Faculté des Sciences de Luminy
DEA d'Indormatique
Méthodes géométriques en optimisation combinatoire

1 Set systems. Ordered sets. Antichains

1.1 Set systems. Antichains

A *partially ordered set* (*poset* for short) is a set X with a binary relation $\leq$ (sometimes $\subseteq$) such that
(i) $a \leq a$ for all $a \in X$ (reflexivity)
(ii) if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity)
(iii) if $a \leq b$ and $b \leq a$ then $a = b$ (antisymmetry).

If for all $a, b \in X$ either $a \leq b$ or $b \leq a$, then the partial order is called a total order. If a subset of X is totally ordered, it is called a *chain*. An *antichain* is a set of elements of X that are pairwise incomparable.

With the natural order, namely $A \leq B$ if $A \subseteq B$, the boolean $\mathcal{P}(X)$ (denoted also $[n]$ if $|X| = n$) is a poset. A *set system* (on X) is a pair $(X, \mathcal{F})$, where $\mathcal{F} \subseteq \mathcal{P}(X)$. Every set system can be represented as the subset of vertices of the boolean cube $\{\pm 1\}^X$ by encoding each set $Y \in \mathcal{F}$ by its characteristic function s_Y : namely, set $s_Y(x) = +1$ if $x \in Y$ and $s_Y(x) = -1$ otherwise.

We start with the following nice theorem of Dilworth (1950) on posets.

Théorème 1 *(Dilworth) Let S be a partially ordered finite set. The minimum number m of disjoint chains which together contain all elements of X is equal to the maximum number M of elements in an antichain of X.*

Preuve. Clearly $m \geq M$. To show the converse, use induction on $|X|$. If $|P| = 1, 2$ is nothing to prove. Let C be a maximal chain of X. If every antichain of $X - C$ contains at most $M - 1$ elements, we are done. So assume that $A = \{a_1, a_2, \ldots, a_M\}$ is an antichain of $X - C$. Define

$$X^- := \{x \in X : x \leq a_i \text{ for some } a_i\}, \qquad X^+ = \{x \in X : a_i \leq x \text{ for some } a_i\}.$$

Notice that X^- and X^+ cover X and $X^- \cap X^+ = A$. Since C is a maximal chain, the largest element of C is not in X^-, hence by the induction hypothesis, the result holds for X^-. Hence X^- is the union of M disjoint chains $C_1^-, \ldots, C_M^-$, where $a_i \in C_i^-$. If $x \in C_i^-$ and $x > a_i$, then by definition of X^- there is a j such that $x \leq a_j$. By transitivity $a_i \leq a_j$, a contradiction. Thus a_i is the maximal element of the chain C_i^-. We do the same and get a partition of X^+ into M chains $C_1^+, \ldots, C_M^+$, where a_i is the minimal element of C_i^+. By combining the chains the theorem follows. $\square$

A "dual" to Dilworth's theorem is due to Mirsky (1971).

Théorème 2 *(Mirsky) Let X be a partially ordered set. If X possesses no chain of $m + 1$ elements, then X is the union of m antichains.*

Preuve For $m = 1$ the result is trivial. Let $m \geq 2$ and assume that the theorem is true for $m-1$. Let Max be the set of maximal elements of X. Max is an antichain. Suppose $x_1 \leq x_2 \leq \ldots \leq x_m$ is a chain of $X - Max$. Then this will be a maximal chain in X hence $x_m \in Max$, a contradiction. Hence $X - Max$ has no chain of m elements. By the induction hypothesis, $X - Max$ is the union of $m-1$ antichains. Adding the antichain Max we are done. □

The following famous theorem is due to Sperner (1928) and is in the same spirit. It estimates the chardinality of a maximal antichain of the boolean lattice $\mathcal{P}(X) = [n]$ if $|X| = n$. By a kth level of $\mathcal{P}(X)$ we will understand the collection of all subsets of cardinality k.

Théorème 3 *(Sperner) If $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$ are subsets of an n–element set X such that A_i is not a subset of A_i if $i \neq j$, then $m \leq \binom{n}{\lfloor n/2 \rfloor .}$*

Preuve As we said, $\mathcal{A}$ is an antichain of $(\mathcal{P}(X), \subseteq)$. A maximal chain C in this poset will share a set with each $k$level, $k = 0, 1, \ldots, n$. It starts with empty set, then any singleton set (n choices), then any 2-subset containing the singleton ($n-1$ choices), etc. Thus there are $n!$ maximal chains. Analogously, there are exactly $k!(n-k)!$ maximal chains which contain a given k–subset.

Now we will count the number of ordered pairs (A, C), such that $A \in \mathcal{A}$, C is a maximal chain, and $A \in C$. Since each maximal chain contains at most one member of an antichain, this number is at most $n!$. If we let α_k denote the number of sets $A \in \mathcal{A}$ in the kth level, then this number is $\sum_{k=0}^{n} \alpha_k k!(n-k)!$. Thus

$$\sum_{k=0}^{n} \alpha_k k!(n-k)! \leq n!,$$

or equivalently, $\sum_{k=0}^{n} \alpha_k / \binom{n}{k} \leq 1$.

Since $\binom{n}{k}$ is maximal for $k = \lfloor n/2 \rfloor$ and $\sum \alpha_k = m$, the result follows. □

Another proof (in the spirit of "duality" between chains and antichains) of the theorem of Sperner can be derived in the following way. A *symmetric chain* of sets of an n-set is a sequence $C_k \subset C_{k+1} \ldots, \subset C_{n-k}$ such that $|C_i| = i$. We will discribe an algorithm that splits $[n]$ into symmetric chains. Proceed by induction on n, the case $n = 1$ being trivial. If $[n]$ has been split into symmetric chains, then for each such symmetric chain $C_k, \ldots, C_{n-k}$ define two symmetric chains in $[n+1]$, namely $C_{k+1}, \ldots, C_{n-k}$ and $C_k, C_{k+1} \cup \{n+1\}, \ldots, C_{n-k} \cup \{n+1\}$. It is easy to see that this family of chains provides the job. Now, every symmetric chain contains exactly one set of cardinality $\lfloor n/2 \rfloor$. Thus the family of symmetric chains thus constructed contains exactly $\binom{n}{\lfloor n/2 \rfloor}$ chains. Since every antichain contains at most one set in each chain, the Sperner's theorem follows.

Sperner theorem can be used to solve the following problem. Suppose $x_1, x_2, \ldots, x_n$ are real numbers of modulo at least 1. Form all 2^n sums of the form $x_{i_1} + x_{i_2} + \ldots + x_{i_t}$. *At most how many of these sums can differ from each other by less than 1?* For $A \subset [n]$ let $x_A = \sum_{i \in A} x_i$. In this problem x_i may be replaces by $-x_i$ (replace A by $A \Delta \{i\}$ and x by $x - x_i$) so we may assume that $x_i \geq 1$ for every i. Let $\mathcal{S}$ be such that $|x_A - x_B| < 1$ for $A, B \in \mathcal{S}$. Then $\mathcal{S}$ must be an antichain, because if $A \subset B$ then $|x_A - x_B| = x_{B-A} \geq 1$, so at most one of A and B can belong to $\mathcal{S}$. Hence, by Sperner's theorem, $|\mathcal{S}| \leq \binom{n}{\lfloor n/2 \rfloor}$ (the born is sharp, just take all numbers to be 1). This result was generalized by Kleitman (1970) to vectors in any normed spaces, thus solving an open problem by Littlewood and Offord (1943) for vectors in the Euclidean plane. Namely, Kleitman established that *if B is a normed space and $x_1, x_2, \ldots, x_n$ are vectors of B with $||x_i|| \geq 1$, $i = 1, \ldots, n$, then there are at most $\binom{n}{\lfloor n/2 \rfloor}$ vectors of the form $x_{i_1} + x_{i_2} + \ldots + x_{i_t}$, such that that the difference of any two of these vectors has norm less than 1.* The proof uses the decomposition of all sets into chains quite close in the spirit to the second proof of Theorem 3.

We will derive now a proof of a theorem known as P.Hall's *marriage theorem* (1935). Consider a set family $\mathcal{F} = \{F_1, \ldots, F_m\}$ on X. We define a *system of distinct representatives* (or a *transversal*) of $\mathcal{F}$ to be a sequence of n distinct elements $a_1, a_2, \ldots, a_m \in X$ with $a_i \in F_i$, $(1 \leq i \leq m)$. Question: WHEN A SET FAMILY ADMITS A SYSTEM OF DISTINCT REPRESENTATIVES? On can formulate this problem in graph terms. Construct a *bipartite graph* $G = (\mathcal{F}, X; E)$ where a set F_i and an element $s \in X$ are adjacent if and only if $s \in F_i$. A *matching* is a subset of edges such that no vertex is incident with more than one edge. A *perfect matching* is a matching such that every vertex is incident with an edge in it. One can easily see that $\mathcal{F}$ admits a system of distinct representatives if and only if the bipartite graph G has a perfect matching. BUT WHEN A BIPARTITE GRAPH $G = (X, Y; E)$ HAS A PERFECT MATCHING? The answer is provided by the Hall's theorem.

Théorème 4 *(Hall) A necessary and sufficient condition for there to be a perfect matching in a bipartite graph $G = (X, Y; E)$ is that $|N(A)| \geq |A|$ for every $A \subseteq X$, where $N(A) = \cup_{x \in A} N(x)$ and $N(x) = \{y \in Y : xy \in E\}$.*

Preuve. There are different proofs of this result. We wiil use the theorem of Dilworth. Let $|X| = n, |Y| = n' \geq n$. We introduce a partial order by defining $x_i < y_j$ if and only if there is an edge from x_i to vertex y_j. Suppose that the largest antichain contains s elements. Let this antichain be $\{x_1, \ldots, x_h, y_1, \ldots, y_k\}$, where $h + k = s$. Since $N(\{x_1, \ldots, x_h\}) \subseteq Y - \{y_1, \ldots, y_k\}$, we have $h \leq n' - k$. Hence $s \leq n'$. The poset is the union of s disjoint chains. This will consist of a matching of size a, the remaining $n - a$ elements of X, and the remaining $n' - a$ elements of Y. Therefore $a + n - a + n' - a = s \leq n'$, i.e. $a \geq n$, which means that we have a perfect matching. $\square$

We continue with a theorem of König.

Théorème 5 *(König) The minimum number of lines of a (0,1)–matrix A that contain all the 1's of A is equal to the maximum number of 1's in A no two on a line. Equivalently, the minimum number of vertices of a bipartite graph $G = (X, Y; E)$ covering all edges of G is equal to the maximal matching of G.*

Preuve. Let m be the minimum number of lines of A containing all the 1's of A and let M be the maximum number of 1's, no two on a line. Clearly $m \geq M$. Let the minimum covering by lines consists of r rows and s columns $(r + s = m)$. Without loss of generality there are the first r rows and the first s columns. Define the sets A_i $1 \leq i \leq r$, by $A_i = \{j > s : a_{ij} = 1\}$. If some

k-tuple of the A_i's contained less than k elements, then we could replace the corresponding k rows still covering the 1's. Since this is impossible, we see that A_i's satisfy the theorem of Hall, i.e. $\{A_i\}$ has a system of distinct representatives. This means that there are r 1's no two on a line, in the first r rows and not in the first s columns. By the same argument there are s 1's no two on a line, in the first s columns and not in the first r rows. This shows $M \geq r+s=m$ and we are done. $\square$

1.2 The trace and the VC-dimension of a set system

Let X be a set (finite or not) and let $\mathcal{S} \subset \mathcal{P}(X)$. Given a set $Y \subset X$, we call $\mathcal{S}_Y = \{F \cap Y : F \in \mathcal{S}\}$ the *trace* of $\mathcal{S}$ to Y. A set Y is called *shattered by* $\mathcal{S}$ if $\mathcal{S}_Y = \mathcal{P}(Y)$, i.e. every subset of Y can be obtained by intersecting Y with a subset from $\mathcal{S}$. The *Vapnik-Chervonenkis dimension* (*VC-dimension* for short) of a set system $\mathcal{S}$ is the cardinality of the largest subset of X shattered by $\mathcal{S}$, otherwise it is ∞ if arbitrarily large subsets are shattered.

Examples. (i) $\mathcal{B}$ be the set of all closed balls in E^d. The VC-dimension of this set system is $d+1$. To see this, note that the set of ball shatters any $d+1$ points which form a simplex in E^d. If on the other hand, a set A of at least $d+2$ points is given, then Radon's theorem ensures that there is a partition of A into subsets A_1 and A_2 such that $conv(A_1) \cap conv(A_2) \neq \emptyset$. Assume A is shattered; then there are balls B_1, B_2 with $B_1 \cap A = A_1$ and $B_2 \cap A = A_2$. Let h be a hyperplane separating $B_1 - B_2$ from $B_2 - B_1$. If the balls are disjoint or have just one point in common, such a hyperplane trivially exists- otherwise we choose h to be the hyperplane spanned by the sphere that is the intersection of the boundaries of B_1 and B_2. Clearly, $B_1 \cap B_2$ contains no element of A, so h also separates A_1 from A_2, a contradiction to the fact that the convex hulls intersect. Hence it follows that A is not shattered.

(ii) $\mathcal{P}$ be the set of all polytopes in E^d. This space has infinite VC-dimension: let A be a set of points on a sphere and A' an arbitrary subset of A. Clearly $conv(A')$ is a polytope containing exactly the elements from A', so A is shattered, where $|A|$ can be arbitrarily large.

(iii) Consider a finite set H of n hyperplanes in E^d (an *arrangement of hyperplanes*). Every hyperplane $h_i \in H$ defines two open halfspaces. Arbitrarily choose one of these two halfspaces to be called h_i^+, or the positive halfspace of h_i, and another to be called h_i^-, or the negative halfspace. The set H dissect E^d into connected pieces of various dimensions, called *faces*. The d-faces are called *cells*. Every cell C can be encoded by a ± 1 n-vector $x_C = (x_1, \dots, x_n)$, where $x_i = +1$ if C belongs to h_i^+ and $x_i = -1$ if $C \subset h_i^-$. Clearly, the sign vectors of cells corresponds to a set system by encoding $+1$ by 1 and -1 by 0. It can be shown that the resulting set system has VC-dimension d and that there are at most $\sum_{i=0}^{d} \binom{n}{i}$ cells in the resulting dissection (exercise).

We will generalize the last result by establishing that a set system $\mathcal{S}$ on X, $|X| = n$ of VC-dimension d contains at most $\sum_{i=0}^{d} \binom{n}{i} = O(n^d)$ sets. The result has been conjectured by Erdös, and has been established independently by Sauer, Shelah, and Vapnik&Chervonenkis. The latter found apllications in statistics and learning theory. Recently, the VC-dimension find an important use in computational geometry. Actually it can be viewed as a kind of a topological dimension in the abstract setting of set systems.

But before, for $Y \subset X$ define

$$\mathcal{S}^Y = \{S \in \mathcal{S} : S \cap Y = \emptyset, S \cup Y' \in \mathcal{S} \text{ for every } Y' \subseteq Y\}.$$

Remark 1. *If $\mathcal{S}$ has VC-dimension d, then $\mathcal{S}^x$ is of VC-dimension at most $d-1$ for all $x \in X$.*

Assume $Y \subseteq X - \{x\}$ is shattered in $\mathcal{S}^x$. We claim that $Y \cup \{x\}$ is shattered in $\mathcal{S}$. Let Y' be a subset of $Y \cup \{x\}$. If $Y' \subset Y$, there is $S \in \mathcal{S}^x \subset \mathcal{S}$ with $S \cap (Y \cup \{x\}) = S \cap Y = Y'$. Otherwise, if $x \in Y'$, there is $S_0 \in \mathcal{S}^x$ with $S_0 \cap Y = Y' - \{x\}$. But then $(S_0 \cup \{x\}) \cap (Y \cup \{x\}) = Y'$, where $S_0 \cup \{x\} \in \mathcal{S}$. Hence $Y \cup \{x\}$ is shattered by $\mathcal{S}$. This imply that $|Y| \leq d-1$, establishing the remark.

Remark 2. $|\mathcal{S}| = |\mathcal{S}_{X-\{x\}}| + |\mathcal{S}^x|$ *for any set system $\mathcal{S}$ and any $x \in X$.*

By deleting x from the sets of $\mathcal{S}$, exactly the pairs of sets (S, S') with $x \notin S$ and $S' = S \cup \{x\}$ collapse to one subset of $X - \{x\}$. Since there are $|\mathcal{S}^x|$ such pairs, we conclude that $|\mathcal{S}| = |\mathcal{S}_{X-\{x\}}| + |\mathcal{S}^x|$.

Théorème 6 *(Vapnik-Chervonenkis, Sauer, Shelah) Let $\mathcal{S}$ be a set system on X, $|X| = n$, of VC-dimension d. Then $|\mathcal{S}| \leq \sum_{i=0}^{d} \binom{n}{i} =: \Phi_d(n)$.*

Preuve. The assertion is true for $d = 0$ and for $n = d \geq 0$. Now let $\mathcal{S}$ has VC-dimension d $|X| = n > d$, and assume that the theorem holds for any set system of VC-dimension at most $d-1$ and for any set system of dimension d with at most $n-1$ elements.

Choose $x \in X$. Clearly, the set system $\mathcal{S}_{X-\{x\}}$ is of VC-dimension at most d, so

$$|\mathcal{S}_{X-\{x\}}| \leq \Phi_d(n-1)$$

by hypothesis. From Remark 1 we know that $\mathcal{S}^x$ is of dimension at most $d-1$, which means

$$|\mathcal{S}^x| \leq \Phi_{d-1}(n-1).$$

Since $|\mathcal{S}| = |\mathcal{S}_{X-\{x\}}| + |\mathcal{S}^x|$ by Remark 2, we conclude that $|\mathcal{S}| \leq \Phi_d(n-1) + \Phi_{d-1}(n-1)$. Using the equality $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$ we easily obtain $\Phi_d(n-1) + \Phi_{d-1}(n-1) = \Phi_d(n)$, and the result is established. □

One of the consequences (not immediate) of this result is that if $\mathcal{S}$ is a set system on $X, |X| = n$, of VC-dimension d and $\epsilon < 1/2$ such that every set of $\mathcal{S}$ contains at least $n\epsilon$ elements, then there exists $N \subset X$ of cardinality at most $\frac{d}{\epsilon}(log\frac{1}{\epsilon} + 2loglog\frac{1}{\epsilon} + 6)$ elements which intersects every set of $\mathcal{S}$. This shows that set systems of small VC-dimension can be statistically very well represented by taking relatively small samples from their vertex sets.

1.3 Ramsay's theorem

In 1930, F.P. Ramsay (a brilliant economist in the circle of Keynes) proved a lemma in a paper on mathematical logic. The lemma turned to be of greater importance than the theorem it was used to prove, and has given its author's name to an area where combinatorics, logic, topology and probability interact. Ramsay's theorem is a deep generalisation of the well-known *Pigeonhole principle,* which asserts that *if $n+1$ letters are placed in n pigeonholes, then some pigeonhole must contain more than one letter.* Sometimes, this principle is called *Dirichlet principle*, because Dirichlet made the most important application of this principle. His result concerns the existence of good rational approximations to an irrational number:

Proposition 1 *(Dirichlet) if α is irrational, then there exist infinitely many different rational numbers p/q for which $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.*

*Preuve.*Let $\{x\}$ denote the fractional part of x. We will prove the following: *for any natural number n, there is a rational number p/q with $q \leq n$ such that $|\alpha - p/q| < 1/(nq)$.* Of course then $|\alpha - p/q| < 1/(q^2)$. Moreover, since α is irrational, $\alpha \neq p/q$, and we can find n_1 with $|\alpha - p/q| > 1/n_1$. Then repeating the argument with n_1 in place of n gives another solution p_1/q_1 which is different from p/q (since $|\alpha - p_1/q_1| \leq 1/n_1 < |\alpha - p/q|$). Continuing this process, we find infinitely many such "good" rational approximations.

To establish the assertion, consider the $n+1$ numbers $\{i\alpha\}$, for $i = 1, 2, \ldots, n+1$. We put these numbers into the n pigeonholes $(j/n, (j+1)/n)$, for $j = 0, \ldots, n-1$. (None of the numbers coincides with an end-point of the intervals, since α is irrational). By the Pigeonhole Principle, some interval contains more than one of the numbers, say $\{i_1\alpha\}$ and $\{i_2\alpha\}$, which therefore differ by less than $1/n$. Putting $q = |i_1 - i_2|$, we see that there exists an integer p such that $|q\alpha - p| < \frac{1}{n}$, from which the result follows on division by q. Moreover, q is the difference between two integers in the range $1, 2, \ldots, n+1$, so $q \leq n$. □

Another elegant application of the Pigeonhole Principle is due to Erdös and Szekeres.

Proposition 2 *(Erdös and Szekeres) If $x_1, x_2, \ldots, x_N$ is any sequence of distinct real numbers with $N \geq mn+1$, then there is either a monotonic increasing sequence of length greater than m, or a monotone decreasing sequence of length greater then n.*

Preuve. It suffices to establish the result for $N = mn+1$. So suppose that we have a sequence of $mn+1$ distinct real numbers, and suppose that it contains no monotone increasing sequence of length $m+1$ or greater. For $i = 1, \ldots, m$ let

$$K_i = \{k : \text{the longest monotone increasing sequence ending at } x_k \text{ has length } i\}.$$

Now we have partitioned the set $\{1, 2, \ldots, mn+1\}$ into m subsets $K_1, \ldots, K_m$. By the Pigeonhole Principle, some one of these sets, say K_i, contains at least $n+1$ members.

We claim that K_i indexes a monotone decreasing subsequence. Suppose not, i.e. there are $k, l \in K_i$ with $k < l$ and $x_k < x_l$. Now, by definition of K_i, there is a monotone increasing sequence of length i ending at k, say $x_{j_1} < x_{j_2} < \ldots < x_k$. But then $x_{j_1} < x_{j_2} < \ldots < x_k < x_l$

is a monotone increasing sequence ending at x_l, contradicting the fact that $l \in K_i$. This claim establishes the result. □

An amusing formulation of this result is the following. Suppose that $n^2 + 1$ people are lined shoulder to shoulder in a straight line. Then it is always possible to choose $n + 1$ of the people to take one step forward so that going from left to right their heights are increasing (or decreasing).

Instead of pigeonholes (we are serious people), further we use the terminology of colouring. The Pigeonhole Principle states that, if $r + 1$ objectes are coloured with r different colours, then there must be two objects with the same colour. In order to move towards Ramsay's Theorem, we quantify the result further as follows (whose proof is obvious, but less trivial than that of the Pigeonhole Principle). Actually we already used this assertion in the proof of previous result.

Proposition 3 *Suppose that $n \geq 1 + r(l - 1)$. Let n objects be coloured with r colours, then there exist l objects with the same colour.*

We continue our list of "non-serious" results in serious "emballage", still approaching Ramsay's theorem.

Proposition 4 *Suppose that the 2-element subsets of a 6-element set are coloured with two colours red and blue. Then there is a 3-element set, all of whose 2-element subsets have the same colour. In other words, among every 6 persons either there are 3 which know each other or there are 3 which do not know each other.*

Preuve. Consider the five 2-subsets 16,26,36,46,56. These are coloured with two colours; so there must be three of the five edges which have the same colour. Let us suppose that 16,26 and 36 are red. Now there are two possibilities: if one of 12,23,31 is red (say 12), there is a red triangle (126); but if none of the three is red, then (123) is a blue triangle. □

Proposition 5 *(i) If the 2-subsets of a 9-set are coloured red and blue, then there is either a red 3-set or a blue 4-set.*

(ii) If the 2-subsets of a 18-set are coloured red and blue, there is a monochromatic 4-set.

(iii) If the 2-subsets of a 17-set are coloured red, blue and green, there is a monochromatic 3-set.

Preuve. Left to the reader.

The results above suggest their generalisation, which is known as Ramsay's theorem.

Théorème 7 *(Ramsay) Let r, k, l be positive integers. Then there is a positive integer n with the following property. If the k-subsets of an n-set are coloured with r colours, then there is a monochromatic l-set, i.e., one all of whose k-sets have the same colour. More generally, let $r, k, a_1, \ldots, a_r$ be given. Then there exists n with the property that, if the k-subsets of an n-set are coloured with r colours $c_1, \ldots, c_r$, then for some i in the range $1, \ldots, r$, there is an a_i-set, all of whose subsets have colour c_i.*

Preuve. We denote by $R(r,k,l)$ the smallest n for which Ramsay's theorem holds, and by $R^*(r,k;a_1,\ldots,a_r)$ the smallest n for which the "more general" statement holds. Clearly we have $R(r,k,l) = R^*(r,k;l,l,\ldots,l)$. To familiarise the notation, notice that previous propositions establish that $R(2,2,3) = 6; R^*(2,2;3,4) = 9; R(2,2,4) = 18; R(3,2,3) = 17$; and

$$R^*(r,1;a_1,\ldots,a_r) = \sum_{i=1}^{r} a_i - r + 1.$$

Moreover, there are some trivial evaluations: $R(r,k,k) = k, R(1,k,l) = l$.

It is also true that

$$R^*(r+1,k;a_1,\ldots,a_r,k) = R^*(r,k;a_1,\ldots,a_r).$$

For, if there is a k-set of colour c_{r+1} we are done; otherwise, only the first r colours occur.

The proof of Ramsay's theorem uses induction (we will prove the "more general" assertion). We already have the result for $k = 1$, so assume that $k > 1$. We may assume that $a_i > k$ for all i. By induction, we may assume that the numbers

$$A_i = R^*(r,k;a_1,\ldots,a_{i-1},a_i - 1,a_{i+1},\ldots,a_r)$$

are defined (and the statement is true for these).

Take $n = 1+R^*(r,k-1;A_1,\ldots,A_r)$. Let X be a set of n points, whose k-sets are coloured with r colours $c_1,\ldots,c_r$. Take a point $x \in X$, and let $Y = X - \{x\}$. We define a colouring of the $(k-1)$-subsets of Y with colours $c_1^*,\ldots,c_r^*$, by the rule that, for any $(k-1)$-subset U, the colour of U is c_i^* if and only if the colour of $U \cup \{x\}$ is c_i. By definition of n, for some i, there is a c_i^*-monochromatic set Z_i of size A_i. By definition of A_i, the set Z_i contains either a set of size a_j with all its k-sets of colour c_j for some $j \neq i$, or a set V of size $a_i - 1$ with all its k-sets of colour c_i. In the first case, we are done. In the second case, $\{x\} \cup V$ is a set of size a_i, and all its k-sets have colour c_i- by assumption for subsets not containing x, and by the definition of the c^*-colouring and the fact that all $(k-1)$-subsets have colour c_i^* in the case of subsets containing x. $\square$

It is extremely difficult to calculate exact values of Ramsay numbers. Apart from the values presented above, only seven values are known precisely:

$$R^*(2,2;3,l) = 14, 18, 23, 36 \text{ for } l = 5,6,7,8,9;$$

$$R^*(2,2;4,) = 25; R(2,3,4) = 14.$$

In absence of exact values, we rely on upper and lower bounds. The proof gives a "recurrence inequality" for the Ramsay numbers, viz.

$$R^*(r,k;a_1,\ldots,a_r) \leq 1 + R^*(r,k-1;A_1,\ldots,A_r),$$

where

$$A_i = R^*(r,k;a_1,\ldots,a_{i-1},a_i - 1,a_{i+1},\ldots,a_r).$$

Proposition 6 *If $a_1, a_2 \geq 2$, then*

$$R^*(2,2;a_1,a_2) \leq \binom{a_1+a_2-2}{a_1-1}.$$

Preuve. If $a_1 = 2$, then

$$R^*(2,2;2,a_2) = R^*(1,2;a_2) = a_2 = \binom{2+a_2-2}{2-1},$$

and the result is true; similarly, if $a_2 = 2$. So we will use induction, assuming the result is true when either a_1 or a_2 is reduced. In the notation of the Ramsay's Theorem,

$$A_1 = R^*(2,2,a_1-1,a_2) \leq \binom{a_1+a_2-3}{a_1-2},$$

$$A_2 = R^*(2,2;a_1,a_2-1) \leq \binom{a_1+a_2-3}{a_1-1},$$

where the inequalities are the inductive hypothesis; so

$$R^*(2,2;a_1,a_2) \leq 1 + R^*(2,1;A_1,A_2) = 1 + (A_1 + A_2 - 1) =$$
$$(A_1 + A_2) \leq \binom{a_1+a_2-3}{a_1-2} + \binom{a_1+a_2-3}{a_1-1} = \binom{a_1+a_2-2}{a_1-1},$$

where the second line comes from the Pigeonhole Principle. □

From this result, we deduce that $R(2,2,l) \leq \binom{2l-2}{l-1}$. On the other hand, it can be shown that $R(2,2,l) \geq 2^{(l-2)/2}$ for $l \geq 3$.

We conclude this section with the following geometric application of Ramsay's theorem.

Proposition 7 *(Erdös and Szekeres). There is a function f such that, given any $f(n)$ points in the plane with no three collinear, some set of n of the points form a convex polygon.*

Preuve. We need two preliminary facts:

(a) Given any five points in the plane, no three collinear, some four of the points form a convex quadrilateral.

This is clear if the convex hull of the points is a pentagon or quadrilateral. So suppose that it is a triangle, with vertices A, B, C, and let D and E be hte remaining points. Then the line DE meets two sides of the triangle, say AB and AC; and the quadrilateral $BCDE$ (or $BCED$ is convex).

(b) Given a set of n points in the plane, if every four points form a convex quadrilateral, then all n points form a convex polygon.

Obvious.

Now, let $f(n) = R^*(2,4;5,n)$. Given $f(n)$ in the plane, colour a 4-set red if it is a convex quadrilateral, blue otherwise. By (a), there is no blue 5-set. So there is a red n-set; and by fact (b), it is a convex polygon with n points. □

The exact value of the function $f(n)$ is unknown for n of moderate size.

1.4 Social choice and Arrow's theorem

One of the problems of politics involves averaging individual preferences to reach decisions acceptable to society as a whole. Here you prove Arrow's theorem which shows that this is indeed not obvious (this is a rare mathematical result whose author was recompensed with the Nobel premium).

We suppose that I is a society consisting of n individuals. These individuals have a choice among a set X of options, for example, by a referendum. We assume that each member i of the society has made his mind about the relative worth of the opinions, described by a total order $\leq_i$ on X. A *social choice function* is a rule which, given the individual preferences $\leq_i$ for each $i \in I$, comes up with a "social preference" $\leq$ on X, subject to four conditions listed (and justified) below. In other words, it is a function from the set of all n-tuples of X to the set of total orders satisfying Axioms (A1)-(A4) below.

(A1) *If $x \leq y$ in the social preference, then the same remains true if the individual preferences are changed in y's favour.*

(This means that, if $\leq_i'$ is another system of individual preferences satisfying $u \leq_i v \leftrightarrow u \leq_i' v$ for all $u, v \neq y$, and $u \leq_i y \to u \leq_i' y$ for all u, and $\leq'$ is the corresponding social preference, then $x \leq' y$ holds.)

(A2) *If $Y \subseteq X$ and two sets $\{\leq_i\}, \{\leq_i'\}$ of individual preferences have the propoerty that $\leq_i$ and $\leq_i'$ induce the same ordering on Y for each $i \in I$, then the corresponding social preferences $\leq$ and $\leq'$ induce the same ordering on Y.*

(This axiom assert that the social choice is not affected if some of the opinions got out.)

(A3) *For any distinct $x, y \in X$, there is some system of individual preferences for which the corresponding social preference has $x \leq y$.*

(In other words, it should be possible for society to prefer y to x if enough individuals do so. In fact, it follows from (A1)-(A3) that, if $x \leq_i y$ for all $i \in I$, then $x \leq y$: that is, if everybody prefers y to x, then society does too).

(A4) *There is no individual i such that $\leq_i$ coincides with $\leq$ for all systems of individual preferences.*

(This axiom requires that there should not be a dictator whose opinions prevail against all opposition).

Théorème 8 *(Arrow) If $|X| \geq 3$, then no social choice function verifying Axioms (A1)-(A4) exists. In other words, the unique social choice function verifying (A1)-(A3) is the dictatorial one.*

Preuve. Suppose that we have a social choice function. If (x, y) is an ordered pair of distinct opinions, we say that a set J of individuals is (x, y)-decisive if, whenever all members of J prefer y to x, then so does the social order; formally, if $x <_i y$ for all $i \in J$, then $x < y$. Further, we say that J is *decisive* if it is (x, y)-decisive for some distinct x, y. We claimed after the statement of (A3) that the whole society I is (x, y)-decisive for all x, y. Let us prove this. By (A3), we can suppose that x and y are the only options. Now, by (A3), there is some system of individual preferences which causes $x < y$ to hold; and by (A1), this remains true if we alter them so that all individuals prefer y to x.

Let J be a minimal decisive set. Then $J \neq \emptyset$, by (A3). Suppose that J is (x, y)-decisive, and let i be a member of J.

CLAIM. $J = \{i\}$.

Let $J' = J - \{i\}$ and $K = I - J$. Let z be a member of X different from x and y (which exists because $|X| \geq 3$). Consider the individual preferences for which

$$x <_i y <_i z;$$

$$z <_j x <_j y \quad for \quad all \quad j \in J';$$

$$y <_k z <_k x \quad for \quad all \quad k \in K.$$

Then

$x < y$, since all members of the (x, y)-determining set J think so;

$y < z$, since if $z < y$ then J' is (z, y)-decisive, contradicting the minimality of J.

Hence $x < z$. But then $\{i\}$ is (x, z)-decisive, since nobody else agrees with this order. By minimality of J, we have $J = \{i\}$, establishing the claim.

The proof shows, in fact, $\{i\}$ is (x, z)-decisive for all $z \neq x$.

CLAIM. *i is a dictator.*

Choose $w \neq x$, and $z \neq w, x$. Consider the individual preferences in which

$w <_i x <_i z$,

$z <_k w <_k x$ for all $k \neq i$.

Then $w < z$ (because everybody thinks so) and $x < z$ (because i thinks so); so $w < z$, and $\{i\}$ is (w, z)-decisive. Finally, a similar argument shows that $\{i\}$ is (w, x)-decisive for any $w \neq x$. The claim is proved. So, the Axiom (A4) is violated, proving the theorem. □

2 Blocking systems and bottleneck extrema

We start with a following problem.

MAXIMUM-TRAFFIC-FLOW PROBLEM. Let G be a connected simple graph, and u and v two distinguished nodes of G. We regard G as a sytem of roads connecting u and v. Each edge e has a non–negative capacity $c(e)$. Let γ be an elementary chain joining u and v. Define the capacity $c(\gamma)$ of γ to be the minimum capacity of an edge of γ. An edge e' of γ with $c(e') = c(\gamma)$ is a *bottleneck* of γ. The problem is to determine an elementary chain γ^* joining u and v which has the maximum capacity, i.e., we want to determine γ^* such that

$$c(\gamma^*) = \max_\gamma c(\gamma) = \max_\gamma \min_{e \in \gamma} c(e),$$

where the maximum is taken over all elementary chains γ joining u and v and the minimum is over all edges e of γ. A *cut separating* u and v is a set of edges of G whose removal leaves u and v in different connected components of the obtained graph. An *elementary cut separating* u and v is a minimal by inclusion cut separating u and v. Evidently for any elementary cut K and any elementary chain γ one has $c(\gamma) \leq \max_{e \in K} c(e)$. Therefore,

$$c(\gamma) \leq \min_K \max_{e \in K} c(e),$$

where the maximum is taken over all elementary cuts separating u and v. Since this inequality is true for all elementary chains joining u and v, it follows that

$$\max_{\gamma} c(\gamma) \leq \min_K \max_{e\in K} c(e),$$

where the maximum on the left side is taken over all elementary chains joining u and v. Therefore

$$\max_{\gamma} \min_{e\in\gamma} \leq \min_K \max_{e\in K} c(e).$$

We shall see that equality actually holds, and how to determine a chain γ^* and a cut K^* such that the equality holds.

We now consider the distinguishing feature of this problem. Let E be the set of edges of G. Let $\mathcal{P}$ be the collection of edge sets of elementary chains connecting u and v, and $\mathcal{K}$ be the set of all elementary cuts separating u and v. Since the chains and cuts are elementary, they form antichains (clutters), that is, if P_1 and P_2 are two members of $\mathcal{P}$ with $P_1 \subseteq P_2$ then $P_1 = P_2$. Since every chain connecting u and v contains an edge of every cut, we conclude that $P \cap K \neq \emptyset$ for every member $P \in \mathcal{P}$ and $K \in \mathcal{K}$. Moreover, every set of edges E' intersecting every elementary chain contains an elementary cut. This is a consequence of the fact that every cut contains an elementary cut separating u and v (thus this is true for the cut E'). In order to have a general setting for such problems, we make the following definition. Let E be a finite set, and let $\mathcal{P}$ and $\mathcal{K}$ be two antichains on E. Then the pair $(\mathcal{P}, \mathcal{K})$ is called a *blocking system* for E provided the following property holds:

For each partition of E into two sets E_1 and E_2 either there is a member P of $\mathcal{P}$ with $P \subseteq E_1$ or there is a member K of $\mathcal{K}$ with $K \subseteq E_2$, but not both.

Théorème 9 *Let E be a finite set and $\mathcal{P}$ an antichain on E. Let $\mathcal{K}$ consist of all subsets of E which have a non–empty intersection with each member of $\mathcal{P}$ and which are minimal with respect this property. Then $\mathcal{K}$ is the unique antichain on E such that $(\mathcal{P}, \mathcal{K})$ is a blocking system for E.*

Preuve Because of the minimality condition in the definition of $\mathcal{K}$, $\mathcal{K}$ is an antichain on E. We first show that $(\mathcal{P}, \mathcal{K})$ is a blocking system for E. Let E be partitioned into E_1, E_2. Suppose that no member of $\mathcal{P}$ is a subset of E_1. Then every member of $\mathcal{P}$ has a non–empty intersection with E_2. Hence by definition of $\mathcal{K}$, E_2 contains a member of $\mathcal{K}$. Now suppose there were both $P \subseteq E_1$ and $K \subseteq E_2$ hold for P in $\mathcal{P}$ and K in $\mathcal{K}$. Since $E_1 \cap E_2 = \emptyset$, we have $P \cap K = \emptyset$, a contradiction. We conclude that $(\mathcal{P}, \mathcal{K})$ is a blocking system.

We now show there is at most one antichain $\mathcal{K}'$ on E for which $(\mathcal{P}, \mathcal{K}')$ is a blocking system. It will then follow from what we have already proved that $\mathcal{K}$ is the unique antichain for which $(\mathcal{P}, \mathcal{K})$ is a blocking system for E.

Let by way of contradiction $(\mathcal{P}, \mathcal{K}_1)$ and $(\mathcal{P}, \mathcal{K}_2)$ be blocking systems for E with $\mathcal{K}_1$ different from $\mathcal{K}_2$. We may suppose, without loss of generality, that there is a member K_1 of $\mathcal{K}_1$ which is not a member of $\mathcal{K}_2$. Take the partition $\{E - K_1, K_1\}$ of E. By the definition of the blocking system, no member of $\mathcal{P}$ is contained in $E - K_1$. Therefore there is a member K_2 of $\mathcal{K}_2$ with $K_2 \subseteq K_1$. Since K_1 is not a member of $\mathcal{K}_2$, $K_2 \neq K_1$. Now consider the partition $\{E - K_2, K_2\}$ of E. Suppose that there were a member K_1' of $\mathcal{K}_1$ with $K_1' \subseteq K_2$. Then since

$K_2 \subset K_1$, this would imply that $K_1' \subset K_1$, which contradicts the fact that $\mathcal{K}_1$ is an antichain. Thus no member of $\mathcal{K}_1$ is a subset of K_2. Therefore a member P of $\mathcal{P}$ is a subset of $E - K_2$. But now for the partition $\{E - K_2, K_2\}$ we have a member $P \in \mathcal{P}$ in $E - K_2$ and in addition K_2 is a member of $\mathcal{K}_2$. This contradicts the fact that $(\mathcal{P}, \mathcal{K}_2)$ is a blocking system on E, thus concluding the proof.

$\square$

One call $\mathcal{K}$ the *blocker* of $\mathcal{P}$ and denote it by $b(\mathcal{P})$. From this result we immediately deduce that the blocker of a blocker coincides with the initial antichain:

$$b(b(\mathcal{P})) = \mathcal{P}.$$

EXAMPLE Let $G = (V, E)$ be a connected graph. Let $\mathcal{P}$ be the collection of edge sets of spanning trees of G. Then the blocker $\mathcal{K}$ of $\mathcal{P}$ consists of all sets of edges which intersect every spanning tree and which are minimal with respect to this property. Therefore a set K is a member of $\mathcal{K}$ if and only if (a) the graph obtained by removing all edges of K is not connected and (b) K is minimal with respect to this property.

We continue with the main result of this subsection due to Edmonds and Fulkerson (1970).

Théorème 10 *(Edmonds and Fulkerson) Let $(\mathcal{P}, \mathcal{K})$ be a blocking system for the finite set E and let f be a real-valued function defined on E. Then*

$$max_{P\in\mathcal{P}} min_{e\in P} f(e) = min_{K\in\mathcal{K}} max_{e\in K} f(e).$$

Conversely, let $\mathcal{P}$ and $\mathcal{K}$ be antichains and suppose that this equality holds for every real-valued function defined on E. Then $(\mathcal{P}, \mathcal{K})$ is a blocking system.

Preuve Let P be a member of $\mathcal{P}$ and K a member of $\mathcal{K}$. It follows from previous result that there is an element $e_0 \in P \cap K$. Hence

$$\min_{e\in P} f(e) \leq f(e_0) \leq \max_{e\in K} f(e),$$

or

$$\min_{e\in P} f(e) \leq \max_{e\in K} f(e).$$

Since this holds for all P in $\mathcal{P}$ and all K in $\mathcal{K}$, we obtain

$$\max_{P\in\mathcal{P}} \min_{e\in P} f(e) \leq \min_{K\in\mathcal{K}} \max_{e\in K} f(e). \qquad (*)$$

We now show that equality holds in $(*)$. Let $a_1, a_2, \ldots, a_m$ be the distinct values assumed by the function f, where $a_1 > a_2 > \ldots > a_m$. Let $F_0 = \emptyset$, and for $i = 1, 2, \ldots, m$ let F_i be the subset of E consisting of all those elements e in E for which $f(e) = a_i$. Let k be the first integer such that $F_0 \cup F_1 \cup \ldots \cup F_k$ contains a member P' of $\mathcal{P}$. Since $F_0 \cup F_1 \cup \ldots \cup F_{k-1}$ contains no member of $\mathcal{P}$, it follows that $P' \cap F_k \neq \emptyset$ and hence

$$\min_{e\in P'} f(e) = a_k.$$

Therefore

$$\max_{P\in\mathcal{P}}\min_{e\in P} f(e) \geq a_k. \tag{1}$$

Now $F_0 \cup F_1 \cup \ldots \cup F_{k-1}$ and $F_k \cup F_{k+1} \cup \ldots \cup F_m$ constitute a partition of E. Since $F_0 \cup F_1 \cup \ldots \cup F_{k-1}$ contains no member of $\mathcal{P}$, there is a member K' of $\mathcal{K}$ with $K' \subseteq F_k \cup \ldots \cup F_m$. Since $P' \subseteq F_0 \cup F_1 \cup \ldots \cup F_k$, the set K' is not contained in $F_{k+1} \cup \ldots \cup F_m$. Hence $K' \cap F_k \neq \emptyset$, and it follows that

$$\max_{e\in K'} f(e) = a_k.$$

Therefore

$$\min_{K\in\mathcal{K}}\max_{e\in K} f(e) \leq a_k. \tag{2}$$

Combining this with (1), we obtain

$$\min_{K\in\mathcal{K}}\max_{e\in K} f(e) \leq \max_{P\in\mathcal{P}}\min_{e\in P} f(e).$$

To establish the converse, let E_1, E_2 be a partition of E. Let $f(e) = 1$ or 0 according as $e \in E_1$ or $e \in E_2$. Suppose there is no $P \in \mathcal{P}$ with $\subseteq E_1$. Then

$$\max_{P\in\mathcal{P}}\min_{e\in P} = 0 = \min_{K\in\mathcal{K}}\max_{e\in K} f(e).$$

If there is no $K \in \mathcal{K}$ with $K \subseteq E_2$, we would have

$$\min_{K\in\mathcal{K}}\max_{e\in K} f(e) = 1,$$

a contradiction. Hence there is $K \in \mathcal{K}$ with $K \subseteq E_2$. On the other hand, if there were both $P \in \mathcal{P}$ and $K \in \mathcal{K}$ with $P \subseteq E_1$ and $K \subseteq E_2$, then

$$\max_{P\in\mathcal{P}}\min_{e\in P} f(e) = 1, \quad \min_{K\in\mathcal{K}}\max_{e\in K} f(e) = 0,$$

again a contradiction. □

The above proof contains an algorithm for determining a P' of $\mathcal{P}$ such that

$$\min_{e\in P'} f(e) = \max_{P\in\mathcal{P}}\min_{e\in P} f(e).$$

In order to apply it, one needs to be able to identify when a subset of E contains a member of $\mathcal{P}$.This can be efficiently done for the maximum-traffic-flow problem (we leave it as an exercise for the reader).

We conclude with another application of both theorems.

Bottleneck assignment problem. There are n people who are to be assigned to n jobs on a serial production line. Let c_{ij} represent the rate at which the ith person can process if he is assigned job j. It is clear that the production line can be proceed only as rapidly as the slowest person . The problem is to determine an assignment of people to jobs which has fastest slowest person. We can identify assignments with permutations. Let $i_1 i_2 \ldots i_n$ be an assignment. Then the minimum of the numbers $c_{1i_1} c_{2i_2}, \ldots, c_{ni_n}$ is the productivity of the assignment. Thus the problem is to determine

$$\max_{i_1 i_2 \ldots i_n}\min_{1\leq j\leq n} c_{ji_j},$$

where the maximum is taken over all assignmemts. Consider the bipartite graph G whose nodes are s_1, s_2, s_n (the n people) and $t_1, t_2, \ldots, t_n$ (the n jobs) and such that there is an edge joining each s_i to each t_j. The assignments to jobs correspond to perfect matchings in G. Thus the members of $\mathcal{P}$ are the perfect matchings. Moreover, $\mathcal{K}$ consists of all sets of edges which have a non-empty intersection with every assignment and which are minimal with respect to this property. The proof of second theorem contains an algorithm for computing the optimal assignment.

3 Les matroïdes I: un point de vue "glouton"

3.1 Definition. Exemples.

Un *matroïde* est un couple $M = (E, \mathcal{I})$ formé d'un ensemble fini non–vide E est d'une famille $\mathcal{I}$ non–vide de sous–ensembles de E, appelée sous-ensembles *indépendents* de E, que vérifie les conditions suivantes.

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

(I2) Si $I \in \mathcal{I}$ et $I' \subseteq I$, alors $I' \in \mathcal{I}$ (on dit que $\mathcal{I}$ est *héreditaire* si elle vérifie cette propriété);

(I3) Si $I_1, I_2 \in \mathcal{I}$ et $|I_1| < |I_2|$, alors il existe un élément $e \in I_2 - I_1$ tel que $I_1 \cup \{e\} \in \mathcal{I}$ (on dit que M vérifie la *propriété d'échange*).

Le mot "matroïde" est due à H. Whitney. Il a étudié les *matroïdes matriciels,* dans lesquels les éléments de E sont les lignes d'une matrice donnée A et un ensemble de lignes est indépendent si les lignes sont linéairement indépendentes, au sens habituel du term. On peut facilement montrer que cette structure définit un matroïde $M_A = (E, \mathcal{I}_A)$.

Proposition 8 *$M_A = (E, \mathcal{I}_A)$ est un matroïde.*

Preuve On voit bien que $\mathcal{I}_A$ est héréditaire. Il reste donc à montrer que M_A vérifie la propriété d'échange. Soit W le sous-éspace défini par $I_1 \cup I_2$. Le diménsion dim$W$ de W est au moins $|I_2|$. Supposons que $I_1 \cup e$ est linéairement dépendent pour chaque $e \in I_2 - I_1$. Donc, W est contenu dans le sous-éspace défini par I_1. Alors $|I_2| \leq dimW \leq |I_1| < |I_2|$, une contradiction. $\square$

Comme autre exemple de matroïdes, considérons le *matroïde graphique* $M_G = (E_G, \mathcal{I}_G)$ défini en fonction d'un certain graphe non orienté $G = (V_G, E_G)$ de la manière suivante. Si F est un sous-ensemble de E_G, alors $F \in \mathcal{I}_G$ si et seulement si F est acyclique. Autrement dit, un ensemble d'arêtes est indépendent si et seulement si il forme une forêt.

Proposition 9 *Si G est un graphe non orienté, alors $M_G = (E_G, \mathcal{I}_G)$ est un matroïde.*

Preuve $\mathcal{I}_G$ est héréditaire, puisqu'un sous–ensemble d'une forêt est une forêt. Il reste donc à montrer que M_G vérifie la propriéte d'échange. On suppose que I_1 est I_2 sont des forêtes de G et que $|I_2| > |I_1|$. Une forêt de k arêtes contient exactement $|V_G| - k$ arbres. Donc, la forêt I_1 contient $|V_G| - |I_1|$ arbres, et la forêt I_2 contient $|V_G| - |I_2|$ arbres. Comme la forêt I_2 possède moins d'arbres que I_1, elle doit contenir un arbre T dont les sommets se trouvent dans des arbres différents de la forêt I_1. Par ailleurs, puisque T est connexe, il doit contenir une arête (u, v) telle que les sommets u est v sont dans des arbres différents de la forêt I_1. Comme (u, v) relie des sommets appartenant à des arbres différents de la forêt I_1, l'arête (u, v) peut être ajoutée à la forêt I_1 sans création de cycles. Donc, M_G vérifie la propriété d'échange. □

Comme dernier exemple important de matroïdes, considédons le *matroïde de transversaux partielles* d'une famille des sous-ensembles $\mathcal{F} = \{F_1, F_2, \ldots, F_m\}$ d'un ensemble fini S. Un sous-ensemble I de S est une *transversale partiélle* de $\mathcal{F}$ si I est une transversale (un systéme de réprésentants distincts) d'une sous–famille $\mathcal{F}'$ de $\mathcal{F}$. Soit $\mathcal{I}_T$ la famille de transversaux partielles d'une famille $\mathcal{F}$ des sous-ensembles de S.

Proposition 10 *$M_T = (S, \mathcal{I}_T)$ est un matroïde.*

Preuve. $\mathcal{I}_T$ est héréditaire, puisqu'un sous-ensemble I' d'une transversale partielle I est aussi une transversale partielle. Il rest donc à montrer que M_T vérifie (I3). Soit I_1, I_2 deux transversaux partielles, $|I_1| < |I_2|$. On peut trouver deux couplages W_1 est W_2 issue de I_1 et I_2. Soit W la différence symmétrique de W_1 et W_2. On suppose que les arêtes de $W_1 - W_2$ sont coloré en rouge et les arêtes de $W_2 - W_1$ sont coloré en bleu. Soit Δ le graph induit par les arêtes de W. Comme $|I_1| = |W_1|$ et $|I_2| = |W_2|$, Δ contient plus d'arêtes bleu que d'arêtes rouge. Comme W_1 est W_2 sont des couplages, chaque sommet de Δ est de degree un ou deux. Donc, chaque composent connexe de Δ est un circuit de longeur pair ou une chaîne. Dans chaque chaîne de longeur pair il y a un même nombre des arêtes de chaque couleur. Donc il existe une chaîne P de longeur impair. La premier et la dérnier arêtes de P sont des arêtes bleu. Soit $v_1, v_2, \ldots, v_{2k}$ les sommets de P. On peut supposé sans pérdre la généralité que $v_1 \in S$. Comme v_1 est incident à une arête bleu, $v_1 \in I_2 - I_1$. Plus général, $v_3, v_3, \ldots, v_{2k-1} \in I_1 \cap I_2$. Les sommets $v_2, v_4, \ldots, v_{2k}$ réprésentent des ensembles de famille $\mathcal{F}$. Méntenant, on change les couleurs des arêtes de P sans changer le couleur des autres arêtes de Δ. Dans le graph recoloré on a plus d'arêtes rouges que bleu. D'autre côté, l'ensemble des arêtes rouge forment un couplage. Donc, $I_1 \cup \{v_1\}$ est une transversale partiélle de $\mathcal{F}$, ce qui complète la démonstration établissant que M_T est un matroïde. □

3.2 Algorithmes gloutons et matroïdes

Les nombreux problèmes pour lesquels une approche gloutonne donne les solutions optimales peuvent être ramenés à une recherche d'un sous-ensemble indépendent de pondération maximale dans un matroïde pondéré. Autrement dit, on dispose d'un matroïde pondéré $M = (E, \mathcal{I}, w)$, $(w : E \to R^+ \cup \{0\})$ et on souhaite trouver un ensemble indépendent I pour lequel $w(I) = \sum_{e \in I} w(e)$ est maximisé. Comme la pondération $w(e)$ d'un élément $e \in E$ quelconque est positive, un sous-ensemble optimal est toujours un sous-ensemble indépendent maximal.

Un algorithme glouton pour ce problème considère chaque élément $e \in E$ l'un après l'autre par ordre de poids décroissant et l'ajoute immédiatement à l'ensemble B_G si $B_G \cup \{e\}$ est indépendent.

GLOUTON(M,w)
$B_G \leftarrow \emptyset$
trier E par ordre de poids décroissant
pour chaque $e \in E$, pris par ordre décroissant
    faire si $I \cup \{e\} \in \mathcal{I}$
        alors $B_G \leftarrow B_G \cup \{e\}$
retourner B_G

Théorème 11 *(Edmonds-Rado-Boruvka) Soit $\mathcal{I}$ une famille de sous-ensembles d'un ensemble fini E que vérifie les conditions (I1) et (I2) (i.e. $\emptyset \in \mathcal{I}$ et $I \in \mathcal{I}$, $I' \subseteq I$ alors $I' \in \mathcal{I}$). Le couple $M = (E, \mathcal{I})$ est un matroïde si et seulement si pour chaque fonction de pondération non-negative w l'appel GLOUTON(M,w) retourne un sous-ensemble optimal.*

Preuve. Soit $M = (E, \mathcal{I})$ un matroïde et w une pondération quelconque. Pour montrér que GLOUTON(M,w) retourne un sous-ensemble optimal on utilise deux résultats.

Lemme 1 *Tous les sous-ensembles indépendents maximaux d'un matroïde ont la même taille.*

Preuve. Supposons au contraire que I_1, I_2 sont deux sous-ensembles indépendents maximaux et $|I_1| < |I_2|$. Alors, la propriété d'échange implique que $I_1 \cup \{e\} \in \mathcal{I}$ pour un certain $e \in I_2 - I_1$, ce qui contredit l'hypothèse d'un I_1 maximal. $\square$

Soit $B_G = \{e_1, e_2, \ldots, e_r\}$ la solution retourné par GLOUTON(M,w), où $w(e_1) \geq w(e_2) \geq \ldots \geq w(e_r)$. Soit $B = \{f_1, f_2, \ldots f_r\}$ un sous-ensemble indépendent maximal quelconque, où $w(f_1) \geq w(f_2) \geq \ldots \geq w(f_r)$. On montre ensuite une propriété plus forte de B_G (connu sur le nom d'*optimalité de Gale*).

Lemme 2 *Pour chaque $1 \leq i \leq r$, alors $w(e_i) \geq w(f_i)$.*

Preuve. Supposons le contraire. Soit k le premier entier tel que $w(e_k) < w(f_k)$. Soit $I_1 = \{e_1, \ldots, e_{k-1}\}$ et $I_2 = \{f_1, \ldots, f_{k-1}, f_k\}$. Comme $|I_1| < |I_2|$, il existe un élément $f_j \in I_2 - I_1$ tel que $I_1 \cup \{f_j\} \in \mathcal{I}$. Mais $w(f_j) \geq w(f_k) > w(e_k)$. Donc à l'itération k GLOUTON(M,w) doit choisir f_j et pas e_k. $\square$

Pour démontrer l'implication invérse, on suppose que I_1 et I_2 sont des sous-ensembles indépendents tel que $|I_1| < |I_2|$ mais $I_1 \cup \{e\} \notin \mathcal{I}$ pour chaque $e \in I_2 - I_1$. Comme $0 < |I_1 - I_2| < |I_2 - I_1|$ il exist un $\epsilon > 0$ tel que

$$0 < (1+\epsilon)|I_1 - I_2| < |I_2 - I_1|.$$

Soit $w : E \to R$ defini par

$$w(e) = \begin{cases} 2, \text{ si } e \in I_1 \cap I_2, \\ 1/|I_1 - I_2|, \text{ si } e \in I_1 - I_2, \\ (1+\epsilon)/|I_2 - I_1|, \text{ si } e \in I_2 - I_1, \\ 0, \text{ dans le cas contraire.} \end{cases}$$

L'algorithme glouton choisira les éléments de $I_1 \cap I_2$, ensuite les éléments de $I_1 - I_2$. Comme il peut pas prendre des éléments de $I_2 - I_1$, il choisira des éléments de $E - (I_1 \cup I_2)$. Par conséquent,

$$w(B_G) = 2|I_1 \cap I_2| + |I_1 - I_2|(1/|I_1 - I_2|) = 2|I_1 \cap I_2| + 1.$$

Soit I_2' un indépendent maximal que contient I_2. Donc,

$$w(I_2') \geq w(I_2) = 2|I_1 \cap I_2| + |I_2 - I_1|[(1+\epsilon)/|I_2 - I_1|] = 2|I_1 \cap I_2| + 1 + \epsilon > w(B_G),$$

ce qui contredit le caractère optimal de B_G. $\square$

Un problème intéressant pouvant être resolu grâce aux matroïdes est le *problème de l'ordonnancement optimal de tâches unitaires* sur un processeur unique, où chaque tâche dispose d'un temp limite d'exécusion au delà duquel une penalité doit être payée. On spécifie le problème de la façon suivant:

–un ensemble $E = \{1, 2, \ldots, n\}$ de n tâches unitaires;

–un ensemble de n dates échues $d_1, d_2, \ldots, d_n$, tel que chaque d_i vérifie $1 \leq d_i \leq n$ et la tâche i est supposée se terminer avant la date d_i;

–un ensemble de n pénalités positives $w_1, w_2, \ldots, w_n$, tel qu'une pénalité w_i est donnée si la tâche i n'est pas terminée avant la date d_i et aucune penalité n'est pas donnée si une tâche se termine avant sa date échue.

On souhaite trouver un ordonnancement de E qui minimise la somme des pénalités soubis pour non-respect des dates échue. On dit qu'un ensemble I des tâches est indépendent s'il existe un ordonnancement pour ces tâches tel qu'aucune de ces tâches ne soit en retard. Pour $t = 1, \ldots, n$ soit $N_t(I)$ le nombre de tâches de I dont la date échue est inférieure ou gale t. On voit bien que l'ensemble I est indpendent si et seulement si pour $t = 1, \ldots, n$ $N_t(I) \leq t$.

Proposition 11 *Si E est un ensemble de tâches unitaires et $\mathcal{I}$ la famille de tous les ensembles de tâches indépendents, alors le couple $(E, \mathcal{I})$ est un matroïde.*

Preuve. Pour prouver la propriété d'échange, on suppose que $I_1, I_2 \in \mathcal{I}$ et $|I_1| < |I_2|$. Soit k le plus grand t tel que $N_t(I_2) \leq N_t(I_1)$. Puisque $N_n(I_1) = |I_1|$ et $N_n(I_2) = |I_2|$ on doit avoir $k < n$ et $N_j(I_2) > N_j(I_1)$ pour tout j de l'intervalle $k + 1 \leq j \leq n$. Donc I_2 contient plus de tâches de date échue $k + 1$ que I_1. Soit e une tâche de $I_2 - I_1$ de date échue $k + 1$. Soit $I' = I \cup \{e\}$. Pour $1 \leq t \leq k$, on a $N_t(I') = N_t(I_1) \leq t$, et pour $k \leq t \leq n$ on a $N_t(I') \leq N_t(I_2) \leq t$, puisque I_1 et I_2 sont des indépendents. Donc $I' \in \mathcal{I}$. $\square$

4 Matroïdes II: un guide routard

Il existe une théorie élégante sur les matroïdes, que nous allons présenter dans cette section.

4.1 Les circuits

Un sous-ensemble dépendent minimal (par inclusion) d'un matroïd M est appellé *circuit*. Soit $\mathcal{C}$ (où $\mathcal{C}(M)$) l'ensemble de circuits de M. Il est facile à montrer les propriétés suivantes des circuits:

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

(C2) si $C_1, C_2 \in \mathcal{C}$ et $C_1 \subseteq C_2$, alors $C_1 = C_2$.

Lemme 3 *$\mathcal{C}$ vérifie la condition suivante*

(C3) si $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$ et $e \in C_1 \cap C_2$, alors il existe un circuit $C_3 \in \mathcal{C}$ tel que $C_3 \subseteq (C_1 \cup C_2) - e$.

Preuve. Supposons au contraire que $(C_1 \cup C_2) - e$ est un sous-ensemble indépendent de M. La propriété $(C2)$ implique que $C_2 - C_1 \neq \emptyset$, alors on peut choisir $f \in C_2 - C_1$. C_2 est un sous-ensemble dépendent minimal, alors $C_2 - f \in \mathcal{I}$. Soit $I \subset C_1 \cup C_2$ un sous-ensemble indépendent de taille maximale tel que $C_2 - f \subseteq I$. Evidemment $f \notin I$. Comme C_1 est un circuit, alors il existe $g \in C_1$ tel que $g \notin I$. Comme $f \in C_2 - C_1$, les éléments f et g sont différents. Donc

$$|I| \leq |(C_1 \cup C_2) - \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) - 1|.$$

On applique la propriété (I3) aux sous-ensembles I et $(C_1 \cup C_2) - e$. Le sous-ensemble résultant contredit le choix de I. □

Lemme 4 *Soit E un ensemble fini est $\mathcal{C}$ une famille de sous-ensembles de E qui vérifie les conditions (C1)-(C3). Soit $\mathcal{I}$ la famille de sous-ensembles de E qui contient aucun sous-ensemble de $\mathcal{C}$. Alors $(E, \mathcal{I})$ est un matroïde est $\mathcal{C}$ est sa famille de circuits.*

Preuve. $\emptyset \in \mathcal{I}$, puisque $\emptyset \notin \mathcal{C}$ par (C1). Si I contient aucun sous-ensemble de $\mathcal{C}$ et $I' \subset I$, alors I' contient aucun sous-ensemble de $\mathcal{C}$, donc $\mathcal{I}$ vérifie (I2).

Pour montrer (I3), soit $I_1, I_2 \in \mathcal{I}$, $|I_1| < |I_2|$. Supposons au contraire que (I3) est faux pour (I_1, I_2). $\mathcal{I}$ contient au moins un sous-ensemble de $I_1 \cup I_2$ de cardinalité plus grande que $|I_1|$. Soit I_3 un tel sous-ensemble avec $|I_1 - I_3|$ minimal. Comme (I3) est faux, $I_1 - I_3$ est non vide, alors il existe un élément $e \in I_1 - I_3$. Pour chaque élément $f \in I_3 - I_1$, soit $T_f := (I_3 \cup e) - f$. On a $T_f \subseteq I_1 \cup I_2$ et $|I_1 - T_f| < |I_1 - I_3|$. Donc $T_f \notin \mathcal{I}$, alors T_f contient un sous-ensemble C_f de $\mathcal{C}$. On observe que $f \notin C_f$. Aussi $e \in C_f$, en cas contraire $C_f \subset I_3$, que contredit le choix de $I_3 \subset \mathcal{I}$.

Soit $g \in I_3 - I_1$. Si $C_g \cap (I_3 - I_1) = \emptyset$, alors $C_g \subseteq ((I_1 \cap I_3) \cup e) - g \subseteq I_1$, que est impossible. Donc il existe un élément $h \in C_g \cap (I_3 - I_1)$. Comme $e \in C_g \cap C_h$, la condition (C3) implique q'il existe un sous-ensemble C de $\mathcal{C}$ tel que $C \subseteq (C_g \cup C_h) - e$. Comme C_g et C_h sont des sous-ensembles de $I_3 \cup e$, on obtien $C \subset I_3$, une contradiction. Donc $(E, \mathcal{I})$ est un matroïde. □

Les deux lemmes précédents conduisent au théorème suivant:

Théorème 12 *Soit $\mathcal{C}$ est une famille de sous-ensembles d'un ensemble fini E. Alors $\mathcal{C}$ est la famille de circuits d'un matroïde de M si et seulement si $\mathcal{C}$ vérifie les conditions suivantes:*

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

(C2) si $C_1, C_2 \in \mathcal{C}$ et $C_1 \subseteq C_2$, alors $C_1 = C_1$;

(C3) si $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$ et $e \in C_1 \cap C_2$, alors il existe un sous-ensemble $C_3 \in \mathcal{C}$ tel que $C_3 \subseteq (C_1 \cup C_2) - e$.

4.2 Les bases

Un sous-ensemble indépendent maximal d'un matroïde $M = (E, \mathcal{I})$ est appellé *base.* Soit $\mathcal{B}$ (où $\mathcal{B}(M)$) la famille de bases de M. On a deja montré que tous les bases ont la même taille. Une autre propriété simple:

(B1) $\mathcal{B}(M)$ est non vide.

La propriété suivante est moins triviale.

Lemme 5 *$\mathcal{B}$ vérifie la condition*

(B2) si $B_1, B_2 \in \mathcal{B}(M)$ et $x \in B_1 - B_2$, alors il existe un élément $y \in B_2 - B_1$ tel que $(B_1 - x) \cup y \in \mathcal{B}$.

Preuve. $B_1 - x$ et B_2 sont sous-ensembles indépendents. En plus, $|B_1 - x| < |B_2|$, donc il exist un élément $y \in B_2 - (B_1 - x)$ tel que $(B_1 - x) \cup y \in \mathcal{I}(M)$. Evidemment $y \in B_2 - B_1$. Puisque $(B_1 - x) \cup y$ est indépendent, il est contenu dans un sous-ensemble indépendent maximal B_1'. Alors, $|B_1'| = |B_1| = |(B_1 - x) \cup y|$. Donc $(B_1 - x) \cup y = B_1'$, i.e. $(B_1 - x) \cup y$ est une base de M. $\square$

Lemme 6 *Soit E un ensemble fini et $\mathcal{B}$ une famille de sous-ensembles de E que vérifie (B1) et (B2). Soit $\mathcal{I}$ la famille de sous-ensembles contenu dans les sous-ensembles de $\mathcal{B}$. Alors $(E, \mathcal{I})$ est un matroid et $\mathcal{B}$ est sa famille de bases.*

Preuve. Puisque $\mathcal{B}$ vérifie (B1), $\mathcal{I}$ vérifie (I1). Si $I' \subseteq I$ et $I \in \mathcal{I}$, alors $I' \subseteq I \subseteq B$ pour un certain $B \in \mathcal{B}$, donc (I2) est vérifie.

On montre ensuite que les sous-ensembles de $\mathcal{B}$ ont la même taille. Supposons non: il existe $B_1, B_2 \in \mathcal{B}$ tel que $|B_1| > |B_2|$ et $|B_1 - B_2|$ soit minimal. Evidemment, $B_1 - B_2 \neq \emptyset$. Alors, si $x \in B_1 - B_2$, on peut trouver un élément $y \in B_2 - B_1$, tel que $(B_1 - x) \cup y \in \mathcal{B}$. Mais $|(B_1 - x) \cup y| = |B_1| > |B_2|$ et $|((B_1 - x) \cup y) - B_2| < |B_1 - B_2|$, que contredit le choix de B_1 et B_2. Donc tous les sous-ensembles de $\mathcal{B}$ ont la même taille.

Montrons enfin (I3). Supposons que on peut trouver $I_1, I_2 \in \mathcal{I}$, $|I_1| < |I_2|$ tel que $I_1 \cup e \notin \mathcal{I}$ pour chaque $e \in I_2 - I_1$. Par la definition de $\mathcal{B}$, on peut choisir $B_1, B_2 \in \mathcal{B}$ tel que $I_1 \subseteq B_1$ et $I_2 \subseteq B_2$. On suppose de plus que B_2 minimise $|B_2 - (I_2 \cup B_1)|$. Par le choix de I_1 et I_2,

$$I_2 - B_1 = I_2 - I_1. \tag{1}$$

Supposons que $B_2 - (I_2 \cup B_1)$ est non vide. Soit $x \in B_2 - (I_2 \cup B_1)$. La propriété (B2) implique q'il existe $y \in B_1 - B_2$ tel que $(B_2 - x) \cup y \in \mathcal{B}$. Dans ce cas $|((B_2 - x) \cup y) - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$, en contradiction avec le choix de B_2. Donc $B_2 - (I_2 \cup B_1)$ est vide, alors $B_2 - B_1 = I_2 - B_1$. Le rélation (1) implique que

$$B_2 - B_1 = I_2 - I_1. \tag{2}$$

Montrons ensuite que $B_1 - (I_1 \cup B_2)$ est vide. Supposons non: soit $x \in B_1 - (I_1 \cup B_2)$ et $y \in B_2 - B_1$ tel que $(B_1 - x) \cup y \in \mathcal{B}$. Puisque $I_1 \cup y \subseteq (B_1 - x) \cup y$, alors $I_1 \cup y \in \mathcal{I}$. Comme $y \in B_2 - B_1$, l'égalité (2) implique que $y \in I_2 - I_1$, que contredit le choix de I_1 et I_2. Par conséquent, $B_1 - (I_1 \cup B_2)$ est vide, donc $B_1 - B_2 = I_1 - B_2$. Puisque $I_1 - B_2 \subseteq I_1 - I_2$, cela implique que

$$B_1 - B_2 \subseteq I_1 - I_2. \tag{3}$$

Comme $|B_1| = |B_2|$, on deduit que $|B_1 - B_2| = |B_2 - B_1|$. Alors, (2) et (3) impliquaient $|I_1 - I_2| \geq |I_2 - I_1|$, donc $|I_1| \geq |I_2|$, que contredit le choix de I_1 et I_2. $\square$

Théorème 13 *Soit $\mathcal{B}$ une famille de sous-ensembles d'un ensemble fini E. Alors $\mathcal{B}$ est la famille de bases d'un matroïde si est seulement si $\mathcal{B}$ vérifie les conditions suiventes:*

(B1) $\mathcal{B}$ est non vide;

(B2) Si $B_1, B_2 \in \mathcal{B}$ et $x \in B_1 - B_2$, alors il existe un élément $y \in B_2 - B_1$ tel que $(B_1 - x) \cup y \in \mathcal{B}$.

Note. Pour trouver un lien entre $\mathcal{B}(M)$ et $\mathcal{C}(M)$ on note que $\mathcal{B}(M)$ est la famille de sous-ensembles maximaux de E que contient aucun des sous-ensembles de $\mathcal{C}(M)$, et $\mathcal{C}(M)$ est la famille de sous-ensembles minimaux de E que sont contenu dans aucun des sous-ensembles de $\mathcal{B}(M)$.

4.3 La fonction de rang

Soit $M = (E, \mathcal{I})$ un matroïde et $X \subseteq E$. Soit $\mathcal{I}|X = \{I \subseteq X : I \in \mathcal{I}\}$. On peut vérifie facilement que $(X, \mathcal{I}|X)$ est un matroïde que on l'appelle la *restriction de M sur X* (notation: $M|X$ où $M \backslash (E - X)$). On peut montrer que

$$\mathcal{C}(M|X) = \{C \subseteq X : C \in \mathcal{C}(M)\}.$$

Comme $M|X$ est un matroïde, tous les bases sont de même cardinalité. On appelle *rang* de X la taile $r(X)$ d'une base de $M|X$. Evidemment, r est une application de 2^E dans l'ensemble des entiers naturels. Cette fonction, la *fonction de rang* de M, est noté par r où r_M. Les propriétés suivantes sont evident:

(R1) si $X \subseteq E$, alors $0 \leq r(X) \leq |X|$.

(R2) si $X \subseteq Y \subseteq E$, alors $r(X) \leq r(Y)$.

De plus:

Lemme 7 *La fonction de rang d'un matroïde M vérifie la propriété de sous-modularité: (R3) si X et Y sont des sous-ensembles de E, alors*

$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

Preuve. Por sela, soit $B_{X\cap Y}$ une base de $X\cap Y$. Alors $B_{X\cap Y}$ est un sous-ensemble indépendent de $M|(X \cup Y)$, donc il est contenu dans une base $B_{X\cup Y}$ de ce matroïde. Comme $B_{X\cup Y} \cap X$ et $B_{X\cup Y} \cap Y$ sont des sous-ensembles indépendents de $M|X$ et $M|Y$, alors

$$|B_{X\cup Y} \cap X| \leq r(X) \text{ et } |B_{X\cup Y} \cap Y| \leq r(Y).$$

Donc

$$r(X)+r(Y) \geq |B_{X\cup Y}\cap X|+|B_{X\cup Y}\cap Y| =$$

$$|(B_{X\cup Y} \cap X) \cup (B_{X\cup Y} \cap Y)| + |(B_{X\cup Y} \cap X) \cap (B_{X\cup Y)} \cap Y)| =$$

$$|B_{X\cup Y} \cap (X \cup Y)| + |B_{X\cup Y} \cap X \cap Y|$$

Puisque $B_{X\cup Y} \cap (X \cup Y) = B_{X\cup Y}$ et $B_{X\cup Y} \cap X \cap Y = B_{X\cap Y}$, alors

$$r(X) + r(Y) \geq |B_{X\cup Y}| + |B_{X\cap Y}| = r(X \cup Y) + r(X \cap Y).$$

□

Lemme 8 *Soit E un ensemble fini et $r : 2^E \to \mathbb{N}$ une fonction que vérifie les conditions (R1)-(R3). Soit $\mathcal{I}$ la famille de sous-ensembles X de E tel que $r(X) = |X|$. Alors $(E, \mathcal{I})$ est un matroïde avec la fonction de rang r.*

Preuve. On commence par un résultat auxiliaire.

Lemme 9 *Dans les conditions de lemme précedent, si X et Y sont deux sous-ensembles de E tel que $r(X \cup y) = r(X)$ pour chaque $y \in Y - X$, alors $r(X \cup Y) = r(X)$.*

Preuve. Soit $Y - X = \{y_1, \ldots, y_k\}$. Le preuve est par induction sur le nombre k. Le résultat est immediat si $k = 1$. Supposons que le résultat est vrai pour $k = n$ et on suppose que $k = n + 1$. Par l'hypothèse d'induction et (R3) on deduit que

$$\begin{aligned} r(X) + r(X) &= r(X \cup \{y_1, \ldots, y_n\}) + r(X \cup y_{n+1}) \\ &\geq r((X \cup \{y_1, \ldots, y_n\}) \cup (X \cup y_{n+1})) + r((X \cup \{y_1, \ldots, y_n\}) \cap (X \cup y_{n+1})) \\ &= r(X \cup \{y_1, \ldots, y_{n+1}\}) + r(X) \geq r(X) + r(X). \end{aligned}$$

Alors on a des egalités partout, donc

$$r(X \cup \{y_1, \ldots, y_n, y_{n+1}\}) = r(X).$$

□

Par (R1) $0 \leq r(\emptyset) \leq |\emptyset| = 0$, alors $r(\emptyset) = |\emptyset|$ et $\emptyset \in \mathcal{I}$, donc $\mathcal{I}$ vérifie (I1). Supposons $I \in \mathcal{I}$ et $I' \subseteq I$. Comme $r(I) = |I|$, (R3) implique

$$r(I' \cup (I - I')) + r(I' \cap (I - I')) \leq r(I') + r(I - I'),$$

alors

$$r(I) + r(\emptyset) \leq r(I') + r(I - I'). \tag{1}$$

Mais $r(I) = |I|$ et $r(\emptyset) = 0$. De plus, (R2) implique $r(I') \leq |I'|$ et $r(I - I') \leq |I - I'|$. In en résulte de (1) que

$$|I| \leq r(I') + r(I - I') \leq |I'| + |I - I'| = |I|.$$

Comme la prémier et la derniér quantités sont egaux, l'egalité doit être partout. Alors $r(I') = |I'|$, donc $I' \in \mathcal{I}$.

Il reste donc a montrer que $\mathcal{I}$ vérifie (I3). Pour cela, on suppose le contraire, i.e., q'il existe $I_1, I_2 \in \mathcal{I}$ tel que $|I_1| < |I_2|$ mais $I_1 \cup e \notin \mathcal{I}$ pour chaque $e \in I_2 - I_1$. Alors, $r(I_1 \cup e) \neq |I_1 \cup e|$ pour tous $e \in I_2 - I_1$. Les conditions (R1), (R2) et le choix de $I_1 \in \mathcal{I}$ implique que

$$|I_1| + 1 > r(I_1 \cup e) \geq r(I_1) = |I_1|,$$

alors $r(I_1 \cup e) = |I_1|$. D'après le lemme 23 où $X = I_1$ et $Y = I_2$, on deduit $r(I_1) = r(I_1 \cup I_2)$. Comme $|I_1| = r(I_1)$ et $r(I_1 \cup I_2) \geq r(I_2) = |I_2|$, donc $|I_1| \geq |I_2|$, une contadiction. Alors $\mathcal{I}$ vérifie (I3), donc $(E, \mathcal{I})$ est un matroïde. $\square$

Théorème 14 *Soit E un ensemble fini. Une fonction $r : 2^E \to \mathbb{N}$ est la fonction de rang d'un matroïde si est seulement si elle vérifie les conditions suivantes:*

(R1) si $X \subseteq E$, alors $0 \leq r(X) \leq |X|$;

(R2) si $X \subseteq Y \subseteq E$, alors $r(X) \leq r(Y)$;

(R3) si X et Y sont deux sous-ensembles de E, alors

$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

Proposition 12 *Soit $M = (E, \mathcal{I})$ un matroïde et $X \subseteq E$. Alors*

(i) X est indépendent ssi $|X| = r(X)$;

(ii) X est une base ssi $|X| = r(X) = r(M)$;

(iii) X est un circuit ssi $X \neq \emptyset$ et pour chaque $x \in X$ alors $r(X - x) = |X| - 1 = r(X)$.

Preuve. La preuve est immédiate. $\square$

4.4 La fermeture

Dans un espace vectoriel V, si un vecteur $\mathbf{v}$ est dans le sous-espace engendré par les vecteurs $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, alors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ et $\{\mathbf{v}_1, \ldots, \mathbf{v}_n, \mathbf{v}\}$ engendrent le même sous-espace. Soit $M = (E, \mathcal{I})$ un matroïde et r est sa fonction de rang. Soit $\sigma : 2^E \to 2^E$ une fonction tel que pour un sous-ensemble $X \subseteq E$

$$\sigma(X) = \{x \in E : r(X \cup x) = r(X)\}.$$

Cette fonction σ est appellé l'*operateur de fermeture* de M.

Lemme 10 *L'operateur de fermeture d'un matroïde vérifie les propriétes suivantes:*

(F1) si $X \subseteq E$, alors $X \subseteq \sigma(X)$;

(F2) si $X \subseteq Y \subseteq E$, alors $\sigma(X) \subseteq \sigma(Y)$;

(F3) si $X \subseteq E$, alors $\sigma(\sigma(X)) = \sigma(X)$;

(F4) si $X \subset E, x \in E$ et $y \in \sigma(X \cup x) - \sigma(X)$, alors $x \in \sigma(X \cup y)$ (la propriété d'échange de Mac Lane-Steinitz).

Preuve. (F1) est triviale. Pour montrer (F2), soit $X \subseteq Y$ et $x \in \sigma(X) - X$. Alors $r(X \cup x) = r(X)$. Donc, si B_X est une base de X, alors B_X est une base de $X \cup x$. Alors $Y \cup x$ contient une base $B_{Y \cup x}$ tel que $B_X \subseteq B_{Y \cup x}$ mais $x \notin B_{Y \cup x}$. Comme $B_{Y \cup x}$ est une base de Y, alors $r(Y \cup x) = |B_{Y \cup x}| = r(Y)$ et donc $x \in \sigma(Y)$, d'où l'inclusion $\sigma(X) \subseteq \sigma(Y)$ est immédiate.

Pour montrer (F3), on obsérve facilement que $\sigma(X) \subseteq \sigma(\sigma(X))$. Pour établir l'inclusion réciproque, soit $x \in \sigma(\sigma(X))$. Dans ce cas $r(\sigma(X) \cup x) = r(\sigma(X))$. Pour tous $y \in \sigma(X) - X$ on a $r(X \cup y) = r(X)$. La lemme 9 implique $r(X) = r(X \cup (\sigma(X) - X)) = r(\sigma(X))$. Donc $r(\sigma(X) \cup x) = r(X)$. La propriété (R2) implique $r(\sigma(X) \cup x) \geq r(X \cup x) \geq r(X)$. Alors on a des egalités partout, donc $x \in \sigma(X)$. Donc $\sigma(\sigma(X)) \subseteq \sigma(X)$ et (F3) est prouvé.

La preuve de (F4) est basé sur un résultat simple.

Lemme 11 *Si $X \subseteq E$ et $x \in E$, alors $r(X) \leq r(X \cup x) \leq r(X) + 1$.*

Preuve. Soit B_X une base de X. Alors B_X où $B_{X \cup x}$ est une base de $X \cup x$, donc $r(X \cup x)$ est $r(X)$ où $r(X) + 1$. $\Box$

Supposons $y \in \sigma(X \cup x) - \sigma(X)$. Alors $r(X \cup x \cup y) = r(X \cup x)$ et $r(X \cup y) \neq r(X)$. De cette inégalité et dérniere lemme on peut deduit que $r(X \cup y) = r(X) + 1$. Alors

$$r(X) + 1 = r(X \cup y) \leq r(X \cup y \cup x) = r(X \cup x) \leq r(X) + 1.$$

Donc $r(X \cup y \cup x) = r(X \cup y)$, alors $x \in \sigma(X \cup y)$. $\Box$

Lemme 12 *Soit $\sigma : 2^E \to 2^E$ une fonction que verifie les conditiones (F1)-(F4). Soit*

$$\mathcal{I} = \{X \subseteq E : x \notin \sigma(X - x) \text{ pour chaque } x \in X\}.$$

Alors $(E, \mathcal{I})$ est un matroïde.

Preuve. (I1) est evident. Soit $I \in \mathcal{I}$ et $I' \subseteq I$. Si $x \in I'$, alors $x \in I$, donc $x \notin \sigma(I - x)$. (F2) implique que $\sigma(I - x)$ contient $\sigma(I' - x)$, donc $x \notin \sigma(I' - x)$, i.e. $I' \in \mathcal{I}$. Alors $\mathcal{I}$ verifie (I2).

Pour (I3) on a besoin d'une nouvelle lemme.

Lemme 13 *Soit $X \subseteq E$ et $x \in E$. Si $X \in \mathcal{I}$ mais $X \cup x \notin \mathcal{I}$, alors $x \in \sigma(X)$.*

Preuve. Comme $X \cup x \notin \mathcal{I}$, il existe un élément $y \in X \cup x$ tel que $y \in \sigma((X \cup x) - y)$. Si $y = x$, le résultat de lemme est immédiat. Si non, alors $(X \cup x) - y = (X - y) \cup x$ et $y \in \sigma((X - y) \cup x) - \sigma(X - y)$. Donc (F4) implique que $x \in \sigma((X - y) \cup y) = \sigma(X)$. □

On montre ensuite (I3). Supposons par contraire q' on peut choisir $I_1, I_2 \in \mathcal{I}$, $|I_1| < |I_2|$ pour lesquelles (I3) est faux. Soit $|I_1 \cap I_2|$ plus grand possible. Soit $y \in I_2 - I_1$. Supposons $I_1 \subseteq \sigma(I_2 - y)$. Les conditiones (F2) et (F3) impliquaient $\sigma(I_1) \subseteq \sigma(I_2 - y)$. Comme $y \notin \sigma(I_2 - y)$, alors $y \notin \sigma(I_1)$. La lemme précédente implique $I_1 \cup y \in \mathcal{I}$, alors (I3) est vraie pour I_1 et I_2, une contradiction. Donc I_1 est pas contenu dans $\sigma(I_2 - y)$, alors on peut choisir $t \in I_1 - \sigma(I_2 - y)$. Evidemment $t \in I_1 - I_2$. Encore une référence au lemme précédente implique $(I_2 - y) \cup t \in \mathcal{I}$. Comme $|I_1 \cap ((I_2 - y) \cup t)| > |I_1 \cap I_2|$, (I3) est vraie pour la paire $(I_1, (I_2 - y) \cup t)$. Donc pour un certain $x \in ((I_2 - y) \cup t) - I_1$ l'ensemble $I_1 \cup x$ est dans $\mathcal{I}$. Comme $x \in I_2 - I_1$, (I3) est vérifié pour la paire (I_1, I_2), une contradiction. □

Théorème 15 *Soit E un ensemble fini. Une fonction $\sigma : 2^E \to 2^E$ est une fonction de fermeture d'une matroïde si et seulement si les conditiones (F1)-(F4) sont vérifié.*

Si $X = \sigma(X)$, alors X s'appelle un sous-ensemble *fermé* de M. Un *hyperplan* de M est un fermé X tel que $r(X) = r(M) - 1$. Un *générateur* de M est un sous-ensemble X de E tel que $\sigma(X) = E$.

Proposition 13 *Soit M un matroïde et X un sous-ensemble de E. Alors*
(i) X est un générateur ssi $r(X) = r(M)$;
(ii) X est une base ssi X est un générateur minimal;
(iii) X est un hyperplan ssi X est un sous-ensemble maximal non-générateur;
(iv) X est un circuit ssi X est un sous-ensemble minimal tel que $x \in \sigma(X - x)$ pour chaque $x \in X$;
(v) $\sigma(X) = X \cup \{x \in E :$ il exist un circuit C tel que $x \in C \subseteq X \cup x\}$.

Proposition 14 *Soit G un graphe connexe. Alors H est un hyperplan de M_G ssi $E - H$ est une coupe minimal de G.*

4.5 Dualité

Cette section étudie la notion de dualité dans les matroïdes.

Théorème 16 *Soit M un matroïde avec la famille de bases $\mathcal{B}(M)$. Alors la famille*

$$\mathcal{B}^*(M) := \{E - B : B \in \mathcal{B}(M)\}$$

est la famille de bases d'un matroïde.

Preuve. Le preuve utilise le résultat suivant.

Lemme 14 *La famille de bases de M vérifie la condition*

(B2)* si $B_1, B_2 \in \mathcal{B}(M)$ et $x \in B_2 - B_1$, alors il existe un élément $y \in B_1 - B_2$ tel que $(B_1 - y) \cup x \in \mathcal{B}(M)$.

Preuve. Soit $C(x, B_1)$ le circuit unique contenu dans $B_1 \cup x$. Comme $C(x, B_1)$ est dépendant et B_2 est indépendant, alors $C(x, B_1) - B_2$ est non vide. Soit y un élement de ce sous-ensemble. Evidemment $y \in B_1 - B_2$. Comme $(B_1 - y) \cup x$ ne contient pas $C(x, B_1)$, le dernier est indépendent. Finalement, comme $(B_1 - y) \cup x$ et B_1 sont de même taille, ce sous-ensemble est une base. □

$\mathcal{B}(M)$ est non-vide, alors $\mathcal{B}^*(M)$ est aussi non vide. Supposons $B_1^*, B_2^* \in \mathcal{B}^*(M)$ et $x \in B_1^* - B_2^*$. Soit $B_i = E - B_i^*$, $i = 1, 2$. Alors $B_1, B_2 \in \mathcal{B}(M)$ et $B_1^* - B_2^* = B_2 - B_1$. La propriété (B2)* implique que, comme $x \in B_2 - B_1$, il exist un élément $y \in B_1 - B_2$ tel que $(B_1 - y) \cup x \in \mathcal{B}(M)$. On peut déduire que $y \in B_2^* - B_1^*$ et $E - ((B_1 - y) \cup x) \in \mathcal{B}^*(M)$. Mais $E - ((B_1 - y) \cup x) = ((E - B_1) - x) \cup y = (B_1^* - x) \cup y$. Donc $\mathcal{B}^*(M)$ vérifie (B2), alors $\mathcal{B}^*(M)$ est la famille de bases d'un matroïde. □

Le matroïde de dernier théorème (avec $\mathcal{B}^*(M)$ comme famille de bases) est appellé le *dual* de M et est noté par M^*.

Corollaire 1 $(M^*)^* = M$.

Corollaire 2 *$\mathcal{B}$ est la famille de bases d'un matroïde ssi $\mathcal{B}$ vérifie les conditiones (B1) et (B2)*.*

Les bases de M^* sont appellé cobases de M. De manière analogue on peut definir les *cocircuits*, les *cohyperplans*, les *cogénérateurs*, les *coindépendents.*

Proposition 15 *Soit M un matroïde et X un sous-ensemble de E. Alors*
(i) X est un indépendent ssi $E - X$ est un cogénérateur;
(ii) X est un générateur ssi $E - X$ est un coindépendent;
(iii) X est un hyperplan ssi $E - X$ est un cocircuit;
(iv) X est un circuit ssi $E - X$ est un cohyperplan.
(v) C est un circuit ssi C est un sous-ensemble minimal tel que $|C \cap C^*| \neq 1$ pour chaque cocircuit C^*.

Soit M un matroïde et soit $\mathcal{B}, \mathcal{C}, \mathcal{H}, \mathcal{B}^*, \mathcal{C}^*$ et $\mathcal{H}^*$ les familles des bases, circuits, hyperplans, cobases, cocircuits et cohyperplans de M. Rappellons, que $b(\mathcal{A})$ est le bloquer d'une antichaine $\mathcal{A}$.

Proposition 16 $\mathcal{C}^* = b(\mathcal{B})$, $b(\mathcal{C}^*) = \mathcal{B}$, $\mathcal{C} = b(\mathcal{B}^*)$, $b(\mathcal{C}) = \mathcal{B}^*$.

Duals de matroïdes matriciels. Soit $M[A]$ le matroïde matriciel d'une matrice A. $M[A]$ rest intact si on effectuer des opérationes élémentaires sur les lignes où/et les colonnes de A. Il est bien connu que utilisent des opérationes de ce type on peut écrire A de façon $[I_r|D]$, où I_r est la matrice unitaire de taille $r \times r$ et D est une matrice de taille $r \times (n-r)$. Evidemment, r est le rang de $M[A]$, i.e., $r = r(M[A])$. Soit $e_1, e_2, \ldots, e_r, e_{r+1}, \ldots, e_n$ l'ordre des colonnes de matrice $[I_r|D]$. Supposons que les colonnes de matrice $[-D^T|I_{n-r}]$ sont ordonnée de même façon. Rappellons que le rang d'une matrice est le nombre maximal de colonnes linéaire indépendant (ou, de façon équivalent, le nombre maximal de lignes linéaire indépendent).

Théorème 17 *Si M est le matroïde matriciel de $[I_r|D]$, alors M^* est le matroïde matriciel de $[-D^T|I_{n-r}]$.*

Preuve. Soit B une base de M. Il suffit de montrer que $E - B$ et une base de matroïde de $[-D^T|I_{n-r}]$. Utilisent un rearrangement de lignes et des colonnes on peut supposer que il existe un tel $t \in \{0, 1, \ldots, r\}$ que $B = \{e_{r-t+1}, e_{r-t+2}, \ldots, e_r, e_{r+1}, \ldots, e_{2r-t}\}$. Alors $[I_r|D]$ peut être decomposé dans des bloques de façon suivant:

$$\left[\begin{array}{c} I_{r-t} || \ 0 \ |D_1||D_2 \\ \hline 0 \ \ ||I_t|D_3||D_4 \end{array}\right]$$

La matrice

$$\left[\begin{array}{c} 0 \ |D_1 \\ \hline I_t|D_3 \end{array}\right]$$

est de rang r car B est une base. Alors D_1 et $-D_1^T$ ont rang $r - t$. La partition de $[I_r|D]$ induit la partition suivante de $[-D^T|I_{n-r}]$:

$$\left[\begin{array}{c} -D_1^T|| - D_3^T|I_{r-t}|| \quad 0 \\ \hline - D_2^T|| - D_4^T| \ 0 \quad || \ I_{n-(2r-t)} \end{array}\right]$$

Dans cette matrice, la sous-matrice corréspondent à $E - B$ est

$$\left[\begin{array}{c} -D_1^T| \quad 0 \\ \hline - D_2^T| \quad I_{n-2(2r-t)} \end{array}\right]$$

Le rang de cette matrice est la summe de rangs de $I_{n-(2r-t)}$ et de $-D_1^T$, donc $(n - (2r - t)) + (r - t) = n - r$. Alors, $E - B$ est une base de matroïde de $[-D^T|I_{n-r}]$.
$\square$

Duals des matroïdes graphiques. Soit $M(G)$ le matroïde d'un graphe connexe G et soit $M^*(G)$ son dual. Pour lesquells graphes G le matroïde $M^*(G)$ est graphique?

Lemme 15 *Les matroïdes $M^*(K_5)$ et $M^*(K_{3,3})$ ne sont pas graphiques.*

Figure 1: Un matroïde affin de rang 4

Preuve. On presentera seulement la preuve pour $M = M^*(K_5)$ (le cas de $M^*(K_{3,3})$ est similair). Supposons que $M = M(G)$ pour un graphe connexe G. Le matroid $M(K_5)$ contient 10 éléments et son rang est 4. Donc M contient 10 elements et son rang est 6. Alors G contient 10 arêtes et 7 sommets. On peut déduire que G contient un sommet de degré ≤ 2 et on peut déduire que M^* contient un circuit de diménsion 1 ou 2 (rappelons que X est un circuit de M ssi X est un cocircuit de M^*). Donc K_5 contient un tel circuit, une contradiction. $\square$

Soit G un graphe planaire représenté dans le plan. G divide le plan en régions, appelé *faces*. On defini le *dual géométrique* G^* de G de façon suivant. On choisir un sommet v_F pour chaque face F de G. Ils sont les sommets de G^*. Deux sommets $v_{F'}, v_{F"}$ sont adjacent dans le graphe G^* par k arêtes $e'_1, \ldots e'_k$ ssi les faces F' et F'' contient k arêtes communes $e_1, \ldots, e_k$. On peur montrer facilement que $(G^*)^* = G$.

Proposition 17 *Si G^* est le dual géométrique d'un graphe planaire G, alors $M(G^*) = M^*(G)$.*

Théorème 18 *Le dual d'un matroïde graphique $M(G)$ est un matroïde graphique ssi G est un graphe planaire.*

4.6 La représentation géometrique de matroïdes de petit rang

Soit $S = \{\underline{v_1}, \ldots, \underline{v_k}\}$ un multi-ensemble de points de l'espace vectoriel V_m. On dit que les points de V_m sont *affinement dépendent* si il existe des nombres $a_1, a_2, \ldots, a_k$ aux moins un different de 0 tel que $\sum_{i=1}^{k} \underline{v_i} a_i = \underline{0}$ et $\sum_{i=1}^{k} a_i = 0$. De façon equivalent, S est affinement dépendent ssi l'ensemble de vecteurs $\{(1, \underline{v_1}), \ldots, (1, \underline{v_k})\}$ est linéairement dépendent en V_{m+1}. Un multi-ensemble S de V_m est *affinement indépendent* ssi il est pas affinement dépendent. Evidemment dans ce cas S est un ensemble.

Proposition 18 *Soit E un multi-ensemble de points de V_m. Soit $\mathcal{I}$ la famille de sous-ensembles X de E qui constituent un sous-ensemble affinement indépendent. Alors $(E, \mathcal{I})$ est un matroïde.*

Preuve. On peut facilement deduire que $(E, \mathcal{I}) = M[A]$, où A est la matrice de taille $(m+1) \times k$ avec $(1, \underline{v_i})^T$ come colonne i. $\square$

Le matroïde $(E, \mathcal{I})$ est appelé *matroïde affin.* In général, si M est un matroïde affin de rang $m + 1 \leq 4$, alors un sous-ensemble X de E est dépendent si dans la représentation de M en R^m où X contient deux points identiques, où trois points collineairs, où quatre points dans un plan, où cinq points. Donc les sous-ensembles fermes de M de rang un, deux, où trois sont représenté géometriquement par points, lignes, et plans.

Chaque un des diagrammes de Fig.2 représent un martoïde. De théorème de Pappus on peut deduire que le deuxième matroïde on peut pas le représenté comme un matroïde affin. La caractérisation des matroïdes représentables (affines) rest un problème ouvert tres difficile.

Figure 2: Le matroïde Pappus et le matroïde non-Pappus

5 Oriented matroids: a clin d'oeil

In this lecture we will present a brief course on oriented matroids. Before giving their definition and characterizations, we will present two important examples.

5.1 Oriented matroids from directed graphs.

Let us consider the simple cycles of a directed graph $D = (V, E)$ with arc set E, together with an orientation of each such cycle. Then every arc of a cycle is either a forward (positive) arc or a backward (negative) arc of this cycle. This allows us to consider the cycles as signed subsets of E, which consists of a positive and a negative part. Such a signed subset coming from a cycle (actually a cycle of the underlying graphic matroid) is called a *signed circuit* of D. In general, we will write $C = (C^+, C^-)$ for such signed sets, where $C^+ \cap C^- = \emptyset$. We will call C^+ the set of *positive elements* and C^- the set of *negative elements*. Note that if we reverse the orientation of C, then we will obtain the "opposite" signed set $-C = (C^-, C^+)$. The signed circuits obtained from a digraph D in this way form the collection

$$\mathcal{C} = \{C = (C^+, C^-) : C \text{ is a signed circuit of } D\}.$$

The *oriented matroid* $\mathcal{M} = \mathcal{M}_D$ of D is the pair $(E, \mathcal{C})$. Note that it contains a pair of opposite signed circuits $\pm C$ for every circuit of the *underlying matroid* $\underline{\mathcal{M}} = (E, \underline{\mathcal{C}})$, where $\underline{\mathcal{C}} = \{\underline{C} : C \in \mathcal{C}\}$ is simply the collection of undirected simple cycles of the graph.

By a minimal cut of D we mean a partition $V = V_1 \cup V_2$ of the vertices such that removing the arcs between V_1 and V_2 increases the number of components of the underlying graph. Letting Y^+ be the forward arcs of this cut, i.e. the arcs from V_1 to V_2, and Y^- the backward arcs from V_2 to V_1, we again get signed sets $Y = (Y^+, Y^-)$. We will call them the *signed cocircuits* of D, and denote

$$\mathcal{C}^* = \{Y = (Y^+, Y^-) : Y \text{ is a cocircuit of } D\}.$$

Before we continue our discussion, we will give a method for encoding signed sets. It records every signed sets by its signed incidence vector in $\{+1, -1, 0\}^E$, or shorter, in $\{+, -, 0\}^E$. Thus X with $X^+ = \{2, 6\}, X^- = \{1, 5\}$ is now represented by $X = (-+00-+)$.

We have now seen how to get the collection of signed circuits and signed cocircuits from a digraph D. It is then easy to derive the analogous of the usual matroid axioms for signed circuits and cocircuits. Namely,

(OC0) $\emptyset$ is not a signed circuit.

(OC1) If C is a signed circuit, then so is $-C$.

(OC2) No proper subset of a circuit is a circuit.

(OC3) If C_1 and C_2 are signed circuits with $C_1 \neq C_2$ and $e \in C_1^+ \cap C_2^-$, then there is a third circuit C with $C^+ \subseteq (C_1^+ \cup C_2^+) - \{e\}$ and $C^- \subseteq (C_1^- \cup C_2^-) - \{e\}$.

Exercise. Check that these axioms are satisfied by the signed circuits and cuts of digraphs.

Finally, we observe the important orthogonality property: if a directed cycle traverses a cut, then it also have to traverse it in the opposite direction. This translate into the following property for oriented matroids. Let

$$S(X,Y) := (X^+ \cap Y^-) \cup (X^- \cap Y^+)$$

denote the *separation set* of two sign vectors X and Y. Then the orthogonality condition can be written as

($\perp$) If X is a circuit and Y a cocircuit, then $S(X,-Y) \neq \emptyset$ if and only if $S(X,Y) \neq \emptyset$.

Why orthogonality property? This expresses the fact (in a weak but unique possible form) that if two vectors x, y of a vector space are orthogonal and $x_i y_i > 0$ for some i then must be a coordinate j for which $x_i x_j < 0$.

For two arbitrary sign maps $X, Y \in \{+,-,0\}^E$, we will write $X \perp Y$ and say that X and Y are *orthogonal* if the sets $S(X,Y)$ and $S(X,-Y)$ are either both empty or both non-empty.

Actually, for graphs the circuits and cocircuits are orthogonal in the usual sense. Indeed, the scalar product of the incidence vectors of a circuit and a cocircuit equals the number of times the circuit traverses the cut in one direction minus the number of times it traverses this cut in the opposite direction.

For graphs we have the following analogous of the Farkas lemma.

Lemme 16 *For every edge e of a digraph $D = (V,E)$ either there is a circuit X with $e \in X$ and $X^- = \emptyset$ or there is a cocircuit Y such that $e \in Y$ and $Y^+ = \emptyset$ but noth both.*

The result follows from the next claim applied to the graph $D - e$ and the endvertices of $e = (v,u)$.

Claim. Let $G = (V,E)$ be a connected graph and $u, v \in V$. Then either there is a $u{-}v$-path P with $P^- = \emptyset$ or there is a $u - v$-cut Y with $Y^+ = \emptyset$.

Indeed, let V_1 be the set of vertices reached from u by a directed path. If $v \in V_1$ then we get the first situation. Otherwise, all edges of the cut $(V_1, X - V_2)$ are directed from $V - V_1$ to V_1, thus we found a $u - v$-cut Y with $Y^+ = \emptyset$.

5.2 Point configuration and hyperplane arrangements

There are several closely related ways in which oriented matroids arise from geometric configurations in vector spaces.

Vector configurations. Given a finite set $E = \{v_1, \ldots, v_n\}$ of vectors that spans a vector space of dimension r as we mentioned already, the minimal linear dependences yield the circuits of a matroid of rank r. A minimal linear dependence looks like

$$\sum_{i=1}^{n} \lambda_i v_i = 0$$

with $\lambda_i \in R$. Here the sets $\underline{C} := \{i : \lambda_i \neq 0\}$ corresponding to the minimal linear dependences are the circuits of the (unoriented) matroid For the associated *oriented matroid*, we consider the signed sets $C = (C^+, C^-)$ given by

$$C^+ = \{i : \lambda_i > 0\}, C^- = \{i : \lambda_i < 0\}$$

for all the minimal dependences among the v_i. This yiels the oriented matroid of a vector configuration E in terms of its collection $\mathcal{C}$ of signed circuits. Note that the coefficients of a minimal linear dependence are unique up to a common scalar. This means that for a given circuit $\underline{C}$ of the matroid, there are exactly two signed circuits, namely $C = (C^+, C^-)$ and (C^-, C^+).

It can be verified that $\mathcal{C}$ obeys the axioms stated in the previous section. Actually (OC1) and (OC2) are clear from the definition, (OC3) needs some work.

The bases of a matroid are exactly the subsets of vectors which define matrices whose determinants are nonzero: $\{v_{i_1}, \ldots, v_{i_r}\}$ is a basis if and only if $det(v_{i_1}, \ldots, v_{i_r}) \neq 0$. For a vector configuration E we consider the sighs of the determinants of ordered r-subsets of $\{v_1, \ldots, v_n\}$. This leads us to define the *basis orientation* or *chirotope* of a vector configuration, by

$$\chi(i_1, \ldots, i_r) := sign(det(v_{i_1}, \ldots, v_{i_r})) \in \{+, -, 0\}.$$

Note that χ is an antisymmetric function. In addition to this, the determinants also satisfy further relations, known as the *Grassmann-Pluecker relations:* for all $v_1, \ldots, v_r, w_1, \ldots, w_r$ we have the identity:

$$det(x_1, x_2, \ldots, x_r) \cdot det(y_1, y_2, \ldots, y_r) = \sum_{i=1}^{r} det(y_i, x_2, \ldots, x_r) \cdot det(y_1, \ldots, y_{i-1}, x_1, y_{i+1}, \ldots, y_r).$$

If these relations are reduced to the sign patterns they imply, then one obtains the *basis axioms* for oriented matroids.

We can also interpret the cocircuits of a vector configuration: for this consider any linear hyperplane H spanned by some subset of E and let Y_H^+ be the set of vectors on one side of H and let Y_H^- be the set of vectors on the other side of H. Then the cocircuits are exactly the signed sets that arise as $Y := (Y_H^+, Y_H^-)$ in this way. two signed circuits, namely $C = (C^+, C^-)$ and (C^-, C^+).

It can be verified that $\mathcal{C}$ obeys the axioms stated in the previous section. Actually (OC1) and (OC2) are clear from the definition, (OC3) needs some work.

The bases of a matroid are exactly the subsets of vectors which define matrices whose determinants are nonzero: $\{v_{i_1}, \ldots, v_{i_r}\}$ is a basis if and only if $det(v_{i_1}, \ldots, v_{i_r}) \neq 0$. For a vector configuration E we consider the sighs of the determinants of ordered r-subsets of $\{v_1, \ldots, v_n\}$. This leads us to define the *basis orientation* or *chirotope* of a vector configuration, by

$$\chi(i_1, \ldots, i_r) := sign(det(v_{i_1}, \ldots, v_{i_r})) \in \{+, -, 0\}.$$

Note that χ is an antisymmetric function. In addition to this, the determinants also satisfy further relations, known as the *Grassmann-Pluecker relations:* for all $v_1, \ldots, v_r, w_1, \ldots, w_r$ we have the identity:

$$det(x_1, x_2, \ldots, x_r) \cdot det(y_1, y_2, \ldots, y_r) = \sum_{i=1}^{r} det(y_i, x_2, \ldots, x_r) \cdot det(y_1, \ldots, y_{i-1}, x_1, y_{i+1}, \ldots, y_r).$$

If these relations are reduced to the sign patterns they imply, then one obtains the *basis axioms* for oriented matroids.

We can also interpret the cocircuits of a vector configuration: for this consider any linear hyperplane H spanned by some subset of E and let Y_H^+ be the set of vectors on one side of

H and let Y_H^- be the set of vectors on the other side of H. Then the cocircuits are exactly the signed sets that arise as $Y := (Y_H^+, Y_H^-)$ in this way.

Point configurations. Every vector configuration in R^r corresponds to an affine point configuration in an $(r-1)$-dimensional affine space and vice versa. So the oriented matroids from point configurations will not be something new. Nethertheless, it is quite instructive to consider them.

In this example $E = \{x_1, \ldots, x_n\}$ is a set of n points in affine space R^d. The *affine dependences* of X are the vectors $\lambda \in R^n$ with $\sum_{i=1}^n \lambda_i$ such that $\sum_{i=1} \lambda_i x_i = 0$. These vectors λ form a vector subspace $Dep(X)$ of R^n. Geometrically, let λ be an affine dependence. Then we can look at the set of negative and positive coordinates of λ, $N(\lambda) = \{i : \lambda_i < 0\}$ and $P(\lambda) = \{i : \lambda_i > 0\}$. Let $\Lambda := \sum_{i \in P(\lambda)} \lambda_i = -\sum_{i \in N(\lambda)} \lambda_i > 0$. By multiplying with $\frac{1}{\Lambda}$ we can rewrite the affine dependence λ as

$$\sum_{i \in P(\lambda)} \frac{\lambda_i}{\Lambda} x_i = \sum_{i \in N(\lambda)} \frac{-\lambda_i}{\Lambda} x_i =: y,$$

so that

$$y \in conv\{x_i : i \in P(\lambda)\} \cap conv\{x_i : i \in N(\lambda)\}$$

represents a point that lies in both convex hull of the points with positive coefficients and the points with the negative coefficients. In particular, we are interested in the special case of affine dependences involving a minimal set of points from X. For them the corresponding convex hulls are simplices whose relative interiors intersect in a unique point y. Such configurations are known as *minimal Radon partitions.* Thus the *signed circuits* of the orented matroid of X are the sign vectors corresponding to minimal affine dependences of the points in X. The *signed vectors* of this oriented matroid are sign vectors corresponding to affine dependences of the point in X. To find these vectors and circuits, we take the vector subspace $Dep(X)$ and take the sign vectors of respective vectors from $Dep(X)$. The circuits will be the sign vectors corresponding to *elementary vectors* of $Dep(X)$, i.e. vectors with minimal support (the *support* of a vector λ is the set $P(\lambda) \cup N(\lambda)$).

From every affine function f on R^d of the form $f(x) = cx - z$, for $c \in (R^d)^*, z \in R$, we get a vector called an *affine value vector,*

$$(f(x_1), \ldots, f(x_n)) = (cx_1 - z, \ldots, cx_n - z)$$

which records the values of $cx - z$ on the points x_i of X. We note that the set $Val(X)$ of affine value vectors is a vector subspace of $(R^n)^*$. Geometrically, the sign vector of an affine value vector records which points of X are on the positive side $H_f^+ - H_f = \{x \in R^n : f(x) > 0\}$ of the hyperplane H_f, on H_f itself, or on the negative side of H_f. The *signed covectors* of X are the sign vectors corresponding to affine functions of the points in X. The *signed cocircuits* of X are the signed covectors of minimal support, for which the hyperplane H_f is spanned by points in X.

Hyperplane arrangements. Let $\mathcal{A} = \{H_1, \ldots, H_n\}$ be a *hyperplane arrangements*, that is, a finite set of hyperplanes throught the origin in R^r. Where is the matroid? Every hyperplane is given by a linear function $l_i(x) = \sum_{i=1}^r a_{ij} x_j$, so we can write $H_i = \{x \in R^r : l_i(x) = 0\}$. Now we can interpret the l_i as vectors in the dual space $(R^r)^*$. So the l_i form a vector configuration in $(R^r)^*$, which determines an oriented matroid (as before). This is the oriented matroid we associate with $\mathcal{A}$. In fact, with the choice of l_i we have distinguished a positive side of every hyperplane H_i given by $H_i^+ = \{x \in R^r : l_i \geq 0\}$, and the oriented matroid corresponds to the arrangement of halfspaces $\{H_i^+ : 1 \leq i \leq n\}$. Equivalently, via $S_i^+ := H_i^+ \cap S^{r-1}$ we get an *arrangement of hemispheres* $\mathcal{S} = \{S_i^+ : 1 \leq i \leq n\}$ on the sphere $S^{r-1} = \{x \in R^r : ||x|| = 1\}$.

One can ask: arrangements of halfspaces give rise to vector configurations and vice versa; so why do we study hyperplanes arrangements in connection with oriented matroids, if they are trivial reformulations of vector configurations? The answer is that thre are two nice aspects of this way of viewing realisable oriented matroids. First, not only every arrangement of hyperplanes give rise to an oriented matroid but the converse is nearly true: every oriented matroid comes from an arrangements of pseudohyperplanes or pseudospheres. Second, oriented matroids encodes a lot of geometric information about the hyperplane arrangement in a very simple and explicit way. For this observe that every hyperplane arrangement decomposes the spaces into a collection of pieces. Each of these cells is exactly determined by the information whether for the hyperplane H_i, the cell is on its positive side, its negative side, or on the hyperplane itself. This leads us to associate a sign vector with every cell. These sign vectors are exactly the covectors of the oriented matroid. If the hyperplanes of $\mathcal{A}$ share only the origin, then the origin get the zero string as its covector, while the one-dimensional rays corresponds to the cocircuits of the oriented matroid.

A *maximal vector* is a vector whose support is maximal with respect to the inclusion. A *maximal covector* is a covector whose support is maximal with respect to the inclusion. Maximal covectors are usually called *topes*. They correspond to the open cell in an arrangement of hyperplanes

5.3 Axiomatics

A *signed set* X is a set $\underline{X}$ together with a partition (X^+, X^-) into two distinguished subsets: X^+ the set of *positive elements* and X^- the set of *negative elements*. The set $\underline{X} = X^+ \cup X^-$ is the *support* of X. By $X = Y$ we mean $X^+ = Y^+$ and $X^- = Y^-$. A signed subset of a finite set E can be identified with an element of $\{-, 0, +\}^E$.

The opposite of a signed set X, denoted by $-X$ is the signed set with $(-X)^+ = X^-$ and $(-X)^- = X^+$.

Circuits. A collection $\mathcal{C}$ of signed subsets of a set E is the set of *signed circuits* of an *oriented matroid* on E if and only if it satisfies the following axioms:

(OC0) $\emptyset \notin \mathcal{C}$,

(OC1) $\mathcal{C} = -\mathcal{C}$,

(OC2) for all $X, Y \in \mathcal{C}$, if $\underline{X} \subseteq \underline{Y}$, then $X = Y$ or $X = -Y$,

(OC3) for all $X, Y \in \mathcal{C}$, $X \neq -Y$, and $e \in X^+ \cap Y^-$, there is a $Z \in \mathcal{C}$ such that

$$Z^+ \subseteq (X^+ \cup Y^+) - \{e\}$$

and

$$Z^- \subseteq (X^- \cup Y^-) - \{e\}.$$

By forgetting signs, (OC0),(OC2), and (OC3) reduce to the axioms of ordinary matroids. Thus the circuits supports of an oriented matroid $\mathcal{M}$ constitute the circuits of a matroid $\underline{\mathcal{M}}$ called the *underlying matroid of* $\mathcal{M}$.

Let V be a linear subspace of R^E. The signed support $s(u)$ of a vector $u \in V$ is the signed set defined by $s^+(u) = \{e \in E : u(e) > 0\}$ and $s^-(u) = \{e \in E : u(e) < 0\}$. Let $\mathcal{V} = Supp(V)$ be the set of signed supports of all vectors of V, and let $\mathcal{C} = Min(\mathcal{V})$, the subset of inclusion-minimal (non-empty) signed supports.

Théorème 19 *$\mathcal{C}$ is the set of circuits of an oriented matroid.*

Proof. Clearly $\mathcal{C}$ satisfies (OC0) and (OC1). To prove (OC2), suppose there exist $X, Y \in \mathcal{C}$ such that $\underline{X} \subseteq \underline{Y}$ but $X \neq Y$ and $X \neq -Y$. By minimality X and Y have the same support. Let $u, v \in V$ such that $X = s(u)$ and $Y = s(v)$. Then u, v are two non-zero vectors with the same support which are not proportional. Let $e \in \underline{X}$. Then the vector $w = u - \frac{u(e)}{v(e)}v \in V$ is non-zero, and its support satisfies $s(w) \subseteq s(u) - e$. This contradicts the minimality of $X = s(u)$.

Let us see that (OC3) holds for $\mathcal{V}$. Let $X, Y \in \mathcal{V}, X \neq -Y$, and $e \in X^+ \cap Y^-$. By definition of $\mathcal{V}$ there are $u, v \in V$ such that $X = s(u)$ and $Y = s(Y)$. We have $u(e) > 0$ and $v(e) < 0$. The vector $w = u - \frac{u(e)}{v(e)}v$ is a non-zero linear combination of u and v with positive coefficients such that $e \notin s(w)$. Set $Z = s(w) \in \mathcal{V}$. One can easily see that Z is positive (resp. negative) in $x \neq e$ if x is positive (resp. negative) in at least one of X or Y. Thus $\mathcal{V}$ verifies (OC3). However, Z need not be a circuit. We have to replace $s(w)$ by a minimal dependence whose sign is compatible with $s(w$. We show that this is always possible.

Claim. Let $\mathcal{S} \subseteq \{-, 0, +\}^E$ be such that $0 \notin \mathcal{S}, \mathcal{S} = -\mathcal{S}$ and $\mathcal{S}$ verifies the signed elimination axiom (OC3). Then

(i) for any $X \in \mathcal{S}$ there is $Y \in Min(\mathcal{S})$ with $Y^+ \subseteq X^+$ and $Y^- \subseteq X^-$;

(ii) $Min(\mathcal{S})$ verifies (OC3).

Proof. Suppose X is positive (otherwise use reorientation). Let $Y \in \mathcal{S}$ such that $\underline{Y} \subseteq \underline{X}$ and $|Y|$ is as small as possible. If $Y \in Min(\mathcal{S})$ then $X \in Min(\mathcal{S})$ and we are done. Otherwise consider $Z \in Min(\mathcal{S})$ with $\underline{Z} \subseteq \underline{Y}$ such that $|Z^-|$ minimal. By definition of Z we have $Z^- \neq \emptyset$. Applying (OC3) to Y, Z and $e \in Y^+ \cap Z^-$, there is $Z' \in \mathcal{S}$ with $\underline{Z'} \subseteq \underline{Y} - e$ and $|Z'^-| < |Z^-|$, a contradiction.

We now prove (OC3) for Min($\mathcal{S}$). Let $X, Y \in Min(\mathcal{S}), X \neq -Y$, and $e \in X^+ \cap Y^-$. Applying (OC3) to X, Y and e, there is $Z' \in \mathcal{S}$ such that $Z'^+ \subseteq (X^+ \cup Y^-) - e$ and $Z'^- \subseteq (X^- \cup Y^-) - e$. By (i) there is $Z \in Min(\mathcal{S})$ which is a restriction of Z'. We have $Z^+ \subseteq (X^+ \cup Y^+) - e$ and $Z^- \subseteq (X^- \cup Y^-) - e$ as desired.

Duality. Two signed sets X, Y are said to be *orthogonal*, denoted by $X \perp Y$, if either $\underline{X} \cap \underline{Y} = \emptyset$, or the restriction of X and Y to their intersection are neither equal nor opposite, i.e. there are $e, f \in \underline{X} \cap \underline{Y}$ such that $X(e)Y(e) = -X(f)Y(f)$.

Proposition 19 *Let $\mathcal{M}$ be an oriented matroid on a set E with set of circuits $\mathcal{C}$.*

(i) There is a unique signature $\mathcal{C}$ of the cocircuits of $\underline{\mathcal{M}}$ such that

$$(\perp) \qquad X \perp Y \textit{ for all } X \in \mathcal{C}, Y \in \mathcal{C}^*$$

.

(ii) The collection $\mathcal{C}^*$ is the set of (signed) circuits of an oriented matroid on E called the dual (or orthogonal) of $\mathcal{M}$ and denoted by $\mathcal{M}^*$.

(iii) We have $\mathcal{M}^{**} = \mathcal{M}$.

Théorème 20 *Let M be a matroid, let $\mathcal{C}$ be a circuit signature of M and $\mathcal{C}^*$ a cocircuit signature of M. Then the following conditions are equivalent:*

($\perp$) $\mathcal{C}$ *and* $\mathcal{C}^*$ *are the circuits collections of a pair of dual oriented matroids.*

($\perp'$) $X \perp Y$ *for all* $X \in \mathcal{C}$ *and* $Y \in \mathcal{C}^*$.

The following characterization is an analogous of the Minty's lemma for directed graphs (used to prove the mincut-maxflow theorem).

Théorème 21 *(painting axioms) Let $\mathcal{C}$ and $\mathcal{C}^*$ be two collections of signed subsets of a set E. Then $\mathcal{C}$ is the set of of circuits and $\mathcal{C}^*$ is the set of cocircuits of an oriented matroid on E if and only if they both satisfy (OC0), (OC1). (OC2) and (3P)*

(3P) for all 3-partitions $E = B \cup G \cup R$ and $e \in B$ either there is an $X \in \mathcal{C}$ such that $e \in \underline{X} \subseteq B \cup G$ and $\underline{X} \cap B \subseteq X^+$, or there is a $Y \in \mathcal{C}^*$ such that $e \in \underline{Y} \subseteq B \cup R$ and $\underline{Y} \cap B \subseteq Y^+$, but not both.

Exercise. Prove Minty's lemma for directed graphs.

Specializing (3P) for the case $G = R = \emptyset$ we get the following version of Farkas Lemma.

Corollaire 3 *Any element of an oriented matroid belongs either to a positive circuit or to a positive cocircuit, but not to both.*

Basis orientation and chirotopes. A basis orientation of an oriented matroid $\mathcal{M}$ is a mapping χ of the set of ordered bases of $\mathcal{M}$ to $\{-,+\}$ satisfying the following two properties:

(OB1) χ is alternating.

(PV) for any two ordered bases of $\mathcal{M}$ of the form $(e, x_2, \ldots, x_r)$ and $(f, x_2, \ldots, x_r), e \neq f$, we have

$$\chi(f, x_2, \ldots, x_r) = -C(e)C(f)\chi(e, x_2, \ldots, x_r),$$

where C is one of the two opposite signed circuits of $\mathcal{M}$ in the set $\{e, f, x_2, \ldots, x_r\}$.

If χ is a basis orientation of $\mathcal{M}$ we can read the signature of signed circuits of $\mathcal{M}$ as follows. For a circuit $\underline{C}$ of $\underline{\mathcal{M}}$ choose the elements $x_1, \ldots, x_r, x_{r+1}$ such that $\underline{C}$ is contained in $\{x_1, \ldots, x_r, x_{r+1}\}$ and $\{x_1, \ldots, x_r\}$ is a basis of $\underline{\mathcal{M}}$. Then

$$C(x_i) = (-1)^i \chi(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{r+1}).$$

Given an oriented matroid in terms of its signed circuits $\mathcal{C}$ its basis orientation can be computed as follows. Assuming that the ground set E is ordered, we identify each base $B = \{x_1, x_2, \ldots, x_r\}$ of $\underline{\mathcal{M}}$ with its increasing permutation. Now, the *basis graph* $BG_{\underline{\mathcal{M}}}$ of the matroid $\underline{\mathcal{M}}$ has as vertices the bases and as edges the pairs of bases that differ in exactly one element. Note that this graph is clearly connected. For an edge $\{B_1, B_2\}$ of the basis graph we define a sign $\nu(B_1, B_2)$ by the following rule: if $B_1 = (x_1, \ldots, x_r), B_2 = (y_1, \ldots, y_r), B_1 \Delta B_2 = \{x_i, y_j\}$, and if $C \in \mathcal{C}$ is one of the two opposite circuits contained in $B_1 \cup B_2$, then

$$\nu(B_1, B_2) = (-1)^{1+i+j} C(x_i)C(y_j).$$

This way we get the signed basis graph $SBG(\mathcal{M})$ of the oriented matroid $\mathcal{M}$. To construct the basis orientation χ from $SBG(\mathcal{M})$ it is sufficient to determine the values $\chi(B)$ for increasingly ordered bases B. Put $\chi(B_0) = +1$ for some arbitrary chosen basis B_0. Then, for any other basis B,

$$\chi(B) = \prod_{i=1}^{k} \nu(B_{i-1}, B_i)$$

where $B_0, B_1, B_2, \ldots, B_k = B$ is an arbitrary path from B_0 to B in the basis graph!

A *chirotope* of rank r on E is a mapping $\chi : E^r \to \{-, 0, +\}$ which satisfies the following three properties:

(OB0) χ is not identically zero;

(OB1) χ is alternating, that is, $\chi(x_{\sigma_1}, \ldots, x_{\sigma_r}) = sign(\sigma)\chi(x_1, \ldots, x_n)$ for all $x_1, \ldots, x_n \in E$ and every permutation.

(OB2) for all $x_1, \ldots, x_r, y_1, \ldots, y_r \in E$ such that

$$\chi(y_i, x_2, \ldots, x_r) \cdot \chi(y_1, \ldots, y_{i-1}, x_1, y_{i+1}, \ldots, y_r) \geq 0$$

for $i = 1, 2, \ldots, r$, we have

$$\chi(x_1, x_2, \ldots, x_r) \cdot \chi(y_1, y_2, \ldots, y_r) \geq 0.$$

Axiom (OB2) is a signed version of the Grassmann-Pluecker relations for r-order determinants.

Théorème 22 *A mapping $\chi : E^r \to \{-, 0, +\}$ is a basis orientation of an oriented matroid of rank r on E if and only if it is a chirotope.*

5.4 Arrangements of pseudohyperplanes, pseudospheres and oriented matroids

We will now start to discuss one topic where nonrealizable oriented matroids come up-the study of pseudoline arrangements. To make a connection, consider an arrangementt $\mathcal{A}$ of n hyperplanes in R^d (all hyperplanes through the origin). To draw an represent this, we consider the intersection with an affine hyperplane: a hyperplane not through the origin, but parallel to one of the hyperplanes of $\mathcal{A}$. Thus we get an *affine arrangement* of $n-1$ affine hyperplanes. The entire combinatorial structure $\mathcal{A}$ can easily be reconstructed from its "affine picture", so nothing is lost by this reduction. In particular, one can read off the oriented matroid of $\mathcal{A}$ from the affine arrangement, asuming that the affine hyperplanes are labeled and that positive sides are determined.

However, it turns out that if we have an arrangement of "nonstraight" lines in the plane, then we can also, in some way read off an oriented matroid of rank 3. A *pseudoline* is a polygonal curve without sel-intersections with finitely many break-points in R^2 and whose ends go to infinity in opposite directions. An *arrangement of pseudolines* is a finite set of pseudolines in the plane such that any two pseudolines either are disjoint or they meet in a single point and cross in this point.

Now let $\mathcal{P}$ be an arrangement of $n-1$ pseudolines $l_1, \ldots, l_{n-1}$, and where a positive side has been chosen for each of them. For each $X \in \{+, 0, -\}^{n-1}$, let F^X be the set of all those points $x \in R^2$ which lie on the positive side of l_i if $X_i^F = +$, on the negative side of l_i if

$X_i^- = -$, and on l_i if $X_i^F = 0$. This set F^X may be empty; if not, it is called the *face* of $\mathcal{P}$ associated with X. Similarly, we asign labels to the faces at infinity: namely, we get a "face at infinity" for every unbounded face in $\mathcal{P}$ where we have to take into account that "parallel lines meet at infinity".

Théorème 23 *Let $\mathcal{P} = \{l_1, \ldots, l_{n-1}\}$ be a labeled arrangement of pseudolines, for which positive sides have been chosen. Then the family of sign vectors*

$$\mathcal{V}^*(\mathcal{P}) := \{(X^F, +) : F \text{ is a face of } \mathcal{P}\} \cup \{(-X^F, -) : F \text{ is a face of } \mathcal{P}\}$$
$$\cup \{(Y^G, 0) : G \text{ is a face at infinity for } \mathcal{P}\}$$

is an oriented matroid of rank 3.

From an arrangement $\mathcal{P}$ of $n-1$ pseudolines one can reconstruct a linear arrangement of n pseudoplanes through the origin in R^3, where the nth pseudoplane is the straight plane, corresponding to the line at infinity in $\mathcal{P}$.

In fact, there is a surprisingly strong theorem available here: Lawrence's *topological representation theorem* states that

Theorem 24 (Lawrence) *every linear arrangement of n pseudohyperplanes in R^d yields an oriented matroid of rank d. Conversely, every oriented matroid on n elements of rank d can be represented by an arrangement of n linear pseudohyperplanes in R^d.*

The second part of this result is very difficult to prove even for $d = 3$.

References

[1] M. Aigner, Combinatorial Theory. Springer 1979.

[2] A. Bachem, W.Kern, Linear Programming Duality.An Introduction to Oriented Matroids, Springer-Verlag.

[3] A. Björner, M. Las Vergnas, B. Sturmfels, N. White, G. Ziegler, Oriented Matroids, Encyclopedia of Mathematics and its Applications 46, Cambridge University Press.

[4] B. Bollobás, Combinatorics. Setsystems, hypergraphs, families of vectors, and combinatorial probability. Cambridge University Press, 1986.

[5] Th. Cormen, Ch.Leiserson, R. Rivest, Introduction à l'algorithmique, Dunod (1994).

[6] P.J. Cameron, Combinatorics. Topics, techniques, algorithms, Cambridge University Press, 1996.

[7] J.H. van Lint and R.M. Wilson, A Course in Combinatorics, Cambridge University Press, 1994.

[8] J. Edmonds, D.R. Fulkerson, Bottleneck extrema, *J. Combinatorial Theory* **8** (1970), 299-306.

[9] D.R. Fulkerson, Networks, frames, blocking systems, in *Mathematics of the Decision Sciences,* Part I, AMS (Providence, R.I.), 1968, 303-334.

[10] J. Pach and P.J. Agarwal, Combinatorial Geometry, John Wiley & Sons 1996.

[11] J.G. Oxley, Matroid Theory, Oxford Science Publications (1992).

[12] N. Sauer, On the density of families of sets, *J. Combin. Th. Ser. A* 13 (1972), 145-147.

[13] V.N. Vapnik and A.Y. Chervonenskis, On the uniform convergence of relative frequences of events to their probability, *Th. Probab. Appl.* 16 (1971), 264-280.

[14] G. Ziegler, Lectures on Polytopes, Graduate Texts in Mthematics 152, Springer Verlag.