has a minimally non-ideal minor  $\mathcal{C}' := \mathcal{C} \setminus I/J$  obtained after deleting  $I$  and contracting  $J$  for some



disjoint subsets  $I, J \subseteq V_1 \cup \dots \cup V_n$ . Observe that  $\mathcal{C} \setminus I$  is another multipartite uniform clutter whose ground set is partitioned into nonempty parts  $U_1, \dots, U_n$  where  $U_i := V_i \setminus I$  for  $i \in [n]$ . In particular, every member  $C$  of  $\mathcal{C} \setminus I$  satisfies  $|C \cap U_i| = 1$  for  $i \in [n]$ . Suppose that  $J \cap U_i = \emptyset$  for some  $i \in [n]$ . Then  $|(C - J) \cap U_i| = |C \cap U_i| = 1$  for every member  $C$  of  $\mathcal{C} \setminus I$ . As  $\mathcal{C}'$  is obtained after contracting  $J$  from  $\mathcal{C} \setminus I$ , we have  $|C' \cap U_i| = 1$  for every member  $C'$  of  $\mathcal{C}'$ . This contradicts Lemma 2.6 due to our assumption that  $\mathcal{C}'$  is minimally non-ideal. Therefore, for each  $i \in [n]$ ,  $J \cap U_i \neq \emptyset$ , so we have that  $J \cap V_i \neq \emptyset$ . Then,  $\mathcal{C}'$  is a minor of a localization. Therefore, one of  $\mathcal{C}$ 's localizations is non-ideal, as required.  $\square$

In contrast to idealness, even if all localizations have the MFMC property, a multipartite uniform clutter may not have the MFMC property. For example, all localizations of  $Q_6 = \text{mult}(R_{1,1})$  are isomorphic to the clutter over ground set  $\{1, 2, 3\}$  whose members are  $\{1\}, \{2\}, \{3\}$ . The clutter over 3 elements trivially has the MFMC property, but  $Q_6$  does not [23, 33].

### 3 Vector spaces, matroids, and sunflower bases

Take a prime power  $q$ , and consider the Galois field  $GF(q)$  of order  $q$ , with additive and multiplicative identities denoted as 0 and 1, respectively. Take an integer  $n \geq 1$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ .

We assume basic knowledge of Matroid Theory throughout this paper (see [27] for reference) though we recall matroid theoretic notions as needed. Let us observe a routine way to associate a  $GF(q)$ -represented matroid to the vector space  $S$ . Let  $A$  be a matrix over  $n$  columns with entries in  $GF(q)$  such that  $S = \{x \in GF(q)^n : Ax = \mathbf{0}\}$ , where the equality in the linear system  $Ax = \mathbf{0}$  holds over  $GF(q)$ . The *underlying matroid of  $S$* , denoted  $\text{Matroid}(S)$ , is the matroid represented by  $A$  over  $GF(q)$ . The *dimension* of vector space  $S$  is defined as the maximum number of linearly independent vectors in  $S$  over  $GF(q)$ . Note that

$$\text{the dimension of } S = n - \text{rank}(A) = n - \text{rank}(\text{Matroid}(S))$$

where  $\text{rank}(A)$  is the matrix rank of  $A$  over  $GF(q)$  and  $\text{rank}(\text{Matroid}(S))$  is the matroid rank of  $\text{Matroid}(S)$  over  $GF(q)$ . Although the representation matrix  $A$  is not unique for vector space  $S$ , our terminology suggests that  $\text{Matroid}(S)$  is. The remark below justifies this.

**Remark 3.1.** *Take a prime power  $q$ , and let  $S$  be a vector space over  $GF(q)$ . Then the clutter of circuits of  $\text{Matroid}(S)$  is the set of inclusion-wise minimal members of  $\{\text{support}(x) : x \in S, x \neq \mathbf{0}\}$ .*

Given vectors  $v^1, \dots, v^r \in GF(q)^n$ , let  $\langle v^1, \dots, v^r \rangle := \left\{ \sum_{i \in [r]} \lambda_i v^i : \lambda_i \in GF(q) \text{ for } i \in [r] \right\}$ , where addition is done over  $GF(q)$ . The set  $\langle v^1, \dots, v^r \rangle$ , which we call the *span* of the vectors, is a vector space over  $GF(q)$ . A *basis* of a vector space  $S$  is an inclusion-wise minimal set of vectors whose span is  $S$ . In this section, we characterize in terms of the underlying matroid when a vector space is spanned by a set of vectors of disjoint supports, or a set of vectors that form a sunflower.

**Matroid minors.** We start by arguing that matroid deletions and contractions in  $\text{Matroid}(S)$  correspond to restrictions and projections in  $S$ . For a matroid  $\mathcal{M}$  and disjoint subsets  $I, J$  of the ground set of  $\mathcal{M}$ , we denote

by  $\mathcal{M} \setminus I/J$  the matroid minor of  $\mathcal{M}$  obtained after deleting  $I$  and contracting  $J$ . Let  $\mathcal{C}(\mathcal{M})$  denote the clutter of circuits of  $\mathcal{M}$ .

**Lemma 3.2.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Then  $\text{Matroid}(S) \setminus I/J$  for some disjoint  $I, J \subseteq [n]$  is precisely  $\text{Matroid}(S')$  where  $S' \subseteq GF(q)^{n-|I|-|J|}$  is the vector space over  $GF(q)$  obtained from  $S \cap \{x \in GF(q)^n : x_i = 0 \forall i \in I\}$  after dropping coordinates in  $I \cup J$ .*

*Proof.* It is clear that  $S'$  is a vector space over  $GF(q)$ , so  $\text{Matroid}(S')$  is well-defined. To show that  $\text{Matroid}(S) \setminus I/J = \text{Matroid}(S')$ , we will argue that  $\mathcal{C}(\text{Matroid}(S) \setminus I/J) = \mathcal{C}(\text{Matroid}(S'))$ .

If  $\mathcal{C}(\text{Matroid}(S) \setminus I/J) = \emptyset$ , then every  $C \in \mathcal{C}(\text{Matroid}(S))$  intersects  $I$ , which means that  $\text{support}(x)$  intersects  $I$  for every  $x \in S - \{\mathbf{0}\}$ . This implies that  $S' = \{\mathbf{0}\}$ , in which case  $\mathcal{C}(\text{Matroid}(S')) = \emptyset$ . Thus we may assume that  $\mathcal{C}(\text{Matroid}(S) \setminus I/J) \neq \emptyset$ .

Let  $C_1 \in \mathcal{C}(\text{Matroid}(S) \setminus I/J)$ . Then there exists  $C \in \mathcal{C}(\text{Matroid}(S))$  such that  $C \cap I = \emptyset$  and  $C_1 = C - J$ . Then  $C = \text{support}(x)$  for some  $x \in S$  by the definition of  $\text{Matroid}(S)$  (see also Remark 3.1). As  $C \cap I = \emptyset$ , it follows that  $x_i = 0$  for  $i \in I$ , which implies that there exists  $x' \in S' - \{\mathbf{0}\}$  such that  $\text{support}(x') = \text{support}(x) - J = C - J$ . So, there exists  $C_2 \in \mathcal{C}(\text{Matroid}(S'))$  such that  $C_2 \subseteq C_1$ . Therefore, every member of  $\mathcal{C}(\text{Matroid}(S) \setminus I/J)$  contains a member of  $\mathcal{C}(\text{Matroid}(S'))$ .

Let  $C_2 \in \mathcal{C}(\text{Matroid}(S'))$ . Then  $C_2 = \text{support}(x')$  for some  $x' \in S'$  by Remark 3.1. This implies that there is some  $x \in S$  such that  $x_i = 0$  for  $i \in I$  and  $\text{support}(x) - J = \text{support}(x')$ . Since  $\text{support}(x)$  contains a circuit of  $\text{Matroid}(S)$  and  $\text{support}(x) \cap I = \emptyset$ , it follows that  $C_2 = \text{support}(x')$  contains a circuit of  $\text{Matroid}(S) \setminus I/J$ . Therefore, we deduce that  $\mathcal{C}(\text{Matroid}(S) \setminus I/J) = \mathcal{C}(\text{Matroid}(S'))$ , as required.  $\square$

**Direct sum.** Consider matroids  $M_1, \dots, M_\ell$  over pairwise disjoint ground sets  $E_1, \dots, E_\ell$  and independent set families  $\mathcal{I}_1, \dots, \mathcal{I}_\ell$ , respectively. The *direct sum* of  $M_1, \dots, M_\ell$ , denoted  $M_1 \oplus \dots \oplus M_\ell$ , is the matroid over ground set  $E_1 \cup \dots \cup E_\ell$  whose independent set family is  $\{I_1 \cup \dots \cup I_\ell : I_i \in \mathcal{I}_i, i \in [\ell]\}$ . We shall need the following basic remark about the direct sum of matroids. For the remark, we need to recall two notions. First, a *block* of a graph  $G$  is any maximal vertex-induced subgraph of  $G$  that is 2-vertex-connected. Secondly, we denote the *cycle matroid* of a graph  $G$  by  $\text{Matroid}(G)$ . Finally, we say that a vector space  $S$  is the *product* of vector spaces  $S_1$  and  $S_2$  if  $S = \{(x, y) : x \in S_1, y \in S_2\} =: S_1 \times S_2$ .

**Lemma 3.3.** *The following statements hold:*

1. *Let  $G$  be a graph, and let  $G_1, \dots, G_k$  be the blocks of  $G$ . Then  $\text{Matroid}(G) = \text{Matroid}(G_1) \oplus \dots \oplus \text{Matroid}(G_k)$ .*
2. *Take a prime power  $q$  and two  $GF(q)$ -representable matroids  $M_1, M_2$  over disjoint ground sets. If  $A_1$  and  $A_2$  are  $GF(q)$ -representations of  $M_1$  and  $M_2$ , respectively, then  $M_1 \oplus M_2$  can be represented by  $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ .*
3. *Take a prime power  $q$  and a vector space  $S$  over  $GF(q)$ . Then  $S = S_1 \times S_2$  for some vector spaces  $S_1, S_2$  over  $GF(q)$  if and only if  $\text{Matroid}(S) = \text{Matroid}(S_1) \oplus \text{Matroid}(S_2)$ .*

*Proof.* (1), (2): See Chapters 4.1 and 4.2 of [27]. (3) follows immediately from (2).  $\square$

**Disjoint supports basis.**

**Lemma 3.4.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Then the following statements are equivalent:*

- (i)  $\text{Matroid}(S) = \text{Matroid}(G)$  where every block of  $G$  is either a bridge or a circuit,
- (ii)  $S = \langle v^1, \dots, v^r \rangle$  where  $v^1, \dots, v^r \in GF(q)^n$  have pairwise disjoint supports,
- (iii)  $S = S_1 \times \dots \times S_k$  where each  $S_i$  has dimension at most 1.

*Proof.* It can be readily checked that (ii) and (iii) are equivalent. The equivalence of (i) and (iii) follows from the fact that for a vector space  $T$  over  $GF(q)$ ,  $T = \{0\}$  if and only if  $\text{Matroid}(T)$  is the cycle matroid of a bridge, and  $T$  has dimension 1 if and only if  $\text{Matroid}(T)$  is the cycle matroid of a circuit.  $\square$

**Sunflower basis.** Given an integer  $t \geq 3$ , denote by  $A_t$  the graph that consists of two vertices and  $t$  parallel edges connecting them.

**Lemma 3.5.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $T \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Then  $\text{Matroid}(T)$  is the cycle matroid of a subdivision of  $A_t$  for some  $t \geq 3$  if and only if  $T$  is generated by a sunflower basis.*

*Proof.* ( $\Rightarrow$ ): Assume that  $\text{Matroid}(T) = \text{Matroid}(G)$  where  $G$  is a subdivision of  $A_t$  for some  $t \geq 3$ . Notice that  $G$  consists of two vertices and  $t$  internally vertex-disjoint paths connecting them. Let  $P_0, \dots, P_{t-1}$  denote the paths, and let  $E(P_0), \dots, E(P_{t-1})$  denote their edge sets. Then it follows from Remark 3.1 that  $T$  contains a point whose support is  $E(P_0) \cup E(P_i)$ . Therefore,  $T$  contains  $t-1$  points  $v^1, \dots, v^{t-1}$  (in row vectors) of the following form:

$$\begin{array}{c}
 v^1 \\
 v^2 \\
 \vdots \\
 v^{t-1}
 \end{array}
 \left[
 \begin{array}{c|c|c|c|c}
 u_1^0 & u^1 & \mathbf{0} & \cdots & \mathbf{0} \\
 u_2^0 & \mathbf{0} & u^2 & \cdots & \mathbf{0} \\
 \vdots & \vdots & \vdots & \vdots & \vdots \\
 u_{t-1}^0 & \mathbf{0} & \mathbf{0} & \cdots & u^{t-1}
 \end{array}
 \right]$$

where  $u_1^0, \dots, u_{t-1}^0 \in GF(q)^{|E(P_0)|}$  and  $u^i \in GF(q)^{|E(P_i)|}$  for  $i \in [n]$  are vectors of nonzero entries. As  $T$  is a vector space in  $GF(q)^n$ ,  $\text{Matroid}(T)$  is over  $n$  edges, and therefore,  $G$  has  $n$  edges. Since  $G$  is a subdivision of  $A_t$ , a spanning tree of  $G$  has  $n - (t-1)$  edges, which means that  $\text{Matroid}(T) = \text{Matroid}(G)$  has rank  $n - (t-1)$ . Then the dimension of  $T$  is  $n - \text{Matroid}(T) = t-1$ , so we have  $T = \langle v^1, \dots, v^{t-1} \rangle$ . Now, let us argue that we may assume that  $u_1^0 = \dots = u_{t-1}^0$  without loss of generality. As  $P_1 \cup P_2$  is a circuit of  $G$ , Remark 3.1 implies that there is a point  $v \in T$  whose support is  $E(P_1) \cup E(P_2)$ . Then  $v$  can be written as  $v = \mu_1 v^1 + \mu_2 v^2$  for some  $\mu_1, \mu_2 \in GF(q) - \{0\}$ . As the support of  $v$  is  $E(P_1) \cup E(P_2)$ , we have that  $\mu_1 u_1^0 + \mu_2 u_2^0 = 0$ , which implies that  $u_2^0 = \lambda_2 u_1^0$  for some nonzero  $\lambda_2$ . Similarly, we obtain  $u_i^0 = \lambda_i u_1^0$  for some nonzero  $\lambda_i$  for  $i \in [t-1]$ , as required. Therefore, after scaling  $v^i$ 's if necessary, we may assume that  $u_1^0 = \dots = u_{t-1}^0$ , as required.

( $\Leftarrow$ ): Suppose  $T = \langle v^1, \dots, v^{t-1} \rangle$  where  $v^1, \dots, v^{t-1} \in GF(q)^n$  are vectors of the following form (in row vectors), after permuting the coordinates, for some  $t \geq 3$ :

$$\begin{array}{c} v^1 \\ v^2 \\ \vdots \\ v^{t-1} \end{array} \left[ \begin{array}{c|c|c|c|c} u^0 & u^1 & \mathbf{0} & \cdots & \mathbf{0} \\ u^0 & \mathbf{0} & u^2 & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ u^0 & \mathbf{0} & \mathbf{0} & \cdots & u^{t-1} \end{array} \right]$$

for some row vectors  $u^0, u^1, \dots, u^{t-1}$  with no zero entries. Let  $E_i$  be the support of  $u^i$  for  $i = 0, 1, \dots, t-1$ . Let  $C$  be a circuit of  $\text{Matroid}(T)$ . Then  $C = \text{support}(x)$  for some  $x \in T$ . Let  $x = \sum_{i=1}^{t-1} \mu_i v^i$ . Then  $x$  is of the form

$$x \left[ \sum_{i=1}^{t-1} \mu_i u^0 \mid \mu_1 u^1 \mid \mu_2 u^2 \mid \cdots \mid \mu_{t-1} u^{t-1} \right]$$

If  $C \cap E_0 \neq \emptyset$ , then it means  $\sum_{i=1}^{t-1} \mu_i \neq 0$ , and therefore,  $C \cap E_0 = E_0$ . This implies that the elements in  $E_0$  are in series. If  $C \cap E_i \neq \emptyset$  for some  $1 \leq i \leq t-1$ , then  $\mu_i \neq 0$ . This indicates that  $C \cap E_i = E_i$ , implying in turn that the elements in  $E_i$  are in series.

Then consider the case where each  $u^i$  is 1-dimensional, under which we have  $E_i = \{e_i\}$  is a singleton for  $i = 0, \dots, t-1$ . Observe that  $|\text{support}(x)| \geq 2$  for any  $x \in T$ . Then none of  $\{e_0\}, \{e_1\}, \dots, \{e_{t-1}\}$  is a circuit. However, we know that  $\{e_0, e_i\}$  for  $i = 1, \dots, t-1$  are circuits of  $\text{Matroid}(T)$  because  $v^1, \dots, v^{t-1} \in T$ . Moreover,  $v^i + (q-1)v^j$  for  $i \neq j$  has support  $\{e_i, e_j\}$ , and therefore,  $\{e_i, e_j\}$  for distinct  $i, j \in \{1, \dots, t-1\}$  are all circuits. Then  $\{\{e_i, e_j\} : i, j \in \{0, 1, \dots, t-1\}, i \neq j\}$  is the family of circuits of  $\text{Matroid}(T)$  because any subset of the ground set of size at least 3 would contain  $\{e_i, e_j\}$  for some  $i \neq j$ . Therefore,  $\text{Matroid}(T)$  is  $\text{Matroid}(A_t)$ .

In general, as the elements of each  $E_i$  are in series,  $\text{Matroid}(T)$  is a series extension of  $\text{Matroid}(A_t)$ , which is equivalent to the cycle matroid of a subdivision of  $A_t$ , as required.  $\square$

### Putting it altogether.

**Corollary 3.6.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Then the following statements are equivalent:*

- (i)  $\text{Matroid}(S) = \text{Matroid}(G)$  where every block of  $G$  is a bridge, a circuit, or a subdivision of  $A_t$  for some  $t \geq 3$ ,
- (ii)  $S = S_1 \times \cdots \times S_k$  where each  $S_i$  has dimension at most 1, or admits a sunflower basis.

## 4 The MFMC property and odd prime powers

Let  $q$  be a power of a prime number  $p$ . Recall that we denote by 0 and 1 the additive and multiplicative identities of  $GF(q)$ . Then there must exist an integer  $\ell$  such that  $a + a + \cdots + a$  ( $\ell$  times) equals 0 for all  $a \in GF(q)$ , and in fact, the smallest of such integers is  $p$ . Here,  $p$  is often referred to as the *characteristic* of  $GF(q)$ . Throughout this paper, we denote by  $-v$  and  $v^{-1}$  the additive and multiplicative inverses of  $v$  for each  $v \in GF(q) - \{0\}$ .

In this section, we prove three lemmas that are useful for this section as well as the next three. Then we prove Theorem 1.4 that characterizes when the multipartite uniform clutter of a vector space has the MFMC property. Lastly, we prove Theorem 1.1 for the case when  $q$  is an odd prime power.

**Lemma 4.1.** *Take an integer  $n \geq 3$  and  $n$  non-empty sets  $V_1, \dots, V_n$ , and let  $S \subseteq V_1 \times \dots \times V_n$ . If  $\text{mult}(S)$  contains no  $\Delta_3$  as a minor, then for any distinct  $a, b, c \in S$  and distinct  $i, j, k \in [n]$  such that*

$$a_i = b_i \neq c_i, \quad b_j = c_j \neq a_j, \quad c_k = a_k \neq b_k, \quad (\star)$$

there exists  $d \in S - \{a, b, c\}$  that satisfies the following:

- (1)  $d_\ell \in \{a_\ell, b_\ell, c_\ell\}$  for all  $\ell \in [n]$ , and
- (2) at least two of  $d_i = c_i$ ,  $d_j = a_j$ , and  $d_k = b_k$  hold.

*Proof.* Let  $V$  denote the ground set of  $\text{mult}(S)$ . We may assume that there exist three distinct points  $a, b, c \in S$  satisfying  $(\star)$  for some distinct  $i, j, k \in [n]$ . Take subsets  $I, J$  of  $[n]$  as follows:

$$I = V - \{a_\ell, b_\ell, c_\ell : \ell \in [n]\} \quad \text{and} \quad J = \{a_\ell, b_\ell, c_\ell : \ell \in [n] - \{i, j, k\}\}.$$

We will show that if  $d \in S - \{a, b, c\}$  satisfying (1) and (2) does not exist, then  $\text{mult}(S) \setminus I/J$  contains  $\Delta_3$  as a minor.

Notice that  $\text{mult}(S) \setminus I$  is  $\text{mult}(R_0)$  where  $R_0 = \{v \in S : v_\ell \in \{a_\ell, b_\ell, c_\ell\} \text{ for } \ell \in [n]\}$  and that each member of  $\text{mult}(R_0)$  is  $\{v_1, \dots, v_n\}$  for some  $v \in S$ . Furthermore, each  $v \in R_0$  satisfies  $\{v_1, \dots, v_n\} - J = \{v_i, v_j, v_k\}$ , so  $\{v_1, \dots, v_n\} - J$  remains minimal after contracting  $J$  from  $\text{mult}(R_0)$ . This in turn implies that  $\text{mult}(R_0)/J$  is equal to  $\text{mult}(R)$  where  $R := \{(v_i, v_j, v_k) : v \in S, v_\ell \in \{a_\ell, b_\ell, c_\ell\} \text{ for } \ell \in [n]\}$ . So,  $\text{mult}(S) \setminus I/J = \text{mult}(R)$ . By definition,  $R$  contains points  $(a_i, a_j, a_k)$ ,  $(b_i, b_j, b_k)$ , and  $(c_i, c_j, c_k)$  that are obtained from  $a, b, c$ . Suppose that there is no  $d \in S - \{a, b, c\}$  that satisfies (1) and (2). Let  $d \in S$  with  $d_\ell \in \{a_\ell, b_\ell, c_\ell\}$  for  $\ell \in [n]$ . Since  $d$  satisfies (1),  $d$  does not satisfy (2). Then  $(d_i, d_j, d_k)$  can be  $(c_i, b_j, c_k)$ ,  $(a_i, a_j, c_k)$ ,  $(a_i, b_j, b_k)$ , or  $(a_i, b_j, c_k)$ , implying in turn that

$$R \subseteq \{(a_i, a_j, a_k), (b_i, b_j, b_k), (c_i, c_j, c_k), (c_i, b_j, c_k), (a_i, a_j, c_k), (a_i, b_j, b_k), (a_i, b_j, c_k)\}.$$

To argue that  $\text{mult}(R)$  contains  $\Delta_3$  as a minor, let us look at the incidence matrix of  $\text{mult}(R)$ :

$$\begin{array}{c} a \\ b \\ c \end{array} \begin{pmatrix} a_i & \widehat{c_i} & \widehat{a_j} & b_j & c_k & \widehat{b_k} \\ 1 & \mathbf{0} & \mathbf{1} & 0 & 1 & \mathbf{0} \\ 1 & \mathbf{0} & \mathbf{0} & 1 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & \mathbf{0} & 1 & 1 & \mathbf{0} \\ & & & \vdots & & \end{pmatrix}$$

Observe that a row of  $M(\text{mult}(R))$  other than the ones for  $a, b, c$ , if any, has at least two ones in the columns for  $a_i, b_j, c_k$ . So, after contracting the columns for  $c_i, a_j, b_k$  and removing non-minimal rows, the resulting incidence matrix is precisely  $M(\Delta_3)$ . This implies that we obtain  $\Delta_3$  after contracting  $c_i, a_j, b_k$  from  $\text{mult}(R)$ , a contradiction to the assumption that  $\text{mult}(S)$  has no  $\Delta_3$  minor.  $\square$

**Lemma 4.2.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . If  $S$  does not admit a basis with vectors of pairwise disjoint supports, then  $\text{mult}(S)$  contains  $\Delta_3$  or  $Q_6$  as a minor. Moreover, if  $q$  is an odd prime power, then  $\text{mult}(S)$  contains  $\Delta_3$  as a minor.*

*Proof.* Assume that  $S$  does not admit a basis with vectors of pairwise disjoint supports. We will show that if  $\text{mult}(S)$  does not contain  $\Delta_3$  as a minor, then  $q$  is a power of 2 and  $\text{mult}(S)$  contains  $Q_6$  as a minor.

Assume that  $S$  contains no  $\Delta_3$  as a minor. Let  $v^1, \dots, v^r \in GF(q)^n$  be a basis of  $S$ . After elementary arithmetic operations over  $GF(q)$ , we may assume that for each  $i = 1, \dots, r$ ,

$$v_i^i = 1 \quad \text{and} \quad v_j^i = 0 \quad \forall j \in [r] - \{i\}$$

Since there is no basis of  $S$  with vectors of pairwise disjoint supports, we may assume that  $v_{r+1}^1, v_{r+1}^2 \neq 0$ . This in turn implies that  $n \geq 3$ . Let  $x$  and  $y$  be the multiplicative inverses of  $v_{r+1}^1$  and  $v_{r+1}^2$  in  $GF(q)$ , respectively. Let  $a := \mathbf{0} \in GF(q)^n$ ,  $b := xv^1$ , and  $c := yv^2$ . Notice that  $a, b, c \in S$  and that  $a, b, c$  satisfy

$$(a_1, a_2, a_{r+1}) = (0, 0, 0), \quad (b_1, b_2, b_{r+1}) = (x, 0, 1), \quad (c_1, c_2, c_{r+1}) = (0, y, 1).$$

Now we consider  $R = \{d \in S : d_j \in \{a_j, b_j, c_j\} \text{ for } j \in [n]\}$ .

**Claim 1.**  $R \subseteq \{\lambda_1 v^1 + \lambda_2 v^2 : \lambda_1 \in \{0, x\}, \lambda_2 \in \{0, y\}\}$ .

*Proof of Claim.* Let  $u \in R$ . Then  $u = \sum_{j=1}^r \lambda_j v^j$  for some  $\lambda_1, \dots, \lambda_r \in GF(q)$ . Since  $a_j = b_j = c_j = 0$  for  $j = 3, \dots, r$ , it follows that  $u_3 = \dots = u_r = 0$ , which implies that  $\lambda_3 = \dots = \lambda_r = 0$  and so  $u = \lambda_1 v^1 + \lambda_2 v^2$ . Notice that  $\lambda_1 \in \{0, x\}$  and  $\lambda_2 \in \{0, y\}$ , because  $a_1, b_1, c_1 \in \{0, x\}$  and  $a_2, b_2, c_2 \in \{0, y\}$ .  $\diamond$

**Claim 2.**  $q$  is a power of 2 and  $R = \{\lambda_1 v^1 + \lambda_2 v^2 : \lambda_1 \in \{0, x\}, \lambda_2 \in \{0, y\}\}$ .

*Proof of Claim.* By Lemma 4.1,  $R$  contains a  $d \notin \{a, b, c\}$  such that  $(d_1, d_2, d_{r+1}) = (0, y, 0), (x, 0, 0), (x, y, 1)$ , or  $(x, y, 0)$ . By Claim 1,  $d \in \{\lambda_1 v^1 + \lambda_2 v^2 : \lambda_1 \in \{0, x\}, \lambda_2 \in \{0, y\}\}$ . As  $d \neq a, b, c$ , it must be that  $xv^1 + yv^2 = d$ , so  $xv^1 + yv^2 \in R$ . In particular,  $R = \{\lambda_1 v^1 + \lambda_2 v^2 : \lambda_1 \in \{0, x\}, \lambda_2 \in \{0, y\}\}$ . Since  $d = xv^1 + yv^2$ , we obtain  $(xv^1 + yv^2)_{r+1} = 1 + 1 = d_{r+1} \in \{0, 1\}$ . Since  $1 \neq 0$ , we have  $1 + 1 = 0$ , so  $q$  is a power of 2, as required.  $\diamond$

By Claim 2,  $R = \{\lambda_1 v^1 + \lambda_2 v^2 : \lambda_1 \in \{0, x\}, \lambda_2 \in \{0, y\}\}$ , so the projection of  $R$  onto the space of coordinates  $1, 2, r + 1$  is precisely  $R_{1,1}$ . Since  $\text{mult}(R_{1,1}) = Q_6$ ,  $\text{mult}(S)$  has  $Q_6$  as a minor by Lemma 2.4. So, we have shown that if  $\text{mult}(S)$  has no  $\Delta_3$  as a minor, then  $q$  is a power of 2 and  $\text{mult}(S)$  contains  $Q_6$  as a minor, as required.  $\square$

**Lemma 4.3.** *Take an integer  $n \geq 1$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . If  $S$  has a basis with vectors of pairwise disjoint supports, then  $\text{mult}(S)$  has the MFMC property, and is therefore ideal.*

*Proof.* Assume that  $S$  has a basis of vectors with pairwise disjoint supports. Then we may assume that  $S = \langle u^1 \rangle \times \dots \times \langle u^r \rangle \times \{\mathbf{0}\}$  for some vectors  $u^1, \dots, u^r$  with no zero entries over  $GF(q)$ , by Lemma 3.4. Subsequently,  $\text{mult}(S) = \text{mult}(\langle u^1 \rangle) \times \dots \times \text{mult}(\langle u^r \rangle) \times \text{mult}(\{\mathbf{0}\})$ , and to prove  $\text{mult}(S)$  has the MFMC property, it suffices

to argue that  $\text{mult}(\langle u^i \rangle)$  for  $i \in [r]$  and  $\text{mult}(\{\mathbf{0}\})$  have the MFMC property, by Lemma 2.3. First, notice that  $\text{mult}(\{\mathbf{0}\})$  has only one member, so it clearly has the MFMC property. In fact, we can argue that each  $\text{mult}(\langle u^i \rangle)$  has pairwise disjoint members as well. Notice that for any distinct  $x, y \in GF(q)$ ,  $xu^i$  and  $yu^i$  do not have common coordinates, implying in turn that the members of  $\text{mult}(\langle u^i \rangle)$  corresponding to  $xu^i$  and  $yu^i$  are disjoint. That means that the members of  $\text{mult}(\langle u^i \rangle)$  are pairwise disjoint, implying in turn that it has the MFMC property, thereby proving that  $\text{mult}(S)$  has the MFMC property, as required.  $\square$

Having proved Lemmas 4.2 and 4.3, we are now ready to show Theorem 1.4. The basic flow of our proof is as follows. Lemma 4.3 shows that if a vector space  $S$  has a basis with vectors of pairwise disjoint supports, then  $\text{mult}(S)$  has the MFMC property. Conversely, Lemma 4.2 argues that if a vector space  $S$  does not admit such a basis, then  $\text{mult}(S)$  has some minors certifying that the clutter does not have the MFMC property. More details are explained in the proof as follows.

**Proof of Theorem 1.4.** (iii) $\Rightarrow$ (ii) follows from Lemma 4.2. (ii) $\Rightarrow$ (i) follows from Lemma 4.3. (i) $\Rightarrow$ (iii): Assume that  $\text{mult}(S)$  has the MFMC property.  $\Delta_3$  is a non-ideal clutter, so it does not have the max-flow min-cut property. Recall that  $Q_6$  is the clutter of triangles in  $K_4$ . Notice that the minimum number of edges required to intersect every triangle in  $K_4$  is two and that the maximum number of disjoint triangles in  $K_4$  is one. This implies that  $\tau(Q_6, \mathbf{1}) = 2$  and  $\nu(Q_6, \mathbf{1}) = 1$ , so  $Q_6$  does not have the max-flow min-cut property. Like idealness, the MFMC property is a minor-closed property [33]. Therefore, a clutter with the MFMC property contains none of  $\Delta_3, Q_6$  as a minor, implying in turn that  $\text{mult}(S)$  has none of  $\Delta_3, Q_6$  as a minor.  $\square$

The proof of Theorem 1.1 works similarly as that of Theorem 1.4. The additional component is that when  $q$  is an odd prime power and a vector space  $S$  over  $GF(q)$  does not admit a basis with vectors of pairwise disjoint supports, then  $\text{mult}(S)$  has a non-ideal minor due to Lemma 4.2.

**Proof of Theorem 1.1.** Take an integer  $n \geq 1$  and an odd prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Since  $\Delta_3$  is non-ideal, direction (i) $\Rightarrow$ (iii) is clear. Direction (iii) $\Rightarrow$ (ii) follows from Lemma 4.2, and Lemma 4.3 shows direction (ii) $\Rightarrow$ (i). Therefore, (i)–(iii) are equivalent.  $\square$

## 5 Fields of characteristic 2: a structure theorem

In this section, we prove Theorem 5.5 which provides an important tool for characterizing the idealness of  $\text{mult}(S)$  where  $S$  is a vector space over  $GF(2^k)$  for  $k \geq 2$ . To be more precise, Theorem 5.5 characterizes the structure of the underlying matroid  $\text{Matroid}(S)$  when  $\text{mult}(S)$  is ideal and thus has no  $\Delta_3$  as a minor.

**Lemma 5.1.** *Let  $q$  be a power of 2, and let  $S \subseteq GF(q)^4$  be a vector space over  $GF(q)$ . If  $\text{Matroid}(S)$  is isomorphic to  $U_{2,4}$ , then  $\text{mult}(S)$  has  $\Delta_3$  as a minor.*

*Proof.* Suppose for a contradiction that  $\text{mult}(S)$  has no  $\Delta_3$  as a minor. Since the rank of  $U_{2,4}$  is 2, the dimension of  $S$  is  $4 - 2 = 2$ . Let  $v^1, v^2 \in GF(q)^4$  be two generators of  $S$ . By elementary row operations, we may assume that  $(v_1^1, v_2^1) = (1, 0)$  and  $(v_1^2, v_2^2) = (0, 1)$ . Then

$$\begin{array}{l} v^1 \\ v^2 \end{array} \left[ \begin{array}{cc|cc} 1 & 0 & x & y \\ 0 & 1 & z & w \end{array} \right]$$

where  $x, y, z, w \in GF(q)$ . Each circuit of  $U_{2,4}$  has size 3, so  $x, y, z, w \neq 0$ . Then  $a := (-x^{-1}z)v^1$ ,  $b := v^2$ ,  $c := a + b$  are vectors in  $S$ . Observe that

$$\begin{array}{l} a \\ b \\ c \end{array} \left[ \begin{array}{ccc|ccc} -x^{-1}z & 0 & -z & -x^{-1}yz & & \\ 0 & 1 & z & w & & \\ -x^{-1}z & 1 & 0 & -x^{-1}yz + w & & \end{array} \right]$$

and that  $a_1 = c_1 \neq b_1$ ,  $b_2 = c_2 \neq a_2$ . We also have that  $a_3 = b_3 \neq c_3$ , because  $q$  being a power of 2 implies  $z + z = 0$  and  $z = -z$ . By Lemma 4.1, there is a vector  $d \in GF(q)^4$  that satisfies at least two of  $d_1 = b_1 = 0$ ,  $d_2 = a_2 = 0$ ,  $d_3 = c_3 = 0$  and satisfies  $d_4 \in \{-x^{-1}yz, w, -x^{-1}yz + w\}$ . But then the support of  $d$  has size at most 2. Since every circuit of  $U_{2,4}$  has size 3,  $d = \mathbf{0}$ , and therefore,  $d_4 = -x^{-1}yz + w = 0$ . This implies the support of  $c$  has size 2, a contradiction.  $\square$

**Graph minors.** We say that a graph  $H$  is a *graph minor* of a graph  $G$  if  $H$  can be obtained from  $G$  after a series of edge deletions, edge contractions, and deletions of isolated vertices. If  $G$  is connected, then  $H$  is a graph minor of  $G$  if and only if for some disjoint subsets  $E_1, E_2$  of  $E(G)$ , we can obtain  $H$  from  $G$  by deleting  $E_1$  and contracting  $E_2$ . It is well-known that if  $H$  is a graph minor of  $G$ , then  $\text{Matroid}(H)$  is a matroid minor of  $\text{Matroid}(G)$  (see Chapter 3.2 in [27]).

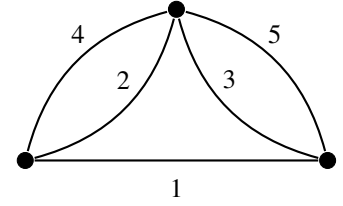


Figure 1:  $K_4/e$

$K_4$  is the complete graph on 4 vertices, and we denote by  $K_4/e$  what is obtained from  $K_4$  after contracting an edge from it (see Figure 1).

**Lemma 5.2.** *Let  $q = 2^k$  for some  $k \geq 2$ , and let  $S \subseteq GF(q)^5$  be a vector space over  $GF(q)$ . If  $\text{Matroid}(S)$  is isomorphic to  $\text{Matroid}(K_4/e)$ , then  $\text{mult}(S)$  has  $\Delta_3$  as a minor.*

*Proof.* In Figure 1, we can see that the fundamental circuits of  $K_4/e$  with respect to spanning tree  $\{4, 5\}$  are  $\{1, 4, 5\}$ ,  $\{2, 4\}$ ,  $\{3, 5\}$ . Pick vectors  $v^1, v^2, v^3 \in S$  whose supports are the three circuits. Notice that these vectors are linearly independent. Since the dimension of  $S$  is  $5 - 2 = 3$ , vectors  $v^1, v^2, v^3$  generate  $S$ . After elementary row operations,  $S$  is generated by the 3 vectors  $v^1, v^2, v^3$  of the following forms:

$$\begin{array}{l} v^1 \\ v^2 \\ v^3 \end{array} \left[ \begin{array}{ccc|cc} 1 & 0 & 0 & x & y \\ 0 & 1 & 0 & z & 0 \\ 0 & 0 & t & 0 & w \end{array} \right]$$

where  $t, x, y, z, w \neq 0$ . Since  $q > 2$ , we may assume that  $z$  and  $w$  are distinct nonzero elements in  $GF(q)$ . Now consider the restriction  $S'$  of  $S$  defined as follows:

$$S' := S \cap \{x \in GF(q)^5 : x_1 \in \{0, z, w\}, x_2 \in \{0, x\}, x_3 \in \{0, ty\}\}.$$

We will show that  $\text{mult}(S')$  has  $\Delta_3$  as a minor. Then as  $S'$  is a restriction of  $S$ , it follows from Lemma 2.4 that  $\text{mult}(S)$  also has  $\Delta_3$  as a minor. Notice that

$$S' = \left\{ \sum_{i=1}^3 \lambda_i v^i : \lambda_1 \in \{0, z, w\}, \lambda_2 \in \{0, x\}, \lambda_3 \in \{0, y\} \right\}.$$



Consider three distinct points  $a := zv^1$ ,  $b := wv^1$ ,  $c := xv^2 + yv^3$  in  $S'$ :

$$\begin{array}{l} a \\ b \\ c \end{array} \left[ \begin{array}{ccc|cc} z & 0 & 0 & zx & zy \\ w & 0 & 0 & wx & wy \\ 0 & x & ty & zx & wy \end{array} \right]$$

As  $z \neq w$ , we have that  $c_4 = a_4 \neq b_4$  and  $b_5 = c_5 \neq a_5$ . We also have  $a_3 = b_3 \neq c_3$ , because  $ty \neq 0$ . Suppose for a contradiction that  $\text{mult}(S')$  has no  $\Delta_3$  as a minor. By Lemma 4.1, there is  $d \in S' - \{a, b, c\}$  that satisfies

- (1)  $d_1 \in \{0, z, w\}$ ,  $d_2 \in \{0, x\}$ ,  $d_3 \in \{0, ty\}$ ,  $d_4 \in \{zx, wx\}$ ,  $d_5 \in \{zy, wy\}$ , and
- (2) at least two of  $d_3 = ty$ ,  $d_4 = wx$ ,  $d_5 = zy$  hold.

The points of  $S' - \{a, b, c\}$  are the following:

$$S' - \{a, b, c\} = \left\{ \begin{array}{ccc|cc} (0, 0, 0, 0, 0) & (0, x, 0, zx, 0) & (0, 0, ty, 0, wy) \\ (z, x, 0, 0, zy) & (z, 0, ty, zx, (z+w)y) & (w, x, 0, (z+w)x, wy) \\ (w, 0, ty, wx, 0) & (z, x, ty, 0, (z+w)y) & (w, x, ty, (z+w)x, 0) \end{array} \right\}.$$

Since  $z, w \neq 0$  and  $z \neq w$ ,  $(z+w)x \notin \{zx, wx\}$  and  $(z+w)y \notin \{zy, wy\}$ . Since  $z, w, x, y \neq 0$ ,  $0 \notin \{zx, wx\}$  and  $0 \notin \{zy, wy\}$ . This indicates that no point in  $S' - \{a, b, c\}$  satisfies condition (1), a contradiction. Therefore,  $\text{mult}(S')$  has  $\Delta_3$  as a minor, and so does  $\text{mult}(S)$ , as required.  $\square$

How does a graph with no  $K_4/e$  graph minor look like? We have the following result.

**Lemma 5.3.** *Let  $G = (V, E)$  be a connected graph. If  $G$  contains no  $K_4/e$  as a graph minor, then each block of  $G$  is a bridge, a circuit, or a subdivision of  $A_t$  for some  $t \geq 3$ .*

*Proof.* See §A in the appendix.  $\square$

We call a graph a *series-parallel network* if each of its blocks is a series-parallel graph.

**Theorem 5.4** ([8]). *Let  $M$  be a matroid. Then the following statements are equivalent:*

- (i)  $M$  contains none of  $U_{2,4}$  and  $\text{Matroid}(K_4)$  as a matroid minor;
- (ii)  $M$  is the cycle matroid of a series-parallel network.

**Theorem 5.5.** *Let  $q = 2^k$  for some  $k \geq 2$ , and let  $S$  be a vector space over  $GF(q)$ . If  $\text{mult}(S)$  has no  $\Delta_3$  as a minor, then for some  $k \geq 1$ ,  $\text{Matroid}(S) = M_1 \oplus \cdots \oplus M_k$ , where each  $M_i$  is the cycle matroid of a bridge, a circuit, or a subdivision of  $A_t$  for some  $t \geq 3$ .*

*Proof.* Assume that  $\text{mult}(S)$  has no  $\Delta_3$  as a minor. Suppose for a contradiction that  $\text{Matroid}(S)$  contains  $U_{2,4}$  or  $\text{Matroid}(K_4/e)$  as a matroid minor. This in turn implies that there exists  $S'$  obtained from  $S$  after a series of restrictions and projections such that  $\text{Matroid}(S')$  is isomorphic to  $U_{2,4}$  or  $\text{Matroid}(K_4/e)$  by Lemma 3.2. Here,  $\text{mult}(S')$  contains  $\Delta_3$  as a minor by Lemmas 5.1 and 5.2. As  $\text{mult}(S')$  is a minor of  $\text{mult}(S)$  due to Lemma 2.4, it follows that  $\text{mult}(S)$  also contains a  $\Delta_3$  as a minor, a contradiction. Hence,  $\text{Matroid}(S)$  contains none of  $U_{2,4}$  and  $\text{Matroid}(K_4/e)$  as a matroid minor. As  $\text{Matroid}(K_4/e)$  is a matroid minor of  $\text{Matroid}(K_4)$ , Theorem 5.4 implies that  $\text{Matroid}(S)$  is the cycle matroid of a series-parallel network not containing  $K_4/e$  as a graph minor. Then by Lemma 5.3, each block of the graph is a subdivision of  $A_t$  for some  $t \geq 3$ , a bridge, or a circuit. So, the assertion follows from Lemma 3.3, as required.  $\square$

Suppose  $S$  is a vector space over  $GF(2^k)$  for some  $k \geq 2$ . By Theorem 5.5, if  $\text{mult}(S)$  has no  $\Delta_3$  as a minor, then the underlying matroid can be decomposed as the direct sum of some structured graphic matroids. Then it follows from Corollary 3.6 that  $S$  can be represented as  $S = S_1 \times \cdots \times S_k$  where each  $S_i$  has dimension at most 1, or admits a sunflower basis. Then the idealness of  $S$  is determined by  $S_1, \dots, S_k$  according to Lemma 2.3. In particular, we need to understand the case where  $S_i$  is a vector space that admits a sunflower basis. In the next section, we provide tools for characterizing when the multipartite uniform clutter of a vector space that admits a sunflower basis is ideal.

## 6 Fields of characteristic 2: a study of the localizations for $A_t$

Suppose  $S$  is a vector space over  $GF(2^k)$  for  $k \geq 2$ . At the end of Section 5, we discussed that understanding vector spaces that admit a sunflower basis is the key to characterizing when  $\text{mult}(S)$  is ideal. In this section, we consider the case when  $\text{Matroid}(S) = \text{Matroid}(A_n)$  for some  $n \geq 3$ , where  $A_n$  denotes the graph that consists of two vertices and  $n$  parallel edges connecting them. Recall that by Theorem 2.7,  $\text{mult}(S)$  is ideal if and only if all its localizations are ideal. In this section, we prove three lemmas on properties of localizations of  $\text{mult}(S)$ .

**Lemma 6.1.** *Take an integer  $n \geq 3$  and a prime power  $q$ , and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . Then  $\text{Matroid}(S) = \text{Matroid}(A_n)$  if and only if  $S \cong \{x \in GF(q)^n : x_1 + \cdots + x_n = 0\}$ .*

*Proof.* Let  $\{1, 2, 3, \dots, n\}$  denote the edge set of  $A_n$ . Then  $\{1, 2\}, \{1, 3\}, \dots, \{1, n\}$  are circuits of  $\text{Matroid}(A_n)$ . ( $\Leftarrow$ ): Let  $\mathcal{S}$  be the clutter of the minimal supports of the points in  $S - \{0\}$ . Then  $\mathcal{S} = \{\{i, j\} : i \neq j\}$ , so  $\text{Matroid}(S) = \text{Matroid}(A_n)$  by Remark 3.1. ( $\Rightarrow$ ): Since  $\text{Matroid}(S) = \text{Matroid}(A_n)$ ,  $S$  contains  $n - 1$  points  $u^1, \dots, u^{n-1}$  whose supports are  $\{1, 2\}, \{1, 3\}, \dots, \{1, n\}$ , respectively. Notice that  $u^1, \dots, u^{n-1}$  are linearly independent over  $GF(q)$ , so the dimension of  $S$  is at least  $n - 1$ . On the other hand, the dimension is less than  $n$ , because  $S \neq GF(q)^n$ . Thus,  $S = \langle u^1, \dots, u^{n-1} \rangle$ . After scaling the  $u^i$ 's, if necessary, we may assume that the first coordinate of each  $u^i$  is 1. Hence,  $u^1, \dots, u^{n-1}$  are of the form displayed below (left), where  $\lambda_1, \dots, \lambda_{n-1} \in GF(q) - \{0\}$ . Notice that  $\{x \in GF(q)^n : x_1 + \cdots + x_n = 0\} = \langle v^1, \dots, v^{n-1} \rangle$  where  $v^1, \dots, v^{n-1}$  are displayed below (right):

$$\begin{array}{l} u^1 \\ u^2 \\ \vdots \\ u^{n-1} \end{array} \begin{bmatrix} 1 & \lambda_1 & 0 & \cdots & 0 \\ 1 & 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & \lambda_{n-1} \end{bmatrix} \quad \begin{array}{l} v^1 \\ v^2 \\ \vdots \\ v^{n-1} \end{array} \begin{bmatrix} 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{bmatrix},$$

implying in turn that  $\{x \in GF(q)^n : x_1 + \cdots + x_n = 0\} = \{(x_1, -\lambda_1^{-1}x_2, -\lambda_2^{-1}x_3, \dots, -\lambda_{n-1}^{-1}x_n) : x \in S\}$ . Therefore,  $S \cong \{x \in GF(q)^n : x_1 + \cdots + x_n = 0\}$ , as required.  $\square$

By Lemma 6.1, we may focus on the set

$$S = \{x \in GF(q)^n : x_1 + \cdots + x_n = 0\}$$

to understand vector spaces whose underlying matroids are  $\text{Matroid}(A_n)$ . Recall that a localization of  $\text{mult}(S)$  with respect to  $\alpha \in GF(q)^n$ , denoted  $\text{local}(S, \alpha)$ , is the minor of  $\text{mult}(S)$  after contracting the elements corresponding to  $\alpha$  (see Section 2).  $\text{mult}(S)$  is defined over ground set  $V_1 \cup \cdots \cup V_n$  where each  $V_i$  is a copy of  $GF(q)$ ,

and  $\text{local}(S, \alpha)$ 's ground set is given by  $U_1 \cup \dots \cup U_n$  where  $U_i = V_i - \{\alpha_i\}$ . The following lemma provides a characterization of the members of  $\text{local}(S, \alpha)$  for any  $\alpha \notin S$ .

**Lemma 6.2.** *Take an integer  $n \geq 3$ . Let  $q$  be a power of 2, and let  $\alpha \in GF(q)^n$  with  $\sigma := \alpha_1 + \dots + \alpha_n \neq 0$ . Let  $C \subseteq U_1 \cup \dots \cup U_n$  where  $U_i = GF(q) - \{\alpha_i\}$ . Then the following statements are equivalent:*

- (i)  $C$  is a member of  $\text{local}(S, \alpha)$ .
- (ii)  $C$  contains at most one element in  $U_i$  for each  $i \in [n]$  and  $\sum(v : v \in C) = \sigma + \sum(\alpha_i : C \cap U_i \neq \emptyset)$ .

*Proof.* (i) $\Rightarrow$ (ii) There exists  $x = (x_1, \dots, x_n) \in S$  such that  $C = \{x_1, \dots, x_n\} - \{\alpha_1, \dots, \alpha_n\}$ . Then  $C \cap U_i = \{x_i\} - \{\alpha_i\}$ , implying that  $C \cap U_i$  has at most one element. Without loss of generality, we may assume that  $x = (x_1, \dots, x_k, \alpha_{k+1}, \dots, \alpha_n)$  and  $x_1 \neq \alpha_1, \dots, x_k \neq \alpha_k$  for some  $1 \leq k \leq n$ . Then  $C = \{x_1, \dots, x_k\}$ . Since  $x \in S$ , we have

$$\sum_{i=1}^n x_i = \sum_{i=1}^k x_i + \sum_{j=k+1}^n \alpha_j = 0.$$

As the characteristic of  $GF(q)$  is 2,  $\sum_{i=1}^k x_i = -\sum_{i=1}^k x_i$ , implying in turn that  $\sum_{i=1}^k x_i = \sum_{j=k+1}^n \alpha_j$ . As  $\sum_{i=1}^n \alpha_i = \sigma$ , we also get  $\sum_{j=k+1}^n \alpha_j = \sigma + \sum_{i=1}^k \alpha_i$ , and therefore, we obtain  $\sum_{i=1}^k x_i = \sigma + \sum_{i=1}^k \alpha_i$ , as required.

(ii) $\Leftarrow$ (i) Without loss of generality, we may assume that  $C = \{x_1, \dots, x_k\}$  where  $x_i \in U_i$  for  $i \in [k]$ . Then  $\{x_1, \dots, x_k\} \cap \{\alpha_1, \dots, \alpha_n\} = \emptyset$ . Since  $\sum_{i=1}^k x_i = \sigma + \sum_{i=1}^k \alpha_i$ , we have  $\sum_{i=1}^k x_i + \sum_{j=k+1}^n \alpha_j = \sigma + \sum_{i=1}^n \alpha_i = 0$ , implying in turn that  $(x_1, \dots, x_k, \alpha_{k+1}, \dots, \alpha_n) \in S$ . As  $C = \{x_1, \dots, x_k, \alpha_{k+1}, \dots, \alpha_n\} - \{\alpha_1, \dots, \alpha_n\}$ , it follows that  $C$  is a member of  $\text{local}(S, \alpha)$ , as required.  $\square$

Using Lemma 6.2, we can show the following lemma providing a characterization of the members of size 1 and 2 in  $\text{local}(S, \alpha)$  for  $\alpha \notin S$ .

**Lemma 6.3.** *Take an integer  $n \geq 3$ . Let  $q$  be a power of 2, and let  $\alpha \in GF(q)^n$  with  $\sigma := \alpha_1 + \dots + \alpha_n \neq 0$ . Then the following statements hold:*

- (1) *the members of size 1 of  $\text{local}(S, \alpha)$  are  $\{\alpha_1 + \sigma\}, \dots, \{\alpha_n + \sigma\}$ .*
- (2) *the members of size 2 of  $\text{local}(S, \alpha)$  form a graph that consists of  $\frac{q}{2} - 1$  connected components  $G_1, \dots, G_{\frac{q}{2}-1}$  satisfying the following: for each  $j = 1, \dots, \frac{q}{2} - 1$ ,*
  - $G_j$ 's vertex set is  $\{\beta_1^j, \beta_1^j + \sigma\} \cup \dots \cup \{\beta_n^j, \beta_n^j + \sigma\}$  where  $\{\beta_i^j, \beta_i^j + \sigma\} \subseteq U_i - \{\alpha_i + \sigma\} = GF(q) - \{\alpha_i, \alpha_i + \sigma\}$  for  $i \in [n]$ ,
  - $G_j$  is a bipartite graph with bipartition  $\{\beta_1^j, \dots, \beta_n^j\} \cup \{\beta_1^j + \sigma, \dots, \beta_n^j + \sigma\}$ ,
  - $\beta_i^j = \beta_1^j + \alpha_1 + \alpha_i$  for  $i \in [n]$ , and
  - $G_j$ 's edge set is  $\left\{ \left\{ \beta_i^j, \beta_k^j + \sigma \right\} : i \neq k \right\}$ , i.e.,  $G_j$  is obtained from a complete bipartite graph after removing the edges of a perfect matching (see Figure 2 for an illustration).

*Proof.* See §B of the appendix.  $\square$

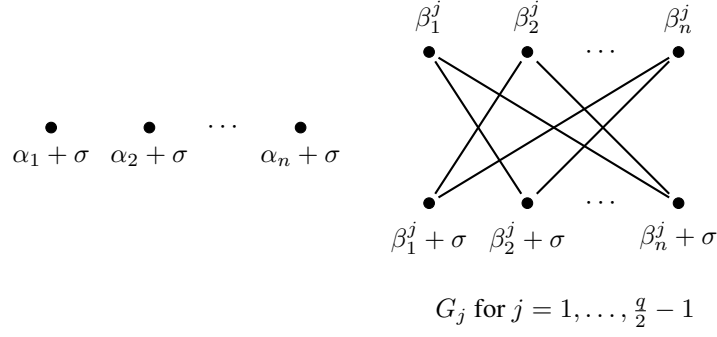


Figure 2: Members of size 1 and 2 of  $\text{local}(S, \alpha)$

## 7 The $q = 4$ case

In this section, we prove Theorem 1.2 characterizing when the multipartite uniform clutter of a vector space over  $GF(4)$  is ideal. The proof of Theorem 1.2 uses the following two lemmas. We first show Lemma 7.1 which implies that  $\text{mult}(T)$  is ideal if  $T$  is a vector space over  $GF(4)$  such that  $\text{Matroid}(T) \cong \text{Matroid}(A_n)$  for some  $n \geq 3$ . We then prove in Lemma 7.2 that idealness is closed under “series extensions”.

**Lemma 7.1.** *Let  $T = \{x \in GF(4)^n : x_1 + \dots + x_n = 0\}$  for some  $n \geq 3$ . Then  $\text{mult}(T)$  is ideal.*

*Proof.* By Theorem 2.7, it suffices to argue that all localizations of  $\text{mult}(T)$  are ideal. Let  $\alpha = (\alpha_1, \dots, \alpha_n) \notin T$ . We will show that the localization of  $\text{mult}(T)$  with respect to  $\alpha$ , denoted  $\text{local}(T, \alpha)$ , is ideal. Let  $\sigma = \alpha_1 + \dots + \alpha_n \neq 0$ . Note that  $\text{local}(T, \alpha)$  has  $n$  members of cardinality 1,  $\{\alpha_1 + \sigma\}, \dots, \{\alpha_n + \sigma\}$  by Lemma 6.3 (1). By Lemma 6.3 (2), the members of cardinality 2 form a connected bipartite graph  $G$  where

- $G$  is bipartite on  $\{\beta_1, \dots, \beta_n\} \cup \{\beta_1 + \sigma, \dots, \beta_n + \sigma\}$  where  $\{\beta_i, \beta_i + \sigma\} = GF(4) - \{\alpha_i, \alpha_i + \sigma\}$  for  $i \in [n]$ ,
- $\beta_i = \beta_1 + \alpha_1 + \alpha_i$  for  $i \in [n]$ , and
- the edge set of  $G$  is  $\{\{\beta_i, \beta_k + \sigma\} : i \neq k\}$ .

We will show that there is no member of cardinality at least 3 in  $\text{local}(T, \alpha)$ . Suppose for a contradiction that  $\text{local}(T, \alpha)$  has a member  $C$  whose cardinality is at least 3. As  $C$  does not contain any of the members of  $\text{local}(T, \alpha)$  that have cardinality 1 or 2,  $C \subseteq \{\beta_1, \dots, \beta_n\}$  or  $C \subseteq \{\beta_1 + \sigma, \dots, \beta_n + \sigma\}$ . Without loss of generality, we may assume that  $C = \{\beta_1, \dots, \beta_k\}$  for some  $k \geq 3$ . Then, by Lemma 6.2, we have  $\sum_{i=1}^k \beta_i = \sigma + \sum_{i=1}^k \alpha_i$ . Substituting  $\beta_i = \beta_1 + \alpha_1 + \alpha_i$  for  $i = 2, \dots, k$ , we obtain  $\sum_{i=1}^k (\beta_1 + \alpha_1) = \sigma$ . Since  $\sigma$  is nonzero and  $\sum_{i=1}^k (\beta_1 + \alpha_1)$  is either  $\beta_1 + \alpha_1$  or 0, we get  $\sum_{i=1}^k (\beta_1 + \alpha_1) = \beta_1 + \alpha_1 = \sigma$ . However,  $\beta_1 + \alpha_1 = \sigma$  in turn implies that  $\beta_i = \beta_1 + \alpha_1 + \alpha_i = \alpha_i + \sigma$ , contradicting the assumption that  $\beta_i \in GF(4) - \{\alpha_i, \alpha_i + \sigma\}$ . Therefore,  $\text{local}(T, \alpha)$  does not have a member of cardinality at least 3, as required.

Thus the members of  $\text{local}(T, \alpha)$  have size either 1 or 2. Let  $\mathcal{C}$  be what is obtained from  $\text{local}(T, \alpha)$  after deleting every element that appears in a member of cardinality 1. As no minimally non-ideal clutter has a member

of cardinality 1,  $\text{local}(T, \alpha)$  is ideal if and only if  $\mathcal{C}$  is ideal. Notice that  $M(\mathcal{C})$ , the incidence matrix of  $\mathcal{C}$ , is the edge - vertex incidence matrix of a bipartite graph. It follows from König's theorem for bipartite matching that  $\mathcal{C}$  is ideal. Therefore,  $\text{local}(T, \alpha)$  is ideal, and  $\text{mult}(T)$  is ideal, as required.  $\square$

**Lemma 7.2.** *Suppose that  $S$  is a vector space over  $GF(q)$  such that  $\text{Matroid}(S)$  has elements in series. Let  $S'$  be a projection of  $S$  obtained after dropping one of the elements in series. Then  $\text{mult}(S)$  is ideal if and only if  $\text{mult}(S')$  is ideal.*

*Proof.* Without loss of generality, assume that  $\text{Matroid}(S)$  has  $n$  elements and that elements  $n-1, n$  are in series. Let  $S'$  be defined as the projection of  $S$  obtained after dropping the  $n^{\text{th}}$  coordinate of the points in  $S$ . Then  $S'$  is a vector space in  $GF(q)^{n-1}$ , and by Lemma 3.2,  $\text{Matroid}(T) = \text{Matroid}(S)/\{n\}$ .

Let  $x \in S$ . Then  $\text{support}(x)$  is the union of some circuits of  $\text{Matroid}(S)$  by Remark 3.1. As  $n-1, n$  are series elements, a circuit of  $\text{Matroid}(S)$  contains  $n-1$  if and only if it contains  $n$ , implying in turn that  $n-1 \in \text{support}(x)$  if and only if  $n \in \text{support}(x)$ . Let  $v^1, \dots, v^r$  give rise to a basis of  $S$ . If  $n \in \text{support}(x)$  for some  $x \in S$ , then  $n \in \text{support}(v^\ell)$  for some  $\ell \in [r]$ , and thus, we may assume that  $n \in \text{support}(v^1)$  and that  $v_n^1 \neq 0$ . After scaling the  $v^\ell$ 's, if necessary, we may assume that  $v_n^\ell = 0$  for  $\ell \in [r] - \{1\}$ . Since  $n-1 \in \text{support}(x)$  if and only if  $n \in \text{support}(x)$  for  $x \in S$ , we have that  $v_{n-1}^1 \neq 0$  and  $v_{n-1}^\ell = 0$  for  $\ell \in [r] - \{1\}$ . Then for some  $y, z \in GF(q) - \{0\}$ ,

$$\begin{array}{l} v^1 \\ v^2 \\ \vdots \\ v^r \end{array} \left[ \begin{array}{c|cc} \cdots & y & z \\ \cdots & 0 & 0 \\ \vdots & 0 & 0 \\ \cdots & 0 & 0 \end{array} \right].$$

Then it follows that  $S = \{(x_1, \dots, x_{n-1}, zy^{-1}x_{n-1}) : (x_1, \dots, x_{n-1}) \in S'\}$ , and by Remark 2.2,  $\text{mult}(S) \cong \text{mult}(T)$  where  $T = \{(x_1, \dots, x_{n-1}, x_{n-1}) : (x_1, \dots, x_{n-1}) \in S'\}$ . Let  $V_1 \cup \dots \cup V_n$  be the ground set of  $\text{mult}(S)$  where each  $V_i$  is a copy of  $GF(q)$ . Then

$$\text{mult}(T) = \{C : C' \in \text{mult}(S'), C \cap (V_1 \cup \dots \cup V_{n-1}) = C', C \cap V_n = C' \cap V_{n-1}\}.$$

In words,  $\text{mult}(T)$  is obtained from  $\text{mult}(S')$  after duplicating the element in  $V_{n-1}$  of each member  $C' \in \text{mult}(S')$ . Then the  $V_{n-1}$  part and the  $V_n$  part of the members of  $\text{mult}(T)$  are identical. Hence,  $\text{mult}(T)$  is ideal if and only if  $\text{mult}(S')$ . As  $\text{mult}(S)$  is isomorphic to  $\text{mult}(T)$ , it follows that  $\text{mult}(S)$  is ideal if and only if  $\text{mult}(S')$  is ideal.  $\square$

Now we are ready to prove Theorem 1.2. The proof first reduces to the case when the vector space  $T$  admits a sunflower basis. Then the idea is to show that  $\text{Matroid}(T)$  is a series extension of  $\text{Matroid}(T')$  where  $\text{Matroid}(T') \cong \text{Matroid}(A_t)$  for some  $t \geq 3$ . We then use Lemmas 7.1 and 7.2 to show that  $\text{mult}(T)$  is ideal.

**Proof of Theorem 1.2.** Take an integer  $n \geq 1$ , and let  $S \subseteq GF(4)^n$  be a vector space over  $GF(4)$ . First of all, (i) $\Rightarrow$ (iii) is straightforward as  $\Delta_3$  is non-ideal. In what follows, we will show directions (iii) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i).

(iii) $\Rightarrow$ (ii): By Theorem 5.5,  $\text{Matroid}(S) = M_1 \oplus \dots \oplus M_k$  for some  $k \geq 1$  where for each  $i \in [k]$ ,  $M_i$  is the cycle matroid of a bridge, a circuit, or a subdivision  $A_t$  for some  $t \geq 3$ . Then it follows from Corollary 3.6 that  $S$  satisfies (ii).

(ii) $\Rightarrow$ (i): It suffices to show that  $\text{mult}(S_i)$  is ideal for every  $i \in [k]$  due to Lemma 2.3. To this end, take an  $i \in [k]$ . If  $S_i$  has dimension at most 1, then  $S_i = \{\mathbf{0}\}$  or  $S_i = \langle v \rangle$  for some nonzero vector  $v$ , in which case it follows from Lemma 4.3 that  $S_i$  is ideal. Thus we may assume that  $S_i = \langle v^1, \dots, v^r \rangle$  where  $r \geq 2$  and  $v^1, \dots, v^r$  give rise to a sunflower basis of  $S_i$ . Let  $T' = \langle w^1, \dots, w^r \rangle$  where

$$\begin{array}{c} w^1 \\ w^2 \\ \vdots \\ w^r \end{array} \left[ \begin{array}{c|c|c|c|c} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{array} \right].$$

Then  $T' = \{x \in GF(4)^{r+1} : x_1 + \dots + x_{r+1} = 0\}$ , so by Lemma 7.1,  $\text{mult}(T')$  is ideal. Suppose that  $v^i$  is of the form  $(u^0, u^i)$  for  $i \in [r]$ , and let  $d_\ell$  denote the number of entries in  $u^\ell$  for  $\ell = 0, 1, \dots, r$ . Then we define  $T$  as

$$T := \left\{ \underbrace{(x_1, \dots, x_1)}_{d_0}, \underbrace{(x_2, \dots, x_2)}_{d_1}, \dots, \underbrace{(x_{r+1}, \dots, x_{r+1})}_{d_r} : (x_1, x_2, \dots, x_{r+1}) \in T' \right\}.$$

Then  $T$  is generated by  $y^1, \dots, y^r$  where

$$\begin{array}{c} y^1 \\ y^2 \\ \vdots \\ y^r \end{array} \left[ \begin{array}{c|c|c|c|c} \overbrace{\mathbf{1}}^{d_0} & \overbrace{\mathbf{1}}^{d_1} & \overbrace{\mathbf{0}}^{d_2} & \cdots & \overbrace{\mathbf{0}}^{d_r} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} \end{array} \right].$$

Note that  $T'$  is a projection of  $T$  obtained after dropping the coordinates that correspond to some series elements of  $\text{Matroid}(T)$ . As  $\text{mult}(T')$  is ideal, it follows from Lemma 7.2 that  $\text{mult}(T)$  is ideal. Moreover,  $S_i$  can be obtained from  $T$  by taking coordinate-wise bijections. Hence, Remark 2.2 implies that  $\text{mult}(S_i) \cong \text{mult}(T)$ , thereby showing that  $\text{mult}(S_i)$  is ideal, as required.  $\square$

## 8 Powers of 2 greater than 4

In this section, we prove Theorem 1.3 which characterizes when the multipartite uniform clutter of a vector space  $S$  over  $GF(2^k)$  with  $k > 2$  is ideal. We start by proving Lemmas 8.1 and 8.2 which imply that if  $\text{mult}(S)$  is ideal, then the underlying matroid  $\text{Matroid}(S)$  does not contain two distinct circuits that intersect. The proofs of the lemmas rely on the tools from Section 6.

For the first lemma, recall that  $C_5^2$  is the clutter of edges in a cycle of length 5, and that  $C_5^2$  is non-ideal.

**Lemma 8.1.** *Let  $q$  be a power of 2 greater than 4, and let  $S \subseteq GF(q)^3$  be a vector space over  $GF(q)$  such that  $\text{Matroid}(S)$  is isomorphic to  $\text{Matroid}(A_3)$ . Then  $\text{mult}(S)$  has  $C_5^2$  as a minor.*

*Proof.* By Lemma 6.1, we may assume that  $S = \{x \in GF(q)^3 : x_1 + x_2 + x_3 = 0\}$ . Let  $\alpha = (\alpha_1, \alpha_2, \alpha_3) \notin S$ . We will show that  $\text{local}(S, \alpha)$  has  $C_5^2$  as a minor. Let  $\sigma = \alpha_1 + \alpha_2 + \alpha_3$ , and we choose  $a, b \in GF(q)$  such that  $a \in GF(q) - \{\alpha_1, \alpha_1 + \sigma\}$  and  $b \in GF(q) - \{\alpha_1, \alpha_1 + \sigma, a, a + \sigma\}$ .

**Claim 1.**  $a + b + \alpha_1 \in GF(q) - \{\alpha_1, \alpha_1 + \sigma, a, a + \sigma, b, b + \sigma\}$ .

*Proof of Claim.* If  $a + b + \alpha_1 = \alpha_1$  or  $\alpha_1 + \sigma$ , then  $b = a$  or  $b = a + \sigma$ , contradicting the choice of  $b$ . If  $a + b + \alpha_1 = a$  or  $a + \sigma$ , then  $b = \alpha_1$  or  $b = \alpha_1 + \sigma$ , contradicting the choice of  $b$ . If  $a + b + \alpha_1 = b$  or  $b + \sigma$ , then  $a = \alpha_1$  or  $a = \alpha_1 + \sigma$ , a contradiction as  $a \notin \{\alpha_1, \alpha_1 + \sigma\}$ . Therefore,  $a + b + \alpha_1 \notin \{\alpha_1, \alpha_1 + \sigma, a, a + \sigma, b, b + \sigma\}$ , as required.  $\diamond$

By Lemma 6.3 (2), the members of cardinality 2 in  $\text{local}(S, \alpha)$  form a graph with  $\frac{q}{2} - 1$  connected components  $G_1, \dots, G_{\frac{q}{2}-1}$  where the vertex set of  $G_j$  is

$$\{\beta_1^j, \beta_1^j + \sigma\} \cup \{\beta_2^j, \beta_2^j + \sigma\} \cup \{\beta_3^j, \beta_3^j + \sigma\}$$

where  $\beta_i^j, \beta_i^j + \sigma \in U_i - \{\alpha_i + \sigma\}$  and  $U_i = GF(q) - \{\alpha_i\}$  for  $i \in [3]$ . Furthermore,  $G_1, \dots, G_{\frac{q}{2}-1}$  are 6-cycles by Lemma 6.3 (2) (see Figure 3 for an illustration). As  $\frac{q}{2} - 1 \geq 3$ , without loss of generality, we may assume that  $\beta_1^1 = a, \beta_1^2 = b$ , and  $\beta_1^3 = a + b + \alpha_1$ , i.e.,  $G_1, G_2, G_3$  contain  $a, b, a + b + \alpha_1 \in U_1 - \{\alpha_1 + \sigma\}$ , respectively.

**Claim 2.** *The following statements hold:*

- (1)  $\beta_1^1 + \sigma = a + \sigma, \beta_2^1 + \sigma = a + \alpha_1 + \alpha_2 + \sigma$ , and  $\beta_3^1 = a + \alpha_1 + \alpha_3$ ,
- (2)  $\beta_2^2 = b + \alpha_1 + \alpha_2$  and  $\beta_2^2 + \sigma = b + \alpha_1 + \alpha_2 + \sigma$ , and
- (3)  $\beta_3^3 + \sigma = a + b + \alpha_3 + \sigma$ .

*Proof of Claim.* The claim follows from Lemma 6.3 (2).  $\diamond$

Now keep elements  $\beta_1^1, \beta_1^1 + \sigma, \beta_2^2, \beta_2^2 + \sigma, \beta_3^3$  in  $G_1, \beta_2^2, \beta_2^2 + \sigma$  in  $G_2$ , and  $\beta_3^3 + \sigma$  in  $G_3$  and delete the other elements from  $\text{local}(S, \alpha)$ . (see Figure 3 for an illustration; we keep only the circled elements). Let  $\mathcal{C}$  denote the

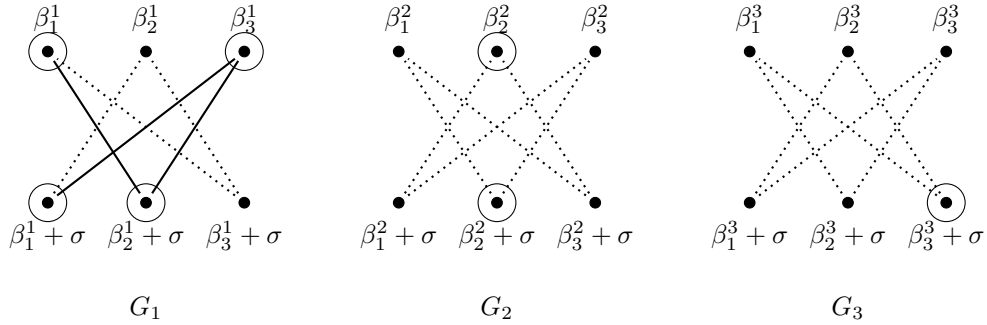


Figure 3: The subgraph of  $H_{n, \alpha}$  after deleting the vertices

resulting minor of  $\text{local}(S, \alpha)$ .

As  $\alpha_i + \sigma$  for  $i \in [n]$  are deleted, we know from Lemma 6.3 (1) that  $\mathcal{C}$  contains no member of size 1. By Lemma 6.3 (2),  $\mathcal{C}$  has 3 members of size 2:  $\{\beta_1^1, \beta_2^1 + \sigma\}$ ,  $\{\beta_3^1, \beta_1^1 + \sigma\}$ ,  $\{\beta_3^1, \beta_2^1 + \sigma\}$ , and these are the only ones. (see Figure 3 for an illustration; the 3 thick edges represent the 3 members of size 2 in  $\mathcal{C}$ ).

**Claim 3.**  $\{\beta_1^1, \beta_2^2, \beta_3^3 + \sigma\}$  and  $\{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}$  are the only members of size greater than 2 in  $\mathcal{C}$ .

*Proof of Claim.*  $\mathcal{C}$  contains at most one element in  $U_i$  for  $i \in [3]$  by Lemma 6.2, so  $\mathcal{C}$  has no member of size greater than 3. Moreover, a member of size 3 contains one element from each  $U_1, U_2, U_3$ . The subsets of size 3 that do not contain a member of size 2 but one element from each of  $U_1, U_2, U_3$  are the following:

$$\begin{aligned} & \{\beta_1^1, \beta_2^2, \beta_3^3\}, \{\beta_1^1, \beta_2^2 + \sigma, \beta_3^3\}, \{\beta_1^1, \beta_2^2, \beta_3^3 + \sigma\}, \{\beta_1^1, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}, \\ & \{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}, \{\beta_1^1 + \sigma, \beta_2^2, \beta_3^3 + \sigma\}, \{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}. \end{aligned}$$

By Lemma 6.2, a subset  $\{x_1, x_2, x_3\}$  where  $x_i \in U_i$  for  $i = 1, 2, 3$  is a member if and only if  $x_1 + x_2 + x_3 = \sigma + \alpha_1 + \alpha_2 + \alpha_3$ . Notice that  $\beta_1^1 + \beta_2^2 + \beta_3^3 = b + \alpha_2 + \alpha_3$  cannot be  $\sigma + \alpha_1 + \alpha_2 + \alpha_3$ , because  $b$  is not  $\alpha_1 + \sigma$  by our choice of  $b$ . This implies that  $\{\beta_1^1, \beta_2^2, \beta_3^3\}$  is not a member. Similarly,  $\{\beta_1^1, \beta_2^2 + \sigma, \beta_3^3\}$  is not a member, because  $b \neq \alpha_1$ . Notice also that  $\{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}$  is not a member, because  $\beta_1^1 + \sigma + \beta_2^2 + \sigma + \beta_3^3 + \sigma = a + b + \alpha_1 + \alpha_2 + \alpha_3 + \sigma$  cannot be  $\sigma + \alpha_1 + \alpha_2 + \alpha_3$  by our assumption that  $a \neq b$ . Observe that  $\beta_1^1 + \beta_2^2 + \beta_3^3 + \sigma = \sigma + \alpha_1 + \alpha_2 + \alpha_3$ , implying in turn that  $\{\beta_1^1, \beta_2^2, \beta_3^3 + \sigma\}$  and  $\{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}$  are members, whereas  $\{\beta_1^1, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}$  and  $\{\beta_1^1 + \sigma, \beta_2^2, \beta_3^3 + \sigma\}$  are not. Therefore,  $\{\beta_1^1, \beta_2^2, \beta_3^3 + \sigma\}$  and  $\{\beta_1^1 + \sigma, \beta_2^2 + \sigma, \beta_3^3 + \sigma\}$  are the only members of size at least 3 in  $\mathcal{C}$ , as required.  $\diamond$

Now that we have characterized all members of  $\mathcal{C}$ , we know that the incidence matrix of the corresponding minor  $\mathcal{C}$  is the following 0,1 matrix:

$$\begin{pmatrix} \beta_1^1 & \beta_2^2 + \sigma & \beta_3^3 & \beta_1^1 + \sigma & \beta_3^3 + \sigma & \beta_2^2 & \beta_2^2 + \sigma \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Contracting the elements corresponding to  $\beta_2^2, \beta_2^2 + \sigma$  from  $\mathcal{C}$ , we obtain a  $C_5^2$  minor. Since  $\mathcal{C}$  is a minor of  $\text{local}(S, \alpha)$ , we deduce that  $\text{local}(S, \alpha)$  also has  $C_5^2$  as a minor, as required.  $\square$

**Lemma 8.2.** *Up to isomorphism,  $\text{Matroid}(A_3)$  is the unique minor-minimal matroid with distinct circuits that have a nonempty intersection. Consequently, if two distinct circuits of a matroid intersect, then the matroid has  $\text{Matroid}(A_3)$  as a minor.*

*Proof.* Let  $M$  be a minor-minimal matroid over ground set  $E$  with distinct circuits that intersect.

Let  $C_1, C_2$  be any pair of distinct circuits that intersect. Observe that  $C_1 \cup C_2 = E$ , for if not,  $M \setminus \overline{C_1 \cup C_2}$  would be a proper matroid minor with distinct circuits, namely  $C_1, C_2$ , that intersect, which cannot be the case. Observe further that  $I := C_1 \cap C_2$ , which by assumption is nonempty, has size one. For if not, for any  $e \in I$ ,  $M/(I - \{e\})$  would be a proper matroid minor with distinct circuits, namely  $C_1 - (I - \{e\}), C_2 - (I - \{e\})$ , that intersect, which cannot be the case.

In summary, every two circuits that intersect, have  $E$  as their union and an intersection of size one. Since  $M$  is a matroid, there is a circuit  $C_3 \subseteq (C_1 \cup C_2) - \{e\}$ . Clearly,  $C_3$  intersects both  $C_1, C_2$ . Thus,  $|C_1 \cap C_3| = |C_2 \cap C_3| = 1$  and  $C_1 \cup C_3 = C_2 \cup C_3 = E$ . It can be readily checked that  $|C_1| = |C_2| = 2$ , implying in turn that  $M \cong \text{Matroid}(A_3)$ , as required.  $\square$



Now we are ready to prove Theorem 1.3. The crux of the proof is outlined as follows. If  $\text{mult}(S)$  is ideal where  $S$  is a vector space over  $GF(2^k)$  for some  $k > 2$ , then  $\text{mult}(S)$  has no  $C_5^2$  as a minor. Then  $\text{Matroid}(S)$  has no two distinct circuits that intersect, by Lemmas 8.1 and 8.2. Then we use Lemma 3.4 to argue that  $S$  has a basis with vectors of pairwise disjoint supports.

**Proof of Theorem 1.3.** Take an integer  $n \geq 1$ . Let  $q$  be a power of 2 larger than 4, and let  $S \subseteq GF(q)^n$  be a vector space over  $GF(q)$ . (iii) $\Rightarrow$ (ii): Since  $\text{mult}(S)$  contains no  $C_5^2$  as a minor,  $\text{Matroid}(S)$  has no  $\text{Matroid}(A_3)$  as a matroid minor, by Lemma 8.1. Thus, every two distinct circuits of  $\text{Matroid}(S)$  must be disjoint, by Lemma 8.2. This implies that  $\text{Matroid}(S)$  is the cycle matroid of a graph whose blocks are bridges and circuits, so (ii) follows from Lemma 3.4. (i) $\Rightarrow$ (iii) follows immediately from the fact that  $C_5^2$  is non-ideal. (ii) $\Rightarrow$ (i) follows immediately from Lemma 4.3.  $\square$

## 9 The Replication and $\tau = 2$ Conjectures

Let  $\mathcal{C}$  be a clutter over ground set  $V$ . Given the weights of the elements  $w \in \mathbb{Z}_+^V$ , the minimum weight of a cover of  $\mathcal{C}$  can be computed by the following integer linear program:

$$\tau(\mathcal{C}, w) = \min \{w^\top x : M(\mathcal{C})x \geq \mathbf{1}, x \in \mathbb{Z}_+^V\}$$

A dual of this integer program is given by the following:

$$\nu(\mathcal{C}, w) = \max \{\mathbf{1}^\top y : M(\mathcal{C})^\top y \leq w, y \in \mathbb{Z}_+^{\mathcal{C}}\},$$

and this computes the maximum size of a *packing* of members of  $\mathcal{C}$  such that each element  $v$  appears in at most  $w_v$  members in the packing. The linear programming relaxations of these two integer programs are the following primal-dual pair:

$$\begin{array}{ll} \tau^*(\mathcal{C}, w) = & \text{minimize} & w^\top x & \nu^*(\mathcal{C}, w) = & \text{maximize} & \mathbf{1}^\top y \\ & \text{subject to} & M(\mathcal{C})x \geq \mathbf{1} & & \text{subject to} & M(\mathcal{C})^\top y \leq w \\ & & x \geq \mathbf{0} & & & y \geq \mathbf{0} \end{array}$$

By linear programming duality, we have that

$$\tau(\mathcal{C}, w) \geq \tau^*(\mathcal{C}, w) = \nu^*(\mathcal{C}, w) \geq \nu(\mathcal{C}, w).$$

Although  $\tau^*(\mathcal{C}, w) = \nu^*(\mathcal{C}, w)$  always holds, it is not always the case that  $\tau(\mathcal{C}, w) = \nu(\mathcal{C}, w)$ . If  $\tau(\mathcal{C}, w) = \nu(\mathcal{C}, w)$  holds for every  $w \in \mathbb{Z}_+^V$ , we say that  $\mathcal{C}$  has the max-flow min-cut property. In fact, the max-flow min-cut property is equivalent to the *total dual integrality* for the integer program computing  $\tau(\mathcal{C}, w)$ . Namely,  $\mathcal{C}$  has the max-flow min-cut property if and only if the linear system  $M(\mathcal{C})x \geq \mathbf{1}, x \geq \mathbf{0}$  is *totally dual integral*. This implies that if  $\mathcal{C}$  has the max-flow min-cut property, then  $Q(\mathcal{C})$  is integral [16, 19] and thus  $\mathcal{C}$  is ideal.

As the max-flow min-cut property is a special case of idealness, a natural question is as to when a clutter has the max-flow min-cut property. In this section, we characterize when the multipartite uniform clutter of a vector space over a finite field has the max-flow min-cut property.

The readers may have already noticed that Theorem 1.4 is similar to Theorem 1.1 and Theorem 1.3. As a direct corollary of these theorems, we obtain the following:

**Theorem 9.1.** Take a prime power  $q$  other than 2, 4, and let  $S$  be a vector space over  $GF(q)$ . Then  $\text{mult}(S)$  is ideal if and only if  $\text{mult}(S)$  has the max-flow min-cut property.

Unlike the case when  $q \notin \{2, 4\}$ , there is a vector space over  $GF(4)$  whose multipartite uniform clutter is ideal but does not have the max-flow min-cut property. The element set of  $GF(4)$  can be represented as  $\{0, 1, a, b\}$  where  $a$  and  $b$  are the numbers satisfying the following addition and multiplication tables:

$$\begin{array}{c|cccc} + & 0 & 1 & a & b \\ \hline 0 & 0 & 1 & a & b \\ 1 & 1 & 0 & b & a \\ a & a & b & 0 & 1 \\ b & b & a & 1 & 0 \end{array} \quad \begin{array}{c|cccc} \times & 0 & 1 & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a & b \\ a & 0 & a & b & 1 \\ b & 0 & b & 1 & a \end{array}$$

**Example.** Consider  $S = \langle (1, 1, 0), (1, 0, 1) \rangle \subseteq GF(4)^3$ . Then

$$S = \left\{ \begin{array}{l} (0, 0, 0), (1, 1, 0), (a, a, 0), (b, b, 0), (1, 0, 1), (0, 1, 1), (b, a, 1), (a, b, 1), \\ (a, 0, a), (b, 1, a), (0, a, a), (1, b, a), (b, 0, b), (a, 1, b), (1, a, b), (0, b, b) \end{array} \right\}.$$

One can check by using PORTA [28] that  $\{x \in \mathbb{R}_+^{12} : M(\text{mult}(S))x \geq \mathbf{1}\}$  is an integral polyhedron, so  $\text{mult}(S)$  is ideal. Notice further that  $\text{mult}(S)$  does not have the max-flow min-cut property, since  $S$  contains

$$\{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\} \cong R_{1,1}$$

as a restriction and so  $\text{mult}(S)$  has  $Q_6$  as a minor by Lemma 2.4.

We say that clutter  $\mathcal{C}$  packs if  $\tau(\mathcal{C}, \mathbf{1}) = \nu(\mathcal{C}, \mathbf{1})$ . We say that  $\mathcal{C}$  has the *packing property* if every minor of  $\mathcal{C}$  packs. It was observed in [11] that minimally non-ideal clutters do not pack due to Lehman's theorem [22] and that if a clutter has the packing property, then it is ideal. Moreover, notice that the packing property is a relaxed notion of the max-flow min-cut property. Here, the *Replication Conjecture* predicts that the packing property implies the max-flow min-cut property. We answer the conjecture in the affirmative for the class of multipartite uniform clutters from coordinate subspaces.

**Proof of Corollary 1.5.** Take a prime power  $q$ , and let  $S$  be a vector space over  $GF(q)$ . Suppose that  $\text{mult}(S)$  has the packing property. Then every minor of  $\text{mult}(S)$  packs and is ideal. Note that  $\Delta_3$  is non-ideal. Moreover, it is easy to check that  $\tau(Q_6, \mathbf{1}) = 2$  and  $\nu(Q_6, \mathbf{1}) = 1$ , which means that  $Q_6$  does not pack. Therefore,  $\text{mult}(S)$  has none of  $\Delta_3$  and  $Q_6$  as a minor. Then it follows from Theorem 1.4 that  $\text{mult}(S)$  has the max-flow min-cut property.  $\square$

Next we consider the  $\tau = 2$  Conjecture [11] which predicts that a stronger statement than the Replication Conjecture holds true. We call a clutter *minimally non-packing* if it does not have the packing property but every proper minor of it does. It is known that a minimally non-packing clutter is either ideal or minimally non-ideal [11]. Here, the  $\tau = 2$  Conjecture is that if a clutter  $\mathcal{C}$  is ideal and minimally non-packing, then its covering number, defined as  $\tau(\mathcal{C}, \mathbf{1})$ , is two. We show that if the multipartite uniform clutter of a coordinate subspace is ideal and minimally non-packing, then its covering number is two.

**Proof of Corollary 1.6.** Take a prime power  $q$ , and let  $S$  be a vector space over  $GF(q)$ . Suppose that  $\text{mult}(S)$  is ideal and minimally non-packing. As  $\text{mult}(S)$  does not pack, it does not have the max-flow min-cut property. Then by Theorem 1.4,  $\text{mult}(S)$  has  $\Delta_3$  or  $Q_6$  as a minor. Note that as  $\Delta_3$  is non-ideal but  $\text{mult}(S)$  is ideal,  $\text{mult}(S)$  has no  $\Delta_3$  as a minor. Then it follows that  $\text{mult}(S)$  has  $Q_6$  as a minor. Since  $Q_6$  itself does not pack and every proper minor of  $\text{mult}(S)$  packs,  $\text{mult}(S)$  is isomorphic to  $Q_6$ . In fact,  $Q_6$  is ideal and minimally non-packing, and it has covering number two, as required.  $\square$

## Acknowledgements and Funding

We would like to thank Gérard Cornuéjols for helpful discussions. This research is supported, in part, by KAIST Starting Fund (KAIST-G04220016), FOUR Brain Korea 21 Program (NRF-5199990113928), and National Research Foundation of Korea (NRF-2022M3J6A1063021).

## References

- [1] Abdi, A. and Cornuéjols, G.: The max-flow min-cut property and  $\pm 1$ -resistant sets. *Discrete Applied Mathematics*, **289**, 455–476 (2020)
- [2] Abdi, A. and Cornuéjols, G.: Idealness and 2-resistant sets. *Operations Research Letters*, **47**(5), 358–362 (2019)
- [3] Abdi, A., Cornuéjols, G., Lee, D.: Resistant sets in the unit hypercube. *Math. Oper. Res.* **46**(1), 82–114 (2020)
- [4] Abdi, A., Cornuéjols, G., Guričanová, N., Lee, D.: Cuboids, a class of clutters. *J. Combin. Theory Ser. B* **142**, 144–209 (2020)
- [5] Abdi, A., Cornuéjols, G., Pashkovich, K.: Ideal clutters that do not pack. *Math. Oper. Res.* **43**(2), 533–553 (2018)
- [6] Berge, C.: Balanced matrices. *Math. Program.* **2**(1), 19–31 (1972)
- [7] Bondy, J.A. and Murty, U.S.R.: *Graph Theory*. Springer (2008)
- [8] Brylawski, T.H.: A combinatorial model for series-parallel networks. *Trans. Amer. Math. Soc.* **154**, 1–22 (1971)
- [9] Conforti, M. and Cornuéjols, G.: Clutters that pack and the max-flow min-cut property: a conjecture. (Available online at <http://www.dtic.mil/dtic/tr/fulltext/u2/a277340.pdf>) *The Fourth Bel-lairs Workshop on Combinatorial Optimization* (1993)
- [10] Cornuéjols, G.: *Combinatorial Optimization, Packing and Covering*. SIAM, Philadelphia (2001)
- [11] Cornuéjols, G., Guenin, B., Margot, F.: The packing property. *Math. Program.* **89**(1), 113–126 (2000)

- [12] Cornuéjols, G. and Novick, B.: Ideal 0,1 matrices. *J. Combin. Theory Ser. B* **60**, 145–157 (1994)
- [13] Ding, G., Feng, L., Zang, W.: The complexity of recognizing linear systems with certain integrality properties. *Math. Program.* **114**, 321–334 (2008)
- [14] Duffin, R.J.: The extremal length of a network. *J. Math. Analysis and Appl.* **5**(2), 200–215 (1962)
- [15] Edmonds, J. and Fulkerson, D.R.: Bottleneck extrema. *J. Combin. Theory Ser. B* **8**, 299–306 (1970)
- [16] Edmonds, J. and Giles, R.: A min-max relation for submodular functions on graphs. *Ann. Discrete Math.* **1**, 185–204 (1977)
- [17] Edmonds, J. and Johnson, E.L.: Matchings, Euler tours and the Chinese postman problem. *Math. Program.* **5**, 88–124 (1973)
- [18] Guenin, B.: A characterization of weakly bipartite graphs. *J. Combin. Theory Ser. B* **83**, 112–168 (2001)
- [19] Hoffman, A.J.: A generalization of max flow-min cut. *Math. Program.* **6**(1), 352–359 (1974)
- [20] Hoffman, A.J. and Kruskal J.B.: Integral boundary points of convex polyhedra. In *Linear inequalities and related systems* (eds. Kuhn H.W. and Tucker A.W.). *Ann. Math. Studies* **38**, 223–246 (1956)
- [21] Lehman, A.: On the width-length inequality. *Math. Program.* **17**(1), 403–417 (1979)
- [22] Lehman, A.: The width-length inequality and degenerate projective planes. *DIMACS Vol. 1*, 101–105 (1990)
- [23] Lovász, L.: Minimax theorems for hypergraphs. *Lecture Notes in Mathematics.* **411**, Springer-Verlag 111–126 (1972)
- [24] Lovász, L.: Normal Hypergraphs and the Perfect Graph Conjecture. *Discrete Math.* **2**, 253–267 (1972)
- [25] Lucchesi, C.L. and Younger, D.H.: A minimax relation for directed graphs. *J. London Math. Soc.* **17** (2), 369–374 (1978)
- [26] Menger, K.: Zur allgemeinen Kurventheorie. *Fundamenta Mathematicae* **10**, 96–115 (1927)
- [27] Oxley, J.: *Matroid Theory*, second edition. Oxford University Press, New York (2011)
- [28] Christof, T. and Löbel, A.: PORTA - A Polyhedron Representation and Transformation Algorithm, <http://porta.zib.de/>.
- [29] Seymour, P.D.: A forbidden minor characterization of matroid ports. *Quart. J. Math.* **27**(4), 407–413 (1976)
- [30] Seymour, P.D.: The forbidden minors of binary clutters. *J. London Math. Society* **2**(12), 356–360 (1976)
- [31] Seymour, P.D.: Matroids and multicommodity flows. *Europ. J. Combinatorics* **2**, 257–290 (1981)
- [32] Seymour, P.D.: Sums of circuits. *Graph Theory and Related Topics* (Bondy, J.A. and Murty, U.S.R., eds), Academic Press, New York, 342–355 (1979)
- [33] Seymour, P.D.: The matroids with the max-flow min-cut property. *J. Combin. Theory Ser. B* **23**, 189–222 (1977)

## A Proof of Lemma 5.3

We will prove Lemma 5.3 that characterizes graphs with no  $K_4/e$  as a graph minor. Given a graph  $G = (V, E)$  and its block decomposition, we may associate  $G$  with a bipartite graph  $\mathcal{B}(G)$  where

- a part of the bipartition of  $\mathcal{B}(G)$  consists of the cut-vertices of  $G$ ,
- the other part consists of the blocks of  $G$ , and
- a cut-vertex  $u$  and a block  $B$  are adjacent in  $\mathcal{B}(G)$  if  $u$  is a vertex in  $B$ .

It is well-known that  $\mathcal{B}(G)$  is a tree all of whose leaves are blocks of  $G$  (see [7]). We call a vertex of  $G$  that is not a cut vertex an *internal vertex*.

**Proof of Lemma 5.3.** Assume that  $G$  contains no  $K_4/e$  as a graph minor. We will prove by induction on the number of edges that each block of  $G$  is a bridge, a circuit, or a subdivision of  $A_t$  for some  $t \geq 3$ . The base case is trivial. For the induction step, we may assume that  $G$  has at least 3 edges. If  $G$  has more than one block, a block of  $G$  has less edges than  $G$  does, so we may apply the induction hypothesis to each block of  $G$ . Thus we may assume that  $G$  is 2-vertex-connected, in which case,  $G$  has no loop.

Let  $e$  be an edge of  $G$ . By the induction hypothesis, each block of  $G - \{e\}$  is a bridge, a circuit, or a subdivision of  $A_t$  for some  $t \geq 3$ . Moreover, since  $G$  has no loop,  $G - \{e\}$  has no loop either. We first prove the following claim:

**Claim 1.** *Either  $\mathcal{B}(G - \{e\})$  is a single vertex, i.e.,  $G - \{e\}$  is 2-vertex-connected, or  $\mathcal{B}(G - \{e\})$  is a path whose two ends are blocks of  $G$  and  $e$  is incident to internal vertices of the two end blocks of the path.*

*Proof of Claim.* We may assume that  $G - \{e\}$  has at least two blocks. Since  $G$  is 2-vertex-connected,  $e$  connects two distinct blocks  $B_1, B_2$  of  $G - \{e\}$ . Recall that  $\mathcal{B}(G - \{e\})$  is a tree, so there is a unique path between  $B_1$  and  $B_2$  in  $\mathcal{B}(G - \{e\})$ . Then, after putting  $e$  back, the blocks of  $G - \{e\}$  on the path between  $B_1$  and  $B_2$  become a single block in  $G$ . In fact, since  $G$  is 2-vertex-connected,  $G$  has no other block. This implies that  $G - \{e\}$  has no block other than the ones on  $C$ . So,  $\mathcal{B}(G - \{e\})$  contains no vertex outside  $C$ , and therefore,  $\mathcal{B}(G - \{e\})$  is a path where  $B_1, B_2$  are its two ends. If  $e$  is not incident to an internal vertex of  $B_1$ , then  $e$  is incident to the cut-vertex of  $B_1$ , implying that  $B_1$  is separated from  $B_2$  in  $G$ , a contradiction. Thus  $e$  is incident to an internal vertex of  $B_1$ . Similarly,  $e$  is incident to an internal vertex of  $B_2$ , as required.  $\diamond$

Next, we claim the following:

**Claim 2.** *All but at most one block of  $G - \{e\}$  are bridges.*

*Proof of Claim.* We may assume that  $G - \{e\}$  has at least two blocks. Then, by Claim 1,  $\mathcal{B}(G - \{e\})$  is a path  $B_1, u_1, B_2, \dots, u_{k-1}, B_k$  for some  $k \geq 2$ , where  $B_1, \dots, B_k$  are the blocks of  $G - \{e\}$  and  $u_\ell$  is the cut-vertex separating  $B_\ell$  and  $B_{\ell+1}$  for  $\ell \in [k-1]$ . Moreover, by Claim 1,  $e = u_0 u_k$ , where  $u_0$  is an internal vertex of  $B_1$  and  $u_k$  is an internal vertex of  $B_k$ .

Suppose for a contradiction that  $G - \{e\}$  has two blocks that are not bridges. Then  $B_i, B_j$  for some distinct  $i, j \in [k]$  are not bridges. In particular,  $B_i$  and  $B_j$  have cycles  $C_i$  and  $C_j$ , respectively. Here, both  $C_i$  and  $C_j$  have

at least two edges as  $G - \{e\}$  has no loop. After contracting the edges of  $B_\ell$  for  $\ell \in [k] - \{i, j\}$  from  $G - \{e\}$ , the vertices in  $B_1, \dots, B_{i-1}$  are identified with  $u_{i-1}$ , the vertices in  $B_{i+1}, \dots, B_{j-1}$  are identified with  $u_{j-1}$ , and the vertices in  $B_{j+1}, \dots, B_k$  are identified with  $u_j$ . Therefore, the resulting graph is  $u_{i-1}, B_i, u_{j-1}, B_j, u_j$ , where  $u_{i-1}$  and  $u_j$  are internal vertices of  $B_i$  and  $B_j$ , respectively, and  $u_{j-1}$  is the cut-vertex separating  $B_i, B_j$ . Notice that  $e$  connects  $u_{i-1}$  and  $u_j$  after the contraction, because  $u_0, u_k$  were identified with  $u_{i-1}, u_j$ , respectively (see Figure 4 for an illustration). We then delete the edges outside of the cycles  $C_i, C_j$ . After adding  $e$  back, we obtain a

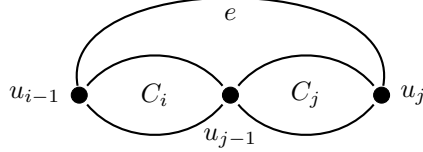


Figure 4:  $e = u_{i-1}u_j$

subdivision of  $K_4/e$ , a contradiction as  $G$  has no  $K_4/e$  as a graph minor. Therefore, at most one block of  $G - \{e\}$  is a bridge.  $\diamond$

If every block of  $G - \{e\}$  is a bridge, then it follows from Claim 1 that  $G$  is a circuit. Thus we may assume that a block  $B$  of  $G - \{e\}$  is a circuit or a subdivision of  $A_t$  for some  $t \geq 3$ . Then, by Claim 2, the other blocks of  $G - \{e\}$  are bridges.

**Claim 3.**  $G$  is the union of  $B$  and a path  $P$  whose ends are two vertices in  $B$  and the other vertices are disjoint from  $V(B)$ .

*Proof of Claim.* It follows from Claim 1 that  $e$  and the bridges of  $G - \{e\}$  form a path  $P$  connecting two vertices of  $B$ . An interior vertex of  $P$ , if exists, is in a block of  $G - \{e\}$  other than  $B$ , so it is not contained in  $V(B)$ , as required.  $\diamond$

As  $B$  is a circuit or a subdivision of  $A_t$  for some  $t \geq 3$ ,  $B$  is a disjoint union of internally vertex-disjoint  $uv$ -paths for some distinct  $u, v \in V(B)$ . Let  $P_1, \dots, P_t$  be the  $uv$ -paths.

**Claim 4.** If  $t = 2$ ,  $G$  is a subdivision of  $A_3$ .

*Proof of Claim.* If  $t = 2$ ,  $B$  is a circuit and  $P$  connects two vertices on the cycle by Claim 3. So,  $G$  is the union of three internally vertex-disjoint paths connecting the two vertices, implying in turn that  $G$  is a subdivision of  $A_3$ .  $\diamond$

By Claim 4, we may assume that  $t \geq 3$ . We will show that  $P$  is also a path connecting  $u$  and  $v$ , thereby proving that  $G$  is a subdivision of  $A_{t+1}$ , obtained from  $uv$ -paths  $P_1, \dots, P_t, P$ .

**Claim 5.**  $P$  is an  $uv$ -path.

*Proof of Claim.* Suppose for a contradiction that  $P$  is not a  $uv$ -path. Then one of  $P$ 's two ends is not in  $\{u, v\}$ .

First, consider the case when one end of  $P$  is in  $\{u, v\}$ . Without loss of generality, we may assume that one end of  $P$  is  $u$  and the other end is  $w \in V - \{u, v\}$ . Without loss of generality, assume that  $w$  is on  $P_1$ . Then

the subgraph of  $G$  obtained after deleting the edges  $E - E(P) \cup E(P_1) \cup E(P_2) \cup E(P_3)$  (see Figure 5 for an illustration) is a subdivision of  $K_4/e$ , contradicting the assumption that  $G$  has no  $K_4/e$  as a graph minor.

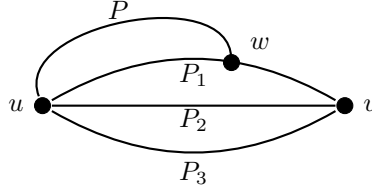


Figure 5:  $w \notin \{u, v\}$

Now consider the case when both ends of  $P$  are not in  $\{u, v\}$ . Let the ends of  $P$  be  $w_1, w_2 \in V - \{u, v\}$ . There are two cases to consider:  $w_1, w_2$  are on the same  $uv$ -path of  $B$ , or  $w_1, w_2$  are on different  $uv$ -paths. If  $w_1, w_2$  are on the same  $uv$ -path, we may assume that they are on  $P_1$  without loss of generality. In this case, deleting the edges  $E - E(P) \cup E(P_1) \cup E(P_2) \cup E(P_3)$  and contracting the edges of the  $uw_1$ -path on  $P_1$  (see Figure 6 for an illustration), we obtain a subdivision of  $K_4/e$ , a contradiction.

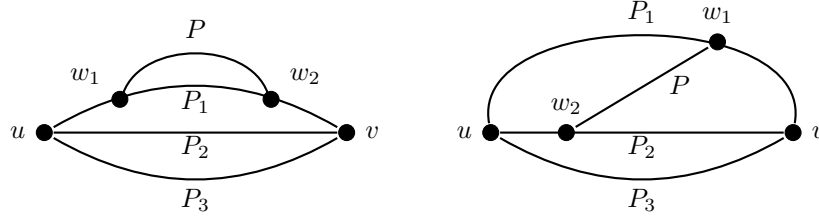


Figure 6:  $w_1, w_2 \notin \{u, v\}$

If  $w_1, w_2$  are on different  $uv$ -paths, we may assume that  $w_1$  is on  $P_1$  and  $w_2$  is on  $P_2$  without loss of generality. Deleting the edges  $E - E(P) \cup E(P_1) \cup E(P_2) \cup E(P_3)$  and contracting the edges of  $P$  (see Figure 6 for an illustration), we obtain a subdivision of  $K_4/e$ , a contradiction as  $G$  has no  $K_4/e$  as a graph minor.  $\diamond$

By Claims 3 and 5,  $P$  is an  $uv$ -path that is internally vertex-disjoint from  $P_1, \dots, P_t$ , implying in turn that  $G$  is a subdivision of  $A_{t+1}$ . This finishes the proof.  $\square$

## B Proof of Lemma 6.3

**Proof of Lemma 6.3.** (1) By Lemma 6.2,  $C$  is a member of size 1 if and only if  $C = \{\sigma + \alpha_i\}$  for some  $i \in [n]$ . Therefore,  $\{\alpha_1 + \sigma\}, \dots, \{\alpha_n + \sigma\}$  are the members of size 1 in  $\text{local}(S, \alpha)$ , as required.

(2) First, we will argue that a member of cardinality 2 contains none of  $\alpha_1 + \sigma, \dots, \alpha_n + \sigma$ . Let  $\{u, v\}$  be a member of size 2 where  $u \in U_i$  and  $v \in U_j$  for some  $i \neq j$ . Then we get  $u + v = \sigma + \alpha_i + \alpha_j$  by Lemma 6.2. If  $u = \alpha_i + \sigma$ , then  $v = \alpha_j$ , contradicting the assumption that  $v \in U_j = GF(q) - \{\alpha_j\}$ . Therefore, the members of cardinality 2 are contained in  $U' := (U_1 - \{\alpha_1 + \sigma\}) \cup \dots \cup (U_n - \{\alpha_n + \sigma\})$ . Notice that we have preserved

the symmetry between  $U_1 - \{\alpha_1 + \sigma\}, \dots, U_n - \{\alpha_n + \sigma\}$  and that  $U_1 - \{\alpha_1 + \sigma\}$  is not different from the other  $U_i - \{\alpha_i + \sigma\}$ 's.

Observe that  $U_1 - \{\alpha_1 + \sigma\} = GF(q) - \{\alpha_1, \alpha_1 + \sigma\}$  has  $q - 2$  elements and that  $U_1 - \{\alpha_1 + \sigma\}$  can be partitioned as  $U_1 - \{\alpha_1 + \sigma\} = \{\beta_1^1, \beta_1^1 + \sigma\} \cup \dots \cup \{\beta_1^{\frac{q}{2}-1}, \beta_1^{\frac{q}{2}-1} + \sigma\}$ , with  $\frac{q}{2} - 1$  sets of cardinality 2, where  $\beta_1^1, \dots, \beta_1^{\frac{q}{2}-1}$  are distinct elements. For  $i = 2, \dots, n$  and  $j = 1, \dots, \frac{q}{2} - 1$ , we denote by  $\beta_i^j \in U_i$  the element satisfying  $\beta_i^j = \beta_1^j + \alpha_1 + \alpha_i$ .

**Claim 1.**  $U_i - \{\alpha_i + \sigma\} = \{\beta_i^1, \beta_i^1 + \sigma\} \cup \dots \cup \{\beta_i^{\frac{q}{2}-1}, \beta_i^{\frac{q}{2}-1} + \sigma\}$  for  $i = 1, \dots, n$ .

*Proof of Claim.* We may assume that  $i \geq 2$ . Let  $j, \ell$  be distinct indices in  $[\frac{q}{2} - 1]$ . As  $\beta_1^j \neq \beta_1^\ell$ , we get  $\beta_i^j \neq \beta_i^\ell$ . Similarly,  $\beta_1^j \neq \beta_1^\ell + \sigma$  implies  $\beta_i^j \neq \beta_i^\ell + \sigma$ . Therefore,  $\beta_i^1, \beta_i^1 + \sigma, \dots, \beta_i^{\frac{q}{2}-1}, \beta_i^{\frac{q}{2}-1} + \sigma$  are distinct elements, so  $\{\beta_i^1, \beta_i^1 + \sigma\}, \dots, \{\beta_i^{\frac{q}{2}-1}, \beta_i^{\frac{q}{2}-1} + \sigma\}$  partition  $U_i - \{\alpha_i + \sigma\}$ , as required.  $\diamond$

By Claim 1, each element in  $U'$  is  $\beta_i^j$  or  $\beta_i^j + \sigma$  for some  $i \in [n]$  and  $j \in [\frac{q}{2} - 1]$ . Now we are ready to characterize what the members of size 2 are.

**Claim 2.** Let  $u, v$  be distinct elements in  $U'$ . Then  $\{u, v\}$  is a member in  $\text{local}(S, \alpha)$  if and only if for some  $j \in [\frac{q}{2} - 1]$  and distinct  $i, k \in [n]$ , we have  $u = \beta_i^j$  and  $v = \beta_k^j + \sigma$  or  $u = \beta_i^j + \sigma$  and  $v = \beta_k^j$ .

*Proof of Claim.* ( $\Leftarrow$ ) Without loss of generality, we may assume that  $j = 1, i = 1$ , and  $k = 2$ . As  $\beta_2^1 = \beta_1^1 + \alpha_1 + \alpha_2$ , we have  $\beta_1^1 + \beta_2^1 + \sigma = \alpha_1 + \alpha_2 + \sigma$ . So, by Lemma 6.2,  $\{u, v\}$  is a member.

( $\Rightarrow$ ) Without loss of generality, we may assume that  $u \in U_1, v \in U_2$ . Then  $u = \beta_1^j$  or  $u = \beta_1^j + \sigma$  for some  $j \in [\frac{q}{2} - 1]$ . If  $u = \beta_1^j$ , then by Lemma 6.2,  $v = \beta_1^j + \alpha_1 + \alpha_2 + \sigma = \beta_2^j + \sigma$ . Similarly, if  $u = \beta_1^j + \sigma$ , we can argue that  $v = \beta_2^j$ , as required.  $\diamond$

For  $j \in [\frac{q}{2} - 1]$ , let  $G_j$  denote the graph induced by the elements in  $\{\beta_1^j, \dots, \beta_n^j\} \cup \{\beta_1^j + \sigma, \dots, \beta_n^j + \sigma\}$ . By Claim 2, the edge set of  $G_j$  is precisely  $\{\{\beta_i^j, \beta_k^j + \sigma\} : i \neq k\}$ . Moreover, Claim 2 also implies that there is no edge between  $G_j$  and  $G_\ell$  if  $j \neq \ell$ , as required.  $\square$