

A new matroid lift construction and an application to group-labeled graphs

Zach Walsh

Department of Mathematics
Louisiana State University
Baton Rouge, U.S.A.

walsh@lsu.edu

Submitted: Apr 16, 2021; Accepted: Nov 29, 2021; Published: Jan 28, 2022

© The author. Released under the CC BY-ND license (International 4.0).

Abstract

A well-known result of Brylawski constructs an elementary lift of a matroid M from a linear class of circuits of M . We generalize this result by constructing a rank- k lift of M from a rank- k matroid on the set of circuits of M . We conjecture that every lift of M arises via this construction.

We then apply this result to group-labeled graphs, generalizing a construction of Zaslavsky. Given a graph G with edges labeled by a group, Zaslavsky's lift matroid K is an elementary lift of the graphic matroid $M(G)$ that respects the group-labeling; specifically, the cycles of G that are circuits of K coincide with the cycles that are balanced with respect to the group-labeling. For $k \geq 2$, when does there exist a rank- k lift of $M(G)$ that respects the group-labeling in this same sense? For abelian groups, we show that such a matroid exists if and only if the group is isomorphic to the additive group of a non-prime finite field.

Mathematics Subject Classifications: 05B35

1 Introduction

This paper is concerned with using structure on the circuits of a matroid M to construct a new matroid on the ground set of M . For example, a collection \mathcal{C} of circuits of a matroid M is a *linear class* if, whenever C_1 and C_2 are circuits in \mathcal{C} so that $|C_1 \cup C_2| - r_M(C_1 \cup C_2) = 2$, then every circuit C of M contained in $C_1 \cup C_2$ is also in \mathcal{C} . Brylawski [2, Prop. 7.4.15] showed that, for each linear class \mathcal{C} of circuits of a matroid M , one can construct a matroid M' on $E(M)$ with rank at most one greater than $r(M)$. Moreover, this matroid M' is an *elementary lift* of M , so there is a matroid P with ground set $E(M) \cup \{e\}$ so that $P \setminus e = M'$ and $P/e = M$.

Theorem 1 (Brylawski '86). *Let M be a matroid, and let \mathcal{C} be a linear class of circuits of M . Then the function $r_{M'}$ defined, for all $X \subseteq E(M)$, by*

$$r_{M'}(X) = \begin{cases} r_M(X) & \text{if each circuit of } M|X \text{ is in } \mathcal{C}, \\ r_M(X) + 1 & \text{otherwise} \end{cases}$$

is the rank function of an elementary lift M' of M . Moreover, every elementary lift of M can be obtained in this way.

Note that \mathcal{C} is precisely the set of circuits of M that are also circuits of M' . Zaslavsky [12] applied this construction to group-labeled graphs (also called gain graphs), by showing that for each graph G with edges labeled by a group, one can use the group-labeling to obtain a natural linear class \mathcal{B} of circuits of the graphic matroid $M(G)$. The circuits in \mathcal{B} are the *balanced* cycles of G with respect to the group-labeling, and the pair (G, \mathcal{B}) is a *biased graph*. So, via Brylawski's construction, each graph G with edges labeled by a group naturally leads to an elementary lift M of $M(G)$; Zaslavsky calls this the *lift matroid* of the biased graph (G, \mathcal{B}) . We will define this terminology in greater detail in Section 2. Note that M respects the group-labeling in the sense that a cycle of G is a circuit of M if and only if it is balanced.

The goal of this paper is to generalize the constructions of Brylawski and Zaslavsky to rank- k lifts for $k \geq 2$. A matroid K is a *lift* of a matroid M if there is a matroid P and a subset X of $E(P)$ so that $P \setminus X = K$ and $P/X = M$. If $r(K) - r(M) = k$, then K is a *rank- k lift* of M . We prove the following generalization of Brylawski's construction, by defining a lift of a matroid M using a given matroid N on the set of circuits of M . Just as Brylawski's construction only applies to a linear class of circuits, the matroid N must satisfy some necessary dependencies of the circuits of M . We say that a collection \mathcal{C}' of circuits of M is *perfect* if $|\cup_{C \in \mathcal{C}'} C| - r_M(\cup_{C \in \mathcal{C}'} C) = |\mathcal{C}'|$, and no circuit in \mathcal{C}' is contained in the union of the others. The matroid N must satisfy the natural condition that if a circuit C of M is contained in the union of the circuits of a perfect collection \mathcal{C}' , then C is spanned by \mathcal{C}' in N .

Theorem 2. *Let M be a matroid, and let N be a matroid on the set of circuits of M so that*

(2*) *if \mathcal{C}' is a perfect collection of circuits of M , then each circuit C' of M contained in $\cup_{C \in \mathcal{C}'} C$ satisfies $C' \in \text{cl}_N(\mathcal{C}')$.*

Then the function r_{M^N} defined, for all $X \subseteq E(M)$, by

$$r_{M^N}(X) = r_M(X) + r_N(\{C : C \text{ is a circuit of } M|X\})$$

is the rank function of a rank- $r(N)$ lift M^N of M .

We remark that the case when $r(N) = 1$ is exactly Brylawski's construction. To see this, note that if C_1 and C_2 are loops of N for which $|C_1 \cup C_2| - r_M(C_1 \cup C_2) = 2$, then condition (2*) implies that every circuit C of M contained in $C_1 \cup C_2$ is also a loop of

N . This implies that the set of circuits of M that are loops of N is a linear class. From the rank function of M^N , we see that the loops of N are precisely the circuits of M that are also circuits of M^N . So when $r(N) = 1$, the matroid M^N is equal to the matroid M' obtained by applying Theorem 1 with the linear class of loops of N .

As an example of Theorem 2 when $r(N) > 1$, let $M = U_{1,n}$. Then the set of circuits of M is the set of 2-element subsets of $[n]$, which is the edge set of the complete graph K_n . So we can think of the matroid $N = M(K_n)$ as a matroid on the set of circuits of $U_{1,n}$. It turns out that $M(K_n)$ satisfies (2*). To see this, let \mathcal{C}' be a perfect collection of circuits of $U_{1,n}$. Let H be the corresponding subgraph of K_n , so $E(H) = \mathcal{C}'$ and $V(H) = \cup \mathcal{C}'$. Then each edge $\{i, j\}$ of H is a leaf of H , or else the circuit $\{i, j\}$ of $U_{1,n}$ is contained in the union of the other circuits in \mathcal{C}' . In particular, H has no cycles. Also, $|\cup_{C \in \mathcal{C}'} C| - 1 = |\mathcal{C}'|$, because \mathcal{C}' is perfect and $r_M(\cup_{C \in \mathcal{C}'} C) = 1$. Since $\cup_{C \in \mathcal{C}'} C = V(H)$ and $\mathcal{C}' = E(H)$, this implies that $V(H) = E(H) + 1$. Then since H is acyclic, this implies that H is a tree. Since H is a tree for which every edge is a leaf, it follows that H is a star. If a circuit $C' = \{i, j\}$ of $U_{1,n}$ is contained in $\cup_{C \in \mathcal{C}'} C$, then $i, j \in V(H)$, so the edge $\{i, j\}$ is spanned in N by $E(H)$. Equivalently, \mathcal{C}' is spanned in N by \mathcal{C}' . Therefore, $N = M(K_n)$ satisfies (2*), so by Theorem 2 we can construct the matroid $U_{1,n}^{M(K_n)}$. This matroid has n elements and rank $r(U_{1,n}) + r(M(K_n)) = 1 + (n - 1) = n$, and is thus the free matroid on ground set $[n]$.

We apply Theorem 2 to group-labeled graphs, taking the matroid M to be the cycle matroid of the underlying graph, and using the group-labeling to construct the matroid N , just as Zaslavsky uses the group-labeling to construct the balanced cycles. We remark that, given a graph G and a set \mathcal{B} of balanced cycles with respect to a group-labeling of G , we can define a rank-1 matroid N on the circuits of $M(G)$, where each cycle in \mathcal{B} is a loop of N , and every other cycle of G is a non-loop of N . Then the matroid $M(G)^N$ is exactly Zaslavsky's lift matroid of the biased graph (G, \mathcal{B}) . For certain finite groups, we will construct a matroid N of rank at least two on the circuits of $M(G)$ using the group-labeling. For each finite group Γ and integer $n \geq 3$, we only consider the *fully* Γ -labeled graph K_n^Γ , which has vertex set $[n]$ and edge set $\binom{[n]}{2} \times \Gamma$. To ensure that the lift M of $M(K_n^\Gamma)$ respects the Γ -labeling, we require that the cycles of K_n^Γ that are circuits of M are precisely the balanced cycles of K_n^Γ . If Γ is isomorphic to \mathbb{Z}_p^j (the direct sum of j copies of the cyclic group of order p) for some prime p and some integer $j \geq 2$, then such a matroid M exists.

Theorem 3. *Let p be a prime, and let $n \geq 3$ and $j \geq 2$ be integers. For each integer i with $1 \leq i \leq j$, there is a rank- i lift M of $M(K_n^{\mathbb{Z}_p^j})$ so that a cycle of $K_n^{\mathbb{Z}_p^j}$ is a circuit of M if and only if it is balanced.*

Surprisingly, these are the only finite abelian groups for which this construction is possible. If Γ is a finite abelian group that is not isomorphic to \mathbb{Z}_p^j for some prime p and integer $j \geq 2$, then there is no rank- k lift of $M(K_n^\Gamma)$ with $k \geq 2$ that respects the group-labeling.

Theorem 4. *Let Γ be a nontrivial finite abelian group, and let $n \geq 3$ be an integer. Let M be a lift of $M(K_n^\Gamma)$ so that a cycle of K_n^Γ is a circuit of M if and only if it is balanced.*

Then either $\Gamma \cong \mathbb{Z}_p^j$ for some prime p and integer $j \geq 2$, or M is an elementary lift of $M(K_n^\Gamma)$.

We conjecture that this result in fact holds for all finite groups, and we make some partial progress in support of this conjecture.

After applying Theorem 2 to group-labeled graphs, we consider Theorem 2 in its own right. This theorem relies on the matroid N , and in general it is unclear how to construct a matroid N of rank at least two on the set of circuits of M so that N satisfies (2*). We show that, for any matroid M with corank at least three, there is a rank-3 matroid N on the circuits of M that satisfies (2*), and there are many rank-2 matroids on the circuits of M that satisfy (2*). For representable matroids we can do much better. Using the derived matroid of Longyear [7] and Oxley and Wang's recent generalization of it [9], we show that if M is representable, then there are many examples of a matroid N on the circuits of M that satisfies (2*).

Theorem 5. *Let M be a matroid representable over a field \mathbb{F} . Then, for each integer k with $1 \leq k \leq r^*(M)$, there is a rank- k matroid N on the set of circuits of M so that N satisfies (2*).*

It is unclear in general when there is a matroid N on the circuits of a given matroid M so that N satisfies (2*). Theorem 1 states that every elementary lift of a given matroid M arises from a linear class of circuits of M . Is it possible that every lift of M arises from a matroid N on the circuits of M that satisfies (2*)? We conjecture an affirmative answer to this question.

Conjecture 6. *Let M be a matroid. For every lift K of M , there is a matroid N on the circuits of M so that N satisfies (2*), and $K \cong M^N$.*

We further conjecture how to construct N given a lift K of M (Conjecture 29).

Finally, we consider Theorem 2 in the dual setting. If a matroid K is an (elementary) lift of a matroid M , then M is an (*elementary*) *projection* or *quotient* of K . Since projections are dual to lifts, one can use Theorem 1 to construct an elementary projection of M^* from a set of hyperplanes of M^* whose complements form a linear class of circuits of M . Such a collection of hyperplanes is called a *linear subclass* of hyperplanes. Equivalently, a collection \mathcal{H} of hyperplanes of a matroid K is a linear subclass if, whenever H_1 and H_2 are hyperplanes in \mathcal{H} so that $r_K(H_1 \cap H_2) = r(K) - 2$, then every hyperplane H of K containing $H_1 \cap H_2$ is also in \mathcal{H} . The following classical result of Crapo [3] constructs an elementary projection from a linear subclass; it is dual to Theorem 1.

Theorem 7 (Crapo '65). *Let K be a matroid, and let \mathcal{H} be a linear subclass of hyperplanes of K . Then the function $r_{K'}$ defined, for all $X \subseteq E(K)$, by*

$$r_{K'}(X) = \begin{cases} r_K(X) - 1 & \text{if each hyperplane of } K \text{ containing } X \text{ is in } \mathcal{H}, \\ r_K(X) & \text{otherwise} \end{cases}$$

is the rank function of an elementary projection K' of K . Moreover, every elementary projection of K can be obtained in this way.

In the same way, we can use Theorem 2 to construct a projection of a matroid K using a given matroid on the set of hyperplanes of K .

Theorem 8. *Let K be a matroid, and let N be a matroid on the set of hyperplanes of K so that*

(8*) *if \mathcal{H}' is a set of hyperplanes of K for which no hyperplane in \mathcal{H}' contains the intersection of the others, and $r_K(\cap_{H \in \mathcal{H}'} H) = r(K) - |\mathcal{H}'|$, then each hyperplane H' of K that contains $\cap_{H \in \mathcal{H}'} H$ satisfies $H' \in \text{cl}_N(\mathcal{H}')$.*

Then the function r_{K_N} defined, for all $X \subseteq E(K)$, by

$$r_{K_N}(X) = r_M(X) - r(N) + r_N(\{H : H \text{ is a hyperplane of } K \text{ that contains } X\})$$

is the rank function of a rank- $r(N)$ projection K_N of K .

Condition (8*) implies that the set \mathcal{H} of hyperplanes of K that are loops of N is a linear subclass of hyperplanes, so when $r(N) = 1$, the matroid K_N is equal to the matroid K' obtained by applying Theorem 7 to the linear subclass \mathcal{H} . By duality, Conjecture 6 is equivalent to the conjecture that every projection of K arises from a matroid N on the hyperplanes of K that satisfies (8*).

2 Preliminaries

Unless stated otherwise, we follow the notation and terminology of Oxley [8]. Zaslavsky [12] showed that elementary lifts of graphic matroids can be encoded using biased graphs. A *theta graph* consists of two distinct vertices x and y , and three pairwise internally disjoint paths from x to y . A set \mathcal{B} of cycles of a graph G satisfies the *theta property* if no theta subgraph of G contains exactly two cycles in \mathcal{B} ; equivalently, \mathcal{B} is a linear class of circuits of the graphic matroid $M(G)$. A *biased graph* is a pair (G, \mathcal{B}) where \mathcal{B} is a collection of cycles of G which satisfies the theta property. The cycles in \mathcal{B} are *balanced*, and the cycles not in \mathcal{B} are *unbalanced*.

Biased graphs were first described by Zaslavsky in [11], and in [12] he defined the following matroid associated with a given biased graph. The *lift matroid* of a biased graph (G, \mathcal{B}) is the matroid with ground set $E(G)$ so that $I \subseteq E(G)$ is independent if and only if the subgraph of G induced by I contains at most one cycle, and no balanced cycle. Equivalently, the lift matroid of (G, \mathcal{B}) is the matroid obtained from applying Theorem 1 to $M(G)$ with the linear class \mathcal{B} . Note that if \mathcal{B} is the set of all cycles of G , then the lift matroid of (G, \mathcal{B}) is isomorphic to $M(G)$.

A natural family of biased graphs arises from graphs whose edges are labeled by elements of a group. We define group-labeled graphs using the notation of [4]. A *group-labeling* of a graph G consists of an orientation of the edges of G , and a function $\phi: E(G) \rightarrow \Gamma$ for some (multiplicative) group Γ . For each walk W in G with edge

sequence e_1, e_2, \dots, e_k , define $c_i(W)$ by

$$c_i(W) = \begin{cases} 1 & \text{if } e_i \text{ is traversed forward in } W, \\ -1 & \text{if } e_i \text{ is traversed backward in } W, \end{cases}$$

and define $\phi(W) = \prod_{i=1}^k \phi(e_i)^{c_i(W)}$. Let \mathcal{B}_ϕ be the set of cycles C of G for which some (and thus every) simple closed walk W around C satisfies $\phi(W) = 1$. Then \mathcal{B}_ϕ satisfies the theta property, so (G, \mathcal{B}_ϕ) is a biased graph [11]. The cycles in \mathcal{B}_ϕ are the balanced cycles with respect to the group-labeling. We will also be interested in the group values of simple closed walks around unbalanced cycles of (G, \mathcal{B}_ϕ) . For each cycle C of G , we define

$$\phi(C) = \{\phi(W) : W \text{ is a simple closed walk around } C\}.$$

Note that C is balanced if and only if $1 \in \phi(C)$.

For each finite group Γ and each integer $n \geq 3$, we write K_n^Γ for the graph with vertex set $[n]$ and edge set $\binom{[n]}{2} \times \Gamma$. We write \mathcal{B}_n^Γ for the set of balanced cycles obtained from the Γ -labeling $\phi(\{i, j\}, \alpha) = \alpha$, and the following edge-orientation: for all $1 \leq i < j \leq n$, each edge between vertices i and j is oriented from vertex i to vertex j . We say that a cycle of K_n^Γ is balanced if it is in \mathcal{B}_n^Γ ; the natural Γ -labeling and edge-orientation will be implicit throughout the remainder of the paper. We denote the lift matroid of $(K_n^\Gamma, \mathcal{B}_n^\Gamma)$ by $\text{LG}(n, \Gamma)$.

3 The Construction

In this section we prove Theorem 2. For a set E and a set \mathcal{X} of subsets of E , we write $\cup \mathcal{X}$ for $\cup_{X \in \mathcal{X}} X$. Given a matroid M , we write $\mathcal{C}(M)$ for the collection of circuits of M . Recall that a collection \mathcal{C}' of circuits of a matroid M is *perfect* if $|\cup \mathcal{C}'| - r_M(\cup \mathcal{C}') = |\mathcal{C}'|$, and no circuit in \mathcal{C}' is contained in the union of the others. The following lemma shows that the set of fundamental circuits of a matroid with respect to some basis is always a perfect collection of circuits.

Lemma 9. *Let M be a matroid. Let B be a basis of M , and, for each $e \in E(M) - B$, let C_e be the unique circuit of $M|(B \cup \{e\})$. Then $\mathcal{C}' = \{C_e : e \in E(M) - B\}$ is a perfect collection of $|E(M)| - r(M)$ circuits of M . Conversely, every perfect collection of $|E(M)| - r(M)$ circuits of M arises in this way.*

Proof. Let $E = E(M)$. Clearly no circuit of \mathcal{C}' is contained in the union of the others, and $\cup \mathcal{C}' = E$. Then $|\cup \mathcal{C}'| - r_M(\cup \mathcal{C}') = |E| - r(M) = |\mathcal{C}'|$, so \mathcal{C}' is perfect. Conversely, let \mathcal{C}' be a perfect collection of $|E(M)| - r(M)$ circuits of M . For each $C \in \mathcal{C}'$, let X_C be the set of elements in C that are not in any other set in \mathcal{C}' . Let T be a transversal of $\{X_C : C \in \mathcal{C}'\}$. Then $|T| = |E| - r(M)$, and $T \subseteq \text{cl}_M(\cup \mathcal{C}') - T$. This implies that $E - T$ is a spanning subset of M of size $r(M)$, and is thus a basis of M . Also, each set in \mathcal{C}' has all but one element in $E - T$, so \mathcal{C}' is the set of fundamental circuits of M with respect to the basis $E - T$. \square

The following theorem easily implies Theorem 2.

Theorem 10. *Let M be a matroid, and let N be a matroid on the set of circuits of M so that*

(10*) *if \mathcal{C}' is a perfect collection of circuits of M , then each circuit C' of M contained in $\cup \mathcal{C}'$ satisfies $C' \in \text{cl}_N(\mathcal{C}')$.*

Let \mathcal{I} denote the collection of sets $X \subseteq E(M)$ for which there exists a collection \mathcal{C}' of $|X| - r_M(X)$ circuits of $M|X$ so that \mathcal{C}' is independent in N . Then \mathcal{I} is the collection of independent sets of a matroid M^N which is a rank- $r(N)$ lift of M . Moreover, the function r_{M^N} defined, for all $X \subseteq E(M)$, by

$$r_{M^N}(X) = r_M(X) + r_N(\{C : C \text{ is a circuit of } M|X\})$$

is the rank function of M^N .

Proof. We first use (10*) to relate subsets of $E(M)$ with perfect collections of circuits.

Claim 11. *Let $X \subseteq E(M)$, and let \mathcal{C}' be a perfect collection of $|X| - r_M(X)$ circuits of $M|X$. Then $\mathcal{C}(M|X) \subseteq \text{cl}_N(\mathcal{C}')$. Moreover, if $X \in \mathcal{I}$, then \mathcal{C}' is independent in N .*

Proof. We have $|\cup \mathcal{C}'| - r_M(\cup \mathcal{C}') = |\mathcal{C}'| = |X| - r_M(X)$, where the first equality holds because \mathcal{C}' is perfect. If there is a circuit C of $M|X$ that is not contained in $\cup \mathcal{C}'$, then $\mathcal{C}' \cup \{C\}$ is a collection of greater than $|X| - r_M(X)$ circuits of $M|X$ such that none is contained in the union of the others, a contradiction. Thus, each circuit of $M|X$ is contained in $\cup \mathcal{C}'$. Then (10*) implies that $\mathcal{C}(M|X) \subseteq \text{cl}_N(\mathcal{C}')$. In particular, this implies that $r_N(\mathcal{C}(M|X)) \leq r_N(\mathcal{C}')$. Now suppose that $X \in \mathcal{I}$. By the definition of \mathcal{I} , we know that $r_N(\mathcal{C}(M|X)) \geq |X| - r_M(X)$. Then $r_N(\mathcal{C}') \geq |X| - r_M(X)$, and since $|X| - r_M(X) = |\mathcal{C}'|$, this implies that $r_N(\mathcal{C}') \geq |\mathcal{C}'|$, so \mathcal{C}' is independent in N . \square

We now show that \mathcal{I} is the collection of independent sets of a matroid on $E(M)$. Clearly $\emptyset \in \mathcal{I}$, since \emptyset is independent in N . Let Y be a nonempty set in \mathcal{I} , let $e \in Y$, and let $X = Y - \{e\}$. We will show that $X \in \mathcal{I}$. If $e \notin \text{cl}_M(X)$, then $|X| - r_M(X) = |Y| - r_M(Y)$, and $M|X$ and $M|Y$ have the same circuits. Since $Y \in \mathcal{I}$, this implies that $X \in \mathcal{I}$, so we may assume that $e \in \text{cl}_M(X)$. Let B be a basis of $M|X$, and, for each $e' \in Y - B$, let $C_{e'}$ denote the unique circuit of $M|(B \cup \{e'\})$. Let $\mathcal{C}' = \{C_{e'} : e' \in Y - B\}$. Then, by Lemma 9 applied to $M|Y$, \mathcal{C}' is a perfect collection of $|Y| - r_M(Y)$ circuits of $M|Y$, and, by 11, \mathcal{C}' is independent in N . Then $\mathcal{C}' - \{C_e\}$ is a collection of $|X| - r_M(X)$ circuits of $M|X$ which is independent in N , so $X \in \mathcal{I}$.

We now show that \mathcal{I} satisfies the augmentation property.

Claim 12. *Let I_1 and I_2 be sets in \mathcal{I} so that $|I_1| < |I_2|$. Then there is some $e \in I_2 - I_1$ so that $I_1 \cup \{e\} \in \mathcal{I}$.*

Proof. Suppose that there is no element $e \in I_2 - I_1$ so that $I_1 \cup \{e\} \in \mathcal{I}$. We first show that $I_2 \subseteq \text{cl}_M(I_1)$. If not, then let $e \in I_2 - \text{cl}_M(I_1)$. Since $|I_1 \cup \{e\}| - r_M(I_1 \cup \{e\}) = |I_1| - r_M(I_1)$, and $\mathcal{C}(M|(I_1 \cup \{e\})) = \mathcal{C}(M|I_1)$, we have $I_1 \cup \{e\} \in \mathcal{I}$, a contradiction. Thus, $I_2 \subseteq \text{cl}_M(I_1)$, and so $|I_2| - r_M(I_2) > |I_1| - r_M(I_1)$.

Let B be a basis of $M|I_1$. For each $e \in (I_1 \cup I_2) - B$, let C_e denote the unique circuit of $M|(B \cup \{e\})$. Let $\mathcal{C}_1 = \{C_e : e \in I_1 - B\}$, and let $\mathcal{C}_2 = \{C_e : e \in I_2 - I_1\}$. Then, by Lemma 9 applied to $M|I_1$ and $M|(I_1 \cup I_2)$, \mathcal{C}_1 is a perfect collection of $|I_1| - r_M(I_1)$ circuits of $M|I_1$, and $\mathcal{C}_1 \cup \mathcal{C}_2$ is a perfect collection of $|I_1 \cup I_2| - r_M(I_1 \cup I_2)$ circuits of $M|(I_1 \cup I_2)$. Then 11 with $(X, \mathcal{C}') = (I_1, \mathcal{C}_1)$ implies that $\mathcal{C}(M|I_1) \subseteq \text{cl}_N(\mathcal{C}_1)$, and that \mathcal{C}_1 is independent in N . Also, 11 with $(X, \mathcal{C}') = (I_1 \cup I_2, \mathcal{C}_1 \cup \mathcal{C}_2)$ implies that $\mathcal{C}(M|I_2) \subseteq \text{cl}_N(\mathcal{C}_1 \cup \mathcal{C}_2)$.

Since \mathcal{C}_1 is independent in N , we have $r_N(\mathcal{C}_1 \cup \mathcal{C}_2) = r_N(\mathcal{C}_1)$, or else there is some $e \in I_2 - I_1$ so that $I_1 \cup \{e\} \in \mathcal{I}$, by the definitions of \mathcal{I} and \mathcal{C}_2 . But then

$$r_N(\mathcal{C}(M|I_2)) \leq r_N(\mathcal{C}_1 \cup \mathcal{C}_2) \leq |\mathcal{C}_1| = |I_1| - r_M(I_1) < |I_2| - r_M(I_2),$$

which contradicts that $I_2 \in \mathcal{I}$. □

We now know that \mathcal{I} is the collection of independent sets of a matroid M^N on $E(M)$. Next we compute the rank function of M^N . Let $X \subseteq E(M)$, and let B be a basis of $M|X$. For each $e \in X - B$, let C_e denote the unique circuit of $M|(B \cup \{e\})$. Let $\mathcal{C}' = \{C_e : e \in X - B\}$. Then by Lemma 9 applied to $M|X$, \mathcal{C}' is a perfect collection of $|X| - r_M(X)$ circuits of $M|X$, so 11 implies that $r_N(\mathcal{C}') = r_N(\mathcal{C}(M|X))$. Let \mathcal{C}'' be a subset of \mathcal{C}' so that $|\mathcal{C}''| = r_N(\mathcal{C}') = r_N(\mathcal{C}(M|X))$. Then $|B \cup (\cup \mathcal{C}'')| - r_M(B \cup (\cup \mathcal{C}'')) = |\mathcal{C}''|$, by the definition of \mathcal{C}' . Since \mathcal{C}'' is independent in N , this implies that $B \cup (\cup \mathcal{C}'')$ is independent in M^N , by the definition of \mathcal{I} . Therefore,

$$r_{M^N}(X) \geq |B \cup (\cup \mathcal{C}'')| = |B| + |\mathcal{C}''| = r_M(X) + r_N(\mathcal{C}(M|X)).$$

We now show that the reverse inequality holds. Let I be a basis of $M^N|X$, and let \mathcal{C}' be a collection of $|I| - r_M(I)$ circuits of $M|I$ so that \mathcal{C}' is independent in N . Then $|I| - r_M(I) \leq r_N(\mathcal{C}(M|I))$, and so

$$r_{M^N}(X) = |I| \leq r_M(I) + r_N(\mathcal{C}(M|I)) \leq r_M(X) + r_N(\mathcal{C}(M|X)),$$

since $I \subseteq X$. From the rank function of M^N , it is easy to see that $r(M^N) = r(M) + r(N)$.

Finally, we show that each circuit of M^N is a union of circuits of M ; this implies that M^N is a lift of M (see [8, Prop. 7.3.6]). Let Y be a circuit of M^N . If Y has an element e not in any circuit of $M|Y$, then from the rank function of M^N it follows that $r_{M^N}(Y - \{e\}) < r_{M^N}(Y)$, since $\mathcal{C}(M|(Y - \{e\})) = \mathcal{C}(M|Y)$. But then Y is not a circuit of M^N . Thus, each element of Y is in a circuit of $M|Y$, so Y is a union of circuits of M . □

4 The Construction for \mathbb{Z}_p^j -Labeled Graphs

In this section we prove Theorem 3. Let $j \geq 2$ be an integer, and let p be a prime. Recall that each cycle C of $K_n^{\mathbb{Z}_p^j}$ has a set $\phi(C) \subseteq \mathbb{Z}_p^j$ of values of simple closed walks around C ,

and that C is balanced if and only if $\phi(C)$ contains the identity element of \mathbb{Z}_p^j . It is not hard to see that the set $\phi(C)$ is closed under inverses, since taking the reverse of a simple closed walk results in the inverse group element in \mathbb{Z}_p^j . Also, since \mathbb{Z}_p^j is abelian, any two simple closed walks around C with the same cyclic ordering have the same value in \mathbb{Z}_p^j , so $|\phi(C)| \leq 2$.

For each proper divisor i of j , the group $(\mathbb{Z}_p^i)^{j/i}$ is isomorphic to \mathbb{Z}_p^j , and is the additive group of the vector space $\text{GF}(p^i)^{j/i}$. Thus, there is a natural map f_i from \mathbb{Z}_p^j to the vector space $\text{GF}(p^i)^{j/i}$. This can be extended to a natural map f'_i from \mathbb{Z}_p^j to the ground set of the projective geometry $\text{PG}((j/i) - 1, p^i)$.

For each unbalanced cycle C of $K_n^{\mathbb{Z}_p^j}$, the set $\phi(C)$ has size two and is closed under inverses; thus, both elements of \mathbb{Z}_p^j in $\phi(C)$ map to the same element of $\text{PG}((j/i) - 1, p^i)$ under f'_i . Therefore, the map g_i from the set of unbalanced cycles of $K_n^{\mathbb{Z}_p^j}$ to $E(\text{PG}((j/i) - 1, p^i))$ defined by $g_i(C) = f'_i(\alpha)$ for some $\alpha \in \phi(C)$ is well-defined. Since each projection (or lift) of $\text{PG}((j/i) - 1, p^i)$ has the same ground set as $\text{PG}((j/i) - 1, p^i)$, we can use g_i to define a matroid on the set of cycles of $K_n^{\mathbb{Z}_p^j}$ using any projection of $\text{PG}((j/i) - 1, p^i)$. The following definition makes this idea precise.

Definition 13. Let $n \geq 3$ and $j \geq 2$ be integers, and let p be a prime. Let i be a positive divisor of j , and let K be a projection of $\text{PG}((j/i) - 1, p^i)$. We define $N = N(n, j, p, K)$ to be the matroid on the set of cycles of $K_n^{\mathbb{Z}_p^j}$ for which each set \mathcal{C} of unbalanced cycles satisfies

$$r_N(\mathcal{C}) = r_K(\{g_i(C) : C \in \mathcal{C}\}),$$

and each balanced cycle is a loop of N .

If $K = \text{PG}((j/i) - 1, p^i)$, then $r_N(\mathcal{C})$ is simply the rank in the vector space $\text{GF}(p^i)^{j/i}$ of the set of vectors associated with the cycles in \mathcal{C} by the map f_i . Also, if K is a projection of $\text{PG}((j/i) - 1, p^i)$, then the map g_i shows that $N(n, j, p, K)$ is a projection of $N(n, j, p, \text{PG}((j/i) - 1, p^i))$.

In order to apply Theorem 2 with $M = M(K_n^{\mathbb{Z}_p^j})$ and $N = N(n, j, p, K)$, we must show that N satisfies (2*). The following lemma shows that we need only consider the case in which K is actually a projective geometry.

Proposition 14. *Let M be a matroid. If N is a matroid on $\mathcal{C}(M)$ that satisfies (2*), then every projection of N also satisfies (2*).*

Proof. Let N' be a projection of N . Let \mathcal{C}' be a perfect collection of circuits of M , and let C be a circuit of M so that $C \subseteq \cup \mathcal{C}'$. Then $C \in \text{cl}_N(\mathcal{C}')$, by (2*). Since N' is a projection of N , we have $\text{cl}_{N'}(\mathcal{C}') \subseteq \text{cl}_N(\mathcal{C}')$ (see [8, Prop. 7.3.6]). Thus, $C \in \text{cl}_{N'}(\mathcal{C}')$, as desired. \square

We now show that the matroid $N = N(n, j, p, K)$ on the circuits of $M(K_n^{\mathbb{Z}_p^j})$ satisfies (2*).

Proposition 15. *Let $n \geq 3$ and $j \geq 2$ be integers, and let p be a prime. Let i be a positive divisor of j , and let $N = N(n, j, p, \text{PG}((j/i) - 1, p^i))$. If \mathcal{C}' is a perfect collection of circuits of $M(K_n^{\mathbb{Z}_p^j})$ and C is a circuit of $M(K_n^{\mathbb{Z}_p^j})$ contained in $\cup \mathcal{C}'$, then $C \in \text{cl}_N(\mathcal{C}')$.*

Proof. We write $G = K_n^{\mathbb{Z}_p^j}$, for convenience. Let $|\mathcal{C}'|$ be minimal so that the claim is false; then $|\mathcal{C}'| \geq 2$. Let C be a circuit of $M(G)$ contained in $\cup \mathcal{C}'$. We freely use the fact that each subset of \mathcal{C}' is also a perfect collection of circuits of $M(G)$. This implies that for each cycle $C' \in \mathcal{C}'$, there is at least one edge in $C' \cap C$ that is not in any other cycle in \mathcal{C}' . Let X be a transversal of these edges of $\cup \mathcal{C}'$; note that $X \subseteq C$. Then

$$|(\cup \mathcal{C}') - X| = |\cup \mathcal{C}'| - |X| = r_{M(G)}(\cup \mathcal{C}') + |\mathcal{C}'| - |X| = r_{M(G)}(\cup \mathcal{C}'),$$

since \mathcal{C}' is perfect, so $T = (\cup \mathcal{C}') - X$ is the edge-set of a spanning forest of the graph $G[\cup \mathcal{C}']$. By the minimality of $|\mathcal{C}'|$ and the fact that $G[C]$ is connected, this forest is in fact a tree. We use the tree T to define two cycles.

Claim 16. *There are cycles C_1, C_2 contained in $\cup \mathcal{C}'$ which form a theta graph with C , such that $C_1, C_2 \in \text{cl}_N(\mathcal{C}')$.*

Proof. Let v_1, v_2 be distinct vertices of $G[C]$, and let P be the unique path in T from v_1 to v_2 . Let v'_1 be the first vertex of P in C other than v_1 , and let P' be the segment of P from v_1 to v'_1 . Then P' is a path with both ends in C which is internally vertex-disjoint from C , so $G[C \cup P']$ is a theta graph.

Let P_1, P', P_2 denote the three internally vertex-disjoint paths of the theta graph $G[C \cup P']$ from v_1 to v'_1 . Then P_1 and P_2 each contain an element of X ; if P_i and X are disjoint, then $G[P_{3-i} \cup P']$ is a circuit of the tree T . Let $e_1 \in P_1 \cap X$ and let $e_2 \in P_2 \cap X$, and for each $i \in \{1, 2\}$ let C'_i denote the circuit in \mathcal{C}' that contains e_i .

For each $i \in \{1, 2\}$ let $C_i = P_i \cup P'$; then C_i is a cycle that does not contain e_{3-i} . Since \mathcal{C}' is perfect, no element of $C'_2 - (\cup \mathcal{C}')$ is in a cycle of $G[(\cup \mathcal{C}') - \{e_2\}]$; otherwise $|\cup \mathcal{C}'| - r_{M(G)}(\cup \mathcal{C}') > |\mathcal{C}'|$. Since C_1 does not contain e_2 and C_1 is a cycle, it follows that $C_1 \subseteq \cup(\mathcal{C}' - \{C'_2\})$. Similarly, $C_2 \subseteq \cup(\mathcal{C}' - \{C'_1\})$. So by the minimality of $|\mathcal{C}'|$, we have $C_2 \in \text{cl}_N(\mathcal{C}' - \{C'_1\})$ and $C_1 \in \text{cl}_N(\mathcal{C}' - \{C'_2\})$, and thus $C_1, C_2 \in \text{cl}_N(\mathcal{C}')$. \square

We now use the definition of N .

Claim 17. $C \in \text{cl}_N(\{C_1, C_2\})$.

Proof. Assume without loss of generality that the edges of P' and P_1 are oriented from v_1 to v'_1 , and the edges of P_2 are oriented from v'_1 to v_1 . Let α_1 and α' denote the values in \mathbb{Z}_p^j of the walks from v_1 to v'_1 on P_1 and P' , respectively, and let α_2 denote the value of the walk from v'_1 to v_1 on P_2 . Then $\alpha_1 + \alpha_2 \in \phi(C)$, while $\alpha_1 - \alpha' \in \phi(C_1)$ and $\alpha' + \alpha_2 \in \phi(C_2)$. By the definition of $N = N(n, j, p, \text{PG}((j/i) - 1, p^i))$, this implies that $\{C, C_1, C_2\}$ is a circuit of N , and so the claim holds. \square

Claims 16 and 17 combine to show that $C \in \text{cl}_N(\{\mathcal{C}'\})$. \square

By Proposition 15, we may use Theorem 2 to define the matroid $M(K_n^{\mathbb{Z}_p^j})^{N(n, j, p, K)}$ for each prime p , each integer $j \geq 2$, each positive divisor i of j , each integer $n \geq 3$, and each projection K of $\text{PG}((j/i) - 1, p^i)$. This matroid is a rank- $r(K)$ lift of $M(K_n^{\mathbb{Z}_p^j})$. We now prove Theorem 3.

Proof of Theorem 3. By Proposition 15, the matroid $N(n, j, p, \text{PG}(j - 1, p))$ on the set of cycles of $K_n^{\mathbb{Z}_p^j}$ satisfies (2*). Also, by Definition 13, a cycle of $K_n^{\mathbb{Z}_p^j}$ is a loop of $N(n, j, p, \text{PG}(j - 1, p))$ if and only if it is balanced. Let K be the $(j - i)$ -th truncation of $\text{PG}(j - 1, p)$. Then K is a projection of $\text{PG}(j - 1, p)$, and each $X \subseteq E(\text{PG}(j - 1, p))$ satisfies $r_K(X) = \min(r_{\text{PG}(j-1,p)}(X), i)$. Since K is a projection of $\text{PG}(j - 1, p)$, the map g_1 shows that $N(n, j, p, K)$ is a projection of $N(n, j, p, \text{PG}(j - 1, p))$. Then since $N(n, j, p, \text{PG}(j - 1, p))$ satisfies (2*), Proposition 14 with $N = N(n, j, p, \text{PG}(j - 1, p))$ implies that $N(n, j, p, K)$ also satisfies (2*). Also, each element e of $\text{PG}(j - 1, p)$ satisfies $r_K(\{e\}) = \min(r_{\text{PG}(j-1,p)}(\{e\}), i) = 1$, so K is loopless. Since K is loopless, by Definition 13, a cycle of $K_n^{\mathbb{Z}_p^j}$ is a loop of $N(n, j, p, K)$ if and only if it is balanced. By Theorem 2, this implies that a cycle of $K_n^{\mathbb{Z}_p^j}$ is a circuit of $M = M(K_n^{\mathbb{Z}_p^j})^{N(n,j,p,K)}$ if and only if it is balanced. Since $r(K) = i$, the matroid $M(K_n^{\mathbb{Z}_p^j})^{N(n,j,p,K)}$ is a rank- i lift of $M(K_n^{\mathbb{Z}_p^j})$. Thus, the theorem holds with $M = M(K_n^{\mathbb{Z}_p^j})^{N(n,j,p,K)}$. \square

To prove Theorem 3, we used the construction of Theorem 2. Conversely, we conjecture that every lift of $M(K_n^{\mathbb{Z}_p^j})$ that has each balanced cycle of $K_n^{\mathbb{Z}_p^j}$ as a circuit arises from this construction.

Conjecture 18. Let $n \geq 3$ and $j \geq 2$ be integers, let p be a prime, and let M be a lift of $M(K_n^{\mathbb{Z}_p^j})$ so that each balanced cycle of $K_n^{\mathbb{Z}_p^j}$ is a circuit of M . Then there is a positive divisor i of j and a projection K of $\text{PG}((j/i) - 1, p^i)$ so that $M \cong M(K_n^{\mathbb{Z}_p^j})^{N(n,j,p,K)}$.

This may be easier to prove in the case that no unbalanced cycle of $K_n^{\mathbb{Z}_p^j}$ is a circuit of M .

5 Other Abelian Groups

In this section we prove Theorem 4. For each finite group Γ and integer $n \geq 3$, we define $\mathcal{M}_{n,\Gamma}$ to be the class of lifts M of $M(K_n^\Gamma)$ for which a cycle of K_n^Γ is a circuit of M if and only if it is a balanced cycle of K_n^Γ . These are the lifts of $M(K_n^\Gamma)$ that respect the Γ -labeling. Note that each matroid in $\mathcal{M}_{n,\Gamma}$ is simple, since each 2-element cycle of $M(K_n^\Gamma)$ is unbalanced. Also, if Γ is the trivial group, then $\mathcal{M}_{n,\Gamma}$ is empty, so we will restrict our attention to nontrivial groups.

For each nontrivial finite group Γ and integer $n \geq 3$, the class $\mathcal{M}_{n,\Gamma}$ certainly contains the rank-1 lift $\text{LG}(n, \Gamma)$. Theorem 4 says that if Γ is a nontrivial finite abelian group that is not isomorphic to \mathbb{Z}_p^j for some prime p and integer $j \geq 2$, then $\mathcal{M}_{n,\Gamma}$ contains only $\text{LG}(n, \Gamma)$, up to isomorphism. To prove this, we will use three lemmas, which each apply to arbitrary finite groups.

The first lemma uses local information about the balanced cycles of K_n^Γ . For each element $\alpha \in \Gamma$, we write E_α for $\{(\{i, j\}, \alpha) : 1 \leq i < j \leq n\}$; these are the edges of K_n^Γ labeled by α . More generally, for each set $A \subseteq \Gamma$, we write E_A for $\{(\{i, j\}, \alpha) : 1 \leq i <$

$j \leq n$ and $\alpha \in A$ }. For convenience, for each $\alpha \in \Gamma$ and $1 \leq i < j \leq n$, we write α_{ij} for the edge $(\{i, j\}, \alpha)$.

Lemma 19. *Let $n \geq 3$ be an integer, let Γ be a finite group with identity ϵ , and let $M \in \mathcal{M}_{n,\Gamma}$. Then each non-identity element $\alpha \in \Gamma$ satisfies $r_M(E_{\{\alpha,\epsilon\}}) = n$, and $E_\alpha \cap \text{cl}_M(E_\epsilon) = \emptyset$.*

Proof. Clearly E_ϵ spans $M(K_n^\Gamma)$, since each element of $M(K_n^\Gamma)$ is parallel to an element in E_ϵ . Let $B = \{\alpha_{12}\} \cup E_\epsilon$. For each $3 \leq j \leq n$, the cycle $\{\alpha_{12}, \epsilon_{2j}, \alpha_{1j}\}$ is balanced, and is thus a circuit of M , since $M \in \mathcal{M}_{n,\Gamma}$. Since $\{\alpha_{12}, \epsilon_{2j}, \alpha_{1j}\}$ is a circuit of M for all $3 \leq j \leq n$, it follows that $\alpha_{1j} \in \text{cl}_M(B)$ for each $2 \leq j \leq n$. For all $2 \leq i < j \leq n$, the cycle $\{\epsilon_{1i}, \alpha_{ij}, \alpha_{1j}\}$ is balanced, and is thus a circuit of M ; this implies that $\alpha_{ij} \in \text{cl}_M(B)$. Thus, $E_\alpha \subseteq \text{cl}_M(B)$, so $r_M(E_{\{\alpha,\epsilon\}}) \leq r(M(K_n^\Gamma)) + 1 = n$.

We now show that $E_\alpha \cap \text{cl}_M(E_\epsilon) = \emptyset$; this implies that $r_M(E_{\{\alpha,\epsilon\}}) = n$. If $\alpha_{12} \in \text{cl}_M(E_\epsilon)$, then by the previous paragraph we have $E_\alpha \subseteq \text{cl}_M(E_\epsilon)$. Since M is a lift of $M(K_n^\Gamma)$ and $M|_{E_\epsilon} = M(K_n^\Gamma)|_{E_\epsilon}$, this implies that $M|(E_{\{\alpha,\epsilon\}}) = M(K_n^\Gamma)|(E_{\{\alpha,\epsilon\}})$. But M is simple and $M(K_n^\Gamma)|(E_{\{\alpha,\epsilon\}})$ is not, so this is a contradiction. Thus, $\alpha_{12} \notin \text{cl}_M(E_\epsilon)$. The same argument applies to each element of E_α , so $E_\alpha \cap \text{cl}_M(E_\epsilon) = \emptyset$. \square

The next lemma uses a more global argument.

Lemma 20. *Let $n \geq 3$ be an integer, let Γ be a finite group with identity ϵ , and let $M \in \mathcal{M}_{n,\Gamma}$. Let A be a subset of Γ , and let $\langle A \rangle$ be the subgroup of Γ generated by A . Then $E_{\langle A \rangle} \subseteq \text{cl}_M(E_{A \cup \{\epsilon\}})$.*

Proof. Let \circ be the (multiplicative) group operation of Γ . We write $B = E_{A \cup \{\epsilon\}}$ for convenience. Let $\alpha, \beta \in \Gamma$ so that $E_\alpha \cup E_\beta \subseteq \text{cl}_M(B)$. We will show that $E_{\alpha^{-1}} \subseteq \text{cl}_M(B)$, and that $E_{\alpha\circ\beta} \subseteq \text{cl}_M(B)$; then each element $\gamma \in \Gamma$ generated by A satisfies $E_\gamma \subseteq \text{cl}_M(B)$, and so $E_{\langle A \rangle} \subseteq \text{cl}_M(B)$. We freely use the fact that each balanced cycle of K_n^Γ is a circuit of M , since $M \in \mathcal{M}_{n,\Gamma}$.

Since $\{\alpha_{12}^{-1}, \alpha_{23}, \epsilon_{13}\}$ is a circuit of M and $\alpha_{23}, \epsilon_{13} \in \text{cl}_M(B)$, we have $\alpha_{12}^{-1} \in \text{cl}_M(B)$. Then, since $\{\alpha_{12}^{-1}, \epsilon_{2j}, \alpha_{1j}^{-1}\}$ is a circuit of M and $\alpha_{12}^{-1}, \epsilon_{2j} \in \text{cl}_M(B)$, we have $\alpha_{1j}^{-1} \in \text{cl}_M(B)$ for each $2 \leq j \leq n$. Finally, since $\{\alpha_{1i}, \alpha_{ij}^{-1}, \epsilon_{1j}\}$ is a circuit of M and $\alpha_{1i}, \epsilon_{1j} \in \text{cl}_M(B)$, we have $\alpha_{ij}^{-1} \in \text{cl}_M(B)$ for all $2 \leq i < j \leq n$, and thus $E_{\alpha^{-1}} \subseteq \text{cl}_M(B)$.

We now show that $E_{\alpha\circ\beta} \subseteq \text{cl}_M(B)$. Since $\{(\alpha \circ \beta)_{12}, \beta_{23}^{-1}, \alpha_{13}\}$ is a circuit of M and $\beta_{23}^{-1}, \alpha_{13} \in \text{cl}_M(B)$, we have $(\alpha \circ \beta)_{12} \in \text{cl}_M(B)$. Since $\{\beta_{12}^{-1}, \alpha_{2j}^{-1}, (\alpha \circ \beta)_{1j}\}$ is a circuit of M and $\beta_{12}^{-1}, \alpha_{2j}^{-1} \in \text{cl}_M(B)$, we have $(\alpha \circ \beta)_{1j} \in \text{cl}_M(B)$ for each $2 \leq j \leq n$. Finally, since $\{\alpha_{1i}^{-1}, (\alpha \circ \beta)_{ij}, \beta_{1j}\}$ is a circuit of M and $\alpha_{1i}^{-1}, \beta_{1j} \in \text{cl}_M(B)$, we have $(\alpha \circ \beta)_{ij} \in \text{cl}_M(B)$ for all $2 \leq i < j \leq n$. Thus $E_{\alpha\circ\beta} \subseteq \text{cl}_M(B)$. \square

The following lemma defines an equivalence relation on the non-identity elements of Γ . Its proof follows without difficulty from Lemmas 19 and 20.

Lemma 21. *Let $n \geq 3$ be an integer, let Γ be a finite group with identity ϵ , and let $M \in \mathcal{M}_{n,\Gamma}$. For $\alpha, \beta \in \Gamma - \{\epsilon\}$, write $\alpha \sim \beta$ if $r_M(E_{\{\alpha,\beta,\epsilon\}}) = n$. Then*

- (i) \sim is an equivalence relation,
- (ii) each equivalence class A of \sim satisfies $r_M(E_{A \cup \{\epsilon\}}) = n$, and
- (iii) for each equivalence class A of \sim , the set $A \cup \{\epsilon\}$ is a subgroup of Γ .

We now prove the following restatement of Theorem 4.

Theorem 22. *Let $n \geq 3$ be an integer, let Γ be a finite abelian group, and let $M \in \mathcal{M}_{n,\Gamma}$. If $r(M) - r(M(K_n^\Gamma)) > 1$, then there is a prime p and an integer $j \geq 2$ so that $\Gamma \cong \mathbb{Z}_p^j$.*

Proof. Let \circ be the (multiplicative) group operation of Γ , and let ϵ denote the identity element of Γ . For $\alpha, \beta \in \Gamma - \{\epsilon\}$, we write $\alpha \sim \beta$ if $r_M(E_{\{\alpha, \beta, \epsilon\}}) = n$; then \sim is an equivalence relation by Lemma 21(i). Let \mathcal{A} denote the set of equivalence classes under \sim ; by hypothesis and Lemma 21(ii) we have $|\mathcal{A}| \geq 2$. By Lemma 20, this implies that Γ is not cyclic.

We first use the fact that Γ is abelian.

Claim 23. *Let $\alpha, \beta \in \Gamma - \{\epsilon\}$. If there is a prime that divides the order of α but not the order of β , then $\alpha \sim \beta$.*

Proof. By hypothesis, there are elements $\alpha', \beta' \in \Gamma$ with distinct prime orders so that α generates α' , and β generates β' . Then $\alpha' \sim \alpha$, and $\beta' \sim \beta$, by Lemma 20. Since α' and β' have distinct prime orders and Γ is abelian, the subgroup of Γ generated by $\{\alpha', \beta'\}$ is cyclic. Thus, Lemma 20 implies that $\alpha' \sim \beta'$. Since \sim is an equivalence relation, this implies that $\alpha \sim \beta$. □

We now find the prime p .

Claim 24. *There is a prime p so that each element of Γ has order p .*

Proof. By 23, for any two elements of Γ in different equivalence classes, there is a prime p so that each has order equal to a power of p . Since there are at least two equivalence classes of \sim , this implies that each element of Γ has order equal to a power of p .

Now, let α be an element of order p . We will show that each element in a different equivalence class has order p . Since there are at least two equivalence classes, this implies that each element of Γ has order p . Let β be in a different equivalence class than α , and suppose that the order of β is not p . Then the subgroup of Γ generated by $\{\alpha, \beta\}$ is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_{p^j}$ for some $j \geq 2$. The elements $(0, 1)$ and $(0, p)$ are in a common cyclic subgroup, as are the elements $(1, 1)$ and $(0, p)$. By Lemma 20, this implies that $(0, 1) \sim (0, p) \sim (1, 1)$, so $(0, 1) \sim (1, 1)$. But the set $\{(0, 1), (1, 1)\}$ generates $\mathbb{Z}_p \oplus \mathbb{Z}_{p^j}$, so by Lemma 21(iii), all elements of the subgroup generated by $\{\alpha, \beta\}$ are equivalent. In particular, $\alpha \sim \beta$, a contradiction. □

Since Γ is abelian and not cyclic, 24 implies that $\Gamma \cong \mathbb{Z}_p^j$ for some $j \geq 2$. □

We conjecture that Theorem 22 can be extended to all finite groups.

Conjecture 25. Let $n \geq 3$ be an integer, let Γ be a finite group, and let $M \in \mathcal{M}_{n,\Gamma}$. If $r(M) - r(M(K_n^\Gamma)) > 1$, then there is a prime p and an integer $j \geq 2$ so that $\Gamma \cong \mathbb{Z}_p^j$.

We expect that Lemmas 19-21 would all be useful for proving this conjecture. Indeed, Lemma 21 implies that if $M \in \mathcal{M}_{n,\Gamma}$ and $r(M) - r(M(K_n^\Gamma)) > 1$, then Γ has a nontrivial decomposition into subgroups with pairwise trivial intersection. This decomposition is a *partition* of Γ , and the classification of finite groups that admit a nontrivial partition was completed by Baer, Kegel, and Suzuki [1, 6, 10]. While Lemma 21 and this classification make partial progress towards Conjecture 25, it is unclear how to proceed for non-abelian groups with a nontrivial partition.

6 Examples

Now that we have applied Theorem 2 to group-labeled graphs, we consider other applications. Given a matroid M , it is unclear when there exists a matroid N of rank at least three on the set of circuits of M that satisfies (10*) (or equivalently, (2*)). A rank-1 matroid N on the circuits of M can be constructed from any linear class \mathcal{C} of circuits of M , by taking \mathcal{C} to be precisely the set of loops of N . Also, the rank-2 uniform matroid on the set of circuits of M trivially satisfies (10*), because the collection \mathcal{C}' is always spanning in N . In this case, the matroid M^N can also be obtained from applying Brylawski's construction (Theorem 1) to M with the empty linear class, and then again applying the construction with the empty linear class. The following proposition shows that, for any matroid M of corank at least three, there exists a rank-3 matroid N on the set of circuits of M that satisfies (10*).

Proposition 26. *Let M be a matroid of corank at least three, and let \mathcal{I} be the collection of sets of circuits of M so that $\mathcal{C} \in \mathcal{I}$ if and only if $|\mathcal{C}| \leq 3$ and each $\mathcal{C}' \subseteq \mathcal{C}$ satisfies $|\mathcal{C}'| \leq |\cup \mathcal{C}'| - r_M(\cup \mathcal{C}')$. Then \mathcal{I} is the collection of independent sets of a rank-3 matroid N on the set of circuits of M , and N satisfies (10*).*

Proof. Clearly $\emptyset \in \mathcal{I}$ and \mathcal{I} is closed under taking subsets. Note that each 2-element set $\{\mathcal{C}_1, \mathcal{C}_2\}$ of circuits of M is in \mathcal{I} , because $|\mathcal{C}_1 \cup \mathcal{C}_2| - r_M(\mathcal{C}_1 \cup \mathcal{C}_2) \geq 2$ since $M|(\mathcal{C}_1 \cup \mathcal{C}_2)$ contains distinct circuits. Let \mathcal{C}_1 and \mathcal{C}_2 be sets in \mathcal{I} so that $|\mathcal{C}_1| < |\mathcal{C}_2|$. Assume that there is no circuit $C \in \mathcal{C}_2$ for which $\mathcal{C}_1 \cup \{C\} \in \mathcal{I}$. Since each 2-element set of circuits is in \mathcal{I} , we may assume that $|\mathcal{C}_1| = 2$ and $|\mathcal{C}_2| = 3$.

Let $C \in \mathcal{C}_2 - \mathcal{C}_1$. Then each 2-element subset of $\mathcal{C}_1 \cup \{C\}$ is in \mathcal{I} . Thus,

$$2 \leq |\cup \mathcal{C}_1| - r_M(\cup \mathcal{C}_1) \leq |\cup (\mathcal{C}_1 \cup \{C\})| - r_M(\cup (\mathcal{C}_1 \cup \{C\})) < 3,$$

where the first inequality holds because $\mathcal{C}_1 \in \mathcal{I}$, and the third holds because $\mathcal{C}_1 \cup \{C\} \notin \mathcal{I}$ and each subset is in \mathcal{I} . So equality holds throughout, which implies that $C \subseteq \cup \mathcal{C}_1$. The same reasoning applies to each circuit in $\mathcal{C}_2 - \mathcal{C}_1$, and so $\cup \mathcal{C}_2 \subseteq \cup \mathcal{C}_1$. But then

$$|\cup \mathcal{C}_2| - r_M(\cup \mathcal{C}_2) \leq |\cup \mathcal{C}_1| - r_M(\cup \mathcal{C}_1) = 2,$$

so $\mathcal{C}_2 \notin \mathcal{I}$, a contradiction. Thus, \mathcal{I} is the collection of independent sets of a matroid N of rank at most three. Since M has corank at least three, it contains three circuits C_1, C_2, C_3 such that none is contained in the union of the other two; then $\{C_1, C_2, C_3\} \in \mathcal{I}$, so $r(N) = 3$.

We now show that N satisfies (10*). Let \mathcal{C}' be a perfect collection of circuits of M , and let $C \notin \mathcal{C}'$ be a circuit of M contained in $\cup \mathcal{C}'$. We may assume that $r_N(\mathcal{C}') = 2$, or else (10*) trivially holds since $r(N) = 3$. Since no circuit in \mathcal{C}' is contained in the union of the others, this implies that $|\mathcal{C}'| = 2$. Since $C \subseteq \cup \mathcal{C}'$, we have

$$|\cup(\mathcal{C}' \cup \{C\})| - r_M(\cup(\mathcal{C}' \cup \{C\})) = |\cup \mathcal{C}'| - r_M(\cup \mathcal{C}') = |\mathcal{C}'| < |\mathcal{C}' \cup \{C\}|,$$

and so $\mathcal{C}' \cup \{C\} \notin \mathcal{I}$. Then $r_N(\mathcal{C}' \cup \{C\}) = r_N(\mathcal{C}')$, and so $C \in \text{cl}_N(\mathcal{C}')$, as desired. \square

For representable matroids we can do much better, using the derived matroid of Longyear [7] and Oxley and Wang [9]. Let M be an \mathbb{F} -representable matroid with ground set $E = \{e_1, e_2, \dots, e_m\}$ for some field \mathbb{F} , and fix an \mathbb{F} -representation A of M with column vectors $\varphi(e_1), \varphi(e_2), \dots, \varphi(e_m)$. For each circuit C of M , there is a vector $\mathbf{c}_C = (c_1, c_2, \dots, c_m)$ in \mathbb{F}^m such that $\sum_{i=1}^m c_i \varphi(e_i) = 0$ and $c_i \neq 0$ if and only if $e_i \in C$; this vector is unique up to multiplying by a nonzero scalar. Let A' denote the matrix over \mathbb{F} with columns indexed by the circuits of M so that the column vector of each circuit C is \mathbf{c}_C . Then $M(A')$ is the *derived matroid* of the representation A of M . Oxley and Wang show that the rank of the derived matroid of any representation of M is $r(M^*)$ [9, Prop. 9.2.2]. In addition, they show that the derived matroid of any representation of $U_{1,n}$ is $M(K_n)$ [9, Lemma 2.5], because each pair of elements in $[n]$ forms a circuit of $U_{1,n}$. Note that $r(M(K_n)) = n - 1 = r^*(U_{1,n})$. We show that the derived matroid of any representation of a matroid M satisfies (10*).

Proposition 27. *Let M be matroid representable over a field \mathbb{F} , and let N be the derived matroid of a representation A of M . Then N satisfies (10*), and M^N is the free matroid on $E(M)$.*

Proof. Let \mathcal{C}' be a perfect collection of circuits of M . Since each circuit in \mathcal{C}' has an element that is not in any other circuit in \mathcal{C}' , the set \mathcal{C}' is independent in N . Let N' denote the derived matroid of the matrix $A[(\cup \mathcal{C}')]$; then N' is a restriction of N , and

$$r(N') = r((M|(\cup \mathcal{C}'))^*) = |\cup \mathcal{C}'| - r_M(\cup \mathcal{C}') = |\mathcal{C}'|,$$

where the last equality holds because \mathcal{C}' is perfect. Since \mathcal{C}' is independent in N , this implies that \mathcal{C}' is a basis of N' . Thus, each circuit C of M contained in $\cup \mathcal{C}'$ satisfies $C \in \text{cl}_N(\mathcal{C}')$, and so N satisfies (10*). Since $r(N) = r(M^*)$, Theorem 10 shows that $r(M^N) = r(M) + r(M^*) = |M|$, so M^N is a free matroid. \square

For example, the derived matroid $M(K_n)$ of any representation of $U_{1,n}$ satisfies (10*), and $U_{1,n}^{M(K_n)}$ is the free matroid on $[n]$ because $r(U_{1,n}^{M(K_n)}) = r(U_{1,n}) + r(M(K_n)) = n$.

Given one matroid N on the circuits of M that satisfies (10*), we can construct many more, using Proposition 14. If M is representable, then Propositions 27 and 14 show that,

for each integer $1 \leq k < r^*(M)$, there are many rank- k matroids on the circuits of M that satisfy (10*). This proves Theorem 5. However, if N and N' are two different matroids on the circuits of M , it may be the case that $M^N = M^{N'}$. For example, a matroid M representable over a field \mathbb{F} other than $\text{GF}(2)$ or $\text{GF}(3)$ may have several non-isomorphic derived matroids, depending on the representation [9, Theorem 2.6], and these all lead to the free matroid, by Proposition 27.

7 The Converse

Theorem 1 states that every elementary lift of a given matroid M arises from a linear class of circuits of M . More generally, the following restatement of Conjecture 6 states that every lift of M arises from the construction of Theorem 10.

Conjecture 28. Let M be a matroid. For every lift K of M , there is a matroid N on the circuits of M so that N satisfies (10*), and $K \cong M^N$.

This is certainly true if $r(M) = 0$; then the set of circuits of M is precisely $E(M)$, and we can take $N = K$. It is also true if M has corank at most two, by Theorem 1 and the fact that the rank-2 uniform matroid on the circuits of M satisfies (10*). It is tedious but not difficult to check that it is true for certain small matroids of corank three, such as $U_{1,4}$ or $U_{2,5}$. However, Conjecture 28 seems difficult to prove even for the very basic class of rank-1 uniform matroids.

In general, if there exists a matroid N so that M^N is the free matroid on $E(M)$, then Proposition 14 shows that Theorem 10 can be used to construct a potentially huge number of lifts of M , and this provides some evidence that Conjecture 28 is true for M . In particular, the constructions of the previous section provide evidence that this conjecture is true for representable matroids and matroids of corank three.

One way to prove Conjecture 28 would be to explicitly construct the matroid N , given K and M . We make the following conjecture in this direction:

Conjecture 29. Let M be a matroid, and let K be a lift of M . Let \mathcal{I} be the collection of subsets \mathcal{C}' of $\mathcal{C}(M)$ for which there is no matroid K' such that

- K' is a projection of K and a lift of M ,
- each set in \mathcal{C}' is a circuit of K' , and
- $r(K) - r(K') < |\mathcal{C}'|$.

Then \mathcal{I} is the collection of independent sets of a matroid N on $\mathcal{C}(M)$, and $K \cong M^N$.

If K is the free matroid on $E(M)$, then K' is only required to be a lift of M , since every matroid on $E(M)$ is a projection of the free matroid on $E(M)$. Conjecture 29 may be easier to prove in this special case.

8 The Dual Construction

All of the previous results about lifts of a matroid M give rise to results about projections of M^* . For a set E and a set \mathcal{X} of subsets of E , we write $\cap \mathcal{X}$ for $\cap_{X \in \mathcal{X}} X$. Given a matroid K , we write $\mathcal{H}(K)$ for the set of hyperplanes of K . We say that a collection \mathcal{H}' of hyperplanes of K is *perfect* if $r_K(\cap \mathcal{H}') = r(K) - |\mathcal{H}'|$, and no hyperplane in \mathcal{H}' contains the intersection of the others. It is easy to check that \mathcal{H}' is a perfect collection of hyperplanes of K if and only if $\{E - H : H \in \mathcal{H}'\}$ is a perfect collection of circuits of K^* . The following is a restatement of Theorem 8. We omit the proof, as it is a straightforward application of duality.

Theorem 30. *Let K be a matroid, and let N be a matroid on the set of hyperplanes of K so that*

(30*) *if \mathcal{H}' is a perfect collection of hyperplanes of K , and H is a hyperplane of K that contains $\cap \mathcal{H}'$, then $H \in \text{cl}_N(\mathcal{H}')$.*

Then the function r_{K_N} defined, for all $X \subseteq E(K)$, by

$$r_{K_N}(X) = r_K(X) - r(N) + r_N(\{H \in \mathcal{H}(K) : X \subseteq H\})$$

is the rank function of a rank- $r(N)$ projection K_N of K .

Theorem 7 states that every elementary projection of a given matroid K arises from a linear subclass of hyperplanes of K . More generally, we conjecture that every projection of K arises from the construction of Theorem 30; this is dual to Conjecture 28. We close by stating the dual of Conjecture 29.

Conjecture 31. Let K be a matroid, and let M be a projection of K . Let \mathcal{I} denote the collection of subsets \mathcal{H}' of $\mathcal{H}(K)$ for which there is no matroid K' such that

- K' is a projection of K and a lift of M ,
- each set in \mathcal{H}' is a hyperplane of K' , and
- $r(K') - r(M) < |\mathcal{H}'|$.

Then \mathcal{I} is the collection of independent sets of a matroid N on $\mathcal{H}(K)$, and $M \cong K_N$.

Acknowledgements

The author would like to thank James Oxley for his helpful comments on the manuscript.

References

- [1] R. Baer. Partitionen endlicher Gruppen. *Math. Z.*, 75:333-372, 1960/1961.
- [2] T. H. Brylawski. Constructions. In *Theory of matroids* (ed. N. White), pp. 127-223. Cambridge University Press, Cambridge, 1986.
- [3] H. H. Crapo. Single-element extensions of matroids. *J. Res. Nat. Bur. Standards Sect. B*, 69B:55–65, 1965.
- [4] M. DeVos, D. Funk, I. Pivotto. When does a biased graph come from a group labeling? *Adv. in Appl. Math.*, 61:1-18, 2014.
- [5] T. A. Dowling. A class of geometric lattices based on finite groups. *J. Combin. Theory Ser. B*, 14:61-86, 1973.
- [6] O. H. Kegel. Nicht-einfache Partitionen Endlicher Gruppen. *Arch. Math.*, 12:170-175, 1961.
- [7] J. Q. Longyear. The circuit basis in binary matroids. *J. Number Theory*, 12:71-76, 1980.
- [8] J. Oxley. *Matroid Theory*, Second Edition. Oxford Graduate Texts in Mathematics. Oxford University Press, 2011.
- [9] J. Oxley, S. Wang. Dependencies among dependencies in matroids. *Electron. J. Combin.*, 26(3), #P3.46, 2019.
- [10] M. Suzuki. On a finite group with a partition. *Arch. Math.*, 12:241-274, 1961.
- [11] T. Zaslavsky. Biased graphs. I. Bias, balance, and gains. *J. Combin. Theory Ser. B*, 47:32-52, 1989.
- [12] T. Zaslavsky. Biased graphs. II. The three matroids. *J. Combin. Theory Ser. B*, 51:46-72, 1991.