

Where innovation starts

Universal Representations of Matroids

Stefan van Zwam

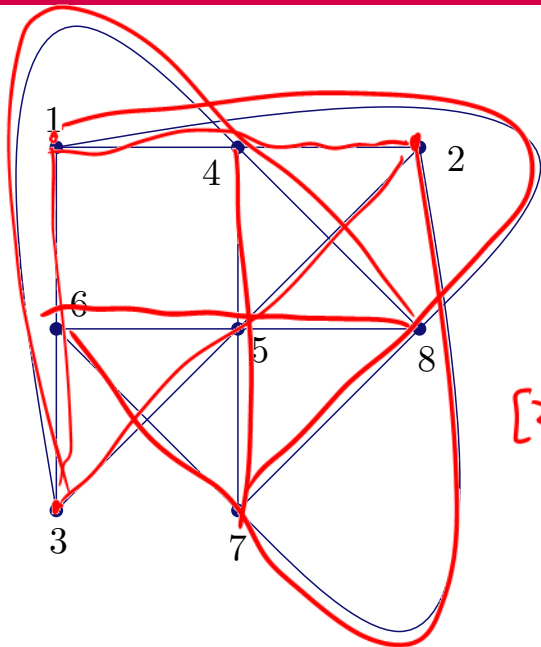
TU e

Technische Universiteit
Eindhoven
University of Technology

Based on joint work with Rudi Pendavingh
May 21, 2008



Example



dep. sets * 2 incident pts.
 * 3 on a line
 * 4 in a plane

$$\begin{array}{ccc|c} 3 & 4 & \delta & \\ 0 & 1 & 1 & \\ 0 & 1 & u & \\ 1 & 0 & v & \end{array} = u-1 = 0$$

[267): $z - x = 0$

$x - v + 1 = 0 \quad v = x + 1$

$1 - y + x = 0$

$$\begin{array}{ccc|c} 1 & 7 & \delta & \\ 0 & x+1 & 1 & \\ 0 & x & x+1 & \end{array}$$

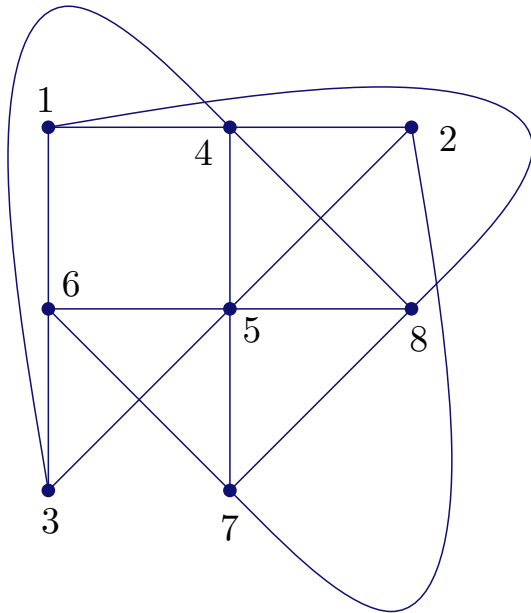
$$= (x+1)^2 - x$$

$$= x^2 + x + 1$$

$$= 0$$

	1	2	3	4	5	6	7	8
1	1	0	0	1	0	1	1	1
2	0	1	0	1	1	0	$x+1$	1
3	0	0	1	0	1	x	x	$x+1$

Example



$$\begin{bmatrix} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 0 & 1 & 1 & 0 & x+1 & 1 \\ 3 & 0 & 0 & 1 & 0 & 1 & x & x & x+1 \end{bmatrix}$$

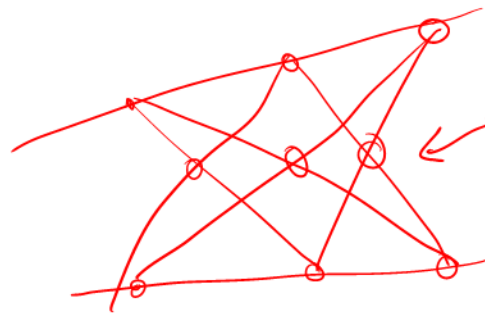
- How to find (all) representations of “combinatorial geometries”.

What is a matroid?

A matroid is a pair (E, \mathcal{B}) , where E is a finite set and \mathcal{B} a collection of subsets of E , the *bases*, satisfying the axioms

- (i) \mathcal{B} is nonempty;
- (ii) If $B_1, B_2 \in \mathcal{B}$, and $x \in B_1 \setminus B_2$, then there exists a $y \in B_2 \setminus B_1$ such that $(B_1 \setminus x) \cup y \in \mathcal{B}$.

Example: E is a set of vectors in some vector space.
Note that not all matroids arise in this way!



not on a line
 \Rightarrow not representable!

Representability

If A is $r \times E$ matrix over field \mathbb{F} , then $M(A) = (E, \mathcal{B})$ is matroid with $E = \{\text{columns of } A\}$ and $\mathcal{B} = \{\text{maximal linearly independent sets}\}$. $M(A)$ invariant under

(i) Swapping columns *and labels*

(ii) Row operations

(iii) Column scaling

Standard representation: some basis forms identity matrix.

$$\left[\begin{array}{ccc|c} & x & & y \\ 1 & & 0 & \\ & \dots & & A' \\ 0 & & 1 & \end{array} \right] \leftrightarrow x \left[\begin{array}{c} y \\ A' \end{array} \right]$$

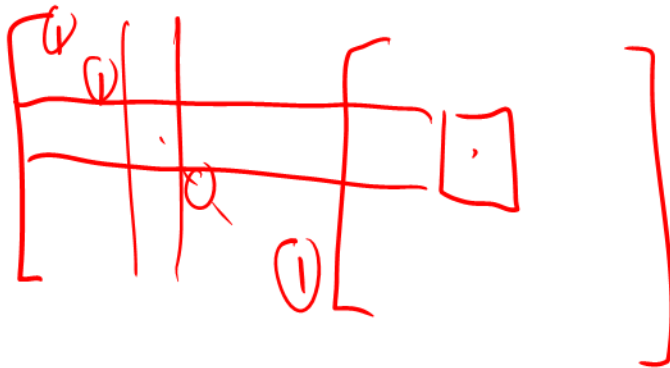
Standard representation

7

Note: 1-1 correspondence between square submatrices of A and $r \times r$ submatrices of $[I|A]$.

Notation: suppose $X' \subseteq X, Y' \subseteq Y$. Then $A[X', Y']$ is restriction of A to rows X' , columns Y' . If $Z \subseteq X \cup Y$ then $A[Z] = A[X \setminus Z, Y \cap Z]$.

Now a set $Z \subseteq X \cup Y$ is a basis of $M([I|A])$ if and only if $|Z| = r$ and $\det(A[Z]) \neq 0$.



Move between standard representations by *pivoting* on a nonzero entry:

$$A = \begin{array}{c} x \\ x' \end{array} \left[\begin{array}{c|c} y & Y' \\ \hline a & b \\ c & D \end{array} \right] \rightarrow \begin{array}{c} y \\ x' \end{array} \left[\begin{array}{c|c} x & Y' \\ \hline a^{-1} & a^{-1}b \\ -a^{-1}c & D - a^{-1}cb \end{array} \right] = A^{xy}.$$

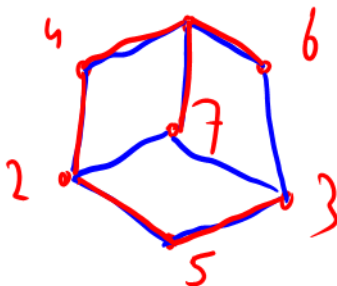
In matrix $[I|A]$ this is row reduction followed by column exchange.

Normalization

Choose basis X . A is an $X \times Y$ rep. matrix over \mathbb{F} .

- Positions of zeroes are fixed.
- $G(A)$ is bipartite graph with vertex classes X, Y .
 $xy \in E(G)$ if and only if $A_{xy} \neq 0$.
- Suppose edges x_1y_1, \dots, x_ky_k form spanning forest of $G(A)$. Let $\theta_1, \dots, \theta_k \in \mathbb{F}^*$. Can scale rows and columns so that $A_{x_iy_i} = \theta_i$ for all i .
- A is *normalized* if, for some spanning forest T , $A_{xy} = 1$ for all $xy \in T$.

$$\begin{array}{c} 1 \\ 2 \\ 3 \end{array} \begin{bmatrix} 4 & 5 & 6 & 7 \\ \textcircled{1} & 0 & \textcircled{1} & \textcircled{1} \\ \textcircled{1} & \textcircled{1} & 0 & 1 \\ 0 & \textcircled{1} & -1 & 1 \end{bmatrix}$$



$M = (X \cup Y, \mathcal{B})$; X basis. $A_{M,X} = (a_{ij})$ $X \times Y$ matrix; a_{ij} unknowns. For each $B \in \mathcal{B}$ an unknown i_B . Ring $\mathbb{Z}[\{a_{ij}\} \cup \{i_B\}]$. Construct ideal I :

- If $(X \setminus i) \cup j \notin \mathcal{B}$ then $a_{ij} \in I$;
- T spanning forest of $G(A)$. If $ij \in T$ then $a_{ij} - 1 \in I$;
- $Z \subseteq X \cup Y$, $|Z| = r$. If $Z \notin \mathcal{B}$ then $\det(A_{M,X}[Z]) \in I$;
- $Z \subseteq X \cup Y$, $|Z| = r$. If $Z \in \mathcal{B}$ then $\det(A_{M,X}[Z])i_Z - 1 \in I$.

$$\overline{\mathbb{B}}_M := \mathbb{Z}[\{a_{ij}\} \cup \{i_B\}]/I.$$

(Fenton 1984, mostly)

Theorem 1. *If A is an $X \times Y$ matrix over field \mathbb{F} such that $M = M([I|A])$, and A is T -normalized, then there is a ring homomorphism $\varphi : \overline{\mathbb{B}}_M \rightarrow \mathbb{F}$ such that*

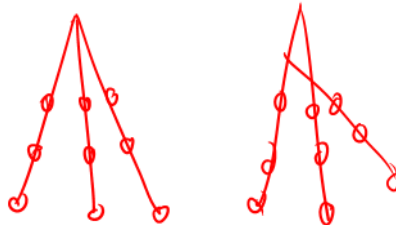
$$\varphi(A_{M,X}) = A.$$

Theorem 2. *$\overline{\mathbb{B}}_M$ does not depend on choice of X or T (different choices give isomorphic rings).*

While this construction works for any fixed matroid, often *classes* of matroids are of interest. For example:

- Free spikes, free swirls (there's one of each for each rank r);
- One-element co-extensions of $\text{PG}(2, q)$, that are still representable over $\text{GF}(q)$;
- Uniform matroids (cf. “The Main Conjecture for MDS codes”).

$U_{r,n}$



- If M_1, M_2 are matroids, how to test if $\overline{\mathbb{B}}_{M_1} \cong \overline{\mathbb{B}}_{M_2}$?
- What rings can occur as $\overline{\mathbb{B}}_M$?



Theorem 3 (Tutte 1965). *If M is binary and 3-connected, then $\overline{\mathbb{B}}_M \cong \text{GF}(2)$ or $\overline{\mathbb{B}}_M \cong \mathbb{Z}$.*

Theorem 4 (Whittle 1997). *If M is ternary, nonbinary, and 3-connected, then $\overline{\mathbb{B}}_M \cong \text{GF}(3)$ or $\mathbb{Z}[1/2]$ or $\mathbb{Z}[\zeta]$ or $\mathbb{Z}[\alpha, 1/\alpha, 1-\alpha, 1/(1-\alpha)]$. Here ζ is a root of $x^2 - x + 1$.*

Note: no finite list for $\text{GF}(q)$, $q \geq 4$. Otherwise no results known for nonbinary and nonternary classes.

A' is a *minor* of A (notation: $A' \preceq A$) if A' can be obtained from A by a sequence of the following operations:

- (i) Multiplying the entries of a row or column by a unit;
- (ii) Deleting rows or columns;
- (iii) Permuting rows or columns (together with labels);
- (iv) Pivoting over a nonzero entry.

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & p & 1 \end{array} \right] \quad \begin{array}{c} \circ \\ \circ \\ \circ \\ \circ \end{array}$$
$$\left(\begin{array}{c} 1 \\ 1 \\ p^{-1} \end{array} \right) \quad \left(\begin{array}{c} -1 \\ p^{-1} \\ 1 \end{array} \right)$$

$$\text{Cr}(A) := \left\{ p : \begin{bmatrix} 1 & 1 \\ p & 1 \end{bmatrix} \preceq A \right\}.$$

Occur in pairs of (at most) six:

$$\left\{ p, 1-p, \frac{1}{1-p}, \frac{p}{p-1}, \frac{p-1}{p}, \frac{1}{p} \right\}.$$

Theorem 5. $\overline{\mathbb{B}}_M$ equals the subring generated by $\text{Cr}(A_{M,x})$.

Fundamental elts.: $\mathcal{F}(\mathbb{B}_M) := \{p \in \mathbb{B}_M^* \mid 1 - p \in \mathbb{B}_M^*\}$.

$\tilde{F} := \{\tilde{p} \mid p \in \mathcal{F}(\mathbb{B}_M)\}$ set of symbols, I ideal in $\mathbb{Z}[\tilde{F}]$ generated by

(i) $\tilde{0} - 0; \tilde{1} - 1;$

(ii) $\widetilde{-1} + 1$ if $-1 \in \mathcal{F}(\mathbb{B}_M);$

(iii) $\tilde{p} + \tilde{q} - 1$, where $p, q \in \mathcal{F}(\mathbb{B}_M), p + q = 1;$

(iv) $\tilde{p}\tilde{q} - 1$, where $p, q \in \mathcal{F}(\mathbb{B}_M), pq = 1;$

(v) $\tilde{p}\tilde{q}\tilde{r} - 1$, where $p, q, r \in \text{Cr}(A_{M,X}), pqr = 1$, and

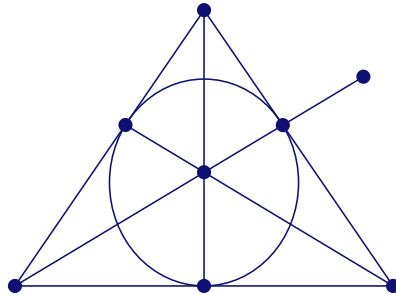
$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & p & q^{-1} \end{bmatrix} \preceq A_{M,X}. \quad (1)$$

Theorem 6. M is representable over $\mathbb{Z}[\tilde{F}]/I$.

For this to be useful beyond ternary matroids, need:

- Understand the set $\mathcal{F}(\mathbb{B}_M)$, or
- Manage to replace $\mathcal{F}(\mathbb{P})$ by $\text{Cr}(A)$ throughout and characterize relations (iii), (iv) in terms of minors.

Nasty example: universal partial field of following configuration is $\text{GF}(2)[\alpha, \cancel{1-\alpha}, 1/\alpha, 1/(1-\alpha)]$. The set of fundamental elements is *infinite*, since $1 - \alpha^{2^k} = (1 - \alpha)^{2^k}$.



Suggestions?