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. $F_\cap^{[m]} = \mathbb{C}^{[m]}$.

2 Rigidity Conjecture

TODO: $\mathbb{C}_0[[X]]$ the set of formal power series with the constant coefficient being 0 forms a $\mathbb{C}$-algebra with composition being the composition.

2.1 Reciprocal of a Power Series

Definition 5 (Cauchy Product)**.** For two power series $f(X) = \sum_{k\in\mathbb{N}_0} a_k X^k \in \mathbb{C}[[X]]$ and $g(X) = \sum_{k\in\mathbb{N}_0} b_k X^k \in \mathbb{C}[[X]]$, we define their Cauchy product by

$$f(X) \times g(X) := \sum_{k\in\mathbb{N}_0} c_k X^k \quad \text{where} \quad c_k := \sum_{i=0}^{k} a_i b_{k-i}.$$

Remark. If one of the power series is also a polynomial, the formula above produces the same result as primitivly expanding would do.

Example 5.1. Take the alternating series $f(X) = \sum_{k\in\mathbb{N}_0} (-1)^k X^k$ and the geometric series $g(X) = \sum_{k\in\mathbb{N}_0} X^k$ and consider their Cauchy product $f \times g$. The coefficients of the product is given by

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} (-1)^i (1)^{k-i} = \sum_{i=0}^{k} (-1)^i = \begin{cases} 1 \text{ if } k \text{ is even} \\ 0 \text{ if } k \text{ is odd} \end{cases}$$

hence we have $f(X) \times g(X) = \sum_{k\in\mathbb{N}_0} X^{2k} = 1 + X^2 + X^4 + \cdots$.

Notice that both the alternating series f and the geometric series g only converge for values $|X| < 1$ and thus, through the lense of analysis, their product only makes sense with that limitation. However, as algebraists we are not beholden to such bounds.

If we declare $|X| < 1$, then with the help of the analytical tools, we may evaluate both series as

$$f(X) = \frac{1}{1+X} \quad \text{and} \quad g(X) = \frac{1}{1-X}$$

therefore

$$f(X) \cdot g(X) = \frac{1}{1+X} \cdot \frac{1}{1-X} = \frac{1}{1-X^2}$$

which matches our expectation exactly as the last expression is the simplied form of $\sum_{k\in\mathbb{N}_0} X^{2k} = f(X) \times g(X)$.

It is well-known that the set of power series over a ring is again a ring. In particular, $\mathbb{C}[[X]]$ with the usual coefficient-wise addition and the Cauchy product is a commutative ring with unity. It is, however, not a field because not all power series have a mulitplicative inverse. It turns out however, that strikingly many of the power series have a mulitplicative inverse.

Proposition 6. A power series $f(X) = \sum_{k\in\mathbb{N}_0} a_k X^k$ has a mulitplicative inverse if and only if its constant coefficient a_0 is non-zero.

The reciprocal of f, denoted by if it exsists, #blablabla

$$b_0 = \frac{1}{a_0} \quad \text{and for } k \geq 1 \text{ it is} \quad b_k = -\frac{1}{a_0} \sum_{i=1}^{k} a_i b_{k-i}$$

Example 6.1. Consider $f(X) = \sum_{k=0}^{\infty} (k+1) X^k$

It's insane that the inverse is $(X-1)^2$

Remark. Point out that the multiplicative inverse of the power series is a simple polynomial and in turn, many (maybe all, there was something with Gauss about this in algebra) polynomial only have an inverse as a power series.

2.2 Formal Differentiation

Definition 7 (Formal Differentiation)**.** Given a formal power series $f(X) = \sum_{k\in\mathbb{N}_0} a_k X^k \in \mathbb{C}[[X]]$ its *formal derivative*, denoted f', is defined by

$$f'(X) := \sum_{k\in\mathbb{N}_0} a_k \cdot k \cdot X^{k-1}.$$

When talking about differentiation, how can one resist to use the exponential function as an example?

Example 7.1. Consider the series representation of ce^x which is

$$f(X) = \sum_{k\in\mathbb{N}_0} \frac{1}{k!} X^k.$$

Formal differentiation gives

$$f'(X) = \sum_{k\in\mathbb{N}_+} \frac{c}{k!} \cdot k \cdot X^{k-1} = \sum_{k\in\mathbb{N}_+} \frac{c}{(k-1)!} \cdot X^{k-1} = \sum_{k\in\mathbb{N}_0} \frac{c}{k!} X^k = f(X).$$

which is expected from analysis. Indeed, it is not difficult to show that $f = f'$ if and only if $f(X) = ce^X$. This proof can be found in functology book.

Remark. difference with analytic view of differentiation

Proposition 8 (Linearity of Formal Differentiation)**.** Formal differentiation as an operator is linear, i.e. if we view $\mathbb{C}[[X]]$ as a $\mathbb{C}$-vector space, then $(*)' : \mathbb{C}[[X]] \longrightarrow \mathbb{C}[[X]]$ satisfies additivity and homogeneity.

As expected, the usual rules of differentiation such as the product rule and the chain rule may be transfered one-to-one from the analytical world to the one of algebra and formal power series. For this paper, only the chain rule is of interest. Before we formaly introduce the chain rule however, we require the notion of composition of power series.

2.3 Composition of Formal Power Series

Proposition 9 (Chain Rule)**.** If $f \in \mathbb{C}[[X]]$ and $g \in \mathbb{C}[[X]]$ are two formal power series, then the formal differentiation on their composition may be expressed as

$$(f \circ g)' = (f' \circ g) \cdot g'$$

When we consider compositions of formal power series, we always want the constant term to be 0.

The following example is taken from:

https://math.stackexchange.com/questions/1212053/defining-composition-of-two-formal-series-what-is-going-on

Example 9.1. Let $f = \sum_{k\in\mathbb{N}_0} a_k X^k$ and $g = 1 + X$. Consider $f \circ g$. We have

$$\begin{aligned} f \circ g &= \sum_{k\in\mathbb{N}_0} a_k (1+X)^k \\ &= a_0 + a_1 + a_1 X + a_2 + 2a_2 X + a_2 X^2 + \cdots \end{aligned}$$

If $f \circ g$ is again a formal power series, then we should be able to write $f \circ g = \sum_{k\in\mathbb{N}_+} c_k X^k$ for some $c_k \in \mathbb{C}$. However, we see that c_0 is the sum of all a_k and we cannot evaluate that as algebraists. Thus composition of formal power series only makes sense if the constant coefficient is 0.

Proposition 10. A power series $f(X) = \sum_{k\in\mathbb{N}_+} a_k X^k \in \mathbb{C}[[X]]$ has a compositional inverse $f^{-1}(X)$ if and only if $a_1 \neq 0$, in which case $f^{-1}(X)$ is unique.

Proof. Assume $g(X) = b_1X + b_2X^2 + \cdots$ satisfies $f(g(X)) = X$. We then have

$$a_1(b_1X + b_2X^2 + \cdots) + a_2(b_1X + b_2X^2 + \cdots)^2 + a_3(b_1X + b_2X^2 + \cdots)^3 = X$$

Equating coefficients on both sides yields the infinite system of equations

$$\begin{aligned} a_1b_1 &= 1 \\ a_1b_2 + a_2b_1^2 &= 0 \\ a_1b_3 + 2a_2b_1b_2 + a_3b_1^3 &= 0 \\ &\vdots \end{aligned}$$

□

Another proof:

https://www.math.uwaterloo.ca/ dgwagner/co430I.pdf But there is no simple formula for the coefficients of the inverse (see enumerative combinatorics).

Lemma 11 (Lagrange Inversion Formula)**.** Let K be a field of charateristic

$$f^{-1}(X) = \sum_{n\in\mathbb{N}_+} b_nX^n$$
$$\text{where } b_n = \frac{1}{n} \cdot [X^{n-1}] \left(\frac{X}{f(X)}\right)^n$$

Proof. We will prove that the given formula for b_n, i.e. the n-th coefficient of the compositional inverse, is merited. Thus begin by fixing an arbitary integer $n \in \mathbb{N}_+$.

By proposition #XXX, f is guranteed to have a unique compositional inverse which we will denote by $f^{-1}(X) = \sum_{k\in\mathbb{N}_+} b_kX^k$ with $b_k \in \mathbb{C}$ for all $k \in \mathbb{N}_+$. Applying the original f to both sides yields $f(f^{-1}(X)) = X$ on the left side and on the right we have

$$f\left(\sum_{k\in\mathbb{N}_+} b_kX^k\right) = \sum_{k\in\mathbb{N}_+} b_kf(X)^k$$

due to the linearity of f as a map, thus $X = \sum_{k\in\mathbb{N}_+} b_kf(X)^k$. Now, formal differentiation with the chain rule #sure? gives

$$1 = \sum_{k\in\mathbb{N}_+} k \cdot b_k \cdot f(X)^{k-1} \cdot f'(X).$$

Let $n \in \mathbb{N}$ #with0? be an integer. #moremotivation Dividing the above equation with the n-th power of the reciprocal produces

$$f(X)^{-n} = \sum_{k\in\mathbb{N}_+} k \cdot b_k \cdot f(X)^{k-n-1} \cdot f'(X).$$

After □

2.4 Rigidity Conjecture

Theorem 12 (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 $\sum_{k\in\mathbb{N}_0} a_k X^k$ 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 $a_1 = 1$.

Theorem 13 (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 14 (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 15. 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 15.1 (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 16 (Lemma 2.20 (Additive Inversion Formula))**.** Let $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ be complex numbers. The formal inverse of $a(X) = X(1 - (\alpha_1 X + \cdots + \alpha_m X^m))$ is given by the following formula

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

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 17 (Proposition 2.23)**.** Let $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ 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 18. 1. The inclusion $E^{[m]} \subset F_n^{[m]}$ implies $R(m)_n$

Definition 19.

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