LECTURE NOTES ON MATROIDS

MARTIN LOEBL

Abstract. These are lecture notes for the first part of the lecture "Introduction to Mathematical Programming".

1. Basic concepts

Definition 1.1. 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 $A' \in S$,
I3 $U, V \in S$ and $|U| = |V| + 1$ then there is $x \in U - V$ so that $V \cup \{x\} \in S$.

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

Definition 1.2. 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, $r(A)$, equals maximum $|A'|; A' \subset A, A' \in S$. 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 1.1 we get

Corollary 1.3.
- *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 1. *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.*

Date: This edition: December 1, 2005 First edition: March 20, 2003.

Key words and phrases: matroid, graph, code .

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: 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 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. $\square$

Theorem 2. *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.*

I'3 *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 [I'3] is simply equivalent to [I3]. □

Theorem 3. *An integer function r on X is the rank function of a matroid on X if and only if the following conditions are satisfied.*

R1 $r(\emptyset) = 0$,

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

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 maximal independent in 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 independent if $r(A) = |A|$. Obviously the set of the independent sets satisfies [I1]. If A independent and $B \subset A$ then $r(B) = |B|$ since otherwise (by [R2]) $r(A) \le |B - A| + r(B) < |A|$. Hence [I2] holds. If [I3] doesnot 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. *An integer function on X is the rank function of a matroid on X if and only if the following conditions are satisfied.*

R'1 $0 \le r(Y) \le |Y|$,

R'2 $Z \subset Y$ *then* $r(Z) \le r(Y)$,

R'3 $r(Y \cup Z) + r(Y \cap Z) \le r(Y) + r(Z)$. *This property is called* submodularity.

Proof. Clearly [R'1.R'2] hold for matroids. To show [R'3] let B be a maximal independent set in $Y \cap Z$ and let B_Y, B_Z be maximal independent in Y, Z containing B. We have $r(Y \cap Z) = |B_Y \cap B_Z|$ and simply $r(B_Y \cup B_Z) \le |Y \cup Z|$. Hence [R'3] follows. On the other hand, [R1,R2,R3] simply follow from [R'1,R'2,R'3].

□

Theorem 5. *$\sigma(A)$ is the smallest (w.r.t. inclusion) closed set containing A.*

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

Theorem 6. *A function σ on X is the closure operator of a matroid on X if and only if the following conditions are satisfied.*

S1 $Y \subset \sigma(A)$,
S2 $Z \subset Y$ *then* $\sigma(Z) \leq \sigma(Y)$,
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 property is called* Steinitz-Maclane exchange axiom.

We say that matroids $M_i = (X_i, S_i), i = 1, 2$ are izomorphic if there is a bijection f from X_1 to X_2 so that A independent if and only if $f(A)$ independent.

2. Basic Examples

We have already learned vectorial matroids. A matroid is *representable* if it is izomorphic to a vectorial matroid.

Example. Let $G = (V, E)$ be a graph and let $M(G) = (E, S)$ and $S = \{F \subset E; F \text{ acyclic }\}$. Then $M(G)$ is a matroid called *cycle matroid* of G. Its rank function is $r(F) = |V| - k(V, F)$, where $k(V, F)$ is the number of connectivity components of (V, F). The matroids izomorphic to cycle matroids of graphs are called *graphic matroids.* Let us repeat some basic facts about an acyclic subset F of edges: (V, F) has at least 2 vertices of degree 1 (this may be proved in a greedy way), If $e \in F$ goes to vertex x of degree 1 then $k(V, F) = k(V - x, F - e)$ (obvious) and $|F| = |V| - k(V, F)$ (this may be proved by induction using the previous fact).

Example. Let $G = (V, E)$ be a graph. *matching matroid* of G is (V, S) where $A \in S$ if A may be covered by a matching of G. This is a matroid since the basis axiom corresponds to the exchange along an alternating path of two maximum matchings of G.

Example: a geometric representation of simple matroids of rank 3.

A matroid is *simple* if $r(A) = |A|$ whenever $|A| < 3$. Each matroid is determined by its rank function and so each simple matroid M of rank 3 is determined by set $L(M) = \{A \subset X; |A| > 2, r(A) = 2, A \text{ closed }\}$ (if $|A| > 2$ then $r(A) = 2$ iff A is a subset of an element of $L(M)$).

Lemma 2.1. *$A, B \in L(M)$ then $|A \cap B| \leq 1$.*

Proof. 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 5 to any closed set containing $\{x, z\}$...a contradiction.

$\square$

A set $C \subset 2^X$ is *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 7. *Each configuration is 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 $r(A) = 2$ iff A is a subset of an element of C. 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 $r(Y) = r(Y \cup \{y, z\})$. $\square$

Hence we can represent the simple matroids of rank 3 by a system of 'lines' on the plane corresponding to the elements of $L(M)$. As an exercise, draw the most famous picture of matroid theory, the Fano matroid: it is the vectorial matroid over $GF[2]$ (finite field of two elements) of a matrix whose columns are all non-zero vectors of $GF[2]^3$.

3. Greedy Algorithm

Let (X, S) be a set system and c a weight function on X. Assume we want to find $J \in S$ such that $\sum_{x \in X} c(x)$ is maximized. The *greedy algorithm* to solve this problem is as follows:

- Order elements of X so that $c(x_1) \geq c(x_2) \geq \dots c(x_n)$ $(n = |X|)$,
- $J := \emptyset$,
- For $i = 1, \dots, n$ do: if $J \cup \{x_i\} \in S$ and $c(x_i) \geq 0$ then $J := J \cup \{x_i\}$.

Theorem 8. *Let (X, S) be a hereditary non-empty set system. Then the greedy algorithm works for any weight function c on X if and only if (X, S) is a matroid.*

Proof. As a homework prove that if a hereditary system is not a matroid then there is a weight function c for which the greedy algorithm doesnot work. Let us prove the opposite implication:

let m be maximal such that $x_m \geq 0$. Let x' be the characteristic vector of a set produced by the greedy algorithm and let x be the characteristic vector of any other set of S. Let $T_i = \{x_1, \ldots, x_i\}$ for $i \leq m$. Notice that $x'(T_i) \geq x(T_i)$ for each i since $J \cap T_i$ is a maximal subset of T_i in S. We have

$$cx \leq \sum_{i=1}^{m} c(x_i)x_{x_i} = \sum_{i=1}^{m}(x(T_i) - x(T_{i-1})) =$$

$$\sum_{i=1}^{m-1}(c(x_i) - c(x_{i+1}))x(T_i) + c(x_m)x(T_m) \leq$$

$$\sum_{i=1}^{m-1}(c(x_i) - c(x_{i+1}))x'(T_i) + c(x_m)x'(T_m) = cx'.$$

□

Note that the only property we used was that $x' \geq 0$ and $x(T_i) \leq x'(T_i) = r(T_i)$. Hence the greedy algorithm solves also the following linear program:

maximize cx

$x(A) \leq r(A)$, $A \subset X$;

$x \geq 0$.

Hence we get the following corollary.

Corollary 3.1. *Edmonds Matroid Polytope Theorem: For any matroid, the convex hull of the characteristic vectors of the independent sets is described by the above system of linearinequalities.*

Finally note that the greedy algorithm is polynomial if there is a polynomial algorithm to answer the question 'Is J independent'. It is usual for matroids to be represented, for algorithmic purposes, by such an independence-teting oracle.

4. Connectivity

Definition 4.1. A *circuit* is each minimal (w.r.t. inclusion) non-empty dependent set.

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

Theorem 9. *A collection $\mathcal{C} \neq \{\emptyset\}$ of sets is the set of the circuits of a matroid iff the following conditions are satisfied.*

C1 *If C_1, C_2 are distinct circuits then C_1 is not a subset of C_2,* C2 *If C_1, C_2 are distinct 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 one is obvious. For the second one 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,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 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 uniqueness of C. J_3 is closer to J_1, a contradiction. □

Corollary 4.2. *If A is independent then $A \cup \{x\}$ contains at most one circuit.*

Proposition 4.3. *A stronger statement than [C3] is true for matroids: If C_1, C_2 are distinct circuits, $z \in C_1 \cap C_2, y \in C_1 - C_2$ then $(C_1 \cup C_2) - z$ contains a circuit through y.*

Theorem 10. *Let $A \subset X$ and $x \notin A$. Then $x \in \sigma(A)$ iff there is a circuit C with $x \in C \subset A \cup \{x\}$.*

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

Definition 4.4. A matroid is *connected* if for each x, y in X, there is a circuit containing both x, y.

Proposition 4.5. *Graphic matroid $M(G)$ is connected iff G is 2-connected.*

Proposition 4.6. *Let $A \subset X$. There is a circuit C such that $C \cap A \neq \emptyset \neq C \cap (X - A)$ iff $r(A) + r(X - A) > r(X)$.*

Proof. If C is such a circuit and B_A, B_{X-A} maximal independent subsets in $A, X - A$ containing $C \cap A, C \cap (X - A)$ then $B_A \cup B_{X-A}$ dependent since it contains a circuit, and $\sigma(B_A \cup B_{X-A}) = X$ by the choice of B_A, B_{X-A}. On the other hand if B_A, B_{X-A} maximal independent subsets in $A, X - A$ then the condition $r(A) + r(X - A) > r(X)$ implies that their union is dependent and hence contains the desired circuit. □

Definition 4.7. If $M = (X, S)$ then $M - A = M|(X - A)$ is the matroid on $X - A$ such that I is independent in $M|(X - A)$ iff $I \in S$ and $I \subset X - A$.

It is very simple to verify that $M - A$ is matroid. This operation is called 'deletion of A'. Matroid $M|A$ is called 'restriction' of M to A.

Theorem 11. *M connected iff for each $A \subset X$, $r(A) + r(X - A) > r(X)$.*

Proof. The condition is necessary by 4.6. On the other hand let $x \in X$ and let A be the set of all y such that x, y belong to a common circuit. For a contradiction assume that $X \neq A$ and $|X|$ is as small as possible. Let C be a circuit intersecting both $A, X - A$. Let $y \in C \cap A$ and D be a circuit containing x, y. Note that $M - (X - (C \cup D))$ satisfies the condition of the theorem. Hence if $X \neq (C \cup D)$ we can use the minimality of X to get a circuit containing x and any other element of $(C \cup D)$, a contradiction. Hence $X = (C \cup D)$...

not finished $\square$

5. Basic Operations

Definition 5.1. A *truncation* of M is matroid M' on X such that for some k, A is independent iff $|A| < k$ and A independent in M.

Again each truncation of a matroid is a matroid.

Definition 5.2. 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 independent iff $A \cap X_1$ independent in M_1 and $A \cap X_2$ independent in M_2.

Definition 5.3. Let X be a disjoint union of $X_i, i = 1, \ldots, n$ and let $S_i = \{A \subset X_i; |A| \leq 1\}$. Then $\sum_i (X_i, S_i)$ is called *partition matroid.*

Proposition 5.4. *Define a relation $x \leq y$ iff x, y belong to the same circuit. Then this relation is an equivalence on X.*

Proof. Observe: If C, D are circuits with non-empty intersection then M restricted to $C \cup D$ is connected (by Theorem 11). $\square$

Definition 5.5. Let A be a class of $' \leq '$. Then $M|A$ is called *connectivity component* of M.

Proposition 5.6. *Each matroid is the sum of its connectivity components.*

Proof. The following observation is simple and sufficient to prove the proposition: if $r(A) + r(X - A) = r(X)$ then for each $Y \subset X$, $r(A) + r(Y - A) = r(Y)$. $\square$

Definition 5.7. Let $T \subset X$ and let J be a maximal independent subset of $X - T$. $M.T$ (contraction of M on T) is matroid on T defined so that A is independent iff $A \cup J$ independent in M.

Theorem 12. *$M.T$ is a matroid and its rank function r' satisfies $r'(A) = r(A \cup T) - r(T)$. Hence $M.T$ doesnot depend on the choice of J.*

Proof. Obviously $M.T$ satisfies I1, 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 if J, J'. $\square$

6. Duality

Definition 6.1. Let $M = (X, S)$ be a matroid. Its *dual matroid* M^* is (X, S^*) such that $I \in S^*$ iff $r(X - I) = r(X)$ (r is rank of M).

Proposition 6.2. *M^* is a matroid and its rank function r^* satisfies $r^*(A) = |A| - r(X) + r(X - A)$.*

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

The objects (bases, circuits, closed sets) of M^* are called dual objects or coobjects, e.g. dual bases or cobases, cocircuits... Realise 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 6.3. *Let G be a graph. Then the cocircuits are exactly minimal (w.r.t. inclusion) edge cuts.*

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

Definition 6.4. M is called *minor* of N if M is obtained from N by several deletions and contractions.

Let G be a graph. Minor of G is a graph obtained from G by deletions and contractions. Observe the following: H minor G if and only if $M(H)$ minor $M(G)$.

The following series of propositions is proved by comparing the rank functions (remember that the rank function uniquelly determines the matroid).

Proposition 6.5.

1. *M connected iff M^* connected,*
2. *$(M.T)^* = M^*|T$,*
3. *$(M|T)^* = M^*.T$,*
4. *M is minor of N iff M^* is a minor of N^*,*
5. *M is minor of N iff M may be obtained from N by a restriction (contraction) followed by a contraction (restriction).*

Matroid M is called *cographic* if it is izomorphic to $M^*(G)$ for some graph G. It is also called cocycle matroid of G. U_4^2 is not cographic.

Next we relate the duality in matroids with planar graphs. Recall the basic theorem of Kuratowski: G is planar iff G has no minor izomorphic to K_5 or $K_{3,3}$.

Proposition 6.6. *$M(K_5)$ and $M(K_{3,3})$ are not cographic.*

Proof. Assume $M(K_{3,3}) = M^*(G)$. Then $|E(G)| = 9$, and each edge cut of G has at least 4 edges. Hence each degree of G is at least 4 and we get $4|V(G)| \leq 18$.... a contradiction.

For K_5 go on analogously and use the fact that such a graph G has no circuit of length 3. □

The following is a basic theorem of Whitney.

Theorem 13. *G planar iff its cycle matroid is cographic.*

Proof. G planar then $M(G) = M^*(G^*)$ where G^* is the geometric dual of G. To show the other direction, using the Kuratowsky theorem it suffices to observe that a minor of a cographic matroid is cographic (this is dualising the statement that a minor of a graphic matroid is graphic), and use 6.6. □

Here is an equivalent formulation: Matroid M is both graphic and cographic iff M is a cycle matroid of a planar graph.

In the end of this section let us introduce a linear algebra duality between edge-cuts and circuits of a graph $G = (V, E)$. Let $D = (V, D(E))$ be an arbitrary orientation of G. Define $V \times E(D)$ matrix $A(D)$ by $a_{v,e} = 1$ if v is the tail of e, $a_{v,e} = -1$ if v is the head of e, and $a_{v,e} = 0$ otherwise.

Theorem 14. *$A(D)$ represents $M(G)$ over arbitrary field.*

Proof. Note that a set of columns is linearly dependent iff its index set contains a circuit of G. □

Let $A(G) = A(D)$ over $GF[2]$. Hence $A(G)$ is the standard incidence matrix of G. A subset A of edges is called *even* if (V, A) has each degree even (possibly zero).

Theorem 15.

1. *$Ker_2(A(G)) = \{x; A(G)x = 2(mod2)\}$ (the kernel over $GF[2]$) is a vector space over $GF[2]$; it is the set of the characteristic vectors of even subsets of edges.*
2. *Its basis may be constructed as follows: let $T \subset E$ be a maximal acyclic set of edges in G. For $e \notin T$ let C_e be the unique circuit in $T \cup \{e\}$. Then the characterictic vectors of the sets $C_e, e \notin T$ form a desired basis.*

Proof. To observe the first part note that if x is the characteristic vector of $A \subset E$ then $[A(G)x]_v$ equals the number of edges of A incident with v. To show the second part first note that the constructed vectors are obviously linearly independent. Let D be an even set of edges and let W be an even set of edges such that its characteristic vectors equals the sum of C_e, $e \in D - T$. Then the symmetric difference of D, W is a subset of T hence acyclic hence the empty set hence $D = W$. □

Corollary 6.7. *The number of even subsets of edges is 2^{E-V+k} where k is the number of connectivity components of G.*

Theorem 16. *The orthogonal complement of $Ker_2(A(G))$ is the set of the characteristic vectors of edge-cuts of G.*

Proof. The orthogonal complement of the kernel is generated by the rows of $A(G)$. The rows are the incidence vectors of $N(v), v \in V$ where $N(v) = \{e; v \in e\}$. Note that C is the characteristic vector of an edge-cut defined by $V' \subset V$ iff C is the sum of the rows of the vertices of V'. □

7. Matroid intersection

Given two matroids on the same set X, the matroid intersection problem is to find a maximum cardinality common independent set. 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 arcs to the same vertex.

Theorem 17. *For matroids S_1, S_2 on X, maximum $|J|$ such that $J \in S_1 \cap S_2$ equals minimum of $r_1(A) + r_2(X - A)$, 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 $J \cap (X - A) \in S_2$. Hence $|J| \leq r_1(A) + r_2(X - A)$. The second part is proved by induction on $|X|$. Let k equal minimum of $r_1(A) + r_2(X - A)$ 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 $A = \{x; r_1(\{x\}) = 0$ and we are done. Let $X' = X - x$. If the minimum over $A \subset X'$ of $r_1(A) + r_2(X - A)$ equals k too then we are done by the induction assumption. Let S_i' denote S_i contracted on $X - x$. If the minimum over $A \subset X'$ of $r_1'(A) + r_2'(X - A)$ is at least $k - 1$ then 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 happen then there are $A, B \subset X'$ so that

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

and

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

Adding and applying submodularity we get

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

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

Note that the above theorem gives a good characterization. A polynomial algorithm exists, even for the weighted case, but we do not include it here.

8. Matroid union

Matroid union (sometimes called matroid partitioning)is closely related to matroid intersection, as you will see. Let us start with a basic theorem of Edmonds:

Theorem 18. *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. Note that $r(U)$ equals maximum size of a common independent set in M' and the partition matroid (X', W) induced by the family $(F^{-1}(s); s \in U)$. □

Definition 8.1. If $M_i = (X_i, S_i), i = 1, \dots, k$ are matroids then their union is the set-system $(\cup_i X_i, \{I_1 \cup I_2 \cdots \cup I_k; I_i \in S_i\}$.

Corollary 8.2. *Matroid union (partitioning) theorem: The union of matroids is again a matroid, with its rank function given by*

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

Definition 8.3. Let $G = (V, W, E)$ be a bipartite graph. For each $x \in V$ define matroid M_x on the set of neighbours of x so that a set is independent iff its cardinality is at most one. Then the union of $M_x, x \in V$ is called *transversal matroid.*

Proof. To see that it is a matroid, make X_i first disjoint and then use the previous theorem. For the rank function also use the previous theorem. □

Corollary 8.4. *Maximum size of a union of k independent sets of a matroid M is*

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

Corollary 8.5. *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 8.6. *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 8.7. *A finite subset X of a vector space can be covered by k linearly independent sets if and only if for each $U \subset X$,*

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

9. Representable matroids

Matroid is called *binary* if representable over $GF[2]$. It is called *regular* if representable over arbotrary field. Let A be a matrix representing matroid M and let A' be obtained from A by an elementary row operation. Then again A' represents M. A representation of matroid M is called *standard* w.r.t. a basis B if it has form $I|A$, where I is the identity matrix of $r(M)$ rows whose columns are idexed 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 19. *Let $I|A$ be a standard representation of M. Then $A^T|I$ is a representation of M^*.*

Proof. standard linear algebra

□

Corollary 9.1. *If M representable over F and N is minor of M then N is representable over F.*

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

Corollary 9.2. *If N is not representable over F and N is minor of M then M is not representable over F.*

Theorem 20. *U_2^4 is not binary. Hence binary matroids do not have U_2^4 as a minor.*

Proof. It is easy to show that a standard representation cannot exist. □

Next we list some basic theorems of Tutte, characterising classes of matroids by a few forbidden 'pictures'.

Theorem 21. *M binary if and only if M does not have U_2^4 as a minor.*

Theorem 22. *M regular if and only if M binary and does not have F_7 or F_7^* as a minor.*

Remember that F_7 is the famous Fano matroid.

Theorem 23. *M graphic if and only if M regular and does not have $M(K_5)^*$ or $M(K_{3,3})^*$ as a minor.*

10. Submodular functions

Function f on subsets of X is *submodular* if $f(T) + f(U) \geq f(T \cap U) + f(T \cup U)$.

Theorem 24. *Function f is submodular if and only if*

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

Proof. We show sufficiency by induction on $|U\delta T|$. If $|U\delta T| \leq 2$ we have it from the assumption. If $|U\delta T| \geq 3$ then we may assume w.l.o.g. that $|T - U| \geq 2$; let $t \in T - U$. Then, by induction,

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

as $|T\delta((T - \{t\}) \cup U)| < |T\delta U|$.

□

Define two plyhedra associated with a set function f:

- Polymatroid: $P_f = \{x \in R^X; x \geq 0, x(U) \leq f(U)$ for each $U \subset X\}$,
- Extended polymatroid: $EP_f = \{x \in R^X; x(U) \leq f(U)$ for each $U \subset X\}$.

Edmonds showed that it is possible to optimize a linear function $w^T x$ over an (extended) polymatroid by an extension of the greedy algorithm.

Moreover, there is a strongly polynomial algorithm to find the minimum value of a submodular function, given by a value-giving oracle.

KAM MFF UK and, Institute of Theoretical Computer Science (ITI), Charles University, Malostranske n. 25, 118 00 Praha 1, L Czech Republic.

E-mail address: loebl@kam.mff.cuni.cz