Recall $\Sigma \subseteq K\{Y_1, \dots, Y_n\}$: a finite set of nonzero δ-polys

- Ritt-Wu's well-ordering principle

$\Sigma_0 = \Sigma$	$\Sigma_1 = \Sigma \cup R_0$	$\cdots$	$\Sigma_r = \Sigma_{r-1} \cup R_{r-1}$
A_0	A_1	$\cdots$	A_r
$R_0 \neq \phi$	$R_1 \neq \phi$	$\cdots$	$R_r = \phi$

A_i: a basic set of Σ_i

$R_i = \delta\text{-rem}(\Sigma_i \setminus A_i, A_i) \setminus \{0\}$

$\mathcal{A} \triangleq A_r$: a characteristic set of Σ

properties: ① $\mathcal{A} \subseteq [\Sigma]$ & $\delta\text{-rem}(\Sigma, \mathcal{A}) = \{0\}$

② $W(\mathcal{A}/H_{\mathcal{A}}) \subseteq W(\Sigma) \subseteq W(\mathcal{A})$

③ $W(\Sigma) = W(\mathcal{A}/H_{\mathcal{A}}) \cup \bigcup_{A \in \mathcal{A}} \left(W(\Sigma, I_A) \cup W(\Sigma, S_A) \right)$

- Zero-decomposition theorem: Weak Form

$$W(\Sigma) = \bigcup_{j=1}^{l} W(CS_j / H_{CS_j})$$

CS_j: autoreduced sets with $\delta\text{-rem}(\Sigma, CS_j) = \{0\}$ & $CS_j \leq b.s.(\Sigma)$

$$\left(W(\Sigma/G) = \bigcup_{j=1}^{l} W(CS_j / H_{CS_j} G) \right)$$

- $\mathcal{A}$: autoreduced set in $K\{Y\}$

$\mathcal{A}$ is a δ-char set of a prime δ-ideal

$\Leftrightarrow$ $\mathcal{A}$ is a char set of a prime algebraic ideal

(Say, $(\mathcal{A} : H_{\mathcal{A}}^{\infty})_{K[V]}$, with $V \subseteq \overline{\Theta(Y)}$ minimal s.t. $\mathcal{A} \subseteq K[V]$)

• Irreducible ascending chain in $K[u_1,\dots,u_d,x_1,\dots,x_p]$: $u_1<\cdots<u_d<x_1<\cdots x_p$

Algebraic case

$$\mathcal{A}:=\begin{cases} A_1(u_1,\dots,u_d,x_1) \\ A_2(u_1,\dots,u_d,x_1,x_2) \\ \vdots \\ A_p(u_1,\dots,u_d,x_1,x_2,\dots,x_p) \end{cases}$$

$A_1(x_1)$ irr in $K(u_1,\dots,u_d)[x_1]$ w/ $A_1(\eta_1)=0$

$\tilde{\eta}_1=(u_1,\dots,u_d,\eta_1)$

$\tilde{A}_2(x_2)=A_2(\tilde{\eta}_1,x_2)\in K(\tilde{\eta}_1)[x_2]$ irr/ w/ $\tilde{A}_2(\eta_2)=0$

$\tilde{\eta}_2=(u_1,\dots,\eta_1,\eta_2)$

$\tilde{A}_p(x_p)=A_p(\tilde{\eta}_{p-1},x_p)\in K(\tilde{\eta}_{p-1})[x_p]$ irr/ w/ $\tilde{A}_p(\eta_p)=0$

$\tilde{\eta}=\tilde{\eta}_p=(u_1,\dots,u_d,\eta_1,\dots,\eta_p)$

$\tilde{\eta}=(u_1,\dots,u_d,\eta_1,\dots,\eta_p)$: a generic point of $\mathcal{A}$

(P1) $f \xrightarrow{\mathcal{A}} 0 \iff f(\tilde{\eta})=0$

(P2) $\mathcal{A}$ is a char set of a prime ideal

$\iff$ $\mathcal{A}$ is irreducible.

Another characterization of irreducibility:

Sps $\mathcal{A}$ is reducible. Then $\exists\, k$ $(1\le k\le p)$ s.t.

$\mathcal{A}_{k-1}:=A_1,\dots,A_{k-1}$ is irreducible

and $\tilde{A}_k(X_k)=A_k(\tilde{\eta}_{k-1},X_k)$ is reducible in $K(\tilde{\eta}_{k-1})[X_k]$.

Assume $\tilde{A}_k = g_1\cdots g_h$ with $g_i\in K(\tilde{\eta}_{k-1})[X_k]$ irr/ $h\ge 2$.

$\Downarrow$ by clearing denominators of coeff

$\tilde{D}\cdot\tilde{A}_k=\tilde{G}_1\cdots\tilde{G}_h$ with $D\in K[u_1,\dots,x_{k-1}]$ $\tilde{D}=D(\tilde{\eta}_{k-1})$

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

$$D\cdot A_k-G_1\cdots G_h=\sum_i B_i(u_1,\dots,x_{k-1})x_k^i$$

$\Downarrow$

$$\tilde{D}\tilde{A}_k-\tilde{G}_1\cdots\tilde{G}_h=\sum_i B_i(\tilde{\eta}_{k-1})x_k^i=0$$

$\forall i,\ B_i(\widetilde{y_{k-1}}) = 0 \Rightarrow B_i \xrightarrow[A_{k-1}]{} 0$, i.e., $\exists \gamma_{ij}$ s.t. $I_1^{\gamma_{i1}} \cdots I_{k-1}^{\gamma_{i,k-1}} B_i \in (A_{k-1})$

Let $\gamma_j = \max_i\{\gamma_{ij}\}$. Then

$$I_1^{\gamma_1} \cdots I_{k-1}^{\gamma_{k-1}} (D \cdot A_k - G_1 \cdots G_h) \in (A_{k-1})$$

Let $D' = I_1^{\gamma_1} \cdots I_{k-1}^{\gamma_{k-1}} D$, $G_1' = I_1^{\gamma_1} \cdots I_{k-1}^{\gamma_{k-1}} G_1$, $G_i' = G_i$ $(i = 2, \ldots, h)$

$\Rightarrow D' A_k - G_1' \cdots G_h' \in (A_{k-1})$ &

By performing reduction for D' & $G_1', \ldots, G_h'$ w.r.t. $A_{k-1}, A_{k-2}, \ldots, A_1$ in turn, we can assume D' & G_i' are reduced w.r.t. A_{k-1}.

$$D' A_k - G_1' \cdots G_h' \in (A_{k-1})$$

$I_{k-1}^{\gamma_0} D' \equiv D_1 \mod (A_{k-1})$

$I_{k-1}^{\gamma_i} G_i' \equiv G_i'' \mod (A_{k-1})$

$\gamma = \max\{\gamma_0, \sum_{i=1}^{h} \gamma_i\}$

$$I_{k-1}^{\gamma-\gamma_0} (I_{k-1}^{\gamma_0} D') A_k - I_{k-1}^{\gamma - \sum \gamma_i} \prod_{i=1}^{h} (I_{k-1}^{\gamma_i} G_i') \in (A_{k-1})$$

$I_{k-1}^{\gamma_0} D' = D_1 + * A_{k-1}$, $G_i'' + * A_{k-1}$

$$\Downarrow$$

$$(I_{k-1}^{\gamma-\gamma_0} D_1) A_k = (I_{k-1}^{\gamma - \sum \gamma_i} G_1'') G_2'' \cdots G_h'' \mod (A_{k-1})$$

reduced w.r.t. A_{k-1}

So we have

$A = A_1, \ldots, A_p$ is reducible

$\Updownarrow$

$\exists k$ s.t. A_{k-1} irreducible & $\exists D \in K[u_1, \ldots, x_{k-1}]$, $G_i \in K[u_1, \ldots, x_k]$ which are reduced w.r.t. A_k satisfying

$$D A_k = G_1 G_2 \mod (A_{k-1}).$$

Back to the differential setting:

$\mathcal{A} = A_1, \dots, A_p$: an autoreduced set of $K\{Y_1, \dots, Y_n\}$

- $\mathcal{A}$ is δ-reducible (irreducible) $\iff$ $\forall\, k$ $(1 \le k \le p)$, there cannot exist a relation $D_k A_k \equiv G_{k1} \cdot G_{k2} \bmod [\mathcal{A}_{k-1}]$ $(*)$

with D_k, G_{k1}, G_{k2} reduced w.r.t. $\mathcal{A}_{k-1}$ & $ld(D_k) < ld(A_k)$ & $ld(G_{ki}) = ld(A_k)$.

- $\mathcal{A}$ is a char set of a prime δ-ideal $\iff$ $\mathcal{A}$ is δ-irreducible ($\mathcal{A}^a$ is alg irreducible)

- If $\mathcal{A}_{k-1}$ is irr & $\exists\, D, G_1, G_2$ satisfying a relation of the form $(*)$:

$$DA_k \equiv G_1 G_2 \bmod [\mathcal{A}_{k-1}]. \quad \text{Then}$$

$$W(\mathcal{A}/H_{\mathcal{A}}) = W(\mathcal{A}, D/H_{\mathcal{A}}) \cup W(\mathcal{A}\{A_k\} \cup \{G_1\}/DH_{\mathcal{A}}) \cup W(\mathcal{A}\{A_k\} \cup \{G_2\}/DH_{\mathcal{A}}).$$

Theorem 5.2.10 (Zero-decomposition Theorem: Strong Form)

There is an algorithmic procedure which permits to detect whether $W(\Sigma) = \emptyset$ for any finite subset Σ, and if $W(\Sigma) \neq \emptyset$, to furnish an irreducible decomposition of $W(\Sigma)$:

$$W(\Sigma) = \bigcup_{i=1}^{r} W(\mathcal{A}_i/R_i)$$

where $\mathcal{A}_i$ irreducible, $R_i = \delta\text{-rem}(G_i, H_{\mathcal{A}_i}, \mathcal{A}_i) \neq 0$ for some $G_i \in K\{Y\}$.

Proof. (Sketch) By the weak form of the zero-decomposition theorem,

$\exists\ CS_1, \dots, CS_\ell$ autoreduced set s.t.

$$\mathbb{V}(\mathcal{Z}) = \bigcup_{j=1}^{\ell} \mathbb{V}\left(CS_j / H_{CS_j}\right).$$

Case 1) $\forall j$, $CS_j \cap K \neq \phi$ or $\delta\text{-rem}(H_{CS_j}, CS_j) = 0$, $\mathbb{V}(\mathcal{Z}) = \phi$.

Case 2) $\forall j$, CS_j ivr $\Longrightarrow \mathbb{V}(\mathcal{Z}) = \bigcup_j \mathbb{V}(CS_j / R_j)$ w/ $R_j = \delta\text{-rem}(H_{CS_j}, CS_j) \neq 0$

Case 3) $\exists j$, $CS_j = A_1, \dots, A_p$ reducible at stage k. $\left(DA_k = G_1 G_2 \bmod [A_{k-1}]\right)$

$$\mathbb{V}(CS_j / H_{CS_j}) = \underbrace{\mathbb{V}(CS_j, D / H_{CS_j})}_{<CS_j} \cup \bigcup_{i=1}^{2} \underbrace{\mathbb{V}(CS_j \setminus A_k, G_i / DH_{CS_j})}_{<CS_j}$$

Repeat the process recursively which finally will terminate by performing well-ordering principle or weak form of zero decomposition for the obtained autoreduced sets are strictly decreasing.

Finally, we get $\mathbb{V}(\mathcal{Z}) = \bigcup_j \mathbb{V}(A_j / H_{A_j} G_j)$ w/ A_j ivr and $G_j \in K\{Y\}$

Take $R_j = \delta\text{-rem}(H_{A_j} G_j, A_j)$. If $R_j = 0$, omit $\mathbb{V}(A_j / H_{A_j} G_j) = \phi$.

$\Longrightarrow \mathbb{V}(\mathcal{Z}) = \bigcup_j \mathbb{V}(A_j / R_j)$. ∎

Theorem 5.2.11 (δ-variety decomposition theorem)

There is an algorithmic procedure to decompose $\mathbb{V}(\mathcal{Z})$ for any finite subset $\mathcal{Z} \subseteq K\{Y\}$ into a finite union of irreducible δ-varieties: $\mathbb{V}(\mathcal{Z}) = \bigcup_{i=1}^{\ell} \mathbb{V}(\mathrm{sat}(A_i))$ w/ A_i ivr.

Proof. By Theorem 5.2.10, we can compute a finite number of δ-irr autoreduced sets $A_1, \ldots, A_\ell$ s.t.

$$W(Z) = \bigcup_{i=1}^{\ell} W(A_i / R_i) \quad \text{w/ } 0 \neq R_i = \delta\text{-rem}(H_{A_i} G_i, A_i).$$

For each i, $W(A_i/R_i) = W(A_i/(H_{A_i} G_i))$ $\quad (H_{A_i}^m \cdot H_{A_i} G_i \equiv R_i \ [A_i])$

$$\subseteq W(\text{sat}(A_i))$$

So $W(Z) \subseteq \bigcup_{i=1}^{\ell} W(\text{sat}(A_i))$.

Take a generic point ξ_i of $\text{sat}(A_i)$, $\forall\, A \in A_i$, $A(\xi_i) = 0$ and $R_i(\xi_i) \neq 0$ (R_i reduced w.r.t. A_i).

So $\xi_i \in W(A_i/R_i) \subseteq W(Z) \Rightarrow W(\text{sat}(A_i)) \subseteq W(Z)$.

Thus, $W(Z) = \bigcup_{i=1}^{\ell} W(\text{sat}(A_i))$.

Remark: To get an irredundant irr decomposition of $W(Z)$, we need to find a basis for $\text{sat}(A_i)$. In the algebraic case, there are several methods including the one based on Gröbner basis and the one based on Chow form, so we can get an irredundant irreducible decomposition for $W(Z)$. In the diff case, this is still open.

Recent decomposition Algorithms: To avoid factorization, there are more efficient factorization-free algorithms implemented in Maple.

① Regular decomposition: $\{\Sigma\} = ([A_1] : H_1^\infty) \cap \cdots \cap ([A_m] : H_m)^\infty$

② Characterizable decomposition: $\{\Sigma\} = \mathrm{Sat}(A_1) \cap \cdots \cap \mathrm{Sat}(A_e)$ with A_i being a char set of $\mathrm{Sat}(A_i)$.

Maple: with(DifferentialAlgebra), RosenfeldGroebner(Σ, R)

Example for Zero-decomposition theorem

Consider the δ-poly set $\Sigma = \{f_1, f_2\} \subseteq \mathbb{Q}\{Y_1, Y_2, Y_3\}$ with

$$f_1 = Y_2'^2 - Y_1, \quad f_2 = Y_3 - Y_2$$

Take the elimination ranking: $Y_1 < Y_2 < Y_3$.

$\Sigma_0 = \{f_1, f_2\}$, $\mathrm{rk}(\Sigma_0) = \{Y_2'^2, Y_3\}$

$A_0 = f_1, f_2$, $R_0 = \emptyset$. So $A = A_0$ is a char set of Σ.

$I_{f_1} = I_{f_2} = S_{f_2} = 1$ & $S_{f_1} = 2Y_2'$

So $V(f_1, f_2) = V(f_1, f_2 / 2Y_2') \cup V(f_1, f_2, 2Y_2')$

Let $\Sigma^{(1)} = \{f_1, f_2, Y_2'\}$ $\qquad Y_2'^2 - Y_1 \xrightarrow{Y_2'} -Y_1$

$\Sigma_0^{(1)} = \Sigma^{(1)}$, $\mathrm{rk}(\Sigma_0^{(1)}) = \{Y_2'^2, Y_3, Y_2'\}$

$A_0^{(1)} = Y_2', Y_3 - Y_2$

$\delta\text{-rem}(f_1, A_0^{(1)}) = -Y_1 \neq 0$ $\quad R_0^{(1)} = \{-Y_1\}$

$\Sigma_1^{(1)} = \{f_1, f_2, Y_2', -Y_1\}$ $\quad rk(\Sigma_1^{(1)}) = \{Y_2'^2, Y_3, Y_2', Y_1\}$

$A_1^{(1)} = Y_1, Y_2', Y_3$

$\delta\text{-rem}(f_1, A_1^{(1)}) = 0$ so $R_1^{(1)} = \phi$. $A^{(1)} = A_1^{(1)}$ is a char set of $\Sigma^{(1)}$.

$W(f_1, f_2, Y_2') = W(A^{(1)})$

Thus, $W(f_1, f_2) = W(\underbrace{f_1, f_2}_{\text{irreducible}} / 2Y_2') \cup W(Y_1, Y_2', Y_3)$

$= W(\underbrace{sat(f_1, f_2)}_{\not\ni}) \cup W(Y_1, Y_2', Y_3)$ irr-decomposition

§5.3 Applications to Mechanical Theorem proving and discovering

Theorems are restricted to the ones for which both hypothesis and conclusions are expressed in the form of $p=0$ with p a certain δ-poly in $K\{Y_1, \cdots, Y_n\}$. That is, we only consider diff geometry statements of Equation Type.

Hypothesis: $h_i(Y_1, \cdots, Y_n) = 0$ $(i = 1, \cdots, r)$ $(HYP = \{h_1, \cdots, h_r\})$

Conclusion: $C(Y_1, \cdots, Y_n) = 0$. $(h_i, C \in K\{Y_1, \cdots, Y_n\})$

Note that a point $W(h_1, \ldots, h_r)$ is just a geometrical configuration (over possibly certain extended field) verifying the hypothesis of the given theorem. So to prove a theorem to be true seems thus equivalent to the following problem:

(A) To decide whether $C=0$ follows from $HYP=0$ or not, i.e., to decide whether

$$W(HYP/C) = \phi \qquad (1)$$

or not.

By the strong form of zero-decomposition theorem, there exist r.s. autoreduced sets $A_1, \ldots, A_l$ s.t.

$$W(HYP) = \bigcup_{i=1}^{l} W(A_i/R_i) \quad \text{w/ } R_i = S\text{-}rem(H_{A_i} G_i, A_i).$$

Proposition 5.3.1 $\quad W(HYP/C) = \phi$

$$\Updownarrow$$

$$\forall\, i=1, \ldots, l, \quad S\text{-}rem(C, A_i) = 0.$$

Proof. "$\Rightarrow$" Sps $W(HYP/C)=\phi$. $\forall i$, $W(A_i/R_i) \subseteq W(C)$

Let ξ_i be a generic point of $sat(A_i)$. Then $\xi_i \in W(A_i/R_i)$.

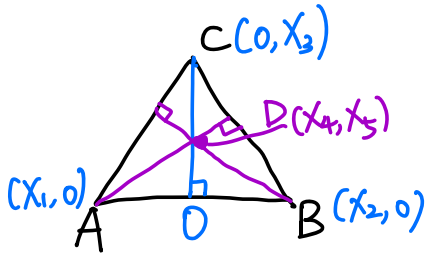
So $\xi_i \in W(C)$ and $C \in sat(A_i)$ follows. That is $C \xrightarrow{A_i} 0\ (\forall i)$.

"$\Leftarrow$" Sps $\forall i=1,\dots,l$, ξ-rem$(C, A_i)=0$. $\Rightarrow$ $W(A_i/H_{A_i}) \subseteq W(C)$

$\Rightarrow$ $W(HYP) \subseteq W(C)$, i.e., $W(HYP/C)=\emptyset$. $\Big|$ $\bigcup W(A_i/R_i)$

$\square$.

However, this proposition doesn't meet the reality of geometrical situations, and in this sense it cannot be accepted as a correct solution to the problem of mechanical theorem proving. That is because, no theorem will be true by definition (1) and theorems we encounter in all kinds of geometry are usually true only if certain subsidiary non-degeneracy conditions are observed. For example,



From $AD \perp BC$ & $BD \perp AC$, to show D is on $\overline{CO}$.

$AD \perp BC \Rightarrow h_1 = X_3X_5 - X_2(X_4-X_1)=0$

$BD \perp AC \Rightarrow h_2 = X_3X_5 - X_1(X_4-X_2)=0$

C: $X_4=0$ (i.e., D is on $\overline{CO}$).

$W(h_1,h_2) = W((X_2-X_1)X_4, (X_2-X_1)X_3X_5 + (X_2-X_1)X_1X_2/(X_2-X_1)X_3)$
$\cup W(h_1,h_2,X_2-X_1) \cup W(h_1,h_2,X_4)$

$= W(X_4, \underset{A_1}{X_3X_5 + X_2X_1/(X_2-X_1)X_3}) \cup W(X_2-X_1, \underset{A_2}{X_3X_5 - X_4X_1 + X_1^2/X_3})$

$X_4 \xrightarrow{\mathcal{A}_1} 0$ but $X_4 \not\xrightarrow{\mathcal{A}_2} 0$.

Non-degeneracy conditions:

$$\begin{cases} X_2 - X_1 \neq 0 \iff A \neq B \\ X_3 \neq 0 \Rightarrow C \text{ is not on } \overline{AB}. \end{cases}$$

To lay down a correct formulation of how a theorem is true to be defined, we first introduce the notion of dimension for irreducible autoreduced sets.

Definition 5.3.2 Let $\mathcal{A} = A_1, \ldots, A_p$ be an autoreduced sets in $K\{y_1, \ldots, y_n\}$ w.r.t. some ranking that is δ-irreducible. The integer $n-p$ is defined as the δ-dimension of $\mathcal{A}$, denoted by $\delta\text{-dim}(\mathcal{A})$.

Proposition 5.3.3 Let $\mathcal{A}$ be a char set of a prime δ-ideal $\mathfrak{p}$ under an arbitrary ranking R. Then $\delta\text{-dim}(\mathfrak{p}) = \delta\text{-dim}(\mathcal{A})$.

proof. (In page 1 of DA-10, we proved when R is some

elimination ranking, the result holds.)

Case 1). suppose $|\mathcal{A}| = n$ and we prove in this case $\delta\text{-dim}(p) = 0$. Let $\mathcal{A} = A_1, \cdots, A_n$.

Let $r_0 = \max_i \{ord(A_i)\} + 1$ and take $r \geq r_0$.

Set $\mathcal{L}_r = \left\{ \begin{array}{l} A_1, A_1', \cdots, A_1^{(r-o_1)}; \\ A_2, A_2', \cdots, A_2^{(r-o_2)}; \\ \cdots\cdots \\ A_n, A_n', \cdots, A_n^{(r-o_n)} \end{array} \right\}$ w/ $o_i = ord(ld(A_i))$.

Clearly, $\forall\, f \in sat(\mathcal{A}) \cap K[Y^{[r]}]$ $\left(Y^{[r]} = \{y_i^{(j)} : j \leq r\}\right)$,

$\delta\text{-rem}(f, \mathcal{A}) = prem(f, \mathcal{L}_r) = 0$.

So $sat(\mathcal{A}) \cap K[Y^{[r]}] = \underbrace{asat(\mathcal{L}_r)}_{(\mathcal{L}_r) : I_{\mathcal{L}_r}^{\infty}} \cap K[Y^{[r]}]$

Since $\dim(asat(\mathcal{L}_r)) = \#\{\text{parametric variables of } \mathcal{L}_r\}$

$w_{sat(\mathcal{A})}(r)$

$= \dim(sat(\mathcal{A}) \cap K[Y^{[r]}]) = \dim(asat(\mathcal{L}_r) \cap K[Y^{[r]}]) = ord(\mathcal{A})$

$= \sum_{i=1}^{n} o_i < \infty$. So $\delta\text{-dim}(sat(\mathcal{A})) = 0$. Case 1) ✓.

Now, assume $|\mathcal{A}| < n$ and let $U = Y \setminus lv(\mathcal{A})$. Then it is easy to show $\mathcal{A}$ is a char set of $\mathcal{I} = [P]_{K\langle U \rangle \{lv(\mathcal{A})\}}$. Since $|\mathcal{A}| = |lv(\mathcal{A})|$, by

Case 1), $\delta\text{-dim}(\mathcal{I}) = 0$. Thus, $\forall\ y_i \in lv(\mathcal{A})$, $\mathcal{I} \cap K\langle U \rangle\{y_i\} \neq \{0\}$, i.e., $P \cap K\{U, y_i\} \neq \{0\}$. Since $P \cap K\{U\} = \{0\}$, U is a parametric set of P. So $\delta\text{-dim}(P) = |U| = n - p$. 证.

Definition 5.3.4 A theorem with hypothesis system (HYP) and conclusion C is said to be generically true if for the decomposition formula $V(HYP) = \bigcup_i V(\mathcal{A}_i / R_i)$, $V(\mathcal{A}_i / R_i C) = \phi$ for all indices i for which $\delta\text{-dim}(\mathcal{A}_i) = \delta\text{-dim}(V(HYP))$ $(= \max_i \{\delta\text{-dim}(\mathcal{A}_i)\})$.

Since $V(\mathcal{A}_i / R_i C) = \phi \Longleftrightarrow \delta\text{-rem}(C, \mathcal{A}_i) = 0$, we have the following theorem which meets the reality of geometrical situations and forms the underlying principle of our method of mechanical theorem proving.

Theorem 5.3.5 There is a mechanical procedure

which permits to decide in a finite number of steps whether the hypothesis system is contradictory or not, and if not so, whether the theorem is generally true or not. In case that the theorem is generically true, then the procedure itself gives a proof of the theorem.

As the procedure for irreducible decomposition requires factorization which is usually quite complicated and is thus not so convenient to use in practice, we shall adopt an alternative definition for a theorem to be true.

Definition 5.3.6 Let HYP and C be as before. Let N be a $\mathcal{S}$-poly s.t. $\mathrm{NF}(\mathrm{HYP}/N.C) = \phi$. Then we say that the theorem is true generically under the subsidiary non-degeneracy condition $N \neq 0$.

The condition is said to be reasonable if

$$\delta\text{-dim}\,(\mathbb{V}(HYP, N) < \delta\text{-dim}(\mathbb{V}(HYP)).$$

Difficulty: To find such a δ-poly N !!! The following theorem meets such a difficulty and is at the basis of Wu's method of mechanical thm proving

Theorem 5.3.7 Let A be a char set of HYP (may be reducible) and $R = \delta\text{-rem}(C, A)$. (obtained by using well-ordering principle)

If $R = 0$, then the theorem is true generically under the subsidiary non-degeneracy condition $H_A \neq 0$.

If A is δ-irreducible, then the converse is also true.

Proof. If $R = \delta\text{-rem}(C, A) = 0$, then $\exists\, m \in \mathbb{N}$,

$$H_A^m \cdot C \equiv 0, \mod [A].$$

So $\mathbb{V}(A/H_A) \subseteq \mathbb{V}(C)$, i.e., $\mathbb{V}(A/H_A C) = \emptyset$.

If $\mathcal{A}$ is δ-irreducible, let ξ be a generic point of $sat(\mathcal{A})$. Then $\xi \in W(\mathcal{A}/H_{\mathcal{A}})$.

So $W(\mathcal{A}/H_{\mathcal{A}}C) = \phi \Rightarrow C(\xi) = 0 \Rightarrow \delta\text{-rem}(C, \mathcal{A}) = 0$. ∎

Procedures for Mechanical Theorem Proving:

Step 1. Select a coordinate system and form the δ-poly sets $HYP = 0$ and $C = 0$.

Step 2. Take a ranking R and use the well ordering principle to decompose $W(HYP)$:

$$W(HYP) = W(\mathcal{A}/H_{\mathcal{A}}) \cup \bigcup_{A \in \mathcal{A}} (W(HYP, I_A) \cup W(HYP, S_A)).$$

Step 3. Compute $R = \delta\text{-rem}(C, HYP)$.

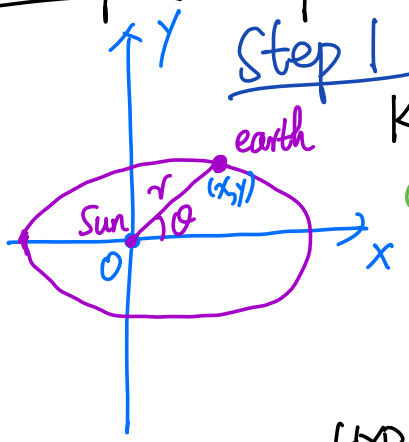
If $R = 0$, then the theorem is true generically under the subsidiary condition $H_{\mathcal{A}} \neq 0$.

If $R \neq 0$, check whether $\mathcal{A}$ is irreducible. In case $\mathcal{A}$ is irreducible, there is a geometric configuration s.t. the conclusion is not valid on $W(\mathcal{A}/H_{\mathcal{A}})$.

(Step 4. In case $\mathcal{A}$ is reducible, we can compute a more refined decomposition for $\mathcal{V}(HYP) = \bigcup_i \mathcal{V}(\mathcal{A}_i/\mathcal{R}_i)$ and compute whether $\delta\text{-}\dim(C, \mathcal{A}_i) = 0$ for $\delta\text{-}\dim(\mathcal{A}_i)$ maximal.)

In general, steps 1-3 are enough and quite efficient in practise.

Example (Kepler's law $\Longrightarrow$ Newton's Gravitation laws)



Step 1

Kepler's law $\begin{cases} (K1)\ r = \dfrac{p}{1-e\cos\theta},\ (p' = e' = 0) & \text{椭圆定律} \\ (K2)\ r^2\theta' = h\ (h: \text{constant}),\ h' = 0 & \text{面积定律} \end{cases}$

(polar coordinates (r, θ))

$\Downarrow$ 极坐标转化为直角坐标

$x = r\cos w$, $y = r\sin w$, $\cos^2 w + \sin^2 w = 1$, $(\cos w)' = -\sin w \cdot w'$, $(\sin w)' = \cos w \cdot w'$

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

(rectangular coordinates (x, y))

Newton's law $\begin{cases} (N1)\ a = \dfrac{const}{r^2} \\ (N2)\ (x'', y'') = const \cdot (-x, -y) \end{cases}$

$\Downarrow$

$$\begin{cases} (x'')^2 + (y'')^2) \cdot r^4 = k \\ k' = 0 \\ x''y - xy'' = 0 \end{cases}$$

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

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

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

Step 2.

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

$$HYP \Longleftrightarrow \Sigma_1 := \begin{cases} F_1 = X_{21}' \\ F_2 = X_{22}' \\ F_3 = X_{21} + X_{22}X_{32} - X_{31} \\ F_4 = X_{32}X_{33}' - X_{32}'X_{33} - X_{51} \\ F_5 = X_{51}' \\ F_6 = X_{32}^2 + X_{33}^2 - X_{31}^2 \\ F_7 = X_{32}''^2 \cdot X_{31}^4 + X_{33}''^2 \cdot X_{31}^4 - X_{52} \end{cases} \qquad C \Longleftrightarrow \begin{matrix} X_{52}' \\ X_{32}''X_{33} - X_{33}''X_{32} \end{matrix}$$

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

$$A_1 = F_1, F_2, F_3, F_6, F_4, F_7$$

$$r_1 = \delta\text{-}rem(F_5, A_1) = 4X_{21}\left[(X_{31}^3 X_{22}^2 - X_{31}^3 + 2X_{31}^2 X_{21} - X_{31}X_{21}^2)X_{31}'' + X_{31}X_{21}X_{31}'^2 - X_{31}'^2 X_{21}^2 \right]$$

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

$A_2 = F_1, F_2, r_1, F_3, F_6, F_4, F_7$

$R_2 = \phi$

So $A = A_2$ is a char set of Σ_1.

Step 3. $\xi\text{-rem}(X_{52}, A) = 0$ with $h_1 = -128 X_{33}^8 X_{22}^8 X_{21}^2$

$\xi\text{-rem}(X_{32}'' X_{33} - X_{32} X_{33}'', A) = 0$ with $h_2 = 16 X_{33}^3 X_{22}^3 X_{21}$

So $W(HYP/H_{HYP}) \subseteq W(C)$.

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

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

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) can derive (N1) and (N2).

Remark: In maple 15, with Rosenfeld-Gröbner (Σ_1, R) only 0.5 s is used to compute A (and other chains). Also, with Wu-Ritt's well-ordering principle, we can discover new properties with geometric or physical meanings.

Review for ordinary differential algebra

Chapter 1 Notions: differential rings (R, δ) / δ-ideals

Notation: $S \subseteq R$, $[S]$ ($\{S\}$) denote the (radical) δ-ideal generated by S.

- In general, $\{S\} \neq \sqrt{[S]}$ and a maximal δ-ideal might not be prime.
- For each radical δ-ideal $I \neq R$, $I = \bigcap_{I \subseteq P \text{ prime}} P$.
- If R is a Ritt algebra (i.e., $\mathbb{Q} \subseteq R$), $\{S\} = \sqrt{[S]}$ and a maximal δ-ideal is prime.

Chapter 2 Notions: diff poly ring $K\{y_1, \dots, y_n\}$ (K: δ-field of char 0)

diff homomorphism, diff zero, diff variety

diff characteristic set (ranking, leader/initial/separant/rank, autoreduced set / diff reduction formula, equivalent conditions)

Ritt-Raudenbush basis theorem / Minimal prime decomposition for radical δ-ideals in $K\{y_1, \dots, y_n\}$

Chapter 3 Two inclusion-reversing maps:

$$\mathbb{I}: \{\delta\text{-varieties in } K^n\} \longrightarrow \{\text{radical } \delta\text{-ideals in } K\{y_1, \dots, y_n\}\}$$

$$V \qquad\qquad \mathbb{I}(V)$$

$$\mathbb{V}: \{\text{radical } \delta\text{-ideals in } K\{y\}\} \longrightarrow \{\delta\text{-varieties in } K^n\}$$

$$J \qquad\qquad \mathbb{V}(J)$$

- Fact: $\mathbb{V}(\mathbb{I}(V)) \overset{J}{=} V$.

- Diff Hilbert Nullstellensatz $\mathbb{I}(\mathbb{V}(J)) = J$
- Irreducible decomposition for diff varieties
- Ritt's component theorem for a single δ-poly:

  Given $A \in K\{y_1, \dots, y_n\} \setminus K$ irr, a minimal prime decomposition of $\{A\}$:

  $$\{A\} = \mathrm{sat}(A) \cap P_2 \cap \cdots \cap P_e,$$

  where $\mathrm{sat}(A) = [A] : S_A^\infty = \{A\} : S_A$ is the general component of A,

  $P_2, \dots, P_e$ are singular components of A with $S_A \in P_i$.

  Moreover, $P_i = \mathrm{sat}(B_i)$ for some irr $B_i \in K\{y\}$ and $\mathrm{ord}(B_i) < \mathrm{ord}(A)$.

Chapter 4 Notions: diff algebraic/transcendental, δ-transcendence basis/degree, diff dimension, diff dimension polynomial

Main results: (K, δ): a δ-field of char 0.

① $K \subseteq L \Rightarrow \delta$ can be extended to L.

The extension is unique $\Leftrightarrow$ L/K is algebraic.

② primitive element theorem: If $C_K \neq K$ and $K\langle y_1, \dots, y_n\rangle$ is a δ-alg $/K$, then $\exists\, y$ s.t. $K\langle y_1, \dots, y_n\rangle = K\langle y\rangle$ ($y = a_1 y_1 + \cdots + a_n y_n$ w/ $a_i \in K$).

Non-vanishing theorem for diff poly

③ • $\delta\text{-}\dim(V) = \delta.\mathrm{tr.deg}\, K\langle V\rangle / K$

$= \delta.\mathrm{tr.deg}\, K\langle y_1, \dots, y_n\rangle / K$ ($(y_1, \dots, y_n)$: a generic point of V)

- $W_V(t) = \text{tr.deg}\, K(\eta_1^{[t]}, \ldots, \eta_n^{[t]})/K$

  $= \delta\text{-dim}(V) \cdot (t+1) + \text{ord}(V)$

- relative order of V w.r.t. a parametric set U
- diff resolvents for irr varieties

Chapter 5. Notions: basic set / characteristic set of a δpoly set

well-ordering principle

Zero-decomposition theorems: weak / strong form

Variety-decomposition theorem