Contents

My notes on "The Strong Factorial Conjecture" by Eric Edo and Arno van den Essen.
See: https://arxiv.org/abs/1304.3956

1 Factorial Conjecture

For the first half of the coin, the Factorial Conjecture, presented here, let $m \in \mathbb{N}_+$ be a positive integer and consider the set of all polynomials $\mathbb{C}[X_1, X_2, \ldots, X_m]$ in m variables over $\mathbb{C}$. In the interest of brevity, we will denote this set by $\mathbb{C}^{[m]} := \mathbb{C}[X_1, X_2, \ldots, X_m]$.

Equipped with the usual addition and multiplication, $\mathbb{C}^{[m]}$ forms a $\mathbb{C}$-algebra, and as such, it is generated by the following monomial basis

$$\mathcal{B} = \left\{ X_1^{l_1} \cdots X_m^{l_m} \;\middle|\; l_k \in \mathbb{N}_0 \text{ for all } 1 \leq k \leq m \right\}.$$

Thus, any linear map is fully specified by its values on the elements of this basis. Such linear map is the factorial map.

Definition 1 (Definition 2.1)**.** A factorial map is a linear map linear map $\mathcal{L} : \mathbb{C}^{[m]} \longrightarrow \mathbb{C}$ defined by

$$\mathcal{L}(X_1^{l_1} \cdots X_m^{l_m}) = l_1! \cdots l_m! \qquad \text{for all } l_1, \ldots, l_m \in \mathbb{N}$$

Example 1.1. Consider $f(X) = 3X - 5XY + 7Y^2 \in \mathbb{C}^{[2]}$. Applying the factorial map yields

$$\begin{aligned} \mathcal{L}(f(X)) &= 3\mathcal{L}(X) - 5\mathcal{L}(XY) + 7\mathcal{L}(Y^2) \\ &= 3 \cdot 1 - 5 \cdot 1 + 7 \cdot 2 \\ &= 12. \end{aligned}$$

Example 1.2. If we limit our selves to a polynomial in one indeterminate, such as $f(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ for a fixed $n \in \mathbb{N}_0$ and $a_k \in \mathbb{C}$ for all $1 \leq k \leq n$, we have

$$\mathcal{L}(f(X)) = \sum_{k=0}^{n} a_k \mathcal{L}(X^k) = \sum_{k=0}^{n} a_k k!$$

Remark (Remark 2.2)**.** Let $\sigma \in S_n$ be a permutation on the set $\{X_1, \ldots, X_m\}$. We extend σ to an automorphism $\tilde{\sigma}$ of the $\mathbb{C}$-algebra $\mathbb{C}^{[m]}$ by setting

$$\tilde{\sigma}\left(X_1^{l_1} \cdots X_m^{l_m}\right) = \sigma(X_1)^{l_1} \cdots \sigma(X_m)^{l_m}.$$

Then, $\mathcal{L}(\tilde{\sigma}(f)) = \mathcal{L}(f)$ for any $f \in \mathbb{C}^{[m]}$.

Proof. Let σ also denote the permutation on $\{1, \ldots, m\}$ where $\sigma(X_i) = X_{\sigma(i)}$. For any monomial $X_1^{l_1} \cdots X_m^{l_m}$, we have

$$\mathcal{L}\left(\tilde{\sigma}\left(X_1^{l_1} \cdots X_m^{l_m}\right)\right) = \mathcal{L}\left(X_{\sigma(1)}^{l_1} \cdots X_{\sigma(m)}^{l_m}\right) = l_1! \cdots l_m!$$

Thus, for any monomial basis element $B \in \mathcal{B}$, $\mathcal{L}(\tilde{\sigma}(B)) = \mathcal{L}(B)$. By linearity of both $\tilde{\sigma}$ and $\mathcal{L}$, it is

$$\mathcal{L}(\tilde{\sigma}(f)) = \mathcal{L}(f) \text{ for all } f \in \mathbb{C}^{[m]}.$$

□

Remark (Remark 2.3)**.** In general, the factorial map $\mathcal{L}$ does not preserve multiplication. However, if two polynomials f and g do not share any indeterminates, i.e. there exsists a subset $I \subset \{1, 2, \ldots, m\}$ such that

$$f(X) \in \mathbb{C}[X_k : k \in I] \;\text{ and }\; g(X) \in \mathbb{C}[X_k : k \notin I],$$

then indeed $\mathcal{L}(fg) = \mathcal{L}(f)\mathcal{L}(g)$.

Proof. Let $B_1 \in \mathcal{B}$ and $B_2 \in \mathcal{B}$ two monomial basis elements of $\mathbb{C}^{[m]}$ that do not share any indeterminates, i.e. there is a subset $I \subset \{1, 2, \ldots, m\}$ such that $B_1 \in \mathbb{C}[X_k : k \in I]$ and $B_2 \in \mathbb{C}[X_k : k \notin I]$.

We first want to renumber the indeterminates conveniently. Let σ be a permutation on $\{ X_1, \ldots, X_m \}$ and $\tilde{\sigma}$ an extension of σ to an automorphism on $\mathbb{C}^{[m]}$ such that for an $n \in \mathbb{N}$

$$\tilde{\sigma}(B_1) \in \mathbb{C}[X_k : k \in \{1, \ldots, n\}] \text{ and } \tilde{\sigma}(B_2) \in \mathbb{C}[X_k : k \in \{n+1, \ldots, m\}]$$

Now, we have

$$\begin{aligned}
\mathcal{L}(B_1)\mathcal{L}(B_2) &= \mathcal{L}(\tilde{\sigma}(B_1))\mathcal{L}(\tilde{\sigma}(B_1)) \\
&= \mathcal{L}(X_1^{l_1} \cdots X_n^{l_n})\mathcal{L}(X_{n+1}^{l_{n+1}} \cdots X_m^{l_m}) \\
&= l_1! \cdots l_n! l_{n+1}! \cdots l_m \\
&= \mathcal{L}(B_1 B_2).
\end{aligned}$$

□

Example 1.3. To illustrate that the factorial map $\mathcal{L}$ is not compatible with the multiplication, simply consider $f(X) = X$ and $g(X) = X$ in $\mathbb{C}^{[1]}$. It is

$$\mathcal{L}(fg) = \mathcal{L}(X^2) = 2 \text{ while } \mathcal{L}(f)\mathcal{L}(g) = 1 \cdot 1 = 1.$$

Theorem 2 (Conjecture 2.4)**.** If $f \in \mathbb{C}^{[m]}$ is a polynomial with $\mathcal{L}(f^k) = 0$ for all $k \in \mathbb{N}_+$, then $f = 0$.

Example 2.1. Consider $f(X) = a_0 + a_1 X \in \mathbb{C}^{[1]}$. For f and f^2, the factorial map gives

$$\begin{aligned}
\mathcal{L}(f) &= a_0 + a_1 \\
\mathcal{L}(f^2) &= \mathcal{L}(a_0^2 + 2a_0 a_1 X + a_1^2 X^2) = a_0^2 + 2a_0 a_1 + 2a_1^2.
\end{aligned}$$

If f fulfills the condition for the aforementioned conjecture, we have $a_0 + a_1 = 0$, so $a_0 = -a_1$ in the first equation. Substituting in the second equation, yields $a_0^2 - 2a_0^2 + 2a_0^2 = a_0^2 = 0$, hence $a_0 = a_1 = 0$.

We introduce the following notation. For a polynomial $f \in \mathbb{C}^{[m]}$, $\mathcal{N}(f)$ denotes the number of nonzero monomials in f. For example, $\mathcal{N}(1 + X + X^2) = 3$ and $\mathcal{N}(XYZ) = 1$.

Definition 3. Set the following subsets of $\mathbb{C}^{[m]}$ to be

$$\begin{aligned}
F^{[m]} &= \{0\} \cup \left\{ f \in \mathbb{C}^{[m]} \setminus \{0\} \;\middle|\; \text{there is some } k \in \mathbb{N}_+ \text{ such that } \mathcal{L}(f^k) \neq 0 \right\} \\
F_n^{[m]} &= \{0\} \cup \left\{ f \in \mathbb{C}^{[m]} \setminus \{0\} \;\middle|\; \text{there is some } k \in \{n, \ldots, n + \mathcal{N}(f) - 1\} \text{ such that } \mathcal{L}(f^k) \neq 0 \right\} \\
F_\cap^{[m]} &= \bigcap_{n \in \mathbb{N}_+} F_n^{[m]}
\end{aligned}$$

We call $F^{[m]}$ to be the factorial set and $F_\cap^{[m]}$ to be the strong factorial set.

Remark. The polynomials of the factorial set $F^{[m]}$ are precisely the polynomials that satisfy the factorial conjecture. Thus, the factorial conjecture can be reformulated to $F^{[m]} = \mathbb{C}^{[m]}$.

Proof. The contraposition of the factorial conjecture states: If $f \neq 0$, then there is some $k \in \mathbb{N}_+$ such that $\mathcal{L}(f^k) \neq 0$. Thus, if the factorial conjecture is true, then $F^{[m]} = \mathbb{C}^{[m]}$. □

Theorem 4 (Conjecture 2.8)**.** All polynomials are in the strong factorial set, i.e. $F_\cap^{[m]} = \mathbb{C}^{[m]}$.

Remark. Let $n \in \mathbb{N}_+$ be a positive integer.

1. Let $f \in \mathbb{C}^{[m]}$ be a polynomial. $f \in F_n^{[m]}$ if and only if for all $k \in \{n, \ldots, n + \mathcal{N}(f) - 1\}$

$$\mathcal{L}(f^k) = 0 \text{ implies } f = 0.$$

2. regular system of parameters

Remark. If $\mathcal{N}(f) = 1$, i.e. f is a monomial, then $f \in F_\cap^{[m]}$.

Proof. If $\mathcal{N}(f) = 1$, then $f = X_1^{l_1} \cdots X_m^{l_m}$ and $f^k = X_1^{l_1 k} \cdots X_m^{l_m k}$. Thus, the only case where $\mathcal{L}(f^k) = 0$ for any $k \in \mathbb{N}_+$ is when $f = 0$. Hence f lies in $F_n^{[m]}$ for all $n \in \mathbb{N}_+$ and we have $f \in F_\cap^{[m]}$. □

Remark. If $f \in \mathbb{R}_{\geq 0}^{[m]}$, i.e. all nonzero coefficients are real and positive, then $f \in F_\cap^{[m]}$.

Proof. Should be straight forward. □

Remark (2.11)**.** See proof in other paper.

Example 4.1. Consider $f = X_1 - X_2 \in \mathbb{C}^{[2]}$. For all $n \in \mathbb{N}_+$,

$$\mathcal{L}(f^n) = \mathcal{L}\left(\sum_{k=0}^{n} \binom{n}{k} X_1^{n-k}(-X_2)^k\right) = \sum_{k=0}^{n} \binom{n}{k}(n-k)!k!(-1)^k = \sum_{k=0}^{n} \frac{n!}{k!}k!(-1)^k = n!\sum_{k=0}^{n}(-1)^k$$

Hence $\mathcal{L}(f^n) = n!$ if n is even and $\mathcal{L}(f^n) = 0$ otherwise. Since n or $n+1$ is even, we have $f \in F_n^{[2]}$. Thus $f \in F_\cap^{[2]}$.

2 Rigidity Conjecture

Definition 5. Let $f(X) \in \mathbb{C}[[X]]$ be a power series. We call a power series $f^{-1}(X) \in \mathbb{C}[[X]]$ the compositional inverse of f, if it satisfies $f(f^{-1}(X)) = f^{-1}(f(X)) = X$.

Proposition 6. A power series $f(X) = a_0 + a_1X + \cdots \in \mathbb{C}[[X]]$ has a compositional inverse if and only if $a_0 = 0$ and $a_1 \neq 0$. Moreover, if the compositional inverse exists, then it is unique.

Proof. Assume f has a compositional inverse and denote the compositional inverse by $f^{-1}(X) = b_0 + b_1X + b_2X^2 + \cdots$. Writing out $f(f^{-1}(X)) = X$ gives

$$a_0 + a_1(b_0 + b_1X + b_2X^2 + \cdots)$$

□

2.1 Rigidity Conjecture

Theorem 7 (Conjecture 2.13)**.** Let $a(X) \in \mathbb{C}[X]$ be a polynomial of degree less or equal to $m + 1 \in \mathbb{N}_+$ such that $a(X) \equiv X \mod X^2$. If m consecutive coefficient of the compositional inverse $a^{-1}(X)$ vanish, i.e. $b_{n+1} = b_{n+2} = \cdots = b_{n+m} = 0$ for some $n \in \mathbb{N}_+$ then $a(X) = X$.

Remark. If we denote the polynomial $a(X)$ by $\sum_{k\in\mathbb{N}_0} a_kX^k$ for some $a_k \in \mathbb{C}$ for all $k \in \mathbb{N}_0$, then the condition $a(X) \equiv X \mod X^2$ amounts to $a_0 = 0$ and $a_1 = 1$. UNSURE, BUT PRETTY SURE WE HAVE THIS CONDITION TO ENSURE THE INVERSE EVEN EXISTS.

Theorem 8 (Conjecture 2.14)**.** Let $a(X) \in \mathbb{C}[X]$ be a polynomial of degree less or equal to $m+1 \in \mathbb{N}_+$ such that $a(X) \equiv X \mod X^2$. If the coefficients of $X^{n+1}, \ldots, X^{n+m}$ of the compositional inverse vanish, then $a(X) = X$.

Remark. $R(m)$ if and only if $R(m)_n$ for all $n \in \mathbb{N}_+$.

Lemma 9 (Lemma 2.16)**.** Let $f \in \mathbb{C}[[X]]$ and $g \in \mathbb{C}[[X]]$ be two formal series such that $f(X) \equiv g(X) \mod X^2$, i.e. the constant and the coefficient of the first degree agree. If $f(X) \equiv g(X) \mod X^n$ for some integer $n \geq 2$ then $f^{-1}(X) \equiv g^{-1}(X) \mod X^n$.

Proof. □

Proposition 10.

1. The polynomial $a(X)$ is invertible for the composition.
2. For all $i \in \{1, \ldots, \deg(a-1)\}$, the coefficient a_i is nilpotent element in A. I just don't see this ...

The following lemma and proof are due to #XXX.

Example 10.1 (See 5.4.4)**.** $f(X) = Xe^{-X} = X\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} X^k$

$$[X^n]f^{-1}(X) = \frac{1}{n}[X^{n-1}]e^{nX}$$

Lemma 11 (Lemma 2.20 (Additive Inversion Formula))**.** Let $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ be complex numbers. The formal inverse of $a(X) = X(1 - (\alpha_1X + \cdots + \alpha_mX^m))$ is given by the following formula

$$a^{-1}(X) = X\left(1 + \frac{1}{n+1}\sum_{n\geq 1} u_nX^n\right)$$

where

$$u_n = \frac{1}{n!}\sum_{j_1+2j_2+\cdots+mj_m=n} \frac{(n + j_1 + \cdots + j_m)!}{j_1! \cdots j_m!}\alpha_1^{j_1}\cdots\alpha_m^{j_m}$$

Proposition 12 (Proposition 2.23)**.** Let $\alpha_1, \dots, \alpha_m \in \mathbb{C}$ be complex numbers and let $(u_n)_{n\in\mathbb{N}_+}$ be a sequence defined by AIF in Lemma 2.20. For all $n \in \mathbb{N}_+$, the Rigidity Conjecture $R(m)_n$ is equivalent to the following implication: If $u_n = \cdots = u_{n+m-1} = 0$ then $\alpha_1 = \cdots = \alpha_m = 0$.

Proof. □

Theorem 13. 1. The inclusion $E^{[m]} \subset F_n^{[m]}$ implies $R(m)_n$

Definition 14.

$$E^{[m]} = \{\, X_1 \cdots X_m(\mu_1 X_1 + \cdots + \mu_m X_m) \mid \mu_1, \dots, \mu_m \in \mathbb{C} \,\} \subset$$
$$F_n^{[m]} = \left\{ f \in \mathbb{C}^{[m]} \setminus \{0\} \;\middle|\; \mathcal{L}(f^k) \neq 0 \text{ for some } n \leq k \leq \mathcal{N}(f) - 1 \right\} \cup \{0\}$$