数理解析研究所講究録 第2104巻 2019年 60-64

準素成分から根基でないイデアルの三角形集合の復元とそのビット長の評価

Reconstruction of a non-radical triangular set from its primary components and its bit-size estimate

ダハン　グザビエ*
お茶の水女子大学、プロジェクト教育研究院
Xavier Dahan
Ochanomizu University, Graduate School of General Educational Research

Abstract

根基でないイデアルの三角形集合は、根基イデアル三角形集合に比べてよく理解されていない。Wu-Ritt 氏による三角形分解法においては、一般化された中国剰余定理により三角形集合を分解、また復元するのは大事である。本研究は根基でない場合での復元アルゴリズムを扱う。最近対提案された三角形集合上の係数がある多項式の最大公約因子を使うことにより、このアルゴリズムを導入できることになった。応用として、復元の過程による係数の成長を評価する。

Abstract

Triangular sets that generate a non-radical ideal are far less understood then those that generate a radical one. In the realm of "triangular-decomposition", decomposing and reconstructing such triangular sets is important, based on generalized versions of the Chinese remaindering theorem. In this work we address the reconstruction in the non-radical case. It relies on the recently proposed computation of gcd of univariate polynomials over a non-radical triangular set. As an application, we estimate the coefficient growth entailed in this reconstruction process.

Background A triangular set in this work refers to a zero-dimensional lexicographic Gröbner basis which has a purely triangular shape, as follows:

$$T \left| \begin{array}{l} T_n(X_1, X_2, \cdots, X_{n-1}, X_n) = X_n^{d_n} + \cdots \\ T_{n-1}(X_1, \ldots, X_{n-1}) = X_{n-1}^{d_{n-1}} + \cdots \\ \quad \vdots \\ T_1(X_1) = X_1^{d_1} + \cdots \end{array} \right.$$

If we assume that such a triangular set generates a radical ideal, then its primary components $\mathfrak{q}_i$ are maximal ideals. Therefore, the quotient ring $k[X_1, \ldots, X_n]/\mathfrak{q}_i$ is a field, more precisely it encodes a tower of fields extensions. It is thus possible to apply standard algorithms over fields such as gcd. Now for polynomials having coefficients over a triangular set that generates a radical non-maximal ideal, it is not obvious anymore since there are zero-divisors. The work of Kalkbrener [8] and the D5 principle [7] have shown however how to circumvent this problem. The issue occurring for the division operation, it splits

*dahan.xavier@ocha.ac.jp, xdahan@gmail.com

the underlying triangular set into two ones: in one branch the division is possible, in the other one not. This paradigm is the core of gcd-based view on the triangular decomposition method.

But when the triangular set is not radical, the above description fails apart since the primary components themselves are not all maximal ideals, and elements are not necessarily invertible. The article [5] proves that a kind of gcd notion exists, and highlights a strategy to compute it. The crux is that there is not one gcd but a chain of. A complete algorithm to compute this gcd-chain is still challenging, except in one case described below.

Invertibility in a special case Let $(T_1, \ldots, T_n)$ and let $T = (T_1, \ldots, T_{n-1})$ be a triangular set a be a univariate polynomial in $R[X_n]$ where $R = k[X_1, \ldots, X_{n-1}]/\langle T\rangle$. Let $\mathfrak{p} := \sqrt{\langle T\rangle}$ be the radical of $\langle T\rangle$; This is a maximal ideal.

(H) Assume that $\gcd(a \bmod \mathfrak{p}, T_n \bmod \mathfrak{p}) = 1$ over the field $k[X_1, \ldots, X_{n-1}]/\mathfrak{p}$.

Then the last non-nilpotent subresultant of a and T_n computed in $R[X_n]$ is invertible in R. (In the terminology introduced in [5], the gcd chain has only one block, which is moreover equal to 1). It follows that a is invertible in $R[X_n]/\langle T\rangle = k[X_1, \ldots, X_n]/\langle T_1, \ldots, T_n\rangle$.

Application to Chinese remaindering theorem This simple observation has the implication that undergoing the reconstruction part of the Chinese Algorithm theorem is possible even over a primary triangular set. Additionally, the algorithm works similarly to the one for radical triangular sets [2], as shown below in Algo. 1.

Algorithm 1: Recombination polynomials by the Chinese remaindering theorem

Input: Primary triangular set $\mathbf{t} = (t_1, \ldots, t_n)$ (let $R := (k[X_1, \ldots, X_n]/\langle \mathbf{t}\rangle)$)
family of polynomials $\{a_i\}_{i=1,\ldots,s}$ of $R[y]$, such that $\langle a_1, \ldots, a_s\rangle = \langle 1\rangle$ in $R[y]$
Output: $\{\widetilde{e_i}\}_{i=1,\ldots,s}$ such that $\sum_i \widetilde{e_i} a_i \equiv 1 \bmod \langle \mathbf{t}\rangle$ and $\deg_y(\widetilde{e_i}) < \sum_{j\neq i} \deg_y(a_j)$

1 Compute the product $A \equiv \prod_{i=1}^{s} a_i \bmod \langle \mathbf{t}\rangle$
2 **for** $i = 1, \ldots, s$ **do**
3 $\quad A_i := A/a_i \bmod \langle \mathbf{t}\rangle$
4 $\quad$ Compute the extended subresultant sequence $\{A_i, a_i, S_{r_2}(A_i, a_i), \ldots, S_{r_j}(A_i, a_i), \ldots, S_0\}$
$\quad\quad \{1, 0, u_{r_2}, \ldots, u_{r_j} \ldots, u_0\}$ and $\{0, 1, v_{r_2}, \ldots, v_{r_j}, \ldots, v_0\}$ // $\deg_y(S_{r_j}) = r_j$,
$\quad\quad u_{r_j} A_i + v_{r_j} a_i = S_{r_j}$
5 $\quad t_0 \leftarrow S_0^{-1} \bmod \langle \mathbf{t}\rangle$
6 $\quad \widetilde{e_i} \leftarrow v_0 \cdot t_0 \bmod \langle \mathbf{t}\rangle$
7 **return** $\{\widetilde{e_1}, \ldots, \widetilde{e_s}\}$

Comments The novelty is that the subresultant sequence of A_i and a_i can be computed in $R = k[X_1, \ldots, X_n]/\langle \mathbf{t}\rangle$ using the classical PRS of Brown [1]: the division made over R are always possible. This is because $\langle \mathbf{t}\rangle$ is primary, hence indecomposable.

Next, that $S_0 \in R$ is invertible (line 5). This comes from the fact that A_i and a_i are coprime modulo the maximal ideal $\sqrt{\langle \mathbf{t}\rangle}$. The precise algorithm to compute this inverse is similar to the one that works for triangular sets that generate a maximal ideal (see *e.g.* [9]).

Last, the fact that $\sum_{i=1}^{s} \widetilde{e_i} a_i \equiv 1 \bmod \langle \mathbf{t}\rangle$ is an easy and standard consequence of the algorithm.

Note that the algorithm above is a plain one. There are faster versions[1)] based on so-called subproduct

[1)] In any cases, the complexity of the algorithm ultimately solely depends on which version of the pseudo Euclidean

tree techniques [10, Chap. 10.3].

From the computation of the recombination polynomials output by Algo. 1 we deduce the recombination part of the CRT as follows, We use the notation of Algo. 1.

- Consider some target modular values $f_i \in (R[y]/\langle a_i \rangle)[z_1, \ldots, z_\ell]$
- Compute $f := \sum_{i=1}^{s} \widetilde{e_i} a_i f_i \bmod \langle \mathbf{t} \rangle$.

  (Then we have: $f \in (R[y]/\langle A \rangle)[z_1, \ldots, z_\ell]$ where $A = \prod_{i=1}^{s} a_i$ and $f \equiv f_i \bmod \langle \mathbf{t} \cup \{a_i\} \rangle$)

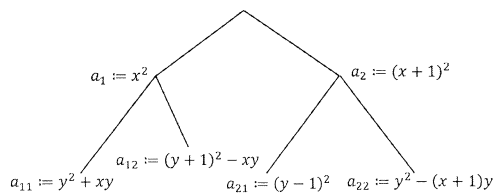
Reconstruction from primary components Next instead of polynomials a_i in the input of Algo. 1, assume that they are "pairwise coprime" triangular sets, how to adapt the algorithm ?

First the input primary triangular sets must be arranged into a natural tree data structure. Second, Algo. 1 is called recursively from the root of the tree up to the parent of the leaves, for each branch. The following example illustrates how the algorithm work:

Example Consider the four primary triangular sets $\mathbf{t}^{11}, \mathbf{t}^{12}, \mathbf{t}^{21}, \mathbf{t}^{22}$:

$$\begin{cases} t_2^{11}(x,y) = y^2 + xy \\ t_1^{11}(x) = x^2 \end{cases} \quad \begin{cases} t_2^{12}(x,y) = (y+1)^2 - xy \\ t_1^{12}(x) = x^2 \end{cases} \quad \begin{cases} t_2^{21}(x,y) = (y-1)^2 \\ t_1^{21}(x) = (x+1)^2 \end{cases} \quad \begin{cases} t_2^{22}(x,y) = y^2 - (x+1)y \\ t_1^{22}(x) = (x+1)^2 \end{cases}$$

These four triangular sets are arranged in the following tree. The number of leaves is equal to the number of primary triangular sets. To alleviate notations, we write: $a_1 := t_1^{11} = t_1^{12} = x^2$, $a_2 = t_1^{21} = t_1^{22} = (x+1)^2$ and $a_{ij} = t_2^{ij}$ for $i = 1, 2$, $j = 1, 2$.



- Problem: Define $R_{ij} := k[x,y]/\langle \mathbf{t}^{ij} \rangle$. Given moduli $f_{ij} \in R_{ij}[z_1, \ldots, z_\ell]$ compute a polynomial $f \in k[x,y][z_1, \ldots, z_\ell]$ such that $f \equiv f_{ij} \bmod \langle \mathbf{t}^{ij} \rangle$, with the degree constraints: $\deg_x(f) < \sum_i \deg_x(a_i)$ and $\deg_y(f) < \max_i(\sum_j \deg_y(a_{ij}))$.

Algo.1 applied to a_1, a_2, then to a_{11}, a_{12} modulo a_1 and to a_{21}, a_{22} modulo a_2 yields:

$$\begin{array}{lcll} \widetilde{e_1} a_1 + \widetilde{e_2} a_2 = 1 & \longrightarrow & \widetilde{e_1} := 3 + 2x, & \widetilde{e_2} := 1 - 2x \\ \widetilde{e_{11}} a_{11} + \widetilde{e_{12}} a_{12} \equiv 1 \bmod \langle a_1 \rangle & \longrightarrow & \widetilde{e_{11}} := 2xy + 2y + 3, & \widetilde{e_{12}} := -2xy - 2y + 1 \\ \widetilde{e_{21}} a_{21} + \widetilde{e_{22}} a_{22} \equiv 1 \bmod \langle a_2 \rangle & \longrightarrow & \widetilde{e_{21}} := 3xy + 5y + 1, & \widetilde{e_{22}} := (-3y+4)x - 5y + 7 \end{array}$$

- Answer: $f \equiv \sum_i a_i \widetilde{e_i} (\sum_j a_{ij} \widetilde{e_{ij}} f_{ij} \bmod \langle a_{i1} a_{i2} \rangle) \bmod \langle a_1 a_2 \rangle$.

This example in the case of triangular sets of two variables generalizes by considering trees of depth larger than two.

Coefficients growth When the input triangular sets are maximal ideals, and the base field is algebraically closed, then these triangular sets are just "ideal of points" like $\langle x-1, y-2 \rangle$. The problem is to

---

division is used. It is well-known that the half-gcd [10, Chap. 11] has a softly linear asymptotic complexity, against a quadratic one for the standard Euclidean algorithm.

interpolate points. The estimation of the growth of coefficients through explicit interpolation formula has been treated in [3]. See [4] for a short survey. The situation is more complicated for primary triangular sets with respect to two points:

First there is no explicit interpolation formula. Algorithm 1 computes gcd cofactors (written v_0 at Line 6) which are more difficult to estimate. The cost of normal forms (the mod used at various places) makes the estimates more complicated.

The second point is the the lack of a precise "Arithmetic Bézout Theorem" in the case of primary triangular sets. This tool is crucial to deduce bit-size from any input polynomial systems. In the realm of Diophantine Geometry where height theory comes from, this has not been treated; As far as I know, at best algebraic cycles of projective varieties have been addressed. Even without this major tool, the bounds obtained are similar to the ones computed for the radical case. This provides a rather good heuristic to believe that comparable "universal" (independent of the describing polynomial system) bounds should hold.

Theorem.[6] *Let* $\{\mathbf{t}^{(\alpha)}\}_{\alpha\in V(\mathbf{T})} \subset \bar{\mathbb{Q}}[X_1,\ldots,X_n]$ *be a finite family of pairwise distinct primary triangular sets over* $\bar{\mathbb{Q}}$*. The unique zero in* $\bar{\mathbb{Q}}^n$ *of the system* $\mathbf{t}^{(\alpha)}$ *is denoted* α*.*

Assume that the lexicographic Gröbner basis of the ideal $I = \prod_\alpha \langle \mathbf{t}^{(\alpha)}\rangle$ *is a triangular* $\mathbf{T}$ *set defined over* $\mathbb{Q}$*. The zeroes* $V(\mathbf{T})$ *of the system* $\mathbf{T}$ *are the* α*'s.*

The reconstruction algorithm described above of $\mathbf{T}$ *from the input* $\{\mathbf{t}^{(\alpha)}\}_{\alpha\in V(T)}$ *induces a growth of coefficients of at most:*

$$h(T_n) \le n\,D\,H(\mathbf{T}) + \tilde{O}(\ n\,L(\mathbf{T})\,D^2\,\mu(\mathbf{T})\ ), \quad \textit{where,}$$

- T_n *is the* n*-th polynomial in the triangular set* $\mathbf{T}$*.*
- *The maximal bit-size of the coefficients in* $\mathbf{t}^{(\alpha)}$ *is denoted* $H(\alpha)$*.*
- *sum and max over the zeroes* α *of* $\mathbf{T}$*:* $H(\mathbf{T}) = \sum_\alpha H(\alpha)$ *and* $\mathsf{L}(\mathbf{T}) := \max_\alpha H(\alpha)$
- $D = d_1 + d_2 + \cdots + d_n$, $\deg_{X_i}(T_i) = d_i$*.*
- $\mu(\mathbf{T}) := \max_\alpha \mu(\alpha)$ *is the maximal multiplicity of the roots in* $\bar{\mathbb{Q}}^n$ *of the system* $\mathbf{T}$*.*

We remark that in the case of a radical ideal, we have $\mu(\mathbf{T}) = 1$, $\mathsf{L}(\mathbf{T}) \ll H(\mathbf{T})$, and the bounds are thus similar, with a small overhead of $\mathsf{L}(\mathbf{T})$, to those obtained in [3] that focused on the radical case only.

References

[1] WS Brown. The subresultant prs algorithm. *ACM Transactions on Mathematical Software (TOMS)*, 4(3):237–249, 1978.

[2] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, 2005.

[3] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC 2004*, pages 103–110. ACM Press, 2004.

[4] Xavier Dahan. On bit-size estimates of triangular systems (数式処理研究の新たな発展–rims 共同研究報告集). 数理解析研究所講究録, 1759:26–42, 2011.

[5] Xavier Dahan. Gcd modulo a primary triangular set of dimension zero. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 109–116, New York, NY, USA, 2017. ACM.

[6] Xavier Dahan. On the bit-size of non-radical triangular sets. In Johannes Blömer, Ilias S. Kotsireas, Temur Kutsia, and Dimitris E. Simos, editors, *Mathematical Aspects of Computer and Information Sciences: 7th International Conference, MACIS 2017, Vienna, Austria, November 15-17, 2017, Proceedings*, pages 264–269, Cham, 2017. Springer International Publishing.

[7] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *EUROCAL '85: Research Contributions from the European Conference on Computer Algebra-Volume 2*, pages 289–290, London, UK, 1985. Springer-Verlag.

[8] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symbolic Comput.*, 15(2):143–167, 1993.

[9] L. Langemyr. Algorithms for computing in algebraic extension. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry, Proceedings of MEGA'90*, volume 141, pages 235–248. Birkhäuser, 1990.

[10] J. von zur Gathen and J. Gerhard. *Modern computer algebra.* Cambridge University Press, New York, NY, USA, 2003. Second Edition.