On Plane Polynomial Curves

Avinash Sathaye * Jon Stenerson

September 10, 2014

Abstract

We study some properties of generator sequences of planar semigroups and give a method of construction of plane curves with one place at infinity with given generator sequences. We also discuss similar questions for polynomial curves.

*We express our deep gratitude and appreciation for to Professor Shreeram S. Abhyankar for being a constant source of our mathematical inspiration.

1 Introduction

Abhyankar and Moh opened a new chapter in the theory of plane algebraic curves with their papers [AM1] [AM2].

To avoid unnecessary technicalities, assume that the ground field has characteristic zero and consider a plane curve C with one place at infinity. There is a semigroup $\Gamma(C)$ consisting of the set of orders of pole for various nonzero elements of the coordinate ring of C. The semigroup is a natural invariant of the defining equation (and hence of the embedding) of the curve in the plane.

Abhyankar and Moh showed that $\Gamma(C)$ is generated by a special set of generators (called a characteristic $\delta - sequence$ here) which can be computed as orders of pole of the (so-called) approximate roots of the defining equation. They also showed several important properties of the $\delta - sequence$, in particular, the semigroup is generated in a special way so that given any integer a we get a " unique standard expression " $a = \sum_0^h a_i\delta_i$ and $a \in \Gamma(C)$ if and only if $a_0 \geq 0$. (See (3.1) for details.)

Sathaye [S1] defined a semigroup generated by such sequences to be " planar " and used the properties to show that certain curves are not embeddable in a plane (even though they are embeddable in space as complete intersections); because their semigroup is not planar. The converse that a planar semigroup (in fact, any give $\delta - sequence$) comes from a plane curve was promised in [S1] but never formally published. We take this opportunity to publish it as well as some useful numerical lemmas for determining the possible generating sequences of a given semigroup. (See sections (2),(3)).

We note that the real power behind all these proofs is the "irreducibility criterion " and the concept of the "standard generation " due to Abhyankar and Moh. We especially note that in [A3] Abhyankar has given a very detailed exposition of the "irreducibilty criterion" and an exhaustive description of all plane curves with one place at infinity. We have included several references of works by Abhyankar, Moh, Richman, Russell, Sathaye and Singh related to expositions and generalizations of these concepts. We do not claim this to be exhaustive and in particular, it does not include works on problems which use the Abhyankar-Moh results.

In the last section, we present some attempts on another related question of Abhyankar. As noted above, plane curves can be constructed to represent any given $\delta - sequence$. The question asks if a *polynomial curve* i.e. a curve parametrized by polynomials in one variable, can represent a given $\delta - sequence$. Any simple counting of constants yields that there are not enough parameters to accomplish this. Indeed, Moh (with Sathaye) had calculated by hand that a polynomial curve cannot represent the sequence $(6, 8, 3)$. This example is not very satisfactory, since the semigroup is simply $(3, 8)\mathbb{N}$ and as such is realized by the curve with the parametrization (t^3, t^8). We rechecked the example with the help of a computer with the hope of extending to higher examples; so far without success. In particular, we propose the sequence $(6, 22, 17)$ as a

possible better example, since in this case, we can argue that if it is not constructible, then the semigroup is not either! (See (4)).

Abhyankar's original question was not really just about the semigroups but rather about the control on the coefficients of the Newton-Puiseux series of the curve at infinity (since this has possible applications to the Jacobian problem). We discuss a very special case of this by analyzing the length of a string of zeros past the first characteristic term. It was interesting to learn from a recent article by Lang [L] that the question as well as the answer was already discovered by the Number Theorists (in the 60's) for totally different reasons. We present a proof and discuss some unsolved problems.

2 Preliminaries and Notation

2.1 Characteristic sequences

Following [A1] 6.4 we first define various characteristic sequences.

Let $\nu \neq 0$ be a given integer and J a subset of of integers bounded below.

We inductively define an integer $h(\nu, J) = h$ and two sequences $m(\nu, J) = (m_1, \cdots, m_h)$ and $d(\nu, J) = (d_1, \cdots, d_{h+1})$ as follows:

(1) If J is empty, then $h = 0$, $d_1 = |\nu|$ and $m(\nu, J)$ is empty.

(2) If J is nonempty, set $D = \gcd(J)$ the greatest common divisor of the set J , $d_1 = |\nu|$, $m_1 = \min J$ and $d_2 = \gcd\{m_1, d_1\}$.

If $d_2 = D$, then put $h = 1$ and stop.

(3) If $d_1, \cdots, d_{r+1}$ and $m_1, \cdots, m_r$ are defined and $D = d_{r+1}$ then put $h = r$ and stop; otherwise, define

$$m_{r+1} = \min\{p \in J \mid p \not\equiv 0 \mod d_{r+1}\}$$

$$d_{r+2} = \gcd\{m_1, \cdots, m_{r+1}\} = \gcd\{d_{r+1}, m_{r+1}\}$$

Note that $D = d_{h+1}|d_h| \cdots |d_2|d_1$.

Some natural expressions in these numbers are also useful to define.

(1) $q_1 = m_1$ and $q_i = m_i - m_{i-1}$ for $i = 2, \cdots, h$

For convenience, we also set $q_{h+1} = m_{h+1} = \infty$.

(2) $s_i = \sum_1^i q_j d_j$ for $i = 1, \cdots, h$

(3) $r_i = s_i/d_i$ and $\delta_i = -r_i$ for $i = 1, \cdots, h$

(4) $n_i = d_i/d_{i+1}$ for $i = 1, \cdots, h$

Note that all the numbers defined here depend on ν, J and should indeed be written as $h(\nu, J), m_i(\nu, J)$, $q_i(\nu, J)$ etc. We may invoke such detailed notations if necessary.

If $u(\tau) \in k((\tau))$ is a meromorphic power series in τ, then we define, for any given integer n, the characteristic sequences of $u(\tau)$ by setting

$$J = \text{ Supp } u(\tau) = \{r \mid \text{ coefficient of } \tau^r \text{ in } u(\tau) \text{ is nonzero } \}$$

Thus $m(\nu, u(\tau)) = m(\nu, J)$ etc. [1]

Further, if $f = f(X, Y)$ is a polynomial such that

$$f(\tau^{-n}, Y) \ = \ \prod_{\omega^n=1} (Y - u(\omega\tau))$$

where n is the $Y-$degree of $f(X, Y)$ then all the power series $u(\omega\tau)$ have the same support and we simply set $m(f) = m(-n, u(\tau))$ etc. In words, we will describe this by saying that the curve defined by f has $h = h(f)$ characteristic terms $m(f) = (m_1(f), \cdots, m_h(f))$ etc. Curves defined by such polynomials are the so-called curves with one place at infinity (at least when $n \not\equiv 0 \mod \text{ char } k$) and we discuss them next.

2.2 Curves with one place at infinity

First we fix some notation. Let k be the ground field, assumed algebraically closed unless otherwise stated. The characteristic char k is either assumed to be 0 or is not allowed to divide certain degrees in case it is nonzero. Let $f = f(X, Y)$ be an irreducible polynomial and let C denote the corresponding (irreducible) curve defined by the ideal (f). Let $A = k[X, Y]/(f)$ be the coordinate ring of C and let "$\leftharpoonup$" denote the corresponding residue class map. Let $K = \text{ qt } A$ be the function field of C.

To avoid making repeated exceptions, we assume forever that $f \notin k[X]$. It is clear that a simple change of variables will accomplish this change and there is no loss of generality.

Recall that the curve C *has one place at infinity* if *there is a unique valuation ring* V *of* K/k *not containing* A . [2] Let v denote the valuation associated with V.

For nonzero elements h of A we define

$$\deg_v h = -v(h).$$

If $h = 0$ then we may extend this by $\deg_v 0 = -\infty$.

[1] In particular we will need $s_h(-n, u(\tau)) = \Sigma_0^h q_i d_i$ where $q_i d_i$ is obtained by setting $\nu = -n$, $J =$ Supp $u(\tau)$.

[2] If k is not algebraically closed then we also need to assume that V is residually rational over k.

If the curve is a plane curve defined by say $f = f(X,Y) = 0$, then we extend this concept of degree to polynomials $h(X,Y)$ by

$$\deg_v h(X,Y) = \deg_v \bar{h}$$

where $\bar{h}$ is the image of $h(X,Y)$ modulo $f(X,Y)$.

We will drop reference to v if it is clear from the context. We will also write $deg(h,f)$ in place of $\deg_v h$ if we wish to mention f and not v.

For a curve C with one place at infinity we get a value semigroup

$$\Gamma(C) = \Gamma(A) = \{deg_v\ h \mid 0 \neq h \in A\}.$$

It is well known that to test whether the given curve has "one place at infinity" one can also check that f is irreducible as an element of $k((X^{-1}))[Y]$. (The assumption that $f \notin k[X]$ is used here!)

One of the main deductions from the Abhyankar-Moh theory is a very efficient algorithm for testing this irreducibility, without developing the full power-series factorization. Unfortunately, their method only works when the $Y-$degree of f is not divisible by char k; in particular, it works in characteristic zero.

Irreducibility Criterion of Abhyankar and Moh *Assume that* $n = \deg_Y f(X,Y) \not\equiv 0 \mod \text{char } k$ *and* $f(X,Y)$ *is monic in* Y. *Then* $f(X,Y)$ *has one place at infinity iff there is a "test series"* $u(\tau) \in k((\tau))$ *such that*

$$\text{ord}_\tau\ f(\tau^{-n}, u(\tau)) > s_h(-n, u(\tau))$$

Moreover, given any series passing this test, there is a "root" $y(\tau)$ (usually called the Newton-Puiseux series of f) satisfying:

$$f(\tau^{-n}, y(\tau)) = 0$$
$$\text{ord}_\tau\ (y(\tau) - u(\tau)) > m_h(-n, u(\tau))$$

Conceptually, this says that if we have a guess $u(\tau)$ which describes the full initial piece of an expected root thru the last characteristic term, then its correctness as well the irreducibility of f can be verified simply by substituting it in f and comparing the order against numbers intrinsically computed from the guess itself! Indeed, this test can be generalized to build the test series $u(\tau)$ itself term by term and is a sharpened version of the original "Newton's algorithm" for the special case of one place. For a very detailed exposition of the irreducibility criterion see [A3]

Moreover, whenever f has a Newton-Puiseux series as described, one gets a factorization as described above, namely:

$$f(\tau^{-n}, Y) = \prod_{\omega^n=1} (Y - y(\omega\tau))$$

and we can talk about the various characteristic sequences associated with f itself as discussed in the previous section.

2.3 The $g-sequence$

A sequence of polynomials $g_0, g_1, \cdots, g_{h+1}$ in $k[X,Y]$ is said to be a $g-sequence$ if the following holds:

(1) $g_0 = X, g_1, \cdots, g_{h+1}$ are monic in Y with one place at infinity.

(2) $\deg_Y\ g_{h+1} = n \not\equiv 0 \mod \text{char } k$. Moreover, g_{h+1} has exactly h characteristic terms. Let us write m_i for the i^{th} characteristic term $m_i(g_{h+1})$ and similarly for all the other sequences associated with g_{h+1}. With this notation we require that $\deg_Y\ g_i = \frac{n}{d_i}$.

(3) There exist Newton-Puiseux series $y_i(\tau)$ for $g_i,\ 1 \le i \le h+1$ such that $\text{ord}_\tau\ y_{h+1}(\tau) - y_i(\tau^{d_i}) = m_i$ for $1 \le i \le h$. We shall denote $y_{h+1}(\tau)$ simply by $y(\tau)$.

It is easy to see that every subsequence of a $g-sequence$ is a $g-sequence$ again. In particular, $m_j(g_i) = \frac{m_j}{d_i}$ for $j \le i \le h$. Similarly, we also get, $d_j(g_i) = \frac{d_j}{d_i}$ for $j \le i \le h$. Finally, for $j \le i \le h$ we get :

$$s_j(g_i) = \frac{s_j}{d_i^2}\ ,\ r_j(g_i) = \frac{r_j}{d_i^2} \text{ and } \delta_j(g_i) = \frac{\delta_j}{d_i^2}.$$

2.4 Substitution Formulas

We assume all the notation of the previous section and consider the Newton-Puiseux series

$$y(\tau) = \alpha_1\tau^{m_1} + \cdots + \alpha_i\tau^{m_i} + \cdots + \alpha_h\tau^{m_h} + \cdots + \beta\tau^{m_i+q} + \cdots$$

where we have identified the characteristic terms and one extra term past the last characteristic term. Let a test series $u(\tau)$ be defined by $u(\tau) - y(\tau) = (Z-\beta)\tau^{m_i+q} + \cdots$ higher terms . By an easy but tedious calculation we get the following results :

$$\begin{array}{lcll} g_i(\tau^{-nd}, u(\tau)) & = & \beta_i'\tau^{d(r_i)} + \cdots \text{ higher terms} & \text{for } 1 \le i \le h \\ & = & \beta_i'\tau^{-d(\delta_i)} + \cdots \text{ higher terms} & \text{for } 1 \le i \le h \\ g_{h+1}(\tau^{-nd}, u(\tau)) & = & (Z-\beta)\beta_{h+1}'\tau^{ds_h+q} + \cdots \text{ higher terms} & \\ & = & (Z-\beta)\beta_h'\tau^{-d_h\delta_h+q} + \cdots \text{ higher terms} & \end{array}$$

Here, β_i' depends only on the coefficients $\alpha_1, \cdots, \alpha_i$ for $1 \le i \le h$ are nonzero elements of k. See [A1] 12 or [A2] 3.4.

2.5 A Lemma on $Y-$degrees

In this section we prove a useful fact about a $g-$ *sequence*.

Degrees of monomials in a $g-$*sequence Let* $g_0 = X, g_1, \cdots, g_{h+1}$ *be a* $g-$*sequence and assume all the notation introduced in the definition above. Let*

$$g* = \prod_0^h g_i^{p_i} \text{ where } 0 \leq p_i \leq n_i - 1 \text{ for } i \geq 1.$$

Then $\deg_Y g* < \deg_Y g_{h+1} = n$.

Proof. Induction on h. If $h = 0$ there is nothing to prove! Now let $h > 0$. Applying the induction hypothesis to $g_0, \cdots, g_h$, we get that

$$\deg_Y \prod_0^{h-1} g_i^{p_i} = \sum_0^{h-1} p_i \frac{n}{d_i} < \deg_Y g_h = \frac{n}{d_h}$$

Hence

$$\begin{aligned} \deg_Y g* &< \frac{n}{d_h} + p_h \deg_Y g_h \\ &\leq \frac{n}{d_h} + (d_h - 1)\frac{n}{d_h} \\ &= n = \deg_Y g_{h+1} \end{aligned}$$

3 Semigroups of Curves with One Place at Infinity

3.1 Planar semigroups

A sequence of positive integers $(\delta_0, \cdots, \delta_h)$ is said to be **a characteristic** $\delta - sequence$ if it satisfies the following three axioms:

(1) Set $d_i = \gcd\{\delta_0, \cdots, \delta_{i-1}\}$ for $1 \leq i \leq h+1$. Set $n_i = \frac{d_i}{d_{i+1}}$ for $1 \leq i \leq h$. Then $d_{h+1} = 1$ and $n_i > 1$ for all $i \geq 2$.

(2) $\delta_i n_i \in \{\delta_0, \cdots, \delta_{i-1}\}\mathbb{N}$ = the semigroup generated by $\{\delta_0, \cdots, \delta_{i-1}\}$.

(3) $\delta_i < \delta_{i-1} n_{i-1}$ for $i \geq 2$. Set $\delta_i = \delta_{i-1} n_{i-1} - q_i$, so that $q_i > 0$ for $i \geq 2$.

A pair of integers is said to be **nonprincipal** if neither of them divides the other. We say that the $\delta - sequence$ $\{\delta_0, \cdots, \delta_h\}$ is **nonprincipal** if δ_0, δ_1 is nonprincipal.

An element of a semigroup will be called **primitive** if it is not a sum of two nonzero elements of the semigroup.

A semigroup generated by a characteristic $\delta - sequence$ is said to be **a planar semigroup.**

The motivation for the definition comes from the Abhyankar-Moh theory which shows that the semigroup of a plane curve with one place at infinity is planar provided the defining equation is monic in Y of degree nondivisible by char k. In fact, in the next section we will show the converse of this! Let us remark that the condition on $Y-$degree is essential. Indeed in char $k = 3$, the semigroup of the rational curve parametrized by $x \mapsto t^9$ and $y \mapsto t^{12} + t^5$ can be calculated to be generated by $\{9, 12, 15, 17, 20, 23, 25, 28\}$ and we will show later in this section that this semigroup is not planar!

In this section, we deduce some purely numerical properties of a planar semigroup which help in determining the planarity of a given semigroup and in determining all possible generator characteristic $\delta - sequences$ for it.

Now let $\Gamma = \{\delta_0, \cdots, \delta_h\}\mathbb{N}$ be a planar semigroup.

(1) Layers of a planar semigroup For a fixed i with $1 \leq i \leq h$, set $\delta'_j = \frac{\delta_j}{d_{i+1}}$.

The semigroup

$$\Gamma_i = \{\delta'_0, \cdots, \delta'_i\}\mathbb{N}$$

is also a planar semigroup for all i from 1 to h generated by the characteristic $\delta - sequence$ $\{\delta'_0, \cdots, \delta'_i\}$. We may call Γ_i the i^th layer of $\Gamma = \Gamma_h$.

(2) Standard Generation Every integer a has a unique expression

$$a = \sum_0^h a_i \delta_i \text{ where } 0 \leq a_i \leq n_i - 1 \text{ for } i \geq 1.$$

Moreover, $a \in \Gamma$ if and only if $a_0 \geq 0$. This kind of expression will be termed the standard expansion of a with respect to the $\delta - sequence$.

(3) The Conductor formula Set

$$c(\Gamma) = 1 - \delta_0 + \sum_0^h (n_i - 1)\delta_i$$

Then we have that $\alpha + \beta = c(\Gamma) - 1$ if and only if exactly one of α , β belongs to Γ. Consequently, $c(\Gamma)$ is the smallest element of Γ such that all integers bigger than or equal to it are in Γ.

(4) Bounds on the generator sequence If the sequence is nonprincipal, then $\max(\delta_0, \delta_1) \leq c(\Gamma) + 1$ and $\delta_i \leq c(\Gamma) - 1$ for all $2 \leq i \leq h$.

(5) Primitivity of Generators Every primitive element of Γ is one of the δ_j and conversely, every δ_j is either primitive or a multiple of some δ_r where either $r > j$ or $\delta_j = \delta_1$ and $\delta_r = \delta_0$.

(6) Prime Numbers in a Planar Semigroup There is at most one primitive prime number in Γ, unless Γ is generated by two primes. In particular, a semigroup containing two or more primitive prime numbers and not generated by them is not planar.

Proof of (1) We fix i and call the corresponding semigroup Γ'. All quantities associated with Γ' will be also denoted by primes of similar quantities of Γ. Then we note that $d'_j = \frac{d_j}{d_{i+1}}$ for $1 \leq j \leq i$. Consequently, $n'_j = n_j$ for $1 \leq j \leq i$ and $h' = i$.

Now all the conditions for a planar semigroup are easily checked by comparing with those of Γ.

Proof of (2) Note that the $\gcd\{\delta_0, \cdots, \delta_h\} = d_{h+1} = 1$ and hence we can write $a = \sum_0^h b_i\delta_i$ for some integers b_i. We now claim that we can assume, without loss of generality that:

$$b_i \geq 0 \text{ for } i \geq 1.$$

To see this, change b_i to $b_i + \lambda_i\delta_0$ for $i \geq 1$ and simultaneously change b_0 to $b_0 - \sum_0^h \lambda_i\delta_i$, then we can arrange that required condition by taking λ_i large enough.

Now we assume that a has been "standardized" past j , i.e.

$$a = \sum_0^j b_{i,j}\delta_i + \sum_{j+1}^h a_p\delta_p$$

where $0 \leq a_p \leq n_p - 1$ and $b_{i,j} > 0$ for $1 \leq i \leq j$. We now prove that the **standardization can then be improved** to $j-1$ such that:

$$a = \sum_0^{j-1} b_{i,(j-1)}\delta_i + \sum_j^h a_p\delta_p$$

where $0 \leq a_j \leq n_j - 1$ and $b_i^{j-1} \geq b_i^j$ for $0 \leq i \leq j-1$.

To see this, write $b_j = un_j + a_j$, with $0 \leq a_j \leq n_j - 1$ using the division algorithm. Also, we have $n_j\delta_j = \sum_0^{j-1} u_i\delta_i$ with $u_i \geq 0$ as guaranteed by the planarity condition. Then setting $b_{i,(j-1)} = b_{i,j} + uu_i$ for $0 \leq i \leq j-1$ gives the required improvement!

Continuing this improvement, we get the desired standard expression. Now we prove uniqueness. If possible, take two distinct standard expressions $a = \sum_0^h a_i\delta_i = \sum_0^h a_i'\delta_i$, then subtracting one from the other, we get

$$0 = \sum_0^j (a_i - a_i')\delta_i$$

where we assume that $(a_j - a_j')$ is the last nonzero term. Clearly, all the earlier terms are divisible by $\gcd\{\delta_0, \cdots, \delta_{j-1}\} = d_j$ and hence we have $d_j | (a_j - a_j')\delta_j$. But clearly, $d_{j+1} = \gcd\{\delta_j, d_j\}$ and hence $n_j = \dfrac{d_j}{d_{j+1}}$ divides $(a_j - a_j')$. Since we have already arranged that $0 \leq a_j, a_j' \leq n_j - 1$, we get $0 < |a_j - a_j'| < n_j$; a contradiction!

Now for the last remark, note that if $a_0 \geq 0$ then clearly $a \in \Gamma$. Conversely, if $a = \sum_0^h b_i\delta_i$ is any expression for an element a with $b_i \geq 0$ for all $0 \leq i \leq h$, then we can apply the improvement process as described above to get a standard expression $a = \sum_0^h a_i\delta_i$. Now we note that $a_0 \geq b_0$ since the coefficient of δ_0 never decreases during the improvement stages. Hence $a_0 \geq 0$ as required.

Proof of (3) Write

$$\alpha = \sum_0^h a_i\delta_i \text{ where } 0 \leq a_i \leq n_i - 1 \text{ for } 1 \leq i \leq h.$$

If $\alpha + \beta = c(\Gamma) - 1$, then we have

$$\beta = (-1 - a_0)\delta_0 + \sum_0^h (n_i - 1 - a_i)\delta_i.$$

This is evidently a standard expression. By the standardness of both the expressions, we get that

$$\begin{aligned} \alpha \in \Gamma &\iff a_0 \geq 0 \\ \beta \in \Gamma &\iff (-1 - a_0) \geq 0 \end{aligned}$$

Clearly, exactly one of the above two conditions is always satisfied and hence exactly one of α, β belong to Γ.

For the last remark, note that $(c(\Gamma)+\nu)+(-\nu-1) = c(\Gamma)-1$ and hence, if $\nu \geq 0$, then $(-\nu-1) \notin \Gamma$ and hence $(c(\Gamma)+\nu) \in \Gamma$ for all $\nu \geq 0$. On the other hand, since $0 \in \Gamma$ we have $c(\Gamma)-1 \notin \Gamma$ and hence $c(\Gamma)$ is the smallest integer such that all integers bigger than or equal to it are in Γ.

Proof of (4) We note that

$$c(\Gamma) - 1 > \sum_{2}^{h} (n_i - 1)\delta_i$$

since the difference of the two sides is:

$$\begin{aligned} &= -\delta_0 + (n_1 - 1)\delta_1 \\ &= -\delta_0 + \frac{\delta_0\delta_1}{d_2} - \delta_1 \\ &= d_2((\frac{\delta_0}{d_2} - 1)(\frac{\delta_1}{d_2} - 1) - 1) \\ &> 0 \end{aligned}$$

The last step follows from the nonprincipality which guarantees that each of the ratios $\frac{\delta_0}{d_2}, \frac{\delta_1}{d_2}$ is bigger than 1.

Also, $n_i > 1$ for all $i \geq 2$ and hence we get

$$\delta_i < \frac{c(\Gamma)-1}{n_i - 1} \leq c(\Gamma) - 1 \text{ for all } 2 \leq i \leq h \tag{1}$$

Now we may assume without loss of generality, that $\delta_0 > \delta_1$ and show that $c(\Gamma)+1 \geq \delta_0$.

We prove this by induction on h. If $h = 0$, then $c(\Gamma) = 0$ and we are done.

For convenience, set $c_i = c(\Gamma_i)$ for $0 \leq i \leq h$.

By the induction hypothesis applied to Γ_{h-1} we get that

$$\frac{\delta_0}{d_h} \leq c_{h-1} + 1$$

Also the conductor formula gives

$$\begin{aligned} c(\Gamma) = c_h &= (c_{h-1} - 1)d_h + (n_h - 1)\delta_h + 1 \\ &= (c_{h-1} + 1)d_h + (d_h - 1)\delta_h - 2d_h + 1 \end{aligned}$$

Thus we get

$$c(\Gamma) + 1 = (c_{h-1} + 1)d_h + (d_h - 1)(\delta_h - 2) \geq \delta_0 + (d_h - 1) + (d_h - 1)(\delta_h - 2).$$

The result is now obvious if $\delta_h \geq 2$. Now we show that under the assumption of nonprincipality, $\delta_h = 1 \Longrightarrow h = 0$; thus completing the proof.

If $\delta_h = 1$, then $1 \in \Gamma$ and hence Γ contains all nonnegative integers. Clearly, $c(\Gamma) = 0$. Then $h \leq 1$ since otherwise we get a contradiction from (1): $\delta_i < c(\Gamma) - 1 = -1$ for $2 \leq i \leq h$.

If $h = 1$ and $c(\Gamma) = -1 + \delta_0 + (n_1 - 1)\delta_1 = 0$, then clearly we have a contradiction unless $n_1 = 1 = \delta_0$. Also, $n_1 = 1$ implies $\delta_1 | \delta_0$ in contradiction to nonprincipality. Thus, $h = 0$ and we are done.

Proof of (5) It is clear that a primitive element of a semigroup belongs to any generating set and hence to $\{\delta_0, \cdots, \delta_h\}$.

Conversely, let δ_j be nonprimitive. If $n_1 = 1$, then δ_1 is not its own standard expression as in (1) but then $\delta_1 = n_1\delta_1$ is a multiple of δ_0 and we are done.

Now assume that δ_j is non-primitive and is its own standard expression (i.e. $n_j > 1$). Let

$$\begin{array}{cc} \delta_j = a + b & \\ \text{where} & 0 \neq a = \sum_0^h a_i\delta_i \in \Gamma \\ \text{and} & 0 \neq b = \sum_0^h b_i\delta_i \in \Gamma \end{array}$$

are standard expressions.

We claim that the expression $\delta_j = \sum_0^h (a_i + b_i)\delta_i$ is not standard, since otherwise, by uniqueness of standard expressions we will get $a = a_j\delta_j$, $b = b_j\delta_j$ and again by uniqueness one of a, b is zero, a contradiction!

Now we start the modification process for the expression of δ_j as described in (1). Let the situation just before the end of the modification process be

$$\delta_j = \sum_0^r (a_i + b_i + v_i)\delta_i \text{ where } a_r + b_r + v_r \neq 0 \text{ and } v_i \geq 0 \text{ for } 1 \leq i \leq r$$

Here v_i are the improvements caused by the previous steps. Now the right hand side of this expression is non-standard and hence $r > 0$. We claim that $r \geq j + 1$. In fact, if r were less than j, then the right hand side will improve to a standard expression in $\{\delta_0, \cdots, \delta_{j-1}\}$, in contradiction to the uniqeuness.

The remaining improvement step must come from:

$$(*) \qquad \begin{array}{ccc} a_r + b_r + v_r & = & un_r \\ & \text{and} & \\ n_r\delta_r & = & \sum_0^{r-1} p_i\delta_i \end{array}$$

Finally, in the equation

$$\delta_j = \sum_0^{r-1} (a_i + b_i + v_i + up_i)\delta_i$$

all the corresponding coefficients of δ_i must match. Since all a_i, b_i, v_i, u, p_i are nonnegative, we see that

$$up_i = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

Thus, $u = p_j = 1, p_i = 0$ for $i \neq j$ and from $(*)$ above, we get

$$n_r \delta_r = \delta_j$$

as claimed. **Proof of (6)** Let a, b be two primitive prime numbers in Γ. By what we just proved, $a = \delta_i$ and $b = \delta_j$ for some i, j and we assume that $i < j$ without loss of generality. If $(i, j) = (0, 1)$ then we are done. Note that $d_{i+1} = 1$ or a and $d_{j+1} = 1$. Thus, $j = h$. If $d_{i+1} = a$, then Γ_i contains $\frac{\delta_i}{d_{i+1}} = \frac{a}{a} = 1$ and hence the semigroup generated by $\delta_0, \cdots, \delta_i = a\Gamma_i = a\mathbb{N}$ and we can change the generator sequence by simply dropping $\delta_0, \cdots, \delta_{i-1}$. Thus, we may assume that $a = \delta_0$ and $d_1 = a$. Now, if $d_2 = a$, then we get $a|\delta_1$ and again, we may drop δ_1 without loss of generality. Thus, we have $d_2 = 1$ and hence $h = 1$, so $j = 1$ and we are done!

Corollary *The semigroup* $\Gamma = \{9, 12, 15, 17, 20, 23, 25, 28\}$ *described earlier is not planar and hence degree-semigroups of plane curves with one place at infinity are not necessarily planar in positive characteristic.*

For proof, note that $17, 23$ are prime and primitive in Γ and do not generate it.

3.2 Characterization of Planar Semigroups

Recall that a semigroup Γ of nonnegative integers is said to be a planar semigroup if it is generated by a characteristic $\delta - sequence$ $(\delta_0, \cdots, \delta_h)$

As remarked earlier, the Abhyankar-Moh semigroup theorem is the motivation behind this definition, since it says:

Abhyankar-Moh Semigroup Theorem *Let f have one place at infinity. Assume that $n = \deg_Y f(X, Y) \not\equiv 0 \mod \text{char } k$. Then its semigroup is planar. Moreover, there is an associated $g-$sequence $(X = g_0, \cdots, g_h, g_{h+1} = f)$ such that the corresponding degree $-$ sequence $(\delta_0 = deg(g_0, f), \cdots, \delta_h = deg(g_h, f))$ is a characteristic $\delta -$ sequence and generates the degree semigroup of f. Furthermore, the images modulo (f) of the "standard monomials" in $(g_0, \cdots, g_h)$ form a $k-$vector space basis of A, the coordinate ring of f such that distinct standard monomials have distinct induced degrees in the degree semigroup Γ. In other words Γ is simply the set of degrees of standard monomials.* In this section, we prove the converse of this, namely,

Theorem *Let $(\delta_0, \cdots, \delta_h)$ be a characteristic $\delta-$sequence such that $\delta_0 \not\equiv 0 \mod \text{char } k$ Then there exists a curve f with one place at infinity whose degree semigroup is generated by $(\delta_0, \cdots, \delta_h)$. Moreover, there is a $g -$ sequence $(g_0, \cdots, g_h, g_{h+1})$ such that $f = g_{h+1}$ and $\delta_i = deg(g_i, f)$ for $0 \leq i \leq h$. Furthermore, $\deg_Y f = \delta_0$*

Proof. Induction on h. For $h = 0$, we have $\delta_0 = 1$ and we simply take $g_0 = X$, $g_1 = Y$ to get the desired result.

Now let $h > 0$. Set $\delta'_i = \frac{\delta_i}{d_h}$ for $i = 1, \cdots, h-1$. Set the corresponding $d - sequence$ equal to $d'_0 = \frac{d_0}{d_h}, \cdots, d'_{h-1} = \frac{d_{h-1}}{d_h}, d'_h = 1$. Other characteristic sequences are defined similarly. Then $(\delta'_0, \cdots, \delta'_{h-1})$ clearly satisfies the induction hypothesis and we get a $g - sequence$ $(X = g_0, \cdots, g_h)$ such that $deg(g_i, g_h) = \delta'_i$ for $i = 0, \cdots, h-1$. By the definition of a $\delta - sequence$ we have:

$$\delta_h = \sum_0^{h-1} p_i \delta'_i \quad \text{and} \quad \delta_h = \delta_{h-1} n_{h-1} - q_h$$

where the expression for δ_h is standard (i.e. $p_0 \geq 0$ and $0 \leq p_i \leq n_i - 1$ for $1 \leq i \leq h-1$). Moreover, $q_h > 0$.

Let c and z be elements of k to be determined later. Set:

$$g_{h+1} \ = \ g_h^{d_h} + cg* \text{ where } g* \ = \ \prod_0^{h-1} g_i^{p_i}$$

Also set $u(\tau) = y_h(\tau^{d_h}) + z\tau^{m_h}$ where y_h is a "Newton-Puiseux series" of g_h, thus,

$$g_h(\tau^{-\delta'_0}, y_h(\tau)) = 0.$$

It follows that

$$g_h(\tau^{-\delta_0}, y_h(\tau^{d_h})) = 0.$$

Note that $\delta_0, \cdots, \delta_h$ is now the $\delta - sequence$ associated with the series $u(\tau)$. Hence note that $s_h(-\delta_0, u(\tau)) = -d_h \delta_h$.

Now we calculate $f(\tau^{-\delta_0}, u(\tau))$.

For convenience, set $\Phi(G(X,Y)) = G(\tau^{\delta_0}, u(\tau))$ for any polynomial $G(X,Y)$. Then by calculations in (2.4) applied to the $g - sequence$ $g_0, \cdots, g_h$ we get:

$$\Phi(g_h) = (za_h)\tau^{-d_h d'_{h-1} \delta'_{h-1} + q_h} + \cdots \text{ higher terms}$$

and

$$\Phi(g_i) = a_i \tau^{-d_h \delta'_i} + \cdots \text{ higher terms}$$

Observe that

$$-d_h d'_{h-1} \delta'_{h-1} + q_h = -d'_{h-1} \delta_{h-1} + q_h = -n_{h-1} \delta_{h-1} + q_h = -\delta_h.$$

Therefore we get:

$$\begin{aligned}\Phi(g_h^{d_h}) &= (za_h)^{d_h}\tau^{-d_h\delta_h} + \cdots \text{ higher terms}\\ \Phi(cg*) &= c(\textstyle\prod_0^{h-1} a_i^{p_i})\tau^{\sum_0^{h-1} -\delta_i p_i} + \cdots \text{ higher terms}\\ &= c(\textstyle\prod_0^{h-1} a_i^{p_i})\tau^{-d_h\delta_h} + \cdots \text{ higher terms}\end{aligned}$$

Here, the constants a_i depend only on the coefficients of the characteristic terms of $y_h(\tau)$ and hence not on z or c.

Now we choose nonzero c and z such that

$$(za_h)^{d_h} + c\prod_0^{h-1} a_i^{p_i} = 0.$$

It follows that $\operatorname{ord}_\tau \Phi(f) > s_h(-\delta_0, u(\tau)) = -d_h\delta_h$. Also, we note that $\deg_Y f = d_h \deg_Y g_h = d_h\delta_0' = \delta_0$ since the $Y-$degree of $g*$ is smaller (See (2.5)). Finally, f has one place at infinity by the Irreducibility criterion. Further, the corresponding Newton-Puiseux series $y(\tau)$ of f coincides with $u(\tau)$ thru the h^{th} characteristic term m_h and hence $\operatorname{ord}_\tau g_i(-\delta_0, y(\tau)) = \operatorname{ord}_\tau g_i(-\delta_0, u(\tau)) = -\delta_i$ and we have the complete $g-$*sequence* $X = 0, g_1, \cdots, g_h, g_{h+1} = f$ as desired. The degree-semigroup $\Gamma(f)$ is also generated by the full $\delta-$*sequence* $\delta_0, \cdots, \delta_h$.

4 Degree Semigroups of Polynomial Curves.

A polynomial curve is one with a parametrization $x = x(t)$, $y = y(t)$, where $x(t)$ and $y(t)$ are polynomials over k. Any rational curve with one place at infinity is a polynomial curve. In this section we shall assume that $\text{char } k = 0$. We discuss the following questions raised by Abhyankar: **Question 1.**

Let Γ be a planar semigroup. Is Γ the semigroup of a polynomial curve?

Question 2. Let $(\delta_0, \ldots, \delta_{h+1})$ be a characteristic δ-sequence for Γ. Let f be a polynomial curve such that $\Gamma(f) = \Gamma$. Is there a g-sequence $(g_0, \ldots, g_{h+1})$ with $f = g_{h+1}$ and $\delta_i = \deg(g_i, f)$ for $0 \leq i \leq h$? (Note: for a polynomial curve $\deg(g_i, f) = \deg_t(g_i(x(t), y(t)))$.

We shall see that the answer to Question 2 is "no". We don't have an answer to Question 1 yet.

As noted in the introduction, Moh [Mo6] observed the following: If $x(t)$ and $y(t)$ are polynomials of degrees 6 and 8 respectively, and $F(X, Y)$ is a polynomial then the Abhyankar-Moh theory plus a calculation shows that $F(x, y)$ cannot have degree 3. (Since [Mo6] didn't actually display the calculation we recently rechecked it hoping that advances in either theory or computer software would make it more amenable to exposition. It is still messy and we will not present the calculation here either.) Hence there is no polynomial curve with characteristic δ-sequence (6,8,3). Of course, the semigroup generated by (6,8,3) is $(3, 8)\mathbb{N}$ which is the semigroup of a polynomial curve, namely $f = X^8 - Y^3$ parametrized by $x = t^3$, $y = t^8$. Therefore the answer to Question 2 is no.

We suspect that the semigroup Γ generated by the characteristic sequence $(6, 22, 17)$ may lead to a negative answer to Question 1. First of all, this semigroup has no other characteristic δ-sequence generating it (other than (22,6,17)). To see this, observe that 6, 22, and 17 are primitive elements of Γ and so by property (5) of section 3.1 they occur in any characteristic δ-sequence for Γ. We now consider various possibilities for the order of 6, 22, and 17 within a characteristic δ-sequence. If either 6 or 22 appears before 17 then upon reaching 17 the sequence has gcd 1 and must end there. So in that case 17 is the last element of the sequence. The other case, where 6 and 22 follow 17, is impossible. For upon reaching either 6 or 22 the gcd drops to 1 and the sequence terminates before reaching the other. Thus we see that 17 is last number in any characteristic δ-sequence for Γ. Then consider two possibilities: the 6 comes before the 22, or the 22 comes before the 6.

In the first case the sequence looks like $(\ldots, 6, \ldots, 22, \ldots, 17)$. Upon reaching the 6 the gcd so far must either be 6,3, or 2. It cannot be 3 for then the gcd drops to 1 upon reaching the 22 and the sequence would end there. It cannot be 2 for then the gcd would not drop upon reaching 22. Therefore it is 6 and 6 is the first term of the sequence (since the sequence is nonprincipal). The next term in the sequence drops the gcd to either 3 or 2. Again it cannot be 3 or the sequence would end too soon. Therefore it is 2. It follows

that the term after the 6 must be 22. The next term must drop the gcd to 1. Therefore it has to be 17. Thus we are reduced to (6,22,17).

In the second case the sequence looks like $(\ldots, 22, \ldots, 6, \ldots, 17)$. As in the last paragraph, the only possibility is that the sequence is (22,6,17).

We thus see that this semigroup has the nice property of having an essentially unique generating characteristic δ-sequence. Now we use the **Lemma.** Let C be a plane polynomial curve and let $\Gamma(C)$ have characteristic δ-sequence (m, n, δ_2). Let $d = d_2 = \gcd(m, n)$, $m' = m/d$, $n' = n/d$. Then there is a corresponding g-sequence (X, Y, g_2) where g_2 is a polynomial of the form

$$g_2(X, Y) = X^{n'} - Y^{m'} + \Sigma a_{ij} X^i Y^j.$$

The sum is over all (i, j) such that $im+jn < mn/d$. Furthermore, there exist polynomials $x(t)$ and $y(t)$ of degrees m and n such that $g_2(x(t), y(t))$ has t-degree δ_2.
Proof. That g_2 has the given form follows from [A1] section 8. The rest follows from Section 3 of this paper. ∎

Therefore let $x(t)$ be a polynomial of degree 6, and $y(t)$ be a polynomial of degree 22. If we can show that $\deg_t g_2(x, y) > 17$ for any polynomial $g_2(X, Y)$ of the above form, it will follow that there is no polynomial curve with degree semigroup $(6, 22, 17)\mathbb{N}$.

Why do we think that $\deg_t g_2(x, y)$ must be more than 17? The idea is that by careful counting we have 22 free variables and 23 equations (presumably independent). Take generic x and y of the appropriate degrees, say $x = t^{22} + a_1 t^{21} + \cdots + a_{22}$, and $y = t^6 + b_1 t^5 + \cdots + b_6$. Our variables are the coefficients of x and of y. There are initially 28. By an automorphism of $k[X, Y]$, $X \mapsto X + p_1 Y^3 + p_2 Y^2 + p_3 Y + p_4$, $Y \mapsto Y + p_5$, we may remove 5 variables. By an automorphism of $k[t]$, $t \mapsto t + p_6$, we remove one more. This leaves 22 free variables.

Our equations are obtained by setting to zero the formal coefficients of t in $g_2(x, y)$. We begin with the coefficient of t^{65} and set it equal to zero and solve for one of the variables (e.g. a_1). The next equation comes from the term is t^{64}. This equation can be ignored since 64 is in the (6,22) semigroup anyway and we can remove the t^{64} term by adding to g_2 a multiple of XY^7. Continue in this manner. All terms whose t-degree are in the (6,22) semigroup may be ignored. The Abhyankar-Moh theory also tells us that no other number divisible by $2 = \gcd(6, 22)$ can occur as the degree of the leading term of any $g_2(x, y)$: when you leave the (6,22) semigroup, you must leave the (6,22) ideal. Therefore, we need only solve equations coming from terms of odd degree between 65 and 19 (we want to leave the degree 17 term non-zero). In fact, there is no possible degree 19 term to worry about either, for 19 is not in the (3,11) semigroup. Thus we have a total of 23 equations!

Since these equations have no apparent dependence we suspect they may have no solution. This remains to be checked.

As a starting point for developing a general theory of the above sort of calculation we analyzed the case where we fix $F(X,Y) = X^m - Y^n$, since this is the simplest polynomial such that the degree of $F(x,y)$ is not completely predictable from the degrees of x and y. What is a lower bound on the t-degree of $F(X,Y)$? While we asked and answered this question it turned out that we were not the first.[3]

Theorem 1.

Let x and y be nonconstant polynomials in $k[t]$. If $x^m - y^n$ is not identically zero, then

$$\deg_t (x^m - y^n) \geq \deg_t (x)\frac{1}{n}(mn - m - n) + 1.$$

Theorem 1 is a consequence of the more general

Theorem 2. Let a and b be nonconstant distinct polynomials of the same degree n. Let ab have k distinct roots. Then

$$\deg_t (a - b) \geq n - k + 1.$$

Notation.

Let $X_1, \ldots, X_n$ be indeterminants. Denote the elementary symmetric polynomials in these variables by

$$e_1 = \Sigma X_i, \ldots, e_n = X_1 X_2 \cdots X_n$$

and the sum of powers symmetric polynomials by

$$p_1 = \Sigma X_i, \ldots, p_n = \Sigma X_i^n$$

Any symmetric polynomial may be expressed as as a polynomial in either the e_i or the p_i. In particular, the p_i may be expressed in terms of the e_i. These relations are the well-known Newton's formulas. For a derivation see the book by Macdonald [Mac]. The first few are:

$$\begin{aligned} p_1 &= e_1, \\ p_2 &= e_1^2 - 2e_2, \\ p_3 &= e_1^3 - 3e_1e_2 + 3e_3, \\ p_4 &= e_1^4 - 4e_1^2e_2 + 4e_1e_3 + 2e_2^2 - 4e_4 \end{aligned}$$

[3]**Note.** We learned from an article by Lang [L] that Theorems 1 and 2 have the following history: In 1965 Birch, Chowla, Hall, and Schinzel [BCHS] conjectured Theorem 1 and Davenport [D] proved it. Theorem 2 was proved by Mason [Mas] in 1984. They were interested in diophantine questions such as estimating $a^3 - b^2$ when a and b are integers. Theorem 1 says that $\deg_t (x^3 - y^2) \geq \frac{1}{2} \deg_t (x) + 1$. One easily finds polynomials x and y with integer coefficients such that equality holds. For example,

$$(t^4 + 4t)^3 - (t^6 + 6t^3 + 6)^2 = -8t^3 + 36 \tag{1}$$

It follows that there exist infinitely many integers a and b such that $|a^3 - b^2| < 9a^{3/4}$. One gets better inequalites by finding such x and y with higher degree.

Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be two sets of quantities. Let $e_i(\alpha)$ and $p_i(\alpha)$ denote the symmetric polynomials in the α_i and let $e_i(\beta)$ and $p_i(\beta)$ denote the symmetric polynomials in the β_i.

The following lemma is immediate: **Lemma.** Let $1 \leq h \leq n$. If $e_i(\alpha) = e_i(\beta)$ for $i = 1, \ldots, h$ then $p_i(\alpha) = p_i(\beta)$ for $i = 1, \ldots, h$.

Proof of Theorem 2.

Factor a and b over the algebraic closure of k :

$$a = \mu(t - \alpha_1) \cdots (t - \alpha_n),$$

$$b = \nu(t - \beta_1) \cdots (t - \beta_n).$$

If $\mu \neq \nu$ then $\deg_t (a - b) = \deg_t a = \deg_t b$ and the theorem is trivially true. So assume $\mu = \nu$. Replacing a and b by $\frac{1}{\mu}a$ and $\frac{1}{\mu}b$ does not change n, k, or $\deg_t (a - b)$. Hence we may assume that a and b are monic.

Now proceed by contradiction. Suppose that $\deg_t (a - b) < n - k + 1$. Hence the first k coefficients of a and b are equal (the coefficients of $t^n, t^{n-1}, \ldots, t^{n-k+1}$). These are the symmetric polynomials in the α_i and the β_i, so we have equations

$$e_i(\alpha) = e_i(\beta) \ , \ i = 1, \ldots, k - 1.$$

So by the lemma

$$p_i(\alpha) = p_i(\beta) \ , \ i = 1, \ldots, k - 1. \tag{2}$$

Call the α_i and β_i collectively γ_i. In other words, define

$$\gamma_i = \alpha_i, \text{ for } i = 1, \ldots, n,$$

$$\gamma_{n+i} = \beta_i, \text{ for } i = 1, \ldots, n.$$

Among the γ there are k distinct numbers by assumption. Renumber so that these are $\gamma_1, \ldots, \gamma_k$. Collect terms so that the equations (2) take the form

$$u_1\gamma_1^i + \cdots + u_n\gamma_k^i = 0 \ , \ i = 1, \ldots, k - 1.$$

where u_i is the multiplicity of γ_i as a root of a minus the multiplicity of γ_i as a root of b. The u_i are not all zero, since this would imply $a = b$, and we have assumed a and b distinct. Also observe that $\Sigma u_i = 0$ since this sum is the number of roots of a minus the number of roots of b and these have the same degree. Putting this in matrix form we have

$$\begin{pmatrix} 1 & \cdots & 1 \\ \gamma_1 & \cdots & \gamma_k \\ \vdots & & \vdots \\ \gamma_1^{k-1} & \cdots & \gamma_k^{k-1} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix} = 0.$$

Since the u_i are not all zero, the Vandermonde matrix in this equation must be singular. On the other hand, the γ_i are distinct so that the matrix must have full rank. This is a contradiction. ∎

Proof of Theorem 1.

If $\deg_t(x^m) \neq \deg_t(y^n)$ then $\deg_t(x^m - y^n)$ is the maximum of the two degrees and the inequality stated in the theorem holds easily in this case. So assume that $\deg_t(x^m) = \deg_t(y^n)$. Then we have for some s, $\deg_t(x) = sn/d$, and $\deg_t(y) = sm/d$ where $d = \gcd(m,n)$. Apply theorem 2 to the case where $a = x^m$, $b = y^n$. We get

$$\begin{aligned}\deg_t(x^m - y^n) &\geq \frac{smn}{d} - \frac{sn}{d} - \frac{sm}{d} + 1 \\ &= \frac{s}{d}(mn - m - n) + 1 \\ &= \frac{\deg_t(x)}{n}(mn - m - n) + 1.\end{aligned}$$

∎

As noted before, one can ask whether it is possible to find x and y of arbitrarily large degree such that equality holds in the above inequality. This may not be possible if one of m , n divides the other. For example, $\deg_t(x^4 - y^2) = \deg_t(x^2 - y) + \deg_t(x^2 + y) \geq 2\deg_t(x)$ (assuming $x^4 - y^2 \neq 0$). This is strictly greater than $\deg_t(x) + 1$ given by the formula in this case.

Conjecture 3. Let m, n be nonprincipal (i.e. neither divides the other). For any positive integer s, there exist polynomials x and y, with complex coefficients and degrees sn, and sm respectively such that

$$\begin{aligned}\deg_t(x^m - y^n) &= \deg_t(x)\frac{1}{n}(mn - m - n) + 1 \\ &= s(mn - m - n) + 1 \\ &= \deg_t(x^m) - \deg_t(x) - \deg_t(y) + 1 \\ &= \deg_t(y^n) - \deg_t(x) - \deg_t(y) + 1\end{aligned}$$

Write $m' = sm$, $n' = sn$, $h = m' + n'$. Proving the conjecture reduces to first finding a solution $(\gamma_1, \ldots, \gamma_h)$ to the system

$$\begin{aligned}m(\gamma_1 + \cdots + \gamma_{n'}) &= n(\gamma_{n'+1} + \cdots \gamma_h), \\ &\vdots \\ m(\gamma_1^{h-2} + \cdots \gamma_{n'}^{h-2}) &= n(\gamma_{n'+1}^{h-2} + \cdots \gamma_h^{h-2}).\end{aligned} \tag{3}$$

Furthermore, the solution must be nondegenerate in the sense that the next equation in the sequence,

$$m(\gamma_1^{h-1} + \cdots \gamma_{n'}^{h-1}) = n(\gamma_{n'+1}^{h-1} + \cdots \gamma_h^{h-1})$$

must not be satisfied, or Theorem 1 would imply that $x^m = y^n$.

We also note that $m(1 + \cdots n' \text{ terms }) + n((1 + \cdots m' \text{ terms }) = 0$. Together with this, put the system (3) in matrix form:

$$\begin{pmatrix} 1 & \dots & 1 \\ \gamma_1 & \dots & \gamma_h \\ \gamma_1 & \dots & \gamma_h \\ \vdots & & \vdots \\ \gamma_1^{h-2} & \dots & \gamma_h^{h-2} \end{pmatrix} \begin{pmatrix} m \\ \vdots \\ m \\ -n \\ \vdots \\ -n \end{pmatrix} = 0.$$

Consider the more general question: For what sequences $(u_1, \dots, u_h) \neq 0$ is there a nondegenerate solution $(\gamma_1, \dots, \gamma_h)$ to the system

$$\begin{pmatrix} \gamma_1 & \dots & \gamma_h \\ \vdots & & \vdots \\ \gamma_1^{h-2} & \dots & \gamma_h^{h-2} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_h \end{pmatrix} = 0? \tag{4}$$

Lemma. The system (4) has infinitely many non-zero (but perhaps degenerate) solutions.

Proof. Think of the equations as $h - 2$ hypersurfaces in $\mathbb{P}^{h-1}$. By Bezout's Theorem, the locus of solutions has dimension 1 or more. ∎

Lemma. Suppose that the sum of all the u_i is zero, but that no proper subset of the u_i sums to zero. Then the system has a nondegenerate solution.

Proof. Let $\gamma_1, \dots, \gamma_h$ be a non-zero solution. Suppose it is degenerate. Then we have:

$$\begin{pmatrix} 1 & \dots & 1 \\ \gamma_1 & \dots & \gamma_h \\ \vdots & & \vdots \\ \gamma_1^{h-2} & \dots & \gamma_h^{h-2} \\ \gamma_1^{h-1} & \dots & \gamma_h^{h-1} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_h \end{pmatrix} = 0.$$

Hence, two of the γ must be equal. Without loss of generality say $\gamma_{h-1} = \gamma_h$. We may therefore rewrite the system, absorbing all references to γ_h into γ_{h-1}, and letting u_{h-1} become $u_{h-1} + u_h$, which is not zero by hypothesis. Finally, remove the last equation. We have:

$$\begin{pmatrix} 1 & \dots & 1 \\ \gamma_1 & \dots & \gamma_{h-1} \\ \vdots & & \vdots \\ \gamma_1^{h-2} & \dots & \gamma_{h-1}^{h-2} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_{h-1} \end{pmatrix} = 0$$

Therefore two of the remaining γ must be equal. Continuing this process we see that all of the γ are equal. But this corresponds to just one point of $\mathbb{P}^{n-2}$, namely $(1, 1, \ldots, 1)$, and we have seen that there must be other solutions which are then nondegenerate.∎

Corollary. Let m and n be relatively prime. Then there exist polynomials x and y of degrees n and m respectively such that $\deg_t (x^m - y^n) = \deg_t (x) \frac{1}{n}(mn - m - n) + 1$

Proof. In this case we have $u_1 = \cdots = u_m = n$ and $u_{m+1} = \cdots = u_{m+n} = -m$. Since m and n are relatively prime, no proper subset of the u_i sums to zero. ∎

Question.

The hypothesis of the theorem doesn't hold if we let x and y have degrees sn and sm for s other than 1. Consider the example (1) where x has degree 4 and y has degree 6. Then $(u_1, \ldots, u_{10}) = (3, 3, 3, 3, -2, -2, -2, -2, -2, -2)$ and there are clearly proper subsets adding to zero (3 + 3 - 2 - 2 - 2). On the other hand $\deg_t (x^3 - y^2) = 4$, the minimum possible. This shows that the hypothesis of the theorem is not necessary.

Is there a condition similar to ours which is necessary and sufficient?

References

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

[A2] Abhyankar, S. S. *On the semigroup of a meromorphic curve,* Proc. Int. Symp. on Algebraic Geometry, Kyoto 1977, 249-414.

[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.

[AM3] Abhyankar, S.S., and Moh, T.T., *Embeddings of the line in the plane,* J. Reine Angew. Math. 276 (1975),148-166.

[AS] Abhyankar, S.S., and Singh,B., *Embeddings of certain curves in the affine plane,* Amer. J. Math. 100(1978), 99-175.

[BCHS] Birch,B., Chowla,S., Hall, M., and Schinzel, A., *On the difference* $x^3 - y^2$*,* K. Norske Vid. Selsk. Forrh. (Trondheim), 38(1965), 65-69.

[D] Davenport, H., *On* $f^3(t) - g^2(t)$*,* K. Norske Vid. Selsk. Forrh.(Trondheim), 38(1965), 86-87.

[L] Lang,S., *Old and new conjectured diophantine inequalities,* Bull. Amer. Math. Soc. (N.S.) 23(1) (1990),37-75.

[Mac] Macdonald, I.G. "Symmetric Functions and Hall Polynomials." Oxford University Press, New York, 1979.

[Mas] Mason, R.C., *Equations over function fields,* Springe Lecture Notes 1068 (1984)149-157, in Number Theory, proceedings of the Noordwijkerhout, 1983.

[Mo1] Moh,T.T., *On characteristic paris of algebroid plane curves for characteristic p,* Bull. Inst. Math. Acad. Sinica, 1(1973), 75-91.

[Mo2] Moh,T.T., *On approximate roots of a polynomial,* J. Reine Angew. Math. 278(1975), 301-306.

[Mo3] Moh,T.T., *On then concept of approximate roots for algebra,* J. Alg. 65(1980),301-306.

[Mo4] Moh, T.T., *On two fundamental theorems for the concept of approximate roots,* J. Math. Soc. Japan 34(1982), 637-652.

[Mo5] Moh,T.T. *On analytic irreducibility at ∞,* Proc. Amer. Math. Soc. 44(1982), 22-24.

[Mo6] Moh, T.T., *On the jacobian conjecture and the configuration of roots,* J. Reine Angew. Math. 340(1983), 331-340.

[Ri] Richman, D. R., *On the computation of mainimal polynomials,* J. of Algebra, 103(1986), 1-17.

[Ru] Russell, P. *Hamburger-Noether expansions and approximate roots of polynomials,* manuscripta math. 31(1980), 25-95.

[S1] Sathaye, A., *On planar curves,* Amer. J. Math. 99(5)(1977),1105-1135.

[S2] Sathaye,A., *Generalized Newton-Puiseux expansion and Abhyankar-Moh semigroup theorem,* Invent. math. 74(1983), 149-157.