MATH4432 | Lecture 4

Recap: A matroid is a set E together with

* a family of bases $\mathcal{B}$ satisfying (B1) + (B2), or
* a family of independent sets $\mathcal{I}$ satisfying (I1) - (I3), or
* a family of circuits $\mathcal{C}$ satisfying (C1) - (C3), or
* a rank function $r : 2^E \to \mathbb{N}$ satisfying (R1) - (R3).

Matroids capture the notion of independence that underlies

(1) vector spaces, and.

(2) graphs.

First (1).

What is a field? $\mathbb{F} = (F, +, *, 0, 1)$

set F, binary operations $+$ and $*$ from $F \times F \to F$

with identities 0 and 1 respectively

where $+$ and $*$ are associative i.e $(a+b)+c = a+(b+c)$ for all $a, b, c \in F$

commutative i.e $a+b = b+a$ for all $a, b \in F$

* $*$ is distributive over $+$ i.e $a*(b+c) = (a*b)+(a*c)$

for all $a, b, c \in F$.

each element has an additive inverse and each element other than 0 has a multiplicative inverse.

e.g. 1 $\mathbb{R}$ with usual addition $+$ and multiplication $*$.

e.g. 2 $GF(2)$ (think: integers mod 2)

$F = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

Let $\mathbb{F}$ be a field. $\mathbb{F}^m$ denotes the m-dimensional vector space over $\mathbb{F}$ where vectors consist of m coordinates, each of which is in $\mathbb{F}$.

Recall a multiset of vectors $\{\underset{\sim}{v}_1, \underset{\sim}{v}_2, \ldots, \underset{\sim}{v}_n\}$ in $\mathbb{F}^m$ is <u>linearly dependant</u> if there exist scalars $a_1, \ldots, a_n \in \mathbb{F}$, not all 0, such that

$$a_1 \underset{\sim}{v}_1 + a_2 \underset{\sim}{v}_2 + \ldots + a_n \underset{\sim}{v}_n = \underset{\sim}{0}.$$

otherwise they are linearly independent.

Formally, a multiset is a pair (S, σ) where S is a set and $\sigma : S \to \mathbb{Z}^+$ (positive integers). Intuitively, σ tells us how many times an element $s \in S$ appears in the multiset.

In practice we write (for example)

$$\{0, 0, 1, 1\}$$ to refer to

the multiset (S, σ) with $S = \{0, 1\}$ and $\sigma(0) = 2$ and $\sigma(1) = 2$.

example Consider the matrix

$$\begin{array}{cccccccc} & a & b & c & d & e & f \\ A = & \left[\begin{array}{c} 1 \\ 0 \\ 0 \end{array}\right. & \begin{array}{c} 0 \\ 1 \\ 0 \end{array} & \begin{array}{c} 0 \\ 0 \\ 1 \end{array} & \begin{array}{c} 1 \\ 1 \\ 0 \end{array} & \begin{array}{c} 1 \\ 0 \\ 1 \end{array} & \left.\begin{array}{c} 0 \\ 1 \\ 1 \end{array}\right] \end{array}$$

over $GF(2)$

$E = \{a, b, c, d, e, f\}$

$\mathcal{I} = \{ X \subseteq E$: the vectors corresponding to X in A are linearly independent$\}$

The columns labelled by $\{a, b, c\}$ are $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$, and these are linearly independent, so $\{a, b, c\} \in \mathcal{I}$.

On the other hand $\{a, b, d\} \notin \mathcal{I}$.

Note: the choice of field matters!

For $\{d, e, f\}$, we have $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \underset{\sim}{0}$ in $GF(2)$

so $\{d, e, f\} \notin \mathcal{I}$ (but this would not be the case if working over $\mathbb{R}$).

Theorem: Let A be a matrix over $\mathbb{F}$, where the columns are labelled by elements of a set E. Let $\mathcal{I}$ be the set of subsets X of E for which the columns labelled by X form a linearly independent set of vectors.
Then $\mathcal{I}$ is the family of independent sets of a matroid on ground set E.

Recall the dimension of a vector space V is the cardinality of a basis for V (a basis is a maximal linearly independent set of vectors of V)

Proof: We want to show $\mathcal{I}$ satisfies (I1) - (I3).

(I1) and (I2) easily follow from the definition of linear independence. It remains to show (I3) holds.

Let $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$.
For simplicity, we also refer to the corresponding set of vectors as I_1 and I_2.

Let W be the subspace of $\mathbb{F}^m$ spanned by the vectors $I_1 \cup I_2$.
Since I_2 is a linearly independent set of vectors,

$$|I_2| \leq \dim W$$

Suppose, for a contradiction, that for every $e \in I_2 - I_1$ $I_1 \cup e$ is linearly dependent. Then for every such e I_1 spans e. So I_1 spans $I_1 \cup I_2$.

Thus $$\dim W \leq |I_1|$$

But now $|I_2| \leq \dim W \leq |I_1| < |I_2|$ which is a contradiction.

So (I3) holds. $\square$

The last theorem shows that every matrix A over a field $\mathbb{F}$ has a corresponding matroid.

Let $\mathbb{F}$ be a field.
Let A be a matrix over $\mathbb{F}$, and let E be a set of column labels of A. Then we denote the matroid described in the last theorem as $M[A]$

and call it the vector matroid of A.

A matroid M is $\mathbb{F}$-representable if there exists a matrix A over $\mathbb{F}$ such that $M \cong M[A]$.

A matroid M is representable or linear if it is $\mathbb{F}$-representable for some field $\mathbb{F}$.

Back to fields

For any prime p, there is a field $GF(p)$ on p elements corresponding to the integers modulo p.

Theorem: For any positive integer q, there is a field with q elements if and only if q is a prime power. Moreover, all fields on q elements are isomorphic.

(Note: q is a prime power if $q = p^n$ for some prime p and positive integer n).

Fields $(F, +, \cdot, 0, 1)$ and $(F', \oplus, \odot, 0', 1')$ are isomorphic if there exists a bijection

$\psi : F \to F'$ s.t. $\psi(a+b) = \psi(a) \oplus \psi(b)$

and $\psi(a * b) = \psi(a) \odot \psi(b)$.

We refer to the field on q elements as $GF(q)$.

e.g. $GF(4)$: $F = \{0, 1, w, w^2\}$

$+$	0	1	w	w^2
0	0	1	w	w^2
1	1	0	w^2	w
w	w	w^2	0	1
w^2	w^2	w	1	0

$*$	0	1	w	w^2
0	0	0	0	0
1	0	1	w	w^2
w	0	w	w^2	1
w^2	0	w^2	1	w

characteristic of a field:

$$\underbrace{1 + 1 + \cdots}_{p \text{ times}} = 0$$

characteristic p

$GF(4)$ has characteristic 2.

$GF(p)$ has characteristic p for prime p.