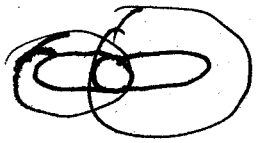
Proof. If vertex u is different from s, t then we have

$$V(u) = \sum_v P_{uv} V(v) = \sum_v \frac{c(uv)}{C(u)V(v)},$$

and hence

$$C(u)V(u) = \sum_v c(uv)V(v).$$

The theorem now follows from the fact proven earlier that each electrical network has a unique solution (Lemma 3.4.1, Theorem 3.4.2). □



$r(Y \cup Z) \leq |B_Y \cup B_Z|$ Neb

Chapter 4

Matroids

Matroids provide a successful connection between graph theory, geometry and linear algebra. Some of the dualities we will discuss later are rooted in the theory of matroids. Moreover, matroids provide a basis for discrete optimization. Several important algorithms, for instance the greedy algorithm, belong to the matroid world. We make a notational agreement in this chapter: the graphs are allowed to have loops and multiple edges.

Definition 4.0.5. Let X be a finite set and $S \subset 2^X$. We say that $M = (X, S)$ is a matroid if the following conditions are satisfied:

(I1) $\emptyset \in S$,

(I2) $A \in S$ and $A' \subset A$ then $A' \in S$ (S is *hereditary*),

(I3) $U, V \in S$ and $|U| = |V| + 1$ then there is $x \in U - V$ so that $V \cup \{x\} \in S$ (S satisfies an *exchange axiom*).

Example 4.0.6. Let X be the set of all columns of a matrix over a field and let S consist of all the subsets of X that are linearly independent. Then (X, S) is a matroid (called *vectorial or linear matroid*).

Definition 4.0.7. Let $M = (X, S)$ be a matroid. The elements of S are called *independent sets* of M. The maximal elements of S (w.r.t. inclusion) are called *bases*. Let $A \subset X$. The *rank* of A, $r(A)$, is defined by $r(A) = max\{|A'|; A' \subset A, A' \in S\}$. The *closure* of A, $\sigma(A)$, equals $\{x; r(A \cup \{x\}) = r(A)\}$. If $A = \sigma(A)$ then A is *closed*.

By repeated use of (I3) in Definition 4.0.5 we get

Corollary 4.0.8. *If $U, V \in S$ and $|U| > |V|$ then there is $Z \subset U - V$, $|Z| = |U - V|$ and $V \cup Z \in S$. All bases have the same cardinality.*

Theorem 4.0.9. *A non-empty collection $\mathcal{B}$ of subsets of X is the set of all bases of a matroid on X if and only if the following condition is satisfied.*

(B1) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$ then there is $y \in B_2 - B_1$ such that $B_1 - \{x\} \cup \{y\} \in \mathcal{B}$.

Proof. Property (B1) is true for matroids: we apply (I3) to $B_1 - \{x\}, B_2$. To show the other implication we need to prove that each hereditary system satisfying (B1) satisfies (I3) too. First we observe that (B1) implies that no element of $\mathcal{B}$ is a strict subset of another one, and by repeated application of (B1) we observe that in fact all the elements of $\mathcal{B}$ have the same size. To show (I3) let B_U, B_V be bases containing U, V from (I3) and such that their symmetric difference is as small as possible. If $(B_V \cap (U - V)) \neq \emptyset$ then any element from there may be added to V and (I3) holds. We show that $(B_V \cap (U - V)) = \emptyset$ leads to a contradiction with the choice of B_U, B_V: If $x \in B_V - B_U - V$ then (B1) produces a pair of bases with smaller symmetric difference. Hence $B_V - B_U - V$ is empty. But then necessarily $|B_V| < |B_U|$, a contradiction. □

Theorem 4.0.10. *A collection S of subsets of X is the set of all independent sets of a matroid on X if and only if (I1), (I2) and the following condition are satisfied.*

(I3') If A is any subset of X then all the maximal (w.r.t. inclusion) subsets Y of A with $Y \in S$ have the same cardinality.

Proof. Property (I3') is clerly equivalent to (I3). □

Theorem 4.0.11. *An integer function r on 2^X is a rank function of a matroid on X if and only if the following conditions are satisfied.*

(R1) $r(\emptyset) = 0$,

(R2) $r(Y) \leq r(Y \cup \{y\}) \leq r(Y) + 1$,

(R3) If $r(Y \cup \{y\}) = r(Y \cup \{z\}) = r(Y)$ then $r(Y) = r(Y \cup \{y, z\})$.

Proof. Clearly (R1),(R2) hold for matroids. To show (R3) let B be a maximal independent subset of Y. If $r(Y) < r(Y \cup \{y, z\})$ then B is not maximal independent in $Y \cup \{y, z\}$, but any enlargement leads to a contradiction.
To show the other direction we say that A is independent if $r(A) = |A|$. Obviously the set of the independent sets satisfies (I1). If A is independent and $B \subset A$ then $r(B) = |B|$ since otherwise, by (R2), $r(A) \leq |B - A| + r(B) < |A|$. Hence (I2) holds. If (I3) does not hold for U, V then by repeated application of (R3) we get that $r(V \cup (U - V)) = r(V)$, but this set contains U, a contradiction. □

Theorem 4.0.12. *An integer function on 2^X is a rank function of a matroid on X if and only if the following conditions are satisfied.*

(R1') $0 \leq r(Y) \leq |Y|$,

(R2') $Z \subset Y$ implies $r(Z) \leq r(Y)$,

(R3') $r(Y \cup Z) + r(Y \cap Z) \leq r(Y) + r(Z)$. This property is called submodularity.

Proof. Clearly (R1') and (R2') hold for matroids. To show (R3') let B be maximal independent set in $Y \cap Z$ and let B_Y, B_Z be maximal independent Y, Z containing B. We have $r(Y \cap Z) = |B_Y \cap B_Z|$ and clearly $r(B_Y \cup B_Z)$ $|Y \cup Z|$. Hence (R3') follows. On the other hand, (R1),(R2) and (R3) foll easily from (R1'), (R2') and (R3').

Theorem 4.0.13. *The closure $\sigma(A)$ is the smallest (w.r.t. inclusion) clo set containing A.*

Proof. First observe that $\sigma(A)$ is closed, since $r(\sigma(A) \cup \{x\}) = r(\sigma(A))$ imp $r(A \cup \{x\}) \leq r(\sigma(A) \cup \{x\}) = r(\sigma(A)) = r(A)$. To show the second part $A \subset C$, C closed and $x \in (\sigma(A) - C)$. Hence $r(C \cup \{x\}) > r(C)$ and this imp $r(A \cup \{x\}) > r(A)$. (exercise: why?) This contradicts $x \in \sigma(A)$.

Theorem 4.0.14. *A function $\sigma : 2^X \to 2^X$ is the closure operator of a mat on X if and only if the following conditions are satisfied.*

(S1) $Y \subset \sigma(Y)$,

(S2) $Z \subset Y$ then $\sigma(Z) \subset \sigma(Y)$,

(S3) $\sigma(\sigma(Y)) = \sigma(Y)$,

(S4) if $y \notin \sigma(Y)$ but $y \in \sigma(Y \cup \{z\})$ then $z \in \sigma(Y \cup \{y\})$. This propert called the Steinitz-MacLane exchange axiom.

We say that two matroids are isomorphic if they differ only in the nam their groundset elements.

4.1 Examples of matroids

We already know vectorial matroids. A matroid is *representable* if it is iso phic to a vectorial matroid.
Let $G = (V, E)$ be a graph and let $M(G) = (E, S)$ where $S = \{F \subset E; F$ for Then $M(G)$ is a matroid, called the *cycle matroid* of G. Its rank functi $r(F) = |V| - c(F)$, where we recall that $c(F)$ denotes the number of conne components of the spanning subgraph (V, F). The matroids isomorphic to matroids of graphs are called *graphic matroids.*
Let $G = (V, E)$ be a graph. The *matching matroid* of G is the pair (V, S) w $A \in S$ if and only if A may be covered by a matching of G. This is a ma since the basis axiom corresponds to the exchange along an alternating pa two maximum matchings of G.

A matroid is *simple* if $r(A) = |A|$ whenever $|A| < 3$. Simple matroi rank 3 have a natural representation that we now describe. Each matr determined by its rank function and so each simple matroid M of rank determined by the set $L(M) = \{A \subset X; |A| > 2, r(A) = 2, A$ closed $\}$; if $|A$ then $r(A) = 2$ if and only if A is a subset of an element of $L(M)$.

Chapter 44

Submodular functions and polymatroids

In this chapter we describe some of the basic properties of a second main object of the present part, the submodular function. Each submodular function gives a polymatroid, which is a generalization of the independent set polytope of a matroid. We prove as a main result the theorem of Edmonds [1970b] that the vertices of a polymatroid are integer if and only if the associated submodular function is integer.

44.1. Submodular functions and polymatroids

Let f be a *set function* on a set S, that is, a function defined on the collection $\mathcal{P}(S)$ of all subsets of S. The function f is called *submodular* if

$$f(T)+f(U)\geq f(T\cap U)+f(T\cup U) \tag{44.1}$$

for all subsets T, U of S. Similarly, f is called *supermodular* if $-f$ is submodular, i.e., if f satisfies (44.1) with the opposite inequality sign. f is *modular* if f is both submodular and supermodular, i.e., if f satisfies (44.1) with equality.

A set function f on S is called *nondecreasing* if $f(T)\leq f(U)$ whenever $T\subseteq U\subseteq S$, and *nonincreasing* if $f(T)\geq f(U)$ whenever $T\subseteq U\subseteq S$.

As usual, denote for each function $w: S\to\mathbb{R}$ and for each subset U of S,

$$w(U):=\sum_{s\in U} w(s). \tag{44.2}$$

So w may be considered also as a set function on S, and one easily sees that w is modular, and that each modular set function f on S with $f(\emptyset)=0$ may be obtained in this way. (More generally, each modular set function f on S satisfies $f(U)=w(U)+\gamma$ (for $U\subseteq S$), for some unique function $w: S\to\mathbb{R}$ and some unique real number γ.)

In a sense, submodularity is the discrete analogue of convexity. If we define, for any $f: \mathcal{P}(S)\to\mathbb{R}$ and any $x\in S$, a function $\delta f_x: \mathcal{P}(S)\to\mathbb{R}$ by: $\delta f_x(T):=f(T\cup\{x\})-f(T)$, then f is submodular if and only if δf_x is nonincreasing for each $x\in S$.

In other words:

Theorem 44.1. *A set function f on S is submodular if and only if*

$$f(U\cup\{s\})+f(U\cup\{t\})\geq f(U)+f(U\cup\{s,t\}) \tag{44.3}$$

for each $U\subseteq S$ and distinct $s,t\in S\setminus U$.

Proof. Necessity being trivial, we show sufficiency. We prove (44.1) by induction on $|T\triangle U|$, the case $|T\triangle U|\leq 2$ being trivial (if $T\subseteq U$ or $U\subseteq T$) or being implied by (44.3). If $|T\triangle U|\geq 3$, we may assume by symmetry that $|T\setminus U|\geq 2$. Choose $t\in T\setminus U$. Then, by induction,

$$f(T\cup U)-f(T)\leq f((T\setminus\{t\})\cup U)-f(T\setminus\{t\})\leq f(U)-f(T\cap U), \tag{44.4}$$

(as $|T\triangle((T\setminus\{t\})\cup U)|<|T\triangle U|$ and $|(T\setminus\{t\})\triangle U|<|T\triangle U|$). This shows (44.1). ■

Define two polyhedra associated with a set function f on S:

$$\begin{aligned} P_f &:= \{x\in\mathbb{R}^S \mid x\geq\mathbf{0}, x(U)\leq f(U) \text{ for each } U\subseteq S\},\\ EP_f &:= \{x\in\mathbb{R}^S \mid x(U)\leq f(U) \text{ for each } U\subseteq S\}. \end{aligned} \tag{44.5}$$

Note that P_f is nonempty if and only if $f\geq\mathbf{0}$, and that EP_f is nonempty if and only if $f(\emptyset)\geq 0$.

If f is a submodular function, then P_f is called the *polymatroid associated with* f, and EP_f the *extended polymatroid associated with* f. A polyhedron is called an (extended) polymatroid if it is the (extended) polymatroid associated with some submodular function. A polymatroid is bounded (since $0\leq x_s\leq f(\{s\})$ for each $s\in S$), and hence is a polytope.

The following observation presents a basic technique in proofs for submodular functions, which we often use without further reference:

Theorem 44.2. *Let f be a submodular set function on S and let $x\in EP_f$. Then the collection of sets $U\subseteq S$ satisfying $x(U)=f(U)$ is closed under taking unions and intersections.*

Proof. Suppose $x(T)=f(T)$ and $x(U)=f(U)$. Then

$$\begin{aligned} f(T)+f(U)&\geq f(T\cap U)+f(T\cup U)\geq x(T\cap U)+x(T\cup U)\\ &= x(T)+x(U)=f(T)+f(U), \end{aligned} \tag{44.6}$$

implying that equality holds throughout. So $x(T\cap U)=f(T\cap U)$ and $x(T\cup U)=f(T\cup U)$. ■

A vector x in EP_f (or in P_f) is called a *base vector* of EP_f (or of P_f) if $x(S)=f(S)$. A *base vector* of f is a base vector of EP_f. The set of all base vectors of f is called the *base polytope* of EP_f or of f. It is a face of EP_f, and denoted by B_f. So

$$B_f=\{x\in\mathbb{R}^S \mid x(U)\leq f(U) \text{ for all } U\subseteq S,\ x(S)=f(S)\}. \tag{44.7}$$

Lemma 4.1.1. *If $A, B \in L(M)$ then $|A \cap B| \leq 1$.*

Proof. We assume for a contradiction $\{x, z\} \subset A \cap B$, $a \in A - B$ and $b \in B - A$. Then both a, b belong to $\sigma(\{x, z\})$ and hence, by Theorem 4.0.13, both a, b belong to any closed set containing $\{x, z\}$: a contradiction.

□

A set $C \subset 2^X$ is a *configuration* on X if each element of C has at least 3 elements and any pair of elements of C have at most one element of X in common.

Theorem 4.1.2. *Each configuration is the set $L(M)$ of a simple matroid of rank 3 on X.*

Proof. Given C, for each $A \subset X$ define $r(A) = |A|$ if $|A| \leq 2$, and if $|A| > 2$ then $r(A) = 2$ if and only if A is a subset of an element of C; $r(A) = 3$ otherwise. We show that r is a rank function of a matroid. Note that $(R1), (R2)$ are obviously satisfied. We show $(R3)$: If $r(Y \cup \{y\}) = r(Y \cup \{z\}) = r(Y)$ then $|Y| \geq 2$ and both $Y \cup \{y\}$, $Y \cup \{z\}$ are subsets of an element of C. They are in fact subsets of the same element of C since their intersection has size 2. Hence $r(Y) = r(Y \cup \{y, z\})$.

□

Hence we can represent simple matroids of rank 3 by a system of 'lines' in the plane corresponding to the elements of $L(M)$. The most famous picture of matroid theory, the *Fano matroid* F_7, is depicted in Figure 4.1. The Fano matroid is the vectorial matroid, over $GF(2)$, of the matrix whose columns are all non-zero vectors of $GF(2)^3$.

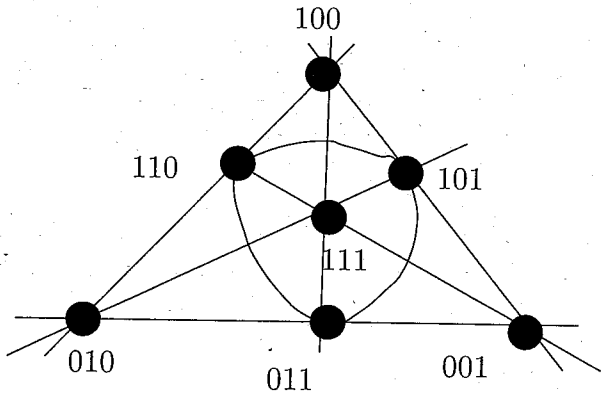


Figure 4.1. Fano matroid F_7

4.2 Greedy algorithm

Let (X, S) be a set system and w a weight function on $X = \{1, 2, \cdots, n\}$. *discrete optimization problem* we may want to find $J \in S$ such that $\sum_{i \in J}$ maximized. We encountered the *greedy algorithm* (GA) in Section 3.1. Th it was shown that GA correctly solves the minimum spanning tree problen order to turn the minimum spanning tree problem into a maximization pro we change the sign of each weight). Let us first define the greedy algorith a more general way, as an algorithm for the general optimisation problem works as follows:

- Order the elements of X so that $w_1 \geq w_2 \geq \cdots \geq w_n$.
- $J := \emptyset$.
- For $i = 1, \cdots, n$ do: if $J \cup \{i\} \in S$ and $w_i \geq 0$ then $J := J \cup \{i\}$.

The next theorem shows that applicability of GA characterizes matroi

Theorem 4.2.1. *Let (X, S) be a hereditary non-empty set system. The greedy algorithm solves the discrete optimization problem correctly for any u function w on X if and only if (X, S) is a matroid.*

Proof. If a hereditary system is not a matroid then it does not satisfy (I3' it is not difficult to construct a weight function w for which the greedy algo does not work. Let us prove the opposite implication: Let m be maximal that $w_m \geq 0$. Let z' be the characteristic vector of a set produced b greedy algorithm and let z be the characteristic vector of any other set Let $T_i = \{1, \cdots, i\}$, $i = 1, \cdots, m$. We notice that for each i

$$z'(T_i) = \sum_{j \leq i} z'_j \geq \sum_{j \leq i} z_j = z(T_i),$$

since $J \cap T_i$ is a maximal subset of T_i which belongs to S (by the definit GA). We have

$$wz \leq \sum_{i=1}^{m} w_i z_i = \sum_{i=1}^{m} w_i (z(T_i) - z(T_{i-1})) =$$

$$\sum_{i=1}^{m-1} (w_i - w_{i+1}) z(T_i) + w_m z(T_m) \leq \sum_{i=1}^{m-1} (w_i - w_{i+1}) z'(T_i) + w_m z'(T_m) =$$

The only property we used in the proof is that $z \geq 0$ and $z(T_i) \leq z'($ $r(T_i)$. GA thus solves also the following problem:

maximize $\sum_{i \in X} w_i z_i$
$z(A) = \sum_{i \in A} z_i \leq r(A)$, $A \subset X$;

$z_i \geq 0$, $i \in X$.

The problems that may be described in this form are called *linear programs*, and the part of optimization which studies linear programs is called *linear programming*.

Corollary 4.2.2. *Edmonds Matroid Polytope theorem: For any matroid, the convex hull of the characteristic vectors of the independent sets is equal to* $\mathcal{P} = \{z \geq 0;$ *for each* $A \subset X, z(A) \leq r(A)\}$.

Proof. (sketch) The convex hull is clearly a subset of $\mathcal{P}$. By the Minkowski-Weyl theorem introduced in the beginning of the book we have that $\mathcal{P}$, a bounded intersection of finitely many half-spaces, is a *polytope*, i.e. a convex hull of its *vertices*. Each vertex c of $\mathcal{P}$ is characterized by the existence of a half-space $\{z; wz \leq b\}$ which intersects $\mathcal{P}$ exactly in $\{c\}$. Since GA solves any problem $\max\{wz; z \in \mathcal{P}\}$, each non-empty intersection of $\mathcal{P}$ with a half-space necessarily contains the incidence vector of an independent set. In particular, each vertex of $\mathcal{P}$ is the incidence vector of an independent set, and the theorem follows. □

Finally we remark that the greedy algorithm is polynomial time if there is a polynomial algorithm to answer the questions 'Is J independent ?'. It is usual for matroids to be given, for algorithmic purposes, by such an independence-testing oracle.

4.3 Circuits

Definition 4.3.1. A *circuit* in a matroid is a minimal (w.r.t. inclusion) non-empty dependent set.

The circuits of graphic matroids are the cycles of the underlying graphs.

Theorem 4.3.2. *A non-empty set $\mathcal{C}$ is the set of the circuits of a matroid if and only if the following conditions are satisfied.*

(C1) If $C_1 \neq C_2$ are circuits then C_1 is not a subset of C_2,

(C2) If $C_1 \neq C_2$ are circuits and $z \in C_1 \cap C_2$ then $(C_1 \cup C_2) - z$ contains a circuit.

Proof. First we show that a matroid satisfies the above properties. The first is obvious. For the second we have $r(C_1 \cup C_2) \leq r(C_1) + r(C_2) - r(C_1 \cap C_2) = |C_1| + |C_2| - |C_1 \cap C_2| - 2 = |C_1 \cup C_2| - 2$. Hence $(C_1 \cup C_2) - z$ must be dependent. On the other hand, we define S to be the set of all subsets which do not contain an element of $\mathcal{C}$ and show that (X, S) is a matroid. Axioms (I1) and (I2) are obvious and we show (I3'): let $A \subset X$ and for a contradiction let J_1, J_2 be maximal subsets of A that belong to S and $|J_1| < |J_2|$, and let $|J_1 \cap J_2|$ be as large as possible. Let $x \in J_1 - J_2$ and C the unique circuit of $J_2 \cup x$. Necessarily there is $f \in C - J_1$ and $J_3 = (J_2 \cup x) - f$ belongs to S by the uniqueness of C. Then $|J_3 \cap J_1| < |J_2 \cap J_1|$, a contradiction. □

Corollary 4.3.3. *If A is independent, then $A \cup \{x\}$ contains at most one circuit.*

Proposition 4.3.4. *Let $A \subset X$ and $x \notin A$. Then $x \in \sigma(A)$ if and only if there is a circuit C with $x \in C \subset A \cup \{x\}$.*

Proof. If $x \in \sigma(A)$ and B is maximal independent in A, then $B \cup x$ is dependent and hence contains a circuit. On the other hand, let D be a maximal independent set in A containing $C - x$. Then D is also maximal independent in $A \cup x$ and hence $x \in \sigma(A)$. □

4.4 Basic operations

Definition 4.4.1. A *k-truncation* of M is a matroid M' on X such that A is independent in M' if and only if $|A| \leq k$ and A is independent in M.

Each truncation of a matroid is a matroid.

Definition 4.4.2. Let M_1, M_2 be matroids and $X_1 \cap X_2 = \emptyset$. $M_1 + M_2$ (direct sum of M_1, M_2) is the matroid on $X_1 \cup X_2$ such that A is independent if and only if $A \cap X_1$ is independent in M_1 and $A \cap X_2$ is independent in M_2.

Definition 4.4.3. Let X be a disjoint union of $X_i, i = 1, \cdots, n$ and let $S_i = \{A \subset X_i; |A| \leq 1\}$. Then $\sum_i (X_i, S_i)$ is called a *partition matroid*.

It follows immediately from the definition that $M \setminus U = (X \setminus U, S|_{X \setminus U})$ is a matroid. This operation is called *deletion of U*.

Definition 4.4.4. Let $T \subset X$ and let J be a maximal independent subset of $T' = X \setminus T$. M/T' (contraction of T') is a matroid on T defined so that A is independent if and only if $A \cup J$ is independent in M.

Theorem 4.4.5. *M/T' is a matroid and its rank function r' satisfies $r'(A) = r(A \cup T) - r(T)$. Hence M/T' does not depend on the choice of J.*

Proof. Obviously M/T' satisfies (I1) and (I2). Let $A \subset T$ and let J' be maximal subset of A that is independent in M/T'. Observe that $J \cup J'$ is maximal independent in $A \cup T'$, by the choices of J, J'. □

4.5 Duality

Definition 4.5.1. Let $M = (X, S)$ be a matroid. Its *dual matroid* is $M^* = (X, S^*)$ such that $I \in S^*$ if and only if $r(X \setminus I) = r(X)$ (r is the rank of M).

Proposition 4.5.2. *M^* is a matroid and its rank function r^* satisfies $r^*(A) = |A| - r(X) + r(X \setminus A)$.*

Proof. Again the only nontrivial property is (I3'). Let $A \subset X$ and let J be maximal subset of A which belongs to S^*. Let B be a maximal independent (in M) subset of $X \setminus A$ and let B' be a basis of M containing B and $B' \subset X \setminus A$. If there is $x \in (A \setminus J) \setminus B'$ then J was not maximal (a contradiction). Hence $A \setminus J \subset B'$ and the formula for r^* follows.