On the Automorphism Group of a Matroid

Galen Dorpalen-Barry[*]

22 June 2017

Talk Outline.

0. Introduction
1. What is a matroid?
2. The Automorphism Group of a Matroid
3. Questions for the Audience

Goal Theorem for the Talk.

Theorem (Harary, Piff, Welsh)**.** *Let H be a group. Then there exists a graph whose associated independence structure has automorphism group isomorphic to H.*

Remark. For the purpose of this talk, I will specialize to the finite case in which an independence structure is a matroid.

[*] These notes were prepared for my talk at Craig Corsi's seminar on Representation Theory. Many thanks to Craig for reading an early draft of these notes and giving comments. If you notice any other errors, let me know!

1 What is a Matroid?

There are many ways to define a matroid. The gist is that you take a finite set S and add some structure to S by identifying sets as independent sets[1]. These independent sets need to satisfy certain axioms, usually if $\mathcal{I}$ is our collection of independent sets then we say

1. $\emptyset \in \mathcal{I}$
2. If $A \in \mathcal{I}$ and $B \subset A$, then $B \in \mathcal{I}$
3. Something else (exchange axiom).

Here I'm being a bit murky about what this third axiom is. And the reason I'm doing that is because there are several different ways to describe it. Vic describes the exchange axiom in the following way:

3. (VR Exchange Axiom) Suppose $I_1, I_2 \in \mathcal{I}$ and that I_1 has strictly larger cardinality than I_2, then there exists $\{a\} \in I_1 - I_2$ such that $I_2 \cup \{a\} \in \mathcal{I}$.

Haray, Piff, and Welsh have an equivalent version of the exchange axiom. They say:

3. (HPW Exchange Axiom) Suppose $I_1, I_2 \in \mathcal{I}$ and that $|I_1| = |I_2| + 1$, then there exists $\{a\} \in I_1 - I_2$ such that $I_2 \cup \{a\} \in \mathcal{I}$.

This is equivalent to the VR Exchange Axiom in the following way.

($\Rightarrow$) The VR Exchange Axiom obviously implies the HPW Exchange Axiom.

($\Leftarrow$) However, the argument bears fleshing out for the sake of precision. Let $I, J \in \mathcal{I}$ with $|I| > |J|$. Let $k = |J| + 1$. Let I' be any k-subset of I. Then the HPW Exchange Axiom tells us that there exists $x \in (I' - J)$ such that $(J \cup \{x\}) \in \mathcal{I}$. Since $x \in (I' - J)$ and $I' \subset I$, it follows that $x \in (I - J)$. This is precisely the condition of the VR Exchange Axiom.

Example 1. Let's consider the matroid structure on the following vectors in $\mathbb{F}_2^3$ indexed by $S = \{1, 2, 3, 4, 5\}$. We have

$$v_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}, \quad v_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad v_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}, \quad v_4 = \begin{pmatrix}1\\1\\1\end{pmatrix}, \quad \text{and} \quad v_5 = \begin{pmatrix}0\\1\\0\end{pmatrix}.$$

Here is what $\mathcal{I}$ looks like for this collection of vectors (note that I have dropped the v_i notation and simply list vectors by their indices)

$$\mathcal{I} = \{\emptyset, 1, 2, 3, 4, 5, 12, 13, 14, 15, 23, 24, 34, 35, 45, 123, 124, 134, 135, 145, 234, 345\}.$$

[1] You can also define independent sets via bases but I won't discuss that here.

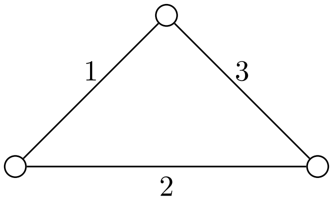

Figure 1: A graph G with edges $\{1, 2, 3\}$.

Note that $\{v_2, v_5\} \notin \mathcal{I}$ since $v_2 = v_5$. Perhaps more interestingly $\{v_1, v_2, v_3, v_4\} \notin \mathcal{I}$ since $v_1 + v_2 + v_3 = v_4$. Indeed, since our vector field is three-dimensional, linear algebra tells us that no independent set will contain more than three vectors.

In this presentation, we'll be focusing on graphic matroids, or matroids whose ground set comes from the edge set of a finite, simple graph. The following two examples are of graphic matroids.

Example 2. Let G be the graph shown in Figure 1. Then the edges $E = \{1, 2, 3, 4, 5\}$ form the ground set of a matroid whose independent sets are

$$\mathcal{I} = \{\emptyset, 1, 2, 3, 12, 13, 23\}.$$

Example 3. Let G be the graph shown in Figure 2. Then the edges $E = \{1, 2, 3, 4, 5\}$ form the ground set of a matroid whose independent sets are

$$\begin{aligned}\mathcal{I} \quad = \quad & \{1,\ 2,\ 3,\ 4,\ 5, \\ & 12,\ 13,\ 14,\ 15,\ 23,\ 24,\ 25,\ 34,\ 35,\ 45, \\ & 124,\ 125,\ 134,\ 135,\ 145,\ 234,\ 235,\ 245,\ 345, \\ & 1245,\ 1345,\ 2345\ \}\end{aligned}$$

1.1 Bases

Another way to characterize matroids is through bases. The bases $\mathcal{B} \subset \mathcal{I}$ are a set of maximal elements of $\mathcal{I}$ such that $\mathcal{B} \neq \emptyset$ and the sets of $\mathcal{B}$ satisfy the basis exchange property:

> (Basis Exchange Property) Let $A, B \in \mathcal{B}$ with $A \neq B$. Then for $a \in (A - B)$, there exists $b \in (B - A)$ such that $(A - \{a\}) \cup \{b\} \in \mathcal{B}$.

Example 4. In the first example the bases are the linear-algebraic bases (independent spanning sets).

$$\mathcal{B} = \{123, 124, 134, 135, 145, 234, 345\}.$$

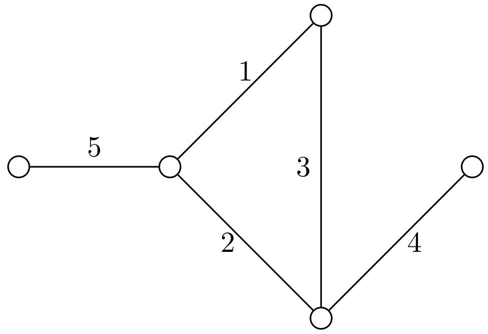

Figure 2: A graph G with edges $\{1, 2, 3, 4, 5\}$.

Example 5. Let G be the graph given in Figure 1. Then the spanning trees of G are the bases. We have

$$\mathcal{B} = \{12, 13, 23\}.$$

1.2 Variation: Independence Structures

We can make a small variation, allowing the ground set to be infinite. In this case, we call the resulting object an independence structure and adding a fourth axiom. We say that $\mathcal{I}$ has finite character.

4. (Finite Character) Let $X \subset 2^E$ be infinite. Then X is independent if every finite subset $Y \subset X$ is independent.

This is not the focus of this presentation, but it does show up in the statement of the main theorem.

2 The Automorphism Group of a Matroid

2.1 What is the automorphism group of a matroid?

For the remainder of this section, we'll take S to be a finite set and denote the cardinality of S by n.

Definition (Preserves Independence)**.** Let $\sigma \in S_n$. We say that σ preserves the independence of our matroid structure if

$$I \in \mathcal{I} \iff \sigma(I) \in \mathcal{I}.$$

Example 6. In our first example, the transposition (25) preserves independence since $v_2 = v_5$ and so for any independent set containing v_2, there must also be an independent set containing v_5.

Non-example. In our first example, the transposition $\sigma = (12)$ does not preserve independence since $\{v_1, v_5\} \in \mathcal{I}$ but $\sigma(\{v_1, v_5\}) = \{v_2, v_5\} \notin \mathcal{I}$.

Definition (Automorphism Group of a Matroid)**.** The automorphism group $A(M)$ of a matroid M with ground set S is a collection of permutations of S, which preserve independence.

When our matroid is obtained from a graph G, I will sometimes abuse notation and write $A(G)$ instead of $A(M(G))$.
The first thing to notice is that this automorphism group will be a subset of S_n. In the proof of the following proposition, we will use the fact that S_n is finite.

Proposition. *The automorphism group of a matroid (or independence structure) is a group.*

Proof. We need to check the group axioms.

1. Closure. Suppose that $\sigma_1, \sigma_2 \in A(M)$. Then for all $I \in \mathcal{I}$, we have $\sigma_1(I) \in \mathcal{I}$. Then $\sigma_2(\sigma_1(I)) \in \mathcal{I}$. Then $(\sigma_2 \circ \sigma_1) \in A(M)$.

2. Associativity. Associativity is inherited.

3. Identity. Certainly permuting nothing preserves independence.

4. Inverses. Let $\sigma \in A(M)$. Since σ preserves independence, it must also preserve non-independence. Now let $I \in \mathcal{I}$ and consider $\sigma^{-1}(I)$. We know that

$$\sigma \circ \sigma^{-1}(I) = I \in \mathcal{I}.$$

   Then σ sends $\sigma^{-1}(I)$ to an independent set. Since σ preserves independence, it must have been that $\sigma^{-1}(I) \in \mathcal{I}$.

Then $A(M)$ is indeed a group. □

We note that an independence-preserving permutation must also preserve cycles (otherwise either it or its inverse wouldn't preserve independence). It may be useful sometimes to use this characterization of the automorphism group. In that case we will emphasize the cycles by adding a C as a subscript to the A. Harary calls this the "cycle automorphism group" and notes that $A_C(G) = A(M(G))$. An explicit definition is given below.

Definition (Cycle Automorphism Group)**.** The cycle automorphism group $A_c(G)$ of G is the set of all permutations σ such that for all cycles $C \subset E$, we have $\sigma(C)$ is also a cycle of G.

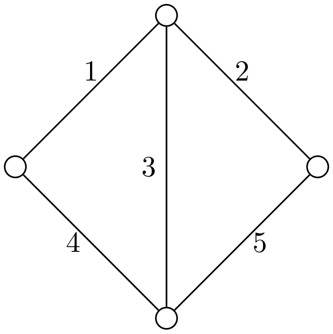

Figure 3: A graph G with edges $\{1, 2, 3, 4, 5\}$.

Let G be a connected graph and let $A(G)$ be the automorphism group of the associated matroid. Then

$$A_C(G) = A(G).$$

Intuitively, if $A_C(G)$ is precisely the set of permutations σ such that cycles of $M(G)$ are preserved, then σ must also preserve non-cycles (independent sets).

Example 7. Let G be the graph shown in Figure 3. Then the edges $E = \{1, 2, 3, 4, 5\}$ form the ground set of a matroid whose independent sets are

$$\begin{aligned} \mathcal{I} \quad = \quad & \{1,\ 2,\ 3,\ 4,\ 5, \\ & 12,\ 13,\ 14,\ 15,\ 23,\ 24,\ 25,\ 34,\ 35,\ 45, \\ & 123,\ 125,\ 124,\ 135,\ 145,\ 234,\ 245,\ 345\} \end{aligned}$$

Instead of looking at which permutations preserve non-cycles, I looked at the permutations that would not create or destroy cycles. For example, every cycle containing 1 must also contain 4, so $\sigma = (14)$ will preserve cycles. The same holds for 2 and 5. Then

$$A(G) = \{(\ ), (14), (25), (14)(25)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

2.2 Graph Theory

We'll use graph theory to understand this group structure on a matroid. Frank Harary (who was one of the main authors on this paper) was mostly a graph theorist. Indeed, according to Wikipedia, he is widely recognized as one of the fathers of modern graph theory. Recall that all matroids structures on graphs can be represented as matroid structures on sets of vectors (linear matroids) or as field extensions (algebraic matroids).

To that end, we look to Graphic Matroids and define two refinements of the previous definition of an automorphism group. Let $G = (V, E)$ be a finite, simple graph and for $i, j \in V$, we denote an edge from i to j by (ij).

Definition (Point Automorphism Group)**.** The point automorphism group $A_p(G)$ of G is the set of all permutations π such that for all edges $(ij) \in E$, the edge $(\pi(i)\pi(j)) \in E$ as well.

Definition (3-connected)**.** Let G be a connected graph and let k be the minimum number of vertices that must be removed from G in order to make G have more than one connected component. If $k \geq 3$, then we say that G is 3-connected.

In other words, we can remove one or two vertices from G and it will still be connected. In the following Lemma, we'll see that being able to remove one or two vertices from a connected graph implies an isomorphism between the point automorphism group and the cycle automorphism group.

Lemma 1 (Theorem 15.4.4 from (3))**.** *If every pair of vertices lies in a circuit of G (G is connected and has no "separating vertices") then all circuit isomorphisms of G are induced by isomorphisms of G if and only if G is 3-connected.*

In our terminology, this implies that "If G is 3-connected, then $A_p(G) \cong A_c(G)$."

Lemma 2. *Let p be a positive integer. Let H be a finite group. Then there exists a finite, p-connected graph G such that $A_p(G) \cong H$.*

Proof. See Sabidussi's "Graphs of a given group and given graph-theoretical properties." □

Pretty much all the work in this paper is being done by Sabidussi's theorem, which is tricky. Indeed, his paper could be a presentation unto itself.

Lemma 3. *Let p be a positive integer. Let H be a group. Then there exists a finite p-connected graph G such that $A_p(G) \cong H$.*

Theorem 1 (Harary, Piff, Welsh)**.** *Let H be a group. Then there exists a graph whose associated independence structure has automorphism group isomorphic to H.*

Remark. An independence structure is a lot like a matroid but the ground set is allowed to be finite. The independence question is "fixed" by saying that an infinite set Y is an independent set if all finite subsets of Y are also independent. However, for the purpose of this talk, I will only discuss finite groups and finite graphs (which yield matroids).

Proof. By Lemma 3, there exists a graph G such that $A_p(G) \cong H$. We observed tht that $A_c(G) = A(M(G))$. By Lemma 1 we have $A_p(G) \cong A_c(G)$ and so

$$H \cong A_p(G) \cong A(M(G)).$$

Thus we have $H \cong A(M(G))$. □

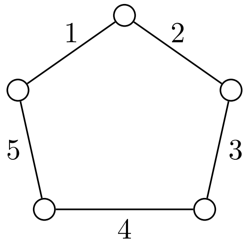

Figure 4: A graph G with $A(G) \cong S_5$.

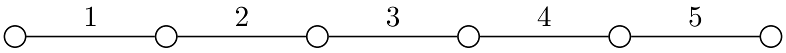

Figure 5: A graph G with $A(G) \cong S_5$.

Corollary. *Let H be a group. Then there exists a geometric lattice whose automorphism group is isomorphic to H.*

Example 8. Let $H = S_5$. Then there are (at least) two graphs whose matroid automorphism group is isomorphic to S_5. They are given in Figure 4 and Figure 5.

There are two things to notice in the previous example. First cycle graph must have "full" automorphism group. Second: so must a tree.

Proposition. *Let $G = (V, E)$ be a tree with n edges, then $A(G) = S_n$.*

Proof. Since G contains no cycles, every subset of E is an independent set. Then for all $X \in \mathcal{I}$, we have $\sigma(X) \in \mathcal{I}$. □

Proposition. *Let $G = (V, E)$ is just a cycle with n edges, then $A(G) = S_n$.*

Proof. By the construction of G, every subset $X \subset E$ such that $|X| < n$ is an independent set. Since permutation preserves the number of elements in a set, applying any $\sigma \in S_n$ to X will produce another set of the same size. This again must be independent. Then for all $X \in \mathcal{I}$, we have $\sigma(X) \in \mathcal{I}$. □

The previous two theorems can be combined by looking at the bases of the associated matroids. Indeed, there is a more general theorem about when you get S_n as your automorphism group. It relies on information about the bases of a matroid.

Theorem 2 (Harary, Piff, Welsh)**.** *Let M be a matroid with a ground set E of cardinality n. Then has $A(M) = S_n$ if and only if M has as bases every k-subset of E for some $k \in [n]$ (i.e. is k-uniform).*

Example 9. Consider the graph G in Figure 4. Every 4-subset of edges is a spanning tree of G. Since $4 \in [5]$, Theorem 2 tells us that the automorphism group $A(G)$ of the matroid associated to G is $S_{|E|} = S_5$.

Example 10. Consider the graph G in Figure 5. The full set of edges is a spanning tree of G. There is only one 5-subset of 5. Since $5 \in [5]$, Theorem 2 tells us that $A(G) \cong S_{|E|} = S_5$.

Theorem 3 (Harary, Piff, Welsh)**.** *There does not exist a matroid on a set of n elements whose automorphism group is equal to the alternating group A_n for $n \geq 3$.*

3 Questions

1. Is it true that a finite group always leads to a finite graph? It is certainly true that a finite graph always has a finite matroid automorphism group but there might be a way to produce some kind of tiling of the plane whose underlying graph has a finite automorphism group.

2. Is there a way to go from a group to a matroid without using graphs?

3. Can we generalize this for other kinds of matroids? All matroids yield an automorphism group and all graphic matroids can be represented as either linear or transcendental matroids. What about matroids arising from bipartite graphs?

4. What other information can you collect about matroids from the automorphism group? (For example: given $A(M)$, can we construct the flats of M?)

4 Sources

1. "On the Automorphism Group of a Matroid" by Harary, Piff, and Welsh (1971)

2. Vic Reiner's notes on matroids.

3. O. Ore's "Theory of Graphs"