Notes on matroids

Antti Roeyskoe

25.12.2019

1 Matroids

1.1 Basics

A *matroid* $M = (E, \mathcal{I})$ is a finite ground set E along with a collection of sets $\mathcal{I} \subseteq 2^E$ known as the *independent sets*, satisfying

1. $\emptyset \in \mathcal{I}$
2. If $A \in I$ and $B \subseteq A$, then $B \in \mathcal{I}$
3. If $A, B \in \mathcal{I}$ and $|A| < |B|$, exists $x \in B \setminus A$ s.t. $A \cup \{x\} \in \mathcal{I}$

We call set A *independent* if $A \in \mathcal{I}$, and *dependent* if $A \notin \mathcal{I}$. We call set A a *circuit* if it is dependent and if all its strict subsets $B \subset A$ are independent. We call set B a *basis* if it is independent and for all $x \in E \setminus B$ the set $B \cup \{x\}$ is dependent. We'll denote the set of circuits with $\mathcal{C}$ and bases with $\mathcal{B}$.

We define the rank function $r : 2^E \mapsto \mathbb{N}$ as the size of its largest independent subset, i.e.

$$r(A) = \max_{X \subseteq A, X \in \mathcal{I}} |X|$$

Note that by the third property of matroids, all basises of a matroid have the same size $|B| = r(E)$.

The *span* of a set $A \subset E$ is defined as $span(A) = \{x \mid r(A \cap \{x\}) = r(A)\}$.

Theorem 1.1. *For any rank function $r : 2^E \mapsto \mathbb{N}$ and $A, B \subseteq E$ we have*

1. $r(A) \leq r(B)$ *if* $A \subseteq B$
2. $r(A \cup B) \leq |A| + r(B)$
3. $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$ *(submodularity)*

Proof. 1. is clear. The second follows from $r(U) \leq |U|$ and submodularity:

$$r(A \cup B) = r(A \cup B) + r(\emptyset) \leq r(A \setminus B) + r(B) \leq |A| + r(B)$$

To show submodularity, select independent $X \subseteq A \cap B, Y \subseteq A \cup B$ s.t. $|X| = r(A \cap B), |Y| = r(A \cup B)$ and $X \subseteq Y$. This is always possible, as we can first take any maximal X and Y', then add to X elements from Y' until we get a maximal $Y \supset X$. Set

$$U = X \cup ((Y \setminus X) \cap A)$$
$$T = X \cup ((Y \setminus X) \cap B)$$

Now $U \subseteq A$, $T \subseteq B$, and $U, B \in \mathcal{I}$ as $U, B \subseteq Y \in \mathcal{I}$, hence

$$\begin{aligned} r(A) + r(B) &\geq |U| + |T| \\ &= |X \cup ((Y \setminus X) \cap A)| + |X \cup ((Y \setminus X) \cap B)| \\ &= 2|X| + |Y \setminus X| \\ &= |X| + |Y| \\ &= r(A \cap B) + r(A \cup B) \end{aligned}$$

as desired. □

Theorem 1.2. *If X is a dependent set, then there exists a circuit $Y \subseteq X$. Further, if $X \setminus \{x\}$ is independent for any $x \in X$, this circuit is unique.*

Proof. The first claim is clear, as if X is not a circuit, we can remove some element from it so that it remains dependent. However, this can be done at most $|X| - 1$ times, as $\emptyset \in \mathcal{I}$.

Next take any $U \in \mathcal{I}$ and v s.t. $U \cup \{v\} \notin \mathcal{I}$. Assume there exist two distinct circuits $C_1, C_2 \subseteq U \cup \{v\}$. Then exists $a \in C_1 \setminus C_2$. Since C_1 is a circuit, $C_1 \setminus \{a\} \in \mathcal{I}$, hence we can extend it to a set Z s.t. $Z \in \mathcal{I}$, $C_1 \setminus \{a\} \subset Z$ and $|Z| = |U|$. But then $Z = U \setminus \{a\} \cup \{v\}$, and $C_2 \subset Z$ as $a \notin C_2$ contradicting the independence of Z. □

We'll denote the unique circuit contained in $Y \cup \{x\}$, $Y \in \mathcal{I}$ as $C(Y, x)$.

Theorem 1.3. *For $A, B \subseteq E$ we have*

1. *$span(A) \subseteq span(B)$ if $A \subseteq B$*
2. *$r(span(A)) = r(A)$*
3. *$span(span(A)) = span(A)$*

Proof. Assume there exists $x \in span(A) \setminus span(B)$. By submodularity $r(A + x) + r(B) \geq r(B + x) + r(A)$, but since $r(A + x) = r(A)$ we have $r(B) = r(B + x)$, hence $x \in span(B)$, a contradiction.

For any $U \subset span(A) \setminus A$ and $x \in span(A) \setminus U$ we have

$$r(A \cup U) + r(A \cup \{x\}) \geq r(A \cup U \cup \{x\}) + r(A)$$

by submodularity. But $r(A \cup \{x\}) = r(A)$, hence $r(A \cup U \cup \{x\}) \leq r(A \cup U)$. By induction therefore $r(span(A)) = r(A)$.

Finally, for the sake of contradiction assume $r(x \cup span(A)) = r(span(A))$ but $r(x \cup A) > r(A)$. But then

$$r(x \cup A) > r(A) = r(span(A)) = r(x \cup span(A))$$

which violates the condition that $r(A) \leq r(B)$ for $A \subseteq B$. □

1.2 Basis exchange

Theorem 1.4. *(Strong basis exchange)*

Given two bases $B_1, B_2 \in \mathcal{B}$, for every $x \in B_1 \setminus B_2$ exists $y \in B_2 \setminus B_1$ s.t. $B_1 + y - x, B_2 - y + x \in \mathcal{B}$.

Proof. Select any $x \in B_1 \setminus B_2$. Set $C = C(B_2, x)$. We have $x \in C$, hence $x \in span(C - x)$, as $r(C - x) = r(C)$ since $C - x$ is independent and C is a circuit. hence $span((B_1 \cup C) - x) = span(B_1 \cup C) = E$, since B_1 is a basis. Hence $(B_1 \cup C) - x$ contains a basis B_1'. Therefore exists $y \in B_1' \setminus B_1$ s.t. $B_1 - x + y \in \mathcal{B}$. But then $y \in C - x \subseteq B_2$, and $B_2 - y + x \in \mathcal{B}$ as removing y breaks the circuit C. □

2 Matroid Intersection

2.1 Exchange graph

Given a matroid $M = (E, \mathcal{I})$ and an integer $k \geq 0$, we define the truncated matroid $M^k = (E, \mathcal{I}')$ as $\mathcal{I}' = \{U \mid U \in \mathcal{I}, |U| \leq k\}$.

The exchange graph $\mathcal{D}_M(U)$ is the bipartite graph with bipartition U and $E \setminus U$, with an edge between $y \in U$ and $x \in E \setminus U$ if $U - y + x \in \mathcal{I}$.

Theorem 2.1. *For any $U, T \in \mathcal{I}$ with $|U| = |T|$, there exists a perfect matching between $U \setminus T$ and $T \setminus U$ in $\mathcal{D}_M(U)$.*

Proof. Induction on size of $|U \setminus T|$. Case $|U \setminus T| = 0$ is clear. Assume $|U \setminus T| > 0$.

Since U and T are independent in $M^{|U|}$, by strong basis exchange exists $x \in U \setminus T$, $y \in T \setminus U$ s.t. $U - x + y, T + x - y \in \mathcal{I}'$. Hence setting $T' = T + x - y$, by the inductive hypothesis there exists a perfect matching between $U \setminus T'$ and $T' \setminus U$, as $|U \setminus T'| = |U \setminus T| - 1$. We can then add the edge (x, y) that exists as $U - x + y \in \mathcal{I}'$ to achieve a perfect matching between $U \setminus T$ and $T \setminus U$ in $\mathcal{D}_M(U)$. □

Theorem 2.2. *Let U be any independent set, and T a set of equal size s.t. there exists a unique perfect matching between $U \setminus T$ and $T \setminus U$ in $\mathcal{D}_M(U)$. then T is independent.*

Proof. Assume a unique perfect matching exists. Orient edges in $\mathcal{D}_M(U)$ from U to $E \setminus U$ if the edge is used in the matching, and from $E \setminus U$ to U otherwise. Then this graph contains no directed cycles, as otherwise the matching would not be unique. Number vertices in $U \setminus T$ and $T \setminus U$ s.t. the matching uses edges $(x_1, y_1), \ldots, (x_k, y_k)$ and the topological ordering of the vertices is $x_1, y_1, x_2, \ldots, x_k, y_k$.

Suppose T is dependent. Then it contains a circuit C. Assume that y_i is the smallest-indexed vertex from $T \setminus U$ in the circuit. Such i must exist as otherwise $C \subset U$ which contradicts the independence of U. Then for any y_j, $j > i$ in the circuit the edge (x_i, y_j) doesn't exist, hence $y_j \in span(U - x_i)$, hence $span(C - y_i) \subset span(U - x_i)$. But C is a circuit, hence $y_i \in span(C - y_i)$, hence $y_i \in span(U - x_i)$, which contradicts the existence of the edge (x_i, y_i). □

For matroids M_1, M_2 and $U \in \mathcal{I}_1 \cap \mathcal{I}_2$, we define the exchange graph $\mathcal{D}_{M_1,M_2}(U)$ as the bipartite graph with bipartition U and $E \setminus U$, a directed edge from $x \in U$ to $y \in E \setminus U$ if $U - x + y \in \mathcal{I}_1$, and a directed edge from $y \in E \setminus U$ to $x \in U$ if $U - x + y \in \mathcal{I}_2$.

2.2 Matroid min-max theorem

Theorem 2.3. *(The matroid min-max theorem)*

Given two matroids on the same base set $M_1 = (E, \mathcal{I}_1), M_2 = (E, \mathcal{I}_2)$, we have

$$\max_{U \in \mathcal{I}_1 \cap \mathcal{I}_2} |U| = \min_{T \subset E} r_1(T) + r_2(E \setminus T)$$

where r_1 is the rank-function for matroid M_1, and r_2 the rank-function for M_2 respectively.

Proof. For any $U \in \mathcal{I}_1 \cap \mathcal{I}_2$ and $T \subseteq E$, we have

$$\begin{aligned} |U| &= |U \cap T| + |U \cap (E \setminus T)| \\ &= r(U \cap T) + r(U \cap (E \setminus T)) \\ &\leq r(T) + r(E \setminus T) \end{aligned}$$

We'll prove that some U, exists T s.t. the bound is tight by giving an algorithm that finds these sets U. The algorithm will start with $U = \emptyset$, and at every step either produce $U' \in \mathcal{I}_1 \cap \mathcal{I}_2$ with $|U'| = |U| + 1$ or find T s.t. U and T achieve equality in the inequality.

Define $Y_1 = \{y \notin U \mid U + y \in \mathcal{I}_1\}$ and $Y_2 = \{y \notin U \mid U + y \in \mathcal{I}_2\}$. If these sets intersect, take $y \in Y_1 \cap Y_2$ and set $U' = U + x$.

If there exists a Y_1-to-Y_2 path $y_1, x_1, \ldots, x_{k-1}, y_k$ in $\mathcal{D}_{M_1,M_2}(U)$, we will find U'. Otherwise, we will find T.

Assume now such a path P exists. We claim that $U' = U \Delta P$ is independent in M_1 and M_2. First we'll show that $U' \in \mathcal{I}_1$. Define the matroid $M_1' = (E + x_0, \mathcal{I}_1')$ with a new dummy element x_0 that doesn't affect independence, where

$$\mathcal{I}_1' = \{U \subseteq (E + x_0) \mid U \setminus \{x_0\} \in \mathcal{I}_1\}$$

Now $U + x_0 \in \mathcal{I}_1'$. We claim that there exists an unique matching between $U \cap P + x_0$ and $P \setminus U$. If this is the case, $U \Delta P \in \mathcal{I}_1'$, hence $U \Delta P \in \mathcal{I}_1$.

At least one perfect matching exists, namely $(x_0, y_1), \ldots, (x_{k-1}, y_k)$. Assume it isn't unique. Then it contains the edge (x_i, y_j) where $j > i + 1$ for some i, j. If $i = 0$, this implies $y_j \in Y_1$, otherwise the directed edge (x_i, y_j) exists in $\mathcal{D}_{M_1,M_2}(U)$ which shortcuts the path. Both cases contradict the path being the shortest Y_1-to-Y_2 path, hence the perfect matching is unique and we are done.

To show $U' \in \mathcal{I}_2$, we do the same with dummy element x_k and unique perfect matching $(x_1, y_1), \ldots, (x_k, y_k)$.

Now assume no Y_1-to-Y_2 path exists. Set $T = \{z \mid z \textit{ can reach a vertex in } Y_2\}$. We claim that for this T we have $r_1(T) = |U \cap T|$ and $r_2(E \setminus T) = |U \cap (E \setminus T)|$. This would imply the claimed equality $|U| = r_1(T) + r_2(E \setminus T)$.

Assume first $r_1(T) > |U \cap T|$. Then exists $y \in T \setminus U$ s.t. $r_1(U \cap T + y) = |U \cap T| + 1$. But then either $U + y \in \mathcal{I}_1$ or we can take $x \in C_1(U, y)$, $x \neq y$ so that $U - x + y \in \mathcal{I}_1$. In either case $y \in Y_1$, but $y \in T$ hence it can reach a vertex in Y_2 and a Y_1-to-Y_2 path exists, a contradiction.

Next assume $r_2(E \setminus T) > |U \cap (E \setminus T)|$. Then exists $y \in E \setminus T \setminus U$ s.t. $r_2(U \cap (E \setminus T) + y) = |U \cap (E \setminus T)| + 1$. But then either $U + y \in \mathcal{I}_2$ or we can take $x \in C_2(U, y)$ $x \neq y$ so that $U - x + y \in \mathcal{I}_2$. In either case $y \in Y_2$, which contradicts the selection of y from $E \setminus T$. □

3 Weighted matroid intersection

Given a weight function $c : E \mapsto R$, we define $c(T) = \sum_{x \in T} c(x)$. For a matroid $M = (E, \mathcal{I})$ we define the *maximum-weight basis* as $\hat{r}(c) = \max_{B \in \mathcal{I}, |B| = r(E)} c(B)$. The main result of this section is the following theorem, which generalises the matroid min-max theorem to a weighted case:

Theorem 3.1. *(The weight-splitting theorem)*

Given two matroids $M_1 = (E, \mathcal{I}_1)$ and $B_2 = (E, \mathcal{I}_2)$ of equal rank, we have

$$\max_{B \in \mathcal{B}_1 \cap \mathcal{B}_2} c(B) = \min_{c_1 + c_2 = c} \hat{r}_1(c_1) + \hat{r}_2(c_2)$$

We call a basis B *c-maximal* if $c(B) = \hat{r}(c)$. We define the maximum-weight basis matroid $M_c = (E, \mathcal{I}')$, where a set is independent if it can be extended to a c-maximal basis, i.e.

$$\mathcal{I}' = \{U \mid \exists B \in \mathcal{I} \ : \ U \subset B, |B| = r(M), c(B) = \hat{r}(c)\}$$

We'll denote the rank function of M_c by r_c.

Theorem 3.2. *The maximum-weight basis matroid $M_c = (E, \mathcal{I}')$ is a matroid*

Proof. Since some basis must be maximal, $\emptyset \in M_c$. Subsets of independent sets are by definition independent.

Take any $A_1, A_2 \in \mathcal{I}'$ with $|A_1| < |A_2|$. Extend A_2 to a c-maximal basis B_2, and extend A_1 to the c-maximal basis B_1 maximising $|B_1 \cap B_2|$.

If $B_1 \subseteq A_1 \cup B_2$, then

$$B_1 \subseteq (A_2 \setminus A_1) \cup (A_1 \cup (B_2 \setminus A_2))$$

But

$$|B_1| > |B_2| - (|A_2| - |A_1|) \geq |A_1 \cup (B_2 \setminus A_2)|$$

hence exists $x \in B_1 \cap (A_2 \setminus A_1)$, and $A_1 \cup \{x\} \in \mathcal{I}'$.

Otherwise, take $x \in B_1 \setminus A_1 \cup B_2$. By the strong basis exchange lemma there exists $y \in B_2$ s.t. $B_1 + y - x, B_2 - y + x \in \mathcal{I}$. Since B_1 and B_2 are c-maximal, we have $c(B_1) \geq c(B_1 + y - x)$ and $c(B_2) \geq c(B_2 - y + x)$, hence $c(y) - c(x) \leq 0$ and $c(x) - c(y) \leq 0$, hence $c(x) = c(y)$ and $B_1' = B_1 + y - x \in \mathcal{I}'$. But $A_1 \subset B_1'$ and $|B_1' \cap B_2| = |B_1 \cap B_2| + 1$, which contradicts the selection of B_1. $\square$