Theory of matroids and applications I

J.L. Ramírez Alfonsín

Institut Montpelliérain Alexander Grothendieck,
Université de Montpellier, France

Curso : Introducción a la Teoría de Matroides,
Valladolid, Spain, March, 2025

Independents

A matroid M is an ordered pair $(E, \mathcal{I})$ where E is a finite set $(E = \{1, \ldots, n\})$ and $\mathcal{I}$ is a family of subsets of E verifying the following conditions :

($I1$) $\emptyset \in \mathcal{I}$,

($I2$) If $I \in \mathcal{I}$ and $I' \subset I$ then $I' \in \mathcal{I}$,

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

The members in $\mathcal{I}$ are called the independents of M. A subset in E not belonging to $\mathcal{I}$ is called dependent.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.
By contradiction, suppose that $I_1 \cup e$ is linearly <u>dependent</u> for any $e \in I_2 \backslash I_1$.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.
By contradiction, suppose that $I_1 \cup e$ is linearly dependent for any $e \in I_2 \backslash I_1$. Let W the space generated by I_1 and I_2.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.
By contradiction, suppose that $I_1 \cup e$ is linearly dependent for any $e \in I_2 \backslash I_1$. Let W the space generated by I_1 and I_2.
On one hand, $dim(W) \geq |I_2|$,

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.
By contradiction, suppose that $I_1 \cup e$ is linearly dependent for any $e \in I_2 \backslash I_1$. Let W the space generated by I_1 and I_2.
On one hand, $dim(W) \geq |I_2|$, on the other hand W is contained in the space generated by I_1.

Representable Matroids

Theorem (Whitney 1935) Let $\{e_1, \ldots, e_n\}$ a set of columns (vectors) of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the family of subsets $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independent in $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

Proof : $(I1)$ et $(I2)$ are trivial.
$(I3)$ Let $I_1', I_2' \in \mathcal{I}$ such that the corresponding columns, say I_1 et I_2, are linearly independent with $|I_1| < |I_2|$.
By contradiction, suppose that $I_1 \cup e$ is linearly dependent for any $e \in I_2 \backslash I_1$. Let W the space generated by I_1 and I_2.
On one hand, $dim(W) \geq |I_2|$, on the other hand W is contained in the space generated by I_1.

$$|I_2| \leq dim(W) \leq |I_1| < |I_2| \quad !!!$$

Representable Matroids

Let A be the following matrix with coefficients in $\mathbb{R}$.

$$A = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

$\{\emptyset, \{1\}, \{2\}, \{4\}, \{4\}, \{5\}, \{1,2\}, \{1,5\}, \{2,4\}, \{2,5\}, \{4,5\}\} \subseteq \mathcal{I}(M)$

A matroid obtained form a matrix A with coefficients in $\mathbb{F}$ is denoted by $M(A)$ and is called representable over $\mathbb{F}$ or $\mathbb{F}$-representable.

Circuits

A subset $X \subseteq E$ is said to be minimal dependent if any proper subset of X is independent. A minimal dependent set of matroid M is called circuit of M.
We denote by $\mathcal{C}$ the set of circuits of a matroid.

Circuits

A subset $X \subseteq E$ is said to be minimal dependent if any proper subset of X is independent. A minimal dependent set of matroid M is called circuit of M.
We denote by $\mathcal{C}$ the set of circuits of a matroid.

$\mathcal{C}$ is the set of circuits of a matriod on E if and only if $\mathcal{C}$ verifies the following properties :

$(C1)$ $\emptyset \notin \mathcal{C}$,

$(C2)$ $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$ then $C_1 = C_2$,

$(C3)$ (elimination property) If $C_1, C_2 \in \mathcal{C}, C_1 \neq C_2$ and $e \in C_1 \cap C_2$ then there exists $C_3 \in \mathcal{C}$ such that $C_3 \subseteq \{C_1 \cup C_2\} \backslash \{e\}$.

Graphic Matroid

Let $G = (V, E)$ be a graph. A cycle in G is a closed walk without repeated vertices.

Graphic Matroid

Let $G = (V, E)$ be a graph. A cycle in G is a closed walk without repeated vertices.

Theorem The set of cycles in a graph $G = (V, E)$ is the set of circuits of a matroid on E.

Graphic Matroid

Let $G = (V, E)$ be a graph. A cycle in G is a closed walk without repeated vertices.

Theorem The set of cycles in a graph $G = (V, E)$ is the set of circuits of a matroid on E.

Proof : Verify $(C1), (C2)$ and $(C3)$ [Exercise].

Graphic Matroid

Let $G = (V, E)$ be a graph. A cycle in G is a closed walk without repeated vertices.

Theorem The set of cycles in a graph $G = (V, E)$ is the set of circuits of a matroid on E.

Proof : Verify $(C1), (C2)$ and $(C3)$ [Exercise].

This matroid is denoted by $M(G)$ and called graphic.

Graphic Matroid

Let $G = (V, E)$ be a graph. A cycle in G is a closed walk without repeated vertices.

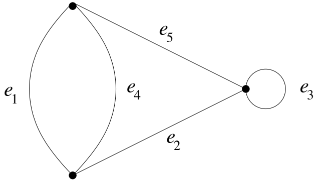
Theorem The set of cycles in a graph $G = (V, E)$ is the set of circuits of a matroid on E.

Proof : Verify $(C1), (C2)$ and $(C3)$ [Exercise].

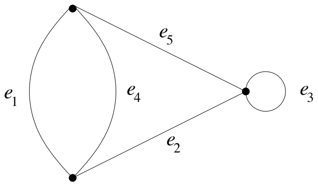
This matroid is denoted by $M(G)$ and called graphic.

A subset of edges $I \subset \{e_1, \ldots, e_n\}$ of G is independent if the graph induced by I does not contain a cycle.

Graphic Matroid



Graphic Matroid

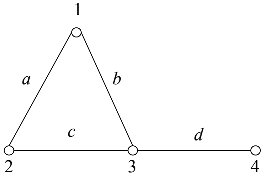


It can be checked that $M(G)$ is isomorphic to $M(A)$ (under the bijection $e_i \to i$).

$$A = \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \left(\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{array} \right) \end{array}$$

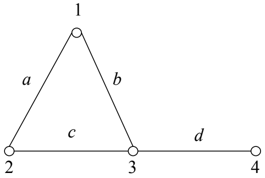
Graphic Matroid

G



$$A = \begin{array}{c} \\ \\ \end{array} \begin{array}{c} \begin{array}{cccc} \;\;y_a & \;\;y_b & \;\;y_c & \;\;y_d \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{array}$$

Graphic Matroid

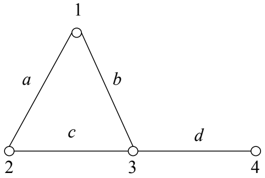
G 

$$A = \begin{array}{c} \begin{array}{cccc} y_a & y_b & y_c & y_d \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{array}$$

$M(G)$ is isomorphic to $M(A)$ $(a \to y_a, b \to y_b, c \to y_c, d \to y_d)$.

Graphic Matroid

G



$$A = \begin{array}{c} \begin{array}{cccc} y_a & y_b & y_c & y_d \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{array}$$

$M(G)$ is isomorphic to $M(A)$ ($a \to y_a, b \to y_b, c \to y_c, d \to y_d$).

The cycle formed by the edges $a = \{1,2\}, b = \{1,3\}$ et $c = \{2,3\}$ in the graph correspond to the linear dependency $y_b - y_a = y_c$.

Bases

A base of a matroid is a maximal independent set.
We denote by $\mathcal{B}$ the set of all bases of a matroid.

Bases

A base of a matroid is a maximal independent set.
We denote by $\mathcal{B}$ the set of all bases of a matroid.
Lemma The bases of a matroid have the same cardinality.
[Exercice]

Bases

A base of a matroid is a maximal independent set.
We denote by $\mathcal{B}$ the set of all bases of a matroid.
Lemma The bases of a matroid have the same cardinality.
[Exercice]

The family $\mathcal{B}$ verifies the following conditions :

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

$(B2)$ (exchange property) $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \backslash B_2$ then there exist $y \in B_2 \backslash B_1$ such that $(B_1 \backslash x) \cup y \in \mathcal{B}$.

Bases

A base of a matroid is a maximal independent set.

We denote by $\mathcal{B}$ the set of all bases of a matroid.

Lemma The bases of a matroid have the same cardinality.

[Exercice]

The family $\mathcal{B}$ verifies the following conditions :

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

$(B2)$ (exchange property) $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \backslash B_2$ then there exist $y \in B_2 \backslash B_1$ such that $(B_1 \backslash x) \cup y \in \mathcal{B}$.

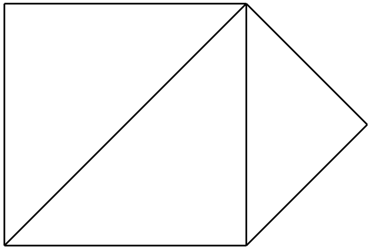
If $\mathcal{I}$ is the family of subsets contained in a set of $\mathcal{B}$ then $(E, \mathcal{I})$ is a matroid.

Bases

Theorem $\mathcal{B}$ is the set of basis of a matroid if and only if it verifies $(B1)$ and $(B2)$. [Exercise]

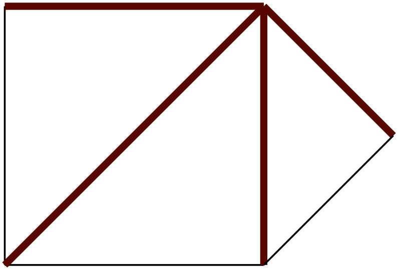
Bases

Theorem $\mathcal{B}$ is the set of basis of a matroid if and only if it verifies $(B1)$ and $(B2)$. [Exercise]

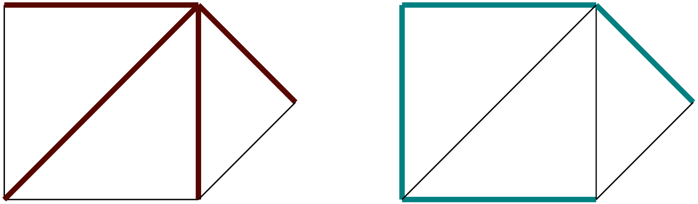


Bases

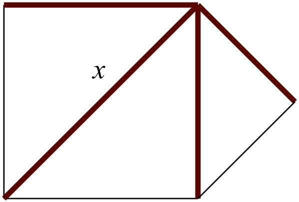
Spanning tree of G

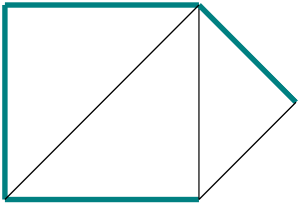


Bases

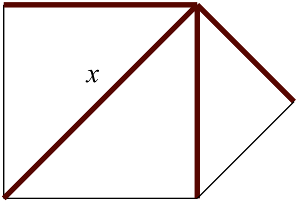


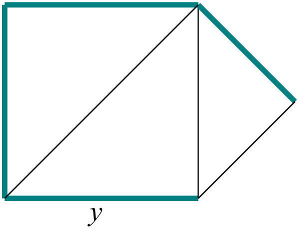
Bases



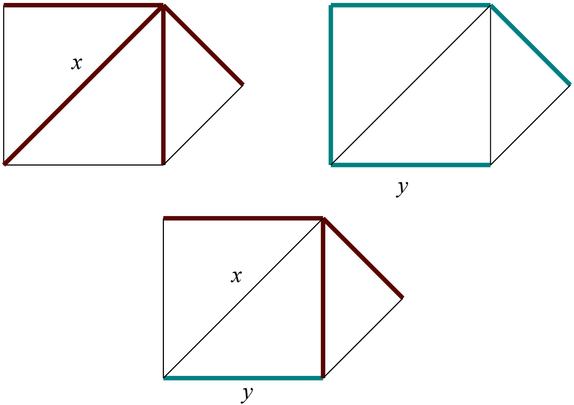


Bases





Bases



Application 1 : Secrete sharing scheme

≪ Imagine that the code of a vault is shared by three different persons. We want that the combination can only be found if at least two of the three persons are present and that no single person can reconstruct the combination by his/her own ≫.

Application 1 : Secrete sharing scheme

≪ Imagine that the code of a vault is shared by three different persons. We want that the combination can only be found if at least two of the three persons are present and that no single person can reconstruct the combination by his/her own ≫.

Shamir's scheme In this scheme, any t out of n shares may be used to recover the secret. The system relies on the idea that one can construct a unique polynomial P of degree $t-1$, find n points (shares) on the curve (we give one to each of the persons), such that each of the t points lies on P (Lagrange's interpolation principle).

Application 1 : Secrete sharing

Secrete sharing scheme

- assume that the secret is held by a dealer, and each share is sent privately to a different participant

- a subset of participants is authorized if their shares determine the secret value

- the access structure of a secret sharing scheme is the family of authorized subsets

- if the size of each share is equal to the size of the secret, then the scheme (or access structure) is ideal. This is the optimal situation for perfect schemes.

Application 1 : Secrete sharing

A matroid port is an access structure whose minimal authorized groups are in correspondence with the circuits of a matroid containing a fixed elements.

Application 1 : Secrete sharing

A matroid port is an access structure whose minimal authorized groups are in correspondence with the circuits of a matroid containing a fixed elements.

Theorem (Brickell, Davenport, 1991) Every ideal access structure is a matroid port.

Application 1 : Secrete sharing

A matroid port is an access structure whose minimal authorized groups are in correspondence with the circuits of a matroid containing a fixed elements.

Theorem (Brickell, Davenport, 1991) Every ideal access structure is a matroid port.

Theorem (Brickell, Davenport, 1991) If an access structure is a matroid port of a representable matroid, then the access structure is ideal.

Rank

The rank of a set $X \subseteq E$ is defined by

$$r_M(X) = \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

Rank

The rank of a set $X \subseteq E$ is defined by

$$r_M(X) = \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

$r = r_M$ is the rank function of a matroid $(E, \mathcal{I})$ (where $\mathcal{I} = \{I \subseteq E : r(I) = |I|\}$) if and only if r verifies the following conditions :

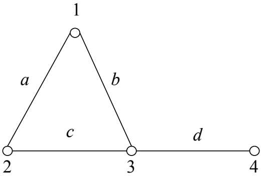
$(R1)$ $0 \leq r(X) \leq |X|$, for all $X \subseteq E$,

$(R2)$ $r(X) \leq r(Y)$, for all $X \subseteq Y$,

$(R3)$ (sub-modulairity) $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$ for all $X, Y \subset E$.

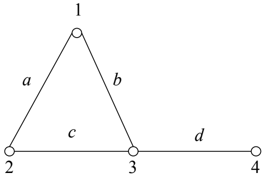
Rank

Let M be a graphic matroid obtained from G



Rank

Let M be a graphic matroid obtained from G



It can be verified that :
$r_M(\{a,b,c\}) = r_M(\{c,d\}) = r_M(\{a,d\}) = 2$ and
$r(M(G)) = r_M(\{a,b,c,d\}) = 3.$

Greedy Algorithm

Let $\mathcal{I}$ be a set of subsets of E verifying $(I1)$ and $(I2)$.
Let $w : E \to \mathbb{R}$, and let $w(X) = \sum_{x \in X} w(x), X \subseteq E, w(\emptyset) = 0$.

Greedy Algorithm

Let $\mathcal{I}$ be a set of subsets of E verifying $(I1)$ and $(I2)$.
Let $w : E \to \mathbb{R}$, and let $w(X) = \sum_{x \in X} w(x), X \subseteq E, w(\emptyset) = 0$.

An optimization problem consist of finding a maximal set B of $\mathcal{I}$ with maximal weight (or minimal).

Greedy algorithm for $(\mathcal{I}, w)$

$X_0 = \emptyset$
$j = 0$
While there is $e \in E \backslash X_j \ : \ X_j \cup \{e\} \in \mathcal{I}$ **do**
    Choose an element e_{j+1} of maximal weight
    $X_{j+1} \leftarrow X_j \cup \{e_{j+1}\}$
    $j \leftarrow j + 1$
$B_G \leftarrow X_j$
Return B_G

Greedy Algorithm

Theorem $(\mathcal{I}, E)$ is a matroid if and only if the following conditions are verified :

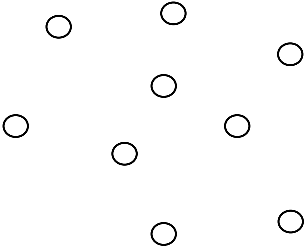
($I1$) $\emptyset \in \mathcal{I}$,

($I2$) $I \in \mathcal{I}, I' \subseteq I \Rightarrow I' \in \mathcal{I}$,

(G) For any function $w : E \to \mathbb{R}$, the greedy algorithm gives a maximal set of $\mathcal{I}$ of maximal weight.

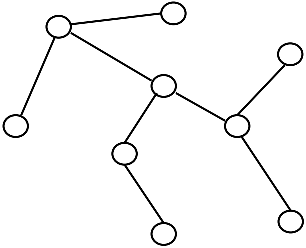
Application 2 : Spanning tree of minimal weight

We want to construct a network (of minimal cost) connecting the 9 cities.



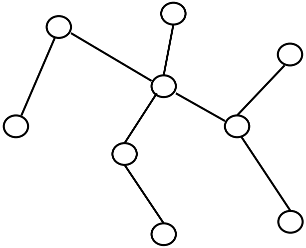
Application 2 : Spanning tree of minimal weight

We want to construct a network (of minimal cost) connecting the 9 cities.



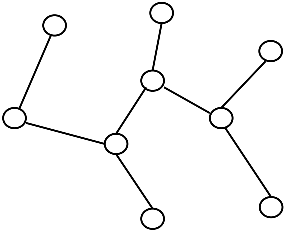
Application 2 : Spanning tree of minimal weight

We want to construct a network (of minimal cost) connecting the 9 cities.



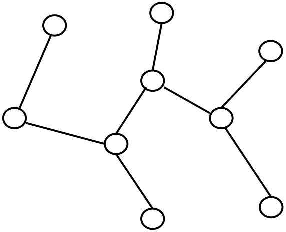
Application 2 : Spanning tree of minimal weight

We want to construct a network (of minimal cost) connecting the 9 cities.



Application 2 : Spanning tree of minimal weight

We want to construct a network (of minimal cost) connecting the 9 cities.



Theorem (Cayley) There exist n^{n-2} labeled trees on n vertices. [Exercise]

Application 2 : Spanning tree of minimal weight

Theorem (Kruskal) Given a complete graph with weights on the edges there exist a polynomial time algorithm that finds a spanning tree of minimal weight.

Application 2 : Spanning tree of minimal weight

Theorem (Kruskal) Given a complete graph with weights on the edges there exist a polynomial time algorithm that finds a spanning tree of minimal weight.

Indeed, the greedy algorithm returns a base (maximal independent) of minimal weight by considering the graphic matroid associated to a complete graph and $w(e)$, $e \in E(G)$ is the the weight of each edge.

Transversal Matroid

Let $S = \{e_1, \ldots, e_n\}$ and let $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$, $n \geq k$.

Transversal Matroid

Let $S = \{e_1, \ldots, e_n\}$ and let $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$, $n \geq k$.
A transversal of $\mathcal{A}$ is a subset $\{e_{j_1}, \ldots, e_{j_k}\}$ of S such that $e_{j_i} \in A_i$.

Transversal Matroid

Let $S = \{e_1, \ldots, e_n\}$ and let $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$, $n \geq k$.

A transversal of $\mathcal{A}$ is a subset $\{e_{j_1}, \ldots, e_{j_k}\}$ of S such that $e_{j_i} \in A_i$.

A set $X \subseteq S$ is called partial transversal of $\mathcal{A}$ if there exists $\{i_1, \ldots, i_l\} \subseteq \{1, \ldots, k\}$ such that X is a transversal of $\{A_{i_1}, \ldots, A_{i_l}\}$.

Transversal Matroid

Let $S = \{e_1, \ldots, e_n\}$ and let $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$, $n \geq k$.

A transversal of $\mathcal{A}$ is a subset $\{e_{j_1}, \ldots, e_{j_k}\}$ of S such that $e_{j_i} \in A_i$.

A set $X \subseteq S$ is called partial transversal of $\mathcal{A}$ if there exists $\{i_1, \ldots, i_l\} \subseteq \{1, \ldots, k\}$ such that X is a transversal of $\{A_{i_1}, \ldots, A_{i_l}\}$.

The collection $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$ is said to be the presentation of the transversal matroid.

Transversal matroid : bipartite graph

Let $G = (S, \mathcal{A}; E)$ be a bipartite graph constructed from $S = \{e_1, \ldots, e_n\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}$ and two vertices $e_i \in S$, $A_j \in \mathcal{A}$ are adjacent if and only if $e_i \in A_j$.

Let $G = (S, \mathcal{A}; E)$ be a bipartite graph constructed from $S = \{e_1, \ldots, e_n\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}$ and two vertices $e_i \in S$, $A_j \in \mathcal{A}$ are adjacent if and only if $e_i \in A_j$.

A matching in a graph is a set of edges without common vertices.

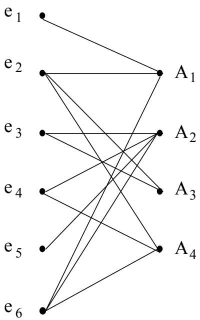
A partial transversal in $\mathcal{A}$ correspond to a matching in $G = (S, \mathcal{A}; E)$.

Transversal matroid : example

$E = \{e_1, \ldots, e_6\}$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ with $A_1 = \{e_1, e_2, e_6\}$, $A_2 = \{e_3, e_4, e_5, e_6\}$, $A_3 = \{e_2, e_3\}$ and $A_4 = \{e_2, e_4, e_6\}$.

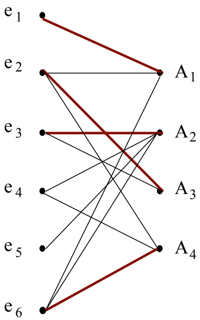
Transversal matroid : example

$E = \{e_1, \ldots, e_6\}$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ with $A_1 = \{e_1, e_2, e_6\}$, $A_2 = \{e_3, e_4, e_5, e_6\}$, $A_3 = \{e_2, e_3\}$ and $A_4 = \{e_2, e_4, e_6\}$.



Transversal matroid : example

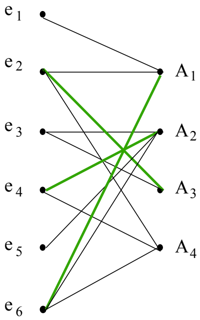
$E = \{e_1, \ldots, e_6\}$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ with $A_1 = \{e_1, e_2, e_6\}$, $A_2 = \{e_3, e_4, e_5, e_6\}$, $A_3 = \{e_2, e_3\}$ and $A_4 = \{e_2, e_4, e_6\}$.



$\{e_1, e_3, e_2, e_6\}$ is a transversal of $\mathcal{A}$.

Transversal matroid : example

$E = \{e_1, \ldots, e_6\}$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ with $A_1 = \{e_1, e_2, e_6\}$, $A_2 = \{e_3, e_4, e_5, e_6\}$, $A_3 = \{e_2, e_3\}$ and $A_4 = \{e_2, e_4, e_6\}$.



$X = \{e_6, e_4, e_2\}$ is a partial transversal of $\mathcal{A}$ since X is a transversal of $\{A_1, A_2, A_3\}$.

Transversal Matroid

Theorem Let $S = \{e_1, \ldots, e_n\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$. Then, the set of partial transversals of $\mathcal{A}$ is the set of independents of a matroid. [Exercise].

Transversal Matroid

Theorem Let $S = \{e_1, \ldots, e_n\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$. Then, the set of partial transversals of $\mathcal{A}$ is the set of independents of a matroid. [Exercise].

Such matroid is called transversal matroid.

Application 3 : Assignment problem

Let $\{t_i\}$ be a set of tasks ordered according to their importance (priority).

Application 3 : Assignment problem

Let $\{t_i\}$ be a set of tasks ordered according to their importance (priority).

Let $\{e_i\}$ be a set of agents each able to perform one or more of the these tasks.

Application 3 : Assignment problem

Let $\{t_i\}$ be a set of tasks ordered according to their importance (priority).

Let $\{e_i\}$ be a set of agents each able to perform one or more of the these tasks.

The tasks are all done at the same time (and thus each agent can perform one task at the time).

Application 3 : Assignment problem

Let $\{t_i\}$ be a set of tasks ordered according to their importance (priority).

Let $\{e_i\}$ be a set of agents each able to perform one or more of the these tasks.

The tasks are all done at the same time (and thus each agent can perform one task at the time).

Problem : Assign the tasks to the agents in an optimal way (maximizing the priorities).

Application 3 : Assignment problem

- tasks : $\{t_1, t_2, t_3, t_4\}$.

Application 3 : Assignment problem

- tasks : $\{t_1, t_2, t_3, t_4\}$.
- priorities : $w(t_1) = 10, w(t_2) = 3, w(t_3) = 3$ and $w(t_4) = 5$.

Application 3 : Assignment problem

- tasks : $\{t_1, t_2, t_3, t_4\}$.
- priorities : $w(t_1) = 10, w(t_2) = 3, w(t_3) = 3$ and $w(t_4) = 5$.
- agents :

e_1 able to perform tasks t_1 and t_2,
e_2 able to perform tasks t_2 and t_3,
e_3 able to perform task t_4.

Application 3 : Assignment problem

- tasks : $\{t_1, t_2, t_3, t_4\}$.
- priorities : $w(t_1) = 10, w(t_2) = 3, w(t_3) = 3$ and $w(t_4) = 5$.
- agents :

e_1 able to perform tasks t_1 and t_2,
e_2 able to perform tasks t_2 and t_3,
e_3 able to perform task t_4.

- Transversal Matroid $M = (\mathcal{I}, \{t_1, t_2, t_3, t_4\})$ where $\mathcal{I}$ is given by the set of matchings of the bipartite graph $G = (U, V; E)$ with $U = \{t_1, t_2, t_3, t_4\}$, $V = \{e_1, e_2, e_3\}$.

Application 3 : Assignment problem

- tasks : $\{t_1, t_2, t_3, t_4\}$.
- priorities : $w(t_1) = 10, w(t_2) = 3, w(t_3) = 3$ and $w(t_4) = 5$.
- agents :

e_1 able to perform tasks t_1 and t_2,
e_2 able to perform tasks t_2 and t_3,
e_3 able to perform task t_4.

- Transversal Matroid $M = (\mathcal{I}, \{t_1, t_2, t_3, t_4\})$ where $\mathcal{I}$ is given by the set of matchings of the bipartite graph $G = (U, V; E)$ with $U = \{t_1, t_2, t_3, t_4\}$, $V = \{e_1, e_2, e_3\}$.

- By applying the greedy algorithm to M we have $X_0 = \emptyset, X_1 = \{t_1\}, X_2 = \{t_1, t_4\}$ and $X_3 = \{t_1, t_4, t_2\}$.

Matroid polytope

Let $M = (\mathcal{B}, E)$ be a matroid with $|E| = n$.

Matroid polytope

Let $M = (\mathcal{B}, E)$ be a matroid with $|E| = n$.
Let v_B be the characteristic vector of B.

Matroid polytope

Let $M = (\mathcal{B}, E)$ be a matroid with $|E| = n$.
Let v_B be the characteristic vector of B.
The Matroid polytope is defined as

$$P_M = conv\{v_B : B \in \mathcal{B}\}$$

Matroid polytope

Let $M = (\mathcal{B}, E)$ be a matroid with $|E| = n$.
Let v_B be the characteristic vector of B.
The Matroid polytope is defined as

$$P_M = conv\{v_B : B \in \mathcal{B}\}$$

Remark $dim(P_M) \leq n - 1$

Matroid polytope

Let $M = (\mathcal{B}, E)$ be a matroid with $|E| = n$.
Let v_B be the characteristic vector of B.
The Matroid polytope is defined as

$$P_M = conv\{v_B : B \in \mathcal{B}\}$$

Remark $dim(P_M) \leq n - 1$

Let Δ_E be the standard simplex in $\mathbb{R}^E$, i.e.,

$$\Delta_E = \{x \in \mathbb{R}^E : \sum_{i \in E} x_i = 1 \text{ and } x_i \geq 0 \text{ for any } i \in E\}.$$

Matroid polytope : characterization

Theorem (Gel'fand, Goresky, MacPherson, Serganova, 1987) Let $P \subseteq \mathbb{R}^E$ be a polytope. Then, P is a matroid polytope if and only if :

a) $P \subseteq r\Delta_E$,
b) the vertices of P belong to $\{1, 0\}^E$ and
c) each edge of P is a translation of $conv(e_i, e_j)$ with $i, j \in E, i \neq j$.

Uniform matroid

Example : The uniform matroid $U_{r,n}$ of rank r on n elements has a set of bases $\mathcal{B}(U_{r,n}) = \{Y \subset [n] : |Y| = r\}$.

Uniform matroid

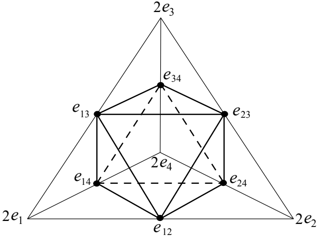
Example : The uniform matroid $U_{r,n}$ of rank r on n elements has a set of bases $\mathcal{B}(U_{r,n}) = \{Y \subset [n] : |Y| = r\}$.

$$P_{U_{2,4}} = conv \left\{ \begin{pmatrix} 1\\1\\0\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\1\\0 \end{pmatrix}, \begin{pmatrix} 1\\0\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\1\\1\\0 \end{pmatrix}, \begin{pmatrix} 0\\1\\0\\1 \end{pmatrix}, \begin{pmatrix} 0\\0\\1\\1 \end{pmatrix} \right\} \subset \mathbb{R}^4.$$

Uniform matroid

Example : The uniform matroid $U_{r,n}$ of rank r on n elements has a set of bases $\mathcal{B}(U_{r,n}) = \{Y \subset [n] : |Y| = r\}$.

$$P_{U_{2,4}} = conv\left\{\begin{pmatrix}1\\1\\0\\0\end{pmatrix},\begin{pmatrix}1\\0\\1\\0\end{pmatrix},\begin{pmatrix}1\\0\\0\\1\end{pmatrix},\begin{pmatrix}0\\1\\1\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\\1\end{pmatrix},\begin{pmatrix}0\\0\\1\\1\end{pmatrix}\right\} \subset \mathbb{R}^4.$$



Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$

where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$

where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Appearing in different contexts :

Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$

where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Appearing in different contexts :

- Lafforgue's work while studying the compactifications of the fine Schubert cell of the Grassmannian. This implies that for a matroid M represented by vectors in $\mathbb{F}^r$, if P_M is indecomposable, then M will be rigid, that is, M will have only finitely many realizations, up to scaling and the action of $GL(r, \mathbb{F})$,

Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$
where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Appearing in different contexts :

- Lafforgue's work while studying the compactifications of the fine Schubert cell of the Grassmannian. This implies that for a matroid M represented by vectors in $\mathbb{F}^r$, if P_M is indecomposable, then M will be rigid, that is, M will have only finitely many realizations, up to scaling and the action of $GL(r, \mathbb{F})$,

- compactification of the moduli space of hyperplane arrangements,

Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$

where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Appearing in different contexts :

- Lafforgue's work while studying the compactifications of the fine Schubert cell of the Grassmannian. This implies that for a matroid M represented by vectors in $\mathbb{F}^r$, if P_M is indecomposable, then M will be rigid, that is, M will have only finitely many realizations, up to scaling and the action of $GL(r, \mathbb{F})$,

- compactification of the moduli space of hyperplane arrangements,

- tropical linear spaces,

Application 4 : Polytope decomposition

P_M is decomposable if $P_M = \bigcup_{i=1}^{t} P_{M_i}$

where P_{M_i} is also a matroid polytope for each $1 \leq i \neq j \leq t$ and the intersection $P_{M_i} \cap P_{M_j}$ is a face of both P_{M_i} and P_{M_j}.

Appearing in different contexts :

- Lafforgue's work while studying the compactifications of the fine Schubert cell of the Grassmannian. This implies that for a matroid M represented by vectors in $\mathbb{F}^r$, if P_M is indecomposable, then M will be rigid, that is, M will have only finitely many realizations, up to scaling and the action of $GL(r, \mathbb{F})$,

- compactification of the moduli space of hyperplane arrangements,

- tropical linear spaces,

- quasisymmetric functions, etc.

Hyperplane split

A decomposition of P_M is called hyperplane split if $t = 2$.

Hyperplane split

A decomposition of P_M is called hyperplane split if $t = 2$.
Let (E_1, E_2) be a partition of $E = E_1 \cup E_2$. Let $r_i > 1, i = 1, 2$ be the rank of $M|_{E_i}$.

(E_1, E_2) is a good partition if there are integers $0 < a_1 < r_1$ et $0 < a_2 < r_2$ such that

(P1) $r_1 + r_2 = r + a_1 + a_2$

(P2) for all $X \in \mathcal{I}(M|_{E_1})$ with $|X| \leq r_1 - a_1$ and
for all $Y \in \mathcal{I}(M|_{E_2})$ with $|Y| \leq r_2 - a_2$
we have $X \cup Y \in \mathcal{I}(M)$.

Lemma Let (E_1, E_2) be a good partition of E. Let

$$\mathcal{B}(M_1) = \{B \in \mathcal{B}(M) : |B \cap E_1| \leq r_1 - a_1\}$$

$$\mathcal{B}(M_2) = \{B \in \mathcal{B}(M) : |B \cap E_2| \leq r_2 - a_2\}$$

where r_i is the rank of $M|_{E_i}$ and a_i verifying (P1) and (P2).

Then, $\mathcal{B}(M_1)$ and $\mathcal{B}(M_2)$ are collection of bases of matroids, say M_1 and M_2.

Lemma Let (E_1, E_2) be a good partition of E. Let

$$\mathcal{B}(M_1) = \{B \in \mathcal{B}(M) : |B \cap E_1| \leq r_1 - a_1\}$$

$$\mathcal{B}(M_2) = \{B \in \mathcal{B}(M) : |B \cap E_2| \leq r_2 - a_2\}$$

where r_i is the rank of $M|_{E_i}$ and a_i verifying (P1) and (P2).

Then, $\mathcal{B}(M_1)$ and $\mathcal{B}(M_2)$ are collection of bases of matroids, say M_1 and M_2.

Theorem (Chatelain, R.A. 2011) Let $M = (E, \mathcal{B})$ be a matroid. Then, $P(M) = P(M_1) \cup P(M_2)$.

Lemma Let (E_1, E_2) be a good partition of E. Let

$$\mathcal{B}(M_1) = \{B \in \mathcal{B}(M) : |B \cap E_1| \leq r_1 - a_1\}$$

$$\mathcal{B}(M_2) = \{B \in \mathcal{B}(M) : |B \cap E_2| \leq r_2 - a_2\}$$

where r_i is the rank of $M|_{E_i}$ and a_i verifying (P1) and (P2).

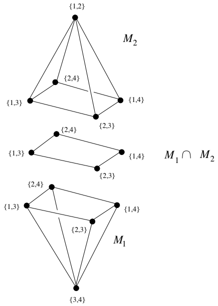
Then, $\mathcal{B}(M_1)$ and $\mathcal{B}(M_2)$ are collection of bases of matroids, say M_1 and M_2.

Theorem (Chatelain, R.A. 2011) Let $M = (E, \mathcal{B})$ be a matroid. Then, $P(M) = P(M_1) \cup P(M_2)$.

Corollary (Chatelain, R.A. 2011) Let $n \geq r + 2 \geq 4$ be integers and let $h(U_{r,n})$ the number of different hyperplane splits of $P(U_{r,n})$. Then, $h(U_{r,n}) \geq \left\lfloor \frac{n}{2} \right\rfloor - 1$.

Example

Consider the uniform matroid $U_{2,4}$. Then $E_1 = \{1,2\}$ and $E_2 = \{3,4\}$ is a good partition with $a_1 = a_2 = 1$.
$\mathcal{B}(M_1) = \{\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$,
$\mathcal{B}(M_2) = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$ and
$\mathcal{B}(M_1) \cap \mathcal{B}(M_2) = \{\{1,3\},\{1,4\},\{2,3\},\{2,4\}\}$



Lattice Path Matroid

A lattice path starts at point $(0,0)$ and uses steps $(1,0)$ and $(0,1)$, called East and North.

Lattice Path Matroid

A lattice path starts at point $(0, 0)$ and uses steps $(1, 0)$ and $(0, 1)$, called East and North.

Let $P = p_1, \ldots, p_{r+m}$ and $Q = q_1, \ldots, q_{r+m}$ be two lattice paths from $(0, 0)$ to (m, r) with P never going above Q.

Lattice Path Matroid

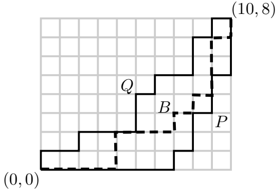
A lattice path starts at point $(0,0)$ and uses steps $(1,0)$ and $(0,1)$, called East and North.
Let $P = p_1, \dots, p_{r+m}$ and $Q = q_1, \dots, q_{r+m}$ be two lattice paths from $(0,0)$ to (m,r) with P never going above Q.
Let $\{p_{s_1}, \dots, p_{s_r}\}$ be the set of North steps of P, $s_1 < \dots < s_r$ and $\{q_{t_1}, \dots, q_{t_r}\}$ be the set of North steps of Q, $t_1 < \dots < t_r$.
We have $t_i < s_i$ for all i.

Lattice Path Matroid

A lattice path starts at point $(0,0)$ and uses steps $(1,0)$ and $(0,1)$, called East and North.
Let $P = p_1, \ldots, p_{r+m}$ and $Q = q_1, \ldots, q_{r+m}$ be two lattice paths from $(0,0)$ to (m,r) with P never going above Q.
Let $\{p_{s_1}, \ldots, p_{s_r}\}$ be the set of North steps of P, $s_1 < \cdots < s_r$ and $\{q_{t_1}, \ldots, q_{t_r}\}$ be the set of North steps of Q, $t_1 < \cdots < t_r$.
We have $t_i < s_i$ for all i.
Let $M[P,Q]$ be the transversal matroid on $\{1, \ldots, m+r\}$ and presentation $[t_i, s_i]$. $M[P,Q]$ is called lattice path matroid (Bonin, de Mier, Noy 2002).

Lattice Path Matroid

A lattice path starts at point $(0,0)$ and uses steps $(1,0)$ and $(0,1)$, called East and North.
Let $P = p_1, \ldots, p_{r+m}$ and $Q = q_1, \ldots, q_{r+m}$ be two lattice paths from $(0,0)$ to (m,r) with P never going above Q.
Let $\{p_{s_1}, \ldots, p_{s_r}\}$ be the set of North steps of P, $s_1 < \cdots < s_r$ and $\{q_{t_1}, \ldots, q_{t_r}\}$ be the set of North steps of Q, $t_1 < \cdots < t_r$.
We have $t_i < s_i$ for all i.
Let $M[P,Q]$ be the transversal matroid on $\{1, \ldots, m+r\}$ and presentation $[t_i, s_i]$. $M[P,Q]$ is called lattice path matroid (Bonin, de Mier, Noy 2002).



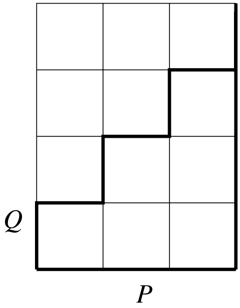
$$\begin{aligned}
A_8 &= \{17, 18\} \\
A_7 &= \{15, 16, 17\} \\
A_6 &= \{14, 15, 16\} \\
A_5 &= \{11, 12, 13, 14\} \\
A_4 &= \{9, 10, 11, 12, 13\} \\
A_3 &= \{8, 9, 10, 11\} \\
A_2 &= \{4, 5, 6, 7, 8, 9, 10\} \\
A_1 &= \{1, 2, 3, 4, 5, 6, 7, 8\}
\end{aligned}$$

$$Q = \{1, 4, 8, 9, 11, 14, 15, 17\}$$
$$Q = NEENEEENNENEEENNENE$$

$$B = \{5, 6, 10, 12, 14, 15, 16, 18\}$$
$$B = EEEENNEEENENENNNEN$$

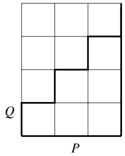
$$P = \{8, 10, 11, 13, 14, 16, 17, 18\}$$
$$P = EEEEEEENENNENNENNN$$

Let $m = 3$ and $r = 4$ and let $M[Q, P]$ be the matroid on $\{1, \ldots, 7\}$ with presentation $(N_i : i \in \{1, \ldots, 4\})$ where $N_1 = [1, 2, 3, 4]$, $N_2 = [3, 4, 5]$, $N_3 = [5, 6]$ and $N_4 = [7]$.



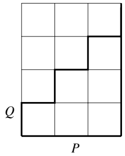
Hyperplan split for lattice path matroids

Hyperplane split for $M[P, Q]$



Hyperplan split for lattice path matroids

Hyperplane split for $M[P, Q]$



(a) M_1, (b) M_2 and (c) $M_1 \cap M_2$.