Characteristic Set and Resolvent for Difference Polynomial Systems

Xiao-Shan Gao

Institute of Systems Science

Chinese Academy of Sciences

Outline of the Talk

- Background
- Difference Ascending Chain
- Coherent and Regular Ascending Chain
- Irreducible Ascending Chain
- A Decomposition Algorithm
- Difference Resolvent System

CS Method: An Example

The 4-cyclic equation system:

$$
\begin{aligned}
&x_4 + x_3 + x_2 + x_1 = 0\\
&x_4 * x_3 + x_3 * x_2 + x_2 * x_1 + x_1 * x_4 = 0\\
&x_4 * x_3 * x_2 + x_3 * x_2 * x_1 + x_2 * x_1 * x_4 + x_1 * x_4 * x_3 = 0\\
&x_4 * x_3 * x_2 * x_1 - 1 = 0
\end{aligned}
$$

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\mathcal{A}_1) \cup \text{Zero}(\mathcal{A}_2)$$

$$\mathcal{A}_1 = \{x_1 x_4 - 1 = 0, x_3 + x_1 = 0, x_1 x_2 + 1 = 0\}$$

$$\mathcal{A}_2 = \{x_1 x_4 + 1 = 0, x_3 + x_1 = 0, x_1 x_2 - 1 = 0\}$$

The Solutions: $x_1 = a, x_2 = -\frac{1}{a}, x_3 = -a, x_4 = \frac{1}{a}$

$x_1 = a, x_2 = \frac{1}{a}, x_3 = -a, x_4 = -\frac{1}{a}$

Ascending Chain: Algebraic Case

$$\mathcal{A} = \begin{cases} A_1(u_1, \ldots, u_q, y_1) & = I_1 y_1^{d_1} + \text{ lower terms in } y_1 \\ A_2(u_1, \ldots, u_q, y_1, y_2) & = I_2 y_2^{d_2} + \text{ lower terms in } y_2 \\ \quad \cdots & \cdots \\ A_p(u_1, \ldots, u_q, y_1, \ldots, y_p) & = I_p y_p^{d_p} + \text{ lower terms in } y_p \end{cases}$$

Number of Parameters q: Dimension of the solutions.

Leading Degree d_i: Number of the solutions.

Idea of CS: Use a minimal chain in an ideal, called CS, to represent the whole ideal.

Saturation Ideal:

$$\mathbf{sat}(\mathcal{A}) = (\mathcal{A}) : \mathbf{I}_{\mathcal{A}}. \quad \mathbf{I}_{\mathcal{A}} = \{J \,|, J = \textstyle\prod_{i=1}^{n} I_i^{s_i}\}$$

Differential Algebra vs CS

In Differential Algebra founded by Ritt, **CS** plays the central role.

1. If $\mathcal{A}$ is irreducible, then $\mathbf{sat}(\mathcal{A})$ is a prime ideal of dimension $\mathbf{dim}(\mathcal{A})$.
2. For a d-polynomial set $\mathbb{P}$, one can construct irreducible chains $\mathcal{A}_i$ such that
$$\mathrm{Zero}(\mathbb{P}) = \cup_i \mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i))$$
3. Formal power series solutions for an irreducible chain can be computed.

In the past 20 years, more efficient algorithms and important applications for CS were found. (ISSAC04, ISSAC05)

Difference Algebra vs CS

In Difference Algebra founded by Cohn, **Difference Kernel** instead of CS plays the central role, which bridges the difference case and the usual algebraic case.

Ritt and Doob defined the difference ascending chain and used them to prove the Noertherian property of difference perfect ideals.

Theories and *algorithms* for difference CS were basically untouched.

Difference Ascending Chain

An Example

$y(x)$: a function in x. Transform operator: $\mathbf{E}x = x + 1$

$P = (y(x+1) - y(x))^2 - 2(y(x+1) + y(x)) + 1 = 0$

$\mathbf{E}P - P = P_1 P_2$

$$P_1 = y(x+2) - y(x),$$

$$P_2 = y(x+2) - 2y(x+1) + y(x) - 2.$$

$\text{Zero}(P) = \text{Zero}(P, P_1) \cup \text{Zero}(P, P_2)$

Solutions:

$\mathcal{A}_1 = P, P_1,$ Solution: $y = (c(x)e^{i\pi x} + \frac{1}{2})^2$

$\mathcal{A}_2 = P, P_2,$ Solution: $y = (x + (c(x))^2$

$c(x)$ is a periodic function: $c(x+1) = c(x)$.

Difference Polynomials (r-pols)

Difference Field: a field with a transforming operation:

$$\mathbf{E}(a+b) = \mathbf{E}a + \mathbf{E}b,\ \mathbf{E}(ab) = \mathbf{E}a \cdot \mathbf{E}b,\ \mathbf{E}a = 0 \Leftrightarrow a = 0.$$

A Difference Field: $\mathbf{K} = \mathbf{Q}(x)$ with $\mathbf{E}f(x) = f(x+1)$.

Difference Polynomials: $\mathbf{K}\{y_1, \ldots, y_n\} = \mathbf{K}[\mathbf{E}^k y_j]$.

Notation: $y_{i,j} = \mathbf{E}^j y_i = y_i(x+j)$.

A Canonical Representation:

$$P(y_1, \ldots, y_p) = I_d y_p(x+o)^d + I_{d-1} y_p(x+o)^{d-1} + \ldots + I_0$$

$p = \mathrm{cls}(P)$, $o = \mathrm{ord}(P, y_p)$, $I_d = \mathrm{init}(P)$, $\mathrm{lead}(P) = y_{p,o}$.

Compare with Differential Case

Differential Case: $y_{(o)}$: $o-$the derivative of y

$$P = Iy_{(o)}^d + I_{d-1}y_{(o)}^{d-1} + \cdots + I_0$$

$$P' = Sy_{(o+1)} + U_1$$

$$P'' = Sy_{(o+2)} + U_2$$

Linear in $y_{(o+i)}, i > 0$. Pivots: I and S.

Difference Case:

$$P = Iy(x+o)^d + I_{d-1}y(x+o)^{d-1} + \cdots + I_0$$

$$\mathbf{E}P = \mathbf{E}I_d y(x+o+1)^d + \cdots + \mathbf{E}I_0$$

$$\mathbf{E}^2 P = \mathbf{E}^2 I_d y(x+o+2)^d + \cdots + \mathbf{E}^2 I_0$$

Not-linear in $y(x+o+i), i > 0$. Pivots: $\mathbf{E}^i I, i = 0, 1, 2, \cdots$.

Difference Asc Chain

P is **Difference Reduced** wrt Q ($\text{lead}(Q) = y_{p,o}$) if

$\deg(P, y_{p,o+i}) < \deg(Q, y_{i,o})$ for $i \geq 0$.

Difference Asc Chain: Auto-reduced r-pol sequence

$$\mathcal{A} = \begin{cases} A_{1,1}(\mathbb{U}, y_1), \ldots, A_{1,k_1}(\mathbb{U}, y_1) \\ A_{2,1}(\mathbb{U}, y_1, y_2), \ldots, A_{2,k_2}(\mathbb{U}, y_1, y_2) \\ \ldots \\ A_{p,1}(\mathbb{U}, y_1, \ldots, y_p), \ldots, A_{1,k_p}(\mathbb{U}, y_1, \ldots, y_p) \end{cases} \tag{1}$$

For y_i: orders of $A_{i,j}$ increase, leading degrees decrease.

Dimension: $\text{ord}(\mathcal{A}) = |\mathbb{U}|$

Order: $\text{ord}(\mathcal{A}) = \sum_{i=1}^{p} \text{ord}(A_{i,1}, y_i)$

Degree: $\deg(\mathcal{A}) = \prod_{i=1}^{p} \text{ldeg}(A_{i,k_i})$

Extensions of Asc Chain

Extension of $\mathcal{A}$: For integers $h_i \geq 0$

$$\mathcal{A}_{(h_1,\cdots,h_p)} = A_{1,1}, \mathbf{E}A_{1,1}, \ldots, \mathbf{E}^{o_{1,2}-o_{1,1}-1}A_{1,1}, A_{1,2}, \\ \ldots, A_{1,k_1}, \mathbf{E}A_{1,k_1}, \ldots, \mathbf{E}^{\hat{h}_1-o_{1,k_1}}A_{1,k_1}$$

where $o_{i,j} = \mathrm{ord}(A_{i,j})$.

To fill the "gaps" and to make all the $y_i(o_{i,1}+k)$ appear.

$\mathcal{A}_{(h_1,\cdots,h_p)}$ is an algebraic triangular set.

Difference Pseudo Remainder:

$$\mathrm{rprem}(P,\mathcal{A}) = \mathrm{prem}(P,\mathcal{A}_{(\mathrm{ord}_{(P,y_1)},\cdots,\mathrm{ord}_{(P,y_p)})})$$

Coherent and Regular Chain

Coherent Asc. Chain

Example: $\mathcal{A} = A_1, A_2$.

$$A_1 = y(x+1)^2 - y^2(x) + 1$$
$$A_2 = y(x+2) + y(x+1)$$

$$\mathbf{E}A_1 - (y(x+2) + y(x+1))A_2 = 1.$$

Need coherent even in ordinary difference case

Coherent Chain: $\mathcal{A} = A_1, \cdots, A_m$; $o_i = \mathrm{ord}(A_i)$

$\mathrm{rprem}(\Delta_{ij}, \mathcal{A}) = 0, (i < j)$, where

(1) if $\mathrm{cls}(A_i) = \mathrm{cls}(A_j)$, $\Delta_{ij} = \mathrm{prem}(\mathbf{E}^{o_j - o_i} A_i, A_j, \mathrm{lvar}(A_j))$.

(2) otherwise, let $\Delta_{ij} = 0$.

Regular Chain: Algebraic Case

P **invertible** wrt $\mathcal{A}$: $(P, \mathcal{A}) \cap \mathbf{K}[\mathbb{U}] \neq \{0\}$

$\mathcal{A}$ is **regular**: I_i is invertible wrt $\mathcal{A}_{i-1}$

Example. $A_1 = x_1^2, A_2 = x_1 x_2$ is not regular.

Saturation Ideal:

$$\mathbf{sat}(\mathcal{A}) = \{P \mid \exists J \in \mathbf{I}_{\mathcal{A}}, JP \in (\mathcal{A})\}$$

Theorem. (Aubry-Lazard-Maza,99) The following are equivalent

1. $\mathcal{A}$ is regular;
2. $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$.
3. $\mathbf{sat}(\mathcal{A}) = \{P \mid \text{prem}(P, \mathcal{A}) = 0\}$.

Regular Difference Chain

P **Difference Invertible wrt** $\mathcal{A}$: P is algebraic invertible wrt $\mathcal{A}_{(\mathrm{ord}(P,y_1),\ldots,\mathrm{ord}(P,y_p))}$.

Difference Regular: $\mathbf{E}^i I_j$ are invertible wrt $\mathcal{A}$ for all i, j.

Theorem. $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$ iff $\mathcal{A}$ is coherent and difference regular.

There is no algorithm to test difference regularity, yet.

Key idea in the proof (1)

Canonical Representation:

Lemma. Let $\mathcal{A} = A_1, \ldots, A_m$ be a coherent ascending chain. Then

$P \in \mathbf{sat}(\mathcal{A}) \Rightarrow JP = \sum_{i,j} Q_{i,j}\mathbf{E}^i A_i$

(1) Leads of $\mathbf{E}^i A_i$ are different

(2) $\mathbf{E}^i A_i$ has the lowest leading degree

$$\begin{array}{rll} \mathcal{A}_{(h_1,\cdots,h_p)} = & A_1, \mathbf{E}A_1, \ldots, \mathbf{E}^{o_2-o_1-1}A_1 & \text{same degree} \\ & A_2, \mathbf{E}A_2, \ldots, \mathbf{E}^{o_3-o_2-1}A_2 & \text{lower degree} \end{array}$$

where $o_i = \mathrm{ord}(A_i, y_1)$.

Key idea in the proof (2)

A modified Rosenfeld lemma:

Lemma. Let $\mathcal{A}$ be a coherent and regular chain, and R an r-pol reduced wrt $\mathcal{A}$. If $R \in \mathbf{sat}(\mathcal{A})$, then $R = 0$.

$R \in \mathbf{sat}(\mathcal{A}) \Rightarrow JR = \sum_{i,j} Q_{i,j}\mathbf{E}^i A_i$

Eliminate $\mathbf{E}^i A_i$: Due to the regularity and coherency

If $\mathbf{E}^s A_i = \mathbf{E}^s I_d y(x+o+s)^d - U$

Replace $y(x+o+s)^d$ by $U/(\mathbf{E}^s I_d)$.

$J'R = \sum_{i,j} Q'_{i,j}\mathbf{E}^i A_i$ with lower order.

Irreducible Chain

Strong Irreducible Chain

P is effective in y_i: $\deg(P, y_i(x)) \neq 0$

$P = y_1(x+1)y_2(x+2)^2 - 1 = \mathbf{E}Q,$
$Q = y_1(x)y_2(x+1)^2 - 1.$
$\mathrm{Zero}(P) = \mathrm{Zero}(Q).$

$\mathcal{A}$ is strong irreducible:

- $\mathcal{A}_{(h_1,\ldots,h_m)}$ is algebraic irreducible for $h_i \geq 0$;
- $A_{c,1}$ is effective in y_c;
- $A_{c,1}$ is irreducible and effective module $\mathcal{A}_{c-1}$. Irreducible and effective in $\mathbf{K}(\eta_{c-1})[y_c(x), \ldots, y_c(x + f_c)]$, where $f_c = \mathrm{ord}(A_{c,1}, y_c)$, $B_c = \mathcal{A}_{(0,\ldots,0)} \cap \mathbf{K}\{U, y_1, \ldots, y_c\}$, and η_c is a generic point for the algebraic irreducible chain B_c.

CS of Reflexive Prime Ideals

Difference Ideal: $P \in I \Rightarrow \mathbf{E}P \in I$.

Reflexive Ideal: $\mathbf{E}P \in I \Rightarrow P \in I$.

Theorem. Let $\mathcal{A}$ be a coherent and strong irreducible chain. Then $\mathbf{sat}(\mathcal{A})$ is a reflexive prime difference ideal.

Conversely, let I be a reflexive prime difference ideal. We may choose a proper order of variables such that among the CSs of I, there exists one $\mathcal{A}$ which is coherent and strong irreducible, and $I = \mathbf{sat}(\mathcal{A})$.

Example. $A = y_2(x+1) - y_1(x)$: effective in y_1 but not in y_2.

There is no algorithm to test strong irreducibility, yet.

Constructive Results

Proper Irreducible Chain: In the definition of strong irreducible chain, replace the irreducibility of $\mathcal{A}_{(h_1,\cdots,h_p)}$ with that of $\mathcal{A}_{(0,\cdots,0)}$.

Algorithm exists to test proper irreducibility.

Main Theorem. $\mathcal{A}$ is coherent and proper irreducible $\Rightarrow \mathcal{A}$ is difference regular.

Key facts in the proof.

Lemma. If P is invertible wrt. $\mathcal{A}$, then $\mathbf{E}P$ is invertible wrt $\mathcal{A}$.

Lemma. If $P \in \mathbf{K}[V]$ where V is the parameter set of $A_{(0,\ldots,0)}$, then $\mathbf{E}P$ is invertible wrt $\mathcal{A}$.

Proper Irreducible Chain is Non-Trivial

Theorem. $\mathcal{A}$ is coherent and proper irreducible $\Rightarrow \mathrm{Zero}(\mathcal{A}/J) \neq \emptyset$.

$\mathrm{Zero}(\mathcal{A}/J) = \mathrm{Zero}(\mathcal{A}) - \mathrm{Zero}(J)$

Zeros are taken in a universal extension system $\mathbf{F}$.

Proper Irreducible Chain is Unmixed

Theorem. Let $\mathcal{A}$ be a coherent and proper irreducible chain, and

$$\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} P_i = \bigcap_{i=1}^{r} \mathbf{sat}(\mathcal{A}_i)$$

is an irredundant intersection of prime ideals. Then

(1) $\mathbb{U}$ is the parameter set of $\mathcal{A}_i$. $\mathbf{dim} P_i = \mathbf{dim} \mathcal{A}$.

(2) $\mathrm{ord}_{\mathbb{U}} P_i = \mathrm{ord} \mathcal{A}_i = \mathrm{ord} \mathcal{A}$.

(3) $\deg(\mathcal{A}) = \sum_{i=1}^{r} \deg(\mathcal{A}_i)$.

Difference Asc Chain

Difference Asc Chain:

$$\mathcal{A} = \begin{cases} A_{1,1}(\mathbb{U}, y_1), \ldots, A_{1,k_1}(\mathbb{U}, y_1) \\ A_{2,1}(\mathbb{U}, y_1, y_2), \ldots, A_{2,k_2}(\mathbb{U}, y_1, y_2) \\ \ldots \\ A_{p,1}(\mathbb{U}, y_1, \ldots, y_p), \ldots, A_{1,k_p}(\mathbb{U}, y_1, \ldots, y_p) \end{cases} \quad (2)$$

For y_i: orders of $A_{i,j}$ increase, leading degrees decrease.

Dimension: $\mathrm{ord}(\mathcal{A}) = |\mathbb{U}|$

Order: $\mathrm{ord}(\mathcal{A}) = \sum_{i=1}^{p} \mathrm{ord}(A_{i,1}, y_i)$

Degree: $\deg(\mathcal{A}) = \prod_{i=1}^{p} \mathrm{ldeg}(A_{i,k_i})$

Example

Example: $A = (y(x+1)-y(x))^2-2(y(x+1)+y(x))+1.$

$\mathbf{E}A - A = A_1 \cdot A_2$

$$A_1 = y(x+2) - y(x),$$

$$A_2 = y(x+2) - 2y(x+1) + y(x) - 2.$$

$\{\mathbf{sat}(A)\} = \mathbf{sat}(\mathcal{A}_1) \cap \mathbf{sat}(\mathcal{A}_2)$

Strong irreducible ascending chains:

$\mathcal{A}_1 = A, y(x+2) - y(x)$

$\mathcal{A}_2 = A, y(x+2) - 2y(x+1) + y(x) - 2$

Key Fact in the Proof

Difference Kernel: Let $\mathcal{D}$ be a difference field. A *difference kernel* R over $\mathcal{D}$ is an extension field, $\mathcal{D}(a, a_1, \ldots, a_r), r \geq 1$, of $\mathcal{D}$, each a_i denoting a vector $(a_i^{(1)}, \ldots, a_i^{(n)})$, and an extension τ of $\mathbf{E}$ to an isomorphism of

$$\mathcal{D}(a, a_1, \ldots, a_{r-1}) \Rightarrow \mathcal{D}(a_1, \ldots, a_r)$$

such that $\tau a_i = a_{i+1}, i = 0, 1, \ldots, r-1$. $(a_0 = a.)$

Lemma (Cohn). Let R be a difference kernel. Then there exists a finite number of principal realizations for R. The sum of the limit degrees of these principal realizations is the limit degree of R.

Cohn used the above result to obtain zero decomposition for a single r-pol. Our result on proper chain could be considered a generalization to the general case.

A Decomposition Algorithm

A Zero Decomposition Theorem

Theorem. Let $\mathbb{P} = \{P_1, \ldots, P_r\}$. Then we can find coherent and proper irreducible ascending chains $\mathcal{A}_i$ s.t.

$$\text{Zero}(\mathbb{P}) = \bigcup_i \text{Zero}(\mathbf{sat}(\mathcal{A}_i)).$$

$$\text{Zero}(\mathbb{P}) = \bigcup_i \text{Zero}(\mathcal{A}_i / J_i).$$

Applications:

(1) Automated theorem proving of theorems about difference equations.

(2) A new method to test radical ideal membership.

An Example

Fibonacci Numbers:

$$F_n\colon \quad F_{n+2} - F_{n+1} - F_n = 0, F_0 = 0, F_1 = 1.$$

Cassini Identity: $\quad F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$

Let $\mathbb{P} = \{P_1, P_2, P_3\}$.

$$P_1 = F_{n+2} - F_{n+1} - F_n$$

$$P_2 = a_{n+1} + a_n, a_0 = 1 \quad \text{(represent } (-1)^n\text{)}$$

$$P_3 = h_n - (F_{n+2}F_n - F_{n+1}^2 + a_n)$$

Under the variable order $h_n < a_n < F_n$

$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbf{sat}(\mathcal{A}))$

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\textbf{sat}(\mathcal{A})) = \text{Zero}(\mathcal{A})$$

$$\mathcal{A} = \begin{cases} h_{n+1} + h_n \\ a_{n+1} + a_n \\ -{F_{n+1}}^2 + F_n F_{n+1} + {F_n}^2 - h_n + a_n \\ F_{n+2} - F_{n+1} - F_n \end{cases}$$

h_n satisfies a first order difference equation

Check initial values: $h_0 = F_2 F_0 - F_1^2 + a_0 = 0$

$h_i = 0$ for all i.

Using linear algebra method: h_n satisfies:

$h_{n+3} - 2\,h_{n+2} - 2\,h_{n+1} + h_n$.

Resolvent Systems of Difference Ideals

The Idea of Resolvent

$\mathbb{P}$: a polynomial set in $x_1, \ldots, x_n$.

$w = \sum_i c_i x_i$: a linear transformation.

Then Zero($\mathbb{P}$) is given by:

$$R(w) = 0, x_1 = R_1(w), \ldots, x_n = R_n(w)$$

Applications of Resolvents: Primitive elements, factorization, QE, etc.

Difference Resolvents: (Cohn, DA)

For a reflexive prime ideal I, after certain linear transformation, $I_i y_{i,m_i} - V_i \in I$ where m_i is a non negative integer.

Resolvent system of a strong irreducible chain

Theorem. Let $\mathcal{A}$ be a coherent and strong irreducible chain.

There exists $\sigma_1, \ldots, \sigma_p$such that the CS of $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)$ under the variable order $\mathbb{U} < w < y_i$ is of the following form

$$R, R_1, \ldots, R_s, I_1 y_{1,0} - V_1, \ldots, I_p y_{p,0} - V_p$$

where $R, R_i, I_i, V_i \in K\{\mathbb{U}, w\}$.

Furthermore, R is effective in w and $\mathrm{ord}(R, w) = \mathrm{ord}(\mathcal{A})$.

Resolvent Ideal: $\mathbf{sat}(R, R_1, \ldots, R_s)$.

Resolvent System: $R, R_1, \ldots, R_s$.

Birational Equivalence

Corollary: Any irreducible difference variety V is birationally equivalent to an irreducible difference variety of codimension one.

Let $W = \text{Zero}(\mathbf{sat}(R, R_1, \ldots, R_s))$. The rational maps are defined as follows:

$$M_1 \ : \ V \Rightarrow W; (\mathbb{U}, y_1, \ldots, y_p) \Rightarrow (\mathbb{U}, \sum_{i=1}^{p} \sigma_i y_i)$$

$$M_2 \ : \ W \Rightarrow V; (\mathbb{U}, w) \Rightarrow (\mathbb{U}, \frac{V_1(\mathbb{U}, w)}{I_1(\mathbb{U}, w)}, \ldots, \frac{V_p(\mathbb{U}, w)}{I_p(\mathbb{U}, w)}).$$

Size of the Resolvent System

Theorem. Let $\mathcal{A}$ be a coherent and strong irreducible chain, $o = \mathrm{ord}(\mathcal{A})$, and $m = \max_i \mathrm{ord}(A_{i,j}, y_i)$. Then in the resolvent system

$$R, R_1, \ldots, R_s$$

we have $s \leq o + m$.

Algorithms for the Resolvent Systems:

$$B = \mathcal{A}_{(o+m)}, w_0 - \sum \lambda_{i,0} y_{i0}, \ldots, w_{o+m} - \sum \lambda_{i,o+m} y_{i,o+m}$$

Then a CS of **a-sat**(B) under the variable order $u_i, \lambda_{i,j}, < w_i, y_i$ if of the following form:

$$R, R_1, \ldots, R_m; P_1, \ldots; P_2, \ldots; \ldots; P_p, \ldots$$

Example

$\mathcal{A} = \{y_1^2 + x, y_{2,1}^2 + y_2^2 + 1, y_{2,2} - y_2\}$.

Let $w = y_1 + y_2$.

Using the difference CS method $(w < y_1 < y_2)$, we have :

$$\begin{aligned} & \text{Zero}(\mathbf{sat}(\mathcal{A}, w - y_1 - y_2)) \\ = & \text{Zero}(\mathcal{A} \cup \{w - y_1 - y_2\}) = \text{Zero}(\mathbf{sat}(B_1)) \end{aligned}$$

where B_1 is:

$R = w_1^8 + (8 + 4w^2)w_1^6 + (16w^2 + 6w^4 + 8x^2 + 16)w_1^4 + (4w^6 + 8w^4 + 32x^2 - 48w^2x^2 - 64w^2x)w_1^2 + w^8 + 8w^4x^2 + 16x^4$,

$R_1 = (2w_1^2w + 2w^3 - 4wx)w_2^2 + (-2w_1^2w^2 + w_1^4 - 3w^4 + 4w_1^2 + 4x^2)w_2 + 4w^3 + w^5 - 8wx - ww_1^4 + 4xw^3 - 4wx^2$,

$P_1 = (-4w^3 - 4w_1^2w + 8wx)y_1 + 4w_1^2 + 2w_1^2w^2 + w^4 + w_1^4 - 8w^2x + 4x^2$,

$P_2 = (-8wx + 4w_1^2w + 4w^3)y_2 - 3w^4 - 2w_1^2w^2 + 4w_1^2 + w_1^4 + 4x^2$.

$\{R, R_1\}$ is a resolvent system for $\mathbf{sat}(\mathcal{A})$.

Example: Proper Irreducible Chain

$\mathcal{A} = \{y_1^2 + x, y_{2,1}^2 + y_2^2 + 1\}$.

Let $w = y_1 + y_2$.

Using the difference CS method, we have:

$$\begin{aligned} & \mathrm{Zero}(\mathbf{sat}(\mathcal{A}, w - y_1 - y_2)) = \mathrm{Zero}(\mathcal{A} \cup \{w - y_1 - y_2\}) \\ = \ & \mathrm{Zero}(\mathbf{sat}(B_1)) \cup \mathrm{Zero}(\mathbf{sat}(B_2)) \end{aligned}$$

$B_1 = R, R_1, P_1, P_2$

$B_2 = \{R, R_1', P_1, P_2\}$, where $R_1' = (-2w_1^2 w - 2w^3 + 4wx)w_2^2 + (-2w_1^2 w^2 + w_1^4 - 3w^4 + 4w_1^2 + 4x^2)w_2$.

$\{R, R_1\}$ and $\{R, R_1'\}$ are the resolvent systems for $\mathbf{sat}(\mathcal{A})$.

A Condition for Resolvent

$\mathbf{K}$ is an aperiodic difference field or $|\mathbb{U}| \neq 0$.

In this case, for any $P \in \mathbf{K}\{\mathbb{U}, y_1, \ldots, y_p\}$, there exist α_i such that $P(\mathbb{U}, \alpha_1, \ldots, \alpha_p) \neq 0$.

Thanks!

The results are joint work with Yong Luo and Chunming Yuan