On Inequivalent Representations

Stefan van Zwam
Princeton University

Based on joint work with
Jim Geelen, Bert Gerards, Rhiannon Hall,
Tony Huynh, Rudi Pendavingh,
Dillon Mayhew, Geoff Whittle

AMS Sectional Meeting, Special Session on Connections between Matroids, Graphs, and Geometry, Oxford, MS, March 2, 2013.

A talk in 4 parts

- I. Matroids, representations
- II. Kahn's Conjecture
- III. The prime field case
- IIII. Arbitrary fields

Part I
Matroids, representations

Linear codes

Definition.
Let $\mathbb{F}$ be finite field. $C \subseteq \mathbb{F}^n$ is an $[n, k, d]$ *linear code* over $\mathbb{F}$ if

(i) C is linear subspace of dimension k

(ii) The minimum weight is $\geq d$

Definition.
For $c \in \mathbb{F}^n$, *support* of c:

$$\|c\| := \{i \in [n] : c_i \neq 0\}.$$

The *weight* of c: size of support.

Linear codes

Definition.
Let $\mathbb{F}$ be finite field. $C \subseteq \mathbb{F}^E$ is an $[E, k, d]$ *linear code* over $\mathbb{F}$ if

(i) C is linear subspace of dimension k

(ii) The minimum weight is $\geq d$

Definition.
For $c \in \mathbb{F}^E$, *support* of c:

$$\|c\| := \{i \in E : c_i \neq 0\}.$$

The *weight* of c: size of support.

Matroids

Definition: *Elementary word:* $c \neq \underline{0}$, inclusionwise minimal support.

Theorem.
Define

$$\mathcal{C}^* := \{\|c\| : c \in C, \textit{elementary}\}.$$

Then $\mathcal{C}^*$ is set of cocircuits of a matroid, $M(C)$.

Matroids

Theorem.
Define

$$\mathcal{C}^* := \{\|c\| : c \in C, \textit{elementary}\}.$$

Then $\mathcal{C}^*$ is set of cocircuits of a matroid, $M(C)$.

(Co)circuit axioms

$\mathcal{C}^*$ is set of cocircuits of a matroid if and only if

- $\emptyset \notin \mathcal{C}^*$
- $C, D \in \mathcal{C}^*$ and $C \subseteq D$ then $C = D$
- $C, D \in \mathcal{C}^*$, $C \neq D$, $e \in C \cap D$, then $(C \cup D) - e$ contains a cocircuit

Usual suspects

Duality/dual code $C^\perp := \{d : \langle c, d\rangle = 0 \ \forall c \in C\}$

$$M(C^\perp) = M(C)^*$$

Deletion/puncturing $C \setminus e$: remove coordinate indexed by e from each word

$$M(C\setminus e) = M(C)\setminus e$$

Contraction/shortening C/e: restrict to words having $c_e = 0$, then remove coordinate

$$M(C/e) = M(C)/e$$

Matrices

Definition.

Generator matrix A: rows form basis of C
Parity check matrix H: rows form basis of $C^{\perp}$

$$c \in C \iff Hc^T = 0$$

Write $M[A]$ for $M(C)$.

The main question:

When is $M(C_1) = M(C_2)$?
When is $M[A_1] = M[A_2]$?

Interpretations:

- Algorithm
- Counting

Algorithm

Theorem (Král' (2007), basically)
If $M[A_1]$ has bounded branch width, can test in polynomial time if $M[A_1] = M[A_2]$.

Conjecture (Geelen, Gerards, Whittle)
There is always a polynomial-time algorithm to test if $M[A_1] = M[A_2]$.

Counting

- Exact, for given matroid: basically previous slide.
- Qualitatively: upper bounds.

Part II
Kahn's Conjecture

Easy cases

Theorem.
If C_1 and C_2 binary, then

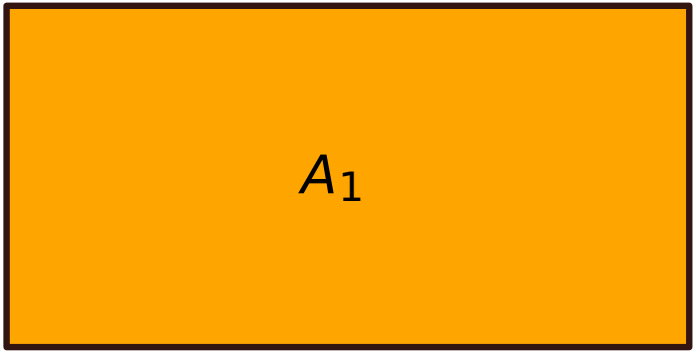
$$M(C_1) = M(C_2) \iff C_1 = C_2.$$

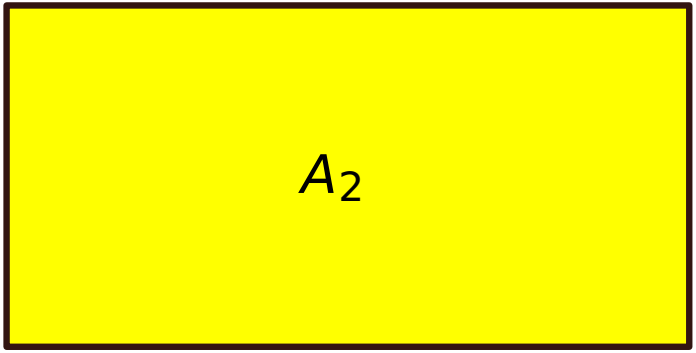
Theorem (Brylawski, Lucas).
If C_1 and C_2 ternary, then

$$M(C_1) = M(C_2) \iff C_1 = C_2'$$

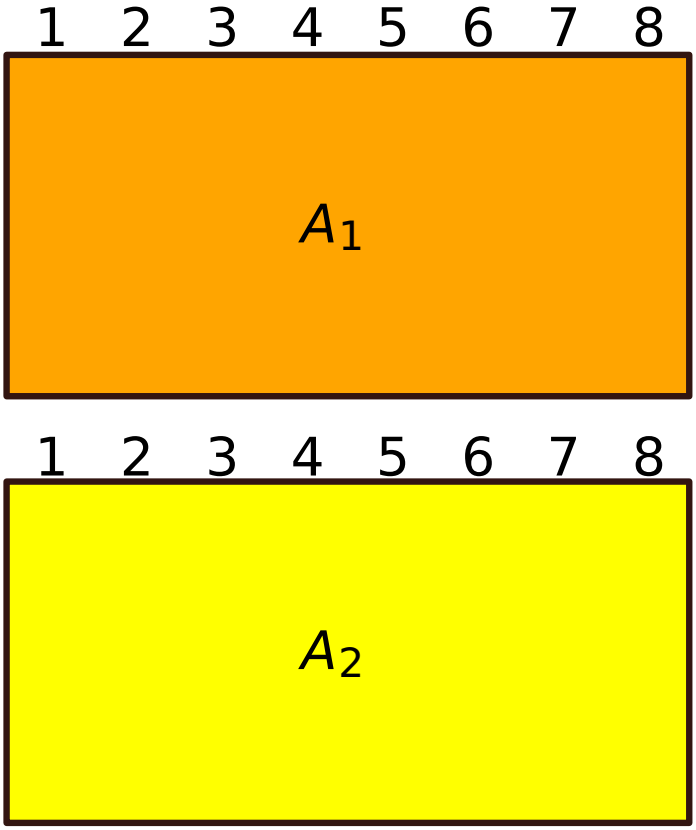
where some coordinates of C_2 were scaled by -1 to get C_2'.

Operations

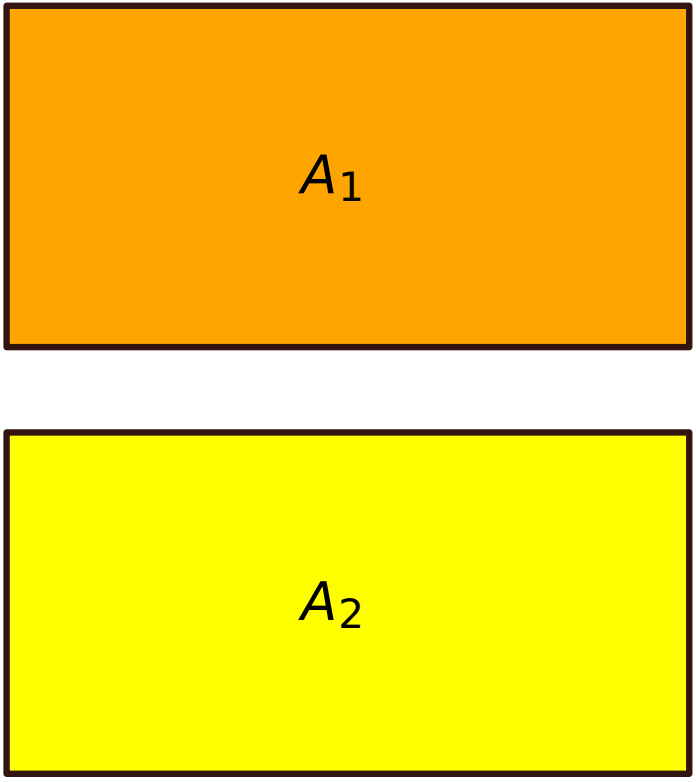




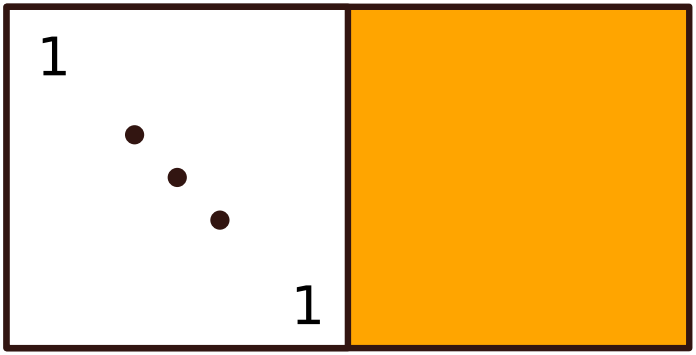
Operations

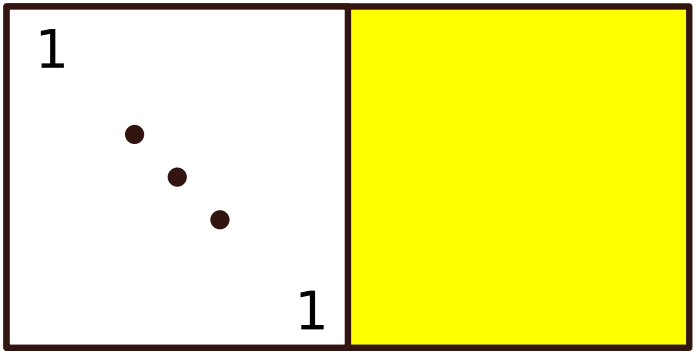


Operations

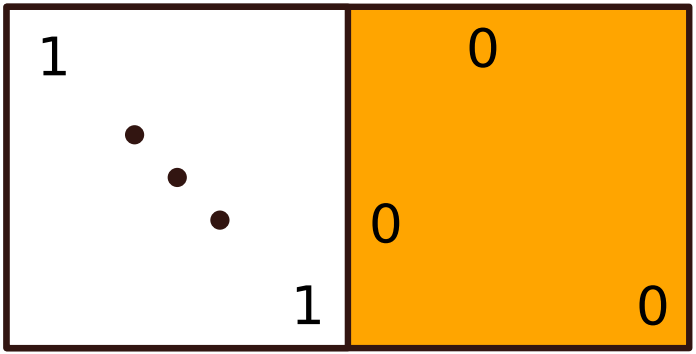


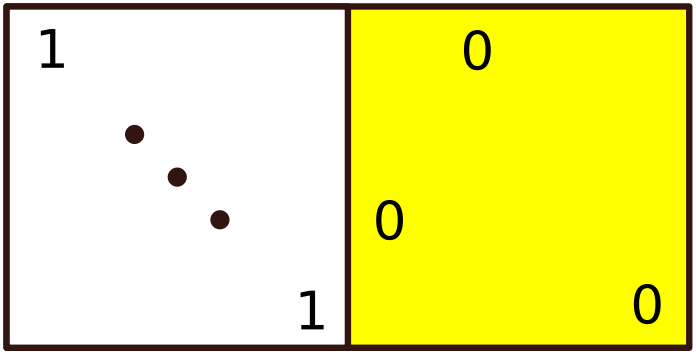
Operations



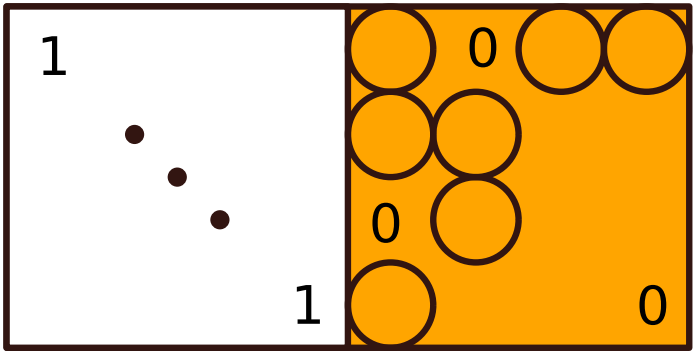


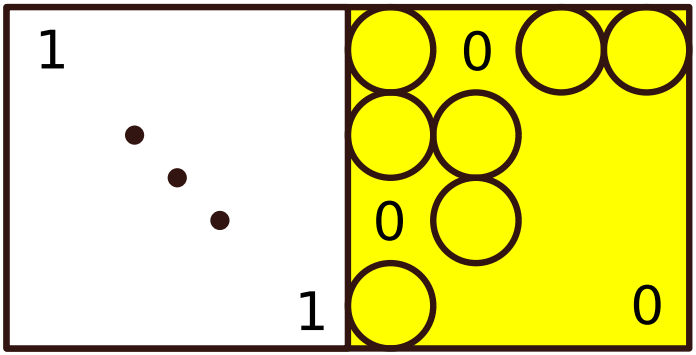
Operations



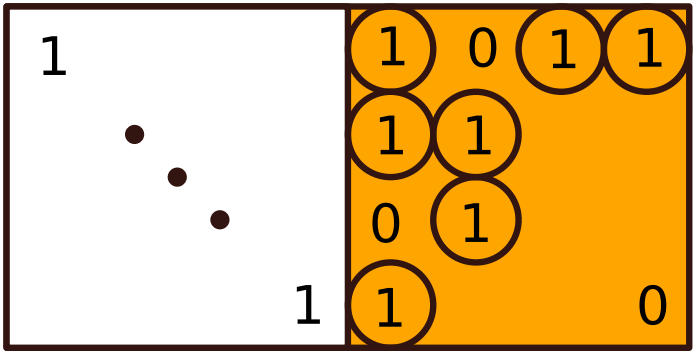


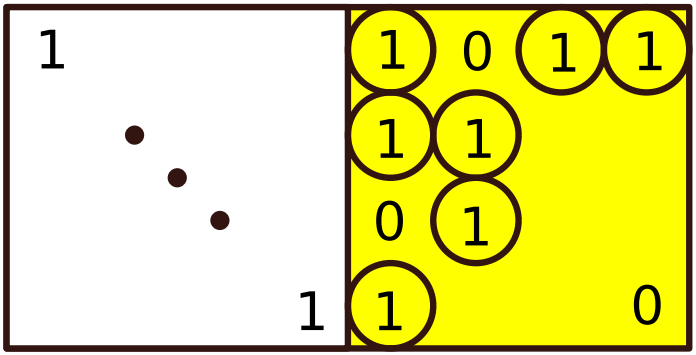
Operations





Operations





No bound?

$$\begin{bmatrix} 1 & 1 & & & & & \\ 1 & 2 & & & & & \\ & & 1 & 1 & & & \\ & & 1 & 3 & & & \\ & & & & 1 & 1 & \\ & & & & 1 & 2 & \\ & & & & & & \ddots \\ & & & & & & & \ddots \\ & & & & & & & & \ddots \end{bmatrix}$$

Relief

Theorem (Kahn 1981).
If A_1, A_2 quaternary, $M[A_1]$ **3-connected**, $M[A_1] = M[A_2]$ then A_1, A_2 related through

- Row operations
- Column scaling
- Field automorphism

Kahn's Conjecture

Conjecture.
For each $\mathbb{F}$, there is c such that each 3-connected M has at most c inequivalent representations.

Hurray!

Theorem (Oxley, Vertigan, Whittle 1995).
For GF(5), each 3-connected M has at most 6 inequivalent representations.

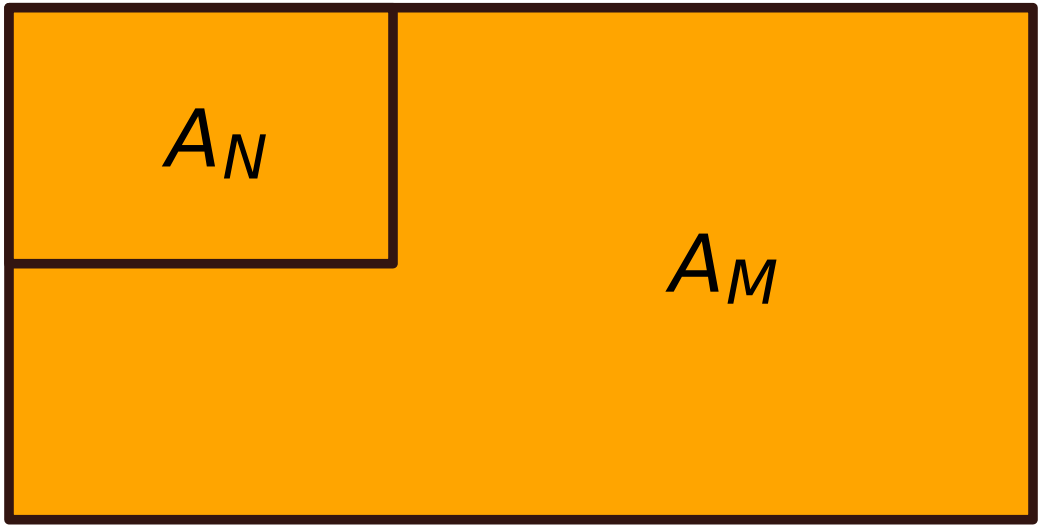
Alas.

Theorem (Oxley, Vertigan, Whittle 1995).
For GF(5), each 3-connected M has at most 6 inequivalent representations.

Theorem (Oxley, Vertigan, Whittle 1995).
Kahn's Conjecture is *false* for all larger fields.

Stabilizers

Stabilizers



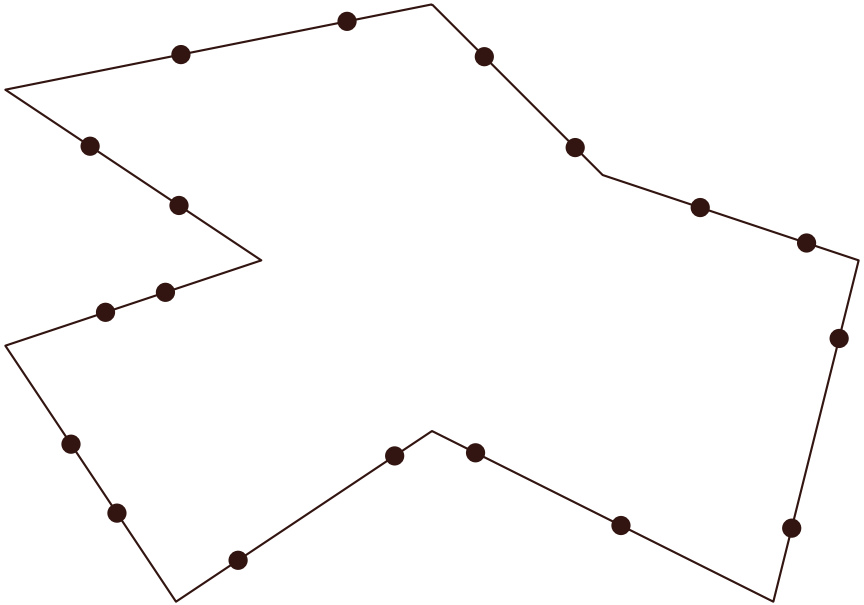
Stabilizer

Whittle's Stabilizer Theorem (1999).
If N is not a stabilizer for a class, it will show after 2 steps.

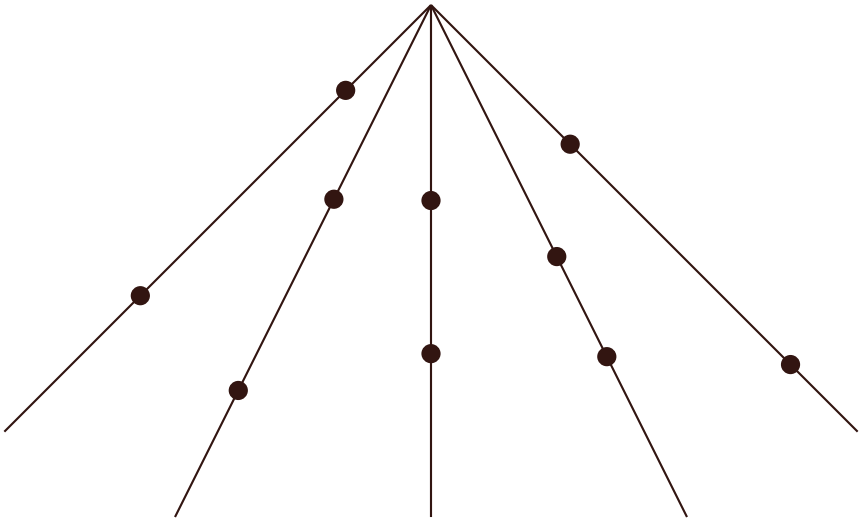
Corollary 4.
$U_{2,4}$ stabilizes 3-connected quaternary matroids.

Corollary 5.
$U_{2,5}$, $U_{3,5}$ stabilize 3-connected quinary matroids. $U_{2,4}$ stabilizes remaining 3-connected quinary matroids.

Counterexamples: swirls



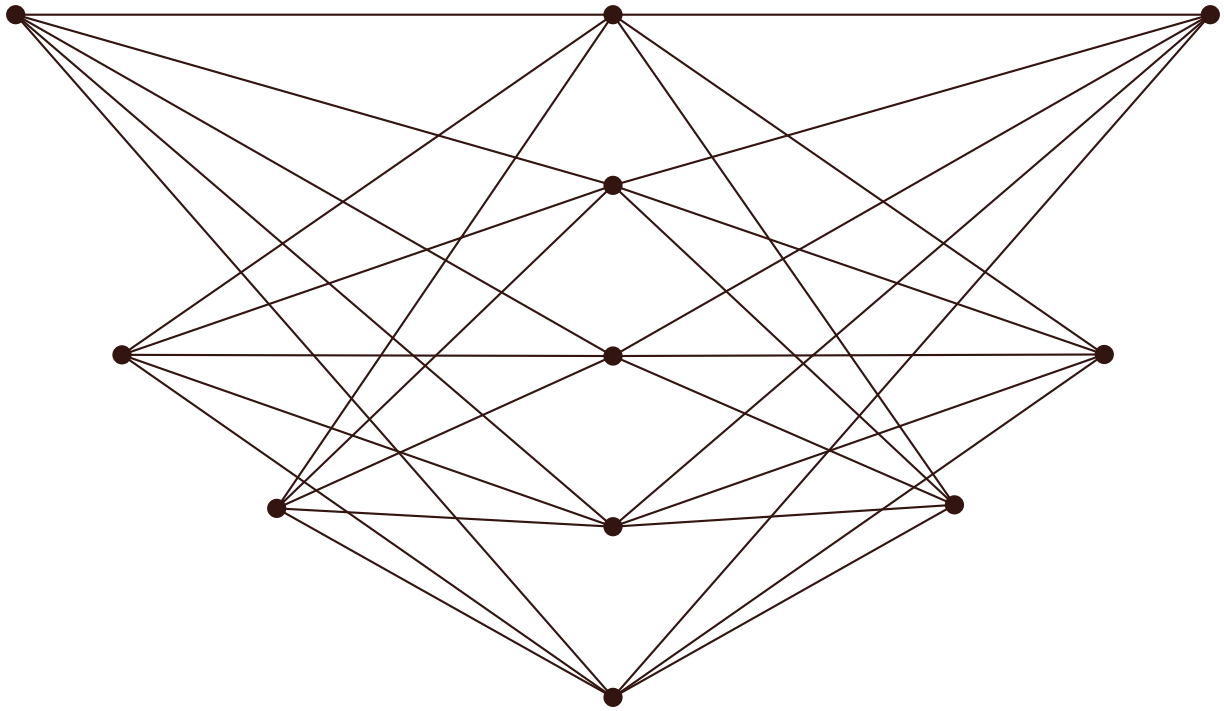
Counterexamples: spikes



New conjecture

Conjecture.
For each $\mathbb{F}$, there is c such that each 4-connected M has at most c inequivalent representations.

Counterexamples: maces



New conjecture

Conjecture.
For each $\mathbb{F}$, there are c, k such that each k-connected M has at most c inequivalent representations.

Part III
The prime field case

The result

Theorem (Geelen, Whittle 2011+).
For each GF(p) there is c such that each 4-connected M has at most c inequivalent representations.

Proof (idea).
Characterize "worst offenders," bound their size. Details: about 275 pages.

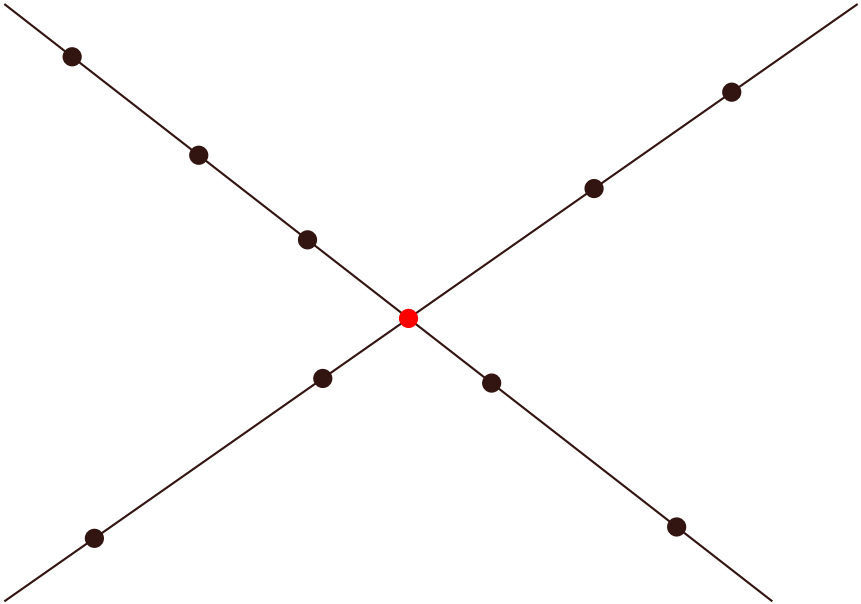
Freedom

Definition.
$\{e, f\}$ is *clonal pair* if exchanging them is isomorphism.

Definition.
e is *fixed* if no extension has independent clonal pair $\{e, f\}$.

Corollary.
If e fixed, then representation of $M \backslash e$ extends uniquely.

Freedom



k-coherence

Definition.
M is *k-coherent* if 3-connected and has no swirl-like flower with $\geq k$ petals.

Worst offenders

Definition.

A *k-skeleton* for GF(p) is 3-connected M with

- M is not wheel, whirl of rank ≥ 3
- If e fixed then $M \backslash e$ not k-coherent
- If e cofixed then M/e not k-coherent

Chain theorem for skeletons

Theorem (Geelen, Whittle 2011+).
Let M be nonempty k-skeleton. One of these situations applies:

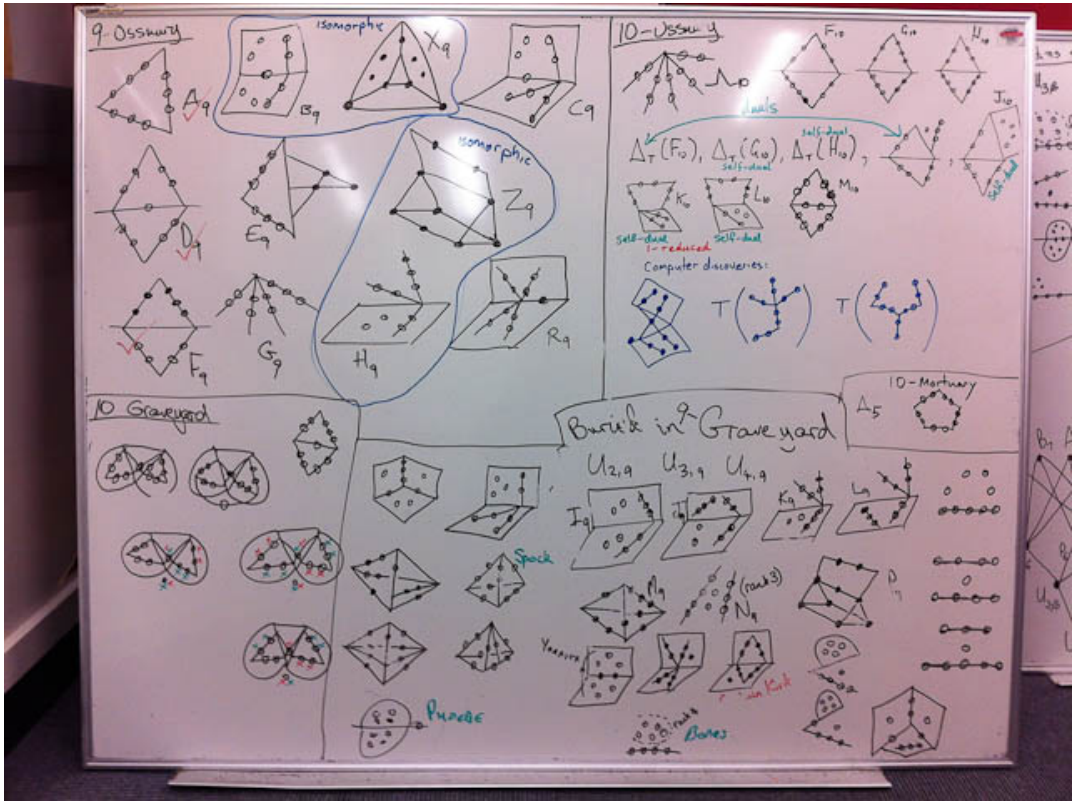
(i) $M \backslash e$ or M/e is k-skeleton for some e

(ii) $M/p \backslash q$ is k-skeleton for some clonal pair $\{p, q\}$

(iii) Special structure stuff that needs $\geq$ 20ish elements and 3- or 4-element reductions.

Work in progress (Hall, Mayhew, vZ).
Use this (and a computer) to get *explicit* bound on 5-coherent, GF(7).

How to do it by hand?



How to do it in Sage?

```
def is_clonal_pair(M,e,f):
    morphism = {}
    for x in M.groundset():
        morphism[x] = x
    morphism[e] = f
    morphism[f] = e
    return M.is_isomorphism(M, morphism)
```

Size	4	5	6	7	8	9	10	11	12	13
Skeletons	1	2	4	10	28	18	20	16*	28*	???

Part IV
Arbitrary fields

New conjecture

Conjecture.
For each finite $\mathbb{F}$, there are c, k such that each k-connected M has at most c inequivalent representations.

"Theorem" (Geelen, Gerards, Huynh, vZ).
True!

(Note: proof gives horrible bounds on c, k).

New connectivity

Definition.
M is (f, k)-connected if, for each l-separation (A, B), $l \leq k$,

$$\min\{|A|, |B|\} \leq f(l).$$

Lemma.
If M is (f, k)-connected, and f non-decreasing, then $M \backslash e$ or M/e is $(2f, k)$-connected.

Lemma.
If M is simple, (f, k)-connected, and critical, then $|E(M)| \leq 2^{r(M)}$.

Chain theorem

“Theorem” (Geelen, Gerards, Huynh, vZ).
Let f grow fast, M huge, (f,k)-connected. Then have (f,k)-connected M' with

$$|E(M)| - |E(M')| \leq 2.$$

Moreover, can protect a small set X.

Constraining freedom

'Theorem' (Geelen, vZ).
If $\mathcal{T}$ is tangle of M (representable over GF(q)), then the nonfixed elements are in a $\mathcal{T}$-small set of bounded order.

Observation.
(f, k)-connectivity gives natural tangle!

Slides at
http://www.math.princeton.edu/~svanzwam/

The End