Constructive Torelli Theorem for Regular Matroids

Alec Elhindi

An essay submitted in partial fulfilment of
the requirements for the degree of
Master of Mathematical Sciences

Pure Mathematics
University of Sydney

October 30, 2024

Contents

Introduction

Graphs are one of the most applicable and easily understood objects in the world of mathematics. They arose from Leonhard Euler's famous paper on the Seven Bridges of Königsberg in 1736, as an abstraction of city maps, where land masses represent vertices (or nodes) and bridges represent edges. Modern applications of graph theory extend to many fields of mathematics such as knot theory, group theory and algebraic topology, as well as other fields such as computer science, physics, chemistry, biology and linguistics models.

Cycles are minimal closed walks in a graph, for example, if vertices represent cities and edges represent roads, you take a trip but return to the city you started at. It's easy to determine the cycles of a graph from its edges and vertices. A famous question first posed in the '90's is: are the cycles enough to determine the graph? If every edge of a graph participates in a cycle we call that graph *2-connected*, and it turns out this property which allows the graph to be essentially reconstructed from its cycles, and the minimal 2-connected subgraphs in any graph are cycles. To determine the structure of a graph from its cycle structure, we need to be able to determine the edges from knowing the cycles alone.

We first consider an algebraic object spanned by the cycles, called the *lattice of integer flows*. The *Discrete Torelli Theorem* – a graphical analogue of a result in algebraic geometry – states that the lattice of integer flows uniquely determines the graph up to an equivalence relation called *2-isomorphism*. This thesis presents a constructive version of this theorem, that is, an algorithm for reconstructing a (2-isomorphic representative of) the original graph from the lattice of integer flows.

Within the lattice of integer flows, the lattice points that are closest to the origin define a shape called the *Voronoi cell*, or *Voronoi polytope*. The main tool we use is Amini's correspondence between the faces of the Voronoi cell and directed 2-connected subgraphs of the graph. Under this correspondence, faces of increasing dimension map to oriented 2-connected subgraphs of decreasing size. The 0-dimensional faces, that is, the vertices, are in correspondence with certain orientations of the graph itself. The codimension one faces are in correspondence to the oriented cycles of the graph. This correspondence is used to choose a suitable basis of the cycle space, from which the graph can be reassembled.

Graphs that can be drawn in a plane without edges crossing are called *planar*. Planar graphs are equipped with a notion of duality: *dual graph* constructed by placing a vertex in each face of the graph, and connecting these vertices across the edges of the original graph. The resulting graph is also planar, the dual of the dual is the original graph. The lattice of integer flows interacts nicely with this duality. Unfortunately, this does not extend to

non-planar graphs, at least not within the category of graphs.

However, all graphs embed in a wider class of combinatorial structures called (regular) matroids. These generalise both graphs and the notion of independent sets of vectors in linear algebra. Every graph can be used to construct a *graphical matroid*, a subclass of regular matroids.

Regular matroids extend the notion of duality to all graphs, in the sense that any graphical matroid has a regular matroid dual, which is graphical if and only if the original graph is planar – and then so is its dual. Matroids which are the dual to a graphical matroid are called *co-graphical*.

The lattice of integer flows extends naturally to regular matroids, and the discrete Torelli Theorem – due to Su and Wagner in this setting – continues to hold. Thus, regular matroids provide a more natural context for the study of cycles and lattices of integer flows than graphs, and the results of this thesis are presented in this more general setting.

The main result of this thesis is an algorithmic reconstruction of the regular matroid from its lattice of integer flows, in other words, a constructive version of the discrete Torelli theorem.

The material In Chapter 1 we will give a basic overview of the necessary graph theory and matroid theory. In Chapter 2 we address notions of connectedness and operations for graphs and matroids. In Chapter 3 we introduce the lattices of integer flows, and prove a strong Torelli theorem for regular matroids (in the style of Greene). In Chapter 4 we provide an explicit algorithm to reconstruct a regular matroid from its lattice of integer flows.

Originality Statement

Chapters 1-3 contain original exposition of the introductory material synthesised from a range of sources including textbooks and research articles (cited throughout). Parts of Chapters 2 and 3 (particularly 2.1 and 3.3) existed only in the graph literature and were generalised to regular matroids by me. The constructive Torelli Theorem I prove in Chapter 4 was initially done for graphs in a preprint by my supervisor and Garoufalidis. The extension to regular matroids, which involved significant re-working of language and several new mathematical ideas, is my original work. It will be submitted as a joint publication with Dancso and Garoufalidis (in place of the initial preprint).

Acknowledgements

First and foremost, I would like to express my immense amount of gratitude to my supervisor, Zsuzsanna Dancso, for supporting me throughout my undergraduate and postgraduate degrees. Thank you, Zsuzsi, for your wise words, persistance with this research project, personal and academic advice, and being so welcoming to myself and fellow students. I do not think I would enjoy academia so much if you hadn't helped me through my undergraduate and masters degree.

I am very thankful to my peers: Damian Lin and Leo Jiang for many helpful and useful conversations – and for the template, Damian. Thank you especially to Leo who provided many insightful ideas and fundamental theorems for several proofs.

My thanks to the knot at lunch group for being so friendly and inviting, whether it was online via Zoom or in person, you made me look forward to discussing our research.

Finally, I would like thank my friends and family for supporting me throughout my studies, I couldn't have done it without you all. I would specifically like to thank my brother James Elhindi who guided me through my mathematics degree, and my dearest friend Daniel Tandany, who has supported every one of my endeavors, including this degree.

Chapter 1

Graphs, Matroids and Orientations

1.1 Graphs

We begin with a short introduction into the wonderful world of graph theory. Behind the formalism of graph theory lies a simply grasped concept which is intuitively introduced in primary school through activities like 'connect the dots'. The formal definition of a (finite) undirected *graph* is a pair, $G = (V, E)$, of sets $V = V(G)$ called *vertices* and $E = E(G)$ called *edges*, where the edges are unordered pairs of two vertices each. In pictures, we represent edges as paths drawn between their two vertices – called *incident* vertices.

See Fig. 1 for example: the two graphs in the figure both have $V(G) = \{v_1, v_2, v_3, v_4\}$ and $E(G) = \{e_1, e_2, e_3, e_4, e_5, e_6\}$. However, note that the definition of e_i is different for the two examples, for example $e_1 = \{v_2, v_3\}$ in the first graph, but $e_1 = \{v_1, v_2\}$ in the second graph.
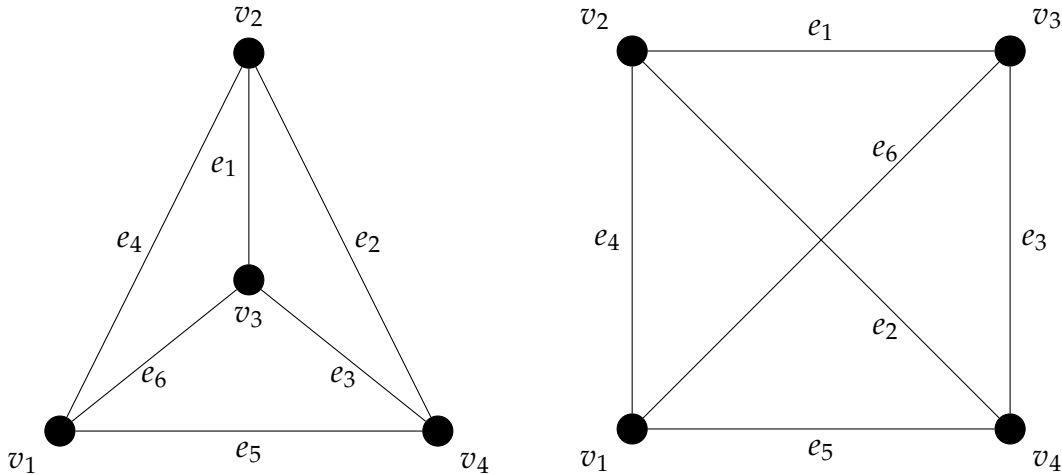

Figure 1: Two graphs with 4 vertices and 6 edges.

We can similarly define a *directed graph* or *oriented graph* by asserting that the edge pairs are ordered. An ordered pair (v_i, v_j) represents an edge from vertex v_i to v_j. An orientation can be applied to any graph by assigning an order (direction) to each edge. See Fig. 2 for an example of an orientation applied to the graphs in Fig. 1.

Connectivity is one of the most important basic features of a graph. The *connected components* of a graph are the maximal subgraphs for which every pair of vertices has a
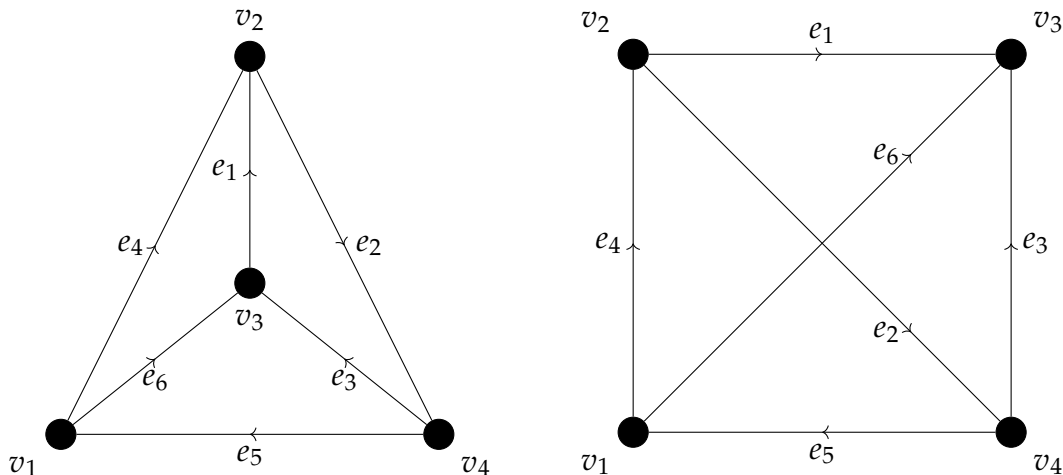
Figure 2: Two oriented graphs with 4 vertices and 6 edges.

path between them. If a graph contains only one connected component then we call that graph *connected*. An edge, which upon removal causes the remaining graph to not be connected, is called a *bridge*.

For a real world example, graphs model road networks between cities. If the graph is connected, this means that there is a road (sequence of edges) between any two cities (vertices). A bridge is a critical road which forms the only connection between two otherwise separate clusters of cities.

The mathematical structure of graphs which have high connectivity is particularly rich. Throughout this essay we focus on 2-edge-connected graphs: those which do not contain any bridges.

In general, an n-edge-connected graph, or n-connected – note that elsewhere in literature n-connected usually refers to n-vertex-connected – if, upon removing any combination of edges less than n, the resulting graph is connected. This is equivalent to saying that every vertex has at least n edges, and the graph has one connected component. The graph on the left of Fig. 3 is 2-connected as it remains connected upon removing any edge, however this is not true for the graph on the right, as removing e_2 does not result in a connected graph, i.e. e_2 is a bridge.

A directed graph is *strongly connected* if, for each connected component, there exists a directed path between any pair of vertices in both directions. Such an orientation is called a *strongly connected orientation* or *strong orientation*. A classical theorem of Robbins (Chapter 12.1, [GY06]) states that a (not necessarily connected) graph G has a strong orientation if and only if all of its connected components are 2-connected. For example, in Fig. 2, the first graph is strongly connected, but the second isn't, as there is no way to get from v_3 to any other vertex, we call such a vertex a *sink*. Thinking of graphs as road or bridges between cities, this is the same as saying there exists a one-way road between any two cities. One of the main applications of these orientations are, as expected, in the design of one-way road networks.

Any subset of the vertices and edges of a graph (oriented or unoriented), such that all
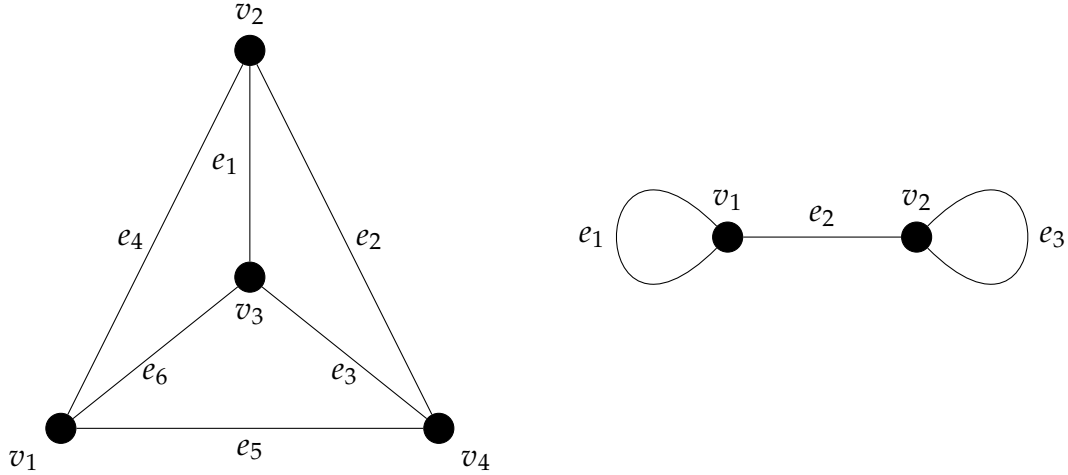
Figure 3: A 2-connected graph (left) and a connected, but not 2-connected, graph (right).

vertices in the edge pairs are included, forms a *subgraph*. A closed walk in a graph, that is a set of edges which start and end at the same vertex, is called a *circuit*. Minimal circuits are called *cycles*[1], where minimal means vertices except the first and last one are not repeated in the walk. The seven cycles contained in the first graph in Fig. 1 are drawn in Fig. 4. If a cycle consists of only one edge, we call this special type of cycle a *loop*.
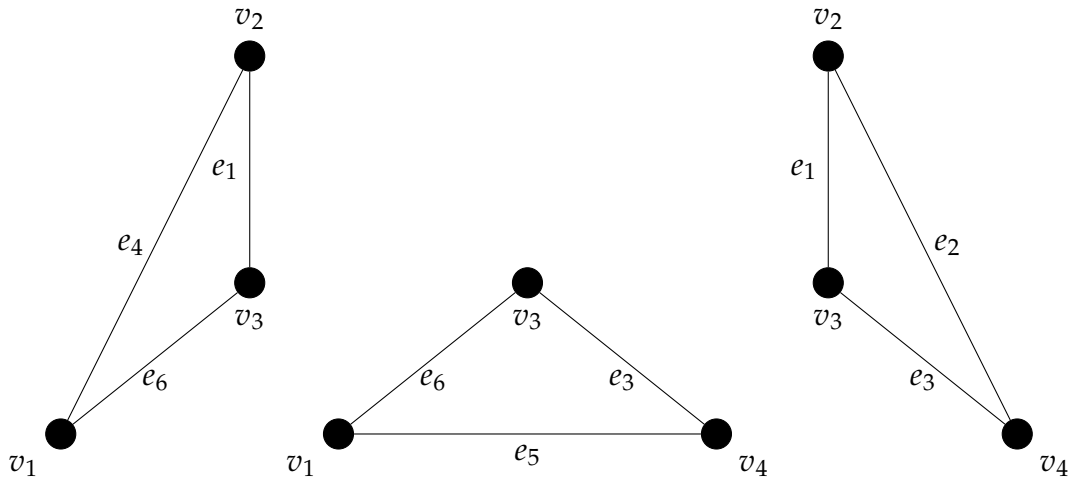

Figure 4: The seven cycles of the graph in Fig. 1.

---
[1]Unfortunately, in matroid terminology, this is flipped, and cycles are called circuits.
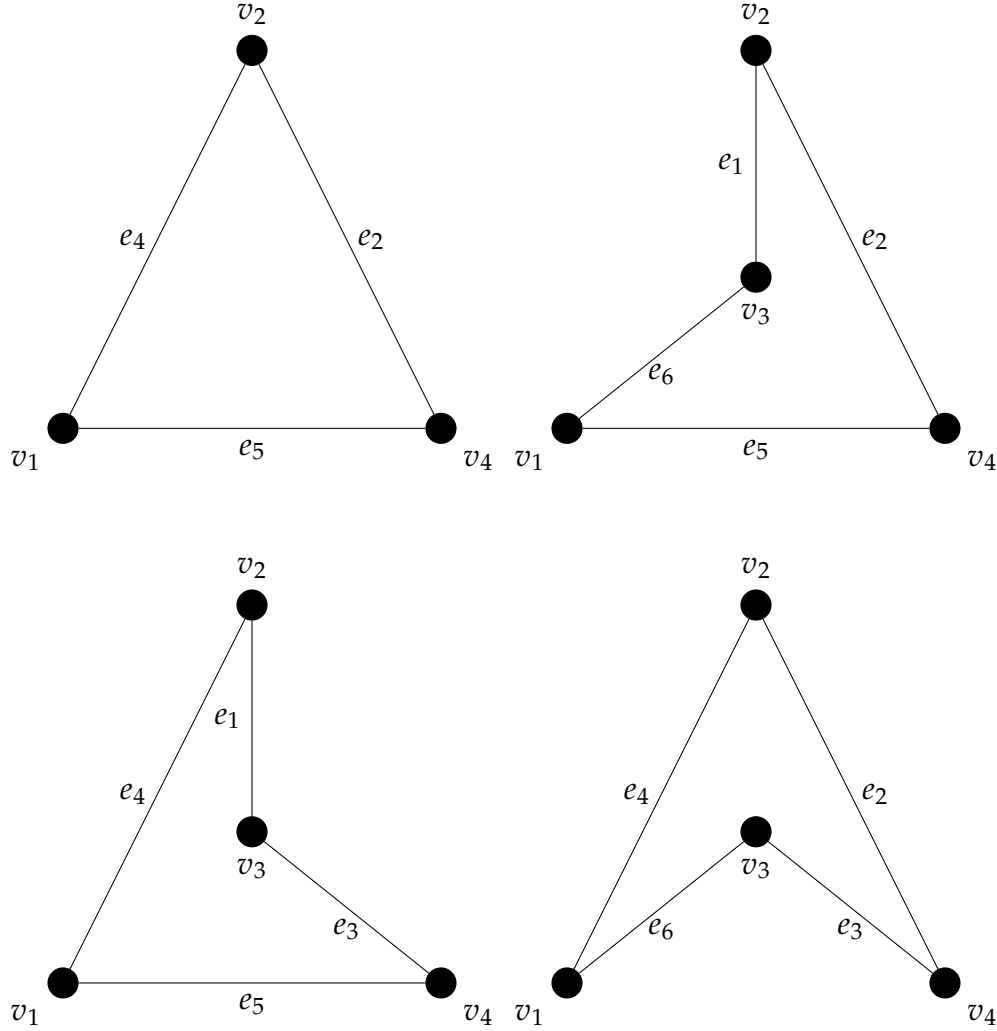
Figure 4: The seven cycles of the graph in Fig. 1.

A set of cycles is called a *cycle basis* for a graph if every edge is contained in some cycle in the cycle basis. The importance of 2-connected graphs arises here: graphs which are not 2-connected – or rather graphs for which not all components are 2-connected – do not have a cycle basis, as bridges do not participate in cycles. On the other hand, any 2-connected graph always has a circuit basis and can be constructed using trees in the graph. A *tree* is a subset of edges which does not contain a cycle, or equivalently, a subgraph which connects any two vertices by exactly one path. A *spanning tree* of a connected graph is a maximal tree, or equivalently, a subset of edges which meets every vertex, but does not contain a cycle. In a connected graph with $|V|$ vertices, any spanning tree contains $|V| - 1$ edges.

Let G be a graph with a spanning tree T, and choose an edge $e = \{v_i, v_j\}$ not in T. By the definition of spanning trees, there exists a unique path between in T connecting v_i and v_j. Adding e to this unique path creates a cycle, called the *fundamental cycle of e with respect to T*. Taking the fundamental cycles of all $e \notin T$ gives rise to the *fundamental cycle basis coordinatised by T*. The fundamental cycle basis thus consists of as many cycles as edges
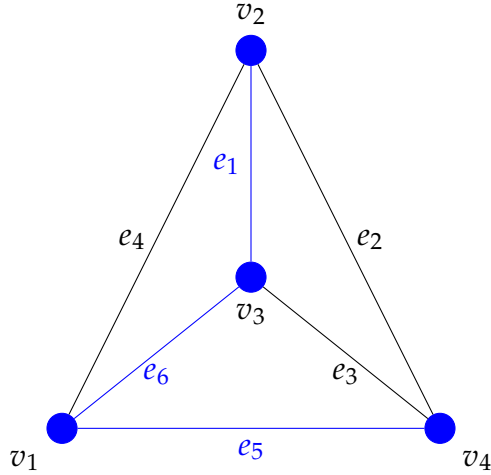
9

Figure 5: The spanning tree $\{e_1, e_5, e_6\}$ of the graph in Fig. 1.

not in the spanning tree, that is, $|E| - (|V| - 1) = |E| - |V| + 1$ cycles. In fact, this is true for any cycle basis.

There are two common notions to describe graphs being "the same". A graph *isomorphism* is a bijective map between vertex sets which preserves the edges, and if an isomorphism exists between two graphs, they are called *isomorphic*. The cycle structure of a graph does not fully determine its isomorphism type. A weaker type of equivalence, called a *2-isomorphism*, is a bijective map between edge sets which preserves cycles. If there exists a 2-isomorphism between graphs, then the graphs are *2-isomorphic*.
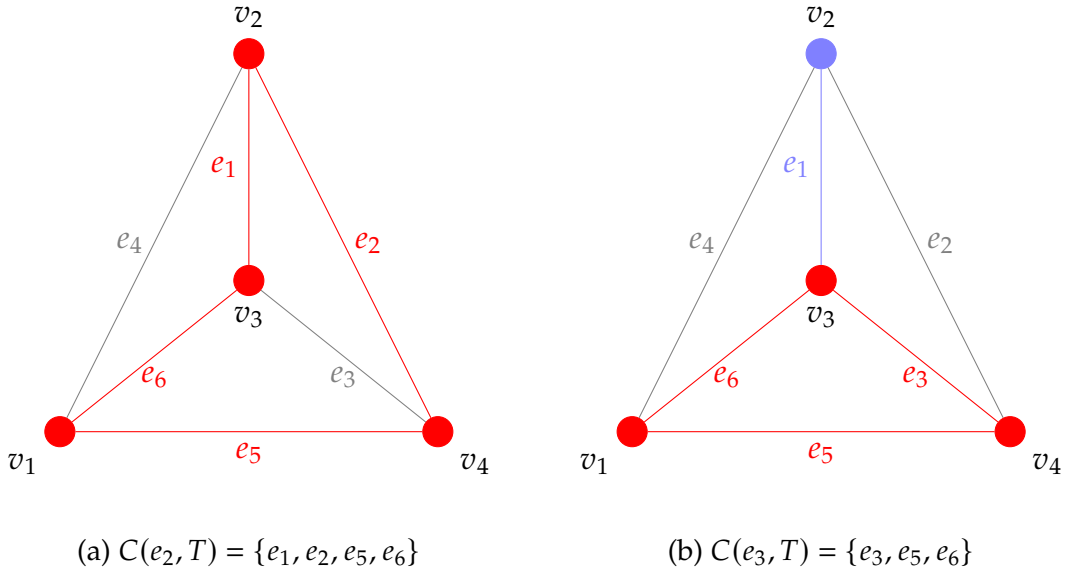

(a) $C(e_2, T) = \{e_1, e_2, e_5, e_6\}$

(b) $C(e_3, T) = \{e_3, e_5, e_6\}$

Figure 6: The fundamental cycles with respect to $T = \{e_1, e_5, e_6\}$ of the graph in Fig. 1, forming a fundamental cycle basis.
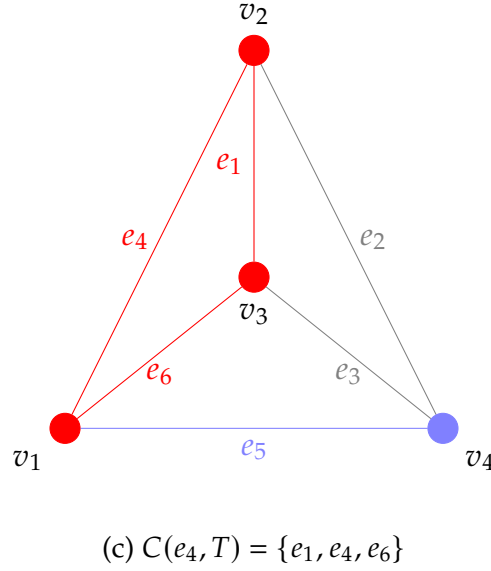
10

(c) $C(e_4, T) = \{e_1, e_4, e_6\}$

Figure 6: The fundamental cycles with respect to $T = \{e_1, e_5, e_6\}$ of the graph in Fig. 1, forming a fundamental cycle basis.

Graphs are often represented by images, with points for vertices and arcs or intervals for edges. A graph can be drawn in different ways, the drawing completely depends on where you place vertices, as the edges are then determined from vertices. For example, the two pictures in Fig. 1 are both drawings of the same graph, this is more obvious if we shift the vertices as shown through the sequence of moves shown in Fig. 7.
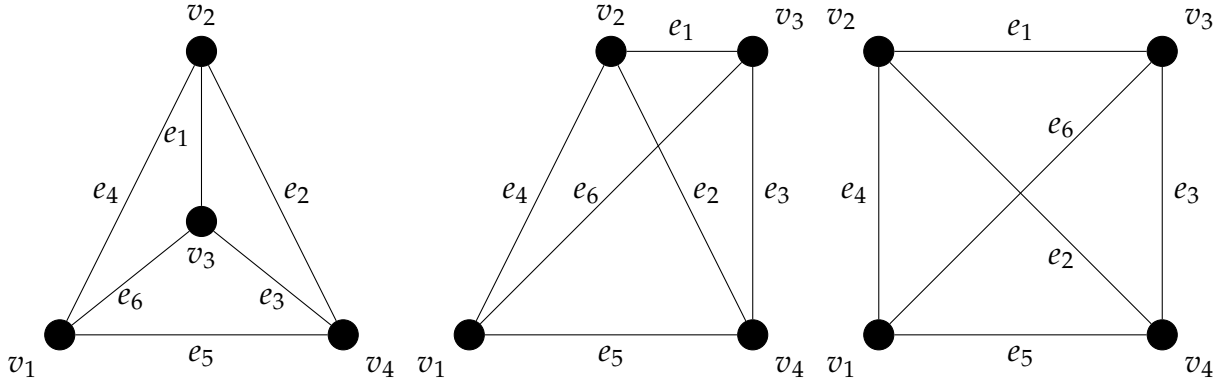
Figure 7: Graph drawings of K_4.

We call a graph *planar* if it can be drawn in the plane without edges crossing. The graphs in Fig. 1 are two ways of drawing K_4, and since one of these drawings is planar (has no edge crossings), therefore K_4 is a planar graph. The graph K_4 is called the *complete graph on 4 vertices* as any pair of its vertices is connected by an edge. This notion extends to n vertices, and is called the *complete graph on n vertices*, denoted K_n. In fact, K_4 is the largest of the complete graphs that is planar, K_n for $n \geq 5$ are not planar.

11

For planar graphs, we define the notion of a *planar dual graph*, which is obtained by placing a vertex in each face of the graph (that is the spaces surrounded by edges, and one for the outside of the graph), and drawing edges by connecting vertices once between each edge. Note that this means a bridge results in a loop in the dual graph, and the labels of vertices is lost, however we usually label the edges in the dual with the same label as the one it is drawn through in the original graph. For an oriented planar graph, there exists a *dual orientation* by taking each edge from the original graph and rotating its orientation 90 degrees clockwise, for example in Fig. 8.
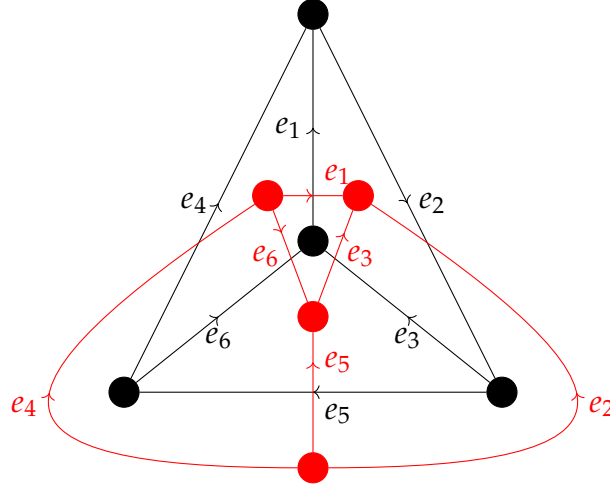

Figure 8: K_4 with some orientation drawn in black, with its oriented planar dual graph drawn in red.

1.2 Matroids

Matroids were originally introduced by Hassler Whitney in 1935 [Whi35] in the paper titled 'On the Abstract Properties of Linear Dependence'. Whitney noticed that for the set E given by columns of a matrix, any subset is either linearly independent or linearly dependent. For convenience we label the set of all independent subsets of E by $\mathcal{I}$. Whitney further noticed that these independent sets satisfy two properties:

(I2) For any $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$, then $I_2 \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$ are such that $|I_1| < |I_2|$, then there exists $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

The first one is quite an obvious feature of independence, if we remove some elements from a set of independent vectors it better be independent, we call it the *hereditary* property. However the second property is not as obvious, we call it the *independence augmentation* property. But what happens when we have a set of elements E that satisfy these properties, is it necessarily a dependence relation with vectors? The answer is no, in fact, in Whitney's paper, an example of such an object which cannot be represented as a set of vectors was

given. The object that arises is what we call a *matroid,* and we call (I2) and (I3) the second and third *matroid independence axioms.* Combined with the first matroid independence axiom, to remove pathological examples, we arrive at the following definition.

Definition 1.1. A (finite) *matroid* $M = (E, I)$ is an ordered pair of a finite set E, called the *base set,* and I, called the "family of independent subsets of E" which satisfies the following axioms:

(I1) $\emptyset \in I$,

(I2) and (I3).

As with graphs we write the base set as $E(M)$, and denote the family of independent subsets of $E(M)$ as $I(M)$. Writing lists of independent sets can be tedious, and (I2) guarantees that any subset of an independent set is independent. For example, if $X = \{1, 2, 3\}$ is an independent set, we know that every element of the power set of X is also independent, so can we just describe these independent sets by X? If we consider all maximal independent sets with respect to inclusion, then we can describe every independent set with just these maximal sets. These maximal independent sets are called *basis sets* and provide a much more convenient way to describe matroids in terms of independence. Just like with independent sets, matroids have an axiomatic formulation in terms of bases, which is often what we consider when thinking about matroids in terms of independence, so matroids can also be defined as $M = (E, \mathcal{B})$ where $\mathcal{B}$ is the set of bases.

Dependent sets are those which are not independent, and they also have an axiomatic way of defining matroids – for example, any dependent set should stay dependent upon adding extra elements, which is clear by taking the complement of (I2). With that in mind, we can once again provide a more convenient way of thinking about matroid dependency, as maximal independent sets describe independence, minimal dependent sets describe dependency. Such sets are known as *circuits,* and once again they have a convenient axiomatic formulation.

Definition 1.2. A (finite) *matroid* $M = (E, C)$ is an ordered pair of a finite set E, called the *base set,* and C, called the "family of circuit subsets of E" which satisfies the following axioms:

(C1) $\emptyset \notin C$.

(C2) For all $C_1, C_2 \in C$ such that $C_1 \subseteq C_2$, then $C_1 = C_2$.

(C3) If $C_1, C_2 \in C$ are distinct circuits with $e \in C_1 \cap C_2$, then there exists $C_3 \in C$ where $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

The family of circuit subsets of $E(M)$ is denoted by $C(M)$. We call (C3) the *(weak) circuit elimination axiom* and is fundamental to the understanding of circuits. Note it is called the weak axiom as there is an equivalent, stronger version of this statement for matroids – that is it can be proven without the need for extra assumptions. All the definitions mentioned are equivalent and throughout we will mostly use the later notion of matroids with their circuit definition.

There is a very important relationship between bases and circuits. As bases are the largest independent sets, adding any element in their complements results in a dependent set, thus must contain circuits. But more can be said about such circuits, for each element in the complement there is only one such circuit, called the fundamental circuit.

Proposition 1.3. Let $B \subsetneq E(\mathcal{M})$ be a basis set in a matroid $\mathcal{M}$. For each $e \in E(\mathcal{M}) \setminus B$, then there exists a unique circuit $C(e, B) \subseteq B \cup \{e\}$ such that $e \in C(e, B)$, called the *fundamental circuit of e with respect to B*.

Proof. $B \cup \{e\}$ is dependent, so it contains some circuit, and any such circuit must contain e, otherwise that circuit was originally part of the independent set B, a contradiction. Assume that there are distinct such circuits C_1, C_2, then by (C3) there exists a circuit $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\} \subseteq B$. However this contradicts the fact that B is independent, so the circuit contained in $B \cup \{e\}$ is unique.

$\square$

In fact, B need not even be a basis, the only requirement is that B is independent and $B \cup \{e\}$ is dependent – which is always true for basis sets. The same proof shows that if $I \cup \{e\}$ is dependent, for an independent set I, then there is a unique circuit contained in that too.

Whilst matroids have a strong foundation in terms of linear independence, someone who has studied graph theory might recognise the above proposition as the fundamental cycle of a graph with respect to a spanning tree. In fact, matroids not only generalise linear independence, but generalise graphs as well. The following example gives a more concrete understanding as to how matroids generalise these notions.

Example 1.4. The first example builds upon the original notion of matroids as a generalisation of vector independence by thinking of columns of a matrix. Given a matrix M over a field $\mathbb{F}$, let E be the set of column vectors of M and $\mathcal{I}$ be the set of subsets of E that are linearly independent sets. Alternatively, let $\mathcal{C}$ be the set of subsets of E that are minimally linearly dependent, i.e. all strict subsets are linearly independent. Then $\mathcal{M}(M) = (E, \mathcal{I})$ is a matroid with respect to Definition 1.1 and $\mathcal{M}(M) = (E, \mathcal{C})$ is a matroid with respect to Definition 1.2 (note these are equivalent). Such a matroid is called an $\mathbb{F}$-*representable matroid* and are an important class of matroids which we will expand upon later.

The second of which relates matroids and graphs, and is the reason why sometimes matroids are considered a generalisation of graphs as well as independence. Given a finite graph G, let $E = E(G)$, let $\mathcal{I}$ be the family of all trees in G and let $\mathcal{C}$ be the family of cycle subsets in G. The pair $\mathcal{M}(G) = (E, \mathcal{I})$ is a matroid with respect to Definition 1.1 and $\mathcal{M}(G) = (E, \mathcal{C})$ is a matroid with respect to Definition 1.2, called the *graphical matroid* (or *cycle matroid*) associated to G.

For a graphical matroid $\mathcal{M}(G)$, the basis sets $B \in \mathcal{B}$ are precisely the spanning trees of G, and the fundamental cycle with respect to a spanning tree corresponds to the fundamental circuit with respect to the basis given by the spanning tree.

Notice that the definition of graphical matroid only requires knowledge of edges and circuits, which are sets of edges, not vertices. So upon the conversion from graph to matroid all information of vertices is lost, so can we convert back from a graphical matroid

to its graph? The answer is not precisely. Most of the graph can be reconstructed by just drawing the cycles out, but the first issue arises when we try to draw edges that do not participate in a cycle, or loops. Where should we draw these? And what if our cycles can be collected into two sets that are disjoint, does the graph then connect at a vertex, or is it not connected? For example, let's consider the matroid $M = (E, C)$ where $E = \{e_1, e_2, e_3\}$ and $C = \{\{e_1\}, \{e_3\}\}$.

Then any of the graphs in Fig. 9 will result in the graphical matroid above even though, for example, the second one is not connected and has two more vertices than the other two examples.
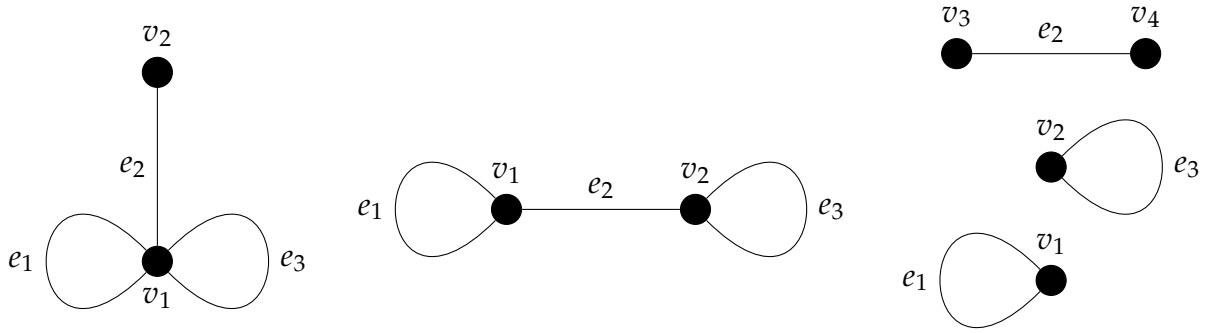

Figure 9: Three graphs resulting in the same graphical matroid.

We again want some sort of notion of when two matroids are the same or not, like we did with graphs. For graph isomorphisms, we required a bijective mapping of vertices and we no longer have knowledge of vertices. However, recall that 2-isomorphisms only required a mapping of edges that preserves circuits. The notion of isomorphisms for matroids borrows from 2-isomorphisms of graphs in the sense that an *isomorphism* of matroids $M = (E, C)$ and $M' = (E', C')$ is a set bijection $\varphi : E \to E'$ such that all subsets of E are circuits in M if and only if they are circuits in M' when mapped under φ. We write $M \cong M'$.

Example 1.5. Any 2-isomorphism of graphs G, G' induces an isomorphism of the corresponding graphical matroids $M(G), M(G')$ under the same set bijection.

When we originally defined graphic and $\mathbb{F}$-representable matroids, we stated that they are matroids that arise from graphs and $\mathbb{F}$-matrices respectively, however we extend this definition slightly by saying that a matroid is *graphic* if it is isomorphic to the graphical matroid $M(G)$ for some graph G. Similarly, a matroid is $\mathbb{F}$-*representable* if it is isomorphic to the $\mathbb{F}$-representable matroid $M(M)$ of some matrix M over $\mathbb{F}$. Finally, we call a matroid *regular* if it is $\mathbb{F}$-representable for every field $\mathbb{F}$. These are a very special class of matroids which we will mostly consider later, as they are only a slight generalisation of graphical matroids.

A *totally unimodular matrix* is a matrix over $\mathbb{R}$ for which every square submatrix has determinant $-1, 0$ or 1. A matroid is regular if and only if it is isomorphic to a matroid $M(M)$ for some totally unimodular matrix M. This is sometimes used as the definition of a regular matroid, or a more convenient way to write a matroid which is representable

over every field. In fact we have a special way of creating the regular matroid associated to a graph by creating a TU matrix. The *signed incidence matrix* of a directed graph with m vertices and n edges is a n-by-m matrix (i.e. rows represent vertices and columns represent edges) with entries a_{ij} given by

$$
a_{ij} = \begin{cases} 1 & \text{if vertex } i \text{ is the tail of edge } j \text{ and } j \text{ is not a loop} \\ -1 & \text{if vertex } i \text{ is the head of edge } j \text{ and } j \text{ is not a loop} \\ 0 & \text{otherwise.} \end{cases}
$$

Lemma 1.6. The signed incidence matrix of a directed graph is totally unimodular.

The proof of this follows from a more general fact that any matrix whose entries are 0 or ± 1 with at most one 1 and one -1 in each column is totally unimodular, so we include a proof of that fact here.

Proof. Let A be such a matrix (in particular the signed incidence matrix of a directed graph is such a matrix). The proof follows by induction on the size of square submatrices. Let X be a $k \times k$ submatrix. If $k = 1$ then clearly $\det X \in \{0, 1, -1\}$, so assume the claim is true for all $k < n$, for some fixed $n \geq 2$. Now let X be a $n \times n$ submatrix for $n \geq 2$. If X has a column with at most one non-zero entry (that is either 1 or -1), then expanding the determinant along that column gives the resulting determinant is that non-zero entry, ± 1, times the determinant of the $n-1 \times n-1$ submatrix, up to a sign depending on the position of the entry. Now by the induction hypothesis this submatrix has determinant 0 or ± 1, so the determinant of X is 0 or ± 1. Now if X only has columns with two non-zero entries, then by assumption there must be exactly one -1 and 1 in each column. Then the rows of X must be linearly dependent as they all sum to the zero vector, so the determinant of X is 0, and the claim is proved.

$\square$

Regular matroids are nicer to work with than general matroids, the reason being that they remain true to the motivation of matroids, as their base set elements correspond to vectors, we can talk about independent and dependent sets in terms of linear independence. This means that for some dependent set D, we can write

$$
\sum_{d \in D} a_d d = 0
$$

and in the case where D is a circuit, i.e. a minimal dependent set, the coefficients a_d are either 1 or -1. Furthermore, we can consider the regular matroid $\mathcal{M}$ over $\mathbb{F}$ as a $\mathbb{F}$-vector space, in the sense that for $|E(\mathcal{M})| = n$, the elements of $E(\mathcal{M})$ are the unit vectors for $\mathbb{F}^n$, i.e. they are the axes in the n dimensional vector space. To be more precise, this vector space is $\mathbb{F}^{E(\mathcal{M})}$, that is linear combinations of elements in $E(\mathcal{M})$ with coefficients in $\mathbb{F}$. We will consider this intuition more later in this paper.

One important notion of matroids, as with graphs, is the idea of a dual matroid. However, unlike graphs, every matroid has a dual. As matroids generalise graphs, we want our matroid dual to generalise the planar graph dual. It is a well-known property that the complement of a spanning tree is a spanning tree in the dual (we omit the proof

of this as the proof for matroids implies it), which in the language of matroids is saying that the complement of basis sets are the basis sets of the dual. This is precisely how the dual matroid is defined. First, let us recall the matroid basis axioms. Writing $\mathcal{B}(M)$ for the family of basis subsets of $E(M)$, where again we denote $M = (E, \mathcal{B})$, then $\mathcal{B}$ satisfies:

(B1) $\mathcal{B} \neq \emptyset$.

(B2) For all $B_1, B_2 \in \mathcal{B}, |B_1| = |B_2|$.

(B3) If $B_1, B_2 \in \mathcal{B}$ are such that there exists $e \in B_1 \setminus B_2$, then there exists $f \in B_2 \setminus B_1$ such that $(B_1 \setminus \{e\}) \cup \{f\} \in \mathcal{B}$.

In fact, only the first and third properties are required to show that the axioms above define a matroid equivalently to the others. However, the second property gives great intuition into the nature of basis sets in a matroid, just like how graphs have the property that their spanning trees are all the same size. Note, the third basis axiom is one of multiple *basis exchange axiom* and is quite important to understanding the relationship of bases.

Proposition 1.7. Let $M = (E, \mathcal{B})$ be a matroid with bases $\mathcal{B}$, then there exists a *dual matroid* of M given by $M^* = (E, \mathcal{B}^*)$ where the bases are $\mathcal{B}^* = \{E \setminus B \mid B \in \mathcal{B}\}$.

Whilst (B3) is that which is used in the definition of matroids and taken as an axiom, an alternate, but similar, basis exchange axiom is required to prove this indeed defines a matroid.

Lemma 1.8. Let $M = (E, \mathcal{B})$ be a matroid with bases set $\mathcal{B}$. Then if $B_1, B_2 \in \mathcal{B}$ are such that there exists $e \in B_2 \setminus B_1$, then there exists $f \in B_1 \setminus B_2$ such that $(B_1 \setminus \{f\}) \cup \{e\} \in \mathcal{B}$.

Proof. Consider the fundamental circuit of e with respect to B_1, $C(e, B_1)$. Since it is a dependent set and B_2 is independent, $C(e, B_1) \setminus B_2$ is nonempty, so there exists $f \in C(e, B_1) \setminus B_2$. Then

$$C(e, B_1) \setminus B_2 \subseteq (B_1 \cup \{e\}) \setminus B_2 = B_1 \setminus B_2$$

as $e \in B_2$, so $f \in B_1 \setminus B_2$. Now $(B_1 \setminus \{f\}) \cup \{e\}$ is independent as $C(e, B_1) \not\subseteq (B_1 \setminus \{f\}) \cup \{e\}$. Furthermore, as $\left|(B_1 \setminus \{f\}) \cup \{e\}\right| = |B_2|$, we have that $(B_1 \setminus \{f\}) \cup \{e\}$ is a basis. $\qquad \square$

Proof of Proposition 1.7. We must verify that this is a matroid in terms of our definition with bases.

The proof of (B1) is straightforward as $\mathcal{B} \neq \emptyset$, there exists $B \in \mathcal{B}$ such that $E \setminus B \in \mathcal{B}^*$, so $\mathcal{B}^* \neq \emptyset$.

Again, the proof of (B2) is straightforward as each basis set in M has the same cardinality, so their complements with respect to E will also have the same cardinality (as they are all subsets of E).

Finally, take $B_1^*, B_2^* \in \mathcal{B}^*$ such that there exists $e \in B_1^* \setminus B_2^*$. Then let $B_1 := E \setminus B_1^*$ and $B_2 := E \setminus B_2^*$, then clearly $B_1, B_2 \in \mathcal{B}$. Now

$$B_1^* \setminus B_2^* = B_1^* \cap (E \setminus B_2^*)$$
$$= (E \setminus B_1) \cap B_2$$
$$= B_2 \cap (E \setminus B_1)$$
$$= B_2 \setminus B_1$$

so $e \in B_2 \setminus B_1$. Then by Lemma 1.8, there exists $f \in B_1 \setminus B_2 = B_2^* \setminus B_1^*$ such that $(B_1 \setminus \{f\}) \cup \{e\} \in \mathcal{B}$. By definition of the dual, the complement of this set is in $\mathcal{B}^*$ and so

$$E \setminus ((B_1 \setminus \{f\}) \cup \{e\}) = ((E \setminus B_1) \setminus \{e\}) \cup \{f\}) = (B_1^* \setminus \{e\}) \cup \{f\} \in \mathcal{B}^*.$$

So as for $B_1^*, B_2^* \in \mathcal{B}^*$ with $e \in B_1^* \setminus B_2^*$, we can find $f \in B_2^* \setminus B_1^*$ such that $(B_1^* \setminus \{e\}) \cup \{f\} \in \mathcal{B}^*$, $\mathcal{B}^*$ satisfies (B3) and thus $\mathcal{M}^*$ is a matroid.

$\square$

The set of circuits of $\mathcal{M}^*$ is called the set of *cocircuits* of $\mathcal{M}$. In general, the prefix 'co-' refers to the dual matroid, so bases of $\mathcal{M}^*$ are cobases of $\mathcal{M}$, etc. Note that cocircuits of $\mathcal{M}$ are the minimal subsets of $E(\mathcal{M})$ with respect to inclusion which intersect every basis of $\mathcal{M}$.

As with graphs, we call a circuit which consists of one element a *loop* and a set which is a circuit in the dual of the matroid a *coloop*. Coloops are elements which participate in every basis, and in the case of graphical matroids, they are precisely the elements which are bridges – they must be a part of every spanning tree as it is the only way to get between the vertices on either side of the bridge.

Proposition 1.9 (Proposition 2.2.22 [Oxl06])**.** The matroid dual of a regular matroid is regular.

In fact, an explicit matrix can be formed to describe the dual matroid. Let $\mathcal{M}$ be a regular matroid represented by an $r \times m$ TU matrix M. Then for any basis $B \in \mathcal{M}(M)$ (note that $|B| = r$), there exists a sequence of moves consisting mainly of elementary row and column operations, over the field $\mathbb{F}$, which results a matrix $M' := \begin{bmatrix} I_r & L \end{bmatrix}$ which represents the same matroid, i.e. $\mathcal{M}(M) \cong \mathcal{M}(M')$. Here L is some $m - r \times r$ matrix, I_r is the $r \times r$ identity matrix, and we call M' the *standard matrix representation of $\mathcal{M}$ with respect to B*. Then:

1. The standard matrix representation of $\mathcal{M}^*$ with respect to B is $\begin{bmatrix} -L^T & I_{|E|-r} \end{bmatrix}$.

2. The matrix

$$U = \begin{bmatrix} -L \\ I_s \end{bmatrix}$$

   is such that $MU = O$, where $s = \dim \ker(M)$, and moreover the columns of U form an ordered basis $B(\mathcal{M}, B)$ of $\mathcal{F}(\mathcal{M})$ called the *fundamental circuit basis of $\mathcal{F}(\mathcal{M})$ coordinatised by B*. This is precisely the set of fundamental circuits with respect to B.

Regular matroids are an important class of matroids due to the fact that they can be described by a matrix which encodes their structure in terms of linear independence. Because of this, many pioneers in matroid theory wanted to try classify all regular matroids. As any graph has an associated signed incidence matrix after applying some arbitrary orientation, all graphic matroids are regular. By Proposition 1.7 we also know that the duals of graphic matroids are regular, in matroid theory these matroids are called *cographic matroids*. Note that a cographic matroid can be graphic, this happens if and only if it is planar – this implies also that its dual is planar.

It's natural to now ask, are there any regular matroids which are not graphic or cographic? The answer is yes, in 1977 Robert Bixby [Bix77] identified a matroid R_{10} which is represented by the following totally unimodular matrix, thus is regular, but is neither graphic nor cographic.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \end{bmatrix}$$

R_{10} actually plays a fundamental role in the characterisation of the class of regular matroids – that is, all regular matroids can be generated by R_{10}, graphic and cographic matroids.

1.3 Oriented (Regular) Matroids

As with graphs, matroids can be oriented, ideally so that it coincides with the definition of an oriented graph. Assume that there is a fixed orientation on the graph, and we say that every edge is 'positive'. Then flipping an edge's orientation is taking the 'negative' of that edge, which makes an orientation just a formal assignment $\epsilon : E(G) \to \{1, -1\}$. The same notion applies to graphs, the signs we assign are called the *orientation*, and we can think of it as a map $\epsilon : E(\mathcal{M}) \to \{1, -1\}$. Note when we flip an edge in a graph, this corresponds to multiplying the corresponding column in its signed incidence matrix by -1. Similarly, when we orient a regular matroid, we are applying a sign to each element in the base set, which corresponds to multiplying the corresponding column by ± 1. Furthermore, this column assignment does not change the underlying matroid – that is removing the notion of orientation, the matroid is identical. Given an orientation ϵ, we call the resulting matroid an *oriented matroid* and denote it $\mathcal{M}^\epsilon$ with representing matrix M^ϵ (which has columns multiplied by their orientation sign). Luckily the idea behind orienting a regular matroid is far simpler than that in general matroid theory, and we only consider regular matroids.

Fortunately, it is far easier to study oriented regular matroids than oriented matroids in general, and we will only be considering regular matroids throughout. Applying an orientation causes the resulting representing matrix M^ϵ to still be a TU matrix, as any submatrix's determinant is altered by at most a sign swap. So the oriented matroid can in reality just be thought of as a regular (unoriented) matroid, i.e. we can freely interchange

between oriented and unoriented matroids, allowing us to utilise parts of oriented matroid theory without unnecessary detail.

The orientation mapping now allows us to extend our notion of subsets under this mapping too. Mapping a set under ϵ results in a *signed set*, where our original set S is partitioned into a positive set S^+ and a negative set S^- that are disjoint. S^+ consists of the elements in S which have positive sign while S^- consists of the elements in S^- which have negative sign, i.e. $S^+ = \epsilon^{-1}[+1]$ and $S^- = \epsilon^{-1}[-1]$. As each element is mapped to a distinct sign, we can write $S = S^+ \sqcup S^-$. The main signed sets we think about are *signed circuits*, and as we will see in the axiomatic definition of oriented matroids, any signed circuit gives rise to another signed circuit which flips all signs, i.e. if C is a signed circuit then $-C$ is also a signed circuit, where $(-C)^- := C^+$ and $(-C)^+ := C^-$. This is clear in terms of graphs, we can choose to traverse a circuit in two directions, which decides which elements are positively oriented and which are negative. If we start by following the direction of e and declare it positive, then following the circuit any edges that agree are positive and any which disagree are negative. However, if we start by following the opposite direction of e and declare that positive, then we get the opposite signed circuit. This is the same as saying multiplying the entire matrix by -1 results in the same regular matroid, but the signs of the elements has been flipped.

We will now work through a complete example. Recall the circuits of K_4 in Fig. 4, they are

$$C_1 = \{e_1, e_4, e_6\}$$
$$C_2 = \{e_3, e_5, e_6\}$$
$$C_3 = \{e_2, e_4, e_5\}$$
$$C_4 = \{e_1, e_2, e_3\}$$
$$C_5 = \{e_2, e_3, e_4, e_6\}$$
$$C_6 = \{e_1, e_3, e_4, e_5\}$$
$$C_7 = \{e_1, e_2, e_5, e_6\}.$$

Under the orientation in Fig. 2, these become the signed circuits

$$\pm C_1 = \pm(\{e_1, e_6\} \sqcup \{e_4\}) := \pm\{+e_1, -e_4, +e_6\}$$
$$\pm C_2 = \pm(\{e_3\} \sqcup \{e_5, e_6\}) := \pm\{+e_3, -e_5, -e_6\}$$
$$\pm C_3 = \pm(\{e_2, e_4, e_5\}) := \pm\{+e_2, +e_4, +e_5\}$$
$$\pm C_4 = \pm(\{e_1, e_2, e_3\}) := \pm\{+e_1, +e_2, +e_3\}$$
$$\pm C_5 = \pm(\{e_2, e_3, e_4\} \sqcup \{e_6\}) := \pm\{+e_2, +e_3, +e_4, -e_6\}$$
$$\pm C_6 = \pm(\{e_1, e_3\} \sqcup \{e_4, e_5\}) := \pm\{+e_1, +e_3, -e_4, -e_5\}$$
$$\pm C_7 = \pm(\{e_1, e_2, e_5, e_6\}) := \pm\{+e_1, +e_2, +e_5, +e_6\}.$$

In the first set of notation, where we have written the sets as a disjoint union, the first set represents the positive elements and the second set represents the negative elements. The second set of notation has been included for convenience, but is a slight abuse of notation. We call circuits for which $C = C^+$ *positive circuits* and circuits for which $C = C^-$ *negative circuits*. Similarly to matroids, oriented matroids satisfy a set of axioms.

Definition 1.10. An *oriented matroid* is an ordered pair $\mathcal{M} = (E, \mathcal{C})$, where E is a set, called the *base set*, and $\mathcal{C}$ is a collection of signed sets, called *signed/oriented circuits* supported on subsets of E, such that $\mathcal{C}$ satisfies the following axioms:

(±C1) $\emptyset \notin \mathcal{C}$.

(±C2) For all $C \in \mathcal{C}$, $-C \in \mathcal{C}$.

(±C3) For all $C_1, C_2 \in \mathcal{C}$, if $C_1 \subseteq C_2$ as sets, then $C_1 = C_2$ or $C_1 = -C_2$.

(±C4) For all $C_1, C_2 \in \mathcal{C}$, if $C_1 \neq -C_2$ and there is an $e \in (C_1)_+ \cap (C_2)_-$, then $\exists\, C_3 \in \mathcal{C}$ such that $(C_3)_+ \subseteq ((C_1)_+ \cup (C_2)_+) \setminus \{e\}$, and $(C_3)_- \subseteq ((C_1)_- \cup (C_2)_-) \setminus \{e\}$.

As with graphs, we want to define a special class of oriented matroid called strongly connected matroids. For graphs it made sense that a strongly connected orientation was one where a path existed between any two vertices in both directions, but with no notion of vertices for matroids, this does not transfer verbatim. Fortunately, it is quite easy to verify that this is equivalent to every edge participating in a positive circuit. We can interpret this statement for oriented matroids, a matroid $\mathcal{M} = (E, \mathcal{C})$ is *strongly connected* if every $e \in E$ is part of a positive circuit. We further say that for any orientation ϵ of $\mathcal{M}$ is strongly connected if $\mathcal{M}^\epsilon$ is strongly connected, we call this a *strongly connected orientation*. If we consider a graph G being 'included' in a graph H if G is a subgraph of H, we can induce a partial ordering on all the subgraphs of some graph G. Specifically, we want to consider this partial ordering on only the subgraphs which are oriented and in fact are oriented with a strongly connected orientation, where for inclusion we also require that the orientation on the subgraph is the induced orientation. Doing so, we arrive at a very important partially ordered set. This notion easily generalises to matroids under the same construction and we can create a partially ordered set (poset) structure on the set of all strongly connected submatroids of a regular matroid.

Definition 1.11. Let $\mathcal{M} = (E, \mathcal{C})$ be a regular matroid with representing matrix M. Then the *poset of strongly connected orientations* of $\mathcal{M}$, denoted $\mathcal{SC}(\mathcal{M})$, contains ordered pairs $(\mathcal{N}, D_{\mathcal{N}})$, where

- $\mathcal{N} = (E', \mathcal{C}')$ is a submatroid of $\mathcal{M}$, that is, $E' \subseteq E$ and $\mathcal{C}'$ contains the induced circuits (i.e. the restriction of $\mathcal{M}$ to E');

- $D_{\mathcal{N}}$ is an orientation of $\mathcal{N}$;

- The resulting oriented matroid after applying the orientation $D_{\mathcal{N}}$ to $\mathcal{N}$ is strongly connected.

Then the ordering is given by $(\mathcal{N}, D_{\mathcal{N}}) \leq (\mathcal{N}', D_{\mathcal{N}'})$ if $\mathcal{N}'$ is a submatroid of $\mathcal{N}$ and $D_{\mathcal{N}'}$ is the induced orientation of $D_{\mathcal{N}}$, i.e. applying the orientation $D_{\mathcal{N}}$ to the matrix representing $\mathcal{N}$ then taking the submatroid corresponding to the elements in $\mathcal{N}'$ gives the same oriented matroid as applying the orientation $D_{\mathcal{N}'}$ to $\mathcal{N}'$.

In fact the poset $\mathcal{SC}(\mathcal{M})$ is a graded poset. For graphs the poset $\mathcal{SC}(G)$ has grading given by g minus the genus of the subgraph, where g is the genus of the original graph G. We will define what this grading is for matroids later in the thesis. Note that, in particular, the maximal non-empty members of the poset are circuits – indeed they are strongly orientable as either positive or negative orientations, and they are maximal as removing any element from a circuit guarantees the resulting matroid cannot be strongly oriented.

Given a regular matroid $\mathcal{M}$, we call a set of circuits $C' \subseteq C$ a *circuit basis* of $\mathcal{M}$ if for every $e \in E(\mathcal{M})$ there exists some circuit in C' that contains e, and the circuits in C' are linearly independent in the sense of vectors in $\mathbb{F}^n$. Note that for any basis set B in $\mathcal{M}$,

$$C' = \{C(e, B) \mid e \in (E(\mathcal{M}) \setminus B)\}$$

is a circuit basis of $\mathcal{M}$, i.e. it consists of the fundamental circuits for every element not in the basis. This is clearly a circuit basis by definition of the fundamental circuit as every element participates in a circuit, and they are certainly linearly independent as each circuit contains a unique $e \notin B$ that cannot be in the others. We call this the *fundamental circuit basis of $\mathcal{M}$ coordinatised by B*. For oriented regular matroids, we can similarly define an *oriented circuit basis*, however if every circuit in the circuit basis is a positive circuit, we call it a *positively oriented circuit basis*.

Chapter 2

Matroid Connectedness and Operations

As with graphs, matroids carry much richer structure and can be understood better when they have some notion of connectedness. Recall for graphs, a graph being connected meant that every pair of vertices, there exists a path between them, i.e. it has one connected component. However, as is the common issue with abstraction to matroids, there are no vertices in the eyes of matroids. As such, this definition does not really transfer to matroids as such, and so the notion of a connected matroid does not exist in the same way as it does for graph. Connected matroids are defined to be the same as 2-connected matroids, and all definitions of connectedness are more aligned with that of vertex connectedness. Fortunately edge connectedness transfers quite easily to a more intuitive notion known as *cogirth*.

The cogirth of a matroid is the length of the shortest cocircuit, which is very similar to vertices in the sense that, for graphical matroids, the edges incident to a vertex are either cocircuits, or a union of cocircuits. The notion of cogirth in a matroid generalises edge connectedness in a graph in the sense that any matroid of cogirth n is n-edge connected, but not $n + 1$-edge connected.

It is well-known that a graph is 2-connected if and only if every for every pair of edges, there is a cycle containing both. This ensures both that there is one connected component, so that the graph is connected, and that every edge is in a circuit, so that the connected graph is 2-connected.

Proposition 2.1. Let G be a connected graph. Then $\mathcal{M}(G)$ has cogirth at least 2 if and only if G is a 2-connected graph.

Proof. ($\Rightarrow$) Assume that G is not 2-connected, then it contains a bridge e which participates in every spanning tree of G. As the spanning trees of G are the basis sets of $\mathcal{M}(G)$, the edge e is contained in every basis set of $\mathcal{M}(G)$. Thus $\{e\}$ is a cocircuit as it intersects every basis set, and must be minimal as it contains a single element and the empty set cannot be a cocircuit. As $\mathcal{M}(G)$ contains a cocircuit of size 1, it has cogirth 1.

($\Leftarrow$) Assume $\mathcal{M}(G)$ has cogirth 1, then there is a cocircuit $\{e\}$. As cocircuits are the sets which intersect every basis, e is contained in every basis of $\mathcal{M}(G)$. The basis sets of $\mathcal{M}(G)$ are in correspondance with the spanning trees of G, so e is contained in every spanning tree of G. So e is a bridge in G, thus G is not 2-connected.

$\square$

Proposition 2.2. If a regular matroid $\mathcal{M}$ is strongly orientable then it is of cogirth ≥ 2.

Proof. Suppose first that $\mathcal{M}$ has a coloop $\{e\}$. Then e is not part of any circuit: assume that $e \in C$ for some circuit C. Since e is a coloop, e has non-trivial intersection with every basis of $\mathcal{M}$, thus $C \setminus \{e\}$ dependent, therefore C is not minimally dependent: a contradiction. If e is not part of any circuit, then in particular it is not part of a positive circuit.

$\square$

For the remainder of this thesis we assume matroids are regular and of cogirth ≥ 2 unless otherwise stated.

2.1 Positive Circuit Bases

The existance of a positive circuit basis is fundamental in recovering a graph or matroid from its lattice of integer flows. Joshua Greene [Gre11] first proved that a positive cycle basis existed for graphs using an algorithmic construction of a spanning tree, for which the corresponding fundamental cycle basis must be positive. The construction begins with a vertex, then branches out a tree one edge at a time, by selecting vertices which have a unique edge connecting them to the previous one. This path of the spanning tree (or forest) forms one positive direction between any two vertices and the construction of this spanning tree guarantees the extra edge added when finding the fundamental cycle will form the other positive path in the reverse direction. The full statement and proof of this algorithm is included below.

Lemma 2.3 (Lemma 3.2 [Gre11]). *For a 2-connected graph G, there exists a maximal spanning forest F and orientation O for which the fundamental cycle basis with respect to F is positive.*

Proof. A *root set* $R \subseteq V(G)$ in a graph is one which contains one vertex in each connected component. Let R_1 be a root set of $G_1 := G$. Now define $G_{i+1} = G_i \setminus R_i$, that is, the graph obtained by deleting the vertices in R_i and removing the edges which used those vertices. Now define R_{i+1} to be a root set in G_{i+1} with the property that each vertex $v_{i+1} \in R_{i+1}$ has a unique neighbour $v_i \in R_i$, and distinguish a single edge $e = (v_i, v_{i+1})$. Let F be the subgraph of G consisting of all such edges e.

By induction on i, there is no vertex in R_i which participates in a cycle in F, so F is a forest. By reverse induction on i, R_i is a root set for the subgraph of F induced on $V(G_i)$, that is, the subgraph of F given by intersecting the vertex set of F and G_i, and take the edges that remain. So R_i is maximal, so $R_1 = F$ is maximal. Given an edge $e \in E(G)$, write $e = (v_i, v_j)$ for $v_i \in R_i$ and $v_j \in R_j$, and $i < j$ (note that $i \neq j$ as each R_i is an independent set). Then the orientation O is given by orienting each e from v_i to v_j, then reversing each edge in $E(G \setminus F)$. Then every fundamental cycle with respect to F is oriented in the same direction, thus is positive.

$\square$

For an example of how the algorithm works, see Fig. 10, where the root sets are given by $R_1 = \{v_1\}, R_2 = \{v_3\}, R_3 = \{v_2\}, R_4 = \{v_4\}$.

(a) $R_1 = \{v_1\}$

(b) $R_2 = \{v_3\}$

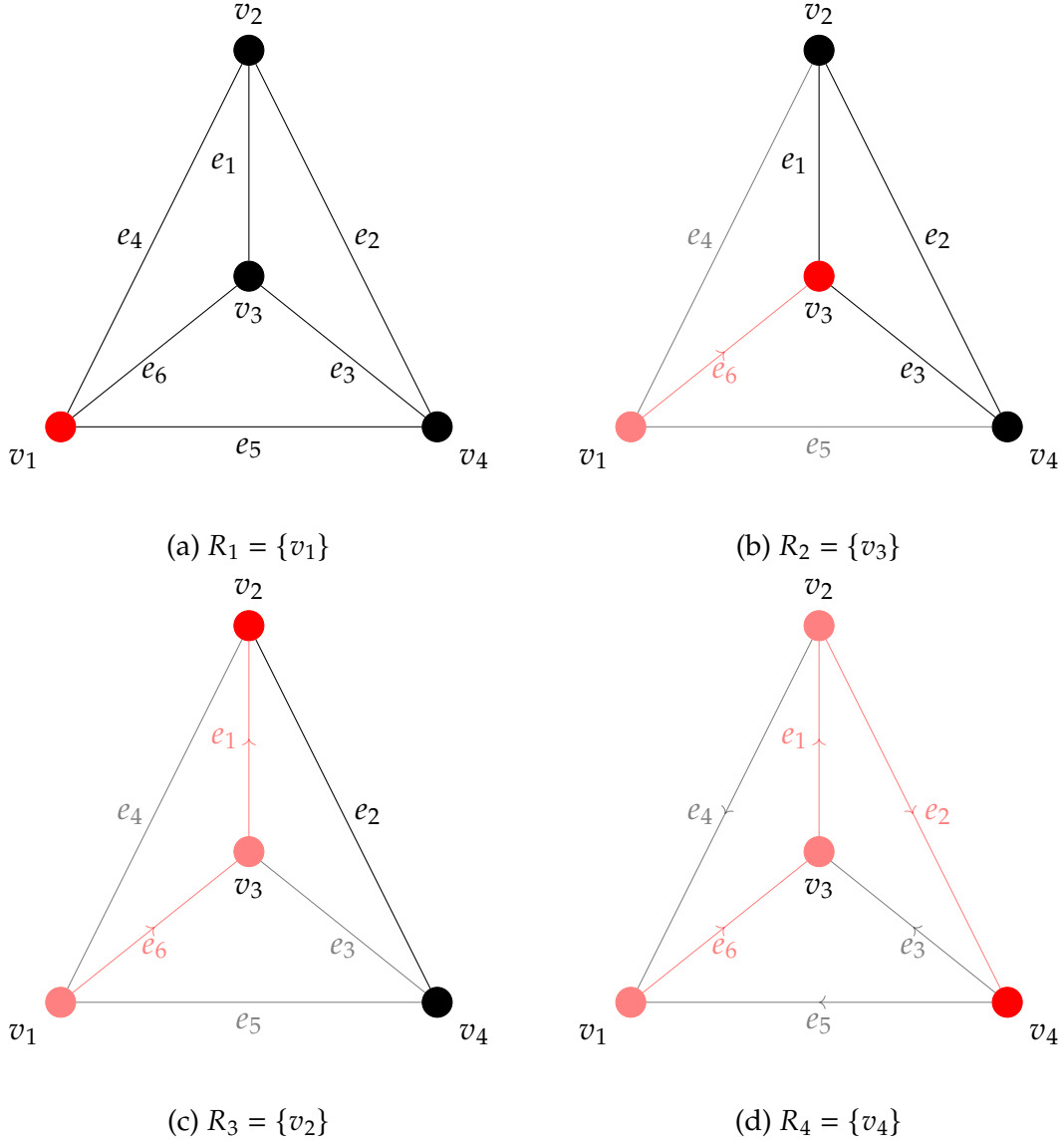(c) $R_3 = \{v_2\}$

(d) $R_4 = \{v_4\}$

Figure 10: Greene's positive circuit basis algorithm applied to K_4.

This gives rise to the spanning forest $\{e_6, e_1, e_2\}$ which are oriented in the order of the root set, i.e. e_6 is oriented from v_1 to v_3 and so on. The remaining edges are oriented backwards, that is, they start at the later vertex in root sets and end at the earlier root set vertex, such that the fundamental cycle is positive. The resulting positive cycle basis is

$$\{\{+e_1, +e_4, +e_6\}, \{+e_1, +e_2, +e_3\}, \{+e_1, +e_2, +e_5, +e_6\}\}.$$

For regular matroids of cogirth ≥ 2, the statement is a bit more complicated to show, we cannot directly recreate Greene's algorithm for matroids as it fundamentally relies on vertices. Whilst cocircuits somewhat do correspond to vertices, they are not always in one to one correspondence for graphs, and so detecting which cocircuits we would want to use is quite challenging, let alone extending this to all regular matroids. In order to prove

25

that a positive circuit basis exists, we appeal to a more classical result of graph theory and its extension to matroid theory.

An orientation of a graph (or matroid) is *acyclic* if there are no positive (or negative) cycles, and is *totally cyclic* if every element participates in a positive (or negative) cycle. A well known result from graph theory is that if an orientation of a planar graph is acyclic, then the dual graph with the induced orientation is totally cyclically oriented, and vice versa. This result natural extends to oriented matroid theory. Without appealing to too much unnecessary oriented matroid theory, we state as a fact that for some oriented matroid $\mathcal{M}^\epsilon$ with orientation ϵ, there exists a unique *dual oriented matroid* $(\mathcal{M}^\epsilon)^*$ such that $(\mathcal{M}^\epsilon)^{**} = \mathcal{M}^\epsilon$. Note that this is just some orientation on the dual matroid $\mathcal{M}^*$. Then the above result for graphs naturally extends as follows.

Proposition 2.4 (Proposition 3.4.8 [Bjö+99])**.** Let $\mathcal{M}^\epsilon$ be an oriented matroid, then $\mathcal{M}^\epsilon$ is acyclic if and only if its oriented dual matroid $(\mathcal{M}^\epsilon)^*$ is totally cyclic.

It turns out that a regular matroid being totally cyclic is equivalent to having a positive circuit basis – indeed one direction is obvious, and the other direction will follow from a later result. So in order to prove that any regular matroid has a positive circuit basis, we want to show that a totally cyclic orientation exists, which is equivalent to showing that $\mathcal{M}^*$ has an acyclic orientation by Proposition Proposition 2.4. Indeedn, the following algorithm shows how to construct an acyclic orientation for any regular matroid.

Lemma 2.5. Let $\mathcal{M}$ be a regular matroid without loops. There exists an orientation ϵ on $\mathcal{M}$ such that $\mathcal{M}^\epsilon$ is acyclic.

Proof. Let $\mathcal{M}$ with $E(\mathcal{M}) = \{e_1, \ldots, e_m\}$ be represented by the matrix M with columns $v_1, \ldots v_n$ in $\mathbb{R}^m$. Then consider the hyperplane arrangement given by these vectors, that is, each vector defines a codimension one plane (called a hyperplane), by considering it as the normal to the plane. The hyperplane corresponding to v_i is given by the surfaces $P_i = \{v \in \mathbb{R}^m \mid v \cdot v_i = 0\}$. The hyperplane arrangement given by these vectors splits $\mathbb{R}^m$ into chambers. Fix some chamber and some vector v in the interior, and define an orientation using the Euclidean inner product $\langle \cdot, \cdot \rangle$ of $\mathbb{R}^m$ as follows:

$$\epsilon_i = \epsilon_{e_i} := \begin{cases} +1 & \text{if } \langle v_i, v \rangle > 0 \\ -1 & \text{if } \langle v_i, v \rangle < 0. \end{cases}$$

We claim that $\mathcal{M}^\epsilon$ is acyclic. Assume there is a positive dependence $\sum_{i=1}^{n} a_i(\epsilon_i v_i) = 0$, where $a_i \geq 0$. Taking the inner product with v gives

$$\left\langle \sum_{i=1}^{n} a_i(\epsilon_i v_i), v \right\rangle = \sum_{i=1}^{n} a_i \langle (\epsilon_i v_i), v \rangle = 0.$$

However, by definition $\langle \epsilon_i v_i, v \rangle = \pm \langle v_i, v \rangle > 0$ for all $i = 1, \ldots, n$, as the inner product is only 0 if v lies in the hyperplane P_i corresponding to v_i, but we have assumed v is interior of a chamber, thus does not lie on any hyperplane. So this is a contradiction and thus $\mathcal{M}^\epsilon$ is acyclic.

$\square$

Finally, Karl Heuer, Raphael Steiner and Sebastian Wiederrecht [HSW22] showed that if a matroid is totally cyclic, then there exists a positive circuit basis.

Lemma 2.6 (Lemma 3.8 [HSW22])**.** Let $\mathcal{M}^\epsilon$ be an oriented regular matroid. If $\mathcal{M}^\epsilon$ is totally cyclic, then the underlying matroid $\mathcal{M}$ admits a positive circuit basis.

Note that in literature, the desired circuit bases are called *directed circuit basis*, which is almost the same as a positive circuit basis except we allow for a circuit basis whose circuits are either positive or negative. However by the circuit axioms, we can easily interchange between a directed circuit basis and a positive circuit basis by reversing the orientation of all negative circuits.

We are now ready to show that for any regular matroid of cogirth ≥ 2 there exists a positive circuit basis.

Proposition 2.7. Let $\mathcal{M}$ be a regular matroid with cogirth ≥ 2. Then $\mathcal{M}$ admits a positive circuit basis.

Proof. First consider the regular matroid $\mathcal{M}^*$ given by the unoriented dual of $\mathcal{M}$. By Lemma 2.5 there exists an orientation ϵ on $\mathcal{M}^*$ for which the oriented matroid $(\mathcal{M}^*)^\epsilon$ is acyclic, as by definition of $\mathcal{M}$ having cogirth ≥ 2, its dual $\mathcal{M}^*$ has no loops. Taking the oriented dual of this matroid $((\mathcal{M}^*)^\epsilon)^*$ results in an oriented matroid that is totally cyclic by Proposition 2.4. This matroid is some oriented matroid whose underlying matroid is $\mathcal{M}$, whose orientation is totally cyclic, so by Lemma 2.6, $\mathcal{M}$ admits a positive circuit basis.
□

Note that this implies that a positive circuit basis exists if and only if a totally cyclic orientation exists, the first implication is clear and we have just shown the converse. Furthermore, the existence of a totally cyclic orientation implies that any regular matroid with cogirth ≥ 2 can be strongly oriented – as a totally cyclic orientation is a strongly connected orientation. Combining this with the reverse implication we mentioned in the previous section, a regular matroid can be strongly oriented if and only if it has cogirth ≥ 2.

2.2 Matroid Operations

As one final abstraction from graphs to matroids, we will define some operations on matroids which naturally arise from graph theory. The first two operations are called restriction/deletion and contraction, and classify a class of submatroids called minors. The study of minors in matroid theory is incredibly useful as, by studying these smaller submatroids, you can often learn information about your original matroid such as whether it is regular or not. The deletion operation is defined as follows.

Definition 2.8. Let $\mathcal{M} = (E, C)$ be a matroid and let $X \subseteq E$. Then the the *deletion of $E \setminus X$ from $\mathcal{M}$* is the matroid denoted by $\mathcal{M} \setminus (E \setminus X)$ or $\mathcal{M}|X$ with base set $E' = X$ and independent sets $\mathcal{I}' = \{I \subseteq X \mid I \in \mathcal{I}(\mathcal{M})\}$.

We will only consider the deletion, rather than the restriction, as it is more intuitive to graph theory, but often in matroid theory literature the restriction is what is defined.

The deletion corresponds to deleting edges from a graph, then remove any isolated vertices that remain as a result of deleting the edges – as matroids do not see vertices anyway. For example, in Fig. 11 we delete edges e_2, e_3, e_5 which leaves v_4 as an isolated vertex, so this is deleted too.

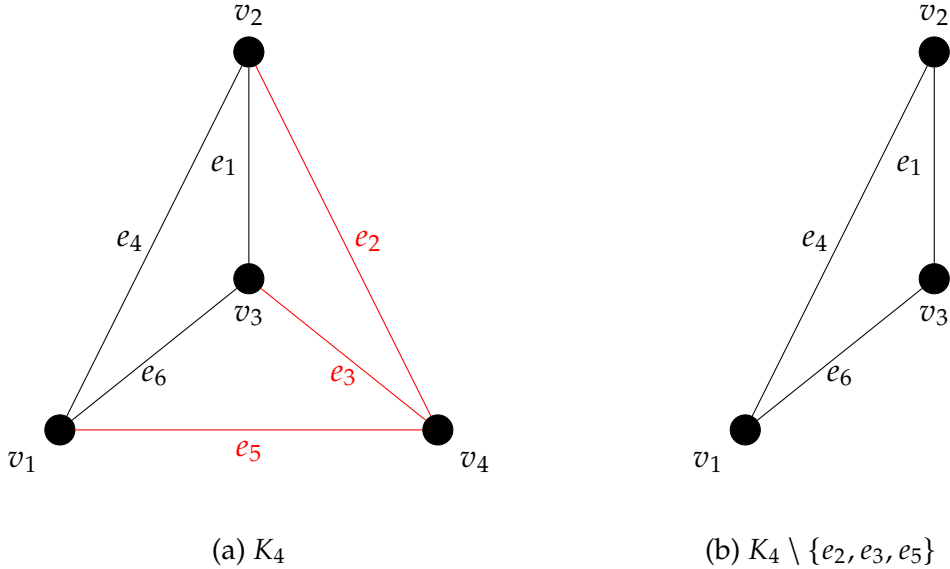(a) K_4 (b) $K_4 \setminus \{e_2, e_3, e_5\}$

Figure 11: Graphical representation of the deletion of $\{e_2, e_3, e_5\}$ from K_4.

One can show this operation coincides with the graph theoretic definition, that is for any subset $\mathcal{M}(G) \setminus T = \mathcal{M}(G \setminus T)$ where the operation is done for matroids and graphs respectively. Given a matroid $\mathcal{M}$, after applying some amount of deletions to arrive at a matroid $\mathcal{N}$, we call the matroid $\mathcal{N}$ a *submatroid* of $\mathcal{M}$.

For some $T \subseteq E$ define the *contraction of T from $\mathcal{M}$* to be $\mathcal{M}/T := (\mathcal{M}^* \setminus T)^*$, that is, contraction is the dual operation to deletion. Again, this corresponds to the graph operation of contracting an edge, i.e. for some edge $e = \{v_i, v_j\}$ we set $v_i = v_j$ and delete any loops that arise, for example the edge e becomes a loop, which is deleted. We will show by example how this operation works for graphs by contracting $\{e_2, e_4\}$ from K_4, using the dual graph we calculated in Fig. 8.
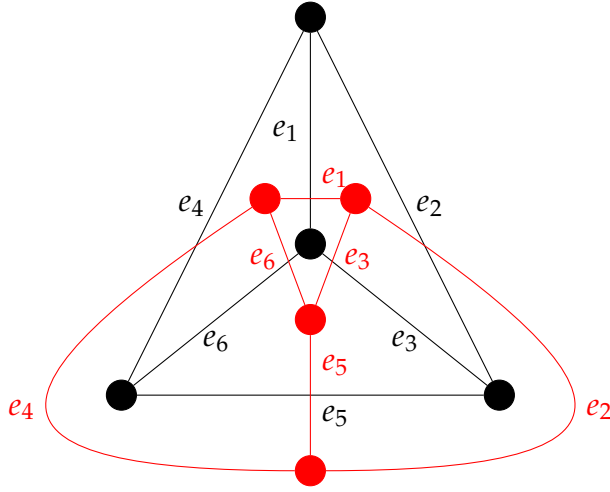
(a) K_4 (black) and dual $(K_4)^*$ (red)
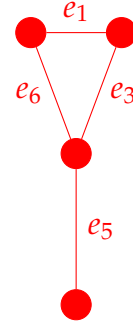
(b) $(K_4)^* \setminus \{e_2, e_4\}$
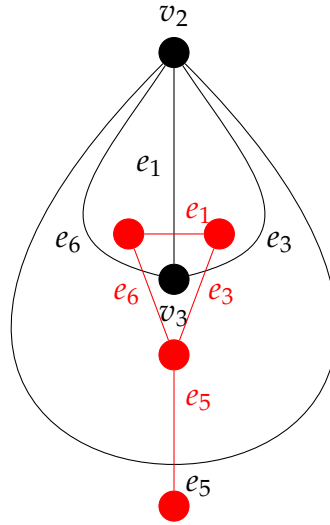
(c) $(K_4)^* \setminus \{e_2, e_4\}$ (red) and dual $((K_4)^* \setminus \{e_2, e_4\})^* = K_4/\{e_2, e_4\}$ (black)

Figure 12: Graphical representation of the contraction of $\{e_2, e_4\}$ from K_4

Fig. 12 demonstrates a graphical example of the contraction of $\{e_2, e_4\}$ from K_4. Looking at the dual graph K_4^* in red and following the definition of the operation, we delete the edges e_2 and e_4 from the dual graph to get $K_4^* \setminus \{e_2, e_4\}$ in Fig. 12(b), then finding the dual of that results in the final graph at in black in Fig. 12(c), $(K_4^* \setminus \{e_2, e_4\})^*$. This graph is precisely what is achieved by contracting e_2 and e_4 in K_4, the vertices v_1 and v_4 get associated to v_2, which turns e_5 into a loop, and the edges e_1, e_3, e_6 are the edges between the two remaining

29

vertices. Note here we included vertex labels to better illustrate the operation by showing the final graph to be the same as the contraction, but we do not necessarily have this information.

Again, one can show this definition coincides for graphical matroids, i.e. $\mathcal{M}(G)/T = \mathcal{M}(G/T)$, see for example Proposition 3.2.1 of [Oxl06]. Any matroid which can be achieved after a sequence of deletions and contractions is called a *minor* – so in particular any submatroid is a minor, but not all minors are submatroids.

As the study of matroid minors is so important, the independent and dependent sets of deletions and contractions have been heavily studied and can be explicitly written. For a matroid $\mathcal{M}$ with base set E and a subset $T \subseteq E$, the independent sets, bases, circuits and cocircuits of the deletion and contraction with respect to T are derived in Chapter 3 of [Oxl06] and are as follows.

- $\mathcal{I}(\mathcal{M} \setminus T) = \{I \subseteq E \setminus T \mid I \in \mathcal{I}(\mathcal{M})\}$;

- $\mathcal{B}(\mathcal{M} \setminus T)$ is the set of maximal members of $\{B \setminus T \mid B \in \mathcal{B}(\mathcal{M})\}$;

- $C(\mathcal{M} \setminus T) = \{C \subseteq E \setminus T \mid C \in C(\mathcal{M})\}$;

- $C^*(\mathcal{M} \setminus T)$ is the set of minimal non-empty members of $\{C^* \setminus T \mid C^* \in C^*(\mathcal{M})\}$;

- Let B_T be a basis of $\mathcal{M}|T = \mathcal{M} \setminus (E \setminus T)$, then

$$\begin{aligned} \mathcal{I}(\mathcal{M}/T) &= \{I \subseteq E \setminus T \mid I \cup B_T \in \mathcal{I}(\mathcal{M})\} \\ &= \{I \subseteq E \setminus T \mid \mathcal{M}|T \text{ has a basis } B \text{ such that } B \cup I \in \mathcal{I}(\mathcal{M})\}; \end{aligned}$$

- Let B_T be a basis of $\mathcal{M}|T = \mathcal{M} \setminus (E \setminus T)$, then

$$\begin{aligned} \mathcal{B}(\mathcal{M}/T) &= \{B' \subseteq E \setminus T \mid B' \cup B_T \in \mathcal{B}(\mathcal{M})\} \\ &= \{B' \subseteq E \setminus T \mid \mathcal{M}|T \text{ has a basis } B \text{ such that } B' \cup B \in \mathcal{B}(\mathcal{M})\}; \end{aligned}$$

- $C(\mathcal{M}/T)$ is the set of minimal non-empty members of $\{C \setminus T \mid C \in C(\mathcal{M})\}$;

- $C^*(\mathcal{M}/T) = \{C^* \subseteq E \setminus T \mid C^* \in C^*(\mathcal{M})\}$.

Note that when we say maximal or minimal members of the set, we mean with respect to inclusion, i.e. if for some B, B' we have $B \setminus T \subseteq B' \setminus T$, then $B' \setminus T$ is a basis in $\mathcal{M} \setminus T$, but $B \setminus T$ is not. Further note that the circuits of the deletion are the cocircuits of the contraction, and vice versa, as they are dual operations.

Chapter 3

Lattices

Lattices are abstract algebraic objects which, in general, are a set with two bilinear operations satisfying a list of rules. For our purposes we need not consider the most abstract definition, and instead consider a more general form of integral lattices.

A *lattice* is a finitely-generated, free abelian group G together with an inner product $\langle \cdot, \cdot \rangle : G \times G \to \mathbb{Q}$. We further call a lattice an *integral lattice* if the inner product is integer valued. A lattice is a set of regular points with some repeating grid-like structure, similar to the standard integer valued grid points on $\mathbb{R}^2$. The idea of the definition of lattices above is that our group generators act as axis labels, and the inner product gives some notion of distance, i.e. it tells us how far each lattice point is away from the origin. Lattices are very similar to vector spaces, except that lattices have integer coefficients, whilst vector spaces need not. Intuitively, an integral lattice over the group G on n generators is just $\mathbb{Z}^n$, but with some coordinate translation/transformation, and we can generally think about them as a subspace of $\mathbb{R}^n$. We call a mapping $\varphi : L_1 \to L_2$ between lattices an *isomorphism* or *isometry* if it is bijective and preserves the inner product, that is $\langle x, y \rangle_{L_1} = \langle \varphi(x), \varphi(y) \rangle_{L_2}$ for all $x, y \in L_1$. We then say that L_1 and L_2 are *isomorphic* or *isometric* and we write $L_1 \cong L_2$.

3.1 The Lattice of Integer Flows

The key example of a lattice that we will consider is the lattice of integer flows of a graph (and subsequently a regular matroid), originally introduced in 1997 by Bacher, de la Harper and Nagnibeda [BLN97]. The lattice of integer flows naturally arises in the setting of homology when considering a graph as a CW-complex, then the first homology group, also called the *cycle space*, with integer coefficient and equipped with the Euclidean inner product. In general, we need not consider such a general definition, as this space is precisely that which is generated by cycles in the graph, thus lattice points are given by combinations of cycles in the graph. In this sense, the cycle/circuit bases we defined previously are precisely the basis for the lattice of integer flows.

But we have another way of defining it which gives better intuition in the abstraction to matroids. Recall that for any graph $G = (E, V)$ we can find the signed incidence matrix associated with G. Consider $\mathbb{R}^E$ and $\mathbb{R}^V$ to be the real vector spaces with standard bases given by E and V, i.e. linear combinations of edges and vertices with real coefficients. Then M acts as the linear transformation $M : \mathbb{R}^E \to \mathbb{R}^V$ by $(v_i, v_j) = e \mapsto v_j - v_i$.

Then we can formally define the *vector space of real valued flows* or *cycle space* of a graph G with signed incidence matrix M to be given by $\Lambda(G) := \ker(M)$. This precisely consists

of all linear combinations of cycles in G with real coefficients. Looking at the kernel of this linear transformation tells us which sets of edges map to 0, that is, start and end at the same vertex. To transform this into a lattice, we equip it with the most natural inner product, the Euclidean inner product, and we restrict this to an integral lattice by enforcing that it has integer coefficients.

Definition 3.1. The *lattice of integer flows* of a graph $G = (E, V)$ with signed incidence matrix M is given by $\mathcal{F}(G) := \ker(M) \cap \mathbb{Z}^E$ equipped with the Euclidean inner product $\langle \cdot, \cdot \rangle : \mathcal{F}(G) \times \mathcal{F}(G) \to \mathbb{Z}$ which acts by

$$\langle e, f \rangle = \begin{cases} 1 & \text{if } e = f \\ 0 & \text{if } e \neq f \end{cases}$$

for any $e, f \in \mathbb{Z}^E$.

We can think of the lattice of integer flows as a copy of $\mathbb{Z}^n$ which sits inside the subspace $\mathbb{R}^n$, corresponding to the cycle space. Notice that the lattice of integer flows does not see bridges/coloops, and our goal is to recover the matroid from its lattice of integer flows, so we cannot expect to do this for matroids that have cogirth equal to 1. Hence why we mainly only consider matroids of cogirth ≥ 2, unless otherwise specified.

Now note that the definition above did not depend on G being a graph, we defined it only in terms of the matrix M. This motivates a natural abstraction to regular matroids. The *lattice of integer flows* of a regular matroid $\mathcal{M} = (E, C)$ with representing matrix M is given by $\mathcal{F}(\mathcal{M}) := \ker(M) \cap \mathbb{Z}^E$ equipped with the Euclidean inner product $\langle \cdot, \cdot \rangle : \mathcal{F}(\mathcal{M}) \times \mathcal{F}(\mathcal{M}) \to \mathbb{Z}$ which acts by

$$\langle e, f \rangle = \begin{cases} 1 & \text{if } e = f \\ 0 & \text{if } e \neq f \end{cases}$$

for any $e, f \in \mathbb{Z}^E$. Notice the definition is near identical to that of graphs, and in fact for graphical matroids the lattice of integer flows for the graph and its corresponding graphical matroid are isometric (i.e. identical up to relabelling of edges). As with graphs, this lattice is spanned by all circuits of the matroid, and a circuit basis is a basis for the lattice of integer flows. The *rank* of $\mathcal{F}(\mathcal{M})$ or $\mathcal{F}(G)$ is given by the number of elements in the basis, and for graphs this coincides with the genus of the graph, so we define the *genus of* $\mathcal{M}$ to be the rank of $\mathcal{F}(\mathcal{M})$. From here on we will only state results for the lattice of integer flows of a regular matroid, as these all apply for graphs, unless otherwise specified.

Furthermore, the isomorphism/isometry class of the lattice of integer flows is independent of the orientation. Reversing the orientation of an edge e reflects the lattice with respect to the hyperplane orthogonal to the e-axis.

Example 3.2. Let us calculate an example of the lattice of integer flows, using our orientation on K_4 from Fig. 2. It has signed incidence matrix given by

$$M = \begin{bmatrix} 0 & 0 & 0 & -1 & 1 & -1 \\ 1 & -1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 & -1 & 0 \end{bmatrix}$$

which in reduced row echelon form is

$$\begin{bmatrix} 1 & 0 & -1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The solution for $M\mathbf{x} = 0$ is then given by

$$\begin{bmatrix} t + u \\ s + t \\ t \\ s - u \\ s \\ u \end{bmatrix}$$

and so a basis for the kernel is

$$\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 1 \end{bmatrix} \right\}$$

which describes the circuit basis given by

$$B = \{\{+e_1, +e_2, +e_3\}, \{+e_2, +e_4, +e_5\}, \{+e_1, -e_4, +e_6\}\}.$$

This is almost a positive circuit basis, the last circuit is the only issue here. If we however add the last two basis elements we get $\{+e_1, +e_2, +e_5, +e_6\}$ which is a positive circuit, so exchanging this with the final basis element gives a new basis

$$B' = \{\{+e_1, +e_2, +e_3\}, \{+e_2, +e_4, +e_5\}, \{+e_1, +e_2, +e_5, +e_6\}\}$$

which is a positive circuit basis. In fact, using the spanning tree in Fig. 5 under the orientation in Fig. 2, the positive circuit basis B' is the fundamental circuit basis of $\mathcal{M}(K_4)$ (with fixed orientation) coordinatised by that basis set $\{e_1, e_2, e_5\}$.

The *Gram matrix* of a set of vectors $\{v_i \mid 1 \leq i \leq n\}$ has entries given by $g_{ij} = \langle v_i, v_j \rangle$. Note by symmetry of the inner product, the Gram matrix is symmetric. The Gram matrix plays an important role in independence, computing it for a basis of an inner product space allows you to describe the inner product for the whole space entirely, by bilinearity. For Example 3.2 the inner products of basis vectors in B' are

$$\langle v_1, v_1 \rangle = 3$$
$$\langle v_1, v_2 \rangle = 1$$
$$\langle v_1, v_3 \rangle = 2$$
$$\langle v_2, v_2 \rangle = 3$$
$$\langle v_2, v_3 \rangle = 2$$
$$\langle v_3, v_3 \rangle = 4$$

and so the Gram matrix is

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \\ 2 & 2 & 4 \end{pmatrix}.$$

3.2 Voronoi Cells

The main result of this thesis is the ability to reconstruct a regular matroid from its lattice of integer flows. Given a lattice of integer flows, we have no knowledge of the original matroid, so the first step is to somehow identify which elements in the lattice are circuits, rather than linear combinations of circuits. In particular we want to detect a circuit basis for the lattice as we can then transform back to a circuit basis for the matroid (and recover the matroid). The key to doing this is through an object called the Voronoi cell, and a theorem by Bacher, de la Harper and Nagnibeda [BLN97].

Definition 3.3. The *Voronoi cell* of a point $\lambda \in \Lambda(\mathcal{M})$ in the cycle space of a matroid $\mathcal{M}$ is given by

$$\mathcal{V}_\lambda = \{x \in \mathcal{F}(\mathcal{M}) \mid \|x - \lambda\| \le \|x - \mu\|, \forall \mu \in \Lambda(\mathcal{M}) \setminus \{0\}\}$$

where the norm is induced by the inner product $\|x\| := \sqrt{\langle x, x \rangle}$.

The Voronoi cell of λ is the set of all lattice points in $\mathcal{F}(\mathcal{M}) \otimes \mathbb{R}$ which are the closest to λ out of all points in $\Lambda(\mathcal{M})$. The Voronoi cell of a point tessellate the entire lattice, and thus are invariant under translations by lattice vectors. So for convenience, we need only consider the Voronoi cell of the origin,

$$\mathcal{V}(\mathcal{F}(\mathcal{M})) := \{x \in \mathcal{F}(\mathcal{M}) \mid \|x\| \le \|x - \mu\|, \forall \mu \in \Lambda(\mathcal{M}) \setminus \{0\}\}$$

for any lattice $\mathcal{F}(\mathcal{M})$. The Voronoi cell is a polytope, whose codimension one faces (that is faces who are one dimension smaller than the cell itself) are supported by the perpendicular bisector hyperplanes of some vectors in the lattice. The following theorem shows that more can be said about these faces. For graphs, this is a classical theorem of Bacher, de la Harpe, and Nagnibeda [BLN97], and the argument is not substantially different for regular matroids, the proof follows from Dancso and Lim [DL23].

Proposition 3.4 (Proposition 6, [BLN97] and Lemma 4.12, [DL23])**.** The following are equivalent:

- The lattice vector $v \in \mathcal{F}(\mathcal{M})$ is a circuit element.

- The perpendicular bisector of v, that is, the hyperplane given by $\langle x, v \rangle = \frac{\langle v,v \rangle}{2}$, supports a codimension one face of the Voronoi cell.

- The vector v is a *strict Voronoi vector*, that is, $\pm v$ are the two unique shortest elements of the coset $v + 2\mathcal{F}(\mathcal{M})$.

Example 3.5. Consider the graph and its Voronoi cell in Fig. 13.
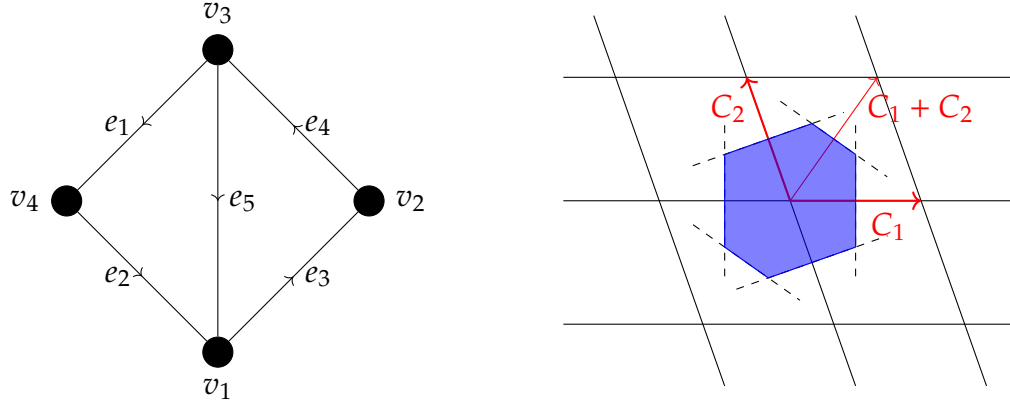

Figure 13: A graph G and the Voronoi cell of its lattice of integer flows.

To obtain the Voronoi cell, we first note that the graph has a circuit basis given by $C_1 = \{+e_1, +e_2, -e_5\}$ and $C_2 = \{+e_3, +e_4, +e_5\}$. We then can calculate the Gram matrix, i.e. the inner products

$$\langle C_1, C_1 \rangle = 3$$
$$\langle C_2, C_2 \rangle = 3$$
$$\langle C_1, C_2 \rangle = -1.$$

Then the lattice of integer flows can be represented isometrically by mapping C_1 to the vector from $[\sqrt{3}, 0]$. Then to find $C_2 = [a, b]$ we have that

$$\langle C_1, C_2 \rangle = -1 \Rightarrow \sqrt{3}a = -1 \Rightarrow a = -\frac{1}{\sqrt{3}}$$

and

$$\langle C_2, C_2 \rangle = 3 \Rightarrow a^2 + b^2 = 3 \Rightarrow b^2 = \frac{8}{3} \Rightarrow b = \frac{2\sqrt{2}}{\sqrt{3}}$$

Consider the 'faces' of the Voronoi cell by dimension, we have 0 dimensional faces called *vertices*, then 1-dimensional faces between vertices called *edges*, so on, until the n-dimensional faces, which connect codimension one faces. This extends to an inclusion on all faces of the Voronoi cell, we define the inclusion to be if an n-dimensional face contains

an m-dimensional face, for $m \leq n$. So, for example, an edge e between vertices v_i, v_j would give the partial ordering $v_i, v_j \leq e$. This a partial ordering on the set of all faces, of all dimensions, of a polygon, so we can consider the set of all faces as a partially ordered set (poset). In particular, for any such Voronoi cell of a lattice $\mathcal{F}(M)$ we can create a partially ordered set (poset) structure on the set of faces of $\mathcal{V}(\mathcal{F}(M))$.

Definition 3.6. The *poset of faces* of the Voronoi cell $\mathcal{V}(\mathcal{F}(M))$ is the pair $(F, \leq)$ of faces F of the cell ordered by inclusion $\leq$, denoted $\mathcal{FP}(\mathcal{F}(M))$. Further, the poset of faces is *graded* by dimension, i.e. faces of the same dimension are not comparable, and if two faces are comparable then the higher dimensional one contains the lower dimensional one.

Recall that for the poset of strongly connected orientations $\mathcal{SC}(M)$ in Definition 1.11, the circuit elements were precisely the minimal cogirth ≥ 2 submatroids, and for each there exists two strongly connected orientations, one where the circuit is positive and one where it is negative. Now Proposition 3.4 tells us that the vectors corresponding to circuits are in correspondance to codimension one faces of the Voronoi cell. Furthermore, the opposite faces correspond to the circuits positive and negative vector. So from Proposition 3.4 we find that the minimal elements in $\mathcal{SC}(M)$ are in bijection with the maximal elements of $\mathcal{FP}(\mathcal{F}(M))$. But can we say anything about the other elements, how do we know how many elements participate in these circuits, and which elements participate in which circuits. Well in fact a lot more is true about the correspondence between these posets and answers these questions. Oded Amini originally proved that the posets were isomorphic as graded posets for graphs in 2010 [Ami10], then in 2022 Zsuzsanna Dancso and Jongmin Lim [DL23] proved that this result generalised to regular matroids.

Theorem 3.7 (Theorem 3.13 [DL23]). *For a finite regular matroid M, $\mathcal{FP}(\mathcal{F}(M)) \cong \mathcal{SC}(M)$ as graded posets.*

Remark 3.8. Note that to be isomorphic as graded posets, this means that the maximal elements $(\emptyset, \emptyset)$ – denoting the empty orientation on the empty set – of $\mathcal{SC}(M)$, and $\mathcal{V}(\mathcal{F}(M))$ – denoting the entire Voronoi cell – of $\mathcal{FP}(\mathcal{F}(M))$ are in correspondence. Then this correspondence continues at each genus, i.e. each level of the poset, so the strongly connected orientations in $\mathcal{SC}(M)$, given by submatroids formed from a single circuit in M, correspond to hyperplanes in $\mathcal{FP}(\mathcal{F}(M))$.

Example 3.9. Let us explicitly calculate the posets for the Voronoi cell and graph in Fig. 13. In this case the strongly orientable submatroids are the strongly orientable subgraphs. Recall that a subgraph is strongly orientable if and only if its connected components are 2-connected – as any submatroid is strongly orientable if and only if it has cogirth ≥ 2, which corresponds to connectedness in graphs. The maximal element in $\mathcal{SC}(M)$ is the empty matroid with empty orientation, $(\emptyset, \emptyset)$. Contained in the maximal element are the circuits and their strong orientations. The circuits in G are $C_1 = \{e_1, e_2, e_5\}, C_2 = \{e_3, e_4, e_5\}$ and $C_3 = \{e_1, e_2, e_3, e_4\}$, so the maximal submatroids are formally $\mathcal{M}_i$ with $E(\mathcal{M}_i) = C_i$ and $C(\mathcal{M}_i) = \{C_i\}$ for $i = 1, 2, 3$. For each $\mathcal{M}_i$ there exists exactly two strong orientations, one where every element is positive ϵ_i^+ and the other where each element is negative ϵ_i^-. Formally, we will declare that the 'positive' orientations are those where e_1, e_2, e_3, e_4 agree with the orientation in Fig. 13, this then uniquely determines our choice of

positive and negative orientations for these circuits. So we have six submaximal elements $(\mathcal{M}_i, \epsilon_i^+), (\mathcal{M}_i, \epsilon_i^-) \leq (\emptyset, \emptyset)$ for $i = 1, 2, 3$.

Now, if we add a new single element from G to C_1 or C_2, the resulting graph is not 2-connected, thus is not strongly orientable. Adding the remaining two elements to C_1 or C_2, or adding the remaining element to C_3 results in the entire graph, and so the next strongly orientable submatroid in the poset must be the entire matroid $\mathcal{M}(G)$. Now it suffices to find all strong orientations of $\mathcal{M}(G)$. For a strong orientation on G, e_1 and e_2 must be oriented the same way, as well as e_3 and e_4, as otherwise there will be no way to reach or leave v_4 and v_2 respectively. So there are $2^3 = 8$ possible options, we will call them $UUU, UUD, \ldots, DDD$ where U represents up and D represents down in the order of the edges $\{e_1, e_2\}, \{e_5\}, \{e_3, e_4\}$ in Fig. 13. Note that the orientations UUU and DDD are not strong orientations as there is no way to leave v_3 and v_1 respectively, and for the other six orientations, they are all strong orientations, as you have a path between the only two vertices via an up U and down D when we disregard v_2, v_4. So the six minimal elements in $\mathcal{SC}(\mathcal{M})$ are $(\mathcal{M}(G), \epsilon_X)$ where $X \in \{UUD, UDU, DUU, UDD, DUD, DDU\}$. We now have the three levels of the poset, but we need to finalise the bottom level of inclusion.

- $(\mathcal{M}(G), \epsilon_{UUD})$ does not contain either the positive or negative C_1, but it does contain the negative C_2 and the negative C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{UUD}) \leq (\mathcal{M}_2, \epsilon_2^-), (\mathcal{M}_3, \epsilon_3^-)$.

- $(\mathcal{M}(G), \epsilon_{UDU})$ contains the negative C_1 and the positive C_2, but it does not contain either the positive or negative C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{UDU}) \leq (\mathcal{M}_1, \epsilon_1^-), (\mathcal{M}_2, \epsilon_2^+)$.

- $(\mathcal{M}(G), \epsilon_{DUU})$ contains the positive C_1, it does not contain either the positive or negative C_2, but it does contain the positive C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{DUU}) \leq (\mathcal{M}_1, \epsilon_1^+), (\mathcal{M}_3, \epsilon_3^+)$.

- $(\mathcal{M}(G), \epsilon_{UDD})$ contains the negative C_1, it does not contain either the positive or negative C_2, but it does contain the negative C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{UDD}) \leq (\mathcal{M}_1, \epsilon_1^-), (\mathcal{M}_3, \epsilon_3^-)$.

- $(\mathcal{M}(G), \epsilon_{DUD})$ contains the positive C_1 and the negative C_2, but it does not contain either the positive or negative C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{DUD}) \leq (\mathcal{M}_1, \epsilon_1^+), (\mathcal{M}_2, \epsilon_2^-)$.

- $(\mathcal{M}(G), \epsilon_{DDU})$ does not contain either the positive or negative C_1, but it does contain the positive C_2 and the positive C_3. So we have the partial ordering $(\mathcal{M}(G), \epsilon_{DDU}) \leq (\mathcal{M}_2, \epsilon_2^+), (\mathcal{M}_3, \epsilon_3^+)$.

We now have all the information needed to describe the poset, a visual representation is given in Fig. 14.

Constructing the poset of faces of $\mathcal{V}(\mathcal{F}(\mathcal{M}))$ is quite simple, we declare that the vertices of the Voronoi cell in Fig. 13 are A, B, C, D, E, F going clockwise from the horizontal axis. These are the zero dimensional faces, and the one dimensional faces are the edges which connect these, which we denote FA, AB, BC, CD, DE, EF. Note the face FA is that which
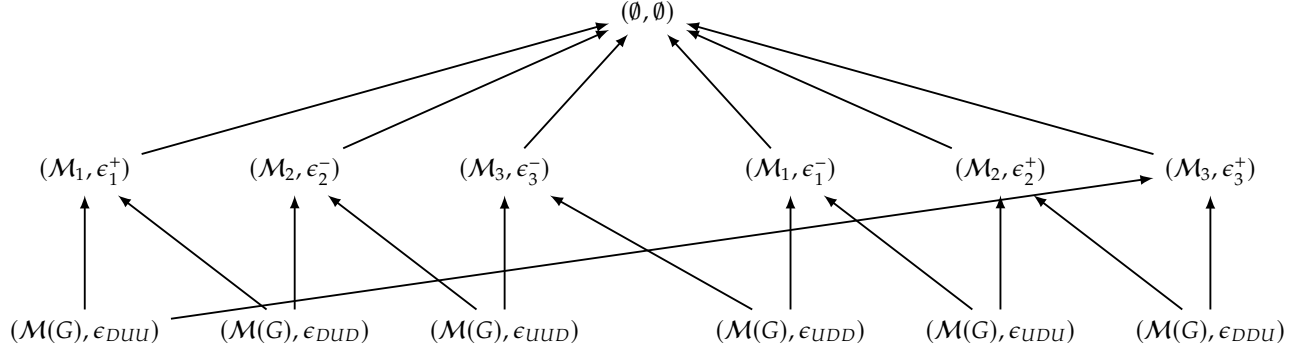
37

Figure 14: The poset of strongly connected orientations of the graphical matroid $\mathcal{M}(G)$ of the graph in Fig. 13.

C_1 passes through, EF is that which $C_1 + C_2$ passes through – which is C_3 – and DE is that which C_2 passes through. Finally, we have the maximal element given by the whole Voronoi cell. The inclusions are then obvious, $FA, AB, BC, CD, DE, EF \leq \mathcal{V}(\mathcal{F}(\mathcal{M}))$ as all one dimensional faces are included in the single two dimensional face. Similarly, the inclusions for vertices are made obvious by the labelling of our edges, i.e. $F, A \leq FA$ and $A, B \leq AB$, etc. This poset can be drawn easily as well, as in Fig. 15.
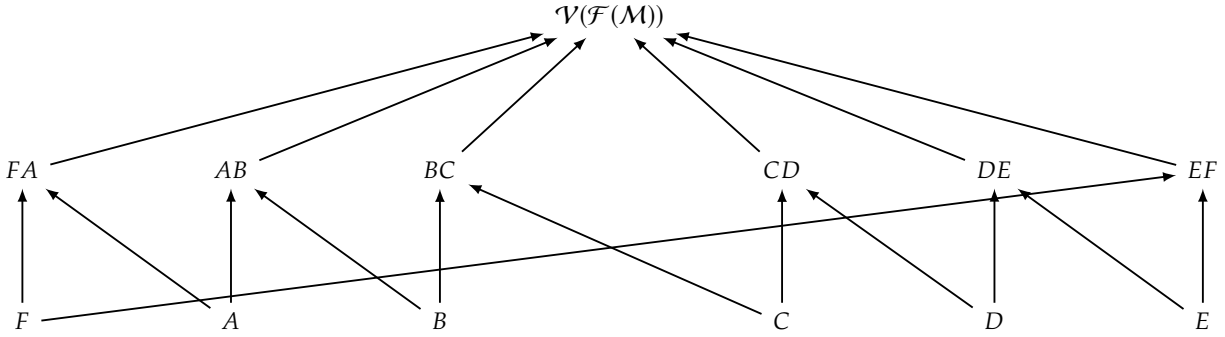

Figure 15: The face poset of the Voronoi cell in Fig. 13.

The correspondence in Theorem 3.7 tells us that these posets are isomorphic as graded posets, in fact, the isomorphism is given precisely as the posets are drawn, so the vertices in Fig. 15 correspond to the orientation on $\mathcal{M}(G)$ in the same position in Fig. 14, same with the codimension one faces (edges) which correspond to a circuit and an orientation. In fact, the way the Voronoi cell in drawn in Fig. 13, with the red vectors representing the positive circuits, shows the correspondance between C_1, C_3 and C_2 under a positive orientation and the faces FA, DE and EF respectively.

3.3 Strong Torelli Theorem

The *discrete Torelli theorems* are a set of theorems which are discrete versions of the famous Torelli theorem in algebraic geometry. They all state that the lattice of integer flows (or some variant thereof) determines a discrete structure up to an appropriate notion of isomorphism. Watkins first showed this for graphs up to 2-isomorphism in the context of graph Laplacians [Wat90] [Wat94]. Caporaso and Viviani established the result for graphs and tropical curves in terms of the Albanese Torus [CV09]. Around the same time Su and Wagner proved the regular matroid version of the theorem: two regular matroids without coloops are isomorphic as matroids if and only if their lattices of integer flows are isomorphic as lattices [SW10]. The goal of this thesis is to prove a constructive version of this theorem: rather than merely knowing that the lattice of integer flows uniquely determines the isomorphism class of a regular matroid without coloops, we explicitly reconstruct it.

In this section we begin by proving a strong version of discrete Torelli theorem for matroids, namely, that the isomorphism of the lattices of integer flows lifts to an isomorphism of the Euclidean lattices spanned by the base sets, which in turn descends to a matroid isomorphism. The proof is inspired by Greene's results in [Gre11], where he proves a different strengthening of the Torelli Theorem for graphs in service of applications in knot theory.

The main technical tool we use is *Greene's rigid embedding theorem* [Gre11, Prop 2.8] for lattices. In order to understand the statement of this theorem, we require some lattice theoretic notions: these are briefly introduced here; the surrounding theory is outside the scope of this thesis.

For an integral lattice Λ, the inner product $\langle \cdot, \cdot \rangle : \Lambda \times \Lambda \to \mathbb{Z}$ extends to a $\mathbb{Q}$-valued inner product on $\Lambda \otimes \mathbb{Q}$. We define the *dual lattice* as

$$\Lambda^* := \{ x \in \Lambda \otimes \mathbb{Q} \mid \langle x, \lambda \rangle \in \mathbb{Z}, \forall \lambda \in \Lambda \},$$

which in particular contains Λ. For a sublattice $\Gamma \subseteq \Lambda$ there is a natural restriction map $r : \Lambda^* \to \Gamma^*$ induced by the inclusion map $\iota : \Gamma \to \Lambda$. If this restriction map surjects, we call the sublattice Γ *primitive*.

Considering Λ^* as an abelian group, $\Lambda^*/2\Lambda^*$ forms a quotient group. Equipping this with the inner product induced by that on Λ^* forms a *quotient lattice*. Within the quotient lattice $\Lambda^*/2\Lambda^*$ there exists a distinguished coset

$$\mathrm{Char}(\Lambda) = \{ \chi \in \Lambda^* \mid \langle \chi, \lambda \rangle \equiv |\lambda| \pmod 2, \forall \lambda \in \Lambda \},$$

whose inner product with any element $\lambda \in \Lambda$ is the same parity as its norm $\langle \lambda, \lambda \rangle$. We call this coset the *characteristic covectors* of Λ. For any characteristic covector $\chi \in \mathrm{Char}(\Lambda)$ and any $\mu, \lambda \in \Lambda$

$$\langle \chi + 2\mu, \lambda \rangle = \langle \chi, \lambda \rangle + 2 \langle \mu, \lambda \rangle \equiv \langle \chi, \lambda \rangle \equiv |\lambda| \pmod 2.$$

In other words, adding multiples of 2μ for some $\mu \in \Lambda$ to a characteristic covector returns a characteristic covector. Thus, consider the equivalence classes of elements of $\mathrm{Char}(\Lambda)$ modulo 2Λ, to define

$$\chi(\Lambda) := \text{Char}(\Lambda) \pmod{2\Lambda},$$

and for $\chi \in \text{Char}(\Lambda)$ denote the equivalence class χ in $\chi(\Lambda)$ by $[\chi]$. Finally, the *short characteristic covectors* are the elements of minimal norm (self-pairing) in these equivalence classes:

$$\text{Short}(\Lambda) := \{\chi \in \text{Char}(\Lambda) \mid |\chi| \le |\chi'|, \forall \chi' \in [\chi]\}.$$

Example 3.10. Equipping the abelian group $\mathbb{Z}^n$ with the Euclidean inner product makes it an integral lattice, called the *standard Euclidean lattice*. It has short characteristic covectors given by

$$\text{Short}(\mathbb{Z}^n) = \{\chi \mid \langle \chi, e_i \rangle = \pm 1, \forall i = 1, \dots, n\}$$

where $\{e_1, \dots, e_n\}$ is the standard orthonormal basis of $\mathbb{Z}^n$. In particular, for the standard Euclidean lattice $\mathbb{Z}^{E(\mathcal{M})}$ indexed by $E(\mathcal{M})$, the short vectors are those of the form

$$\sum_{e \in E(\mathcal{M})} \varepsilon_e e$$

where $\varepsilon_e = \pm 1$.

With this in mind, we state Greene's rigid embedding theorem:

Theorem 3.11 (Proposition 2.8 [Gre11])**.** *Let Λ denote a lattice, B_Λ a basis for Λ, Z_i a lattice with orthonormal basis B_i, and $\iota_i : \Lambda \hookrightarrow Z_i$ an embedding, $i = 1, 2$. Suppose that ι_1 has the property that*

$$\langle \iota_1(x), e \rangle \in \{0, 1\}, \quad \forall x \in B_\Lambda, e \in B_1, \tag{3.1}$$

and

$$\forall e \in B_1, \exists x \in B_\Lambda \quad s.t. \quad \langle \iota_i(x), e \rangle \ne 0; \tag{3.2}$$

and suppose that both restriction maps $Z_i^* \to \Lambda^*$ induce surjections

$$r_i : \text{Short}(Z_i) \to \text{Short}(\Lambda).$$

Then there exists an embedding $\iota : Z_1 \hookrightarrow Z_2$ such that $\iota_2 = \iota \circ \iota_1$.

Note that in the simple case where Λ is a sublattice of Z_i, we can use the *canonical embedding* $\iota_{can} : \Lambda \hookrightarrow Z_i$, that is, the map which is the identity on all of Λ. This is the case for $\mathcal{F}(\mathcal{M})$, which is naturally a sublattice of $\mathbb{Z}^{E(\mathcal{M})}$, so there is a canonical embedding $\iota_{can} : \mathcal{F}(\mathcal{M}) \hookrightarrow \mathbb{Z}^{E(\mathcal{M})}$. Recalling that we want to lift an automorphism $f : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{M})$, we consider the case

- $\Lambda := \mathcal{F}(\mathcal{M})$,

- $B_\Lambda := B_{\mathcal{F}(\mathcal{M})}$, that is a circuit basis of $\mathcal{F}(\mathcal{M})$,

- $Z_1 = Z_2 := \mathbb{Z}^{E(\mathcal{M})}$,

- $B_1 = B_2 := B$ the standard basis of $\mathbb{Z}^{E(\mathcal{M})}$ (that is $B = \{e \mid e \in E(\mathcal{M})\}$),

- $\iota_1 := \iota_{can} : \mathcal{F}(\mathcal{M}) \hookrightarrow \mathbb{Z}^{E(\mathcal{M})}$,

- $\iota_2 := \iota_{can} \circ f : \mathcal{F}(\mathcal{M}) \hookrightarrow \mathbb{Z}^{E(\mathcal{M})}$.

Then if Theorem 3.11 holds, we will have some embedding $F : \mathbb{Z}^{E(\mathcal{M})} \hookrightarrow \mathbb{Z}^{E(\mathcal{M})}$ such that $\iota_{can} \circ f = F \circ \iota_{can}$, which is to say that there exists a lift of f, as the following diagram commutes:

$$
\begin{array}{ccc}
\mathbb{Z}^{E(\mathcal{M})} & \xrightarrow{\;\;F\;\;} & \mathbb{Z}^{E(\mathcal{M})} \\
\Big\uparrow{\scriptstyle \iota_{can}} & & \Big\uparrow{\scriptstyle \iota_{can}} \\
\mathcal{F}(G) & \xrightarrow{\;\;f\;\;} & \mathcal{F}(G)
\end{array}
$$

So what precisely do we need to show? In this case Eq. (3.1) states that for each x in the circuit basis of $\mathcal{F}(\mathcal{M})$, the inner product with any element in the standard basis is either 0 or 1. In other words, every $e \in E(\mathcal{M})$ has coefficient 0 or 1 in x, which is precisely the condition that $B_{\mathcal{F}(\mathcal{M})}$ is a positive circuit basis.

Next, Eq. (3.2) states that every $e \in E(\mathcal{M})$ participates in some circuit in the circuit basis: this follows from the fact that $\mathcal{M}$ is of cogirth ≥ 2. The property Eq. (3.2) also requires that each $e \in E(\mathcal{M})$ participates in some circuit in the f-image of $B_{\mathcal{F}(\mathcal{M})}$, which is immediate from the fact that f is an automorphism.

The final condition is a technical condition about the short vector of the lattice of integer flows – similar to saying that the lattice of integer flows is a primitive lattice. Greene proved this for graphs [Gre11, Proposition 2.7] and the proof follows verbatim for matroids, as it is a statement purely about the flow lattices:

Lemma 3.12 (Proposition 2.7 [Gre11])**.** For a graph G and a matroid $\mathcal{M}$, the restriction maps

$$
\text{Short}\left(\mathbb{Z}^{E(G)}\right) \to \text{Short}\left(\mathcal{F}(G)\right)
$$

and

$$
\text{Short}\left(\mathbb{Z}^{E(\mathcal{M})}\right) \to \text{Short}\left(\mathcal{F}(\mathcal{M})\right)
$$

surject.

We are now ready to show that automorphisms of the lattice of integer flows of a regular matroid lift to automorphisms of the matroid itself.

Proposition 3.13. For a regular matroid $\mathcal{M}$ of cogirth ≥ 2, an automorphism $f : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{M})$ and the canonical embedding $\iota_{can} : \mathcal{F}(\mathcal{M}) \hookrightarrow \mathbb{Z}^{E(\mathcal{M})}$, there exists a lifted lattice automorphism $\varphi : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{M})}$ such that φ restricts to f, that is, the following diagram commutes:

$$
\begin{array}{ccc}
\mathbb{Z}^{E(\mathcal{M})} & \xrightarrow{\quad \varphi \quad} & \mathbb{Z}^{E(\mathcal{M})} \\
\Big\uparrow {\scriptstyle \iota_{can}} & & \Big\uparrow {\scriptstyle \iota_{can}} \\
\mathcal{F}(\mathcal{M}) & \xrightarrow{\quad f \quad} & \mathcal{F}(\mathcal{M})
\end{array}
$$

Proof. First define $B_{\mathcal{F}(\mathcal{M})}$ to be a positive circuit basis of $\mathcal{M}$ as in Proposition 2.7. Then using the substitutions as above, the conditions of Theorem 3.11 follow from the discussion above, noting that lattice automorphisms preserve short characteristic covectors.

Then by Theorem 3.11 there exists an automorphism $F : \mathbb{Z}^E \to \mathbb{Z}^E$ such that $\iota_{can} \circ f = F \circ \iota_{can}$, and this F restricts to f.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

It is well-known that the lattice of integer flows is a complete isomorphism invariant for matroids with cogirth ≥ 2 and thus a complete 2-isomorphism invariant for 2-connected graphs. For regular matroids this was shown by Su and Wagner [SW10]:

Theorem 3.14 (Theorem 1, [SW10])**.** *Let $\mathcal{M}$ and $\mathcal{N}$ be regular matroids. Then $\mathcal{F}(\mathcal{M}) \cong \mathcal{F}(\mathcal{N})$ as lattices if and only if the matroid minors obtained by contracting coloops of $\mathcal{M}$ and $\mathcal{N}$ respectively are isomorphic.*

Since matroids with cogirth ≥ 2 have no coloops, we obtain the following two corollaries.

Corollary 3.15. Let $\mathcal{M}$ and $\mathcal{N}$ be regular matroids of cogirth ≥ 2. Then $\mathcal{F}(\mathcal{M}) \cong \mathcal{F}(\mathcal{N})$ if and only if $\mathcal{M} \cong \mathcal{N}$.

Corollary 3.16 (Corollary 2, [SW10])**.** Let G and H be 2-edge-connected graphs. Then $\mathcal{F}(G) \cong \mathcal{F}(H)$ if and only if G and H are 2-isomorphic.

One of the main results of this thesis is the following *strong Torelli theorem*, namely, a more explicit form of Corollary 3.15:
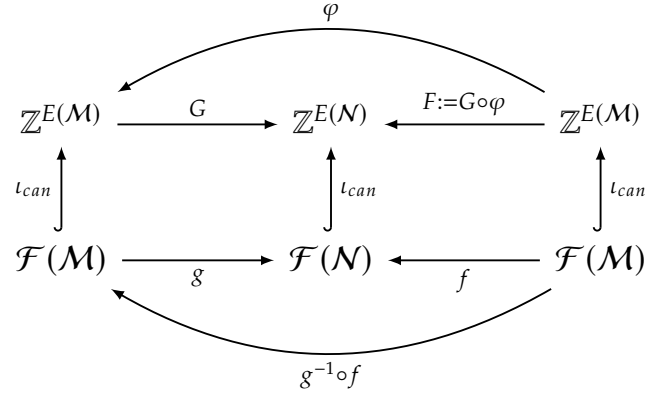
Theorem 3.17. *Given regular matroids $\mathcal{M}, \mathcal{N}$ of cogirth ≥ 2 and an isomorphism $f : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{N})$ of the lattices of integer flows, there exists a lifted lattice isomorphism $F : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{N})}$, which restricts to f and induces a matroid isomorphism $F : E(\mathcal{M}) \to E(\mathcal{N})$.*

Proof. As $\mathcal{M}$ and $\mathcal{N}$ have cogirth ≥ 2, by Corollary 3.15, there exists a matroid isomorphism $G : E(\mathcal{M}) \to E(\mathcal{N})$. This is in particular a set bijection, which we can linearly extend to an isomorphism $G : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{N})}$. Since g is a matroid isomorphism, it is necessarily cycle-preserving, and hence restriction $g := G|_{\mathcal{F}(\mathcal{M})}$ is an isomorphism $g : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{N})$, though g does not necessarily coincide with f.

The composition $g^{-1} \circ f : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{M})$ is then an automorphism of $\mathcal{F}(\mathcal{M})$, which, by Proposition 3.13, lifts to a lattice automorphism $\varphi : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{M})}$. Thus, the composition $F := G \circ \varphi : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{N})}$ is an isomorphism which restricts to f.

Note that any lattice isomorphism $F : \mathbb{Z}^{E(\mathcal{M})} \to \mathbb{Z}^{E(\mathcal{N})}$ induces a matroid isomorphism $F : E(\mathcal{M}) \to E(\mathcal{N})$, because for each $e \in E(\mathcal{M})$, the image $F(e)$ is of norm 1 in $\mathbb{Z}^{E(\mathcal{N})}$, therefore $F(e) = \pm e'$ for some $e' \in E(\mathcal{N})$. Thus F induces a set bijection $F : E(\mathcal{M}) \leftrightarrow E(\mathcal{N})$, which is cycle-preserving since F restricts to an isomorphism $f : \mathcal{F}(\mathcal{M}) \to \mathcal{F}(\mathcal{N})$.

The proof is summarised by the following diagram:

$$
\begin{array}{ccccc}
\mathbb{Z}^{E(\mathcal{M})} & \xrightarrow{\;\;G\;\;} & \mathbb{Z}^{E(\mathcal{N})} & \xleftarrow{F:=G\circ\varphi} & \mathbb{Z}^{E(\mathcal{M})} \\
\big\uparrow{\scriptstyle \iota_{can}} & & \big\uparrow{\scriptstyle \iota_{can}} & & \big\uparrow{\scriptstyle \iota_{can}} \\
\mathcal{F}(\mathcal{M}) & \xrightarrow{\;\;g\;\;} & \mathcal{F}(\mathcal{N}) & \xleftarrow{\;\;f\;\;} & \mathcal{F}(\mathcal{M})
\end{array}
$$

with arcs labelled φ (top) and $g^{-1}\circ f$ (bottom).

$\square$

Corollary 3.18. Given 2-connected graphs G, H and an isomorphism $f : \mathcal{F}(G) \to \mathcal{F}(H)$ of the integer flow lattices, there exists a lifted isomorphism of Euclidean lattices $F : \mathbb{Z}^{E(G)} \to \mathbb{Z}^{E(H)}$, which restricts to f, thus inducing a 2-isomorphism $F : E(G) \to E(H)$ of graphs.

The proof for graphs follows immediately by the same argument, using the positive circuit basis constructed in Lemma 2.3 rather than Proposition 2.7, or alternatively by noting that graphs form graphical matroids, which are regular.

Chapter 4

Recovering $\mathcal{M}$ From $\mathcal{F}(\mathcal{M})$

Circuit recognition of $\mathcal{M}$ immediately followed from Proposition 3.4, however this provides no knowledge of the elements which participate in the circuit. In order to recover the underlying matroid from its lattice of integer flows, we need to better understand Theorem 3.7 and how it can be used to determine which elements.

We call oriented circuits C_1 and C_2 in an oriented matroid $\mathcal{M}$ *compatible* if every for every common element, their orientations agree, i.e. for each $e \in C_1 \cap C_2$ either $e \in C_1^- \cap C_2^-$ or $e \in C_1^+ \cap C_2^+$. Note in particular any two positive circuits or any two negative circuits are always compatible. Then an immediate corollary of Theorem 3.7 is the following:

Corollary 4.1. Let F be a face of $\mathcal{V}(\mathcal{F}(\mathcal{M}))$ expressed as an intersection of

$$F = F_{C_1} \cap F_{C_2} \cap \cdots \cap F_{C_s}$$

where $\{F_{C_i} \mid i = 1, \ldots, s\}$ are the codimension one faces corresponding to oriented circuits $C_1, C_2, \ldots C_s$ respectively. Then the orientations of these circuits are compatible, and the face F under the isomorphism in Theorem 3.7 corresponds to the submatroid $\mathcal{M}$ restricted to $C_1 \cup C_2 \cup \cdots \cup C_s$ with the orientation induced by the circuits.

This observation allows us to choose slightly better circuit basis for our lattice of integer flows, i.e. better recognise which elements are circuit elements. We call a circuit basis *cancellation-free* if, for any pair of basis circuits C_i and C_j, the number of edges in the intersection is computed by the pairing: $|C_i \cap C_j| = |\langle C_i, C_j \rangle|$. Note that positive circuit bases are always cancellation-free, and so cancellation-free bases exist for any regular matroid. We want to be able to detect cancellation-free bases off the information of $\mathcal{F}(\mathcal{M})$ alone, without knowledge of $\mathcal{M}$ or a basis of $\mathcal{M}$. The following remark explains how we can do precisely this.

Remark 4.2. For any pair of circuits C_i and C_j, there are three possibilities:

1. The orientations of C_i and C_j are compatible. This is the case if and only if the corresponding faces F_{C_i} and F_{C_j} intersect.

2. The orientations of C_i and $-C_j$ are compatible. This is the case if and only if the corresponding faces F_{C_i} and F_{-C_j} intersect. (Note that for any circuit C and corresponding face F_C, $F_{-C} = -F_C$ where $-F_C$ is the face parallel to and geometrically opposite from F_C. Note also that (1) and (2) co-occur if and only if the circuits C_i and C_j are disjoint.)

3. Neither of the above is true, that is, C_i and C_j cannot be compatibly oriented, as in Fig. 16. This is the case if and only if the faces $\{F_{C_i}, F_{C_j}, F_{-C_i}, F_{-C_j}\}$ are pairwise disjoint.

In the first two cases, $\left|C_i \cap C_j\right| = \left|\langle C_i, C_j \rangle\right|$, but not in the third case. Hence, to choose a cancellation-free basis, we only need to make sure that all pairs of basis circuits are of the first two types. This can be done by examining the codimension one faces of $\mathcal{FP}(\mathcal{F}(\mathcal{M}))$, that is, those corresponding to circuits in $\mathcal{M}$.
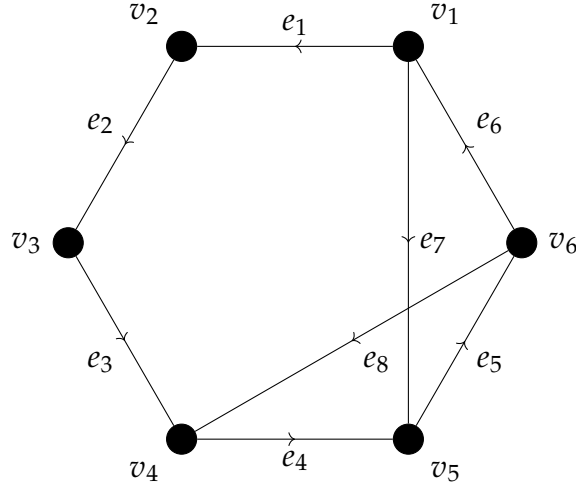

Figure 16: A graph with no compatible orientation for $C_1 = \{e_1, \ldots, e_6\}$ and $C_2 = \{e_4, e_6, e_7, e_8\}$.

In the above remark, we noted that reversing the orientation of a circuit results corresponds to finding the face which is parallel and opposite. However we can say a bit more, in fact the above case was an example of different strongly connected orientations on the circuit, the only two such that exist. In fact for any submatroid of $\mathcal{M}$ the strongly connected orientations' corresponding faces are all parallel in the Voronoi cell.

Proposition 4.3. Let N be a strongly orientable submatroid of $\mathcal{M}$. Let ω_N be a strongly connected orientation of N and let F_{N,ω_N} be the face of $\mathcal{FP}(\mathcal{F}(\mathcal{M}))$ corresponding to (N, ω_N). Then the set of faces corresponding to the different strongly connected orientations of N is the set of faces parallel to, and of the same codimension, as F_{N,ω_N}.

Proof. If F_{N,ω_N} is of codimension s then it can be written (not necessarily uniquely) as an intersection $F_{N,\omega_N} = F_{C_1} \cap F_{C_2} \cap \cdots \cap F_{C_s}$, where $F_{C_1}, \ldots, F_{C_s}$ are codimension one faces corresponding to oriented circuits $C_1, \ldots, C_s$. Then by Corollary 4.1 the matroid corresponding to F_{N,ω_N} is $\mathcal{M}$ restricted to $C_1 \cup C_2 \cup \cdots \cup C_s$. Now consider another codimension s face F', and write $F' = F_{C_1'} \cap F_{C_2'} \cap \cdots \cap F_{C_s'}$ as an intersection of s codimension one faces.

The "direction" of F_{N,ω_N} is the orthogonal complementary subspace to the span of $\{C_1, \ldots, C_s\}$ and similarly for F'. So F_{N,ω_N} and F' are parallel if and only if $\text{span}\{C_1, \ldots, C_s\} = \text{span}\{C_1', \ldots, C_s'\}$.

Now span$\{C_1, \ldots, C_s\}$ is the cycle space of N by our previous remark, and similarly span$\{C'_1, \ldots, C'_s\}$ is the cycle space of N' which is the matroid M restricted to $C'_1 \cup C'_2 \cup \ldots C'_s$. As N and N' have cogirth ≥ 2, every element in $E(N)$ and $E(N')$ participates in a circuit in N and N' respectively. So the cycle spaces are equal if and only if the matroids are equal, i.e. $N = N'$.

$\square$

4.1 Regular Matroids of Cogirth $\geq$ 3

In order to reconstruct the matroid M from its lattice of integer flows, we need to be able to detect the elements of $E(M)$ and the circuits. We can detect circuits by Theorem 3.7 and our construction of the cancellation-free basis as in Remark 4.2, so we now need to find $E(M)$. Matroids with cogirth ≥ 3 can be reconstructed with greater ease than matroids that have cogirth strictly equal to 2 by examining the edges of the Voronoi cell, i.e. the one dimensional faces. By Theorem 3.7 the edges correspond to pairs (N, ω_N) where N is a proper submatroid of M that is strongly orientable with strongly connected orientation ω_N. Any maximal proper submatroid of M is of the form $M \setminus \{e\}$ for some $e \in E(M)$, which is strongly orientable as it is must have cogirth ≥ 2, using an orientation which results in a positive circuit basis as in Proposition 2.7.

Note that Corollary 4.1 defines an equivalence relation on the set of faces, i.e. two faces are equivalent if they are parallel and of the same codimension. Then the equivalence classes, which we call *parallel classes*, correspond to the proper strongly orientable submatroids of M. Then this immediately results in the following reconstruction of M from $\mathcal{F}(M)$.

Theorem 4.4. *Let M be a matroid of cogirth ≥ 3 with lattice of integer flows $\mathcal{F}(M)$ and Voronoi cell $\mathcal{V}(\mathcal{F}(M))$.*

1. *There is a bijection between $E(M)$ and the parallel classes of edges of $\mathcal{V}(\mathcal{F}(M))$.*

2. *There is a bijection between the circuits of M and the parallel classes of codimension one faces of $\mathcal{V}(\mathcal{F}(M))$.*

3. *A given element $e \in E(M)$ belongs to a circuit C if and only if no member of the parallel class of edges corresponding to e belongs to the face F_C (and consequently none of them belong to F_{-C} either).*

4.2 Regular Matroids of Cogirth 2

The situation is simpler in the cogirth ≥ 3 case as any maximal proper strongly orientable submatroid is of the form $M \setminus \{e\}$, which is not necessarily true for cogirth 2 matroids. We still have that edges of the Voronoi cell correspond to pairs (N, ω_N), where N is a maximal strongly orientable proper submatroid of M. We need to understand what N is in this case.

Constructing M requires understanding the complements S in $E(M)$ of maximal strongly orientable proper submatroids. They turn out to be what we will call *2-cut*

blocks, so we begin by defining and describing these blocks. Throughout this section let $\mathcal{M}$ be a regular matroid of cogirth 2.

In the case of graphs, the following three lemmas can be deduced using classical results on minimally 2-connected graphs (see for example [Bol78], Chapter 1.6). We will prove the statements for matroids, for which a proof for graphs follows verbatim.

Lemma 4.5. The relation "elements e and f are either the same or form a 2-cut in $\mathcal{M}$" is an equivalence relation on $E(\mathcal{M})$.

Proof. The reflexive and symmetric properties are obvious, so we only need to prove transitivity, i.e. if e, f, g are three distinct elements, where $\{e, f\}$ and $\{f, g\}$ are both cocircuits, then $\{e, g\}$ is a cocircuit as well.

As $\{e, f\}$ and $\{f, g\}$ are circuits of the matroid $\mathcal{M}^*$, we can use the circuit elimination axiom to find that there is a circuit

$$C_3 \subseteq (\{e, f\} \cup \{f, g\}) \setminus \{e\} = \{f, g\}$$

in $\mathcal{M}^*$, and as $\mathcal{M}$ is of cogirth 2, any cocircuit must have at least two elements, so $C_3 = \{f, g\}$ is a cocircuit.

$\square$

We call the equivalence classes of [Lemma 4.5](#) *2-cut blocks* in $E(\mathcal{M})$, whose name originates from the same notion in graph theory, where cocircuits of size 2 are instead 2-cuts in the graph.

Lemma 4.6. If $S \subseteq E(\mathcal{M})$, then the submatroid $\mathcal{N} = \mathcal{M} \setminus S$ is a maximal proper strongly orientable submatroid of $\mathcal{M}$ if and only if S is a 2-cut block.

Proof. Let S be a 2-cut block. By Lemma [2.5](#), $\mathcal{N}$ is strongly orientable if and only if it has no coloops, i.e., is of cogirth ≥ 2. Assume by contradiction that there exists a coloop $\{e\}$ in $\mathcal{N}$. Cocircuits of $\mathcal{N}$ are all of the form $K \setminus S$ for a cocircuit K in $\mathcal{M}$, that is, $\{e\} = K \setminus S$ where $K = \{e, e_1, \ldots, e_n\}$ is a cocircuit in $\mathcal{M}$, and $\{e_1, \ldots, e_n\} \subseteq S$.

If $n = 1$ then $\{e, e_1\}$ is a cocircuit of size 2, meaning that by definition $e \in S$, a contradiction. If $n \geq 2$ then as $\{e_1, \ldots, e_n\} \subseteq S$, by definition $\{e_1, e_2\}$ is a cocircuit in $\mathcal{M}$ a contradiction as a cocircuit cannot include another. Thus, for any 2-cut block S, the matroid $\mathcal{M} \setminus S$ is always of cogirth ≥ 2, and hence strongly orientable.

Now let $\mathcal{N}$ be a maximal proper strongly orientable sub-matroid, that is, maximal with cogirth ≥ 2, and set $S := E(\mathcal{M}) \setminus E(\mathcal{N})$. If $e \in S$ participates in a cocircuit of size 2 in $\mathcal{M}$, the entire corresponding 2-cut block is contained in S. Indeed, if $\{e, f\}$ is a cocircuit, then $f \in S$ as otherwise $\{f\}$ would be a cocircuit in $\mathcal{N}$, a contradiction. Thus, S is a union of 2-cut blocks, and therefore by the maximality of $\mathcal{N}$, S is a single 2-cut block.

$\square$

For each edge ϵ of the Voronoi cell $\mathcal{V}(\mathcal{F}(\mathcal{M}))$, let $[\epsilon]$ denote the set of all edges of $\mathcal{V}(\mathcal{F}(\mathcal{M}))$ which are parallel to ϵ, that is, the parallel class of ϵ. By [Proposition 4.3](#), the parallel classes $[\epsilon]$ are in one-to-one correspondence with maximal proper submatroids $\mathcal{N} = \mathcal{M} \setminus S$ of cogirth ≥ 2, where S is a 2-cut block. Recall that S is a single element $\{e\}$ if

and only if $M \setminus \{e\}$ has cogirth ≥ 2 – that is, if e does not participate in any cocircuits of size 2 in M. Let $S_{[\epsilon]}$ be the 2-cut block corresponding to the parallel class $[\epsilon]$.

The construction of M then comes down to detecting the size of $S_{[\epsilon]}$ for each $[\epsilon]$. As in the case of matroids with cogirth ≥ 3 in Theorem 4.4, one can then list the circuits of M and tell which 2-cut blocks participate in each circuit based on the face poset $\mathcal{FP}(\mathcal{F}(M))$ of $\mathcal{V}(\mathcal{F}(M))$. Note that circuits are always unions of entire 2-cut blocks, as the following lemma shows.

Lemma 4.7. If S is a 2-cut block and C is a circuit in M, then either S and C are disjoint or $S \subseteq C$.

Proof. Assume $S \cap C \neq \emptyset$ and let $e \in S \cap C$ be some element in the intersection. Let $f \in S$ be any other element in S. We need to show that $f \in C$.

Since $f \in S$, we know that $\{e, f\}$ is a cocircuit in M, hence $\{e\}$ is a coloop in $M \setminus \{f\}$, so e does not participate in any circuit in $M \setminus \{f\}$. So C is not a circuit in $M \setminus \{f\}$, therefore $f \in C$.

$\square$

Let $n_{[\epsilon]} := |S_{[\epsilon]}|$ denote the cardinality of the 2-cut block $S_{[\epsilon]}$. To finish the construction of M, we need to compute the numbers $n_{[\epsilon]}$. Let $B = \{C_1, \ldots, C_r\}$ be a cancellation-free circuit basis of $\mathcal{F}(M)$ chosen as in Remark 4.2. For each $S_{[\epsilon]}$ there is some circuit $C_i \in B$ for which $S_{[\epsilon]} \subseteq C_i$, by Lemma 4.7 and the fact that B is a circuit basis. Each $C_i \in B$ corresponds to a codimension one face of $\mathcal{V}(\mathcal{F}(M))$, denoted F_{C_i}. For each $C_i \in B$, the elements in C_i can be expressed as a disjoint union of the sets $S_{[\epsilon]}$, as 2-cut blocks are disjoint, where $[\epsilon]$ runs over all edge directions of the Voronoi cell which *do not* participate in the face F_{C_i}, as in Theorem 4.4. Hence, for $i = 1, \ldots, r$ one can write the linear equations

$$\sum_{[\epsilon] \notin F_{C_i}} n_{[\epsilon]} = \langle C_i, C_i \rangle, \tag{4.1}$$

where the notation $[\epsilon] \notin F_{C_i}$ means that no edge parallel to ϵ participates in the face F_{C_i}. In addition we have a similar linear equation for each pair of circuits $C_i, C_j \in B$, as the number of edges in $C_i \cap C_j$ is given by the absolute value of their pairing $|C_i, C_j|$, as B is a cancellation-free circuit basis.

$$\sum_{[\epsilon] \notin F_{C_i}, F_{C_j}} n_{[\epsilon]} = \left| \langle C_i, C_j \rangle \right|. \tag{4.2}$$

Note that the resulting system of linear equations always has a positive integer solution, namely, the numbers $n_{[\epsilon]}$ determined by the matroid M. The following proposition shows us that this gives a unique reconstruction for M.

Proposition 4.8. The system (4.1), (4.2) has a unique positive integer solution $\{n_{[\epsilon]}\}$.

Proof. Assume that $\{n_{[\epsilon]}\}$ is the solution given by the sizes of 2-cut blocks in M, and $\{n'_{[\epsilon]}\}$ is a different positive integer solution. Our strategy is to construct a corresponding matroid with 2-cut blocks $S'_{[\epsilon]}$ of sizes $n'_{[\epsilon]}$, and show that M and M' are isomorphic.

The elements of $E(\mathcal{M})$ are partitioned by the sets $S_{[\epsilon]}$, with $\left|S_{[\epsilon]}\right| = n_{[\epsilon]}$. Assume that for some ϵ, $n'_{[\epsilon]} > n_{[\epsilon]}$. Choose an arbitrary element e of $S_{[\epsilon]}$ and split it into $n'_{[\epsilon]} - n_{[\epsilon]} + 1$ elements, in the sense that, we add $n'_{[\epsilon]} - n_{[\epsilon]}$ arbitrary extra elements to $E(\mathcal{M})$ and add these elements to any circuits $C \in \mathcal{C}(\mathcal{M})$ for which $e \in C$, where the orientation is inherited from e. Call the resulting matroid $\mathcal{N}$, and the changed 2-cut block $T_{[\epsilon]}$. First, note that in $\mathcal{N}$, $T_{[\epsilon]}$ is in fact a 2-cut block, that is, any two of its elements form a 2-cut. Furthermore, $\left|T_{[\epsilon]}\right| = n'_{[\epsilon]}$, and all other 2-cut blocks are unchanged. In addition, the circuits of $\mathcal{M}$ are in bijection with the circuits of $\mathcal{N}$ – informally speaking, the element splitting operation does not chance the circuit structure of $\mathcal{M}$ except for their lengths.

On the other hand, if for some ϵ, $n'_{[\epsilon]} < n_{[\epsilon]}$, choose $n_{[\epsilon]} - n'_{[\epsilon]}$ arbitrary elements in $S_{[\epsilon]}$ to contract and denote this subset X, as defined in Section 2.2. Again call the resulting matroid $\mathcal{N} := \mathcal{M}/X$, and call the new 2-cut block $T_{[\epsilon]}$, which is a 2-cut block in $\mathcal{N}$ of cardinality $n'_{[\epsilon]}$, while all other 2-cut blocks are unchanged.

The circuits of $\mathcal{N}$ are the minimal non-empty members of $\{C \setminus X \mid C \in \mathcal{C}(\mathcal{M})\}$. Any circuit in $\mathcal{M}$ which intersects $S_{[\epsilon]}$ contains it, by Lemma 4.7, so the same is true for X. As $n'_{[\epsilon]} > 0$, circuits are not contracted to nothing, and circuits are in correspondence with those of $\mathcal{M}$, in the sense that none vanish. To see this note that if for some distinct $C, C' \in \mathcal{C}(\mathcal{M})$, if $S_{[\epsilon]} \subseteq C$ then $C \setminus X \subseteq C' \setminus X$ if and only if $C \subseteq C'$, regardless of whether C' contains the 2-cut block or is disjoint from it, a contradiction. Now if C is disjoint from the 2-cut block, then $C \setminus X \subseteq C' \setminus X$ if and only if $C \subseteq C' \setminus X \subseteq C'$, again a contradiction. So we cannot have $C \setminus X \subseteq C' \setminus X$, and as no circuits vanish, we must have that the circuits of $\mathcal{N}$ are precisely $\{C \setminus X \mid C \in \mathcal{C}(\mathcal{M})\}$, thus are in bijection with the circuits of $\mathcal{M}$.

Now carry out this process for all $[\epsilon]$ to create a new matroid $\mathcal{M}'$ with 2-cut blocks $S'_{[\epsilon]}$ of sizes $n'_{[\epsilon]}$. We claim that $\mathcal{F}(\mathcal{M}) \cong \mathcal{F}(\mathcal{M}')$. Recall that $\{C_1, \dots, C_r\}$ is a circuit basis for $\mathcal{F}(\mathcal{M})$, and call the gram matrix corresponding to this circuit basis M. Let $\{C'_1, \dots, C'_r\}$ be the circuits in $\mathcal{M}$ in bijection with $\{C_1, \dots, C_r\}$ under the operations above. As circuits were preserved, these form a circuit basis for $\mathcal{F}(\mathcal{M}')$; let us call the corresponding Gram matrix M'.

Since the C_i form a cancellation-free basis of $\mathcal{F}(\mathcal{M})$, the entries of the absolute value $|M|$ are the sizes of the intersections $\left|C_i \cap C_j\right|$, with $i, j = 1, \dots, r$. The basis $\{C'_1, \dots, C'_r\}$ is also cancellation-free: the characterisation of Remark 4.2 shows that the element splittings and contractions do not change this property. Since the $\{n_{[\epsilon]}\}$ and $\{n'_{[\epsilon]}\}$ are both solutions to the system of equations (4.1) and (4.2), we deduce that $|M| = |M'|$.

Furthermore, the sign of the (i, j) entry of M depends on whether C_i and C_j are oriented compatibly or opposite (where opposite means that the orientation of C_i is compatible with that of $-C_j$). This is unchanged by element splittings and contractions, hence the sign of each entry is the same in M and M'. So $M = M'$ and $\mathcal{F}(\mathcal{M}) \cong \mathcal{F}(\mathcal{M}')$. Thus, by Theorem 3.17, this lifts to an isomorphism $E(\mathcal{M}) \to E(\mathcal{M}')$, which sends each element of $\mathcal{M}$ to a signed element of $\mathcal{M}'$, creating bijections within the 2-cut blocks. So $\{n_{[\epsilon]}\} = \{n'_{[\epsilon]}\}$ for all ϵ as needed.

$\square$

We can now state the reconstruction explicitly:

Theorem 4.9. *The matroid M of cogirth 2 can be computed explicitly (up to isomorphism) from the lattice of integer flows $\mathcal{F}(M)$ by the following algorithm:*

1. *List the one-codimensional face of the Voronoi cell $\mathcal{V}(\mathcal{F}(M))$ of $\mathcal{F}(M)$, and use this to choose a good circuit basis $\{C_1, \ldots, C_r\}$ for $\mathcal{F}(M)$ as explained in Remark 4.2.*

2. *List the edges $\{\epsilon\}$ of $\mathcal{V}(\mathcal{F}(M))$, and group them into parallel classes $\{[\epsilon]\}$. For each circuit C, list which edge directions participate in the face F_C.*

3. *For each basis circuit $C_i, i = 1, \ldots, r$, write the equation*

$$\sum_{[\epsilon] \notin F_{C_i}} n_{[\epsilon]} = \langle C_i, C_i \rangle,$$

and for each pair of basis circuits $\{\{C_i, C_j\}, i, j = 1, \ldots, r, i \neq j\}$ write the equation

$$\sum_{[\epsilon] \notin F_{C_i}, F_{C_j}} n_{[\epsilon]} = \left| \langle C_i, C_j \rangle \right|.$$

4. *Solve the system of linear equations, to find the unique positive integer solution $\{n_{[\epsilon]}\}$.*

5. *The ground set of M is the disjoint union of the sets $\{S_{[\epsilon]}\}$ whose sizes are given by the solution $\{n_{[\epsilon]}\}$.*

6. *The element e belongs to a circuit C if and only if no member of the corresponding edge parallel class $[\epsilon]$ in $\mathcal{V}(\mathcal{F}(M))$ belongs to the face F_C.*

Example 4.10. As an example, let us carry out the algorithm for the lattice of integer flows, with Gram matrix given by

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 0 \\ 2 & 0 & 4 \end{pmatrix}.$$

The Voronoi cell is a rhombic dodecahedron, as in Fig. 17

1. The Voronoi cell has 12 faces (note these are codimension one faces, which are 2 dimensional). Of these we choose three pairwise intersecting ones, thus forming a cancellation-free basis: let F_{C_1} be the top right (white) face of the dodecahedron, F_{C_2} be the top (light blue) face, and F_{C_3} be the front (light purple) face.

2. There are 24 edges, which belong to four parallel classes (of 6 edges each). Let ϵ_1 be the edge between the two left side faces (dark blue and dark purple), ϵ_2 be the edge between the two right side faces (white and orange), ϵ_3 be the edge between the front and top left faces (light purple and dark blue), and ϵ_4 be the edge between the front and top right faces (light purple and white).

   Note that each face is a parallelogram, so they contain two pairs of parallel edges. The parallel classes $\{[\epsilon_2], [\epsilon_4]\}$ appear in F_{C_1}, $\{[\epsilon_1], [\epsilon_2]\}$ appear in F_{C_2}, and $\{[\epsilon_3], [\epsilon_4]\}$ appear in F_{C_3}.
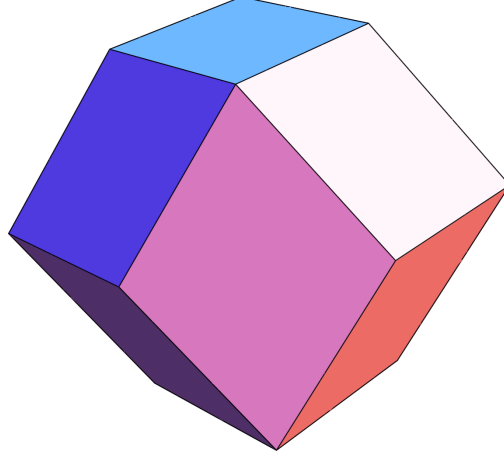
Figure 17: A rhombic dodecahedron.

3. The equations are given as follows. Firstly, for the equations given by (4.1): for C_1, the parallel classes of edges $[\epsilon_1]$ and $[\epsilon_3]$ do not participate, so $n_1 + n_3 = \langle C_1, C_1 \rangle = 3$, similarly, for C_2 we have $n_3 + n_4 = 3$ and for C_3 we have $n_1 + n_2 = 4$. For the equations given by (4.2): for C_1, C_2, the parallel class of edges $[\epsilon_3]$ does not participate, so $n_3 = \langle C_1, C_2 \rangle = 1$, similarly, for C_1, C_3 we have $n_1 = 2$ and for C_2, C_3 we have $0 = 0$, as all parallel classes of edges participate in the faces corresponding to C_2, C_3.

4. Solving this system of linear equations gives $n_1 = 2, n_2 = 2, n_3 = 1, n_4 = 2$.

5. There are 7 elements in the base set, let $S_1 = \{e_1, e_2\}, S_2 = \{e_3, e_4\}, S_3 = \{e_5\}, S_4 = \{e_6, e_7\}$ where $|S_i| = n_i$, then $E(\mathcal{M}) = \cup_{i=1}^{4} S_i = \{e_1, \dots, e_7\}$.

6. There are six (unoriented) circuits corresponding to the 6 pairs of parallel faces, that is each of the visible faces in Fig. 17 and their corresponding parallel face on the opposite (non-visible) side. Then we have the three circuits we described, C_1 corresponding to the top right (white) face, C_2 corresponding to the top (light blue) face and C_3 corresponding to the front (light purple) face. We also have three more corresponding to the other faces, which are linear combinations of the circuit basis circuits above, namely $C_4 = C_3 + C_2 - C_1$ corresponding to the top left (dark blue) face, $C_5 = C_1 - C_2$ corresponding to the bottom right (orange) face and $C_6 = C_3 - C_1$ corresponding to the bottom left (dark purple) face. Then the circuits are made up of the union of S_i where the parallel class of edges $[\epsilon_i]$ does not participate in the face. So for C_1, as it contains the parallel classes of edges $\{[\epsilon_2], [\epsilon_4]\}$, the circuit is $C_1 = S_1 \cup S_3 = \{e_1, e_2, e_5\}$. Similarly,

$$C_2 = S_3 \cup S_4 = \{e_5, e_6, e_7\}$$
$$C_3 = S_1 \cup S_2 = \{e_1, e_2, e_3, e_4\}$$
$$C_4 = S_2 \cup S_4 = \{e_3, e_4, e_6, e_7\}$$
$$C_5 = S_1 \cup S_4 = \{e_1, e_2, e_6, e_7\}$$
$$C_6 = S_2 \cup S_3 = \{e_3, e_4, e_5\}.$$

So the matroid is $\mathcal{M}$ with $E(\mathcal{M}) = \{e_1, \ldots, e_7\}$ and $\mathcal{C}(\mathcal{M}) = \{C_1, \ldots, C_6\}$ as above.

In fact this is a graphical matroid, so we can find a representing graph by drawing out the cycles. A representing graph is given in Fig. 18, note that this is only a representing graph up to 2-isomorphism and up to extra non-participating vertices.
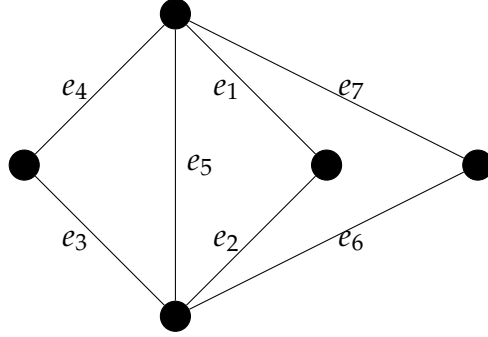

Figure 18: A graph G representing the 2-isomorphism class for the graphical matroid $\mathcal{M}$ reconstructed in Example 4.10.
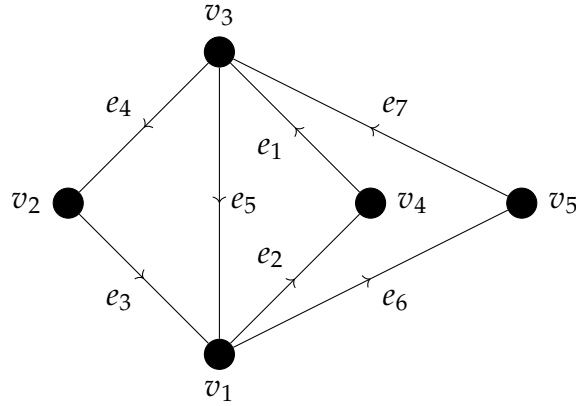

Figure 19: A graph G representing the 2-isomorphism class of the matroid $\mathcal{M}$ reconstructed in Example 4.10, with an orientation applied.

Applying the orientation given in Fig. 19, and arbitrarily labelling the vertices, we can write the signed incidence matrix.

$$\begin{bmatrix} 0 & -1 & 1 & 0 & 1 & -1 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 & 1 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

Indeed, with the choice of circuit basis $C_1 = \{+e_1, +e_2, +e_5\}$, $C_2 = \{+e_5, +e_6, +e_7\}$, $C_3 = \{+e_1, +e_2, +e_3, +e_4\}$, we obtain

$$\langle C_1, C_1 \rangle = 3$$
$$\langle C_2, C_2 \rangle = 3$$
$$\langle C_3, C_3 \rangle = 4$$
$$\langle C_1, C_2 \rangle = 1$$
$$\langle C_1, C_3 \rangle = 2$$
$$\langle C_2, C_3 \rangle = 0,$$

and this results in the same Gram matrix as the one we started out with:

$$\begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 0 \\ 2 & 0 & 4 \end{pmatrix}.$$

References

[Ami10]   Omid Amini. *Lattice of Integer Flows and Poset of Strongly Connected Orientations*. Preprint. 2010. DOI: https://doi.org/10.48550/arXiv.2202.13265.

[Bix77]   Robert E Bixby. "Kuratowski's and Wagner's theorems for matroids". In: *Journal of Combinatorial Theory, Series B* 22.1 (1977), pp. 31–53. ISSN: 0095-8956. DOI: https://doi.org/10.1016/0095-8956(77)90047-8.

[Bjö+99] Anders Björner et al. *Oriented Matroids*. 2nd ed. Encyclopedia of Mathematics and its Applications 46. Cambridge University Press, 1999.

[BLN97]   Roland Bacher, Pierre de La Harpe, and Tatiana Nagnibeda. "The lattice of integral flows and the lattice of integral cuts on a finite graph". In: *Bulletin de la Société Mathématique de France* 125.2 (1997), pp. 167–198. ISSN: 0037-9484. DOI: https://doi.org/10.24033/bsmf.2303.

[Bol78]   Béla Bollobás. *Extremal graph theory*. Vol. 11. London Mathematical Society Monographs. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978, pp. xx+488. ISBN: 0-12-111750-2.

[CV09]   Lucia Caporaso and Filippo Viviani. "Torelli theorem for graphs and tropical curves". In: *Duke Mathematical Journal* 153 (Jan. 2009). DOI: https://doi.org/10.1215/00127094-2010-022.

[DL23]   Zsuzsanna Dancso and Jongmin Lim. "Lattice of integer flows and the poset of strongly connected orientations for regular matroids". In: *Discrete Math.* 346.12 (Dec. 2023). ISSN: 0012-365X. DOI: https://doi.org/10.1016/j.disc.2023.113589.

[Gre11]   Joshua Greene. "Lattices, graphs, and Conway mutation". In: *Inventiones Mathematicae* 192.3 (2011), pp. 717–750. ISSN: 00209910, 14321297. DOI: https://doi.org/10.1007/s00222-012-0421-4.

[GY06]   Jonathan L. Gross and Jay Yellen. *Graph theory and its applications*. Second. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xiv+779. ISBN: 978-1-58488-505-4; 1-58488-505-X.

[HSW22]   Karl Heuer, Raphael Steiner, and Sebastian Wiederrecht. "Even circuits in oriented matroids". In: *Combinatorial Theory, 2 (1)* 2 (1 2022). DOI: https://doi.org/10.5070/C62156875.

[Oxl06]   James G. Oxley. *Matroid Theory (Oxford Graduate Texts in Mathematics)*. USA: Oxford University Press, Inc., 2006. ISBN: 0199202508.

[SW10]   Yi Su and David G Wagner. "The lattice of integer flows of a regular matroid".
           In: *Journal of Combinatorial Theory, Series B* 100.6 (2010), pp. 691–703. ISSN: 0095-
           8956. DOI: https://doi.org/10.1016/j.jctb.2010.07.003.

[Wat90]   William Watkins. "The Laplacian matrix of a graph: unimodular congruence".
           In: *Linear and Multilinear Algebra* 28.1-2 (1990), pp. 35–43. ISSN: 0308-1087,1563-
           5139. DOI: https://doi.org/10.1080/03081089008818027.

[Wat94]   William Watkins. "Unimodular congruence of the Laplacian matrix of a graph".
           In: *Linear Algebra Appl.* 201 (1994), pp. 43–49. ISSN: 0024-3795,1873-1856. DOI:
           https://doi.org/10.1016/0024-3795(94)90102-3.

[Whi35]   Hassler Whitney. "On the Abstract Properties of Linear Dependence". In: *American Journal of Mathematics* 57.3 (1935), pp. 509–533. ISSN: 00029327, 10806377.
           DOI: https://doi.org/10.1007/978-0-8176-4842-8_5.