§6.2 Differential Decomposition Theorems / Algorithms

Recall (Wu-Ritt Well-ordering Principle)

Given a finite subset $\Sigma \subseteq K\{Y\} = K\{y_1, \cdots, y_n\}$, to compute a characteristic set $\mathcal{A}$ of Σ w.r.t. a ranking in a mechanical way:

$$\boxed{\begin{array}{ccccccc} \Sigma_1 = \Sigma & \subseteq & \Sigma_2 = \Sigma_1 \cup R_1 \subseteq & \cdots & \subseteq \Sigma_e = \Sigma_{e-1} \cup R_{e-1} \\ \mathcal{A}_1 & > & \mathcal{A}_2 & > \cdots > & \mathcal{A}_e \\ R_1 \neq \phi & & R_2 \neq \phi & \cdots & R_e = \phi \end{array}}$$

where $\mathcal{A}_i \triangleq$ basic set of Σ_i and $R_i = \{\delta\text{-rem}(f, \mathcal{A}_i) \mid f \in \Sigma_i \setminus \mathcal{A}_i\} \setminus \{0\}$.

Set $\mathcal{A} = \mathcal{A}_e$ which is a characteristic set of Σ. And we have

$$\mathbb{V}(\mathcal{A}/H_{\mathcal{A}}) \subseteq \mathbb{V}(\Sigma) = \mathbb{V}(\Sigma_2) = \cdots = \mathbb{V}(\Sigma_e) \subseteq \mathbb{V}(\mathcal{A})$$

$$\mathbb{V}(\Sigma) = \underset{\substack{\| \\ (\{\eta \in \bar{K}^n \mid \mathcal{A}(\eta) = 0 \ \& \ H_{\mathcal{A}}(\eta) \neq 0\} \text{ with } H_{\mathcal{A}} = \prod_{A \in \mathcal{A}} I_A S_A)}}{\mathbb{V}(\mathcal{A}/H_{\mathcal{A}})} \cup \bigcup_{A \in \mathcal{A}} \mathbb{V}(\Sigma \cup \{I_A\}) \cup \mathbb{V}(\Sigma \cup \{S_A\}).$$

Continuing this procedure for $\Sigma \cup \{I_A\}$ or $\Sigma \cup \{S_A\}$ and also for the new δ-poly sets obtained, since the basic sets are strictly decreasing, this procedure has to end in a finite number of steps and so we get the following

<u>Zero Decomposition Theorem (Weak Form)</u> There is an algorithmic procedure which permits us to give for Σ a decomposition of the form

$$\mathbb{V}(\Sigma) = \bigcup_k \mathbb{V}(\mathcal{B}_k / H_{\mathcal{B}_k})$$

where $\mathcal{B}_k$ is a characteristic set for some δ-polynomial set.

In this section, we shall consider the main decomposition problem in differential algebra and give a partial answer to it:

<u>Decomposition Problem</u> Given a finite subset $\Sigma \subseteq K\{Y\}$, decompose the radical δ-ideal $\{\Sigma\}$ into an <u>irredundant</u> intersection of prime δ-ideals: $\{\Sigma\} = P_1 \cap P_2 \cap \cdots \cap P_r$.

Since a prime δ-ideal P is completely determined by its characteristic set $\mathcal{A}$ (i.e., $P = \mathrm{sat}(\mathcal{A})$), the above decomposition problem can be separated into the following two problems:

Problem 1: Given Σ, to find a finite set Λ of autoreduced sets of $K\{Y\}$, each of which is a characteristic set of a prime δ-ideal containing Σ, such that Λ contains a characteristic set of each component of $\{\Sigma\}$.

That is, $\{\Sigma\} = \mathrm{sat}(\mathcal{B}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{B}_l)$ with $\Lambda = \{\mathcal{B}_1, \ldots, \mathcal{B}_l\}$.

Problem 2: Given an autoreduced set $\mathcal{A}$ of $K\{Y\}$, to determine whether or not $\mathcal{A}$ is a characteristic set of a component of $\{\Sigma\}$.

or

Problem 2′ Given that $\mathcal{A}$ and $\mathcal{B}$ are characteristic sets of the prime δ-ideals P and Q respectively, to determine whether or not $P \subseteq Q$.

Decomposition problem = Problem 1 + Problem 2

= Problem 1 + Problem 2′

Remark: ① Problem 1 has been solved (Ritt-Kolchin decomposition Algorithm)

② Problem 2 in the general case is still not solved, and we have a complete answer for the case when Σ consists of a single δ-poly given by Ritt's component theorem and the low power theorem.

③ Although it is trivial to decide whether $P = Q$, Problem 2′ is currently still open, even for the special case below:

Ritt's problem Given $A \in K\{Y\}$ irreducible with $A(0, \ldots, 0) = 0$, to determine whether $(0, \ldots, 0)$ is a zero of $\mathrm{sat}(A)$, or equivalently, whether $\mathrm{sat}(A) \subseteq [y_1, \ldots, y_n]$.

In this section, we shall focus on a solution of problem 1.

Question: Given an autoreduced set $\mathcal{A} \subseteq K\{Y\}$, give a necessary and sufficient condition for $\mathcal{A}$ to be a characteristic set of a prime δ-ideal $P \subseteq K\{Y\}$?

<u>Lemma 1</u> (Rosenfeld's lemma in ordinary differential case)

Let $\mathcal{A} = A_1, \cdots, A_p$ be an autoreduced set in $K\{Y\}$ w.r.t. a ranking and $f \in K\{Y\}$ be partially reduced w.r.t. $\mathcal{A}$. Then

$$f \in \operatorname{sat}(\mathcal{A}) = [\mathcal{A}] : H_{\mathcal{A}}^{\infty} \Longleftrightarrow f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}.$$

Proof. "$\Leftarrow$" Trivial

"$\Rightarrow$" Suppose $f \in \operatorname{sat}(\mathcal{A})$. Then $\exists\ m \in \mathbb{N}$ and $C_{ij} \in K\{Y\}$

$$H_{\mathcal{A}}^{m} f = \sum_{i=1}^{p} C_{i0} A_i + \sum_{i=1}^{p} \sum_{j=1}^{k_i} C_{ij} A_i^{(j)}. \quad (*)$$

Note that for $j \geq 1$, $A_i^{(j)} = S_{A_i} \delta^{j}(u_{A_i}) + T_{ij}$ for some $T_{ij} \in K\{Y\}$ free of $\delta^{j} u_{A_i}$. Let $\Phi = \{\delta^{j}(u_{A_i}) \mid C_{ij} \neq 0,\ j \geq 1,\ i = 1, \ldots, p\}$.

If $\Phi \neq \phi$, take the greatest $v = \delta^{j}(u_{A_i})$ in Φ and substitute $\delta^{j}(u_{A_i}) = -\frac{T_{ij}}{S_{A_i}}$ at both sides of $(*)$ and set $\Phi = \Phi \setminus \{v\}$. Continue this process and successively substitute $\delta^{j}(u_{A_i}) = -\frac{T_{ij}}{S_{A_i}}$ into $(*)$ for all $\delta^{j}(u_{A_i})$ in Φ.

Clearing denominators by multiplying a power product $S_{\mathcal{A}}^{l}$ of S_{A_i} at both sides of the obtained equality, we have

$$S_{\mathcal{A}}^{l} \cdot H_{\mathcal{A}}^{m} f = \sum_{i=1}^{p} \overline{C_{i0}} A_i \quad \text{where } \overline{C_{i0}} \in K\{Y\}.$$

Thus, $f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$. ▨

<u>Lemma 2.</u> Let $\mathcal{A}$ be an autoreduced set in $K\{Y\}$ w.r.t. a ranking $\mathcal{R}$. Then $\mathcal{A}$ is a δ-characteristic set of a prime δ-ideal

$\Longleftrightarrow$ $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ is a prime algebraic ideal in $K\{Y\}$

and $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ contains no nonzero element reduced w.r.t. $\mathcal{A}$.

"δ-char set" is used to distinguish with the algebraic case.

Proof. "$\Rightarrow$" Take a finite subset $V \subseteq \Theta(Y)$ such that $\mathcal{A} \subseteq K[V]$.
Let $I_{\mathcal{A}} = \{f \in K[V] \mid \exists\, m \in \mathbb{N} \text{ s.t. } H_{\mathcal{A}}^m f \in (\mathcal{A})\}$. Then we have

$$(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}} \text{ and } I_{\mathcal{A}} = ((\mathcal{A}) : H_{\mathcal{A}}^{\infty}) \cap K[V].$$

(Indeed, for $\forall f \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$, $\exists\, C_A \in K\{Y\}$ s.t. $H_{\mathcal{A}}^m f = \sum_{A \in \mathcal{A}} C_A \cdot A$. Rewrite f and each C_A as δ-polys in $\Theta(Y) \setminus V$ with coefficients in $K[V]$, then $f = \sum_i f_i(V) M_i$ and $C_A = \sum_i C_{A,i}(V) M_i$ with M_i being distinct δ-monomials in $\Theta(Y) \setminus V$. Then $H_{\mathcal{A}}^m f_i = \sum_{A \in \mathcal{A}} C_{A,i} \cdot A$ in $K[V]$. Thus $f_i \in I_{\mathcal{A}}$ and $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}}$. Similarly, $((\mathcal{A}) : H_{\mathcal{A}}^{\infty}) \cap K[V] = I_{\mathcal{A}}$.)

By Lemma 1, $\text{Sat}(\mathcal{A}) \cap K[V] = ((\mathcal{A}) : H_{\mathcal{A}}^{\infty}) \cap K[V] = I_{\mathcal{A}}$. So $I_{\mathcal{A}}$ is a prime ideal and consequently, $(\mathcal{A}) : H_{\mathcal{A}}^{\infty} = (I_{\mathcal{A}})_{K\{Y\}}$ is prime too.
Since $\mathcal{A}$ is a char set of $\text{Sat}(\mathcal{A})$, $(\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ contains no nonzero δ-poly reduced w.r.t. $\mathcal{A}$.

"$\Leftarrow$" To show ① $\text{Sat}(\mathcal{A})$ is prime and ② $\mathcal{A}$ is a char set of $\text{Sat}(\mathcal{A})$.

① Given $f_1, f_2 \in K\{Y\}$ with $f_1 f_2 \in \text{Sat}(\mathcal{A})$. Let $r_i = \delta\text{-rem}(f_i, \mathcal{A})$. Then $H_{\mathcal{A}}^{m_i} f_i \equiv r_i \mod [\mathcal{A}] \Rightarrow r_1 r_2 \in \text{Sat}(\mathcal{A})$ partially reduced w.r.t. $\mathcal{A}$
$\Rightarrow$ By Lemma 1, $r_1 \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ or $r_2 \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$. Thus, $f_1 \in \text{Sat}(\mathcal{A})$ or $f_2 \in \text{Sat}(\mathcal{A})$.

② $\forall f \in \text{Sat}(\mathcal{A})$, suppose $r = \delta\text{-rem}(f, \mathcal{A})$. Then $r \in (\mathcal{A}) : H_{\mathcal{A}}^{\infty}$ by Lemma 1. Since r is reduced w.r.t. $\mathcal{A}$, $r = 0$. Thus, $\mathcal{A}$ is a δ-char set of $\text{Sat}(\mathcal{A})$.

<u>Remark 3.</u> Given an autoreduced set $\mathcal{A} \subseteq K\{Y\}$, denote V to be the set of all derivatives appearing effectively in $\mathcal{A}$. By the proof of Lemma 2,

$$\boxed{\begin{array}{l} \mathcal{A} \text{ is a } \delta\text{-characteristic set of a prime } \delta\text{-ideal} \\ \Longleftrightarrow \text{In } K[V],\ \mathcal{A} \text{ is an algebraic characteristic set of } I_{\mathcal{A}}. \end{array}}$$

So the question has been reduced to an algebraic one. Below, we follow Wu's constructive theory for irreducible ascending chains.

Algebraic Case Let $\mathcal{A} = A_1, \ldots, A_p \subseteq K[u_1, \ldots, u_d, x_1, \ldots, x_p]$ be an ascending chain (i.e., an autoreduced set with all elts of order 0) w.r.t. the ranking $u_1 < \cdots < u_d < x_1 < \cdots < x_p$ and $ld(A_i) = y_i$.

$$\mathcal{A} \begin{cases} A_1 = I_1(u_1, \ldots, u_d) X_1^{m_1} + * X_1^{m_1 - 1} + \cdots + * X_1 + * ; \\ A_2 = I_1(u_1, \ldots, u_d, x_1) X_2^{m_2} + * X_2^{m_2 - 1} + \cdots + * ; \\ \cdots \\ A_p = I_p(u_1, \ldots, u_d, x_1, \ldots, x_{p-1}) X_p^{m_p} + * X_p^{m_p - 1} + \cdots + * . \end{cases} \quad \begin{matrix} \deg(A_i, X_j) < m_j \\ \text{for } j < i. \end{matrix}$$

Def 4. (Irreducible ascending chain)

$\mathcal{A} := A_1, \ldots, A_p$ is said to be irreducible if $\mathcal{A}$ possesses the following properties:

- Let $K_0 = K(u_1, \ldots, u_d)$ be transcendental extension field of K adjoining $u_1, \ldots, u_d$. Then A_1, as a poly $\tilde{A}_1$ in $K_0[X_1]$, is irreducible in $K_0[X_1]$.
  Take a solution y_1 of $\tilde{A}_1(x_1) = 0$ and set $K_1 = K_0(y_1)$.
- $\tilde{A}_2 = A_2(u_1, \ldots, u_d, y_1, X_2) \in K_1[X_2]$ is irreducible.
  Take a solution y_2 of $\tilde{A}_2(x_2) = 0$ and set $K_2 = K_1(y_2)$.
- $\tilde{A}_3 = A_3(u_1, \ldots, u_d, y_1, y_2, x_3) \in K_2[X_3]$ is irreducible.
  Take a solution y_3 of $\tilde{A}_3(x_3) = 0$ and set $K_3 = K_2(y_3)$.
- Suppose that proceeding in the same manner, we get successively algebraic extensions $K_i = K_{i-1}(y_i)$, polynomial $\tilde{A}_i = A_i(u_1, \ldots, u_d, y_1, \ldots, y_{i-1}, X_i)$ is irreducible in $K_{i-1}[X_i]$.

The obtained point $\tilde{y} = (u_1, \ldots, u_d, y_1, \ldots, y_p)$ is called a generic point of the irreducible $\mathcal{A}$.

Note: The irreducibility of $\mathcal{A}$ could be determined mechanically relying on factorization algorithms on towers of algebraic extensions.

<u>Lemma 5.</u> If the ascending chain $\mathcal{A}$ is irreducible with a generic point $\tilde{\eta}=(u_1,\dots,u_d,\eta_1,\dots,\eta_p)$, then

$$\mathrm{prem}(f,\mathcal{A})=0 \iff f(\eta)=0.$$

Furthermore, $\mathrm{asat}(\mathcal{A})=(\mathcal{A}):I_{\mathcal{A}}^{\infty}$ is a prime ideal with $\mathcal{A}$ a char set of it.

(Remark: $\mathrm{prem}(f,\mathcal{A})$ $(=\delta\text{-rem}(f,\mathcal{A}))$ obtained only by performing the proof of Thm 2.1.12)

Proof. Let $\mathcal{A}_k=A_1,\dots,A_k$ $(1\le k\le p)$. Then $\mathcal{A}_k$ is irreducible in $K[u_1,\dots,u_d,x_1,\dots,x_k]$ with a generic point $\tilde{\eta}_k=(u_1,\dots,u_d,\eta_1,\dots,\eta_k)$.

We shall prove by induction on k the following two assertions:

(1_k) $I_k(\tilde{\eta}_{k-1})\ne 0$ for $I_k=\mathrm{init}(A_k)$.

(2_k) If $R_k\in K[u_1,\dots,u_d,x_1,\dots,x_k]$ is reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta}_k)=0$, then $R_k\equiv 0$.

First, note that (1_k) is a consequence of (2_{k-1}). And (1_1) is trivial. So it suffices to prove (2_k) by induction on k.

For $k=1$, if R_1 is reduced w.r.t. $\mathcal{A}_1=A_1$, then $\deg(R_1,x_1)<m_1$.

But $R_1(\tilde{\eta}_1)=0 \Rightarrow A_1 \mid R_1 \Rightarrow R_1\equiv 0$.

Suppose (2_{k-1}) has been proved. Consider any $R_k\in K[u_1,\dots,u_d,x_1,\dots,x_k]$ reduced w.r.t. $\mathcal{A}_k$ and $R_k(\tilde{\eta}_k)=0$. Rewrite R_k as a poly in x_k, then $R_k=S_0x_k^r+S_1x_k^{r-1}+\dots+S_r$ for $S_i\in K[u_1,\dots,u_d,x_1,\dots,x_{k-1}]$ and $r<m_k$. Since R_k is reduced w.r.t. $\mathcal{A}_k$, each S_i is reduced w.r.t. $\mathcal{A}_{k-1}$. Since $R_k(\tilde{\eta}_k)=0=\tilde{S}_0\eta_k^r+\tilde{S}_1\eta_k^{r-1}+\dots+\tilde{S}_r$ w/ $\tilde{S}_i=S_i(u_1,\dots,u_d,\eta_1,\dots,\eta_{k-1})$, $r<m_k \Rightarrow \tilde{S}_i=0$ $\forall i=0,\dots,r$. By induction hypothesis on (2_{k-1}), $S_i\equiv 0 \Rightarrow R_k\equiv 0$, which completes the proof of (2_k).

Thus, by induction, (1_k) and (2_k) are proved.

If $\mathrm{prem}(f,\mathcal{A})=0$, $I_1^{l_1}\cdots I_p^{l_p}f\in(\mathcal{A})\Rightarrow f(\tilde{\eta})=0$ by (1).

Given f w/ $f(\tilde{\eta})=0$, $r=\mathrm{prem}(f,\mathcal{A}) \Rightarrow r(\tilde{\eta})=0 \Rightarrow r=0$ by (2).

Thus, $\mathrm{prem}(f, \mathcal{A}) = 0 \Leftrightarrow f(\tilde{\eta}) = 0$.

Clearly, $\mathrm{asat}(\mathcal{A}) = \{ f \in K[u_1, \dots, u_d, x_1, \dots, x_p] \mid f(\tilde{\eta}) = 0 \}$. Thus $\mathrm{asat}(\mathcal{A})$ is prime and $\mathcal{A}$ is a characteristic set of $\mathrm{asat}(\mathcal{A})$. ☒

Another characterization of irreducibility of ascending sets.

Consider now $\mathcal{A} := A_1, \dots, A_p$ not necessarily irreducible. Suppose $\exists k$ s.t. $\mathcal{A}_{k-1} := A_1, \dots, A_{k-1}$ is irreducible with a generic point $\tilde{\eta}_{k-1} = (u_1, \dots, u_d, \eta_1, \dots, \eta_{k-1})$. and $\tilde{A}_k \in K_{k-1}[x_k]$ is reducible with

$$\tilde{A}_k = g_1 \cdots g_h$$

in which each $g_i \in K_{k-1}[x_k]$ is irreducible and $h \geq 2$.

Since the denominators of coefficients of g_i are polynomials in $\tilde{\eta}_{k-1}$, by multiplying a common multiple of the denominators, we get

$$\tilde{D} \tilde{A}_k = \tilde{G}_1 \cdots \tilde{G}_h$$

in which $D \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$, $G_i \in K[u_1, \dots, u_d, x_1, \dots, x_k]$ and $\tilde{G}_i = G_i(\tilde{\eta}_{k-1})$.

We may also assume D and G_i are reduced w.r.t. $\mathcal{A}_k$.

Write $DA_k - G_1 \cdots G_h = \sum_i B_i x_k^i$ with $B_i \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$.

$\Rightarrow \sum_i \tilde{B}_i(\tilde{\eta}_{k-1}) x_k^i = 0 \Rightarrow B_i \in \mathrm{asat}(\mathcal{A}_{k-1}) \Rightarrow I_1^{r_{i1}} \cdots I_{k-1}^{r_{i,k-1}} B_i \in (\mathcal{A}_{k-1})$.

$\Rightarrow I_1^{s_1} \cdots I_{k-1}^{s_{k-1}} (DA_k - G_1 \cdots G_h) \in (A_1, \dots, A_k)$ where $s_j = \max_i \{ r_{ij} \}$.

<u>Lemma 6</u> Given an autoreduced set $\mathcal{A} = A_1, \dots, A_p$, if $\mathcal{A}$ is reducible, then $\exists k \ (1 \leq k \leq p)$ and some $D \in K[u_1, \dots, u_d, x_1, \dots, x_{k-1}]$ and $G_i \in K[u_1, \dots, x_k]$ s.t. $\mathcal{A}_{k-1} = A_1, \dots, A_{k-1}$ is irreducible and

$$DA_k \equiv G_1 G_2 \cdots G_h \mod (\mathcal{A}_{k-1})$$

where D is reduced w.r.t. $\mathcal{A}_{k-1}$ and $\deg(G_i, x_k) > 0$. alg variety

done with alg case

Thus, $\mathrm{Zero}(\mathcal{A}/I_{\mathcal{A}}) = \mathrm{Zero}(\mathcal{A}, D/I_{\mathcal{A}}) \cup \mathrm{Zero}(\mathcal{B}_1/I_{\mathcal{A}}^{*}D) \cup \cdots \cup \mathrm{Zero}(\mathcal{B}_h/I_{\mathcal{A}}^{*}D)$,

where $\mathcal{B}_i$ is obtained from $\mathcal{A}$ by replacing A_k by G_i.

Return to the differential case: Fix a ranking R on $K\{Y\}$.

Given a finite subset $\Sigma \subseteq K\{Y\}$, mechanical procedures to decompose $\mathbb{V}(\Sigma)$

Step 1: Apply well-ordering principle to Σ:

$$\mathbb{V}(\Sigma) = \mathbb{V}(\mathcal{A}/H_{\mathcal{A}}) \cup \bigcup_{A \in \mathcal{A}} \mathbb{V}(\mathcal{A} \cup \{I_A\}) \cup \mathbb{V}(\mathcal{A} \cup \{S_A\})$$
$$= \cdots = \bigcup_k \mathbb{V}(\mathcal{B}_k/J_k)$$

Step 2: Consider $\mathbb{V}(\mathcal{B}_k/J_k)$. If $\mathcal{B}_k$ is reducible, then regard $\mathcal{B}_k$ as an algebraic ascending chain in $K[V]$ w.r.t. the ordering induced by R. Then at stage i, $\mathcal{B}_{k,i-1} = B_{k1}, \dots, B_{k,i-1}$ is irreducible and

$$D B_{k,i} \equiv G_1 \cdots G_h \mod (\mathcal{B}_{k,i-1})$$

where D is reduced w.r.t. $\mathcal{B}_{k,i-1}$ and each G_j has the same leader as $B_{k,i}$.

Thus, $\mathbb{V}(\mathcal{B}_k/J_k) = \mathbb{V}(\mathcal{B}_k, D/J_k) \cup \bigcup_{k=1}^{h} \mathbb{V}(\hat{\mathcal{B}}_{k,j}/D * J_k)$ ← obtained by replacing $B_{k,i}$ by G_j.

$$\cdots = \bigcup_j \mathbb{V}(\mathcal{C}_{k,j}/H_{\mathcal{C}_{k,j}}).$$

Continue this procedure until we get the following

<u>Zero-decomposition Theorem</u> (Strong Form)

There is an algorithmic procedure which allows us to give for any finite Σ a decomposition of the form

$$\mathbb{V}(\Sigma) = \bigcup_k \mathbb{V}(IRR_k/J_k * G_k)$$

where IRR_k is d-irreducible autoreduced set and $J_k = H_{IRR_k}$.

<u>Differential decomposition Theorem</u>

$\mathbb{V}(\Sigma) = \bigcup_k \mathbb{V}(\mathrm{sat}(IRR_k))$, or equivalently, $\{\Sigma\} = \bigcap_k \mathrm{sat}(IRR_k)$.

Recent Algorithms: ① Regular decomposition: $\{\Sigma\} = ([A_1] : H_{\mathcal{Q}_1}^{\infty}) \cap \cdots \cap ([A_m] : H_{\mathcal{Q}_m}^{\infty})$

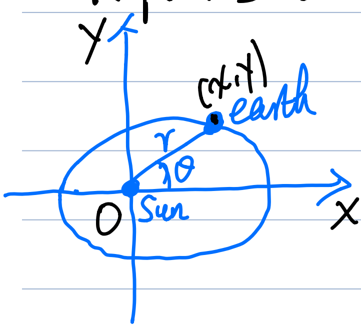
factorization-free ② Characterizable decomposition: $\{\Sigma\} = \mathrm{sat}(\mathcal{A}_1) \cap \cdots \cap \mathrm{sat}(\mathcal{A}_l)$, with $\mathcal{A}_i$ being a characteristic set of $\mathrm{sat}(\mathcal{A}_i)$.

Rosenfeld-Gröbner algorithm / Maple

Application (Mechanical Theorem Proving).

Example: Kepler's laws $\Rightarrow$ Newton's Gravitation laws

Kepler's laws
$$\begin{cases} (K1)\ (椭圆定律)\quad r = \dfrac{p}{1-e\cos(\theta)} \quad (p, e \text{ 常数}) \\ (K2)\ 面积定律\quad r^2\theta' = h \quad (h \text{ 常数}) \end{cases}$$



$\Downarrow$ 极坐标转化为直角坐标

$$\begin{cases} r = p + ex \\ p' = e' = 0 \\ xy' - x'y = h \\ h' = 0 \end{cases}$$

Newton's Law
$$\begin{cases} (N1)\quad a = \dfrac{\text{Const}}{r^2} \\ (N2)\quad (x'', y'') = -\text{Const}\cdot(-x, -y) \end{cases} \Longrightarrow \begin{cases} ((x'')^2 + (y'')^2) r^4 \triangleq k \\ k' = 0 \\ x''y - xy'' = 0 \end{cases}$$

$$\text{HYP} = \{ r - p - ex,\ p',\ e',\ xy' - x'y - h,\ h',\ ((x'')^2 + (y'')^2) r^4 - k \}$$

$$\text{Conc} = \{ k',\ x''y - xy'' \}$$

To show $\text{HYP} = 0 \xrightarrow[\text{condition } J \neq 0]{\text{under non-degenerate}} \text{Conc} \neq 0$

Rename variables and take the elimination ranking:

$$(p, e, r, x, y, h, k) = (x_{21} < x_{22} < x_{31} < x_{32} < x_{33} < x_{51} < x_{52})$$

Use the well-ordering principle with selecting "weak" basic set (not necessarily autoreduced, but initials and separants are partially reduced).

$$\text{Hyp}\begin{cases} r = p + ex \\ p' = 0 \\ e' = 0 \\ xy' - x'y = h \\ h' = 0 \\ r^2 = x^2 + y^2 \\ r^4(x''^2 + y''^2) = k \end{cases} \Longrightarrow \Sigma_1 \begin{cases} X_{21}' = F_1 \\ X_{22}' = F_2 \\ X_{21} + X_{22} X_{32} - X_{31} = F_3 \\ X_{32} X_{33}' - X_{32}' X_{33} - X_{51} = F_4 \\ X_{51}' = F_5 \\ X_{32}^2 + X_{33}^2 - X_{31}^2 = F_6 \\ X_{32}''^2 \cdot X_{31}^4 + X_{33}''^2 \cdot X_{31}^4 - X_{52} = F_7 \end{cases}$$

$\Sigma_1 = \{F_1, F_2, \dots, F_7\}$

$\mathcal{A}_1 = F_1, F_2, F_3, F_6, F_4, F_7$

$r_1 = \delta\text{-rem}(F_5, \mathcal{A}_1) = 4X_{21}\left[(X_{31}^3 X_{22}^2 - X_{31}^3 + 2X_{31}^2 X_{21} - X_{31} X_{21}^2) X_{31}'' + X_{31} X_{21} (X_{31}')^2 - X_{31}'^2 X_{21}^2\right]$

$\Sigma_2 = \Sigma_1 \cup \{r_1\}$

$\mathcal{A}_2 = \{F_1, F_2, r_1, F_3, F_4, F_6, F_7\}$ (0.1s)

$R_2 = \phi$

So $\mathcal{A} = \mathcal{A}_2$.

$$\begin{cases} \delta\text{-Rem}(X_{52}, \mathcal{A}) = 0 \quad \text{with } h_1 = -128 X_{33}^8 X_{22}^8 X_{21}^2 \\ \delta\text{-Rem}(X_{32}'' X_{33} - X_{32} X_{33}'', \mathcal{A}) = 0 \quad \text{with } h_2 = 16 X_{33}^3 X_{22}^3 X_{21}. \end{cases}$$

So $\mathbb{W}(\text{HYP}/H_{\text{HYP}}) \subseteq \mathbb{W}(\text{Cone})$.

Note that $H_{\text{HYP}} = 4X_{21}(X_{31}^3 X_{22}^2 - X_{31}^3 + 2X_{31}^2 X_{21} - X_{31} X_{21}^2) X_{33} X_{22}$

$\overset{F_3}{=\!=} 4X_{21} X_{31} X_{22}^3 X_{33}^3$

Non-degenerate elliptic orbits $\Longrightarrow$ $X_{21} = p \neq 0$, $X_{31} = r \neq 0$, $X_{22} = e \neq 0$

$X_{33} = y \neq 0$

Thus, Kepler's Laws (K1) and (K2) $\Longrightarrow$ (N1) and (N2).