Reynolds Operator & Finite Generation of Invariant Rings

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 ·

  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

  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!

$G = SL(3)$ $\quad V = \mathbb{C}^{\binom{n+2}{2}}$ $\quad x^a y^b z^c$ $\quad n = a+b+c$

[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

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

  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

(optional material)

- 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

(optional material)

- 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?

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

Averaging Operator (Reynolds operator in the finite case)

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

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

$(1)(2)(3)$
$(1\ 2)(3)$
$(1\ 3)(2)$
$(1\ 2\ 3)$
$(1\ 3\ 2)$
$(1)(2\ 3)$

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

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

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

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

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

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

$f : G \to G$ permutation

$g \mapsto hg$

$hg_1 = hg_2 \iff g_1 = g_2$

invariant!

$\downarrow$

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

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 $\rho(p) \neq 0$

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

$g(p+q) = g \circ p + g \circ q$

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 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!

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

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 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

$\underbrace{\mathbb{C}[\mathbf{x}]_0}_{\mathbb{C}}$

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)

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

$\longrightarrow$ 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

ρ 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!

$d = \deg(p) = \deg(a_i b_i) \geq \underbrace{\deg(a_i)}_{\geq 1} + \deg(\rho(b_i))$

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

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

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

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

This concludes the proof.