Matroids and chromatic polynomials

Tobias Boege

Max-Planck Institute for Mathematics in the Sciences, Leipzig

Geometry of Lorentzian polynomials day
MPI-MiS Leipzig, 24 May 2022

Combinatorial geometries

- Matroids arise as a common combinatorial abstraction of independence in linear algebra and graph theory.
- But appear also in numerous other contexts such as algebraic or stochastic independence, game theory, rigidity theory, cryptography ...

Combinatorial geometries

- Matroids arise as a common combinatorial abstraction of independence in linear algebra and graph theory.
- But appear also in numerous other contexts such as algebraic or stochastic independence, game theory, rigidity theory, cryptography ...
- Example: Let $(v_1, \ldots, v_n)$ be elements of a vector space. The subsets $I \subseteq [n]$ such that $(v_i : i \in I)$ are linearly independent form a matroid.

Combinatorial geometries

- Matroids arise as a common combinatorial abstraction of independence in linear algebra and graph theory.
- But appear also in numerous other contexts such as algebraic or stochastic independence, game theory, rigidity theory, cryptography ...
- Example: Let $(v_1, \ldots, v_n)$ be elements of a vector space. The subsets $I \subseteq [n]$ such that $(v_i : i \in I)$ are linearly independent form a matroid.
- Example: Let $G = (V, E)$ be an undirected graph. The sets $I \subseteq E$ which do not contain a cycle form a matroid.

Matroid cryptomorphisms I: Independent sets

A matroid on ground set N is specified by its collection of independent sets $\mathcal{I} \subseteq 2^N$ satisfying:

- $\emptyset \in \mathcal{I}$,
- $J \subseteq I \in \mathcal{I}$ implies $J \in \mathcal{I}$,
- if $I, J \in \mathcal{I}$ with $|I| > |J|$, then there exists $x \in I \setminus J$ such that $J \cup \{ x \} \in \mathcal{I}$.

Matroid cryptomorphisms I: Independent sets

A matroid on ground set N is specified by its collection of independent sets $\mathcal{I} \subseteq 2^N$ satisfying:

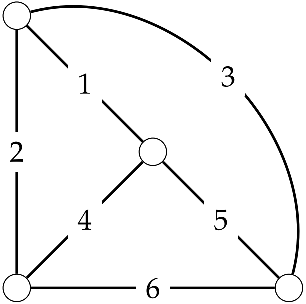
- $\emptyset \in \mathcal{I}$,
- $J \subseteq I \in \mathcal{I}$ implies $J \in \mathcal{I}$,
- if $I, J \in \mathcal{I}$ with $|I| > |J|$, then there exists $x \in I \setminus J$ such that $J \cup \{ x \} \in \mathcal{I}$.

The independent sets of matroids are special (pure) simplicial complexes:

n	1	2	3	4	5	6
Simplicial complexes	1	2	5	20	180	16 143
Matroids	1	2	4	9	21	60

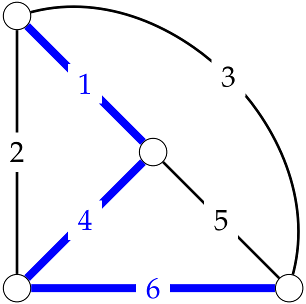
Nelson (2016): Almost all matroids are not linearly representable.

Example



Independent sets:

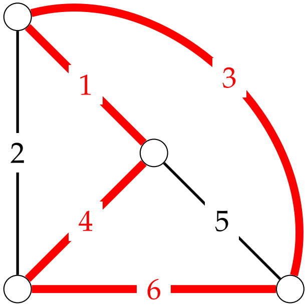
Example



Independent sets:

- $\{1, 4, 6\}$

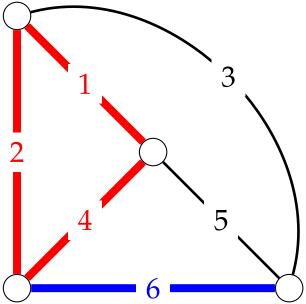
Example



Independent sets:

- $\{1, 4, 6\}$

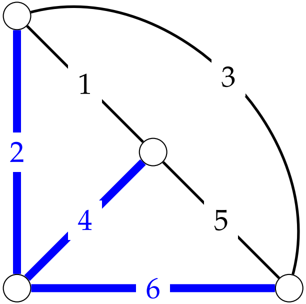
Example



Independent sets:

- $\{1,4,6\}$

Example



Independent sets:

- $\{1, 4, 6\}$
- $\{2, 4, 6\}$ ...

Matroid cryptomorphisms II: Rank function

A matroid on ground set N is specified by its rank function $r : 2^N \to \mathbb{Z}$ satisfying:

- $r(\emptyset) = 0$,
- $r(A) \leq r(B)$ for $A \subseteq B$,
- $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$,
- $r(A) \leq |A|$.

Matroid cryptomorphisms II: Rank function

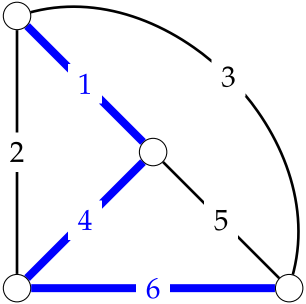
A matroid on ground set N is specified by its rank function $r : 2^N \to \mathbb{Z}$ satisfying:

- $r(\emptyset) = 0$,
- $r(A) \leq r(B)$ for $A \subseteq B$,
- $r(A) + r(B) \geq r(A \cup B) + r(A \cap B)$,
- $r(A) \leq |A|$.

Equivalence of independent sets and rank:

- A set I is independent if and only if $r(I) = |I|$.
- The rank of any set $A \subseteq N$ is $\max \{ |I| : A \supseteq I \in \mathcal{I} \}$.

Example



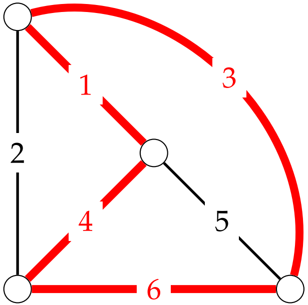
Independent sets:

- $\{1, 4, 6\}$
- $\{2, 4, 6\}$ ...

Ranks:

- $r(\{1, 4, 6\}) = 3$

Example



Independent sets:

- $\{1, 4, 6\}$
- $\{2, 4, 6\}$ ...

Ranks:

- $r(\{1, 4, 6\}) = 3$
- $r(\{1, 3, 4, 6\}) = 3 < 4$ ...

Matroid cryptomorphisms III: Closure operator

A matroid on ground set N is specified by its closure operator $c : 2^N \longrightarrow 2^N$ satisfying:

- $A \subseteq c(A)$,
- $c(A) = c(c(A))$,
- $c(A) \subseteq c(B)$ for $A \subseteq B$,
- if $x \in c(A \cup \{ y \}) \setminus c(A)$ then $y \in c(A \cup \{ x \}) \setminus c(A)$.

The closed sets are called *flats* and they form a lattice.

Matroid cryptomorphisms III: Closure operator

A matroid on ground set N is specified by its closure operator $c : 2^N \longrightarrow 2^N$ satisfying:

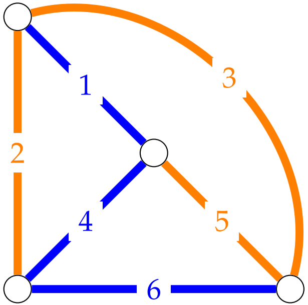
- $A \subseteq c(A)$,
- $c(A) = c(c(A))$,
- $c(A) \subseteq c(B)$ for $A \subseteq B$,
- if $x \in c(A \cup \{ y \}) \setminus c(A)$ then $y \in c(A \cup \{ x \}) \setminus c(A)$.

The closed sets are called *flats* and they form a lattice.

Equivalence of rank and closure operator:

- A is closed if and only if $r(A \cup \{ x \}) > r(A)$ for all $x \notin A$.
- The rank of any set $A \subseteq N$ is its rank in the lattice of flats.

Example



Independent sets:

- $\{1,4,6\}$
- $\{2,4,6\}$ ...

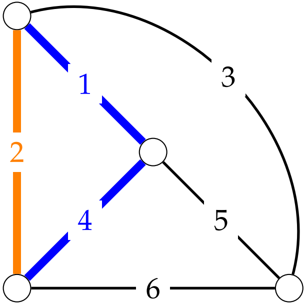
Ranks:

- $r(\{1,4,6\}) = 3$
- $r(\{1,3,4,6\}) = 3 < 4$ ...

Closures:

- $c(\{1,4,6\}) = \{1,2,3,4,5,6\}$

Example



Independent sets:

- $\{1, 4, 6\}$
- $\{2, 4, 6\}$ ...

Ranks:

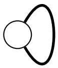
- $r(\{1, 4, 6\}) = 3$
- $r(\{1, 3, 4, 6\}) = 3 < 4$ ...

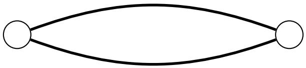
Closures:

- $c(\{1, 4, 6\}) = \{1, 2, 3, 4, 5, 6\}$
- $c(\{1, 4\}) = \{1, 2, 4\}$ ...

Some terminology

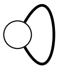
- $x \in N$ is a loop if $r(\{x\}) = 0$.
- $x \neq y \in N$ are parallel if they are not loops and $r(\{x, y\}) = 1$.
- A matroid is simple if it has neither loops or parallel elements.

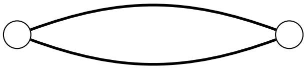




Some terminology

- $x \in N$ is a loop if $r(\{x\}) = 0$.
- $x \neq y \in N$ are parallel if they are not loops and $r(\{x, y\}) = 1$.
- A matroid is simple if it has neither loops or parallel elements.





Given a matroid M on N with rank function r and an element $x \in N$ we define two new matroids on $N \setminus \{x\}$:

- The deletion of x defines $M \setminus x$ whose rank function is the restriction $r|_{2^{N \setminus \{x\}}}$.
- The contraction of x defines M / x with rank function $r(A \cup \{x\}) - r(\{x\})$.

Chromatic polynomial of a graph

The chromatic polynomial of a graph $G = (V, E)$ is

$$\chi_G(q) := \# \text{ proper colorings of } G \text{ with } q \text{ colors.}$$

This is a polynomial because (provided x is neither a loop nor a coloop)

$$\chi_G(q) = \chi_{G \backslash x}(q) - \chi_{G/x}(q),$$
$$\chi_G(q) = q^n \text{ if } |V| = n \text{ and } E = \emptyset.$$

Chromatic polynomial of a matroid

Chromatic (or characteristic) polynomial of a matroid: (See also: Tutte polynomial.)

$$\chi_M(q) = \chi_{M\setminus x}(q) - \chi_{M/x}(q)$$
$$= \sum_{A\subseteq N} (-1)^{|A|} q^{r(N)-r(A)} =: \sum_{k=0}^{r(N)} w_k q^{r(N)-k}.$$

w_k are the Whitney numbers of the first kind and they have alternating signs.

Teaser: Adiprasito-Huh-Katz: The sequence $|w_k|$ is log-concave and unimodal.

Further reading

Karim Adiprasito, June Huh, and Eric Katz. "Hodge theory for combinatorial geometries". English. In: *Ann. Math. (2)* 188.2 (2018), pp. 381–452. ISSN: 0003-486X. DOI: 10.4007/annals.2018.188.2.1.

Federico Ardila. "The geometry of matroids". English. In: *Notices Am. Math. Soc.* 65.8 (2018), pp. 902–908. ISSN: 0002-9920. DOI: 10.1090/noti1720.

Dominic J. A. Welsh. *Matroid theory*. Vol. 8. London Mathematical Society Monographs. Academic Press, 1976.