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

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 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 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 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 a 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 a 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 $B' \subset X \setminus J$. 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. □

The objects (bases, circuits, closed sets) of M^* are called dual objects or coobjects, e.g., dual bases or cobases. Let us note some simple facts: $M^{**} = M$. The dual bases are exactly complements of the bases. The cocircuits are minimal (w.r.t. inclusion) sets intersecting each basis. The cocircuits are exactly complements of hyperplanes. A *hyperplane* of M is a closed set whose rank is one less than $r(X)$).

Proposition 4.5.3. *Let G be a graph. Then the cocircuits of the graphic matroid $M(G)$ are exactly the minimal edge cuts.*

Proof. Note that edge cuts are exactly the sets of edges intersecting each basis of $M(G)$. □

Corollary 4.5.4. *Let G be a planar graph and G^* its geometric dual. Then $M(G^*) = M(G)^*$.*

Definition 4.5.5. M is called a *minor* of N if M is obtained from N by some finite sequence of deletions and contractions.

Let G be a graph. A minor of G is a graph obtained from G by deletions and contractions of edges. Observe the following: H is a minor of G if and only if $M(H)$ is a minor of $M(G)$.
The following series of propositions are proved by comparing the rank functions (we recall that the rank function uniquely determines the matroid).

Proposition 4.5.6. *We have*

(1) $(M/T)^* = M^* \setminus T$,

(2) $(M \setminus T)^* = M^*/T$,

(3) M is a minor of N if and only if M^* is a minor of N^*,

(4) M is a minor of N if and only if M may be obtained from N by a deletion (contraction) followed by a contraction (deletion).

A matroid M is called *cographic* if it is isomorphic to $M^*(G)$ for some graph G. It is also called a *cocycle matroid* of G. For example, it is not difficult to observe that $U_4^2 = (\{1,2,3,4\}, \{\emptyset, 1,2,3,4,12,13,14,23,24,34\})$ is not cographic. Next we recall Kuratowski's theorem (Theorem 2.10.15): G is planar if and only if G has no minor isomorphic to K_5 or $K_{3,3}$.

Proposition 4.5.7. *$M(K_5)$ and $M(K_{3,3})$ are not cographic.*

Proof. Assume $M(K_{3,3}) = M^*(G)$. Then $|E(G)| = 9$, G is a simple graph because no pair of edges separates $K_{3,3}$, and each edge cut of G contains at least 4 edges. Hence each degree of G is at least 4 and we get $4|V(G)| \leq 18$: a contradiction because G is simple. For K_5 one can use the fact that such a graph G has no circuit of length 3. □

Next comes a restatement of a classical theorem of Whitney about planar graphs.

Theorem 4.5.8. *G is planar if and only if its cycle matroid is cographic.*

Proof. By Corollary 4.5.4, if G is planar then $M(G) = M^*(G^*)$. To show the other direction, using the Kuratowski theorem, it suffices to observe that a minor of a cographic matroid is cographic (by dualizing the statement that a minor of a graphic matroid is graphic), and use Proposition 4.5.7. □

Here is an equivalent formulation: a matroid M is both graphic and cographic if and only if M is the cycle matroid of a planar graph.

4.6 Representable matroids

A matroid is called *binary* if it is representable over the 2-element field $GF(2)$. It is called *regular* if it is representable over an arbitrary field. Let A be a matrix representing matroid M and let A' be obtained from A by operations of adding a row to another row. Then again A' represents M. A representation of a matroid M is called *standard* w.r.t. a basis B if it has the form $I|A$, where I is the identity matrix of $r(M)$ rows whose columns are indexed by the elements of B. Since the elementary row operations do not change the matroid, we get that each representable matroid has a standard representation w.r.t. an arbitrary basis.

Theorem 4.6.1. *Let $I|A$ be a standard representation of M. Then $A^T|I$ is a representation of M^*.*

Corollary 4.6.2. *If M is representable over a field $\mathbb{F}$ and N is a minor of M then both M^* and N are representable over $\mathbb{F}$.*

Proof. Deletion clearly corresponds to deletion of the corresponding column in a representation. For contraction we use Theorem 4.6.1 and the duality between contraction and deletion. □

Clearly, U_2^4 is not binary. Hence binary matroids do not have U_2^4 as a minor. Next we list some seminal results of Tutte, characterizing classes of matroids by forbidden minors.

Theorem 4.6.3. *M is binary if and only if M does not have U_2^4 as a minor. M is regular if and only if M is binary and does not have F_7 or F_7^* as a minor. M is graphic if and only if M is regular and does not have $M(K_5)^*$ or $M(K_{3,3})^*$ as a minor.*

We recall that F_7 denotes the Fano matroid. It is easy to observe that the graphic matroids are regular: Let $D = (V, E)$ be an arbitrary orientation of G and let I_D be the incidence matrix of D (see Section 2.3). Then I_D represents $M(G)$ over an arbitrary field, since a set of columns is linearly dependent if and only if its index set contains a cycle of G.

4.7 Matroid intersection

Given two matroids on the same set X, the matroid intersection problem is to find a common independent set of maximum cardinality. Let us mention two special cases: maximum matching in bipartite graphs (here the two matroids are partition matroids), and maximum branching in a digraph (branching is a forest in which each node has in-degree at most one); here one of the matroids is the corresponding graphic matroid and the second one is a partition matroid of the set-system of sets of the incoming edges at each vertex.

Theorem 4.7.1. *For two matroids (X, S_1) and (X, S_2), the maximum $|J|$ such that $J \in S_1 \cap S_2$ equals the minimum of $r_1(A) + r_2(X \setminus A)$, over all $A \subset X$.*

Proof. If $J \in S_1 \cap S_2$ then for each $A \subset X$, $J \cap A \in S_1$ and $J \cap (X \setminus A) \in S_2$. Hence $|J| \leq r_1(A) + r_2(X \setminus A)$. The second part is proved by induction on $|X|$. Let k equal the minimum of $r_1(A) + r_2(X \setminus A)$ and let x be such that $\{x\} \in S_1 \cap S_2$. Note: if there is no such x then $k = 0$, and if we take $A = \{x; r_1(\{x\}) = 0\}$, we are done. Let $X' = X - x$. If the minimum over $A \subset X'$ of $r_1(A) + r_2(X \setminus A)$ also equals k then we are done by the induction assumption. Let S_i' denote S_i contracted on $X \setminus x$. If the minimum over $A \subset X'$ of $r_1'(A) + r_2'(X \setminus A)$ is at least $k - 1$ then the induction gives a common independent set of S_1', S_2' of size $k-1$ and adding x gives the desired common independent set of S_1, S_2. If none of these happens, then there are $A, B \subset X'$ so that

$$r_1(A) + r_2(X' \setminus A) \leq k - 1$$

and

$$r_1(B \cup \{x\}) - 1 + r_2((X' \setminus B) \cup \{x\}) - 1 \leq k - 2.$$

Adding and applying submodularity we get

$$r_1(A \cup B \cup \{x\}) + r_1(A \cap B) + r_2(X \setminus (A \cap B)) + r_2(X \setminus (A \cup B \cup \{x\})) \leq 2k - 1.$$

It follows that the sum of the middle two terms or the sum of the outer two terms is at most $k - 1$, a contradiction. □

A polynomial time algorithm exists provided the rank can be found in polynomial time, even for the weighted case, but we do not include this here.

4.8 Matroid union and min-max theorems

The matroid union is closely related to the matroid intersection, as we will see.

Theorem 4.8.1. *Let $M' = (X', S')$ be a matroid and f an arbitrary function from X' to X. Let $S = \{f(I); I \in S'\}$. Then (X, S) is a matroid with rank function*

$$r(U) = min_{T \subset U}\{|U - T| + r'(f^{-1}(T))\}.$$

Proof. It suffices to show the formula for the rank function since obviously S is non-empty and hereditary. The formula follows from Theorem 4.7.1 since $r(U)$ is equal to the maximum size of a common independent set of M' and the partition matroid (X', W) induced by the family $(f^{-1}(s); s \in U)$. □

Definition 4.8.2. If $M_i = (X_i, S_i), i = 1, \cdots, k$ are matroids and $X = \cup X_i$ then their union is defined as $(X, \{I_1 \cup I_2 \cdots \cup I_k; I_i \in S_i\})$.

Corollary 4.8.3. *Matroid union (partitioning) theorem: The union of matroids is again a matroid, with its rank function given by*

$$r(U) = min_{T \subset U}\{|U - T| + r_1(T \cap X_1) + \cdots + r_k(T \cap X_k)\}.$$

Proof. We first make X_i mutually disjoint and then use Theorem 4.8.1. □

Example 4.8.4. Let $G = (V, W, E)$ be a bipartite graph. For each $u \in V$ define a matroid M_u on the set of neighbours of u so that a set is independent if and only if its cardinality is at most one. Then the union of $M_u, u \in V$ is called the *transversal matroid.*

Corollary 4.8.5. *The maximum size of a union of k independent sets of a matroid M is*

$$min_{T \subset X}\{|X \setminus T| + kr(U)\}.$$

Corollary 4.8.6. *X can be covered by k independent sets if and only if for each $U \subset X$,*

$$kr(U) \geq |U|.$$

Proof. X can be covered by k independent sets if and only if there is a union of k independent sets of size $|X|$. □

Corollary 4.8.7. *There are k disjoint bases if and only if for each $U \subset X$,*

$$k(r(X) - r(U)) \leq |X - U|.$$

Proof. There are k disjoint bases if and only if the maximum size of the union of k independent sets is $kr(X)$. □

Corollary 4.8.8. *A finite subset X of a vector space can be covered by k linearly independent sets if and only if for each $U \subset X$,*

$$k.r(U) \geq |U|.$$

These are some examples of *min-max theorems*, the pillars of discrete optimization.