Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

Approximate Roots in Graded Rings

T. Beck, J. Schicho

RICAM-Report 2005-03

Approximate Roots in Graded Rings*

Tobias Beck, Josef Schicho
{Tobias.Beck, Josef.Schicho}@oeaw.ac.at
RICAM-Linz

- last updated March 1, 2005 -

Abstract

An approximate root of an univariate polynomial over a graded ring A is an element in A for which the evaluated polynomial vanishes up to a prescribed order. We give an algorithm for deciding existence of approximate roots and computing essentially all of them. Based on this algorithm we also suggest a finite representation for multivariate algebraic power series.

Contents

1 Introduction **2**

2 Graded rings and sliced rings **3**

3 Induced slicings and Newton equations **6**

4 Approximate and exact roots **10**

*This work was supported by the Austrian Science Fund (FWF) in the frame of the special research area SFB 013, subproject 03.

1 Introduction

If A is a multivariate polynomial algebra over a field, and p is a univariate polynomial over A, then an approximate root is an element $a \in A$ such that the order of the residual $p(a)$ is larger than a given integer. In this paper, we solve the problem of deciding whether approximate roots exist and to compute essentially all of them (cf. Propositions 7 and 8).

We have approximate roots of any order if and only if there exists a root in the formal power series algebra, by Wavrik's version [9] of the Artin Approximation Theorem. Assuming formal solvability, we can use our algorithm for expanding such a power series solution up to any given order.

If the input polynomial is square-free then any approximate root of sufficiently high order is a truncation of a power series solution, which is then uniquely determined. This observation provides a way to finitely represent algebraic power series, namely by minimal polynomial and suitable approximate root (cf. Corollary 10).

The idea is to increase the order of the residual iteratively, looking for a homogeneous solution in each step. The algorithm is similar to the classical Newton-Puiseux algorithm for solving bivariate polynomials. That algorithm has been generalized to the multivariate case by McDonald [6] and Beringer, Richard-Jung [3]. In these generalizations, the constructed solutions are contained in a suitable extension of the power series ring. In contrast to these, we concentrate on solutions in the original power series ring (or approximate solutions in the original polynomial ring). The algorithm does not guarantee the existence of approximate roots of arbitrary order and therefore the existence of power series solutions. On the other hand, there are situations where formal solvability is guaranteed, e.g. Tougeron's Implicit Function Theorem (cf. [7]) or the theorem of Jung-Abhyankar for quasi-ordinary polynomials (cf. [5, 4]).

The theoretical results apply to integral domains graded over arbitrary well-ordered monoids. The algorithms work if the order is isomorphic to ω, in particular for power series rings with an ordering based on total degree.

Our motivation for studying this problem originally was the intention to implement the algorithm of Alonso, Luengo and Raimondo [1] for solving quasi-ordinary polynomials. To do this, it would have been necessary to finitely represent algebraic power series. Such a representation was suggested in [2]. But then we observed that exact representation of the intermediate results is not really necessary, because for expansion up to a given order it suffices to work with approximate roots throughout.

2 Graded rings and sliced rings

In this section we give some generalities about graded rings, we introduce notation and the concept of sliced rings which is important for the rest of the article.

Throughout this article $\mathfrak{M}$ will denote an Abelian monoid that is endowed with a compatible well-ordering $<$, i.e. $\forall r, s, t \in \mathfrak{M} : r < s \Rightarrow r + t < s + t$. We write $\mathrm{succ}(r) := \min(\{s \mid s > r\})$ for the successor element of $r \in \mathfrak{M}$.

The fact that $\mathfrak{M}$ is ordered in such a way has several implications. First, $\mathfrak{M}$ has the cancellation property, i.e. $r \mapsto r+t$ for any $t \in \mathfrak{M}$ is an injective map. Indeed if $r \neq s$, say $r < s$, then $r + t < s + t$.

Second, 0 is the smallest element of $\mathfrak{M}$. For if r_0 is the smallest element, then $r_0 \leq 0$ and $r_0 + r_0 \leq r_0$ by compatibility. Hence $r_0 + r_0 = r_0$ and $r_0 = 0$ by the cancellation property. This also means that for $s + t = r$ we have $s \leq r$ and $t \leq r$ (because $0 \leq t$ implies $s \leq s + t$). All elements of $\mathfrak{M}$ being positive or zero implies that $\mathfrak{M}$ has no inverses.

Third, every element $r \in \mathfrak{M}$ can be written as a sum in only finitely many ways, i.e. the set $\{(s, t) \in \mathfrak{M}^2 \mid s + t = r\}$ is finite. Indeed assume it is infinite then we can find a subset $\{(s_i, t_i)\}_{i\in\mathbb{N}}$ s.t. $s_i < s_{i+1}$ for all i. Together with $r = s_i + t_i = s_{i+1} + t_{i+1}$ this implies $t_i > t_{i+1}$. So $\mathfrak{M}$ would contain an infinite descending chain, contradiction.

By A we will denote an $\mathfrak{M}$-graded integral domain. I.e. A can be decomposed as

$$A = \bigoplus_{r\in\mathfrak{M}} A_r$$

s.t. for $a \in A_r$ and $b \in A_s$ we have $ab \in A_{r+s}$. For $a \in A$ we write $\deg_{\mathfrak{M}}(a) = \max(\{r \mid a_r \neq 0\})$. Most of the time we apply the degree to elements $a \in A_r$ and say that a is homogeneous of degree r.

Example *Let $A := \mathbb{Q}[x_1, x_2]$ be the ring of bivariate polynomials over the field of rational numbers. Then A may be considered a graded ring over $\mathfrak{M} := \mathbb{N}^2$: The direct summands are $A_{(\nu_1,\nu_2)} = \{cx_1^{\nu_1}x_2^{\nu_2} \mid c \in \mathbb{Q}\} \cong \mathbb{Q}$. Let $\mathbb{N}^2$ be ordered first by total degree and second reverse lexicographically:*

$$\begin{aligned}(\nu_1, \nu_2) < (\mu_1, \mu_2) \quad :\Leftrightarrow \quad & \nu_1 + \nu_2 < \mu_1 + \mu_2 \text{ or} \\ & \nu_1 + \nu_2 = \mu_1 + \mu_2 \text{ and } \nu_2 < \mu_2\end{aligned}$$

With this definition $\mathbb{N}^2$ is order-isomorphic to ω.

In our setting we can embed A into a larger ring $\bar{A}$:

Definition 1 (Sliced rings)
Let A be an $\mathfrak{M}$-graded integral domain. We first define the associated formal series ring $\bar{A}$ as a product of modules

$$\bar{A} := \prod_{r \in \mathfrak{M}} A_r.$$

For $a = (a_r)_{r \in \mathfrak{M}} \in \bar{A}$ and $b = (b_r)_{r \in \mathfrak{M}} \in \bar{A}$ we define multiplication as follows:

$$ab := \left(\sum_{s+t=r} a_s b_t \right)_{r \in M}$$

*We call B an **$\mathfrak{M}$-sliced ring** if there is an $\mathfrak{M}$-graded ring A s.t. $A \subseteq B \subseteq \bar{A}$.*

Observe that multiplication is well-defined – meaning that the involved sums are finite – because of the properties of $\mathfrak{M}$. It is not hard to deduce that an $\mathfrak{M}$-sliced ring is integral because A was assumed integral in the definition.

Example (continued ...) *If $A = \mathbb{Q}[x_1, x_2]$ as above then $\bar{A}$ is isomorphic to the ring of formal power series $\mathbb{Q}[[x_1, x_2]]$ and every sub-ring of $\mathbb{Q}[[x_1, x_2]]$ containing all polynomials is an $\mathbb{N}^2$-sliced ring.*

The definition of sliced rings allows a uniform treatment in particular of the rings A and $\bar{A}$. We will also write elements of a sliced ring as sums rather than as tuples and speak of homogeneous and heterogeneous elements as in the graded situation.

Definition 2 (Support)
*Let B be an $\mathfrak{M}$-sliced ring. The **support** is defined as follows:*

$$\mathrm{Supp}_{\mathfrak{M}} : B \to 2^{\mathfrak{M}} : \sum_{r \in \mathfrak{M}} a_r \mapsto \{r \in \mathfrak{M} \mid a_r \neq 0\}$$

Definition 3 (Projections)
Let B be an $\mathfrak{M}$-sliced ring. For an element $a = \sum_{r \in \mathfrak{M}} a_r \in \bar{A}$, $s \in \mathfrak{M}$ and a binary relation $* \in \{=, \leq, \geq, <, >\}$ we write $a_{*s} := \sum_{r * s} a_r$. For abbreviation (and in consistence with the notation for the sum decomposition) we also write $a_s := a_{=s}$.

Definition 4 (Order)
*Let B be an $\mathfrak{M}$-sliced ring. Then the **order** is defined as follows:*

$$\mathrm{ord}_{\mathfrak{M}} : B \setminus \{0\} \to \mathfrak{M} : a \mapsto \min(\mathrm{Supp}_{\mathfrak{M}}(a))$$

The usual rules for the order apply. E.g. for all $a, b \in B \setminus \{0\}$ we have $\mathrm{ord}_{\mathfrak{M}}(ab) = \mathrm{ord}_{\mathfrak{M}}(a) + \mathrm{ord}_{\mathfrak{M}}(b)$. If $a + b \neq 0$ then $\mathrm{ord}_{\mathfrak{M}}(a + b) \geq \min(\mathrm{ord}_{\mathfrak{M}}(a), \mathrm{ord}_{\mathfrak{M}}(b))$ and equality holds if $\mathrm{ord}_{\mathfrak{M}}(a) \neq \mathrm{ord}_{\mathfrak{M}}(b)$. The fact that $\mathfrak{M}$ has no inverses implies that the only elements of sliced rings that have multiplicative inverses must have order 0.

The ring $\mathbb{Q}[[x_1, x_2]]$ of our example can also be defined as the I-adic completion of $\mathbb{Q}[x_1, x_2]$ w.r.t. the maximal ideal $I := \langle x_1, x_2 \rangle$. This can be generalized under certain additional assumptions on A.

Proposition 1 (Isomorphic completions)
Let A be an $\mathfrak{M}$-graded integral domain. Assume the ordering on $\mathfrak{M}$ is isomorphic to ω and there is $0 < s \in \mathfrak{M}$ s.t. A is generated by all A_r with $r \leq s$. Let $\bar{A}$ be the associated formal series ring (as in definition 1), $I := \langle A_r \rangle_{r>0}$ and C the I-adic completion of A. Then $\bar{A} \cong C$.

Proof: For every $r \in \mathfrak{M}$ the set $J_r := \{a \in A \mid a = 0 \text{ or } \mathrm{ord}_{\mathfrak{M}}(a) \geq r\}$ is a homogeneous ideal and $J_r \supseteq J_s$ for $r \leq s$. Since the ordering is isomorphic to ω the system $\{J_r\}_{r \in \mathfrak{M}}$ induces a metric s.t. $\bar{A}$ becomes the completion of A. In order to prove that the two completions are isomorphic we have to show that

a) for all $r \in \mathfrak{M}$ we can find $n \in \mathbb{N}$ s.t. $I^n \subseteq J_r$ and

b) for all $n \in \mathbb{N}$ we can find $r \in \mathfrak{M}$ s.t. $J_r \subseteq I^n$.

First we show a): Let $\mathtt{1} := \mathrm{succ}(0)$. By definition we have $I = J_{\mathtt{1}}$ and thus $I^n = J_{\mathtt{1}}^n$. An element $0 \neq a \in J_{\mathtt{1}}^n$ is of the form

$$a = \sum_{1 \leq k \leq u} \left(\prod_{1 \leq l \leq n} a_{k,l} \right)$$

with all $a_{k,l} \neq 0$ and $\mathrm{ord}_{\mathfrak{M}}(a_{k,l}) \geq \mathtt{1}$. Then $\mathrm{ord}_{\mathfrak{M}}(a) \geq n\mathtt{1}$ and hence $a \in J_{n\mathtt{1}}$. This shows $I^n \subseteq J_{n\mathtt{1}}$. Now for all $r \in \mathfrak{M}$ we can find $n \in \mathbb{N}$ s.t. $r \leq n\mathtt{1}$ because of the order-isomorphism with ω. Then $I^n \subseteq J_{n\mathtt{1}} \subseteq J_r$.

For part b) we choose $r = ns$. The proof of $J_r = J_{ns} \subseteq I^n$ is by induction. The statement is clear for $n = 0$. Now let $n > 0$ and assume the statement holds for $n - 1$. Since J_{ns} is a homogeneous ideal it is sufficient to show that for all homogeneous $a \neq 0$ s.t. $\deg_{\mathfrak{M}}(a) \geq ns$ we have $a \in I^n$. Because of the assumption on A we can write

$$a = \sum_{1 \leq k \leq u} a_k b_k$$

with all a_k, b_k homogeneous and non-zero, $0 < \deg_{\mathfrak{M}}(a_k) \leq s$ and $\deg_{\mathfrak{M}}(a_k) + \deg_{\mathfrak{M}}(b_k) = \deg_{\mathfrak{M}}(a)$. This implies $\deg_{\mathfrak{M}}(b_k) \geq (n-1)s$ and therefore $b_k \in I^{n-1}$ by the induction hypothesis. Of course $a_k \in I$ and together $a \in I^n$. $\square$

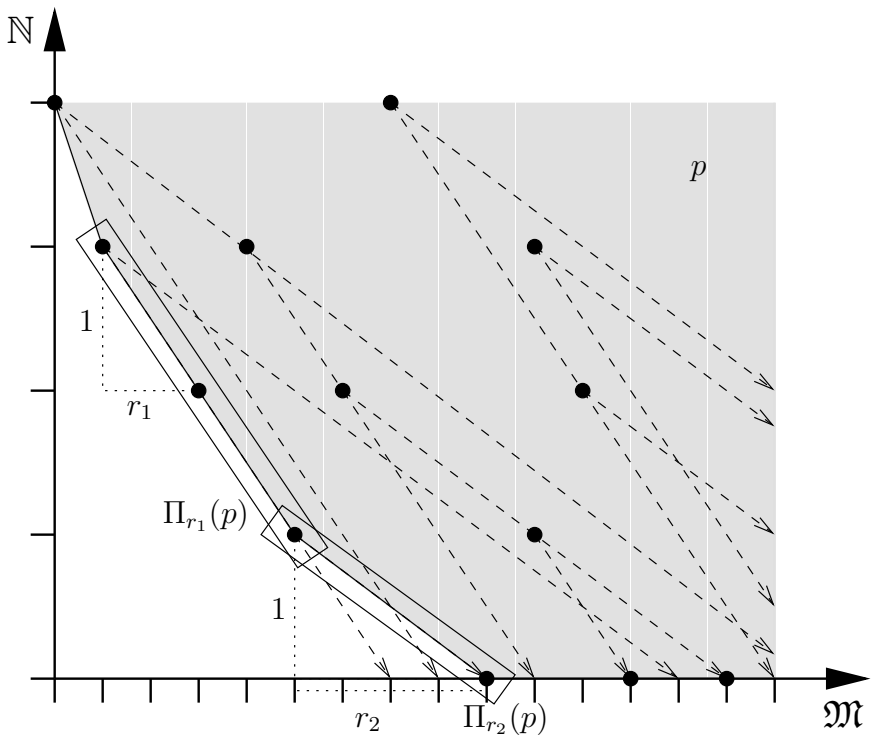

Figure 1: The r-induced slicing

Given a polynomial $p \in B[z]$ we view $\mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p)$, depicted by $\bullet$-s, in the $\mathfrak{M} \times \mathbb{N}$-plane. We indicate the $\mathfrak{M} \times \mathbb{N}$-slices that are affected by a translation with a homogeneous element of degree r_1 (resp. $r_2 > r_1$). The slices along one arrow have the same degree in the r_1-induced (resp. r_2-induced) slicing. Those with minimum degree form the r_1-st (resp. r_2-nd) Newton equation.

3 Induced slicings and Newton equations

Here we introduce the notion of Newton equation which will be the fundamental tool for finding approximate solutions in section 4.

For this section let B be an $\mathfrak{M}$-sliced ring. Then the polynomial ring $B[z]$ is $\mathbb{N}$-graded as well as $\mathfrak{M} \times \mathbb{N}$-sliced, i.e. an element $p \in B[z]$ can be written either $p = \sum_{j\in\mathbb{N}} p_j z^j$ with $p_j \in B$ or $p = \sum_{(s,j)\in\mathfrak{M}\times\mathbb{N}} p_{j,s} z^j$ with $p_{j,s} \in B$ homogeneous of degree s. Both notations will be used in the sequel.

In the classical Newton-Puiseux algorithm for curves (cf. [8]) the Newton polygon plays a central role. The algorithm solves iteratively so called edge equations. They are given by that part of the polynomial whose support lies on a certain edge of the Newton polygon, i.e. on a one-dimensional face that minimizes a special linear functional. This can be generalized. The following definitions and theorems are illustrated in figure 1.

Definition 5 (r-induced slicings)
For $r \in \mathfrak{M}$ we define the linear functional

$$h_r : \mathfrak{M} \times \mathbb{N} \to \mathfrak{M} : (s, j) \mapsto s + jr.$$

Then $B[z]$ may be viewed as a subset of $\prod_{t\in\mathfrak{M}} P_t$ with

$$P_t = \left\{ p \in B[z] \;\middle|\; p = \sum_{(s,j)\in\mathfrak{M}\times\mathbb{N}} p_{j,s} z^j \text{ and } h_r(s,j) = t \text{ for all } p_{j,s} \neq 0 \right\}.$$

*This way $B[z]$ becomes an $\mathfrak{M}$-sliced ring. We call that slicing the **r-induced slicing** on $B[z]$ and we write $\mathrm{Supp}_{\mathfrak{M},r}$, $\mathrm{ord}_{\mathfrak{M},r}$, $\deg_{\mathfrak{M},r}$.*

Definition 6 (Newton equations)
*Given a polynomial $0 \neq p \in B[z]$ and $r \in \mathfrak{M}$ we define the **r-th Newton equation** $\Pi_r(p) \in B[z]$ to be that part of p whose support minimizes the linear functional h_r. More precisely:*

$$\Pi_r(p) := p_{\mathrm{ord}_{\mathfrak{M},r}(p)}$$

(Again in other words the r-th Newton equation is the initial form w.r.t. the r-induced slicing.)

Example (continued . . .) *From now on we consider a polynomial p as follows:*

$$\begin{aligned}
p_1(z) &:= (x_1+x_2)z - (x_1+x_2)(x_2 + x_1^2 - 2x_1x_2 - x_2^3) + x_2^5 \\
p_2(z) &:= z^3 + (1-x_1)(x_1x_2 - x_2^2 + x_1^3)z + x_2(x_1x_2 - x_2^2 + x_1^3)^2 \\
p(z) &:= p_1(z)p_2(z) \\
&= (x_1 + \dots)z^4 + (-x_1x_2 + \dots)z^3 + (x_1^2x_2 + \dots)z^2 \\
&\quad + (-x_1^2x_2^2 + \dots)z - x_1^3x_2^4 + \dots
\end{aligned}$$

p would decompose as follows in the $(0,1)$-induced slicing:

$$\begin{aligned}
p \;=\; & \underbrace{(-x_1^2x_2^2z + x_1^2x_2z^2)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(2,3)} + \underbrace{(-x_1x_2z^3 + x_1z^4)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(1,4)} + \underbrace{(x_2^4z - x_2^3z^2 - x_2^2z^3 + x_2z^4)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(0,5)} \\
& + \underbrace{(-2x_1^4x_2z + x_1^4z^2)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(4,2)} + \underbrace{(2x_1^3x_2^2z - x_1^3z^3)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(3,3)} + \underbrace{(x_1^2x_2^3z)}_{\deg_{\mathbb{N}^2,(0,1)}(\dots)=(2,4)} + \dots
\end{aligned}$$

I.e. $\mathrm{ord}_{\mathbb{N}^2,(0,1)}(p) = (2,3)$ and the homogeneous part of that degree is $\Pi_{(0,1)}(p) = -x_1^2x_2^2z + x_1^2x_2z^2$.

One routinely checks the standard properties of initial forms w.r.t. the ring operations: For $0 \neq p \in B[z], 0 \neq q \in B[z]$ and $r \in \mathfrak{M}$ we have $\Pi_r(pq) = \Pi_r(p)\Pi_r(q)$. If $\mathrm{ord}_{\mathfrak{M},r}(p) < \mathrm{ord}_{\mathfrak{M},r}(q)$ then $\Pi_r(p+q) = \Pi_r(p)$. And if $\mathrm{ord}_{\mathfrak{M},r}(p) = \mathrm{ord}_{\mathfrak{M},r}(q)$ but $\Pi_r(p) + \Pi_r(q) \neq 0$ then $\Pi_r(p+q) = \Pi_r(p) + \Pi_r(q)$. For a polynomial ring the next interesting operation is composition.

Theorem 2 (Newton Equations and composition)
Let $0 \neq p \in B[z], 0 \neq q \in B[z]$ *and* $r \in \mathfrak{M}$ *s.t.* $\deg_{\mathbb{N}}(\Pi_r(q)) > 0$ *and* $s := \mathrm{ord}_{\mathfrak{M},r}(q)$. *Then* $\Pi_r(p \circ q) = \Pi_s(p) \circ \Pi_r(q)$ *and* $\mathrm{ord}_{\mathfrak{M},r}(p \circ q) = \mathrm{ord}_{\mathfrak{M},s}(p)$.

Proof: We point out that the condition on the Newton equation of q implies amongst others $\mathrm{ord}_{\mathfrak{M},r}(q) \geq r$.
First we study composition for the most simple case when p has singleton support. Write $p = \bar{p}z^j$ where $0 \neq \bar{p} \in B$ homogeneous of some degree $t \in \mathfrak{M}$:

$$(\bar{p}z^j) \circ q = \bar{p}q^j = \bar{p}(\Pi_r(q) + (q - \Pi_r(q)))^j =$$
$$\underbrace{\bar{p}\Pi_r(q)^j}_{=:A} + \underbrace{\sum_{1 \leq i \leq j} \binom{j}{i} \bar{p}\Pi_r(q)^{j-i}(q - \Pi_r(q))^i}_{=:B}$$

The term A is homogeneous in the r-induced slicing and $\deg_{\mathfrak{M},r}(A) = t + j\,\mathrm{ord}_{\mathfrak{M},r}(q) = t + js = \deg_{\mathfrak{M},s}(\bar{p}z^j)$. If $q - \Pi_r(q) \neq 0$ then $\mathrm{ord}_{\mathfrak{M},r}(B) \geq \min_{1 \leq i \leq j}(t + (j-i)\,\mathrm{ord}_{\mathfrak{M},r}(q) + i\,\mathrm{ord}_{\mathfrak{M},r}(q - \Pi_r(q))) > t + js$. In any case $\Pi_r((\bar{p}z^j) \circ q) = A = (\bar{p}z^j) \circ \Pi_r(q)$ and $\mathrm{ord}_{\mathfrak{M},r}((\bar{p}z^j) \circ q) = \deg_{\mathfrak{M},r}(A) = \deg_{\mathfrak{M},s}(\bar{p}z^j)$.
Now we consider the general case:

$$p \circ q = (\Pi_s(p) + (p - \Pi_s(p))) \circ q = \underbrace{\Pi_s(p) \circ q}_{=:C} + \underbrace{(p - \Pi_s(p)) \circ q}_{=:D}$$

Let $\Pi_s(p) = \sum_{0 \leq j \leq d} p_j z^j$ then $C = \sum_{0 \leq j \leq d}(p_j z^j) \circ q$. For j s.t. $p_j \neq 0$ we have $\Pi_r((p_j z^j) \circ q) = (p_j z^j) \circ \Pi_r(q)$ from above and $\mathrm{ord}_{\mathfrak{M},s}((p_j z^j) \circ q) = \deg_{\mathfrak{M},s}(p_j z^j) = \mathrm{ord}_{\mathfrak{M},s}(p)$ being equal for all j. On the other hand $\deg_{\mathbb{N}}(\Pi_r((p_j z^j) \circ q)) = j \deg_{\mathbb{N}}(\Pi_r(q))$ which is different for all such j. This implies in particular $\sum_{0 \leq j \leq d, p_j \neq 0} \Pi_r((p_j z^j) \circ q) \neq 0$. From the properties of initial forms we deduce $\Pi_r(C) = \sum_{0 \leq j \leq d, p_j \neq 0} \Pi_r((p_j z^j) \circ q) = \sum_{0 \leq j \leq d}(p_j z^j) \circ \Pi_r(q) = \Pi_s(p) \circ \Pi_r(q)$ and $\mathrm{ord}_{\mathfrak{M},r}(C) = \mathrm{ord}_{\mathfrak{M},s}(p)$.
If $D = 0$ we are finished. Otherwise let $0 \neq p - \Pi_s(p) = \sum_{0 \leq j \leq \bar{d}} \bar{p}_j z^j$ with $\mathrm{ord}_{\mathfrak{M}}(\bar{p}_j) + js > \mathrm{ord}_{\mathfrak{M},s}(p)$ then $D = \sum_{0 \leq j \leq \bar{d}} \bar{p}_j q^j$ and $\mathrm{ord}_{\mathfrak{M},r}(D) \geq \min_{0 \leq j \leq \bar{d}}(\mathrm{ord}_{\mathfrak{M},r}(\bar{p}_j) + j\,\mathrm{ord}_{\mathfrak{M},r}(q)) = \min_{0 \leq j \leq \bar{d}}(\mathrm{ord}_{\mathfrak{M}}(\bar{p}_j) + js) > \mathrm{ord}_{\mathfrak{M},s}(p)$. Again from the properties of initial forms we deduce $\Pi_r(p \circ q) = \Pi_r(C + D) = \Pi_r(C) = \Pi_s(p) \circ \Pi_r(q)$ and $\mathrm{ord}_{\mathfrak{M},r}(p \circ q) = \mathrm{ord}_{\mathfrak{M},s}(p)$. $\square$

This theorem has a very important specialization.

Corollary 3 (Newton Equations and translation)
Let $0 \neq p \in B[z]$, $a \in B$ *and* $r \in \mathfrak{M}$, *then* $\Pi_r(p \circ (z+a)) = \Pi_r(p \circ (z+a_{<r})) \circ (z+a_r)$ *and* $\mathrm{ord}_{\mathfrak{M},r}(p \circ (z+a)) = \mathrm{ord}_{\mathfrak{M},r}(p \circ (z+a_{<r}))$.

Proof: Apply theorem 2 to $p \circ (z+a) = (p \circ (z+a_{<r})) \circ (z+a_{\geq r})$. □

Example (continued . . .) *Given* p *as above. We translate by* $a = x_2$ *(which is homogeneous of degree* $(0,1)$*) and view the result in the* $(0,1)$*-induced slicing:*

$$p \circ (z+x_2) = \underbrace{(x_1^2x_2^2z + x_1^2x_2z^2)}_{\deg_{\mathbb{N}^2,(0,1)}(\ldots)=(2,3)} + \underbrace{(x_1x_2^3z + 3x_1x_2^2z^2 + 3x_1x_2z^3 + x_1z^4)}_{\deg_{\mathbb{N}^2,(0,1)}(\ldots)=(1,4)} + \ldots$$

We see that the r*-homogeneous part of* $p \circ (z+a)$ *is given by the translation of the* r*-homogeneous part of* p. *In particular for the* $(0,1)$*-st Newton equation we have* $\Pi_{(0,1)}(p \circ (z+x_2)) = \Pi_{(0,1)}(p) \circ (z+x_2) = x_1^2x_2^2z + x_1^2x_2z^2$.
Translating by a heterogeneous element of order $(0,1)$, *e.g.* $a = x_2 + x_1^2$, *in general violates the* $(0,1)$*-induced slicing. Nevertheless the* $(0,1)$*-st Newton equation is changed in a controlled way. We still have* $\Pi_{(0,1)}(p \circ (z+x_2+x_1^2)) = \Pi_{(0,1)}(p \circ (z+x_2)) = \Pi_{(0,1)}(p) \circ (z+x_2) = x_1^2x_2^2z + x_1^2x_2z^2$.

The r-induced order of a polynomial and the $\mathbb{N}$-degree of its r-th Newton equation are monotone in r:

Theorem 4 (Monotonicity)
For $0 \neq p \in B[z]$ *and* $s > r$ *we have*

a) $\deg_{\mathbb{N}}(\Pi_s(p)) \leq \mathrm{ord}_{\mathbb{N}}(\Pi_r(p)) \leq \deg_{\mathbb{N}}(\Pi_r(p))$ *and*

b) $\mathrm{ord}_{\mathfrak{M},s}(p) \geq \mathrm{ord}_{\mathfrak{M},r}(p)$ *where equality holds iff* $\mathrm{ord}_{\mathbb{N}}(\Pi_r(p)) = 0$.

Proof: First recall that

$$\begin{aligned}(t,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_r(p)) &\Leftrightarrow (t,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p) \text{ and } t + jr = \mathrm{ord}_{\mathfrak{M},r}(p),\\ (t,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_s(p)) &\Leftrightarrow (t,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p) \text{ and } t + js = \mathrm{ord}_{\mathfrak{M},s}(p).\end{aligned}$$

To prove claim a) let $j_0 := \mathrm{ord}_{\mathbb{N}}(\Pi_r(p))$ and t_0 s.t. $(t_0, j_0) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_r(p))$. Let $j_1 := \deg_{\mathbb{N}}(\Pi_s(p))$ and t_1 s.t. $(t_1, j_1) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_s(p))$. Now assume indirectly $j_1 > j_0$. Since $t_1 + j_1r \geq \mathrm{ord}_{\mathfrak{M},r}(p)$ we have $t_1 + j_1r \geq t_0 + j_0r$, hence $t_1 + (j_1 - j_0)r \geq t_0$, hence $t_1 + (j_1 - j_0)s > t_0$, hence $t_1 + j_1s > t_0 + j_0s$. But then $\mathrm{ord}_{\mathfrak{M},s}(p) > t_0 + j_0s$, a contradiction.

Now we prove claim b): Choose arbitrary $(t,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_s(p))$. Then immediately $\mathrm{ord}_{\mathfrak{M},s}(p) = t + js \geq t + jr \geq \mathrm{ord}_{\mathfrak{M},r}(p)$.

Let $\mathrm{ord}_{\mathbb{N}}(\Pi_r(p)) = 0$, then a) implies also $\mathrm{ord}_{\mathbb{N}}(\Pi_s(p)) = 0$. I.e. there is $(t_0, 0) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_s(p)) \cap \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_r(p))$ and $\mathrm{ord}_{\mathfrak{M},s}(p) = t_0 = \mathrm{ord}_{\mathfrak{M},r}(p)$.

Let now $\mathrm{ord}_{\mathfrak{M},s}(p) = \mathrm{ord}_{\mathfrak{M},r}(p)$. Then there is $(t_0, j_0) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_s(p))$ s.t. $t_0 + j_0 s = \mathrm{ord}_{\mathfrak{M},s}(p) = \mathrm{ord}_{\mathfrak{M},r}(p) \leq t_0 + j_0 r$. This implies $j_0 = 0$, $(t_0, 0) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(\Pi_r(p))$ and hence $\mathrm{ord}_{\mathbb{N}}(\Pi_r(p)) = 0$. □

Example (continued . . .) *Now we compare p in the $(0,1)$- and $(1,2)$-induced slicing. Observe that $(1,2) > (0,1)$. We have $\mathrm{ord}_{\mathbb{N}^2,(1,2)}(p) = (3,4)$ and $\Pi_{(1,2)}(p) = -x_1^2x_2^2z - x_1^3x_2^4$. We see that $\mathrm{ord}_{\mathbb{N}^2,(1,2)}(p) > \mathrm{ord}_{\mathbb{N}^2,(0,1)}(p) = (2,3)$, $\deg_{\mathbb{N}}(\Pi_{(1,2)}(p)) = 1 \leq \mathrm{ord}_{\mathbb{N}}(\Pi_{(0,1)}(p)) = 1$ and $\mathrm{ord}_{\mathbb{N}}(\Pi_{(1,2)}(p)) = 0$. For all $r > (1,2)$ we consequently get $\mathrm{ord}_{\mathbb{N}^2,r}(p) = (3,4)$ and $\Pi_r(p) = -x_1^3x_2^4$.*

4 Approximate and exact roots

Given $p \in B[z]$ we would like to find $a \in B$ s.t. $p \circ a = 0$. In general this will not be possible, except if $B = \prod_{r\in\mathfrak{M}} B_r$ is in fact an algebraically closed field. But in this case the slicing would be trivial, i.e. $B_r = 0$ for $r \neq 0$ (because in particular we would need inverses). Instead we will look for approximate solutions, in our context we want to find $a \in B$ s.t. $\mathrm{ord}_{\mathfrak{M}}(p \circ a)$ is big.

A basic observation is that $p \circ a$ equals the constant coefficient in $p \circ (z + a)$. The method proposed in this section will successively compute the homogeneous parts of an approximate solution a (in the order dictated by $\mathfrak{M}$) and translate p by these homogeneous elements in order to "sweep away the constant coefficient of $p \circ (z + a)$ as far as possible".

First we study the link between Newton equations and evaluation:

Proposition 5 (Newton equations and evaluation)
Let $0 \neq p \in B[z]$, $a \in B$, $r \in \mathfrak{M}$ and $s := \mathrm{ord}_{\mathfrak{M},r}(p \circ (z + a_{<r}))$. Then

$$\Pi_r(p \circ (z + a_{<r})) \circ a_r = (p \circ a)_s.$$

(In other words from a partial translation up to degree r, we know the complete evaluation at degree s.)

Proof: By corollary 3 we know that $s = \mathrm{ord}_{\mathfrak{M},r}(p \circ (z + a))$. The constant coefficient of $\Pi_r(p \circ (z + a))$ equals the homogeneous part of degree $(s, 0)$ of $p \circ (z + a)$ in the $\mathfrak{M} \times \mathbb{N}$-slicing, that again equals the homogeneous part of degree s of $p \circ a$ in the $\mathfrak{M}$-slicing. In other words $(p \circ a)_s = \Pi_r(p \circ (z + a)) \circ 0$. And again

using corollary 3 we get $\Pi_r(p \circ (z+a)) \circ 0 = \Pi_r(p \circ (z+a_{<s})) \circ (z+a_s) \circ 0 = \Pi_r(p \circ (z+a_{<s})) \circ a_s$. □

Now we can give an exact criterion for the approximation order.

Theorem 6 (Approximation criterion)
Let $p \in B[z]$, $a \in B$ and $s \in \mathfrak{M}$. The following are equivalent:

a) $p \circ a = 0$ or $p \circ a \neq 0$ and $\mathrm{ord}_{\mathfrak{M}}(p \circ a) \geq s$

b) if r is s.t. $\mathrm{ord}_{\mathfrak{M},r}(p \circ (z+a_{<r})) < s$ then a_r is a root of $\Pi_r(p \circ (z+a_{<r}))$

Proof: Clearly a) holds iff $(p \circ a)_{s'} = 0$ for all $s' < s$.

a) ⇒ b) Follows immediately from proposition 5.

b) ⇒ a) Assume the contrary and choose a minimal $s' < s$ s.t. $(p \circ a)_{s'} \neq 0$.

Then $\mathrm{ord}_{\mathfrak{M},s'}(p \circ (z+a)) = \min(\{r + js' \mid (r,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p \circ (z+a))\})$. For $(r,j) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p \circ (z+a))$ we have two possible cases: Either $j > 0$ or $j = 0$. In the second case $r \geq s'$ because s' was chosen minimal s.t. $0 \neq (p \circ a)_{s'} = (p \circ (z+a))_{(s',0)}$. In each case $r + js' \geq s'$ and this boundary is reached. Hence we get $\mathrm{ord}_{\mathfrak{M},s'}(p \circ (z+a)) = s'$.

By corollary 3 we have $\mathrm{ord}_{\mathfrak{M},s'}(p \circ (z+a_{<s'})) = \mathrm{ord}_{\mathfrak{M},s'}(p \circ (z+a)) = s' < s$ and by proposition 5 we have $\Pi_{s'}(p \circ (z+a_{<s'})) \circ a_{s'} = (p \circ a)_{s'} \neq 0$, a contradiction to the assumption. □

Proposition 5 and theorem 6 are visualized in figure 2. They imply a recursive algorithm scheme (cf. *FindApproximateRoots*, *FindRecursive*, algorithms 1 and 2) for finding approximate roots. In order to specify the output we have to say what approximate roots are and when they are essentially the same.

Definition 7 (Equivalence on s-approximate roots)
*Let $p \in B[z]$. The element $a \in B$ is called an **s-approximate root** iff $p \circ a = 0$ or $\mathrm{ord}_{\mathfrak{M}}(p \circ a) \geq s$. Two s-approximate roots $a, a' \in B$ are **equivalent**, $a \equiv_{p,s} a'$, iff $a_r = a'_r$ for all $r \in \mathfrak{M}$ s.t. $\mathrm{ord}_{\mathfrak{M},r}(p \circ (z+a_{<r})) < s$.*

From now on, we assume that $\mathfrak{M}$ is order-isomorphic to ω. We also fix the $\mathfrak{M}$-graded ring A s.t. $A \subseteq B \subseteq \bar{A}$. In this case an equivalence class of s-approximate roots has representatives within the graded ring A. These assumptions are necessary to ensure termination of the algorithms.

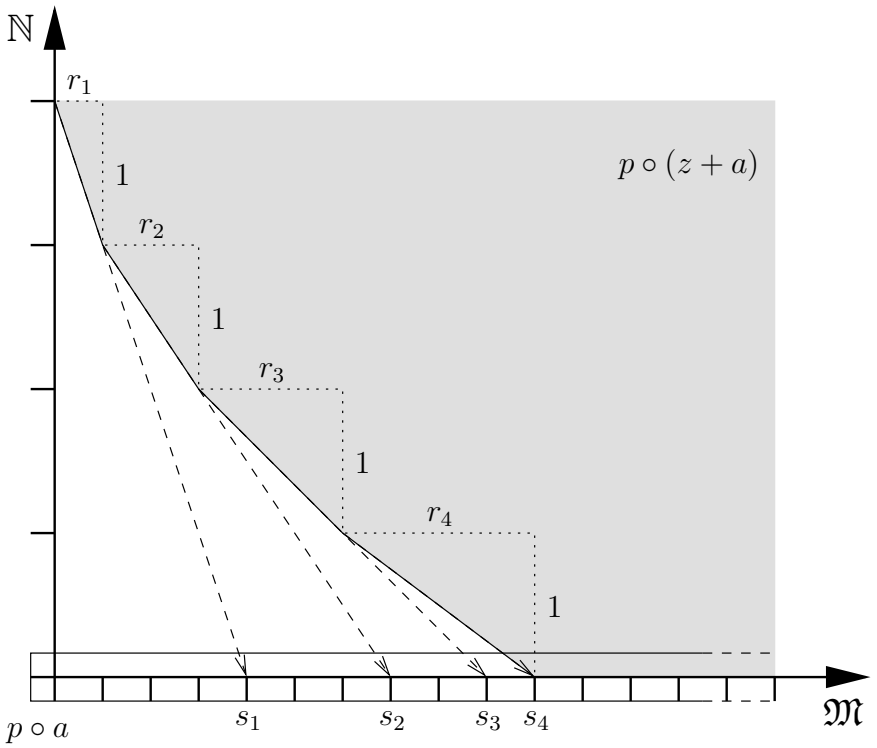

Figure 2: Approximate roots

Given an s_4-approximate root a of p, we show the Newton equations of the translated polynomial $p \circ (z + a)$ for orders r_i. The orders $s_i = \mathrm{ord}_{\mathfrak{M},r_i}(p \circ (z + a)) = \mathrm{ord}_{\mathfrak{M},r_i}(p \circ (z + a_{<r_i}))$ show the influence of these Newton equations on the evaluation.

Algorithm 1 $FindApproximateRoots(p : B[z], s : \mathfrak{M}) : 2^A$

Input : a polynomial $0 \neq p \in B[z]$ and an approximation order $s \in \mathfrak{M}$
Output : a system $S \subset A$ of representatives of all s-approximate roots

1: **return** $FindRecursive(p, s, 0)$;

Algorithm 2 $FindRecursive(p : B[z], s : \mathfrak{M}, r : \mathfrak{M}) : 2^A$

Input : a polynomial $0 \neq p \in B[z]$, an approximation order $s \in \mathfrak{M}$ and an order $r \in \mathfrak{M}$ s.t. for all $r' < r$ holds $z|\Pi_{r'}(p)$ and $\mathrm{ord}_{\mathfrak{M},r'}(p) < s$

Output : a system $S \subset A$ of representatives of all s-approximate roots s.t. $\mathrm{ord}_{\mathfrak{M}}(a) \geq r$ for all $a \in S$

1: **if** $\mathrm{ord}_{\mathfrak{M},r}(p) \geq s$ **then**
2: **return** $\{0\}$;
3: $S := \emptyset$; $\bar{S} := HomogeneousRoots(\Pi_r(p), r)$;
4: **for** $a \in \bar{S}$ **do**
5: $q := p \circ (z + a)$;
6: $R := FindRecursive(q, s, \mathrm{succ}(r))$;
7: $S := S \cup (\{a\} + R)$;
8: **return** S;

Algorithm 3 $HomogeneousRoots(p : A[z], r : \mathfrak{M}) : 2^A$

Input : a polynomial $0 \neq p \in A[z]$ homogeneous in the r-induced slicing

Output : the set $\{a \in A \mid p \circ a = 0, a = 0$ or homogeneous of degree $r\}$

Example (continued ...) *Given p as above. Then $a := x_2 + x_1^2 - 2x_1x_2 - x_2^3$ is a $(1,7)$-approximate root, because $\mathrm{ord}_{\mathbb{N}^2}(p \circ a) = (1,7)$ and one can check:*

$\Pi_{(1,0)}(p) = x_1z^4$,
$\Pi_{(0,1)}(p) = x_1^2x_2z^2 - x_1^2x_2^2z$ *with root* x_2,
$\Pi_{(2,0)}(p \circ (z + x_2)) = x_1^2x_2^2z - x_1^4x_2^2$ *with root* x_1^2,
$\Pi_{(1,1)}(p \circ (z + x_2 + x_1^2)) = x_1^2x_2^2z + 2x_1^3x_2^3$ *with root* $-2x_1x_2$,
$\Pi_r(p \circ (z + x_2 + x_1^2 - 2x_1x_2)) = x_1^2x_2^2z$ *for* $(0,2) \leq r \leq (1,2)$,
$\Pi_{(0,3)}(p \circ (z + x_2 + x_1^2 - 2x_1x_2)) = x_1^2x_2^2z + x_1^2x_2^5$ *with root* $-x_2^3$,
$\Pi_r(p \circ (z + x_2 + x_1^2 - 2x_1x_2 - x_2^3)) = x_1^2x_2^2z$ *for* $(4,0) \leq r \leq (0,4)$ *and*
$\Pi_r(p \circ (z + x_2 + x_1^2 - 2x_1x_2 - x_2^3)) = x_1x_2^7$ *for* $r \geq (5,0)$ *which is unsolvable.*

Since $\Pi_{(5,0)}(p \circ (z + a))$ has no homogeneous root, a cannot be extended to an s-approximate root for any $s > (1,7)$. Also $\mathrm{ord}_{\mathbb{N}^2}(p(\bar{a})) = (1,7)$ for all $\bar{a}$ s.t. $\bar{a}_{<(5,0)} = a_{<(5,0)}$. Such $\bar{a}$ is an $(1,7)$-approximate root as well and $\bar{a} \equiv_{p,(1,7)} a$.
If we call algorithm 1 with p and approximation order $(1,7)$ we get two roots

$$FindApproximateRoots(p, (1,7)) = \{-x_1x_2^2 + x_2^3, \quad x_2 + x_1^2 - 2x_1x_2 - x_2^3\}.$$

The first interesting Newton equation of p is $\Pi_{(0,1)}(p) = x_1^2x_2z^2 - x_1^2x_2^2z$. To compute its homogeneous roots of degree $(0,1)$ we set $z = cx_2$ and get $\Pi_{(0,1)}(p) \circ cx_2 = c(c-1)x_1^2x_2^3$. This shows that for a fine grading like this we actually have to solve polynomial equations in $\mathbb{Q}[c]$ only and we find $c \in \{0,1\}$. Thus $\Pi_{(0,1)}(p)$ has the two roots 0 and x_2. The algorithm branches according to these roots. The

two elements of the output correspond to the different choices. Looking for higher order approximate roots results in a singleton set, for example

$$FindApproximateRoots(p,(4,4)) = \{-x_1x_2^2 + x_2^3 - x_1^3x_2\}.$$

Algorithm 1 is just a wrapper of algorithm 2, so it is sufficient to show correctness and termination of that algorithm.

Proposition 7 (Correctness)
If algorithm 2 terminates it is correct. More precisely:

a) If $b \in B$ is an s-approximate root of p and $\mathrm{ord}_{\mathfrak{M}}(b) \geq r$ then there is $b' \in S$ s.t. $b \equiv_{p,s} b'$.

b) If $b' \in S$ then b' is an s-approximate root of p and $\mathrm{ord}_{\mathfrak{M}}(b') \geq r$.

c) For all $b', b'' \in S$ we have $b' \not\equiv_{p,s} b''$.

Proof: If $\mathrm{ord}_{\mathfrak{M},r}(p) \geq s$ then we end up in line 2. In this case 0 is an s-approximate root of p by theorem 6. Indeed it follows from theorem 4 that for $r' \in \mathfrak{M}$ the condition $\mathrm{ord}_{\mathfrak{M},r'}(p \circ (z + 0_{<r'})) = \mathrm{ord}_{\mathfrak{M},r'}(p) < s$ implies $r' < r$. From the input specification we know that in this case $z | \Pi_{r'}(p) = \Pi_{r'}(p \circ (z + 0_{<r'}))$, hence $0_{r'} = 0$ is a root of that equation. Now let $0 \neq b \in B$ be any s-approximate root s.t. $\mathrm{ord}_{\mathfrak{M}}(b) \geq r$ then $b_{r'} = 0$ for $r' < r$ hence $b \equiv_{p,s} 0$. This shows claims a), b) and c) in case the recursion ends.

Next we show the claims when $\mathrm{ord}_{\mathfrak{M},r}(p) < s$, i.e. when the algorithm might go into recursion. It is not hard to show that the arguments to the recursive calls always meet the input specification of the algorithm. Now we assume correctness of the recursive call:

a) Let $b \in B$ be an s-approximate root of p s.t. $\mathrm{ord}_{\mathfrak{M}}(b) \geq r$. Then b_r must be a root of $\Pi_r(p \circ (z + b_{<r}))$ by theorem 6. Hence $b_r = a$ for some $a \in \bar{S}$ (cf. line 3 and the input specification of algorithm 3). Then $b - a$ is an s-approximate root of $q = p \circ (z + a)$ s.t. $\mathrm{ord}_{\mathfrak{M}}(b - a) \geq \mathrm{succ}(r)$. Then there must be $c' \in R$ (cf. line 6) s.t. $c' \equiv_{q,s} b - a$. This implies $a + c' \equiv_{p,s} b$ and $a + c' \in S$ after line 7.

b) If $b' \in S$ then there is $a \in \bar{S}$ and $b' = a + c'$ where c' is an s-approximate root of $q = p \circ (z + a)$ s.t. $\mathrm{ord}_{\mathfrak{M}}(c') \geq \mathrm{succ}(r)$ if $c' \neq 0$. Then of course b' is an s-approximate root of p and $\mathrm{ord}_{\mathfrak{M}}(b') \geq r$ if $b' \neq 0$.

c) Let $b', b'' \in S$. If $b'_r \neq b''_r$ then for sure $b' \not\equiv_{p,s} b''$ by the definition of equivalence. Hence it is sufficient that $b', b'' \in \{a\} \cup R$ for $a \in \bar{S}$ and R as in line 6 are pairwise not equivalent. This follows from $b' = a + c'$, $b'' = a + c''$ and $c' \not\equiv_{q,s} c''$. □

Proposition 8 (Termination)
Algorithm 2 terminates.

Proof: Assume algorithm 2 is called with $p \in B[z]$ and $r, s \in \mathfrak{M}$. If $\mathrm{ord}_{\mathfrak{M},r}(p) \geq s$ in line 1 or $\bar{S} = \emptyset$ in line 3 it terminates. Otherwise the algorithm will call itself recursively. If q is defined as in line 5 of the algorithm and $a \in \bar{S}$, then $\mathrm{ord}_{\mathbb{N}}(\Pi_r(q)) = \mathrm{ord}_{\mathbb{N}}(\Pi_r(p \circ (z + a))) = \mathrm{ord}_{\mathbb{N}}(\Pi_r(p) \circ (z + a)) > 0$ because a is a root of $\Pi_r(p)$. It follows from theorem 4 that $\mathrm{ord}_{\mathfrak{M},r'}(q) > \mathrm{ord}_{\mathfrak{M},r}(p)$. So the respective order is increasing with every recursive call and because of the order-isomorphism with ω the case $\mathrm{ord}_{\mathfrak{M},s}(p) < r$ cannot happen forever. □

Remark 1 (Effectivity)
In order to turn this algorithm scheme effectively into an algorithm, we additionally have to provide an algorithm HomogeneousRoots (for its specification see algorithm 3) that solves for homogeneous roots. In the case of power series over a field with a monomial slicing this boils down to univariate root solving over the ground field (see example).
Algorithms 1 and 2 take as input elements of a sliced ring but produce elements of a graded ring only (which are usually finite objects). So the algorithms are independent of a representation for elements of the sliced ring as long as some very elementary operations are possible.

Under certain assumptions there is essentially one approximate root of a fixed minimum order.

Proposition 9 (Uniqueness of approximate roots)
Let $0 \neq p \in B[z]$ *and* $r, s \in \mathfrak{M}$ *be s.t.* $\deg_{\mathbb{N}}(\Pi_r(p)) = 1$ *and* $s \geq \mathrm{ord}_{\mathfrak{M},r}(p)$. *If* $a, b \in B$ *are* s*-approximate roots with* $\mathrm{ord}_{\mathfrak{M}}(a) \geq r$ *and* $\mathrm{ord}_{\mathfrak{M}}(b) \geq r$ *then* $a \equiv_{p,s} b$.

Proof: We have to show that $a_{r'} = b_{r'}$ for all r' s.t. $\mathrm{ord}_{\mathfrak{M},r'}(p \circ (z + a_{<r'})) < s$.
The proof is by induction on r'. $a_{r'} = b_{r'} = 0$ for $r' < r$ by assumption. Now let $r' \geq r$ and assume $\mathrm{ord}_{\mathfrak{M},r'}(p \circ (z + a_{<r'})) < s$ and $a_{<r'} = b_{<r'}$. Then because of theorem 6 both $a_{r'}$ and $b_{r'}$ must be roots of $\Pi_{r'}(p \circ (z + a_{<r'})) = \Pi_{r'}(p \circ (z + b_{<r'}))$. This implies that $\deg_{\mathbb{N}}(\Pi_{r'}(p \circ (z + a_{<r'}))) > 0$. On the other hand $\deg_{\mathbb{N}}(\Pi_{r'}(p \circ (z + a_{<r'}))) \leq \deg_{\mathbb{N}}(\Pi_r(p \circ (z + a_{<r'}))) = \deg_{\mathbb{N}}(\Pi_r(p \circ (z + a_{<r})) \circ (z + a_r)) = \deg_{\mathbb{N}}(\Pi_r(p)) = 1$ because of theorem 4 and corollary 3. Hence $\Pi_{r'}(p \circ (z + a_{<r'}))$ is a linear equation and has exactly one root $a_{r'} = b_{r'}$. □

Moreover if in this situation a is an exact root then it clearly is an s-approximate root for any order s. Calling algorithm 2 with increasing approximation orders

will return only singleton sets and so would be a method to expand a up to prescribed order. Proposition 9 is reflected in the algorithm as follows: All relevant Newton equations are linear and may be solved by a single division only (even by the same element). We give an iterative version (cf. algorithm 4) that expands an exact root using only divisions of homogeneous elements. It also provides a way to represent certain elements of B. This is stated more precisely in the next corollary.

Algorithm 4 *Expand*$(p : B[z], r : \mathfrak{M}, r' : \mathfrak{M}) : A$

Input : a polynomial $0 \neq p \in B[z]$, a minimum order $r \in \mathfrak{M}$ and an expansion order $r' \in \mathfrak{M}$ s.t. $r \leq r'$, $\deg_{\mathbb{N}}(\Pi_r(p)) = 1$ and there is $a \in B$ with $p(a) = 0$ and $\mathrm{ord}_{\mathfrak{M}}(a) \geq r$ if $a \neq 0$

Output : a polynomial $b \in A$ with $b = a_{<r'}$

1: $q := p$; $u := \frac{\partial q}{\partial z} \circ 0$; {i.e. u is the coefficient of z^1}
2: $s := \mathrm{ord}_{\mathfrak{M}}(u)$; $c := u_s$; $b := 0$;
3: **for** $r \leq t < r'$ **do**
4: $\quad v := q \circ 0$; {i.e. v is the coefficient of z^0}
5: $\quad d := -v_{s+t}/c$; {division of homogeneous elements}
6: $\quad q := q \circ (z + d)$; $b := b + d$;
7: **return** b;

Corollary 10 (Representation)
Let $0 \neq p \in B[z]$ be a square-free polynomial and $a \in B$ with $p(a) = 0$. Then there is $r \in \mathfrak{M}$ s.t. $\deg_{\mathbb{N}}(\Pi_r(p \circ (z + a_{<r}))) = 1$. For all $b \in B[z]$ s.t. $p(b) = 0$ and $b_{<r} = a_{<r}$ we have $b = a$. (And using algorithm 4 one can compute $a_{<r'}$ given p, $r' > r$ and $a_{<r}$.)

Proof: We have $z \mid p \circ (z + a)$ because a is a root of p but $z^2 \nmid p \circ (z + a)$ because p is square-free. Choose any $r \in \mathfrak{M}$ s.t. $(r, 1) \in \mathrm{Supp}_{\mathfrak{M}\times\mathbb{N}}(p \circ (z + a))$. Indeed one can show that $\deg_{\mathbb{N}}(\Pi_r(p \circ (z + a))) = 1$. Then $\deg_{\mathbb{N}}(\Pi_r(p \circ (z + a))) = \deg_{\mathbb{N}}(\Pi_r(p \circ (z + a_{<r})) \circ (z + a_r)) = \deg_{\mathbb{N}}(\Pi_r(p \circ (z + a_{<r})))$ by corollary 3. Now $a_{\geq r}$ is a root of $p \circ (z + a_{<r})$ with $\mathrm{ord}_{\mathfrak{M}}(a_{\geq r}) \geq r$. The rest follows from proposition 9 and algorithm 4. □

The **implicit function theorem** tells when an algebraic equation has an unique formal series root that vanishes at the origin. Unfortunately proposition 9 does not give a sufficient condition for the existence of an exact root to an algebraic equation. But in analogy with this theorem it describes when a root vanishing at the origin with sufficiently high order is uniquely determined. And in certain situations existence can be deduced by other means.

Example (continued . . .) *The polynomial of our examples is of the form $p = p_1 p_2$. Here $x_2(\partial p_2/\partial z \circ 0)^2 = x_2(1 - x_1)^2(x_1 x_2 - x_2^2 + x_1^3)^2$ divides $p_2 \circ 0 =$*

$x_2(x_1x_2 - x_2^2 + x_1^3)^2$ *in* $\mathbb{Q}[[x_1, x_2]]$ *because they differ only by a unit. Tougeron's Implicit Function Theorem (cf. [7]) tells that in this case* p_2 *(and thus* p*) has a root* $a \in \mathbb{Q}[[x_1, x_2]]$ *in the ideal generated by* $x_2(\partial p_2/\partial z \circ 0)$*. This root is equivalent to the* $(4,4)$*-approximate root* $-x_1x_2^2 + x_2^3 - x_1^3x_2$ *computed above.*

One computes $\Pi_{(2,2)}(p \circ (z - x_1x_2^2 + x_2^3 - x_1^3x_2)) = -x_1^2x_2^2z - x_1^4x_2^4$*. Corollary 10 means that the triple* $(p, a_{<(2,2)}, (2,2)) = (p, -x_1x_2^2 + x_2^3 - x_1^3x_2, (2,2))$ *could be used to represent* a *by a finite amount of information. Assume we want to use algorithm 4 to compute* a *up to total degree* 8*:*

$$\begin{aligned} a_{<(9,0)} &= -x_1x_2^2 + x_2^3 - x_1^3x_2 + Expand(p \circ (z - x_1x_2^2 + x_2^3 - x_1^3x_2), (2,2), (9,0)) \\ &= -x_1x_2^2 + x_2^3 - x_1^3x_2 - x_1^2x_2^2 + x_1x_2^3 - x_1^4x_2 - x_1^3x_2^2 + x_1^2x_2^3 - x_1^5x_2 \\ &\quad -x_1^4x_2^2 + x_1^3x_2^3 - x_1^6x_2 - x_1^5x_2^2 + x_1^4x_2^3 + x_1^2x_2^5 - 2x_1x_2^6 + x_2^7 \\ &\quad -x_1^7x_2 - x_1^6x_2^2 + x_1^5x_2^3 + 2x_1^4x_2^4 + 2x_1^3x_2^5 - 8x_1^2x_2^6 + 4x_1x_2^7 \end{aligned}$$

Remark 2 (Quasi-ordinary polynomials)
Let $\mathbb{K}$ *be an algebraically closed field of characteristic zero. The Jung-Abhyankar theorem (cf. for example [5]) guarantees the existence of series roots with fractional exponents for certain polynomials* $p \in \mathbb{K}[[x_1, \ldots, x_n]][z]$*. More precisely if* $p(0, \ldots, 0, z) = z^d v$ *with* $v \in \mathbb{K}[z]$ *s.t.* $v(0) \neq 0$ *and* $\mathrm{disc}_z(p) = x_1^{\mu_1} \ldots x_n^{\mu_n} u$ *with* $u \in \mathbb{K}[[x_1, \ldots, x_n]]$ *s.t.* $u(0, \ldots, 0) \neq 0$ *then there are exactly* d *pairwise distinct roots* $a_i \in \mathbb{K}[[x_1^{1/d!}, \ldots, x_n^{1/d!}]]$ *through the origin. I.e.* $p(a_i) = 0$ *and* $a_i(0, \ldots, 0) = 0$ *for* $1 \leq i \leq d$*.*

The same can be stated without fractional exponents: If p *is as above, then* $\bar{p} := p(x_1^{d!}, \ldots, x_n^{d!}, z)$ *has roots* $\bar{a}_i := a_i(x_1^{d!}, \ldots, x_n^{d!}) \in \mathbb{K}[[x_1, \ldots, x_n]]$*. In this situation one can use algorithm 1 to compute the set of* s*-approximate roots for increasing values of* s *until the output consists of* d *different approximate roots each corresponding to one of the exact series roots. Those may be expanded up to arbitrary order using algorithm 4.*

We close with a remark on the denominators: Choosing $d!$ *always works, but the actually necessary denominator is much smaller. It is possible, but a little technical, to adapt algorithm 1 in order to introduce denominators only as needed.*

Remark 3 (Quadratic convergence)
Algorithm 4 can be modified further to use some sort of Newton iterations. The exact division of two homogeneous elements in each iteration would be replaced by "truncated division of heterogeneous elements". The modified algorithm attains quadratic convergence.

References

[1] Alonso, M. E., Luengo, I., and Raimondo, M. An algorithm on quasi-ordinary polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*, vol. 357 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1989, pp. 59–73.

[2] Alonso, M. E., Mora, T., and Raimondo, M. A computational model for algebraic power series. *J. Pure Appl. Algebra 77*, 1 (1992), 1–38.

[3] Beringer, F., and Richard-Jung, F. Multi-variate polynomials and Newton-Puiseux expansions. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, vol. 2630 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2003, pp. 240–254.

[4] González Pérez, P. D. Singularités quasi-ordinaires toriques et polyèdre de Newton du discriminant. *Canad. J. Math. 52*, 2 (2000), 348–368.

[5] Luengo, I. A new proof of the Jung-Abhyankar theorem. *J. Algebra 85*, 2 (1983), 399–409.

[6] McDonald, J. Fiber polytopes and fractional power series. *J. Pure Appl. Algebra 104*, 2 (1995), 213–233.

[7] Ruiz, J. M. *The basic theory of power series*. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1993.

[8] Walker, R. J. *Algebraic curves*. Springer-Verlag, New York, 1978. Reprint of the 1950 edition.

[9] Wavrik, J. J. A theorem of completeness for families of compact analytic spaces. *Trans. Amer. Math. Soc. 163* (1972), 147–155.