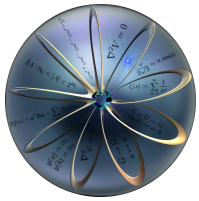

# planetmath.org

Math for the people, by the people.

## matroid

| | |
|---|---|
| Canonical name | Matroid |
| Date of creation | 2013-03-22 13:08:56 |
| Last modified on | 2013-03-22 13:08:56 |
| Owner | mps (409) |
| Last modified by | mps (409) |
| Numerical id | 16 |
| Author | mps (409) |
| Entry type | Definition |
| Classification | msc 05B35 |
| Synonym | independence structure |
| Related topic | ChromaticPolynomial |
| Related topic | DependenceRelation |
| Defines | submodular inequality |

A *matroid* is a combinatorial structure whose properties imitate those of linearly independent subsets of a vector space. Notions such as rank and independence (of a subset) have a meaning for any matroid, as does the notion of duality.

# 1 Definitions of a matroid

A matroid permits several equivalent formal definitions: two definitions in terms of a rank function, one in terms of independent subsets, and several more. We discuss several definitions below.

## First rank definition

**Definition 1** *A matroid consists of a set $E$ and a function $r\colon \mathcal{P}(E) \to \mathbb{N}$ satisfying the axioms:*

*r1 For any $S \in \mathcal{P}(E)$, $r(S) \leq |S|$.*

*r2 The function $r$ is order-preserving.*

*r3 The function $r$ satisfies the submodular inequality. That is, for any $S$, $T \in \mathcal{P}(E)$,*

$$r(S \cup T) + r(S \cap T) \leq r(S) + r(T).$$

In this situation, $r$ is called the *rank function* of the matroid $(E, r)$. If every singleton of $E$ has rank equal to 1, then $(E, r)$ is called a normal matroid.

An isomorphism of matroids $(E, r) \to (F, s)$ consists of a bijection $f : E \to F$ which preserves rank, that is, satisfies $s(f(A)) = r(A)$ for all $A \in \mathcal{P}(E)$.

## Second rank definition

**Definition 2** *A matroid consists of a set $E$ and a function $r\colon \mathcal{P}(E) \to \mathbb{N}$ satisfying the axioms:*

*q1 $r(\emptyset) = 0$.*

*q2 If $x \in E$ and $S \in \mathcal{P}(E)$, then $r(S \cup \{x\}) - r(S)$ is either 0 or 1.*

*q3* *If* $x$, $y \in E$ *and* $S \in \mathcal{P}(E)$, *then* $r(S \cup \{x\}) = r(S \cup \{y\}) = r(S)$ *implies* $r(S \cup \{x, y\}) = r(S)$.

## Independent set definition

**Definition 3** *A matroid is a pair* $(E, \mathcal{I})$ *with* $\mathcal{I} \subseteq \mathcal{P}(E)$ *(called the* independent sets *of* $E$*) satisfying the axioms:*

*i1* *The empty set is independent.*

*i2* *Every subset of an independent set is independent.*

*i3* *For any* $U \subseteq E$, *any two subsets of* $U$ *which are maximal with respect to membership in* $\mathcal{I}$ *have the same cardinality.*

The matroid $(E, I)$ is normal if every singleton in $E$ is independent.

## Base definition

**Definition 4** *A matroid is a pair* $(E, \mathcal{B})$ *with* $\mathcal{B} \subseteq \mathcal{P}(E)$ *(called the* bases *of* $E$*) a subset of* $\mathcal{P}(E)$ *satisfying the axioms:*

*b1* $E$ *has at least one base.*

*b2* *The proper subsets of a base are not bases.*

*b3* *If* $S$ *and* $T$ *are bases and* $x \in E \setminus S$, *then for some* $y \in E \setminus T$, *the set* $(S \cup \{x\}) \setminus \{y\}$ *is a base.*

The matroid $(E, \mathcal{B})$ is called normal if each singleton of $E$ is contained in a base of $E$.

## Closure definition

**Definition 5** *A matroid consists of a set* $E$ *and a function* $\mathrm{cl}\colon \mathcal{P}(E) \to \mathcal{P}(E)$, *called the* closure operator, *satisfying the axioms:*

*cl1* *Any subset of* $E$ *is contained in its closure.*

*cl2* *If* $S \subseteq \mathrm{cl}(T)$ *then* $\mathrm{cl}(S) \subseteq \mathrm{cl}(T)$.

*cl3 If $x$ is in the closure of $S \cup \{y\}$ but not that of $S$, then $y$ is in the closure of $S \cup \{x\}$.*

The closure operator is sometimes also called the *span mapping* of the matroid. In this case $\mathrm{cl}(A)$ is called the span of $A$.

The matroid $(E, \mathrm{cl})$ is normal if the empty set is its own closure.

## Circuit definition

**Definition 6** *A matroid is a pair $(E, \mathcal{C})$ with $\mathcal{C} \subset \mathcal{P}(E)$ (called the* circuits *of $E$) satisfying the axioms:*

*c1 The empty set is not a circuit.*

*c2 The proper supersets of a circuit are not circuits.*

*c3 If $x$ is in the intersection of two distinct circuits $S$ and $T$, then there is a circuit $U \subseteq S \cup T$ which does not contain $x$.*

The matroid $(E, \mathcal{C})$ is normal if no singleton of $E$ is a circuit.

## Combinatorial optimization definition

There's yet another definition of matroids from "Combinatorial Optimization" by Papadimitriou and Steiglitz. pp. 280-285.

It requires three definitions to generate their definition of matroids. These are more or less grabbed from the book above.

A *subset system* (E,g) is a finite set E with g a collection of subsets of E closed under inclusion, meaning that if $A \in g$, and $B \subseteq A$, then $B \in g$.

Definition 2: The *"combinatorial optimization problem"* (nonstandard term used in book) is as follows. Let (E,g) be a subset system and weight w, a nonnegative real function on E. Find the subset in g with the largest total weight.

Definition 3: Let (E,g) be a subset system and w, a weight function defined as above to give the "combinatorial optimization problem". The greedy algorithm for construction of a subset I in g is as follows. Start with I being the empty set. Take the next highest weight element, e in E (w(e) ¿= w(f) for all f in E). If the union of I and e is in g, then add element e to I. Repeat until you exhaust all elements of E.

Now we have the definition of a matroid.

Definition 4:Let M=(E,g) be a subset system. M is a "matroid" if the greedy algorithm correctly solves the "combinatorial optimization problem" for any weight function associated with M.

# 2 Equivalence of the definitions

It would take several pages to spell out what is a circuit in terms of rank, and likewise for each other possible pair of the alternative defining notions, and then to prove that the various sets of axioms unambiguously define the same structure. So let me sketch just one example: the equivalence of Definitions 1 (on rank) and 6 (on circuits). Assume first the conditions in Definition 1. Define a circuit as a minimal subset $A$ of $\mathcal{P}(E)$ having the property $r(A) < |A|$. With a little effort, we verify the axioms (c1)-(c3). Now assume (c1)-(c3), and let $r(A)$ be the largest integer $n$ such that $A$ has a subset $B$ for which

– $B$ contains no element of $C$

– $n = |B|$.

One now proves (r1)-(r3). Next, one shows that if we define $C$ in terms of $r$, and then another rank function $s$ in terms of $C$, we end up with $s$=$r$. The equivalence of (r*) and (c*) is easy enough as well.

# 3 Examples of matroids

Let $V$ be a vector space over a field $k$, and let $E$ be a finite subset of $V$. For $S \subset E$, let $r(S)$ be the dimension of the subspace of $V$ generated by $S$. Then $(E, r)$ is a matroid. Such a matroid, or one isomorphic to it, is said to be representable over $k$. The matroid is normal iff $0 \notin E$. There exist matroids which are not representable over any field.

The second example of a matroid comes from graph theory. The following definition will be rather informal, partly because the terminology of graph theory is not very well standardised. For our present purpose, a graph consists of a finite set $V$, whose elements are called vertices, plus a set $E$ of two-element subsets of $V$, called edges. A circuit in the graph is a finite set of at least three edges which can be arranged in a cycle:

$$\{a, b\}, \{b, c\}, \ldots \{y, z\}, \{z, a\}$$

such that the vertices $a, b, \ldots z$ are distinct. With circuits thus defined, $E$ satisfies the axioms in Definition 6, and is thus a matroid, and in fact a normal matroid. (The definition is easily adjusted to permit graphs with loops, which define non-normal matroids.) Such a matroid, or one isomorphic to it, is called "graphic".

Let $E = A \cup B$ be a finite set, where $A$ and $B$ are nonempty and disjoint. Let $G$ a subset of $A \times B$. We get a "matching" matroid on $E$ as follows. Each element of $E$ defines a "line" which is a subset (a row or column) of the set $A \times B$. Let us call the elements of $G$ "points". For any $S \subset E$ let $r(S)$ be the largest number $n$ such that for some set of points $P$:

– $|P| = n$

– No two points of $P$ are on the same line

– Any point of $P$ is on a line defined by an element of $S$.

One can prove (it is not trivial) that $r$ is the rank function of a matroid on $E$. That matroid is normal iff every line contains at least one point. Matching matroids participate in combinatorics, in connection with results on "transversals", such as Hall's marriage theorem.

# 4 The dual of a matroid

Proposition: Let $E$ be a matroid and $r$ its rank function. Define a mapping $s : \beta(E) \to \mathbb{N}$ by

$$s(A) = |A| - r(E) + r(E - A).$$

Then the pair $(E, s)$ is a matroid (called the dual of $(E, r)$.

We leave the proof as an exercise. Also, it is easy to verify that the dual of the dual is the original matroid. A circuit in $(E, s)$ is also referred to as a cocircuit in $(E, r)$. There is a notion of cobasis also, and cospan.

If the dual of $E$ is graphic, $E$ is called cographic. This notion of duality agrees with the notion of same name in the theory of planar graphs (and likewise in linear algebra): given a plane graph, the dual of its matroid is the matroid of the dual graph. A matroid that is both graphic and cographic is called planar, and various criteria for planarity of a graph can be extended to matroids. The notion of orientability can also be extended from graphs to matroids.

# 5 Binary matroids

A matroid is said to be binary if it is representable over the field of two elements. There are several other (equivalent) characterisations of a binary matroid $(E, r)$, such as:

– The symmetric difference of any family of circuits is the union of a family of pairwise disjoint circuits.

– For any circuit $C$ and cocircuit $D$, we have $|C \cap D| \equiv 0 \pmod 2$.

Any graphic matroid is binary. The dual of a binary matroid is binary.

# 6 Miscellaneous

The definition of the chromatic polynomial of a graph,

$$\chi(x) = \sum_{F \subset E} (-1)^{|F|} x^{r(E)-r(F)},$$

extends without change to any matroid. This polynomial has something to say about the decomposibility of matroids into simpler ones.

Also on the topic of decomposibility, matroids have a sort of structure theory, in terms of what are called minors and separators. That theory, due to Tutte, goes by induction; roughly speaking, it is an adaptation of the old algorithms for putting a matrix into a canonical form.

Along the same lines are several theorems on "basis exchange", such as the following. Let $E$ be a matroid and let

$$A = \{a_1, \ldots, a_n\}$$

$$B = \{b_1, \ldots, b_n\}$$

be two (equipotent) bases of $E$. There exists a permutation $\psi$ of the set $\{1, \ldots, n\}$ such that, for every $m$ from 0 to $n$,

$$\{a_1, \ldots, a_m, b_{\psi(m+1)}, \ldots, b_{\psi(n)}\}$$

is a basis of $E$.

# 7 Further reading

A good textbook is:

James G. Oxley, *Matroid Theory*, Oxford University Press, New York etc., 1992

plus the updates-and-errata file at Dr. Oxley's `http://www.math.lsu.edu/ oxley`website.

The chromatic polynomial is not discussed in Oxley, but see e.g. `http://www.math.binghamton`