A hierarchy of matroid descriptions

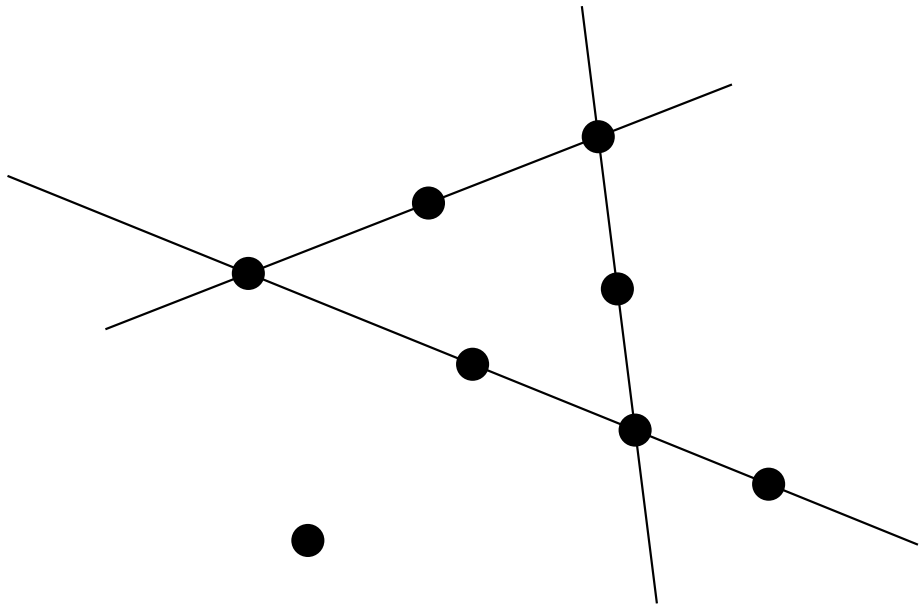
Dillon Mayhew

Victoria University of Wellington

Joint work with Michael Snook

Introduction to matroids

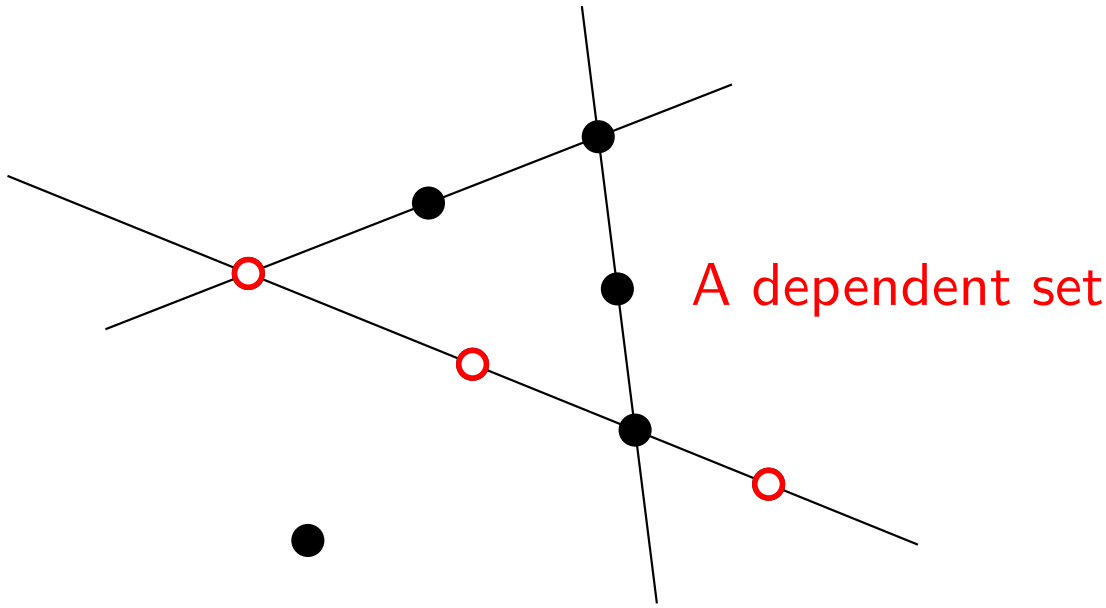
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



Let E be a finite set of points in the plane. A set of 3 points is dependent if it is contained in a line. Otherwise it is a basis.

Introduction to matroids

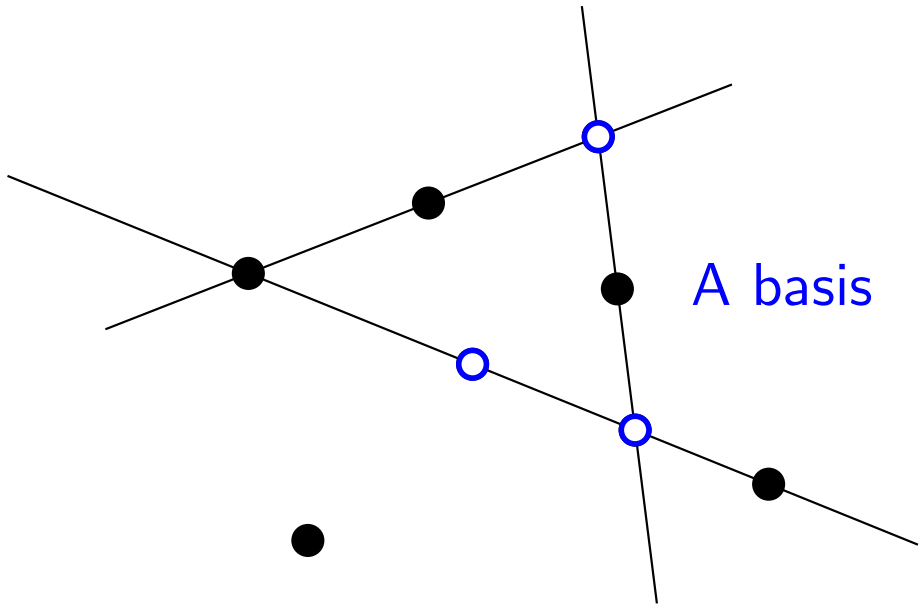
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



Let E be a finite set of points in the plane. A set of 3 points is dependent if it is contained in a line. Otherwise it is a basis.

Introduction to matroids

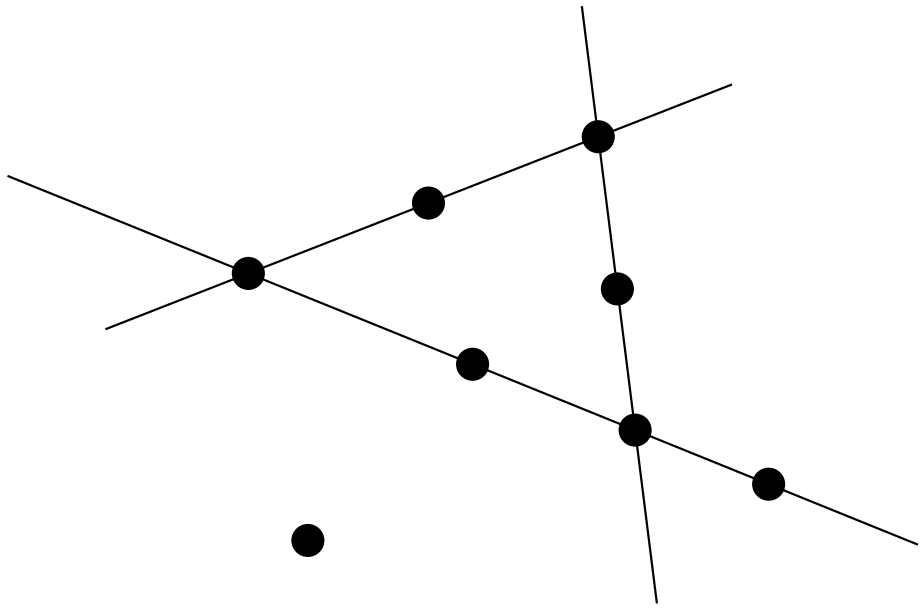
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



Let E be a finite set of points in the plane. A set of 3 points is dependent if it is contained in a line. Otherwise it is a basis.

Introduction to matroids

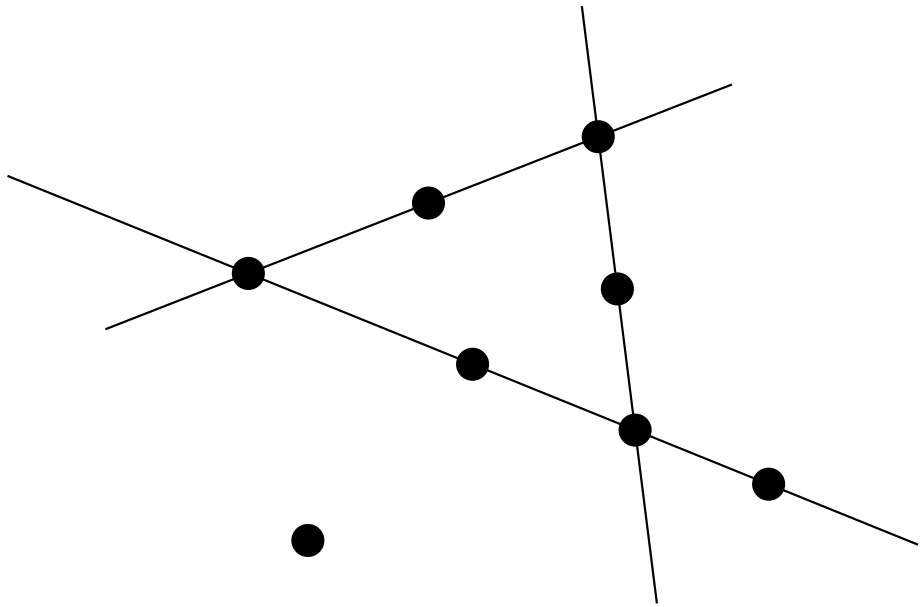
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



Higher dimensions work in the same way. For example, in 3 dimensions, a set of 4 points is a basis if it is not contained in a plane.

Introduction to matroids

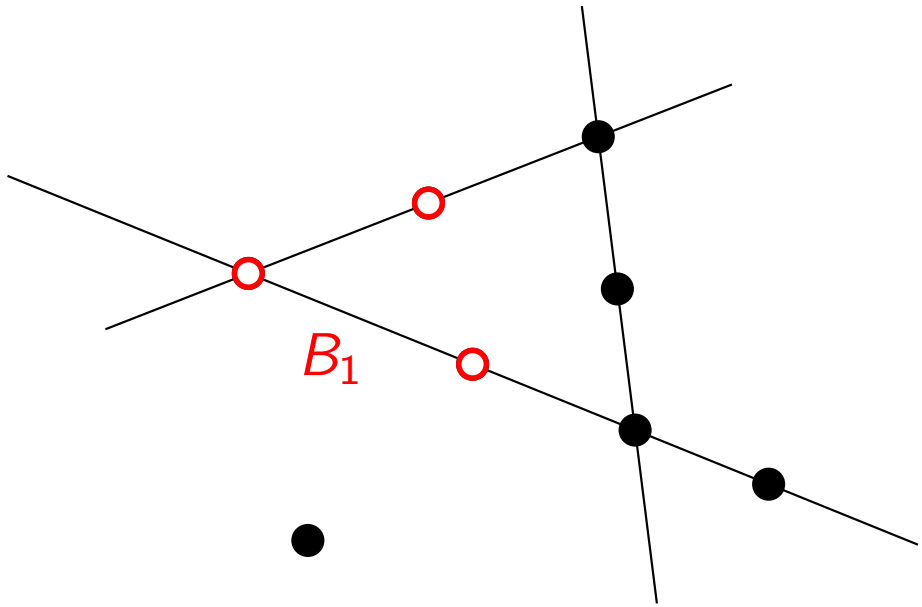
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

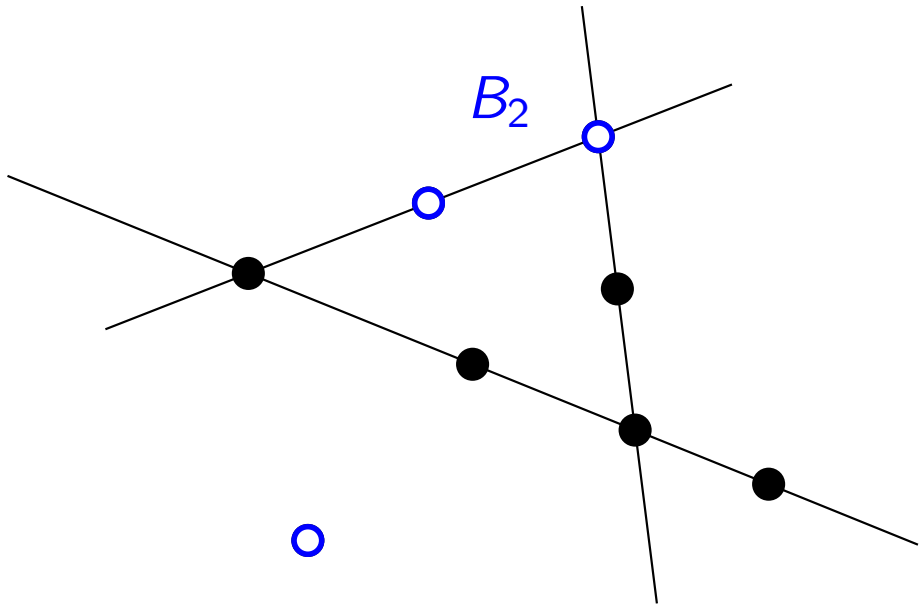
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

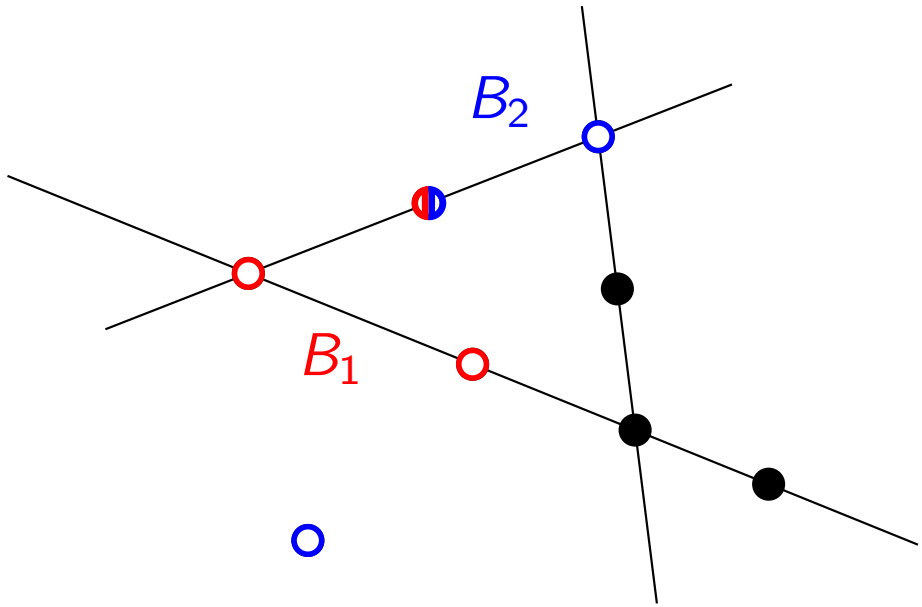
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

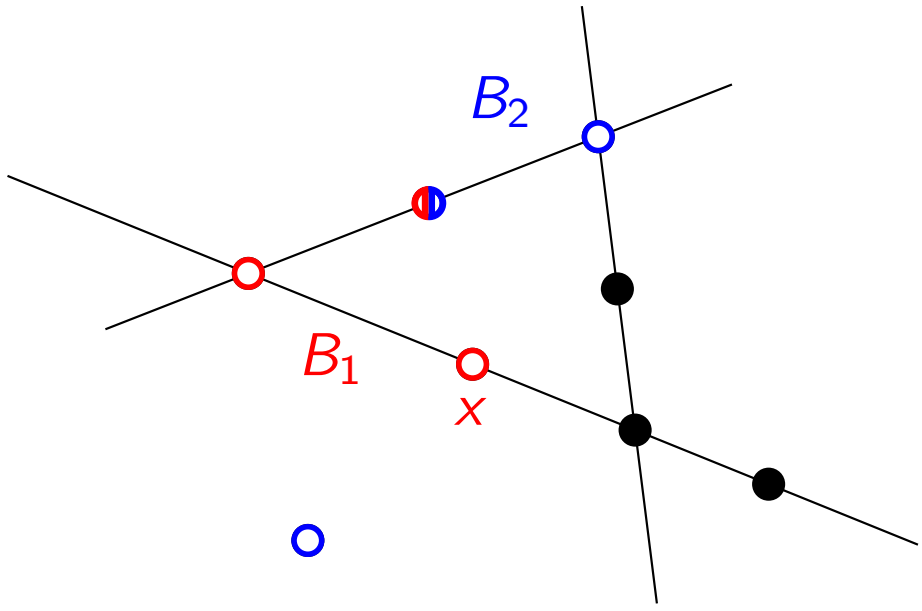
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

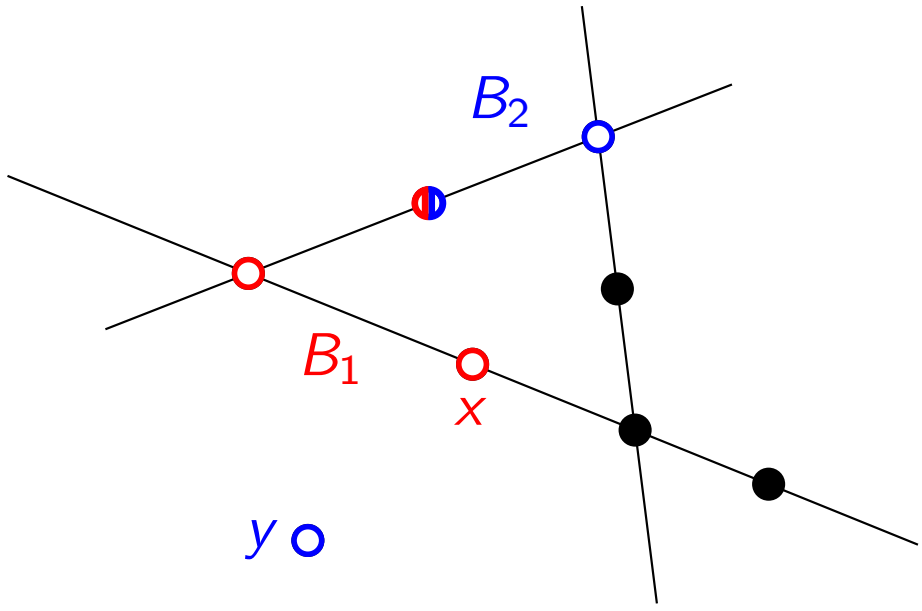
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

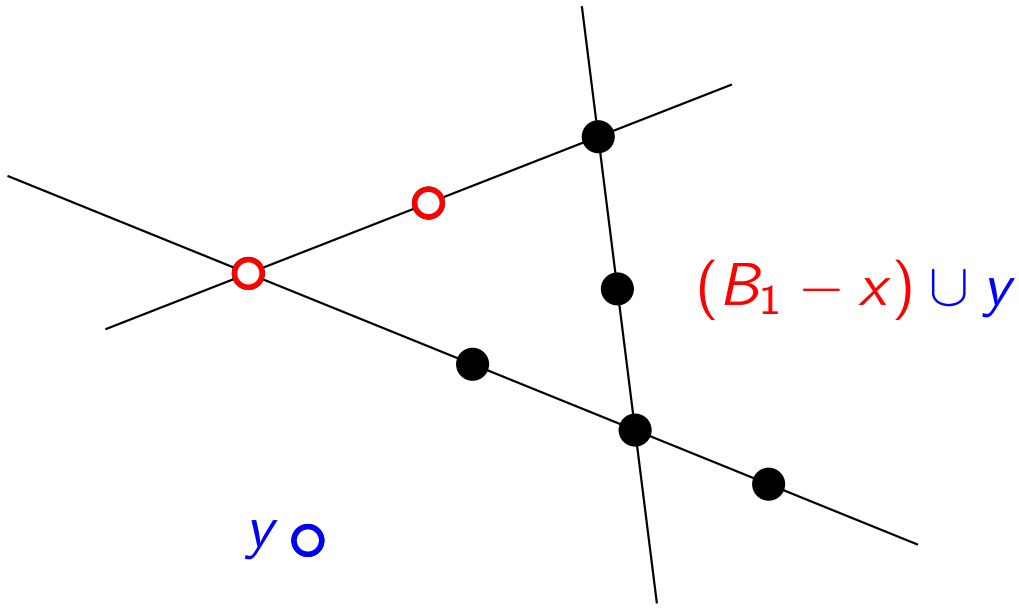
Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

Matroids abstract the notion of (linear, algebraic, geometric) dependence.



If B_1 and B_2 are distinct bases, and $x \in B_1 - B_2$, then there is an element $y \in B_2 - B_1$ such that $(B_1 - x) \cup y$ is a basis.

Introduction to matroids

Definition

A matroid $M = (E, \mathcal{B})$ consists of a finite set, E, and a non-empty family, $\mathcal{B}$, of subsets of E, satisfying:

- if $B_1, B_2 \in \mathcal{B}$, and $x \in B_1 - B_2$, then there exists $y \in B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

E is called the ground set. Members of $\mathcal{B}$ are called bases.

Exercise

Bases are equicardinal.

Introduction to matroids

Matroids can be described by listing subsets other than bases:

- independent sets are subsets of bases,
- dependent sets are subsets that are not independent,
- circuits are minimal dependent subsets,
- spanning sets are subsets that contain bases,
- hyperplanes are maximal non-spanning sets,
- flats are intersections of hyperplanes.

In addition, the rank of $X \subseteq E$ is the size of a largest-possible independent subset in X. The rank function describes the matroid.

Matroid oracles

Let T be a Turing Machine augmented with an oracle which can be queried in unit time about a subset X of the ground set.

The oracle returns YES if X is independent, NO otherwise.

If T halts in polynomial time, given an input string of $|E|$ ones, for every matroid $(E, \mathcal{B})$, then T is a polynomial-time oracle machine.

Theorem (Seymour — 1981)

There is a polynomial-time oracle machine that will decide if a matroid is graphic. There is no polynomial-time oracle machine that will decide if a matroid is binary.

Matroid complexity

Matroid complexity has been dominated by oracle algorithms because there is no polynomial-length description of matroids.

Formally, there is no injective function

$$f : \{\text{Matroids}\} \to \{0,1\}^*$$

and polynomial p such that

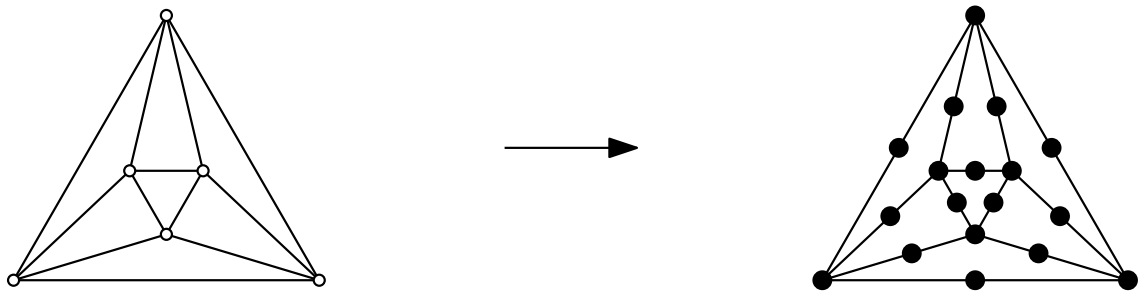
$$|f(M)| \leq p(|E|)$$

for every matroid $M = (E, \mathcal{B})$.

This led to the belief that if the input is a list of bases (for example), then the input is so long that every computational problem is in P.

Matroid complexity

However, there are matroid problems that are intractable, even when the input is a list of bases.



A reduction from graphs to matroids.

The image of this reduction has a polynomial number of bases.

Using this reduction, we can translate graph problems into matroid problems.

Matroid complexity

Theorem

The following problem is isomorphism-complete.

INPUT: Matroids M and N, described via lists of bases.
QUESTION: Are M and N isomorphic?

Theorem

The following problem is NP-complete.

INPUT: Matroids M and N, described via lists of bases.
QUESTION: Does M have a restriction isomorphic to N?

Matroid complexity

The choice of matroid description can have a radical effect on complexity.

3-Matroid Intersection

INPUT: Matroids M_1, M_2, and M_3 on the same ground set.
QUESTION: Do M_1, M_2, and M_3 have a common basis?

If M_1, M_2, and M_3 are described via lists of bases, 3-Matroid Intersection is in P.

If M_1, M_2, and M_3 are described via lists of circuits, 3-Matroid Intersection is NP-complete.

A hierarchy of inputs

Let

$$f_1 : \{\text{Matroids}\} \to \{0,1\}^* \quad \text{and} \quad f_2 : \{\text{Matroids}\} \to \{0,1\}^*$$

be two injective functions.

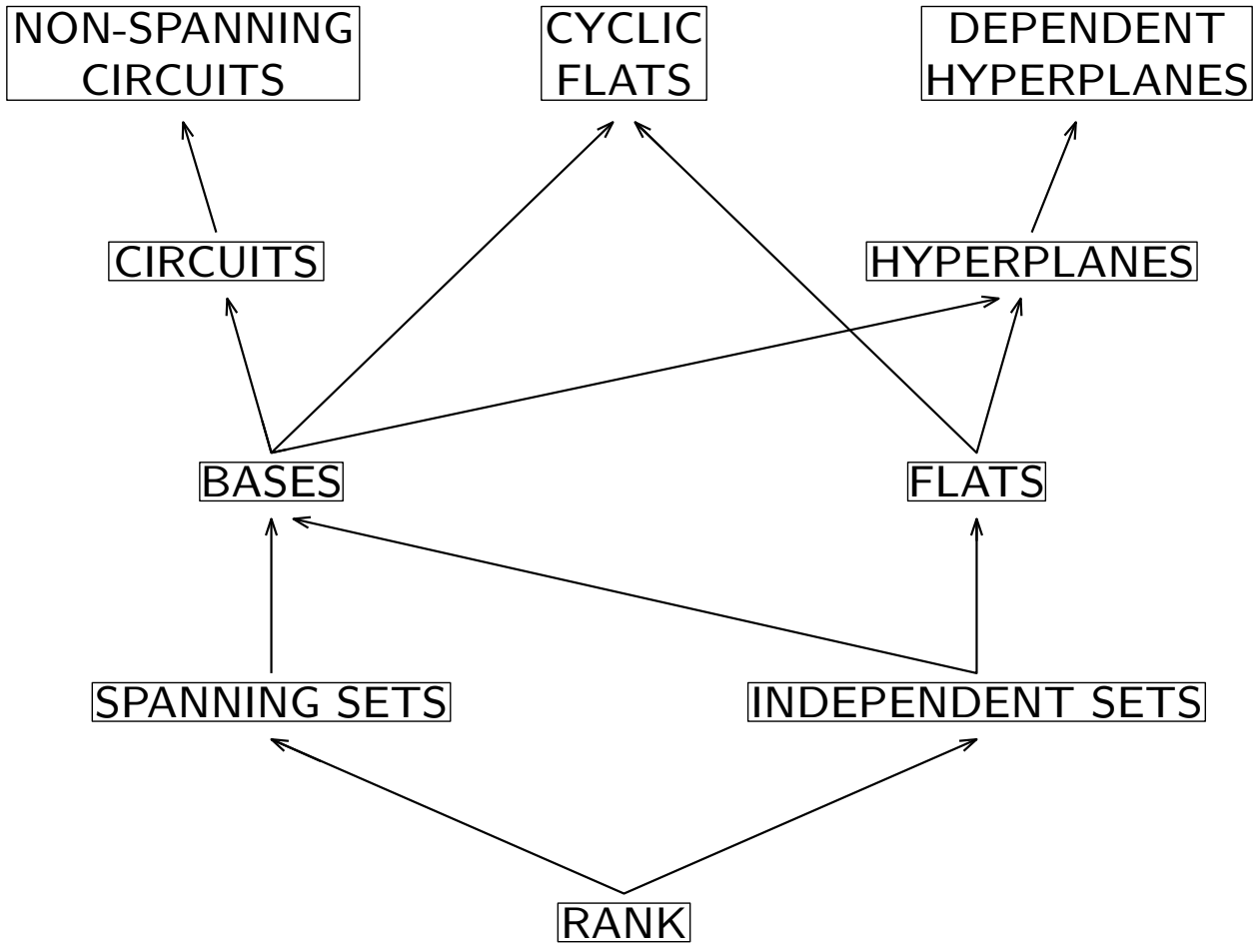
Definition

$f_1 \preccurlyeq f_2$ if there exists a polynomial-time Turing Machine which produces $f_2(M)$ as output, given $f_1(M)$ as input, for any matroid M.

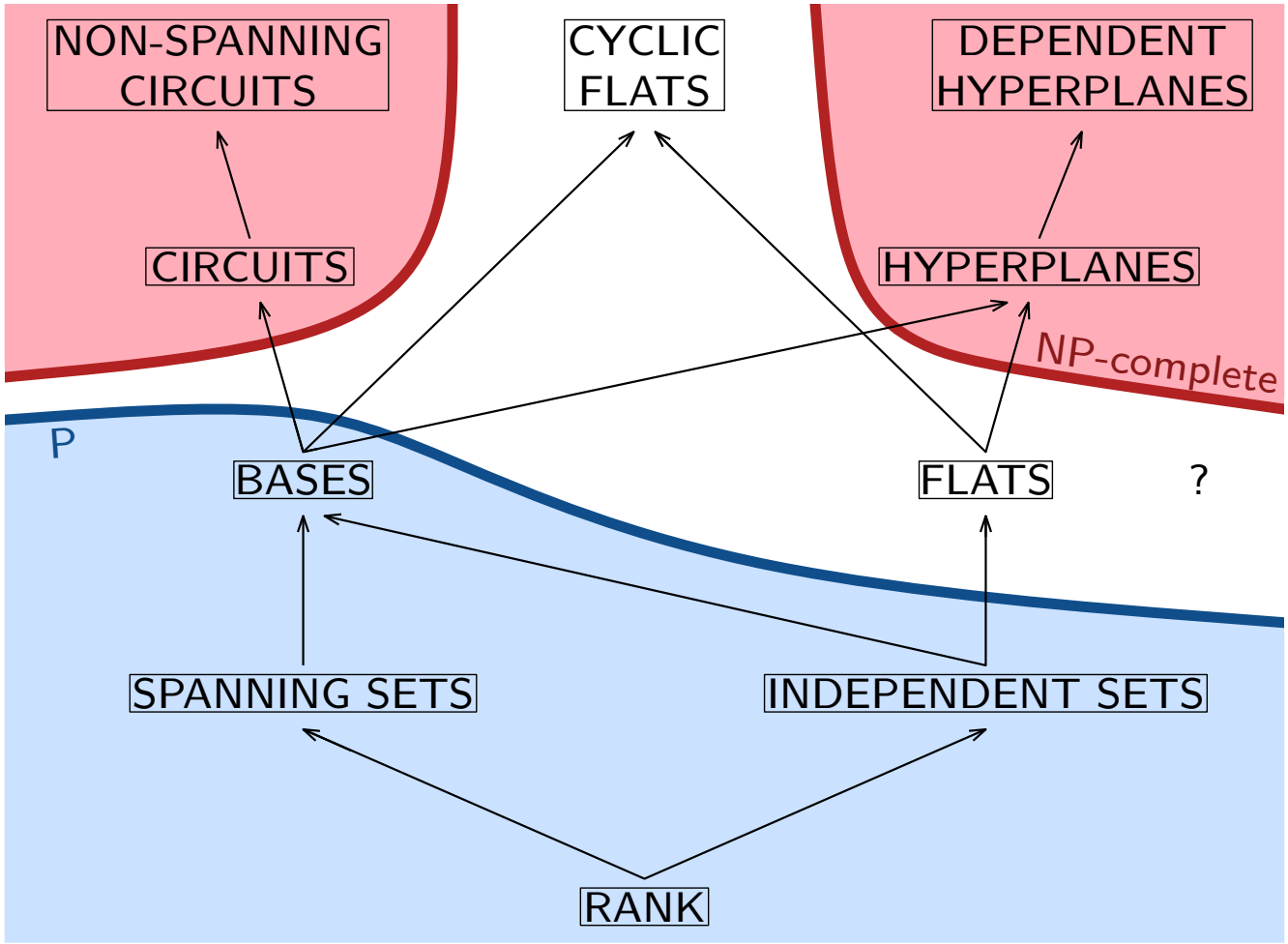
Example

If f_1 lists independent sets, and f_2 lists bases, then $f_1 \preccurlyeq f_2$, but $f_2 \not\preccurlyeq f_1$.

A hierarchy of inputs



A hierarchy of inputs



The complexity of 3-Matroid Matching

A hierarchy of inputs

Let $\mathcal{F}$ be the set of all injective functions

$$f : \{\text{Matroids}\} \to \{0,1\}^*.$$

What is the structure of the quasi-order $(\mathcal{F}, \preccurlyeq)$?

- Does it have a maximal element?
- Does it have infinite antichains?
- Does it have infinite descending chains?
- Does it have infinite ascending chains?

A hierarchy of inputs

An alternative formulation:

Let

$$M_1, M_2, M_3, ...$$

be an enumeration of all matroids.

An injective function $f : \{\text{Matroids}\} \to \{0,1\}^*$ can be seen as an infinite, countable, sequence of finite, distinct, binary strings:

$$f(M_1), f(M_2), f(M_3), \ldots .$$

Let $A = (A_1, A_2, A_3, ...)$ and $B = (B_1, B_2, B_3, ...)$ be two such sequences. Then $A \preccurlyeq B$ if there is a polynomial-time Turing Machine that will output B_i on input A_i, for any $i \in \mathbb{Z}^+$. What is the structure of this quasi-order?

Infinite antichains

Let

$$S_1, S_2, S_3, \ldots$$

be an infinite (countable) sequence of subsets of $\mathbb{Z}^+$ such that $\{[S_1], [S_2], [S_3], \ldots\}$ is an antichain of Turing degrees.

Let $f_i : \{\text{Matroids}\} \to \{0,1\}^*$ be an injective function that lists bases, except that we add a 'flag' to the end of $f_i(M_k)$ if $k \in S_i$.

Then

$$\{f_1, f_2, f_3, \ldots\}$$

is an infinite antichain in $(\mathcal{F}, \preccurlyeq)$.

Infinite descending chains

Let f_0 be in $\mathcal{F}$.

Let $S_1, S_2, S_3, \ldots$ be subsets of $\mathbb{Z}^+$ so that

$$[S_1] <_T [S_2] <_T [S_3] <_T \cdots$$

is an infinite chain of Turing degrees.

For $i \geq 1$ let $f_i \in \mathcal{F}$ be equal to f_0, except that we add a 'flag' to the end of $f_i(M_k)$ if $k \in S_i$.

Then

$$f_0 \succcurlyeq f_1 \succcurlyeq f_2 \succcurlyeq f_3 \succcurlyeq \cdots$$

is an infinite descending chain in $(\mathcal{F}, \preccurlyeq)$.

Infinite ascending chains

Let f_0 be in $\mathcal{F}$.

Assume that $N_1, N_2, N_3 \ldots$ is a sequence of matroids such that

- $|f_0(N_1)|, |f_0(N_1)|, |f_0(N_2)|, \ldots$ grows super-polynomially,
- there is a polynomial-time Turing Machine which will output k on input $f_0(N_k)$.

For example, if f_0 lists bases, then $N_1, N_2, N_3, \ldots$ could be $U_{1,1}, U_{2,2}, U_{3,3}, \ldots$.

Let $p_1, p_2, p_3, \ldots$ be the primes. Let f_i be equal to f_0, except that when k is multiple of one of $p_1, \ldots, p_i$, we replace $f_0(N_k)$ with k.

Then $f_0, f_1, f_2, \ldots$ is an ascending chain in $(\mathcal{F}, \preccurlyeq)$.

Questions

Does every (countable) partial order embed in $(\mathcal{F}, \preccurlyeq)$?

What happens to the structure of $(\mathcal{F}, \preccurlyeq)$ if we impose conditions on the injective functions $f : \{\text{Matroids}\} \to \{0,1\}^*$?

- $|f(M)| \leq C_f 2^{|E|}$ for every matroid $M = (E, \mathcal{B})$, where C_f is a constant.
- There exists a polynomial-time Turing Machine, which can simulate an independence oracle for any matroid $M = (E, \mathcal{B})$, given $f(M)$.
- There exists a Turing Machine which outputs $f(M)$, given $\mathcal{B}$, for any matroid $M = (E, \mathcal{B})$.

What happens if we remove the condition 'polynomial-time' from the definition of $\preccurlyeq$?