Polynomially Recursive Relations on Power-Series Roots

Kosaku Nagasaka
Kobe University
nagasaka@main.h.kobe-u.ac.jp

ABSTRACT
In the combinatorics and probability theory, there are two concepts, *differentiably finite* and *polynomially recursive* and they are related each other. Using those well known facts, we give an algorithm to construct recursive formulas and calculate the power-series roots of bivariate polynomials. The computational cost of the algorithm is linear w.r.t. the given cutoff degree. We also show some linear dependent relations on the coefficients of the power-series roots. By this property, we prove completeness of a bivariate polynomial factorization algorithm using zero-sum relations which is a base algorithm of a recent approximate factorization method.

1. INTRODUCTION
Stanley wrote a book about enumerative combinatorics [7], in which there are the following concepts: *differentiably finite* and *polynomially recursive*. We note that we use their abbreviations, D-finite and P-recursive, respectively, and our discussion is over $\mathbb{C}[u]$ and $\mathbb{C}[[u]]$ which are a polynomial ring in u over $\mathbb{C}$ and a formal power-series ring in u over $\mathbb{C}$, the complex field, respectively.

Definition 1 (D-finite [7]). *For any $\varphi(u) \in \mathbb{C}[[u]]$, we say $\varphi(u)$ is D-finite power-series if there exist polynomials $p_0(u)$, …,$p_d(u) \in \mathbb{C}[u]$ satisfying*

$$\sum_{i=0}^{d} p_i(u)\varphi(u)^{(i)} = 0, \tag{1.1}$$

where $p_d(u) \neq 0$ and $\varphi(u)^{(i)}$ denotes i-th partial differential $\partial^i \varphi(u)/\partial u^i \in \mathbb{C}[[u]]$, of $\varphi(u)$ w.r.t. u.

Definition 2 (P-recursive [7]). *A function $c : \mathbb{N} \to \mathbb{C}$ is called P-recursive if for all $k \in \mathbb{N}$, there exist polynomials P_0, …, $P_b \in \mathbb{C}[k]$ satisfying*

$$P_b(k)c(k+b) + P_{b-1}(k)c(k+b-1) + \cdots + P_0(k)c(k) = 0, \tag{1.2}$$

where $P_b \neq 0$.

The important fact is that algebraic functions are D-finite and we can see several examples of D-finite power-series and P-recursive functions in the book [7]. Benali and Jean-Paul [1] studied some algebraic properties of D-finite sequences satisfying additional conditions. Moreover, Lipshitz [2] studied the generalized multivariate D-finite power-series and P-recursive functions. However, we note that there are only few papers in the algebra while there are several papers about D-finite power-series in the combinatorics and probability theory. We try to use those concepts for symbolic algebraic computations in this paper.

P-recursive functions are similar to linear recurrence functions. We can compute power-series by using P-recursiveness as we can use some linear recurrence relations to compute linear quantities. Our aim is to show such an algorithm. Generally, computing the power-series roots of polynomials is done by the symbolic Newton's method, the generalized Hensel construction or their variants. Those methods have a characteristic that computational costs are non-linear w.r.t. the given cutoff degree bound. On the other hand, a computational cost is linear w.r.t. the given cutoff degree bound if we use P-recursiveness of D-finite power-series to compute the power-series roots.

In this paper, we give degree bounds of polynomials $p_0(u)$, …, $p_d(u)$ in the relation (1.1), and by which we give an algorithm to compute the power-series roots of bivariate polynomials. These discussions also give us an additional property: linear dependent relations on coefficients of the power-series roots of bivariate polynomials. Using these properties, we also give a proof of completeness of a bivariate factorization algorithm [5, 4] which are the exact version of approximate factorization [3] and has not been proved for any polynomial cutoff degree bounds.

This paper is formed as follows. We review some basic properties of D-finite power-series and P-recursive sequences in the section **2**. We prepare some degree bounds in the section **3** to show an expansion algorithm in the section **4**. In the section **5**, as an application of former sections, we give a proof of completeness of the bivariate factorization algorithm [5, 4]. Finally, we give a conclusion in the section **6**.

In this paper, we denote the quotient field of $\mathbb{C}[u]$ by $\mathbb{C}(u)$. $F(u,x) \in \mathbb{C}[u,x]$ is the given polynomial in u and the main variable x and put

$$F(u,x) = f_n x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0.$$

And we suppose that $F(u,x)$ is square-free w.r.t. x and put $n = \deg_x(F)$ and $e = \deg_u(F)$.

2. D-FINITE AND P-RECURSIVE

In this section, we review some useful properties of D-finite power-series and D-recursive functions, briefly. We recommend to read the Stanley's book [7] if you are interested in the details, especially for their proofs.

PROPOSITION 1 (PROPOSITION 6.4.3 IN [7]). *Let $\varphi(u)$ be a power-series in u and put $\varphi(u) = \sum_{k\geq 0} c(k)u^k \in \mathbb{C}[[u]]$. Then, $\varphi(u)$ is D-finite if and only if $c(k)$ is P-recursive.*

THEOREM 1 (THEOREM 6.4.6 IN [7]). *For any power-series roots $\varphi(u) \in \mathbb{C}[[u]]$ of $F(u,x)$ w.r.t. x, $\varphi(u)$ is D-finite and $\varphi(u)$ satisfies the relation (1.1) with $d = n$.*

The proposition 1 and the theorem 1 mean that we can compute the coefficients of the power-series roots of $F(u,x)$ if we construct a corresponding P-recursive function $c(k)$. The proofs of the above can be found in the book [7] (The latter proof is done by treating $\mathbb{C}[u,x]/(F(u,x))$ as a vector space whose dimension is equal to or less than n).

3. DEGREE BOUNDS

We only consider the power-series roots of the given polynomial $F(u,x)$ as D-finite power-series. At first, we show degree bounds of polynomials $p_0(u), \ldots, p_d(u)$ satisfying the relation (1.1) for the power-series roots of $F(u,x)$. Since, in the book [7], the theorem 1 is proved by using the total differential of $F(u,\varphi(u))$ and representing $\varphi^{(1)}$ as an element in $\mathbb{C}(u,\varphi)$, so we treat $\varphi^{(1)}$ as an element in $\mathbb{C}(u,\varphi)$, differentiate it recursively and give degree bounds of polynomials $p_0(u), \ldots, p_d(u)$.

The total differential of $F(u,\varphi(u))$ is given as follows.

$$0 = \frac{d}{du}F(u,\varphi) = \left.\frac{\partial F(u,x)}{\partial u}\right|_{x=\varphi} + \varphi^{(1)} \left.\frac{\partial F(u,x)}{\partial x}\right|_{x=\varphi}, \tag{3.1}$$

where $expr(x)|_{x=\varphi}$ denotes substituting φ for x. Since the given polynomial $F(u,x)$ is square-free w.r.t. x, we have $\partial F(u,x)/\partial x|_{x=\varphi} \neq 0$. Hence, the following relation follows from the relation (3.1).

$$\varphi^{(1)} = -\frac{\left.\frac{\partial F(u,x)}{\partial u}\right|_{x=\varphi}}{\left.\frac{\partial F(u,x)}{\partial x}\right|_{x=\varphi}} \in \mathbb{C}(u,\varphi). \tag{3.2}$$

This means that $\varphi^{(1)}$ is differentiable hence we have $\varphi^{(i)}$ $(i = 0,1,\ldots,n) \in \mathbb{C}(u,\varphi)$. In the rest of this paper, we use the following notations for these partial differentials for simplicity.

$$N_1(u,\varphi) = -\left.\frac{\partial F(u,x)}{\partial u}\right|_{x=\varphi}, \quad D(u,\varphi) = \left.\frac{\partial F(u,x)}{\partial x}\right|_{x=\varphi}. \tag{3.3}$$

LEMMA 1. *$\varphi^{(i)}(u)$ $(i = 1,\ldots,n)$ can be represented as*

$$\varphi^{(i)} = N_i(u,\varphi)/D(u,\varphi)^{2i-1}, \tag{3.4}$$

where $D(u,\varphi)$, $N_i(u,\varphi)$ $(i = 1,\ldots,n) \in \mathbb{C}[u,\varphi]$ and these polynomials satisfy the following degree bounds.

$$\begin{array}{ll} deg_\varphi(N_i) \leq (2i-1)n - 2(i-1), & deg_\varphi(D) \leq n-1, \\ deg_u(N_i) \leq (2i-1)e - i, & deg_u(D) \leq e. \end{array}$$

PROOF. The degree bounds of D follow from the definition (3.3) hence it is valid. Therefore, we prove the relation (3.4) and the degree bounds of N_i by the mathematical induction.

For $i = 1$, the lemma is valid by the definition and the assumption. Suppose that the lemma is valid for $i = 1,\ldots,\kappa$. For $i = \kappa+1$, by differentiating $\varphi^{(\kappa)}$, we have

$$\varphi^{(\kappa+1)} = \frac{N_\kappa^{(1)}D - (2\kappa-1)N_\kappa D^{(1)}}{D^{2\kappa}}. \tag{3.5}$$

Here, $N_\kappa^{(1)}$ and $D^{(1)}$ are polynomials in u, φ and $\varphi^{(1)}$. By substituting the relations (3.2) and (3.3) for $\varphi^{(1)}$ in $N_\kappa^{(1)}$ and $D^{(1)}$, we have $N_\kappa^{(1)}$, $D^{(1)} \in \mathbb{C}(u,\varphi)$.

Since any denominators of rational expressions in $N_\kappa^{(1)}$ and $D^{(1)}$ is D or a factor of D, we can reduce denominators of the numerator of the expression (3.5) to the common denominator D and let the numerator of the numerator be $N_{\kappa+1}$ which is formed as

$$\begin{aligned} N_{\kappa+1} = {} & (D\tfrac{\partial N_\kappa(u,x)}{\partial u}|_{x=\varphi} + N_1\tfrac{\partial N_\kappa(u,x)}{\partial x}|_{x=\varphi})D \\ & - (2\kappa-1)N_\kappa(D\tfrac{\partial D(u,x)}{\partial u}|_{x=\varphi} + N_1\tfrac{\partial D(u,x)}{\partial x}|_{x=\varphi}). \end{aligned}$$

Hence, the expression (3.5) can be written as

$$\varphi^{(\kappa+1)} = \frac{N_{\kappa+1}}{D^{2\kappa+1}} = \frac{N_{\kappa+1}}{D^{2(\kappa+1)-1}}, \quad N_{\kappa+1} \in \mathbb{C}[u,\varphi].$$

Degree bounds of $N_{\kappa+1}$ are bounded as follows.

$$\begin{array}{rcl} \deg_\varphi(N_{\kappa+1}) & \leq & \max\{\deg_\varphi(N_\kappa^{(1)}) + \deg_\varphi(D), \\ & & \quad \deg_\varphi(N_\kappa) + \deg_\varphi(D^{(1)})\} \\ & = & \max\{\deg_\varphi(N_\kappa) + 2\deg_\varphi(D), \\ & & \quad 2\deg_\varphi(D) + \deg_\varphi(N_\kappa)\} \\ & = & \deg_\varphi(N_\kappa) + 2\deg_\varphi(D) \\ & \leq & (2\kappa-1)n - 2(\kappa-1) + 2(n-1) \\ & = & (2(\kappa+1)-1)n - 2((\kappa+1)-1), \end{array}$$

$$\begin{array}{rcl} \deg_u(N_{\kappa+1}) & \leq & \max\{\deg_u(N_\kappa^{(1)}) + \deg_u(D), \\ & & \quad \deg_u(N_\kappa) + \deg_u(D^{(1)})\} \\ & = & \max\{\deg_u(N_\kappa) + 2\deg_u(D) - 1, \\ & & \quad 2\deg_u(D) - 1 + \deg_u(N_\kappa)\} \\ & = & \deg_u(N_\kappa) + 2\deg_u(D) - 1 \\ & \leq & (2\kappa-1)e - \kappa + 2e - 1 \\ & = & (2(\kappa+1)-1)e - (\kappa+1). \end{array}$$

Therefore, the lemma is proved by the mathematical induction. □

The polynomials $p_0(u), \ldots, p_n(u)$ that are considered in this section satisfy the following equation by the definition 1 and the theorem 1.

$$\begin{aligned} p_n(u)\varphi(u)^{(n)} + p_{n-1}(u)\varphi(u)^{(n-1)} + \cdots \\ + p_1(u)\varphi(u)^{(1)} + p_0(u)\varphi(u) = 0. \end{aligned} \tag{3.6}$$

By multiplicating the least common denominator of $\varphi(u)^{(i)}$ $(i=0,\ldots,n)$, we can rewrite the equation (3.6) as the following linear equation w.r.t. unknown coefficients of polynomials $p_0(u)$, …, $p_n(u)$.

$$\begin{aligned} p_n(u)\phi_n(u,\varphi)+p_{n-1}(u)\phi_{n-1}(u,\varphi)+\cdots \\ +p_1(u)\phi_1(u,\varphi)+p_0(u)\phi_0(u,\varphi)=0, \end{aligned} \tag{3.7}$$

where $\phi_i(u,\varphi)$ $(i=0,\ldots,n)\in\mathbb{C}[u,\varphi]$.

Lemma 2. *$\phi_0,\ldots,\phi_n$ satisfy the following degree bounds.*

$$deg_\varphi(\phi_i)\le 2n^2-3n+2,$$
$$deg_u(\phi_i)\le(2n-1)e-i.$$

Proof. Since, by the lemma 1, each least common denominators of $\varphi(u)^{(i)}$ is $D(u,\varphi)^{2n-1}$ or its factor, we can rewrite ϕ_i as follows.

$$\phi_i=\begin{cases} D(u,\varphi)^{2n-1}\varphi & (i=0),\\ D(u,\varphi)^{2(n-i)}N_i(u,\varphi) & (i=1,\ldots,n).\end{cases}$$

Therefore, the lemma is proved by the lemma 1. □

We note that we have to discuss all the quantities over $\mathbb{C}[u,\varphi]/(F(u,\varphi))$ to treat the power-series roots of $F(u,\varphi)$ as D-finite power-series. We rewrite the system (3.7) as follows.

$$\begin{aligned} p_n(u)R_n(u,\varphi)+p_{n-1}(u)R_{n-1}(u,\varphi)+\cdots \\ +p_1(u)R_1(u,\varphi)+p_0(u)R_0(u,\varphi)=0, \end{aligned} \tag{3.8}$$

where $R_i\in\mathbb{C}[u,\varphi]$ $(i=0,\ldots,n)$ are residuals of ϕ_i by $F(u,\varphi)$ w.r.t. φ.

Lemma 3. *We have*

$$\begin{aligned} deg_\varphi(R_i)&\le n-1\\ deg_u(R_i)&\le 2(n^2-n+1)e-i \end{aligned} \quad (i=0,\ldots,n).$$

Proof. As in the proof of the lemma 2, we can rewrite ϕ_i as follows.

$$\phi_i=\begin{cases} D(u,\varphi)^{2n-1}\varphi & (i=0),\\ D(u,\varphi)^{2(n-i)}N_i(u,\varphi) & (i=1,\ldots,n).\end{cases}$$

For each divisions by $F(u,\varphi)$, a degree of a residual is increased by e. The lemma follows from a summation of all the increase degrees. □

Theorem 2. *The polynomials $p_0,\ldots,p_n$ satisfy the following degree bounds.*

$$deg_u(p_i)\le d_i(e),$$

where

$$d_i(e)=\frac{1}{2}(4en^3-(4e+1)n^2+(4e-1)n-2)+i.$$

Proof. The linear equation (3.8) must have non-trivial solutions by the theorem 1. Therefore, the theorem follows from letting the degrees of p_i such that the number of unknowns is larger than the number of equations: put $\deg_u(p_0)=k$, $\deg_u(p_1)=k+1$, $\deg_u(p_2)=k+2$, …, $\deg_u(p_{n-1})=k+n-1$ and $\deg_u(p_n)=k+n$ such that each products $p_i(u)R_i(u,\varphi)$ has the same degree. The system (3.8) has $(n+1)(k+1)+n(n+1)/2$ unknowns and $n(2(n^2-n+1)e+k+1)$ equations, hence the theorem is proved by solving the following inequality w.r.t. k.

$$n(2(n^2-n+1)e+k+1)\le(n+1)(k+1)+n(n+1)/2.$$

□

Since the degree bounds d_i $(i=0,\ldots,n)$ are sufficient degree bounds, actual degrees of polynomials p_0, …, p_n are equal to or smaller than these bounds as in the example in the next section. We note that these bounds d_i can be replaced with actual degrees of p_i, though all the discussions in the rest of this paper are based on these sufficient degree bounds d_i.

4. RECURSIVE ALGORITHM

A formula to compute coefficients $c(k)$ can be derived from the relation (1.2) if we have polynomials $P_i(k)$ $(i=0,\ldots,b)$. However, we do not know those polynomials while we obtained the degree bounds of polynomials $p_0,\ldots,p_n$ in the previous section. Therefore, we calculate polynomials p_0, …, p_n by solving the system (3.8), and derive a formula to compute coefficients of the power-series roots of $F(u,x)$ by the relation (1.1). To do this, we need to 1) solve the system (3.8), 2) construct a recursive formula to compute coefficients, and 3) calculate an initial power-series root up to enough degree. We have several suitable methods to do 1) and 3). Hence we derive the recursive formula in this section.

Lemma 4. *Suppose that the power-series root φ satisfying the relation (1.1) is already calculated up to degree $k-1$ $(\ge n-1)$ w.r.t. u and put $\varphi=\sum_{j=0}^{k}c_ju^j$ and $p_i=\sum_{j=0}^{d_i}p_{i,j}u^j$. Then, c_k can be computed as the following formula provided $p_{n,0}\ne 0$.*

$$c_k=-\sum_{t=0}^{n}\sum_{i+j=k-t,\ i,j\ge 0,\ j\ne k}\frac{j!(k-n)!}{(j-n+t)!k!}\frac{p_{n-t,i}\,c_j}{p_{n,0}}.$$

Proof. Since the power-series root φ is D-finite, it satisfies the relation (1.1). By extracting coefficients of terms whose degree is $k-n$ w.r.t. u from the expression (1.1), we have

$$\sum_{t=0}^{n}\sum_{i+j=k-t,\ i,j\ge 0}\frac{j!}{(j-n+t)!}\,p_{n-t,i}\,c_j=0.$$

Solving the above equation w.r.t. c_k gives us the following solution.

$$c_k=-\frac{\sum_{t=0}^{n}\sum_{i+j=k-t,\ i,j\ge 0,\ j\ne k}\frac{j!}{(j-n+t)!}\,p_{n-t,i}\,c_j}{\frac{k!}{k-n!}p_{n,0}}.$$

The lemma follows from simplifying the above solution. □

Corollary 1. *If the power-series root φ is calculated up to degree $k-1$ $(\ge d_n-1)$ w.r.t. u, and $p_{n,0}\ne 0$, then we* *have the following formula to compute* c_k*.*

$$c_k = -\frac{\left(\begin{array}{r}\sum_{t=1}^{n}\sum_{i=0}^{d_{n-t}} \frac{(k-i-t)!}{(k-i-n)!}\, p_{n-t,i}\, c_{k-t-i} \\ +\sum_{i=1}^{d_n} \frac{(k-i)!}{(k-i-n)!}\, p_{n,i}\, c_{k-i}\end{array}\right)}{\frac{k!}{(k-n)!}\, p_{n,0}}.$$

We note that the above formula is corresponding to a quotient of the expression in the definition 2 by $P_b(k)$, since the formula for c_k in the corollary 1 is a linear sum of products of functions in k and c_i $(i < k)$.

We simplify the formula in the corollary 1 as the following expression (4.1), and give an algorithm to compute the power-series roots.

$$\begin{array}{r} -\frac{1}{p_{n,0}}(\sum_{t=1}^{n}\sum_{i=0}^{d_{n-t}} \frac{(k-i-t)!}{(k-i-n)!}\frac{(k-n)!}{k!}\, p_{n-t,i}\, c_{k-t-i} \\ +\sum_{i=1}^{d_n} \frac{(k-i)!}{(k-i-n)!}\frac{(k-n)!}{k!}\, p_{n,i}\, c_{k-i}).\end{array} \tag{4.1}$$

Algorithm 1. (D-finite Power-Series Roots Expansion)

Input **:** a polynomial $F(u, x)$ and a cutoff degree E

Output **:** the power-series roots of $F(u, x)$ up to E

Step 1 Solve the system (3.8), calculate p_0, ..., p_n, and construct a recursive formula (4.1).

Step 2 Expand the power-series roots by the conventional methods up to actual degree $(d_n - 1)$ w.r.t. u.

Step 3 While $k \le E$, for each power-series roots, compute c_k by the formula (4.1) and let $k = k + 1$.

Step 4 Output the computed power-series roots and finish the algorithm.

We note that the computational cost of each coefficients is $O(en^5)$ complexity over $\mathbb{C}$ at worst. This cost does not depend on the cutoff degree or iteration index k while the conventional methods do. Hence the total computational cost of the step 3 is linear w.r.t. cutoff degree bound E.

COROLLARY 2. *The coefficient* c_k *of terms whose degree is* k $(\ge d_n)$*, of the power-series root* φ *of* $F(u, x)$*, does not depend on coefficients:* $c_0, c_1, \ldots, c_{k-d_n-1}$*.*

COROLLARY 3. *Each the power-series roots of* $F(u, x)$ *has the same P-recursive relation and can be computed by the same formula.*

In the Stanley's book [7], the given polynomial is supposed to be irreducible, and there is not any notes for reducible polynomials. If the given polynomial is reducible, the power-series roots of $F(u, x)$ also satisfy the all of the above expressions corresponding to polynomial factors of $F(u, x)$, which has the root.

Example 1. We give an example of the algorithm 1 for the simple bivariate polynomial $F(u, x) = x^2 - u - 1$.

As the initialization step, We compute degree bounds of polynomials p_0, p_1 and p_2. These bounds are $d_0 = 8$, $d_1 = 9$ and $d_2 = 10$ since we have $n = 2$ and $e = 1$.

In the step 1, we solve the system (3.8), calculate p_0, ..., p_n, and construct a recursive formula (4.1). At first, we differentiate the power-series root φ as follows.

$$\begin{array}{rcl}\varphi^{(1)} &=& \frac{1}{2\varphi}, \\ \varphi^{(2)} &=& -\frac{1}{4\varphi^3}.\end{array}$$

The least common denominator of the above derivatives is $4\varphi^3$. Hence we have the following system.

$$p_2R_2 + p_1R_1 + p_0R_0 = 0,$$
$$R_2 = -1,\ R_1 = 2 + 2u,\ R_2 = 4 + 8u + 4u^2.$$

According to the above system, we refine the degree bounds as $d_0 = 0$, $d_1 = 1$ and $d_2 = 2$, and we have the following solution (we note that there are other solutions).

$$p_0 = -1,\ p_1 = 3 + 3u,\ p_2 = 2 + 4u + 2u^2.$$

Therefore, we have the following recursive formula of c_k.

$$c_k = (\frac{5}{2k} - 2)c_{k-1} + (\frac{5}{2k} - 1)c_{k-2}.$$

In the step 2, we calculate the power-series roots $\varphi_1(u)$ and $\varphi_2(u)$ up to degree $d_n - 1 = 1$ as follows.

$$\begin{array}{rcl}\varphi_1 &=& -1 - 1/2u, \\ \varphi_2 &=& 1 + 1/2u.\end{array}$$

In the step 3, we compute coefficients of the power-series roots, using the above recursive formula.

$$\begin{array}{rcl}\varphi_1 &\to& \{-1, -1/2, 1/8, -1/16, 5/128, -7/256, \ldots\}, \\ \varphi_2 &\to& \{1, 1/2, -1/8, 1/16, -5/128, 7/256, \ldots\}.\end{array}$$

In this case, by solving the above recursive formula, we can derive the following general expression for all the coefficients.

$$c_k = \pm\frac{(-4)^{-k}\binom{2k}{k}}{1 - 2k}.$$

Example 2. We give another example of a recursive formula for the following bivariate polynomial which is reducible and monic w.r.t. x.

$$F(u, x) = x^5 - (u - 1)x^3 - (u + 1)x^2 + u^2 - 1.$$

We have the following recursive formula for $F(u, x)$.

$$\begin{array}{rcl}c_k &=& -\frac{1}{6k}c_{k-1} \\ && +\frac{-984+2170k-1853k^2+767k^3-154k^4+12k^5}{12k(24-50k+35k^2-10k^3+k^4)}c_{k-2} \\ && +\frac{35352-30990k+8994k^2-864k^3}{10368k(24-50k+35k^2-10k^3+k^4)}c_{k-3} \\ && +\frac{1276-607k+72k^2}{10368k(24-50k+35k^2-10k^3+k^4)}c_{k-4} \\ && +\frac{176-65k+6k^2}{10368k(24-50k+35k^2-10k^3+k^4)}c_{k-5}.\end{array}$$

Moreover, the above polynomial is factorized as $F(u, x) = (x^3 - u - 1)(x^2 - u + 1)$, and we have the following recursive formulas for $x^3 - u - 1$ and $x^2 - u + 1$, respectively.

$$\begin{array}{rcl}c_k &=& \frac{4-3k}{3k}c_{k-1} - \frac{1}{k(k-1)}c_{k-2} + \frac{10-3k}{3k(k^2-3k+2)}c_{k-3}, \\ c_k &=& \frac{2k-5}{2k}c_{k-1} + \frac{2k-5}{2k(k-1)}c_{k-2}.\end{array}$$

Remark 1. As in the previous and this sections, we can also calculate degree bounds of polynomials $P_0, \ldots, P_b$ and give an alternative algorithm to construct the recursive formula (4.1) directly, using the relation (1.2). However, this idea is not efficient because we have to solve a linear system over $\mathbb{C}$ even if the given polynomial is over $\mathbb{R}$ or $\mathbb{Q}$.

5. APPLICATION

As shown in the previous sections, considering the power-series roots as D-finite power-series gives us useful properties. Especially the corollaries 2 and 3 are useful for discussions about some theories using the power-series roots. In this section, we give such an application of the properties.

Recently, we have several approximate factorization algorithms, moreover, one algorithm using zero-sum relations is practical, which is studied by Sasaki [3]. One may think to use the zero-sum relations for exact ones. In fact, Sasaki and et al. [5, 6, 4] studied such an exact factorization algorithm. However, they have not done the proof of completeness of the main theorem which is a key of their algorithm. We give the proof by the properties of D-finite power-series in this section, even though a bivariate case only.

5.1 Known Theorem To Be Proved

We use the following notations.

- $\lceil F \rceil^a$ = the sum of terms of total-degrees $\le a$, of F;
- $\lfloor F \rfloor_b$ = the sum of terms of total-degrees $\ge b$, of F;
- $[F]_b^a = \lceil \lfloor F \rfloor_b \rceil^a$;

Let the truncated power-series roots of $F(u,x)$ w.r.t. the main variable x be $\varphi_1(u), \ldots, \varphi_n(u)$ and the cutoff degree be E, satisfying

$$F(u,x) \equiv f_n(u)(x - \varphi_1(u)) \cdots (x - \varphi_n(u)) \pmod{u^{E+1}}.$$

We suppose that $F(0,x)$ is square-free w.r.t. x and put $\deg_u(f_i) = e_i$ $(i = n, n-1, \ldots, 0)$ hence $\max\{e_n, \ldots, e_0\} = e = \deg_u(F)$.

Definition 3. *Let $\mathcal{H}$ be a two-dimensional convex hull such that points $(0,0)$, $(0,e_0)$, $(1,e_1)$, $\ldots$, (n,e_n) and $(n,0)$ are on $\mathcal{H}$. We define a number $\bar{e}$ such that a point $(n-1,\bar{e})$ is on the upper edges of $\mathcal{H}$.*

Theorem 3 (Theorem 1 in [3]). *Let the cutoff degree $E = n\bar{e}$ and $h_1(u), \ldots, h_m(u) \in \mathbb{C}[u]$, and suppose that we have the relations*

$$\begin{cases} \lceil f_n \cdot (\varphi_1^1 + \cdots + \varphi_m^1) \rceil^{n\bar{e}} = h_1(u), & \deg_u(h_1) \le 1\bar{e}, \\ \vdots & \vdots \\ \lceil f_n^m \cdot (\varphi_1^m + \cdots + \varphi_m^m) \rceil^{n\bar{e}} = h_m(u), & \deg_u(h_m) \le m\bar{e}. \end{cases}$$

Then, $P = f_n \cdot (x - \varphi_1) \cdots (x - \varphi_m)$ is a polynomial factor of $f_n F(u,x)$, and vice versa.

Although the theorem 3 has been proved and the approximate factorization method [3] is practical, we need to prove the following alternative theorem 4 to use the exact version of algorithm because the algorithm finds those linear dependent relations in the theorem 4 instead of the relations in the theorem 3, indirectly. The theorem 4 has not been proved for any polynomial cutoff degree E, even though the theorem has been proved [5] for infinite cutoff degree E by the Galois theory.

Theorem 4 (Theorem 5.3 in [5]). *For each j in $\{1, \ldots, n\}$, let $\lambda_j \in \mathbb{C}$, $h_j(u) \in \mathbb{C}[u]$ and $\deg_u(h_j) \le j\bar{e}$. Let the power-series roots $\varphi_1(u), \ldots, \varphi_n(u)$ of $F(u,x)$ satisfy (some of $\lambda_1, \ldots, \lambda_n$ may be 0)*

$$\begin{cases} \lambda_1 \lceil (f_n\varphi_1)^1 \rceil^E + \cdots + \lambda_n \lceil (f_n\varphi_n)^1 \rceil^E = h_1(u), \\ \lambda_1 \lceil (f_n\varphi_1)^2 \rceil^E + \cdots + \lambda_n \lceil (f_n\varphi_n)^2 \rceil^E = h_2(u), \\ \quad \cdot \quad \cdot \quad \cdot \qquad\qquad \cdots \\ \lambda_1 \lceil (f_n\varphi_1)^n \rceil^E + \cdots + \lambda_n \lceil (f_n\varphi_n)^n \rceil^E = h_n(u). \end{cases}$$

This system holds iff, among the elements of $\{\lambda_1, \ldots, \lambda_n\}$, all the elements that correspond to the roots of each irreducible factor in $\mathbb{C}[u,x]$, of $F(u,x)$ are the same.

The above theorem 4 for a polynomial cutoff degree E guarantees that the exact version of the zero-sum factorization algorithm can find correct factors. We give the proof for certain finite cutoff degrees in the next subsection.

Remark 2. Sasaki's approximate factorization method [3] uses some sub-routines to find linear dependent relations. We note that there might exist another way to prove completeness of the algorithm.

5.2 Proof Of The Theorem 4

The theorem 4 was proved by Sasaki et al. [5] with $E \to \infty$ using the Galois theory. Hence, in this section, we prove that a polynomial cutoff degree case can be treated as same as the case $E \to \infty$. We use the following useful lemmas (the latter lemma 6 is proved by Sasaki et al. [4]).

Lemma 5 (Newton's formula). *Let $S_i(X_1, \ldots, X_m)$ and $P_i(X_1, \ldots, X_m)$ $(i = 1, \ldots, m)$ be defined as follows (S_i is the elementary symmetric polynomial of degree i).*

$$\begin{cases} S_1(X_1, \ldots, X_m) = X_1 + X_2 + \cdots + X_m, \\ S_2(X_1, \ldots, X_m) = X_1X_2 + \cdots + X_1X_m \\ \qquad\qquad + \cdots + X_{m-1}X_m, \\ \vdots \\ S_m(X_1, \ldots, X_m) = X_1X_2 \cdots X_{m-1}X_m, \end{cases}$$

$$\begin{cases} P_1(X_1, \ldots, X_m) = X_1 + X_2 + \cdots + X_m, \\ P_2(X_1, \ldots, X_m) = X_1^2 + X_2^2 + \cdots + X_m^2, \\ \vdots \\ P_m(X_1, \ldots, X_m) = X_1^m + X_2^m + \cdots + X_m^m. \end{cases}$$

Then, for any integer i, $1 \le i \le m$, we have

$$P_i - P_{i-1}S_1 + P_{i-2}S_2 - \cdots + (-1)^{i-1}P_1S_{i-1} + (-1)^i iS_i = 0.$$

Lemma 6. *Assume that the polynomial factor $G(u,x)$ of $f_nF(u,x)$ is given as*

$$G(u,x) = f_n \cdot (x - \varphi_1) \cdots (x - \varphi_m).$$

Then, we have the following degree bounds for the sum of powers of roots.

$$deg_u(\,(f_n\varphi_1)^i + \cdots + (f_n\varphi_m)^i\,) \leq i\bar{e} \quad (i = 1, \ldots, m).$$

We consider the polynomials $F_i(u, x)$ of degree n w.r.t. x, whose roots are $\varphi_1^i, \ldots, \varphi_n^i$. Substituting $X_1 = f_n\varphi_1, \ldots, X_n = f_n\varphi_n$ and $X_{n+1} = 0, \ldots, X_{n^2} = 0$ in the lemma 5, we have the following degree bounds by the lemma 6.

$$\deg_u(\,(f_n\varphi_1)^j + \cdots + (f_n\varphi_n)^j\,) \leq j\bar{e} \quad (j = 1, \ldots, n^2).$$

By the lemma 5, we also have

$$\deg_u(F_i(u, x)) \leq ni\bar{e}, \quad F_i(u, x) = f_n^i(x - \varphi_1^i)\cdots(x - \varphi_n^i).$$

By applying the corollaries 2 and 3 to $F_i(u, x)$, we have that coefficients of terms whose degrees are equal to or larger than $d_n(ni\bar{e}) + n\bar{e}$ does not depend on coefficients of terms whose degrees are equal to or less than $n\bar{e}$, and coefficients of terms whose degrees are equal to or larger than $d_n(ni\bar{e})+n\bar{e}$, of the power-series roots, have the same linear dependent relations for coefficients of terms whose degrees are less than $d_n(ni\bar{e})+n\bar{e}$ and equal to or larger than $n\bar{e}$. Therefore, there must not exist any other linear independent relations on coefficients of powers of the power-series roots if we calculate the power-series roots up to the following degree.

$$d_n(ni\bar{e})+n\bar{e} = 2i\bar{e}n^4 - 2i\bar{e}n^3 + \frac{(4i\bar{e}-1)}{2}n^2 + \frac{(2\bar{e}-1)}{2}n + i - 1.$$

We use the largest degree $d_n(n^2\bar{e}) + n\bar{e}$ as the cutoff degree. This means that the theorem 4 is equal to the theorem with $E \to \infty$. Therefore, the theorem 4 is proved for the polynomial cutoff degree E as follows.

$$d_n(n^2\bar{e}) + n\bar{e} = 2\bar{e}n^5 - 2\bar{e}n^4 + 2\bar{e}n^3 - \frac{1}{2}n^2 + \frac{(2\bar{e}+1)}{2}n - 1.$$

We note that we can decrease the cutoff degree $d_n(n^2\bar{e})$ by $O(en^4)$ if the given polynomial is monic w.r.t. x, since $D(u, \varphi)$ becomes a monic polynomial w.r.t. φ and leading terms w.r.t. degree bounds, of $N_i(u, \varphi)$ are 0.

6. CONCLUSION

Applying concepts, D-finite power-series and P-recursive sequences, to the power-series roots of bivariate polynomials, give us new polynomially recursive algorithm to compute the power-series roots. Although the new algorithm has a weak point that we have to calculate a polynomially recursive formula (4.1) by differentiating and solving the system (3.8) as initial computations, its computational cost is linear w.r.t. the given cutoff degree. The algorithm is useful to compute the power-series roots up to higher degrees than n, the degree of the given polynomial w.r.t. the main variable. For some cases, we can construct general expressions of coefficients of power-series roots from recursive formulas. Moreover, these discussions also give us useful properties of the power-series roots. The proof in the section 5 is such an application use.

We can expand the D-finite power-series roots to multivariate polynomials and derive similar degree bounds and a multivariate version of the algorithm, using definitions of multivariate D-finite power-series and P-recursive functions by Lipshitz [2]. In fact, we have a result similar to the bivariate case though it is complicated. These results will be published in the future.

7. REFERENCES

[1] B. Benzaghou and J.-P. Bézivin. Propriétés algébriques de suites différentiellement finies. *Bull. Soc. Math. France*, 120(3):327–346, 1992.

[2] L. Lipshitz. D-finite power series. *J. Algebra*, 122:353–373, 1989.

[3] T. Sasaki. Approximate multivariate polynomial factorization based on zero-sum relations. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation, ISSAC 2001*, pages 284–291, 2001.

[4] T. Sasaki and K. Nagasaka. Approximate multivariate factorization and its time complexity. *preprint*, 1998.

[5] T. Sasaki, T. Saito, and T. Hilano. Analysis of approximate factorization algorithm I. *Japan J. Indust. Appl. Math.*, 9:351–368, 1992.

[6] T. Sasaki and M. Sasaki. A unified method for multivariate polynomial factorizations. *Japan J. Indust. Appl. Math.*, 10:21–39, 1993.

[7] R. P. Stanley. *Enumerative Combinatorics Volume 2, Cambridge Studies in Advanced Mathematics 62.* Cambridge University Press, Cambridge, 1997.