An evaluation approach to computing invariants rings of permutation groups

Nicolas Borie (joint work with Nicolas M. Thiéry)

Univ. Paris-Sud 11, Laboratoire de Mathématiques d’Orsay, Orsay Cedex, F-91405; CNRS, France

MEGA 2011       June 2, 2011
Motivations

Take advantage of symmetries in computations:

- Effective Galois theory
  [ Colin, Abdeljaoued, ... ]
- Solving system of polynomial equations
  [ Gatermann, Colin, Faugère, Rahmany, ... ]
- Isomorphism test of graphs
  [ Thiéry ]
- ...

The Typical need: compute generators of the invariant ring
Motivations

Take advantage of symmetries in computations:

- Effective Galois theory
  [ Colin, Abdeljaoued, ... ]
- Solving system of polynomial equations
  [ Gatermann, Colin, Faugère, Rahmany, ... ]
- Isomorphism test of graphs
  [ Thiéry ]
- ...

The Typical need: compute generators of the invariant ring
Take advantage of symmetries in computations:

- **Effective Galois theory**
  [ Colin, Abdeljaoued, ... ]

- **Solving system of polynomial equations**
  [ Gatermann, Colin, Faugère, Rahmany, ... ]

- **Isomorphism test of graphs**
  [ Thiéry ]

- ...

**The Typical need**: compute generators of the invariant ring
Motivations

Take advantage of symmetries in computations:

- Effective Galois theory
  [ Colin, Abdeljaoued, ... ]
- Solving system of polynomial equations
  [ Gatermann, Colin, Faugère, Rahmany, ... ]
- Isomorphism test of graphs
  [ Thiéry ]
- ...

The Typical need: compute generators of the invariant ring
Motivations

Take advantage of symmetries in computations:

- Effective Galois theory
  [ Colin, Abdeljaoued, ... ]
- Solving system of polynomial equations
  [ Gatermann, Colin, Faugère, Rahmany, ... ]
- Isomorphism test of graphs
  [ Thiéry ]
- ...

**The Typical need:** compute generators of the invariant ring
Our approach

The problem of constructing generators of the ring of invariants is usually dealt with Gröebner basis. Goals of our approach are:

- try to get results faster (if possible...)
- Take advantage of symmetries (instead of breaking them)
- Get a better control and understanding of the complexity
- Introduce more combinatorics in the problem
Our approach

The problem of constructing generators of the ring of invariants is usually dealt with Gröbner basis. Goals of our approach are:

- try to get results faster (if possible...)
- Take advantage of symmetries (instead of breaking them)
- Get a better control and understanding of the complexity
- Introduce more combinatorics in the problem
The problem of constructing generators of the ring of invariants is usually dealt with Gröbner basis. Goals of our approach are:

- try to get results faster (if possible...)
- Take advantage of symmetries (instead of breaking them)
- Get a better control and understanding of the complexity
- Introduce more combinatorics in the problem
Our approach

The problem of constructing generators of the ring of invariants is usually dealt with Gröbner basis. Goals of our approach are:

- try to get results faster (if possible...)
- Take advantage of symmetries (instead of breaking them)
- Get a better control and understanding of the complexity
- Introduce more combinatorics in the problem
Our approach

The problem of constructing generators of the ring of invariants is usually dealt with Gröbner basis. Goals of our approach are:

- try to get results faster (if possible...)
- Take advantage of symmetries (instead of breaking them)
- Get a better control and understanding of the complexity
- Introduce more combinatorics in the problem
1 Introduction

2 Quotienting by evaluation

3 Computing secondary invariants

4 Complexity

5 Further developments
Permutation groups

Definition (Symmetric group)

$S_n$: group of all permutations of the set $\{1, 2, \ldots, n\}$

- $S_n$ is of cardinality $n!$

Definition (Permutation group)

A subgroup $G$ of $S_n$

- Example: $C_3 = \langle (1, 2, 3) \rangle \subset S_3$
Definition (Symmetric group)

$S_n$: group of all permutations of the set \( \{1, 2, \ldots, n\} \)

- \( S_n \) is of cardinality \( n! \)

Definition (Permutation group)

A subgroup \( G \) of \( S_n \)

- Example: \( C_3 = \langle (1, 2, 3) \rangle \subset S_3 \)
### Definition (Symmetric group)

\( S_n \): group of all permutations of the set \( \{1, 2, \ldots, n\} \)

- \( S_n \) is of cardinality \( n! \)

### Definition (Permutation group)

A subgroup \( G \) of \( S_n \)

- Example: \( C_3 = \langle (1, 2, 3) \rangle \subset S_3 \)
# Permutation groups

**Definition (Symmetric group)**

$S_n$: group of all permutations of the set $\{1, 2, \ldots, n\}$

- $S_n$ is of cardinality $n!$

**Definition (Permutation group)**

A subgroup $G$ of $S_n$

- Example: $C_3 = \langle (1, 2, 3) \rangle \subset S_3$
Natural action on $\mathbb{K}[x]$

Let $\mathbb{K}$ be a field and $x = x_1, x_2, \ldots, x_n$. $\mathbb{K}[x]$ is the ring of multivariate polynomials in variables $x_1, x_2, \ldots, x_n$.

**Action of $S_n$ on $\mathbb{K}[x]$**

$$
\begin{pmatrix}
S_n,
\mathbb{K}[x]
\end{pmatrix} \rightarrow 
\begin{pmatrix}
\mathbb{K}[x]
\end{pmatrix}
$$

$$
\begin{pmatrix}
\sigma,
P(x_1, x_2, \ldots, x_n)
\end{pmatrix} \mapsto 
P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})
$$

**Example:**

$$(1, 2) \cdot (x_1^2 x_2 + x_1 x_3 - x_4^3) = x_2^2 x_1 + x_2 x_3 - x_4^3$$

$\mathbb{K}$ will be of characteristic 0 in this all this study.
Let $\mathbb{K}$ be a field and $\mathbf{x} = x_1, x_2, \ldots, x_n$. 
$\mathbb{K}[\mathbf{x}]$ is the ring of multivariate polynomials in variables $x_1, x_2, \ldots, x_n$.

**Action of $S_n$ on $\mathbb{K}[\mathbf{x}]$**

$$
\begin{pmatrix}
S_n, & \mathbb{K}[\mathbf{x}]
\end{pmatrix} \rightarrow \mathbb{K}[\mathbf{x}]
$$
$$
\begin{pmatrix}
\sigma, & P(x_1, x_2, \ldots, x_n)
\end{pmatrix} \mapsto P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})
$$

**Example:**

$$(1, 2) \cdot (x_1^2 x_2 + x_1 x_3 - x_4^3) = x_2^2 x_1 + x_2 x_3 - x_4^3$$

$\mathbb{K}$ will be of characteristic 0 in this all this study.
Introduction

Invariant polynomials

Definition

\( P \in \mathbb{K}[x] \) is invariant under \( G \) if \( \sigma \cdot P = P, \ \forall \sigma \in G \)

Fact: Products and sums of invariant polynomials are also invariant under the action of \( G \)

Definition

We denote \( \mathbb{K}[x]^G \) the ring of invariants polynomials under the action of \( G \).

\[ \mathbb{K}[x]^G = \{ P \in \mathbb{K}[x] | \forall \sigma \in G : \sigma \cdot P = P \} \]

Theorem (fundamental theorem of Symmetric polynomials)

Sym\((x)\) : The invariant ring of polynomial under \( S_n \).
Sym\((x) = \mathbb{K}[e_1, e_2, \ldots, e_n] \)
\{e_1, e_2, \ldots, e_n\} are the elementary symmetric polynomials.
Invariant polynomials

**Definition**

\( P \in K[x] \) invariant under \( G \) if \( \sigma \cdot P = P, \forall \sigma \in G \)

Fact: Products and sums of invariant polynomials are also invariant under the action of \( G \)

**Definition**

We denote \( K[x]^G \) The ring of invariants polynomials under the action of \( G \).

\[ K[x]^G = \{ P \in K[x] | \forall \sigma \in G : \sigma \cdot P = P \} \]

**Theorem (fundamental theorem of Symmetric polynomials)**

\( \text{Sym}(x) : The \text{ invariant ring of polynomial under } S_n \).
\( \text{Sym}(x) = K[e_1, e_2, \ldots, e_n] \)
\( \{e_1, e_2, \ldots, e_n\} \) are the elementary symmetric polynomials.
Invariant polynomials

Definition

\( P \in \mathbb{K}[x] \) \textit{invariant} under \( G \) if \( \sigma \cdot P = P, \forall \sigma \in G \)

Fact: Products and sums of invariant polynomials are also invariant under the action of \( G \)

Definition

We denote \( \mathbb{K}[x]^G \) The \textit{ring of invariants polynomials} under the action of \( G \).

\[ \mathbb{K}[x]^G = \{ P \in \mathbb{K}[x] | \forall \sigma \in G : \sigma \cdot P = P \} \]

Theorem (fundamental theorem of Symmetric polynomials)

\text{Sym}(x) : The \textit{invariant ring of polynomial under} \( S_n \).
\text{Sym}(x) = \mathbb{K}[e_1, e_2, \ldots, e_n]
\{e_1, e_2, \ldots, e_n\} \text{ are the elementary symmetric polynomials.}
Invariant polynomials

**Definition**

\( P \in \mathbb{K}[x] \) *invariant* under \( G \) if \( \sigma \cdot P = P, \forall \sigma \in G \)

**Fact** : Products and sums of invariant polynomials are also invariant under the action of \( G \)

**Definition**

We denote \( \mathbb{K}[x]^G \) The *ring of invariants polynomials* under the action of \( G \).

\[
\mathbb{K}[x]^G = \{ P \in \mathbb{K}[x] | \forall \sigma \in G : \sigma \cdot P = P \}
\]

**Theorem (fundamental theorem of Symmetric polynomials)**

\( \text{Sym}(x) \) : *The invariant ring of polynomial under} \ S_n \\
\( \text{Sym}(x) = \mathbb{K}[e_1, e_2, \ldots, e_n] \) \\
\{e_1, e_2, \ldots, e_n\} *are the elementary symmetric polynomials.*
Reynolds operator

**Definition (Reynolds operator)**

\[ R : \mathbb{K}[x] \longrightarrow \mathbb{K}[x]^G \]
\[ p \quad \longmapsto \quad \frac{1}{|G|} \sum_{g \in G} g \cdot p, \]

- \( R \) map is a graded projection onto \( \mathbb{K}[x]^G \).
- \( R \) fix pointwise invariant polynomials (and only them).
- \( R \) is a \( \mathbb{K}[x]^G \)-morphism.

In practice, The Reynold’s operator is used to build generating family of the ring of invariant.
Reynolds operator

Definition (Reynolds operator)

\[
R : \ K[x] \longrightarrow \ K[x]^G \\
p \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \ qua
Reynolds operator

Definition (Reynolds operator)

\[ R : K[x] \rightarrow K[x]^G \]

\[ p \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot p, \]

- \( R \) map is a graded projection onto \( K[x]^G \).
- \( R \) fix pointwise invariant polynomials (and only them).
- \( R \) is a \( K[x]^G \)-morphism.

In practice, The Reynold's operator is used to build generating family of the ring of invariant.
Reynolds operator

Definition (Reynolds operator)

\[ R : \mathbb{K}[x] \mapsto \mathbb{K}[x]^G \]

\[ p \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot p , \]

- \( R \) map is a graded projection onto \( \mathbb{K}[x]^G \).
- \( R \) fix pointwise invariant polynomials (and only them).
- \( R \) is a \( \mathbb{K}[x]^G \)-morphism.

In practice, The Reynold’s operator is used to build generating family of the ring of invariant.

Reynolds operator

**Definition (Reynolds operator)**

\[
R : \mathbb{K}[x] \mapsto \mathbb{K}[x]^G
\]

\[
p \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot p,
\]

- \( R \) map is a graded projection onto \( \mathbb{K}[x]^G \).
- \( R \) fix pointwise invariant polynomials (and only them).
- \( R \) is a \( \mathbb{K}[x]^G \)-morphism.

In practice, The Reynold’s operator is used to build generating family of the ring of invariant.
$\mathbb{K}[x]^G$ is a finitely generated algebra

Let $G$ be a permutation group, subgroup of $S_n$.

**Theorem**

*There exists $n$, but not $n + 1$, algebraically independent invariants.*

Equivalently, $\mathbb{K}[x]^G$ has Krull dimension $n$.

**Theorem (Noether)**

*For any $G$ subgroup of $S_n$, $\mathbb{K}[x]^G$ is generated as an algebra over $\mathbb{K}$ by a finite number of homogeneous invariants, of degree not exceeding $|G|$.***

**Theorem (Garsia, Stanton (1984))**

$\mathbb{K}[x]^G$ is generated by a finite number of homogeneous invariants, of degree not exceeding $\binom{n}{2}$.***
Hilbert series

\( \mathbb{K}[x]^G \) is a graded connected commutative algebra \( \mathbb{K}[x]^G = \bigoplus_{d \geq 0} \mathbb{K}[x]^G_d \).

It admits \textit{Hilbert series}:

\[
H(\mathbb{K}[x]^G, z) := \sum_{d=0}^{\infty} z^d \dim \mathbb{K}[x]^G_d.
\]

It can be calculated using Molien’s formula:

\[
\text{Theorem (Molien’s formula)}
\]

\[
H(\mathbb{K}[x]^G, z) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(\text{Id} - zM)}.
\]

Nicolas Borie

An evaluation approach to computing invariants rings
\[ K[x]^G \] is Cohen-Macaulay

**Theorem**

\[ K[x]^G \text{ is Cohen Macaulay} \]

Namely: \[ K[x]^G \text{ is a free module over } \text{Sym}(x) \text{ of rank } r = \frac{n!}{|G|} \]

We thus get the following direct sum

\[
K[x]^G = \bigoplus_{i=1}^{r} \eta_i K[e_1, e_2, \ldots, e_n]
\]

which is called an *Hironaka decomposition* of \( K[x]^G \).

**Goal**

*Construct all polynomials \( \eta_i, i \in \{1, 2, \ldots, r\} \) (named system of secondary invariants)*

Such a goal constitute a good test case for new approaches, as this is a typical computation in invariant theory.
\( \mathbb{K}[x]^G \) is Cohen-Macaulay

**Theorem**

\( \mathbb{K}[x]^G \) is Cohen Macaulay

Namely: \( \mathbb{K}[x]^G \) is a free module over \( \text{Sym}(x) \) of rank \( r = \frac{n!}{|G|} \)

We thus get the following direct sum

\[
\mathbb{K}[x]^G = \bigoplus_{i=1}^{r} \eta_i \mathbb{K}[e_1, e_2, \ldots, e_n]
\]

which is called an *Hironaka decomposition* of \( \mathbb{K}[x]^G \).

**Goal**

*Construct all polynomials \( \eta_i, i \in \{1, 2, \ldots, r\} \) (named system of secondary invariants)*

Such a goal constitutes a good test case for new approaches, as this is a typical computation in invariant theory.
\( \mathbb{K}[x]^G \) is Cohen-Macaulay

**Theorem**

\( \mathbb{K}[x]^G \) is Cohen Macaulay

Namely: \( \mathbb{K}[x]^G \) is a free module over \( \text{Sym}(x) \) of rank \( r = \frac{n!}{|G|} \)

We thus get the following direct sum

\[
\mathbb{K}[x]^G = \bigoplus_{i=1}^{r} \eta_i \mathbb{K}[e_1, e_2, \ldots, e_n]
\]

which is called an *Hironaka decomposition* of \( \mathbb{K}[x]^G \).

**Goal**

*Construct all polynomials \( \eta_i, i \in \{1, 2, \ldots, r\} \) (named system of secondary invariants)*

Such a goal constitute a good test case for new approaches, as this is a typical computation in invariant theory.
Let $G$ be the cyclic group of order 3: $C_3$, subgroup of $S_3$.

\[
\begin{align*}
e_1 &= x_1 + x_2 + x_3 \\
e_2 &= x_1x_2 + x_1x_3 + x_2x_3 \\
e_3 &= x_1x_2x_3
\end{align*}
\]

$e_1$, $e_2$, and $e_3$ generate $\mathbb{K}[x_1, x_2, x_3]^{S_3}$.

Quotienting the two Hilbert series, we get the polynomial

\[
H(\mathbb{K}[x]^G, z)/H(\text{Sym}(x), z) = 1 + z^3
\]

$\eta_1 = 1$

$\eta_2 = R(x_1^2x_2) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$

**Hironaka decomposition of $\mathbb{K}[x]^{C_3}$**

\[
\mathbb{K}[x]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus R(x_1^2x_2) \cdot \mathbb{K}[e_1, e_2, e_3]
\]
Example

Let $G$ be the cyclic group of order 3: $C_3$, subgroup of $S_3$.

$$e_1 = x_1 + x_2 + x_3$$
$$e_2 = x_1x_2 + x_1x_3 + x_2x_3$$
$$e_3 = x_1x_2x_3$$

$e_1$, $e_2$ and $e_3$ generate $\mathbb{K}[x_1, x_2, x_3]^{S_3}$.

Quotienting the two Hilbert series, we get the polynomial

$$H(\mathbb{K}[x]^G, z)/H(\text{Sym}(x), z) = 1 + z^3$$

$\eta_1 = 1$

$\eta_2 = R(x_1^2 x_2) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$

Hironaka decomposition of $\mathbb{K}[x]^{C_3}$

$$\mathbb{K}[x]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus R(x_1^2 x_2) \cdot \mathbb{K}[e_1, e_2, e_3]$$
Example

Let $G$ be the cyclic group of order 3: $C_3$, subgroup of $S_3$.

$$e_1 = x_1 + x_2 + x_3$$
$$e_2 = x_1x_2 + x_1x_3 + x_2x_3$$
$$e_3 = x_1x_2x_3$$

$e_1$, $e_2$, and $e_3$ generate $\mathbb{K}[x_1, x_2, x_3]^{S_3}$. Quotienting the two Hilbert series, we get the polynomial

$$H(\mathbb{K}[x]^G, z)/H(\text{Sym}(x), z) = 1 + z^3$$

$\eta_1 = 1$
$\eta_2 = R(x_1^2x_2) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$

Hironaka decomposition of $\mathbb{K}[x]^{C_3}$

$$\mathbb{K}[x]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus R(x_1^2x_2) \cdot \mathbb{K}[e_1, e_2, e_3]$$
Picture of the quotient

\[ \mathbb{K}[x] \]
An evaluation approach to computing invariants rings

Nicolas Borie
Picture of the quotient

\[ K[x] \]

Primary invariants

deg

\[
\begin{align*}
\text{deg 3} & \quad e_3 \\
\text{deg 2} & \quad e_2 \\
\text{deg 1} & \quad e_1 \\
\text{deg 0} &
\end{align*}
\]
Introduction Quotienting by evaluation Computing secondary invariants Complexity Further developments

Picture of the quotient

\[ \langle \text{Sym}(x)^+ \rangle^G \]

Primary invariants

\[ \mathbb{K}[x] \]

deg

deg 3

deg 2

deg 1

deg 0

e_3

e_2

e_1

Nicolas Borie

An evaluation approach to computing invariants rings
Picture of the quotient

\[ \langle \text{Sym}(x)^+ \rangle^G \]

Primary invariants

\[ \mathbb{K}[x]^G \]

\[ \mathbb{K}[x] \]
An evaluation approach to computing invariants rings
Introduction

Quotienting by evaluation

Computing secondary invariants

Complexity

Further developments

Picture of the quotient

\[ \langle \text{Sym}(x)^+ \rangle^G \]

Primary invariants

Secondary invariants

\[ \mathbb{K}[x]^G / \langle \text{Sym}(x)^+ \rangle^G \]

Nicolas Borie

An evaluation approach to computing invariants rings
Usual approach using Gröbner basis

A lot of implementations have been done in different software using (SAGBI)-Gröbner basis. PerMuVAR MuPAD, finvar Singular, MAGMA, ...

For all these implementations, given a group, it is hard to guess computational time...

In Singular:

... 
(8, 5): 19.10000000000001,
(8, 6): 2046.1400000000001,
(8, 7): day, # not ended
(8, 8): day, # not ended
(8, 9): 8.650000000000000,
(8, 10): 72.780000000000001,
(8, 11): 14.92,
(8, 12): day, # not ended
(8, 13): 10863.76,
(8, 14): day, # not ended
(8, 15): day, # not ended
...

Nicolas Borie
An evaluation approach to computing invariants rings
Usual approach using Gröbner basis

The classical problems of such implementation:

- They break the symmetries
- No really control on complexity
- No chance to introduce some combinatorics
Usual approach using Gröbner basis

The classical problems of such implementation:

- They break the symmetries
- No really control on complexity
- No chance to introduce some combinatorics
Usual approach using Gröbner basis

The classical problems of such implementation:
- They break the symmetries
- No really control on complexity
- No chance to introduce some combinatorics
Working by evaluation is a standard trick to compute in quotient, is this feasible in this context?

Choose a set of points $S \subset \mathbb{K}^n$.

Evaluation morphism $\Psi$

$\Psi : \mathbb{K}[x]^G \rightarrow (\mathbb{K}^{|S|},.)$

$P \mapsto (P(s))_{s \in S}$

where . is the pointwise product

Fact: $\Psi$ is an algebra morphism.

Goal: Choose $S$ on which the primary invariants vanish, but not the secondary invariants.
An approach by evaluation

Working by evaluation is a standard trick to compute in quotient, is this feasible in this context?

Choose a set of points $S \subset \mathbb{K}^n$.

**Evaluation morphism $\Psi$**

\[
\begin{align*}
\Psi : \quad \mathbb{K}[x]^G & \longrightarrow (\mathbb{K}^{|S|},.) \\
P & \mapsto (P(s))_{s \in S}
\end{align*}
\]

where . is the pointwise product

**Fact**: $\Psi$ is an algebra morphism.

**Goal**: Choose $S$ on which the primary invariants vanish, but not the secondary invariants.
Working by evaluation is a standard trick to compute in quotient, is this feasible in this context?

Choose a set of points $S \subset \mathbb{K}^n$.

**Evaluation morphism $\Psi$**

$$
\Psi : \mathbb{K}[x]^G \longrightarrow (\mathbb{K}^{|S|}, .)
$$

where . is the pointwise product

**Fact:** $\Psi$ is an algebra morphism.

**Goal:** Choose $S$ on which the primary invariants vanish, but not the secondary invariants.
Let $\rho$ be an $n$-th primitive roots of unity. For now, we assume $K$ contains $\rho$. (no loss of generality in non-modular case)

$$(x^n - 1) = \prod_{i=1}^{n} (x - \rho^i)$$

**Trick**: Expand on the right, write coefficient-root relations

| $e_1(1, \rho, \ldots, \rho^{n-1})$ | $= 0$ |
| $e_{n-1}(1, \rho, \ldots, \rho^{n-1})$ | $= 0$ |
| $e_n(1, \rho, \ldots, \rho^{n-1})$ | $= (-1)^{n+1}$ |
Elementary symmetric polynomials and roots of unity

Let $\rho$ be an $n$-th primitive roots of unity.
For now, we assume $\mathbb{K}$ contains $\rho$. (no loss of generality in non-modular case)

$$(x^n - 1) = \prod_{i=1}^{n} (x - \rho^i)$$

Trick: Expand on the right, write coefficient-root relations

| $e_1(1, \rho, \ldots, \rho^{n-1})$ | $= 0$ |
| $\vdots$ | \ $\vdots$ |
| $e_{n-1}(1, \rho, \ldots, \rho^{n-1})$ | $= 0$ |
| $e_n(1, \rho, \ldots, \rho^{n-1})$ | $= (-1)^{n+1}$ |
Choosing the good points

We define the identity point $A_{id} = (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$S_n$ acts on points living in $\mathbb{K}^n$. For $\sigma \in S_n$:

$$\sigma \cdot A_{id} = (\rho^{\sigma(1)-1}, \rho^{\sigma(2)-1}, \ldots, \rho^{\sigma(n)-1})$$

The orbit of $A_{id}$ under $S_n$ is of cardinality $n!$
Any symmetric polynomial is constant on this orbit.

**Invariants under $G$ are constant on $G$-orbits**

$$\forall A \in \mathbb{K}^n, \forall P \in \mathbb{K}[x]^G, \forall \sigma \in G : P(\sigma \cdot A) = P(A)$$

It is thus sufficient to take one point per coset
Choosing the good points

We define the identity point $A_{id} = (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$S_n$ acts on points living in $\mathbb{K}^n$. For $\sigma \in S_n$ :

$$\sigma \cdot A_{id} = (\rho^{\sigma(1)-1}, \rho^{\sigma(2)-1}, \ldots, \rho^{\sigma(n)-1})$$

The orbit of $A_{id}$ under $S_n$ is of cardinality $n$!

Any symmetric polynomial is constant on this orbit.

Invariants under $G$ are constant on $G$-orbits

$$\forall A \in \mathbb{K}^n, \forall P \in \mathbb{K}[x]^G, \forall \sigma \in G : P(\sigma \cdot A) = P(A)$$

It is thus sufficient to take one point per coset.
Choosing the good points

We define the identity point $A_{id} = (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$S_n$ acts on points living in $\mathbb{K}^n$. For $\sigma \in S_n$:

$$\sigma \cdot A_{id} = (\rho^{\sigma(1)-1}, \rho^{\sigma(2)-1}, \ldots, \rho^{\sigma(n)-1})$$

The orbit of $A_{id}$ under $S_n$ is of cardinality $n!$
Any symmetric polynomial is constant on this orbit.

**Invariants under $G$ are constant on $G$-orbits**

$$\forall A \in \mathbb{K}^n, \forall P \in \mathbb{K}[x]^G, \forall \sigma \in G : P(\sigma \cdot A) = P(A)$$

It is thus sufficient to take one point per coset.
Choosing the good points

We define the identity point $A_{id} = (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$S_n$ acts on points living in $\mathbb{K}^n$. For $\sigma \in S_n$:

$$\sigma \cdot A_{id} = (\rho^{\sigma(1)-1}, \rho^{\sigma(2)-1}, \ldots, \rho^{\sigma(n)-1})$$

The orbit of $A_{id}$ under $S_n$ is of cardinality $n!$
Any symmetric polynomial is constant on this orbit.

**Invariants under $G$ are constant on $G$-orbits**

$$\forall A \in \mathbb{K}^n, \forall P \in \mathbb{K}[x]^G, \forall \sigma \in G : P(\sigma \cdot A) = P(A)$$

It is thus sufficient to take one point per coset
Choosing the good points

Let $L$ be a set composed by representative of right cosets $S_n/G$. We define

**Definition (Key morphism $\Phi$)**

$$
\Phi : \ K[x]^G \rightarrow \ K_{\frac{n!}{|G|}}^{|P|}
$$

$$
P \mapsto (P(\sigma \cdot A_{id}))_{\sigma \in L}
$$

The key morphism $\Phi$ realizes:

**Proposition**

$\Phi$ is a surjective algebra morphism

**Remarks:**

- $\Phi(Sym(x)) = \langle (1,1,\ldots,1) \rangle_K$
- $dim(Im(\Phi)) = dim(K[x]^G / \langle Sym(x)^+ \rangle^G)$
Choosing the good points

Let \( L \) be a set composed by representative of right cosets \( S_n/G \). We define

**Definition (Key morphism \( \Phi \))**

\[
\Phi : \quad \mathbb{K}[x]^G \quad \longrightarrow \quad \mathbb{K}^{n!} \bigg/ \langle \text{Sym}(x)^+ \rangle^G
\]

\[ P \quad \longmapsto \quad (P(\sigma \cdot \text{Id}))_{\sigma \in L} \]

The key morphism \( \Phi \) realizes:

**Proposition**

\( \Phi \) is a surjective algebra morphism

**Remarks :**

- \( \Phi(\text{Sym}(x)) = \langle (1,1,\ldots,1) \rangle_{\mathbb{K}} \)
- \( \dim(\text{Im}(\Phi)) = \dim(\mathbb{K}[x]^G / \langle \text{Sym}(x)^+ \rangle^G) \)
Choosing the good points

Let \( L \) be a set composed by representative of right cosets \( S_n/G \). We define

**Definition (Key morphism \( \Phi \))**

\[
\Phi : \mathbb{K}[x]^G \rightarrow \mathbb{K}^{\frac{n!}{|G|}}
\]

\( P \mapsto (P(\sigma \cdot A_{id}))_{\sigma \in L} \)

The key morphism \( \Phi \) realizes:

**Proposition**

\( \Phi \) is a surjective algebra morphism

**Remarks**:

- \( \Phi(\text{Sym}(x)) = \langle (1,1,\ldots,1) \rangle_{\mathbb{K}} \)
- \( \dim(\text{Im}(\Phi)) = \dim(\mathbb{K}[x]^G / \langle \text{Sym}(x)^+ \rangle^G) \)
Choosing the good points

Let $L$ be a set composed by representative of right cosets $S_n/G$. We define

**Definition (Key morphism $\Phi$)**

$$\Phi : \mathbb{K}[x]^G \rightarrow \mathbb{K}^{\frac{n!}{|G|}}$$

$$P \mapsto (P(\sigma \cdot A_{id}))_{\sigma \in L}$$

The key morphism $\Phi$ realizes:

**Proposition**

$\Phi$ is a surjective algebra morphism

**Remarks:**

- $\Phi(\text{Sym}(x)) = \langle (1, 1, \ldots, 1) \rangle_{\mathbb{K}}$
- $\text{dim}(\text{Im}(\Phi)) = \text{dim}(\mathbb{K}[x]^G / \langle \text{Sym}(x)^+ \rangle^G)$
Calculation in the quotient

We recall the Hironaka decomposition

\[ K[x]^G = \bigoplus_{i=1}^{r} \eta_i K[e_1, e_2, \ldots, e_n] \]

Let \( S_d = \{ \eta_j \mid \deg(\eta_j) = d \} \).

\[ K[x]^G_d = \{ P \in K[x]^G \mid \deg(P) = d \} \]

**Theorem**

The key morphism \( \Phi \) realizes

- for \( 0 \leq d < n \):
  \[ \Phi(K[x]^G_d) = \Phi(\langle S_d \rangle_K) \]
- for \( d \geq n \):
  \[ \Phi(K[x]^G_d) = \Phi(\langle S_d \rangle_K) \oplus \Phi(K[x]^G_{d-n}) \]

Sketch of proof: use properties of \( \Phi \) and the Hironaka decomposition
Calculation in the quotient

We recall the Hironaka decomposition

\[ K[x]^G = \bigoplus_{i=1}^r \eta_i K[e_1, e_2, \ldots, e_n] \]

Let \( S_d = \{ \eta_j \mid \deg(\eta_j) = d \} \).

\[ K[x]^G_d = \{ P \in K[x]^G \mid \deg(P) = d \} \]

**Theorem**

*The key morphism \( \Phi \) realizes*

for \( 0 \leq d < n \):
\[ \Phi(K[x]^G_d) = \Phi(\langle S_d \rangle_K) \]

for \( d \geq n \):
\[ \Phi(K[x]^G_d) = \Phi(\langle S_d \rangle_K) \oplus \Phi(K[x]^G_{d-n}) \]

Sketch of proof: use properties of \( \Phi \) and the Hironaka decomposition
Calculation in the quotient

We recall the Hironaka decomposition

\[ \mathbb{K}[x]^G = \bigoplus_{i=1}^r \eta_i \mathbb{K}[e_1, e_2, \ldots, e_n] \]

Let \( S_d = \{ \eta_j \mid \deg(\eta_j) = d \} \).

\[ \mathbb{K}[x]_d^G = \{ P \in \mathbb{K}[x]^G \mid \deg(P) = d \} \]

**Theorem**

*The key morphism \( \Phi \) realizes*

for \( 0 \leq d < n \):

\[ \Phi(\mathbb{K}[x]_d^G) = \Phi(\langle S_d \rangle_\mathbb{K}) \]

for \( d \geq n \):

\[ \Phi(\mathbb{K}[x]^G) = \Phi(\langle S_d \rangle_\mathbb{K}) \oplus \Phi(\mathbb{K}[x]_{d-n}^G) \]

Sketch of proof: use properties of \( \Phi \) and the Hironaka decomposition
Example

Let $G$ be the cyclic group of order 3: $C_3$, subgroup of $S_3$.


\[
\frac{n!}{|G|} = \frac{3!}{3} = 2
\]

\[
L = \{A_{id} = (1, j, j^2), A_{(1,2)} = (j, 1, j^2)\}
\]

Deg 0 : $\Phi(1) = (1, 1)$, thus $\Phi(\mathbb{K}[x]^G_0) = \langle (1, 1) \rangle_{\mathbb{K}}$ and $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[x]^G_3) = \Phi(\mathbb{K}[x]^G_0) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$\Phi(R(x^3_1)) = \Phi(\frac{x_1^3 + x_2^3 + x_3^3}{3}) = (\frac{1^3 + j^3 + j^6}{3}, \frac{j^3 + 1^3 + j^6}{3}) = (1, 1)$

$\Phi(R(x^2_1x_2)) = \Phi(\frac{x_1^2x_2 + x_2^2x_3 + x_3^2x_1}{3}) = (\frac{j^4 + j^4 + j^4}{3}, \frac{j^2 + j^2 + j^5}{3}) = (j, j^2)$

($(j, j^2) \notin \Phi(\mathbb{K}[x]^G_0)) \Rightarrow (R(x^2_1x_2) \in S_3)$

$\eta_1 = 1$ and $\eta_2 = R(x^2_1x_2)$
def SecondaryInvariants(G):
    for each degree $d$ :  
        $(d)$ appearing in the secondary invariant polynomial
        $a_d = \dim(\mathbb{K}[x]^G_d)$
        $S_d \leftarrow \{\}; I_d \leftarrow \{\}$
        if $d \geq n$ :
            $V_d \leftarrow V_{d-n}$  
                (Correction due to $\Phi(e_n) = (-1)^{n+1}$)
        else :
            $V_d \leftarrow \{\vec{0}\}$  
                ($V_d = \Phi(\mathbb{K}[x]^G_d)$ at the end of the loop)
        $D \leftarrow a_d + \dim(V_d)$  
                (Correction due to $\Phi(e_n) = (-1)^{n+1}$)
    for $(\eta, \eta') \in S_k \times I_l$ such that $k + l = d$ :
        if $\Phi(\eta)\Phi(\eta') \notin V_d$ :  
            (Products of smaller secondaries)
            $S_d \leftarrow S_d \cup \{\eta\eta'\}$
            $V_d \leftarrow V_d \oplus \langle \Phi(\eta\eta') \rangle_{\mathbb{K}}$
        while $\dim(V_d) < D$ :  
            (completing with irreducibles)
            $P \leftarrow$ good candidate to be secondary invariant
            if $\Phi(P) \notin V_d$ :
                $I_d \leftarrow I_d \cup \{P\}$
                $S_d \leftarrow S_d \cup \{P\}$
                $V_d \leftarrow V_d \oplus \langle \Phi(P) \rangle_{\mathbb{K}}$
    return ($\{S_0, S_1, S_2, \ldots \}$, $\{I_0, I_1, I_2, \ldots \}$)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)
- Interface to Singular / Magma / MuPAD (Checking Results)
- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox: Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)
- The algorithm by evaluation (around 500 lines of code with documentation)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)

- Interface to Singular / Magma / MuPAD (Checking Results)

- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox: Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)
- The algorithm by evaluation (around 500 lines of code with documentation)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)

- Interface to Singular / Magma / MuPAD (Checking Results)

- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox: Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)

- The algorithm by evaluation (around 500 lines of code with documentation)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)
- Interface to Singular / Magma / MuPAD (Checking Results)
- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox : Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)
- The algorithm by evaluation (around 500 lines of code with documentation)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)
- Interface to Singular / Magma / MuPAD (Checking Results)
- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox : Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)
- The algorithm by evaluation (around 500 lines of code with documentation)
Implementation in Sage

What was provided in Sage:

- An interface to GAP:
  - A database of Transitive Groups (Benchmarks)
  - Right Cosets for quotient (Evaluation points)
  - Fast computation of Moliens series (dimension bounds)
  - Stabilizer chain (Enumeration)
- Interface to Singular / Magma / MuPAD (Checking Results)
- Cyclotomic fields
  - Fast basic arithmetic (Evaluation)
  - Linear algebra (Linbox : Multi-modular possibility)

What we did implement:

- Orderly generation of integer lists modulo the action of a permutation group. (1000 lines of code)
- The algorithm by evaluation (around 500 lines of code with documentation)
Turning on the verbose

sage: G = TransitiveGroup(8,42)
sage: G.cardinality()
288
sage: I = InvariantRingPermutationGroup(G, QQ)
sage: I.secondary_invariants_series()
z^28 + z^26 + z^25 + 3*z^24 + 2*z^23 + 5*z^22 + 4*z^21 + 7*z^20 + 6*z^19 + 9*z^18 + 7*z^17 + 11*z^16 + 8*z^15 + 10*z^14 + 8*z^13 + 11*z^12 + 7*z^11 + 9*z^10 + 6*z^9 + 7*z^8 + 4*z^7 + 5*z^6 + 2*z^5 + 3*z^4 + z^3 + z^2 + 1
sage: I.secondary_invariants(verbos=True)
Initialization of secondary of degree 0

Secondaries of degree 1 :
     We must search 0 secondary invariants

Secondaries of degree 2 :
     We must search 1 secondary invariants
     Research of product of secondaries of degree smaller
     Research now to complete with new irreducible secondaries
     New irreducible [2]
     ...

Nicolas Borie
An evaluation approach to computing invariants rings
Turning on the verbose

Secondaries of degree 6:

We must search 5 secondary invariants

Research of product of secondaries of degree smaller

Add product $[2, 4]$
Add product $[2, 5]$
Register new relation: $[3, 3]$
Add product $[2, 2, 2]$

Research now to complete with new irreducible secondaries

$(5, 1, 0, 0, 0, 0, 0, 0)$ is not a good secondary invariant
$(5, 0, 0, 1, 0, 0, 0, 0)$ is not a good secondary invariant
New irreducible $[7]$

$(4, 1, 1, 0, 0, 0, 0, 0)$ is not a good secondary invariant
$(4, 1, 0, 1, 0, 0, 0, 0)$ is not a good secondary invariant
$(4, 0, 0, 2, 0, 0, 0, 0)$ is not a good secondary invariant
$(4, 0, 0, 1, 1, 0, 0, 0)$ is not a good secondary invariant
$(3, 3, 0, 0, 0, 0, 0, 0)$ is not a good secondary invariant
New irreducible $[8]$

....
sage: D = I.irreducible_secondary_invariants()
sage: for i in D:
    if len(D[i]) >= 1:
        print (i, D[i])
....:
(0, [[[0, 0, 0, 0, 0, 0, 0, 0]]])
(2, [[[1, 0, 0, 0, 0, 0, 0, 0]]])
(3, [[[2, 0, 0, 0, 0, 0, 0, 0]]])
(4, [[[3, 0, 0, 0, 0, 0, 0, 0], [[2, 0, 0, 0, 0, 0, 0, 0]]])
(5, [[[4, 0, 0, 0, 0, 0, 0, 0]]])
(6, [[[4, 0, 0, 0, 0, 0, 0, 0], [[3, 0, 0, 0, 0, 0, 0, 0]]])
(7, [[[4, 0, 0, 0, 0, 0, 0, 0]]])
(8, [[[5, 0, 0, 0, 0, 0, 0, 0]]])
(9, [[[6, 0, 0, 0, 0, 0, 0, 0]]])
(10, [[[7, 0, 0, 0, 0, 0, 0, 0]]])
Rough complexity analysis

Proposition

Using $\Phi$, computing secondary invariants presents a cost bounded by $O(n!^2 + n!^3/|G|^2)$ arithmetic operations in $\mathbb{K}$.

Sketch of proof:

- Number of evaluation points: $n!/|G|$.
- Number of orbit sums of monomials under staircase $n!$.
- Evaluation of the orbit sums: $O(\frac{n!}{|G|} n! |G| = (n!)^2)$.
- Gauss Elimination: $O(n!^3/|G|^2)$ arithmetic operations (Echelonize a matrix of size $(n!, n!/|G|)$ of rank $n!/|G|$).

Nicolas Borie

An evaluation approach to computing invariants rings
Rough complexity analysis

**Proposition**

*Using Φ, computing secondary invariants presents a cost bounded by $O(n!^2 + n!^3/|G|^2)$ arithmetic operations in $K$.*

**Sketch of proof:**

- Number of evaluation points: $\frac{n!}{|G|}$.
- Number of orbit sums of monomials under staircase $n!$.
- Evaluation of the orbit sums: $O(\frac{n!}{|G|} n!|G| = (n!)^2)$.
- Gauss Elimination: $O(n!^3/|G|^2)$ arithmetic operations (Echelonize a matrix of size $(n!, n!/|G|)$ of rank $n!/|G|$).
Rough complexity analysis

**Proposition**

*Using \( \Phi \), computing secondary invariants presents a cost bounded by* \( O(n!^2 + n!^3/|G|^2) \) *arithmetic operations in \( \mathbb{K} \).*

**Sketch of proof:**

- **Number of evaluation points:** \( \frac{n!}{|G|} \).
- **Number of orbit sums of monomials under staircase** \( n! \).
- **Evaluation of the orbit sums:** \( O\left(\frac{n!}{|G|} \cdot n! \cdot |G| = (n!)^2\right) \)
- **Gauss Elimination:** \( O(n!^3/|G|^2) \) arithmetic operations
  
  (Echelonize a matrix of size \( (n!, n!/|G|) \) of rank \( n!/|G| \))
Proposition

Using $\Phi$, computing secondary invariants presents a cost bounded by $O(n!^2 + n!^3/|G|^2)$ arithmetic operations in $\mathbb{K}$.

Sketch of proof:

- Number of evaluation points: $\frac{n!}{|G|}$.
- Number of orbit sums of monomials under staircase $n!$.
- Evaluation of the orbit sums: $O\left(\frac{n!}{|G|} \cdot n! |G| = (n!)^2\right)$.
- Gauss Elimination: $O(n!^3/|G|^2)$ arithmetic operations.
  (Echelonize a matrix of size $(n!, n!/|G|)$ of rank $n!/|G|$)
Rough complexity analysis

**Proposition**

*Using $\Phi$, computing secondary invariants presents a cost bounded by $O(n!^2 + n!^3/|G|^2)$ arithmetic operations in $K$.***

**Sketch of proof:**

- Number of evaluation points: $n!/|G|$.
- Number of orbit sums of monomials under staircase $n!$.
- Evaluation of the orbit sums: $O(n!/|G| \cdot n!/|G| = (n!)^2)$.
- Gauss Elimination: $O(n!^3/|G|^2)$ arithmetic operations (Echelonize a matrix of size $(n!, n!/|G|)$ of rank $n!/|G|$).
Comparative benchmark with Singular
Complexity by number of evaluation points

- $n! / |G|$
- $\leq 100 \mu s$
- $100 \mu s$
- $100 s$
- $10 s$
- $1 s$
- $100 ms$
- $10 ms$
- $1 ms$
- $100 ks$
- $10 ks$
- $1 ks$
- $100 s$
- $10 s$
- $1 s$
- $100 ms$
- $10 ms$
- $1 ms$
- $100 \mu s$
- $\leq 100 \mu s$
- $n! / |G|$
- $\geq 1 \text{ day}$
- $1 \text{ day}$
- $1 \text{ hour}$
- $1 \text{ minute}$
- $1 \text{ second}$
- $10^{-1}$
- $10^{-2}$
- $10^{-3}$
- $10^{-4}$
- $10^{-5}$

Nicolas Borie
An evaluation approach to computing invariants rings
Further developments

Problem

Evaluations are vectors with $\frac{n!}{|G|}$ coordinates. In practice, we never build a basis of such dimension because the calculation is degree by degree.

For $C_7 = \langle (1, 2, 3, 4, 5, 6, 7) \rangle$.
$|C_7| = 7$. The Noether bound for secondary invariant is thus 7. 100 points (instead of $6! = 720$) were enough to compute irreducible secondaries for $C_7$.

Question

Is there a way to reduce the number of evaluation points?
Further developments

Problem

Evaluations are vectors with \( \frac{n!}{|G|} \) coordinates. In practice, we never build a basis of such dimension because the calculation is degree by degree.

For \( C_7 = \langle (1, 2, 3, 4, 5, 6, 7) \rangle \).

\(|C_7| = 7.\) The Noether bound for secondary invariant is thus 7.

100 points (instead of \( 6! = 720 \)) were enough to compute irreducible secondaries for \( C_7 \).

Question

Is there a way to reduce the number of evaluation points?
### Problem

*Construct invariants with nice properties under evaluation by $\Phi$ (sparsity, ...). A promising starting point are double Schubert polynomials, as they form a basis of $\mathbb{K}[x]$ as $\text{Sym}(x)$-module whose image under $\Phi$ is triangular.*

### Problem (Dream)

*Give a combinatorial description of secondary invariants.*

The Dream problem is only known for parabolic subgroups of $S_n$ (Garcia, Stanton (1984)).
Thank you!

Acknowledgments:
National Science Foundation Grant No. DMS-0821725
(1 full month over 4 CPU at 2,4 Ghz on machine ‘sage‘ at Seattle.)
This research was driven by computer exploration using the open-source mathematical software Sage and its algebraic combinatorics features developed by the Sage-Combinat community.