On the Incompatability of Diophantine Equations Arising from the Strong Factorial Conjecture

Brady Rocks[a,1,*]

[a]*Department of Mathematics, Washington University in St. Louis, St. Louis, MO 63130, United States*

Abstract

In the present article, we establish new evidence in support of the Strong Factorial Conjecture of Edo and van den Essen [5] by proving it in several special cases. In particular, we establish in Theorem 3.3 that powers of linear forms satisfy the conjecture and in Theorem 3.10 we also establish that sums of prime powers of variables also satisfy the conjecture. In addition, Theorem 3.12 is a novel result which shows how to build new examples of polynomials satisfying the conjecture from known examples. Finally, we we use the theory of resultants and Newton polygons to study the case where F is the sum of two monomials and prove the conjecture in some special cases and provide many partial results for others.

Keywords: Polynomial automorphisms, Jacobian Conjecture, Factorial Conjecture, Rigidity Conjecture, Newton Polygons, Irreducible Polynomials

1. Introduction

A problem of growing interest related to the famous Jacobian Conjecture (see [12] for a detailed account of this problem) is the Factorial Conjecture introduced in [13]. If true, the result would provide substantial evidence in support of Zhao's Image Conjecture [14, Conjecture 1.3] which is known to imply the Jacobian Conjecture [14, Theorem 3.7].

Recently, in [5], Edo and van den Essen discovered a connection between the Factorial Conjecture [13] and the Rigidity Conjecture of Furter [6] which is known to imply the Length 2 Polydegree Conjecture [6, Theorem 3]. As a result, Edo and Essen formulated the Strong Factorial Conjecture [5].

It is precisely because of its links to some of the most outstanding problems in the field of Affine Algebraic Geometry (those mentioned above) that the Strong Factorial Conjecture merits an investigation.

In Section 3 we prove that the Strong Factorial Conjecture holds in several special cases. In particular, we establish the conjecture for powers of linear forms and sums of prime powers of variables. In addition, we provide a novel result which shows how to build new examples of polynomials satisfying the conjecture from old. Finally, using the theory of resultants and Newton Polygons we study the conjecture for polynomials that are the sum of two

*Corresponding author.

Email address: rocks@maiboxl.sc.edu (Brady Rocks)

[1]Present Address: Department of Mathematics, University of South Carolina, Columbia, SC 29208

monomials by first showing how the problem can be tackled by studying the solution sets of certain systems of diophantine equations.

1.1. Notation

The following notation and conventions will be in effect throughout the rest of the article:

1. Given a positive integer m we denote by $\mathbb{C}^{[m]} = \mathbb{C}[Z_1, \ldots, Z_m]$ the $\mathbb{C}$-algebra of complex polynomials in m variables. Unless otherwise specified, Z denotes the vector $(Z_1, \ldots, Z_m)$.
2. Given $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$ we set $|\alpha| = \sum_{i=1}^m \alpha_i$. We also denote by Z^α and $\alpha!$ the products $\prod_{i=1}^m Z_i^{\alpha_i}$ and $\prod_{i=1}^m \alpha_i!$, respectively.
3. Given $\alpha \in \mathbb{N}^m$ we denote by $\binom{|\alpha|}{\alpha}$ the multinomial coefficient. That is, $\binom{|\alpha|}{\alpha} = \dfrac{|\alpha|!}{\alpha!}$.
4. For any m-tuple $H = (H_1, \ldots, H_m)$ of polynomials $H_i \in \mathbb{C}^{[m]}$ and any $\alpha \in \mathbb{N}^m$ we write H^α to denote the product $\prod_{i=1}^m H_i^{\alpha_i}$.
5. If $G = (G_1, \ldots, G_m)$ is another m-tuple of elements of $\mathbb{C}^{[m]}$ then we write $H * G$ to denote the m-tuple obtained by componentwise multiplication, i.e., $H*G = (H_1G_1, \ldots, H_mG_m)$.
6. Given $F \in \mathbb{C}^{[m]}$ we denote by $\mathcal{N}(F)$ the number of monomials that appear in F with a nonzero coefficient.
7. Given a field K and a subset $S \subset\in K^{[m]}$ we set $\mathcal{Z}(S) = \{\lambda \in K^m : F(\lambda) = 0 \text{ for all } F \in S\}$.

1.2. The Strong Factorial Conjecture

Let us recall the definition of the *factorial map* (see [13, Definition 1.2]):

Definition 1.1. We denote by $\mathcal{L}$ the $\mathbb{C}$-linear functional on $\mathbb{C}^{[m]}$ defined by $\mathcal{L}(Z^\alpha) = \alpha!$.

Remark 1.2. If we let D_m denote the non-negative m-tant $Z_1 \geq 0, \ldots, Z_m \geq 0$ in $\mathbb{R}^m$ then for $F \in \mathbb{C}^{[m]}$ $\mathcal{L}(F)$ can be realized as

$$\mathcal{L}(F) = \int_{D_m} F e^{-|Z|}\, dZ$$

where $dZ = dZ_1 \cdots dZ_m$ and $|Z| = Z_1 + \cdots + Z_m$.

Remark 1.3. Let $\langle \cdot, \cdot \rangle$ denote the Hermitian inner product defined on $\mathbb{C}^{[m]}$ by

$$\langle F, G \rangle = \int_{D_m} F(Z)\overline{G(Z)} e^{-|Z|} dZ$$

We note that this restricts to a positive definite form on $\mathbb{R}^{[m]}$. In particular, we have $\mathcal{L}(F^{2n}) = \langle F^n, F^n \rangle$ for all $n \geq 1$ and for all $F \in \mathbb{R}^{[m]}$. Moreover, $\mathcal{L}(F^{2n}) > 0$ for all $n \geq 1$ if $F \in \mathbb{R}^{[m]} \setminus \{0\}$.

Remark 1.4. The map $\mathcal{L}$ is not compatible with multiplication. However, if $F, G \in \mathbb{C}^{[m]}$ are two polynomials such that there exists an $I \subset \{1, \ldots, m\}$ such that $F \in \mathbb{C}[Z_i : i \in I]$ and $G \in \mathbb{C}[Z_i : i \notin I]$ then $\mathcal{L}(FG) = \mathcal{L}(F)\mathcal{L}(G)$.

We also recall the Factorial Conjecture [13, Conjecture 4.2].

Conjeture 1.5 (Factorial Conjecture)**.** *Let m be a positive integer and $F \in \mathbb{C}^{[m]}$. If $\mathcal{L}(F^n) = 0$ for all $n \geq 1$ then $F = 0$.*

The conjecture remains open in all dimensions greater than one. To give a stronger version of this conjecture, the authors of [5] introduced the following subsets of $\mathbb{C}^{[m]}$:

Definition 1.6. For all positive integers n we set

$$\mathcal{F}_n^m = \left\{F \in \mathbb{C}^{[m]} \setminus \{0\} \mid \exists\, n \leq k \leq n + \mathcal{N}(F) - 1 \text{ with } \mathcal{L}\left(F^k\right) \neq 0\right\} \cup \{0\}.$$

We define the *strong factorial set* as:

$$\mathcal{F}^m = \bigcap_{n \geq 1} \mathcal{F}_n^m.$$

We now recall the Strong Factorial Conjecture:

Conjeture 1.7 (Strong Factorial Conjecture)**.** $\mathcal{F}^m = \mathbb{C}^{[m]}$ *for all positive integers m.*

Remark 1.8. A non-zero $F \in \mathbb{C}^{[m]}$ belongs to the strong factorial set if and only if for each positive integer n there exists $0 \leq i \leq \mathcal{N}(F) - 1$ such that $\mathcal{L}(F^{n+i}) \neq 0$.

The conjecture remains open in all dimensions.

1.3. The Strong Factorial Conjecture and Diophantine Eqautions

In this section we fix an integer $d \geq 2$ and monomials $M_1, \ldots, M_d \in \mathbb{C}^{[m]}$. In order to study Conjecture 1.7 we ask whether there exists a non-zero polynomial of the form $F = \sum_{i=0}^{d} \lambda_i Z_i$ and a positive integer n such that one of $\mathcal{L}(F^{n+i})$, $0 \leq i \leq \mathcal{N}(F) - 1$, is non-zero. If we we think of $\lambda_1, \ldots, \lambda_d$ as variables then for every positive integer n the image $\mathcal{L}(F^n)$ is a homogeneous integer polynomial in the variables $\lambda_1, \ldots, \lambda_d$ of degree n.

Definition 1.9. Given a positive integers $n \geq 1$, monomials $M_1, \ldots, M_d \in \mathbb{C}^{[m]}$ and a non-zero multi-variate complex polynomial of the form $F = F = \sum_{i=0}^{d} \lambda_i Z_i$ we set

$$S_{n,F} = \left\{\mathcal{L}\left(F^{n+i}\right) \mid 0 \leq i \leq n + \mathcal{N}(F) - 1\right\} \subset \mathbb{Z}[\lambda_i \mid \lambda_i \neq 0].$$

It follows from the preceeding remarks that $F \in \mathcal{F}_n^m$ if and only if $\mathcal{Z}(S_{n,F}) = \{\vec{0}\}$. By the Nullstellensatz, $\mathcal{Z}(S_{n,F}) = \{\vec{0}\}$ if and only if $S_{n,F}$ generates a homogoeneous ideal of $\mathbb{Q}[\lambda_i \mid \lambda_i \neq 0]$ whose radical is equal to the maximum homogeneous ideal.

The previous paragraph shows that Conjecture 1.7 can be viewed as an assertion about the incompatibility of certain systems of diophantine equations arising from the factorial map. It is this viewpoint that made it possible to obtain the main results of this article.

2. Preliminaries

In this section we collect some basic facts and tools that will be used in the proofs of our main results. Both the resultant and Newton polygon have been valuable tools for the studying Conjecture 1.7 in the case F is a sum of two monomials.

2.1. Univarite Resultant

Throughout this section R will denote a UFD and $f, g \in k[x]$ will denote polynomials of degree $t > 0$ and $s > 0$, respectively. Write f and g as

$$\begin{aligned} f &= a_s x^r + \cdots + a_0 \\ g &= b_t x^n + \cdots + b_0 \end{aligned} \tag{2.1}$$

For any $l > 0$ let S_l denote the R-module 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 $S_{s-1} \bigoplus S_{t-1} \to S_{s+t-1}$ 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

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

Definition 2.1. Given f and g as in (2.1) the resultant of f and g with respect to x, denoted by $\mathrm{Res}(f, g, x)$, is the determinant of $\mathrm{Syl}(f, g, x)$.

The following facts about the resultant are well known; see, for example, [3, 7].

Proposition 2.2. *Let f, g be as in* (2.1)*. Then:*

(i) $\mathrm{Res}(f, g, x) = 0$ *if and only if f and g have no irreducible factors in common.*

(ii) Denote by k the algebraic closure of the quotient field of R. If $\alpha_1, \ldots, \alpha_s \in k$ and $\beta_1, \ldots, \beta_t \in k$ are the roots of f and g, respectively, then

$$\mathrm{Res}(f, g, x) = a_r^s b_s^r \prod_{i,j} (\alpha_i - \beta_j).$$

(iii) $\mathrm{Res}(f, g, x) = (-1)^{st} \mathrm{Res}(g, f, x)$.

(iv) Suppose $s \geq t$. Write $f = qg + r$ for some polynomials q and r with $\deg(r) = u < t$*. Then* $\mathrm{Res}(f, g, x) = b_t^{s-u} \mathrm{Res}(r, g, x)$.

(v) $\mathrm{Res}\left(x^l, g, x\right) = g(0)^l$ *for all $l \geq 1$.*

(vi) If $h \in R[x]$ then $\mathrm{Res}(fh, g, x) = \mathrm{Res}(f, g, x) \cdot \mathrm{Res}(h, g)$.

(vii) If $\lambda \in R^*$ then $\mathrm{Res}(f(\lambda x), g(\lambda x), x) = \lambda^{st} \mathrm{Res}(f, g, x)$.

2.2. The Newton Polygon

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$. Let p be a prime. For an integer $j \neq 0$, we denote by $\nu_p(j)$ the exponent in the largest power of p dividing j. We define $\nu_p(0) = +\infty$. Let S denote the set of points $(i, \nu_p(a_i))$, for $0 \leq i \leq n$, in the extended plane. The Newton polygon of f with respect to the prime p is the polygonal path along the lower edges of the convex hull of S from $(0, \nu_p(a_0)$, and the right-most edge has $(n, \nu_p(a_0)$. The endpoints of every edge belong to S, and each edge has a distinct slope that increases as we move along the polygonal path from left to right.

The following theorem, due to G. Dumas [4], connects the Newton polygon of $f(x)$ to the Newton polyogns of it's factors.

Theorem 2.3. *Let $g(x), h(x) \in \mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let $k = \nu_p(g(0)h(0)$. Then the edges of the Newton polygon for $f(x) = g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beggining at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing as we move left to right.*

The above theorem yields the following useful corrollaries that we will use later on (the proofs of which can be found in [9]).

Corollary 2.4. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$, and let p be a prime. If the lattice points along the edges of the Newton polygon of $f(x)$ with respect to p are $(a_1, b_1), \ldots, (a_r, b_r)$ and $d_i = a_i - a_{i-1}$ for $1 \leq i \leq r$, then the set $\{1, \ldots, r\}$ can be written as a disjoint union of sets $S_1, \ldots, S_t$ where t is the number of irreducible factors of $f(x)$ (counted with multiplicities) and the t numbers $\sum_{u \in S_i} d_u$, for $1 \leq i \leq t$, are the degrees of the irreducible factors of $f(x)$.*[2]

Corollary 2.5. *Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$, and let p be a prime. If d is a positive integer that divides the denominator of each slope (in lowest terms) of the Newton polygon of f with respect to p then d divides the degree of each irreducible factor of f.*

Corollary 2.6. *Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{l} b_i x^i$ with $a_0 a_n$, $b_0 b_l \neq 0$, and let p be a prime. If the slopes of the Newton polygon of $f(x)$ with respect to p are distinct from the slopes of the Newton polygon of g with respect to p then $f(x)$ and $g(x)$ are relatively prime.*

Remark 2.7. The above theorem and its consequences hold in much more generality. For example, the function n_p can be extended to $\mathbb{Q}$ and therefore $\mathbb{Z}[x]$ can be replaced with $\mathbb{Q}[x]$ in the above results. Moreover, $\mathbb{Z}$ can also be replaced by any UFD.

[2]It is important to consider all lattice points along the edges and not just points of the form $(i, \nu_p(a_i))$.

3. Main Results

In this section we present new evidence in support of the Strong Factorial Conjecture by proving it in several special cases. First, we show that powers of linear forms satisfy the conjecture. As a consequence, we extend this result to all linear polynomials. Secondly, we show that sums of prime powers of the variables (each exponent involves the same prime) also satisfy the conjecture. Thirdly, we prove a novel result which shows one instance of how to uild new examples of poynomials satisfying the conjecture using known examples. Finally, we study the conjecture for polynomials that are the sum of two monomials. Using the theory of resultants and Newton polygons we obtain several partial results and indicate how one might solve these cases completely.

3.1. Powers of Linear Forms

In this section we consider the following general polynomial:

$$G(Z) = \sum_{i=0}^{m} \lambda_i Z_i \tag{3.1}$$

where $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{C}^n$. It was shown in [13] that G^r satisfies the Factorial Conjecture for all positive integers r and m. In the present article, we extend this result by showing that G^r satisfies the Strong Factorial Conjecture for all positive integers r and m.

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** $h_{n,m}(x)$ of degree $n \geq 0$ in m variables is defined by

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

When $n = 0$ it should be understood that $h_{0,m}(x) = 1$.

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

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

When $k = 0$ we set $e_{0,m}(x) = 1$.

The polynomials $h_{n,m}(x)$ and $e_{k,m}(x)$ 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

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

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

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

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

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 $\mathcal{L}(F^{n+i}) = 0$ for each $i \in \{0, 1, \ldots, m-1\}$ then $F = 0$.*

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

$$\begin{aligned} \mathcal{L}(G^n) &= \sum_{|\alpha|=n} \binom{n}{\alpha} \alpha! \lambda^\alpha \\ &= n! \sum_{|\alpha|=n} \lambda^\alpha \\ &= n! h_{n,m}(\lambda) \end{aligned} \tag{3.5}$$

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

Proposition 3.4. *Let $m \geq 2$ be a positive integer and let K be any field. For every $n, r \geq 1$ the set of polynomials*
$\{h_{ir,m} \colon n \leq i \leq n + m - 1\}$ 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 $h_{i,m}$ for $n \leq i \leq n + m - 1$ then $h_{i,m}(\lambda) = 0$ for all $i \geq n$. Thus $P_\lambda(U) \in (K[U])^* = K^*$. Therefore $\lambda_i = 0$ for $1 \leq i \leq m$ which is what we wanted to show.

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

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

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 $QB_j = Q_j \in A[U^r]$ 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 $k \geq 1$:

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

Now suppose λ is a common root of $\{h_{ir,m} \colon n \leq i \leq n+m-1\}$. 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

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

Recall that there is no cancellation amongst the summands of

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

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 $h_{a,m}(x)$ with $a \in A$ has no common nontrivial zeroes was considered by Conca, Krattenthaler, and Watanabe in [2]. Proposition 3.4 is a new example of such a subset A.

The following is an immediate consequence of the preceeding proposition.

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 $P^{-1}(U) = 1 + a_1 U + a_2 U^2 + \cdots$ 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. 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 $P^{-1}(U) = \sum_{i=0}^\infty h_{i,m}(\lambda)U^i$, and therefore $a_i = h_{i,m}(\lambda)$. 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 $\mathcal{L}(F^{n+i}) = 0$ 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 $f_n = \mathcal{L}(F^n)/n!$, $n \geq 1$, and let $\lambda = (\lambda_1,\ldots,\lambda_m)$. Without loss of generality we may assume each $\lambda_i \neq 0$. Using Equation (3.5) we calculate f_n:

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

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 $g = \sum_{k=0}^m (-1)^k e_{k,m}(\lambda) f_{n+m-k}$ and write $g = \sum_{k=0}^{n+m} g_k \lambda_0^k$. Then

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

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

$$G(Z) = \lambda_1 Z_1^{p^{\beta_1}} + \lambda_2 Z_2^{p^{\beta_2}} + \cdots + \lambda_m Z_m^{p^{\beta_m}} \tag{3.8}$$

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:

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

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

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

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

$$g_l(x) = \sum_{|\alpha|=l} \binom{l}{\alpha} \frac{\left(p^\beta \alpha\right)!}{\alpha!} x^\alpha$$

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

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 $0 \leq j \leq m$ (Note that $1/k! \in \mathbb{F}_p$ since $k < n + m < p$). 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. New Examples from Old

In this setion we ask whether there is a way of building up new examples of polynomials satisfying the conjecture from already known ones. We detail detail one such way. Remark 1.4 is used in the proof of the following theorem.

Theorem 3.12. *Set $U = U_1$. Suppose $F \in \mathbb{C}^{[m]}$ satisfies the Strong Factorial Conjecture. Then $G = \lambda U + F$ also satisfies the conjecture.*

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

$$g_n = f_n + \lambda g_{n-1} \tag{3.14}$$

for each $n \geq 1$. Now suppose that $\mathcal{L}(G^{n+i}) = 0$ 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 (3.14) that $f_{n+i} = 0$ for $1 \leq i \leq N$, and therefore $\mathcal{L}(F^j) = 0$ for $n + 1 \leq j \leq n + N$. Since F satisfies the Strong Factorial Conjecture it must be the case that $F = 0$. So $G = \lambda U$ and since $\mathcal{L}(G^n) = 0$ we must have $\lambda = 0$. □

Corollary 3.13. *Suppose $L \in \mathbb{C}^{[l]} := \mathbb{C}[U_1, \ldots, U_l]$ is a linear form and $F \in \mathbb{C}^{[m]}$ satisfies the Strong Factorial Conjecture. Then $G = L + F$ also satisfies the conjecture.*

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

3.4. Sum of Two Monomials

Throughout this section x will denote a single variable, rather than a vector of variables. In this section we study Conjecture 1.7 in the case F is of the form $\lambda_1 M_1 + \lambda_2 M_2$ where $M_1, M_2 \in \mathbb{C}^{[m]}$ are monomials. In order to show that F satisfies the conjecture we must show that one of $\mathcal{L}(F^n)$, $\mathcal{L}(F^n)$ is nonzero for all $n \geq 2$. Since the conjecture obviously holds for monomials, we may assume that $\lambda_1, \lambda_2 \neq 0$. Furthermore, since $\mathcal{L}(F^n)$ 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:

$$f_n(x) = \sum_{k=0}^{n}\binom{n}{k}\mathcal{L}\left(M_1^{n-k}M_2^k\right)x^k. \tag{3.15}$$

Then $f_n(\lambda_2) = \mathcal{L}(F^n)$. From this we see that F satisfies the conjecture if and only if $f_n(x), f_{n-1}(x)$ have no common zeroes (over $\mathbb{C}$) for all $n \geq 2$.

One way to attack the problem is to use Zeilberger's algorithm (see [11]) 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. [10]) 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 $f_n(x) = \sum_{k=0}^{n} \binom{n}{k}(2k)!x^k$. 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 3.14. *For all $n \geq 2$ the polynomials $f_n(x)$ and $f_{n-1}(x)$ have no common zeroes in the following cases:*

1. $F = 1 + \lambda Z_1$
2. $F = Z_1^2 + \lambda Z_1$
3. $F = Z_1^3 + \lambda Z_1^2$
4. $F = Z_1^2 + \lambda Z_1 Z_2$
5. $F = Z_1^3 + \lambda Z_1^2 Z_2$

Proof. We proceed case by case.

1. In this case we have $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^k \lambda^k$ which gives $f_n(x) = \sum_{k=0}^{n} \frac{n!}{(n-k)!}x^k$. 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 $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^{2n-k} \lambda^k$ which gives $f_n(x) = \sum_{k=0}^{n} \binom{n}{k}(2n-k)!x^k$. 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 $F^n = \sum_{k=0}^{n} Z_1^{3n-k} \lambda^k$ which gives $f_n(x) = \sum_{k=0}^{n} \binom{n}{k}(3n-k)!x^k$. 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 **??** 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 $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^{2n-k} Z_2^k \lambda^k$ 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 $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^{3n-k} Z_2^k \lambda^k$ 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 **??**. So f_n and f_{n-1} have no common zeroes.

□

Let us now turn our attention to $F = Z_1^m(\lambda_1 + \lambda_2 Z_1)$ where $\lambda_1, \lambda_2 \in \mathbb{C}^*$. From the above Proposition we know that F satisfies Conjecture 1.7 for $m = 0, 1, 2$. Once again assuming $\lambda_1 = 1$ we have the following partial result for the general case.

Proposition 3.15. *Let $F = Z_1^m(1 + \lambda Z_1)$ 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 $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^{nm+k} \lambda^k$ 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 $f_n(x) = \sum\limits_{k=0}^{n} \binom{n}{k} \frac{(nm+k)!}{(nm)!} x^k$. 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 $R_n(t) = \mathrm{Res}(F_n(t,x), F_{n-1}(t,x), x)$. 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 $R_n(m) = \mathrm{Res}\,(f_n, f_{n-1})$. So using Proposition 2.2 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 $R[t]$. Therefore $F_n(t,x)$ and $F_{n-1}(t,x)$ have no common factor over $\mathbb{Q}(t)$ by Gauss's Lemma. So it follows from Proposition **??** 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 $R_n(0) = \det\left(\mathrm{Syl}\left(F_n(0,x), F_{n-1}(0,x)\right)\right)$. Now $Q_{n,k}(0) = k!$ and so $F_n(0,x) = \sum_{k=0}^{n} \dfrac{n!}{(n-k)!} x^k$. Since $\deg_x F_n(0,x) = n$ for each $n \geq 1$ it follows that $R_n(0) = \mathrm{Res}\,(F_n(0,x), F_{n-1}(0,x))$ 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 2.2 that

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

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

The above method can also be applied to other polynomials to obtain similar results.

Proposition 3.16. *Let $F = Z_1^m\,(Z_2 + \lambda Z_1 Z_3)$ where $m > 0$. If $m \nmid (n!)^{n-1}$ then $\mathcal{L}\,(F^n) \neq 0$ or $\mathcal{L}\,(F^{n-1}) \neq 0$.*

Proof. Suppose $n > 0$. We have $F^n = \sum_{k=0}^{n} \binom{n}{k} Z_1^{nm+k} Z_2^{n-k} T_3^k \lambda^k$ which gives

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

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 3.15. Note $f_n(\lambda) = 0$ if and only if $\mathcal{L}\,(F^n) = 0$. Also $F_n(m,x) = f_n(x)/(nm)!$. Now, like in the proof of the previous proposition, set $R_n(t) = \mathrm{Res}\,(F_n, F_{n-1}, x)$. Then $R_n(0) = \mathrm{Res}\,(g_n(x), g_{n-1}(x), x)$ where $g_n(x) = \sum_{k=0}^{n} k!x^k$. Since $g_n = g_{n-1} + n!x^n$ it follows from Proposition 2.2 *(iii)* that

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

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 3.17. *Let $F = (Z_1 Z_2)^m\,(Z_1 + \lambda Z_2)$ 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

$$F^s = \sum_{k=0}^{s} \binom{s}{k} Z_1^{sm+s-k} Z_2^{sm+k} \lambda^k$$

and therefore

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

Let $Q_{s,k}(t)$ be the polynomial defined in the proof of Proposition 3.15 and for each $s \geq 0$ define $F_s(t,x) = \sum_{k=0}^{s} \binom{s}{k} Q_{s,k}(t) Q_{s,s-k}(t) x^k$ (here we define $Q_{s,0} = 1$). Then $F_s(m,\lambda) = \mathcal{L}\left(F^s\right)/((nm)!)^2$. If we set $R(t) = \operatorname{Res}\left(F_n(t,x), F_l(t,x), x\right)$ then $R(m) = \operatorname{Res}\left(f_n, f_l, x\right)$. Now $R(0) = \operatorname{Res}\left(g_n(x), g_l(x), x\right)$ 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 $R(0) = (n!)^l (l!)^n \operatorname{Res}\left(g_n(x)/n!, g_l(x)/l!\right)$. Denote each $g_s(x)/s!$ by $h_s(x)$. We claim that $\operatorname{Res}\left(h_a(x), h_b(x), x\right) = 1$ whenever $\gcd(a+1, b+1) = 1$. Note that a or b is even since $\gcd(a+1, b+1) = 1$, and therefore $\operatorname{Res}\left(h_a, h_b, x\right) = \operatorname{Res}\left(h_b, h_a, x\right)$.We proceed by induction on $a+b$. The base case $a+b = 1$ holds because $g_0 = 1$ and therefore $\operatorname{Res}\left(1, g_1, x\right) = 1$. 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 2.2 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 $\mathcal{L}\left(F^l\right) \neq 0$. $\square$

Remark 3.18. In each of the above proofs the idea was to express the resultant of f_n and f_{n-1} as a polynomial in m. While we haven't succeeded in computing this polynomial in its entirety, we do have computational evidence that suggests that the polynomials $R_n(t)$ are Hurwitz stable, i.e. has all of its roots in the left half-plane. If this were true then each coefficient of $R_n(t)$ is positive (since $R_n(0)¿0$), and therefore F satisfies the Strong Factorial Conjecture.

Remark 3.19. Let us briefly return to the case $F = Z_1^m(1 + \lambda Z_1)$. In order to show F satisfies Conjecture 1.7 it is necessary and sufficient to show that $f_n(x)$ and f_{n-1} are relatively prime over $\mathbb{Q}$ where $f_n(x) = \sum_{k=0}^{l} \binom{n}{k} \frac{(nm+k)!}{(nm)!} x^k$. Fix a positive integer n. 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} are relatively prime. It is also straightforward to show that $f_n(x) \nmid f_{n+1}(x)$ which shows that f_n and f_{n+1} are relatively prime. By fixing m and applying the same analysis one also concludes that f_n is irreducible for infinitely many n yielding the same observations as those preceeding. The same arguments can also be applied to $F = Z_1^m(Z_2 + \lambda Z_2 Z_3)$. There is ample evidence that both these polynomials satisfy the conjecture.

For the rest of the chapter we will focus our efforts on the special case $F = 1 + \lambda Z_1^m$ 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

$$f_n(x) = \sum_{k=0}^{n} \binom{n}{k} (mk)! x^k \tag{3.16}$$

It is not hard to show that $f_n \nmid f_{n+1}$ for all $n \geq 1$.

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:

$$\begin{aligned} \nu_p(k!) &= \sum_{j=1}^{\infty} \left\lfloor \frac{k}{p^j} \right\rfloor \\ &= \frac{k - s_k}{p - 1} \end{aligned} \tag{3.17}$$

Proposition 3.20. *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 $N_p(f_n(x))$ consists of a single edge. We do this by showing that $\nu_p\left(\binom{n}{k}(mk)!\right) \geq \frac{k}{n}\nu_p((mn)!)$ for each $0 < k < n$. Using (3.17) we compute $\nu_p((mn)!) =$

$\frac{ma(p^r-1)}{p-1}$ 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 $\dfrac{k}{n}\nu_p(mn!)$:

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

For $1 \le j \le r$ write $\dfrac{mk}{p^i} = \left\lfloor \frac{mk}{p^i} \right\rfloor + a_j$ where $0 \le a_j < 1$. 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 $\sum_{j=1}^{r} \dfrac{mk}{p^j} < \sum_{j=1}^{r} \left\lfloor \dfrac{mk}{p^j} \right\rfloor + r - \nu_p(k)$. Finally, $mk < p^{r+1}$ since $ma < p$ and therefore $\sum_{j=1}^{r} \left\lfloor \dfrac{mk}{p^j} \right\rfloor = \nu_p((mk)!)$.

We have shown that the Newton polygon of f_n 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 2.5. □

Corollary 3.21. *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 $\nu_p\left((p^rk)!\right) = kb + \nu_p(k!)$ 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. $\nu_p\left(\binom{n}{k}\frac{(p^rk)!}{p^{kb}}\right) = \nu_p\left(\frac{n!}{(n-k)!}\right)$ 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 3.22. *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 (3.17) 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 (3.17), 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 3.23. *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 3.22 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 2.5
2. If $n = p^l$ then p^l divides the degree of any irreducible factor is divisible by p^r by part 1. Therefore f_n is irreducible. The second statement follows from the fact that f_n is irreducible and $f_n \nmid f_{n+1}$.
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 3.20 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 3.24. *Let $F(Z_1) = \lambda_1 + \lambda_2 Z_1^2$. Then F satisfies the Strong Factorial Conjecture.*

Proof. We may once again assume $\lambda_1 = 1$. Let $f_n(x)$ be the polynomials given in (3.16) 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. [8] or [1]) we define for each non-negative integer k the **double factorial** $(2k-1)!!$ by setting

$$(2k-1)!! = \begin{cases} 1 & k = 0 \\ \prod_{j=1}^{k}(2j-1) & k \geq 1 \end{cases} \tag{3.18}$$

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

$$g_n(x) = \sum_{k=0}^{n}(2k-1)!!b_{n,k}x^k \tag{3.19}$$

for each $n \geq 1$. Note that g_2 and g_3 are irreducible by Corollary 3.23. 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

$$\begin{aligned} r_j(x) &= A_j(x) + 2^{n-2}b_{n,n-1}x^j g_1(x) \\ &= A_j(x) + 2^{n-2}n!x^j(1+x) \\ &= A_j(x) + 2^{n-2}n!\left(x^j + x^{j+1}\right) \end{aligned} \tag{3.20}$$

where g_1 was calculated using Equation (3.19). 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 (3.20) 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 3.22. Therefore $g_n(x)$ and $r_j(x)$ have no common zeroes by Corollary **??**.

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 **??**

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 **??**. 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 $\tilde{r}_2(x) \equiv -A_1 x \mod 2 \equiv x \mod 2$. It follows that

$$\tilde{r}_2(x) = \tilde{A}_2(x) + 4n \sum_{k=2}^{n-2} \left[(2k-1)!! - (2n-3)(2n-5)(2k-5)!!\right] b_{n-1,k} x^k \tag{3.21}$$

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 (3.21) can be simplified as $(2n-5)!!\left[(2k-1)(2k-3) - (2n-3)(2n-5)\right]$ and simplifying further we find that

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

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

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

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

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

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

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

Set $A_2(x) = -\tilde{\tilde{A}}_2(x)/(2n-3)$ and $r_2(x) = A_2(x) + 16 b_{n,3} \sum_{k=2}^{n-3} (2k-5)!! b_{n-3,k} x^k$. 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.

□

[1] Callan, D., 2009. A combinatorial survey of identities for the double factorial. arXiv preprint arXiv:0906.1317.

[2] Conca, A., Krattenthaler, C., Watanabe, J., 2008. Regular sequences of symmetric polynomials. arXiv preprint arXiv:0801.2662.

[3] Cox, D., Little, J., O'Shea, D., 1992. Ideals, varieties, and algorithms. Undergraduate Texts in Mathematics. Springer-Verlag, New York, an introduction to computational algebraic geometry and commutative algebra.
URL http://dx.doi.org/10.1007/978-1-4757-2181-2

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

[5] Edo, E., van den Essen, A., 2014. The strong factorial conjecture. J. Algebra 397, 443–456.
URL http://dx.doi.org/10.1016/j.jalgebra.2013.09.011

[6] Furter, J.-P., 2013. Polynomial composition rigidity and plane polynomial automorphisms. Unpublished preprint.
URL http://perso.univ-lr.fr/jpfurter

[7] Gelfand, I. M., Kapranov, M., Zelevinsky, A., 2008. Discriminants, resultants, and multidimensional determinants. Springer Science & Business Media.

[8] Meserve, B. E., 1948. Classroom Notes: Double Factorials. Amer. Math. Monthly 55 (7), 425–426.
URL http://dx.doi.org/10.2307/2306136

[9] Mott, J. L., 1995. Eisenstein-type irreducibility criteria. In: Zero-dimensional commutative rings (Knoxville, TN, 1994). Vol. 171 of Lecture Notes in Pure and Appl. Math. Dekker, New York, pp. 307–329.

[10] Paule, P., Schorn, M., 1995. fastZeil package for Mathematica. http://www.risc.jku.at/research/combinat/risc/software/.

[11] Petkovšek, M., Wilf, H. S., Zeilberger, D., 1996. A= B, AK Peters Ltd. Vol. 30.

[12] van den Essen, A., 2000. Polynomial automorphisms and the Jacobian conjecture. Vol. 190 of Progress in Mathematics. Birkhäuser Verlag, Basel.
URL http://dx.doi.org/10.1007/978-3-0348-8440-2

[13] van den Essen, A., Wright, D., Zhao, W., 2011. On the image conjecture. J. Algebra 340, 211–224.
URL http://dx.doi.org/10.1016/j.jalgebra.2011.04.036

[14] Zhao, W., 2010. Images of commuting differential operators of order one with constant leading coefficients. J. Algebra 324 (2), 231–247.
URL http://dx.doi.org/10.1016/j.jalgebra.2010.04.022