ON DECOMPOSABLE RATIONAL FUNCTIONS WITH GIVEN NUMBER OF SINGULARITIES

CLEMENS FUCHS, ATTILA PETHŐ* AND SZABOLCS TENGELY**

Dedicated to the 70th birthday of Professor Masami Ito

1. Introduction

These notes are based on the papers [1] and [3]; the talk was delivered by Attila Pethő at the Workshop "Algebraic Systems and Theoretical Computer Science", RIMS, Kyoto, February 20, 2012.

Let k be an algebraically closed field of characteristic zero and let $k(x)$ be the rational function field in one variable over k. For $f \in k(x)$ we define $\deg f = [k(x) : k(f(x))]$.

We are interested in $f \in k(x)$ that are *decomposable* as rational functions, i.e., for which there exist $g, h \in k(x)$, $\deg g, \deg h \geq 2$ such that $f(x) = g(h(x))$ holds.

Such a decomposition is only unique up to a linear fractional transformation $\lambda = \dfrac{ax+b}{cx+d} \in \mathrm{GL}_2(k)$, i.e. with $ad - bc \neq 0$, since we may always replace $g(x)$ by $g(\lambda(x))$ and $h(x)$ by $\lambda^{-1}(h(x))$ without affecting the equation $f(x) = g(h(x))$. Especially we are interested in such decompositions when f is a "lacunary" rational function.

There are different possible notions of "lacunarity". The most common notion is that the number of non-constant terms appearing in a given representation of $f(x) = P(x)/Q(x), P, Q \in k[x]$ is bounded.

Andrej Schinzel conjectured that if for fixed g the polynomial $g(h(x))$ has at most l non-constant terms, then the number of terms of h is bounded only in terms of l. This was confirmed in a more general form by Umberto Zannier [8]. He actually proved that if one starts with a positive integer l, then one can describe effectively all decompositions of polynomials $f \in k[x]$ having at most l non-constant terms if one excludes the inner function h being of the exceptional shape $ax^n + b, a, b \in k, n \in \mathbb{N}$.

This description was "algorithmic" in the sense that all possible polynomials and decompositions were described by letting the possible coefficients

Date: May 18, 2012.

*Paper was written, when the second author visited University of Niigata with a long term research fellowship of JSPS.

**Research supported in part by OTKA PD75264 and János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

vary in some effectively computable affine algebraic varieties and the exponents in some computable integer lattices.

There are also other possibilities to think of the "lacunarity". In these notes we are interested in rational functions f with a *bounded number of zeros and poles*. This means that the number of distinct roots of P, Q in a reduced expression of f is bounded. We assume that the number of zeros and poles is fixed, whereas the actual values of the zeros and poles and their multiplicities are considered as variables.

There are some simple families of such decomposable functions.

• **Example 1.** If the multiplicities of the zeros and poles of f all have a common divisor, say $m \in \mathbb{N}$, then $f(x) = (h(x))^m$ for some $h \in k(x)$. Clearly f and g have the same number of singularities, but h is not controlled by n. For this reason we say that if $g(x) = (\lambda(x))^m$ for a suitable $\lambda \in \mathrm{PGL}_2(k)$ then g is of exceptional shape (also called the forbidden shape later).

• **Example 2.** Let λ_1, λ_2 be the roots of $x^2 - x - 1$ in $k = \mathbb{C}$ then for $g(x) = x^{k_1}(x-1)^{k_2}, h(x) = x(x-1)$ we have

$$f(x) = g(h(x)) = x^{k_1}(x-1)^{k_1}(x-\lambda_1)^{k_2}(x-\lambda_2)^{k_2}$$

for every $k_1, k_2 \in \mathbb{Z}$. Thus we have constructed infinitely many rational functions f with four distinct zeros and poles altogether and which are decomposable. This phenomenon can easily be generalized to rational functions with an arbitrary number of singularities and shows that the multiplicities cannot underly severe restrictions (we will see later that the only condition we have to take into account is whether the sum of the k_i vanishes or not).

We shall also give a complete description of composite f's in analogy to Zannier's result. This result was proved in [1]. Our proof was algorithmic, it provided a method to find all possible decomposable rational functions not of exceptional shape with a fixed number of singularities. In [3] we performed these computations if the number of singularities is at most four and found many examples if this number is at most six.

To make the understanding of the main results simpler we work out a non-trivial, but simple enough example.

2. A non-trivial example

Assume that $f(x)$ has three singularities: two roots of order one and two respectively, and one pole of order four, i.e.

$$f(x) = \frac{(x-\alpha_1)^2(x-\alpha_2)}{(x-\alpha_3)^4}.$$

Moreover assume that $f(x) = g(h(x))$ with

$$\begin{aligned} g(x) &= (x-\beta_1)^{l_1} \cdots (x-\beta_r)^{l_r}, \quad l_1, \ldots, l_r \in \mathbb{Z}, \\ h(x) &= \frac{h_1(x)}{h_2(x)}, \quad \gcd(h_1, h_2) = 1. \end{aligned}$$

Inserting $h(x)$ into $g(x)$ we get the equation

$$g(h(x)) = (h(x)-\beta_1)^{l_1}\cdots(h(x)-\beta_r)^{l_r} = \frac{(x-\alpha_1)^2(x-\alpha_2)}{(x-\alpha_3)^4}.$$

Taking into account that $\gcd(h_1(x)-\beta_i h_2(x), h_1(x)-\beta_j h_2(x)) = 1, 1 \le i < j \le r$ we get $r \le 3$. The possibilities $r = 1$ and $r = 3$ can be excluded, because in the first case $l_1 = 1$ and in the second $h(x)$ is linear, which are excluded.

Thus $r = 2$. Then either $l_1 = l_2 = 2$, which is again impossible, or $l_1 = l_2 = 1$. Then

$$\left(\frac{h_1(x)}{(x-\alpha_3)^2} - \beta_1\right)\left(\frac{h_1(x)}{(x-\alpha_3)^2} - \beta_2\right) = \frac{(x-\alpha_1)^2(x-\alpha_2)}{(x-\alpha_3)^4}.$$

Hence after possible change of the enumeration we get

$$\begin{aligned} h_1(x) - \beta_1(x-\alpha_3)^2 &= (x-\alpha_1)^2, \\ h_1(x) - \beta_2(x-\alpha_3)^2 &= x-\alpha_2. \end{aligned}$$

Eliminating $h_1(x)$ and comparing coefficients we get

$$\begin{aligned} \beta_2 - \beta_1 &= 1, \\ \alpha_1 - \alpha_3 &= -1/2, \\ \alpha_1 + \alpha_3 &= 2\alpha_2. \end{aligned}$$

Hence $\alpha_1 = \alpha_3 - 1/2$ and $\alpha_2 = \alpha_3 - 1/4$. Thus the only possibility is

$$\begin{aligned} f(x) &= \frac{(x-\alpha_3+1/2)^2(x-\alpha_3+1/4)}{(x-\alpha_3)^4}, \\ g(x) &= (x-\beta_1)(x-\beta_1+1), \end{aligned}$$

where $\alpha_3, \beta_1 \in k$.

3. Main theorem

To simplify slightly the statement we make the following remark. By changing $g(x)$ into $g(\theta x)$ with an appropriate $\theta \in k$ we may assume that the rational function h is the quotient of two monic polynomials and by dividing both sides of the equation $f(x) = g(h(x))$ by a suitable constant we may even assume the same for f and g. Now we are in the position to formulate the main result of [1].

Main Theorem. *Let n be a positive integer. Then there exists a positive integer J and, for every $i \in \{1,\dots,J\}$, an affine algebraic variety $\mathcal{V}_i$ defined over $\mathbb{Q}$ and with $\mathcal{V}_i \subset \mathbb{A}^{n+t_i}$ for some $2 \le t_i \le n$, such that:*

(i) *If $f, g, h \in k(x)$ with $f(x) = g(h(x))$ and with $\deg g, \deg h \ge 2$, g not of the shape $(\lambda(x))^m, m \in \mathbb{N}, \lambda \in \mathrm{PGL}_2(k)$, and f has at most n zeros and poles altogether, then there exists for some $i \in \{1,\dots,J\}$ a point $P = (\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_{t_i}) \in \mathcal{V}_i(k)$, a vector $(k_1,\cdots,k_{t_i}) \in \mathbb{Z}^{t_i}$ with $k_1 + k_2 + \cdots + k_{t_i} = 0$ or not depending on $\mathcal{V}_i$, a partition of*

$\{1,\dots,n\}$ *in* t_i+1 *disjoint sets* $S_\infty, S_{\beta_1},\dots,S_{\beta_{t_i}}$ *with* $S_\infty=\emptyset$ *if* $k_1+k_2+\cdots+k_{t_i}=0$, *and a vector* $(l_1,\dots,l_n)\in\{0,1,\dots,n-1\}^n$, *also both depending only on* $\mathcal{V}_i$, *such that*

$$f(x)=\prod_{j=1}^{t_i}(w_j/w_\infty)^{k_j},\qquad g(x)=\prod_{j=1}^{t_i}(x-\beta_j)^{k_j},$$

and

$$h(x)=\begin{cases}\beta_j+\frac{w_j}{w_\infty}\ (j=1,\dots,t_i), & \text{if } k_1+k_2+\cdots+k_{t_i}\neq 0,\\ \frac{\beta_{j_1}w_{j_2}-\beta_{j_2}w_{j_1}}{w_{j_2}-w_{j_1}}\ (1\le j_1<j_2\le t_i), & \text{otherwise,}\end{cases}$$

where

$$w_j=\prod_{m\in S_{\beta_j}}(x-\alpha_m)^{l_m},\quad j=1,\dots,t_i$$

and

$$w_\infty=\prod_{m\in S_\infty}(x-\alpha_m)^{l_m}.$$

Moreover, we have $\deg h\le(n-1)/(t_i-1)\le n-1$.

(ii) *Conversely for given data* $P\in\mathcal{V}_i(k),(k_1,\dots,k_{t_i}),S_\infty,S_{\beta_1},\dots,S_{\beta_{t_i}}$, $(l_1,\dots,l_n)$ *as described in* (i) *one defines by the same equations rational functions* f,g,h *with* f *having at most* n *zeros and poles altogether for which* $f(x)=g(h(x))$ *holds.*

(iii) *The integer* J *and equations defining the varieties* $\mathcal{V}_i$ *are effectively computable only in terms of* n.

The theorem says that all decomposable rational functions with at most n singularities and all their decompositions arise from finitely many *generic* such decompositions, namely that for each $i\in\{1,\dots,n\}$ there are rational functions $F_i,G_i,H_i\in\mathbb{Q}[\mathcal{V}_i][x]$ with $\deg H_i\le n-1$ and with $F_i=G_i\circ H_i$ having at most n singularities. Precise formulae for these functions in terms of expressions from the coordinate ring of the corresponding variety are explicitly given in the statement, and if f,g,h are as in (i) above, then there is an i and a point $P\in\mathcal{V}_i(k)$ such that $f(x)=F_i(P,x),g(x)=G_i(P,x),h(x)=H_i(P,x)$.

Example 2. is obtained by taking

$$n=4,t=2,S_\infty=\emptyset,S_0=\{1,2\},S_\beta=\{3,4\},l_1=l_2=l_3=l_4=1$$

and $P=(0,1,\lambda_1,\lambda_2,1)=(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\beta)\in\mathcal{V}(\mathbb{C})$, where the variety $\mathcal{V}\subset\mathbb{A}^5$ is defined as the zero locus of the system of algebraic equations $\alpha_1\alpha_2-\alpha_3\alpha_4-\beta=0,\alpha_1+\alpha_2-\alpha_3-\alpha_4=0$.

4. Preparation for the proof of the main theorem

Observe first that for $g(x) = \frac{g_1(x)}{g_2(x)}, g_1, g_2 \in k[x]$, $\gcd(g_1(x), g_2(x)) = 1$ and $\deg g_1 = \deg g_2$ every pole of h will be canceled in the decomposition $f(x) = g(h(x))$.

Indeed, if $h(x) = h_1(x)/h_2(x)$ and $\deg h_2 > 0$, then

$$g(h(x)) = g_1\left(\frac{h_1(x)}{h_2(x)}\right)/g_2\left(\frac{h_1(x)}{h_2(x)}\right) = \frac{h_2(x)^{\deg g_1} g_1\left(\frac{h_1(x)}{h_2(x)}\right)}{h_2(x)^{\deg g_2} g_2\left(\frac{h_1(x)}{h_2(x)}\right)}.$$

As the numerator and denominator belong to $k[x]$ and the denominator is coprime to $h_2(x)$ the claim is proved.

Hence a priori h could have arbitrary poles; this explains the difference between the two cases below. We also mention that if the number of distinct zeros and poles of g is two, then g has exactly one zero and one pole both with the same multiplicity and then we are in the forbidden shape for g.

For every $\theta \in k$ there is a valuation defined by the order of vanishing of f at $x = \theta$. Moreover for $f(x) = P(x)/Q(x), P, Q \in k[x]$ a non-archimedean valuation is defined by $v_\infty(f) = \deg Q - \deg P$. In this way all valuations $\mathcal{M}$ of $k(x)$ are obtained.

Then we have

$$\deg f = \sum_{v \in \mathcal{M}} \max\{0, v(f)\} = -\sum_{v \in \mathcal{M}} \min\{0, v(f)\}.$$

In other words the degree is just the number of zeros respectively poles of f (in $\mathbb{P}^1(k)$) counted by their multiplicities.

The Mason-Stothers theorem [2] says: *Let $f, g \in k(x)$, not both constant, with $f + g = 1$ and let S be any set of valuations of $k(x)$ containing all the zeros and poles in $\mathbb{P}^1(k)$ of f and g. Then we have* $\max\{\deg f, \deg g\} \leq |S| - 2$.

More generally Zannier [6] proved: *Let S be any set of valuations of $k(x)$ containing all the zeros and poles in $\mathbb{P}^1(k)$ of $g_1, \ldots, g_m$. If $g_1, \ldots, g_m \in k(x)$ span a k-vector space of dimension $\mu < m$ and any μ of the g_i are linearly independent over k, then*

$$-\sum_{v \in \mathcal{M}} \min\{v(g_1), \ldots, v(g_m)\} \leq \frac{1}{m - \mu}\binom{\mu}{2}(|S| - 2).$$

After these preparations we are in the position to give the proof of the main theorem; since the proof is not long, for the readers convenience, we repeat all details (compare with [1]).

5. Proof of the main theorem

Let n be a positive integer. Let $f, g, h \in k(x), \deg g, \deg h \geq 2, g$ not of the exceptional shape $(\lambda(x))^m, m \in \mathbb{N}, \lambda \in \mathrm{PGL}_2(k)$ and with f having at most n zeros and poles in $\mathbb{A}^1(k)$ altogether and such that $f(x) = g(h(x))$.

Since k is algebraically closed we can write

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)^{f_i}$$

with pairwise distinct $\alpha_i \in k$ and $f_i \in \mathbb{Z}$ for $i = 1, \ldots, n$.

Similarly we get

$$g(x) = \prod_{j=1}^{t} (x - \beta_j)^{k_j} \tag{1}$$

with pairwise distinct $\beta_j \in k$ and $k_j \in \mathbb{Z}$ for $j = 1, \ldots, t$ and $t \in \mathbb{N}$. Thus we have

$$\prod_{i=1}^{n} (x - \alpha_i)^{f_i} = f(x) = g(h(x)) = \prod_{j=1}^{t} (h(x) - \beta_j)^{k_j}.$$

We now distinguish two cases depending on $k_1 + k_2 + \cdots + k_t \neq 0$ or not; observe that this condition is equivalent to $v_\infty(g) \neq 0$ or not.

We shall write $h(x) = p(x)/q(x)$ with $p, q \in k[x], p, q$ coprime.

First assume that $v_\infty(g) \neq 0$. It follows that the poles in $\mathbb{A}^1(k)$ of h are among the values α_i: This is true because $q(\theta) = 0$ for $\theta \in k$ implies $h(\theta) = \infty$, where $\infty = (0 : 1)$ is the unique point at infinity of $\mathbb{P}^1(k)$, and $h(\theta) - \beta_j = \infty$. Also the valuation v_θ of h and $h(x) - \beta_j$ is the same. Thus $v_\theta(f) = v_\infty(g) v_\theta(h) \neq 0$, i.e. $g(h(\theta)) \in \{0, \infty\}$, and hence $\theta = \alpha_i$ for some $i \in \{1, \ldots, n\}$.

This implies that there is a subset S_∞ of the set $\{1, \ldots, n\}$ such that the α_m for $m \in S_\infty$ are precisely the poles in $\mathbb{A}^1(k)$ of h, i.e.

$$q(x) = \prod_{m \in S_\infty} (x - \alpha_m)^{l_m},\ l_m \in \mathbb{N}.$$

Furthermore h and $h(x) - \beta_j$ have the same number of poles counted by multiplicity, which means that their degrees are equal.

Calculating the valuations v_{α_m} of both sides of the equation $f(x) = g(h(x))$ we infer that

$$(k_1 + k_2 + \cdots + k_t) l_m = v_\infty(g) v_{\alpha_m}(h) = v_{\alpha_m}(f) = f_m$$

for $m \in S_\infty$. We also point out that for $\beta_i \neq \beta_j$ the factors $h(x) - \beta_i$ and $h(x) - \beta_j$ do not have any zeros (in $\mathbb{A}^1(k)$) in common; therefore we have $t \leq n$.

It follows that there is a partition of the set $\{1,\dots,n\}\backslash S_\infty$ in t disjoint subsets $S_{\beta_1},\dots,S_{\beta_t}$ such that

$$h(x)=\beta_j+\frac{1}{q(x)}\prod_{m\in S_{\beta_j}}(x-\alpha_m)^{l_m}, \tag{2}$$

where $l_m\in\mathbb{N}$ satisfies $l_mk_j=f_m$ for $m\in S_{\beta_j}, j=1,\dots,t$.

Since we assume that g is not of the shape $(\lambda(x))^m$ it follows that $t\geq 2$. Let $1\leq i<j\leq t$ be given. We have at least two different representations of h and thus we get

$$\beta_i+\frac{1}{q(x)}\prod_{r\in S_{\beta_i}}(x-\alpha_r)^{l_r}=\beta_j+\frac{1}{q(x)}\prod_{s\in S_{\beta_j}}(x-\alpha_s)^{l_s}$$

or equivalently $\beta(u_i-u_j)=1$, where $\beta=1/(\beta_j-\beta_i)$ and

$$u_i=\frac{1}{q(x)}\prod_{r\in S_{\beta_i}}(x-\alpha_r)^{l_r}=\frac{w_i}{w_\infty}.$$

The u_i are S-units for the set of valuations $S=\{v_{\alpha_1},\dots,v_{\alpha_n},v_\infty\}\subset\mathcal{M}$ corresponding to $\alpha_1,\dots,\alpha_n\in k$ and ∞. In fact u_i and u_j have also no zeros in $\mathbb{A}^1(k)$ in common and they have all exactly the same poles (also with multiplicities), namely $\alpha_m, m\in S_\infty$ and possibly ∞.

The Mason-Stothers theorem implies that

$$l_m\leq n-1 \text{ for all } m=1,\dots,n. \tag{3}$$

Observe that an application to $\beta(u_i-u_j)=1$ gives the bound only for those m which are in $S_\infty\cup S_{\beta_i}\cup S_{\beta_j}$; by using the relations from (2) for all possible combinations of $1\leq i<j\leq t$ we see that indeed (3) holds.

More precisely, it follows that the sum L^+ over all $l_m, m\in S_{\beta_i}$ plus $\max\{0,v_\infty(u_i)\}$, and the sum L^- over all $l_m, m\in S_\infty$ plus $-\min\{0,v_\infty(u_i)\}$, is bounded by $n-1$.

This can be immediately improved by an application of Zannier's theorem. First let us define $u_{t+1}:=1$. The k-vector space generated by the S-units $u_1,\dots,u_t,u_{t+1}\in k(x)$ has dimension 2 and any two of the u_i are linearly independent, because $\alpha u_i+\beta u_j=0$ with $\alpha,\beta\in k$ implies either $u_i\in k$, a contradiction, or $\alpha u_i+\beta(u_i-\beta_j+\beta_i)=(\alpha+\beta)u_i+\beta(\beta_i-\beta_j)=0$ and thus $\alpha=\beta=0$. It follows that

$$\deg u_i=L^+=L^-\leq-\sum_{v\in\mathcal{M}}\min\{v(u_1),\dots,v(u_t),0\}\leq\frac{n-1}{t-1}\leq n-1$$

for all $i=1,\dots,t$.

Especially, the degree of h is therefore also bounded by $n-1$ since it is equal to the degree of u_i for all $i=1,\dots,t$, so altogether $\deg h=\deg u_i\leq(n-1)/(t-1)\leq n-1$.

By comparing coefficients in (2) after canceling denominators for all combinations of the equations that have to hold there, we get an affine algebraic

variety $\mathcal{V}$ (possibly reducible) defined over $\mathbb{Q}$ in the variables $\alpha_1, \dots, \alpha_n$, $\beta_1, \dots, \beta_t$; thus $\mathcal{V} \subset \mathbb{A}^{n+t}$.

Notice that the number of variables and the exponents depend only on n. Since $f(x) = g(h(x))$ is given at this point, there are k-rational points on this algebraic variety and one of them corresponds to $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_t)$ coming from f and g.

Now we turn to the case $v_\infty(g) = 0$. Here we have

$$\prod_{i=1}^{n}(x-\alpha_i)^{f_i} = \prod_{j=1}^{t}\left(\frac{p(x)}{q(x)} - \beta_j\right)^{k_j} = \prod_{j=1}^{t}(p(x) - \beta_j q(x))^{k_j}.$$

Observe that a priori we have no control on the poles of h. However, as the factors on the right hand side of the last equation are again pairwise coprime, there is a partition of the set $\{1, \dots, n\}$ in t disjoint subsets $S_{\beta_1}, \dots, S_{\beta_t}$ such that

$$(p(x) - \beta_j q(x))^{k_j} = \prod_{m \in S_{\beta_j}} (x - \alpha_m)^{f_m}.$$

Thus k_j divides f_m for all $m \in S_{\beta_j}, j = 1, \dots, t$. On putting $l_m = f_m/k_j$ for $m \in S_{\beta_j}$ we obtain

$$p(x) - \beta_j q(x) = \prod_{m \in S_{\beta_j}} (x - \alpha_m)^{l_m}, j = 1, \dots, t. \tag{4}$$

Note that the exponents $l_m \in \mathbb{N}$, because $p(x) - \beta_j q(x)$ are polynomials and the α_m's are distinct. We have already pointed out above that in this case we may assume that $t \geq 3$, since g is not of exceptional shape.

Let us choose $1 \leq j_1 < j_2 < j_3 \leq t$. From the corresponding three equations in (4) the so called Siegel identity $v_{j_1,j_2,j_3} + v_{j_3,j_1,j_2} + v_{j_2,j_3,j_1} = 0$ follows, where

$$v_{j_1,j_2,j_3} = (\beta_{j_1} - \beta_{j_2}) \prod_{m \in S_{\beta_{j_3}}} (x - \alpha_m)^{l_m}.$$

The quantities v_{j_1,j_2,j_3} are non-constant rational functions and they are S-units. Observe that by taking $j_1 = 1, j_2 = i, j_4 = j$ with $1 \leq i < j \leq t$ the Siegel identity can be rewritten as

$$\frac{\beta_j - \beta_1}{\beta_j - \beta_i}\frac{w_i}{w_1} + \frac{\beta_1 - \beta_i}{\beta_j - \beta_i}\frac{w_j}{w_1} = 1.$$

Moreover, we get from (4) that

$$\begin{aligned} p(x) &= \frac{1}{\beta_i - \beta_j}\left(\beta_i \prod_{m \in S_{\beta_j}} (x - \alpha_m)^{l_m} - \beta_j \prod_{m \in S_{\beta_i}} (x - \alpha_m)^{l_m}\right) \\ &= \frac{\beta_i w_j - \beta_j w_i}{\beta_i - \beta_j} \end{aligned} \tag{5}$$

and

$$q(x) = \frac{1}{\beta_i - \beta_j}\left(\prod_{m\in S_{\beta_j}}(x-\alpha_m)^{l_m} - \prod_{m\in S_{\beta_i}}(x-\alpha_m)^{l_m}\right) = \frac{w_j - w_i}{\beta_i - \beta_j}. \tag{6}$$

Hence, the numerator of h is in any case given by f, g and the integer vector $(l_1, \dots, l_n)$.

The Mason-Stothers theorem applied to the Siegel identity now implies that $l_m \leq n-1$ for $m \in S_{\beta_1} \cup S_{\beta_i} \cup S_{\beta_j}$; as we may choose e.g. $i = 2$ and $j = 3, \dots, t$ we have actually $l_m \leq n-1$ for $m \in \{1, \dots, n\}$.

More precisely it follows for every i that the sum over all l_m with $m \in S_{\beta_i}$ is bounded by $n-1$, hence by (5) and (6) it follows that the degrees of p, q and hence, since the degree of a rational function is the maximum of the degrees of the numerator and denominator in a reduced representation, the degree of h is bounded by $n-1$.

Again this can be improved: We take $w_{t+1} := w_1$. Then the S-units $w_2/w_1, \dots, w_t/w_1, w_{t+1}/w_1 = 1$ span a k-vector space of dimension 2 and any two are linearly independent, because the w_i are pairwise coprime polynomials and a constant quotient w_i/w_1 would imply that h is constant, a contradiction, and if $\alpha w_i/w_1 + \beta w_j/w_1 = 0$ for $1 \leq i < j \leq t$, then $(\alpha - \beta(\beta_j - \beta_1)/(\beta_1 - \beta_i))w_i/w_1 + \beta(\beta_j - \beta_i)/(\beta_1 - \beta_i) = 0$ and therefore $\beta(\beta_j - \beta_i) = 0$ which implies $\beta = \alpha = 0$.

Thus Zannier's theorem gives that $\deg w_i/w_1 \leq (n-1)/(t-1)$ and, again since the w_i are coprime polynomials, $\deg w_i \leq (n-1)/(t-1)$ for all $i = 1, \dots, t$. The definition of h now implies that $\deg h \leq (n-1)/(t-1) \leq n-1$. By taking the Siegel identities as defining equations we again get an algebraic variety $\mathcal{V} \subset \mathbb{A}^{n+t}$ and $(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_t)$ is a k-rational point on this variety.

Finally we point out that we have $h(x) = \beta_j + w_j/w_\infty$ if $v_\infty(g) \neq 0$ and $S_\infty = \emptyset$ and $h(x) = (\beta_i w_j - \beta_j w_i)/(w_j - w_i)$ otherwise. In conclusion we have now proved (i).

Now we come to (ii) and (iii). The point is that we get all possible decompositions of rational functions with at most n zeros and poles altogether by considering for every integer $2 \leq t \leq n$ and for every partition of $\{1, \dots, n\}$ into $t+1$ disjoint sets $S_\infty, S_{\beta_1}, \dots, S_{\beta_t}$ and for every choice of $(l_1, \dots, l_n) \in \{0, 1, \dots, n-1\}^n$ the variety defined by equating the coefficients given by (2) after canceling denominators and, if $S_\infty = \emptyset$ and $t \geq 3$, the variety given by the various Siegel identities.

If the first system has a k-rational solution, then (2) defines the rational function $h(x)$; afterwards for any choice of integers $k_1, \dots, k_t$ with $k_1 + \dots + k_t \neq 0$ we define a rational function $g(x)$ by (1). If the second system has a k-rational solution, then we define $h(x) = p(x)/q(x)$ by (5) and (6) and then for any choice of integers $k_1, \dots, k_t$ with $k_1 + \dots + k_t = 0$ we define a

rational function $g(x)$ again by (1). Finally, in both cases, we use

$$f(x) = \prod_{j=1}^{t} \Big(\prod_{m \in S_{\beta_j}} (x - \alpha_m)^{l_m} \prod_{m \in S_\infty} (x - \alpha_m)^{-l_m} \Big)^{k_j} = \prod_{j=1}^{t} (w_j / w_\infty)^{k_j}$$

to define the rational function f, which then has at most n zeros and poles altogether and for which $f(x) = g(h(x))$ holds.

The number J of possible varieties is at most $2np(n)n^n$, where $p(n)$ is the partition function and since everything above is completely explicit, the defining equations of the varieties can be found explicitly. This proves the remaining parts of the statement.

6. The algorithm for the computation of the exceptions

The proof of the theorem implies an algorithm for the computation of all decomposable rational functions of given number of singularities. It was implemented by Szabolcs Tengely in MAGMA. We report about the results of the computation in [3]. In the following pseudocode we use the same notation as in the theorem. Especially n denotes the number of singularities.

1) Let $S_\infty, S_{\beta_1}, \ldots, S_{\beta_t}$ be a partition of $\{1, 2, \ldots, n\}$.
2) For the partition and a vector $(l_1, \ldots, l_n) \in \{1, 2, \ldots, n\}^n$ compute the corresponding variety $\mathcal{V}$, given by $v_1 = \cdots = v_r = 0$, where v_i is a polynomial in $\alpha_1, \ldots, \alpha_n$, $\beta_1, \ldots, \beta_t$. Here we used Gröbner basis techniques.
3) To remove contradictory systems we compute

$$\Phi = \prod_{i \neq j} (\alpha_i - \alpha_j) \prod_{i \neq j} (\beta_i - \beta_j).$$

4) For all $v_i = v$ compute

$$u_{i_1} = \frac{v}{\gcd(v, \Phi)},$$

and

$$u_{i_k} = \frac{u_{i_{k-1}}}{\gcd(u_{i_{k-1}}, \Phi)},$$

until $\gcd(u_{i_{k-1}}, \Phi) = 1$.

As the cases $n = 1, 2$ are trivial we performed the algorithm for $n = 3$ and $n = 4$ and obtained a complete list of all decomposable rational functions with number of singularities at most three or four. We have several sporadic examples for $n > 4$ too, but the number of partitions to be considered grows very fast, and we do not understand yet how to exclude very early the contradictory systems or systems of similar shape.

For $n = 3$ there are nine exceptions, but only two are essentially different. The first was shown in Section 2. The second is the following.

$$\begin{aligned} g(x) &= (x-\beta)(x-\beta-4\alpha_1+4\alpha_2), \\ h(x) &= \beta + \frac{(x-\alpha_2)^2}{x-\alpha_1}, \\ f(x) &= \frac{(x-\alpha_2)^2(x-2\alpha_1+\alpha_2)}{(x-\alpha_1)^2}, \end{aligned}$$

where $\alpha_1, \alpha_2, \beta \in k$.

For $n = 4$ we found several hundred exceptions. We give here only one example:

$$\begin{aligned} g(x) &= (x-\beta)(x-\beta+1), \\ h(x) &= \beta + \left(x - \frac{9\alpha+\sqrt{-3}}{9}\right)\left(x - \frac{3\alpha+\sqrt{-3}}{3}\right)^{-3}, \\ f(x) &= \left(x - \frac{9\alpha+\sqrt{-3}}{9}\right)\left(x-\alpha-\sqrt{-3}\right)(x-\alpha)^2\left(x - \frac{3\alpha+\sqrt{-3}}{3}\right)^{-6}, \end{aligned}$$

with $\alpha, \beta \in k$.

References

[1] C. Fuchs, A. Pethő, On composite rational functions having a bounded number of zeros and poles, *Proc. AMS* **139** (2011), 31-38.

[2] R.C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Note Series **96**, Cambridge University Press, Cambridge, 1984.

[3] A. Pethő, Sz. Tengely, *On composite rational functions*, in preparation.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Universitext, 1993.

[5] U. Zannier, Some remarks on the S-unit equation in function fields, *Acta Arith.* **LXIV** (1993), no. 1, 87-98.

[6] U. Zannier, On the number of terms of a composite polynomial, *Acta Arith.* **127** (2007), no. 2, 157-167.

[7] U. Zannier, On composite lacunary polynomials and the proof of a conjecture of Schinzel, *Invent. Math.* **174** (2008), no. 1, 127-138.

[8] U. Zannier, Addendum to the paper: On the number of terms of a composite polynomial, *Acta Arith.* **141** (2009), no. 1, 93-99.

Department of Mathematics, ETH Zurich, Rämistrasse 101, 8092 Zürich, Switzerland

E-mail address: clemens.fuchs@math.ethz.ch

Department of Computer Science, University of Debrecen, H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: Petho.Attila@inf.unideb.hu

Department of Mathematics, University of Debrecen, H-4010 Debrecen, P.O. Box 12, Hungary

E-mail address: tengely@science.unideb.hu