An application of generalized Newton Puiseux Expansions

to a conjecture of D. Daigle and G. Freudenburg

By Avinash Sathaye, University of Kentucky

September 17, 2014

1 Introduction

Let k denote the ground field. Let R be the coordinate ring of an affine curve over k with one place at infinity. Let v denote the valuation associated with the place at infinity and let $\Gamma(R)$ denote the corresponding value semigroup consisting of all the values of nonzero elements of R.

If R is a plane curve (meaning generated by two elements over k) and k is algebraically closed and characteristic zero (or at least if the characteristic does not divide the value of one of a pair of generators), then the well known Abhyankar-Moh theory gives a detailed description of the semigroup and indeed the semigroups obtained from such plane curves (planar semigroups) can be completely characterized as shown in [S1], [SS].

Moreover, the theory shows that the ring R has a distinguished basis over k generated by certain polynomials in the two ring generators of R with the property that distinct basis elements have distinct values and so the value semigroup is nothing but the values of the distinct basis elements.

We generalized the concepts of such plane curves and value semigroups in [S1] to include rings of the form $R[[t_1, \cdots, t_s]]$ where R is still a curve as above, with the valuation denoted by v. We will explain the exact connection below. We will also show the existence of a similar distinguished k basis, which was only partly described in [S1].

We will then show an application to a conjecture of D. Daigle and G. Freudenburg which we reformulate as follows.

Let R be as above and set $\Psi : R[[t]] \longrightarrow R$ be defined as the canonical residue map mod (t). Further, let $u_0(t), u_1(t) \in R[[t]]$, such that $v(\Psi(u_0)) = -n \neq 0$. Set $u_0^* = \Psi(u_0), u_1^* = \Psi(u_1)$.

Let $\phi_1(Y, u_0^*)$ be the minimum monic polynomial of u_1^* over $k(u_0^*)$. Then it is easy to see that $\phi_1(Y, u_0^*) \in k[Y, u_0^*]$. Since we have $\phi_1(u_1^*, u_0^*) = 0$, we see that $\phi_1(u_1, u_0)$ is divisible by some largest power t^{a_1} and we define $u_2 = \phi_1(u_1, u_0)/t^{a_1}$, and $u_2^* = \Psi(u_2)$.

Then **the conjecture is** that every such sequence can be continued indefinitely. Specifically, if $u_0, \cdots, u_m$ are constructed and the corresponding $u_i^* = \Psi(u_i)$ are defined, then the minimum monic polynomial $\phi_m(Y, u_{m-1}^*, \cdots, u_0^*)$ of u_m^* over $k(u_0^*, \cdots, u_{m-1}^*)$ is actually in $k[Y, u_0^*, \cdots, u_{m-1}^*]$ and we can extend the sequence by defining $u_{m+1} = \phi_m(u_m, u_{m-1}, \cdots, u_0)/t^{a_m}$ and $u_{m+1}^* = \Psi(u_{m+1})$, where, as before a_m is the highest power of t that divides the expression.

Actually, the original conjecture used "slow division" by t, which leads to several trivial u_i, where the equation $\Phi_i = Y$ and then $u_{i+1} = u_1/t$. We drop these to get a better match with our construction.

The point of the conjecture is that all the corresponding ϕ_i are polynomials in all their arguments, i.e. u_m^* satisfies an integral relation whose degree matches its field degree over $k(u_0^*, \cdots, u_{m-1}^*)$. [DF]

Our proof of this consists of showing that the quantities $\phi_m(u_m, u_0, \cdots, u_{m-1})$ simply correspond to certain members of our distinguished basis up to multiplication by a power of t. The fact that the degree of an integral relation matches the field degree is simply a consequence of the properties of the generalized Newton-Puiseux expansions.

We begin by giving a review of our generalized theory from [SS], [S1]. As before, the reference to Abhyankar's TIFR notes [A1] is the crucial reference, but we will not give point by point reference. Since we are about to describe an extension of the notion of pseudoapproximate roots we shall try to make this as self contained as possible by repeating several definitions in detail and giving outline of the arguments. We also provide a proof of the irreducibility criterion (2.2.1) which was not essential in [S1] and hence was avoided in that paper.

2 Setup

Let k be the ground field. We shall later assume it to be algebraically closed of characteristic zero. Some of the universal notations shall be:

$$\mathbb{Z} = \text{ the set of integers }, \mathbb{Z}_+ = \{a \in \mathbb{Z} | a \geq 0\}$$

and

$$\mathbb{Q} = \text{ the set of rationals }, \mathbb{Q}_+ = \{a \in \mathbb{Q} | a \geq 0\}.$$

We shall use the "Abhyankar nonzero symbol" θ, which specifies a nonzero constant. This is used in places where we don't have use for the explicit value of the constant and it can stand for different constants even in the same equation.

For $0 \neq n \in \mathbb{Z}_+$, let $\mu_n(k)$ be the set of the n-th roots of unity in k and in our case of algebraically closed characteristic zero k, we can simply write μ_n.

We consider a **generalized power series**

$$f = \sum_{\iota \in \Lambda} f_\iota x^\iota$$

where the coefficients f_ι are in k and the indexing set Λ is a well ordered subset of some chosen ordered abelian group.

By $\mathrm{Supp}\,(f)$ we denote the set of ι for which f_ι is nonzero. We can clearly replace Λ by $\mathrm{Supp}\,(f)$.

In particular, we will need to use the field of multi-Laurent series in p variables $k \ll x \gg = k \ll x_1, \cdots, x_p \gg$, where we use the abelian group $\mathbb{Z}^p$ of p-tuples of integers ordered by reverse lexicographic order [1] and we conveniently write x^i for $x_1^{i_1} \cdots, x_p^{i_p}$. In such fields, we define $\mathrm{ord}\,(f) = \mathrm{ord}_x(f) = \inf\{\iota | \iota \in \mathrm{Supp}\,(f)\}$. Moreover, we define the initial form $\mathrm{Info}\,(f) = a_\iota x^\iota$ if $\iota = \mathrm{ord}\,(f)$ and the corresponding initial coefficient $\mathrm{Inco}\,(f) = a_\iota$.

As customary, we define $\mathrm{ord}_x(0) = \infty$ where ∞ is augmented to the abelian group as a maximal element. The corresponding initial form shall be declared 0. Of course, this is only a technicality and we avoid using the zero element for f.

For an exponent $\iota = (\iota_1, \cdots, \iota_p)$, we need two projection functions, $^-, \pi$ defined as $\bar{\iota} = \iota_1$ and $\pi(\iota) = (\iota_2, \cdots, \iota_p)$.

Given any sequence of positive rational numbers $n = (n_1, \cdots, n_p)$ we can similarly define a field $k \ll x^n \gg = k \ll x_1^{n_1}, \cdots, x_p^{n_p} \gg$ and finally, the multi-Laurent field is defined as $\mathcal{L}(k,p) = \bigcup\{k \ll x^n \gg\}$ where n varies over all sequences of positive rationals.

The **generalized Newton's Lemma** states that for an algebraically closed k of characteristic zero, an algebraic closure of $k \ll x \gg$ is given by $\mathcal{L}(k,p)$.

The proof is easily modified from (5.5) in ET [A1]as follows.

Note that $k \ll x \gg = k \ll x_1, \cdots, x_{p-1} \gg \ll x_p \gg$ and that The **usual Newton's Lemma** says that for a field K of characteristic zero, the field

[1] Recall that reverse lexicographic order means that we say $(m_1, \cdots, m_p) > (n_1, \cdots, n_p)$, if the last m_i distinct from n_i satisfies $m_i > n_i$.

$\mathcal{L}(\overline{K}, 1)$ gives the algebraic closure of $K \ll x \gg$, where $\overline{K}$ is an algebraic closure of K. The result now follows by induction applied to $K = k \ll x_1, \cdots, x_{p-1} \gg$.

2.1 Characteristic terms

We now fix a value of $p \geq 1$.

Given an n-th root of unity $\omega \in \mu_n(k)$ we define as associated automorphism $\overline{\omega}$ of $k \ll x \gg$ by defining

$$\overline{\omega}(\sum a_i x^i) = \sum a_i \omega^{i_1} x^i.$$

In short, this corresponds to sending x_1 to ωx_1 and fixing all other variables.

For a fixed power series $y(x) = \sum a_\iota x^\iota \in k \ll x \gg$, we construct a polynomial

$$f = f(Y) = \prod_{\omega \in \mu_n} (Y - \overline{\omega}(y(x)).$$

It is easy to see that $f \in k \ll x^{\tilde{n}} \gg [Y]$, where $\tilde{n} = (n, 1, \cdots, 1)$. In other words $f \in k \ll x_1^n, \cdots, x_2, \cdots, x_p \gg$. Indeed, if the gcd of n and the set $\{\iota_1 = \bar{\iota} | \iota \in \mathrm{Supp}\,(y(x))\}$ is d, then f is the d-th power of the minimum polynomial of $y(x)$ over the field $k \ll x^{\tilde{n}} \gg$.

Let Λ be the support of $y(x)$. Note that all conjugates $\overline{\omega}(y(x))$ have the same support Λ and we declare it to be also the $\mathrm{Supp}\,(f)$.

For each $\lambda \in \Lambda$ we wish to define some associated quantities inductively.

1. Given any λ, set c_λ to be the coefficient of x^λ in $y(x)$ and thus $\Lambda = \{\lambda | c_\lambda \neq 0\}$.

2. For a set of integers S, by $\gcd(S)$, we mean the gcd of all the elements of S. Set
$$d(\lambda) = \gcd(\{n\} \bigcup \{\iota_1 | \iota \in \Lambda | \iota < \lambda\}\})$$
and note that $d(\lambda) = n$ if λ is the minimum element of Λ.

   Also define $\hat{d}(\lambda) = \gcd(\lambda_1, d(\lambda))$.

   Finally set $n(\lambda) = d(\lambda)/\hat{d}(\lambda)$.

3. Given some $\lambda \in \Lambda$, by a λ-deformation of $y(x)$ we mean a power series $y_\lambda(x)$ with the property that $y_\lambda(x) - y(x)$ has the initial term $(Z - c_\lambda)x^\lambda$. Here Z is best thought of as a brand new indeterminate, or at least

something independent from earlier coefficients. We can specialize Z to convenient quantities afterwards.

It is a simple matter to evaluate $f(y_\lambda(x))$ and note that we get

$$\mathrm{Info}\,(f(y_\lambda(x))) = \theta\,(Z^{n(\lambda)} - c_\lambda^{n(\lambda)})^{\hat{d}(\lambda)} x^{s(\lambda)}.$$

Note that here the coefficient θ is completely determined by the coefficients of $y(x)$ up to the λ term.

The quantity $s(\lambda)$ may be taken as defined by this formula and we will give an alternate expression later.

For future use, we define $r(\lambda) = s(\lambda)/d(\lambda)$.

4. The explanation of the above formula is this.

   We have
$$\mathrm{Info}\,(f(y_\lambda(x))) = \prod_{\omega\in\mu_n} (y_\lambda(x) - \overline{\omega}(y(x))).$$
   and the initial form is simply the product of the initial forms of the various terms, each of which can be rewritten as $(y_\lambda(x)-y(x))-(y(x)-\overline{\omega}(y(x)))$. The initial form of the first piece is $(Z - c_\lambda)x^\lambda$ and it cannot cancel with the initial form of the second piece. The order of the second piece is less than λ exactly when $\omega^{d(\lambda)} \neq 1$ and hence for all such ω, the initial coefficient is free of Z and forms part of the θ. The $d(\lambda)$ terms with $\omega^{d(\lambda)} = 1$ give the order of the second piece bigger than or equal to λ - which is the order of the first piece. Hence the order of such terms is exactly λ and the initial forms are $(Z - c_\lambda\omega^{\overline{\lambda}})x^\lambda$.

   Moreover, if the ratio of two $d(\lambda)$-th roots of unity ω_1 and ω_2 is a $\hat{d}(\lambda)$-th root of unity, then the corresponding initial forms are the same, since $\hat{d}(\lambda)$ divides $\overline{\lambda}$. This easily gives the asserted expression.

5. **Assumption:** Now, for convenience, assume that k is algebraically closed of characteristic zero. In many cases, this assumption can be weakened to assuming that the characteristic does not divide certain important numbers.

   Now we give the more explicit form of $s(\lambda)$, along with a few other conventional characteristic terms, as promised.

   Set $\nu = -n$ for our current application to meromorphic type curves. In general, it is set to be $\pm n$. For the minimum element α in Λ, set $q(\alpha) = \alpha$ and $s(\alpha) = q(\alpha)d(\alpha)$. Inductively, if the quantities are defined thru some β and λ is the next term in the well ordered set, then we define $q(\lambda) = \lambda - \beta$ and $s(\lambda) = s(\beta) + q(\lambda)d(\lambda)$. In case, λ does not have an immediate predecessor in Λ, we have to proceed as follows. Pick some $\theta < \lambda$ in Λ such that $d(\theta) = d(\beta) = d(\lambda)$ for all $\theta < \beta < \lambda$ with $\beta \in \Lambda$. [2] Define $s(\lambda) = s(\theta) + (\lambda - \theta)d(\lambda)$. It is not hard to see that if we replace θ by an intermediate β, then we have $s(\beta) = s(\theta) + (\beta - \theta)d(\beta) = s(\theta) + (\beta - \theta)d(\lambda)$ and clearly $s(\lambda)$ also equals $s(\beta) + (\lambda - \beta)d(\lambda)$. Note that the quantity $q(\lambda)$ cannot be defined in this situation.

It is also clear that the s-function is an increasing function. The corresponding r-function is defined by $r(\lambda) = s(\lambda)/\hat{d}(\lambda)$.

2.2 Newton Puiseux expansions and irreducibility

We constructed $f = f(Y)$ above which was a polynomial in Y with coefficients in $k << x^{\tilde{n}} >>$ starting with a formal generalized power series. For applications at hand, we study polynomials $f = f(Y) = f(Y, w_1, \cdots, w_n) \in A[Y]$ where $A = k[w_1][[w_2, \cdots, w_p]]$.

A generalized Newton Puiseux expansion (NP expansion) for such a polynomial is an expansion $y = y(x) \in k << x >>$ such that $f(y(x), x_1^{n_1}, \cdots, x_p^{n_p}) = 0$ for some integers $n_1, \cdots, n_p$.

To be consistent with our conventions, we need $n_2, \cdots, n_p$ to be positive integers.

Actually, we will be interested in a generalization of usual unibranch curves and so we restrict our attention to them by declaring the following:

For $f = f(Y) \in A[Y]$ **a generalized NP expansion** shall be taken to mean a substitution $Y = y(x), w_1 = x_1^{\nu}, w_2 = x_2, \cdots, w_p = x_p$, such that $f(y(x), x_1^{\nu}, x_2, \cdots, x_p) = 0$.

Here ν is an integer and the case when ν is positive is described as the **generalized algebroid curve**, while the case of a negative ν is the **generalized meromorphic curve.**

Convention: We may simplify our statements by declaring $Y = y(x)$ to be a root of $f(Y)$ **normalized to** $(\nu, 1, \cdots, 1)$ **or simply to** ν**, if the**

[2] Such a θ exists, since there are only a finitely many values of the d-function and $d(\lambda)$ is the gcd of n and all possible $\overline{\beta}$ with $\beta < \lambda$ in Λ.

meaning is clear., when we substitute for w_i as described above.

We generally do not require the power series $y(x)$ to have integral exponents in x_1, but require that for some positive integer D, the power series $y(x)$ is a member of $k << x_1^{1/D}, x_2, \cdots, x_p >>$.

Clearly, if the x_1 is replaced by x_1^d for some positive d, then we get an equivalent but different NP expansion. We can avoid this ambiguity in expansions, if we use fractional powers of w_1 in place of integral powers of x_1.

Further, replacing x_1 by ωx_1 where ω is a $|\nu|$-th root of unity, we get a conjugate expansion which is also considered equivalent. In case of fractional power series, we can allow $|\nu|$-th roots of unity where ν is a common denominator for exponents of w_1.

The curve $f(Y)$ is said to be unibranch, if as a polynomial in Y, $f(Y) \in A[Y]$ is monic of degree n and its roots are a complete set of conjugates by n-th roots of unity, where any one root is $Y = y(x) \in k << x_1, \cdots, x_p >>$ which is normalized to $(\nu, 1, \cdots, 1)$ with $|\nu| = n$. As usual, we extend the definition of unibranch to curves which become unibranch after multiplication by a nonzero constant.

Now we assume that our f is unibranch of degree n as described above. We thus have a factorization as stated before

$$f = f(Y) = \prod_{\omega \in \mu_n} (Y - \overline{\omega}(y(x)) \text{ with } y(x) \in k << x_1, \cdots, x_p >> .$$

REMARK:

Given another power series $y^*(x) = \sum c^*_\iota x^\iota$, let λ be the largest order among the set ord $(y^*(x) - \overline{\omega}(y(x)))$. Without loss of generality, assume that this maximum is reached with $\omega = 1$, i.e. $y^*(x) - y(x)$ has order λ. Then is easy to check, using our above calculations with λ-deformations, that the order of $f(y^*(x))$ is $s(\lambda)$.

Note that the gcd d of n and the first components $\overline{\lambda}$ of λ in the support of $y(x)$ is necessarily 1, since otherwise $y(x)$ would have only n/d distinct conjugates contrary to the assumption.

2.2.1 Irreducibility criterion

Definition of maximal contact Let us formally declare the maximal contact of a polynomial $g(Y)$ with respect to the given $f(Y)$ **normalized to** $(\nu, 1, \cdots, 1)$) **to be the maximum of the orders of differences of**

$y^*(x) - y(x)$**, where** $y^*(x)$ **runs over all roots of** $g(Y)$ **normalized to** $(\nu, 1, \cdots, 1)$**, and** $y(x)$ **ranges over similar roots for** $f(Y)$**.**

We shall prove the following claim:

Now assume that $f(Y) = f(Y, w_1, \cdots, w_p)$ is unibranch of degree n as above.

Let $g(Y) = g(Y, w_1, \cdots, w_p) \in A[Y]$ be monic of degree m in Y such that $m = n/d(\lambda)$ for some λ and assume that the order of $g(y(x), x_1^\nu, x_2, \cdots, x_p) = \theta$ where $\theta \geq s(\lambda)/d(\lambda)$.

Then $g(Y)$ is unibranch with an expansion $Y = y^*(x), w_1 = x_1^\nu, w_2 = x_2, \cdots, w_p = x_p$, so that $y^*(x) \in k << x_1, \cdots, x_p >>$ and $y^*(x) - y(x)$ has order at least λ for one of the roots $y(x)$ of $f(Y)$.

The proof of this claim is a simple adaptation of the original proof of Abhyankar and Moh.[AM1, AM2] and can also be located in the more recent [A3].

To see this, let β be the maximal contact of $g(Y)$ with $f(Y)$ normalized to $(\nu, 1, \cdots, 1)$.

Let $\operatorname{Res}(f, g, Y)$ be the usual Y resultant, which is, upto a sign, the product of differences of roots of f, g. From our calculation above, we see that the order of $\operatorname{Res}(f, g, Y)$ is at most $s(\beta)m$ when we view the resultant as product of evaluations of $f(Y)$ at roots of $g(Y)$. Conversely, when we think of it as evaluations of $g(Y)$ at roots of $f(Y)$, we note that we get the same order θ repeated n times, since the roots of f are conjugate.

Thus we have $ms(\beta) \geq n\theta \geq ms(\lambda)$.

Hence, $g(Y)$ has a root $y^*(x)$ which differs from a root of f past $\beta \geq \lambda$. Moreover, such a root has clearly $n/d(\lambda)$ conjugates (by $n/d(\lambda)$-th roots of unity), and since $m = n/d(\lambda)$ coincides with degree of $g(Y)$, the conjugates must exhaust all the roots of $g(y)$.

This proves that all the roots of $g(Y)$ are conjugate by $m = n/d(\lambda)$-th roots of unity and that any one of them differs from a root of f at or past λ, after we normalize it by substituting $w_1 = x_1^\nu$. This finishes the claim.

2.3 The g-sequence

Now we construct the generalized version of the usual g-sequence, which is also known as the sequence of (certain chosen) approximate or pseudoapproximate roots.

We begin with a unibranch $f = f(Y) \in A[Y]$ with a generalized NP expansion $Y = y(x), w_1 = x_1^\nu, w_2 = x_2, \cdots, w_p = x_p$, as before, where $\nu = -n$

for the meromorphic case and $\nu = n$ for the algebroid case. Let Λ be the support of $y(x)$.

First, we recall the usual sequence of approximate roots of $f(Y)$ as explained in section 3 of [S1]. [3] **Please note that we are using G in place of g in order to save the notation g for the more generalized versions of these approximate roots.** While we don't repeat any proofs, we will explain the inductive construction, partly because we have not introduced the notation m_i yet.

Let α be the order of $y(x)$ and set $G_1 = G_1(Y) = Y$. Set $r_1 = r(\alpha) = \alpha$ and $m_1 = \alpha$.

Note that $G_1(Y)$, is a polynomial of degree $n/d_1 = n/|\nu| = 1$ and is unibranch with maximal contact r_1 with f normalized to $(\nu, 1, \cdots, 1)$, or simply put, normalized to ν.

Set $d_2 = \gcd(\overline{r_1}, d_1)$ and let m_2 be the first exponent in Λ which has the property that $\overline{m_2}$ is not divisible by d_2. Define $G_2(Y)$ to be the approximate d_2-th root of $f(Y)$, i.e. the unique polynomial of degree n/d_2 satisfying the condition that $f(Y) - G_2(Y)^{d_2}$ has Y-degree less than $n - n/d_2$.

Continuing in this fashion, if we have constructed $G_1(Y), \cdots, G_{i-1}(Y)$, then we set $d_i = \gcd(\overline{r_{i-1}}, d_{i-1})$ and define m_i to be the first exponent in Λ for which $\overline{m_i}$ is not divisible by d_i. Define $G_i(Y)$ to be the approximate d_i-th root of $f(Y)$. Set $n_i = d_i/d_{i+1} = n(m_i)$.

The process stops when we reach some number h such that d_{h+1} is the gcd of n and all $\overline{\lambda}$ for $\lambda \in \Lambda$. Indeed, since $f(Y)$ is unibranch, $d_{h+1} = 1$. Then, we can define $G_{h+1}(Y)$ to be simply the polynomial $f(Y)$ itself, since its degree is supposed to be $n/d_{h+1} = n$.

We note that the polynomials $G_1(Y), \cdots, G_h(Y)$ having the following properties.

1. The polynomial $G_i(Y)$ is a monic polynomial in $A[Y]$ of degree $n/d(\lambda(i))$.

2. $G_i(Y)$ has maximal contact $r(m_i)$ with $f(Y)$ normalized to ν. For convenience, we denote it as r_i.

3. Moreover, having fixed an m_i-deformation $y_{m_i}(x)$ of some fixed root $y(x)$ of $f(Y)$, we have that

$$\text{Info}\,(G_j(y_{m_i}(x)) = \theta\, x^{r_i} \text{ for } 1 \leq j < i$$

[3] We take this opportunity to correct a couple of typos in 3.1 of [S1]. First, the notation G in 3.1.1, 3.1.2 should be g. Further, g_e in 3.1.6 should be g.

while

$$\text{Info}\,(G_i(y_{m_i}(x)) = \theta\,(Z - c^*_{m_i})x^{r_i}.$$

In particular, all the $G_i(Y)$ are unibranch.

4. Define a permissible monomial $\prod_j G_j(Y)^{a_j}$ to be a monomial such that $0 \leq a_j < n_i$.

   Let $\mathcal{M}(i)$ denote all permissible monomials in $\{G_j(Y))|1 \leq j < i\}$. Then $\mathcal{M}(i)$ form an A- basis for all polynomials in $A[Y]$ of degree less than the degree of $G_i(Y)$, i.e. n/d_i.

5. In particular, the polynomial $f(Y)$ has a well defined $G_i(Y)$-adic expansion

   $$f(Y) = G_i(Y)^{d_i} + U_1(Y)G_i(Y)^{d_i-1} + \cdots + U_{d_i}(Y)$$

   where U_i are combinations of elements of $\mathcal{M}(i)$ over A. Also, by our assumption, $U_1(Y) = 0$ for $i \geq 2$.

6. We also have an expression for G_{i+1} in terms of $M(i)$ given by

   $$G_{i+1} = G_i^{n_i} + \sum H_a G^a \text{ where } G^a = G_1^{a_1} \cdots G_i^{a_i} \in \mathcal{M}(i+1) \text{ and } H_a \in A.$$

   We further expand $H_a = \sum_\iota H_{a,\iota} w^\iota$ as an element of $A = k[w_1][[w_2, \cdots, w_p] = k[x_1^\nu][[x_2, \cdots, x_p]]$, so that $H_{a,\iota} \in k$.

   Let $\Theta : A[Y] \longrightarrow A[Y]/(f(Y)) = A[y(x)]$ be the canonical map sending Y to $y(x)$. Let θ be the induced order given by $\theta(H(Y)) = \text{ord}_x(H(y(x))$. Note that $\theta(G_i) = r_i$.

7. As explained in section 3 of [S1], the distinct terms $\Theta(w^\iota G^a)$ have distinct x-orders as long as the monomials G^a are permissible. It follows that

   $$\theta(\sum\{H_{a,\iota}G^a|\theta(H_{a,\iota}G^a) \geq \lambda\} = \lambda$$

   . Thus, for every $\lambda = H_{a,\iota}G^a$ between $\theta(G_i^{n_i}) = n_i r_i$ and $\theta(G_{i+1}) = r_{i+1}$, we have that

   $$\theta(G_i^{n_i} + \sum\{H_{a,\iota}G^a|\theta(H_{a,\iota}G^a) < \lambda\} = \theta(\{H_{a,\iota}G^a) = \lambda.$$

   Denote the resulting polynomial by $G^*_{i,\lambda}(Y)$. We have now constructed a Well ordered set of (unibranch) polynomials, $G^*_{i,\lambda}(Y)$, which can be lexicographically ordered by their subscripts.

8. For any fixed i, as a temporary notation, let $G^*_{i,\beta}(Y)$ be the first polynomial in our set. Then G^*i, β is of degree n_i as a polynomial in $G_i(Y)$ with coefficients in $A[G_1(Y), \cdots, G_{i-1}(Y)]$, where we only keep permissible monomials.

   Further, for all $G^*_{i,\beta^*}(Y)$ with $\beta^* > \beta$, the expression is simply linear in $G^*_{i,\beta}$ with coefficients in $A[G_1(Y), \cdots, G_{i-1}(Y)]$ using permissible monomials.

9. For each $G_{i,\lambda}(Y)$, note that its maximal contact with $f(Y)$ is between m_i and m_{i+1} and steadily increases with λ.

   Let us denote the corresponding contact by $\kappa(i, \lambda)$.

   We are finally ready to define the desired g-sequence to match the u-sequence as explained in the introduction.

   Set $g_\beta(Y) = G^*_{i,\lambda}(Y)$ if $\beta = \kappa(i, \lambda)$. Note that, we can recover (i, λ) from κ by first finding i using $m_i < \kappa \leq m_{i+1}$, and then finding $\lambda = \theta(g_\beta(Y))$.

3 Application to Daigle and Freudenburg Conjecture

We start with the ring $R[[t]]$ as explained in the introduction. We can choose a uniformizing parameter ${x^*}_1$ for the valuation v, such that $R[[t]] \subset k << {x^*}_1 >> [[t]] \subset k << {x^*}_1 >><< t >>$. By a suitable change of variables, we can find some x_1 such that

$$u_0 = x_1^{-n} \text{ and } \ k << {x^*}_1 >><< t >>= k << x_1, t >> .$$

As usual, this is done by taking x_1 to be the $-1/n$-th root of u_0 viewed as an element of $k << {x^*}_1 >><< t >>$ and noticing that $x_1 = {x^*}_1 +$ terms in the ideal generated by ${x^*}_1^2, t$.

Now we can match our setup. In this case, $p = 2$ and $x_2 = t$. Let us take $\nu = -n$. Let $A = k[x_1^\nu][[x_2]] = k[u_0][[t]]$, so $w_1 = u_0, w_2 = t$.

Now $u_1 = u_1(x_1, x_2) = \sum_\lambda c_\lambda x^\lambda$ in our notation and this is a generalized NP expansion as above.

It is possible that the gcd of $\overline{\lambda}$ with λ in the support of u_1 is $d > 1$. In this case, we will replace x_1 by $x_1^{1/d}$ and this will arrange

that the new gcd is 1. We will always assume that this is done, beforehand.

Now we take its minimum polynomial

$$f(Y) = \prod_{\omega \in \mu_n} (Y - \tilde{\omega}(u_1))$$

where $\tilde{\omega}$ as before sends x_1 to ωx_1 and x_2 to itself for all n-th roots of unity ω.

3.1 Main property of $f(Y)$

Clearly $F(Y) \in k << x_1^n, x_2 >>$. But we claim that it lives inside the smaller ring $k[w_1][[w_2]][Y] = A[Y]$. This will let us use our above setup and conclusions.

We will now show that the element u_1 is algebraic of degree n over the field $k << x_1^n, x_2 >>$ and is indeed integral over the ring $k[w_1][[w_2]] = k[x_1^{-n}][[x_2]]$. This will clearly establish that the $f(Y)$ is its minimum polynomial and hence in the indicated ring.

1. Since the element $u_0(0)$, obtained from $u_0 \in R[[t]]$ by setting $t = 0$ is in R and has order $-n \neq 0$, it is transcendental over k. Note that R is integral over any of its subring which contains at least one element transcendental over k, hence in particular, it is integral, and hence a finite module over $k[u_0(0)]$. Indeed, the integral closure $\overline{R}$ of R is a finite free module of rank n over the principal ideal Dedekind domain $k[u_0(0)]$.

   Given any such n-element basis for $\overline{R}$ over $k[u_0(0)]$, we claim that it serves as a generating set for $\overline{R}[[t]]$ over $k[u_0][[t]]$.

   This is simply done as follows.

   Fix a generating set $v_1, \cdots, v_n$ for $\overline{R}$ over $k[u_0(0)]$.

   Note that $u_0(0) = u_0 + tu^*$ for some $u^* \in R[[t]]$. Let R_1 be the ring $k[u_0][[t]]$. Given any element $t^m h$ in $t^m\overline{R}$ we claim that there is an element h^* in the R_1 module generated by $v_1, \cdots, v_n$, such that $t^m h = t^m h^* + t^{m+1} h^{**}$, with $h^{**} \in R[[t]]$. Thus we get the desired power series expansion for any element of $\overline{R}$ by repeated application of this process.

   To prove the claim, write $h = \sum_i h_i(u_0(0))v_i$ and take $h^* = \sum_i h_i(u_0)v_i$. Clearly $h_i(u_0(0)) - h_i(u_0) \in tR$ and the element $\sum_i h_i(u_0) - h_i(u_0(0))$ gives the desired th^{**}.

2. Thus u_1 is integral over $A = k[u_0][[t]]$ and indeed satisfies an integral equation of degree n.

   On the other hand, our polynomial $f(Y)$ must divide the integral equation and since both are monic of equal degrees, must coincide. Therefore, the coefficients of $f(Y)$ are necessarily in A as desired.

3. We thus have shown that $f(Y)$ is unibranch in the sense explained above. We now have an associated sequence $g_\lambda(Y)$ of unibranch polynomials corresponding to maximal contacts λ with $f(Y)$. If we substitute, $y = u_1$ in $g_\lambda(Y)$ we clearly get the order to be $r(\lambda) = s(\lambda)/d(\lambda)$ and so we can write:

$$g_\lambda(u_1) = g_\lambda^* t^{\pi(r(\lambda))}.$$

   Then $g_\lambda^* \in k[u_0, u_1][[t]]$ and we claim that the g_λ^* are essentially the u_i of the conjecture.

   The reason to use the word "essentially" is that in general, there will be more g_λ^* than the u_i, since the u_i only correspond to those $g_\lambda(u_1)$ for which there is a jump in the t-order.

   We next explain this in greater detail.

4 Properties of the u-sequence.

4.1 Observations about the current setup

(a) In general, the sequence $g_\lambda(Y)$ is of a large ordinal type, but for our application, it is actually a genuine sequence, i.e. of the same type as the natural numbers.

To see this, note that the sequence of the orders $r(\lambda)$ of the expressions $g_\lambda(u_1)$ has the property that $\overline{r(\lambda)} \leq 0$ for all λ in our sequence. The reason is simply that the expression $g_\lambda(u_1) \in R[[t]]$ is of the form $\sum_{i=m}^{\infty} a_i t^i$, where $a_i \in R$ and $a_m \neq 0$. Then, the order $r(\lambda) = (v(a_m), m)$, so $\overline{r(\lambda)} = v(a_m) \leq 0$ since R has v as the only valuation at infinity.

From the fact that $s(\lambda)$ forms a lexicographically increasing sequence, it is not hard to deduce that for every fixed m, there are only a finite number of λ with $\pi(r(\lambda)) = m$. This proves the claim.

(b) For our semigroup, we paid attention to only the first components $\overline{r(\lambda)}$ of the orders $r(\lambda)$ of $g_\lambda(u_1)$. Now we wish to pay attention to the t-orders as well, or the component $\pi(r(\lambda))$. In general, recall that we construct $g_{\lambda^*}(Y)$,the next polynomial from a given $g_\lambda(Y)$ by adding suitable permissible terms from $\mathcal{M}(\lambda)$ to $g_\lambda(Y)^{n(\lambda)}$ and the expected t-order of $g_{\lambda^*}(u_1)$ satisfies:

$$\text{ord}_t(g_{\lambda^*}(u_1)) \geq n(\lambda)\text{ord}_t(g_\lambda(u_1)).$$

We say that λ^* is special if the above inequality is strict.
We now construct a subsequence of our $g_\lambda(Y)$ by **keeping exactly those terms which correspond to special λ**. Let us reindex them, using an indexing function θ, as $G_1(Y), G_2(Y), \cdots$ so that $G_i(Y) = g_{\theta(i)}(Y)$.
Throw in the initial term $G_0(Y) = u_0$ and note that $G_1(Y) = Y$. We propose that our u-sequence is nothing but $G_i(u_1)$ divided by $t^{\text{ord}_t(G_i(u_1))}$ which is also seen to be given by $u_i = G_i(u_1)/t^{\pi(r(\theta(i)))}$.

(c) We now need some new notation for further calculation. In analogy with our notation $n(\lambda)$ we now need $n^*(i)$ which shall be defined as $d(\theta(i))/d(\theta(i+1))$. If $\theta(i) = \beta$ and $\theta(i+1) = \lambda$, then this is easily seen as the product of all $n(\beta^*)$ with β^* ranging from β up to (but not including) λ.

For convenience, let $\Psi : R[[t]] \longrightarrow R$ be the residue class map given by setting t to 0.

We will now show that the sequence u_i described above satisfies the conditions set in the conjecture. Clearly u_0, u_1 are correct by definition. Set $u_i^* = \Psi(u_i)$ and let K_i be the field generated by $u_0^*, \cdots, u_i^*$.

We wish to show that the minimum polynomial satisfied by u_i^* over K_{i-1} is simply read from the expression of $G_{i+1}(Y)$ as a standard expression in terms of permissible monomials in terms of the earlier $g_\beta(Y)$'s.

First, note that

$$G_{i+1}(Y) = G_i(Y)^{n^*(i)} + \text{ permissible monomials from intermediate } g_\beta(Y)$$

and when we substitute u_1 for Y, then the minimum t-order of terms on the right hand side is $n^*(i)\mathrm{ord}_t(G_i(u_1))$, but since $i+1$ corresponds to a special index, the t-order of the resulting sum is larger than this order. We substitute $Y = u_1$ on both sides and divide both sides by $t^{n^*(i)\mathrm{ord}_t(G_i(u_1))}$. After expressing terms in terms of u_i [4] and taking image of both sides by Ψ we get a monic equation of degree $n^*(i)$ satisfied by $u_i^* = \Psi(u_i)$ of the promised degree over the ring generated by $u_0^*, \cdots, u_{i-1}^*$.

On the other hand, the field degree of u_i^* over the field K_{i-1} generated by $u_0^*, \cdots, u_{i-1}^*$ cannot be any less than this $n^*(i)$ since the v-orders of all elements in K_{i-1} are divisible by $d(\theta(i))$ while the gcd of the orders drops down to $d(\theta(i+1))$, when we include the v-order of u_i.

[4] This actually involves some rearrangement of the usual permissible expression in terms of $\{g_\beta(u_1)\}$ and reinterpreting it as expression in terms of our special $G_j(u_1)$.

References

[A1] Abhyankar, S. S. *"Expansion Techniques in Algebraic Geometry",* Tata Institute of Fundamental Research, 1977.

[A3] Abhyankar, S., S. *Irreducibility criterion for germs of analytic functions of Two complex Variables.* Advances in Mathematics, 74(2), (1989), 190-257.

[AM1] Abhyankar, S.S., and Moh, T.T., *Newton-Puiseux expansion and Tschirnhausen transformation I,* J. Reine Angew. Math. 260 (1973), 47-83.

[AM2] Abhyankar, S.S., and Moh, T.T., *Newton-Puiseux expansion and Tschirnhausen transformation II,* J. Reine Angew. Math. 261 (1973), 29-54.

[DF] Daigle D. and Freudenburg G. *"..."*, ...

[S1] Sathaye,A., *Generalized Newton-Puiseux expansion and Abhyankar-Moh semigroup theorem,* Invent. math. 74(1983), 149-157.

[SS] Sathaye,A. and Stenerson J. *...*, ...