# Lecture 16: Reynolds Operator & Finite Generation of Invariant Rings


Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com


March 10, 2021

# Overview

- Finite Generation of Invariant Rings for Finite Groups
- Reynolds Operator & Finite Generation
- Cayley's $\Omega$-process and Reynolds Operator for $\mathbb{SL}(n)$
- Conclusion
- Acknowledgements

# Invariant Theory

- Emmy Noether
- Dame Francis Kirwan
- Linda Ness

# Finite Generation Problem

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

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

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

[1] Today: finite groups and $\mathbb{SL}(n)$. More generally *linearly reductive*

# Finite Generation Problem

- 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. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^{d+1}$ — linear transformations of curves

[1] Today: finite groups and $\mathbb{SL}(n)$. More generally *linearly reductive*

# Finite Generation Problem

$V = \mathbb{C}^N$ $\quad \mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_N]$

- 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. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^{d+1}$ — linear transformations of curves
- Invariant polynomials form a *subring* of $\mathbb{C}[V]$, denoted $\mathbb{C}[V]^G$
- Question from last lecture:

  Given a nice group $G$ acting linearly on a vector space $V$, is $\mathbb{C}[V]^G$ *finitely generated* as a $\mathbb{C}$-algebra?

$$\mathbb{C}[f_1, \ldots, f_t] = \mathbb{C}[V]^G$$

[1]Today: finite groups and $\mathbb{SL}(n)$. More generally *linearly reductive*

# Finite Generation Problem

- 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. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^{d+1}$ — linear transformations of curves
- Invariant polynomials form a *subring* of $\mathbb{C}[V]$, denoted $\mathbb{C}[V]^G$
- Question from last lecture:

  Given a nice group $G$ acting linearly on a vector space $V$, is $\mathbb{C}[V]^G$ *finitely generated* as a $\mathbb{C}$-algebra?

- Last lecture, we saw this was the case for first example. Is this a general phenomenon?
- Hilbert (twice) 1890, 1893: YES!

$G = SL(3)$ $\quad V = \mathbb{C}^{\binom{n+2}{2}}$

$x^a y^b z^c \quad n = a+b+c$

[1]Today: finite groups and $\mathbb{SL}(n)$. More generally *linearly reductive*

## 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 $\mathbb{C}[\mathbf{x}]^G$

# 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!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

  – non zero
  – homogeneous

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

  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!

# 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!
- Can we generalize this to work for every finite group?

# Averaging Operator

- If $G$ is a finite group acting linearly on $V = \mathbb{C}^N$, let $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

$$\rho(p) = \frac{1}{|G|} \cdot \sum_{g \in G} g \circ p$$

(1)(2)(3)
(1 2)(3)
(1 3)(2)
(1 2 3)
(1 3 2)
(1)(2 3)

$G = S_3 \qquad V = \mathbb{C}^3$

$p(x_1, x_2, x_3) = x_1$

$$\rho(p) = \frac{1}{6}\left(x_1 + x_2 + x_3 + x_2 + x_3 + x_1\right)$$

$$= \frac{1}{3} e_1(x_1, x_2, x_3)$$

$$\rho(p) = \frac{1}{|G|} \sum_{g \in G} g \circ p$$

$$\underline{h \circ \rho(p)} = \frac{1}{|G|} \sum_{g \in G} \underbrace{h \circ (g \circ p)}_{(hg) \circ p}$$

$f : G \longrightarrow G$ permutation

$g \longmapsto hg$

invariant!

$\downarrow$

$hg_1 = hg_2 \iff g_1 = g_2$

$$= \frac{1}{|G|} \sum_{\nu \in G} \nu \circ p = \underline{\rho(p)}$$

# Averaging Operator

- If $G$ is a finite group acting linearly on $V = \mathbb{C}^N$, let $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

$$\rho(p) = \frac{1}{|G|} \cdot \sum_{g \in G} g \circ p$$

- Properties of $\rho$:
  1. $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a linear operator projection
  2. $\rho(p \cdot q) = p \cdot \rho(q)$ for any $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  3. $\deg(\rho(p)) = \deg(p)$ whenever $\rho(p) \neq 0$

$$\rho(p+q) = \frac{1}{|G|} \sum_{g \in G} g(p+q) = \rho(p) + \rho(q)$$

$g \circ p + g \circ q$

whenever $p$ is homogeneous polynomial

non-homogeneous $\deg(\rho(p)) \leq \deg(p)$

# Averaging Operator

- If $G$ is a finite group acting linearly on $V = \mathbb{C}^N$, let $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

$$\rho(p) = \frac{1}{|G|} \cdot \sum_{g \in G} g \circ p$$

- Properties of $\rho$:
  1. $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a linear operator projection
  2. $\rho(p \cdot q) = p \cdot \rho(q)$ for any $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  3. $\deg(\rho(p)) = \deg(p)$ whenever $\rho(p) \neq 0$
- Now, we can use $\rho$ to reduce finite generation as $\mathbb{C}$-algebra to finite generation of ideals!

# Averaging Operator

- If $G$ is a finite group acting linearly on $V = \mathbb{C}^N$, let $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

$$\rho(p) = \frac{1}{|G|} \cdot \sum_{g \in G} g \circ p$$

- Properties of $\rho$:
  1. $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a linear operator projection
  2. $\rho(p \cdot q) = p \cdot \rho(q)$ for any $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  3. $\deg(\rho(p)) = \deg(p)$ whenever $\rho(p) \neq 0$
- Now, we can use $\rho$ to reduce finite generation as $\mathbb{C}$-algebra to finite generation of ideals!
- Note that our ring $\mathbb{C}[\mathbf{x}]$ is graded by degree, and so is our ring of invariants!

$$\mathbb{C}[\bar{x}] = \mathbb{C} \oplus \underbrace{\mathbb{C}[\bar{x}]_1}_{ax+by} \oplus \underbrace{\mathbb{C}[\bar{x}]_2}_{ax^2+bxy+cy^2} \oplus \cdots$$

# Averaging Operator

- If $G$ is a finite group acting linearly on $V = \mathbb{C}^N$, let $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

$$\rho(p) = \frac{1}{|G|} \cdot \sum_{g \in G} g \circ p$$

- Properties of $\rho$:
  1. $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a linear operator projection
  2. $\rho(p \cdot q) = p \cdot \rho(q)$ for any $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  3. $\deg(\rho(p)) = \deg(p)$ whenever $\rho(p) \neq 0$
- Now, we can use $\rho$ to reduce finite generation as $\mathbb{C}$-algebra to finite generation of ideals!
- Note that our ring $\mathbb{C}[\mathbf{x}]$ is graded by degree, and so is our ring of invariants!
- Plus, note that our invariants can always be taken to be homogeneous polynomials (otherwise we can take homogeneous components).

# Finite Generation

- Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]_0 \oplus \mathbb{C}[\mathbf{x}]_1 \oplus \mathbb{C}[\mathbf{x}]_2 \oplus \cdots$ be grading by degree

## Finite Generation

- Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]_0 \oplus \mathbb{C}[\mathbf{x}]_1 \oplus \mathbb{C}[\mathbf{x}]_2 \oplus \cdots$ be grading by degree
- Similarly $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[\mathbf{x}]_0^G \oplus \mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$
- Let $J \subset \mathbb{C}[\mathbf{x}]$ be the *ideal* generated by

$$\mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$$

homogeneous non-constant invariant polynomials

$J$ = ideal of $\mathbb{C}[\bar{x}]$ generated by homogeneous non-constant invariants

# Finite Generation

- Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]_0 \oplus \mathbb{C}[\mathbf{x}]_1 \oplus \mathbb{C}[\mathbf{x}]_2 \oplus \cdots$ be grading by degree
- Similarly $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[\mathbf{x}]_0^G \oplus \mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$
- Let $J \subset \mathbb{C}[\mathbf{x}]$ be the *ideal* generated by

$$\longrightarrow \mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$$

- By Hilbert Basis Theorem (HBT), we know that $J$ is finitely generated.

$f_1, \ldots, f_s$

$$J = (a_1, \ldots, a_t)$$

Moreover, we can take $a_i$'s to be invariants (from proof of HBT)

$$f_i = b_{i1} h_{i1} + b_{i2} h_{i2} + \cdots + b_{il} h_{il}$$

→ homogeneous non-constant invariants

# Finite Generation

- Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]_0 \oplus \mathbb{C}[\mathbf{x}]_1 \oplus \mathbb{C}[\mathbf{x}]_2 \oplus \cdots$ be grading by degree
- Similarly $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[\mathbf{x}]_0^G \oplus \mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$
- Let $J \subset \mathbb{C}[\mathbf{x}]$ be the *ideal* generated by

$$\mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$$

- By Hilbert Basis Theorem (HBT), we know that $J$ is finitely generated.

$$J = (a_1, \ldots, a_t)$$

  Moreover, we can take $a_i$'s to be invariants (from proof of HBT)
- We can assume $a_i$'s are homogeneous (otherwise take their homogeneous components as generators)

# Finite Generation

- Let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[\mathbf{x}]_0 \oplus \mathbb{C}[\mathbf{x}]_1 \oplus \mathbb{C}[\mathbf{x}]_2 \oplus \cdots$ be grading by degree
- Similarly $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[\mathbf{x}]_0^G \oplus \mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$
- Let $J \subset \mathbb{C}[\mathbf{x}]$ be the *ideal* generated by

$$\mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots$$

- By Hilbert Basis Theorem (HBT), we know that $J$ is finitely generated.

$$J = (a_1, \ldots, a_t)$$

  Moreover, we can take $a_i$'s to be invariants (from proof of HBT)
- We can assume $a_i$'s are homogeneous (otherwise take their homogeneous components as generators)
- We will now show that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$

# Finite Generation

- Proof that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$ is by induction on degree.

# Finite Generation

- Proof that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$ is by induction on degree.
- Claim is true for $d = 0$ (base case). Suppose claim is true for all polynomials of degree $< d$ in $\mathbb{C}[\mathbf{x}]^G$, where we now have $d > 0$.

# Finite Generation

- Proof that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$ is by induction on degree.
- Claim is true for $d = 0$ (base case). Suppose claim is true for all polynomials of degree $< d$ in $\mathbb{C}[\mathbf{x}]^G$, where we now have $d > 0$.
- If $p \in \mathbb{C}[\mathbf{x}]^G_d$, since we know that $p \in J$ by definition of $J$, we have

invariant homogeneous of degree d

$$p = a_1 b_1 + \cdots + a_t b_t \in \mathbb{C}[\bar{x}]$$

$a_i$'s invariants

$\mathbb{C}[a_1, \ldots, a_t]$

# Finite Generation

- Proof that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$ is by induction on degree.
- Claim is true for $d = 0$ (base case). Suppose claim is true for all polynomials of degree $< d$ in $\mathbb{C}[\mathbf{x}]^G$, where we now have $d > 0$.
- If $p \in \mathbb{C}[\mathbf{x}]^G_d$, since we know that $p \in J$ by definition of $J$, we have

$$p = a_1 b_1 + \cdots + a_t b_t$$

- Applying the averaging operator on both sides, we have:

$$\begin{aligned} p = \rho(p) &= \rho(a_1 b_1 + \cdots + a_t b_t) \\ &= \rho(a_1 b_1) + \cdots + \rho(a_t b_t) \\ &= a_1 \cdot \rho(b_1) + \cdots + a_t \cdot \rho(b_t) \end{aligned}$$

$\deg(a_i b_i) = \deg(p)$ if $a_i b_i \neq 0$

$p \in J$

$p$ invariant

$\rho$ is linear

$a_i \in \mathbb{C}[\bar{x}]^G$

$\rho(a_i b_i) = a_i \cdot \rho(b_i)$

$\rho(b_i)$'s are invariants!

$d = \deg(p) = \deg(a_i b_i) \geq \deg(a_i) + \deg(\rho(b_i))$, with $\deg(a_i) \geq 1$

# Finite Generation

- Proof that $\mathbb{C}[\mathbf{x}]^G = \mathbb{C}[a_1, \ldots, a_t]$ is by induction on degree.
- Claim is true for $d = 0$ (base case). Suppose claim is true for all polynomials of degree $< d$ in $\mathbb{C}[\mathbf{x}]^G$, where we now have $d > 0$.
- If $p \in \mathbb{C}[\mathbf{x}]^G_d$, since we know that $p \in J$ by definition of $J$, we have

$$p = a_1 b_1 + \cdots + a_t b_t$$

- Applying the averaging operator on both sides, we have:

$$\begin{aligned} p = \rho(p) &= \rho(a_1 b_1 + \cdots + a_t b_t) \\ &= \rho(a_1 b_1) + \cdots + \rho(a_t b_t) \\ &= a_1 \cdot \rho(b_1) + \cdots + a_t \cdot \rho(b_t) \end{aligned}$$

- By induction, and the fact that $\deg(\rho(b_i)) < d$, we have that

$$p \in \mathbb{C}[a_1, \ldots, a_t]$$

induction $\Rightarrow$ $\rho(b_i) \in \mathbb{C}[a_1, \ldots, a_t]$

$P = a_1 \rho(b_1) + \cdots + a_t \rho(b_t)$ $\in \mathbb{C}[a_1, \ldots, a_t]$

- Finite Generation of Invariant Rings for Finite Groups
- Reynolds Operator & Finite Generation
- Cayley's Ω-process and Reynolds Operator for $\mathbb{SL}(n)$
- Conclusion
- Acknowledgements

# Hilbert's Idea

- Let $G$ be our group acting on $\mathbb{C}^N$, and $\mathbb{C}[\mathbf{x}]$ our coordinate ring.
- If we had a procedure which projected any polynomial from $\mathbb{C}[\mathbf{x}]$ onto the ring of invariants $\mathbb{C}[\mathbf{x}]^G$, we could try to do something similar to Hilbert Basis Theorem!

[2] For a proof of this, see Derksen & Kemper Chapter 2

# Hilbert's Idea

- Let $G$ be our group acting on $\mathbb{C}^N$, and $\mathbb{C}[\mathbf{x}]$ our coordinate ring.
- If we had a procedure which projected any polynomial from $\mathbb{C}[\mathbf{x}]$ onto the ring of invariants $\mathbb{C}[\mathbf{x}]^G$, we could try to do something similar to Hilbert Basis Theorem!
- Here are the properties we need from such map $R : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$
  - $R$ is a linear map
  - $R(p) = p$ for all $p \in \mathbb{C}[\mathbf{x}]^G$
  - $R(pq) = p \cdot R(q)$ for each $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  - $\deg(R(q)) = \deg(q)$ whenever $R(q) \neq 0$

    and q homogeneous

[2]For a proof of this, see Derksen & Kemper Chapter 2

# Hilbert's Idea

- Let $G$ be our group acting on $\mathbb{C}^N$, and $\mathbb{C}[\mathbf{x}]$ our coordinate ring.
- If we had a procedure which projected any polynomial from $\mathbb{C}[\mathbf{x}]$ onto the ring of invariants $\mathbb{C}[\mathbf{x}]^G$, we could try to do something similar to Hilbert Basis Theorem!
- Here are the properties we need from such map $R : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$
  - $R$ is a linear map
  - $R(p) = p$ for all $p \in \mathbb{C}[\mathbf{x}]^G$
  - $R(pq) = p \cdot R(q)$ for each $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  - $\deg(R(q)) = \deg(q)$ whenever $R(q) \neq 0$
- a linear map $R_G : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a *Reynolds operator* if it satisfies the following properties:
  1. $R_G(p) = p$ for all $p \in \mathbb{C}[\mathbf{x}]^G$
  2. $R_G$ is $G$-invariant, that is, $R_G(g \circ p) = R_G(p)$ for all $p \in \mathbb{C}[\mathbf{x}]$ and all $g \in G$

any Reynolds operator has these properties

[2] For a proof of this, see Derksen & Kemper Chapter 2

# Hilbert's Idea

- Let $G$ be our group acting on $\mathbb{C}^N$, and $\mathbb{C}[\mathbf{x}]$ our coordinate ring.
- If we had a procedure which projected any polynomial from $\mathbb{C}[\mathbf{x}]$ onto the ring of invariants $\mathbb{C}[\mathbf{x}]^G$, we could try to do something similar to Hilbert Basis Theorem!
- Here are the properties we need from such map $R : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$
  - $R$ is a linear map
  - $R(p) = p$ for all $p \in \mathbb{C}[\mathbf{x}]^G$
  - $R(pq) = p \cdot R(q)$ for each $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$
  - $\deg(R(q)) = \deg(q)$ whenever $R(q) \neq 0$
- a linear map $R_G : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$ is a *Reynolds operator* if it satisfies the following properties:
  1. $R_G(p) = p$ for all $p \in \mathbb{C}[\mathbf{x}]^G$
  2. $R_G$ is $G$-invariant, that is, $R_G(g \circ p) = R_G(p)$ for all $p \in \mathbb{C}[\mathbf{x}]$ and all $g \in G$
- One can prove (requires representation theory) that the Reynolds operator exists (and is unique) when $G$ is reductive and that it has the properties above.[2]

[2] For a proof of this, see Derksen & Kemper Chapter 2

# From Reynolds Operator to Finite Generation

$$R : \mathbb{C}[\bar{x}] \longrightarrow \mathbb{C}[\bar{x}]^G$$

$J$ = ideal generated by non-constant homogeneous invariants

$J = (a_1, \ldots, a_t)$ HBT

$p = a_1 b_1 + \cdots + a_t b_t$

$$p = R(p) = R(a_1 b_1 + \cdots + a_t b_t)$$
$$= R(a_1 b_1) + \cdots + R(a_t b_t)$$
$$= a_1 \underbrace{R(b_1)}_{\in \mathbb{C}[a_1, \ldots, a_t]} + \cdots + a_t \underbrace{R(b_t)}$$

- Finite Generation of Invariant Rings for Finite Groups
- Reynolds Operator & Finite Generation
- Cayley's Ω-process and Reynolds Operator for $\mathbb{SL}(n)$
- Conclusion
- Acknowledgements

# What if our group is not finite?

- We reduced the question of *finite generation of invariants* to the question of computing the *Reynolds Operator* of a group action

# What if our group is not finite?

- We reduced the question of *finite generation of invariants* to the question of computing the *Reynolds Operator* of a group action
- How do we compute the Reynolds Operator?
- Difficult question, today we will see how to do it for $\mathbb{SL}(n)$

Cayley's $\Omega$-process

# Differential Polynomials & Cayley's Ω-process

- Given a polynomial ring $\mathbb{C}[x_1, \dots, x_n]$, can define the ring of differential polynomials $\underline{\mathbb{C}[\partial_1, \dots, \partial_n]}$

$$\partial_i x_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

$$\partial_i x_i^d = d\, x_i^{d-1}$$

$$\partial_i \partial_j : \mathbb{C}[\bar{x}] \longrightarrow \mathbb{C}[\bar{x}]$$

$$\partial_i \partial_j = \partial_j \partial_i$$

$$x_i x_j \longmapsto 1$$

$$x_i^2 \longmapsto 0$$

$$x_i^2 x_j \longmapsto 2x_i$$

$$p \longmapsto \partial_i \partial_j p$$

# Differential Polynomials & Cayley's Ω-process

- Given a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, can define the ring of differential polynomials $\mathbb{C}[\partial_1, \ldots, \partial_n]$
- For each polynomial $f(x_1, \ldots, x_n)$ we have its corresponding differential polynomial $D_f(\partial_1, \ldots, \partial_n)$, acts as a differential operator

$$x_1^2 x_2 \longleftrightarrow \partial_1^2 \partial_2$$

$$a x_1 x_2 + b x_2^2 \longleftrightarrow a \partial_1 \partial_2 + b \partial_2^2$$

# Differential Polynomials & Cayley's $\Omega$-process

- Given a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, can define the ring of differential polynomials $\mathbb{C}[\partial_1, \ldots, \partial_n]$
- For each polynomial $f(x_1, \ldots, x_n)$ we have its corresponding differential polynomial $D_f(\partial_1, \ldots, \partial_n)$, acts as a differential operator
- If $f \in \mathbb{C}[\mathbf{x}]$ homogeneous, we have $D_f \circ f$ is a constant

-2 -2 2

$$(\partial_1\partial_2 + \partial_1^2)(x_1x_2 + x_1^2) = 1 + 0 + 0 + 2$$

$$= 3$$

# Differential Polynomials & Cayley's $\Omega$-process

- Given a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, can define the ring of differential polynomials $\mathbb{C}[\partial_1, \ldots, \partial_n]$
- For each polynomial $f(x_1, \ldots, x_n)$ we have its corresponding differential polynomial $D_f(\partial_1, \ldots, \partial_n)$, acts as a differential operator
- If $f \in \mathbb{C}[\mathbf{x}]$ homogeneous, we have $D_f \circ f$ is a constant
- Other basic properties of differential operators $D_f$:
  1. $D_f(p+q) = D_f(p) + D_f(q)$
  2. $D_{\alpha f}(p) = D_f(\alpha p) = \alpha \cdot D_f(p)$, for constants $\alpha \in \mathbb{C}$
  3. $D_{f+g}(p) = D_f(p) + D_g(p)$
  4. $D_{fg}(p) = D_f D_g(p)$ composition of differential operators

# Differential Polynomials & Cayley's $\Omega$-process

- Given a polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$, can define the ring of differential polynomials $\mathbb{C}[\partial_1, \ldots, \partial_n]$
- For each polynomial $f(x_1, \ldots, x_n)$ we have its corresponding differential polynomial $D_f(\partial_1, \ldots, \partial_n)$, acts as a differential operator
- If $f \in \mathbb{C}[\mathbf{x}]$ homogeneous, we have $D_f \circ f$ is a constant
- Other basic properties of differential operators $D_f$:
  1. $D_f(p+q) = D_f(p) + D_f(q)$
  2. $D_{\alpha f}(p) = D_f(\alpha p) = \alpha \cdot D_f(p)$, for constants $\alpha \in \mathbb{C}$
  3. $D_{f+g}(p) = D_f(p) + D_g(p)$
  4. $D_{fg}(p) = D_f D_g(p)$ composition of differential operators
- We are now ready to define the $\Omega$-process:
  - If $Z$ is the symbolic $n \times n$ matrix over $\mathbb{C}[Z]$
  - Let $\mathbb{C}[\partial]$ be the ring of differential polynomials

$$Z = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

$$\Omega := D_{\det} = \det(\partial_{ij})$$

$$Z = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}$$

$$\partial = \begin{pmatrix} \partial_{11} & \partial_{12} \\ \partial_{21} & \partial_{22} \end{pmatrix}$$

$$\longrightarrow \mathbb{C}[Z] = \mathbb{C}[z_{11}, z_{12}, z_{21}, z_{22}]$$

$$\mathbb{C}[\partial] = \mathbb{C}[\partial_{11}, \partial_{12}, \partial_{21}, \partial_{22}]$$

$$P \overset{\Omega}{\longmapsto} \det(\partial) \cdot P$$

$$\Omega(P) = \det(\partial) \cdot P$$

$$= (\partial_{11}\partial_{22} - \partial_{12}\partial_{21}) P$$

# From $\Omega$-process to Reynolds

- We show how to use the $\Omega$-process to compute the Reynolds Operator via an example:

# From Ω-process to Reynolds

- We show how to use the Ω-process to compute the Reynolds Operator via an example:
- $G = \mathbb{SL}(2)$ acting on $\mathbb{C}^3$ (binary quadratic forms)

$$ax^2 + bxy + cy^2$$

$$(a, b, c)$$

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

$$(a', b', c') \longleftrightarrow a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2$$

# From Ω-process to Reynolds

- We show how to use the Ω-process to compute the Reynolds Operator via an example:
- $G = \mathbb{SL}(2)$ acting on $\mathbb{C}^3$ (binary quadratic forms)
- To get Reynolds operator, do as follows:
  1. Take any polynomial $p \in \mathbb{C}[\mathbf{x}]$ and the *generic* action of the symbolic matrix $Z = (Z_{ij})$

$Z \circ P$

# From Ω-process to Reynolds

- We show how to use the Ω-process to compute the Reynolds Operator via an example:
- $G = \mathbb{SL}(2)$ acting on $\mathbb{C}^3$ (binary quadratic forms)
- To get Reynolds operator, do as follows:
  1. Take any polynomial $p \in \mathbb{C}[\mathbf{x}]$ and the *generic* action of the symbolic matrix $Z = (Z_{ij})$
  2. Compute $Z \circ p$ polynomial in $\mathbb{C}[Z, \mathbf{x}]$

$Z_{11}$ $Z_{12}$ $Z_{21}$ $Z_{22}$

# From Ω-process to Reynolds

- We show how to use the Ω-process to compute the Reynolds Operator via an example:
- $G = \mathbb{SL}(2)$ acting on $\mathbb{C}^3$ (binary quadratic forms)
- To get Reynolds operator, do as follows:
  1. Take any polynomial $p \in \mathbb{C}[\mathbf{x}]$ and the *generic* action of the symbolic matrix $Z = (Z_{ij})$
  2. Compute $Z \circ p$ polynomial in $\mathbb{C}[Z, \mathbf{x}]$
  3. Use Ω-process (repeatedly) to *kill* variables $Z$

# From Ω-process to Reynolds

- We show how to use the Ω-process to compute the Reynolds Operator via an example:
- $G = \mathbb{SL}(2)$ acting on $\mathbb{C}^3$ (binary quadratic forms)
- To get Reynolds operator, do as follows:
  1. Take any polynomial $p \in \mathbb{C}[\mathbf{x}]$ and the *generic* action of the symbolic matrix $Z = (Z_{ij})$
  2. Compute $Z \circ p$ polynomial in $\mathbb{C}[Z, \mathbf{x}]$
  3. Use Ω-process (repeatedly) to *kill* variables $Z$
  4. Resulting polynomial is an invariant!

# Binary Quadrics

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

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

# Binary Quadrics

- 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

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

# Binary Quadrics

- 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

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

# Binary Quadrics

- Take monomial $ac$

# Binary Quadrics

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ $\mathbb{C}[\alpha, \beta, \gamma, \delta]$

↑ variables

- Take monomial $ac$
- Symbolic transformation takes $ac$ to $a'c'$

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

polynomial in $\mathbb{C}[\alpha, \beta, \gamma, \delta, a, b, c]$

# Binary Quadrics

$\det\begin{pmatrix} \partial_\alpha & \partial_\beta \\ \partial_\gamma & \partial_\delta \end{pmatrix} = \partial_\alpha\partial_\delta - \partial_\beta\partial_\gamma$

- Take monomial $ac$
- Symbolic transformation takes $ac$ to $a'c'$

$$\rightarrow (a\alpha^2 + b\alpha\gamma + c\gamma^2)(a\beta^2 + b\beta\delta + c\delta^2)$$

- Apply the $\Omega$-process: $\Omega = \partial_\alpha\partial_\delta - \partial_\beta\partial_\gamma$ until no more variables from symbolic transformation!

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

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

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

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

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

$$\Omega = \partial_\alpha \partial_\delta - \partial_\beta \partial_\gamma$$

$$P = (2a\alpha + b\gamma)(b\beta + 2c\delta) - (b\alpha + 2c\gamma)(2a\beta + b\delta)$$

Apply $\Omega$-process again (because we still have $\alpha, \beta, \gamma, \delta$)

$$\partial_\alpha \partial_\delta P = \partial_\alpha \left[ (2a\alpha + b\gamma) \cdot 2c - (b\alpha + 2c\gamma) \cdot b \right]$$
$$= 4ac - b^2$$

$$\partial_\beta \partial_\gamma P = \partial_\beta \left[ b(b\beta + 2c\delta) - 2c(2a\beta + b\delta) \right]$$
$$= b^2 - 4ac$$

$$\Omega(P) = (4ac - b^2) - (b^2 - 4ac)$$
$$= 2(4ac - b^2)$$ Invariant!

# Binary Quadrics

- Finite Generation of Invariant Rings for Finite Groups
- Reynolds Operator & Finite Generation
- Cayley's $\Omega$-process and Reynolds Operator for $\mathbb{SL}(n)$
- Conclusion
- Acknowledgements

# Conclusion

- Today we proved the first fundamental theorem of invariant theory

  If group $G$ is reductive, the invariant ring is finitely generated as a $\mathbb{C}$-algebra

# Conclusion

- Today we proved the first fundamental theorem of invariant theory

  If group $G$ is reductive, the invariant ring is finitely generated as a $\mathbb{C}$-algebra

- Saw how the Reynolds Operator reduces the finite generation as an *algebra* to finite generation as an *ideal*

# Conclusion

- Today we proved the first fundamental theorem of invariant theory

  If group $G$ is reductive, the invariant ring is finitely generated as a $\mathbb{C}$-algebra

- Saw how the Reynolds Operator reduces the finite generation as an *algebra* to finite generation as an *ideal*
- Learned how to compute Reynolds Operator for finite groups (averaging)
- Learned about the $\Omega$-process, which is used to compute the Reynolds Operator for $\mathbb{SL}(n)$ actions

# Conclusion

- Today we proved the first fundamental theorem of invariant theory

  If group $G$ is reductive, the invariant ring is finitely generated as a $\mathbb{C}$-algebra

- Saw how the Reynolds Operator reduces the finite generation as an *algebra* to finite generation as an *ideal*
- Learned how to compute Reynolds Operator for finite groups (averaging)
- Learned about the $\Omega$-process, which is used to compute the Reynolds Operator for $\mathbb{SL}(n)$ actions
- Explicit formulas for Reynolds Operator important for *analytic* algorithms in invariant theory!
- Even though may be difficult to compute (analogous to Cramer's rule), knowing formula is important and gives us quantitative information!

# Conclusion

- Today we proved the first fundamental theorem of invariant theory

  If group $G$ is reductive, the invariant ring is finitely generated as a $\mathbb{C}$-algebra

- Saw how the Reynolds Operator reduces the finite generation as an *algebra* to finite generation as an *ideal*
- Learned how to compute Reynolds Operator for finite groups (averaging)
- Learned about the $\Omega$-process, which is used to compute the Reynolds Operator for $\mathbb{SL}(n)$ actions
- Explicit formulas for Reynolds Operator important for *analytic* algorithms in invariant theory!
- Even though may be difficult to compute (analogous to Cramer's rule), knowing formula is important and gives us quantitative information!
- Lots of open questions in this area!

Symbolic computation of invariant polynomials

$$\boxed{e_d} = \rho(\underline{x_1 x_2 \cdots x_d})$$

$$= \frac{1}{n!} \sum_{\underline{\sigma} \in S_n} \underline{x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(d)}}$$

wow it must be really hard to compute elementary symmetric polynomials!

# HW 1

$e_1, \dots, e_n$ are very easy to compute!

$$p(x) = \prod_{i=1}^{n} (t + x_i)$$

interpolation over $t$

$e_1, \dots, e_n$

Open: $H \subset S_n$ can we compute quickly a basis for $\mathbb{C}[x_1, \dots, x_n]^H$ ?

$S_n \curvearrowright \mathbb{C}^{\binom{n}{2}}$

permuting vertices
↓
edge permutation

$$S_n \subset S_{\binom{n}{2}}$$

can yield a fast algorithm to solve graph isomorphism problem!

# Acknowledgement

- Lecture based on the wonderful books:
  - Sturmfels: Algorithms in Invariant Theory
  - Derksen, Kemper: Computational Invariant Theory