Matroid Characterizations and Optimization

Recall the definitions of a matroid.

Definition 1 (Matroid)**.** *Let E be a ground set and $\mathcal{I} \subseteq 2^E$ a set system. $\mathcal{M} = (E, \mathcal{I})$ is a* matroid *if the following properties are satisfied:*

(i) $\emptyset \in \mathcal{I}$,

(ii) for all $A \in \mathcal{I}$ and $B \subseteq A$, we have $B \in \mathcal{I}$, and

(iii) for all $A, B \in \mathcal{I}$ with $|A| < |B|$, there exists an element $b \in B \setminus A$ such that $A \cup \{b\} \in \mathcal{I}$.

Properties (i)+(ii) define an independence system. A set $A \subseteq E$ is called *independent* if $A \in \mathcal{I}$, and *dependent* if $A \notin \mathcal{I}$. Minimal dependent sets are called *circuits*, and maximal independent sets are called *bases*.

1 The rank of a matroid and alternative characterizations

All bases of a matroid have the same size. This size is called the *rank* of the matroid. The rank of an arbitrary set $S \subseteq E$ is the size of the largest independent subset of S. More formally, we define the rank function as follows.

Definition 2 (Rank function)**.** *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid. The* rank function $r : 2^E \to \mathbb{N}_{\geq 0}$ *associated to $\mathcal{M}$ is defined as*

$$r(S) := \max_{I \subseteq S s.t. I \in \mathcal{I}} |I|$$

for each $S \subseteq E$. We call $r(E)$ the rank *of $\mathcal{M}$.*

Lemma 1. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid with rank function r. Let $A, B \subseteq E$. Then*

(a) $r(A) \leq |A|$,

(b) $r(A) = |A|$ *if and only if* $A \in \mathcal{I}$,

(c) $r(A) \leq r(A \cup \{e\}) \leq r(A) + 1$ *for all* $e \in E$, *and*

(d) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Proof. The first three statements follow immediately from the definition of the rank function.

For (d), let X_{AB} be a basis of $A \cap B$. Then $|X_{AB}| = r(A \cap B)$. Since $X_{AB} \subseteq A$ and $X_{AB} \in \mathcal{I}$, we can extend X_{AB} to a basis X_A of A. Thus, $X_{AB} \subseteq X_A \subseteq A$, $X_A \in \mathcal{I}$, and $|X_A| = r(A)$. Now, $X_A \subseteq A \cup B$ and $X_A \in \mathcal{I}$. Further, we can extend X_A to a basis $X_{A \cup B}$ of $A \cup B$. So, $X_A \subseteq X_{A \cup B} \subseteq A \cup B$, $X_{A \cup B} \in \mathcal{I}$, and $|X_{A \cup B}| = r(A \cup B)$.

Consider the set $Y = X_{AB} \cup (X_{A \cup B} \setminus X_A)$. Since X_A contains X_{AB} (a basis of $A \cap B$) and $X_A \subseteq A$, any element in $X_{A \cup B} \setminus X_A$ must be in $B \setminus A$. Thus, $Y \subseteq (A \cap B) \cup (B \setminus A) \subseteq B$. Since $X_{A \cup B}$ is an independent set and $Y \subseteq X_{A \cup B}$ (because $X_{AB} \subseteq X_A \subseteq X_{A \cup B}$), Y is an independent set. As $Y \subseteq B$ and $Y \in \mathcal{I}$, its size is at most the rank of B, that is, $|Y| \leq r(B)$.

The sets X_{AB} and $X_{A \cup B} \setminus X_A$ are disjoint (as $X_{AB} \subseteq X_A$). Thus, $|Y| = |X_{AB}| + |X_{A \cup B} \setminus X_A| = |X_{AB}| + (|X_{A \cup B}| - |X_A|)$. Thus,

$$r(B) \geq |Y| = |X_{AB}| + |X_{A \cup B}| - |X_A| = r(A \cap B) + r(A \cup B) - r(A).$$

Rearranging this inequality yields (d). □

With the latter property of the rank function, it is also called a *submodular* function. Submodularity captures the property of *diminishing returns*: adding an element to a larger set never increases the rank by more than adding the same element to a smaller set. This property is central in matroid theory, as it precisely captures the structure and optimizability of many combinatorial problems.

Submodularity allows us to give an alternative characterization of matroids.

Theorem 1 (Characterization of Matroids via the Rank Function)**.** *Let E be a finite set and let $r\colon 2^E \to \mathbb{R}$ be a function satisfying the following three properties:*

(R1) $0 \le r(A) \le |A|$ *for all* $A \subseteq E$*,*

(R2) If $A \subseteq B \subseteq E$*, then* $r(A) \le r(B)$ *(monotonicity),*

(R3) For all $A, B \subseteq E$*,*

$$r(A \cup B) + r(A \cap B) \le r(A) + r(B) \quad \textit{(submodularity).}$$

Then

$$\mathcal{I} := \{Y \subseteq E : |Y| = r(Y)\}$$

defines the independence system of a matroid $\mathcal{M}$ *with ground set* $E(\mathcal{M}) := E$ *and rank function* $r_{\mathcal{M}} = r$*.*

Proof omitted (requires additional properties of the rank function).

We now present another simpler alternative characterization of matroids, showing that it suffices to verify property (iii) only for sets that differ in size by at most one in order to establish the exchange property for a matroid.

Lemma 2 (Alternative Characterizations of Matroids)**.** *Let* $(E, \mathcal{I})$ *be an independence system. Then,* $(E, \mathcal{I})$ *is a matroid if and only if*

(iii') for all $A, C \in \mathcal{I}$ *with* $|A| + 1 = |C|$*, there exists an element* $c \in C \setminus A$ *such that* $A \cup \{c\} \in \mathcal{I}$*.*

Proof. Clearly, (iii) implies (iii'). We now show that (iii') together with (ii) implies property (iii).

Let $A, B \in \mathcal{I}$ with $|A| < |B|$. Choose $C \subseteq B$ such that $|C| = |A| + 1$. By (ii), it holds that $C \in \mathcal{I}$. Then by (iii'), there exists an element $c \in C \setminus A$ such that $A \cup \{c\} \in \mathcal{I}$. Thus, there exists a $c \in C \setminus A \subseteq B \setminus A$ such that $A \cup \{c\} \in \mathcal{I}$. □

2 Matroid optimization

We consider the following matroid optimization problem: Given a matroid $\mathcal{M} = (E, \mathcal{I})$ and a weight function $c\colon E \to \mathbb{R}$, find an independent set $S \subseteq E$ of maximum weight $c(S) := \sum_{e \in S} c_e$.

If $c(e) \ge 0$ for all $e \in E$, this is equivalent to finding a *basis* of maximum weight. If $c(e) < 0$ for some $e \in E$, then e will not be in the optimal solution due to property (ii) (the hereditary property: closed under taking subsets). Thus, such elements e can simply be deleted. In this case, we may not obtain a basis.

The greedy algorithm finds, for each $k \in \mathbb{N}$, a set S_k of maximum weight $c(S)$ among all independent sets $S \subseteq E$ of size $|S| = k$.

Algorithm 1: (Weighted) Greedy Algorithm

Input: An independence system $(E, \mathcal{I})$, weight function $c\colon E \to \mathbb{R}_{\ge 0}$
Output: An independent set $S \in \mathcal{I}$ of maximum total weight

```
S_0 ← ∅;   k ← 1;   U ← E ;
while U ≠ ∅ do
    Select s_k ∈ U with maximum weight c(s_k);
    U ← U \ {s_k};
    if S_{k-1} ∪ {s_k} ∈ I then
        S_k ← S_{k-1} ∪ {s_k};
        k ← k + 1;
return S_k
```

Theorem 2. *For any matroid* $\mathcal{M} = (E, \mathcal{I})$ *and each* k *with* $1 \le k \le r_{\mathcal{M}}(E)$*, the greedy algorithm finds an independent subset of* E *of size* k *whose weight is maximal.*

Proof. The proof is by contradiction. For $1 \le k \le r_{\mathcal{M}}(E)$, let $S_k = \{s_1, s_2, \ldots, s_k\}$ be the independent set constructed by the greedy algorithm with

$$c(s_1) \ge c(s_2) \ge \cdots \ge c(s_k),$$

and let $T_k = \{t_1^k, t_2^k, \ldots, t_k^k\}$ be a maximum-weight independent set of size k with

$$c(t_1^k) \geq c(t_2^k) \geq \cdots \geq c(t_k^k).$$

Assume $c(T_k) > c(S_k)$. Then there must exist an index p with $1 \leq p \leq k$ at which S_k and T_k differ and

$$c(t_p^k) > c(s_p).$$

Now consider the sets

$$A = \{t_1^k, t_2^k, \ldots, t_{p-1}^k, t_p^k\} \quad \text{and} \quad B = \{s_1, s_2, \ldots, s_{p-1}\}.$$

By the exchange property (iii) of matroids and since $|A| > |B|$, there exists an index i with $1 \leq i \leq p$ such that

$$t_i^k \in A \setminus B \quad \text{and} \quad B \cup \{t_i^k\} \in \mathcal{I}.$$

Moreover, since

$$c(t_i^k) \geq c(t_{i+1}^k) \geq \cdots \geq c(t_p^k) > c(s_p),$$

the greedy algorithm would have examined the element t_i^k before s_p and would have selected it instead; a contradiction. □

It is natural to ask whether there exists a class of independence systems more general than matroids that still allows the greedy algorithm to always find a maximum-weight independent set for each cardinality. The following result settles this speculation and shows that the greedy algorithm actually characterizes matroids.

Theorem 3 (Greedy Characterization of Matroids)**.** *Let $\mathcal{M} = (E, \mathcal{I})$ be an independence system. If the greedy algorithm produces maximum-weight independent sets of all cardinalities for every nonnegative weight function $c\colon E \to \mathbb{R}_{\geq 0}$, then $\mathcal{M}$ is a matroid.*

Proof. We show that if $\mathcal{I}$ does not satisfy the exchange property (iii), then there exists a weight function $c\colon E \to \mathbb{R}_{\geq 0}$ for which the greedy algorithm fails to find a maximum-weight independent set.

Suppose there exist $X, Y \in \mathcal{I}$ with $|X| < |Y|$ such that for all $e \in Y \setminus X$, we have $X \cup \{e\} \notin \mathcal{I}$. This violates (iii).

We define a weight function $c\colon E \to \mathbb{R}_{\geq 0}$ by

$$c(e) := \begin{cases} 1+\varepsilon, & \text{if } e \in X, \\ 1, & \text{if } e \in Y \setminus X, \\ 0, & \text{otherwise,} \end{cases}$$

where $\varepsilon > 0$ is a small constant to be chosen.

Consider $Y \in \mathcal{I}$ with $|Y| > |X|$ and weight

$$c(Y) = |X|(1+\varepsilon) + (|Y| - |X|) \cdot 1 = |X|(1+\varepsilon) + |Y| - |X|.$$

With this weight function, the greedy algorithm first selects all elements from X (as $1 + \varepsilon > 1$). It then tries to extend the set to size $|Y|$. However, by assumption, no additional element from $Y \setminus X$ can be added to X (due to the failure of (iii)). Thus, the algorithm only selects elements of weight 0 thereafter.

Let X' denote the set of size $|Y|$ constructed by the greedy algorithm. Then its total weight is

$$c(X') = |X|(1+\varepsilon) + (|Y| - |X|) \cdot 0 = |X|(1+\varepsilon).$$

To reach a contradiction, we choose ε small enough such that

$$c(X') < c(Y) \quad \Leftrightarrow \quad |X|(1+\varepsilon) < |X|(1+\varepsilon) + |Y| - |X| \quad \Leftrightarrow \quad \varepsilon < \frac{1}{|E|}.$$

Such a choice of ε is possible. Therefore, the greedy algorithm does not produce a maximum-weight independent set of size $|Y|$, which is a contradiction. Thus, $\mathcal{I}$ must satisfy the exchange property (iii), and $\mathcal{M}$ is a matroid. □