Lecture 12: Reynolds Operator & Finite Generation of Invariant Rings

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

February 24, 2021

Overview

- 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

Finite Generation Problem

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

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

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

[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. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^d$ — 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?

[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. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^d$ — 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!

[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

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

  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**

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

  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 $\rho : \mathbb{C}[\mathbf{x}] \to \mathbb{C}[\mathbf{x}]^G$

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

projection

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

$$(h \circ g)\, p$$

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

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 ρ:
  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 $\rho(p) \neq 0$

p invariant $q \in \mathbb{C}[\bar{x}]$

$\rho(p \cdot q) = p \cdot \rho(q)$

ρ is a $\mathbb{C}[\bar{x}]^G$-algebra homomorphism

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 ρ:
  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 ρ 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 ρ:
  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 ρ 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!

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 ρ:
  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 ρ 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

quadratic form

$\mathbb{C}$ $a_1x_1 + \cdots + a_nx_n$

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

$$\underbrace{\mathbb{C}[\mathbf{x}]_1^G \oplus \mathbb{C}[\mathbf{x}]_2^G \oplus \cdots}_{\text{non-constant (homogeneous) invariant polynomials}}$$

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.

as an ideal

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

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

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.

$\supseteq$ have by definition

$\mathbb{C}[x]^G \subseteq \mathbb{C}[a_1, \ldots, a_t]$ by induction on degree

$\mathbb{C}[\bar{x}]_0^G \subset \mathbb{C}[a_1, \ldots, a_t]_0$

$\mathbb{C}[\bar{x}]_0^G = \mathbb{C}$, $\quad \mathbb{C}[a_1, \ldots, a_t]_0 = \mathbb{C}$

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

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

$\mathbb{C}[\bar{x}]^G_{d-1}, \ldots, \mathbb{C}[\bar{x}]^G_0 \subset \mathbb{C}[a_1, \ldots, a_t]$

$\Rightarrow \mathbb{C}[\bar{x}]^G_d \subset \mathbb{C}[a_1, \ldots, a_t]$

b_i's may not necessarily be invariants!

by homogeneity have $\deg(a_i b_i) = \deg(p) = d$

$\Rightarrow \deg(b_i) < d$

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:

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

projection

linear

$\mathbb{C}[x]^G$-algebra homomorphism

invariants!

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:

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

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

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

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

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

$\deg(\rho(b_i)) = \deg(b_i)$ (if $\rho(b_i) \neq 0$)
$< d$

- 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 $p \in \mathbb{C}[\mathbf{x}]^G$ projection
  - $R(pq) = p \cdot R(q)$ for each $p \in \mathbb{C}[\mathbf{x}]^G$ and $q \in \mathbb{C}[\mathbf{x}]$ $\mathbb{C}[\bar{x}]^G$ - algebra homomorphism
  - $\deg(R(q)) = \deg(q)$ whenever $R(q) \neq 0$

degree preserved (modulo zero)

[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 $g \in G$

[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

$$\mathbb{C}[\bar{x}]^G = \mathbb{C} \oplus \mathbb{C}[\bar{x}]_1^G \oplus \cdots$$

$$J = \left(\mathbb{C}[\bar{x}]_{\geq 1}^G \right)$$

finitely generated $\quad J = (a_1, \ldots, a_t)$

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

$$p = \sum_{i=1}^{t} a_i b_i$$

$$R_G(p) = \sum_{i=1}^{t} a_i \underbrace{R_G(b_i)}_{\deg < d}$$

- 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 Ω-process

Differential Polynomials & Cayley's Ω-process

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

differential operators in $\mathbb{C}[\bar{x}]$

$\partial_i x_j = \delta_{ij}$

$\partial_i x_i^e = e \cdot x_i^{e-1}$

$\partial_i \partial_j$

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

$$f(x, y) = xy$$

$$D_f(\partial_x, \partial_y) = \partial_x \partial_y$$

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
- If $f \in \mathbb{C}[\mathbf{x}]$ homogeneous, we have $D_f \circ f$ is a constant

$$\partial_x^2 \partial_y (x^2 y)$$

$$= \partial_x^2 (x^2) = 2$$

$$\partial_y^3 (x^2 y) \to \partial_y^2 (x^2) \to 0$$

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
- 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 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
- 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 Ω-process:
  - If Z is the symbolic $n \times n$ matrix over $\mathbb{C}[Z]$
  - Let $\mathbb{C}[\partial]$ be the ring of differential polynomials

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

$G = SL(n)$

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

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

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

$z_{11} \quad z_{12} \quad z_{21} \quad z_{22}$

From Ω-process to Reynolds

- We show how to use the Ω-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)

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 $Z = (Z_{ij})$

$g \circ p$ $\qquad\qquad$ $Z \circ p$

symbolic element of SL(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 $Z = (Z_{ij})$
  2. Compute $Z \circ p$ polynomial in $\mathbb{C}[Z, \mathbf{x}]$

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

$$\underbrace{\Omega(Z \circ p)}_{\deg_z} < \deg_z(Z \circ p)$$

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 $\mathbb{C}[Z, \mathbf{x}]$
  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

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

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

$\updownarrow$

$\mathbb{C}[Z, X]$

Binary Quadrics

- Take monomial ac $\in \mathbb{C}[a, b, c]$

Binary Quadrics

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

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

Binary Quadrics

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longleftrightarrow \begin{pmatrix} \partial_\alpha & \partial_\beta \\ \partial_\gamma & \partial_\delta \end{pmatrix}$$

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

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

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

$\alpha, \beta, \gamma, \delta$

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

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

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

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

Binary Quadrics

$\underline{\partial_\alpha \partial_\delta} - \partial_\beta \partial_\gamma$

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

applying Ω once again, we have:

$$\partial_\alpha \partial_\delta \circ r = 2a \cdot 2c - b^2$$

$$\partial_\beta \partial_\gamma \circ r = b^2 - 2c \cdot 2a$$

$$\Omega(r) = (4ac - b^2) - (b^2 - 4ac)$$

$$= -2(b^2 - 4ac)$$

$D_g(f) \leftarrow$ constant

discriminant

$D_f(f)$ constant (coming from Ω process)

$$p(\bar{x}) = \sum \underset{\mathbb{C}}{\overset{\cup\!\!\!\!\mid}{p_{\bar{e}}}} \bar{x}^{\bar{e}}$$

$$p(z \cdot x) = \sum_{\bar{e}} p_{\bar{e}} f_{\bar{e}}(z) \cdot \bar{x}^{\bar{e}}$$

because action linear $f_{\bar{e}}(z)$ is homogeneous $\deg(f_{\bar{e}}) = \|\bar{e}\|_1 \cdot (\deg \text{action})$

$D_g(f_{\bar{e}})$ if $\deg(g) = \deg(f_{\bar{e}})$

↖ constant

$D_g(p(z \circ x)) \in \mathbb{C}[\bar{x}]$

- 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

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 Ω-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 Ω-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 Ω-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!

Acknowledgement

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

director's cut:

what about syzygies

Hilbert 1890, 1893

that finite generation of invariants $\Rightarrow$ finite generation of syzygies

$$\textcolor{magenta}{\mathbb{C}[y_1, \dots, y_t]} \longrightarrow \overbrace{\mathbb{C}[\bar{x}]^G}^{a_1, \dots, a_t} \longrightarrow 0$$

$\mathbb{C}[\bar{x}] \to S$

$f_1, f_2, f_3 \qquad f_3^2 = f_1 f_2$

$z^3 - xy \qquad z \mapsto f_3 \quad x \mapsto f_1 \quad y \mapsto f_2$

homomorphism

$$\mathbb{C}[x,y,z] \xrightarrow{\varphi} \overbrace{\mathbb{C}[f_1,f_2,f_3]}^{R} \to 0$$

$z^2 - xy \in \ker(\varphi)$

Syzygies form an ideal of

$\mathbb{C}[x,y,z]$ (poly. ring finitely #vars)

ideals also finitely generated!

$\Rightarrow$ Syzygies are also finitely generated.

using modules (over R) we can get finite free resolution