A quantitative version of Mnëv's theorem

Dustin Cartwright

University of Tennessee, Knoxville

April 11, 2015

Mnëv's principle

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)

Polytope realizations

Can these points of a polytope be chosen to have rational coordinates (up to combinatorial equivalence)? For $n = 3$, yes (Steinitz).

Theorem (Perles)

There exists a polytope in $\mathbb{R}^8$ where the coordinates can be chosen to be in $\mathbb{Q}[\sqrt{5}]$, but not in $\mathbb{Q}$.

Theorem (Mnëv)

For any finite extension K of $\mathbb{Q}$, there exists a polytope in $\mathbb{R}^4$ where the coordinates can be chosen to be in K, but not in any smaller field.

Idea: Give combinatorial encoding for minimal polynomial of the field extension K in the structure of the polytope.

Matroids

Given vectors $v_1, \ldots, v_n$ spanning a d-dimensional vector space V, the matroid of this vector configuration answers any of the following equivalent questions:

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

Matroid realizations

The realization scheme C_M of a matroid M parametrizes the vector configurations in V (up to scaling the vectors and changing coordinates on V) having the matroid M, i.e. the same answers to the basis and dimension-of-span questions.

Equivalently:

- Take the Grasmannian $\mathrm{Gr}(d, n)$ in its Plücker embedding.
- Intersect with a torus orbit from the ambient projective space, i.e.

$$\mathrm{Gr}(d, n) \cap \bigcap_{I \in B} \{p_I \neq 0\} \cap \bigcap_{I \notin B} \{p_I = 0\}$$

- Take the quotient by $(K^*)^n$.

Mnëv's theorem

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

If $p_1, \ldots, p_m$ are integral polynomials, then then there exists a rank 3 matroid M with realization space C_M such that:

$$\begin{tikzcd} C_M \arrow[r, "\textit{open imm.}"] \arrow[d, "\textit{surj.}"'] & X \times \mathbb{A}^N \arrow[d] \\ X \arrow[r, equal] & X := \operatorname{Spec} \mathbb{Z}[x_1, \ldots, x_n]/\langle p_1, \ldots, p_m \rangle \end{tikzcd}$$

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 affine scheme X from before.

Elementary monic representation

The $x_1, \ldots, x_n$ are the variables for $p_1, \ldots, p_m$. We start with the change of coordinates:

$$\begin{aligned} y_0 &= t \\ y_1 &= t + x_1 \\ &\vdots \\ y_n &= t + x_n \end{aligned}$$

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.

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 $\mathbb{Z}[x_1, \ldots, x_n]$.

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

Proposition (C)

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

Example continued

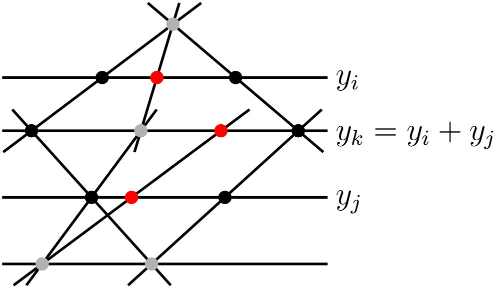
We want to represent $x_1 + x_2 \neq 0$.

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

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

Elementary monic representation to matroid

- Variables y_i become cross-ratios on parallel lines (not 0 or 1)
- Addition, multiplication, equality, inequality, such as the following figure for addition:



For any $x_1, \ldots, x_n$, we can always choose t so that $y_i \neq 0, 1$ and we avoid certain other coincidences.

Second example

Let p be a prime number and we want to represent the equation $p = 0$:

$$\begin{aligned} y_0 &= t \\ y_1 &= y_0 + 1 = t + 1 \\ &\vdots \\ y_p &= y_{p-1} + 1 = t + p \end{aligned}$$

With the equality $y_0 = y_p$.

Second example: more efficiently

Write $p = m^2 + \ell$ (we can take $\ell \leq 2m$).

$$\begin{aligned}
y_0 &= t \\
y_1 &= y_0 + 1 = t + 1 \\
&\vdots \\
y_m &= y_{m-1} + 1 = t + m \\
y_{m+1} &= y_m y_m = t^2 + 2mt + m^2 \\
y_{m+2} &= y_{m+1} + 1 = t^2 + 2mt + m^2 + 1 \\
&\vdots \\
y_{m+\ell+1} &= y_{m+\ell} + 1 = t^2 + 2mt + p
\end{aligned}$$

We've now constructed p modulo t, but in order to get a legal equality, we need to construct $t^2 + 2mt$.

Second example: more efficiently

So far:

$$
\begin{aligned}
&\vdots \\
y_m &= t + m \\
&\vdots \\
y_{m+\ell+1} &= t^2 + 2mt + p \\
y_{m+\ell+2} &= y_m + 1 = t + m + 1 \\
&\vdots \\
y_{m+\ell+m+1} &= y_{m+\ell+m} + 1 = t + 2m \\
y_{m+\ell+m+2} &= y_0 y_{m+\ell+m+1} = t^2 + 2mt
\end{aligned}
$$

and then $y_{m+\ell+1} = y_{m+\ell+m+2}$ is a legal equality defining $p = 0$.
More complicated than before, but we've only used $O(\sqrt{p})$ steps.

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.

Corollary

Lifting a rank 2 divisor of degree d on a tropical curve can depend on the characteristic p, even when $p > d$.

In contrast, lifting a rank 1 divisor can depend on the characteristic p, but only when $p \leq d$.