Matroids

Rich Schwartz

April 22, 2020

These notes are a strict subset of the material contained in §8.2 of West's book. I thought that I would give a somewhat simpler treatment of the topic. I will try to keep the notation consistent with West's notation.

1 Basic Definition

Let E be a set. A *hereditary structure* on E is a classification of the subsets of E into 2 types:

- dependent
- independent

in a way that has the following property: If $I_1 \subset I_2$ and I_2 is independent, then I_1 is also independent. To avoid set-theoretic troubles let assume that there is some finite N such that all independent sets have size at most N.

Given $X \subset E$, a *maximal independent subset* of X is an independent set $I \subset X$ which is not contained in any larger independent subset of X. Notice that X might contain more than one maximal independent subset. E is called a *matroid* if it has the following additional property: For any $X \subset E$, the maximal subsets of X all have the same size.

It is going to turn out that a matroid has many equivalent definitions. Later on, we will show that the definition given above is equivalent to 7 other definitions.

2 Examples of Matroids

2.1 Vectorial Matroids

The example will work for a vector space defined over any field, but let's keep it simple and just consider $E = \boldsymbol{R}^n$. The independent subsets of E are defined to be those which are linearly independent. In other words $\{V_i\}$ is an independent set if, whenever we have a finite sum $\sum a_i V_i = 0$ we have $a_i = 0$ for all i. As is well known, the subset of a linearly independent set is independent. Hence our definition gives E a heriditary structure.

Now we prove that E is a matroid with this hereditary structure. This proof skimps on some familiar details from linear algebra. Given any subset $X \subset E$, the *span* of X is defined to be the set of linear combinations of elements of X. The set $F = \text{span}(X)$ is a subspace of $\boldsymbol{R}^n$. Let I be a maximal independent subset of X. Then $F' = \text{span}(I)$ is a subspace of F. If $F' \neq F$ then we can add some $V \in X - F'$ to I and get a larger independent set. This is a contradiction. Hence $F' = F$. But then, by familiar properies of dimension, the number of elements of I is the dimension of F. Hence, all the maximal independent sets have the same size.

2.2 Matrix Matroids

Consider a matrix M. We let E denote the set of rows of M. A subset of E is defined to be independent if the rows are linearly independent. This is practically the same example as the vectorial example, except that we restrict our sets to be actual rows of M rather than all possible subsets of the vector space that is the row-span of M. The fact uniformity property for matroids really just says that a matrix – in this case the submatrix made from a given subset X of rows – has a well defined rank.

I think that this example is probably the source of the name *matroid*. A matroid is a matrix-like object.

2.3 Cyclic Matroids

Let G be a graph. For convenience, let's take G to be connected. Let E denote the set of edges of G. We call a subset $I \subset E$ independent if E contains no cycles. This definition is obviously a hereditary structure on E.

Now we prove that E is a matroid with this hereditary structure. Let X be a subset of E. Let H denote the graph whose vertices are the vertices incident to edges of X and whose edges are just the edges of X. Let $H_1, ..., H_k$ denote the connected components of H. A maximal independent subset I of X is exactly a union $T_1 \cup ... \cup T_k$, where T_i is a spanning tree for H_i. But we know that all the spanning trees for a connected graph have the same number of edges, namely the number of vertices minus 1. This gives us the formula for the number of elements of I:

$$|I| = \sum_{i=1}^{k} (|V(H_i)| - 1),$$

where $|V(H_i)|$ is the number of vertices of H_i. This formula is the same for all maximal independent sets, so they all have the same size.

2.4 Transversal Matroids

Let $A_1, ..., A_k$ be (possibly) overlapping sets. Let $E = A_1 \cup ... \cup A_k$. We call the original sets *bins* of E. We define the independent subsets of E to be subsets I having the property that each member of I can be placed in a distinct bin of E. This is obviously a hereditary structure. One important thing to note is that a given independent set can be sorted into bins in perhaps more than one way. This doesn't bother us.

Before we prove that E is a matroid, we re-interpret this notion of independence. We can form a bipartite graph G where the white nodes are labeled $1, ..., k$ and the black nodes are the members of E. We join i to $e \in E$ if and only if $e \in A_i$. Here is how we get an independent subset of E. We find a matching between some black and white vertices and we take the union of the black endpoints of the matching. All independent subsets arise this way. Note, however, that different matchings could give rise to the same independent set.

Now we prove that E is a matroid. We first show that all the maximal independent subsets of E have the same size and then we explain the trick that lets us go this for any subset of E. Let I_1 and I_2 be maximal independent subsets of E. These sets correspond to matchings M_1 and M_2 of G. Suppose that $|I_1| < |I_2|$. Then $|M_1| < |M_2|$. We consider the symmetric difference $M_1 \delta M_2$. This is the union of edges in $M_1 \cup M_2$ which are not in $M_1 \cap M_2$. This symmetric difference consists of alternating paths and alternating loops.

Since $|M_1| < |M_2|$ there must be at least one alternating path which has edges in $M_2, M_1, ..., M_1, M_2$. This is an augmenting path for M_1. We can find a new matching M_1' by replacing all the M_1-edges in this path by the M_2-edges in the path. It is important to note that the matching M_1' does not extend the matching M_1. However the black endpoints I_1' of M_1' contain the black endpoints I_1 of M_1. All we have done is add the black endpoint of our path. But this contradicts the fact that I_1 is a maximal independent set.

We have shown that all the maximal independent subsets of E have the same size. Now for the trick. If $X \subset E$, we just restrict our bipartite graph G to the subgraph G' which involves edges incident to members of E. We rerun the same argument with respect to G' and we see that the maximal independent subset of X all have the same size.

3 Bases for a Matroid

Let E be a set with a hereditary structure, not necessarily a matroid. A *basis* of E is defined to be a maximal independent subset. The terminology comes from the vectorial example. A basis for a vectorial matroid is just a basis in the linear algebra sense. In the cycle example, the bases are the spanning trees.

Consider the following two properties:

1. If B_1 and B_2 are bases and $e \in B_1 - B_2$ then there is some $f \in B_2 - B_1$ such that $(B_1 - e) \cup f$ is a basis.

2. If B_1 and B_2 are bases and $f \in B_2 - B_1$ then there is some $e \in B_1 - B_2$ such that $(B_1 - e) \cup f$ is a basis.

These properties both say we can replace an element of B_1 with an element of B_2. The first property says that we can choose which element of B_1 we want to discard. The second property says that we can choose which element we can import.

Lemma 3.1 *If E has a hereditary structure, then either property implies that bases have the same number of elements.*

Proof: Consider this for Property 1. If B_2 has more elements than B_1, then we can continue replacing elements of B_1 by elements of B_2 until we have

a proper subset $B_2' \subset B_2$ which is also a basis. This is a contradiction. A similar argument works for Property 2. ♠

Lemma 3.2 *If E has a hereditary structure, then the two properties are equivalent.*

Proof: Let us assume that E has property 1 and show that E has property 2. Given $f \in B_2$, we use property 1 (with the roles of B_1 and B_2 reversed) so as to swap out all elements of B_2 except f. When we are done, we have a basis consisting of f and elements from B_1. This is the same as saying that we can donate f to B_1.

Now let us assume that E has property 2 and shoe that E has property 1. We can donate all elements of B_1 to B_2 except e. When we are done, we have a new basis consisting of all elements of B_1 and some element of B_2, which we call f. This establishes Property 1. ♠

Lemma 3.3 *A matroid has both properties.*

Proof: Since the two properties are equivalent we just have to show that Property 1 holds. Suppose that B_1 and B_2 are both bases and $e \in B_1$. Consider the set

$$X = (B_1 - e) \cup B_2.$$

The set B_2 is a maximal independent subset of X. The set $B_1 - e$ is an independent subset of X. By the uniformity property, there is some maximal independent subset $B_1' \subset X$ such that $|B_1'| = |B_2|$ and $B_1 \subset B_1'$. But $B_1' = (B_1 - e) \cup f$ for some $f \in B_2$. Moreover, since $|B_1'| = |B_2|$ and B_1' is also an independent subset of E, the uniformity property tells us that B_1' is a basis. ♠

Now we work towards proving that either of the above properties characterizes a matroid. That is, a hereditary set with either property above is a matroid. We first need a preliminary lemma showing that Property 1 above implies an even more powerful property.

Lemma 3.4 *Suppose that E is a hereditary set with Property 1. If I_1 and I_2 are independent sets with $|I_1| < |I_2|$ then there is some $f \in I_2$ such that $I_1 \cup f$ is independent.*

Proof: We can find bases B_1 and B_2 such that $I_1 \subset B_1$ and $I_2 \subset B_2$. If there is any $e \in B_1 - I_1 - B_2$ we can find $f \in B_2 - B_1$ such that $B_1' = B_1 - e \cup f$ is a basis containing I_1. Repeating this finitely many times, we can arrange that $B_1 - I_1 \subset B_2$. Note that $|B_2 - I_2| < |B_1 - I_1|$. If $B_1 - I_1$ is disjoint from I_2 then $B_1 - I_1 \subset B_2 - I_2$, and this contradicts the cardinality inequality. Hence there is some $f \in B_1 - I_1$ that belongs to I_2. But then $I_1 \cup f$ is independent. ♠

The property in the preceding result is called the *augmentation property*. The augmentation property is equivalent to Property 1 because we may apply it to the independent sets $B_1 - e$ and B_2. So, Property 1, Property 2, and the augmentation property are all equivalent.

Lemma 3.5 *Let E be a set with a hereditary structure. If E has any of the properties above then E is a matroid.*

Proof: Since all the properties above are equivalent, we can assume that E has the augmentation property. Let $X \subset E$. Let I_1, I_2 be maximal independent subsets of X. If $|I_1| < |I_2|$ then we can find $f \in I_2$ such that $I_1 \cup f$ is independent but $I_1 \cup f \subset X$. This contradicts the fact that I_1 is a maximal independent subset of X. ♠

4 The Dual Matroid

Let E be a matroid. We define the dual matroid E^* to be the same underlying set E but with a different hereditary structure. To make it clear when we are talking about a subset in the new hereditary structure, we use E^* in place of E even though $E^* = E$.

A *basis* in the dual hereditary structure is a set $B^* \subset E^*$ such that $E^* - E^*$ is a basis of the original hereditary structure. A subset of E^* is (dual) hereditary if and only if it is a subset of a (dual) basis B^* of E^*.

Lemma 4.1 *E^* is a matroid.*

Proof: Suppose that B_1^* and B_2^* are bases for E^*. Choose $e^* \in B_1^* - B_2^*$ and consider the set $B_1^* - e^*$. We would like to show that there is some

$f^* \in B_2^* - B_1^*$ such that $B_1^* - e^* \cup f^*$ is again a (dual) basis. That is, we want to establish Basis Property 1 for the dual structure.

Let $B_j = E^* - B_j^*$. By definition, B_1 and B_2 are bases of E. Let $f = e^*$. Note that $f \in B_2 - B_1$. By the Basis Property 2 for the original structure, there is some $e \in B_1 - B_2$ such $B_1 - e \cup f$ is a basis for the original structure. Let $f^* = e$. So, we have $f^* = e$ and $e^* = f$. But then

$$E - (B_1 - e \cup f) = B_1^* - e^* \cup f^*$$

is a basis in the dual structure. By construction $f^* = e \subset B_2^* - B_1^*$. This establishes Basis Property 1 for the dual structure. ♠

This abstract notion of the dual fits in perfectly with the notion of duality for planar graphs. Let G be a planar graph and let G^* be the dual planar graph. We get G^* by placing one vertex in each face of G and then joining the vertices of G^* by edges in such a way that each edge of G^* crosses some edge of G once, and each edge of G is crossed once.

Let E denote the set of edges of G and let E^* denote the set of edges of G^*. Note that there is a canonical bijection between E and E^*, defined according to the crossings. So, in a sense, we can consider E and E^* to be the same set. (We could take this common set to be the set of intersection points.)

Lemma 4.2 *Suppose T is some subset of E and T^* is the complementary set of E^*. Then T is a spanning tree for G if and only if T^* is a spanning tree for G^*.*

Proof: If T^* does not span G^* then some cycle in G separates some faces of G from other faces, and this gives rise to a cycle in T. So, T^* spans G^* if and only if T has no cycles. But, since $G^{**} = G$, we see that T spans G if and only if T^* has no cycles. Combining these statements, we see that T spans G *and* has no cycles if and only if T^* spans T^* and has no cycles. But this is equivalent to the statement of the lemma. ♠

Let us think about what the previous lemma says: If we start with the cycle matroid of G and takes its dual, it is the same as taking the cycle matroid of the dual of G. So, one could say that the notion of a dual matroid extends the notion of duality from planar graphs to a general matroid.

Note that the cycle matroid makes sense for any graph, not just a planar graph. So, even though a general graph may not have a well defined dual, we can start with a graph, take the cycle matroid, and then consider the dual cycle matroid. One could view this as a kind of duality for general graphs.

4.1 The Rank Function

Let E be a set with a hereditary structure. Assuming that the independent sets of E are finite, we can define the rank function. Given any subset X, we define $r(X)$ to be the maximum size of an independent subsets of X. When E is a matroid, all the independent sets of X has the same size. However, the definition makes sense even when E is not a matroid. Note that the rank function coincides with the ordinary notion of rank from the vector space and matrix examples.

In a way that is similar to what we did for the basis properties, we mention several properties of the rank function and then show that these are equivalent to the uniformity property for matroids.

1. Given any sets $X, Y \subset E$ we have $r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$.
2. If $A, B \subset E$ and $r(A) = r(A \cup b)$ for any $b \in B$, then $r(A) = r(A \cup B)$.

Lemma 4.3 *If E is a matroid, then the rank function has Property 1.*

Proof: Let I_1 be a maximal independent subset of $X \cap Y$. Since I_1 is also an independent subset of $X \cup Y$, and since all maximal independent subsets of $X \cup Y$ have the same size, there is some maximal independent subset I_2 of $X \cup Y$ which contains I_1. By definition

$$r(X \cap Y) + r(X \cup Y) = |I_1| + |I_2|.$$

Note that $I_2 \cap X$ is independent in X and $I_2 \cap Y$ is independent in Y. Hence

$$r(X) + r(Y) \geq |I_2 \cap X| + |I_2 \cap Y| = |I_2| + |I_1|.$$

The second equality comes from the fact that when we compute the sum $|I_2 \cap X| + |I_2 \cap Y|$ we are double counting the elements of I_1. ♠

Lemma 4.4 *If E has a hereditary structure with Property 1 then E has property 2.*

Proof: For convenience we will give the proof when B is a finite set. The same argument works when B is countably infinite. If you are really interested in the case when B is uncountable, you can use the Axiom of Choice and transfinite induction. But let's not go there.

When B is a single element there is nothing to prove. Suppose we know the result for all cases when B has k elements and we want to prove the result when B has $k+1$ elements. Write $B = B' \cup b$ where b is the $(k+1)$st element. Define

$$X = A \cup b, \qquad Y = A \cup B'.$$

By induction $r(X) = r(Y) = r(A)$. Also, $r(X \cup Y) = r(A)$. Since $A \cup B = X \cup Y$, Property 1 and the information above gives us $r(A \cup B) \leq r(A)$. But certainly $r(A \cup B) \geq r(A)$. Hence $r(A \cup B) = r(A)$. ♠

As an immediate corollary, we see that the rank function of a matroid satisfies both properties.

Lemma 4.5 *If E has a hereditary structure with Property 2 then E is a matroid.*

Proof: Let $X \subset E$. Suppose that I_1 and I_2 are both maximal subsets of E. We want to see that these sets have the same size. Since I_1 is maximal independent set, we see that $I_1 \cup x$ is dependent for any $x \in X - I_1$. But this means that $r(I_1 \cup x) \leq r(I_1)$. Since $r(I_1 \cup x) \geq r(I_1)$ as well, we must have $r(I_1 \cup x) = r(I_1)$. Property 2 now shows that $r(X) = r(I_1)$. But $r(I_1) = |I_1|$. Hence $|I_1| = r(X)$. But the same argument applies to I_2 and gives $|I_2| = r(X)$. Hence $|I_1| = |I_2|$. ♠

Now we know that the rank function of a matroid satisfies both properties above, and that either property suffices to define a matroid.

4.2 Circuits

A *circuit* in a matroid is a minimal dependent set. In other words, a circuit is a dependent set but any subset of a circuit is an independent set. Referring to the cycle matroid, the circuits are exactly the cycles in the graph.

Let us establish two more properties of matroids:

1. If C_1 and C_2 are two distinct circuits and $x \in C_1 \cap C_2$, then $C_1 \cup C_2 - x$ contains another circuit.

2. If I is independent and $e \notin I$, then $I \cup e$ has at most one circuit.

Lemma 4.6 *If E is a matroid, then E has the circuit property 1.*

Proof: We suppose this is false and derive a contradiction. We use Property 1 of the rank function. By definition $C_1 - x$ and $C_2 - x$ are independent. Hence $r(C_j - x) = |C_j| - 1$, for $j = 1, 2$. Hence

$$r(C_1) + r(C_2) = |C_1| + |C_2| - 2.$$

Since C_1 and C_2 are distinct, $C_1 \cap C_2$ is independent. Hence

$$r(C_1 \cap C_2) = |C_1 \cap C_2|.$$

If $C_1 \cup C_2 - x$ is independent then

$$r(C_1 \cup C_2) = |C_1 \cup C_2| - 1.$$

Note also that

$$|C_1| + |C_1| = |C_1 \cap C_2| + |C_1 \cup C_2|.$$

Putting everything together, we see that

$$r(C_1 \cap C_1) + r(C_1 \cup C_2) = |C_1 \cap C_2| + |C_1 \cup C_2| - 1 =$$

$$|C_1| + |C_2| - 1 > r(C_1) - r(C_2).$$

This contradicts the rank Property 1. ♠

Lemma 4.7 *If E is has a hereditary structure with circuit property 1 then E has circuit property 2.*

Proof: Suppose this is false. Let C_1 and C_2 be two distinct circuits of $I \cup e$. Since I is independent, we must have $e \in C_1 \cap C_2$. But then $C_1 \cup C_2 - e$ has a circuit, by property 1. However, $C_1 \cup C_2 - e \subset I$, which is independent. This is a contradiction. ♠

Lemma 4.8 *If E has a heriditary structure with circuit property 2 then E is a matroid.*

Proof: Let B_1 and B_2 be bases for E. We will establish basis property 2. Let $f \in B_2 - B_1$. Note that f is not itself a circuit because f is a subset of a basis. Since $B_1 \cup f$ is dependent, $B_1 \cup f$ has a circuit C_1. Note that C_1 must have some element e of B_1 besides f because f is not itself a circuit. If $B_1 - e \cup f$ has some circuit C_2, then $C_2 \neq C_1$ because C_1 contains e and C_2 does not. This would mean that $B_1 \cup f$ contains 2 distinct circuits, contradicting circuit property 2. Hence $B_1 - e \cup f$ is independent.

Suppose that $B_1 - e \cup f$ is not a basis. Then there is some new element g such that $B_1 - e \cup f \cup g$ is independent. But $B_1 \cup f$ contains the cycle C_1, which has f but not g, and $B_1 \cup g$ contains a cycle which contains g but not f. Hence $C_1 \neq C_2$. Both these cycles belong to

$$(B_1 - e \cup f \cup g) \cup e,$$

and this contradicts the cycle property 2. Hence $B - 1 - e \cup f$ is a basis. ♠

Now we see that a matroid has both cycle properties and either cycle property suffices to define a matroid.

5 Summary

We have proved the following. A set E with a hereditary structure is a matroid if any of the following properties holds:

1. For any $X \subset E$, the maximal independent subsets of X all have the same size.

2. If B_1 and B_2 are bases and $e \in B_1 - B_2$ then there is some $f \in B_2 - B_1$ such that $(B_1 - e) \cup f$ is a basis.

3. If B_1 and B_2 are bases and $f \in B_2 - B_1$ then there is some $e \in B_1 - B_2$ such that $(B_1 - e) \cup f$ is a basis.

4. If I_1 and I_2 are independent sets and $|I_1| < |I_2|$ then there is some $f \in I_2$ such that $I_1 \cup f$ is independent.

5. Given any sets $X, Y \subset E$ we have $r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$.

6. If $A, B \subset E$ and $r(A) = r(A \cup b)$ for any $b \in B$, then $r(A) = r(A \cup B)$.

7. If C_1 and C_2 are two distinct circuits and $x \in C_1 \cap C_2$, then $C_1 \cup C_2 - x$ contains another circuit.

8. If I is independent and $e \notin I$, then $I \cup e$ has at most one circuit.

The reason for having all these equivalent definitions is that in different examples various of the definitions are closer to what we already know about. For instance, bases and rank are very familiar from the linear algebra examples and the circuit examples are very familiar from the graph examples.

In the book, West lists some additional definitions that are equivalent to the ones above. But the list above seems pretty good.