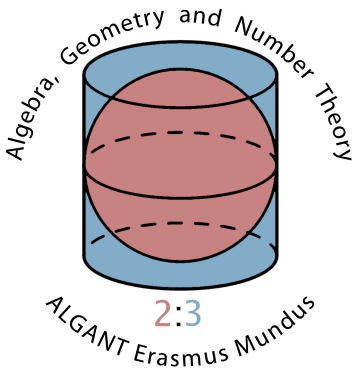

On lacunary polynomials and a generalization of Schinzel's conjecture

Candidate:
Daniele Dona

Supervisor:
prof. Yuri Bilu

ALGANT Master Thesis - July 2015

Concordia University

Université de Bordeaux

Contents

Introduction **1**

1 Schinzel's conjecture **3**
1.1 Historical background . . . 3
1.2 Introduction to the proof . . . 4
1.3 Proof of Theorem 1.3 . . . 5
1.4 Proof of Theorem 1.1 . . . 8

2 General case **9**
2.1 Introduction to the proof . . . 9
2.2 Theorem 2.2: Puiseux expansion . . . 10
2.3 Theorem 2.2: linear dependence . . . 12

3 Explicit bounds **15**
3.1 Bound for Theorem 1.3 . . . 15
3.2 Bound for Theorem 1.1 . . . 17
3.3 Bound for Theorem 2.2: preliminary lemmas . . . 18
3.4 Bound for Theorem 2.2: bound expressions . . . 22
3.5 Bound for Theorem 2.2 and Theorem 2.1 . . . 27

4 Further generalizations **31**

Bibliography **33**

Introduction

A *lacunary polynomial* (also called *sparse polynomial* or *fewnomial*) is a polynomial where the number of its terms is considered fixed, while the degrees and coefficients of its terms may vary. For example we can write $f(x) = a_1 x^{n_1} + \ldots + a_l x^{n_l}$ for a lacunary polynomial with at most l terms, with no control whatsoever on the actual value of the degrees n_i and the coefficients a_i.

The focus on the number of terms of a polynomial rather than on the other data leads to some interesting questions regarding in particular the behaviour of lacunary polynomials under the operation of composition, or in even more general algebraic expressions. The first conjecture that appeared in this direction was raised independently by Erdős and Rényi: given a polynomial $h(x)$, if its square $h(x)^2$ has at most l terms then also $h(x)$ has a bounded number of terms dependent only on l [1]. This was proven by Schinzel [4] in the more general case of $h(x)^d$ being lacunary: he then posed an even more general question, in the case of $g(h(x))$ being lacunary where g is another non-constant polynomial; he also stated that his method was not powerful enough to tackle this new problem, so we don't follow his procedure here.

Schinzel's conjecture has then been solved by Zannier [8]: Zannier's proof will be discussed in Chapter 1. Although it yields an explicit bound $B(l)$ on the number of terms of $h(x)$ (when $g(h(x))$ has at most l non-constant terms), the author didn't bother himself with the actual calculation of this bound, observing only that it should be very large and weaker than the one for the case $h(x)^d$ solved by Schinzel: in Chapter 3 we'll calculate $B(l)$ following his method and discover that he was right in both cases.

Chapter 2 will treat an even more general case: given a polynomial $F(x, y)$ with at most l terms in x and monic of degree d in y, any $h(x)$ such that $F(x, h(x)) = 0$ has at most $\beta(d, l)$ terms. This was solved by Fuchs, Mantova and Zannier [2] adapting the proof contained in [8] to the new situation; as before, also in this case the bounds are explicit but have not been actually calculated: this will be done again to a certain degree in Chapter 3, again confirming the opinion of the authors who considered it to be a highly iterated exponentiation.

Chapter 1

Schinzel's conjecture

1.1 Historical background

As said in the introduction, a lacunary polynomial is a polynomial where the number of its terms is considered fixed, while the degrees and coefficients of its terms may vary. Kalmár, Rédei and Rényi started considering the problem of lacunarity in the case of the square of a polynomial, although formulating it the other way around. Call $Q(k)$ the minimum possible number of terms of the square of a polynomial with k terms: it has been proven by them that $\liminf_{k\to\infty} \frac{Q(k)}{k} = 0$ and Rényi [3] conjectured that $\lim_{k\to\infty} \frac{Q(k)}{k} = 0$, which was proven two years later by Erdős [1]; these and other results were answering questions about the dimension of $Q(k)$ establishing upper limits to it, but in the same paper Erdős said that Rényi told him to have also conjectured something in the other direction:

$$\lim_{k\to\infty} Q(k) = \infty$$

This last assertion means that, given any polynomial with a number of terms k big enough, its square has to have a certain number $Q(k)$ of terms that can be made as big as desired if k is chosen appropriately; in other words this is equivalent to say that if the square of a polynomial $h(x)$ has a bounded number of terms then $h(x)$ itself can't have a number of terms that is too big.

This issue was solved by Schinzel [4], who gave also an explicit bound in a broader case. Consider a polynomial $h(x)$ with $k \geq 2$ terms and a positive integer d, then the number of terms of $h(x)^d$ is at least:

$$d + 1 + \frac{\ln\left(1 + \frac{\ln(k-1)}{d\ln 4d - \ln d}\right)}{\ln 2}$$

This again can be read the other way around. Given any polynomial $h(x)$ and positive integer d, if $h(x)^d$ has at most l terms then there is an upper bound $T(d,l)$ on the number of terms of $h(x)$ which is:

$$T(d,l) \leq \max\{2, 1 + e^{(2^{l-d-1}-1)(d\ln 4d - \ln d)}\} \tag{1.1}$$

This result holds also for a somewhat generic field instead of just for $\mathbb{C}$, making reasonable assumptions about its characteristic; on the other hand, the method that Schinzel uses is

in his own words insufficient to prove the more general case of what is called Schinzel's conjecture, i.e. the same question with the hypothesis that $g(h(x))$ has at most l terms for a certain polynomial g. This is what Zannier proved in [8], and this is what we are going to show in the following sections.

1.2 Introduction to the proof

We want to prove the following theorem ([8, Thm 1]):

Theorem 1.1. *Take any three non-constant polynomials $f, g, h \in \mathbb{C}[x]$: if $f(x) = g(h(x))$ and f has at most l non-constant terms, then $h(x)$ has at most $B(l)$ terms.*

We observe that the bound $B(l)$ is not only independent from the degrees and coefficients of the lacunary $f(x)$ but is also independent from any datum whatsoever about the polynomial $g(x)$. The original conjecture formulated by Erdős and Rényi is the particular case $g(y) = y^2$ and the theorem proven by Schinzel is the case $g(y) = y^d$.

We first say also that what Zannier proves is a dependence also on the degree d of the polynomial $g(x)$; he uses then another independent result (also by Zannier) to control d itself ([7, Thm 1]):

Proposition 1.2. *Take any three non-constant polynomials $f, g, h \in \mathbb{C}[x]$: if $f(x) = g(h(x))$ and f has at most l non-constant terms, then either $h(x)$ is of the form $ax^n + b$ or the bound $\deg g \leq 2l(l-1)$ holds.*

We now explain in a general way the strategy of the proof given in [8], before going into more detail. First we give an intermediate result, from which Theorem 1.1 can be deduced ([8, Prop 2]):

Theorem 1.3. *Take any three non-constant polynomials $f, g, h \in \mathbb{C}[x]$: if $f(x) = g(h(x))$ and f has at most l non-constant terms, then $h(x)$ can be written as the ratio of two polynomials with at most $B_1(l)$ terms.*

To prove Theorem 1.3 we work by induction on l. We consider the equation $f = g(h)$ from a purely formal point of view; the first thing is obtain the Puiseux expansion for h:

$$h = c_{-1} f^{1/d} + c_0 + c_1 f^{-1/d} + c_2 f^{-2/d} + \ldots = \sum_{i=-1}^{\infty} c_i f^{-i/d} \tag{1.2}$$

and after a reparametrisation $y = 1/x$, using the multinomial theorem on the terms $f^{-i/d}$ we can write $\tilde{h}(y) = y^{n_l/d} h(1/y)$ as sum of terms in y with only non-negative exponents. Therefore we must have a bound on these exponents:

$$(1+i)\frac{n_l}{d} + h_1 n_1 + h_2 n_2 + \ldots h_l n_l \leq \deg_y \tilde{h} = \deg_x h = \frac{n_l}{d}$$

and then a bound on i and h_j (which means a bound on the number of terms); if we had a condition of the form $n_1 \geq \varepsilon n_l$ then this last bound would be independent from the exponents n_j and could be expressed only in terms of l, d and ε. This is clearly not always the case, but we can use a trick to reconduct ourselves to this situation.

We divide the exponents n_j into two groups, the "small" ones $(n_1, \ldots, n_p)$ and the "large" ones $(n_{p+1}, \ldots, n_l)$ in a suitable way. Doing this we can consider the small ones as part of the coefficients and the large ones as satisfying the condition mentioned above: in this way we have a control on the number of terms as explained before, with the downside that now the coefficients are not anymore in $\mathbb{C}$ but in a function field $K \supseteq \mathbb{C}(x)$; at this point though we can use the inductive hypothesis, as these new coefficients are algebraic expressions containing a truncated f which will be a lacunary polynomial with at most $p < l$ terms.

This was the outline of the proof for Theorem 1.3: the reason why we have to use first this form of the result, where we allow ratios of polynomials, is that in the last mentioned step negative exponents might appear inside the coefficients containing the truncated f. Notice that deducing Theorem 1.1 from Theorem 1.3 is not immediate, as shown by this elementary example:

$$\frac{1-x^n}{1-x} = 1 + x + x^2 + \ldots + x^{n-1}$$

where the ratio of two polynomials with two terms each can have an arbitrarily large number of terms.

1.3 Proof of Theorem 1.3

Now we go into more details, keeping in mind the outline of the previous section.

As we said, we work by induction on l. Suppose $l = 1$, i.e. $f(x)$ has only one non-constant term: we can then subtract the eventual constant term from f and g without loss of generality and therefore suppose $g(h(x)) = a_1 x^{n_1}$; in this situation it's obvious that g can't have two distinct roots, hence $g(x) = b(x-\xi)^d$. Now $h(x) = \xi + (a/b)^{1/d} x^{n_1/d}$ is the only possible solution: in fact if any other solution not of this form existed then by Proposition 1.2 we would have $\deg g \leq 0$ which is absurd; so we obtain $B_1(1) = 2$.

We suppose now that the theorem is proven for $1, \ldots, l-1$. As we said, the first passage is to obtain an expression of the form (1.2) starting from the formal equation $f = g(h)$. Let's work concretely with an example to show the passages involved: suppose we have $f = h^2 - h$ (with $d = 2$). We start finding a solution of the form $h = cf^{1/2} + o(f^{1/2})$, substituting inside we see pretty easily that we can take $c = 1$ in order to obtain the cancellation of the highest powers of f in the expression; at this point we substitute inside the original equation $h = f^{1/2} + f^{1/2}h'$ (we precise that here h' is not the derivative of h, it's just a new formal variable):

$$\begin{aligned} 0 = h^2 - h - f &= (f^{1/2} + f^{1/2}h')^2 - (f^{1/2} + f^{1/2}h') - f \\ &= f^{1/2}\left(f^{1/2}h'^2 + 2f^{1/2}h' - h' - 1\right) \end{aligned}$$

thus obtaining a new equation $f^{1/2}h'^2 + 2f^{1/2}h' - h' - 1 = 0$. Now we repeat the above steps: we find a solution of the form $h' = cf^{-1/2} + o(f^{-1/2})$ to eliminate the highest powers of f, we can choose $c = \frac{1}{2}$ for this purpose, then we substitute $h' = \frac{1}{2}f^{-1/2} + f^{-1/2}h''$ (again,

h'' is not the derivative of h'):

$$\begin{aligned}0 &= f^{1/2}h'^2 + 2f^{1/2}h' - h' - 1\\ &= f^{1/2}\left(\frac{1}{2}f^{-1/2} + f^{-1/2}h''\right)^2 + 2f^{1/2}\left(\frac{1}{2}f^{-1/2} + f^{-1/2}h''\right) - \left(\frac{1}{2}f^{-1/2} + f^{-1/2}h''\right) - 1\\ &= f^{-1/2}h''^2 + 2h'' - \frac{1}{4}f^{-1/2}\end{aligned}$$

At this point going back to the original h we have already obtained a solution of the form $h = f^{1/2} + \frac{1}{2} + o(f^{-1/2})$; clearly we only need to go on with this process and we'll obtain an expression of the form (1.2) for h.

Now we have obtained an expansion of h as a formal series in f starting from the original equation $f = g(h)$. As anticipated, we operate the substitution $y = 1/x$, and we define:

$$\begin{aligned}\tilde{h}(y) &:= x^{-n_l/d}h(x) = y^{n_l/d}h(1/y)\\ \tilde{f}(y) &:= \frac{f(x)}{a_l x^{n_l}} =: 1 + b_1 y^{n_1} + \ldots + b_l y^{n_l}\end{aligned}$$

In the first definition notice that $\deg_x h = \deg_y \tilde{h} = n_l/d$ so that in fact $\tilde{h}$ is still a polynomial, and it has also the same number of terms as h, so it will suffice to prove the thesis for $\tilde{h}$; in the second definition notice that we have renominated both the coefficients and the exponents, but it won't matter (in accordance with the spirit of the theorem itself that doesn't care about the degrees of the terms of f).

At this point we introduce the (for the moment arbitrary) distinction between "small" and "large" exponents n_j. We fix an integer p between 0 and $l-1$ and we define:

$$\delta_p(y) := 1 + b_1 y^{n_1} + \ldots + b_p y^{n_p}$$

obtaining therefore:

$$\begin{aligned}\tilde{f}(y) &= \delta_p(y)\left(1 + \frac{b_{p+1}}{\delta_p(y)}y^{n_{p+1}} + \ldots + \frac{b_l}{\delta_p(y)}y^{n_l}\right)\\ \tilde{f}(y)^{s/d} &= \delta_p(y)^{s/d}\left(1 + \frac{b_{p+1}}{\delta_p(y)}y^{n_{p+1}} + \ldots + \frac{b_l}{\delta_p(y)}y^{n_l}\right)^{s/d}\\ &= \sum_{h_{p+1},\ldots,h_l\in\mathbb{N}} C_{s,d,h_{p+1},\ldots,h_l}\delta_p(y)^{\frac{s}{d}-h_{p+1}-\ldots-h_l} b_{p+1}^{h_{p+1}}\ldots b_l^{h_l} y^{h_{p+1}n_{p+1}+\ldots+h_l n_l} \qquad (1.3)\end{aligned}$$

where the last passage uses the multinomial theorem. We substitute the definitions of $\tilde{h}$ and $\tilde{f}$ and the expression (1.3) inside (1.2); the result is that now $\tilde{h}(y)$ is a sum of terms of the form:

$$C\delta_p(y)^{\frac{s}{d}-h_{p+1}-\ldots-h_l} y^{\frac{1}{d}(1-s)n_l + h_{p+1}n_{p+1}+\ldots+h_l n_l} \qquad (1.4)$$

Hence at this point we can collect all "too big" terms (with regards to the exponent of y) in an error term and write:

$$\tilde{h}(y) = t_1 + t_2 + \ldots + t_L + O(y^{2n_l}) \qquad (1.5)$$

where the t_i are the terms (1.4) having exponent $< 2n_l$ for y.

Now let's stop for a moment and think about what we have obtained and what we still have to find. The last equation is a good result but it has some issues that must be solved in order to prove Theorem 1.3 as we would like to: the first problem is that the number of terms L is bounded by something that depends not only on l (and possibly d) but also on the ratio n_l/n_{p+1}; we can say in fact that:

$$1-2d \leq s \leq 1, \qquad 0 \leq h_i \leq \frac{2n_l}{n_i},$$
$$L \leq (2d+1)\left(1+\frac{2n_l}{n_i}\right)^{l-p} \leq (2l-1)^2\left(1+\frac{2n_l}{n_{p+1}}\right)^{l} \tag{1.6}$$

but for now we still have to show how to control n_l/n_{p+1} only in terms of l (this will obviously have something to do with our choice of p). The other problem is that we have y also in the coefficients δ_p, so it's not obvious at all that we can just ignore the error term $O(y^{2n_l})$ as the $2n_l$ refers only to the exponent of y and nothing is known about the contribution of the coefficient.

Let's see how to solve these issues. In (1.5) we can suppose the t_i to be linearly independent by possibly substituting them with multiples; we can then distinguish two cases: $\tilde{h}, t_1, \ldots, t_L$ being linearly dependent or independent over $\mathbb{C}$.

In the first case what we basically obtain is the elimination of the error term in (1.5). Also, all the terms t_i where we have some $\delta_p^{j/d}$ not being a polynomial must cancel each other out in the equation, thus leaving $\tilde{h}$ expressed as the sum of terms of the form:

$$C\eta_p(y)^{\frac{1}{e}(s-(h_{p+1}+\ldots+h_l)d)}y^{\frac{1}{d}(1-s)n_l+h_{p+1}n_{p+1}+\ldots+h_ln_l} \tag{1.7}$$

where e is the smallest divisor of d such that $\eta_p(y)=\delta_p(y)^{e/d}$ is still a polynomial. At this point though $\eta_p(y)^{d/e}=\delta_p(y)$ and the right hand side is a lacunary polynomial of $p<l$ non-constant terms, so by inductive hypothesis $\eta_p(y)$ is ratio of polynomials with at most $B_1(p) \leq B_1(l-1)$ terms, and combining this with the information about the number of terms t_i we get a certain bound $B_2(l, n_l/n_{p+1})$.

In the second case we use the following lemma ([8, Prop 1]):

Lemma 1.4. *Let $K/\mathbb{C}$ be a function field in one variable of genus $\mathfrak{g}$, let $\varphi_1, \ldots, \varphi_n \in K$ be linearly independent over $\mathbb{C}$ and let $\sigma = \sum_{i=1}^n \varphi_i$; take $0 \leq r \leq n$ and call S a finite set of places of K containing all the poles of $\varphi_1, \ldots, \varphi_n$ and all the zeros of $\varphi_1, \ldots, \varphi_r$. We have then:*

$$\sum_{v\in S}\left(v(\sigma)-\min_{i=1}^{n} v(\varphi_i)\right) \leq \binom{n}{2}(\#S+2\mathfrak{g}-2)+\sum_{i=r+1}^{n}\deg\varphi_i$$

This lemma controls the valuation of the sum σ in terms of the valuations and the degrees of its addenda (and of the data about the field, too). We use it in our situation in the following way:

$$r=L, \qquad n=L+1, \qquad \varphi_i=-t_i (1\leq i\leq L), \qquad \varphi_{L+1}=\tilde{h}$$

The set S containing the poles and zeros of the t_i and the poles of $\tilde{h}$ has at most $d(n_p+2)$ places, while $2\mathfrak{g}-2 \leq dn_p$; here we have that the sum σ is the error term in (1.5) with $v_0(\sigma) \geq 2n_l$, where v_0 is a place above 0 and belongs to S. Using Lemma 1.4 we obtain:

$$2n_l \leq \binom{L+1}{2}(d(n_p+2)+dn_p)+n_l$$

and then:

$$n_l/n_p \leq 2^{4l+5} d^3 (n_l/n_{p+1})^{2l} \leq 2^{4(l+2)} l^3 (l-1)^3 (n_l/n_{p+1})^{2l} \tag{1.8}$$

At this point we are done: in fact for each p (and each version of (1.5)) we either have a bound $B_2(l, n_l/n_{p+1})$ or an estimate (1.8). Therefore we consider the biggest p such that the first alternative occurs and we have the bound B_2, but iterating (1.8) for the p' between $p+1$ and l we can reconduct ourselves to $n_l/n_l = 1$ and get a bound $B_1(l)$ depending only on l; if the first alternative never occurs then we can use (1.8) from n_l/n_1 to $n_l/n_l = 1$, and find a bound $B_1(l)$ as described in the outline.

1.4 Proof of Theorem 1.1

Finally we can deduce Theorem 1.1 from Theorem 1.3. Suppose we have $f(x) = g(h(x))$ with $h(x)$ not of the form $ax^n + b$ (so that $\deg g \leq 2l(l-1)$ by Proposition 1.2); from the previous result we have that $h(x)$ is a ratio $h_1(x)/h_2(x)$ of two polynomials with at most $B_1(l)$ terms. We multiply $f(x) - g(h(x)) = 0$ by a suitable power of $h_2(x)$ so as to obtain an equation in $\mathbb{C}[x]$: now, since the whole left hand side must vanish, necessarily there must be equalities involving the exponents of the resulting monomials, which give a linear system of the exponents of f, h_1, h_2; since the number of monomials is bounded dependently only on l, also the number of possible linear systems is bounded only in terms of l.

We solve the linear system, so that the exponents of f, h_1, h_2 are now combinations of some variables u_j: the number J of these variables and the resulting coefficients in the combinations depend only on the linear system, therefore they're all bounded by a certain function of l only. At this point we consider f, h_1, h_2 in a different way, i.e. as functions depending on the u_j in the following way:

$$f(x) = F(x^{u_1}, \ldots, x^{u_J}), \qquad h_{1,2}(x) = H_{1,2}(x^{u_1}, \ldots, x^{u_J})$$

where $F, H_1, H_2 \in \mathbb{C}[z_1^{\pm 1}, \ldots, z_J^{\pm 1}]$. The u_j can be chosen arbitrarily in $\mathbb{Z}$, so the equality $f = g(h_1/h_2)$ (which holds for every choice of the u_j) gives in fact $F = g(H_1/H_2)$; but then H_1/H_2 must also be in $\mathbb{C}[z_1^{\pm 1}, \ldots, z_J^{\pm 1}]$ as this is integrally closed. Moreover, its degree is limited by the sum of the degrees of H_1, H_2, thus giving us a limitation on the number of terms of H_1/H_2 which is bounded by $(1 + 2\deg H_1 + 2\deg H_2)^J$: all these can be bounded by functions of l as they depend only on the linear system, so that we have finally the same bound $B(l)$ for the number of terms of $h(x)$ too.

Chapter 2

General case

2.1 Introduction to the proof

We want now to prove the more general theorem ([2, Thm 1.1]):

Theorem 2.1. *Take any polynomial $F(x, y) \in \mathbb{C}[x, y]$ monic of degree d in y and having at most l terms in x: if there is $h(x) \in \mathbb{C}[x]$ such that $F(x, h(x)) = 0$, then $h(x)$ has at most $\beta(d, l)$ terms.*

As we notice the dependence of the bound by d reappears, since Proposition 1.2 can't be applied in this situation, but $\beta(d, l)$ is still independent from the degrees of the terms in x and from any coefficient appearing in the polynomial F. Theorem 2.1 contains Theorem 1.1 as a special case, when $F(x, y) = g(y) - f(x)$.

Again we make use of an intermediate result ([2, Prop 2.5]):

Theorem 2.2. *Take any polynomial $F(v_1, \dots, v_l, y) \in \mathbb{C}[v_1, \dots, v_l, y]$ monic in y and of degree at most d in each variable: if there is $h(x) \in \mathbb{C}[x]$ and there are $n_1, \dots, n_l \in \mathbb{N}$ such that $F(x^{n_1}, \dots, x^{n_l}, h(x)) = 0$, then $h(x)$ can be written as the ratio of two polynomials with at most $\beta_1(d, l)$ terms.*

The technique used to prove Theorem 2.2 follows a very similar path to that used for Theorem 1.3, although filled with many more annoying details. We divide the exponents n_j in "small" ones and "big" ones and we still obtain a Puiseux expansion for h as (1.2) (although with a different procedure): notice that once this is done in a suitable way we are approximately in the same situation as in the previous chapter, because while working with the Puiseux expansion we didn't use any information about its origin (i.e. the polynomial $g(x)$) except for its degree d which appeared in fact in the expansion itself; therefore a very similar reasoning can be used to treat the Puiseux expansion that we are going to obtain from $F(x, y)$.

As before, we write h as the sum of a certain (bounded) number of "small" terms with coefficients in a function field $K \supseteq \mathbb{C}(x)$ and a "big" error term as in (1.5): Lemma 1.4 still holds, so again we have either a bound like (1.8) that links n_p to n_{p+1} or a bound coming from the elimination of the big error term, the information about the number of the small terms and the inductive hypothesis that provides a β_1 depending on $p < l$. The annoying details that render the proof of Theorem 2.2 more than just a mere rewriting of the previous

one are concentrated mostly in the process of obtaining the Puiseux expansion; moreover, we won't be able to have nice terms of the form (1.4) where the $\delta_p(x)$ containing the small exponents appears just as a power in the coefficients, but in general the dependence from δ_p would be more complicated, leading to other technical difficulties.

We'll focus on these two issues, observing that the rest of the proof will use the same framework as in Theorem 1.3.

2.2 Theorem 2.2: Puiseux expansion

Let's start with the Puiseux expansion. Remember that in the previous situation we were constructing the expansion by requiring the cancellation of the highest powers and then performing a change of variables at the end to obtain an error term that collects the terms with high exponents (that would have been low exponents in the original variable): now we use a more direct approach and require the elimination of the smallest powers from the beginning.

Consider again a concrete example: suppose that $F(x,y) = x^2 + 2yx + y^2 + y^2x^2$ (we always suppose for simplicity that $x \nmid F(x,y)$). In Theorem 1.3 we always start with a solution of the form $h = cf^{1/d} + o(f^{1/d})$, while in this situation we just require that there will be some form of cancellation of the lowest terms, leaving freedom also in the choice of the exponent. Let's say we take $y = -x+o(x)$, that leads to cancellations in the first three terms of F; the next step is to obtain a new expression with a new y' and continue the expansion of y term by term, and this will be done in two different ways according to the nature of the solution chosen. If the solution $y = cx^e + o(x^e)$ is such that the lowest terms of F (where the cancellation occurs) are of the form $sx^t(y - cx^e)^u$ for suitable s, t, u, we follow the strategy called (S1) in [2]: the next expression will be $F(x,y) = F(x, cx^e + y')$; our example satisfies this condition, as $x^2+2yx+y^2 = (y+x)^2$, so to obtain the next term of the expansion we will work with $F(x, -x + y') = x^4 - 2y'x^3 + y'^2 + y'^2x^2$. If the condition is not satisfied then we use the strategy (S2): the new expression will be then $x^{-t}F(x, cx^e + x^e y')$ with a suitable t such that x does not divide everything; given for example $F(x,y) = x^2 + 3yx + 2y^2 + y^2x^2$ we still have the possible solution $y = -x + o(x)$ but we'll have to adopt (S2) in this case, giving us $x^{-2}F(x, -x + xy') = x^2 - y - 2yx^2 + 2y^2 + y^2x^2$. Notice that (S2) is basically the strategy always adopted in the analogous situation of Theorem 1.3.

The two strategies don't produce different solutions, but only different ways of writing the same solution. Considering the first example we made, using always (S1) or always (S2) regardless of the aforementioned condition, choosing appropriately c and e at every step we obtain the same result:

$$y_{(S1)} = -x + ix^2 + x^3 - ix^4 - x^5 + \dots$$
$$y_{(S2)} = -x + x(ix + x(x + x(-ix + x(-x + \dots))))$$

The same would happen using any random sequence of choices between (S1) and (S2), altering only the placement of the parentheses but not the nature of the solution.

So why do we adopt such a technique to find the Puiseux expansion if it's the same in any case? The reason is in the behaviour of the error term in the more general case when the number p of small exponents is positive, and then the field K of the coefficients of the variable y is bigger than $\mathbb{C}$. Consider a polynomial $F(x,y) \in K[x,y]$ with $K \supseteq \mathbb{C}(x)$: the variable x is present both in the expression F and its coefficients, so a way to find a

Puiseux expansion is to consider formally $F(z,y) \in K[z,y]$ with $K \supseteq \mathbb{C}(x)$, then extract an expansion of y with respect to z and at the end substitute again $z = x$; this is what happened in Theorem 1.3 where we treated δ_p as a coefficient disregarding the x hidden inside it. Unfortunately the situation is not as nice as before: in fact $\delta_p(x)^s x^t = O(x^t)$ for any $s \in \mathbb{Z}$ since $\delta_p(x) = 1 + b_1 x^{n_1} + \ldots + b_p x^{n_p}$, but for a more arbitrary $a(x) \in K$ even if we have $a(x)z^t = O(z^t)$ we don't have also $a(x)x^t = O(x^t)$; this means that even if using the formal variable z we get a sufficiently big error term (with respect to z) it's not guaranteed that the error term remains big when seen with respect to x, leading ultimately to the impossibility of using Lemma 1.4. The alternation between (S1) and (S2) becomes useful for the following reason: it turns out that the final substitution $z = x$ is relatively painless when (S1) is used, while it's possible to make it work in the (S2) case at the cost of a modification of the meaning of "small" and "large" exponents; however, with the condition provided, it is possible to prove that (S2) occurs only in a finite number of steps, thus saving the whole argument.

We will be more explicit in the next chapter, where the details will be important to work out the actual bound; for now we just expose things to have a better understanding of the situation. Let $F(z,y)$ be of the form:

$$F(z,y) = \sum_{i=0}^{d} y^i \sum_{j=0}^{s_i} a_{ij} z^{r_{ij}} \tag{2.1}$$

with $a_{ij} \in K \supseteq \mathbb{C}(x)$ coefficients collecting the small exponents (which we express by bounding the height of the a_{ij} by a certain m) and with r_{ij} being the large exponents (which we express by saying that the smallest of the nonzero r_{ij} is at least ε times the biggest one, for a certain ε); then the following facts are true:

- (S2) is used at most $d+1$ times ([2, Prop 4.5]).
- Suppose we have an expansion:

  $$y = c_1 z^{e_1} + c_2 z^{e_2} + \ldots + c_j z^{e_j} + O(z^{e_{j+1}})$$

  obtained using at all steps always the strategy (S1), and suppose that m is small enough, i.e. not comparable to the smallest nonzero r_{ij}; then for $F(x,y)$ we also have an expansion:

  $$y = c_1 x^{e_1} + c_2 x^{e_2} + \ldots + c_j x^{e_j} + O(x^{e_j - \delta_j})$$

  where δ_j is small, in the sense that it's linearly bounded by m ([2, Prop 5.2]). Since we always use (S1) it can be seen that the coefficients $c_1, \ldots, c_j$ still belong to K and their height is still linearly bounded by m; also the exponents $e_1, \ldots, e_j$ are positive linear combinations of the r_{ij}: these facts imply that we can continue the expansion without changing the initial data m, ε that regulate the meaning of "small" and "large", which is why we consider (S1) to be the reasonable one between the two strategies and we want to use it in all but finitely many steps.
- Suppose now that we are not in the nice situation described above: this means that either we are starting already with (S2) or that the first term of the expansion is not large enough; in fact previously e_1 was a positive combination of the r_{ij}, which means at least as big as the smallest of them (if nonzero): this is not always the case, and the conditions above don't take care of this situation.

It's at this point that the use of the less intuitive writing of the polynomial $F(x,y)$ as $F(x^{n_1},\dots,x^{n_l},y)$ becomes important. At the beginning clearly the idea is that the n_i (more precisely the "large" ones among the n_i) and the r_{ij} are chosen to be the same thing, which we express by the concept that every r_{ij} is $\vec{e}_k\cdot\vec{n}$ for the vector $\vec{n}=(n_{p+1},\dots,n_l)$ and some $\vec{e}_k=(0,\dots,0,1,0,\dots,0)$. However, we can change the meaning of the n_i in such a way that we still have $r_{ij}=\vec{q}_k\cdot\vec{n}$ for some $\vec{q}_k$ with bounded integer values and at the same time satisfy the condition that the linear combinations of the r_{ij} that will appear while working with the Puiseux expansion are at least $\varepsilon|\vec{n}|_\infty$ (which is the same nice condition that we had in the previous point); this operation obviously comes at a certain cost: namely, some of the new n_i may turn out to be "small" in the new situation, which in general changes the value of p,m,ε.

With this technical condition fulfilled, we can use (S2) without much pain; if m is small enough (in the sense already described in the previous case) we find an expansion:

$$y=cx^e+x^eO(x^\delta)$$

where δ is big (i.e. linearly bounded from below by $\varepsilon|\vec{n}|_\infty$), e is a rational combination of the r_{ij} and $c\in\overline{K}$ with height bounded in terms of m ([2, Prop 5.3]). Notice that this time the field K must be enlarged to $K(c)$ at the next step but the genus (fundamental datum when using Lemma 1.4) can still be controlled: the change of the field is another good reason to use (S2) only finitely many times; also, even if the expansion features rational exponents it's easy to see that we can suppose them to be integers: taking a new variable x' with $x'^n=x$ for a suitable n does not change the proof, since if $h(x^n)$ is the ratio of two polynomials with at most β terms then the same can be said about $h(x)$ (with the same β, [2, Lemma 2.8]).

Following the results above, we manage then to expand y in the polynomial $F(x,y)$ as:

$$y=\sum_{\vec{q}}c_{\vec{q}}x^{\vec{q}\cdot\vec{n}}+\sigma \tag{2.2}$$

where σ can be taken big enough to use effectively Lemma 1.4; we find ourselves in the same situation as in the proof of Theorem 1.3: $\{\vec{q}\}$ is a bounded collection, the field K has a well-bounded genus, the entries n_i of $\vec{n}$ are considered large (i.e. $n_i\geq\varepsilon|\vec{n}|_\infty$ for a certain independent ε).

2.3 Theorem 2.2: linear dependence

As said before, the other important issue that distinguishes Theorem 2.2 from Theorem 1.3 is the way the coefficients $c_{\vec{q}}$ in (2.2) depend on the small exponents n_i: in (1.5) the terms t_i simply contained a rational power of $\delta_p(y)$ (the polynomial made of the small monomials), but in this case it's not as easy.

In the previous chapter we distinguished the two cases of $\tilde{h},t_1,\dots,t_L$ being linearly dependent or independent, and we're doing the same also here. If we suppose $y,c_{\vec{q}}x^{\vec{q}\cdot\vec{n}}$ to be independent we apply Lemma 1.4 obtaining an estimate of the type $m\geq\varepsilon'|\vec{n}|_\infty$: this ideally corresponds to the bound (1.8), as the indicator of "small" quantities (m here, n_p before) is in both cases chained to the indicator of "large" quantities ($\varepsilon|\vec{n}|_\infty$ here, n_{p+1} before); if we

suppose them to be dependent we practically obtain the elimination of the σ in (2.2): this is the case we examine now.

Let then $h(x)$ be the sum of some $c_{\vec{q}} x^{\vec{q}\cdot\vec{n}}$ (a subset of the terms in (2.2); also the $c_{\vec{q}}$ now are possibly $\mathbb{C}$-multiples of the previous ones). K is constructed using the $c_{\vec{q}}$ which are coefficients of the Puiseux expansion, thus being algebraic expressions of the x^{n_i} (the small ones); now we repeat in a more general context what happened in Theorem 1.3.

Consider elements $a_{\vec{q}} \in \overline{\mathbb{C}(v_1, \ldots, v_p)}$ which we think of as the $c_{\vec{q}}$ with v_i instead of x^{n_i}; the $a_{\vec{q}}$ will generate a field $K_v \supseteq \mathbb{C}(v_1, \ldots, v_p)$ and given a primitive element b in it we can write them as:

$$a_{\vec{q}} = \sum_{j=0}^{e-1} C_{\vec{q}j} b^j \tag{2.3}$$

for some e and some $C_{\vec{q}j} \in \mathbb{C}(v_1, \ldots, v_p)$. We then take a valuation ring $\mathcal{O} \subseteq K_v$ and the projection map $\pi : \mathcal{O} \to \overline{\mathbb{C}(x)}$ defined in the intuitive way: we send v_i to x^{n_i}, so that $a_{\vec{q}}$ becomes $c_{\vec{q}}$ and K_v becomes K. Take as an example the case of Theorem 1.3: we have coefficients $c_{\vec{q}}$ of the form $C\delta_p(x)^{j/d}$ and K generated by $\delta_p(x)^{1/d}$ over $\mathbb{C}(x)$, so we consider $a_{\vec{q}} = C(1 + v_1 + \ldots + v_p)^{j/d}$ and K_v generated by $b = (1 + v_1 + \ldots + v_p)^{1/d}$ over $\mathbb{C}(v_1, \ldots, v_p)$ (e indicates the same thing in both cases).

In this specific example everything works smoothly: writing $h(x)$ as a combination of $\pi(a_{\vec{q}})$ and using (2.3) we have that all terms with $j > 0$ must cancel out, leaving us only some $C_{\vec{q}ej} = Cb^{ej} = C\eta_p(x)^j$ with $C \in \mathbb{C}$; then the inductive hypothesis saves us and gives the bound on the terms of the ratio that we were longing for. This is not in general the case: in fact the $C_{\vec{q}j}$ could be outside $\mathcal{O}$ and then $\pi(C_{\vec{q}j})$ could be not well-defined; or the minimal polynomial for b could have coefficients outside $\mathcal{O}$ and then $\pi(b)$ could in general be not an algebraic function.

This problem though is easily avoidable: in fact this means that we can find a polynomial at the denominator of the $C_{\vec{q}j}$ or of the coefficients of the minimal polynomial which goes to 0 through π; but then this implies a relation between the exponents n_i since at least two different monomials must specialize to something with the same degree, thus giving us:

$$k_1 n_1 + \ldots + k_p n_p = 0 \tag{2.4}$$

for some suitably bounded integers k_i. Thanks to this we can express n_1 as combination of $n_2, \ldots, n_p$ (assuming for example $k_1 \neq 0$) and decrease the number of variables v_i we're dealing with: again, the inductive hypothesis concludes the job.

When everything is already inside $\mathcal{O}$ we can follow the same path as in Theorem 1.3. The rest of the proof of Theorem 2.2 is pretty much a rewriting of the previous one, and the exact same procedure that proves Theorem 1.1 proves also Theorem 2.1.

Chapter 3

Explicit bounds

3.1 Bound for Theorem 1.3

We provide now explicit values for the bounds in the various theorems we have encountered before. We start with the bound for Theorem 1.3:

Proposition 3.1. *Under the notation of Theorem 1.3 we have* $B_1(l) \leq 2^{(2l)^{16(2l)^{l-1}}}$ *for every integer* $l \geq 1$.

Proof. We notice immediately that for $l = 1$ we retrieve the easy bound $B_1(1) = 2 \leq 2^{2^{16}}$; from now on we suppose $l \geq 2$.

We re-examine now the proof of Theorem 1.3. We defined p as the number of "small" non-constant terms in the polynomial $f(x)$, and for each $0 \leq p \leq l-1$ we had only two possibilities: either $\tilde{h}(y)$ (which has the same number of terms as $h(x)$) can be written as a ratio of two polynomials with at most $B_2(l, n_l/n_{p+1})$ terms, or we can control n_l/n_p in terms of l and n_l/n_{p+1}.

Suppose that the first possibility is sometimes verified, and call p the biggest number for which this happens: in this case we have the bound $B_2(l, n_l/n_{p+1})$, but at this point we can express n_l/n_{p+1} in terms of l and n_l/n_{p+2}, then again n_l/n_{p+2} in terms of l and n_l/n_{p+3} and so on until we reach $n_l/n_l = 1$; in this way we would have established an absolute bound, depending only on l. Suppose instead that the first possibility never realizes: this means that with a similar process as before it's possible to control n_l/n_1 only in terms of l; it's then possible to find an upper bound to the number of terms using the fact that $\varepsilon_l n_l \leq n_1 < n_2 < \ldots < n_l$, where ε_l depends only on l.

Let's begin with the bound B_2. We recall that in the considered situation $\tilde{h}(y)$ is the sum of terms of the following shape:

$$C\eta_p(y)^{\frac{1}{e}(s-(h_{p+1}+\ldots+h_l)d)} y^{\frac{1}{d}(1-s)n_l+h_{p+1}n_{p+1}+\ldots+h_l n_l} \tag{3.1}$$

where we required that the exponent of y doesn't exceed $2n_l$; the bound on the number L of such terms is the one provided in (1.6). Also we know by inductive hypothesis that $\eta_p(y)$ can be written as ratio of two polynomials with at most $B_1(p) \leq B_1(l-1)$ terms; finally its exponent E has absolute value at most:

$$E \leq d(2 + (l-p)2n_l/n_{p+1}) \leq 4l(l-1)(1 + ln_l/n_{p+1})$$

After bringing everything to common denominator we have L terms (3.1) each with at most $B_1(l-1)^{E+1}$ at the numerator and denominator, since the exponent of $\eta_p(y)$ ranges from 1 to $-E$; hence:

$$B_2(l, n_l/n_{p+1}) \leq (2l-1)^2(1+2n_l/n_{p+1})^l B_1(l-1)^{4l(l-1)(1+ln_l/n_{p+1})+1} \tag{3.2}$$

Now we estimate n_l/n_{p+1}. It's sufficient to iterate the estimate found in (1.8):

$$\begin{aligned} n_l/n_{p+1} &\leq 2^{4(l+2)}l^3(l-1)^3(n_l/n_{p+2})^{2l} \\ &\leq \left[2^{4(l+2)}l^3(l-1)^3\right]^{1+2l+\ldots+(2l)^{l-p-2}} \\ &\leq \left[2^{4(l+2)}l^3(l-1)^3\right]^{2(2l)^{l-2}} \end{aligned} \tag{3.3}$$

Then we put this in (3.2). We work first with the exponent:

$$\begin{aligned} 4l(l-1)(1+ln_l/n_{p+1})+1 &\leq 4l(l-1)\left(1+l\left[2^{4(l+2)}l^3(l-1)^3\right]^{2(2l)^{l-2}}\right)+1 \\ &\leq 8l^3\left[2^{4(l+2)}l^6\right]^{2(2l)^{l-2}} = 2^{3+8(l+2)(2l)^{l-2}}l^{3+12(2l)^{l-2}} \\ &\leq 2^{2^{l+2}l^{l-1}}l^{2^{l+2}l^{l-2}} =: K(l) \end{aligned}$$

and then with the coefficient:

$$\begin{aligned} (2l-1)^2(1+2n_l/n_{p+1})^l &\leq (2l-1)^2\left(1+2\left[2^{4(l+2)}l^3(l-1)^3\right]^{2(2l)^{l-2}}\right)^l \\ &\leq 4l^2 2^l\left[2^{4(l+2)}l^6\right]^{(2l)^{l-1}} = 2^{2+l+4(l+2)(2l)^{l-1}}l^{2+6(2l)^{l-1}} \\ &\leq 2^{2^{l+2}l^l}l^{2^{l+2}l^{l-1}} =: H(l) \end{aligned}$$

thus obtaining $B_1(l) \leq H(l)B_1(l-1)^{K(l)}$.

We already observed at the beginning that the bound was verified for $l=1$. Supposing now the statement true for $l-1$, we want then to prove:

$$H(l)\cdot 2^{K(l)\cdot(2l-2)^{16(2l-2)^{l-2}}} \leq 2^{(2l)^{16(2l)^{l-1}}} \tag{3.4}$$

We start working with the exponent on the left hand side:

$$\begin{aligned} K(l)\cdot(2l-2)^{16(2l-2)^{l-2}} &\leq 2^{2^{l+2}l^{l-1}}l^{2^{l+2}l^{l-2}}(2l)^{16(2l)^{l-2}} \\ &= 2^{8(2l)^{l-1}+16(2l)^{l-2}}\cdot l^{16(2l)^{l-2}+16(2l)^{l-2}} \\ &\leq (2l)^{16(2l)^{l-1}-16(2l)^{l-2}} \end{aligned}$$

Using this in (3.4) and passing to the logarithm we find:

$$\begin{aligned} \log_2 H(l) + (2l)^{16(2l)^{l-1}-16(2l)^{l-2}} &\leq 2^{l+2}l^l + 2^{l+2}l^{l-1}\log_2 l + (2l)^{16(2l)^{l-1}-16(2l)^{l-2}} \\ &\leq 8(2l)^l + (2l)^{16(2l)^{l-1}-16(2l)^{l-2}} \\ &\leq \left(\frac{16(2l)^{l-2}}{(2l)^{16(2l)^{l-2}}}\cdot 2l^2+1\right)(2l)^{16(2l)^{l-1}-16(2l)^{l-2}} \\ &\leq (2l)^2(2l)^{16(2l)^{l-1}-16(2l)^{l-2}} \leq (2l)^{16(2l)^{l-1}} \end{aligned}$$

thus proving the bound we were looking for.

The case when the bound B_2 never realizes for any p is easy now. In fact n_l/n_1 is controlled with the same bound as in (3.3) and $\tilde{h}(y)$ is the sum of $\gamma_0 y^{n_l/d}$ and some terms with the exponent of y being $h_1 n_1 + \ldots + h_l n_l \leq n_l/d \leq n_l$; hence the number of terms is bounded by:

$$1 + \left(1 + \left[2^{4(l+2)} l^3 (l-1)^3\right]^{2(2l)^{l-2}}\right)^l$$

which is in turn already smaller than $H(l)$. □

3.2 Bound for Theorem 1.1

The next bound the retrieve is the one in Theorem 1.1.

Proposition 3.2. *Under the notation of Theorem 1.1 we have $B(l) \leq B_1(l)^{5B_1(l)^2}$ for every integer $l \geq 1$, where $B_1(l)$ is the bound of Proposition 3.1.*

Proof. Again, we re-examine the proof of Theorem 1.1. We write explicitly the equation $f(x) - g(h_1(x)/h_2(x)) = 0$:

$$\begin{aligned} f(x) &= \sum_{i=1}^{l} a_i x^{m_i}, \qquad g(x) = \sum_{j=0}^{d} b_j x^j, \qquad h_r(x) = \sum_{k=1}^{B_1(l)} c_{rk} x^{n_{rk}} \quad (r = 1, 2) \\ 0 &= h_2(x)^d (f(x) - g(h_1(x)/h_2(x))) \\ &= \left(\sum_{k=1}^{B_1(l)} c_{2k} x^{n_{2k}}\right)^d \left(\sum_{i=1}^{l} a_i x^{m_i}\right) - \sum_{j=0}^{d} b_j \left(\sum_{k=1}^{B_1(l)} c_{1k} x^{n_{1k}}\right)^j \left(\sum_{k=1}^{B_1(l)} c_{2k} x^{n_{2k}}\right)^{d-j} \end{aligned}$$

As we can observe, when we build the linear system of the exponents m_i, n_{1k}, n_{2k} the coefficients that appear are all bounded by d ($\leq 2l(l-1)$ by Proposition 1.2); also, if J is the number of independent parametres for the solution of the system, then it is limited by the total number of variables, i.e. $J \leq l + 2B_1(l)$. Solving the linear system we find that the coefficients $v_j^{(\cdot)}$ in the solution:

$$m_i = \sum_{j=1}^{J} v_j^{(i)} u_j, \qquad n_{1k} = \sum_{j=1}^{J} v_j^{(1k)} u_j, \qquad n_{2k} = \sum_{j=1}^{J} v_j^{(2k)} u_j$$

are determinants of square matrices of side $l + 2B_1(l) - J$ and entries bounded by d; this technically does not catch all the solutions, because we need the $v_j^{(\cdot)}$ to be integer, but what we have is sufficient as in the proof we need only to be able to choose the u_j arbitrarily in $\mathbb{Z}$. A bound on these determinants is given then by $(l + 2B_1(l) - J)! d^{l+2B_1(l)-J}$, and we notice that they are also the degrees of the monomials appearing in H_1, H_2, so that in the end:

$$\begin{aligned} B(l) &\leq \left(1 + 4(l + 2B_1(l) - J)! d^{l+2B_1(l)-J}\right)^J \leq \left(1 + 4(l + 2B_1(l))! d^{l+2B_1(l)}\right)^{l+2B_1(l)} \\ &\leq 4^{l+2B_1(l)} (l + 2B_1(l))!^{l+2B_1(l)} (2l^2)^{(l+2B_1(l))^2} \\ &\leq 2^{(l+2B_1(l))^2 + 2(l+2B_1(l))} l^{2(l+2B_1(l))^2} e^{l+2B_1(l)-(l+2B_1(l))^2} (l + 2B_1(l))^{l+2B_1(l)+(l+2B_1(l))^2} \end{aligned}$$

where the last inequality uses the fact that $x! \leq ex(x/e)^x$; also $2^{x^2+2x}e^{x-x^2} < 1$ when the condition $x \geq 1 + 2 \cdot 2^{2^{16}}$ is satisfied, therefore we obtain:

$$\begin{aligned} B(l) &\leq l^{2(l+2B_1(l))^2}(l+2B_1(l))^{l+2B_1(l)+(l+2B_1(l))^2} \\ &\leq l^{18B_1(l)^2}(3B_1(l))^{l+2B_1(l)+l^2+4lB_1(l)}3^{4B_1(l)^2}B_1(l)^{4B_1(l)^2} \\ &\leq (l^{18}3^{12})^{B_1(l)^2}B_1(l)^{8lB_1(l)}B_1(l)^{4B_1(l)^2} \end{aligned}$$

We have also easily that $16l \leq 3^{24}l^{36} \leq B_1(l)$, and this finally proves our thesis. □

We can compare this bound with what Schinzel found in the special case of his conjecture. The bound $T(d,l)$ given in (1.1) (with the not very restrictive hypothesis that the maximum is not achieved by 2) combined with the bound on d given by Proposition 1.2 (be careful that l includes the constant term in the first case and it doesn't in the second) gives us:

$$\begin{aligned} T(d,l) &\leq 1 + e^{(2^{l-d-1}-1)(d\ln 4d - \ln d)} \leq e^{2^{l-1}d\ln 4d} = (4d)^{2^{l-1}d} \\ &\leq (8l(l+1))^{2^l l(l+1)} \leq (4l)^{2^{l+2}l^2} \end{aligned}$$

which, as Zannier thought, is a much stronger bound than $B(l)$ in this particular situation.

We add that in fact an even stronger bound exists, proven by Schinzel and Zannier [5], that reduces the double exponentiation of the original result by Schinzel to a single exponentiation; with the conditions already mentioned above we get:

$$T(d,l) \leq 1 + (4d)^{l-2} \leq (4l)^{2(l-2)}$$

3.3 Bound for Theorem 2.2: preliminary lemmas

These last sections deal with explicit bounds for the general case, examined in Chapter 2. The discussion here follows closely the results and passages contained in [2], so in order to thoroughly understand the whole argument it is advised to read it. Also, it has to be understood that sometimes not optimal approximations have been made in order to simplify the writing of some quantities: this has been done mostly to make possible to work with expressions that so many times had to be nested one into the other.

We start with a series of preliminary lemmas that estimate other quantities used in the main argument that were left mostly implicit in the original paper.

Lemma 3.3. $C_0(C) = C(C+1)^2$.

Proof. In [2, Prop 5.1] we are considering a polynomial $F(z,y)$ as in (2.1) where $d, s_i \leq C$ and the height of the a_{ij} is bounded by Cm, and we want to find a bound $h(F) \leq C_0 m$; but the height of F is trivially bounded by the sum of the heights of its coefficients, so:

$$h(F) \leq \sum_{i,j} h(a_{ij}) \leq \#\{a_{ij}\}_{i,j} Cm \leq (C+1)^2 Cm$$

thus giving our result. □

Lemma 3.4. $C_1(C) = 2C^2(C+1)^2$.

Proof. In [2, Prop 5.2] C_1 is defined as $2CC_0$, so we use Lemma 3.3. □

Lemma 3.5. $C_2(C) = C + C^2(C+1)^2$.

Proof. In [2, Prop 5.4] we are starting with $F(z,y)$ as in (2.1) with bounds $d, s_i \leq C$ and $h(a_{ij}) \leq Cm$; we also suppose that we are using the step (S2) to pass to a new polynomial $F_{new}(z,y)$:

$$F_{new}(z,y) = z^{-t}F(z, cz^e + z^e y) = \sum_{i,j,k} a_{ij}\binom{i}{k}c^k y^{i-k} z^{r_{ij}+ei-t}$$

where also $h(c) \leq C_0 m$, and we are first looking for a bound $C'm$ on the height of the coefficients of F_{new}. This is easy to find:

$$h\left(a_{ij}\binom{i}{k}c^k\right) \leq h(a_{ij}) + kh(c) \leq Cm + dC_0 m \leq (C + C^2(C+1)^2)m$$

and summing more of these terms together (to get the coefficients of F_{new}) gives the same bound, as height is in practice the degree with respect to x in this situation; therefore $C'(C) = C + C^2(C+1)^2$. The quantity C_2 has the purpose of allowing to reconduct ourselves to the original situation with the new polynomial F_{new}: C_2 is then defined as $\max\{C^2, C'\}$, where C^2 accounts for the other conditions that must be satisfied, involving for instance the number of terms of F_{new} and the degree of the extension $K(c)$; hence looking at the previous expression we clearly have $C_2 = C'$. □

Lemma 3.6. $\varepsilon_1(C,\varepsilon) = \frac{\varepsilon}{C(C+2)}$.

Proof. By definition in [2, Prop 5.4]. □

Lemma 3.7. $C_3(C) = C^{2C^3}$.

Proof. In [2, Prop 5.6] we are starting with a $q \times q$ square matrix Q ($q \leq C$) with rational entries with height bounded by C (in the proposition we are considering the logarithmic height, but in the rest of the paper the absolute height is implicitly used, so here the latter is used): we are searching for a bound C_3 on the height of $\det(Q)$ and of the entries of Q^{-1}. For the determinant we have:

$$H_{\mathbb{Q}}(\det(Q)) = H_{\mathbb{Q}}\left(\sum_{\sigma}\prod_{i=1}^{q} Q_{i\sigma(i)}\right) \leq q! C^{q^3} \leq C^{C^3+C}$$

The entries of the adjoint matrix of Q are determinants of smaller $(q-1)\times(q-1)$ matrices with the same entries as Q, so for the inverse matrix:

$$H_{\mathbb{Q}}((Q^{-1})_{ij}) \leq H_{\mathbb{Q}}(\det(Q))H_{\mathbb{Q}}(\mathrm{adj}(Q)_{ij}) \leq C^{C^3+C}C^{(C-1)^3+C-1} \leq C^{2C^3}$$

the last inequality being true for all integers $C \geq 1$. □

Lemma 3.8. $C_4(C) = C^{4C^3+1}$.

Proof. In [2, Cor 5.9] C_4 is defined as $CC_3(1+C_3)$: we can apply Lemma 3.7 to it with the slight improvement $1 + C_3 \leq C^{2C^3}$ which is true for every integer $C \geq 2$ (we are going in fact to work always with at least $C \geq 4$). □

Lemma 3.9. $\varepsilon_2(C,\varepsilon) = \frac{\varepsilon}{C^{2C^3+1}}$.

Proof. In [2, Cor 5.9] ε_2 is defined as $\frac{\varepsilon}{CC_3}$, so we just apply Lemma 3.7. □

Lemma 3.10. $\varepsilon_3(C,\varepsilon) = \frac{\varepsilon^{3C+4}}{2^{6C+7}C^{6C+8}}$.

Proof. In [2, Lemma 5.11] ε_3 is defined as:

$$\varepsilon_3 = \frac{\varepsilon}{2C\left(\frac{L(L+1)^n}{n!}+1\right)^2\left(C\frac{L(L+1)^n}{n!}+2\right)}$$

with $L = \frac{4C^2}{\varepsilon}+1$ and $n \le C$; everywhere in our discussion we'll assume $C \ge 4$ and $\varepsilon \le 1$, as this is what we will always work with. Since $L > C$ we have $\frac{(L+1)^n}{n!} \le \frac{(L+1)^C}{C!}$; then we observe that with our conditions we get:

$$C!(L-1)^{C+1} - L(L+1)^C > \left(C! - \left(\frac{3}{2}\right)^{C+1}\right)(L-1)^{C+1} > (L-1)^{C+1} > C!$$

so that $\frac{L(L+1)^C}{C!}+1 > (L-1)^{C+1}$, and consequently also $\frac{L(L+1)^C}{C!}+\frac{2}{C} > (L-1)^{C+1}$. Hence:

$$\begin{aligned}\varepsilon_3 &\ge \frac{\varepsilon}{2C\left(\frac{L(L+1)^C}{C!}+1\right)^2\left(C\frac{L(L+1)^C}{C!}+2\right)} > \frac{\varepsilon}{2C(L-1)^{2(C+1)}C(L-1)^{C+1}} \\ &= \frac{\varepsilon}{2C^2}\left(\frac{4C^2}{\varepsilon}\right)^{-2(C+1)}\left(\frac{4C^2}{\varepsilon}\right)^{-(C+1)} = \frac{\varepsilon^{3C+4}}{2^{6C+7}C^{6C+8}}\end{aligned}$$

so we can give the last one as new definition of ε_3. □

Lemma 3.11. $C_5(C) = C^{C+4}$.

Proof. By definition in [2, Lemma 5.13]. □

Lemma 3.12. $C_6(C) = 2C^{2C^{C+2}}$.

Proof. In [2, Lemma 5.14] we are analyzing the situation of the linear dependence we discussed in Chapter 2. We are given elements $a_{\vec{q}} \in \overline{\mathbb{C}(v_1,\dots,v_p)}$ roots of monic polynomials $p_{\vec{q}}(z) \in \mathbb{C}(v_1,\dots,v_p)[z]$, a primitive element b of the field K_v generated by the $a_{\vec{q}}$ and relations as in (2.3): we ask that the number of $a_{\vec{q}}$ is at most $C+1$, that the degree in z of the $p_{\vec{q}}$ is at most C and that the degree in each v_i of all the coefficients of the $p_{\vec{q}}$ is at most C; what we want is to find a bound C_6 on the degree in each v_i of all the $C_{\vec{q}j}$ and of the coefficients of the minimal polynomial for b.

The latter bound has already been found in [2, Lemma 5.13] as C_5, so we want $C_6 \ge C_5$ (it will be easily satisfied anyway). Call b_σ the conjugates of b in $\overline{\mathbb{C}(v_1,\dots,v_p)}$ and call $a_{\vec{q}\sigma}$ the conjugates of the $a_{\vec{q}}$; we have:

$$a_{\vec{q}\sigma} = \sum_{j=0}^{e-1} C_{\vec{q}j} b_\sigma^j$$

exactly as in (2.3). First of all, $e = [K_v : \mathbb{C}(v_1, \dots, v_p)]$ and K_v is generated by the (at most) $C+1$ elements $a_{\vec{q}}$ whose minimal polynomials have degree (at most) C, thus $e \leq C^{C+1}$; also the height of the b_σ are bounded by C^3, being roots of the minimal polynomial of b; $(b_\sigma^j)_{j,\sigma}$ is an invertible $e \times e$ square matrix, so each $C_{\vec{q}j}$ can be expressed as the sum of e terms $a_{\vec{q}\sigma} b'_{\sigma j}$ where the $b'_{\sigma j}$ are entries of the inverse matrix. From all this, with respect to each v_i we obtain:

$$\begin{aligned} h(C_{\vec{q}j}) &\leq \sum_\sigma h(a_{\vec{q}\sigma}) + h(b'_{\sigma j}) \leq e(C^3 + 2e!(1 + C^3 + 2C^3 + \ldots + (e-1)C^3)) \\ &= e\left(C^3 + 2e!\left(1 + C^3 \frac{e(e-1)}{2}\right)\right) \leq eC^3(1 + e^e e^2) \leq 2C^3 e^{e+3} \\ &\leq 2C^3 C^{(C+1)(C^{C+1}+3)} = 2C^{C^{C+2}+C^{C+1}+3C+6} \leq 2C^{2C^{C+2}} \end{aligned}$$

which satisfies also $C_6 \geq C_5$. □

Lemma 3.13. $N_1(C,p) = C^{3pC^{C+3}}$.

Proof. In [2, Prop 5.16] we are working in the linear dependence case, more specifically when everything is inside $\mathcal{O}$. We have a sum of at most $C+1$ elements $C_{\vec{q}j}$ which we project through the map π: each $C_{\vec{q}j}$ has degree at most C_6 in each variable, thus being ratio of polynomials with at most $(C_6+1)^p$ terms (and the same will evidently be true after the projection, since monomials go to monomials); using Lemma 3.12 we obtain then a bound N_1 on the number of terms for the sum:

$$\begin{aligned} N_1 &\leq (C+1)(C_6+1)^{p(C+1)} = (C+1)(2C^{2C^{C+2}}+1)^{p(C+1)} \leq 3^{p(C+1)} C^{2C^{C+2}p(C+1)+1} \\ &\leq C^{2pC^{C+3}+2pC^{C+2}+pC+C+1} \leq C^{3pC^{C+3}} \end{aligned}$$

□

Lemma 3.14. $C_7(C) = C^{C^{5C^{2C+9}}}$.

Proof. We say immediately that in [2, Prop 5.17] $C_7(C,p)$ is actually defined depending also on p; in every application however we have the inequalities $p \leq l \leq 2^l \leq C$, therefore we can express C_7 as dependent only on C.

We are again in the situation of linear dependence, and C_7 is defined to be the maximum of three different bounds. The first is the bound C'_7 in $h(c_{\vec{q}}) \leq C'_7 n_p$: we already know that $a_{\vec{q}}$ has degree at most C^3 in each variable, so after the substitutions $v_i \mapsto x^{n_i}$ the height of $c_{\vec{q}}$ in x is at most $pC^3 n_p$; therefore $C'_7 = C^4$. To define the second and the third bound, consider the minimal polynomial p^* of b and two polynomials G_1, G_2 such that:

$$G_1 p^* + G_2 \frac{\partial p^*}{\partial z} = 1$$

then if $G_1 \notin \mathcal{O}$ or $G_2 \notin \mathcal{O}$ we get a linear relation (2.4) with $|k_i| \leq C''_7$, while if $G_1, G_2 \in \mathcal{O}$ we get a bound $2\mathfrak{g} - 2 \leq C'''_7 n_p$ on the genus of K.

The degrees of p^*, $\frac{\partial p^*}{\partial z}$ in z and the degrees of their coefficients in each v_i are all bounded by $C_5 = C^{C+4}$: by Euclidean division G_1, G_2 have degree less than C_5 in z and their

coefficients have degree at most $2C_5(C_5-1)$ in each v_i, so by [2, Prop 5.15] we have a bound:

$$\begin{aligned} C_7'' &= 2C_6\left(2C_5(C_5-1)\right) \leq 2C_6\left(2C_5^2\right) = 2\cdot 2(2C^{2(C+4)})^{2(2C^{2(C+4)})^{2C^{2(C+4)}+2}} \\ &\leq C^{(2C+9)2(2C^{2(C+4)})^{2C^{2(C+4)}+2}} \leq C^{(2C^{2(C+4)})^{2C^{2(C+4)}+3}} \\ &\leq C^{C^{(2C+9)(2C^{2C+8}+3)}} = C^{C^{4C^{2C+9}+18C^{2C+8}+6C+27}} \leq C^{C^{5C^{2C+9}}} \end{aligned}$$

where the last one holds because we will use C_7 only with $C \geq C_4(4) = 2^{514}$. For the last bound we use Riemann-Hurwitz, so we need the ramification points which are the poles of $\pi(G_1)$ and $\pi(G_2)$; since the degree of each coefficient in each v_i is $\leq 2C_5(C_5-1)$ and there are at most C_5 coefficients, the poles of both functions after the projection π are at most $4C_5^2(C_5-1)pn_p$. Also, each ramification point has ramification degree bounded by C, therefore using Riemann-Hurwitz:

$$C_7''' \leq 4C_5^2(C_5-1)p(C-1) \leq 4C^{3(C+4)}C^2 = 4C^{3C+14}$$

So in the end we get:

$$C_7 = \max\left\{C_7', C_7'', \frac{1}{2}C_7''' + \frac{1}{n_p}\right\} \leq \max\left\{C^4, C^{C^{5C^{2C+9}}}, 2C^{3C+14}+1\right\} = C^{C^{5C^{2C+9}}}$$

□

3.4 Bound for Theorem 2.2: bound expressions

Now that we have the previous lemmas we can proceed to the next step. The proof of Theorem 2.2 contained in [2] makes use of a big intermediate proposition which contains most of the hardcore job for finding explicit bounds: we are going now to analyze the passages of this proposition in order to obtain bound expressions which depend on some initial data that are easily provided in the proof of the main theorem.

Here is the proposition ([2, Prop 5.18]):

Proposition 3.15. *Consider two real numbers $C \geq 1$ and $0 < \varepsilon \leq 1$ and an integer $m \geq 0$, consider a function field K over $\mathbb{C}(x)$ with $[K:\mathbb{C}(x)] \leq C$ and consider a height function h and a valuation v on $\overline{K}$ such that $h(x) = v(x) = 1$. Take a polynomial $P(x)$ (already a Puiseux expansion):*

$$P(x) = c_0 x^{\vec{k}_0\cdot\vec{n}} + c_1 x^{\vec{k}_1\cdot\vec{n}} + \ldots + c_s x^{\vec{k}_s\cdot\vec{n}} + x^{\vec{k}_{s+1}\cdot\vec{n}}\xi$$

where the error term ξ is root of a $\phi(y)$ as follows:

$$\phi(y) = \sum_{i=0}^{d} y^i \sum_{j=0}^{s_i} a_{ij} x^{\vec{q}_{ij}\cdot\vec{n}}$$

and suppose the following conditions to be satisfied:

1. *$0 = n_0 < n_1 \leq \ldots \leq n_p \leq \ldots n_l$ with $0 \leq p < l$, $n_{p+1} \geq \varepsilon n_l$ and $m = n_p$, and we have also $\vec{n} = (n_{p+1}, \ldots, n_l)$ (so the exponents $n_1, \ldots, n_p$ are the "small" ones and $n_{p+1}, \ldots, n_l$ are the "large" ones);*

2. $s, s_i, d \leq C$;

3. $c_i, a_{ij} \in K - \{0\}$ *and* $h(c_i), h(a_{ij}) \leq Cm$;

4. *if* $p > 0$ *then the coefficients* c_i, a_{ij} *are in the image of the map* $\pi : v_i \mapsto x^{n_i}$ *given in the previous chapter, they're roots of polynomials of degree* $\leq C$ *with coefficients of degree* $\leq C$ *in each* v_i*, and the field* K *is generated by them;*

5. *the genus* $\mathfrak{g}$ *of* K *is at most* Cm;

6. $P(x)$ *has degree at most* $C^2 n_l$;

7. $\vec{k}_i, \vec{q}_{ij} \in \mathbb{Z}^{l-p}$*, also* $H_{\mathbb{Q}}(\vec{k}_i), H_{\mathbb{Q}}(\vec{q}_{ij}) \leq C$ *and* $\vec{q}_{ij} \neq \vec{q}_{ik}$ *for every* $j \neq k$*: we also define* $r_{ij} = \vec{q}_{ij} \cdot \vec{n}$ *and we call* $\vec{r}$ *the vector of all the nonzero* r_{ij};

8. $v(\xi) > \varepsilon n_l$;

9. *there is an integer* $e \leq d$ *such that* $r_{ej} = 0$ *for some* j*: we suppose* e *to be the minimum with this property.*

Finally say that Theorem 2.2 is true for all integers $< l$*. Then there are three numbers* N_2, C_8, ε_4 *such that at least one of these three conclusions holds:*

(C1) $P(x)$ *is ratio of two polynomials with at most* N_2 *terms;*

(C2) there are integers k_i *with* $|k_i| \leq C_8$*, not all zero, such that* $k_1 n_1 + \ldots + k_l n_l = 0$;

(C3) $m = n_p \geq \varepsilon_4 n_l$.

We now follow the proof of this proposition in all its steps, so that we will be able to reconstruct at the end the three numbers. The proof is based on a double induction, on $l - p$ and on e.

Step 1: First, if $(\vec{q}_{ij} - \vec{q}_{ik}) \cdot \vec{n} = 0$ for some $j \neq k$ then we get (C2) with some $|k_i| \leq 2C$; therefore $C_8 \geq 2C$. From now on we suppose that this does not happen.

Step 2: We reparametrize the components of $\vec{n}$ (thus changing the vectors $\vec{k}_i, \vec{q}_{ij}$ too, while leaving untouched the scalar products) in such a way that a suitable class of linear combinations of the r_{ij} are now "not too small", i.e. at least $\varepsilon |\vec{n}|_\infty$ (up to a change of ε too): this procedure will not be described in detail here, concentrating only on the results; we remind that the nice condition above is a starting point for the use of the strategies (S1), (S2).

We obtain new large exponents $n'_{p+1}, \ldots, n'_l$ and we call p' the minimum such that $n'_{p'+1} \geq n'_l$ (in general $p \leq p' < l$) and $m' = \max\{m, n'_{p'}\}$; we can have two possibilities: either the procedure is successful and our nice condition is satisfied with C_4 instead of C and ε_2 instead of ε, or we get $m' \geq \frac{\varepsilon_2}{4C} n'_l$. In the latter possibility we can substitute ε with $\frac{\varepsilon_2}{4C}$ and have again the same two possibilities but with a smaller p', until eventually we fall into the first possibility (again with $p' \geq p$).

Step 3: If after having reached the first alternative in the previous step we still have $p' > p$ we are reduced to conditions 1-8 of the proposition being satisfied (and also 9 after an irrelevant division) for $l - p' < l - p$ so we exit with $N_2, C_8, \varepsilon_4(l - p')$ or we have a condition $n'_{p'} \geq \varepsilon_4 n'_l$; in the latter case we start again with $p' - 1$ with Step 2 until repeating these two steps enough times we get $p' = p$.

Let's stop for a moment and find a bound for what we have obtained until now. We have to decrease our p' at most $l - p - 1$ times: every time we decrease we can either have the substitution:

$$\varepsilon \mapsto \frac{\varepsilon_2}{4C} = \frac{\varepsilon}{4C^{2C^3+2}}$$

or the substitutions:

$$\begin{aligned} C &\mapsto C_4 = C^{4C^3+1} \\ \varepsilon &\mapsto \varepsilon_4(C_4, \varepsilon_2, l - p') = \varepsilon_4\left(C^{4C^3+1}, \frac{\varepsilon}{C^{2C^3+1}}, l - p'\right) \end{aligned}$$

and with the second there is also an exit case with $N_2, C_8, \varepsilon_4(C_4, \varepsilon_2, l - p')$. If we define ε_4 in such a way that the second subsitution gives a smaller ε than the first one (which will trivially be the case: as we can expect, N_2 and C_8 are huge and ε_4 is tiny), then we can suppose that the bounds when we finally arrive to $p' = p$ are given by the repetition $l - p - 1$ times of the second substitution.

Hence at the end of Step 3 (when finally $p' = p$) we are working with $C' = \mathcal{C}_{l-p-1}$ and $\varepsilon' = \mathcal{E}_{l-p-1}$ where we are recursively defining:

$$\begin{aligned} \mathcal{C}_0 &= C^{4C^3+1} & \mathcal{E}_0 &= \frac{\varepsilon}{C^{2C^3+1}} \\ \mathcal{C}_n &= \mathcal{C}_{n-1}^{4\mathcal{C}_{n-1}^3+1} & \mathcal{E}_n &= \frac{\varepsilon_4(\mathcal{C}_{n-1}, \mathcal{E}_{n-1}, n = l - p')}{\mathcal{C}_{n-1}^{2\mathcal{C}_{n-1}^3+1}} \end{aligned}$$

and the current bounds on the unknown quantities, given by the exit values at the last step (which are obviously bigger than the ones from the previous passages), are:

$$\begin{aligned} N_2 &\geq N_2(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l - p - 1) \\ C_8 &\geq C_8(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l - p - 1) \\ \varepsilon_4 &\leq \varepsilon_4(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l - p - 1) \end{aligned}$$

Step 4: At this point we really start expanding $P(x)$ according to our strategies. We begin supposing that we have to use (S2) (so that by the condition we gave in this case we must have $e > 1$).

We expand $\xi = c'x^e + x^e\xi'$: condition 4 is still satisfied with $\max\{C', C^3\} = C'$ (since now the a_{ij} appear in the polynomial that has c' as a root and they have height $\leq C^3$) and for the new field $K' = K(c')$ either we have $\mathfrak{g}' \leq C_7(C^3)n'_p$ and so condition 5 or we reach (C2) with $C_7(C^3)$ (so $C_8 \geq C_7(C^3)$). Finally we have either (C3) with $\frac{\varepsilon'_2}{4C'}$ or (C3) with $\frac{\varepsilon'^2}{8C'^4}$ or all the conditions 1-9 satisfied

by the new extended expression with $e' < e$; therefore we can work by induction on e and say that using (S2) we have also these conditions:

$$\begin{aligned} C_8 &\geq C'' = \max\{C_7(C^3), C'\} \\ \varepsilon_4 &\leq \varepsilon'' = \min\left\{\frac{\varepsilon'}{4C'^{2C'^3+2}}, \frac{\varepsilon'^2}{8C'^4}\right\} \\ N_2 &\geq N_2(C'', \varepsilon'', e-1) \\ C_8 &\geq C_8(C'', \varepsilon'', e-1) \\ \varepsilon_4 &\leq \varepsilon_4(C'', \varepsilon'', e-1) \end{aligned}$$

Step 5: Suppose now that we have to use the strategy (S1), i.e. we have an expansion $\xi = c'_0 x^{e_0} + c'_1 x^{e_1} + \ldots + c'_j x^{e_j} + \xi'$. First we call j_{max} the maximum j that gives such an expansion using (S1) for every term (it could be possible that $j_{max} = \infty$); then we call j_{min} the minimum j such that we have:

$$v(\xi') \geq \left(2C'^2 + \frac{\varepsilon'}{2}\right) n'_l$$

We find that we can suppose $j_{min} = \left(2C'^2 + \frac{\varepsilon'}{2}\right)\frac{l}{\varepsilon'}$ or that $n'_l \leq l$, so that we can reduce ourselves to a smaller l: this gives us by induction on l other bounds $N_2, C_8, \varepsilon_4(C', \varepsilon', l-1)$.

Now there are two possibilities: either j_{min} exists (which means that j_{max} is bigger than the expression above given for j_{min}; this is always the case when we have $e = 1$, since in this situation $j_{max} = \infty$) or it doesn't (which means j_{max} smaller than the same expression). Suppose that we are in the former case. First we calculate the new condition 4 in this situation: c'_0 is root again of a polynomial with coefficients having at most degree C in each v_i, so nothing changes for $j = 0$; c'_0 itself has height $\leq C^3$, so the coefficients of the new $\phi(x, c'_0 x^{e_0} + y')$ have height $\leq C^{3d}$, and the same can be said about the polynomial for c'_1. Therefore the height for the even newer ϕ is at most $C^{(3d)^2}$ and it's easy to see by induction that condition 4 is fulfilled with $C^{(3d)^j}$ (calling j the expression for j_{min}); hence we fall into one of the three conclusions given in the thesis:

$$\begin{aligned} N_2 &\geq N_1(C^{(3d)^j}, p) \\ C_8 &\geq 2C_6(C^{(3d)^j}) \\ \varepsilon_4 &\geq \varepsilon' \varepsilon_3(C^{(3d)^j}, \varepsilon') \end{aligned}$$

Step 6: Suppose instead that there is no such j_{min}; this means that we arrive to $j_{max} = j$ expanding only with (S1) and that for the next step we are obliged to use (S2): so we just need to find which new C satisfies conditions 1-9 and then we can reapply the whole proposition from Step 1 without falling into (S1) anymore (thus avoiding Steps 5-6). As aforementioned we have condition 4 with $C^{(3d)^j}$; condition 2 holds with $j + C + 1$, condition 3 with $pC^{(3d)^{j+1}}$. The exponent e_0 is always a difference $r_{ab} - r_{cd}$, so the new exponents in the first new ϕ are of the form:

$$e_0 k + r_{ef} = k(\vec{q}_{ab} - \vec{q}_{cd}) \cdot \vec{n} + \vec{q}_{ef} \cdot \vec{n}$$

and condition 7 would be respected for $C'(2d+1)$ instead of C' (obviously $k \leq d$); iterating this process we get in the end condition 7 for $C'(2d+1)^{j+1}$, and using it we also get condition 6 for $l-p$ times the square root of the condition 7. The maximum of all these is the bound for condition 3 (it's easy to see it if we suppose $C \geq (d+1)^2$, which again will always be the case), therefore we are repeating the proposition this time with ε' instead of ε and with $pC^{(3d)^{j+1}}$ instead of C.

At this point we know that the strategy (S2) can be used at most $e+1 \leq d+1$ times, and that actually the possibility of $e+1$ can be realized only when (S2) is the starting step ([2, Prop 4.5]). Therefore we get at most a succession of steps like:

$$\overbrace{(\text{S2})(\text{S1})(\text{S2})(\text{S1})\dots(\text{S2})(\text{S1})}^{2d+2 \text{ steps}}$$

Call then $N_2^{[A]}, C_8^{[A]}, \varepsilon_4^{[A]}$ the bounds coming from the first part of the procedure, before the choice of the strategy (Steps 1-3), call $C_8^{[B]}, \varepsilon_4^{[B]}$ the bounds coming from the choice of (S2) (Step 4) and call $N_2^{[C]}, C_8^{[C]}, \varepsilon_4^{[C]}$ the bounds coming from the choice of (S1) (Steps 5-6); also define:

$$\begin{aligned} \theta_1(C) &= pC^{(3d)^{j+1}} & \theta_2(C) &= C'' \\ \chi_1(\varepsilon) &= \varepsilon' & \chi_2(\varepsilon) &= \varepsilon'' \end{aligned}$$

so that θ_1, χ_1 tell us what to replace C, ε with after (S1) and θ_2, χ_2 after (S2). Then:

$$\begin{aligned} N_2^{[A]} &= N_2(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l-p-1) \\ C_8^{[A]} &= \max\{2C, C_8(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l-p-1)\} \\ \varepsilon_4^{[A]} &= \varepsilon_4(\mathcal{C}_{l-p-2}, \mathcal{E}_{l-p-2}, l-p-1) \\ C_8^{[B]} &= C'' \\ \varepsilon_4^{[B]} &= \varepsilon'' \\ N_2^{[C]} &= \max\left\{N_2(C', \varepsilon', l-1), N_1(C^{(3d)^j}, p)\right\} \\ C_8^{[C]} &= \max\left\{C_8(C', \varepsilon', l-1), 2C_6(C^{(3d)^j})\right\} \\ \varepsilon_4^{[C]} &= \min\left\{\varepsilon_4(C', \varepsilon', l-1), \varepsilon'\varepsilon_3(C^{(3d)^j}, \varepsilon')\right\} \end{aligned}$$

and the final bounds are coming from the [B] bounds at the $(2d+1)$-th step and from the

[A] and [C] bounds at the $(2d+2)$-th step:

$$\begin{aligned}
N_2 = \max\{&N_2^{[A]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right), \\
&N_2^{[C]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right)\} \\
C_8 = \max\{&C_8^{[A]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right), \\
&C_8^{[B]}\left(\theta_2(\theta_1\theta_2)^{d}(C), \chi_2(\chi_1\chi_2)^{d}(\varepsilon)\right), \\
&C_8^{[C]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right)\} \\
\varepsilon_4 = \min\{&\varepsilon_4^{[A]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right), \\
&\varepsilon_4^{[B]}\left(\theta_2(\theta_1\theta_2)^{d}(C), \chi_2(\chi_1\chi_2)^{d}(\varepsilon)\right), \\
&\varepsilon_4^{[C]}\left((\theta_1\theta_2)^{d+1}(C), (\chi_1\chi_2)^{d+1}(\varepsilon)\right)\}
\end{aligned}$$

Here we took some liberties in the notation for the sake of legibility. First of all, the internal multiplications and powers are to be intended as compositions; moreover, the arguments of these functions at every step of the composition are the values found at the previous step (which is not trivial to specify, since in the case of χ_1, χ_2 the result depends on ε but also on C). For example:

$$\begin{aligned}
\chi_2(\varepsilon) &:= \chi_2(\varepsilon, C) \\
\chi_1\chi_2(\varepsilon) &:= \chi_1\left(\chi_2(\varepsilon), \theta_2(C)\right) \\
\chi_2\chi_1\chi_2(\varepsilon) &:= \chi_2\left(\chi_1\chi_2(\varepsilon), \theta_1\theta_2(C)\right)
\end{aligned}$$

and so on.

3.5 Bound for Theorem 2.2 and Theorem 2.1

With the expressions of the previous section it is finally possible to find the values of $\beta_1(d,l)$ and $\beta(d,l)$.

The base case $l = 1$ is easy and does not need the heavy machinery that we developed in full generality. For $l = 1$ we have the equation $F(x^{n_1}, h(x)) = 0$, therefore we can expand $h(x)$ as:

$$h(x) = \sum_{i=0}^{\infty} c_i x^{n_1 e_i}$$

Notice that we can suppose that the e_i are actually integers, up to a change of variables $x \mapsto x^e$ that gets rid of the common denominator; at this point, since the degree of $h(x)$ is bounded by dn_1, we have the condition $e_i \leq d^2$ and then $\beta(d,1) = \beta_1(d,1) \leq d^2 + 1$ (it's important to observe that the change of variables doesn't affect this bound).

Then we work by induction on l: what we want is to work on the original equation $F(x^{n_1}, \dots, x^{n_l}, h(x)) = 0$ so that we will be able to apply Proposition 3.15. Firstly, we already have all the conditions 2-7 and 9 satisfied with the choices:

$$\phi(y) = F(x^{n_1}, \dots, x^{n_l}, y), \quad C = (d+1)^l, \quad \varepsilon = 1, \quad p = 0, \quad \xi = h(x), \quad K = \mathbb{C}(x).$$

Then we reparametrize (as in Step 2 of Proposition 3.15) in order to make condition 1 satisfied too: with this process we could get either $m' = n'_{p'} \geq \frac{\varepsilon_2}{4C} n'_l$ (since $p = 0$ implies

that $m = 0$) or we could have condition 1 with C_4 instead of C and ε_2 instead of ε; in the former case we reobtain the same two possibilities with a lower p' after substituting ε with $\frac{\varepsilon_2}{4C}$, and eventually we will get condition 1 after at most $l-1$ iterations. Hence we have satisfied conditions 1-7 and 9 with the values:

$$\begin{aligned}
C &= C_4((d+1)^l) = (d+1)^{4l(d+1)^{3l}+l} \\
\varepsilon &= \varepsilon_2\left(\frac{1}{4(d+1)^l}\varepsilon_2\left(\frac{1}{4(d+1)^l}\dots\varepsilon_2((d+1)^l,1)\dots,1\right),1\right) \\
&= \frac{1}{(d+1)^{2l(d+1)^{3l}+l}\left(4(d+1)^{2l(d+1)^{3l}+2l}\right)^{l-1}} = \frac{1}{2^{2l-2}(d+1)^{2l^2(d+1)^{3l}+2l^2-l}} \\
&\geq \frac{1}{2^{2l}(d+1)^{3l^2(d+1)^{3l}}}
\end{aligned}$$

Finally, to satisfy condition 8, we start using (S2) to expand $h(x)$ (independently of whether it should be used or not): every time either we obtain conditions 1-9 with C_2 and ε_1 or we decrease the value of p' with $\frac{\varepsilon_2}{4C}$ or $\frac{\varepsilon^2}{8C^4}$; again, the first possibility will be certainly obtained after at most $l-1$ iterations of the second alternative. Working out the math we see easily that for the first iteration we would have $\frac{\varepsilon_2}{4C} \leq \frac{\varepsilon^2}{8C^4}$ while for all the following ones we would have the inequality in the other direction; so at the end we are left with the values:

$$\begin{aligned}
C &= (d+1)^{4l(d+1)^{3l}+l}\left(1+(d+1)^{4l(d+1)^{3l}+l}\left(1+(d+1)^{4l(d+1)^{3l}+l}\right)^2\right) \\
&\leq 2(d+1)^{16l(d+1)^{3l}+4l} \\
\varepsilon^{-1} &= \left[2^{2l}(d+1)^{3l^2(d+1)^{3l}}\right]^{2^{l-2}}\left[4(d+1)^{(4l(d+1)^{3l}+l)(2(d+1)^{12l(d+1)^{3l}+3l}+2)}\right]^{2^{l-2}} \cdot \\
&\quad \cdot \left[8(d+1)^{16l(d+1)^{3l}+4l}\right]^{2^{l-2}-1}(d+1)^{4l(d+1)^{3l}+l}\left[(d+1)^{4l(d+1)^{3l}+l}+2\right] \\
&\leq 2^{2^{l-1}(l+4)-2}(d+1)^{2^{l+2}l(d+1)^{12l(d+1)^{3l}+6l}} \leq 2^{2^{l+1}l}(d+1)^{(d+1)^{12l(d+1)^{3l}+9l}}
\end{aligned}$$

At this point it is possible to apply Proposition 3.15 with the values above, reaching one of the three conclusions. If we reach (C1) we are done; if we reach (C2) then we can reduce to the previous step by induction applying the following lemma ([2, Lemma 2.9]):

Lemma 3.16. *Suppose that we have proven Theorem 2.2 for $l-1$ and for every d, and suppose that we have integers $k_1,\dots,k_l$ (not all zero) with $|k_i| \leq C$ and $k_1n_1+\dots+k_ln_l = 0$. Then $h(x)$ can be written as the ratio of two polynomials with at most $\beta_1(2dC, l-1)$ terms.*

If we reach (C3), we substitute ε with the ε_4 we obtained and reapply Proposition 3.15 with $p-1$ instead of p; in the end when $p=0$ it would be impossible to obtain (C3) again, so at most we reach (C1) or (C2) in $l-1$ steps. Therefore the bound β_1 is:

$$\beta_1(d,l) = \max\left\{N_2(C,\varepsilon_4^{l-1}(C,\varepsilon)), \beta_1(2dC_8(C,\varepsilon_4^{l-1}(C,\varepsilon)), l-1)\right\}$$

where C,ε are the ones given before and with ε_4^{l-1} we mean the composition $l-1$ times of ε_4, where in the argument we put every time the ε_4 of the step before and always the same C.

The bound β is obtained in exactly the same way as the bound B in Proposition 3.2; the condition $3^{24}l^{36} \leq \beta_1(d,l)$ is still easily satisfied for $l > 1$, hence:

$$\begin{aligned} \beta(d,1) &= \beta_1(d,1) = d^2 + 1 \\ \beta(d,l) &= \beta_1(d,l)^{5\beta_1(d,l)^2} \qquad\qquad (l > 1) \end{aligned}$$

Chapter 4

Further generalizations

We reserve this last brief chapter to some conclusive remarks about possible generalizations of Theorem 2.1.

The first problem that comes to mind is likely whether the result holds for other fields than $\mathbb{C}$. Rényi [3] and Erdős [1] already asked questions in this direction: their papers deal in fact with the cases $\mathbb{Q}$ and $\mathbb{R}$ rather than $\mathbb{C}$, but their results are easily valid for $\mathbb{C}$ too; in particular Rényi wondered if the function $Q(k)$ defined in the first section had the same value when working with rational, real or complex coefficients.

Also Schinzel [4] worked with more general fields than just $\mathbb{C}$ to find the bound $T(d, l)$: his results in practice hold for $h(x) \in K[x]$ where K has either zero characteristic or characteristic big enough to avoid nasty reductions of the degree of the monomials of $h(x)^d$. As he himself wrote though, his method is not generalizable even in the case of Schinzel's conjecture, as it relies on the behaviour of the polynomial $x^d - y$ in the field K considered. On the other hand, the method used to prove Theorem 1.1 and Theorem 2.1 makes extensive use of the properties of the complex field: to construct the Puiseux expansion, and in particular to use the fact that there is a finite common denominator for all the exponents, we require to be in an algebraically closed field of zero characteristic; moreover Lemma 1.4, which is the heart of the second part of both proofs, requires a function field that is a finite extension of $\mathbb{C}(x)$. However, Zannier [6] gave a similar result for general algebraically closed fields of characteristic zero, so it could be possible with some carefulness to generalize Theorem 2.1 at least in this case.

Another direction that is worth exploring involves a generalization of the concept of lacunary polynomial, which is also most likely the reason why people tackling this problem started considering projections of $F(v_1, \dots, v_l, y)$ through $\pi : v_i \mapsto x^{n_i}$ rather than the more simple-looking $F(x, y)$. We can consider in fact complex tori $\mathbb{G}_m^l$ and then restrictions of regular functions to 1-parameter subgroups given by $\pi : v_i \mapsto x^{n_i}$, or even to 1-parameter cosets given by $\pi : v_i \mapsto \lambda_i x^{n_i}$: in this context a lacunary polynomial is simply such restriction of a regular function; it could then be of interest to generalize the definition of lacunary polynomial to the case of powers of algebraic varieties other than $\mathbb{G}_m$: the authors of [2] ask whether analogues of the various results here presented, from Schinzel's result to Theorem 1.1 to Theorem 2.1, can be found in this new situation, even with just an elliptic curve instead of $\mathbb{G}_m$. Here we limit ourselves to observe that the generalization described before from $\mathbb{C}$ to a more generic K with $K = \overline{K}$ and char $K = 0$ is more natural from the

viewpoint of algebraic geometry, thanks to the Lefschetz principle.

Bibliography

[1] Erdős P.: On the number of terms of the square of a polynomial, *Nieuw Archief voor Wiskunde (2)* **23** (1949), 63-65.

[2] Fuchs C., Mantova V., Zannier U.: On fewnomials, integral points and a toric version of Bertini's theorem, `arXiv:1412.4548`.

[3] Rényi A.: On the minimal number of terms of the square of a polynomial, *Hungarica Acta Mathematica* **1** (1947), 30-34.

[4] Schinzel A.: On the number of terms of a power of a polynomial, *Acta Arithmetica* **XLIX** (1987), 55-70.

[5] Schinzel A., Zannier U.: On the number of terms of a power of a polynomial, *Rendiconti Lincei - Matematica e Applicazioni* **20(1)** (2009), 95-98.

[6] Zannier U.: Some remarks on the S-unit equation in function fields, *Acta Arithmetica* **LXIV** (1993), 87-98.

[7] Zannier U.: On the number of terms of a composite polynomial, *Acta Arithmetica* **CXXVII** (2007), 157-167.

[8] Zannier U.: On composite lacunary polynomials and the proof of a conjecture of Schinzel, *Inventiones mathematicae* **174** (2008), 127-138.