Spring 5-15-2015

Incompatibility of Diophantine Equations Arising from the Strong Factorial Conjecture

Brady Jacob Rocks
Washington University in St. Louis

WASHINGTON UNIVERSITY IN ST. LOUIS

Department of Mathematics

Dissertation Examination Committee:
David Wright, Chair
Jeff Gill
N. Mohan Kumar
Peter Luthy
John Shareshian

Incompatibility of Diophantine Equations Arising from the Strong Factorial Conjecture

by

Brady J Rocks

A dissertation presented to the
Graduate School of Arts and Sciences
of Washington University in
partial fulfillment for the degree
of Doctor of Philosophy

May 2015

Saint Louis, Missouri

Contents

Acknowledgements

I cannot express enough thanks to my advisor David Wright for his continued support and encouragement. His ideas helped shape this thesis. He has also had a tremendous influence on the way I think about mathematics.

I would also like to extend my gratitude to the entire Mathematics Department. Profs. N. Mohan Kumar and John Shareshian in particular have been so supportive; they were always willing to discuss mathematics with me.

To all my friends in the department, thank you. Dave Meyer, Ryan Keast, B3PO, Peter Luthy, Tim Chumalumadingdong, Joey Palmer, Chris Cox, Danny Z, Bingyuan Liu, Tian Wang, Casey Boyett, Josh Brady and so many others have made the past sever years so amazing.

Finally, to my mom and dad, thank you; you're always there for me.

Chapter 1

Introduction

This dissertation is mainly concerned with the study of the **Strong Factorial Conjecture**, a new and exciting problem first introduced by van den Essen and Edo in [13]. The conjecture is concerned with the following map, which was introduced in [33].

Definition 1.1 (Factorial Map)**.** For any ring R and variables $T_1, \ldots, T_m$, let $\mathcal{L} : R\left[T_1, \ldots, T_m\right] \to R$ be the R-linear map defined by $\mathcal{L}\left(\prod_{i=1}^{m} T_i^{\alpha_i}\right) = \prod_{i=1}^{m} \alpha_i!$.

In [33] van den Essen, Wright, and Zhao formulated the **Factorial Conjecture** after noticing a curious connection between the map $\mathcal{L}$ and Zhao's own **Image Conjecture** (see Chapter 2 for more information).

Conjeture 1.2 (Factorial Conjecture (**FC**))**.** *Let* $m \geq 1$ *be an integer and suppose* $F \in \mathbb{C}\left[T_1, \ldots, T_m\right]$ *is such that* $\mathcal{L}\left(F^n\right) = 0$ *for all* $n \geq 1$*. Then* $F = 0$*.*

To somebody coming across it for the first time, the Factorial Conjecutre might look simple; either it is easy to prove or a counterexample shouldn't be too hard to find. However no proof or counterexample has yet to be discovered. The authors of [33] succeeded in showing that the conjecture holds in some very special cases, and in particular, they proved it for the univariate polynomial ring $\mathbb{C}[T]$ (cf. [33, Theorem 4.9]). The problem remains open for all $m > 1$.

Recently, in [13], Edo and Essen introduced the Strong Factorial Conjecture, after noticing a connection between the factorial map and a conjecture of Furter (see Chapter 2 for more information):

Conjeture 1.3 (Strong Factorial Conjecture (**SFC**))**.** *Let $m \geq 1$, $F \in \mathbb{C}[T_1, \ldots, T_m] \setminus \{0\}$ and let $\mathcal{N}(F)$ be the number of of monomials that appear in F with nonzero coefficient. Then for any $n \geq 1$ there exists $0 \leq i \leq \mathcal{N}(F) - 1$ such that $\mathcal{L}(F^{n+i}) \neq 0$.*

The conjecture asserts that if $F \neq 0$ then amongst any $\mathcal{N}(F)$ consecutive powers of F there should be at least one that is mapped, under $\mathcal{L}$, to some nonzero complex number. Once again, no proof or counterexample has been given. Indeed, less is known about the Strong Factorial Conjecture than its weaker counterpart; it is not even known whether it holds for $m = 1$. The results of this disseration show that the conjecture holds in many special cases, some of which extend previously known results about the weak Factorial Conjecture found in [33]. We also give many partial results in which we etablish that for particular choices of n the condition $\mathcal{L}(F^{n+i}) = 0$ for $0 \leq i \leq \mathcal{N}(F) - 1$ implies $F = 0$.

In order to study Conjecture 1.3 we view the condition $\mathcal{L}(F^n) = 0$ as a diophantine equation in the coefficients of F. As a result, the conjecture leads us to the problem of determining the incompatibility of a finite collection of certain homogeneous diophantine equations. In order to obtain the positive results that are contained in this thesis we have made use of two well known techniques that have been used to study the common zeroes of polynomials: the resultant and the Newton Polygon (see Chapter 2 for more details).

The thesis is organized as follows:

- In Chapter 2 we introduce notations and conventions used throughout the disertation as well as provide a historical background for the Strong Factorial Conjecture. We also cover the necessary backround material.

- In Chapter 3 we present new evidence for the **SFC** by proving it in several special instances.

Chapter 2

Preliminaries

In this chapter we introduce notations and conventions that will be used throughout the dissertation, we motivate the study of the Strong Factorial Conjecture, and we give the necessary background required to understand the proofs of the main results.

2.1 Notation

Throughout this thesis we will make use of the following notation and conventions (all rings are assumed to be commutative and unital):

- For any ring R we denote by R^* the group of units of R.
- Given a prime integer p we denote by $\mathbb{F}_p$ the finite field of p elements.
- If I is an ideal of R and $a \in R$ then we denote by $\overline{a}$ the image of a under the natural quotient map $R \to R/I$.
- For any ring R and any positive integer m we denote by $R^{[m]}$ the ring $R\left[T_1, \dots, T_m\right]$ of polynomials in m variables. We also set $T = (T_1, \dots, T_m)$.
- Given $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{N}^m$ we set $|\alpha| = \sum_{i=1}^m \alpha_i$. We also set $\alpha! = \prod_{i=1}^m \alpha_i!$.
- Given $\alpha \in \mathbb{N}^m$ we denote by $\binom{|\alpha|}{\alpha}$ the multinomial coefficient. That is, $\binom{|\alpha|}{\alpha} = \dfrac{|\alpha|!}{\alpha!}$.

- For any $H = (H_1, \dots, H_m) \in \left(R^{[m]}\right)^m$ and any $\alpha \in \mathbb{N}$ we write H^α to denote the product $\prod_{i=1}^m H_i^{\alpha_i}$.

- If $G = (G_1, \dots, G_m)$ is another element of $\left(R^{[m]}\right)^m$ then we write HG to denote the m-tuple obtained by componentwise multiplication, i.e., $HG = (H_1G_1, \dots, H_mG_m)$.

- We denote by $\mathcal{L}$ the factorial map which was defined in Definition 1.1.

- Given $F \in R^{[m]}$ we denote by $\mathcal{N}(F)$ the number of monomials that appear in F with a nonzero coefficient (as in Conjecture 1.3).

- Given a subset $S \subset R^{[m]}$ we set $\mathcal{Z}_R(S) = \{\lambda \in R^m : F(\lambda) = 0 \text{ for all } F \in S\}$.

2.2 Background and Motivation

The study of the Strong Factorial Conjecture, which is interesting by itself, is motivated by some important problems in Affine Algebraic Geometry: the **Jacbobian**, **Vanishing**, **Image**, and **Rigidity** conjectures.

A **polynomial map** is a map $F = (F_1, \dots, F_m) : \mathbb{C}^m \to \mathbb{C}^m$ where each $F_i \in \mathbb{C}^{[m]}$. The map F is said to be invertible if there exists a polynomial map $G = (G_1, \dots, G_m)$ such that $G_i(F) = T_i$ for each i. If F is an invertible polynomial map then the determinant of the Jacobian matrix $\left(\dfrac{\partial F_i}{\partial T_j}\right)$ is a nonzero constant. The Jacobian Conjecture, first posed by Ott-Heinrich Keller in 1939, asserts that the converse is true.

Conjeture 2.1 (*Jacobian Conjecture* (**JC**))**.** *Let F be a polynomial map of $\mathbb{C}^m$. If the determinant of JF is a nonzero constant then F is invertible.*

Despite intense research by mathematicians, the conjecture remains open for all $m \geq 2$. The interested reader should see [3] and [32] for more history and known results on the Jacobian conjecture.

One of the earliest breakthroughs on the **JC** is the so called *cubic homogeneous reduction*, discovered by Bass, Connell, and Wright [3] and independently by Jagžev [23]. The reduction asserts that in order to prove the **JC** it suffices to consider polynomial maps of the form $F = T - H$ where each component H_i of H is a cubic homogeneous polynomial. During the past twelve years, some remarkable breakthroughs have been made on the **JC**. First, de Bondt and van den Essen [9] and Meng [25] independently discovered that in order to prove or disprove the **JC** it suffices to consider only symmetric polynomial maps. That is, it suffices to consider only polynomial maps of the form $F = T - \nabla P$ where $P \in \mathbb{C}^{[m]}$ and $\nabla P = \left(\frac{\partial P}{\partial T_1}, \dots, \frac{\partial P}{\partial T_m}\right)$ is the gradient of P. Combining this with the classic cubic homogeneous reduction, one may further assume that P is homogeneous of degree four. In this case the condition det $JF \in \mathbb{C}^*$ implies that $J(\nabla P)$ is nilpotent.

Based on the symmetric reduction, Zhao formulated the following vanishing conjecture for the Laplacian $\Delta = \sum_{i=0}^{m} \frac{\partial^2}{\partial T_i^2}$ in [35] and showed that it is equivalent to the **JC**:

Conjeture 2.2 (Vanishing Conjecture **VC**). *If $P \in \mathbb{C}^{[m]}$ is homogeneous and such that $\Delta^n (P^n) = 0$ for all $n \geq 1$ then $\Delta^n (P^{n+1}) = 0$ for all $n >> 0$.*

In particular, Zhao showed that the condition $\Delta^n (P^n) = 0$ for all $n \geq 1$ is equivalent to the nilpotency of $J(\nabla(P))$ and he also showed that the condition $\Delta^n (P^{n+1}) = 0$ for all $n >> 0$ is equivalent to the invertibility of the polynomial map $F = T - \nabla P$.

More recently, inspired by a conjecture of Mathieu (see [24]) that closely resembles his own **VC**, Zhao introduced the concept of a **Mathieu subspace** in [36] and using this concept formulated the Image conjecture.

Definition 2.3. Let K be a field, and R a commutative K-algebra. A K-vector subspace $\mathcal{M}$ of R is a **Mathieu subspace** if the following property holds: If $f \in R$ and $f^n \in \mathcal{M}$ for all positive n then for any $g \in R$ $f^n g \in \mathcal{M}$ for all but finitely many n.

Let R and K be as in the definition above. Let $(a_1, \dots, a_m)$ be a sequence of elements of R and consider the m commuting differential operators $D_i = \frac{\partial}{\partial T_i} - a_i$. Set $\operatorname{Im} \mathcal{D} = \sum_{i=1}^{m} D_i R^{[m]}$. Finally, recall that a sequence $(a_1, \dots, a_m)$ is called a **regular sequence** in R if a_1 is a nonzero divisor of R and for each i a_i is a nonzero divisor in $R/(a_1, \dots, a_{i-1})$.

Conjeture 2.4 (Image Conjecture **IC**)**.** *If* $(a_1, \ldots, a_m)$ *is a regular sequence in* R *then* $\operatorname{Im} \mathcal{D}$ *is a Mathieu subspace of* $R^{[m]}$

Van den Essen, Wright and Zhao proved the **IC** in the case $K = \mathbb{F}_p$ [33, Theorem 2.2]. In the characteristic zero case, some partial results are known for the special case $m = 1$ (see [33], and more recently, [34]).

Zhao also formulated the following specific version of the **IC** in [36]. Let $Z = (Z_1, \ldots, Z_m)$ be another sequence of m variables that commutes with $T = (T_1, \ldots, T_m)$. Set $R = \mathbb{C}[Z]$ and consider the set of commuting differential operators $D_i = Z_i - \dfrac{\partial}{\partial T_i}$, $1 \leq i \leq m$ on the polynomial ring $R^{[m]}$. Finally, set $\operatorname{Im} \mathcal{D} = \sum_{i=0}^{m} D_i \mathbb{C}[Z, T]$.

Conjeture 2.5 (Special Image Conjecture **SIC**)**.** $\operatorname{Im} \mathcal{D}$ *is a Mathieu subspace of* $\mathbb{C}[Z, T]$.

In [36] it is shown that if the above conjecture is true for all $m \geq 1$ then the **JC** is true for all $m \geq 1$. In fact, it was shown that the in order to prove the Jacobian conjecture it suffices to consider the image conjecture for a certain subset of polynomials $F \in R^{[m]}$.

Theorem 2.6 ([36], Theorem 3.6)**.** *The following two statements are equivalent:*

1. *For any* $m \geq 1$ *and homogeneous* $P(T) \in \mathbb{C}^{[m]}$ *of degree* 4*, the* ***SIC*** *holds for* $F(Z, T) = \left(\sum\limits_{i=0}^{m} Z_i^2 \right) P(T)$
2. ***JC*** *holds for all* $m \geq 1$.

To see how the **SIC** relates to the **FC** define the $\mathbb{C}$-linear map $\mathcal{E} : R^{[m]} \to \mathbb{C}^{[m]}$ by setting

$$\mathcal{E}\left(Z^\alpha T^\beta\right) = \left(\prod_{i=1}^{m} \frac{\partial^{\alpha_i}}{\partial T_i^{\alpha_i}} \right) \left(T^\beta\right)$$

where $\alpha, \beta \in \mathbb{N}^m$. Then:

Theorem 2.7 ([36], Theorem 3.1)**.** $\operatorname{Im} \mathcal{D} = \ker \mathcal{E}$

So in order to determine whether $\operatorname{Im}\mathcal{D}$ is Mathieu subspace, one has to consider polynomials $F \in R^{[m]}$ such that

$$\mathcal{E}\left(F^{n}\right) = 0, \text{ for all } n \geq 1 \tag{2.1}$$

In order to study condition (2.1) the authors [33] defined a multi-grading on $R^{[m]}$ that would be preserved under $\mathcal{E}$. Specifically, they defined the multi-degree of a monomial $Z^{\alpha}T^{\beta}$ to be $\beta - \alpha \in \mathbb{Z}^{m}$. Since $\mathbb{C}^{[m]}$ can be viewed as a subring of $R^{[m]}$ this multi-grading restricts to a multigrading on $\mathbb{C}^{[m]}$. Obviously, the multi-degree is preserved under $\mathcal{E}$.

In order that $\ker\mathcal{E}$ form a Mathieu subspace it is necessary that the multi-degree $(0, \ldots, 0)$ part of $\ker\mathcal{E}$ also form a Mathieu subspace. It was observed in [33] that any element of $R^{[m]}$ having multi-degree $(0, \ldots, 0)$ belongs to $A = \mathbb{C}\left[U_1, \ldots, U_m\right]$ where $U_i = Z_iT_i$, $1 \leq i \leq m$. Setting $U = (U_1, \ldots, U_m)$ one easily calculates $\mathcal{E}\left(U^{\alpha}\right) = \alpha!$. Thus, the restriction of $\mathcal{E}$ to A is precisely the factorial map $\mathcal{L}$. So if the **IC** is true, then $\ker\mathcal{L}$ is necessarily a Mathieu subspace. The **FC** is a stronger assertion of this necessity.

We end this section by discussing how the Rigidity conjecture of Furter, formulated in [20], motivated the **SFC**. Before we can do that, we need to recall some facts from Affine Algebraic Geometry. Let K be a field and denote by $\mathrm{GA}_m(K)$ the group of polynomial automorphisms in two variables. Two subgroups of $\mathrm{GA}_m(K)$ that are of interest are as follows:

1. The affine group $Af_m(K)$ is the subgroup consisting of invertible polynomial maps $F = (F_1, \ldots, F_m)$ where $\deg\left(F_i\right) = 1$ for $1 \leq i \leq m$.

2. The triangular subgroup $BA_m\left(K\right)$ is the subgroup generated by polynomial automorphisms of the form $F = (F_1, \ldots, F_m)$ where $F_i = a_iX_i + G_i$ with $a_i \in K^*$ and $G_i \in K\left[T_{i+1}, \ldots, T_m\right]$ for $1 \leq i \leq m$.

The classical Jung-van der Kulk Theorem (see [32]) asserts that GA_2 is generated by BA_2 and Af_2. Moreover, it gives the structure of GA_2 as the amalgamated product of the two subgroups along their intersection. Given $F \in \mathrm{GA}_2$ the **polydegree** (or multidegree) of F is the sequence of degrees of the triangular automorphisms used in the decomposition of F as a product of triangular and affine automorphisms. The **length** of F is then the number of triangular automorphisms used in the decomposition. The concept of polydegree and length was first defined in [16] and separately in [17].

In [31], the the group GA_2 was endowed with the structure of an infinite-dimensional algebraic variety. Then in [18], it was shown that the length of a plane polynomial automorphism is lower semicontinuous with respect to the Zarisky topology of $GA_2(K)$. A partial order $\preceq$ was also introduced in [18] to describe the closure of the set of plane polynomial automorphisms having fixed polydegree $d \in \mathbb{N}_+^l$, $l \geq 1$. It was also conjectured that the closure of the set $\mathcal{G}_d$ of polynomials having polydegree d is the union of all $\mathcal{G}_e$ where $e \preceq d$ (cf. [18]). However, in [12] it was shown that the conjecture is false in general, and in particular, a counter example for polydegree d of length three was provided. The conjecture for polydegree of length two remains open (cf. [19] or[11]).

Recently, Furter introduced the Rigidity Conjecture (see [20]):

Conjeture 2.8 (Rigidity Conjecture **RC**)**.** *Let $a(x) \in \mathbb{C}[x]$ be a univarite polynomial of degree at most $m+1$ such that $a(x) \equiv x \mod x^2$. If m consecutive coefficients of the formal inverse $a^{-1}(x)$ vanish then $a(x) = x$.*

He then showed, remarkably, that the **RC** implies the length two polydegree conjecture. As of now, the **RC** is has only been resolved in the cases $m = 1$ and $m = 2$ (see [13]).

In [13] , van den Essen and Edo posed the **SFC** after noticing the following connection with the **RC**: Given a univariate polynomial of the form $a(x) = x\,(1 - \lambda_1 x) \cdots (1 - \lambda_m x)$ with each $\lambda_i \in \mathbb{C}$ the coefficient of x^n in the formal inverse $a^{-1}(x)$ is equal to $\mathcal{L}\left(F^n\right) / \left(n!\right)^{m+1}$ where $F = \left(\prod_{i=1}^m T_i\right)\left(\lambda_1 T_1 + \cdots + \lambda_m T_m\right)$. Using this equality they proved the following:

Theorem 2.9 ([13], Theorem 2.25(d))**.** *The following statements are equivalent:*

1. *Every polynomial of the form $F = \left(\prod_{i=1}^m T_i\right)\left(\lambda_1 T_1 + \cdots + \lambda_m T_m\right)$ with each $\lambda_i \in \mathbb{C}$ satisfies the **SFC***

*2. The **RC** holds for all $m' \leq m$*

2.3 First Observations

In this section we collect some useful initial observations about the **SFC**, some of which will be refered to later on in the dissertation. We begin by noting that the **SFC** holds for $F = \lambda M$ where $\lambda \in \mathbb{C}$ and M is a monomial in $\mathbb{C}^{[m]}$, since $\mathcal{L}\left(F^n\right) = 0$ obviously implies $\lambda = 0$. In [13] it was shown that the **SFC** fails to hold in finite characteristic. For this, consider $F = T_1 - T_2$. Then $F^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k T_1^{n-k} T_2^k$ for all $n \geq 1$. It now follows that $\mathcal{L}\left(F^n\right) = n! \sum_{k=0}^{n} (-1)^k$. So $\mathcal{L}\left(F^n\right) = n!$ whenever n is even, and is zero otherwise. If char $R = 2$ then $\mathcal{L}\left(F^n\right) = 0$ whenever n is even, and is therefore equal to zero for all $n \geq 1$. The previous calculation also shows that the **FC** fails in finite characteristic as well.

Let $\sigma \in \mathfrak{S}_m$ be a permutation of the set $\{T_1, \ldots, T_m\}$ and extend σ to an automorphism $\tilde{\sigma}$ of the $\mathbb{C}$-algebra $\mathbb{C}^{[m]}$. For any $\alpha \in \mathbb{N}^m$ it is easy to see that $\mathcal{L}\left(\tilde{\sigma}\left(T^\alpha\right)\right) = \alpha! = \mathcal{L}\left(T^\alpha\right)$. It follows that $\mathcal{L}\left(\tilde{\sigma}\left(F\right)\right) = \mathcal{L}(F)$ for all $F \in \mathbb{C}^{[m]}$.

The factorial map $\mathcal{L}$ is not multiplicative in general. For example take $F = T_1 \cdot T_1$ and observe that $\mathcal{L}\left(F^2\right) = 2 \neq 1 = \mathcal{L}\left(T_1\right)^2$. Nonetheless $\mathcal{L}(FG) = \mathcal{L}(F)\mathcal{L}(G)$ whenever $F, G \in \mathbb{C}^{[m]}$ are two polynomials such that there exists an $I \subset \{1, \ldots, m\}$ such that $F \in \mathbb{C}\left[T_i : i \in I\right]$ and $G \in \mathbb{C}\left[T_i : i \notin I\right]$.

Our final observation is that the factorial image $\mathcal{L}\left(F^n\right)$ can be realized via an integration formula. Let $T = (T_1, \ldots, T_m)$ and let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$. The following multi-variable formula can easily be proven using induction (integration by parts is needed to prove the base case):

$$\int_{D_m} T^\alpha e^{-|T|} dT = \alpha!$$

In the above formula $dT = \prod_{i=1}^{m} dT_i$ and D_m denotes the non-negative m-tant $T_1 \geq 0, \ldots, T_m \geq$

0 in $\mathbb{R}^m$. It follows that for $F \in \mathbb{C}^{[m]}$, $\mathcal{L}(F)$ can be realized as

$$\mathcal{L}(F) = \int_{D_m} F(T) e^{-|T|} dT \tag{2.2}$$

Let $\langle \cdot, \cdot \rangle$ denote the Hermitian inner product defined on $\mathbb{C}^{[m]}$ by

$$\langle F, G \rangle = \int_{D_m} F(T) \overline{G(T)} e^{-|T|} dT \tag{2.3}$$

We note that this restricts to a positive definite form on $\mathbb{R}^{[m]}$. In particular, we have $\mathcal{L}\left(F^{2n}\right) = \langle F^n, F^n \rangle$ for all $n \geq 1$ and for all $F \in \mathbb{R}^{[m]}$. Moreover, $\mathcal{L}\left(F^{2n}\right) > 0$ for all $n \geq 1$ if $F \in \mathbb{R}^{[m]}$ and $F \neq 0$. This observation produces the following easy to prove proposition:

Proposition 2.10. *The Strong Factorial Conjecture holds for all* $F \in \mathbb{R}^{[m]}$

We also have the following corollary, which we will invoke in Section 3 of Chapter 3 to prove the *SFC* in some very special cases.

Corollary 2.11. *Let* $F \in \mathbb{C}^{[m]}$. *If* $\mathcal{L}\left(F^{2n}\right) = 0$ *for some* $n \geq 1$ *then* $F \in \mathbb{C}^{[m]} \setminus \mathbb{R}^{[m]}$.

2.4 Diophantine Equations Arising from the SFC

In this section we fix an integer $d \geq 2$ and monomials $M_1, \ldots, M_d \in \mathbb{C}^{[m]}$. Given $\lambda = (\lambda_1, \ldots, \lambda_d) \in \mathbb{C}^d$ we consider the polynomial $F = \sum_{i=1}^{d} \lambda_i M_i$. If we set $M = (M_1, \ldots, M_d)$ then for any $n \geq 1$ we have:

$$\begin{aligned} \mathcal{L}\left(F^n\right) &= \mathcal{L}\left(\sum_{\alpha \in \mathbb{N}^d, |\alpha| = n} \binom{n}{\alpha} M^\alpha \lambda^\alpha\right) \\ &= \sum_{\alpha \in \mathbb{N}^d, |\alpha| = n} \binom{n}{\alpha} \mathcal{L}\left(M^\alpha\right) \lambda^\alpha \end{aligned} \tag{2.4}$$

Let $x = (x_1, \ldots, x_m)$ be m commuting variables. The above formula leads us to define, for each $n \geq 1$, a polynomial $f_n(x)$ given by

$$f_n(x) = \sum_{\alpha \in \mathbb{N}^d, |\alpha| = n} \binom{n}{\alpha} \mathcal{L}\left(M^\alpha\right) x^\alpha \tag{2.5}$$

Note that $f_n(x) \in \mathbb{Z}[x]$ is homogeneous of degree n and that $f_n(\lambda) = \mathcal{L}\left(F^n\right)$. Moreover $\mathcal{L}\left(F^n\right) = 0$ if and only if λ is a solution to the homogeneous diophantine equation $f_n(x) = 0$. Thus the Strong Factorial Conjecture for the polynomial F asserts that $\mathscr{Z}_{\mathbb{C}}\left(\left\{f_n(x), \ldots, f_{n+\mathcal{N}(F)-1}(x)\right\}\right) = \{(0, \ldots, 0)\}$ for all $n \geq 1$. Therefore we can view the Strong Factorial Conjecture as an assertion about the incompatibility of certain systems of homogeneous diophantine equations.

Let $I \subset \mathbb{Q}^{[d]}$ be the ideal generated by $\left\{f_n(x), \ldots, f_{n+\mathcal{N}(F)-1}(x)\right\}$. By the Nullstellensatz, $\mathscr{Z}_{\mathbb{C}}(I) \supset \{(0, \ldots, 0)\}$ if and only if $\sqrt{I} \subset (x_1, \ldots, x_d)$, which, in turn, happens if and only $\mathscr{Z}_{\overline{\mathbb{Q}}}(I) \supset \{(0, \ldots, 0)\}$ where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$. This observation leads to the following remark, which appeared in [33] and was used by the authors to resolve several instances of the weak factorial conjecture. While we have not used this particular observation to produce evidence for the strong factorial conjecture, we still make use of the theory of valuations in this dissertation, and therefore think it is worth mentioning.

Remark 2.12 (Extension of primes)**.** Given $\lambda = (\lambda_1, \ldots, \lambda_d) \in \overline{Q}^d$ there exists an $l \in \mathbb{Z}$ such that λ_i is integral over $\mathbb{Z}\left[1/l\right]$ for $1 \leq i \leq d$. Note that $\mathbb{Z}\left[1/l\right]$ is a localization of a Dedekind domain, and therefore it is also a Dedekind domain. Letting $\mathcal{O}$ be the integral closure of $\mathbb{Z}\left[1/l\right]$ in $\mathbb{Q}\left(\lambda_1, \ldots, \lambda_m\right)$ we observe that $\mathbb{Q}\left[\lambda_1, \ldots, \lambda_d\right]$ has a dedekind extension in $\overline{\mathbb{Q}}$ that is integral over $\mathbb{Z}[1/l]$. All but finitely many primes $p \in \mathbb{Z}$ (specifically, those primes not dividing l) extend to a proper ideal of $\mathbb{Z}\left[1/l\right]$. For such a prime p we can choose a prime ideal $\mathfrak{p} \subset \mathcal{O}$ lying over p. Since $\mathcal{O}$ is Dedekind, $\mathfrak{p}$ gives a discrete valuation of $\mathbb{Q}\left(\lambda_1, \ldots, \lambda_m\right)$. Since $\mathfrak{p}$ lies over p the valuation will be positive at p. Thus, for all but finitely primes, there is a (not necessarily unique) discrete valuation on $\mathcal{O}$ that is positive at p.

2.5 Univariate Resultant

In Section 3 of Chapter 3 we study the case $F = \lambda_1 M_1 + \lambda_2 M_2$ where $\lambda_1, \lambda_2 \in \mathbb{C}^*$ and M_1, M_2 are monomials in $\mathbb{C}^{[m]}$. As we shall see in that section, we can assume, without loss of generality, that $\lambda_1 = 1$ or $\lambda_2 = 1$. Taking the approach outlined in the previous section, resolving the strong factorial conjecture for $F \in \mathbb{C}^{[m]}$ a sum of two monomials boils to showing that two univariate polynomials (note that $\mathcal{N}(F) = 2$) have no common zeroes. One way of determining whether two univariate polynomials have any common factors (or zeroes) is to compute their resultant, which we will describe now.

Let k be a field and let $f, g \in k[x]$ be polynomials of degree $m > 0$ and $n > 0$, respectively. Write the polynomials in the form

$$\begin{aligned} f &= a_m x^m + \cdot + a_0 \\ g &= b_n x^n + \cdots + b_0 \end{aligned} \tag{2.6}$$

For any $l > 0$ let S_l denote the k-vector space of polynomials of degree at most l. The **Sylvester matrix** of f and g, denoted by $\mathrm{Syl}(f, g, x)$, is the matrix of the linear transformation $S_{n-1} \bigoplus S_{m-1} \to S_{m+n-1}$ defined by $(A, B) \to Af + Bg$ with respect to the ordered bases $\{(x^{n-1}, 0), \ldots, (1, 0), (0, x^{m-1}), \ldots, (0, 1)\}$ and $\{x^{m+n-1}, \ldots, 1\}$. For example, if $f = 1 + 2x + 3x^2$ and $g = x + 3x^3$ then

$$\mathrm{Syl}(f, g, x) = \begin{bmatrix} 3 & 0 & 0 & 3 & 0 \\ 2 & 3 & 0 & 0 & 3 \\ 1 & 2 & 3 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The **resultant** of f and g with respect to x, denoted $\mathrm{Res}(f, g, x)$ is the determinant of the Sylvester matrix. If $c \in k^*$ then $\mathrm{Res}(f, c, x) := c^m$. The following is well known; see, for example, [8, Proposition 5.8]:

Proposition 2.13. *The resultant* $\operatorname{Res}(f, g, x) = 0$ *if and only if* f *and* g *have a common factor in* $k[x]$*. Thus,* f *and* g *have a common zero in* $\overline{k}$ *if and only if the resultant is zero.*

Here is another formula for the resultant of f and g. A proof can be found in [21].

Proposition 2.14. *Let* $f, g \in k[x]$ *be as in* (2.6)*. If* $\alpha_1, \ldots, \alpha_m \in \overline{k}$ *are the roots of* f *and* $\beta_1, \ldots, \beta_n \in \overline{k}$ *are the roots of* g *then the resultant of* f *and* g *is given by the formula* $\operatorname{Res}(f, g, x) = a_m^n b_n^m \prod_{i,j} (\alpha_i - \beta_j)$*.*

Finally, we have the following useful facts about the resultant. These are all well known and can be found in [21] or [8].

Proposition 2.15. *The resultant satisfies the following:*

(i) $\operatorname{Res}(f, g, x) = (-1)^{mn} \operatorname{Res}(g, f, x)$

(ii) Suppose $m \geq n$*. Write* $f = qg + r$ *for some polynomials* r *and* q *with* $\deg(r) = s < n$*. Then* $\operatorname{Res}(f, g, x) = b_n^{m-s} \operatorname{Res}(r, g, x)$

(iii) $\operatorname{Res}(x^l, g, x) = g(0)^l$ *for all* $l \geq 1$*.*

(iv) If $h \in k[x]$ *then* $\operatorname{Res}(fh, g, x) = \operatorname{Res}(f, g, x) \cdot \operatorname{Res}(h, g, x)$

(v) If $\lambda \in k^*$ *then* $\operatorname{Res}(f(\lambda x), g(\lambda x), x) = \lambda^{mn} \operatorname{Res}(f, g, x)$

2.6 Newton Polygon

In this section we describe the Newton Polygon method and collect all the results pertaining to it that are relevant for this dissertation. The polygon originated in the work of Newton in 1676 (see [4, p. 372]), and was later revived by Puiseux in 1850 [30]. It was used by Newton (and later Puiseux) to prove the following theorem, which nowadays is often referred to as the **Newton-Puisseux Theorem**: If K is an algebraically closed field and the characteristic of K does not divide the degree of $f(x) \in K((t))[x]$ where $K((t))$ is the field of Laurent series in the variable t, then $f(x)$ factors into a product of linear factors involving fractional power series in t. In short, the slope of the segments of the Newton Polygon of $f(x)$ determine the possible exponents that appear in the fractional power series (see [2] or [6] for more details).

The Newton Polygon was eventually developed in a more general setting, and made appearences in the work of Hensel [22] and Dumas [10]. In the general setting, the Newton Polygon provides valuative and combinatorial information about the roots of a polynomial $f(x) \in K[x]$ where K is a non-archimedean valued field (see below for definition). As a result, the Newton Polygon has many applications to the area of polynomial factorization. For example, it has been used by Dumas [10], Filaseta [15], and Filaseta and Lam [14] to obtain irreducibility criteria for rational polynomials of a certain form.

In this disseration we use the Newton Polygon to study the Strong Factorial conjecture for polynomials F that are the sum of two monomials. As was mentioned in Section 2 of this chapter, systems of Diophantine equations naturally arise in the study of the conjecture. When F is a sum of two monomials we are led to consider the common solutions of a system of two diophantine equations in one variable. By using the information provided by the Newton Polygon we can determine in some very special cases that the polynomials in question have no common solutions over the complex numbers.

Our main source of information regarding the Newton Polygon has been the paper by Mott [27] and the book by Neukirch [28].

Let (K, ν) be a non-archimedean valued field. That is, $\nu : K \to \mathbb{R} \cup \{\infty\}$ satisfying the following properties:

1. $\nu(0) := \infty$

2. $\nu(xy) = \nu(x) + \nu(y)$ for all $x, y \in K$

3. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ with equality if $\nu(x) \neq \nu(y)$

Example 2.16. Fix a prime $p \in \mathbb{Z}$. For any $q \in \mathbb{Q}^*$ there exists integers $a, b, n \in \mathbb{Z}$ with $p \nmid ab$ such that $q = \frac{a}{b}p^n$. Define $\nu_p : \mathbb{Q} \to \mathbb{Z}$ by setting $\nu_p(q) = n$. Then ν_p is a non-archimedean valuation. The function ν_p is often referred to as the "p-adic valuation" or "p-adic order".

Let $f = \sum\limits_{i=1}^{n} a_i x^i \in K[x]$ where $a_n a_0 \neq 0$. The **Newton Polygon**, $N_\nu(f(x))$, of f is the lower convex hull of the set of points $\{(i, \nu(a_i)) : 0 \leq i \leq n\} \subset \mathbb{R}^2$. In other words, $N_\nu(f(x)$ is a union of edges $E_1, E_2, \ldots, E_t$, increasing in slope from left to right, and connecting $(0, \nu(a_0))$ to $(n, \nu(a_n))$. Moreover, each point $(i, \nu(a_i))$, where $1 \leq i \leq n$, lies on or above the edges $E_1, \ldots, E_t$.

If $(i, \nu_p(a_i))$ and $(j, \nu_p(a_j))$ where $i < j$ are end points of an edge of $N_p(f(x))$ then the difference $\nu_p(a_j) - \nu_p(a_i)$ is called the **height** of the edge and the length $j - i$ is called the **width** of the edge. The height is allowed to be zero or negative, while the width is always positive. If $E_1, \ldots, E_t$ are the edges of the polygon with heights $h_1, \ldots, h_t$, and widths $w_1, \ldots, w_t$, respectively, then:

$$h_1 + h_2 + \ldots + h_t = \nu(a_n) - \nu(a_0)$$

$$w_1 + w_2 + \ldots + w_t = n$$

Example 2.17. Set $K = \mathbb{Q}$ and let $\nu = \nu_2$ be thel 2-adic valuation on $\mathbb{Q}$ that was defined in Example 2.16. The Newton Polygon for $f(x) = x^9 - 2x^4 + 4x^2 - 8$ relative to the 2-adic valuation consists of two edges connecting $(0, 3), (4, 1)$, and $(9, 0)$.

Suppose L/K is an algebraic extension. It is well known (cf. [28, Chapter 2, Section 8]) that ν may be extended to a (not necessarily uniqure) valuation $\tilde{\nu}$ on L (there is a unique extension when K is complete with respect to the ν-adic topology; see [28, Theorem 4.8]). The central property of the Newton Polygon for a given polynomial $f(x)$ is that the slopes of its edges give the $\tilde{\nu}$-values of its roots.

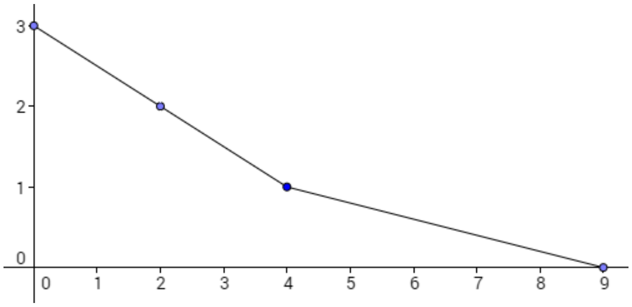

Figure 2.1: The 2-adic Newton Polygon of $f(x) = x^9 - 2x^4 + 4x^2 - 8$

Proposition 2.18. *Let $f(x) = \sum_{k=0}^{n} a_i x^i$, $a_n a_0 \neq 0$, be a polynomial over the field K, ν a non-archimedean valuation of K, and $\tilde{\nu}$ an extension to the splitting field L of f. Suppose $(i, a_i)\,, (j, a_j)\,, i < j$ are endpoints of some edge E of $N_\nu(f(x))$. If m is the slope of E then $f(x)$ has precisely $j - i$ roots $\alpha_1, \ldots, \alpha_{j-i} \in L$ of value*

$$\tilde{\nu}(\alpha_1) = \cdots = \tilde{\nu}(\alpha_{j-i}) = -m$$

Proof. See the proof of Propoisition 6.4 in[28] □

One useful consequence of Proposition 2.18 is the following:

Corollary 2.19. *If for two non constant polynomials $f(x), g(x) \in K[x]$, the Newton polygons $N_\nu(f(x))$ and $N_\nu(g(x))$ have no edges with the same slope, then $f(x)$ and $g(x)$ have no common factors. In particular, $f(x)$ and $g(x)$ have no common roots over $\overline{K}$.*

Since this dissertation is more concerned with integer polynomials we spend the rest of the section discussing the case $K = \mathbb{Q}$. We would like to remark that the following results hold in more general settings (specifically, when K is equipped with a discrete valuation).

We fix a prime $p \in \mathbb{Z}$ and set $\nu = \nu_p$ where ν_p is the p-adic valuation defined in Example 2.16. Before giving the next proposition let us recall how one extends ν to L when L is a finite extension of $\mathbb{Q}$. Let $\mathcal{O}$ be the integral closure of $\mathbb{Z}$ in L. Choose a prime $\mathfrak{p} \subseteq \mathcal{O}$ lying over p. Denote by $\nu_\mathfrak{p}$ the discrete valuation of L associated to $\mathfrak{p}$. If $q \in \mathbb{Q}^*$ then $\nu_\mathfrak{p}(q) = e\nu(q)$ where $e = e(\mathfrak{p}|p)$ is the ramification index. Define $\tilde{\nu}$ by setting $\tilde{\nu}(\alpha) = \nu_\mathfrak{p}(\alpha)/e$ for all $\alpha \in L$.

One easily sees that $\tilde{\nu}$ is a valuation on L extending ν. Note that $\tilde{\nu}$ is possibly $\mathbb{Q}$-valued.

Proposition 2.20. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ with $a_n a_0 \neq 0$, and suppose that $N_\nu(f(x))$ consists of t edges having widths $w_1, \ldots, w_t$ and heights $h_1, \ldots, h_t$. Furthermore, let $s_i = gcd\,(h_i, w_i)$ and set $d_i = w_i/s_i$. If $h(x) \in \mathbb{Q}[x]$ is an irreducible factor of $f(x)$ then $\deg(h(x)) = \sum_{i=1}^{t} a_i d_i$ where $0 \leq a_i \leq s_i$ for each i.*

Proof. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$, $\tilde{\nu}$ an extension of ν to L, and let $h(x) \in \mathbb{Q}[x]$ be an irreducible factor of $f(x)$. If $\alpha \in L$ is a root of $h(x)$ then α is also a root of $f(x)$ and therefore $\tilde{\nu}(\alpha) = -h_i/w_i$ for some i by Proposition 2.18. So if E is an edge of $N_\nu(h(x))$ having width w and height h then $h/w = h_i/w_i$ for some i. Moreover, $w \leq w_i$, otherwise $f(x)$ would have more than w_i roots in L having $\tilde{\nu}$-value $-h_i/w_i$, violating the previous proposition. Now writing h_i/w_i in lowest terms we can conclude that d_i divides w. Set $a_i = w/d_i$ and observe that $a_i \leq s_i$ since $w \leq w_i$. Since $\deg(h(x))$ is equal to the sum of widths of the edges of $N_\nu(h(x))$ we see that $\deg(h(x)) = \sum_{i=1}^{t} a_i d_i$ where $a_i = 0$ if $h(x)$ has no roots of value $-h_i/w_i$. □

Corollary 2.21. *Let $f(x)$, w_i, h_i, s_i, and d_i be as in Proposition 2.20. Set $d = gcd\,(d_1, \ldots, d_t)$. If $h(x) \in \mathbb{Q}[x]$ is an irreducible factor of $f(x)$ then $d \mid \deg(h(x))$.*

The following corollary was first proved by Dumas [10]. We would like to note that it can be used to prove Eisenstein's criteria, and therefore should be thought of as a generalization thereof.

Corollary 2.22. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x]$ with $a_n a_0 \neq 0$. If $gcd\,(\nu\,(a_n)\,, n) = 1$ and $\nu\,(a_i) \geq \nu\,(a_n)\, i/n$ for each $1 \leq i \leq n$, then $f(x)$ is irreducible over $\mathbb{Q}[x]$.*

Proof. The inequality $\nu\,(a_i) \geq \nu\,(a_n)\, i/n$ implies that $N_\nu(f(x))$ consists of a single edge with slope $\nu\,(a_n)\,/n$. Since the $gcd\,(\nu\,(a_n)\,, n) = 1$ the d in the previous corollary is equal to n. So $f(x)$ is irreducible. □

Chapter 3

Main Results

In this chapter we present new evidence in support of the *SFC* by proving it in several special instances. First, we show that powers of linear forms satisfy the conjecture. Additionally, we prove it for all linear polynomials. In Section 2 we consider polynomials that are sums of prime powers of variables while in Section 3 we study polynomials that are the sum of two monomials. Lastly, we show one particular instance of how one can build new examples of polynomials that satisfy the *SFC* using known examples.

3.1 Linear Polynomials

In this section we consider the following polynomial:

$$G = \sum_{i=1}^{m} \lambda_i T_i \tag{3.1}$$

where $\lambda_i \in \mathbb{C}$, $1 \leq i \leq m$. In [33] it was shown that G^r satisfies the **FC**. We extend this result by showing that G^r satisfies the **SFC** (see Theorem 3.3). We also show that $\lambda_0 + G$ satisfies the **SFC** (see Theorem 3.7).

Let $x = (x_1, \ldots, x_m)$ be m commuting variables. The following two families of polynomials will be of use to us.

Definition 3.1. Let K be a field. The **complete homogeneous symmetric polynomial** $h_n(x)$ of degree $n \geq 0$ is defined by

$$h_n(x) = \sum_{\alpha \in \mathbb{N}^m,\, |\alpha|=n} x^\alpha$$

When $n = 0$ it should be understood that $h_0(x) = 1$.

Definition 3.2. Let K be a field. For $1 \leq k \leq m$ the kth **elementary symmetric polynomial** in m variables over K is given by

$$e_k(x) = \sum_{1 \leq i_1 < \cdots < i_k \leq m} \prod_{j=1}^{m} x_j^{i_j}$$

When $k = 0$ we set $e_0(x) = 1$.

The polynomials $h_n(x)$ and $e_k(x)$ are related to each other in the following way: Let U be an indeterminate and set $P(U) = \prod_{i=1}^{m} (1 - x_i U) \in (K[x])[U]$. Then $P(U)$ has a mulitplicative inverse belonging to $K[x][[U]]$ (since its constant coefficient is equal to 1). Furthermore, we have

$$P(U) = \sum_{k=0}^{m} (-1)^k e_k(x) U^k \tag{3.2}$$

$$P(U)^{-1} = \sum_{n=0}^{\infty} h_n(x) U^n \tag{3.3}$$

From the equality $P(U)P(U)^{-1} = 1$ one obtains the following relation which holds for all $n \geq 1$ (with the caveat $h_n = 0$ for $n < 0$).

$$\sum_{k=0}^{m} (-1)^k e_k h_{n-k} = 0 \tag{3.4}$$

Theorem 3.3. *Let G be given as in* (3.1)*, and set $F = G^r$ where $r \geq 1$. If there exists $n \geq 1$ such that $\mathcal{L}\left(F^{n+i}\right) = 0$ for each $i \in \{0, 1, \ldots, m-1\}$ then $F = 0$.*

Proof. For any $n > 0$ we have $G^n = \sum_{|\alpha|=n} \binom{n}{\alpha} T^\alpha \lambda^\alpha$. Thus

$$\begin{aligned}\mathcal{L}\left(G^n\right) &= \sum_{|\alpha|=n} \binom{n}{\alpha} \alpha! \lambda^\alpha \\ &= n! \sum_{|\alpha|=n} \lambda^\alpha \\ &= n! h_n(\lambda) \qquad (3.5)\end{aligned}$$

Returning to $F = G^r$ we see that $\mathcal{L}\left(F^n\right) = \mathcal{L}\left(G^{nr}\right) = 0$ implies $h_{nr}(\lambda) = 0$. Therefore, to prove our claim, it suffices to show that the polynomials $h_{nr}(x)$, $h_{(n+1)r}(x) \dots, h_{(n+m-1)r}(x)$ have no nontrivial common zeroes for all $n \geq 1$. This is the content of Proposition 3.4. □

Proposition 3.4. *Let K be any field. For every $n, r \geq 1$ the set of polynomials $\{h_{ir} \colon n \leq i \leq n+m-1\}$ have no nontrivial common zeroes.*

Proof. Fix integers $n \geq 1$. Set $A = K[x]$ and let $P(U)$ be the polynomial defined in (3.2). Additionally, given $\lambda \in K^m$ and $H(U) \in A[[U]]$ let $H_\lambda(U) = \mathrm{ev}_\lambda(H(U))$, where $\mathrm{ev}_\lambda \colon A \to K$ is the evaluation at λ extended to $A[[U]]$ in the obvious way.

Suppose $r = 1$, and fix $n \geq 1$. Equation (3.4) implies the following: If λ is a common root of h_i for $n \leq i \leq n+m-1$ then $h_i(\lambda) = 0$ for all $i \geq n$. Thus $P_\lambda(U) \in (K[U])^* = K^*$. In particular, this implies that $e_k(\lambda) = 0$ for $1 \leq k \leq m$. Since $e_m(\lambda) = 0$ it follows that $\lambda_i = 0$. By using induction on m we see that $e_k(\lambda) = 0$, $1 \leq k \leq m$ if and only if $\lambda = (0, \dots, 0)$. This proves our claim for $r = 1$.

Now suppose $r > 1$. First, we will show that the set $\{h_{kr} \colon k \geq 1\}$ satisfies a recursive formula similar to the one found in Equation (3.4). For each $0 \leq i \leq r-1$ let $B_i = \sum_{k \geq 0} h_{kr+i}(x) T^{nr} \in A\left[[U^r]\right]$. It follows from Equation (3.3) that

$$P(U)^{-1} = B_0 + B_1 U + \cdots + B_{r-1} U^{r-1}.$$

Next, we define $Q(U) = \prod_{i=1}^{m} \left(1 - x_i^r U^r\right) \in A\left[U^r\right]$. A straightforward calculation then shows that

$$Q(U)/P(U) = \prod_{i=1}^{m} \left(\sum_{j=0}^{r-1} x_i^j U^j \right) \in A[U]$$

Furthermore $\deg(Q(U)/P(U) = mr - m$.

Write $Q(U)/P(U) = Q_0 + Q_1 U + \cdots + Q_{r-1} U^{r-1}$ for some $Q_0, Q_1, \ldots, Q_{r-1} \in A[U^r]$. We now have the following equality:

$$\sum_{j=0}^{r-1} QB_j U^j = Q(U)/P(U) = \sum_{j=0}^{r-1} Q_j U^j \in A[U] \tag{3.6}$$

Since QB_j, Q_j all lie in $A[[U^r]]$ for $0 \leq j \leq r-1$ there is neither cancellation amongst the summands of the left hand side of (3.6) nor is there cancellation amongst the summands of the right hand side, and therefore $QB_j = Q_j \in A\left[U^r\right]$ for each j. Expanding $Q(U)$ we obtain $Q(U) = \sum_{j=0}^{m} (-1)^j e_j(x^r) U^{jr}$. Write $Q_0 = q_0 + q_1 U^r + \cdots + q_l U^{lr}$ for some $q_j \in K[x]$, and some $l \in \mathbb{N}$. Note that $lr \leq \deg(Q(U)/P(U)) = mr - m$ implies that $l < m$. Equating Q_0 to QB_0 yields the following recursive relation which holds for all $k \geq 1$:

$$h_{kr} - e_1\left(x^r\right) h_{kr-k} + \cdots + (-1)^m e_m\left(x^r\right) h_{kr-mr} = \begin{cases} q_k & k \leq l \\ 0 & k > l \end{cases} \tag{3.7}$$

Now suppose λ is a common root of $\{h_{ir} \colon n \leq i \leq n+m-1\}$. Equation (3.7) implies that $h_{kr}(\lambda) = 0$ for all $k \geq n+m > l$, and as a result $(B_0)_\lambda \in K[U]$. Note that $(B_0)_\lambda \neq 0$ since it has constant coefficient equal to one. Finally, we consider the equality

$$Q_\lambda = Q_\lambda\left(P_\lambda^{-1} P_\lambda\right) = \left(Q_\lambda\left(B_0\right)_\lambda + \cdots + Q_\lambda\left(B_{r-1}\right)_\lambda U^{r-1}\right) P_\lambda$$

Recall that there is no cancellation amongst the summands of

$$Q_\lambda\left(B_0\right)_\lambda + \cdots + Q_\lambda\left(B_{r-1}\right)_\lambda U^{r-1}$$

and hence the sum has degree at least the degree of $Q_\lambda\,(B_0)_\lambda$. Since $(B_0)_\lambda$ is a nonzero polynomial it follows that the above sum has degree at least the degree of Q_λ. This shows that the degree of P_λ is equal to zero, i.e., $P_\lambda = 1$. So once again $e_k(\lambda) = 0$ for $1 \leq k \leq m$, and hence $\lambda = (0, \ldots, 0)$.

□

Remark 3.5. The problem of describing the subsets $A \subset \mathbb{N}_+$ of size m such that the set of polynomials $h_a(x)$ with $a \in A$ has no common nontrivial zeroes was considered by Conca, Krattenthaler, and Watanabe in [7]. Proposition 3.4 is a new example of such a subset A.

In addition to proving **SFC** for linear forms, Proposition 3.4 also yields the following corrollary.

Corollary 3.6. *Let K be any field, $P(U) \in K[U] \setminus K$ a polynomial with constant term 1, $\deg(P) = m \geq 1$, and let $P^{-1}(U) = 1 + a_1U + a_2U^2 + \cdots$ be its multiplicative inverse in the power series ring $K[[U]]$. For each $n, r \geq 1$ there exists $0 \leq i \leq m-1$ such that $a_{(n+i)r} \neq 0$.*

Proof. We write $\overline{K}$ for the algebraic closure of K. Suppose $P(U)$ is nonconstant with constant term 1, and let $m = \deg(P)$. Since the constant term of P is equal to 1 there exists $\lambda \in \overline{K}^m \setminus \{(0, \ldots, 0)\}$ such that $P(U) = \prod_{j=1}^{m} (1 - \lambda_j U)$. It now follows that $P^{-1}(U) = \sum_{i=0}^{\infty} h_i(\lambda) U^i$, and therefore $a_i = h_i(\lambda)$. Now apply the previous proposition to conclude that for all $n \geq 1$ there is some integer $i \in [n, n+m-1]$ such that $a_i \neq 0$. □

We conclude this section with the following result.

Theorem 3.7. *Let G be as in (3.1) and set $F = \lambda_0 + G$ where $\lambda_0 \in \mathbb{C}$. If there exists $n \geq 1$ such that $\mathcal{L}\left(F^{n+i}\right) = 0$ for each $i \in \{0, 1, \ldots, m-1\}$ then $F = 0$.*

Proof. If $\lambda_0 = 0$ then we are done by Theorem 3.3. So we assume $\lambda_0 \neq 0$. Set $f_n = \mathcal{L}\left(F^n\right)/n!$,

$n \geq 1$, and let $\lambda = (\lambda_1, \ldots, \lambda_m)$. Using Equation (3.5) we calculate f_n:

$$\begin{aligned} f_n &= \sum_{k=0}^{n} \frac{1}{k!(n-k)!} \mathcal{L}\left(G^{n-k}\right) \lambda_0^k \\ &= \sum_{k=0}^{n} \frac{(n-k)!}{k!(n-k)!} h_{n-k}(\lambda) \lambda_0^k \\ &= \sum_{k=0}^{n} \frac{1}{k!} h_{n-k}(\lambda) \lambda_0^k \end{aligned}$$

Note that $\mathcal{N}(F) = m+1$, and so we must show that one of $f_n, \ldots, f_{n+m}$ is not zero for all $n \geq 1$. Fix $n \geq 1$ and let $g = \sum_{k=0}^{m} (-1)^k e_k(\lambda) f_{n+m-k}$ and write $g = \sum_{k=0}^{n+m} g_k \lambda_0^k$. Then

$$g_k = \frac{1}{k!} \sum_{j=0}^{m} (-1)^j e_j(\lambda) h_{n+m-k-j}(\lambda), \quad 0 \leq k \leq n+m$$

Using Equation (3.4) we obtain $g_k = 0$ for $0 \leq k \leq n+m-1$ and $g_{n+m} = 1$. Thus $g = \lambda_0^{n+m}/(n+m)! \neq 0$. Since g is a $\mathbb{C}$-linear combination of $f_n, \ldots, f_{n+m}$ it follows that one of $f_n, \ldots, f_{n+m}$ is not zero. □

3.2 Sums of Prime Powers

In this section we fix a prime $p \in \mathbb{Z}$. Let $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{C}^m$, $\beta = (\beta_1, \ldots, \beta_m) \in (\mathbb{N}_+)^m$ and consider the polynomial

$$G(T) = \lambda_1 T_1^{p^{\beta_1}} + \lambda_2 T_2^{p^{\beta_2}} + \cdots + \lambda_m T_m^{p^{\beta_m}} \tag{3.8}$$

Recall that given $f \in \mathbb{Z}^{[m]}$ we denote by $\overline{f}$ the image of f in $\mathbb{F}_p^{[m]}$ under the canonical map. The following two lemmas will be important in the proofs that follow.

Lemma 3.8. *If k and l are positive integers then $\left(p^l k\right)!/\left(p^{ka} k!\right) \in \mathbb{Z}$ where $a = (p^l - 1)/(p-1)$. Moreover, $\left(p^l k\right)!/\left(p^{ka} k!\right) \equiv (-1)^{ka} \mod p$.*

Proof. We first consider the case $l = 1$. Set $Q(t) = \prod_{i=1}^{p-1}(pt - i)$. Then

$$\begin{aligned}(pk)! &= pkQ(k)(pk-p)Q(k-1)\cdots pQ(1)\\ &= \prod_{j=1}^{k} pj \cdot \prod_{j=1}^{k} Q(j)\\ &= p^k k! \prod_{j=1}^{k} Q(j) \end{aligned} \tag{3.9}$$

So $(pk)!/\left(p^k k!\right) = \prod_{j=1}^{k} Q(j) \in \mathbb{Z}$. Clearly, $Q(j) \equiv (-1)^{p-1}(p-1)! \mod p$ for all integers j. Noting $(-1)^{p-1} \equiv 1 \mod p$ for any prime and appealing to Wilson's Theorem we see that $Q(j) \equiv -1 \mod p$ for all integers j. Thus $\prod_{j=1}^{k} Q(j) \equiv (-1)^k \mod p$ which is what we wanted to show.

For the general case we define $P(n) = \prod_{j=1}^{n} Q(j)$ where $n \in \mathbb{Z}$. We also set $k_j = p^{l-j}k$, $1 \le j \le l$. Applying the $l = 1$ case we obtain

$$(k_j)! = (pk_{j+1})! = p^{k_{j+1}} k_{j+1}! P\left(k_{j+1}\right), \quad 0 \le j \le l-1 \tag{3.10}$$

It follows from Equation (3.10) that

$$\left(p^l k\right)! = p^{\sum_{j=1}^{l} k_j} k_l! \prod_{j=1}^{l} P\left(k_j\right)$$

Now $k_l = k$ and $\sum_{j=1}^{l} k_j = k\sum_{j=1}^{l} p^{l-j} = ka$, and therefore $\left(p^l k\right)!/\left(p^{ka}k!\right) = \prod_{j=1}^{l} P\left(k_j\right)$ is an integer. Finally, since $P\left(k_j\right) \equiv (-1)^{k_j} \mod p$ it follows that $\prod_{j=1}^{l} P\left(k_j\right) \equiv (-1)^{ka} \mod p$. □

Lemma 3.9. *Suppose I is a proper homogeneous ideal of $\mathbb{Z}^{[m]}$. If $\mathcal{Z}_{\overline{\mathbb{F}}_p}(\overline{I}) = \{(0,\ldots,0)\}$ then $\mathcal{Z}_{\overline{\mathbb{Q}}}(I) = \{(0,\ldots,0)\}$.*

Proof. By the Projective Nullstellensatz we must show that $I \bigotimes_{\mathbb{Z}} \mathbb{Q}$ contains all monomials of degree d for $d >> 0$. Let $V_d \subset \mathbb{Z}^{[m]}$ be the $\mathbb{Z}$-module of d-forms. Let I_d be the $\mathbb{Z}$-module of d-forms belonging to I, i.e, $I_d = V_d \cap I$. Note that I_d and V_d are finitely generated. Furthermore, we have that $\mathbb{Z}^{[m]} = \bigoplus_{d=0}^{\infty} V_d$ and $I = \bigoplus_{d=0}^{\infty} I_d$. Since $\mathcal{Z}_{\overline{\mathbb{F}}_p}(\overline{I}) = \{(0,\ldots,0)\}$ it follows from the Nullstellensatz that

$$V_d = I_d + pV_d \qquad\qquad d >> 0 \tag{3.11}$$

Now let $S = \mathbb{Z} \setminus (p)$, and denote by $\mathfrak{m}$ the maximal ideal of the local ring $S^{-1}\mathbb{Z}$. Localizing (3.11) at (p) yields $S^{-1}V_d = S^{-1}I_d + \mathfrak{m}S^{-1}V_d$ for $d >> 0$. Thus, $S^{-1}V_d = S^{-1}I_d$ for $d >> 0$ by Nakayamas Lemma. Since $V_d \bigotimes \mathbb{Q}$ is a further localization of $S^{-1}V_d$ we obtain $V_d \bigotimes \mathbb{Q} = I_d \bigotimes \mathbb{Q}$ for $d >> 0$.

□

Theorem 3.10. *Let G be as in* (3.8) *and set $F = G^r$, $r \geq 1$. If there exists $n \geq 1$ such that $\mathcal{L}(F^{n+i}) = 0$ for $0 \leq i \leq m-1$ then $F = 0$.*

Proof. Given $\gamma = (\gamma_1, \ldots, \gamma_m) \in \mathbb{Z}^m$ set $p^\gamma = (p^{\gamma_1}, \ldots, p^{\gamma_m})$. For any $n > 0$ we have $G^n = \sum_{|\alpha|=n} \binom{n}{\alpha} T^{p^\beta \alpha} \lambda^\alpha$ where $p^\beta \alpha = \left(p^{\beta_1}\alpha_1, \ldots, p^{\beta_m}\alpha_m\right)$. Thus:

$$\frac{\mathcal{L}(G^n)}{n!} = \sum_{|\alpha|=n} \frac{(p^\beta \alpha)!}{\alpha!} \lambda^\alpha$$

Let $x = (x_1, \ldots, x_m)$ be m commuting variables. For each $n > 0$ define

$$f_n(x) = \sum_{|\alpha|=n} \frac{(p^\beta \alpha)!}{\alpha!} x^\alpha$$

Then the $\lambda \in \mathbb{C}^m$ for which $\mathcal{L}(G^n) = 0$ are exactly the zeroes of $f_n(x)$. Let I_n be the homogeneous ideal of $\mathbb{Z}[x]$ generated by $\left\{f_{(n+i)r}(x) : 0 \leq i \leq n+m-1\right\}$. Our claim will be proven if we can show that $\mathcal{Z}_{\mathbb{C}}(I_n) = \{(0,\ldots,0)\}$ for each $n > 0$.

Using Lemma 3.8 we know that $\left(p^{\beta_j}\alpha_j\right)! = p^{\alpha_j b_j}\alpha_j! C_{\alpha_j}$ where $b_j = \left(p^{\beta_j} - 1\right)/(p-1)$ and

C_{α_j} is an integer congruent modulo p to $(-1)^{\alpha_j b_j}$. So if we set $\gamma_\alpha = (\alpha_1 b_1, \ldots, \alpha_m b_m)$ then

$$\left(p^\beta \alpha\right)! = p^{|\gamma_\alpha|} \alpha! C_\alpha \tag{3.12}$$

where $C_\alpha = \prod_{j=1}^m C_{\alpha_j}$. Since each $C_{\alpha_j} \equiv (-1)^{\alpha_j b_j} \mod p$ it follows that $C_\alpha \equiv (-1)^{|\gamma_\alpha|} \mod p$.

Let $\tilde{\beta} = (b_1, \ldots, b_m)$, $\tilde{x} = (-p)^{-\tilde{\beta}} x$, and for each $n > 0$ define $g_n(x) = f_n(\tilde{x})$. If J_n is the homogeneous ideal of $\mathbb{Z}[x]$ genearted by $\left\{g_{(n+i)r}(x) : 0 \leq i \leq n+m-1\right\}$ then $\mathcal{Z}_{\mathbb{C}}(J_n) = \{(0, \ldots, 0)\}$ if and only if $\mathcal{Z}_{\mathbb{C}}(I_n) = \{(0, \ldots, 0)\}$. We will show the former. Let us first simplify the expression for g_n. Using Equation (3.12) we calculate

$$\begin{aligned} g_n(x) &= \sum_{|\alpha|=n} \frac{\left(p^\beta \alpha\right)!}{\alpha!} \left((-p)^{-\tilde{\beta}} x\right)^\alpha \\ &= \sum_{|\alpha|=n} (-1)^{|\gamma_\alpha|} \frac{\left(p^\beta \alpha\right)!}{p^{|\gamma_\alpha|} \alpha!} x^\alpha \\ &= \sum_{|\alpha|=n} (-1)^{|\gamma_\alpha|} \frac{p^{|\gamma_\alpha|} \alpha! C_\alpha}{p^{|\gamma_\alpha|} \alpha!} x^\alpha \\ &= \sum_{|\alpha|=n} (-1)^{|\gamma_\alpha|} C_\alpha x^\alpha \end{aligned} \tag{3.13}$$

Since $C_\alpha \equiv (-1)^{|\gamma_\alpha|} \mod p$ it follows that $g_n(x) \equiv \sum_{|\alpha|=n} x^\alpha = h_n(x)$. In particular, we have $\overline{J}_n = \left\langle h_{nr}, \ldots, h_{(n+m-1)r} \right\rangle$. It follows from Proposition 3.4 that $\mathcal{Z}_{\overline{F}_p}\left(\overline{J}_n\right) = \{(0, \ldots, 0)\}$ and hence $\mathcal{Z}_{\mathbb{C}}(J_n) = \{(0, \ldots, 0)\}$ by Lemma 3.9.

□

We end this section with the following partial result.

Proposition 3.11. *Let $p > m$ be a prime integer, and let $F = \lambda_0 + G$ where G is given in 3.8. If $\mathcal{L}\left(F^{n+j}\right) = 0$ for some $n < p - m$ and $0 \leq j \leq m$ then $F = 0$.*

Proof. Note $\mathcal{N}(F) = m + 1$. For $n > 0$ we have

$$\mathcal{L}\left(F^n\right) = \sum_{k=0}^{n} \binom{n}{k} \mathcal{L}\left(G^{n-k}\right) \lambda_0^k$$

Let y and $x = (x_1, \ldots, x_m)$ be indeterminates. For each $l > 0$ define

$$g_l(x) = \sum_{|\alpha|=l} \binom{l}{\alpha} \frac{(p^\beta \alpha)!}{\alpha!} x^\alpha$$
$$f_l(y, x) = \frac{1}{l!} \sum_{k=0}^{l} \binom{l}{k} g_{l-k}\left((-p)^{-\tilde{\beta}} x\right) y^k$$

where $\tilde{\beta} = (p-1)^{-1}\left(p^{\beta_1} - 1, \ldots, p^{\beta_m} - 1\right)$. Note that $l! f_l\left(\lambda_0, (-p)^{\tilde{\beta}} \lambda\right) = \mathcal{L}\left(F^l\right)$ for all $l \geq 0$. So our claim will be proven if we can show that $f_n, \ldots, f_{n+m}$ have no common nontrivial solutions over $\mathbb{C}$.

It follows from Lemma 3.8 and the proof of the previous theorem that $g_l\left((-p)^{-\tilde{\beta}} x\right)/l! \in \mathbb{Z}[x]$ and $g_l\left(p^{-\tilde{\beta}} x\right)/l! \equiv h_l(x) \mod p$ where $h_n(x)$ is defined in 3.1. Therefore

$$\overline{f}_{n+j}(y, x) \equiv \sum_{k=0}^{n+j} \frac{1}{k!} h_{n+j-k}(x) y^k \mod p$$

for $0 \leq j \leq m$. Since $n + m < p$ it follows that $k! \not\equiv 0 \mod p$ for all $0 \leq k \leq n + m$ and so $1/k! \in \mathbb{F}_p$, and so the above sum makes sense in $\mathbb{F}_p[x]$. Appealing to the proof of Theorem 3.7 we obtain the following:

$$\overline{f}_{n+m}(y, x) - e_1(x)\overline{f}_{n+m-1}(y, x) + \cdots + (-1)^m e_m(x)\overline{f}_n(y, x) = \frac{y^{n+m}}{(n+m)!}$$

If $(\lambda_0, \lambda) \in \overline{\mathbb{F}}_p^{m+1}$ is a common root of $\overline{f}_n, \ldots, \overline{f}_{n+m}$ then $\lambda_0 = 0$ by the above equality. So $0 = \overline{f}_{n+j}(\lambda_0, \lambda) = h_{n+j}(\lambda)$ and therefore $\lambda = (0 \ldots, 0)$ by Proposition 3.4. Thus $\overline{f}_n, \ldots, \overline{f}_{n+m}$ have no nontrivial common zeroes in $\overline{\mathbb{F}}_p$ and therefore $f_n, \ldots, f_{n+m}$ have no common zeroes over $\mathbb{C}$ by Lemma 3.9. □

3.3 Sum of Two Monomials

Throughout this section x will denote a single variable, rather than a vector of variables. In this section we study the **SFC** in the case F is of the form $\lambda_1 M_1 + \lambda_2 M_2$ where M_1 and M_2 are monomials. In order to show that the **SFC** holds for $F \neq 0$ we must show that one of $\mathcal{L}\left(F^n\right), \mathcal{L}\left(F^n\right)$ is nonzero for all $n \geq 2$. Since the **SFC** holds for monomials we may assume that $\lambda_1, \lambda_2 \neq 0$. Furthermore, since $\mathcal{L}\left(F^n\right)$ is homogeneous in λ_1, λ_2 we may assume, without loss of generality, that $\lambda_1 = 1$. For each $n \geq 0$ we define the following polynomial:

$$f_n(x) = \sum_{k=0}^{n} \binom{n}{k} \mathcal{L}\left(M_1^{n-k} M_2^{k}\right) x^k. \tag{3.14}$$

Then $f_n\left(\lambda_2\right) = \mathcal{L}\left(F^n\right)$. It follows that the **SFC** holds for F if and only if $f_n(x), f_{n-1}(x)$ have no common zeroes for all $n \geq 2$.

One way to attack the problem is to use Zeilberger's algorithm (see [29]) to find a recurrence relation between $f_n(x)$ and $f_{n-1}(x)$. The algorithm has been implemented in both Mathematica and Maple. For example, after downloading the fastZeil package (cf. [1]) for Mathematica, the command

```
Zb[Binomial[n,k] (2 k)! x^k,{k,0,n},n]:
SumCertificate[%]
```

will produce a recurrence relation for the polynomials $f_n(x) = \sum\limits_{k=0}^{n} \binom{n}{k}(2k)! x^k$. In some special cases, the relation obtained by Zeilberger's algorithm can be used in a very straightforward manner to show that f_n and f_{n-1} have no common zeroes.

Proposition 3.12. *For all $n \geq 2$ the polynomials $f_n(x)$ and $f_{n-1}(x)$ have no common zeroes in the following cases:*

1. $F = 1 + \lambda T_1$

2. $F = T_1^2 + \lambda T_1$

3. $F = T_1^3 + \lambda T_1^2$

4. $F = T_1^2 + \lambda T_1 T_2$

5. $F = T_1^3 + \lambda T_1^2 T_2$

Proof. We proceed case by case.

1. In this case we have $F^n = \sum\limits_{k=0}^{n} \binom{n}{k} T_1^k \lambda^k$ which gives $f_n(x) = \sum\limits_{k=0}^{n} \frac{n!}{(n-k)!} x^k$. Using Zeilberger's lgorithm we obtain the relation: $f_n(x) = nxf_{n-1}(x) + 1$. If $\lambda \in \mathbb{C}$ is a common root of f_n and f_{n-1} then $1 = 0$ which is a contradiction.

2. In this case we have $F^n = \sum_{k=0}^{n} \binom{n}{k} T_1^{2n-k} \lambda^k$ which gives $f_n(x) = \sum\limits_{k=0}^{n} \binom{n}{k} (2n-k)! x^k$. Using Zeilberger's We have the following relation:

$$f_n(x) - 2n(2n-1)f_{n-1}(x) - n(n-1)x^2 f_{n-2}(x) = 0$$

   Suppose $\lambda \in \mathbb{C}$ is a common root of f_n and f_{n-1}. Since $f_l(0) \neq 0$ for all $l \in \mathbb{N}$ follows that $f_{n-2}(\lambda) = 0$. Changing n to $n-1, \ldots, 2$ in the above recurrence relation shows that λ is a root of $f_n, f_{n-1}, \ldots, f_0$. But f_0 is a nonzero constant and we get a contradiction.

3. In this case we have $F^n = \sum\limits_{k=0}^{n} T_1^{3n-k} \lambda^k$ which gives $f_n(x) = \sum\limits_{k=0}^{n} \binom{n}{k} (3n-k)! x^k$. Zeilberger's algorithm produces the relation:

$$(x - 9n + 12)f_n(x) - p_n(x)f_{n-1}(x) + q_n(x)f_{n-2}(x) = 0$$

   where

$$p_n(x) = x^3 - 3(3n-2)x^2 + (27n^2 - 27n + 6)x - (243n^3 - 567n^2 + 378n - 72)$$

and

$$q_n(x) = 2(2n-3)n(n-1)x^3(x-3(3n-1))$$

Suppose λ is a common root of f_n and f_{n-1}. Then $q_n(\lambda) = 0$ or $f_{n-2}(\lambda) = 0$. If $q_n(\lambda) = 0$ then $\lambda = 0$ or $\lambda = 3(3n-1)$. Since $f_l(0) \neq 0$ for all l, λ cannot be equal to zero. Since n or $n-1$ is even it follows from Corollary 2.11 that $\lambda \in \mathbb{C} \setminus \mathbb{R}$ and therefore $\lambda \neq 3(3n-1)$. So $f_{n-2}(\lambda) = 0$. Replacing n with $n-1, \ldots, 2$ in the recurrence relation and repeating the same argument as before shows that $f_l(\lambda) = 0$ for $0 \leq l \leq n$. However, f_0 is a nonzero constant and we get a contradiction.

4. In this case we have $F^n = \sum_{k=0}^{n} \binom{n}{k} T_1^{2n-k} T_2^k \lambda^k$ which gives $f_n(x) = \sum\limits_{k=0}^{n} \frac{n!}{(n-k)!}(2n-k)!x^k$. Using Zeilberger's algorithm we obtain the relation: $(x-1)f_n(x) - n^2x^2 f_{n-1} = n(2n-1)!(x-2)$. If λ is a common root of f_n and f_{n-1} then $\lambda = 2$. But this impossible since $f_n(2) > 0$ for all n.

5. In this case we have $F^n = \sum_{k=0}^{n} \binom{n}{k} T_1^{3n-k} T_2^k \lambda^k$ which gives $f_n(x) = \sum\limits_{k=0}^{n} \frac{n!}{(n-k)!}(3n-k)!x^k$. Using Zeilberger's algorithm we obtain the relation: $(x-1)^2 f_n(x) - 2n^2(2n-1)x^3 f_{n-1} = (3n-2)!np_n(x)$ where $p_n(x) = (4n-2)x^2 - 5(3n-1)x + 3(3n-1)$. If λ is a common root of f_n and f_{n-1} then λ is also a root of p_n. The discriminant of p_n is equal to $81n^2 - 30n + 1$ which is positive for all $n > 0$. Therefore $\lambda \in \mathbb{R}^*$. Since n or $n-1$ is even this would contradict Corollary 2.11. So f_n and f_{n-1} have no common zeroes.

□

Let us now turn our attention to $F = T_1^m(\lambda_1 + \lambda_2 T_1)$ where $\lambda_1, \lambda_2 \in \mathbb{C}^*$. From the above Proposition we know that F satisfies the **SFC** for $m = 0, 1, 2$. Once again assuming $\lambda_1 = 1$ we have the following partial result for the general case.

Proposition 3.13. *Let $F = T_1^m(1 + \lambda T_1)$ where $m \geq 3$. If $m \nmid ((n-1)!)^n$ then $\mathcal{L}(F^n) \neq 0$ or $\mathcal{L}(F^{n-1}) \neq 0$.*

Proof. We have $F^n = \sum_{k=0}^n \binom{n}{k} T_1^{nm+k}\lambda^k$ and so $\mathcal{L}(F^n) = \sum\limits_{k=0}^{n} \binom{n}{k}(nm+k)!\lambda^k$. For each $n \geq 0$ define a polynomial $f_n(x)$ by setting $f_n(x) = \sum\limits_{k=0}^{n} \binom{n}{k} \dfrac{(nm+k)!}{(nm)!}x^k$. We have $f_n(\lambda) = \mathcal{L}(F^n)/(nm)!$. Note that $f_n(x) \in \mathbb{Z}[x]$. Introduce a new variable t and for each $k > 0$ define $Q_{n,k}(t) = \prod\limits_{j=1}^{k}(nt+j)$. For each $n > 0$ we define a bivariate polynomial $F_n(t,x) \in \mathbb{Z}[t,x]$ by setting

$$F_n(t,x) = 1 + \sum_{k=1}^{n} \binom{n}{k} Q_{n,k}(t)x^k.$$

Observe that $F_n(m,x) = f_n(x)$. For each $n \geq 2$ we wish to compute the resultant of $F_n(t,x)$ and $F_{n-1}(t,x)$ with respect to the variable x. It is for this reason we define, for each $n \geq 2$, the polynomial $R_n(t) = \operatorname{Res}(F_n(t,x), F_{n-1}(t,x), x)$. It follows from the definition of the resultant that $R_n(t) \in \mathbb{Z}[t]$. Also, since $F_n(m,x) = f_n(x)$ it follows from the determinant formula for the resultant that $R_n(m) = \operatorname{Res}(f_n, f_{n-1})$. So using Proposition 2.13 we see that F satisfies the *SFC* if and only if $R_n(m) \neq 0$ for all $n \geq 2$.

Let $p_n(t) = (nt+1)$ and let $R = \mathbb{Z}[t]$. Since p_n is linear and primitive it is an irreducible elmement of the ring R, which is a UFD. Observe that p_n does not divide the constant coefficient of $F_n(t,x)$ when regarded as an element of $R[x]$. Also, $p_n(t)$ divides the coefficients of $Q_{n,k}$ for $1 \leq k \leq n$, but $p_n^2 \nmid Q_{n,n}$. Thus, by applying Eisensteins criteria to the reciprocal polynomial $F_n^*(t,x) = x^n F_n(t, 1/x)$ we see that $F_n(t,x)$ is an irreducible element of $R[t]$. Thus $F_n(t,x)$ and $F_{n-1}(t,x)$ have no common factor over $\mathbb{Q}(t)$ by Gauss's Lemma. So it follows from Proposition 2.13 that $R_n(t) \neq 0$.

Since $R_n(t) \in \mathbb{Z}[t] \setminus \{0\}$ we know that $R_n(m) \neq 0$ if $m \nmid R_n(0)$. Therefore we calculate $R_n(0)$. Since the determinant commutes with the evaluation map we have
$R_n(0) = \det(\operatorname{Syl}(F_n(0,x), F_{n-1}(0,x)))$. Now $Q_{n,k}(0) = k!$ and so $F_n(0,x) = \sum\limits_{k=0}^{n} \dfrac{n!}{(n-k)!}x^k$. Since $\deg_x F_n(0,x) = n$ for each $n \geq 1$ it follows that $R_n(0) = \operatorname{Res}(F_n(0,x), F_{n-1}(0,x))$ for each $n \geq 2$. Next, a straightforward calculation shows that $F_n(0,x) = nxF_{n-1}(0,x) + 1$. It

now follows from part *(ii)* of Proposition 2.15 that

$$R_n(0) = \operatorname{Res}\left(F_n(0,x), F_{n-1}(0,x)\right) = ((n-1)!)^n \operatorname{Res}\left(1, F_{n-1}(0,x)\right) = ((n-1)!)^n .$$

So $R_n(0) \neq 0$ if $m \nmid ((n-1)!)^n$ □

In the above proof the idea was to express the resultant of f_n and f_{n-1} as a polynomial in m. This transforms the problem into one about deciding whether m is an integer root of this polynomial. Below, we list $R_n(t)$ for small values of n:

$$\begin{aligned}
R_2(t) &= (t+1)^2 \\
R_3(t) &= (t+1)^2(8 + 44t + 69t^2 + 22t^3 + t^4) \\
R_4(t) &= (t+1)^2(1296 + 19872t + 122328t^2 + 385184t^3 + 655289t^4 \\
&\qquad + 586650t^5 + 251751t^6 + 47580t^7 + 3543t^8 + 106t^9 + t^{10})
\end{aligned}$$

The first thing we notice is that each coefficient is positive. Further computations with the computer suggest that this is true in general. However, we have been unsuccessful at effectively computing $R_n(t)$ in general. The only other information we know about $R_n(t)$ is its degree and its leading coefficient. If in the Sylvester matrix of F_n and F_{n-1} we replace each $Q_{n,k}(t)$ and $Q_{n-1,k}(t)$ with their leading terms then the determinant of the resulting matrix will give the leading term (assuming the determinant is nonzero). Looking at the entries of the resulting matrix we see that its determinant is equal to the resultant of the polynomials $\sum_{k=0}^{n} \binom{n}{k}(nt)^k x^k$ and $\sum_{k=0}^{n-1} \binom{n-1}{k}((n-1)t)^k x^k$, which factor as $(1+ntx)^n$ and $(1+(n-1)tx)^{n-1}$, respectively. Note that these polynomials have roots belonging to the field $\mathbb{Q}(t)$. So using the product formula for the resultant (see Proposition 2.14) one can calculate the leading term $\operatorname{LT}(R_n(t))$ of

$R_n(t)$ as follows:

$$\begin{aligned}
\mathrm{LT}\left(R_n(t)\right) &= \mathrm{Res}\left((1+ntx)^n, (1+(n-1)tx)^{n-1}\right) \\
&= (nt)^{n-1}((n-1)t)^n \left(-\frac{1}{nt} + \frac{1}{(n-1)t}\right)^{n(n-1)} \\
&= (n(n-1)^{n(n-1)}t^{n(n-1)} \left(\frac{t}{t(n(n-1)}\right)^{n(n-1)} \\
&= t^{n(n-1)}
\end{aligned}$$

Even though we have not succeded in computing $R_n(t)$ the method can be used on other special instances of $F = \lambda_1 M_1 + \lambda_2 M_2$ to obtain results similar to Proposition 3.13. Of course, the following results rely on our abilitiy to compute the constant coefficient of the determinant of A where A is a square matrix with entries belonging to $\mathbb{Z}[t]$.

Proposition 3.14. *Let $F = T_1^m\left(T_2 + \lambda T_1 T_3\right)$ where $m > 0$. If $m \nmid (n!)^{n-1}$ then $\mathcal{L}\left(F^n\right) \neq 0$ or $\mathcal{L}\left(F^{n-1}\right) \neq 0$.*

Proof. Suppose $n > 0$. We have $F^n = \sum_{k=0}^n \binom{n}{k} T_1^{nm+k} T_2^{n-k} T_3^k \lambda^k$ which gives

$$\begin{aligned}
\mathcal{L}\left(F^n\right) &= \sum_{k=0}^n \binom{n}{k}(n-k)!k!(nm+k)!\lambda^k \\
&= n! \sum_{k=0}^n (nm+k)!\lambda^k
\end{aligned}$$

We define $f_n(x) = \sum_{k=0}^n (nm+k)!x^k$ and $F_n(t,x) = 1 + \sum_{k=1}^n Q_{n,k}(t)x^k$ where $Q_{n,k}$ was defined in the proof of Proposition 3.13. Note $f_n(\lambda) = 0$ if and only if $\mathcal{L}\left(F^n\right) = 0$. Also $F_n(m,x) = f_n(x)/(nm)!$. Now, like in the proof of the previous proposition, set $R_n(t) = \mathrm{Res}\left(F_n, F_{n-1}, x\right)$. Then $R_n(0) = \mathrm{Res}\left(g_n(x), g_{n-1}(x), x\right)$ where $g_n(x) = \sum_{k=0}^n k!x^k$. Since $g_n = g_{n-1} + n!x^n$ it follows from Proposition 2.15 *(iii)* that

$$R_n(0) = \mathrm{Res}\left(n!x^n, g_{n-1}, x\right) = (n!)^{n-1}.$$

If $m \nmid (n!)^{n-1}$ then $R_n(m) \neq 0$ and therefore f_n and f_{n-1} have no common zeroes. □

Proposition 3.15. *Let $F = (T_1T_2)^m (T_1 + \lambda T_2)$ where $m > 0$. If $l, n > 0$ are such that $gcd(l+1, n+1) = 1$ and if $m \nmid (l!)^n(n!)^l$ then $\mathcal{L}(F^n) \neq 0$ or $\mathcal{L}\left(F^l\right) \neq 0$.*

Proof. Suppose $n, l > 0$ satisfy the hypothesis. For any $s \geq 0$ we have

$$F^s = \sum_{k=0}^{s} \binom{s}{k} T_1^{sm+s-k} T_2^{sm+k} \lambda^k$$

and therefore

$$\mathcal{L}(F^s) = \sum_{k=0}^{s} \binom{s}{k} (sm+k)!(sm+s-k)!\lambda^k.$$

Let $Q_{s,k}(t)$ be the polynomial defined in the proof of Proposition 3.13 and for each $s \geq 0$ define $F_s(t,x) = \sum\limits_{k=0}^{s} \binom{s}{k} Q_{s,k}(t) Q_{s,s-k}(t) x^k$ (here we define $Q_{s,0} = 1$). Then $F_s(m, \lambda) = \mathcal{L}(F^s)/((nm)!)^2$. If we set $R(t) = \text{Res}(F_n(t,x), F_l(t,x), x)$ then $R(m) = \text{Res}(f_n, f_l, x)$. Now $R(0) = \text{Res}(g_n(x), g_l(x), x)$ where

$$\begin{aligned} g_s(x) &= \sum_{k=0}^{s} \binom{s}{k} k!(s-k)! x^k \\ &= s! \sum_{k=0}^{s} x^k \end{aligned}$$

Using the definition of the resultant we see that $R(0) = (n!)^l (l!)^n \,\text{Res}(g_n(x)/n!, g_l(x)/l!)$. Denote each $g_s(x)/s!$ by $h_s(x)$. We claim that $\text{Res}(h_a(x), h_b(x), x) = 1$ whenever $\gcd(a+1, b+1) = 1$. Note that a or b is even since $\gcd(a+1, b+1) = 1$, and therefore $\text{Res}(h_a, h_b, x) = \text{Res}(h_b, h_a, x)$.We proceed by induction on $a + b$. The base case $a + b = 1$ holds because $g_0 = 1$ and therefore $\text{Res}(1, g_1, x) = 1$. Now suppose $a + b = d \geq 2$ and assume the claim is true for all pairs (a', b') satisfying $gcd((a'+1, b'+1) = 1$ and $n' + m' < d$.

Without loss of generality we may assume $a > b$. Write $a + 1 = q(b+1) + r$ for some positive integers q, r with $r \leq b+1$. Now it is not too hard too see that

$$h_a(x) = \left(1 + x^{b+1} + \cdots + x^{(q-1)(b+1)}\right) h_b(x) + x^{q(b+1)} h_{r-1}(x)$$

Setting $P = x^{q(m+1)} h_{r-1}(x)$ and appealing to Proposition 2.15 we conclude that

$$\begin{aligned} \operatorname{Res}\left(h_a, h_b\right) &= \operatorname{Res}\left(P, h_n\right) \\ &= \operatorname{Res}\left(x^{q(b+1}, h_b\right) \operatorname{Res}\left(h_{r-1}, h_b\right) \\ &= \operatorname{Res}\left(h_{r-1}, h_b\right) \end{aligned}$$

Since $\gcd(a+1, b+1) = 1$ it follows that $\gcd(b+1, r) = 1$. Since $a + r < d$ the result now follows from by the inductive hypothesis.

Since $\gcd(n+1, l+1) = 1$ we can conclude that

$$R(0) = (n!)^l (l!)^n \operatorname{Res}\left(g_n(x)/n!, g_l(x)/l!\right) = (n!)^l (l!)^n.$$

Since $m \nmid (n!)^{n-1}$ it follows that $R(m) \neq 0$ and therefore $\mathcal{L}\left(F^n\right) \neq 0$ or $\mathcal{L}\left(F^l\right) \neq 0$. □

Remark 3.16. Let us briefly return to the situation of $F = T_1^m\left(1 + \lambda T_1\right)$. In order to show that F satisfied the *SFC* one needs to show that $f_n(x)$ and $f_{n-1}(x)$ have no common zeroes where

$$f_l(x) = \sum_{k=0}^{l} \binom{l}{k} \frac{(lm+k)!}{(lm)!} x^k.$$

Fix an $n > 0$. By Dirchlet's prime number theorem we know that $nm+1$ is prime for infinitely many m. For such m we can show, using Eisensteins criteria, that $f_n(x)$ is irreducible over $\mathbb{Q}$ and therefore $f_n(x)$ and f_{n-1} have no common zeroes over $\mathbb{C}$. It is also straightforward to show that $f_n(x) \nmid f_{n+1}(x)$ which implies f_n and f_{n+1} have no common zeroes as well. We can also fix m, and applying the same theorems, conclude that f_n is irreducible for infinitely many m. The same arguments can also be applied to $F = T_1^m\left(T_2 + \lambda T_1 T_3\right)$. So there is ample evidence that both these polynomials satisfy the conjecture. The main reason we cannot resolve it in either of those two cases comes down to the fact that we cannot effectively compute the resultant $R_n(t)$. What's interesting is that computer experiments suggest that $R_n(t)$ is a stable polynomial, i.e., the complex zeroes of $R_n(t)$ lie in the left half plane. If this were so, then the coefficients of $R_n(t)$ would all be positive (since $R_n(0) > 0$), and therefore $R_n(m) \neq 0$. Stable polynomials are of great interest in general, and criteria for determining the stability of polynomials with real coefficients exits; however, we our attempts at utilizing these techniques have yet to succeed.

For the rest of the chapter we will focus our efforts on the special case $F = 1 + \lambda T_1^m$ where $m > 0$. We have $F^n = \sum_{k=0}^{n} \binom{n}{k} (mk)! \lambda^k$, and so we are interested in determining whether $f_n(x)$ and $f_{n-1}(x)$ have common zeroes, where

$$f_n(x) = \sum_{k=0}^{n} \binom{n}{k} (mk)! x^k \tag{3.15}$$

The first observation we would like to make is: if $n > 0$ then $f_n \nmid f_{n+1}$ over $\mathbb{Q}[x]$. Indeed, if $q(x) f_n(x) = f_{n+1}$ then $q(x) = ax + 1$ where $a = (mn+m)!/(mn)! \in \mathbb{Z}$. As a result we would have $(n+1)m! = (mn+m)!/(mn)! + n(m!)$, i.e. $m! = (mn+m)!/(mn)!$. But the last equality is true if and only if $m = 0$, a contradiction.

By studying the Newton polygon of $f_n(x)$ we can determine values of m and n for which f_n and f_{n-1} have no common zeroes. When $m = 2$ we solve the case completely. Given a prime p, we denote by ν_p the p-adic valuation. Given $k \in \mathbb{N}$ expand k in base p: $k = a_0 + a_1 p + \ldots + a_t p^t$. Set $s_k = a_0 + \cdots + a_t$. The following formulas are well known:

$$\begin{aligned} \nu_p(k!) &= \sum_{j=1}^{\infty} \left\lfloor \frac{k}{p^j} \right\rfloor \\ &= \frac{k - s_k}{p - 1} \end{aligned} \tag{3.16}$$

Proposition 3.17. *Suppose $n = ap^r$ where p is prime, $r > 0$ and $ma < p$. Then any* *irreducible factor of $f_n(x)$ over $\mathbb{Q}$ has degree divisible by p^r.*

Proof. We will show that $N_p\left(f_n(x)\right)$ consists of a single edge. We do this by showing that $\nu_p\left(\binom{n}{k}(mk)!\right) \geq \dfrac{k}{n}\nu_p((mn)!)$ for each $0 < k < n$. Using (3.16) we compute $\nu_p\left((mn)!\right) = \frac{ma(p^r-1)}{p-1}$ Next, if $0 < k < n$ then

$$\begin{aligned}\nu_p((n-k)!) &= \sum_{j=1}^{\infty}\left\lfloor \frac{ap^r - k}{p^j}\right\rfloor \\ &= \sum_{j=1}^{r}\left\lfloor \frac{ap^r - k}{p^j}\right\rfloor \\ &= \nu_p\left((ap^r)!\right) + \sum_{j=1}^{r}\left\lfloor \frac{-k}{p^j}\right\rfloor\end{aligned}$$

In the second line, the sum stops at $j = r$ because $0 < n - k < n < p^{r+1}$. Now

$$\nu_p(k!) + \sum_{j=1}^{r}\left\lfloor \frac{-k}{p^j}\right\rfloor = \sum_{j=1}^{r}\left\{\left\lfloor \frac{k}{p^j}\right\rfloor + \left\lfloor \frac{-k}{p^j}\right\rfloor\right\}$$

If $\dfrac{k}{p^j} \in \mathbb{Z}$ then $\left\lfloor \frac{k}{p^j}\right\rfloor + \left\lfloor \frac{-k}{p^j}\right\rfloor = 0$. Otherwise $\left\lfloor \frac{k}{p^j}\right\rfloor + \left\lfloor \frac{-k}{p^j}\right\rfloor = -1$. It follows that $\nu_p(k!) + \sum_{j=1}^{r}\left\lfloor \frac{-k}{p^j}\right\rfloor = \nu_p(k) - r$, and thus

$$\begin{aligned}\nu_p\left(\binom{n}{k}\right) &= \nu_p(n!) - (\nu_p((n-k)! + \nu_p(k!)) \\ &= \nu_p(n!) - \left(\nu_p(n!) + \nu_p(k!) + \sum_{j=1}^{r}\left\lfloor \frac{-k}{p^j}\right\rfloor\right) \\ &= r - \nu_p(k)\end{aligned}$$

We now consider the quantity $\dfrac{k}{n}\nu_p(mn!)$:

$$\begin{aligned}\frac{k}{n}\nu_p((mn)!) &= \frac{k}{ap^r}\frac{ma\,(p^r-1)}{p-1}\\ &= \frac{mk}{p^r}\left(p^{r-1}+\cdots+p+1\right)\\ &= \frac{mk}{p}+\cdots+\frac{mk}{p^r}\end{aligned}$$

For $1 \leq j \leq r$ write $\dfrac{mk}{p^i} = \left\lfloor \frac{mk}{p^i} \right\rfloor + a_j$ where $0 \leq a_j < 1$. Observe that $a_j = 0$ if and only if $p^j \nmid mk$. But $m < p$ and so $p^j \nmid mk$ if and only if $p^j \nmid k$. Thus $\sum_{j=1}^r \dfrac{mk}{p^j} < \displaystyle\sum_{j=1}^{r} \left\lfloor \frac{mk}{p^j} \right\rfloor + r - \nu_p(k)$. Finally, $mk < p^{r+1}$ since $ma < p$ and therefore $\displaystyle\sum_{j=1}^{r} \left\lfloor \frac{mk}{p^j} \right\rfloor = \nu_p((mk)!)$.

We have shown that $N_p\left(f_n\right)$ consists of a single edge connecting $(0,0)$ to $(n, ma\left(p^{r-1}+\cdots+1\right))$. The gcd of the height and width is equal to a and therefore any nontrivial irreducible factor of $f_n(x)$ has degree equal to ip^r for some $1 \leq i \leq a$ by Corollary 2.20. □

Corollary 3.18. *If $m < p$ then f_n is irreducible over $\mathbb{Q}[x]$ when $n = p^r$ for any positive r. Moreover, f_n and f_{n-1} have no common zeroes. The same is true for f_n and f_{n+1}.*

Proof. That f_n is irreducible follows from the previous proposition. Since $\mathbb{Q}[x]$ is a PID and since f_n is irreducible, f_n and f_{n-1} have no common roots. Since f_n does not divide f_{n+1} they do not have any common roots either. □

Suppose $m = p^r$ and set $b = \dfrac{p^r-1}{p-1}$. Then $\nu_p\left((p^r k)!\right) = kb + \nu_p(k!)$ by 3.8. This leads us to consider the polynomials $g_n(x) = f_n\left(x/p^b\right)$ for two reasons:

1. f_n and f_{n-1} have a common zero if and only if g_n and g_{n-1} have a common zero.

2. $\nu_p\left(\binom{n}{k}\frac{(p^r k)!}{p^{kb}}\right) = \nu_p\left(\frac{n!}{(n-k)!}\right)$ and so g_n has the same Newton polygon as $\sum_{k=0}^n \frac{n!}{(n-k)!}x^k$

Reason two is important because we can calculate the Newton polygon of $\sum_{k=0}^n \frac{n!}{(n-k)!}x^k$, and hence we can calculate the Newton polygon of g_n.

Proposition 3.19. *Let $n \geq 1$ be given and write $n = a_1p^{n_1} + a_2p^{n_2} + \cdots + a_tp^{n_t}$ where $0 < a_1, a_2, \ldots, a_t \leq p-1$ and $0 \leq n_1 < n_2 < \cdots < n_t$. Set $x_0 = 0$ and for $1 \leq s \leq t$ set $x_s = a_1p^{n_1} + \cdots + a_sp^{n_s}$. The x-coordinates of the vertices of $N_p\left(g_n(x)\right)$ are located at $x_s, 0 \leq s \leq t$. If $1 \leq s \leq t$ then the slope of the sth edge is given by $m_s = \frac{p^{n_s}-1}{p^{n_s}(p-1)}$.*

Proof. We write $\nu = \nu_p$. From the observations above we know that the coefficient of x^k has the same p-adic value as $\dfrac{n!}{(n-k)!}$. Since multiplying g_n by a constant has the effect of shifting the polygon up or down, we may assume that the coefficients are in fact $\frac{1}{(n-k)!}$. Using Equation (3.16) we calculate that

$$\nu\left((n-x_s)!\right) = \frac{n - x_s - (a_{s+1} + \cdots + a_t)}{p-1}$$

and therefore the slope of the line segment connecting the $(x_{s-1}, -\nu\left((n-x_{s-1})!\right))$ to $(x_s, -\nu\left((n-x_s)!\right))$ is equal to

$$\frac{x_s - x_{s_1} - a_s}{(x_s - x_{s-1})\,(p-1)} = \frac{p^{n_s}-1}{p^{n_s}(p-1)}.$$

Since $n_1 < n_2 < \cdots < n_t$ it follows that $m_1 < m_2 < \cdots < m_t$. So all that remains to show is that $(x, -\nu((n-x)!))$ lies on or above the edges connecting these points for each integer $1 \leq x \leq n$ that is not equal to some x_s. Choose $1 \leq s \leq t$ so that $x_{s-1} < x < x_s$. It follows that $n - x_s < n - x < n - x_{s-1}$. Set $\Delta x = x_s - x$, and observe that $n - x_{s-1} = n - x_s + a_sp^{n_s}$ implies $\Delta x < a_sp^{n_s}$, and therefore the base p expansion of Δx has no nonzero digit past the p^{n_s}-place. Since $n_s < n_{s+1}$ and since $n - x_s = a_{s+1}p^{n_{s+1}} + \cdots + p_t^{n_t}$ it now follows that the base p expansion of $n-x$ is obtained by concatenating the base p expansions of $n - x_s$ and Δx. Using Equation (3.16), one can obtain that $\nu((n-x)!) = \nu\left((n-x_s)!\right) + \nu((\Delta x)!)$

Finally, the slope between the points $(x, -\nu((n-x)!))$ and $(x_s, -\nu\left((n-x_s)!\right))$ is equal to

$$\begin{aligned}\frac{-\nu\left((n-x_s)!\right)+\nu((n-x)!)}{\Delta x} &= \frac{\nu((\Delta x)!)}{\Delta x}\\ &= \frac{\Delta x - s_{\Delta x}}{\Delta x(p-1)}\end{aligned}$$

We claim that $\dfrac{\Delta x - s_{\Delta x}}{\Delta x(p-1)} < m_s$, or equivalently, $p^{n_s}\left(\Delta x - s_{\Delta x}\right) < \Delta x\left(p^{n_s}-1\right)$. To prove this inequality, it suffices to show that $\Delta x < s_{\Delta x}p^{n_s}$, and this follows easily from the fact $\Delta x = b_0 + b_1 p + \cdots + b_{n_s}p^{n_s}$ for some $0 \leq b_0, b_1, \ldots, b_{n_s} \leq p-1$. From this, one can conclude that $(x, -\nu((n-x)!))$ lies above the line connecting $(x_{s-1}, -\nu\left((n-x_{s-1})!\right))$ to $(x_s, -\nu\left((n-x_s)!\right))$. □

Corollary 3.20. *Let $n \geq 1$ and suppose $m = p^r$ for some prime p and $r \geq 1$. Then:*

1. *If n is divisible by p then the degree of any irreducible factor of f_n is divisible by $p^{\nu(n)}$.*

2. *If $n = p^l$ for some $l > 0$ then f_n is irreducible. Thus f_n has no roots in common with f_{n-1} and it has no roots in common with f_{n+1}*

3. *If $n = p^l q^k$ where $l, k > 0$ and q is a prime satisfying $p^{r+l} < q$ then f_n is irreducible. Thus f_n has no roots in common with f_{n-1} and it has no roots in common with*

Proof. 1. In Proposition 3.19 we computed the slopes of the Newton polygon of f_n. The denominator of each slope (in lowest terms) is equal to p^s where $s \geq \nu_p(n)$. If $g(x)$ is an irreducible factor of f_n then $p^{\nu_p(n)} \mid \deg(g(x))$ by 2.21

2. If $n = p^r$ then $N_p\left(f_n(x)\right)$ consists of a single edge by Proposition 3.19. The slope of this edge is equal to $\frac{p^r-1}{p^r(p-1)} = \frac{1+p+\cdots+p^{r-1}}{p^r}$. So p^r divides the denominator of the slope in lowest terms, and therefore f_n is irreducible by Corollary 2.22. The second statement follows from the fact that f_n is irreducible and from the fact that $f_n \nmid f_{n+1}$.

3. Let $g(x)$ be an irreducible factor of $f_n(x)$. Then $p^r \mid \deg\left(g(x)\right)$ by (1). Furthermore, n satisfies the hypothesis of 3.17 and therefore $q^l \mid \deg\left(g(x)\right)$. We conclude that

$n \mid \deg(g(x))$ and so f_n is irreducible. The second statement follows easily.

□

The main result of the section is the following.

Theorem 3.21. *Let $F(T) = \lambda_1 + \lambda_2 T^2$. Then F satisfies the **SFC**.*

Proof. We may once again assume $\lambda_1 = 1$. Let $f_n(x)$ be the polynomials given in (3.15) where $m = 2$ and let $g_n(x) = f_n(x/2)$. In order to prove our claim we must show that $g_n(x)$ and $g_{n-1}(x)$ have no common roots for each $n \geq 1$. Following the usual convention (cf. [26] or [5]) we define for each non-negative integer k the **double factorial** $(2k-1)!!$ by setting

$$(2k-1)!! = \begin{cases} 1 & k = 0 \\ \prod_{j=1}^{k}(2j-1) & k \geq 1 \end{cases} \tag{3.17}$$

We also set $b_{n,k} = n!/(n-k)!$ for $0 \leq k \leq n$. We then have

$$g_n(x) = \sum_{k=0}^{n} (2k-1)!! b_{n,k} x^k \tag{3.18}$$

for each $n \geq 1$. Note that g_2 and g_3 are irreducible by Corollary 3.20. So we assume $n \geq 5$. We will prove the following claim:

Claim 1. For each $1 \leq j < n/2$ there exists a rational polynomial

$$r_j(x) = A_j(x) + 2^{2j} b_{n,2j+1} x^j g_{n-(2j+1)}(x)$$

belonging to (g_n, g_{n-1}) such that the following holds:

1. $\deg(A_j) = j - 1$

2. The 2-adic values of the coefficient of x^k in $A_j(x)$ are positive if $0 \leq k \leq j-2$. The 2-adic value of the coefficient of x^{j-1} is equal to 0. In particular, $A_j(x) \neq 0$.

Asuming Claim 1 holds, let us prove the theorem. Suppose n is even and set $j = (n/2)-1$. Then $2j = n-2$, $2j+1 = n-1$ and $n-(2j+1) = 1$ which yields

$$\begin{aligned} r_j(x) &= A_j(x) + 2^{n-2} b_{n,n-1} x^j g_1(x) \\ &= A_j(x) + 2^{n-2} n! x^j (1+x) \\ &= A_j(x) + 2^{n-2} n! \left(x^j + x^{j+1}\right) \end{aligned} \tag{3.19}$$

where g_1 was calculated using Equation (3.18). In order to show that g_n and g_{n-1} have no common roots it suffices to show that $r_j(x)$ has no roots in common with g_n since $r_j \in (g_n, g_{n-1})$. The fact that the 2-adic value of $r_j(0)$ is positive includes the possibility that $\nu_2(r_j(0)) = \infty$, i.e. $r_j(0) = 0$. So let us first assume $r_j(0) \neq 0$. From the claim, we know that the coefficient of x^k in $A_j(x)$ has positive 2-adic value if $0 \leq k \leq j-2$ while the 2-adic valuation of the coefficient of x^{j-1} is precisely zero. Since the 2-adic value of $2^{n-2}n!$ is clearly positive it follows that $(j-1, 0)$ is a vertex of $N_{\nu_2}(r_j)$. Moreover, any edge to the left of the vertical line $x = j-1$ has negative slope. Using Equation (3.19) we see that the only edge of the Newton Polygon of r_j having positive slope connects the point $(j-1, 0)$ to $(j+1, n-2+\nu_2(n!)$, and it has slope equal to $(n-2+\nu_2(n!))/2 > 1$ (since $n \geq 5$). On the other hand the slopes of $N_{\nu_2}(g_n(x))$ belong to the half open interval $[0,1)$ by Proposition 3.19. Therefore $g_n(x)$ and $r_j(x)$ have no common zeroes by Corollary 2.19.

Now assume that $r_j(0) = 0$. Choose $1 \leq j \leq j-2$ such that $x^k \mid r_j(x)$ but $x^{k+1} \nmid r_j(x)$. Since $g_n(0) \neq 0$ we need only show that $g_n(x)$ and $s_j(x) = r_j(x)/x^k$ have no common roots. The argument used above also works for $s_j(x)$. This time, any edge of $N_{\nu_2}(s_j(x))$ to left of the vertical line $x = j-1-k$ has non positive slope, while the only edge of postive slope connecting $(j-1-k, 0)$ to $(j+1-k, n-2+\nu_2(n!))$ has slope greater than one. Therefore $g_n(x)$ and $s_j(x)$ have no common zeroes by Corollary 2.19

Now suppose n is odd, and set $j = (n-1)/2$. A similar calculation to the one done above shows that

$$r_j(x) = A_j(x) + 2^{n-1}n!x^j$$

Once again, in order to prove the theorem, it suffices to show that r_j and g_n have no roots in common. Assume $A_j(0 \neq 0$. Condition (2) from the claim shows that $N_{\nu_2}(r_j(x))$ has only one edge of positive slope. This edge, which connects $(j-1, 0)$ to $(j, n-1+\nu_2(n!)$, has slope greater than 1. So once again the Newton polygon of g_n does not have any edges with slopes in common with that of $r_j(x)$ and therefore the two polynomials have no common zeroes by Corollary 2.19. If $A_j(0) = 0$ we consider $s_j(x) = r_j(x)/x^k$ where $1 \leq k \leq j-2$ is chosen so that $x^k \mid r_j(x)$ but $x^{k+1} \nmid r_j(x)$. The same argument shows that $N_{\nu_2}(s_j(x))$ has only one edge of positive slope, and that this slope is greater than one. Therefore $g_n(x)$ and $s_j(x)$ have no common zeroes.

Let us now prove the claim using induction on j. For the base case we will construct $r_1(x)$ and $r_2(x)$. Then in the inductive step, we will show how $r_{j+1}(x)$ can be obtained from $r_j(x)$ and $r_{j-1}(x)$ assuming those polynomials exist.

We first consider the case $j = 1$. The leading coefficient of $g_n(x)$ is $(2n-1)!!n!$ while the leading coefficient of $g_{n-1}(x)$ is equal to $(2n-3)!!(n-1)!$. We therefore set $\tilde{r}_1(x) = f_n(x) - (2n-1)nxf_{n-1}(x)$. First of all, observe that

$$\begin{aligned}(2n-1)nxf_{n-1}(x) &= \sum_{k=0}^{n-1}(2k-1)!!(2n-1)n\frac{(n-1)!}{(n-1-k)!}x^{k+1}\\ &= \sum_{k=1}^{n}(2k-3)!!(2n-1)n\frac{(n-1)!}{(n-k)!}x^{k}\\ &= \sum_{k=1}^{n}(2k-3)!!(2n-1)b_{n,k}x^{k}\end{aligned}$$

Now calculating $\tilde{r}_1(x)$ we have:

$$\begin{aligned}
\tilde{r}_1(x) &= 1 + \sum_{k=1}^{n} \left((2k-1)!! - (2n-1)(2n-3)!!\right) b_{n,k}x^k \\
&= 1 + \sum_{k=1}^{n} (2k-3)!!((2k-1) - (2n-1))b_{n,k}x^k \\
&= 1 + 2\sum_{k=1}^{n-1} (2k-3)!!(k-n)b_{n,k}x^k \\
&= 1 - 2n\sum_{k=1}^{n-1} (2k-3)!!b_{n-1,k}x^k
\end{aligned}$$

Note that the leading coefficient of $\tilde{r}_1(x)$ is equal to $-2n!(2n-5)!!$. Next, we reduce the degree of $\tilde{r}_1(x)$ by computing $(2n-3)\tilde{r}_1(x) + 2ng_{n-1}(x)$:

$$\begin{aligned}
(2n-3)\tilde{r}_1(x) + 2ng_{n-1}(x) &= (2n-3) + 2n + 2n\sum_{k=1}^{n-2} \left[(2k-1)! - (2n-3)(2k-3)!\right] b_{n-1,k}x^k \\
&= 4n - 3 + 2n\sum_{k=1}^{n-2} (2k-3)!! \left[(2k-1) - (2n-3)\right] b_{n-1,k}x^k \\
&= (4n-3) - 4n(n-1)\sum_{k=1}^{n-2} (2k-3)!!b_{n-2,k}x^k \\
&= (4n-3) - 4b_{n,2}\sum_{k=1}^{n-2} (2k-3)!!b_{n-2,k}x^k
\end{aligned}$$

We set $A_1 = 3 - 4n$ and $r_1(x) = -((2n-3)\tilde{r}_1(x) + 2ng_{n-1}(x)) \in (g_n, g_{n-1})$. Note that A_1 is an odd integer, and therefore has 2-adic value equal to zero. If we factor out an x from the sum and reindex we find that

$$\begin{aligned} r_1(x) &= A_1 + 4b_{n,2}x\sum_{k=1}^{n-2}(2(k-1)-1)!!\frac{(n-2)!}{(n-3-(k+1))!}x^{k-1} \\ &= A_1 + 4b_{n,3}x\sum_{k=0}^{n-3}(2k-1)!b_{n-3,k}x^k \\ &= A_1 + 4b_{n,3}g_{n-3}(x) \end{aligned}$$

Next, we use $r_1(x)$ and $g_{n-1}(x)$ to construct $r_2(x)$. We first observe that the leading coefficient of $r_2(x)$ is equal to $4n(2n-7)!!$. Therefore we set

$$\tilde{r}_2(x) = 4ng_{n-1}(x) - (2n-3)(2n-5)xr_1(x)$$

Note that $\tilde{r}_2(x) \equiv -A_1x \mod 2 \equiv x \mod 2$. It follows that

$$\tilde{r}_2(x) = \tilde{A}_2(x) + 4n\sum_{k=2}^{n-2}\left[(2k-1)!! - (2n-3)(2n-5)(2k-5)!!\right]b_{n-1,k}x^k \tag{3.20}$$

where $\tilde{A}_2(x) \in \mathbb{Z}[x]$ and $\tilde{A}_2(x) \equiv x \mod 2$. The difference inside the brackets appearing in Equation (3.20) can be simplified as $(2n-5)!!\left[(2k-1)(2k-3) - (2n-3)(2n-5)\right]$ and simplifying further we find that

$$\begin{aligned} (2k-1)(2k-3) - (2n-3)(2n-5) &= (2k-1)\left[(2k-3) - (2n-5)\right] \\ &\quad + (2n-5)\big[(2k-1)_{(}2k-3)\big] \\ &= (2k-2n+2)\left[2k+2n-6\right] \\ &= -4(n-1-k)(k+n-3) \end{aligned}$$

Since $(n-1-k)b_{n-1,k} = (n-1)b_{n-2,k}$ it follows that

$$\tilde{r}_2(x) = \tilde{A}_2(x) - 16b_{n,2}\sum_{k=2}^{n-2}(2k-5)!!(k+n-3)b_{n-2,k}x^k$$

Next we calculate $\tilde{\tilde{r}}_2(x) = (2n-7)\tilde{r}_2(x) + 4(2n-5)r_1(x)$. Observe that the sum is congruent modulo 2 to x. Setting $C(k) = k+n-3$ we have

$$\begin{aligned}\tilde{\tilde{r}}_2(x) &= \tilde{\tilde{A}}_2(x) + 16b_{n,2}\sum_{k=2}^{n-3}\left[(2k-3)!!(2n-5) - (2n-7)(2k-5)!!C(k)\right]b_{n-2,k}x^k \\ &= \tilde{\tilde{A}}_2(x) + 16b_{n,2}\sum_{k=2}^{n-3}(2k-5)!!\left[(2k-3)(2n-5) - (2n-7)C(k)\right]b_{n-2,k}x^k\end{aligned}$$

where $\tilde{\tilde{A}}_2(x)$ is a linear integer polynomial and $\tilde{\tilde{A}}_2(x) \equiv x \mod 2$. Now setting $D(k) = (2k-3)(2n-5) - (2n-7)C(k)$ we calculate $D(k)$:

$$\begin{aligned}D(k) &= (2n-5)\left[(2k-3) - (2n-7)\right] + (2n-7)\left[(2n-5) - C(k)\right] \\ &= (2n-5)(2k-2n+4) + (2n-7)(n-2-k) \\ &= -(n-2-k)(2n-3)\end{aligned}$$

Since $(n-2-k)b_{n-2,k} = (n-2)b_{n-3,k}$ it follows that

$$(2n-7)\tilde{r}_2(x) + 4(2n-5)r_1(x) = \tilde{\tilde{A}}_2(x) - 16b_{n,3}(2n-3)\sum_{k=2}^{n-2}(2k-5)!!b_{n-3,k}x^k$$

Set $A_2(x) = -\tilde{\tilde{A}}_2(x)/(2n-3)$ and $r_2(x) = A_2(x) + 16b_{n,3}\sum_{k=2}^{n-3}(2k-5)!!b_{n-3,k}x^k$. It follows from above that $r_2(x) \in (g_n, g_{n-1})$ and that $A_2(x)$ is a rational linear polynomial satisfying condition (2) of the claim above. Moreover, dividing out x^2 from the sum and reindexing gives $r_2(x) = A_2(x) + 16b_{n,5}g_{n-5}(x)$.

Now assume that $r_j(x)$ and $r_{j-1}(x)$ have been constructed for some $2 \leq j < \frac{n}{2} - 1$. We have

$$r_{j-1}(x) = A_{j-1}(x) + 4^{j-1} b_{n,j} \sum_{k=j-1}^{n-j} (2k-(2j-1))!! b_{n-j,k} x^k$$
$$r_j(x) = A_j(x) + 4^j b_{n,j+1} \sum_{k=j}^{n-j-1} (2k-(2j+1))!! b_{n-(j+1),k} x^k$$

Observe that the leading coefficient of $r_{j-1}(x)$ is equal to $4^{j-1} n!(2n-4j+1)!!$ and that the leading coefficient of $r_j(x)$ is equal to $4^j n!(2n-4j-3)!!$. We set $B = (2n-4j+1)(2n-4j-1)$ and define $\tilde{r}_{j+1}(x) = 4r_{j-1}(x) - Bxr_j(x)$. If we let

$$\tilde{A}_{j+1}(x) = 4A_{j-1}(x) + 4^j b_{n,j} \left[b_{n-j,j-1} x^{j-1} + b_{n-j,j} x^j \right] + BxA_j(x)$$

then

$$\tilde{r}_{j+1} = \tilde{A}_{j+1}(x) + 4^j b_{n,j} \sum_{k=j+1}^{n-j-1} \left[(2k-(2j-1))!! - B(2k-(2j+3))!! \right] b_{n-j,k} x^k$$

Since B is odd and since the 2-adic valuation of the leading coefficient of $A_j(x)$ is zero it follows that $\tilde{A}_{j+1}(x)$ has degree j and that the 2-adic valuation of its leading coefficient is zero. Moreover, the other coefficients of $\tilde{A}_{j+1}(x)$ are sums of rational numbers having positive 2-adic valuation, and therefore also have positive 2-adic valuation. Now set $C = (2k-2j+1)(2k-2j-1)$ and observe that

$$\begin{aligned} C - B &= (2k-2j+1)\left[(2k-2j-1) - (2n-4j-1)\right] \\ &\quad + (2n-4j-1)\left[2k-2j+1-(2n-4j+1)\right] \\ &= 2(k-(n-j))\left[(2k-2j+1)+(2n-4j-1)\right] \\ &= -2(n-j-k)(2k+2n-6j) \\ &= -4(n-j-k)(k+n-3j) \end{aligned}$$

If we set $D(k) = k + n - 3j$ then it follows from above that

$$\begin{aligned}\tilde{r}_{j+1} &= \tilde{A}_{j+1} + 4^j b_{n,j} \sum_{k=j+1}^{n-j-1} (2k-2j-3)!!(C-B) b_{n-j,k} x^k \\ &= \tilde{A}_{j+1} - 4^{j+1} b_{n,j+1} \sum_{k=j+1}^{n-j-1} (2k-2j-3)!!D(k) b_{n-(j+1),k} x^k\end{aligned}$$

Next, we set $\tilde{\tilde{r}}_{j+1}(x) = (2n-4j-3)\tilde{r}_{j+1}(x) + 4D(n-j-1)r_j(x)$. If we set $\tilde{\tilde{A}}_{j+1}(x) = (2n-4j-3)\tilde{A}_{j+1}(x) + 4D(n-j-1)(A_j(x) + 4^j b_{n,j+1} \cdot b_{n-j-1,j} x^j$ then

$$\tilde{\tilde{r}}_{j+1} = \tilde{\tilde{A}}_{j+1}(x) + 4^{j+1} b_{n,j+1} \sum_{k=j+1}^{n-j-2} (2k-2j-3)!!E(k) b_{n-j-1,k} x^k$$

where $E(k) = (2k-2j-1)D(n-j-1) - (2n-4j-3)D(k)$. Observer that since $(2n-4j-3)$ is odd and since every coefficient of $4D(n-j-1)(A_j(x) + 4^j b_{n,j+1} \cdot b_{n-j-1,j} x^j$ has positive 2-adic valuation the leading coefficient of $\tilde{\tilde{A}}_{j+1}(x)$ has 2 adic valuation equal to zero while the other coefficients have positive 2-adic valuation. Let us now simplify $E(k)$:

$$\begin{aligned}E(k) &= D(n-j-1)\left[(2k-2j-1) - (2n-4j-3)\right] + (2n-4j-3)\left[D(n-j-1) - D(k)\right] \\ &= 2(k-(n-(j+1))D(n-j-1) + (2n-4j-3)\left[(2n-4j-1) - (k+n-3j)\right] \\ &= 2(k-(n-(j+1))D(n-j-1) + (2n-4j-3)(n-(j+1)-k) \\ &= (k-(n-(j+1))[2(2n-4j-1) - (2n-4j-3)] \\ &= -(n-(j+1)-k)(2n-4j+1)\end{aligned}$$

It now follows that

$$\tilde{\tilde{r}}_{j+1} = \tilde{\tilde{A}}_{j+1}(x) - 4^{j+1}(2n-4j+1) b_{n,j+2} \sum_{k=j+1}^{n-j-2} (2k-2j-3)!! b_{n-(j+2),k} x^k$$

Finally, we set $A_{j+1}(x) = -\tilde{\tilde{A}}_{j+1}(x)/(2n-4j+1)$ and $r_{j+1}(x) = -\tilde{\tilde{r}}_{j+1}/(2n-4j+1)$. It follows from above that

$$\begin{aligned} r_{j+1}(x) &= A_{j+1}(x) + 4^{j+1} b_{n,j+2} \sum_{k=j+1}^{n-j-2} (2k-2j-3)!! b_{n-(j+2),k} x^k \\ &= A_{j+1}(x) + 4^{j+1} b_{n,2j+3} x^{j+1} \sum_{k=0}^{n-(2j+3} (2k-1)!! b_{n-(2j+3),k} x^k \\ &= A_{j+1}(x) + 4^{j+1} b_{n,2j+3} x^{j+1} g_{n-(2j+3)}(x) \end{aligned}$$

Since $2n-4j+1$ is an odd integer the 2-adic valuations of the coefficients of $\tilde{\tilde{A}}_{j+1}(x)$ are unaffected when passing to $A_{j+1}(x)$ and therefore $A_{j+1}(x)$ satisfies the conditions of the claim made at the beginning of the proof.

□

3.4 New Examples from Old

In this final example we detail one way of constructing new examples of polynomials satisfying the **SFC** from existing examples. For this, we will make use of the fact that $\mathcal{L}(FG) = \mathcal{L}(F)\mathcal{L}(G)$ whenever $F, G \in \mathbb{C}^{[m]}$ are two polynomials such that there exists an $I \subset \{1, \ldots, m\}$ such that $F \in \mathbb{C}[T_i : i \in I]$ and $G \in \mathbb{C}[T_i : i \notin I]$. Let $U_1, \ldots, U_l$ be indeterminates that commute with $T_1, \ldots, T_m$. We have the following theorem.

Theorem 3.22. *Set $U = U_1$. Suppose $F \in \mathbb{C}^{[m]} := \mathbb{C}[T_1, \ldots, T_m]$ satisfies the* ***SFC****. Then $G = \lambda U + F$ also satisfies the* ***SFC****.*

Proof. Let $N = \mathcal{N}(F)$. Then $\mathcal{N}(G) = N + 1$. If we set $f_n = \mathcal{L}(F^j)/n!$ and $g_n = \mathcal{L}(G^n)/n!$,

$n \geq 1$, then

$$\begin{aligned} g_n &= \mathcal{L}\left(\frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}F^{n-k}U^k\lambda^k\right) \\ &= \sum_{k=0}^{n}\frac{1}{(n-k)!k!}\mathcal{L}\left(F^{n-k}U^k\right)\lambda^k \\ &= \sum_{k=0}^{n}\frac{1}{(n-k)!k!}\mathcal{L}\left(F^{n-k}\right)\mathcal{L}\left(U^k\right)\lambda^k \\ &= \sum_{k=0}^{n} f_{n-k}\lambda^k \end{aligned}$$

It easily follows from above that

$$g_n = f_n + \lambda g_{n-1} \tag{3.21}$$

for each $n \geq 1$. Now suppose that $\mathcal{L}\left(G^{n+i}\right) = 0$ for some $n \geq 1$ and $0 \leq i \leq n+N$. Then $g_{n+i} = 0$ for $0 \leq i \leq N$. It then follows from Equation (3.21) that $f_{n+i} = 0$ for $1 \leq i \leq N$, and therefore $\mathcal{L}\left(F^j\right) = 0$ for $n+1 \leq j \leq n+N$. Since F satisfies the **SFC** we must have $F = 0$. So $G = \lambda U$ and since $\mathcal{L}\left(G^n\right) = 0$ we must have $\lambda = 0$. □

Corollary 3.23. *Suppose $L \in \mathbb{C}^{[l]} := \mathbb{C}\left[U_1, \ldots, U_l\right]$ is a linear form and $F \in \mathbb{C}^{[m]}$ satisfies the **SFC**. Then $G = L + F$ satisfies the **SFC**.*

Proof. By induction on l and the previous Theorem. □

Bibliography

[1] `http://www.risc.jku.at/research/combinat/risc/software/`.

[2] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1990.

[3] Hyman Bass, Edwin H. Connell, and David Wright. The Jacobian conjecture: reduction of degree and formal expansion of the inverse. *Bull. Amer. Math. Soc. (N.S.)*, 7(2):287–330, 1982.

[4] Egbert Brieskorn, Horst Knörrer, and John Stillwell. *Plane Algebraic Curves: Translated by John Stillwell*. Springer Science & Business Media, 2012.

[5] David Callan. A combinatorial survey of identities for the double factorial. *arXiv preprint arXiv:0906.1317*, 2009.

[6] Eduardo Casas-Alvero. *Singularities of plane curves*, volume 276 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000.

[7] Aldo Conca, Christian Krattenthaler, and Junzo Watanabe. Regular sequences of symmetric polynomials. *arXiv preprint arXiv:0801.2662*, 2008.

[8] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra.

[9] Michiel de Bondt and Arno van den Essen. A reduction of the Jacobian conjecture to the symmetric case. *Proc. Amer. Math. Soc.*, 133(8):2201–2205 (electronic), 2005.

[10] Gustave Dumas. Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, pages 191–258, 1906.

[11] Eric Edo. Some families of polynomial automorphisms. II. *Acta Math. Vietnam.*, 32(2-3):155–168, 2007.

[12] Eric Edo and Jean-Philippe Furter. Some families of polynomial automorphisms. *J. Pure Appl. Algebra*, 194(3):263–271, 2004.

[13] Eric Edo and Arno van den Essen. The strong factorial conjecture. *J. Algebra*, 397:443–456, 2014.

[14] M. Filaseta and T.-Y. Lam. On the irreducibility of the generalized Laguerre polynomials. *Acta Arith.*, 105(2):177–182, 2002.

[15] Michael Filaseta. A generalization of an irreducibility theorem of I. Schur. In *Analytic number theory, Vol. 1 (Allerton Park, IL, 1995)*, volume 138 of *Progr. Math.*, pages 371–396. Birkhäuser Boston, Boston, MA, 1996.

[16] Shmuel Friedland and John Milnor. Dynamical properties of plane polynomial automorphisms. *Ergodic Theory Dynam. Systems*, 9(1):67–99, 1989.

[17] Jean-Philippe Furter. On the variety of automorphisms of the affine plane. *J. Algebra*, 195(2):604–623, 1997.

[18] Jean-Philippe Furter. On the length of polynomial automorphisms of the affine plane. *Math. Ann.*, 322(2):401–411, 2002.

[19] Jean-Philippe Furter. Plane polynomial automorphisms of fixed multidegree. *Math. Ann.*, 343(4):901–920, 2009.

[20] Jean-Philippe Furter. Polynomial composition rigidity and plane polynomial automorphisms, 2013. Preprint avaialable at http://perso.univ-lr.fr/jpfurter.

[21] Izrail M Gelfand, Mikhail Kapranov, and Andrei Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Springer Science & Business Media, 2008.

[22] Kurt Hensel. Neue grundlagen der arithmetik. *Journal für die reine und angewandte Mathematik*, 127:51–84, 1904.

[23] A. V. Jagžev. On a problem of O.-H. Keller. *Sibirsk. Mat. Zh.*, 21(5):141–150, 191, 1980.

[24] Olivier Mathieu. Some conjectures about invariant theory and their applications. In *Algèbre non commutative, groupes quantiques et invariants (Reims, 1995)*, volume 2 of *Sémin. Congr.*, pages 263–279. Soc. Math. France, Paris, 1997.

[25] Guowu Meng. Legendre transform, Hessian conjecture and tree formula. *Appl. Math. Lett.*, 19(6):503–510, 2006.

[26] B. E. Meserve. Classroom Notes: Double Factorials. *Amer. Math. Monthly*, 55(7):425–426, 1948.

[27] Joe L. Mott. Eisenstein-type irreducibility criteria. In *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, volume 171 of *Lecture Notes in Pure and Appl. Math.*, pages 307–329. Dekker, New York, 1995.

[28] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[29] Marko Petkovšek, Herbert S Wilf, and Doron Zeilberger. *A= B, AK Peters Ltd*, volume 30. 1996.

[30] Victor Puiseux. *Recherches sur les fonctions algébriques.* 1850.

[31] I. R. Shafarevich. Letter to the editors: "On some infinite-dimensional groups. II" [Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 1, 214–226, 240; MR0607583 (84a:14021)]. *Izv. Ross. Akad. Nauk Ser. Mat.*, 59(3):224, 1995.

[32] Arno van den Essen. *Polynomial automorphisms and the Jacobian conjecture*, volume 190 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000.

[33] Arno van den Essen, David Wright, and Wenhua Zhao. On the image conjecture. *J. Algebra*, 340:211–224, 2011.

[34] Arno van den Essen and Wenhua Zhao. Mathieu subspaces of univariate polynomial algebras. *J. Pure Appl. Algebra*, 217(7):1316–1324, 2013.

[35] Wenhua Zhao. Hessian nilpotent polynomials and the Jacobian conjecture. *Trans. Amer. Math. Soc.*, 359(1):249–274 (electronic), 2007.

[36] Wenhua Zhao. Images of commuting differential operators of order one with constant leading coefficients. *J. Algebra*, 324(2):231–247, 2010.