LECTURE ON MATROID THEORY AND APPLICATIONS

JORGE RAMÍREZ ALFONSÍN

Abstract. A *matroid* is a combinatorial structure that can be defined by keeping the main 'set properties' of the linear dependency in vector spaces. Matroids satisfy several equivalent axioms and have a fundamental notion of duality giving the right setting to study a number of classical problems. In this notes, we give a basic introduction of the theory of matroids as well as some applications.

Contents

This notes were prepared for the 22nd National School on Algebra, Algebraic and Combinatorial Applications of Toric Ideals, Bucharest, Romania, September 2014.

1. Introduction

The word of *matroid* appears for the first time in the fundamental paper due to Whitney in 1935 [16]. In this paper, the structure of a matroid was introduced as the set abstraction of the dependency relations between the column vectors of a matrix (explaining the suffix 'oid' indicating that is a structure coming from a matrix). The applications of matroids have their origins in the area of combinatorics (graphs, discrete optimisation, polytopes, etc.). For the last thirty years, many other applications of matroid have appeared in many other differents areas as algebraic geometry, stratification of grassmanniennes, discrete geometry, etc. We recommend the reader the book [9] for further details on matroid theory.

2. Axioms

Matroids can be characterized by various different equivalent axioms.

2.1. **Independents.** A *matroid* M is an ordered couple $(E, \mathcal{I})$ where E is a finite set ($E = \{1, \ldots, n\}$) and $\mathcal{I}$ is a collection of subsets of E verifying the following

- $(I1)$ $\emptyset \in \mathcal{I}$,
- $(I2)$ If $I_1 \in \mathcal{I}$ and $I_2 \subset I_1$ then $I_2 \in \mathcal{I}$,
- $(I3)$ *(augmentation property)* If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$ then there exist $e \in I_2 \backslash I_1$ such that $I_1 \cup e \in \mathcal{I}$.

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

Example 2.1. Let $\{e_1, \ldots, e_n\}$ be the set of column vectors of a matrix with coefficients in a field $\mathbb{F}$. Let $\mathcal{I}$ be the collection of all the subsets of $\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} = E$ such that the set of columns $\{e_{i_1}, \ldots, e_{i_m}\}$ are linearly independente on $\mathbb{F}$. Then, $(E, \mathcal{I})$ is a matroid.

A matroid that is isomorpic to a matroid obtained from a matrix over a field $\mathbb{F}$ is called *representable* ou *linear* over $\mathbb{F}$.

Example 2.2. Let A be the following matrix with coefficients in $\mathbb{R}$

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

We have that $\mathcal{I}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{2,4\}, \{3,4\}, \{2,3\}\}$.

2.2. **Circuits.** A subset $X \subseteq E$ is said to be *minimal dependent* if any subset of X, different from X, is independent. A minimal dependent subset of a matroid M is called a *circuit* of M. We denote by $\mathcal{C}$ the set of circuits of a matroid. We observe that $\mathcal{I}$ can be determined by $\mathcal{C}$ (the membres of $\mathcal{I}$ are all the subsets of E not containing a member of $\mathcal{C}$). A circuit of cardinality one is called *loop*.

We have that $\mathcal{C}$ is a set of circuits of a matroid 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 $C_3 \subseteq \{C_1 \cup C_2\} \backslash \{e\}$.

Example 2.3. In the graph $G = (V, E)$, we call *cycle* the set of edges in a cycle of G, and *simple* cycle if such a set is minimal by inclusion. Here, we consider only simple cycles. Let $G = (V, E)$ be a graph and let $\mathcal{C}$ be the set of cycles of G. Then, $\mathcal{C}$ is the set of circuits of a matroid on E, denoted by $M(G)$. A matroid obtained on this way is called *graphic matroid*.

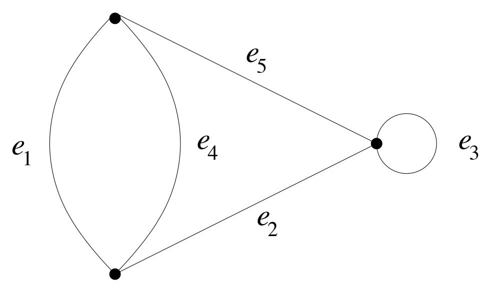


FIGURE 1. Graph with 3 verticess

Remark 2.4. There is not the notion of vertex in a matroid. The matroid associated to a graph do not determine, in general, the graph. For instance, any connected graph without cycle has the same matroid. The associated matroid determine the graph if and only if the graph is *3-connected*.

Example 2.5. Let $M(G)$ be the graphic matroid obtained from graph G in Figure 1, and let A be the matrix over $\mathbb{R}$ given in Exemple 2.2. We can verify that $M(G)$ is isomorphic to $M(A)$ (under the bijection $e_i \to i$).

Remark 2.6. It turns out that a graphic matroid is always linear. Let $G = (V, E)$ be a graph and $\{x_i,\ i \in V\}$ the canonique bases of a vector space over an arbitrary field. We can verify that, as in Example 2.5, the graph $G = (V, E)$ is associated to the same matroid as the set of vectors $x_i - x_j$ pour $(i, j) \in E$.

Example 2.7. Let $M(G')$ be the graphic matroid obtained from graph G' in Figure 2. Let A' be the matrix obtained by following the construction of Remark 2.6.

$$A' = \begin{array}{c} \begin{array}{cccc} x_1 & x_2 & x_3 & x_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \end{array}$$

We can check that $M(G')$ is isomorphic to $M(A')$ (under the bijection $x_i \to i$). Notice that the cycle formed by the edges $a = \{1, 2\}, b = \{1, 3\}$ et $c = \{2, 3\}$ in the graph G' correspond to the linear dependency $x_2 - x_1 = x_3$.

2.3. **Bases.** A *base* of a matroid is a independ set maximal by inclusion. All the bases of a matroid have the same cardinality (the same number of elements). Indeed, otherwise, we would have two bases B_1, B_2 with $|B_1| < |B_2|$ and so, by $(I3)$ there exist $x \in B_2 \backslash B_1$ such that $B_1 \cup x \in \mathcal{I}$ which is a contradiction since B_1 is a maximal independent.

The collection $\mathcal{B}$ of bases verify the following conditions

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

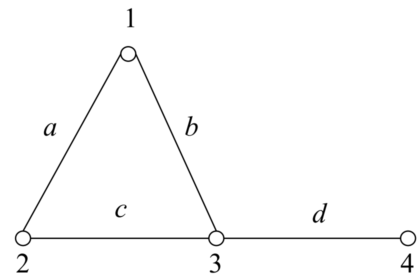


FIGURE 2. Graph G'

(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 collection of subsets contained in one of the members of $\mathcal{B}$ then $(E, \mathcal{I})$ is a matroid.

Remark 2.8. If G is a connected graph then the bases of $M(G)$ correspond to the set of all spanning trees of G.

2.4. **Rank.** Let $M = (E, \mathcal{I})$ and $X \subseteq E$. The *rank* of X, denoted by $r_M(X)$, is the cardinality of the largest independent contained in X, that is,

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

Equivalently, we define the set $\mathcal{I} \backslash X = \{I \subseteq X | I \in \mathcal{I}\}$. Then, $(X, \mathcal{I} \backslash X)$ is a matroid, denoted by $M|_X$ and called *restriction of M to X*. The rank $r_M(X)$ of X is the cardinality of a base in $M|_X$.

It can be proved that $r = r_M$ is the rank function of a matroid $(E, \mathcal{I})$ where

$$\mathcal{I} = \{I \subseteq E : r(I) = |I|\},$$

if and only if r verify 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-modularity)* $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$ for all $X, Y \subset E$.

2.5. **Closure.** The *closure* of a set X in M is defined by

$$cl(X) = \{x \in E | r(X \cup x) = r(X)\}.$$

It can be proved that the function $cl : \mathcal{P}(E) \to \mathcal{P}(E)$ is the closure function of a matroid if and only if cl verify the following conditions

(CL1) *(extensivity)* If $X \subseteq E$ then $X \subseteq cl(X)$.
(CL2) *(increasing)* If $X \subseteq Y \subseteq E$ then $cl(X) \subseteq cl(Y)$.
(CL3) *(indempotent)* If $X \subseteq E$ then $cl(cl(X)) = cl(X)$.
(CL4) *(exchange property)* If $X \subseteq E, x \in E$ and $y \in cl(X \cup x) - cl(X)$ then $x \in cl(X \cup y)$.

Let $X \subset E$, $cl(X)$ is also called *flat* of X. X is said to be *closed* if $X = cl(X)$. The set E is a closed set of rank r_M. The rank 0 closed sets are formed by the loops of M. A closed set of rank 1 or *point* is the class of *parallel* elements. A matroid such that $\emptyset$ is a closed set and all its points contain only one element, is called *simple*. A *hyperplan* is a closed set of rank $r_M - 1$.

Example 2.9. Let $M(G')$ be a graphic matroid obtained from graph G' in Figure 2. It can be verified that : $r(\{a,b,c\}) = r(\{c,d\}) = r(\{a,d\}) = 2$ and $cl\{a,b\} = \{a,b,c\}$.

2.6. **Greedy Algorithm.** Let $\mathcal{I}$ be a set of subsets of E verifying $(I1)$ and $(I2)$. Let $w : E \to \mathbb{R}$ ($w(e)$ is said to be the *weight* of element e). Let $w(X) = \sum_{x \in X} w(x)$ for $X \subseteq E$, and $w(\emptyset) = 0$.

An *optimization problem* consist to find a maximal set B of $\mathcal{I}$ with maximal weight.

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

$X_0 = \emptyset$
$j = 0$
While there exist $e \in E \backslash X_j$ such that $X_j \cup \{e\} \in \mathcal{I}$ **do**
    Choose an element e_{j+1} of maximum weight
    $X_{j+1} \leftarrow X_j \cup \{e_{j+1}\}$
    $j \leftarrow j+1$
$B \leftarrow X_j$
Output B

We can characterize a matroid by using the greedy algorithm. Indeed, $(\mathcal{I}, E)$ 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 output a maximal set of $\mathcal{I}$ of maximal weight.

3. Applications : combinatorial optimisation

3.1. **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 $e_{j_i} \in A_i$ (that is, there exist a bijection between $\{e_{j_1}, \ldots, e_{j_k}\}$ and $\{A_1, \ldots, A_k\}$). A set $X \subseteq S$ is said to be a *partial transversal* of $\mathcal{A}$ if there exists $\{i_1, \ldots, i_l\} \subseteq \{1, \ldots, k\}$ such that X is a transversal of $\{A_{i_1}, \ldots, A_{i_l}\}$.

Let $G = (U, V; E)$ be a bipartite graph formed from $S = \{s_1, \ldots, s_n\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$ where $U = \{u_1, \ldots, u_n\}$, $V = \{v_1, \ldots, v_k\}$ and two vertices $u_i \in U$ and $v_j \in V$ are adjacents if and only if $s_i \in A_j$. We thus have that a set X is a partial transversal of $\mathcal{A}$ if and only if there exists a matching of $G = (U, V; E)$ where each edge of the matching has a vertex of U corresponding to one of the elements of X, see Figure 3.

Example 3.1. Let $E = \{e_1, \ldots, e_6\}$ and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ with $A_1 = \{e_1, e_2, e_6\}$, $A_2 = \{e_3, e_4, e_5, e_6\}$, $A_3 = \{e_2, e_3\}$ et $A_4 = \{e_2, e_4, e_6\}$. Then, $\{e_1, e_3, e_2, e_6\}$ is a transversal of $\mathcal{A}$ and $X = \{e_6, e_4, e_2\}$ is a partial transversal of $\mathcal{A}$ since X is a transversal of $\{A_1, A_2, A_3\}$, see Figure 3.

It can be proved [9] that if $E = \{e_1, \ldots, e_n\}$ and if $\mathcal{A} = \{A_1, \ldots, A_k\}, A_i \subseteq S$ then the set of partial transversals of $\mathcal{A}$ is the set of independents of a matroid. Such a matroid is called *transversal*.

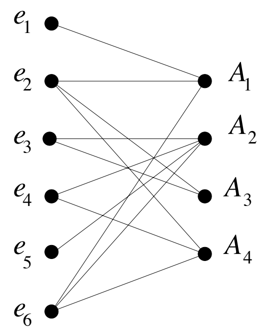


FIGURE 3. Example of a transversal set

3.2. **Assigment Problem.** Let $\{T_i\}$ be a set of works ordered by their importance (priority) and let $\{E_i\}$ a set of employees capable to do one or various of these works. We suppose that the works will be done at the same time (and thus each employee can do just one work each time). The problem is to assign the works to the employees in a optimal way (maximizing the priorities).

The problem can be solved by applying the greedy algorithm to the transversal matroid M where $S = \{T_i\}$ and $\mathcal{A} = \{A_1, \ldots, A_k\}$ with A_i the set of works for which employee i is qualified. We notice that the maximal number of works that can be done at the same time is equals to the biggest partial transversal of $\mathcal{A}$ with $w : S \to \mathbb{R}$ the function corresponding to the importance of the works.

Example 3.2. We have four works $\{t_1, t_2, t_3, t_4\}$ to be done, each with a priority given by the weights : $w(t_1) = 10, w(t_2) = 3, w(t_3) = 3$ and $w(t_4) = 5$. These works can be done by three employees e_1, e_2 and e_3 : employee e_1 is capable to do works t_1 et t_2, employee e_2 is capable to do works t_2 et t_3, and employee e_3 is capable to do work t_4. Let $M = (\mathcal{I}, w)$ be the transversal matroid with $\mathcal{I}$ is the set of matchings of the bipartite graph $G = (U, V; E)$ where $U = \{t_1, t_2, t_3, t_4\}$, $V = \{e_1, e_2, e_3\}$ and $t_i \in U$ et $e_j \in V$ are adjacent if and only if employee e_j is capable to do work t_i. By applying the greedy algorithm to M it is obtained $X_0 = \emptyset, X_1 = \{t_1\}, X_2 = \{t_1, t_4\}$ and $X_3 = \{t_1, t_4, t_2\}$.

4. DUALITY

Let M be a matroid on E and $\mathcal{B}$ the set of bases of M. Then,

$$\mathcal{B}^* = \{E \backslash B \mid B \in \mathcal{B}\}$$

is the set of bases of a matroid on E.
The matroid on E having $\mathcal{B}^*$ as set of bases, denoted by M^*, is called *dual* of M. A base in M^* is also called a *cobase* of M. It is clear that

$$r(M^*) = |E| - r_M \text{ and } M^{**} = M.$$

Moreover the set $\mathcal{I}^*$ of independents of M^* is given by

$$\mathcal{I}^* = \{X \mid X \subset E \text{ such that there exist } B \in \mathcal{B} \text{ with } X \cap B = \emptyset\},$$

and the rank function of M^* is given by

$$r_{M^*}(X) = |X| + r_M(E \backslash X) - r_M,$$

for $X \subset E$.

The family $\mathcal{C}^*$ of circuits of M^* is the set of subsets $D \subset E$ such that $D \cap B \neq \emptyset$ for any base $B \in \mathcal{B}$ and D is minimal by inclusion with this property.

A circuit of M^* is also called *cocircuit* of M and a cocircuit of cardinality one is called an *isthme* of M. It turns out that the cocircuits of a matroid M are the complements of the hyperplans in the set of elements, i.e.

$$\mathcal{C}^* = \{E \backslash H \mid H \in \mathcal{H}\}$$

where $\mathcal{H}$ is the set of hyperplanes of M.
Of course, the cocircuits of a matroid verify the same axioms as the circuits (see Section 2.2).

4.1. **Graphic matroids.** Let $G = (V, E)$ be a graph. A *cocycle*, or *cut*, of G is a set of edges joining the two parts of a partition of the set of vertices of G. A cocycle is *simple* if and only if it is minimal by inclusion. Here, we only consider simple cocycles.

It is known that X is a cocycle of $G = (E, V)$ if and only if X a minimal subset of E having a non empty intersection with each generating forest of G. Thus, if $\mathcal{C}(G)^*$ is the set of simple cocycles of a graph G then $\mathcal{C}(G)^*$ is the set of circuits of a matroid of E, called *bond* (or *cocycle*) matroid of G, denoted by $B(G)$. We have

$$M^*(G) = B(G) \text{ and } M(G) = B^*(G).$$

A natural question is the following one : is it true that if M is graphic then M^* is also graphic ? For instance, if $M = M(K_4)$ where K_4 is the complete graph on 4 vertices then M^* is also graphic since $M(K_4) = M^*(K_4)$. This property is not true in general, for example, $M^*(K_5)$ is not graphic. However, this property is true if and only if G is planar, that is when G admit a dual graph (see Figure 5 for an example). In this case, we have

$$M^*(G) = M(G^*).$$

4.2. **Minors.** Let M be a matroid on E and $A \subset E$. Then, the set of independents of a matroid on $E \backslash A$ is given by

$$\{X \subset E \backslash A \mid X \text{ est un independent of } M\}$$

This matroid is obtained from M by *deleting* the elements of A. Such a matroid is denoted by $M \backslash A = M|_{E \backslash A}$. In order to give the elements $M \backslash A$, we might also use the notation $M(E \backslash A)$. Moreover, the circuits of $M \backslash A$ are the circuits of M contained in $E \backslash A$ and for $X \subset E \backslash A$, we have $r_{M \backslash A}(X) = r_M(X)$.

Let M be a matroid on E, $A \subset E$ and $X \subset E \backslash A$. The following properties are equivalents.
(i) There exist a base B of $M|_A$ such that $X \cup B$ is independent
(ii) For any base B of $M|_A$ the set $X \cup B$ is independent.
(iii) The set of independents of a matroid on $E \backslash A$ is

$$\{X \subset E \backslash A \mid \text{there exists a base } B \text{ of } M|_A \text{ such that } X \cup B \text{ is independent in } M\}$$

This matroid is obtained from M by *contracting* the elements of A. Such matroid is denoted by M/A. Moreover, the circuits of M/A are the nonempty sets minimals by inclusion of the form $C \backslash A$ for C circuit of M. For $X \subset E \backslash A$, we have $r_{M/A}(X) = r_M(X \cup A) - r_M(A)$.

In the case when A consist of one element $A = \{e\}$ for $e \in E$, we simplify notation by $M \backslash e$ et M/e. The matroids $M \backslash e$ are M/e are sometimes called two *principal minors* of M defined by e. Notice that $M \backslash e = M/e$ when e is either an isthme or a loop.

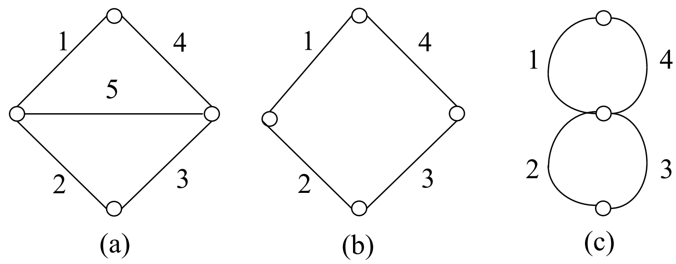


FIGURE 4. (a) G; (b) $G \setminus 5$ and (c) $G/5$.

In a general way, a *minor* of a matroid M is any matroid obtained from M by a sequence of deletions and contractions.

The operations deletion and contraction are associative and comutative, that is,

$$(M \backslash A) \backslash A' = M \backslash (A \cup A'),$$
$$(M/A)/A' = M/(A \cup A')$$

and

$$(M \backslash A)/A' = (M/A') \backslash A.$$

So, any minor of M is of the form

$$M \backslash A/B = M/B \backslash A,$$

for $A, B \subset E$ disjoint.

The operations deletion and contraction are duals, that is,

$$(M \backslash A)^* = (M^*)/A \text{ and } (M/A)^* = (M^*) \backslash A.$$

Example 4.1. Let r and n be integers $0 \leq r \leq n$ and $E = \{1, \ldots, n\}$. Then, $\mathcal{I} = \binom{E}{r}$ the set of r-sets of E is the set of independents of a matroid, denoted by $U_{n,r}$ and called *uniform matroid.* Let $T \subseteq E$ with $|T| = t$. then,

$$U_{n,r} \backslash T = \begin{cases} U_{n-t,n-t} \text{ if } & n \geq t \geq n-r, \\ U_{n-t,r} \text{ if } & t < n-r. \end{cases}$$

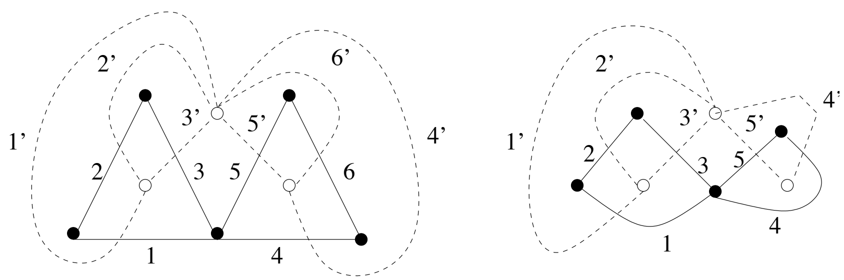
We have

$$U_{n,r}^* \backslash T = U_{n,n-r} \backslash T = \begin{cases} U_{n-t,n-t} \text{ if } & n \geq t \geq r, \\ U_{n-r,n-t} \text{ if } & t < r, \end{cases}$$

and thus

$$U_{n,r}/T = (U_{n,n-r} \backslash T)^* = \begin{cases} (U_{n-t,n-t})^* = U_{0,n-t} \text{ if } & n \geq t \geq r, \\ (U_{n-r,n-t})^* = U_{r-t,n-t} \text{ if } & t < r. \end{cases}$$

Example 4.2. In the graphic case, the notions of minors of the associated matroid coincide with the usual notions on graphs. More precisely, let $G = (V, E)$ be a graph and let $T \subseteq E$. It can be verified that $M(G) \backslash T = M(G \backslash T)$ and $M(G)/T = M(G/T)$, see Figure 4.



(a) (b)

FIGURE 5. (a) G and its dual G^* ; (b) $G^* \setminus 6'$ and $(G^* \setminus 6)^* = G/6$.

Therefore, we have that any minor of a graphic matroid is graphic. This property is not true for other classes of matroids, for instance, it is not true for transversal matroids. Figure 5 illustrate a planar graph, its dual and the deleting and contraction operation of an edge.

5. Representable matroids

Let $\mathbb{F}$ be a field, $d \geq 1$ an integer, E a finite set and $\mathcal{V} = (v_e)_{e \in E}$ a family of vectors of $\mathbb{F}^d$ with index on E. We have already seen that

$$\mathcal{I} = \{X \subset E \mid \text{ the vectors } v_e,\ e \in X, \text{ are linearly independent on } \mathbb{F}\}$$

is the set of independents of a matroid on E, called $\mathbb{F}$-representables, or representable over $\mathbb{F}$.

Example 5.1. *Matroid of Fano* $\mathbf{F}_7$. Figure 6. The matroid $\mathbf{F}_7$ is the finite projective plan of order $m = 2$. By the classical formula [6] it has $m^2+m+1 = 7$ elements. It can be verified that $\mathbf{F}_7$ is the matroid of linear dependances on $\mathbb{Z}_2$ of 7 non zero vectors of $\mathbb{Z}_2^3$, that is the linear dependences on $\mathbb{Z}_2$ of the columns of matrix B. On the contrary, this matroid is not representable over $\mathbb{R}$.

$$\begin{array}{cc} & \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ B = & \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Remark 5.2. If M is defined by the vectors given by the columns $(I \mid A)$ of size $r \times n$, where I_r is the identity $r \times r$ (their columns is an arbitray base on E) and A is the matrix $r \times (n-r)$, then the dual matroid M^* is defined by the vector columns of the matrix $(-{}^tA \mid I_{n-r})$ where I_{n-r} is the identity $(n-r) \times (n-r)$ and ${}^tA$ the transpose of A. Some authors call M^* the *orthogonal* matroid of M since the duality for representable matroids is a generalization of the notion of orthogonality in vector spaces. Indeed, let V be a subspace of $\mathbb{F}^E$. We recall that the *orthogonal espace* $V^\perp$ is defined from the canonical interior product $\langle u, v \rangle = \sum_{e \in E} u(e)v(e)$ by

$$V^\perp = \{v \in \mathbb{F}^E \mid \langle u, v \rangle = 0 \text{ for any } u \in V\}.$$

It is known [9, Proposition 2.2.23] that the orthogonal espace generated by the column vectors of $(I \mid A)$ is given by the espace generated by the column vectors of $(-{}^tA \mid I_{n-r})$.

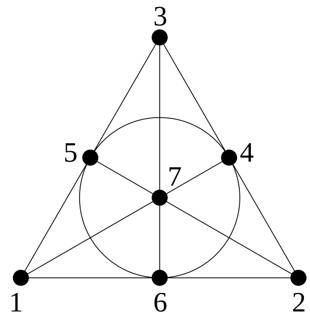


FIGURE 6. Affine representation of Fano matroid $\mathbf{F}_7$ in the plane. $\mathbf{F}_7$ is a rank 3 matroid with 7 elements where three form a base if and only if they are not on the same line. The line 456 is represented by a circle. It is representable over $\mathbb{Z}_2$ (represented by matrix B), but it is not representable over $\mathbb{R}$.

.

By Remark 5.2 we have that the dual of a representable matroid M in a field $\mathbb{F}$ is also representable in $\mathbb{F}$. We also have that any minor of a representable over a field $\mathbb{F}$ is also representable over $\mathbb{F}$. Indeed, the deletion of an element is just the deletion of the corresponding column in the matrix, and thus still representable in $\mathbb{F}$. For the contraction, we can simply apply deletion and contraction, that is, contracting an element comes down to take the dual matroid (that is representable in $\mathbb{F}$) delete an element (obtaining a representable matroid in $\mathbb{F}$) and then take the its dual (that is again representable in $\mathbb{F}$).
The property to be representable in a field $\mathbb{F}$ is thus kept by taking minors. For any field $\mathbb{F}$ there exist a list of *excluded minors*, that is, not representable matroids in $\mathbb{F}$ but where any proper minor is representable over $\mathbb{F}$. The determination of a list of *excluded minors for* $\mathbb{F}$ constitute a characterization of representable matroids over $\mathbb{F}$: *a matroid is representable over* $\mathbb{F}$ *if and only if none of its minors is on the list of excluded minors over* $\mathbb{F}$.

- For $\mathbb{F} = \mathbb{R}$, the list of exclded minors is infinite [9], and it looks difficult to determine it.
- For $\mathbb{F} = GF(2) = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$: the list is reduced to one mtaroid $U_{2,4}$ [13, 14].
- For $\mathbb{F} = GF(3) = \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$: the list has 4 matroids F_7 F_7^* $U_{2,5}$ $U_{3,5}$ [7].
- For $\mathbb{F} = GF(4)$: the list has 8 matroids described explicitely in [5].

A big open question is the follwoing one : *Is the list of excluded minors finite for a given finite field ?*

We finally note that there exist nonrepresentable matroids (that is, over any field), a classical example is the rank 3 matroid obtained from the configuration of Non-Pappus, see Figure 7.

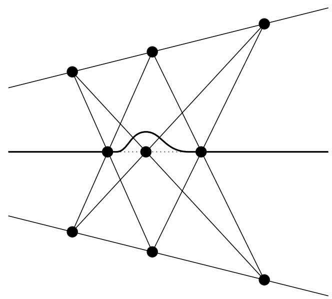


FIGURE 7. Non-Pappus. The matroid is defined on the 9 represented points. The points over the same line form a circuits. In the vectorial case, the three points in the middle are necessarily aligned (Pappus Theorem). Here (Non-Pappus) we decide that this three points form a base instead of a circuit. We still obtain a matroid but not representable over any field (see Section 5).

6. Regular matroids

A matroid representable over any field $\mathbb{F}$ is called *regular*. For example, graphic matroids are regular (see Remark 2.6). In general, regular matroids are equivalent to *totally unimodular matrices*[1].

Since any minor of a regular matroid is regular (by the results given in Section 5), we can characterize regular matroids by a list of excluded minors. By a theorem due to Tutte [13, 14] this list is finite having 3 matroids : $U_{2,4}$, F_7 et F_7^*.

7. Union of matroids

Let $M_1, M_2, \ldots, M_k$ $k \geq 2$ be matroids on E, and let $\mathcal{I}_i$ be the set of independents of M_i for $i = 1, 2, \ldots, k$. Let us set

$$\mathcal{I} = \{X_1 \cup X_2 \cup \cdots \cup X_k \mid X_i \in \mathcal{I}_i \text{ for } i = 1, 2, \ldots, k\}$$

Nash-Williams [8] proved that $\mathcal{I}$ is the set of independents of a matroid on E, called *union of matroids* $(M_i)_{i=1,2,\ldots,k}$ and denoted $M_1 \vee M_2 \vee \cdots \vee M_k$.
The rank function of $M_1 \vee M_2 \vee \cdots \vee M_k$ for any $A \subset E$ is given by

$$r_{M_1 \vee M_2 \vee \cdots \vee M_k}(A) = \min_{X \subset A} \left(\sum_{i=1}^{i=k} r_i(X) + |A \backslash X| \right).$$

The assumption that the matroids M_i are on the same set is by commodity. Without lost of generality, we can always come back to this case. Indeed, if the matroids M_i are on different sets E_i, we set $E = \bigcup_{i=1}^{k} E_i$. For $i = 1, \ldots, k$, we define the matroid $\widetilde{M_i}$ on E by the conditions $\widetilde{M_i}(E_i) = M_i$ and $r_{\widetilde{M_i}}(e) = 0$ for $e \in E \backslash E_i$, that is, we extend M_i to E by adding loops. Clearly, the set $\mathcal{I}$ do not change while passing from M_i to $\widetilde{M_i}$.
One of a number of consequences of the union of matroids is the well-kwon intersection Theorem due to Edmonds [4] stating that for any integer k, there exist $X \in \mathcal{I}_1 \cap \mathcal{I}_2$ such that $|X| \geq k$ if and only if $r_1(A) + r_2(E \backslash A) \geq k$ for any $A \subset E$.

[1]A *modular* matrix is a square matrix with integers coefficients having determinant equals to -1 or 1. A *totally modular* matrix is a matrix with coefficients 0,1,-1 where the determinat of all square submatrices are equal to 0,1 or -1.

One of the motivations of this result yielded from the fact that the corresponding result in terms of graphs has had proved some years earlier.

It is natural to consider the problem on the generalization of the intersection theorem of 2 matroids to the intersection of $k \geq 2$ matroids. Unfortunately, such a result is not known and looks unlikely the existence of such solution. One reason is given by the theory of complexity of algorithms. A decision problem is said to be in the class NP (*'deterministic polynomial'*) if its solution can be verified in polynomial time, that is, by an algorithm that uses a polynomial number of steps. A typical exemple of a NP problem is *satisfiability*.

The intersection problem of 3 matroids is NP-complete. On the contrary, there exist a polynomial time algorithm for the intersection of matroids is polynomial (assuming the existence of an oracle for independency).

8. Tutte Polynomial

The *Tutte polynôme de Tutte* of a matroid M is the generating function defined as

$$t(M;x,y) = \sum_{X \subseteq E} (x-1)^{r(E)-r(X)}(y-1)^{|X|-r(X)}.$$

This polynomial was introduced by Tutte [15] for graphs and then generilized to matroids by Crapo [3]. Its many rich properties, including several equivalent definitions, have led to an abundant literature in a continual development [2]. This is a good example of remarkable object in the theory of matroids. After presenting a few fundamental general properties we will give a more specifique applications.

Example 8.1. Recall that $U_{3,2}$ is the uniform rank 2 matroid on 3 elements. Then, $t(U_{3,2};x,y) = x^2 + x + y$.

8.1. **General properties.** Recall that a *loop* of a matroid M is a circuit of cardinality one and that an *isthme* of M is an element which is in all bases of M. The Tutte polynomial can be expressed recursively as

$$t(M;x,y) = \begin{cases} t(M \setminus e;x,y) + t(M/e;x,y) & \text{if } e \text{ is neither a loop nor a isthme,} \\ xt(M \setminus e;x,y) & \text{if } e \text{ is an isthme,} \\ yt(M/e;x,y) & \text{if } e \text{ is a loop.} \end{cases}$$

We state some basic and numerative properties of Tutte polynomial.

(*i*) $t(M^*;x,y) = t(M;y,x)$.

(*ii*) Let M_1 and M_2 two matroids on the sets E_1 et E_2 respectively with $E_1 \cap E_2 = \emptyset$. Then, $t(M_1 \oplus M_2;x,y) = t(M_1;x,y) \cdot t(M_2;x,y)$.

(*iii*) $t(M;2,2)$ counts the number of subsets of E.

(*iv*) $t(M;1,1)$ counts the number of bases of M.

(*v*) $t(M;2,1)$ counts the number of independents of M.

(*vi*) $t(M;1,2)$ counts the number of generating sets of M.

The Tutte polynomial appears in many counting problems in graph theory, matroids and even in mechanical statistics.

8.2. **Chromatic Polynomial.** Let $G = (V, E)$ be a graph and let λ be a positive integer. A λ-*coloring* of G is a function $\phi : V \longrightarrow \{1, \ldots, \lambda\}$. The coloring is said to be *good* if for any edge $\{u, v\} \in E(G)$, $\phi(u) \neq \phi(v)$. Let $\chi(G, \lambda)$ be the number of good λ-colorings of G.

The following result can be proved by using the inclusion-exclusion principle: if $G = (V, E)$ is a graph and λ is a positive integer, then,

$$\chi(G, \lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\omega(G[X])},$$

where $\omega(G[X])$ denote the number of connected components of the subgraphe induced by X.

The chromatic polynomial was introduced by Birkhoff [1] as a tool to attack the four color problem. Indeed, if for a planar graph G we have $\chi(G, 4) > 0$ then G admit a good 4-coloring. The chromatic polynomial is essentially an evaluation of the Tutte polynomial of $M(G)$. Indeed, if $G = (V, E)$ is a graph with $\omega(G)$ connected components, then

$$\chi(G, \lambda) = \lambda^{\omega(G)} (-1)^{|V(G)| - \omega(G)} t(M(G); 1 - \lambda, 0).$$

8.3. **Chromatic polynomial with defect.** Let G be a graph, we define the *chromatic polynomial with defect* $B(G, \lambda, s)$ as

$$B(G, \lambda, s) = \sum_{i} b_i(G, \lambda) s^i$$

, where $b_i(G, \lambda)$ denote the number λ-colorings of G with exactly i edges having the their extremes with the same color. We have

$$B(G, \lambda, s) = \lambda^{\omega(G)} (s - 1)^{r(G)} t \left(M(G); \frac{s + \lambda - 1}{s - 1}, s \right).$$

8.4. **Flow Polynomial.** Let G be an oriented graph (each edge has a *positive* end and a *negative* end). Let $S \subset V(G)$ and let $\omega_G^+(S)$ (resp. $\omega_G^-(S)$) the set of edges of G with positive ends (resp. negative ends) in S and negative ends (resp. positive ends) in $V \setminus S$. Let H be an abelian group (with additive notation). A H-flow in G is a function $\phi : E(G) \longrightarrow H$ such that the sum of weights of the edges getting into v is equal to the sum of the weights of the edges getting out of v for all $v \in V(G)$. A H-flow of G is called *nonwhere zero* if $\phi(e) \neq 0$ for all $e \in E(G)$.

Let $f_\lambda(G)$ be the number of nonwhere zero H-flow of G. $f_\lambda(G)$ is called *flow polynomial* of G. If G is connected and if H a finite abelian group of order λ, then

$$f_\lambda(G) = (-1)^{|E(G)| - r(E)} t(M(G); 0, 1 - \lambda).$$

The notion of nonwhere zero k-flow can be seen as the dual of good colorings. Indeed, if G is a connected planar graph, then

$$\chi(G, \lambda) = \lambda F_\lambda(G^*).$$

8.5. **Ehrhart polynomial.** The theory of Ehrhart was interested in counting the number of integer points lying inside a polytope. We say that a polytope is *integral* if all their vertices have integer coordinates. Given an integer polytope P, Ehrhart studied the function i_P that counts the number of integer points inside the P dilated by a factor t, that is

$$\begin{aligned} i_P : \ & \mathbb{N} \longrightarrow \mathbb{N}^* \\ & t \mapsto |tP \cap \mathbb{Z}^d| \end{aligned}$$

Ehrhart proved that the function i_P is a polynomial on t of degree d,

$$i_P(t) = c_d t^d + c_{d-1} t^{d-1} + \cdots + c_1 t + c_0.$$

$i_P(t)$ is called *Ehrhart polynomial.* The coefficients c_i gives information about the polytope P. Par example, c_d is equals to $Vol(P)$ (the volume of P), c_{d-1} is equals to $Vol(\partial(P)/2)$ where $\partial(P)$ is the surface of P, and $c_0 = 1$ is Euler's characteristic of P. All other coefficients remains a mystery.

Recall that the *Minkowski sum* of two sets A and B of $\mathbb{R}^d$ is

$$A + B = \{a + b | a \in A, b \in B\}.$$

Let $V = \{v_1, \ldots, v_k\}$ be a finite set of elements of $\mathbb{R}^d$. A *zonotope* generated by V, denoted by $Z(A)$, is the polytope formed by the Minkowski sum of line segments

$$Z(A) = \{\alpha_1 + \cdots + \alpha_k | \alpha_i \in [-v_i, v_i]\}.$$

Let M be a regular matroid and let A one of its representation by a totally unimodular matrix. Then, the Ehrhart polynomial associeted to zonotope $Z(A)$ is given [12] by

$$i_{Z(A)}(q) = q^{r(M)} t\left(M; 1 + \frac{1}{q}, 1\right).$$

8.6. **Acyclic and totally cyclic orientations.** Let $G = (V, E)$ be a connected graph. An *orientation* of G is an orientation of the edges of G. We say that an orientation is *acyclic* if the oriented graph has not an oriented cycle (i.e., a cycle where the oriented edges are all clockwise or anticlockwies). A classical result is due to Stanley [11] states that the number of acyclic orientations $a(G)$ of a graph $G = (V, E)$ is

$$a(G) = (-1)^{|V(G)|} \chi(G, -1) = t(M(G); 2, 0).$$

An orientation of a graph G is called *totally cyclic* if every directed edge lies in at least one directed cycle. One can show that this is equivalent to the condition that the orientation on each connected component of G is *strongly connected* : for every $x, y \in V(G)$ in the same connected component of G there exist directed paths both from x to y and from y to x. It turns out that the number of totally cyclic orientations $a^*(G)$ of a connected graph G is :

$$a^*(G) = a^*(M(G)) = a(M(G)^*) = t(M(G); 0, 2).$$

References

[1] G.D. Birkhoff, *A determinant formula for the number of ways of coloring a map*, Annals of Math. **14**, 42-46 (1912-13).

[2] T. Brylawski, J. Oxley, *The Tutte polynomial and its applications*, Matroid Applications (ed. N. White), Cambridge University Press, 123-225 (1992).

[3] H.H. Crapo, *The Tutte polynomial*, Aequationes Mathematicae **3**, 211-229 (1969).

[4] J. Edmonds, Lehman's switching game and a theorem of Tutte and Nash-Williams, *Res. Nat. Bur. Standards Sect. B*, **69** 73-77 (1965).

[5] J.F. Geeelen, A.M.H. Gerards, A. Kapoor, *The excluded minors for GF(4)-representable matroids*, J. Comb. Th. Ser. B **79**, 247-299 (2000).

[6] D.R. Hughes, F.Piper, *Projective Planes*, Springer-Verlag, New York, (1973).

[7] J. Kahn, P. Seymour, On forbidden minors for GF(3), *Proc. Amer. Math. Soc.*, **102**, 437-440(1988).
[8] C. St. A. Nash-Williams, *An application of matroids to graph theory*, Theory of graphs (Int. Sympos. Rome), Dunod Paris, 363-365 (1966).
[9] J. Oxley, *Matroid Theory*, Oxford University Press, (1992).
[10] P. Seymour, *Decomposition of regular matroid*, J. Comb. Th. Ser. B **28**, 305-359 (1980).
[11] R.P. Stanley, *Acyclic orientations of graphs*, Disc. Math. **5**, 171-178 (1973).
[12] R.P. Stanley, *A zonotope associated with graphical degree sequences*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **4**, 555-570 (1991).
[13] W.T. Tutte, *A homotopy theorem for matroids I*, Trans. Amer. Math. Soc. **88**, 144-160 (1958).
[14] W.T. Tutte, *A homotopy theorem for matroids II*, Trans. Amer. Math. Soc. **88**, 161-174 (1958).
[15] W.T. Tutte, *A contribution to the theory of chromatic polynomials*, Can. J. Math. **6**, 80-91 (1954).
[16] H. Whitney, *On the abstract properties of linear dependence*, Amer. J. Math. **57**, 509-533 (1935).

I3M, Université Montpellier 2, Place Eugène Bataillon, 34095 Montpellier, France
E-mail address: `jramirez@univ-montp2.fr`