Reflection group counting and q-counting

Vic Reiner
Univ. of Minnesota
reiner@math.umn.edu

Summer School on
Algebraic and Enumerative Combinatorics
S. Miguel de Seide, Portugal
July 2-13, 2012

Outline

What is a reflection?

Definition

An element r in $GL_n(\mathbb{F})$ fr some field $\mathbb{F}$ is a reflection if

- it has finite order, and
- its fixed space

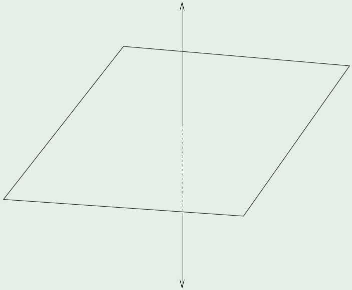
$$V^r = \{v \in V : r(v) = v\}$$

when acting on $V = \mathbb{F}^n$ is a hyperplane, that is, a linear subspace of codimension 1.

Orthogonal reflections

Example

Orthogonal reflections r through a hyperplane H in $\mathbb{R}^n$.



Unitary reflections

Example

Unitary reflections r = Matrices in $\mathbb{C}^{n\times n}$ diagonalizable to

$$\begin{bmatrix} \zeta & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

with ζ a root-of-unity in $\mathbb{C}$.

Transvections

Example

Transvections r = Matrices in $\mathbb{F}^{n \times n}$ with $\mathrm{char}(\mathbb{F}) = p$ similar to

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Not diagonalizable!

But can occur only in characteristic p.

Transvections

Example

Transvections r = Matrices in $\mathbb{F}^{n\times n}$ with $\mathrm{char}(\mathbb{F}) = p$ similar to

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Not diagonalizable!

But can occur only in characteristic p.

Transvections

Example

Transvections r = Matrices in $\mathbb{F}^{n\times n}$ with $\mathrm{char}(\mathbb{F}) = p$ similar to

$$\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

Not diagonalizable!
But can occur only in characteristic p.

The theorem of Shephard-Todd and Chevalley

Let W be a finite subgroup of $GL_n(\mathbb{C})$, acting on the polynomial algebra $S = \mathbb{C}[x_1, \ldots, x_n]$ by linear substitutions.

Theorem (Shephard-Todd, Chevalley (1955))

The W-invariant subalgebra $S^W = \mathbb{C}[f_1, \ldots, f_n]$ is a polynomial algebra if and only if W is generated by (unitary) reflections.

Such groups W are called complex reflection groups or unitary groups generated by reflections.

Same holds replacing $\mathbb{C}$ by fields $\mathbb{F}$ of characteristic zero, or even $\mathbb{F}$ in which $|W|$ is invertible.

The theorem of Shephard-Todd and Chevalley

Let W be a finite subgroup of $GL_n(\mathbb{C})$,
acting on the polynomial algebra $S = \mathbb{C}[x_1, \ldots, x_n]$
by linear substitutions.

Theorem (Shephard-Todd, Chevalley (1955))

The W-invariant subalgebra $S^W = \mathbb{C}[f_1, \ldots, f_n]$ is a polynomial algebra if and only if W is generated by (unitary) reflections.

Such groups W are called complex reflection groups
or unitary groups generated by reflections.

Same holds replacing $\mathbb{C}$ by fields $\mathbb{F}$ of characteristic zero,
or even $\mathbb{F}$ in which $|W|$ is invertible.

The theorem of Shephard-Todd and Chevalley

Let W be a finite subgroup of $GL_n(\mathbb{C})$,
acting on the polynomial algebra $S = \mathbb{C}[x_1, \ldots, x_n]$
by linear substitutions.

Theorem (Shephard-Todd, Chevalley (1955))

The W-invariant subalgebra $S^W = \mathbb{C}[f_1, \ldots, f_n]$ is a polynomial algebra if and only if W is generated by (unitary) reflections.

Such groups W are called complex reflection groups
or unitary groups generated by reflections.

Same holds replacing $\mathbb{C}$ by fields $\mathbb{F}$ of characteristic zero,
or even $\mathbb{F}$ in which $|W|$ is invertible.

The theorem of Shephard-Todd and Chevalley

Let W be a finite subgroup of $GL_n(\mathbb{C})$, acting on the polynomial algebra $S = \mathbb{C}[x_1, \ldots, x_n]$ by linear substitutions.

Theorem (Shephard-Todd, Chevalley (1955))

The W-invariant subalgebra $S^W = \mathbb{C}[f_1, \ldots, f_n]$ is a polynomial algebra if and only if W is generated by (unitary) reflections.

Such groups W are called complex reflection groups or unitary groups generated by reflections.

Same holds replacing $\mathbb{C}$ by fields $\mathbb{F}$ of characteristic zero, or even $\mathbb{F}$ in which $|W|$ is invertible.

The theorem of Shephard-Todd and Chevalley

Let W be a finite subgroup of $GL_n(\mathbb{C})$, acting on the polynomial algebra $S = \mathbb{C}[x_1, \ldots, x_n]$ by linear substitutions.

Theorem (Shephard-Todd, Chevalley (1955))

The W-invariant subalgebra $S^W = \mathbb{C}[f_1, \ldots, f_n]$ is a polynomial algebra if and only if W is generated by (unitary) reflections.

Such groups W are called complex reflection groups or unitary groups generated by reflections.

Same holds replacing $\mathbb{C}$ by fields $\mathbb{F}$ of characteristic zero, or even $\mathbb{F}$ in which $|W|$ is invertible.

Degrees

Proposition

When $S^W = \mathbb{F}[f_1, \ldots, f_n]$, although there are many choices of the basic invariants $f_1, \ldots, f_n$,

- *they can always be chosen homogeneous, and*
- *their degrees $d_1, d_2, \ldots, d_n$ are uniquely determined as a multiset.*

For example, they are determined by the Hilbert series

$$\mathrm{Hilb}(S^W, q) := \sum_{d \geq 0} q^d \cdot \dim_{\mathbb{F}}(S^W)_d$$

$$= \frac{1}{(1-q^{d_1})(1-q^{d_2})\cdots(1-q^{d_n})}.$$

Proof.

See the exercises. □

Proposition

When $S^W = \mathbb{F}[f_1, \ldots, f_n]$, although there are many choices of the basic invariants $f_1, \ldots, f_n$,

- *they can always be chosen homogeneous, and*
- *their degrees $d_1, d_2, \ldots, d_n$ are uniquely determined as a multiset.*

For example, they are determined by the Hilbert series

$$\mathrm{Hilb}(S^W, q) := \sum_{d \geq 0} q^d \cdot \dim_{\mathbb{F}}(S^W)_d$$
$$= \frac{1}{(1-q^{d_1})(1-q^{d_2}) \cdots (1-q^{d_n})}.$$

Proof.

See the exercises. □

Degrees

Proposition

When $S^W = \mathbb{F}[f_1, \ldots, f_n]$, although there are many choices of the basic invariants $f_1, \ldots, f_n$,

- *they can always be chosen homogeneous, and*
- *their degrees $d_1, d_2, \ldots, d_n$ are uniquely determined as a multiset.*

For example, they are determined by the Hilbert series

$$\mathrm{Hilb}(S^W, q) := \sum_{d \geq 0} q^d \cdot \dim_{\mathbb{F}}(S^W)_d$$

$$= \frac{1}{(1-q^{d_1})(1-q^{d_2})\cdots(1-q^{d_n})}.$$

Proof.

See the exercises. ☐

Degrees

Proposition

When $S^W = \mathbb{F}[f_1, \ldots, f_n]$, although there are many choices of the basic invariants $f_1, \ldots, f_n$,

- *they can always be chosen homogeneous, and*
- *their degrees $d_1, d_2, \ldots, d_n$ are uniquely determined as a multiset.*

For example, they are determined by the Hilbert series

$$\mathrm{Hilb}(S^W, q) := \sum_{d \geq 0} q^d \cdot \dim_{\mathbb{F}}(S^W)_d$$

$$= \frac{1}{(1-q^{d_1})(1-q^{d_2})\cdots(1-q^{d_n})}.$$

Proof.

See the exercises. □

Degrees

Proposition

When $S^W = \mathbb{F}[f_1, \ldots, f_n]$*, although there are many choices of the basic invariants* $f_1, \ldots, f_n$*,*

- *they can always be chosen homogeneous, and*
- *their degrees* $d_1, d_2, \ldots, d_n$ *are uniquely determined as a multiset.*

For example, they are determined by the Hilbert series

$$\mathrm{Hilb}(S^W, q) := \sum_{d \geq 0} q^d \cdot \dim_{\mathbb{F}}(S^W)_d$$

$$= \frac{1}{(1-q^{d_1})(1-q^{d_2})\cdots(1-q^{d_n})}.$$

Proof.

See the exercises. □

Definition

For W a subgroup of $GL_n(\mathbb{F})$ having S^W polynomial, define the degrees of W to be the multiset $(d_1, \ldots, d_n)$ of degrees of any homogenous invariants $f_1, \ldots, f_n$ for which $S^W = \mathbb{F}[f_1, \ldots, f_n]$.

Very important for us! Let's see some examples ...

Examples of degrees-symmetric groups

Example

The symmetric group $W = \mathfrak{S}_n$ inside $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ acts on $S = \mathbb{R}[x_1, \ldots, x_n]$ or $\mathbb{C}[x_1, \ldots, x_n]$ by permuting variables.

$$S^W = \mathbb{C}[e_1, \ldots, e_n]$$

where e_i are the elementary symmetric polynomials:

$$\begin{aligned} e_1 &= x_1 + x_2 + \cdots + x_n \\ e_1 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ &\vdots \\ e_n &= x_1x_2 \cdots x_n \end{aligned}$$

So $W = \mathfrak{S}_n$ has degrees $(d_1, d_2, \ldots, d_n) = (1, 2, \ldots, n)$.

Examples of degrees-symmetric groups

Example

The symmetric group $W = \mathfrak{S}_n$ inside $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ acts on $S = \mathbb{R}[x_1, \ldots, x_n]$ or $\mathbb{C}[x_1, \ldots, x_n]$ by permuting variables.

$$S^W = \mathbb{C}[e_1, \ldots, e_n]$$

where e_i are the elementary symmetric polynomials:

$$\begin{aligned} e_1 &= x_1 + x_2 + \cdots + x_n \\ e_1 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ &\vdots \\ e_n &= x_1 x_2 \cdots x_n \end{aligned}$$

So $W = \mathfrak{S}_n$ has degrees $(d_1, d_2, \ldots, d_n) = (1, 2, \ldots, n)$.

Examples of degrees-hyperoctahedral groups

Example

The hyperoctahedral group $W = \mathfrak{S}_n^{\pm}$ inside $GL_n(\mathbb{R})$ consists of all possible permutations and sign changes,

that is, all $n \times n$ monomial matrices with one nonzero entry, equal to ± 1, in each row and column.

$$S^W = \mathbb{C}[e_1(\mathbf{x}^2), \ldots, e_n(\mathbf{x}^2)]$$

where

$$f(\mathbf{x}^2) := f(x_1^2, \ldots, x_n^2).$$

So $W = \mathfrak{S}_n^{\pm}$ has degrees $(d_1, d_2, \ldots, d_n) = (2, 4, \ldots, 2n)$.

(See exercises.)

Examples of degrees-hyperoctahedral groups

Example

The hyperoctahedral group $W = \mathfrak{S}_n^{\pm}$ inside $GL_n(\mathbb{R})$ consists of all possible permutations and sign changes,
that is, all $n \times n$ monomial matrices with one nonzero entry, equal to ± 1, in each row and column.

$$S^W = \mathbb{C}[e_1(\mathbf{x}^2), \ldots, e_n(\mathbf{x}^2)]$$

where

$$f(\mathbf{x}^2) := f(x_1^2, \ldots, x_n^2).$$

So $W = \mathfrak{S}_n^{\pm}$ has degrees $(d_1, d_2, \ldots, d_n) = (2, 4, \ldots, 2n)$.

(See exercises.)

Examples of degrees-hyperoctahedral groups

Example

The hyperoctahedral group $W = \mathfrak{S}_n^{\pm}$ inside $GL_n(\mathbb{R})$ consists of all possible permutations and sign changes,
that is, all $n \times n$ monomial matrices with one nonzero entry, equal to ± 1, in each row and column.

$$S^W = \mathbb{C}[e_1(\mathbf{x}^2), \ldots, e_n(\mathbf{x}^2)]$$

where

$$f(\mathbf{x}^2) := f(x_1^2, \ldots, x_n^2).$$

So $W = \mathfrak{S}_n^{\pm}$ has degrees $(d_1, d_2, \ldots, d_n) = (2, 4, \ldots, 2n)$.

(See exercises.)

Examples of degrees-general linear groups

The finite general linear group $W = GL_n(\mathbb{F}_q)$ acts on $S = \mathbb{F}_q[x_1, \ldots, x_n]$ by $\mathbb{F}_q$-linear subsitutions of variables.

Theorem (L.E. Dickson 1911)

$$S^W = \mathbb{F}_q[D_{n,0}, D_{n,1}, \ldots, D_{n,n-1}]$$

where $D_{n,i}$ are the coefficients in the expansion

$$\prod_{(c_1,\ldots,c_n)\in\mathbb{F}_q^n} (t - (c_1 x_1 + \cdots c_n x_n)) = \sum_{i=0}^{n} t^{q^i} \cdot D_{n,i}(\mathbf{x}).$$

(See exercises.)

Here the Dickson polynomial $D_{n,i}$ has degree $q^n - q^i$,
so $W = GL_n(\mathbb{F}_q)$ has degrees $(q^n - q^{n-1}, \ldots, q^n - q^1, q^n - q^0)$.

Examples of degrees-general linear groups

The finite general linear group $W = GL_n(\mathbb{F}_q)$ acts on $S = \mathbb{F}_q[x_1, \ldots, x_n]$ by $\mathbb{F}_q$-linear subsitutions of variables.

Theorem (L.E. Dickson 1911)

$$S^W = \mathbb{F}_q[D_{n,0}, D_{n,1}, \ldots, D_{n,n-1}]$$

where $D_{n,i}$ are the coefficients in the expansion

$$\prod_{(c_1,\ldots,c_n)\in\mathbb{F}_q^n} (t - (c_1 x_1 + \cdots c_n x_n)) = \sum_{i=0}^{n} t^{q^i} \cdot D_{n,i}(\mathbf{x}).$$

(See exercises.)
Here the Dickson polynomial $D_{n,i}$ has degree $q^n - q^i$, so $W = GL_n(\mathbb{F}_q)$ has degrees $(q^n - q^{n-1}, \ldots, q^n - q^1, q^n - q^0)$.

Aside: characteristic p and Serre's theorem

This last example raises a question:
Which finite subgroups of $GL_n(\mathbb{F})$ with $|W|$ not invertible in $\mathbb{F}$ have S^W polynomial?

Not known in general, although one has this result:

Theorem (Serre 1967)

If S^W is polynomial, then W is generated by reflections (but one needs transvections, in general).

The converse fails, e.g. finite symplectic, orthogonal groups are generated by reflections, but have S^W not polynomial.

The cases where W acts irreducibly and S^W is polynomial were classified by Kemper and Malle in 1997.

Aside: characteristic p and Serre's theorem

This last example raises a question:
Which finite subgroups of $GL_n(\mathbb{F})$ with $|W|$ not invertible in $\mathbb{F}$ have S^W polynomial?

Not known in general, although one has this result:

Theorem (Serre 1967)

If S^W is polynomial, then W is generated by reflections (but one needs transvections, in general).

The converse fails, e.g. finite symplectic, orthogonal groups are generated by reflections, but have S^W not polynomial.

The cases where W acts irreducibly and S^W is polynomial were classified by Kemper and Malle in 1997.

Aside: characteristic p and Serre's theorem

This last example raises a question:
Which finite subgroups of $GL_n(\mathbb{F})$ with $|W|$ not invertible in $\mathbb{F}$ have S^W polynomial?

Not known in general, although one has this result:

Theorem (Serre 1967)

If S^W is polynomial, then W is generated by reflections (but one needs transvections, in general).

The converse fails, e.g. finite symplectic, orthogonal groups are generated by reflections, but have S^W not polynomial.

The cases where W acts irreducibly and S^W is polynomial were classified by Kemper and Malle in 1997.

Aside: characteristic p and Serre's theorem

This last example raises a question:
Which finite subgroups of $GL_n(\mathbb{F})$ with $|W|$ not invertible in $\mathbb{F}$ have S^W polynomial?

Not known in general, although one has this result:

Theorem (Serre 1967)

If S^W is polynomial, then W is generated by reflections (but one needs transvections, in general).

The converse fails, e.g. finite symplectic, orthogonal groups are generated by reflections, but have S^W not polynomial.

The cases where W acts irreducibly and S^W is polynomial were classified by Kemper and Malle in 1997.

The generalization of $n!$ is $d_1 d_2 \cdots d_n$

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$);
See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.

The generalization of $n!$ is $d_1 d_2 \cdots d_n$

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$);
See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.

The generalization of $n!$ is $d_1 d_2 \cdots d_n$

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$);
See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$);
See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.

The generalization of $n!$ is $d_1 d_2 \cdots d_n$

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$); See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.

The generalization of $n!$ is $d_1 d_2 \cdots d_n$

Here is a taste of the numerology of reflection groups.

Theorem

A finite subgroup W of $GL_n(\mathbb{F})$ with S^W polynomial and degrees $(d_1, \ldots, d_n)$ has $|W| = d_1 \cdots d_n$.

Proof.

Molien's theorem on $\mathrm{Hilb}(S^W, q)$ (at least for $\mathbb{F} = \mathbb{C}$);
See the exercises! □

Example

- $W = \mathfrak{S}_n$ has $|W| = n! = 1 \cdot 2 \cdots n$,
- $W = \mathfrak{S}_n^{\pm}$ has $|W| = 2^n \cdot n! = 2 \cdot 4 \cdots 2n$,
- $W = GL_n(\mathbb{F}_q)$ has $|W| = (q^n - 1)(q^n - q^1) \cdots (q^n - q^{n-1})$.