An Algorithm for Transforming Regular Chain into Normal Chain*

Banghe Li and Dingkang Wang

Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
Beijing 100080, China
libh@amss.ac.cn, dwang@mmrc.iss.ac.cn

Abstract. We present an improved algorithm to compute the normal chain from a given regular chain such that their saturation ideals are the same. Our algorithm is based on solving a system of linear equations and the original method computes the resultants of multivariate polynomials. From the experiments, for the random polynomials, our algorithm is much more efficient than the original one.

1 Introduction

Characteristic set method has been successfully applied to automatic theorem proving by Wu [11]. In fact, this method also can be used for solving systems of polynomial equations. In order to solve a system of polynomial equations, the polynomial system should be decomposed into chains. Wu himself proposed an algorithm to compute such decompositions. The regular zeros of the chain in the decomposition maybe empty and some redundant components may be introduced by using Wu's method. Yang introduced regular chain and the regular zeros of a regular chain should not be empty [12]. Both Yang and Kalbrener presented algorithms to decompose a system of polynomials into a series of regular chains such that the zeros of the system of polynomials are the union of the regular zeros of the regular chains. Efficient algorithms to decompose a system of polynomials into regular chains have been proposed by Moreno [6] and Wang [10].

In [3], Gao introduced the concept of p-chain in order to solve systems of equations of parametric polynomials. To avoid the confusion, we will rename the p-chain as normal chain in this paper. To compute the normal chain from a given regular chain, the resultants of multivariate polynomials will be computed and the computation of resultants will be too costly. In [9], normal chain is introduced and an algorithm is proposed to compute a normal chain from a chain if it does not fail. An algorithm to decompose polynomial system into normal chains is given in [8].

* Partially supported by NKBRPC (2004CB318000) and NSFC (10771206).

D. Kapur (Ed.): ASCM 2007, LNAI 5081, pp. 236–245, 2008.

In all the existed algorithms to compute the normal chain from a regular chain, the computation of polynomial resultant is needed and resultant computation of polynomials is quite cost.

In this paper, we will present a new algorithm to compute the normal chain from a regular chain. Our algorithm is based on solving system of linear equations. It is not needed to compute the resultants of multivariate polynomials in our algorithm and the experiment results show that our algorithm is much more efficient than the original one.

After giving some preliminaries in section 2, we will give an algorithm to compute the inverse of a uni-variable polynomial modulo another uni-variable polynomial. A table to record the timings for computing the inverses of random polynomials is given in section 3. An algorithm will be given to compute a normal chain from a regular chain such that they have the same saturation ideal in section 4. An example to decompose the Lorentz polynomial system into normal chains will be reported in section 5. The conclusions will be given in the last section.

2 Preliminaries

Let $\mathrm{K}[u_1, \cdots, u_p, y_1, \cdots, y_s]$ be the polynomial ring with $u_1, \cdots, u_p, y_1, \cdots, y_s$ as indeterminates and coefficients in a field K. Let $\mathrm{U} = \{u_1, \cdots, u_p\}$. $\mathrm{Y} = \{y_1, \cdots, y_s\}$. $\mathrm{K}[u_1, \cdots, u_p, y_1, \cdots, y_s]$ is denoted by $\mathrm{K}[\mathrm{U}, \mathrm{Y}]$. In this paper, we always assume that the variable ordering is $u_1 < \cdots < u_p < y_1 < \cdots < y_s$.

Let E be an algebraic closed extension field containing K. For a polynomial set $\mathbb{F}$, $(\mathbb{F})$ denotes the ideal generated by $\mathbb{F}$ over the ring $\mathrm{K}[\mathrm{U}, \mathrm{Y}]$. $\mathrm{Zero}(\mathbb{F})$ denotes the common zeros in $\mathrm{E}^{(p+s)}$ of the polynomials in $\mathbb{F}$. Let D be a polynomial, $\mathrm{Zero}(\mathbb{F}/D)$ denotes the common zeros in $\mathrm{E}^{(p+s)}$ of the polynomials in $\mathbb{F}$ which are not zeros of D.

For any nonzero polynomial P, the leading variable of P is denoted as v_P, the leading coefficient of P with respect to v_P is called the initial of P, denoted by $\mathrm{I}(P)$. We denote $\deg(P, y_i)$ the degree of P w.r.t. y_i.

Let $\mathcal{A} : A_1, \cdots, A_s$ be a chain and the leading variables of A_i is y_i. We will use $I_{\mathcal{A}}$ to denote the product of the initials of the polynomials in $\mathcal{A}$, i.e. $I_{\mathcal{A}} = \prod_{i=1}^{s} \mathrm{I}(A_i)$.

For two univariable polynomials P and Q, the remainder of P divided by Q w.r.t. y will be denoted by $\mathrm{rem}(P, Q, y)$. If P and Q are multivariable polynomials, the psudoremainder of P divided by Q w.r.t. y_i will be denoted by $\mathrm{prem}(P, Q, y_i)$. For two polynomials P, Q , the Sylvester resultant of P and Q with respect to y_i is denoted by $\mathrm{res}(P, Q, y_i)$.

Definition 1. *Let P be a polynomial, $\mathcal{A} = A_1, \cdots, A_s$ be a chain with y_i as the leading variable of A_i. Let $R_s = P$, $R_{i-1} = \mathrm{res}(R_i, A_i, y_i)$ for $i = s, \cdots, 1$. R_0 is called the resultant of P with respect to $\mathcal{A}$, denoted by* $\mathrm{Res}(P; \mathcal{A})$.

It is easy to see that R_0 is in $K[u_1, \cdots, u_p]$. There are polynomials F, G_i for $i = 1, \cdots, s$ such that

$$FP + \sum_{i=1}^{s} G_i A_i = \mathrm{Res}(P; \mathcal{A}) \tag{1}$$

Definition 2. *Suppose $\mathcal{A}$ is a chain, if $\xi \in E^n$ and $\xi \in Zero(\mathcal{A}/I_{\mathcal{A}})$, then ξ is called a regular zero of $\mathcal{A}$.*

The regular zeros of a chain maybe empty.

Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain, the ideal generated by $\mathcal{A}$ over $\mathrm{K}[\mathrm{U}, y_1, \cdots, y_s]$ will be denoted by $(\mathcal{A})$. Let $\mathcal{A}_i = A_1, \cdots, A_i$ for $1 \leq i \leq s$, each $\mathcal{A}_i$ is also a chain and the ideal generated by $\mathcal{A}_i$ over $\mathrm{K}[\mathrm{U}, y_1, \cdots, y_i]$ will be denoted by $(\mathcal{A}_i)$.

Definition 3. *Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain in* $\mathrm{K}[\mathrm{U}, \mathrm{Y}]$ *and P be a polynomial in* $\mathrm{K}[\mathrm{U}, \mathrm{Y}]$. *$P$ is said to be invertible w.r.t. $\mathcal{A}$ if $(\mathcal{A}, P) \cap \mathrm{K}[\mathrm{U}] \neq \{0\}$*

If P is invertible w.r.t. $\mathcal{A}$, then there exist Q in $\mathrm{K}[\mathrm{U}, \mathrm{Y}]$ and $M \neq 0$ in $\mathrm{K}[\mathrm{U}]$ such that $PQ \equiv M \mod (\mathcal{A})$

An algorithm to test if a polynomial is invertible with respect to a chain is given in [2]. Procedures to compute the inverse of a polynomial with respect to a chain are given in [2,5,6].

Definition 4. *Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain. Let $\mathcal{A}_i = A_1, \cdots, A_i$ for $i = 1, \cdots s$. $\mathcal{A}$ is a regular chain if s=1 or* $\mathrm{Res}(\mathrm{I}(A_i); \mathcal{A}_{i-1}) \neq 0$ *for $i = 2, \cdots, s$.*

The regular chain is introduced by Yang et. al. in [12]. The above definition implies that the regular zeros of a regular chain are not empty.

Definition 5. *Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain and $\xi \in E^{(p+s)}$ be a zero of $\mathcal{A}$. $\xi = (\xi_1, \cdots, \xi_p, \xi_{p+1}, \cdots, \xi_{p+s})$, ξ is called to be a generic regular zero of $\mathcal{A}$ if $(\xi_1, \cdots, \xi_p)$ are algebraically independent over* K.

The following theorem establishes the relationship between regularity of a chain and invertibility of its initials.

Theorem 1. *Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain, the following statements are equivalent:*

1. *$\mathcal{A}$ is a regular chain*
2. *For $i = 1, \cdots, s$,* $\mathrm{I}(A_i)$ *is invertible w.r.t. $\mathcal{A}$.*
3. *For any generic regular point ξ,* $\mathrm{I}(A_i)(\xi) \neq 0$ *for $i = 1, \cdots, s$.*

Please see [2] or [10] for the proof of the theorem.

Definition 6. *A chain $\mathcal{A} = A_1, \cdots, A_s$ is called a normal chain if* $\mathrm{I}(A_i)$ *is in* $\mathrm{K}[\mathrm{U}]$ *for $i = 1, \cdots, s$.*

This definition means that a normal chain must be a regular chain. To compute the regular zeros of a normal chain is much easier than to compute the regular zeros of a regular chain. A normal chain is also called a p-chain in Gao and Chou [3]. Some properties about normal chains have been discussed in Wang [10].

Definition 7. *Let $\mathcal{A} = A_1, \cdots, A_s$ be a chain, the saturation ideal of $\mathcal{A}$, denoted by $(\mathcal{A}) : I_{\mathcal{A}}^{\infty}$, is defined as follows*

$$(\mathcal{A}) : I_{\mathcal{A}}^{\infty} = \{P | I_{\mathcal{A}}^{k} P \in (\mathcal{A}) \ \textit{for some integer } k \geq 0 \ \} \tag{2}$$

Lemma 1. *Let* $\mathcal{A} = A_1, \cdots, A_s$ *be a regular chain, let* P *be a polynomial in* K[U, Y], $P \in (\mathcal{A}) : I_{\mathcal{A}}^{\infty}$ *if and only if there exist a polynomial* L *in* K[U]\{0} *such that* $LP \in (\mathcal{A})$.

Please refer [2,5] for the proof.

3 An Algorithm to Compute the Inverse of a Polynomial Modulo an Ideal

Let P, Q be polynomials in K[x]. If P and Q have no common divisors, there exist polynomial P' and Q' such that $\deg(P', x) < \deg(Q, x)$, $\deg(Q', x) < \deg(P, x)$ and $PP' + QQ' = 1$. The extended Euclidean algorithm can compute out P' and Q'. Let $d = \deg(Q, x)$, suppose $P' = a_{d-1}x^{d-1} + \cdots + a_0$, from $\mathrm{rem}(PP' - 1, Q, x) = 0$, we can get a system of linear equations on the variables $a_0, \cdots, a_{d-1}$. It is easy to solve all the a_i for $i = 0, \cdots, d-1$.

Let's see a simple example:

$P = 4x^3 + 8x^2 + 7x + 3$, $Q = 5x^4 + 4x^3 + 3x^2 + 6$.
Let $P' = a_3x^3 + a_2x^2 + a_1x + a_0$,
$\mathrm{rem}(PP' - 1, Q, x) = (-\frac{61}{125}a_3 + \frac{19}{25}a_2 + \frac{24}{5}a_1 + 4a_0)x^3 + (-\frac{657}{125}a_3 + \frac{3}{25}a_2 + \frac{23}{5}a_1 + 8a_0)x^2 + (-\frac{144}{25}a_3 - \frac{24}{5}a_2 + 3a_1 + 7a_0)x + (-\frac{114}{125}a_3 - \frac{144}{25}a_2 - \frac{24}{5}a_1 + 3a_0 - 1)$.
If $\mathrm{rem}(PP' - 1, Q, x) = 0$, we have

$$\begin{array}{l} -\frac{61}{125}a_3 + \frac{19}{25}a_2 + \frac{24}{5}a_1 + 4a_0 = 0 \\ -\frac{657}{125}a_3 + \frac{3}{25}a_2 + \frac{23}{5}a_1 + 8a_0 = 0 \\ -\frac{144}{25}a_3 - \frac{24}{5}a_2 + 3a_1 + 7a_0 = 0 \\ -\frac{114}{125}a_3 - \frac{144}{25}a_2 - \frac{24}{5}a_1 + 3a_0 - 1 = 0 \end{array} \tag{3}$$

The solution is $a_0 = \frac{2194}{13255}, a_1 = -\frac{1614}{13255}, a_2 = -\frac{709}{79530}, a_3 = \frac{2309}{15906}$. then $P' = \frac{2309}{15906}x^3 - \frac{709}{79530}x^2 - \frac{1614}{13255}x + \frac{2194}{13255}$. P' is the inverse of P modulo the polynomial Q.

For polynomials P and Q, the following algorithm will compute the inverse of P modulo Q.

Algorithm 1. InverseModUniVarPol

Input : P,Q are two polynomials in K[x] which have no common divisors.
Output: P' such that $PP' = 1 \bmod (\mathrm{Q})$.
$d \leftarrow \deg(Q, x)$
$P' \leftarrow a_{d-1}x^{d-1} + \cdots + a_0$
$r \leftarrow \mathrm{rem}(PP', Q, x)$
$H \leftarrow coeffs(r - 1, x)$; The set of the coefficients r w.r.t x.
$S \leftarrow$ *solution* of $H = 0$ for a_i for $i = 0, \cdots, d-1$
$P' \leftarrow subs(S, P')$; substitute the solutions for the a_i's in P'
return P'

Suppose $Q = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is a monic polynomial , the companion matrix of Q is the $n \times n$ square matrix

$$G = \begin{pmatrix} 0\,0\cdots & 0 & -a_0 \\ 1\,0\cdots & 0 & -a_1 \\ 0\,1\cdots & 0 & -a_2 \\ \vdots\,\vdots\,\ddots & \ddots & \vdots \\ 0\,0\cdots & 1 & -a_{d-1} \end{pmatrix}$$

To compute the inverse of a polynomial modulo a monic polynomial, we have the following theorem.

Theorem 2. *Suppose $P, Q \in K[x]$, Q is monic, and P, Q have no common divisors. Let G be the companion matrix of Q, $P' = b_{d-1}x^{d-1} + \cdots + b_0$, then P' is the inverse of P modulo Q, i.e. $PP' = 1$ mod Q if and only if $(b_0, \cdots, b_{d-1})^T$ is the solution of $P(G)y = (1, 0, \cdots, 0)^T$.*

Proof. Let I be the ideal generated by Q in $K[x]$. $K[x]/I$ can be thought as a finite dimensional linear vector space over K. $\{1, x, \cdots, x^{d-1}\}$ is a monomial basis of $K[x]/I$. M_x is a linear map from $K[x]/I$ to itself, M_x is defined by $M_x(F) = xF \mod \text{I}$ for any F in $K[x]/I$. It is easy to check that G is the matrix representation of M_x on the monomial basis $\{1, x, \cdots, x_{d-1}\}$. Let $M_P(F) = PF \mod \text{I}$, M_P is a linear map defined by P on $K[x]/I$ and $P(G)$ is the matrix representation of M_P, hence $M_P(P') = PP' = 1 \mod \text{I}$ if and only if $(b_0, \cdots, b_{d-1})^T$ is the solution of $P(G)y = (1, 0, \cdots, 0)^T$.

Another proof of this theorem also can be found in [7].

If P, Q are polynomial in K[U, $y_1, \cdots, y_i$], we can extend the above algorithm to find polynomial P' in K[U, $y_1, \cdots, y_i$] and M in K[U, $y_1, \cdots, y_{i-1}$] such that $\text{prem}(PP' - M, Q, y_i) = 0$.

Algorithm 2. InverseModPol

Input : P,Q are two polynomials in K[U, $y_1, \cdots, y_i$] which have no common divisors.
Output: $P' \in$ K[U, $y_1, \cdots, y_i$] and $M \in$ K[U, $y_1, \cdots, y_{i-1}$] such that $\text{prem}(PP' - M, Q, y_i) = 0$.
$d \leftarrow \deg(Q, y_i)$
$P' \leftarrow a_{d-1}y_i^{d-1} + \cdots + a_0$
$r \leftarrow \text{prem}(PP' - M, Q, y_i)$
$H \leftarrow coeffs(r, y_i)$; The set of the coefficients r w.r.t x.
$S \leftarrow solution$ of $H = 0$ for a_i for $i = 0, \cdots, d-1$ and M is considered as a parameter
$P' \leftarrow subs(S, P')$; substitute the solutions for the a_i's in P'
$M \leftarrow denom(P')$; M is the denominator of P'.
return (P', M)

For P, Q are polynomial in $\mathrm{K[U}, y_1, \cdots, y_i]$, we know that there exists P' and Q' in $\mathrm{K[U}, y_1, \cdots, y_i]$ and M in $\mathrm{K[U}, y_1, \cdots, y_{i-1}]$ such that $P'P + Q'Q = M$.

We have implemented the above algorithm. The following is a table which records the timings to compute the inverse of a polynomial modulo another polynomial.

Timings of Computing the Inverse

Number of Variables	Total Degree	Timings	
		InverseModPol	InverseModPol-SubRes
3	3	0.046	0.040
3	4	0.198	0.311
3	5	0.880	1.608
3	6	4.492	9.917
3	7	23.343	64.644
3	8	119.563	407.158
3	9	587.672	2138.584
4	3	0.145	0.067
4	4	1.728	1.564
4	5	43.377	55.396
4	6	1109.934	1426.564
4	7	19673.498	39052.547

If we apply the above algorithm successively, then we can compute the the inverse of a polynomial modulo the saturation ideal of a regular chain. Let P be a polynomial, $\mathcal{A} = A_1, \cdots, A_s \subset \mathrm{K[U, Y]}$ be a regular chain, P is invertible w.r.t. $\mathcal{A}$, then there exist polynomial $P' \in \mathrm{K[U, Y]}$ and $M \in \mathrm{K[U]}$ such that $PP' - M = 0 \bmod ((\mathcal{A}) : \mathrm{I}_{\mathcal{A}}^{\infty})$.

The following algorithm will compute the inverse of a polynomial modulo the saturation ideal of a regular chain.

Algorithm 3. InverseModSat

Input : P is a polynomial in $\mathrm{K[U, Y]}$, $\mathcal{A} = A_1, \cdots, A_s$ is a regular chain in $\mathrm{K[U, Y]}$, y_i is the leading variable of A_i for $i = 1, \cdots, s$, P is invertible w.r.t. $\mathcal{A}$.

Output: $P' \in \mathrm{K[U, Y]}$, $M \in \mathrm{K[U]}$ such that $PP' = M \bmod ((\mathcal{A}) : \mathrm{I}_{\mathcal{A}}^{\infty})$.

$Q \leftarrow 1$
for *i from s to 1 step -1* **do**
  $(P', M) \leftarrow \mathrm{InverseModPol}(P, Q, y_i)$
  $P \leftarrow M$
  $Q \leftarrow QP'$
end
$P' \leftarrow Q$
$M \leftarrow P$
return (P', M)

4 Transforming Regular Chain into Normal Chain

Let $\mathcal{A} = A_1, \cdots, A_s$ be a regular chain and $\mathcal{A}_i = A_1, \cdots, A_i$ for $i = 1, \cdots, s$, let I_i be the initial of A_i, i.e. $I_i = \mathrm{I}(A_i)$, $I_1 \in \mathrm{K[U]}$, for $i = 2, \cdots, s$, I_i is invertible w.r.t. $\mathcal{A}$, then there exist I_i' in $\mathrm{K}[\mathrm{U}, y_1, \cdots, y_{i-1}]$, M_i in K[U] such that $\mathrm{prem}(I_i I_i' - M_i; \mathcal{A}_{i-1}) = 0$. i.e. $I_i I_i' = M_i + N_i$ and $N_i \in (\mathcal{A}_{i-1}) : I_{\mathcal{A}_{i-1}}^{\infty}$. We let $B_1 = A_1$, $H_1 = 1$, and for $i = 2, \cdots, s$, $B_i = M_i y_i^{n_i} + I_i' R_i$ and $H_i = M_2 \cdots M_i$, with $A_i = I_i y_i^{n_i} + R_i$. Let $\mathcal{B}_i = B_1, \cdots, B_i$.

Theorem 3. *For $\mathcal{A}$ and $\mathcal{B}$ as above, $\mathcal{A}$ is a regular chain and $\mathcal{B}$ is a normal chain , we have $(\mathcal{A}) : I_{\mathcal{A}}^{\infty} = (\mathcal{B}) : I_{\mathcal{B}}^{\infty}$.*

Proof. We will prove $(\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty} = (\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$ for $i = 1, \cdots, s$.

($\subset$) We will prove $(\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty} \subset (\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$ by induction on i. It is true for $i = 1$. Suppose it is also true for $i - 1$, we will prove it for i.

For any $P \in (\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty}$ then there exist a nonzero polynomial $L_i \in \mathrm{K[U]}$ such that $L_i P \in (\mathcal{A}_i)$ by lemma 1, i.e. there exist polynomial Q_i such that $L_i P = Q_i A_i \bmod (\mathcal{A}_{\mathrm{i}-1})$.

$$\begin{aligned} H_i L_i P &= H_{i-1} M_i Q_i A_i \bmod (\mathcal{A}_{\mathrm{i}-1}) \\ &= H_{i-1} Q_i (I_i I_i' - N_i) A_i \bmod (\mathcal{A}_{\mathrm{i}-1}) \\ &= H_{i-1} Q_i (I_i B_i + N_i y_i^{n_i} - N_i A_i) \bmod (\mathcal{A}_{\mathrm{i}-1}) \end{aligned}$$

By induction, we know that $H_i L_i P$ is in $(\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$. Since $H_i, L_i \in \mathrm{K[U]}$, we know that P is in $(\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$ by lemma 1.

($\supset$) For any $P \in (\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$, then there exist a nonzero polynomial $L_i \in \mathrm{K[U]}$ such that $L_i P$ is in $(\mathcal{B}_i)$ by lemma 1. From $I_i' A_i = B_i + N_i y_i^{n_i}$, we know that $L_i P \in (\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty}$. Since L_i is in K[U] and $\mathcal{A}_i$ is a regular chain, then P is in $(\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty}$.

Let $B_1' = B_1$, $\mathcal{B}_1' = B_1$, for $i = 2, \cdots, s$, let B_i' be the remainder of B_i w.r.t $\mathcal{B}_{i-1}'$ and $\mathcal{B}_i' = B_1', \cdots, B_i'$. Let $\mathcal{B}' = \mathcal{B}_s'$. It is easy to see that $\mathcal{B}'$ is a normal chain and $(\mathcal{B}) : I_{\mathcal{B}}^{\infty} = (\mathcal{B}') : I_{\mathcal{B}'}^{\infty}$. $\mathcal{B}'$ is called the normalization of $\mathcal{A}$. It is easy to check that

$$\mathrm{Zero}(\mathcal{B}'/I_{\mathcal{B}'}) \subset \mathrm{Zero}(\mathcal{A}/I_{\mathcal{A}}) \subset \mathrm{Zero}(\mathcal{A}) \subset \mathrm{Zero}(\mathcal{B}')$$

According to the above theorem, we have the following algorithm to transform a regular chain into a normal chain.

From the above theorem, we have

Corollary 1. *For a polynomial set $\mathbb{F}$, there is an algorithm to compute a series of normal chains $\mathcal{B}_i$ such that*

$$\mathrm{Zero}(\mathbb{F}) = \bigcup_i \mathrm{Zero}((\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}) \tag{4}$$

Proof. For a polynomial set $\mathbb{F}$, there are algorithms to compute a series of regular chains $\mathcal{A}_i$ such that

$$\mathrm{Zero}(\mathbb{F}) = \bigcup_i \mathrm{Zero}((\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty})$$

Algorithm 4. Reg2Norm

Input : $\mathcal{A} = A_1, \cdots, A_s$ is a regular chain in K[U, Y], y_i is the leading variable of A_i for $i = 1, \cdots, s$
Output: $\mathcal{B} = B_1, \cdots, B_s$ is a normal chain in K[U, Y] such that $(\mathcal{A}) : I_{\mathcal{A}}^{\infty} = (\mathcal{B}) : I_{\mathcal{B}}^{\infty}$

$Q \leftarrow 1$
if *s=1* **then return** $\mathcal{A}$
$B_1 \leftarrow A_1$
for $i \leftarrow 2$ **to** s **do**
  $I_i \leftarrow \mathrm{I}(A_i)$
  $(I_i', M_i) \leftarrow \mathrm{InverseModSat}(I_i, \mathcal{A}_{i-1})$
  $n_i \leftarrow \deg(A_i, y_i)$
  $R_i \leftarrow A_i - I_i y_i^{n_i}$
  $B_i \leftarrow M_i y_i^{n_i} + I_i' R_i$
end
$\mathcal{B} \leftarrow B_1$
for $i \leftarrow 2$ **to** s **do**
  $\mathcal{B} \leftarrow \mathcal{B}, Reduce(B_i, \mathcal{B})$
end
return $\mathcal{B}$

where $\mathcal{A}_i$'s are regular chains. For each $\mathcal{A}_i$, the above algorithm will compute a normal chain $\mathcal{B}_i$ such that $(\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty} = (\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty}$, and so

$$\mathrm{Zero}(\mathbb{F}) = \bigcup_i \mathrm{Zero}((\mathcal{A}_i) : I_{\mathcal{A}_i}^{\infty}) = \bigcup_i \mathrm{Zero}((\mathcal{B}_i) : I_{\mathcal{B}_i}^{\infty})$$

The corollary is proved.

If the polynomial system $\mathbb{F}$ is zero dimensional, then we have

$$\mathrm{Zero}(\mathbb{F}) = \bigcup_i \mathrm{Zero}(\mathcal{B}_i)$$

Corollary 2. *For a polynomial set* $\mathbb{F}$*, there is an algorithm to compute a series of normal chains* $\mathcal{A}_i$ *such that*

$$\mathrm{Zero}(\mathbb{F}) = \bigcup_i \mathrm{Zero}(\mathcal{A}_i / I_{\mathcal{A}_i})) \tag{5}$$

5 Examples

Example 1. Solving the following Lorentz problem:

$$\begin{aligned} f_1 &= x_2(x_3 - x_4) - x_1 + c = 0 \\ f_2 &= x_3(x_4 - x_1) - x_2 + c = 0 \\ f_3 &= x_4(x_1 - x_2) - x_3 + c = 0 \\ f_4 &= x_1(x_2 - x_3) - x_4 + c = 0 \end{aligned}$$

where x_1, x_2, x_3 and x_4 are variables and c is a parameter.

This problem has been discussed in [3]. In order to solve this system of equations of parametric polynomials. We will decompose this polynomial system into normal chains.

Let $F = \{f_1, f_2, f_3, f_4\}$, for a variable order $x_4 > x_3 > x_2 > x_1 > c$, we have the zero decomposition

$$\text{Zero}(F) = \bigcup_{i=1}^{9} \text{Zero}(\mathcal{A}_i / I_{\mathcal{A}_i})$$

where $\mathcal{A}_i$'s are regular chains.

We can transform the regular chains $\mathcal{A}_i$ into normal chains $\mathcal{B}_i$ by using algorithm *Reg2Norm* such that $\bigcup_{i=1}^{9} \text{Zero}(\mathcal{B}_i / I_{\mathcal{B}_i}) \subset \text{Zero}(F)$. For this example, we have

$$\text{Zero}(F) = \bigcup_{i=1}^{9} \text{Zero}(\mathcal{B}_i / I_{\mathcal{B}_i})$$

where $\mathcal{B}_i$ are normal chains. By our new algorithm, it takes 63 seconds to get the normal chains while the old algorithm will cost 106 seconds.

The following is a table which records the length of the chain and the number of the terms of the polynomials in the normal chains which are in the decomposition of the Lorentz polynomial system.

The normal chains in the decomposition

normal chains	length of the chain	number of terms				
1	4	2	2	2	2	
2	4	1291	1289	410	13	
3	5	1	2	1	2	2
4	5	2	2	1	2	3
5	5	2	2	2	2	2
6	5	3	6	7	5	3
7	5	1	2	2	2	3
8	5	9	9	9	5	5
9	5	15	15	15	8	8

6 Conclusions

We give a new algorithm to compute the normal chain from a regular chain such that their saturation ideals are the same. Our algorithm is based on solving system of linear equations and it is much more efficient than the original algorithm to compute the normalization of a regular chain.

References

1. Aubry, P., Lazard, D., Maza, M.M.: On the Theories of Triangular Sets. J. Symbolic Computation 28, 105–124 (1999)
2. Bouziane, D., Kandri Rody, A.K., Maarouf, H.: Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. J. Symbolic Computation. 31, 631–649 (2001)

3. Gao, X.S., Chou, S.C.: Solving parametric algebraic systems. In: Proceedings ISSAC 1992, Berkeley, July 27-29, pp. 335–341. Association for Computing Machinery, New York (1992)
4. Kalbrener, M.: A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. J. Symbolic Computation 15, 143–167 (1993)
5. Lazard, D.: A new method for solving algebraic systems of positive demension. Discrete Appl. Math. 33, 147–160 (1991)
6. Moreno, M.M.: On triangular decompositions of algebraic varieties. In: MEGA 2000, Bath, England (presented, 2000)
7. Pan, V.Y.: Sturctured Matrices and Polynomials. Birkhäuser, Boston (2001)
8. Wang, D.K., Zhang, Y.: An algorithm for decomposing a polynomial system into normal ascending sets. Science in China, Series A: Mathematics 50(10), 1441–1450 (2007)
9. Wang, D.M.: Some Notes on Algebraic Method for Geometric Theorem Proving
10. Wang, D.M.: Elimination Method. Springer, New York (2001)
11. Wu, W.T.: Basic principles of mechanical theorem proving in elementray geometries. J. Syst. Sci. Math. Sci. 4, 20–235 (1984)
12. Yang, L., Zhang, J.Z.: Search dependency between algebraic equations: An algorithm applied to automated reasoning. Technical Report ICTP/91/6, International Center For Theoretical Physics, Trieste (1991)