Characteristic sets of matroids

Dustin Cartwright

University of Tennessee, Knoxville

December 17, 2021

Bases and circuits in vector spaces

- K: a field
- V: a finite-dimensional K-vector space

Some definitions:

- Vectors $v_1, \ldots, v_n \in V$ are dependent if there exist $c_1, \ldots, c_n \in K$ such that:

  $$c_1 v_1 + \ldots + c_n v_n = 0$$

  Otherwise, independent.
- A basis is a maximal independent set
- A circuit is a minimal set of dependent vectors $v_1, \ldots, v_n$.

Properties of bases and circuits

Basis exchange property: If B and B' are bases for V, and $v \in B \setminus B'$, then there exists $w \in B' \setminus B$ such that $B \cup \{w\} \setminus \{v\}$ is also a basis.

Corollary

All bases for V have the same number of elements.

Circuit axiom: If C and C' are circuits, and $v \in C \cap C'$, then there exists a circuit $C'' \subset C \cup C' \setminus \{v\}$.

Proposition

The basis exchange property and the circuit axiom are equivalent

Algebraic independence

- L/K: finitely generated field extension

Some parallel definitions:

- A set of elements $x_1, \ldots, x_n \in L$ is algebraically dependent if there exists a non-trivial polynomial relation:

$$\sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} = 0$$

  Otherwise, algebraically independent
- A (transcendence) basis is a maximal algebraically independent set.
- A circuit is a minimal algebraically dependent set.

Algebraic matroids

The circuits of a field extension form a matroid

Realizability

A matroid is a finite set of elements together with (equivalently) either of:

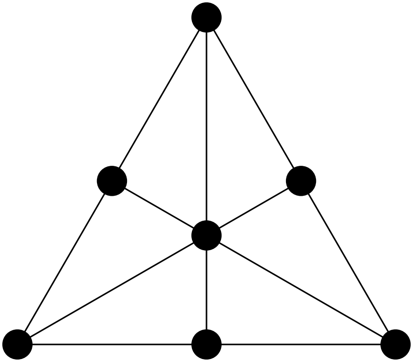
- A collection of bases satisfying the basis exchange axiom
- A collection of circuits satisfying the circuit axiom.

The matroid M is:

- linearly realizable over K if there exists a K-vector space V and a function from the elements of M to V with the same bases.
- algebraically realizable over K if there exists an extension L/K and a function from elements of M to L with the same (transcendence) bases.

Non-Fano matroid

Any 3 vertices not on a line are a basis.



Linearly realizable over a field K if and only if K has characteristic not 2.

Algebraically realizable over any field:

$$x, y, z, xyz, xy, xz, yz \in K(x, y, z)$$

Linear characteristic sets

The linear characteristic set of a matroid M is the set of characteristics of fields over which it is linearly realizable.

Theorem (Rado, Vamós, Kahn, Reid)

The linear characteristic set is either:

- *a finite set not containing* 0*, or*
- *a cofinite set (complement of a finite set) containing* 0*.*

Any set of either of these types is possible.

Algebraic characteristic sets

The algebraic characteristic set of a matroid M is the set of characteristics of fields for which it is algebraically realizable.

- $\chi_L(M) \subset \chi_A(M)$.
- If $0 \in \chi_A(M)$, then $0 \in \chi_L(M)$, so $\chi_L(M) \subset \chi_A(M)$ are cofinite.
- $\chi_A(M)$ can be empty (Vámos)
- $\chi_A(M)$ can be the set of all (positive) primes (Lindström)
- $\chi_A(M)$ can be neither finite nor cofinite (Evans-Hrushovski)

Main theorem

Theorem (C.-Varghese)

Let $C_L \subset C_A$ be either finite or cofinite subsets of the set of primes and 0. Suppose that either $0 \in C_L, C_A$ and C_L is cofinite, or $0 \notin C_L, C_A$ and C_L is finite.
Then there exists a matroid M such that $\chi_L(M) = C_L$ and $\chi_A(M) = C_A$.

Dually: algebraic matroid of a variety

Given $x_1, \ldots, x_n \in L/K$, we can define a prime ideal $J = \ker(K[x_1, \ldots, x_n] \to L)$ which defines an irreducible variety $X \subset \mathbb{A}^n_K$. The independent sets of X are the subsets I such that the projection $\pi_B(V(J))$ is dense in $\mathbb{A}^I_K$.

One-dimensional group construction

- K: algebraically closed field
- G: a 1-dimensional, connected algebraic group over K
- $\mathbb{E}$: the ring of endomorphisms of G. If $a, b \in \mathbb{E}$, $g \in G$

$$a \cdot b = a \circ b \qquad (a+b)(g) = a(g) + b(g)$$

- $N \in \mathbb{E}^{n \times d}$ matrix

Then N defines a group homomorphism $G^d \to G^n$:

$$(g_1, \ldots, g_d) \mapsto \big(N_{11}(g_1) + \cdots + N_{1d}(g_d), \ldots, N_{n1}(g_1) + \cdots + N_{nd}(g_d)\big)$$

Then the algebraic matroid of $N(G^d) \subset G^n$ is the same as the linear matroid of the rows of N, over the division ring generated by $\mathbb{E}$.

1-dimensional connected algebraic groups

Classification of 1-dimensional connected algebraic groups over an algebraically closed K:

- $\mathbb{G}_a = (K, +)$. Endomorphisms: K in characteristic 0, $K[F]$ in characteristic p.
- $\mathbb{G}_m = (K \setminus \{0\}, \cdot)$. Endomorphisms: $\mathbb{Z}$.
- E, an elliptic curve. Endomorphisms: $\mathbb{Z}$ or maximal order in imaginary quadratic number field, or (in positive characteristic) order in quaternion algebra.

Endomorphisms of $\mathbb{G}_a$

The endomorphisms of $\mathbb{G}_a$ are isomorphic to twisted polynomial ring

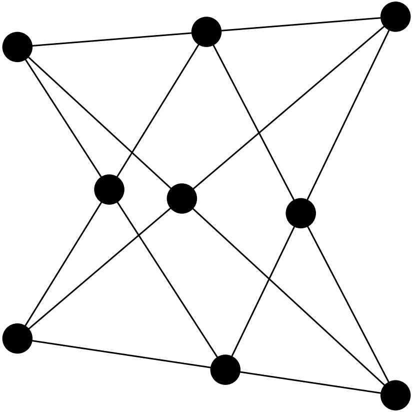
$$K[F] = \{a_n F^n + \cdots + a_0 : a_n, \ldots, a_0 \in K\}$$

with the commutation relation:

$$F\alpha = \alpha^p F \quad \text{for } \alpha \in K$$

Non-Pappus matroid

The non-Pappus matroid is linear over any non-commutative division ring, but not over any field.

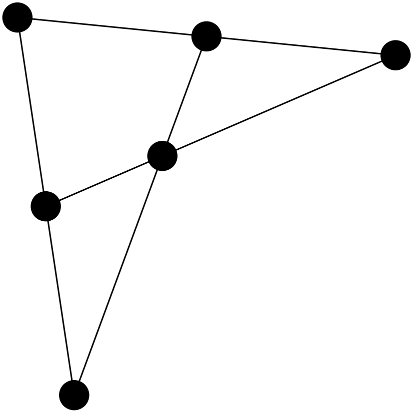


Therefore, $\chi_L(M) = \emptyset$, and by the 1-dimensional group construction, $\chi_A(M)$ is the set of all primes.

Evans-Hrushovski

Theorem (Evans-Hrushovski)

Any algebraic realization of the matroid below is equivalent to a realization by the 1-dimensional group construction.



Evans-Hrushovski

Theorem (Evans-Hrushovski)

Given a suitable system of equations Φ, there exists a matroid M such that:

- *M has a linear realization over K if and only if Φ has solutions over K.*
- *M has an algebraic realization over K if and only if there exists a 1-dimensional connected algebraic group G with endomorphism ring $\mathbb{E}$ such that Φ has solutions in the division ring generated by $\mathbb{E}$*

Other algebraic characteristic sets?

Up to finite difference:

- $\emptyset$
- all primes
- For $f \in \mathbb{Z}[x]$, the set of primes p such that f does not factor into linear terms in $\mathbb{F}_p[x]$.

Q: Other possiblities?