AN OUTLINE OF MATROID THEORY
MATH 580, FALL 2001

Version of January 30, 2008.

Web site: `http://math.binghamton.edu/zaslav/580.F01/`

I. **Basic Examples.**

A. **Vector Sets.**

That is, an arbitrary subset $E \subseteq V$, a (finite-dimensional) vector space.

1. Definitions.
   a. Independent sets: $\mathcal{I}(E)$
   b. Bases: $\mathcal{B}(E)$
   c. Circuits (minimal dependent sets): $\mathcal{C}(E)$
   d. Rank function: $r_E(S) = \dim\langle S\rangle$. ($\langle S\rangle$ is the subspace spanned by S.) (We know that $\dim\langle S\rangle = \max\{|I| : I \subseteq S, I \in \mathcal{I}\}$.
2. Properties (that have to be proved).
   a. Independent set properties:
      (1) $\varnothing \in \mathcal{I}$.
      (2) Hereditary property: $I \subseteq J$ and $J \in \mathcal{I} \Rightarrow I \in \mathcal{I}$.
      (3) Augmentation: If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there is $y \in J$ such that $I \cup y \in \mathcal{I}$.
   b. Basis properties:
      (1) $\mathcal{B} \neq \varnothing$.
      (2) Basis exchange: If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then $\exists y \in B_2 \setminus B_1$ such that $B_1 \setminus x \cup y \in \mathcal{B}$.
   c. Circuit properties:
      (1) $\varnothing \notin \mathcal{C}$.
      (2) $\mathcal{C}$ is an antichain: If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.
      (3) Circuit exchange (weak): If $C_1, C_2 \in \mathcal{C}$ and $z \in C_1 \cap C_2$, then there is $C_3 \subseteq C_1 \cup C_2 \setminus z$ with $C_3 \in \mathcal{C}$.
   d. Rank properties:
      (1) Normalization: (a) $r(\varnothing) = 0$ and (b) $r(\{x\}) \leq 1$ for $x \in E$;
      (2) Monotonicity: If $S \subseteq T$, then $r(S) \leq r(T)$);
      (3) Semimodularity (also called submodularity):
      $$r(S \cap T) + r(S \cup T) \leq r(S) + r(T).$$

B. **Graphs.**

A *graph* for our purposes is $\Gamma = (V, E, \iota)$ where V and E are sets (disjoint), called the vertex set and the edge set, and ι is the *incidence function* that tells you which vertices are the endpoints of an edge e. The rule for ι is that $\iota(e)$ is a submultiset of size 2 of V. If the endpoints of e are distinct vertices, then e is a *link*. If the endpoints coincide, then e is a *loop*.

Terminology: the *size* of a graph is the cardinality of its edge set.

1. Definitions.
   a. $\mathcal{I}(\Gamma)$: An independent set is the edge set of a forest.
   b. $\mathcal{B}(\Gamma)$: A basis is the edge set of a maximal forest. If Γ is connected, it is the edge set of a spanning tree (a tree that includes every vertex).
   c. $\mathcal{C}(\Gamma)$: A circuit is the edge set of a simple closed path. (Synonyms for simple closed path in graph theory: circuit, cycle, circle, polygon.)
   d. r_Γ: The rank of $S \subseteq E$ is the maximum size of a forest in S. One can prove that the rank of $S \subseteq E$ is the number of vertices less the number of connected components of (V, S); that is, $r_\Gamma(S) = |V| - c(V, S)$.
2. Properties to be proved: the same as with vector sets.
   a. Independent set properties.
   b. Basis properties.
   c. Circuit properties.
   d. Rank properties.

C. **Transcendental field extensions.**

Let K be an extension of F.

1. Definitions.
   a. Independence: $x_1, \ldots, x_k \in K$ are independent if for each i, $F(x_1, \ldots, x_k)$ is transcendental over $F(x_1, \ldots, \hat{x}_i, \ldots, x_k)$.
   b. Basis: $\{x_1, \ldots, x_k\}$ that is independent and such that K is algebraic over $F(x_1, \ldots, x_k)$.
   c. Circuit: a minimal dependent set.
   d. Rank: $r(S) =$ transcendence degree of $F(S)$ over F.
   (E.g., if $S \subseteq F$, then $r(S) = 0$.)
2. Properties to be proved: the same as with vector sets. Proofs: omitted in this course.

II. **Definition of a Matroid (start).**

A. **Definitions.**

A *matroid* is a structure M with several attributes or aspects, amongst which are

1. The *point set* or *element set*, $E(M)$.
(This must be specified.)

2. One or more of the following equivalent aspects that determine the structure of the matroid.

a. A class of *independent sets*: $\mathcal{I}(M) \subseteq \mathcal{P}(E)$ such that the following *independence axioms* hold:
(1) $\varnothing \in \mathcal{I}$;
(2) $\mathcal{I}$ is hereditary: $I \subseteq J$ and $J \in \mathcal{I} \Rightarrow I \in \mathcal{I}$;
(3) *augmentation*: if $I, J \in \mathcal{I}$ and $|I| < |J|$, then there is $y \in J$ such that $I \cup y \in \mathcal{I}$.

b. A class of *bases*: $\mathcal{B}(M) \subseteq \mathcal{P}(E)$ such that the following *basis axioms* hold:
(1) $\mathcal{B} \neq \varnothing$;
(2) *basis exchange*: if $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then $\exists y \in B_2 \setminus B_1$ such that $B_1 \setminus x \cup y \in \mathcal{B}$.

c. A class $\mathcal{C}(M) \subseteq \mathcal{P}(E)$ of *circuits* such that the following *circuit axioms* hold:
(1) $\varnothing \notin \mathcal{C}$;
(2) $\mathcal{C}$ is an antichain: if $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$;
(2) *(weak) circuit exchange*: If $C_1, C_2 \in \mathcal{C}$ and $z \in C_1 \cap C_2$, then there is $C_3 \subseteq C_1 \cup C_2 \setminus z$ with $C_3 \in \mathcal{C}$.

d. A *rank function* $r_M : \mathcal{P}(E) \to \mathbb{Z}$ such that the following *rank axioms* hold:
(1) *Normalization*: (a) $r(\varnothing) = 0$, and (b) $r(x) \leq 1$ for $x \in E$;
(2) *Monotonicity*: if $S \subseteq T$, then $r(S) \leq r(T)$;
(3) *Semimodularity* or *submodularity*:

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

e. A class of *dependent sets*, which we might call $\mathcal{I}^c(M)$, such that axioms hold that are easily derived from those of independent sets.

f. *Nullity*, a function $n_M : \mathcal{P}(E) \to \mathbb{Z}$, such that appropriate axioms hold. (They can be derived from those of rank.)

g. A *closure operator* $\varphi_M : \mathcal{P}(E) \to \mathcal{P}(E)$, with the following properties (1–4), of which the first three are those of a general *(abstract) closure operator* φ (including topological closure, etc.):
(1) *Increase*: $S \subseteq \varphi(S)$;
(2) *Monotonicity*: If $S \subseteq T$, then $\varphi(S) \subseteq \varphi(T)$;
(3) *Idempotence*: $\varphi(\varphi(S)) = \varphi(S)$.
There are various theorems about abstract closure operators. For instance, $\varphi(S \cup x) = \varphi(\varphi(S) \cup x)$.
(4) *Maclane–Steinitz Exchange Property*: If $x, y \notin \varphi(S)$ and $y \in \varphi(S \cup x)$, then $x \in \varphi(S \cup y)$.

h. A class $\mathcal{L}(M) \subseteq \mathcal{P}(E)$ of *flats* or *closed sets* satisfying:
   (1) $E \in \mathcal{L}$;
   (2) *Closure Under Intersections*: If $A, B \in \mathcal{L}$, then $A \cap B \in \mathcal{L}$;
   (3) *Local Semimodularity*: If $A, B \in \mathcal{L}$ and there is a flat G covered by A and B, then there is a flat F that covers A and B.

   Any closure operator φ has a class $\mathcal{L}$ of closed sets satisfying (1–2), and conversely. $\mathcal{L}$ forms a *lattice* (in the algebraic sense): this is a set with binary operations $\wedge$ (*meet*) and $\vee$ (*join*) that obey certain laws. Lattices will be discussed later.

i. A class $\mathcal{C}^*(M) \subseteq \mathcal{P}(E)$ of *cocircuits* such that the *circuit axioms* hold of $\mathcal{C}^*(M)$.

   Cocircuits will be discussed when we get to duality.

j. Spanning sets.

k. Copoints (maximal flats below E). (Called hyperplanes in the book.)

l. . . .

m. And many more, of which some will show up later in the course.

B. **Cryptomorphisms.**

All the aspects of a matroid are related by specific conversion rules, or *cryptomorphisms*. Here are a selected "few" of them (there are 11 cryptomorphisms above, making 110 directed pairs of conversions, and I'm only asking you to know 30 of them), left blank for **you to fill in** (test your knowledge!—these are important for working with matroids):

1. a $\rightarrow$ b:
2. b $\rightarrow$ a:
3. a $\rightarrow$ c:
4. c $\rightarrow$ a:
5. b $\rightarrow$ c:
6. c $\rightarrow$ b:
7. a $\rightarrow$ d:
8. d $\rightarrow$ a:
9. b $\rightarrow$ d:
10. d $\rightarrow$ b:
11. c $\rightarrow$ d:
12. d $\rightarrow$ c:
13. a $\rightarrow$ e:
14. e $\rightarrow$ a:
15. b $\rightarrow$ e:
16. e $\rightarrow$ b:
17. c $\rightarrow$ e:

18. e → c:
19. d → e:
20. e → d:
21. a → f:
22. f → a:
23. b → f:
24. f → b:
25. c → f:
26. f → c:
27. d → f:
28. f → d:
29. e → f:
30. f → e: