Calcul des invariants des groupes de permutations par transformée de Fourier

Nicolas Borie

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

2 février 2012
JCB 2012

Les invariants algébriques : histoire et philosophie

.: Exploiter les symétries :.

"Les invariants décrivent les propriétés intrinsèques des objets"

Étant donné un ensemble de symétries, les *invariants* sont des fonctions constantes sur chaque classe d'équivalence

L'enjeu est de trouver des invariants qui séparent autant de classes que possible

Depuis un siècle et demi : Considération de l'ensemble de tous les invariants, description algébrique de sa structure

Depuis environ 20 ans : Théorie des invariants effective

Motivations

Exploiter les symétries dans les problèmes de calculs formels:

Applications remarquables:
Géométrie[*Computational Invariant Theory*, Derksen, Kemper],
Algèbre linéaire,
Vision par ordinateur,
Théorie des graphes[Thiéry],
Codage,
Théorie de Galois effective[Colin, Abdeljaouad, ...],
Résolution de systèmes d'équations polynomiales avec symétries
[Gatermann, Colin, Faugère, Rahmany, ...],
Informatique quantique...

Besoin classique: construire les générateurs de l'anneau des invariants

Motivations

Exploiter les symétries dans les problèmes de calculs formels:

Applications remarquables:
Géométrie[*Computational Invariant Theory*, Derksen, Kemper],
Algèbre linéaire,
Vision par ordinateur,
Théorie des graphes[Thiéry],
Codage,
Théorie de Galois effective[Colin, Abdeljaouad, ...],
Résolution de systèmes d'équations polynomiales avec symétries
[Gatermann, Colin, Faugère, Rahmany, ...],
Informatique quantique...

Besoin classique: construire les générateurs de l'anneau des invariants

L'approche par évaluation

La construction d'un système de générateurs de l'anneau des invariants est usuellement obtenue par élimination (Base de Gröbner et ses variantes)

Question

Qu'attendre des techniques d'évaluation:

- *Exploiter les symétries (au lieu de les casser)*
  - *Résultats plus rapides*
  - *Meilleur contrôle de la complexité des algorithmes*
- *Introduire de la combinatoire dans le problème*

Cas test de cette étude

- Construction des générateurs et invariants secondaires
- Groupes de permutations
- Caractéristique 0

L'approche par évaluation

La construction d'un système de générateurs de l'anneau des invariants est usuellement obtenue par élimination (Base de Gröbner et ses variantes)

Question

Qu'attendre des techniques d'évaluation:

- *Exploiter les symétries (au lieu de les casser)*
  - *Résultats plus rapides*
  - *Meilleur contrôle de la complexité des algorithmes*
- *Introduire de la combinatoire dans le problème*

Cas test de cette étude

- Construction des générateurs et invariants secondaires
- Groupes de permutations
- Caractéristique 0

L'approche par évaluation

La construction d'un système de générateurs de l'anneau des invariants est usuellement obtenue par élimination (Base de Gröbner et ses variantes)

Question

Qu'attendre des techniques d'évaluation:

- *Exploiter les symétries (au lieu de les casser)*
  - *Résultats plus rapides*
  - *Meilleur contrôle de la complexité des algorithmes*
- *Introduire de la combinatoire dans le problème*

Cas test de cette étude

- Construction des générateurs et invariants secondaires
- Groupes de permutations
- Caractéristique 0

L'approche par évaluation

La construction d'un système de générateurs de l'anneau des invariants est usuellement obtenue par élimination (Base de Gröbner et ses variantes)

Question

Qu'attendre des techniques d'évaluation:

- *Exploiter les symétries (au lieu de les casser)*
  - *Résultats plus rapides*
  - *Meilleur contrôle de la complexité des algorithmes*
- *Introduire de la combinatoire dans le problème*

Cas test de cette étude

- Construction des générateurs et invariants secondaires
- Groupes de permutations
- Caractéristique 0

L'approche par évaluation

La construction d'un système de générateurs de l'anneau des invariants est usuellement obtenue par élimination (Base de Gröbner et ses variantes)

Question

Qu'attendre des techniques d'évaluation:

- *Exploiter les symétries (au lieu de les casser)*
  - *Résultats plus rapides*
  - *Meilleur contrôle de la complexité des algorithmes*
- *Introduire de la combinatoire dans le problème*

Cas test de cette étude

- Construction des générateurs et invariants secondaires
- Groupes de permutations
- Caractéristique 0

Groupes de permutations

Définition (Groupe symétrique)

$\mathfrak{S}_n$: groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$

- $|\mathfrak{S}_n| = n!$

Définition (Groupe de permutations)

Sous groupe G de $\mathfrak{S}_n$

- Exemple : $C_3 = \langle (1, 2, 3) \rangle \subset \mathfrak{S}_3$

Groupes de permutations

Définition (Groupe symétrique)

$\mathfrak{S}_n$: groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$

- $|\mathfrak{S}_n| = n!$

Définition (Groupe de permutations)

Sous groupe G de $\mathfrak{S}_n$

- Exemple : $C_3 = \langle (1, 2, 3) \rangle \subset \mathfrak{S}_3$

Groupes de permutations

Définition (Groupe symétrique)

$\mathfrak{S}_n$: groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$

- $|\mathfrak{S}_n| = n!$

Définition (Groupe de permutations)

Sous groupe G de $\mathfrak{S}_n$

- Exemple : $C_3 = \langle (1, 2, 3) \rangle \subset \mathfrak{S}_3$

Groupes de permutations

Définition (Groupe symétrique)

$\mathfrak{S}_n$: groupe des permutations de l'ensemble $\{1, 2, \ldots, n\}$

- $|\mathfrak{S}_n| = n!$

Définition (Groupe de permutations)

Sous groupe G de $\mathfrak{S}_n$

- Exemple : $C_3 = \langle (1, 2, 3) \rangle \subset \mathfrak{S}_3$

Action naturelle sur $\mathbb{K}[\mathbf{x}]$

$\mathbb{K}$ corps de caractéristique 0 et $\mathbf{x} := (x_1, x_2, \ldots, x_n)$
$\mathbb{K}[\mathbf{x}]$: anneau des polynômes en les variables $x_1, x_2, \ldots, x_n$

Action d'une permutation σ sur un polynôme P

$$\sigma \cdot P(x_1, x_2, \ldots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Exemple :

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

Action naturelle sur $\mathbb{K}[\mathbf{x}]$

$\mathbb{K}$ corps de caractéristique 0 et $\mathbf{x} := (x_1, x_2, \ldots, x_n)$
$\mathbb{K}[\mathbf{x}]$: anneau des polynômes en les variables $x_1, x_2, \ldots, x_n$

Action d'une permutation σ sur un polynôme P

$$\sigma \cdot P(x_1, x_2, \ldots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

Exemple :

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

Polynômes invariants

Définition

P: invariant sous G si $\sigma \cdot P = P, \ \forall \sigma \in G$

Remarque: Les produits et sommes d'invariants sont invariants

Définition

Anneau des polynômes invariants sous l'action de G:

$$\mathbb{K}[\mathbf{x}]^G = \{P \in \mathbb{K}[\mathbf{x}] \mid \sigma \cdot P = P, \ \forall \sigma \in G\}$$

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[\mathbf{x}]^{\mathfrak{S}_n}$: anneau des polynômes symétriques
$\{e_1, e_2, \ldots, e_n\}$: polynômes symétriques élémentaires

Théorème (Théorème fondamental des polynômes symétriques)

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[e_1, e_2, \ldots, e_n]$

Polynômes invariants

Définition

P: invariant sous G si $\quad \sigma \cdot P = P, \ \forall \sigma \in G$

Remarque: Les produits et sommes d'invariants sont invariants

Définition

Anneau des polynômes invariants sous l'action de G:

$$\mathbb{K}[\mathbf{x}]^G = \{P \in \mathbb{K}[\mathbf{x}] \mid \sigma \cdot P = P, \ \forall \sigma \in G\}$$

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[\mathbf{x}]^{\mathfrak{S}_n}$: anneau des polynômes symétriques
$\{e_1, e_2, \ldots, e_n\}$: polynômes symétriques élémentaires

Théorème (Théorème fondamental des polynômes symétriques)

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[e_1, e_2, \ldots, e_n]$

Polynômes invariants

Définition

P: invariant sous G si $\quad \sigma \cdot P = P, \ \forall \sigma \in G$

Remarque: Les produits et sommes d'invariants sont invariants

Définition

Anneau des polynômes invariants sous l'action de G:

$$\mathbb{K}[\mathbf{x}]^G = \{P \in \mathbb{K}[\mathbf{x}] \mid \sigma \cdot P = P, \ \forall \sigma \in G\}$$

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[\mathbf{x}]^{\mathfrak{S}_n}$: anneau des polynômes symétriques
$\{e_1, e_2, \ldots, e_n\}$: polynômes symétriques élémentaires

Théorème (Théorème fondamental des polynômes symétriques)

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[e_1, e_2, \ldots, e_n]$

Polynômes invariants

Définition

P: invariant sous G si $\quad \sigma \cdot P = P, \ \forall \sigma \in G$

Remarque: Les produits et sommes d'invariants sont invariants

Définition

Anneau des polynômes invariants sous l'action de G:

$$\mathbb{K}[\mathbf{x}]^G = \{P \in \mathbb{K}[\mathbf{x}] \mid \sigma \cdot P = P, \ \forall \sigma \in G\}$$

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[\mathbf{x}]^{\mathfrak{S}_n}$: anneau des polynômes symétriques
$\{e_1, e_2, \ldots, e_n\}$: polynômes symétriques élémentaires

Théorème (Théorème fondamental des polynômes symétriques)

$\mathrm{Sym}(\mathbf{x}) = \mathbb{K}[e_1, e_2, \ldots, e_n]$

Sommes sur orbite

$\mathbf{v} := (v_1, \ldots, v_n)$ vecteur d'entiers représentant un monôme.

Définition (Somme sur orbite)

$$\begin{array}{rccc} \sum_{orb(G)} : & \mathcal{M} & \longrightarrow & \mathbb{K}[\mathbf{x}]^G \\ & \mathbf{x}^{\mathbf{v}} & \longmapsto & \sum_{\mathbf{w} \in \{\sigma \cdot \mathbf{v} | \sigma \in G\}} \mathbf{x}^{\mathbf{w}} \end{array}$$

Utilisation:

- Fabriquer des invariants
- Construire des familles génératrices d'invariants
- L'ensemble des sommes sur orbite forme une base de $\mathbb{K}[\mathbf{x}]^G$

Sommes sur orbite

$\mathbf{v} := (v_1, \ldots, v_n)$ vecteur d'entiers représentant un monôme.

Définition (Somme sur orbite)

$$\begin{array}{rccc} \sum_{orb(G)} : & \mathcal{M} & \longrightarrow & \mathbb{K}[\mathbf{x}]^G \\ & \mathbf{x}^{\mathbf{v}} & \longmapsto & \sum_{\mathbf{w} \in \{\sigma \cdot \mathbf{v} | \sigma \in G\}} \mathbf{x}^{\mathbf{w}} \end{array}$$

Utilisation:

- Fabriquer des invariants
- Construire des familles génératrices d'invariants
- L'ensemble des sommes sur orbite forme une base de $\mathbb{K}[\mathbf{x}]^G$

Graduation et séries de Hilbert

$\mathbb{K}[\mathbf{x}]^G$: algèbre graduée commutative et connexe $\mathbb{K}[\mathbf{x}]^G = \bigoplus_{d \geq 0} \mathbb{K}[\mathbf{x}]^G_d$.

Série de Hilbert:

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

Facilement calculable:

Théorème (Formule de Molien / énumération de Pólya)

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

Optimisations:

- Somme sur les classes de conjugaison de G
- Type cyclique

Graduation et séries de Hilbert

$\mathbb{K}[\mathbf{x}]^G$: algèbre graduée commutative et connexe $\mathbb{K}[\mathbf{x}]^G = \bigoplus_{d \geq 0} \mathbb{K}[\mathbf{x}]^G_d$.

Série de Hilbert:

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

Facilement calculable:

Théorème (Formule de Molien / énumération de Pólya)

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

Optimisations:

- Somme sur les classes de conjugaison de G
- Type cyclique

Vecteurs d'entiers modulo un groupe de permutations

Le calcul des sommes sur orbites soulève le problème suivant :

Problème

Énumérer les vecteurs d'entiers $\mathbf{v} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ *en n'en gardant qu'un seul par orbite sous l'action de* G*.*

Contient l'énumération des graphes à un isomorphisme près

Des approches algorithmiques connues: génération de manière ordonnée

Définition

Un vecteur $\mathbf{v}$ *est canonique sous l'action de* G *s'il est maximum pour l'ordre lexicographique dans son orbite.*

Vecteurs d'entiers modulo un groupe de permutations

Le calcul des sommes sur orbites soulève le problème suivant :

Problème

Énumérer les vecteurs d'entiers $\mathbf{v} := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ *en n'en gardant qu'un seul par orbite sous l'action de* G*.*

Contient l'énumération des graphes à un isomorphisme près

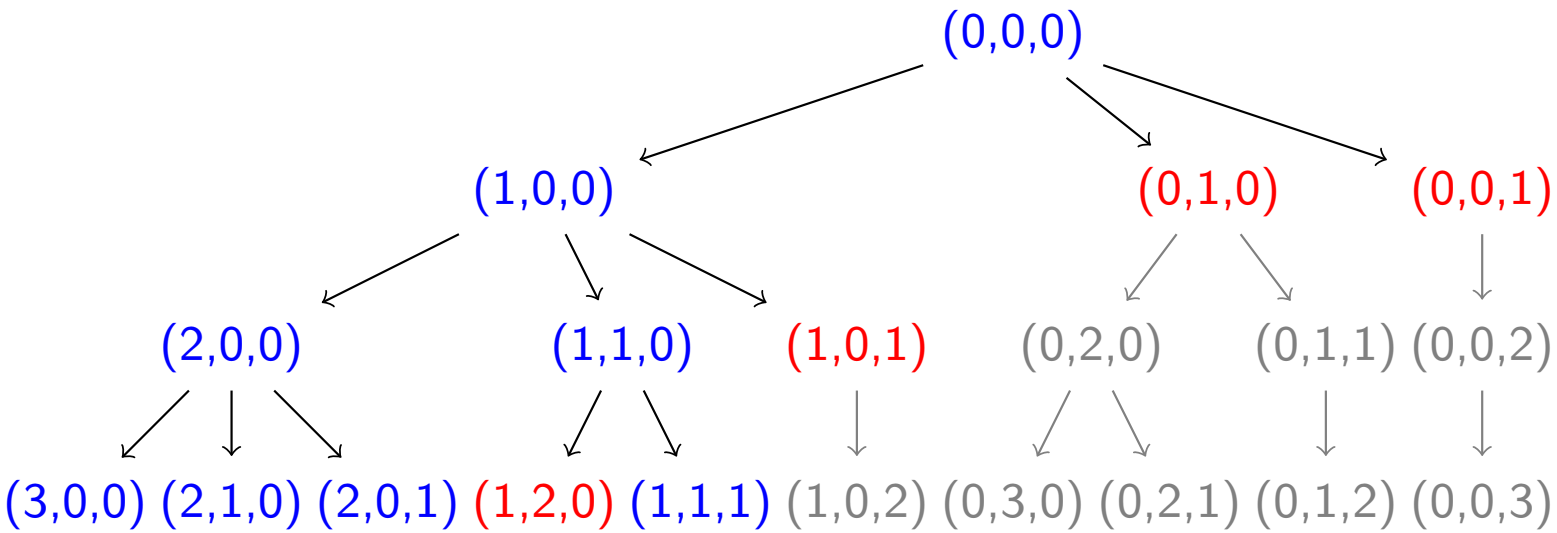
Des approches algorithmiques connues: génération de manière ordonnée

Définition

Un vecteur $\mathbf{v}$ *est canonique sous l'action de* G *s'il est maximum pour l'ordre lexicographique dans son orbite.*

Vecteurs d'entiers modulo un groupe de permutations

Exemple $C_3 = \langle (1,2,3) \rangle$

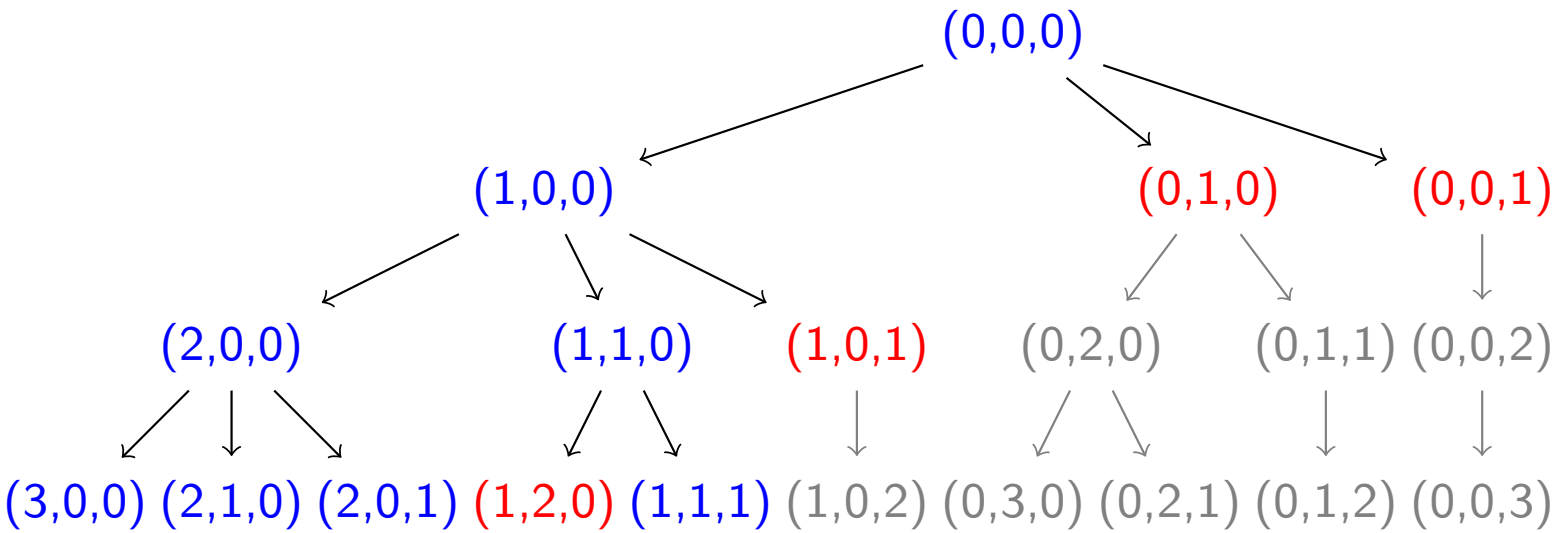


Utilisation de structure arborescente sous-jacente

- Limitation du nombre de test du critère canonique
- Test de canonicité optimisé via la théorie des groupes

Vecteurs d'entiers modulo un groupe de permutations

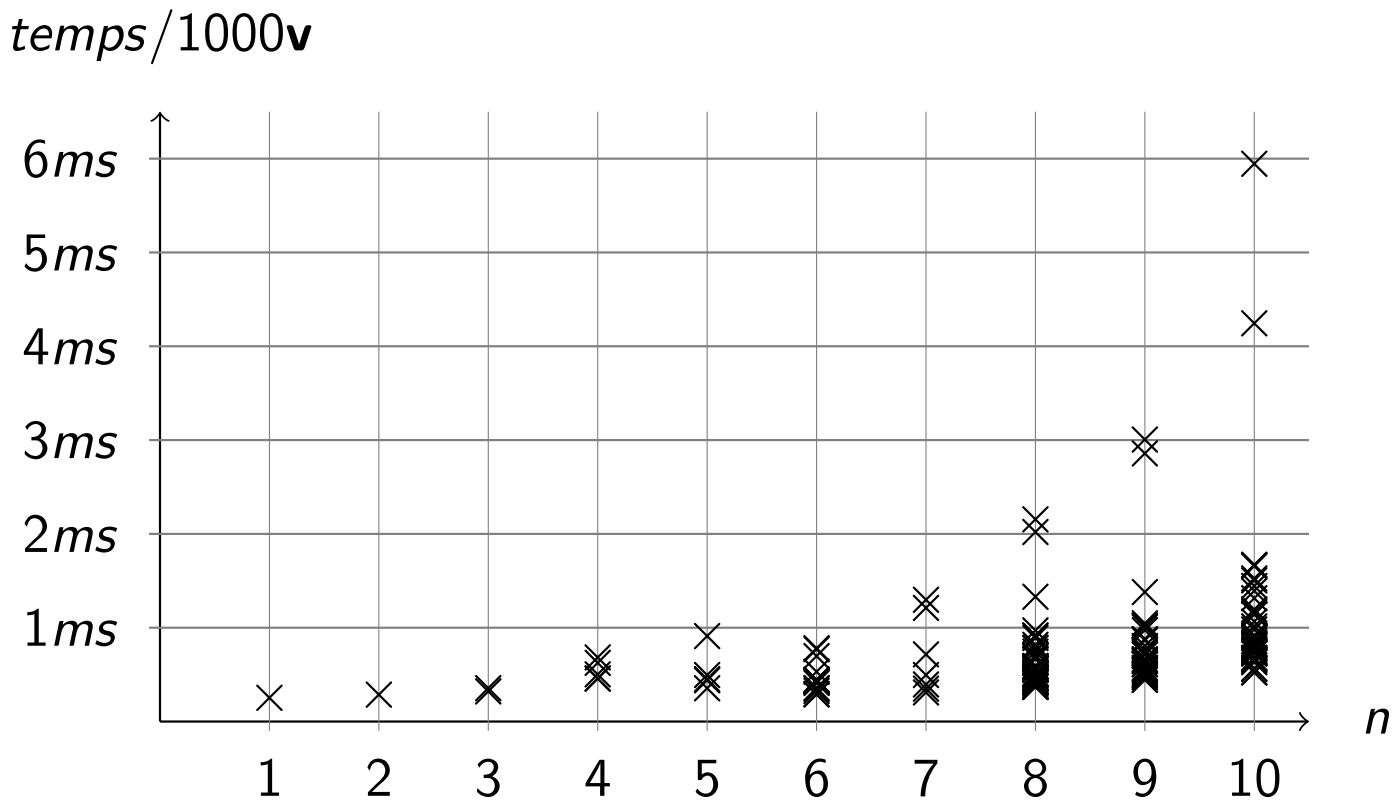
Exemple $C_3 = \langle (1,2,3) \rangle$



Utilisation de structure arborescente sous-jacente

- Limitation du nombre de test du critère canonique
- Test de canonicité optimisé via la théorie des groupes

Vecteurs d'entiers modulo un groupe de permutations



Temps pour générer 1000 vecteurs canoniques sous l'action des groupes transitifs agissant sur au plus 10 variables.
(2000 lignes de code, 4 Tickets)

$\mathbb{K}[\mathbf{x}]^G$ est une algèbre finiment engendrée sur $\mathbb{K}$

Théorème

$\mathbb{K}[\mathbf{x}]^G$ *a pour dimension de Krull* n.
(Les polynômes symétriques élémentaires sont algébriquement indépendants)

Théorème (Noether)

$\mathbb{K}[\mathbf{x}]^G$ *est une algèbre engendrée sur* $\mathbb{K}$ *par un nombre fini d'invariants homogènes de degré n'excédant pas* $|G|$.

Théorème (Garsia, Stanton (1984))

$\mathbb{K}[\mathbf{x}]^G$ *est engendrée par un nombre fini d'invariants homogènes de degré n'excédant pas* $\binom{n}{2}$.

$\mathbb{K}[\mathbf{x}]^G$ est une algèbre finiment engendrée sur $\mathbb{K}$

Théorème

$\mathbb{K}[\mathbf{x}]^G$ *a pour dimension de Krull* n.
(Les polynômes symétriques élémentaires sont algébriquement indépendants)

Théorème (Noether)

$\mathbb{K}[\mathbf{x}]^G$ *est une algèbre engendrée sur* $\mathbb{K}$ *par un nombre fini d'invariants homogènes de degré n'excédant pas* $|G|$.

Théorème (Garsia, Stanton (1984))

$\mathbb{K}[\mathbf{x}]^G$ *est engendrée par un nombre fini d'invariants homogènes de degré n'excédant pas* $\binom{n}{2}$.

$\mathbb{K}[\mathbf{x}]^G$ est une algèbre finiment engendrée sur $\mathbb{K}$

Théorème

$\mathbb{K}[\mathbf{x}]^G$ a pour dimension de Krull n.
(Les polynômes symétriques élémentaires sont algébriquement indépendants)

Théorème (Noether)

$\mathbb{K}[\mathbf{x}]^G$ est une algèbre engendrée sur $\mathbb{K}$ par un nombre fini d'invariants homogènes de degré n'excédant pas $|G|$.

Théorème (Garsia, Stanton (1984))

$\mathbb{K}[\mathbf{x}]^G$ est engendrée par un nombre fini d'invariants homogènes de degré n'excédant pas $\binom{n}{2}$.

$\mathbb{K}[\mathbf{x}]^G$ est de Cohen-Macaulay

Théorème

$\mathbb{K}[\mathbf{x}]^G$ *est de Cohen-Macaulay*
$\mathbb{K}[\mathbf{x}]^G$ *est un* $\mathrm{Sym}(\mathbf{x})$*-module libre de rang* $r = [\mathfrak{S}_n : G] = \frac{n!}{|G|}$*:*

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

C'est la *décomposition de Hironaka* de $\mathbb{K}[\mathbf{x}]^G$

Définition

$\{\eta_i\}_{1 \leqslant i \leqslant r}$*: invariants secondaires (polynômes homogènes)*

$\mathcal{H}(\mathbb{K}[\mathbf{x}]^G, z)/\mathcal{H}(\mathrm{Sym}(\mathbf{x}), z)$: Série des degrés invariants secondaires (toujours un polynôme!)

$\mathbb{K}[\mathbf{x}]^G$ est de Cohen-Macaulay

Théorème

$\mathbb{K}[\mathbf{x}]^G$ est de Cohen-Macaulay
$\mathbb{K}[\mathbf{x}]^G$ est un $\mathrm{Sym}(\mathbf{x})$-module libre de rang $r = [\mathfrak{S}_n : G] = \frac{n!}{|G|}$:

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

C'est la *décomposition de Hironaka* de $\mathbb{K}[\mathbf{x}]^G$

Définition

$\{\eta_i\}_{1 \leqslant i \leqslant r}$: invariants secondaires (polynômes homogènes)

$\mathcal{H}(\mathbb{K}[\mathbf{x}]^G, z)/\mathcal{H}(\mathrm{Sym}(\mathbf{x}), z)$: Série des degrés invariants secondaires (toujours un polynôme!)

Objectif et cas test

Objectif

Construire les invariants secondaires η_i

Choix du cas test:

- Description algébrique fine.
- Donne une famille génératrice.
- Accès à la base de données des groupes transitifs énumérés à un isomorphisme près [GAP, Hulpke].

Objectif et cas test

Objectif

Construire les invariants secondaires η_i

Choix du cas test:

- Description algébrique fine.
- Donne une famille génératrice.
- Accès à la base de données des groupes transitifs énumérés à un isomorphisme près [GAP, Hulpke].

Exemple

Pour $C_3 = \langle (1,2,3) \rangle$ le groupe cyclique d'ordre 3 : $C_3 \subset \mathfrak{S}_3$

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

e_1, e_2 et e_3 engendrent $\mathbb{K}[x_1, x_2, x_3]^{\mathfrak{S}_3}$.

Quotientant les deux séries de Hilbert, on obtient le polynôme

$$\mathcal{H}(\mathbb{K}[\mathbf{x}]^{C_3}, z)/\mathcal{H}(\mathrm{Sym}(\mathbf{x}), z) = 1 + z^3$$

$\eta_1 = 1$
$\eta_2 = \sum_{orb(G)}(x_1^2x_2) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$

Décomposition de Hironaka de $\mathbb{K}[\mathbf{x}]^{C_3}$

$$\mathbb{K}[\mathbf{x}]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus \sum_{orb(G)} (x_1^2x_2) \cdot \mathbb{K}[e_1, e_2, e_3]$$

Exemple

Pour $C_3 = \langle (1,2,3) \rangle$ le groupe cyclique d'ordre 3 : $C_3 \subset \mathfrak{S}_3$

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

e_1, e_2 et e_3 engendrent $\mathbb{K}[x_1, x_2, x_3]^{\mathfrak{S}_3}$.
Quotientant les deux séries de Hilbert, on obtient le polynôme

$$\mathcal{H}(\mathbb{K}[\mathbf{x}]^{C_3}, z)/\mathcal{H}(\mathrm{Sym}(\mathbf{x}), z) = 1 + z^3$$

$\eta_1 = 1$
$\eta_2 = \sum_{orb(G)}(x_1^2x_2) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$

Décomposition de Hironaka de $\mathbb{K}[\mathbf{x}]^{C_3}$

$$\mathbb{K}[\mathbf{x}]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus \sum_{orb(G)} (x_1^2x_2) \cdot \mathbb{K}[e_1, e_2, e_3]$$

Exemple

Pour $C_3 = \langle (1,2,3) \rangle$ le groupe cyclique d'ordre 3 : $C_3 \subset \mathfrak{S}_3$

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

e_1, e_2 et e_3 engendrent $\mathbb{K}[x_1, x_2, x_3]^{\mathfrak{S}_3}$.
Quotientant les deux séries de Hilbert, on obtient le polynôme

$$\mathcal{H}(\mathbb{K}[\mathbf{x}]^{C_3}, z)/\mathcal{H}(\mathrm{Sym}(\mathbf{x}), z) = 1 + z^3$$

$\eta_1 = 1$
$\eta_2 = \sum_{orb(G)}(x_1^2x_2) = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$

Décomposition de Hironaka de $\mathbb{K}[\mathbf{x}]^{C_3}$

$$\mathbb{K}[\mathbf{x}]^{C_3} = \mathbb{K}[e_1, e_2, e_3] \oplus \sum_{orb(G)} (x_1^2x_2) \cdot \mathbb{K}[e_1, e_2, e_3]$$

Comment réaliser le quotient ?

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

Par un corollaire du Lemme de Nakayama gradué, on a:

$$\mathbb{K}[\mathbf{x}]^G / \langle e_1, e_2, \ldots, e_n \rangle \approx \bigoplus_{i=1}^{r} \mathbb{K} \cdot \eta_i$$

Question

Comment mener les calculs dans le quotient ?

Comment réaliser le quotient ?

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

Par un corollaire du Lemme de Nakayama gradué, on a:

$$\mathbb{K}[\mathbf{x}]^G / \langle e_1, e_2, \ldots, e_n \rangle \approx \bigoplus_{i=1}^{r} \mathbb{K} \cdot \eta_i$$

Question

Comment mener les calculs dans le quotient ?

Image du quotient

Image du quotient

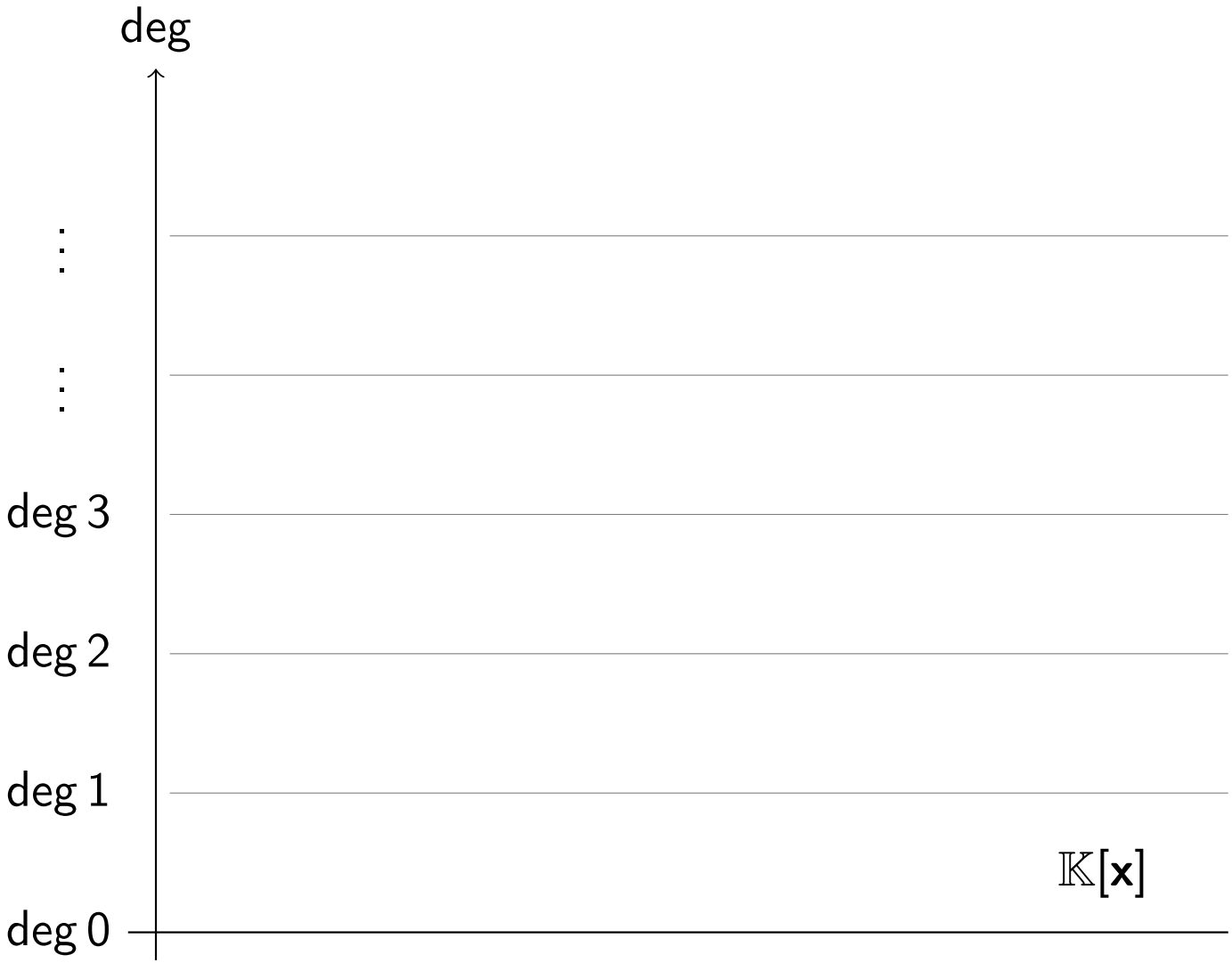


Image du quotient

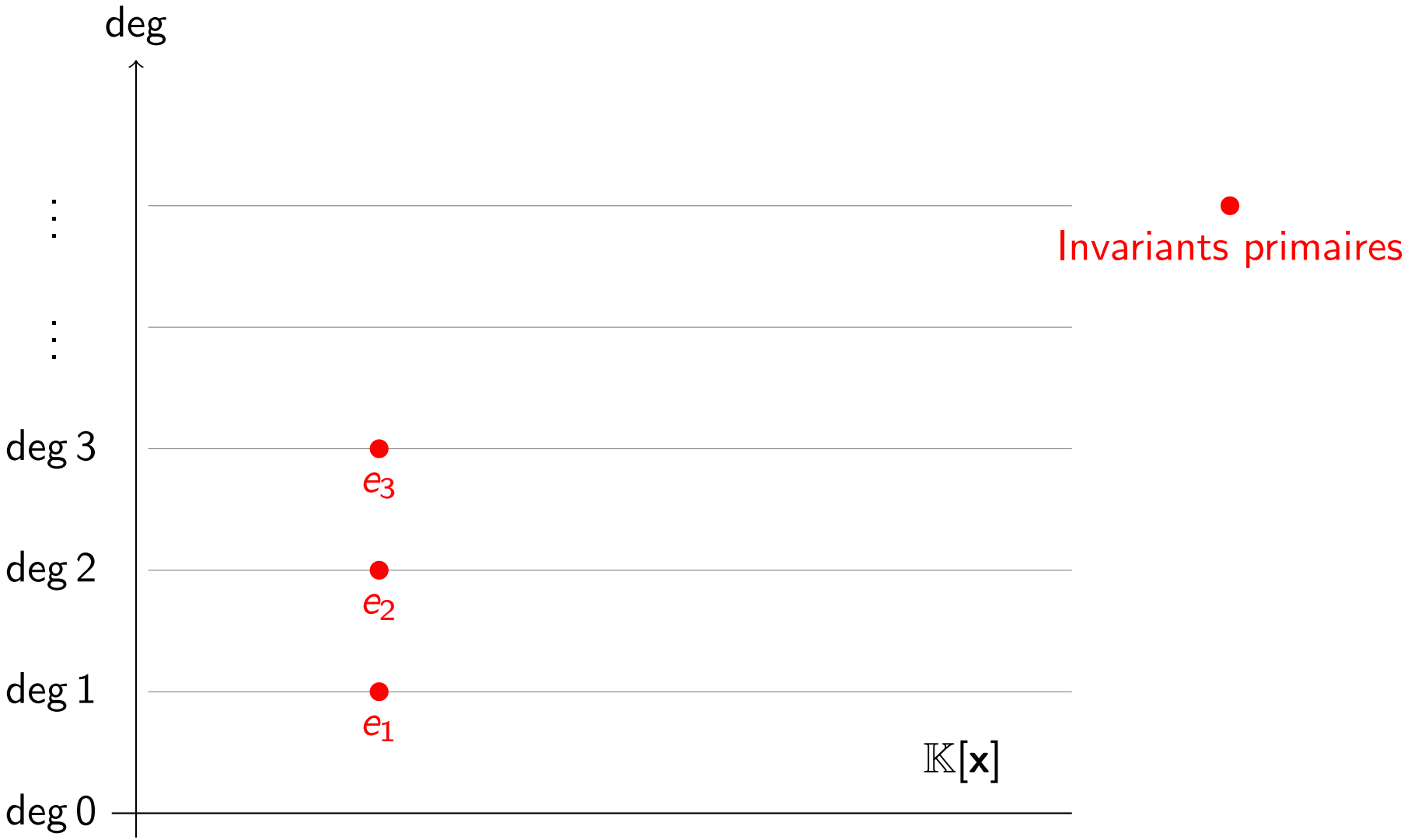


Image du quotient

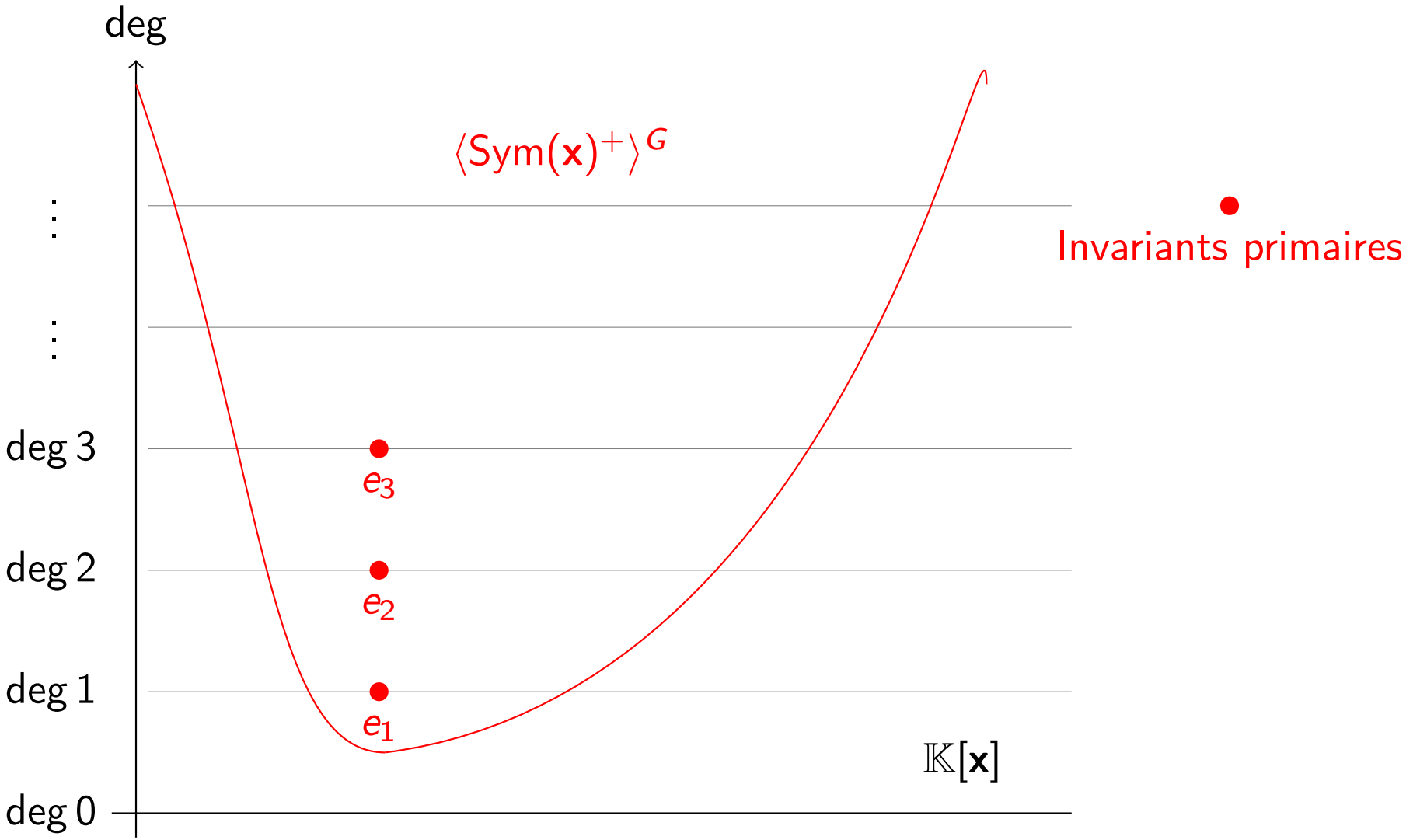


Image du quotient

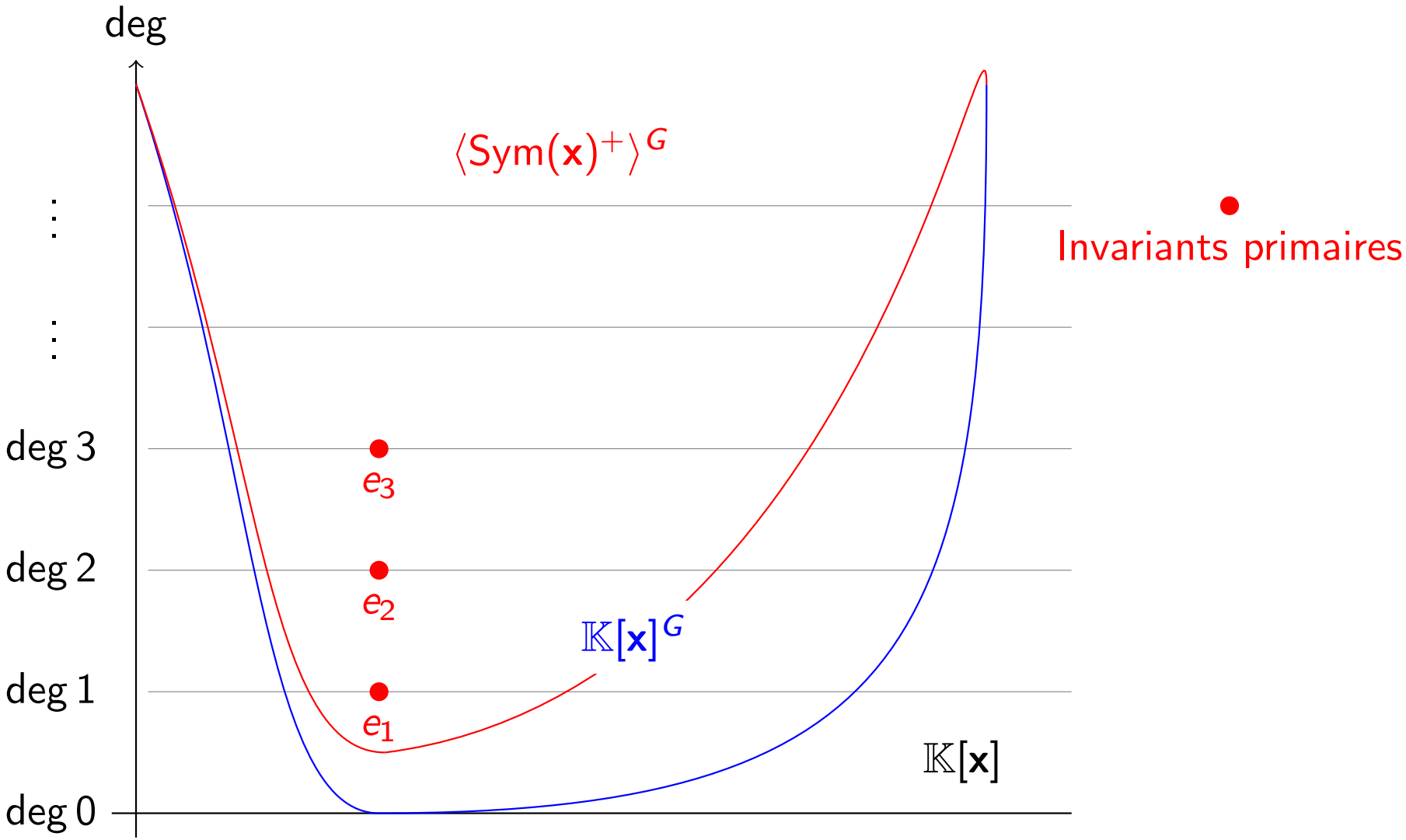


Image du quotient

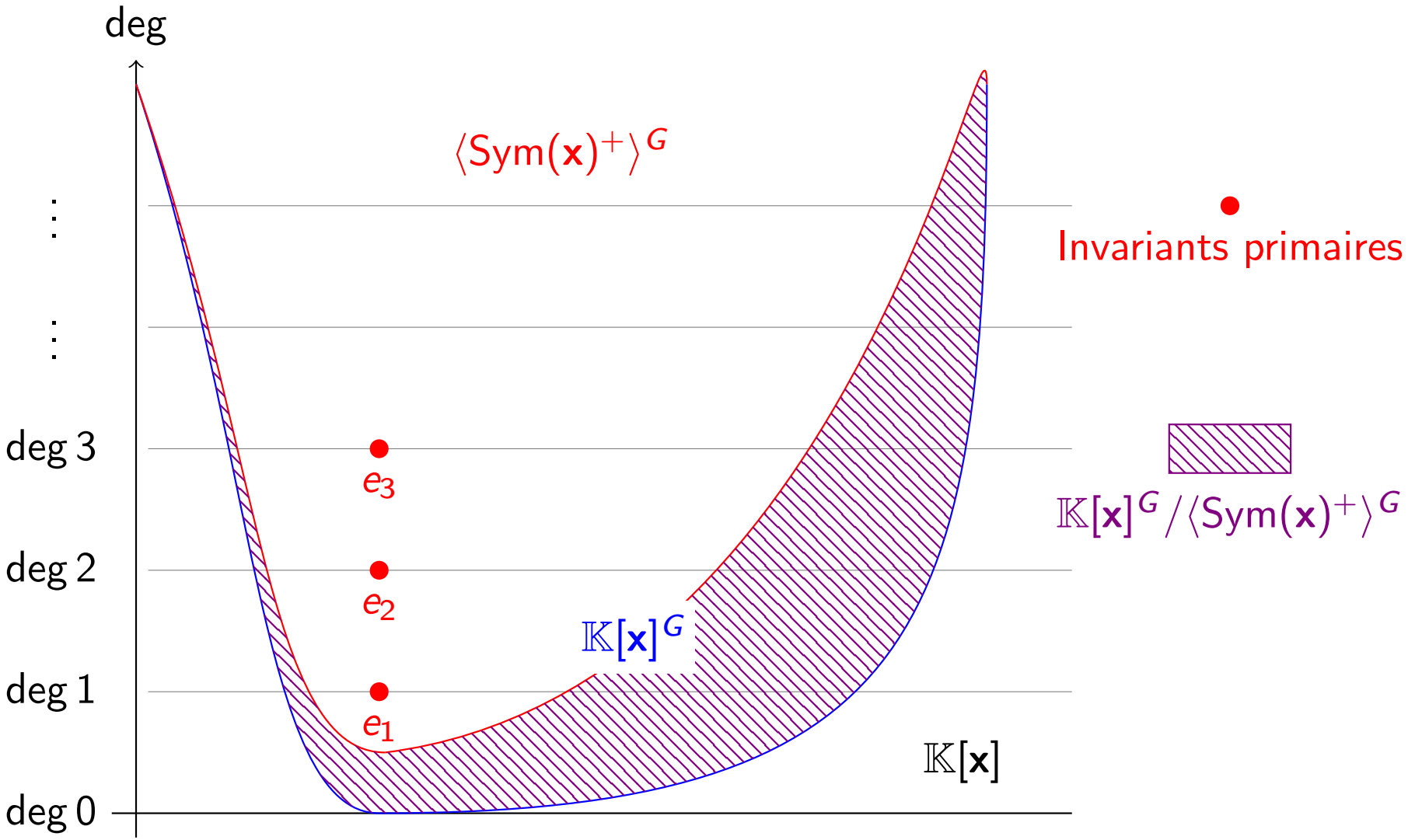
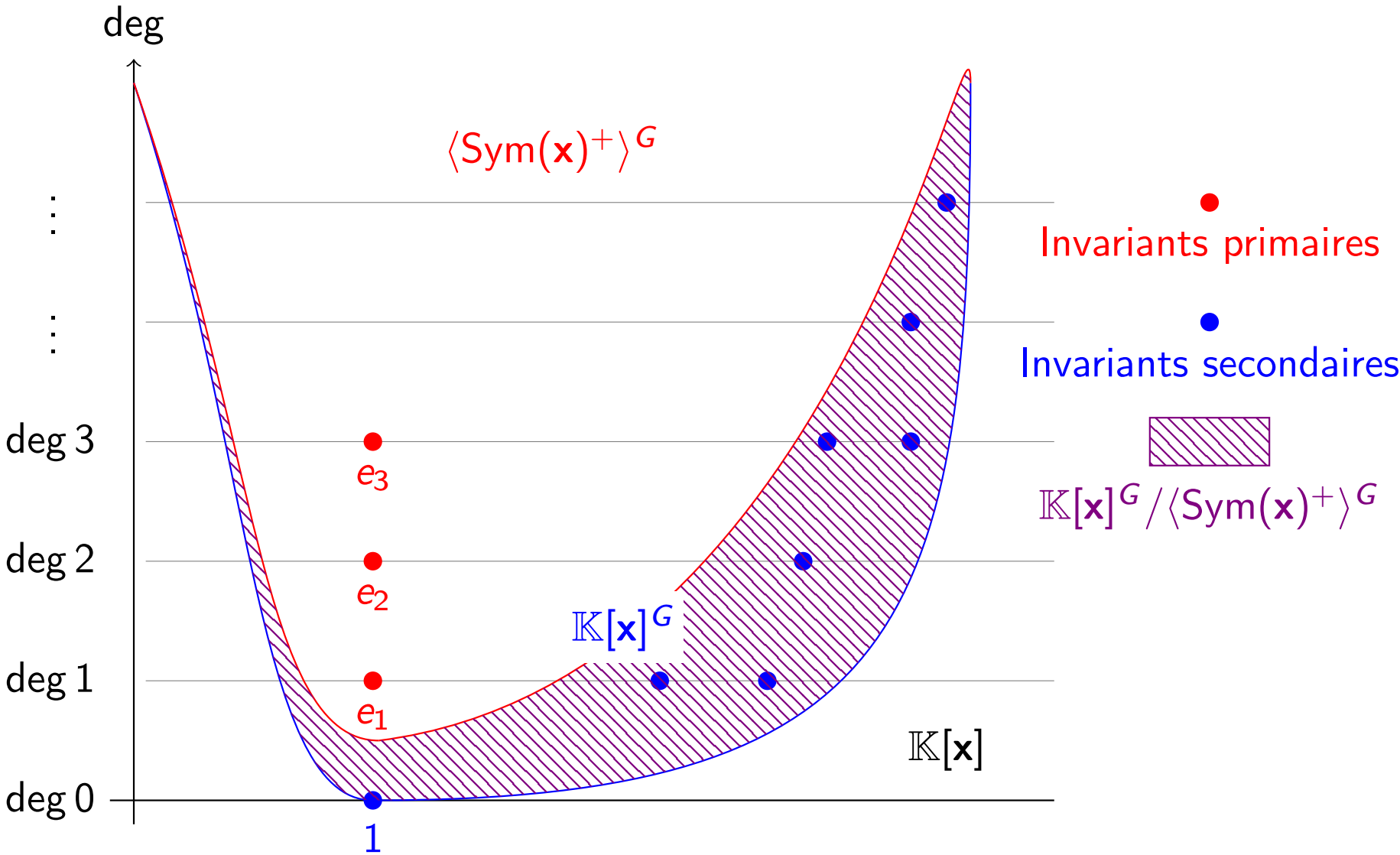


Image du quotient



Approche usuelle par bases de Gröbner

Il existe de nombreuses implantations utilisant les bases de (SAGBI-)Gröbner : Maple, MAGMA, MuPAD (PerMuVAR), Singular (finvar), ...

Problème: manque de contrôle sur la complexité pratique:

Groupe	Cardinal	Tps calcul Singular
(8, 5)	8	19 s
(8, 6)	16	2046 s
(8, 7)	16	$>$ 1 day
(8, 8)	16	$>$ 1 day
(8, 9)	16	8 s
(8, 10)	16	72 s
(8, 11)	16	14 s
(8, 12)	24	$>$ 1 day
(8, 13)	24	10863 s
(8, 14)	24	$>$ 1 day
(8, 15)	32	$>$ 1 day

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Approche usuelle par bases de Gröbner

Les principales limites de ces implantations :

- Les bases de Gröbner cassent les symétries
- L'algèbre linéaire est menée dans un espace de grande dimension
- Les bases de SAGBI-Gröbner exploitent les symétries mais sont grosses
- Faible contrôle de la complexité algorithmique
- Comment introduire de la combinatoire ?

Une approche par évaluation

Travailler par évaluation est une technique classique pour calculer dans un quotient. On se place aux zéros de l'idéal déterminant le quotient. Est-ce faisable dans ce contexte ?

Choix d'un ensemble de points $S \subset \mathbb{K}^n$

Morphisme d'évaluation Φ_S

$$\begin{array}{rccc} \Phi_S : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & (\mathbb{K}^{|S|}, .) \\ & P & \longmapsto & (P(s))_{s \in S} \end{array}$$

où . est le produit point par point (produit de Hadamard)

Fait: Φ_S est un morphisme d'algèbre

Une approche par évaluation

Travailler par évaluation est une technique classique pour calculer dans un quotient. On se place aux zéros de l'idéal déterminant le quotient. Est-ce faisable dans ce contexte ?

Choix d'un ensemble de points $S \subset \mathbb{K}^n$

Morphisme d'évaluation Φ_S

$$\begin{array}{rccc} \Phi_S : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & (\mathbb{K}^{|S|}, .) \\ & P & \longmapsto & (P(s))_{s \in S} \end{array}$$

où . est le produit point par point (produit de Hadamard)

Fait: Φ_S est un morphisme d'algèbre

déformation du quotient

Fait: Φ_S tue les fonctions nulles dans S

Objectif: Comment choisir S qui tue les e_i mais garde les η_i ?

Difficulté: $\mathbf{0} := (0, \ldots, 0)$ est l'unique racine du système $e_1(\mathbf{x}) = \cdots = e_n(\mathbf{x}) = 0$ mais de multiplicité $n!$

Idée: Déformer l'idéal pour éclater complètement l'unique racine multiple en racines simples

$$\langle e_1, \ldots, e_{n-1}, e_n \rangle \longrightarrow \langle e_1, \ldots, e_{n-1}, e_n - \epsilon \rangle$$

déformation du quotient

Fait: Φ_S tue les fonctions nulles dans S

Objectif: Comment choisir S qui tue les e_i mais garde les η_i ?

Difficulté: $\mathbf{0} := (0, \ldots, 0)$ est l'unique racine du système $e_1(\mathbf{x}) = \cdots = e_n(\mathbf{x}) = 0$ mais de multiplicité $n!$

Idée: Déformer l'idéal pour éclater complètement l'unique racine multiple en racines simples

$$\langle e_1, \ldots, e_{n-1}, e_n \rangle \longrightarrow \langle e_1, \ldots, e_{n-1}, e_n - \epsilon \rangle$$

déformation du quotient

Fait: Φ_S tue les fonctions nulles dans S

Objectif: Comment choisir S qui tue les e_i mais garde les η_i ?

Difficulté: $\mathbf{0} := (0, \ldots, 0)$ est l'unique racine du système $e_1(\mathbf{x}) = \cdots = e_n(\mathbf{x}) = 0$ mais de multiplicité $n!$

Idée: Déformer l'idéal pour éclater complètement l'unique racine multiple en racines simples

$$\langle e_1, \ldots, e_{n-1}, e_n \rangle \longrightarrow \langle e_1, \ldots, e_{n-1}, e_n - \epsilon \rangle$$

déformation du quotient

Fait: Φ_S tue les fonctions nulles dans S

Objectif: Comment choisir S qui tue les e_i mais garde les η_i ?

Difficulté: $\mathbf{0} := (0, \ldots, 0)$ est l'unique racine du système $e_1(\mathbf{x}) = \cdots = e_n(\mathbf{x}) = 0$ mais de multiplicité $n!$

Idée: Déformer l'idéal pour éclater complètement l'unique racine multiple en racines simples

$$\langle e_1, \ldots, e_{n-1}, e_n \rangle \longrightarrow \langle e_1, \ldots, e_{n-1}, e_n - \epsilon \rangle$$

Polynômes symétriques élémentaires et racines de l'unité

Proposition

Soit ρ une racine primitive n-ième de l'unité.

$$\begin{cases} e_1(1, \rho, \ldots, \rho^{n-1}) &= 0 \\ &\vdots \\ e_{n-1}(1, \rho, \ldots, \rho^{n-1}) &= 0 \\ e_n(1, \rho, \ldots, \rho^{n-1}) &= (-1)^{n+1} \end{cases}$$

Démonstration:

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

Polynômes symétriques élémentaires et racines de l'unité

Proposition

Soit ρ une racine primitive n-ième de l'unité.

$$\begin{cases} e_1(1, \rho, \ldots, \rho^{n-1}) &= 0 \\ &\vdots \\ e_{n-1}(1, \rho, \ldots, \rho^{n-1}) &= 0 \\ e_n(1, \rho, \ldots, \rho^{n-1}) &= (-1)^{n+1} \end{cases}$$

Démonstration:

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

Choisir les points d'évaluation

Point identité: $A_{id} := (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$|Orb_{\mathfrak{S}_n}(A_{id})| = n!$
Cette orbite forme les $n!$ racines simples de l'idéal déformé
$\langle e_1, \ldots, e_{n-1}, e_n + (-1)^n \rangle$

Remarque

Un invariant sous G est d'évaluation constante sur les G-orbites

Un seul point par G-orbite suffit
$r = [\mathfrak{S}_n : G]$ points d'évaluation, autant que d'invariants secondaires!

Choisir les points d'évaluation

Point identité: $A_{id} := (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$|Orb_{\mathfrak{S}_n}(A_{id})| = n!$
Cette orbite forme les $n!$ racines simples de l'idéal déformé
$\langle e_1, \ldots, e_{n-1}, e_n + (-1)^n \rangle$

Remarque

Un invariant sous G est d'évaluation constante sur les G-orbites

Un seul point par G-orbite suffit
$r = [\mathfrak{S}_n : G]$ points d'évaluation, autant que d'invariants secondaires!

Choisir les points d'évaluation

Point identité: $A_{id} := (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$|Orb_{\mathfrak{S}_n}(A_{id})| = n!$
Cette orbite forme les $n!$ racines simples de l'idéal déformé
$\langle e_1, \ldots, e_{n-1}, e_n + (-1)^n \rangle$

Remarque

Un invariant sous G est d'évaluation constante sur les G-orbites

Un seul point par G-orbite suffit
$r = [\mathfrak{S}_n : G]$ points d'évaluation, autant que d'invariants secondaires!

Choisir les points d'évaluation

Point identité: $A_{id} := (1, \rho, \rho^2, \ldots, \rho^{n-1}) \in \mathbb{K}^n$.

$|Orb_{\mathfrak{S}_n}(A_{id})| = n!$
Cette orbite forme les $n!$ racines simples de l'idéal déformé
$\langle e_1, \ldots, e_{n-1}, e_n + (-1)^n \rangle$

Remarque

Un invariant sous G est d'évaluation constante sur les G-orbites

Un seul point par G-orbite suffit
$r = [\mathfrak{S}_n : G]$ points d'évaluation, autant que d'invariants secondaires!

Choisir les points d'évaluation

Soit L une transversale à droite de G dans $\mathfrak{S}_n$.

Définition (Morphisme d'évaluation Φ)

$$\begin{array}{rccc} \Phi : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathbb{K}^r \\ & P & \longmapsto & (P(A_\sigma))_{\sigma \in L} \end{array}$$

Le morphisme Φ réalise :

Proposition

Φ est un morphisme d'algèbre surjectif.

Remarques :

- $\Phi(\mathrm{Sym}(\mathbf{x})) = \langle (1, 1, \ldots, 1) \rangle_{\mathbb{K}}$
- $dim(Im(\Phi)) = dim(\mathbb{K}[\mathbf{x}]^G / \langle \mathrm{Sym}(\mathbf{x})^+ \rangle^G)$

Choisir les points d'évaluation

Soit L une transversale à droite de G dans $\mathfrak{S}_n$.

Définition (Morphisme d'évaluation Φ)

$$\begin{array}{rccc} \Phi : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathbb{K}^r \\ & P & \longmapsto & (P(A_\sigma))_{\sigma \in L} \end{array}$$

Le morphisme Φ réalise :

Proposition

Φ est un morphisme d'algèbre surjectif.

Remarques :

- $\Phi(\mathrm{Sym}(\mathbf{x})) = \langle (1, 1, \ldots, 1) \rangle_{\mathbb{K}}$
- $dim(Im(\Phi)) = dim(\mathbb{K}[\mathbf{x}]^G / \langle \mathrm{Sym}(\mathbf{x})^+ \rangle^G)$

Choisir les points d'évaluation

Soit L une transversale à droite de G dans $\mathfrak{S}_n$.

Définition (Morphisme d'évaluation Φ)

$$\begin{array}{rccc} \Phi : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathbb{K}^r \\ & P & \longmapsto & (P(A_\sigma))_{\sigma \in L} \end{array}$$

Le morphisme Φ réalise :

Proposition

Φ est un morphisme d'algèbre surjectif.

Remarques :

- $\Phi(\mathrm{Sym}(\mathbf{x})) = \langle (1, 1, \ldots, 1) \rangle_{\mathbb{K}}$
- $dim(Im(\Phi)) = dim(\mathbb{K}[\mathbf{x}]^G / \langle \mathrm{Sym}(\mathbf{x})^+ \rangle^G)$

Choisir les points d'évaluation

Soit L une transversale à droite de G dans $\mathfrak{S}_n$.

Définition (Morphisme d'évaluation Φ)

$$\begin{array}{rccc} \Phi : & \mathbb{K}[\mathbf{x}]^G & \longrightarrow & \mathbb{K}^r \\ & P & \longmapsto & (P(A_\sigma))_{\sigma \in L} \end{array}$$

Le morphisme Φ réalise :

Proposition

Φ est un morphisme d'algèbre surjectif.

Remarques :

- $\Phi(\mathrm{Sym}(\mathbf{x})) = \langle (1, 1, \ldots, 1) \rangle_{\mathbb{K}}$
- $dim(Im(\Phi)) = dim(\mathbb{K}[\mathbf{x}]^G / \langle \mathrm{Sym}(\mathbf{x})^+ \rangle^G)$

Redressement par la graduation

Rappel: les secondaires sont une base de $\mathbb{K}[\mathbf{x}]^G$ sur $\mathrm{Sym}(\mathbf{x})$:

$$\mathbb{K}[\mathbf{x}]^G = \bigoplus_{i=1}^{r} \eta_i \,\mathrm{Sym}(\mathbf{x})$$

Soit $S_d := \{\eta_j | \deg(\eta_j) = d\}$ (secondaires de degré d)

$$\mathbb{K}[\mathbf{x}]^G_d := \{P \in \mathbb{K}[\mathbf{x}]^G | deg(P) = d\}$$

Théorème

Le morphisme d'évaluation Φ réalise

$$\begin{aligned} \text{for } 0 \leqslant d < n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \\ \text{for } d \geqslant n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \oplus \Phi(\mathbb{K}[\mathbf{x}]^G_{d-n}) \end{aligned}$$

Démonstration: appliquer Φ sur la décomposition de Hironaka

Redressement par la graduation

Rappel: les secondaires sont une base de $\mathbb{K}[\mathbf{x}]^G$ sur $\mathrm{Sym}(\mathbf{x})$:

$$\mathbb{K}[\mathbf{x}]^G = \bigoplus_{i=1}^{r} \eta_i \,\mathrm{Sym}(\mathbf{x})$$

Soit $S_d := \{\eta_j | \deg(\eta_j) = d\}$ (secondaires de degré d)

$$\mathbb{K}[\mathbf{x}]^G_d := \{P \in \mathbb{K}[\mathbf{x}]^G | deg(P) = d\}$$

Théorème

Le morphisme d'évaluation Φ réalise

$$\begin{aligned} \text{for } 0 \leqslant d < n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \\ \text{for } d \geqslant n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \oplus \Phi(\mathbb{K}[\mathbf{x}]^G_{d-n}) \end{aligned}$$

Démonstration: appliquer Φ sur la décomposition de Hironaka

Redressement par la graduation

Rappel: les secondaires sont une base de $\mathbb{K}[\mathbf{x}]^G$ sur $\mathrm{Sym}(\mathbf{x})$:

$$\mathbb{K}[\mathbf{x}]^G = \bigoplus_{i=1}^{r} \eta_i \,\mathrm{Sym}(\mathbf{x})$$

Soit $S_d := \{\eta_j | \deg(\eta_j) = d\}$ (secondaires de degré d)

$$\mathbb{K}[\mathbf{x}]^G_d := \{P \in \mathbb{K}[\mathbf{x}]^G | deg(P) = d\}$$

Théorème

Le morphisme d'évaluation Φ réalise

$$\begin{aligned} \text{for } 0 \leqslant d < n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \\ \text{for } d \geqslant n: &\quad \Phi(\mathbb{K}[\mathbf{x}]^G_d) = \Phi(\langle S_d \rangle_{\mathbb{K}}) \oplus \Phi(\mathbb{K}[\mathbf{x}]^G_{d-n}) \end{aligned}$$

Démonstration: appliquer Φ sur la décomposition de Hironaka

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$

$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Exemple

Groupe cyclique d'ordre 3: $C_3 := \langle (1,2,3) \rangle \subset \mathfrak{S}_3$

$\rho = j$: racine primitive troisième de l'unité : $j^3 = 1$.

$$L = \{ \quad A_{id} := (1, j, j^2), \quad A_{(1,2)} := (j, 1, j^2) \quad \}$$

Degré 0 : $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \Phi(\langle S_0 \rangle_{\mathbb{K}})$
$\Phi(1) = (1,1) \neq \mathbf{0}$ donc $\Phi(\mathbb{K}[\mathbf{x}]_0^G) = \langle (1,1) \rangle_{\mathbb{K}}$ et $S_0 = \{1\}$

Deg 3: $\Phi(\mathbb{K}[\mathbf{x}]_3^G) = \Phi(\mathbb{K}[\mathbf{x}]_0^G) \oplus \Phi(\langle S_3 \rangle_{\mathbb{K}})$

$$\Phi(\sum_{orb(G)} (x_1^3)) = \Phi(x_1^3 + x_2^3 + x_3^3) = (1^3 + j^3 + j^6, j^3 + 1^3 + j^6) = (3,3)$$

$$\Phi(\sum_{orb(G)} (x_1^2 x_2)) = \Phi(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) = (j + j^4 + j^4, j^2 + j^2 + j^5) = (3j, 3j^2)$$

$((3j, 3j^2) \notin \Phi(\mathbb{K}[\mathbf{x}]_0^G))$ donc $S_3 = \{ \sum_{orb(G)} (x_1^2 x_2) \}$

Analyse grossière de complexité

Taille du problème:

- $r := [\mathfrak{S}_n : G] = \frac{n!}{|G|}$
- $g := |G|$

Proposition

Borne de complexité du calcul des secondaires par évaluation:
$O(r^2 g^2 + r^3 g)$ opérations arithmétiques dans $\mathbb{K}$

Démonstration:

- Nombre de points d'évaluation: r
- Nombre de monômes sous l'escalier $n! = rg$
- Évaluation de toutes les sommes sur orbite: $O(rg \cdot n!) = O((rg)^2)$
- Réduction de Gauss : $O(r^3 g)$ opérations arithmétiques
  (Échelonnement d'une matrice de taille (rg, r) et de rang r)

Analyse grossière de complexité

Taille du problème:

- $r := [\mathfrak{S}_n : G] = \frac{n!}{|G|}$
- $g := |G|$

Proposition

Borne de complexité du calcul des secondaires par évaluation:
$O(r^2 g^2 + r^3 g)$ *opérations arithmétiques dans* $\mathbb{K}$

Démonstration:

- Nombre de points d'évaluation: r
- Nombre de monômes sous l'escalier $n! = rg$
- Évaluation de toutes les sommes sur orbite: $O(rg \cdot n!) = O((rg)^2)$
- Réduction de Gauss : $O(r^3 g)$ opérations arithmétiques
  (Échelonnement d'une matrice de taille (rg, r) et de rang r)

Analyse grossière de complexité

Taille du problème:

- $r := [\mathfrak{S}_n : G] = \frac{n!}{|G|}$
- $g := |G|$

Proposition

Borne de complexité du calcul des secondaires par évaluation:
$O(r^2 g^2 + r^3 g)$ *opérations arithmétiques dans* $\mathbb{K}$

Démonstration:

- Nombre de points d'évaluation: r
- Nombre de monômes sous l'escalier $n! = rg$
- Évaluation de toutes les sommes sur orbite: $O(rg \cdot n!) = O((rg)^2)$
- Réduction de Gauss : $O(r^3 g)$ opérations arithmétiques
  (Échelonnement d'une matrice de taille (rg, r) et de rang r)

Analyse grossière de complexité

Taille du problème:

- $r := [\mathfrak{S}_n : G] = \frac{n!}{|G|}$
- $g := |G|$

Proposition

Borne de complexité du calcul des secondaires par évaluation:
$O(r^2g^2 + r^3g)$ *opérations arithmétiques dans* $\mathbb{K}$

Démonstration:

- Nombre de points d'évaluation: r
- Nombre de monômes sous l'escalier $n! = rg$
- Évaluation de toutes les sommes sur orbite: $O(rg \cdot n!) = O((rg)^2)$
- Réduction de Gauss : $O(r^3g)$ opérations arithmétiques
  (Échelonnement d'une matrice de taille (rg, r) et de rang r)

Analyse grossière de complexité

Taille du problème:

- $r := [\mathfrak{S}_n : G] = \frac{n!}{|G|}$
- $g := |G|$

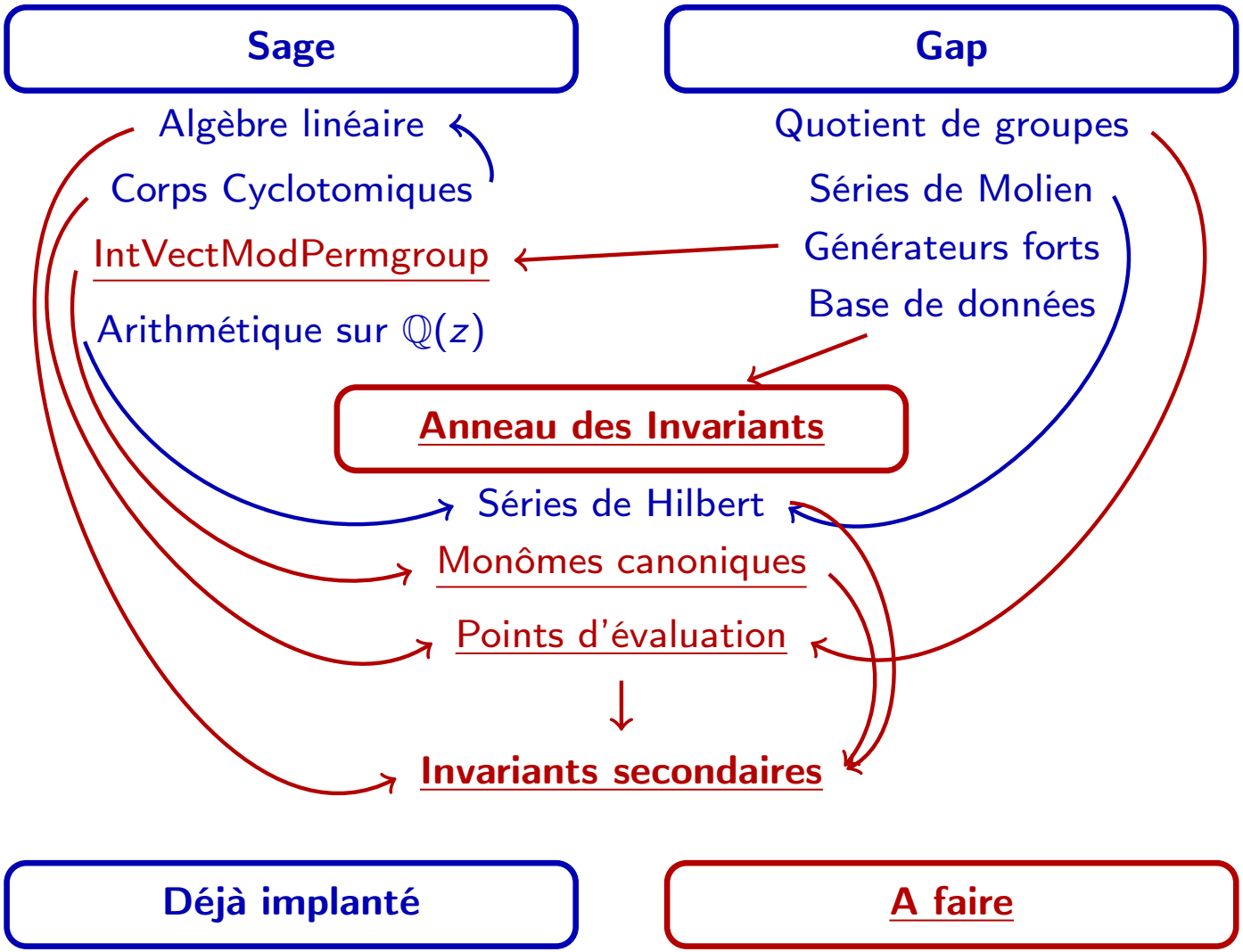
Proposition

Borne de complexité du calcul des secondaires par évaluation:
$O(r^2 g^2 + r^3 g)$ *opérations arithmétiques dans* $\mathbb{K}$

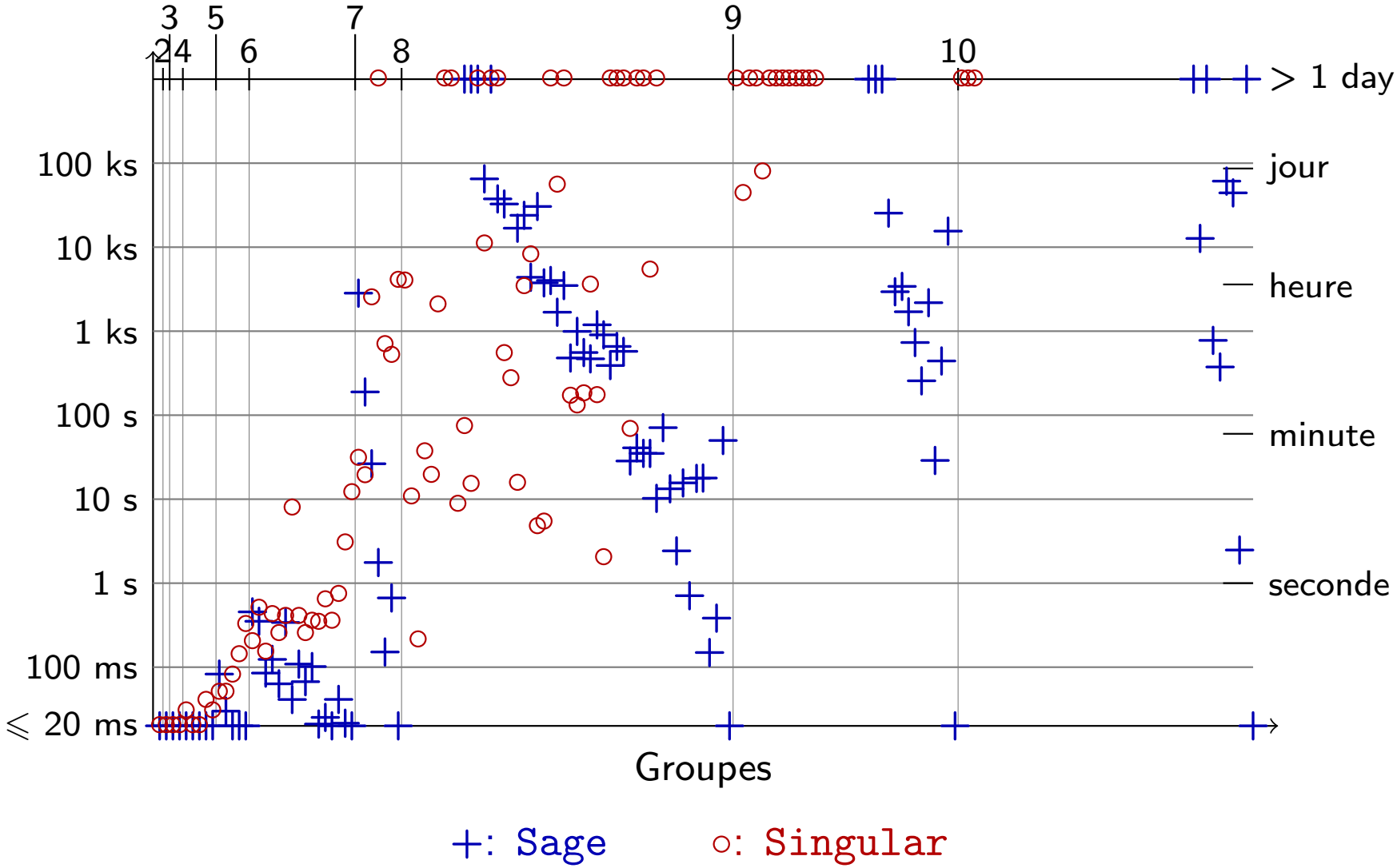
Démonstration:

- Nombre de points d'évaluation: r
- Nombre de monômes sous l'escalier $n! = rg$
- Évaluation de toutes les sommes sur orbite: $O(rg \cdot n!) = O((rg)^2)$
- Réduction de Gauss : $O(r^3 g)$ opérations arithmétiques
  (Échelonnement d'une matrice de taille (rg, r) et de rang r)

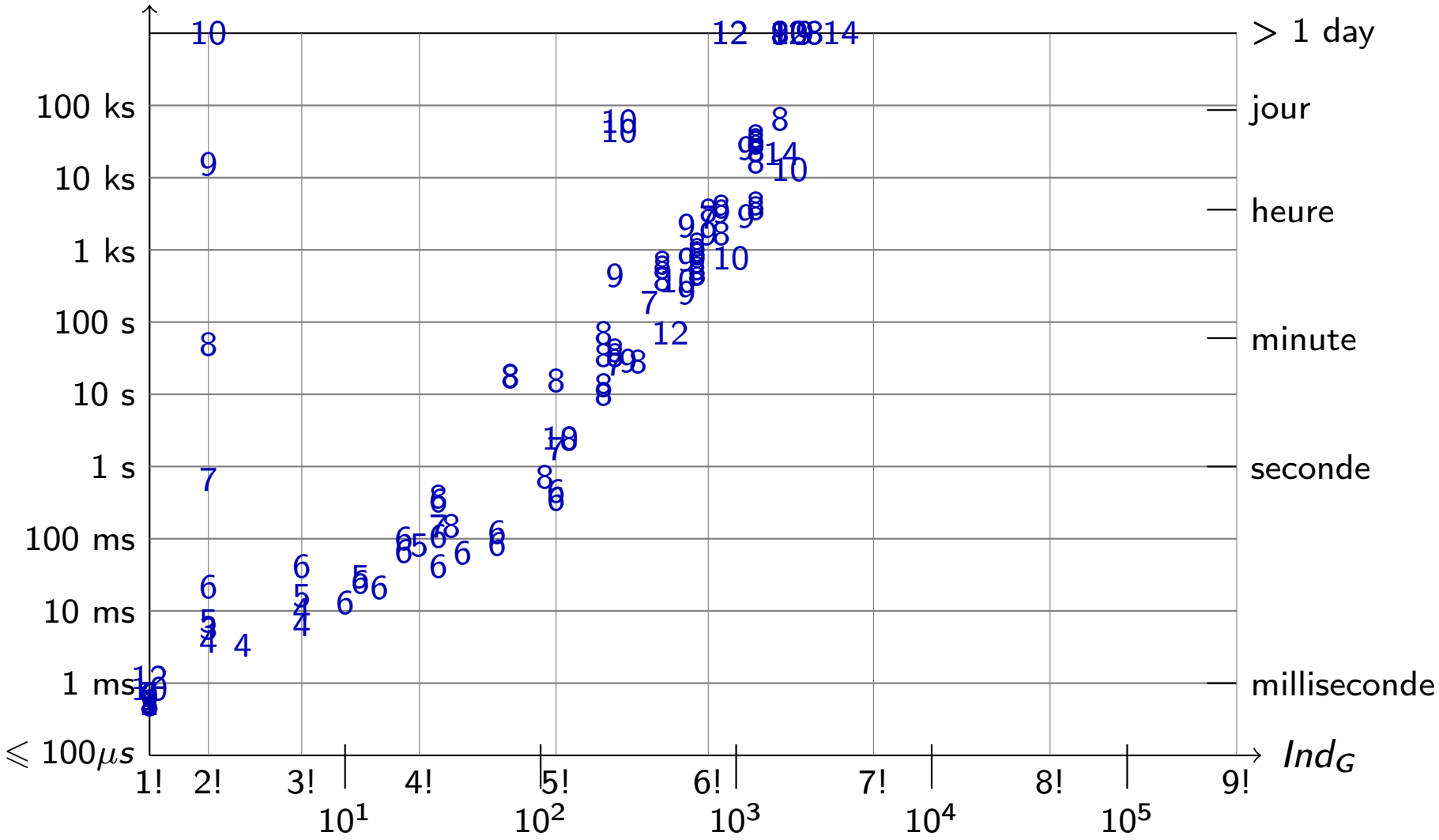
Implantation dans Sage



Bancs d'essais comparatifs avec Singular



Complexité selon l'indice du groupe dans $\mathfrak{S}_n$



Exemple: $G = \texttt{TransitiveGroup(14,61)}$; $|G| = 50\ 803\ 200$; $\frac{n!}{|G|} = 1\ 716$

Questions soulevées

L'algorithmique par évaluation est parallélisable et `Python` supporte le parallélisme (Exploiter ce point!)

Problème

Les évaluations sont des vecteurs comportant $r := \frac{n!}{|G|}$ coordonnées. En pratique, on ne construit jamais une base d'une telle dimension parce que les calculs sont menés degré par degré.

Pour $C_7 = \langle (1,2,3,4,5,6,7) \rangle$. $|C_7| = 7$.
La borne, fournie par Noether, sur le degré des générateurs est 7.
100 points (au lieu de $6! = 720$) sont suffisants pour le calcul des invariants irréductibles du groupe C_7.

Question

Il y a-t-il un moyen de réduire le nombre de points d'évaluation ?

Questions soulevées

L'algorithmique par évaluation est parallélisable et `Python` supporte le parallélisme (Exploiter ce point!)

Problème

Les évaluations sont des vecteurs comportant $r := \frac{n!}{|G|}$ *coordonnées. En pratique, on ne construit jamais une base d'une telle dimension parce que les calculs sont menés degré par degré.*

Pour $C_7 = \langle (1,2,3,4,5,6,7) \rangle$. $|C_7| = 7$.
La borne, fournie par Noether, sur le degré des générateurs est 7.
100 points (au lieu de $6! = 720$) sont suffisants pour le calcul des invariants irréductibles du groupe C_7.

Question

Il y a-t-il un moyen de réduire le nombre de points d'évaluation ?

Questions soulevées

L'algorithmique par évaluation est parallélisable et `Python` supporte le parallélisme (Exploiter ce point!)

Problème

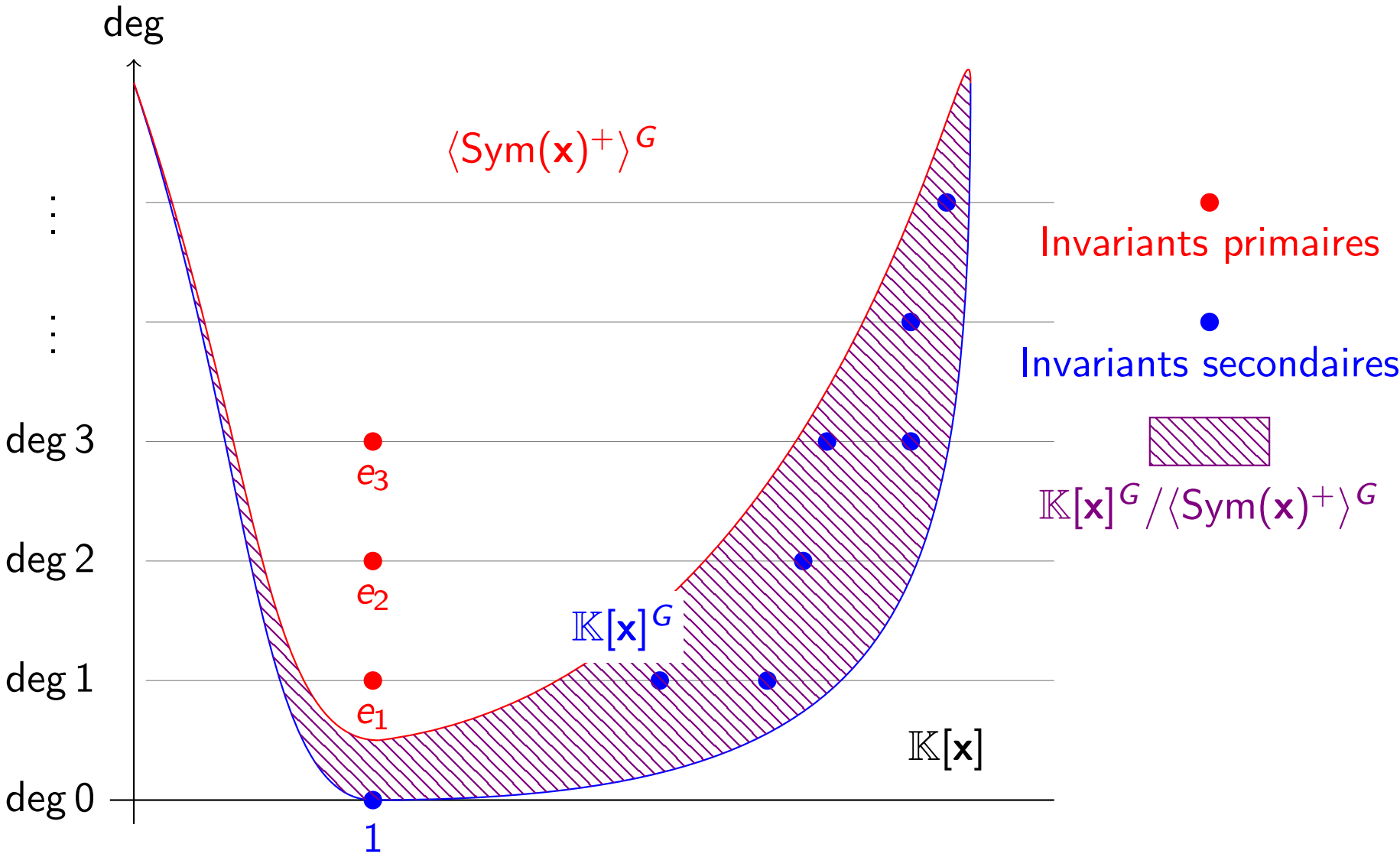
Les évaluations sont des vecteurs comportant $r := \frac{n!}{|G|}$ *coordonnées. En pratique, on ne construit jamais une base d'une telle dimension parce que les calculs sont menés degré par degré.*

Pour $C_7 = \langle (1,2,3,4,5,6,7) \rangle$. $|C_7| = 7$.
La borne, fournie par Noether, sur le degré des générateurs est 7.
100 points (au lieu de $6! = 720$) sont suffisants pour le calcul des invariants irréductibles du groupe C_7.

Question

Il y a-t-il un moyen de réduire le nombre de points d'évaluation ?

Se placer dans une composante homogène du quotient



Questions soulevées

Généralisation immédiate à la famille infinie des groupes de réflexions complexes $G(m, p, n)$

Question: Peut-on espérer une approche semblable pour les cas exceptionnels ?

Problème

Définir une généralisation de cette approche par évaluation pour les groupes de Weyl, groupes de Coxeter, groupes de réflexions complexes exceptionnels.

Questions soulevées

Problème

Construire des invariants avec des propriétés agréables d'évaluation par Φ (évaluation creuse, ...).
Point de départ prometteur: polynômes de Schubert doubles. Ils forment une base des polynômes multivariés en tant que $\mathrm{Sym}(\mathbf{x})$*-module dont l'image par Φ est triangulaire.*

Rêve

Obtenir une description combinatoire des invariants secondaires.

Ce problème est résolu uniquement pour les sous-groupes de Young de $\mathfrak{S}_n$ (Garcia, Stanton (1984)).

Questions soulevées

Problème

Construire des invariants avec des propriétés agréables d'évaluation par Φ (évaluation creuse, ...).
Point de départ prometteur: polynômes de Schubert doubles. Ils forment une base des polynômes multivariés en tant que $\mathrm{Sym}(\mathbf{x})$*-module dont l'image par Φ est triangulaire.*

Rêve

Obtenir une description combinatoire des invariants secondaires.

Ce problème est résolu uniquement pour les sous-groupes de Young de $\mathfrak{S}_n$ (Garcia, Stanton (1984)).

Fin

Merci pour votre attention!