Lecture 11: Introduction to Invariant Theory

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 22, 2021

Overview

- Group Actions on Vector Spaces
- Ring of Invariant Polynomials
- Fundamental Theorems
- Conclusion
- Acknowledgements

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates

$$\sigma \circ (v_1, \dots, v_n) \longrightarrow (v_{\sigma^{-1}(1)}, \dots, v_{\sigma^{-1}(n)})$$

$$(\pi\sigma) \circ (v_1, \dots, v_n) = \pi \circ (\sigma \circ v) = \pi \circ (v_{\sigma^{-1}(1)}, \dots, v_{\sigma^{-1}(n)}) = (v_{\sigma^{-1}\pi^{-1}(1)}, \dots, v_{\sigma^{-1}\pi^{-1}(n)})$$

$$= (v_{\sigma^{-1}\pi^{-1}(1)}, \dots, v_{\sigma^{-1}\pi^{-1}(n)})$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates

$A_n \leftarrow$ set of even permutations

$\{\sigma \mid (-1)^{\sigma} = 1\}$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n$, $V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n$, $V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^{d+1}$ — linear transformations of curves

$$SL(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \,\middle|\, \alpha\delta - \beta\gamma = 1 \right\}$$

$$P(x,y) = a_d x^d + a_{d-1} x^{d-1} y + \cdots + a_0 y^d$$

$$\longleftrightarrow (a_d, a_{d-1}, \ldots, a_0)$$

$$P(x) \xmapsto{g} P(\alpha x + \beta y, \gamma x + \delta y)$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}$$

---

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication

$(gh) \circ A = g \circ (h \circ A)$

$ghA \qquad ghA$

$g \circ A \longmapsto \underbrace{gA}_{\text{matrix multiplication}}$

group action

elementary row operations
(Gaussian elimination)

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation

$g \circ A \longmapsto gAg^{-1}$ changes of basis

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation
  6. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ — row/column scaling

$$\mathbb{ST}(n) = \left\{ \underbrace{\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}}_{A} \;\middle|\; \underbrace{\prod_{i=1}^{n} a_i = 1}_{\det(A)=1} \right\}$$

$$(R, C) \circ X \longmapsto R X C$$

$$X_{ij} \longmapsto \underbrace{R_{ii}}_{\text{scaling row } i} X_{ij} \underbrace{C_{jj}}_{\text{scaling col } j}$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation
  6. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ — row/column scaling
  7. $G = S_n,\ V = \mathbb{C}^{\binom{n}{2}}$ — graph isomorphism

geometry

linear algebra

linear alg

combinatorics

TCS

TCS

$\{i,j\}$ $\quad i \neq j$

$\sigma : [n] \to [n]$

$\sigma \circ \{i,j\} \longrightarrow \{\sigma(i), \sigma(j)\}$

$v_H \in V \qquad v_H\{i,j\} = \begin{cases} 1 & \text{if } \{i,j\} \in E_H \\ 0 & \text{otherwise} \end{cases}$

$\sigma \circ v_H \mapsto v_{\sigma \circ H}$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials.

$$e_1(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$$

$$\| $$

$$x_{\sigma(1)} + \cdots + x_{\sigma(n)}$$

invariant

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials.

2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials (and more)

$$\det V(x_1, \dots, x_n) = \det \begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ \vdots & \vdots & & \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

$$= \prod_{i<j} (x_i - x_j)$$

not invariant under action of (1)

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials.

2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials (and more)

3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ linear transformations of curves

   Discriminants (and more)

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates

   Symmetric polynomials.

2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates

   Symmetric polynomials (and more)

3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ — linear transformations of curves

   Discriminants (and more)

4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication

   Determinant

$$\det(gA) = \underbrace{\cancel{\det(g)}}_{1} \cdot \det(A) = \det(A)$$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates
   Symmetric polynomials.
2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates
   Symmetric polynomials (and more)
3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ linear transformations of curves
   Discriminants (and more)
4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ left multiplication
   Determinant
5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ conjugation
   Trace polynomials.

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates
   Symmetric polynomials.
2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates
   Symmetric polynomials (and more)
3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^d$ linear transformations of curves
   Discriminants (and more)
4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ left multiplication
   Determinant
5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ conjugation
   Trace polynomials.
6. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ row/column scaling
   Matching/Permutation monomials.

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \mathrm{Mat}(n)$ left multiplication

Determinant

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \text{Mat}(n)$ left multiplication

   Determinant

2. $G = \mathbb{GL}(n)$, $V = \text{Mat}(n)$ conjugation

   Trace polynomials.

$$tr(x^k)$$

$$tr((g \circ x)^k) = tr((gxg^{-1})^k) =$$

$$= tr(gx^kg^{-1}) = tr(x^k)$$

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \mathrm{Mat}(n)$ left multiplication

   Determinant

2. $G = \mathbb{GL}(n)$, $V = \mathrm{Mat}(n)$ conjugation

   Trace polynomials.

3. $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

   Matching/Permutation monomials.

$X \;,\; \sigma \in S_n$

$\prod X_{i\sigma(i)}$ invariant

$RXC \qquad \prod_{i=1}^{n} R_{ii} X_{i\sigma(i)} C_{\sigma(i)\sigma(i)} =$

$= \cancel{\left(\prod_{i=1}^{n} R_{ii}\right)}' \prod X_{i\sigma(i)} \cdot \cancel{\left(\prod_{i=1}^{n} C_{\sigma(i)\sigma(i)}\right)}' = \prod X_{i\sigma(i)}$

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \mathrm{Mat}(n)$ left multiplication

   Determinant

2. $G = \mathbb{GL}(n)$, $V = \mathrm{Mat}(n)$ conjugation

   Trace polynomials.

3. $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

   Matching/Permutation monomials.

4. $G = S_n$, $V = \mathbb{C}^{\binom{n}{2}}$ graph isomorphism

   Open.

In particular small algebraic circuits computing "basis" of invariants for 4
$\Rightarrow$ randomized algorithm for graph isomorphism!

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$

p, q invariant

$p + q$ and $p \cdot q$ invariant

constant invariant

$$\mathbb{C}[x]^G := \{ p \mid p \text{ invariant} \}$$

$1, 0$

$$\mathbb{C}[x]^G = \mathbb{C}[\overbrace{p_1, \ldots, p_m}^{\text{generators of invariant ring as } \mathbb{C}\text{-algebra}}]$$

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

$$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, e_2, \ldots, e_n]$$

where

$$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

$$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, e_2, \ldots, e_n]$$

  where

$$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

- Every symmetric polynomial is itself a polynomial function of the *elementary symmetric polynomials*

$q(x) = Q(e_1, \ldots, e_n)$

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

  $$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[\underline{e_1, e_2, \ldots, e_n}]$$

  where

  $$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

- Every symmetric polynomial is itself a polynomial function of the *elementary symmetric polynomials*
- Elementary symmetric polynomials are a *fundamental system of invariants*

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*

$x^\alpha \succ x^\beta$ if $\|\alpha\|_1 > \|\beta\|_1$

or $\|\alpha\|_1 = \|\beta\|_1$ and for some $i \in [n]$

$\alpha_j = \beta_j$ $j < i$ and $\alpha_i > \beta_i$

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

$$\boxed{x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}}$$

with $a_1 \geq a_2 \geq \cdots \geq a_n$

$x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n} \longleftrightarrow x_1^{b_{\sigma(1)}} x_2^{b_{\sigma(2)}} \cdots x_n^{b_{\sigma(n)}}$

monomial in support p

also monomial in support p

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

$$LC(p)\cdot x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

  with $a_1 \geq a_2 \geq \cdots \geq a_n \geq 0$

- Then

$$q(x) = p(x) - LC(p) \cdot \underbrace{e_1^{\overbrace{a_1 - a_2}^{\geq 0}} \cdot e_2^{\overbrace{a_2 - a_3}^{\geq 0}} \cdots e_{n-1}^{\overbrace{a_{n-1} - a_n}^{\geq 0}} \cdot e_n^{\overbrace{a_n}^{\geq 0}}}$$

  has *smaller* leading monomial! division algorithm!

$$x_1^{a_1-a_2} (x_1 x_2)^{a_2-a_3} \cdots (x_1 \cdots x_n)^{a_n}$$

$$= x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

  with $a_1 \geq a_2 \geq \cdots \geq a_n$
- Then

$$p(x) - LC(p) \cdot e_1^{a_1 - a_2} \cdot e_2^{a_2 - a_3} \cdots e_{n-1}^{a_{n-1} - a_n} \cdot e_n^{a_n}$$

  has *smaller* leading monomial! division algorithm!
- Procedure must terminate because of well-ordering of monomial ordering!

when we terminate our polynomial in zero! $\Rightarrow P(x) \in \mathbb{C}[e_1, \ldots, e_n]$.

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants! If $\lambda = (\lambda_1, \ldots, \lambda_n)$ is a partition of d (where $\lambda_i \geq \lambda_{i+1}$) we have

$$s_\lambda = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \cdots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \cdots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \cdots & x_n^{\lambda_n} \end{pmatrix} \Big/ \overbrace{\prod_{i<j}(x_i - x_j)}^{\det(V(x_1,\ldots,x_n))}$$

$\lambda_1 + \lambda_2 + \cdots + \lambda_n = d$ $\qquad$ $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 0$

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants! If $\lambda = (\lambda_1, \ldots, \lambda_n)$ is a partition of d (where $\lambda_i \geq \lambda_{i+1}$) we have

$$s_\lambda = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \cdots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \cdots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \cdots & x_n^{\lambda_n} \end{pmatrix} / \prod_{i<j} (x_i - x_j)$$

- The complete symmetric polynomials are also a fundamental system of invariants!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants! If $\lambda = (\lambda_1, \ldots, \lambda_n)$ is a partition of d (where $\lambda_i \geq \lambda_{i+1}$) we have

$$s_\lambda = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \cdots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \cdots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \cdots & x_n^{\lambda_n} \end{pmatrix} / \prod_{i<j}(x_i - x_j)$$

- The complete symmetric polynomials are also a fundamental system of invariants!
- Relations between these bases is very important in algebraic combinatoric and representation theory!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants! If $\lambda = (\lambda_1, \ldots, \lambda_n)$ is a partition of d (where $\lambda_i \geq \lambda_{i+1}$) we have

$$s_\lambda = \det \begin{pmatrix} x_1^{\lambda_1+n-1} & x_2^{\lambda_1+n-1} & \cdots & x_n^{\lambda_1+n-1} \\ x_1^{\lambda_2+n-2} & x_2^{\lambda_2+n-2} & \cdots & x_n^{\lambda_2+n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{\lambda_n} & x_2^{\lambda_n} & \cdots & x_n^{\lambda_n} \end{pmatrix} / \prod_{i<j}(x_i - x_j)$$

- The complete symmetric polynomials are also a fundamental system of invariants!
- Relations between these bases is very important in algebraic combinatoric and representation theory!
- More generally, fundamental systems of invariants give us great properties and connections between many areas of mathematics!

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

Matching/Permutation monomials.

$\prod x_{i\sigma(i)}$ invariants

they are fundamental system of invariants

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials

  $X = (x_{ij})_{i,j=1}^{n}$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant

non constant

X^α

some row of X doesn't have any variable in X^α say row 1 doesn't have such variable, say row 2 has a variable in X^α

$$\begin{pmatrix} t & & & \\ & t^{-1} & & \\ & & 1 & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} X \longmapsto \begin{pmatrix} tx_{11} & tx_{12} & \cdots & tx_{1n} \\ t^{-1}x_{21} & t^{-1}x_{22} & \cdots & t^{-1}x_{2n} \\ x_{31} & x_{32} & \cdots & x_{3n} \\ \vdots & & & \vdots \\ x_{n1} & & & x_{nn} \end{pmatrix}$$

NOT invariant

$X^\alpha = x_{21} \underbrace{X^\beta}_{}$ $\longrightarrow$ only for 3^{rd} row onwards

$\mapsto t^{-1} x_{21} X^\beta$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant

they are the only ones of degree n

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree $\underline{kn}$ for some $k \in \mathbb{Z}$

moreover every row must have exactly k variables (w/ repetition) appearing in any monomial

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Invariant monomial of degree kn must have exactly k non-zeros in each row, and each column

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \text{Mat}(n)$ row/column scaling

Matching/Permutation monomials.

- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Invariant monomial of degree kn must have exactly k non-zeros in each row, and each column
- Birkhoff-von Neumann theorem, must be in convex hull of permutations

$\|\alpha\| = kn$

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \vdots & & & \\ \alpha_{n1} & \cdots & & \alpha_{nn} \end{pmatrix}$$

X^{α}

$\boxed{\dfrac{\alpha}{k}}$ row 1, col. 1

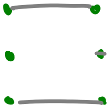
$\hookrightarrow$ doubly-stochastic matrix

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.
- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Invariant monomial of degree kn must have exactly k non-zeros in each row, and each column
- Birkhoff-von Neumann theorem, must be in convex hull of permutations
- Relation to combinatorics: if matrix A is adjacency matrix of a bipartite graph H, then A has *no perfect matching* iff A *vanishes on all invariants*!

$\prod A_{i\sigma(i)} = 0$



not perfect matching.

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.
- Our group is abelian, so invariants are generated by monomials
- No monomial of degree $< n$ can be an invariant
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Invariant monomial of degree kn must have exactly k non-zeros in each row, and each column
- Birkhoff-von Neumann theorem, must be in convex hull of permutations
- Relation to combinatorics: if matrix A is adjacency matrix of a bipartite graph H, then A has *no perfect matching* iff A *vanishes on all invariants*!
- It is no coincidence that polytopes appear naturally with torus actions. Shall see this more later.

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$g^{-1} \circ p = p\left(\underbrace{g\begin{pmatrix} x \\ y \end{pmatrix}}\right)$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$\begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}$$

$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

- If (a', b', c') is the image $g^{-1} \circ p$, we have

$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$$
$$b' = 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma)$$
$$c' = a\beta^2 + b\beta\delta + c\delta^2$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$
$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$
- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$\alpha\delta - \beta\gamma = 1$

$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

$(ax+by)^2 \updownarrow (a'x+b'y)^2$

$\Delta = 0 \updownarrow \Delta' = 0$

much easier way to see it

- If (a', b', c') is the image $g^{-1} \circ p$, we have
$$a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$$
$$b' = 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma)$$
$$c' = a\beta^2 + b\beta\delta + c\delta^2$$
- The discriminant is an *invariant*!
$$\underline{b^2 - 4ac} = \underline{(b')^2 - 4a'c'}$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

- If (a', b', c') is the image $g^{-1} \circ p$, we have

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma) \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

- The discriminant is an *invariant*!

$$b^2 - 4ac = (b')^2 - 4a'c'$$

- It captures exactly the quadratic polynomials which have a double root! We will see again why this is the case in a later lecture.

- Group Actions on Vector Spaces
- Ring of Invariant Polynomials
- Fundamental Theorems
- Conclusion
- Acknowledgements

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.

$G = A_n \qquad V = \mathbb{C}^n$

$$\Big\{ e_1, \dots, e_n \;,\; \underbrace{\Delta = \prod_{i<j} (x_i - x_j)}_{\text{not symmetric}} \Big\}$$

fundamental system of invariants

Δ^2 is symmetric $\therefore$ $\Delta^2 \in \mathbb{C}[e_1, \dots, e_n]$

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

These were the problems Hilbert was trying to solve when he developed the **Hilbert Basis Theorem**, **Nullstellensatz** and **Syzygy** theorem - cornerstones of modern commutative algebra and algebraic geometry.

1890 , 1893

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

  These were the problems Hilbert was trying to solve when he developed the **Hilbert Basis Theorem**, **Nullstellensatz** and **Syzygy** theorem - cornerstones of modern commutative algebra and algebraic geometry.

- Answer to third problem can be done via Gröbner basis methods

Examples of Invariants with Syzygies

- Cyclic group of order 4:

$$G = \left\{ \underset{I}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}},\ \underset{x}{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}},\ \underset{y}{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}},\ \underset{z}{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}} \right\}$$

Examples of Invariants with Syzygies

$\boxed{V = \mathbb{C}^2}$

- Cyclic group of order 4:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$\underline{p(x, y) = p(-y, x)}$$

$\mathbb{C}[V] = \mathbb{C}[x, y]$

Examples of Invariants with Syzygies

- Cyclic group of order 4:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$p(x, y) = p(-y, x)$$

- Three fundamental invariants:

$$f_1 = x^2 + y^2,\ f_2 = x^2y^2,\ f_3 = x^3y - xy^3$$

Examples of Invariants with Syzygies

- Cyclic group of order 4:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$p(x, y) = p(-y, x)$$

- Three fundamental invariants:

$$f_1 = x^2 + y^2, \; f_2 = x^2 y^2, \; f_3 = x^3 y - x y^3$$

- Syzygy:

$$f_3^2 - f_2 f_1^2 + 4 f_2^2$$

Conclusion

- Today we learned the basics about the algebraic side of invariant theory
- Some history
- Many examples of important rings of invariants
- Connections to other areas of mathematics
- Fundamental problems in invariant theory

Acknowledgement

- Lecture based entirely on the wonderful book by Sturmfels: Algorithms in Invariant Theory