Rational Invariants of Finite Abelian Groups

George Labahn

Symbolic Computation Group
Cheriton School of Computer Science
University of Waterloo, Canada.

* Joint work with Evelyne Hubert, INRIA Méditerranée.

Fields Workshop I : Sept 14, 2015

Rational Invariants of Finite Abelian Groups

(1) Given finite, abelian group $\mathcal{G} \subset GL(n, \mathbb{K})$ acting on $\mathbb{K}^n$

Rational Invariants of Finite Abelian Groups

(1) Given finite, abelian group $\mathcal{G} \subset GL(n, \mathbb{K})$ acting on $\mathbb{K}^n$

- construct rational invariants of action
  - rational invariant : $f \in \mathbb{K}(\mathbf{x}) \;:\; f(\, g \cdot \mathbf{x}\,) = f(\,\mathbf{x}\,) \qquad \forall g \in \mathcal{G}$
- determine rewrite rules for this action

Rational Invariants of Finite Abelian Groups

(1) Given finite, abelian group $\mathcal{G} \subset GL(n, \mathbb{K})$ acting on $\mathbb{K}^n$

- construct rational invariants of action
  - rational invariant : $f \in \mathbb{K}(\mathbf{x}) \;:\; f(\, g \cdot \mathbf{x}\,) = f(\,\mathbf{x}\,) \qquad \forall g \in \mathcal{G}$
- determine rewrite rules for this action

(2) Given system of polynomial equations

- if have group action then 'reduce' polynomial system
- conversely : determine finite abelian group action (if possible)

References

This talk is a report on paper

- Hubert & Labahn, Rational invariants of Finite Abelian Groups, To appear in *Mathematics of Computation*

Relevant other publications

- K. Gatermann (ISSAC 1990)
  - : Using group actions to reduce Gröbner bases comp.
- J-C Faugère and J. Svartz (ISSAC 2013)
  - : Using abelian group actions to reduce polynomial systems.
- E. Hubert and G. Labahn (ISSAC 2012, FoCM 2013)
  - : Scaling symmetries

Example : Invariant Polynomial System

Consider the following system of polynomial equations

$$\begin{aligned} x_1 + x_2 + x_3 - x_1x_2 - x_1x_3 - x_2x_3 + 12 &= 0 \\ x_1x_2 + x_2x_3 + x_1x_3 - 15 &= 0 \\ x_1x_2x_3 - 13 &= 0 \end{aligned}$$

Example : Invariant Polynomial System

Consider the following system of polynomial equations

$$\begin{aligned} x_1 + x_2 + x_3 - x_1x_2 - x_1x_3 - x_2x_3 + 12 &= 0 \\ x_1x_2 + x_2x_3 + x_1x_3 - 15 &= 0 \\ x_1x_2x_3 - 13 &= 0 \end{aligned}$$

Solution space of system is invariant under the order 3 permutation

$$(x_1,\ x_2,\ x_3) \ \rightarrow \ (x_2,\ x_3,\ x_1).$$

Goal : work “modulo” this order 3 permutation.

Example : Invariant Polynomial System

(i) Find invariants

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} \left(3x_1{}^2x_2 + 3x_1x_3{}^2 + 3x_2{}^2x_3\right)\eta^2 + \left(3x_1{}^2x_3 + 3x_1x_2{}^2 + 3x_2x_3{}^2\right)\eta + \left(x_1{}^3 + 6x_1x_2x_3 + x_2{}^3 + x_3{}^3\right) \\ (x_1x_2 + x_1x_3 + x_2x_3)\eta^2 + (x_1x_2 + x_1x_3 + x_2x_3)\eta + \left(x_1{}^2 + x_2{}^2 + x_3{}^2\right) \\ x_1 + x_2 + x_3 \end{bmatrix}.$$

(η primitive cube root of unity)

(ii) Rewrite system in terms of invariants

$$\begin{aligned} 3y_2 + 3y_3 - 3y_3{}^2 + 12 &= 0, \\ -3y_2 + 3y_3{}^2 - 15 &= 0, \\ y_1 + \frac{y_2^3}{y_1} + y_3{}^3 - 3y_2y_3 - 13 &= 0. \end{aligned}$$

(iii) Solve invariant system for (y_1, y_2, y_3) (2 solutions)

(iv) Work back to get (x_1, x_2, x_3) (6 solutions)

The Process

- Change coordinates
- Scaling actions
- Arithmetic with exponents
- Polynomial system : solve and work back

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive cube root of unity.

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive cube root of unity.

- Polynomial system now looks like :

$$\begin{aligned} 0 &= 3z_1z_2 + 3z_3 - 3z_3^2 + 12 \\ 0 &= -3z_1z_2 + 3z_3^2 - 15 \\ 0 &= z_1^3 + z_2^3 + z_3^3 - 3z_1z_2z_3 - 13 \end{aligned}$$

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive cube root of unity.

- Group action now looks like :

$$(z_1,\ z_2,\ z_3) \ \to \ (\ \eta \cdot z_1,\ \ \eta^2 \cdot z_2,\ \ z_3\ )$$

Note : Action looks like 'rescaling' of coordinates

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive 3 root of unity.

- Group action now looks like :

$$(z_1,\ z_2,\ z_3) \ \to \ (\ \eta \cdot z_1,\ \ \eta^2 \cdot z_2,\ \ z_3\ )$$

Notice : $\frac{z_2}{z_1^2}$, z_2^3, $z_1 z_2 z_3$ all rational invariant functions

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive cube root of unity.

- Group action now looks like :

$$(z_1,\ z_2,\ z_3) \ \to \ (\ \eta \cdot z_1,\ \ \eta^2 \cdot z_2,\ \ z_3\ )$$

Notice : $z_1^3, \quad z_1 \cdot z_2, \quad z_3$ all rational invariant functions

The Process : $\mathbb{Z}_3$

- Change to 'Fourier' coordinates $(x_1, x_2, x_3) \to (z_1, z_2, z_3)$:

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \eta & \eta^2 & 1 \\ \eta^2 & \eta & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$$

where η is a primitive cube root of unity.

- Group action now looks like :

$$(z_1,\ z_2,\ z_3) \ \to \ (\ \eta \cdot z_1,\ \ \eta^2 \cdot z_2,\ \ z_3\ )$$

Notice : $z_1^3, \quad z_1 \cdot z_2, \quad z_3$ all rational invariant functions

How to rewrite polynomial system in terms of invariants?

The Process : $\mathbb{Z}_3$

- Group action now looks like :

$$(z_1,\ z_2,\ z_3) \ \rightarrow \ (\ \eta \cdot z_1,\ \ \eta^2 \cdot z_2,\ \ z_3\ )$$

Notice :

$$y \ = \ z_1^a \cdot z_2^b \cdot z_3^c \ \ = \ \ \eta^{a+2b} \ \ z_1^a \cdot z_2^b \cdot z_3^c$$

is a rational invariant function iff

$$a + 2b \equiv 0 \mod 3$$

- Kernel determined via integer linear algebra on exponents.

- Rewrite rules reverse such kernel operations

The Process : $\mathbb{Z}_3$

Original transformed polynomial system:

$$\begin{aligned} 0 &= 3z_1z_2 + 3z_3 - 3z_3^2 + 12 \\ 0 &= -3z_1z_2 + 3z_3^2 - 15 \\ 0 &= z_1^3 + z_2^3 + z_3^3 - 3z_1z_2z_3 - 13 \end{aligned}$$

* $y_1 = z_1^3,\ y_2 = z_1 \cdot z_2,\ y_3 = z_3$ – rational invariants

* $z_1 = y_1^{1/3},\ z_2 = \frac{y_2}{y_1^{1/3}},\ z_3 = y_3$ – rewrite rules

- Rational invariant system

$$\begin{aligned} 0 &= 3y_2 + 3y_3 - 3y_3^2 + 12 \\ 0 &= -3y_2 + 3y_3^2 - 15 \\ 0 &= y_1 + \frac{{y_2}^3}{y_1} + y_3^3 - 3y_2y_3 - 13 \end{aligned}$$

General Process : $\mathcal{G} \subset GL_n(\mathbb{K})$

(1) Fourier step $\equiv$ matrix diagonalization

(2) Finite group + diagonalization $\equiv$ scaling

- order and exponent matrices

(3) Rational invariants $\equiv$ kernel of exponents + order

- integer linear algebra

(4) Rewrite rules $\equiv$ 'inverting' kernels

‘Fourier Step = Diagonalization ’

$\mathcal{G}$: finite abelian subgroup $\mathrm{GL}_n(\mathbb{K})$ (order $p = p_1 \cdots p_s$)

‘Fourier Step = Diagonalization ’

$\mathcal{G}$: finite abelian subgroup $\mathrm{GL}_n(\mathbb{K})$ (order $p = p_1 \cdots p_s$)

(i) $\mathcal{G}$ is diagonalizable .

- $\exists$ matrix R such that $\mathcal{D} = R^{-1} \cdot \mathcal{G} \cdot R$ all diagonal matrices

'Fourier Step = Diagonalization '

$\mathcal{G}$: finite abelian subgroup $\mathrm{GL}_n(\mathbb{K})$ (order $p = p_1 \cdots p_s$)

(i) $\mathcal{G}$ is diagonalizable .

- $\exists$ matrix R such that $\mathcal{D} = R^{-1} \cdot \mathcal{G} \cdot R$ all diagonal matrices

- Let $\mathbf{x} = R \cdot \mathbf{z}$. Then have diagonal action

$$\mathcal{D} \times \mathbb{K}^n \to \mathbb{K}^n$$

$$\left(diag(d_1, \ldots, d_n), (z_1, \ldots, z_n) \right) \mapsto (d_1 \cdot z_1, \ldots, d_n \cdot z_n)$$

‘Exponents = Finite Direct Sum ’

$\mathcal{G}$: finite abelian subgroup $\mathrm{GL}_n(\mathbb{K})$ (order $p = p_1 \cdots p_s$)

(ii) Group isomorphism : $\mathcal{D} \leftrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$

Explicit via exponents :

$$\mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s} \rightarrow \mathcal{D}$$

$$(m_1, \ldots, m_s) \mapsto D_1^{m_1} \cdots D_s^{m_s}$$

'Exponents = Finite Direct Sum '

$\mathcal{G}$: finite abelian subgroup $\mathrm{GL}_n(\mathbb{K})$ (order $p = p_1 \cdots p_s$)

(ii) Group isomorphism : $\mathcal{D} \leftrightarrow \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}$

Explicit via exponents :

$$\mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s} \rightarrow \mathcal{D}$$

$$(m_1, \ldots, m_s) \mapsto D_1^{m_1} \cdots D_s^{m_s}$$

Diagonal action:

$$(\ diag(\ d_1, \ \ldots, \ d_n\ ), (z_1, \ldots, z_n) \ ) \mapsto (d_1 \cdot z_1, \ \ldots, \ d_n \cdot z_n)$$

with each $d_j = D_1^{m_{1j}} \cdots D_s^{m_{sj}}$

Notation

- Diagonal action : $(\alpha,\beta) \in \mathbb{Z}_7 \times \mathbb{Z}_5$:

$$(z_1,\ z_2,\ z_3,\ z_4,\ z_5) \to \left(\alpha^6\, z_1,\ \beta^3\, z_2,\ \frac{\beta}{\alpha^4}\, z_3,\ \frac{\alpha}{\beta^4}\, z_4,\ \alpha^3\beta^3\, z_5\right).$$

- Exponent and Order matrices:

$$A := \begin{bmatrix} 6 & 0 & -4 & 1 & 3 \\ 0 & 3 & 1 & -4 & 3 \end{bmatrix} \qquad P := \begin{bmatrix} 7 & & & & \\ & 5 & & & \end{bmatrix}$$

- Notation:

$$(\ \alpha,\ \beta\ )^A = \left(\ \alpha^6\ ,\ \beta^3\ ,\ \frac{\beta}{\alpha^4}\ ,\ \frac{\alpha}{\beta^4}\ ,\ \alpha^3\beta^3\ \right)$$

$$(z_1,\ z_2,\ z_3,\ z_4,\ z_5) \to (\ \alpha,\ \beta\ )^A \star (z_1,\ z_2,\ z_3,\ z_4,\ z_5)$$

Finite Abelian Group Actions

- Rational invariants
- Integer linear algebra
- Rewrite rules

Rational Invariants $\mathbb{K}(z)^A$

$F(z)$ is *invariant* under $\mathbf{z} \mapsto \lambda^A \star \mathbf{z}$ if $F(\lambda^A \star \mathbf{z}) = F(\mathbf{z})$

Lemma

Laurent monomials: $\mathbf{z}^v = z_1^{v_1} \cdots z_n^{v_n}, \quad v \in \mathbb{Z}^n$. *Invariant iff*

$$(\lambda^A \star \mathbf{z})^v = \mathbf{z}^v \quad \Leftrightarrow \quad A \cdot v = 0 \mod P$$

Lemma

Rational Invariants: $F(z) \in \mathbb{K}(z)^A$*:*

$$F(z) = \frac{\sum_{v \in \ker_{\mathbb{Z}} A \mod P} a_v z^v}{\sum_{v \in \ker_{\mathbb{Z}} A \mod P} b_v z^v}$$

Kernel? Use Hermite Normal Form

Diagonal action : $(\alpha, \beta) \in \mathbb{Z}_6 \times \mathbb{Z}_3$:

$$\begin{bmatrix} 4 & -1 & -3 & -6 & 0 \\ -1 & 4 & -3 & 0 & -3 \end{bmatrix}$$

$$[\ A,\ -P\ ]$$

exponent matrix

Kernel? Use Hermite Normal Form

Diagonal action : $(\alpha, \beta) \in \mathbb{Z}_6 \times \mathbb{Z}_3$:

$$\begin{bmatrix} 4 & -1 & -3 & -6 & 0 \\ -1 & 4 & -3 & 0 & -3 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$[\ A,\ -P\ ] \quad \rightarrow \quad [\ H_i \quad 0\ ]$$

exponent matrix

Hermite normal form

Kernel? Use Hermite Normal Form

Diagonal action : $(\alpha, \beta) \in \mathbb{Z}_6 \times \mathbb{Z}_3$:

$$\begin{bmatrix} 4 & -1 & -3 & -6 & 0 \\ -1 & 4 & -3 & 0 & -3 \end{bmatrix} \left[\begin{array}{ccccc} 1 & 1 & 3 & 2 & 1 \\ 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 2 & 1 & 0 \\ 1 & 0 & -1 & 2 & 0 \end{array}\right] = \begin{bmatrix} 3 & 2 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} A, & -P \end{bmatrix} \qquad \begin{bmatrix} V_i & V_n \\ P_i & P_n \end{bmatrix} \qquad \begin{bmatrix} H_i & 0 \end{bmatrix}$$

exponent matrix

unimodular multiplier

Hermite normal form

(Unimodular means $W = V^{-1} \in \mathbb{Z}^{5\times 5}$)

Hermite Normal Form

Diagonal action : $(\alpha, \beta) \in \mathbb{Z}_6 \times \mathbb{Z}_3$:

$$\begin{bmatrix} 4 & -1 & -3 & -6 & 0 \\ -1 & 4 & -3 & 0 & -3 \end{bmatrix} \begin{bmatrix} 1 & 1 & 3 & 2 & 1 \\ 1 & 0 & & 2 & 1 \\ 0 & 0 & & & 1 \\ 1 & 1 & 2 & 1 & 0 \\ 1 & 0 & -1 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 \end{bmatrix}$$

$$[\ A,\ -P\ ] \qquad \begin{bmatrix} V_i & V_n \\ P_i & P_n \end{bmatrix} \qquad [\ H_i \quad 0\ ]$$

exponent matrix

unimodular multiplier

Hermite normal form

Note : V not unique but can be normalized. Implies V_n is special

Rational Invariants and Rewrite Rules

Theorem

$A \in \mathbb{Z}^{s \times n}$, $\quad [A \ , \ -P] \cdot V = [H, 0]$,

$$V = \begin{bmatrix} V_i & V_n \\ P_i & P_n \end{bmatrix}, \qquad W = V^{-1} = \begin{bmatrix} W_u & P_u \\ W_d & P_d \end{bmatrix}$$

(a) $y = [z_1, \ldots, z_n]^{V_n}$ *form generating set of rational invariants.*

(b) V *normalized : components of* $y = [z_1, \ldots, z_n]^{V_n}$ *are polynomials.*

(c) *Rewrite rule :* $F \in \mathbb{K}(z)^A \implies F(z) = F(y^{(W_d - P_d P_u^{-1} W_u)})$

Why?

Rational Invariants and Rewrite Rules

Theorem

$A \in \mathbb{Z}^{s \times n}$, $\quad [A \ , \ -P] \cdot V = [H, 0]$,

$$V = \begin{bmatrix} V_i & V_n \\ P_i & P_n \end{bmatrix}, \qquad W = V^{-1} = \begin{bmatrix} W_u & P_u \\ W_d & P_d \end{bmatrix}$$

(a) $y = [z_1, \ldots, z_n]^{V_n}$ *form generating set of rational invariants.*

(b) V *normalized : components of* $y = [z_1, \ldots, z_n]^{V_n}$ *are polynomials.*

(c) *Rewrite rule :* $F \in \mathbb{K}(z)^A \implies F(z) = F(y^{(W_d - P_d P_u^{-1} W_u)})$

Why? $v = V_n(W_d - P_d P_u^{-1} W_u)v$. any term z^v with $v \in colspan_{\mathbb{Z}} V_n$:

$$\begin{aligned} z^v &= z^{V_n(W_d - P_d P_u^{-1} W_u)v} \\ &= (z^{V_n})^{(W_d - P_d P_u^{-1} W_u)v} \\ &= (y^{(W_d - P_d P_u^{-1} W_u)})^v \end{aligned}$$

Then use Lemma.

Example : Rational Invariants for $\mathbb{Z}_n$

$\mathcal{G}$ be cyclic group of permutations $(1, 2, \cdots, n)$.

- Diagonalizing matrix $R(\eta) = \left[\eta^{ij}\right]$, ($\eta$ n-root of unity)
  $\mathcal{D} : A = \left[1 \quad 2 \quad 3 \quad \ldots \quad n-1 \quad 0\right]$ and $P = \left[n\right]$.

$$V = \left[\begin{array}{c|cccccc} 1 & n & n-2 & \cdots & \cdots & 1 & 0 \\ 0 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \ddots & 0 \\ \vdots & 0 & 0 & \cdots & \cdots & 0 & 1 \\ \hline 0 & 1 & 1 & \ldots & \ldots & 1 & 0 \end{array}\right] \text{ and } W = \left[\begin{array}{cccccc|c} 1 & 2 & 3 & \cdots & n-1 & 0 & -n \\ \hline 0 & -1 & -1 & \cdots & -1 & 0 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & & \ddots & 1 & 0 \\ 0 & \ldots & \ldots & \ldots & 0 & 1 & 0 \end{array}\right].$$

- generating invariants are

$$g = z^{V_n} = \left(z_1^n,\ z_1^{n-2} z_2,\ z_1^{n-3} z_3,\ \ldots,\ z_1 z_{n-1},\ z_n\right),$$

- associated rewrite rules are

$$z \to g^{W_d - P_d P_u^{-1} W_u} = \left(g_1^{\frac{1}{n}},\ \frac{g_2}{g_1^{\frac{n-2}{n}}},\ \ldots \frac{g_{n-1}}{g_1^{\frac{1}{n}}},\ g_n\right), \quad \text{that is,} \quad z_k \to \frac{g_k}{g_1^{\frac{n-k}{n}}}$$

Example : Rational Invariants for $\mathbb{Z}_n \times \mathbb{Z}_n$

- $\mathcal{D} : A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \end{bmatrix}$ and $P = \begin{bmatrix} n & 0 \\ 0 & n \end{bmatrix}$.

$$V = \left[\begin{array}{cc|ccccccc} 2 & -1 & n & 0 & 1 & 2 & \cdots & & n-2 \\ -1 & 1 & 0 & n & n-2 & n-3 & \cdots & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & & 0 & \\ \vdots & \vdots & & & & & \ddots & \vdots & \vdots \\ & & & & & & & 1 & 0 \\ \vdots & \vdots & & & & & & & 1 \\ \hline 0 & 0 & 1 & 1 & 1 & \cdots & \cdots & 1 & 1 \\ 0 & 0 & 1 & 2 & 2 & \cdots & \cdots & 2 & 1 \end{array}\right] \quad W = \left[\begin{array}{cccccc|c} 1 & 1 & 1 & \cdots & 1 & 1 & -n \\ 1 & 2 & 3 & \cdots & n-1 & 0 & 0 \\ \hline 0 & 0 & 0 & \cdots & 0 & -1 & 2 \\ 0 & 0 & -1 & \cdots & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & & & & \vdots \\ \vdots & \vdots & & 1 & & & \vdots \\ \vdots & \vdots & & & \ddots & \vdots & \vdots \\ \vdots & \vdots & & & & \vdots & \vdots \\ 0 & 0 & & & & 1 & 0 \end{array}\right]$$

- generating invariants are

$$g = z^{V_n} = \left(z_1^n,\ z_2^n,\ z_1 z_2^{n-2} z_3,\ z_1^2 z_2^{n-3} z_4,\ \ldots,\ z_1^{n-3} z_2^2 z_{n-1},\ z_1^{n-2} z_2 z_n\right),$$

- associated rewrite rules are

$$z \to g^{W_d - P_d P_u^{-1} W_u} = \left(g_1^{\frac{1}{n}},\ g_2^{\frac{1}{n}},\ \frac{g_3}{g_1^{\frac{1}{n}}\, g_2^{\frac{n-2}{n}}},\ \ldots,\ \frac{g_{n-1}}{g_1^{\frac{n-3}{n}}\, g_2^{\frac{2}{n}}},\ \frac{g_n}{g_1^{\frac{n-2}{n}}\, g_2^{\frac{1}{n}}} \right).$$

Solving Polynomial Systems

- Using invariants and rewrite rules
- $(A \;\; P)$-degree and $(A \;\; P)$-homogeneous
- Solving invariant systems

Example : Invariant Dynamic System

Consider system of polynomial equations (c parameter)[1]

$$\begin{aligned} 1 - cx_1 - x_1x_2^2 - x_1x_3^2 &= 0 \\ 1 - cx_2 - x_2x_1^2 - x_2x_3^2 &= 0 \\ 1 - cx_3 - x_3x_1^2 - x_3x_2^2 &= 0 \end{aligned}$$

[1] Steady state for Neural network model [Noonburg SIAM 1989]

Example : Invariant Dynamic System

Consider system of polynomial equations (c parameter)[1]

$$\begin{aligned} 1 - cx_1 - x_1x_2^2 - x_1x_3^2 &= 0 \\ 1 - cx_2 - x_2x_1^2 - x_2x_3^2 &= 0 \\ 1 - cx_3 - x_3x_1^2 - x_3x_2^2 &= 0 \end{aligned}$$

Solution space of system is invariant under the permutation

$$(x_1,\ x_2,\ x_3) \ \rightarrow \ (x_2,\ x_3,\ x_1).$$

However no polynomial is invariant under the permutation.

[1] Steady state for Neural network model [Noonburg SIAM 1989]

(A, P)-homogeneity (Faugère and Svartz)

Definition

(i) $\deg_{(A,P)}(z^u) = A \cdot u \mod P$

(ii) $f \in \mathbb{K}[z, z^{-1}]$ can be written as

$$f = \sum_{d \in \mathcal{Z}} f_d$$

terms in f_d $\deg_{(A,P)} = d$ (homogeneous of (A, P)-degree d)

Lemma

$f \in \mathbb{K}[z, z^{-1}]$ is (A, P)-homogeneous of (A, P)-degree d iff

$$f\left(\lambda^A \star z\right) = \lambda^d f(z)$$

for all $\lambda \in \mathcal{U}$.

Solving via (A, P)-homogenous components

Theorem

Let $F \subset \mathbb{K}[z, z^{-1}]$ and $F^h = \{f_d \,|f \in F,\ d \in \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}\}$ set of homogeneous components of F.

If set of toric zeros of F is invariant by the diagonal action of $\mathcal{U}$ defined by A then it is equal to toric zeros of F^h.

Solving via (A, P)-homogenous components

Theorem

Let $F \subset \mathbb{K}[z, z^{-1}]$ and $F^h = \{f_d \,|f \in F,\ d \in \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_s}\}$ set of homogeneous components of F.

If set of toric zeros of F is invariant by the diagonal action of $\mathcal{U}$ defined by A then it is equal to toric zeros of F^h.

Why:

Since $f(\lambda^A \star z) = \sum_d \lambda^d f_d(z)$ for all $\lambda \in \mathcal{U}$ we have a square linear system

$$\left(f(\lambda^A \star z)\right)_{\lambda \in \mathcal{U}} = \left(\lambda^d\right)_{\lambda \in \mathcal{U}, d \in \mathcal{Z}} (f_d)_{d \in \mathcal{Z}}\,.$$

With an appropriate ordering of the elements of $\mathcal{U}$ and $\mathcal{Z}$ the square matrix $\left(\lambda^d\right)_{\lambda \in \mathcal{U}, d \in \mathcal{Z}}$ is the Kronecker product of the Vandermonde matrices $\left(\xi_i^{(k-1)(l-1)}\right)_{1 \le k,l \le p_i}$, for $1 \le i \le s$ and ξ_i a primitive p_ith root of unity. So it is invertible.

Example : Neural Network

Recall Neural Network system (c is a parameter):

$$\begin{aligned} 1 - cx_1 - x_1x_2^2 - x_1x_3^2 &= 0 \\ 1 - cx_2 - x_2x_1^2 - x_2x_3^2 &= 0 \\ 1 - cx_3 - x_3x_1^2 - x_3x_2^2 &= 0 \end{aligned} \tag{1}$$

(i) Zeros invariant under permutation $\sigma = (321)$.

(ii) Diagonal action : exponents $A = [1\ 2\ 0]$; order $P = [3]$.

Example : Neural Network

(iii) Change coordinates via $x = R \cdot z$ gives

$$\begin{aligned} 0 &= f_0 &&= \mathfrak{f}_0 - \xi\,\mathfrak{f}_1 - \xi^2\mathfrak{f}_2 \\ 0 &= f_1 &&= \mathfrak{f}_0 - \xi^2\mathfrak{f}_1 - \xi\,\mathfrak{f}_2 \\ 0 &= f_2 &&= \mathfrak{f}_0 - \mathfrak{f}_1 - \mathfrak{f}_2 \end{aligned}$$

where

$$\begin{aligned} \mathfrak{f}_0 &= 1 - cz_3 + z_1^3 + z_2^3 - 2z_3^3 \\ \mathfrak{f}_1 &= cz_1 + 3z_1^2z_2 - 3z_2^2z_3 \\ \mathfrak{f}_2 &= cz_2 + 3z_1z_2^2 - 3z_1^2z_3. \end{aligned}$$

(iv) Each $\mathfrak{f}_i$ is (A, P)-homogeneous of degree i, for $0 \leq i \leq 2$.

Example (cont.)

(i) What about non-toric zeros? Localize at z_1

(ii) The reduced system corresponding to $\left\{f_0, \frac{f_1}{z_1}, \frac{f_2}{z_1^2}\right\}$ is

$$0 = 1+y_1-cy_3-2y_3^2+\frac{y_2^3}{y_1}, \quad 0 = c+3y_2-3\frac{y_2^2y_3}{y_1}, \quad 0 = -3y_3+c\frac{y_2}{y_1}+3\frac{y_2^2}{y_1}.$$

(iii) This system has $6 = 2 + 4$ zeros : union of triangular sets

$$y_3 = 0, \quad y_2 = \frac{c}{3}, \quad y_1^2 + y_1 - \frac{c^3}{27} = 0;$$

and

$$162\,c\,y_3^4 - 54\,y_3^3 + 81\,c^2\,y_3^2 - 108\,c\,y_3 + 4\,c^3 + 27 = 0,$$

$$y_2 = -\frac{81\,c}{49\,c^3 - 27}\,y_3^3 - \frac{14\,c^3}{49c^3 - 27}\,y_3^2 - \frac{93\,c^2}{2(49\,c^3 - 27)}\,y_3 - \frac{c\,(70\,c^3 - 243)}{6\,(49\,c^3 - 27)}$$

$$y_1 = y_3^3 + \frac{c}{2}\,y_3 - \frac{1}{2}.$$

Example (cont.)

Original system has 6 orbits of zeros, that is 18 solutions, where $z_1 = \xi^2 x_1 + \xi x_2 + x_3 \neq 0$.

(i) Given sol. (y_1, y_2, y_3) orbit : by solve triangular system:

$$z_1^3 = y_1, \quad z_1 z_2 = y_2, \quad z_3 = y_3.$$

(ii) With $x = R\, z$ get 18 solutions of the system with 6 orbits.

What about $z_1 = 0$?

(iii) Here, there are three solutions satisfying

$$z_1 = 0, \quad z_2 = 0, \quad 2\, z_3^3 + c\, z_3 - 1 = 0.$$

(iv) They each form an orbit. The corresponding solutions :

$$x_1 = x_2 = x_3 = \eta, \text{ for } 2\,\eta^3 + c\,\eta - 1 = 0.$$

Total number of solutions : 21.

Determining groups of homogeneity

- Matrix of exponents of polynomial system
- Smith Form and finding A and P

Matrix of Exponents of System

Rational functions in $\mathbb{K}(z_1, \ldots, z_n)$. K matrix of exponents.

$$\begin{aligned} f_1 &= {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 - z_1 z_2 z_3 + 8 \\ f_2 &= {z_1}^2 {z_2}^2 {z_3}^2 - {z_2}^3 + 7 \\ f_3 &= z_1^6 z_2^3 z_3^3 - 3 z_1^4 z_2^4 z_3 + z_1^6 + z_2^3 + 32 z_1^3 \end{aligned}$$

Matrix of Exponents :

$$K = \begin{bmatrix} 2 & 0 & 1 & 2 & 0 & 3 & 1 & 3 & -3 \\ 2 & 3 & 1 & 2 & 3 & 3 & 4 & 0 & 3 \\ 2 & 0 & 1 & 2 & 0 & 3 & 1 & 0 & 0 \end{bmatrix}.$$

Smith Normal Form and finding A and P

Smith normal form K : $U \cdot K \cdot V = \begin{bmatrix} diag(1, ..., 1, p_1, ..., p_s) & 0 \end{bmatrix}$

Theorem

$$\textit{Partition: } U = \begin{bmatrix} C \\ A \end{bmatrix} \quad \textit{and} \quad U^{-1} = \begin{bmatrix} U_0 & U_1 \end{bmatrix}$$

(i) F *invariants for diagonal action*

$$P = \text{diag}\,(p_1, \ldots, p_s), \qquad A = \textit{the last } s \textit{ rows of } U.$$

(ii) $[y_1, \ldots, y_n] = z^{\begin{bmatrix} U_0 & U_1 P \end{bmatrix}}$ *minimal generating invariants*

(iii) *Rewrite rule : for any invariant* $f \in \mathbb{K}(z)$ *of* (A, P)*:*

$$f(z) = f\left(y^{\begin{bmatrix} C \\ P^{-1}A \end{bmatrix}}\right).$$

Matrix from previous example:

$$K = \begin{bmatrix} 2 & 0 & 1 & 2 & 0 & 3 & 1 & 3 & -3 \\ 2 & 3 & 1 & 2 & 3 & 3 & 4 & 0 & 3 \\ 2 & 0 & 1 & 2 & 0 & 3 & 1 & 0 & 0 \end{bmatrix}.$$

Smith normal form:

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix} \cdot K \cdot V = \left[\begin{array}{ccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Matrix from previous example:

$$K = \begin{bmatrix} 2 & 0 & 1 & 2 & 0 & 3 & 1 & 3 & -3 \\ 2 & 3 & 1 & 2 & 3 & 3 & 4 & 0 & 3 \\ 2 & 0 & 1 & 2 & 0 & 3 & 1 & 0 & 0 \end{bmatrix}.$$

Smith normal form:

$$\begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 1 \\ 1 & -1 & 0 \end{bmatrix} \cdot K \cdot V = \left[\begin{array}{ccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 3 & & 0 & 0 & 0 & 0 & 0 & 0 \\ & & 3 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

The underlying symmetry group is $\mathbb{Z}_3 \times \mathbb{Z}_3$.

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$$

Invariant exponents:

$$V_n = [\ U_0 \quad U_1 P\ ] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & -3 \\ 1 & 3 & 3 \end{bmatrix} \approx \begin{bmatrix} 3 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Future Research Directions

(i) Extend to parameterized and dynamic systems

(ii) Extend from Finite Abelian to Finite Solvable Group actions

- e.g. Neural network example invariant under S_3.

(iii) Combine scaling symmetries with finite diagonal actions

- makes use of Smith Normal Form