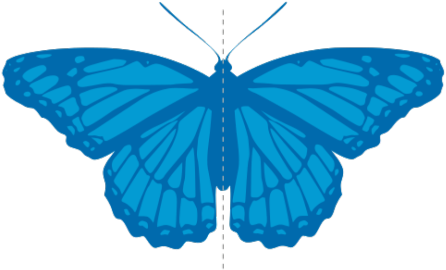
Polynomial invariants of finite groups of sparse matrices

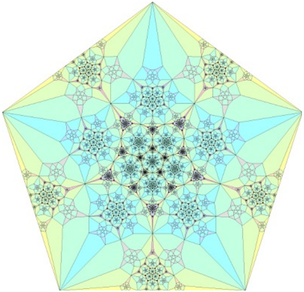
Jia Huang

Department of Mathematics and Statistics
University of Nebraska at Kearney
E-mail address: huangj2@unk.edu

June 15, 2018

Symmetry





Symmetric polynomials

- Let $\mathbb{F}$ be a field (e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_q$, etc).
- $\mathbb{F}[X] := \mathbb{F}[x_1, \ldots, x_n]$ consists of all polynomials in n variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{F}$.
- The *symmetric polynomials* are those invariant under all permutations of the n variables.

Example ($n = 3$)

- The polynomial $x_1^2 + x_2^2 + x_3^2$ is symmetric.
- The polynomial $2x_1x_2 - x_2x_3$ is *not* symmetric, because

$$\text{for } w = 231: \; w(2x_1x_2 - x_2x_3) = 2x_2x_3 - x_3x_1.$$

Fundamental Theorem of Symmetric Polynomials

Fundamental Theorem of Symmetric Polynomials

Any symmetric polynomial in n variables can be written in a unique way as a polynomial in the elementary symmetric polynomials $e_1, \dots, e_n$.

Example ($n = 3$)

$$f(t) = (t + x_1)(t + x_2)(t + x_3)$$

( Vieta's formula)

$$= t^3 + (\underbrace{x_1 + x_2 + x_3}_{e_1})t^2 + (\underbrace{x_1x_2 + x_1x_3 + x_2x_3}_{e_2})t + \underbrace{x_1x_2x_3}_{e_3}.$$

$$x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2.$$

Matrix action on polynomials

- $\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 2 \\ 2 & -1 & 0 \end{pmatrix}$: $x_1 \mapsto x_1 - x_2 + 2x_3$.
- $\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 2 \\ 2 & -1 & 0 \end{pmatrix}$: $x_2 \mapsto x_2 - x_3$.
- $\begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 2 \\ 2 & -1 & 0 \end{pmatrix}$: $x_3 \mapsto x_1 + 2x_2$.
- Permutation matrices: e.g. $231 \leftrightarrow \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Invariants under a matrix group

- Let G be a finite group of some n by n matrices over $\mathbb{F}$.
- The invariant ring $\mathbb{F}[X]^G$ consists of all the polynomials in $\mathbb{F}[X]$ invariant under the matrix group G.
- The symmetric group $S_n = \{n \times n \text{ permutation matrices}\}$.

Fundamental Theorem of Symmetric Polynomials (restated)

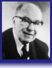
$\mathbb{F}[X]^{S_n} = \mathbb{F}[e_1, \ldots, e_n]$ *is a polynomial algebra in* $e_1, \ldots, e_n$.

Polynomial Algebra Problem

Find all finite matrix groups G such that $\mathbb{F}[X]^G$ is polynomial.

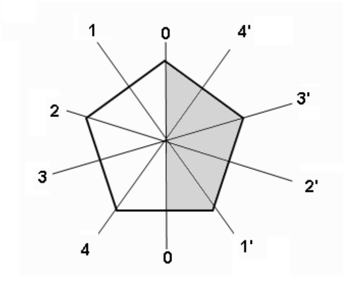
- $1/|G| \in \mathbb{F}$: *solved* *(nice case)*
- $1/|G| \notin \mathbb{F}$: *still open!* *(tricky case)*

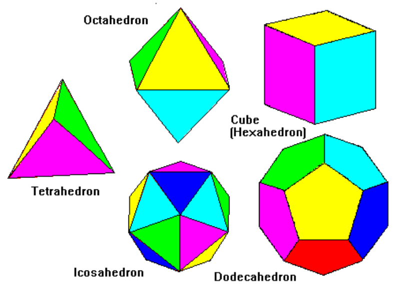
Nice case: reflection groups

Theorem (Chevalley , Shephard , and Todd  1955)

Suppose $1/|G| \in \mathbb{F}$. Then $\mathbb{F}[X]^G$ is polynomial if and only if G is generated by pseudo-reflections (elements fixing a hyperplane).

Example (Symmetry groups of regular polytopes)





Tricky case?

- The symmetric group $S_n = \{\text{all permutations}\}$ has order $n!$ and its invariant ring $\mathbb{F}[X]^{S_n}$ is polynomial over any field $\mathbb{F}$.
- Next, consider the general linear group $GL(n, \mathbb{F}) = \{\text{all } n \times n \text{ invertible matrices over } \mathbb{F}\}$.
- Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of q elements.
- $|GL(n, \mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.
- $|GL(n, \mathbb{F}_q)| = 0$ in $\mathbb{F}_q$.
- What are the polynomial invariants of $GL(n, \mathbb{F}_q)$?

Invariants of $GL(n, \mathbb{F}_q)$

Theorem (L. E. Dickson  1911)

Let $G = GL(n, \mathbb{F}_q)$. Then $\mathbb{F}_q[X]^G = \mathbb{F}_q[c_1, \ldots, c_n]$ is a polynomial algebra in Dickson's invariants $c_1, \ldots, c_n$.

Example ($n = 2$, $q = 2$)

$$
\begin{aligned}
f(t) &= (t + 0x_1 + 0x_2)(t + x_1 + 0x_2)(t + 0x_1 + x_2)(t + x_1 + x_2) \\
&= t^4 + (\underbrace{x_1^2 + x_2^2 + x_1x_2}_{c_1})t^2 + (\underbrace{x_1^2x_2 + x_1x_2^2}_{c_2})t.
\end{aligned}
$$

Fundamental Theorem of Symmetric Polynomials

Fundamental Theorem of Symmetric Polynomials

Any symmetric polynomial in n variables can be written in a unique way as a polynomial in the elementary symmetric polynomials $e_1, \ldots, e_n$.

Example ($n = 3$)

$$f(t) = (t + x_1)(t + x_2)(t + x_3)$$

( Vieta's formula)

$$= t^3 + (\underbrace{x_1 + x_2 + x_3}_{e_1})t^2 + (\underbrace{x_1x_2 + x_1x_3 + x_2x_3}_{e_2})t + \underbrace{x_1x_2x_3}_{e_3}.$$

$$x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2.$$

Subgroups of $GL(n, \mathbb{F}_q)$ whose invariant ring is polynomial

$$\begin{pmatrix} 1 & * & * & * & * \\ & 1 & * & * & * \\ & & 1 & * & * \\ & & & 1 & * \\ & & & & 1 \end{pmatrix}$$

(Bertin 1965)

$$\begin{pmatrix} * & * & * & * & * & * \\ * & * & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & & & & * \end{pmatrix}$$

(Mui 1975, Hewett 1996)

$$\begin{pmatrix} * & * & & & & \\ * & * & & & & \\ * & * & * & * & * & \\ & & & * & * & \\ & & & & * & \\ & & & & * & * \end{pmatrix}$$

(Potechin 2008)

$$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ * & * & * & * & * \\ * & * & * & * & * \end{pmatrix}$$

(Steinberg 1987)

$$\begin{pmatrix} 1 & & & & \\ & & \ddots & & \\ & & & 1 & \\ * & * & 0 & 0 & 1 \end{pmatrix}$$

(Smith 1995)

A common generalization

- A *sparsity pattern* σ assigns a set $\sigma(i,j) \subseteq \mathbb{F}$ to each pair (i,j) with $1 \leq i,j \leq n$.
- $GL_\sigma(n,\mathbb{F}) = \{[a_{ij}] \in GL(n,\mathbb{F}) : a_{ij} \in \sigma(i,j)\}$.
- This includes all previous examples, and gives new examples:

$$\begin{pmatrix} \mathbb{F}_{3^3} & \mathbb{F}_{3^6} \\ 0 & \mathbb{F}_{3^2} \end{pmatrix} \subset GL(2,\mathbb{F}_{3^6}).$$

Example

If $G = \begin{pmatrix} \mathbb{F}_{3^3} & \mathbb{F}_{3^6} \\ 0 & \mathbb{F}_{3^2} \end{pmatrix}$ then $\mathbb{F}_{3^6}[x_1, x_2]^G$ is a polynomial algebra in

$$x_1^{3^3-1} \quad \text{and} \quad (x_2^{3^6} - x_1^{3^6-1}x_2)^{3^2-1}.$$

Theorem 1 (H.)

If $G = GL_\sigma(n, \mathbb{F})$ is a finite group, then $\mathbb{F}[X]^G$ is polynomial.

Proof.

Use matrix operations and some commutative algebra. □

Polynomial gluing construction

If a matrix group G can be written as

$$G = \begin{pmatrix} G_X & \Phi \\ 0 & G_Y \end{pmatrix} \subset GL(m+n, \mathbb{F})$$

where

- G_X is a subgroup of $GL(m, \mathbb{F})$,
- G_Y is a subgroup of $GL(n, \mathbb{F})$,
- Φ is a subspace of $\mathbb{F}^{m \times n}$,
- with some extra technical conditions,

then we say that G is a *polynomial gluing* of G_X and G_Y.

Invariants after gluing

Theorem 2 (H.)

Let G be a polynomial gluing of G_X and G_Y. If both $\mathbb{F}[X]^{G_X}$ and $\mathbb{F}[Y]^{G_Y}$ are polynomial, and so is $\mathbb{F}[X,Y]^G$.

Example ($\Rightarrow$ Theorem 1)

A finite group $GL_\sigma(n,\mathbb{F})$ of sparse matrices is essentially a polynomial gluing of various finite general linear groups $GL(m,\mathbb{F}_q)$.

More examples of polynomial gluing

Example

Nakajima (1983) found all *p-groups* G in $GL(n, \mathbb{F}_p)$ with a polynomial invariant ring $\mathbb{F}_p[X]^G$, which turn out to be polynomial gluings of copies of the trivial group $\{1_{\mathbb{F}}\}$.

Example

The symmetric group S_n has a polynomial invariant ring $\mathbb{F}[X]^{S_n} = \mathbb{F}[e_1, \ldots, e_n]$, but cannot be obtained from polynomial gluing if $n \geq 3$ and $1/n \notin \mathbb{F}$.

Some combinatorics

Proposition

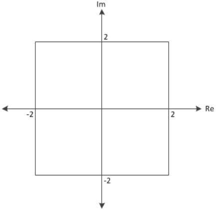
Suppose that $\mathbb{F}[X]^G$ is a polynomial algebra in $f_1, \ldots, f_n$. Then

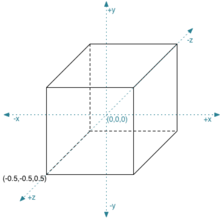
- *one can choose $f_1, \ldots, f_n$ to be homogeneous,*
- *their degrees $d_1, \ldots, d_n$ are uniquely determined,*
- $|G| = d_1 \cdots d_n$ *(e.g. $n! = 1 \cdot 2 \cdots n$), and*
- *The Hilbert series of the invariant ring $\mathbb{F}[X]^G$ is*

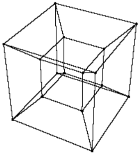
$$\sum_{d \geq 0} \dim_{\mathbb{F}} (\mathbb{F}[X]^G)_d \cdot t^d = \frac{1}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}.$$

Signed permutations

- $S_n^{\pm} = \{\text{signed permutations}\}$; $|S_n^{\pm}| = n! \cdot 2^n$.
- Example: $S_2^{\pm} = \{12, 21, \bar{1}2, \bar{2}1, 1\bar{2}, 2\bar{1}, \bar{1}\bar{2}, \bar{2}\bar{1}\}$.
- $S_n^{\pm}$ is the symmetry group of a hypercube.







- The invariant ring of $S_n^{\pm}$ is a polynomial algebra in $\{e_i(x_1^2, \ldots, x_n^2) : 1 \le i \le n\}$.

Fundamental Theorem of Symmetric Polynomials

Any symmetric polynomial in n variables can be written in a unique way as a polynomial in the elementary symmetric polynomials $e_1, \ldots, e_n$.

Example ($n = 3$)

$$f(t) = (t+x_1)(t+x_2)(t+x_3)$$

( Vieta's formula)

$$= t^3 + (\underbrace{x_1+x_2+x_3}_{e_1})t^2 + (\underbrace{x_1x_2+x_1x_3+x_2x_3}_{e_2})t + \underbrace{x_1x_2x_3}_{e_3}.$$

$$x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2.$$

Invariants of $GL(n, \mathbb{F}_q)$

Theorem (L. E. Dickson  **1911)**

Let $G = GL(n, \mathbb{F}_q)$*. Then* $\mathbb{F}_q[X]^G = \mathbb{F}_q[c_1, \ldots, c_n]$ *is a polynomial algebra in Dickson's invariants* $c_1, \ldots, c_n$*.*

Example ($n = 2$, $q = 2$)

$$
\begin{aligned}
f(t) &= (t + 0x_1 + 0x_2)(t + x_1 + 0x_2)(t + 0x_1 + x_2)(t + x_1 + x_2) \\
&= t^4 + (\underbrace{x_1^2 + x_2^2 + x_1 x_2}_{c_1})t^2 + (\underbrace{x_1^2 x_2 + x_1 x_2^2}_{c_2})t.
\end{aligned}
$$

Generalization?

- $S_n \to GL(n, \mathbb{F}_q)$; $S_n^{\pm} \to O(n, \mathbb{F}_q),\ Sp(n, \mathbb{F}_q)$.
- The invariants of finite orthogonal/symplectic groups form a *complete intersection* (weaker than a polynomial algebra).
- I can define sparsity subgroups of $O(n, \mathbb{F}_q)$ and $Sp(n, \mathbb{F}_q)$.
- What about their invariants?

Thank you!