Matroid theory

Kaiser Travis Chan

Euler Circle

8 July 2025

Outline

Definition of a matroid

Definition

A matroid is an ordered pair $\mathcal{M} = (E, \mathcal{I})$, where E is a finite set called the ground set and $\mathcal{I}$ is the set of independent sets, which is composed of some subsets of E such that:

I-1. The empty set is independent.

I-2. If $A \in \mathcal{I}$, then a set $B \subseteq A$ is also independent.

I-3. (independence augmentation property) If $A, B \in \mathcal{I}$ such that $|B| > |A|$, then there is an element $x \in B \setminus A$ where $A \cup \{x\}$ is also independent.

A subset of E that is not independent is called a dependent set.

We also denote the ground set of a matroid $\mathcal{M}$ with $E(\mathcal{M})$.

Vector and affine matroids

In matroids built using linear algebra, the ground sets are column vectors of a matrix A.

Vector and affine matroids

In matroids built using linear algebra, the ground sets are column vectors of a matrix A.

- Vector matroids use linear independence to determine independent sets. The vector matroid of matrix A is denoted as $M[A]$.

Vector and affine matroids

In matroids built using linear algebra, the ground sets are column vectors of a matrix A.

- Vector matroids use linear independence to determine independent sets. The vector matroid of matrix A is denoted as $M[A]$.
- Affine matroids use affine independence to determine independent sets.

Graphic matroids

- A cycle matroid is a matroid built on a graph G where the ground set consists of the edges, and the independent sets are the sets of edges which do not have any cycles in G.
- A graphic matroid is a matroid that is isomorphic to a cycle matroid of a graph.

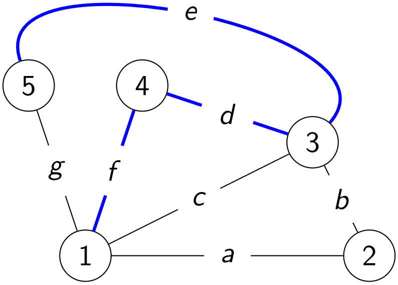

Figure: An example graph H, with an independent set from $M(H)$.

Fano matroid

Proposition

Let $E = \{1, 2, 3, 4, 5, 6, 7\}$ *be the set of points in the Fano plane. Then, let* $\mathcal{I}$ *be the set of sets of points that are not collinear in the Fano plane, which is the projective plane over* $GF(2)$*. Then,* $(E, \mathcal{I})$ *is a matroid and is called the Fano matroid* F_7*.*

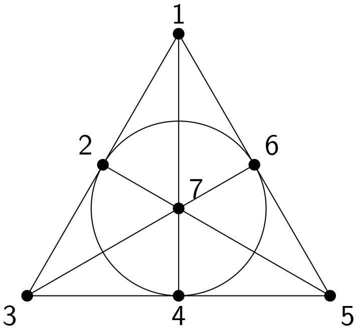

Figure: The Fano matroid F_7.

Other matroids

Proposition

If E is a set with n elements and $\mathcal{I}$ is the set of all subsets A of E such that $|A| \leq r$ for some integer r where $0 \leq r \leq n$, then $U_{r,n} = (E, \mathcal{I})$ is a matroid and is called a uniform matroid.

Other matroids

Proposition

If E is a set with n elements and $\mathcal{I}$ is the set of all subsets A of E such that $|A| \leq r$ for some integer r where $0 \leq r \leq n$, then $U_{r,n} = (E, \mathcal{I})$ is a matroid and is called a uniform matroid.

Proposition

Let $A_1, A_2, A_3, \ldots, A_n$ be disjoint sets, and let $E = A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n$. Then, let $\mathcal{I}$ be the set of all subsets of E that contain zero or one element from each of $A_1, A_2, A_3, \ldots, A_n$. Then, $(E, \mathcal{I})$ is a matroid and is called a transversal matroid.

Bases

Definition

A base of a matroid $\mathcal{M}$ is an independent set of $\mathcal{M}$ with maximal cardinality.

Bases

Definition

A base of a matroid $\mathcal{M}$ is an independent set of $\mathcal{M}$ with maximal cardinality.

Proposition

All bases of a matroid have the same cardinality, called the rank of the matroid, denoted by $r(\mathcal{M})$.

Bases

Lemma

The set of bases $\mathcal{B}$ of a matroid with ground set E satisfies the following properties:

B-1. *The set $\mathcal{B}$ is not empty.*

B-2. *(exchange property) If $B_1, B_2 \in \mathcal{B}$ and $x_1 \in B_1 \setminus B_2$, there exists an element $x_2 \in B_2 \setminus B_1$ such that $B_1 \setminus \{x_1\} \cup \{x_2\}$ is also a base.*

Examples of bases

- In a vector matroid on a matrix A, the bases are the maximal linearly independent sets of columns of A, which are the basis sets of A.

Examples of bases

- In a vector matroid on a matrix A, the bases are the maximal linearly independent sets of columns of A, which are the basis sets of A.
- In a graphic matroid $M(G)$ where G has n vertices, the bases are the spanning trees with n vertices that are subgraphs of G.

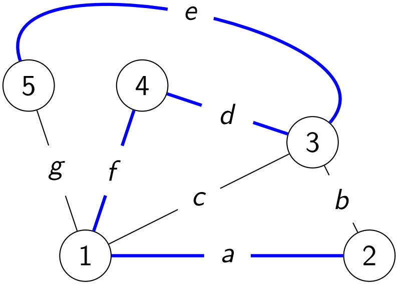

Figure: An example graph H, with a base from $M(H)$.

Circuits

Definition

A circuit is a dependent set of a matroid with minimal cardinality.

Circuits

Definition

A circuit is a dependent set of a matroid with minimal cardinality.

Lemma

The set of circuits $\mathcal{C}$ of a matroid with ground set E satisfies the following properties:

C-1. *The empty set is not a circuit.*

C-2. *If $A \in \mathcal{C}$, then all proper subsets of A are not circuits.*

C-3. *(circuit elimination property) If $C_1, C_2 \in \mathcal{C}$, where $C_1 \neq C_2$, and $x \in C_1 \cap C_2$, then $(C_1 \cup C_2) \setminus \{x\}$ contains a circuit.*

Examples of circuits

- In a vector matroid of a matrix A, the circuits are the minimal linearly dependent sets of column vectors of A.

Examples of circuits

- In a vector matroid of a matrix A, the circuits are the minimal linearly dependent sets of column vectors of A.
- In a graphic matroid $M(G)$, the circuits are the cycles in G with at least one edge. We know that these are of minimal cardinality because if we remove an edge from the cycle, then the resulting subgraph has no cycles.

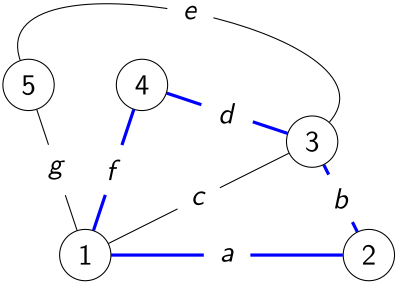

Figure: An example graph H with a circuit from $M(H)$.

The rank function

Definition

The rank function $r_{\mathcal{M}} : 2^E \to \mathbb{N} \cup \{0\}$ of a matroid $\mathcal{M}$ with ground set E is defined such that, if $A \subseteq E$, then $r(A)$ is the cardinality of the largest independent set contained in A. If the matroid being referred to is clear, we usually shorten $r_{\mathcal{M}}$ to r.

The rank function

Definition

The rank function $r_{\mathcal{M}} : 2^E \to \mathbb{N} \cup \{0\}$ of a matroid $\mathcal{M}$ with ground set E is defined such that, if $A \subseteq E$, then $r(A)$ is the cardinality of the largest independent set contained in A. If the matroid being referred to is clear, we usually shorten $r_{\mathcal{M}}$ to r.

Lemma

The rank function r of a matroid with ground set E satisfies the following properties:

R-1. *For a subset A of E, we have $0 \leq r(A) \leq |A|$.*

R-2. *If $A \subseteq B \subseteq E$, then $r(A) \leq r(B)$.*

R-3. *(submodularity property) If $A, B \subseteq E$, we have $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.*

Examples of rank functions

- Let A be a matrix over a field $\mathbb{F}$, and let E be the set of column vectors of A. Then, the rank function of $M[A]$ is given by the rank of the matrix formed by each subset of E.

Examples of rank functions

- Let A be a matrix over a field $\mathbb{F}$, and let E be the set of column vectors of A. Then, the rank function of $M[A]$ is given by the rank of the matrix formed by each subset of E.
- Let G be a graph. Then, the rank function of $M(G)$ is given by the largest number of edges in each subgraph of G that has no cycles.

Duals of graphs

Definition

Let G be a planar graph. The dual of G, denoted by G^*, is constructed by placing a vertex representing every face or region of G, then drawing an edge between pairs of vertices that represent adjacent faces.

Duals of graphs

Definition

Let G be a planar graph. The dual of G, denoted by G^*, is constructed by placing a vertex representing every face or region of G, then drawing an edge between pairs of vertices that represent adjacent faces.

Here, we notice that the spanning trees of G^* are complements of the spanning trees of G.

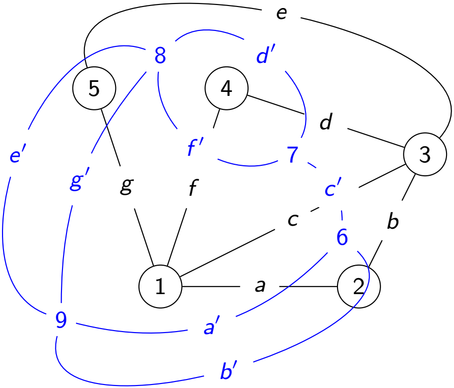

Figure: An example graph H with its dual H^* in blue.

Duals of matroids

Theorem

Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid with $\mathcal{B}$ as the set of its bases. Then, let $\mathcal{B}^* = \{E \setminus x \mid x \in \mathcal{B}\}$ be the set of complements of the elements of $\mathcal{B}$. Then, $\mathcal{B}^*$ is a set of bases of another matroid with ground set E.

The matroid described above is called the dual of $\mathcal{M}$ and is denoted by $\mathcal{M}^*$.

Duals of matroids

Theorem

Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid with $\mathcal{B}$ as the set of its bases. Then, let $\mathcal{B}^* = \{E \setminus x \mid x \in \mathcal{B}\}$ be the set of complements of the elements of $\mathcal{B}$. Then, $\mathcal{B}^*$ is a set of bases of another matroid with ground set E.

The matroid described above is called the dual of $\mathcal{M}$ and is denoted by $\mathcal{M}^*$.

Proposition

Let $\mathcal{M}$ be a matroid. Then, $(\mathcal{M}^*)^* = \mathcal{M}$.

Example of dual matroids

Example

In the uniform matroid $U_{r,n}$, the bases are the subsets of the ground set with r elements, so those of $U^*_{r,n}$ are the subsets of the ground set with $n-r$ elements, therefore $U^*_{r,n} = U_{n-r,n}$. Thus, the dual of a uniform matroid is also a uniform matroid.

Minors of matroids

- Deleting a subset of the ground set is removing its elements from the ground set and all independent sets that have any of those elements.

Minors of matroids

- Deleting a subset of the ground set is removing its elements from the ground set and all independent sets that have any of those elements.
- Contracting a subset of the ground set is deleting that subset in the dual matroid.

Minors of matroids

- Deleting a subset of the ground set is removing its elements from the ground set and all independent sets that have any of those elements.
- Contracting a subset of the ground set is deleting that subset in the dual matroid.
- A minor of a matroid $\mathcal{M}$ is a matroid that can be obtained from $\mathcal{M}$ by a sequence of deletions and contractions.

Minors of matroids

Lemma

Let $\mathcal{M}$ be a matroid with ground set E, and let A and B be disjoint subsets of E. We then have

$$(\mathcal{M} \setminus A) \setminus B = \mathcal{M} \setminus (A \cup B) = (\mathcal{M} \setminus B) \setminus A,$$
$$(\mathcal{M}/A)/B = \mathcal{M}/(A \cup B) = (\mathcal{M}/B)/A,$$
$$(\mathcal{M}/A) \setminus B = (\mathcal{M} \setminus B)/A.$$

Minors of matroids

Lemma

Let $\mathcal{M}$ be a matroid with ground set E, and let A and B be disjoint subsets of E. We then have

$$(\mathcal{M} \setminus A) \setminus B = \mathcal{M} \setminus (A \cup B) = (\mathcal{M} \setminus B) \setminus A,$$
$$(\mathcal{M}/A)/B = \mathcal{M}/(A \cup B) = (\mathcal{M}/B)/A,$$
$$(\mathcal{M}/A) \setminus B = (\mathcal{M} \setminus B)/A.$$

So, any sequence of deletions and contractions can be written as just one deletion and one contraction.

Direct sum of matroids

Proposition

Let $\mathcal{M}_1 = (E_1, \mathcal{I}_1)$ and $\mathcal{M}_2 = (E_2, \mathcal{I}_2)$ be matroids, where E_1 and E_2 are disjoint. Then, define $\mathcal{I}$ to be the set of subsets A of $E_1 \cup E_2$ where $A \cap E_1$ and $A \cap E_2$ are independent in $\mathcal{M}_1$ and $\mathcal{M}_2$, respectively. Then, $(E_1 \cup E_2, \mathcal{I})$ is a matroid and is called the union or direct sum of $\mathcal{M}_1$ and $\mathcal{M}_2$, denoted by $\mathcal{M}_1 \oplus \mathcal{M}_2$.

Representability of matroids

Definition

A matroid with n elements is $\mathbb{F}$-representable if each element of the matroid can be mapped to a column vector in a matrix A with n columns over the field $\mathbb{F}$ so that the column vectors corresponding to the elements in each independent set are linearly independent. The matrix A is called the $\mathbb{F}$-representation of the matroid. Additionally, a matroid is representable if there exists a field $\mathbb{F}$ such that the matroid is $\mathbb{F}$-representable.

Representability of matroids

Definition

A matroid with n elements is $\mathbb{F}$-representable if each element of the matroid can be mapped to a column vector in a matrix A with n columns over the field $\mathbb{F}$ so that the column vectors corresponding to the elements in each independent set are linearly independent. The matrix A is called the $\mathbb{F}$-representation of the matroid. Additionally, a matroid is representable if there exists a field $\mathbb{F}$ such that the matroid is $\mathbb{F}$-representable.

Definition

A matroid is binary if it can be represented over the field $GF(2) = \mathbb{Z}/2\mathbb{Z}$ and ternary if it can be represented over the field $GF(3) = \mathbb{Z}/3\mathbb{Z}$.

Representability of graphic matroids

Definition

Let G be a graph. The *vertex-edge incidence matrix* of G is the matrix that has rows labeled with the vertices of G and the columns labeled with the edges of G. If an edge e in G is a loop (that is, it connects a vertex to itself), then the column corresponding to e is the zero vector. Otherwise, the entry corresponding to vertex v and edge e of G is 1 if v is an end-vertex of e and 0 if it is not.

Representability of graphic matroids

Example

Consider graph H shown to the right. The vertex-edge incidence matrix would then be as follows:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccccc} a & b & c & d & e & f & g \end{array} \\ \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

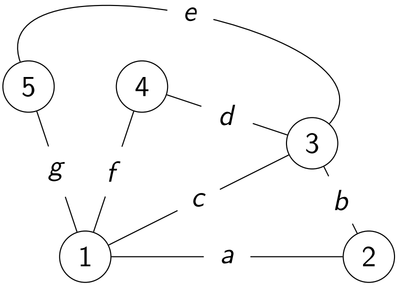

Figure: An example graph H.

Representability of graphic matroids

Theorem

Let $G = (V, E)$ be a graph with vertex-edge incidence matrix A_G. Then, the vector matroid $M[A_G]$ viewed over $GF(2)$ has all subsets of E that do not contain the edges of a cycle in G as its independent sets. Then, $M[A_G] = M(G)$, and $M(G)$ is binary.

The Vámos matroid

Definition

Let $E = \{1, 2, 3, 4, 5, 6, 7, 8\}$ and

$$A = \{\{1, 2, 3, 4\}, \{1, 4, 5, 6\}, \{1, 4, 7, 8\}, \{2, 3, 5, 6\}, \{2, 3, 7, 8\}\}.$$

Then, there exists a matroid $\mathcal{M}$ where all subsets of E with at most three elements are independent, and the five elements of A are the only circuits. This is called the Vámos matroid and is denoted by V_8.

The Vámos matroid

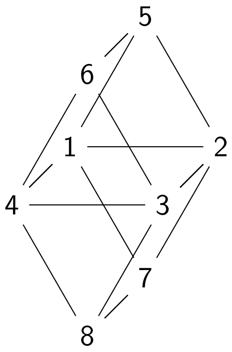

Figure: The Vámos matroid V_8.

The Vámos matroid

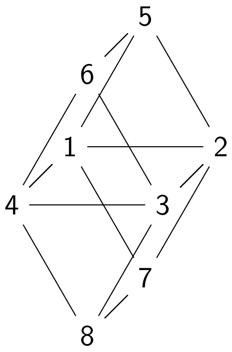

Figure: The Vámos matroid V_8.

Proposition

The Vámos matroid is not representable over any field.

Thank you!