A quantitative version of Mnëv's theorem[1]

Dustin Cartwright

University of Tennessee

March 5, 2016

[1] see "Lifting matroid divisors on tropical curves," Res. Math. Sci. (2015)

Mnëv universality

Combinatorial realization spaces can be arbitrarily complicated.
Such as, realization spaces of:

- Polytopes
- Matroids
- Algebraic geometry moduli spaces (Murphy's law, for smooth surfaces, curves with linear systems)

Matroids

Given vectors $v_1, \ldots, v_n$ spanning a d-dimensional vector space V, the matroid of this vector configuration gives either of the following, equivalent combinatorial data:

- Which subsets of $v_1, \ldots, v_n$ are a basis for V?
- Which subsets of $v_1, \ldots, v_n$ are linearly independent?
- For each subset of $v_1, \ldots, v_n$, what is the dimension of their span?

Matroid realization spaces

The realization space C_M of a rank d matroid M parametrizes the vector configurations in V.

$$
\begin{array}{c}
\mathbb{A}^{d\times n} = \{d \times n \text{ matrices}\} \\
\cup \\
C_M = GL_d \mathbin{\backslash\!\backslash} U_M \mathbin{/\!/} (K^\times)^n,
\end{array}
$$

where U_M is the set of matrices whose columns encode a vector configuration having a fixed matroid M.

Mnëv's theorem

Theorem (Mnëv, Sturmfels, Richter-Gebert, Lafforgue, ...)

For any $p_1, \ldots, p_l \in \mathbb{Z}[x_1, \ldots, x_s]$ are polynomials, there exists a rank 3 matroid M whose realization space C_M (over $\mathbb{Z}$), which is defined by $p_1, \ldots, p_l$, but with more free parameters.
More precisely, C_M fits in the diagram:

$$\begin{array}{ccc} C_M & \xrightarrow{\text{open imm.}} & X \times \mathbb{A}^N \\ \text{surj.}\downarrow & & \downarrow \\ X & = & X := \operatorname{Spec} \mathbb{Z}[x_1, \ldots, x_s]/\langle p_1, \ldots, p_l \rangle \end{array}$$

Quantitative Mnëv's theorem

Theorem (C)

The matroid M in Mnëv's theorem can be chosen with

$$3f + 7a + 7o + 6m + 6e + 3$$

vectors where

- *f is the number of variables,*
- *a is the number of additions of two variables,*
- *o is the number of additions of a variable and 1,*
- *m is the number of multiplications, and*
- *e is the number of equalities and inequalities*

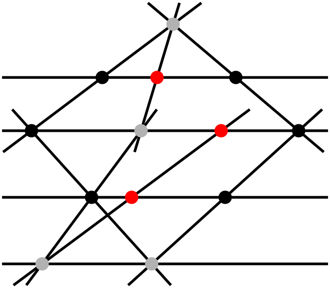
in an elementary monic representation of the ideal $\langle p_1, \ldots, p_l \rangle$.

Cross-ratios: variables from vector configuration

- 4 distinct points on a projective line, up to linear transformation, have a unique invariant: their cross-ratio.
- In coordinates where the first 3 points are at 0, 1, and ∞, the cross-ratio is the coordinate of the 4th point.

Representing basic operations: addition

Two variables and their sum represented by cross-ratios on parallel lines:



In order for these points to be distinct, need y, y', and $y + y'$ all $\neq 0, 1$.

Elementary monic representation

We have polynomials $p_1, \ldots, p_l \in \mathbb{Z}[x_1, \ldots, x_s]$. We change coordinates:

$$\begin{aligned} y_0 &= t \\ y_1 &= t + x_1 \\ &\vdots \\ y_s &= t + x_s \end{aligned}$$

For $i > n$, each y_i is defined in terms of previous variables by:

- Addition of two variables: $y_i = y_j + y_k$ where y_j and y_k have different degrees as polynomials of t.
- Addition of one: $y_i = y_j + 1$.
- Multiplication of two variables: $y_i = y_j y_k$.

Each y_i will be monic polynomial as a polynomial of t. Therefore, t can be chosen so that $y_i \neq 0, 1$.

Example

We can't construct $x_1 + x_2$ or $t + x_1 + x_2$, but we can construct $t^2 + 2t + x_1 + x_2$ (positive powers of t will go away in the end):

$$\begin{aligned} y_0 &= t \\ y_1 &= t + x_1 \\ y_2 &= t + x_2 \\ y_3 &= y_0 y_0 = t^2 \\ y_4 &= y_1 + y_3 = t^2 + t + x_1 \\ y_5 &= y_2 + y_4 = t^2 + 2t + x_1 + x_2 \end{aligned}$$

Equalities and inequalities

The elementary monic representation also comes with equalities $y_i = y_j$ for $(i, j) \in E$ and inequalities $y_i \neq y_j$ for $(i, j) \in I$ such that:

- For each equality or inequality, $f_{ij} = y_i - y_j$ is in $\mathbb{Z}[x_1, \ldots, x_s]$.

We then say that this elementary monic representation represents $\mathbb{Z}[x_1, \ldots, x_l][f_{ij}^{-1}]_{ij \in I} / \langle f_{ij} \rangle_{ij \in E}$.

Proposition (C)

Every scheme of finite type over $\mathbb{Z}$ can be has an elementary monic representation.

Example continued

We want to represent $x_1 + x_2 \neq 0$.

$$\begin{aligned} y_0 &= t \\ &\vdots \\ y_5 &= y_2 + y_4 = t^2 + 2t + x_1 + x_2 \\ y_6 &= y_0 + 1 = t + 1 \\ y_7 &= y_6 + 1 = t + 2 \\ y_8 &= y_6 y_0 = t^2 + 2t \end{aligned}$$

The equality $y_5 \neq y_8$ represents $x_1 + x_2 \neq 0$.

Application: $\mathbb{Z}[p^{-1}]$ and $\mathbb{Z}/p$

Proposition (C.)

For the affine schemes $\mathbb{Z}[p^{-1}]$ and $\mathbb{Z}/p$ with p a prime, the matroid M in Mnëv's theorem has $O(\sqrt{p})$ elements.
In particular, if $p \geq 443$, then M has fewer than p elements.