Composition Lemma for Lean4

Edinah Gnang
Parikshit Chalise

Contents

12 ‘

CHAPTER 1

Composition Lemma

1.1. Overview

The *Composition Lemma* was developed and refined over 6 years, beginning in 2018, as a novel approach to settle in the affirmative the *Graceful Tree Conjecture*. The first of such papers was posted in [3] by Gnang. A further developed series of papers resolving the same conjecture again appeared in [4] and [5]. Recently, the same method has been applied to settle other longstanding conjectures in [1] and [2]. We comment that the series of papers shared on the open-source platform arXiv reflect the evolving landscape of Gnang's thought process, and the frequent re-uploads were driven by the natural progression and refinement of ideas. However, we recognize that these numerous edits may have unintentionally caused confusion and raised questions regarding the success of the method. In the current work, we aim to address these concerns by presenting a detailed blueprint of the proof, with the goal of formalizing it in Lean4.

1.2. Functional Directed Graphs

For notational convenience, let $\mathbb{Z}_n$ denote the set whose members are the smallest n non-negative integers, i.e.,

$$\mathbb{Z}_n := \{0, \dots, n-1\}. \tag{1.2.1}$$

For a function $f : \mathbb{Z}_m \to \mathbb{Z}_n$, we write $f \in \mathbb{Z}_n^{\mathbb{Z}_m}$. For $X \subseteq \mathbb{Z}_m$, $f(X)$ denotes the image of X under f, i.e.,

$$f(X) = \{f(i) : i \in X\}, \tag{1.2.2}$$

and $|f(X)|$ denotes its cardinality. For $Y \subseteq \mathbb{Z}_n$, $f^{-1}(Y)$ denotes the pre-image of Y under f i.e.

$$f^{-1}(Y) = \{j \in \mathbb{Z}_m : f(j) \in Y\} \tag{1.2.3}$$

Definition 1.2.4 (Functional digraphs). For an arbitrary $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$, the *functional directed graph* prescribed by f, denoted G_f, is such that the vertex set $V(G_f)$ and the directed edge set $E(G_f)$ are respectively as follows:

$$V(G_f) = \mathbb{Z}_n,\ E(G_f) = \{(v, f(v)) : v \in \mathbb{Z}_n\}.$$

Definition 1.2.5 (Graceful functional digraphs). The functional directed graph prescribed by $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ is graceful if there exist a bijection $\sigma \in \mathrm{S}_n \subset \mathbb{Z}_n^{\mathbb{Z}_n}$ such that

$$\left\{ \left|\sigma f \sigma^{-1}(i) - i\right| : i \in \mathbb{Z}_n \right\} = \mathbb{Z}_n. \tag{1.2.6}$$

If $\sigma = \mathrm{id}$ (the identity function), then G_f — the functional directed graph prescribed by f — is gracefully labeled.

Definition 1.2.7 (Automorphism group). For a functional directed graph G_f, its automorphism group, denoted $\mathrm{Aut}\left(G_f\right)$, is defined as follows:

$$\mathrm{Aut}(G_f) = \{\sigma \in \mathrm{S}_n : \{(i, f(i)) : i \in \mathbb{Z}_n\} = \{(j, \sigma f \sigma^{-1}(j)) : j \in \mathbb{Z}_n\}\}.$$

For a polynomial $P \in \mathbb{C}[x_0, \dots, x_{n-1}]$, its automorphism group, is the stablizer of P and denoted $\mathrm{Aut}(P)$. Formally defined as follows:

$$\mathrm{Aut}\,(P) = \{\sigma \in \mathrm{S}_n : P\,(x_0, \dots, x_i, \dots, x_{n-1}) = P\left(x_{\sigma(0)}, \dots, x_{\sigma(i)}, \dots, x_{\sigma(n-1)}\right)\}.$$

Definition 1.2.8 (Graceful re-labelings). The set of distinct gracefully labeled functional directed graphs isomorphic to G_f is

$$\mathrm{GrL}\left(G_f\right) := \left\{ G_{\sigma f \sigma^{-1}} : \begin{array}{c} \sigma \text{ is a representative of a coset in } {}^{\mathrm{S}_n}/_{\mathrm{Aut}(G_f)} \text{ and} \\ \mathbb{Z}_n = \left\{\left|\sigma f \sigma^{-1}\,(i) - i\right| \,:\, i \in \mathbb{Z}_n\right\} \end{array} \right\}$$

Definition 1.2.9 (Complementary labeling involution). If $\varphi = n-1-\mathrm{id}$, i.e. $\varphi \in \mathbb{Z}_n^{\mathbb{Z}_n}$ such that

$$\varphi(i) = n-1-i,\ \forall\, i \in \mathbb{Z}_n,$$

The complementary labeling involution is defined as the map whose domain and codomain is $\mathbb{Z}_n^{\mathbb{Z}_n}$ and is prescribed by

$$f \mapsto \varphi f \varphi^{-1},$$

for an arbitrary $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$.

Observe that for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ the complementary labeling involution fixes the induced edge label of each edge as seen from the equality

$$|f(i) - i| = |\varphi f(i) - \varphi(i)|\,, \quad \forall\, i \in \mathbb{Z}_n. \tag{1.2.10}$$

In other words, induced edge labels are fixed by the vertex relabeling effected by φ. We call this induced edge label symmetry the *complementary labeling symmetry* of the functional directed graph G_f.

1.3. Quotient-Remainder Theorem and Lagrange Interpolation

Proposition 1.3.1 (Multivariate Quotient-Remainder). *Let $d(x) \in \mathbb{C}[x]$ be a degree n monic polynomial with simple roots, i.e.,*

$$d(x) = \prod_{i\in\mathbb{Z}_n} (x-\alpha_i) \ \text{ and } \ 0 \neq \prod_{0\le u<v<n} (\alpha_v - \alpha_u), \tag{1.3.2}$$

where $\{\alpha_u : u \in \mathbb{Z}_n\} \subset \mathbb{C}$. For all $P \in \mathbb{C}[x_0, \dots, x_{m-1}]$, there exists a unique remainder $r(x_0,\dots,x_{m-1}) \in \mathbb{C}[x_0,\dots,x_{m-1}]$ of degree at most $n-1$ in each variable such that for quotients: $\{q_k(x_0,\dots,x_{n-1}) : k \in \mathbb{Z}_n\} \subset \mathbb{C}[x_0,\dots,x_{n-1}]$, we have

$$P(x_0,\dots,x_{m-1}) = r(x_0,\dots,x_{m-1}) + \sum_{u\in\mathbb{Z}_m} q_u(x_0,\dots,x_{m-1})\, d(x_u). \tag{1.3.3}$$

Proof. We prove by induction on the number of variables that the remainder admits the expansion

$$r(x_0,\dots,x_{m-1}) = \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_m}} P(\alpha_g) \prod_{i\in\mathbb{Z}_m} \left(\prod_{j_i\in\mathbb{Z}_n\setminus\{g(i)\}} \left(\frac{x_i - \alpha_{j_i}}{\alpha_{g(i)} - \alpha_{j_i}} \right) \right), \tag{1.3.4}$$

where for notational convenience $P(\alpha_g) := P(\alpha_{g(0)},\dots,\alpha_{g(m-1)})$. The base case stems from the univariate quotient-remainder theorem over the field $\mathbb{C}$. The univariate-quotient remainder theorem over the field $\mathbb{C}$ asserts that there exist a unique quotient-remainder pair $(q(x_0),\, r(x_0)) \in \mathbb{C}[x_0] \times \mathbb{C}[x_0]$ subject to

$$H(x_0) = q(x_0)\, d(x_0) + r(x_0), \tag{1.3.5}$$

where $r(x_0) \in \mathbb{C}[x_0]$ is of degree at most $n-1$. It is completely determined by its evaluation over $\{\alpha_i : i \in \mathbb{Z}_n\}$, and by Lagrange interpolation we have

$$r(x_0) = \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_1}} H(\alpha_{g(0)}) \prod_{j_0\in\mathbb{Z}_n\setminus\{g(0)\}} \left(\frac{x_0 - \alpha_{j_0}}{\alpha_{g(0)} - \alpha_{j_0}} \right), \tag{1.3.6}$$

thus establishing the claim in the base case. For the induction step, assume as our induction hypothesis that for all $F \in \mathbb{C}[x_0,\dots,x_{m-1}]$, we have

$$F = \sum_{k\in\mathbb{Z}_m} q_k(x_0,\dots,x_{m-1})\, d(x_k) + \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_m}} F(\alpha_g) \prod_{i\in\mathbb{Z}_m} \left(\prod_{j_i\in\mathbb{Z}_n\setminus\{g(i)\}} \left(\frac{x_i - \alpha_{j_i}}{\alpha_{g(i)} - \alpha_{j_i}} \right) \right). \tag{1.3.7}$$

We proceed to show that the hypothesis implies that every polynomial in $m+1$ variables also admits a similar expansion, thus establishing the desired claim. Consider a polynomial $H \in \mathbb{C}[x_0,\dots,x_m]$. We view H as a univariate polynomial in the variable x_m whose coefficients lie in the field of fraction $\mathbb{C}(x_0,\dots,x_{m-1})$. The univariate quotient-remainder theorem over the field of fractions $\mathbb{C}(x_0,\dots,x_{m-1})$ asserts that there exit a unique quotient-remainder pair

$$(q(x_m),\, r(x_m)) \in (\mathbb{C}(x_0,\dots,x_{m-1}))[x_m] \times (\mathbb{C}(x_0,\dots,x_{m-1}))[x_m]$$

subject to

$$H(x_0,\dots,x_m) = q(x_0,\dots,x_m)\, d(x_m) + r(x_0,\dots,x_m), \tag{1.3.8}$$

where $r\left(x_0,\dots,x_m\right) \in (\mathbb{C}(x_0,\dots,x_{m-1}))[x_m]$ is of degree at most $n-1$ in the variable x_m. We write

$$r\left(x_0,\dots,x_m\right) = \sum_{k\in\mathbb{Z}_n} a_k\left(x_0,\dots,x_{m-1}\right)\left(x_m\right)^k. \tag{1.3.9}$$

We now show that coefficients $\left\{a_k(x_0,\dots,x_{m-1}) : k\in\mathbb{Z}_n\right\}$ all lie in the polynomial ring $\mathbb{C}[x_0,\dots,x_{m-1}]$ via the equality

$$\left(\text{Vander}\begin{pmatrix}\alpha_0\\ \vdots\\ \alpha_u\\ \vdots\\ \alpha_{n-1}\end{pmatrix}\right)\cdot\begin{pmatrix}a_0\left(x_0,\dots,x_{m-1}\right)\\ \vdots\\ a_u\left(x_0,\dots,x_{m-1}\right)\\ \vdots\\ a_{n-1}\left(x_0,\dots,x_{m-1}\right)\end{pmatrix} = \begin{pmatrix}H(x_0,\dots,x_{m-1},\alpha_0)\\ \vdots\\ H(x_0,\dots,x_{m-1},\alpha_u)\\ \vdots\\ H(x_0,\dots,x_{m-1},\alpha_{n-1})\end{pmatrix}, \tag{1.3.10}$$

where

$$\left(\text{Vander}\begin{pmatrix}\alpha_0\\ \vdots\\ \alpha_u\\ \vdots\\ \alpha_u\end{pmatrix}\right)[i,j] = (\alpha_i)^j,\ \forall\, 0\le i,j<n. \tag{1.3.11}$$

Since the Vandermonde matrix is invertible by the fact

$$0\neq\det\left(\text{Vander}\begin{pmatrix}\alpha_0\\ \vdots\\ \alpha_u\\ \vdots\\ \alpha_u\end{pmatrix}\right) = \prod_{0\le u<v<n}(\alpha_v-\alpha_u), \tag{1.3.12}$$

we indeed have

$$\begin{pmatrix}a_0\left(x_0,\dots,x_{m-1}\right)\\ \vdots\\ a_u\left(x_0,\dots,x_{m-1}\right)\\ \vdots\\ a_{n-1}\left(x_0,\dots,x_{m-1}\right)\end{pmatrix} = \left(\text{Vander}\begin{pmatrix}\alpha_0\\ \vdots\\ \alpha_u\\ \vdots\\ \alpha_u\end{pmatrix}\right)^{-1}\cdot\begin{pmatrix}H(x_0,\dots,x_{m-1},\alpha_0)\\ \vdots\\ H(x_0,\dots,x_{m-1},\alpha_u)\\ \vdots\\ H(x_0,\dots,x_{m-1},\alpha_{n-1})\end{pmatrix}. \tag{1.3.13}$$

Therefore, we have

$$H(x_0,\dots,x_m) = q_m(x_0,\dots,x_m)\,d(x_m) + \sum_{g(m)\in\mathbb{Z}_n} H(x_0,\dots,x_{m-1},\alpha_{g(m)}) \prod_{j\in\mathbb{Z}_n\setminus\{g(m)\}}\left(\frac{x_m-\alpha_{j_m}}{\alpha_{g(m)}-\alpha_{j_m}}\right). \tag{1.3.14}$$

Applying the induction hypothesis to coefficients

$$\left\{H\left(x_0,\dots,x_{m-1},\alpha_{g(m)}\right) : \alpha_{g(m)}\in\mathbb{C}\right\}\subset\mathbb{C}[x_0,\dots,x_{m-1}]$$

yields the desired expansion. Finally, quotients $\left\{q_k(x_0,\dots,x_{m-1}) : k\in\mathbb{Z}_m\right\}$ lie in the polynomial ring $\mathbb{C}[x_0,\dots,x_{m-1}]$ since the polynomial $H(x_0,\dots,x_{m-1})-r(x_0,\dots,x_{m-1})$ lies in the ideal generated by members of the set $\left\{d(x_u) : u\in\mathbb{Z}_m\right\}$. $\square$

Proposition 1.3.15 (Ring Homomorphism). *For an arbitrary $H\in\mathbb{C}\left[x_0,\dots,x_{n-1}\right]$, let $\overline{H}$ denote the remainder of the congruence class*

$$H \text{ modulo the ideal generated by } \left\{d(x_i) : i\in\mathbb{Z}_n\right\},$$

where

$$d(x) = \prod_{i\in\mathbb{Z}_n}(x-\alpha_i) \ \text{ and } \ 0\neq\prod_{0\le u<v<n}(\alpha_v-\alpha_u),$$

Then the following hold:

(i) *For all $g\in\mathbb{Z}_n^{\mathbb{Z}_n}$, we have $\overline{H}(\alpha_g)=H(\alpha_g)$.*
(ii) *If $H=H_0+H_1$, where $H_0,H_1\in\mathbb{C}\left[x_0,\dots,x_{n-1}\right]$, then $\overline{H_0}+\overline{H_1}=\overline{H}$.*
(iii) *If $H=H_0\cdot H_1$, where $H_0,H_1\in\mathbb{C}\left[x_0,\dots,x_{n-1}\right]$, then $\overline{H}\equiv\overline{H_0}\cdot\overline{H_1}$.*

PROOF. The first claim follows from Proposition 1.3.1 for we see that the divisor vanishes over the lattice. To prove the second claim we recall that

$$\overline{H} = \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_n}} H(\alpha_g) \prod_{i\in\mathbb{Z}_n} \left(\prod_{j_i\in\mathbb{Z}_n\backslash\{g(i)\}} \left(\frac{x_i - \alpha_{j_i}}{\alpha_{g(i)} - \alpha_{j_i}} \right) \right),$$

$$\implies \overline{H} = \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_n}} \left(H_0(\alpha_g) + H_1(\alpha_g)\right) \prod_{i\in\mathbb{Z}_n} \left(\prod_{j_i\in\mathbb{Z}_n\backslash\{g(i)\}} \left(\frac{x_i - \alpha_{j_i}}{\alpha_{g(i)} - \alpha_{j_i}} \right) \right),$$

$$\implies \overline{H} = \sum_{k\in\mathbb{Z}_2} \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_n}} H_k(\alpha_g) \prod_{i\in\mathbb{Z}_n} \left(\prod_{j_i\in\mathbb{Z}_n\backslash\{g(i)\}} \left(\frac{x_i - \alpha_{j_i}}{\alpha_{g(i)} - \alpha_{j_i}} \right) \right).$$

Thus $\overline{H_0} + \overline{H_1} = \overline{H}$ as claimed. Finally the fact (iii) is a straightforward consequence of Proposition 1.3.16, which is proved next. □

PROPOSITION 1.3.16. *Let $f, g \in \mathbb{Z}_n^{\mathbb{Z}_n}$. For congruence classes prescribed modulo the ideal generated by $\{d(x_i) : i \in \mathbb{Z}_n\}$, if*

$$d(x) = \prod_{i\in\mathbb{Z}_n} (x - \alpha_i) \;\; \text{such that} \;\; 0 \neq \prod_{0\le u<v<n} (\alpha_v - \alpha_u),$$

then

$$L_f(\mathbf{x}) \cdot L_g(\mathbf{x}) \equiv \begin{cases} L_f(\mathbf{x}) & \text{if } f = g \\ 0 & \text{otherwise,} \end{cases}$$

PROOF. Observe that

$$L_f(\mathbf{x}) \cdot L_g(\mathbf{x}) \;=\; \prod_{i\in\mathbb{Z}_n} \left((c_{i,f} \frac{d(x_i)}{x_i - \alpha_{f(i)}})(c_{i,g} \frac{d(x_i)}{x_i - \alpha_{g(i)}}) \right),$$

where

$$c_{i,f} = \prod_{j_i\in\mathbb{Z}_n\backslash\{f(i)\}} \left(\alpha_{f(i)} - \alpha_{j_i}\right)^{-1} \quad \text{and} \quad c_{i,g} = \prod_{j_i\in\mathbb{Z}_n\backslash\{g(i)\}} \left(\alpha_{g(i)} - \alpha_{j_i}\right)^{-1}.$$

If $f \neq g$, then there exists $j \in \mathbb{Z}_n$ such that $f(j) \neq g(j)$ and $L_f(\mathbf{x}) \cdot L_g(\mathbf{x})$ is a multiple of $d(x_j)$, as a result of which we obtain $L_f(\mathbf{x}) \cdot L_g(\mathbf{x}) \equiv 0$. Alternatively if $f = g$, then

$$L_f(\mathbf{x}) \cdot L_g(\mathbf{x}) = \left(L_f(\mathbf{x})\right)^2 = L_f(\mathbf{x}) + \left(\left(L_f(\mathbf{x})\right)^2 - L_f(\mathbf{x}) \right).$$

We now show that $\left(L_f(\mathbf{x})\right)^2 - L_f(\mathbf{x}) \equiv 0$ modulo the ideal generated by $\{d(x_i) : i \in \mathbb{Z}_n\}$.

$$\begin{aligned} \left(L_f(\mathbf{x})\right)^2 - L_f(\mathbf{x}) \;&=\; L_f(\mathbf{x}) \left(L_f(\mathbf{x}) - 1\right) \\ &=\; L_f(\mathbf{x}) \left(L_f(\mathbf{x}) - \sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_n}} L_g(\mathbf{x}) \right) \\ &=\; -L_f(\mathbf{x}) \left(\sum_{g\in\mathbb{Z}_n^{\mathbb{Z}_n}\backslash\{f\}} L_g(\mathbf{x}) \right) \\ &\equiv\; 0, \end{aligned}$$

where the latter congruence identity stems from the prior setting where $f \neq g$. □

DEFINITION 1.3.17 (Polynomial of Grace). We define $P_f \in \mathbb{C}[x_0, \dots, x_{n-1}]$ for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ as follows:

$$P_f(\mathbf{x}) := \underbrace{\prod_{0\le u<v<n} (x_v - x_u)}_{V(x_0,\dots,x_{n-1})} \underbrace{\prod_{0\le u<v<n} \left((x_{f(v)} - x_v)^2 - (x_{f(u)} - x_u)^2\right)}_{E_f(x_0,\dots,x_{n-1})}. \tag{1.3.18}$$

DEFINITION 1.3.19 (Congruence class). For polynomials $P, Q \in \mathbb{C}[x_0, \dots, x_{n-1}]$, if

$$P(\mathbf{x}) \equiv Q(\mathbf{x}) \mod \left\{ \prod_{j \in \mathbb{Z}_n} (x_i - j) : i \in \mathbb{Z}_n \right\}, \tag{1.3.20}$$

we simply write $P \equiv Q$.

Unless otherwise stated, all subsequent congruence identities are prescribed modulo the ideal of polynomials generated by members of the set

$$\left\{ \prod_{j \in \mathbb{Z}_n} (x_i - j) : i \in \mathbb{Z}_n \right\}$$

PROPOSITION 1.3.21 (Certificate of Grace). *Let $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$. The functional directed graph G_f prescribed by f is graceful if and only if $P_f(\mathbf{x}) \not\equiv 0$.*

PROOF. Observe that the vertex Vandermonde factor $V(\mathbf{x})$ is of degree exactly $n-1$ in each variable and therefore equal to its remainder, i.e.,

$$V(\mathbf{x}) = \sum_{\theta \in \mathrm{S}_n} \mathrm{sgn}(\theta) \prod_{i \in \mathbb{Z}_n} (x_i)^{\theta(i)} = \prod_{v \in \mathbb{Z}_n} (v!) \sum_{\theta \in \mathrm{S}_n} \mathrm{sgn}(\theta) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{\theta(i)\}}} \left(\frac{x_i - j_i}{\theta(i) - j_i} \right), \tag{1.3.22}$$

where

$$\mathrm{sgn}(\theta) := \prod_{0 \le u < v < n} \left(\frac{\theta(v) - \theta(u)}{v - u} \right), \quad \forall\, \theta \in \mathrm{S}_n. \tag{1.3.23}$$

When $n > 2$, for every $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$, the induced edge label Vandermonde factor $E_f(\mathbf{x})$ is of degree $> (n-1)$ in some of its variables. Therefore, by Proposition 1.3.1, we have

$$E_f(\mathbf{x}) = \sum_{l \in \mathbb{Z}_m} q_l(\mathbf{x}) \prod_{k \in \mathbb{Z}_n} (x_l - k) + \prod_{v \in \mathbb{Z}_n} (v!) \frac{(n-1+v)!}{(2v)!} \sum_{\substack{g \in \mathbb{Z}_n^{\mathbb{Z}_n} \\ |gf - g| \in \mathrm{S}_n}} \mathrm{sgn}(|gf - g|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{g(i)\}}} (\frac{x_i - j_i}{g(i) - j_i}). \tag{1.3.24}$$

Observe that by the expansions in 1.3.22 and 1.3.24,

$$P_f(\mathbf{x}) = \sum_{l \in \mathbb{Z}_m} q_l(\mathbf{x}) V(\mathbf{x}) \prod_{k \in \mathbb{Z}_n} (x_l - k) +$$

$$\left(\prod_{v \in \mathbb{Z}_n} v! \sum_{\theta \in \mathrm{S}_n} \mathrm{sgn}(\theta) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{\theta(i)\}}} (\frac{x_i - j_i}{\theta(i) - j_i}) \right) \left(\prod_{v \in \mathbb{Z}_n} (v!) \frac{(n-1+v)!}{(2v)!} \sum_{\substack{g \in \mathbb{Z}_n^{\mathbb{Z}_n} \\ |gf - g| \in \mathrm{S}_n}} \mathrm{sgn}(|gf - g|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{g(i)\}}} (\frac{x_i - j_i}{g(i) - j_i}) \right).$$

is congruent to

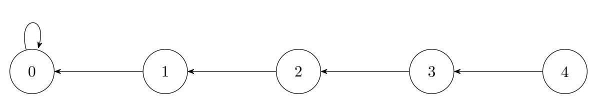
$$\prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \sum_{\substack{\sigma \in \mathrm{S}_n \\ \text{s.t.} \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma\, |\sigma f - \sigma|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}}} (\frac{x_i - j_i}{\sigma(i) - j_i}), \tag{1.3.25}$$

where the permutation $|\sigma f - \sigma|$ denotes the induced edge label permutation associated with a graceful relabeling $G_{\sigma f \sigma^{-1}}$ of G_f. The congruence above stems from Prop. 1.3.16. A graceful labeling necessitates the integer coefficient

$$\prod_{0 \le i < j < n} (j - i)(j^2 - i^2) = \prod_{0 \le i < j < n} (j - i)^2 (j + i) = \prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \neq 0,$$

thus establishing the desired claim. $\square$

EXAMPLE 1.3.26. We present an example of a path on 5 vertices. This is known to be graceful, so we expect a non-zero remainder.



Run the SageMath script `ex1325.sage` to verify.

1.4. The Composition Lemma

Proposition 1.4.1 (Composition Inequality). *Consider an arbitrary* $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ *subject to the fixed point condition* $\left|f^{(n-1)}\left(\mathbb{Z}_n\right)\right| = 1$. *The following statements are equivalent:*

(i)
$$\max_{\sigma \in S_n} \left|\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right| \leq \max_{\sigma \in S_n} \left|\{|\sigma f \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right|.$$

(ii)
$$P_{f^{(2)}}(\mathbf{x}) \not\equiv 0 \implies P_f(\mathbf{x}) \not\equiv 0.$$

(iii)
$$GrL(G_f) \neq \emptyset$$

Proof. If $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ is identically constant, then G_f is graceful. We see this from the fact that the functional digraph of the identically zero function is gracefully labeled and the fact that functional digraphs of identically constant functions are all isomorphic. It follows that all functional directed graphs having diameter less than 3 are graceful. Consequently, all claims hold for all functional digraphs of diameter less than 3. We now turn our attention to functional trees of diameter greater or equal to 3. It follows by definition

$$n = \max_{\sigma \in \mathrm{S}_n} \left|\{|\sigma f \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right| \iff P_f(\mathbf{x}) \not\equiv 0 \iff \mathrm{GrL}(G_f) \neq \emptyset. \tag{1.4.2}$$

We now proceed to show (i) $\iff$ (iii). The backward claim is the simplest of the two claims. We see that if f is contractive, so too is $f^{(2)}$. Then assertions

$$n = \max_{\sigma \in \mathrm{S}_n} \left|\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right| \text{ and } n = \max_{\sigma \in \mathrm{S}_n} \left|\{|\sigma f \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right| \tag{1.4.3}$$

indeed implies the inequality

$$\max_{\sigma \in \mathrm{S}_n} \left|\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right| \leq \max_{\sigma \in \mathrm{S}_n} \left|\{|\sigma f \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\}\right|. \tag{1.4.4}$$

We now establish the forward claim by contradiction. Assume for the sake of establishing a contradiction that for some contractive map $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ we have

$$n > \max_{\sigma \in \mathrm{S}_n} \left|\left\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|, \tag{1.4.5}$$

for we know by the number of edges being equal to n that it is impossible that

$$n < \max_{\sigma \in \mathrm{S}_n} \left|\left\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|. \tag{1.4.6}$$

Note that the range of f is a proper subset of $\mathbb{Z}_n$. By the premise that f is contractive, it follows that $f^{\left(\left\lceil 2^{\lg(n-1)}\right\rceil\right)}$ is identically constant and thus

$$n = \max_{\sigma \in \mathrm{S}_n} \left|\left\{|\sigma f^{\left(\left\lceil 2^{\lg(n-1)}\right\rceil\right)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|, \tag{1.4.7}$$

where lg denotes the logarithm base 2. Consequently there must be some integer $0 \leq \kappa < \lg(n-1)$ such that

$$\max_{\sigma \in \mathrm{S}_n} \left|\left\{|\sigma f^{(\lceil 2^{\kappa} \rceil)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right| > \max_{\sigma \in \mathrm{S}_n} \left|\left\{|\sigma f^{(\lceil 2^{\kappa-1} \rceil)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|. \tag{1.4.8}$$

This contradicts the assertion of statement (i), thereby establishing the backward claim. The exact same reasoning as above establishes (ii) $\iff$ (iii), for we have

$$P_{f^{\left(\left\lceil 2^{\lg(n-1)}\right\rceil\right)}}(\mathbf{x}) \not\equiv 0. \tag{1.4.9}$$

$\square$

Having assembled together the pieces required to prove our main result, we proceed to fit the pieces together to state and prove the *Composition Lemma*.

Lemma 1.4.10 (Composition Lemma). *For all contractive $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$, i.e., functions subject to the fixed point condition $\left|f^{(n-1)}\left(\mathbb{Z}_n\right)\right| = 1$, we have*

$$\max_{\sigma \in S_n} \left|\left\{|\sigma f^{(2)} \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right| \le \max_{\sigma \in S_n} \left|\left\{|\sigma f \sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|. \tag{1.4.11}$$

Proof. Owing to Proposition 1.4.1, we prove the statement by establishing

$$P_{f^{(2)}}(\mathbf{x}) \not\equiv 0 \implies P_f(\mathbf{x}) \not\equiv 0.$$

For simplicity, we prove a generalization of the desired claim. Assume without loss of generality that

$$f(i) > i, \ \forall\, i \in \mathbb{Z}_{n-1} \text{ and } f(n-1) = n-1.$$

Further assume without loss of generality that the vertex labeled 0 is at furthest edge distance from the root in G_f (i.e. the vertex labeled $n-1$). Given that the diameter of G_f is greater than 2, we may also assume without loss of generality that $f^{-1}\left(\{0\}\right) = \emptyset$ and $f^{(2)}(0) \ne f(0)$. Let the contractive map $g \in \mathbb{Z}_n^{\mathbb{Z}_n}$ be devised from f such that

$$g(i) = \begin{cases} f^{(2)}(i) & \text{if } i \in f^{-1}(\{f(0)\}) \\ f(i) & \text{otherwise} \end{cases}, \ \forall\, i \in \mathbb{Z}_n. \tag{1.4.12}$$

We show that

$$P_g(\mathbf{x}) \not\equiv 0 \implies P_f(\mathbf{x}) \not\equiv 0. \tag{1.4.13}$$

Note that the assertion immediately above generalizes the composition lemma since, f is only partially iterated. More precisely, we iterate f on the subset $f^{-1}(\{f(0)\})$. In turn, iterating (at most $n-1$ times) this generalization of the composition lemma yields that all functional trees are graceful, which in turn implies that the *Composition Lemma* as stated in Lemma 1.4.11 holds. For notational convenience, assume without loss of generality that

$$f^{-1}(\{f(0)\}) = \mathbb{Z}_{\left|f^{-1}\left(\{f(0)\}\right)\right|} \text{ and } f(0) = \left|f^{-1}(\{f(0)\})\right|. \tag{1.4.14}$$

If the conditions stated above are not met, we relabel the vertices of G_f to ensure that such is indeed the case. In the remainder of the proof let p be the smallest prime subject to $2n-1 \le p$. We consider the slight variant of the polynomial certificate construction given by

$$\mathcal{P}_f(\mathbf{x}) := \underbrace{\prod_{0 \le u < v < n} (x_v - x_u)}_{V(x_0,\dots,x_{n-1})} \underbrace{\prod_{i \in \mathbb{Z}_n} \Big(\prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} (x_i - j)\Big)}_{\mathcal{S}(x_0,\dots,x_{n-1})} \underbrace{\prod_{0 \le u < v < n} \left(\prod_{t \in \mathbb{Z}_2} \left((x_{f(v)} - x_v) + (-1)^t (x_{f(u)} - x_u)\right)\right)}_{E_f(x_0,\dots,x_{n-1})}.$$

In which case the canonical representative of the congruence class of $\mathcal{P}_f$ modulo the polynomials ideal generated by members of the set

$$\left\{ \prod_{j \in \mathbb{Z}_p} (x_i - j) : i \in \mathbb{Z}_n \right\}$$

is given by

$$\overline{\mathcal{P}_f}(\mathbf{x}) = \prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \prod_{i \in \mathbb{Z}_n} \Big(\prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} (i-j)\Big) \sum_{\substack{\sigma \in \mathrm{S}_n \\ \text{s.t.} \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \operatorname{sgn}(\sigma\, |\sigma f - \sigma|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_p \setminus \{\sigma(i)\}}} \Big(\frac{x_i - j_i}{\sigma(i) - j_i}\Big), \tag{1.4.15}$$

which is a polynomial of degree at most $p-1$ in each variable and

$$\prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \prod_{i \in \mathbb{Z}_n} \Big(\prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} (i-j)\Big) \not\equiv 0 \mod p.$$

A similar expansion holds for g, with the same coefficient up to sign. Next, roughly speaking, we show that there exist a in invertible linear transformation which maps $\mathcal{P}_f$ to $\mathcal{P}_g$ and vice versa. For an arbitrary $h \in \mathbb{Z}_n^{\mathbb{Z}_n}$ let $A_h \in \{0,1\}^{n \times n}$ denote the adjacency matrix of the functional directed graph G_h i.e.

$$A_h[u,v] = \begin{cases} 1 & \text{if } v = h(u) \\ 0 & \text{otherwise} \end{cases}, \quad \forall\, (u,v) \in \mathbb{Z}_n \times \mathbb{Z}_n\,.$$

Observe that signed incidence matrices $(A_{\text{id}} - A_f)$ and $(A_{\text{id}} - A_g)$ of G_f and G_g respectively are both in Row-Echelon form. Induced edge label binomials $x_i - x_{f(i)}$ and $x_i - x_{g(i)}$ correspond to the i-th entry of $(A_{\text{id}} - A_f) \cdot \mathbf{x}$ and $(A_{\text{id}} - A_g) \cdot \mathbf{x}$

respectively. Given that G_f is a functional tree, for each one of the $\binom{n}{2}$ vertex pair $(i,\, j)$ where $0 \le i < j < n$, there exist a unique $\mathbf{v}_{i,j} \in \{-1,0,1\}^{n\times 1}$ such that

$$(x_j - x_i) = \mathbf{v}_{i,j}^{\top} \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x}.$$

By introducing a distinct variable $y_{i,j}$ for each one of the $\binom{n}{2}$ vertex pair $(i,\, j)$ where $0 \le i < j < n$, we subsequently make use of the equality

$$y_{i,j}\,(x_j - x_i) = (y_{i,j}\mathbf{v}_{i,j})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x}.$$

in expressing the multiple of the vertex Vandermonde factor

$$\prod_{0\le i<j<n} y_{i,j}\,(x_j - x_i) = \prod_{0\le i<j<n} ((y_{i,j}\mathbf{v}_{i,j})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x}).$$

Similarly the absolute induced edge label Vandermonde factor is expressed by

$$\prod_{0\le u<v<n} \left(\prod_{t\in\mathbb{Z}_2} ((x_{f(v)} - x_v) + (-1)^t (x_{f(u)} - x_u)) \right) = \prod_{0\le i<j<n} \prod_{t\in\mathbb{Z}_2} \Big((A_{\text{id}}[j,:] \cdot (A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[i,:] \cdot (A_{\text{id}} - A_f)) \cdot \mathbf{x} \Big).$$

Let

$$\mathcal{P}_f(\mathbf{x}, Y) :=$$
$$\prod_{0\le i<j<n} ((y_{i,j}\mathbf{v}_{i,j})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x})\, \mathcal{S}(x_0, \dots, x_{n-1}) \prod_{0\le i<j<n} \prod_{t\in\mathbb{Z}_2} \Big((A_{\text{id}}[j,:] \cdot (A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[i,:] \cdot (A_{\text{id}} - A_f)) \cdot \mathbf{x} \Big).$$

We bypass ring homomorphisms from $\mathbb{Q}[x_0, \dots, x_{n-1}]$ to the quotient ring $\mathbb{Q}[x_0,\dots,x_{n-1}]/\text{Ideal generated by } \left\{ \prod_{j\in\mathbb{Z}_p} (x_i - j) : i \in \mathbb{Z}_n \right\}$ in our analysis by switching the ground field from $\mathbb{Q}$ to the Galois field of order p. More precisely we work over the ring $(\mathbb{Z}/p\mathbb{Z})[x_0, \dots, x_{n-1}]$ instead of $\mathbb{Q}[x_0, \dots, x_{n-1}]$. Over the said ring the polynomial $\mathcal{P}_f(\mathbf{x})$ is indistinguishable from $\overline{\mathcal{P}_f}(\mathbf{x})$ in 1.4.15. In order for variables to be consistently treated by our proposed linear transformation, we re-express the polynomial $\mathcal{P}_f(\mathbf{x}, Y)$ by replacing the factor $\mathcal{S}(x_0, \dots, x_{n-1})$ with an expression featuring instead

$$\mathcal{S}_r(x_0, \dots, x_{r-1}, x_r, x_{r+1}, \dots, x_{n-1}, Y) := \prod_{i<r} \Bigg(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n} (-\,y_{i,r}\,(x_r - x_i) - j\,y_{i,r}) \Bigg) \prod_{i>r} \Bigg(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n} (y_{r,i}\,(x_i - x_r) - j\,y_{r,i}) \Bigg),$$

for all $r \in \mathbb{Z}_n$. In other words

$$\mathcal{S}_r(x_0, \dots, x_{r-1}, x_r, x_{r+1}, \dots, x_{n-1}, Y) =$$
$$\prod_{i<r} \left(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n} \left(-\,(y_{i,r}\mathbf{v}_{i,r})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ x_r \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} - j\,y_{i,r}\right) \right) \prod_{i>r} \left(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n} \left((y_{r,i}\mathbf{v}_{r,i})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ x_r \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} - j\,y_{r,i}\right) \right)$$

Over the chosen ring the following equality holds

$$\mathcal{P}_f(\mathbf{x}, Y) = \sum_{r\in\mathbb{Z}_n} \mathcal{P}_f\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, Y \right)$$

$$\implies \mathcal{P}_f(\mathbf{x}, Y) = \sum_{r\in\mathbb{Z}_n} \prod_{0\le i<j<n} \left((y_{i,j}\mathbf{v}_{i,j})^{\top} \cdot (A_{\text{id}} - A_f) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}\right) \mathcal{S}_r(x_0, \dots, x_{r-1}, 0, x_{r+1}, \dots, x_{n-1}, Y) \times$$

$$\prod_{0\le i<j<n}\prod_{t\in\mathbb{Z}_2}\left(\left(A_{\text{id}}[j,:]\cdot(A_{\text{id}}-A_f)+(-1)^t A_{\text{id}}[i,:]\cdot(A_{\text{id}}-A_f)\right)\cdot\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\right).$$

Thus we have expressed $\mathcal{P}_f(\mathbf{x},Y)$ as a polynomial in the entries of Y as well as the $\binom{n}{2}$ binomials x_j-x_i where $0\le i<j<n$. Albeit the factor $\mathcal{S}_r$ features binomials x_r-x_i when $i<r$ as well as binomials x_i-x_r when $r<i$ where the variable x_r is evaluated to zero.

Observe that the set of row linear combinations

$$\text{Row}_{f(0)}+\text{Row}_i\longrightarrow\text{Row}_i,\ \forall\, i\in f^{-1}(\{f(0)\}).$$

converts the incidence matrix $A_{\text{id}}-A_f$ to the incidence matrix $A_{\text{id}}-A_g$. These row operations are in turn expressed in terms of left elementary matrix action as follows

$$\left(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\right)\cdot(A_{\text{id}}-A_f)=(A_{\text{id}}-A_g).$$

Consider the invertible linear transformation which effects simultaneous maps

$$\mathbf{x}\mapsto\left(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\right)\cdot\mathbf{x}\text{ and }y_{i,j}\mathbf{v}_{i,j}^{\top}\mapsto y_{i,j}\mathbf{v}_{i,j}^{\top}\cdot\left(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}-A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\right).$$

In other words the vector

$$\begin{pmatrix}\mathbf{x}\\ y_{0,1}\mathbf{v}_{0,1}\\ \vdots\\ y_{i,j}\mathbf{v}_{i,j}\\ \vdots\\ y_{n-2,n-1}\mathbf{v}_{n-2,n-1}\end{pmatrix}$$

is mapped to

$$\left(\Big(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\Big)\oplus\left(I_{\binom{n}{2}}\otimes\Big(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}-A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\Big)^{\top}\right)\right)\cdot\begin{pmatrix}\mathbf{x}\\ y_{0,1}\mathbf{v}_{0,1}\\ \vdots\\ y_{i,j}\mathbf{v}_{i,j}\\ \vdots\\ y_{n-2,n-1}\mathbf{v}_{n-2,n-1}\end{pmatrix}.$$

Thus resulting in a map of $\mathcal{P}_f(\mathbf{x},Y)$ to $\mathcal{P}_g(\mathbf{x},Y)$ for all $\mathbf{x}\in(\mathbb{Z}/p\mathbb{Z})^{n\times 1}$. If the induced function

$$\mathcal{P}_f(\mathbf{x},Y)=F_f(y_{0,1}\mathbf{v}_{0,1},\dots,y_{i,j}\mathbf{v}_{i,j},\dots,y_{n-2,n-1}\mathbf{v}_{n-2,n-1})$$

vanishes identically in the ring $(\mathbb{Z}/p\mathbb{Z})[y_{0,1},\dots,y_{n-2,\,n-1}]$ then for all

$$\left(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\right)\cdot\mathbf{x}\in(\mathbb{Z}/p\mathbb{Z})^{n\times 1},$$

the corresponding induced polynomials also vanishes identically in the ring $(\mathbb{Z}/p\mathbb{Z})[y_{0,1},\dots,y_{n-2,\,n-1}]$. For we see that

$$\mathcal{P}_f(\mathbf{x},Y)=\mathcal{P}_f\left(\Big(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\Big)\cdot\Big(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\Big)^{-1}\cdot\mathbf{x},Y\right)$$

$$=\mathcal{P}_f\left(\Big(\prod_{i\in f^{-1}\left(\{f(0)\}\right)}(A_{\text{id}}+A_{\text{id}}[:,i]\cdot A_{\text{id}}[f(0),:])\Big)\cdot\mathbf{x}',Y\right),$$

where $\mathbf{x}' \in (\mathbb{Z}/p\mathbb{Z})^{n\times 1}$ in the equality immediately above is such that

$$\mathbf{x}' = \Big(\prod_{i\in f^{-1}(\{f(0)\})} (A_{\mathrm{id}} + A_{\mathrm{id}}[:,i]\cdot A_{\mathrm{id}}[f(0),:])\Big)^{-1}\cdot \mathbf{x} = \Big(\prod_{i\in f^{-1}(\{f(0)\})} (A_{\mathrm{id}} - A_{\mathrm{id}}[:,i]\cdot A_{\mathrm{id}}[f(0),:])\Big)\cdot \mathbf{x}.$$

Thus the ring isomorphism which maps the induced $F_f(y_{0,1}\mathbf{v}_{0,1},\dots,y_{n-2,n-1}\mathbf{v}_{n-2,n-1})$ in $(\mathbb{Z}/p\mathbb{Z})[y_{0,1},\dots,y_{n-2,\,n-1}]$ to its image

$$F_f\left(\Big(\prod_{i\in f^{-1}(\{f(0)\})} (A_{\mathrm{id}} - A_{\mathrm{id}}[:,i]\cdot A_{\mathrm{id}}[f(0),:])\Big)^{\top} y_{0,1}\mathbf{v}_{0,1},\dots,\Big(\prod_{i\in f^{-1}(\{f(0)\})} (A_{\mathrm{id}} - A_{\mathrm{id}}[:,i]\cdot A_{\mathrm{id}}[f(0),:])\Big)^{\top} y_{n-2,n-1}\mathbf{v}_{n-2,n-1}\right),$$

ensures that the image induced polynomial function of vectors vanish identically if its pre-image vanishes identically for all

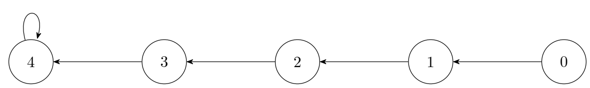
$$\left(\prod_{i\in f^{-1}(\{f(0)\})} (A_{\mathrm{id}} + A_{\mathrm{id}}[:,i]\cdot A_{\mathrm{id}}[f(0),:])\right)\cdot \mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^{n\times 1}.$$

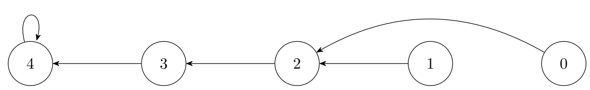
By which if $\mathcal{P}_g(\mathbf{x},Y)$ admits a non-vanishing point for some assignment of $\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^{n\times 1}$ then $\mathcal{P}_f(\mathbf{x},Y)$ also admits a non-vanishing point for some assignment of $\mathbf{x} \in (\mathbb{Z}/p\mathbb{Z})^{n\times 1}$ which yields in turn that

$$\Big(P_g(\mathbf{x}) \not\equiv 0 \mod \big\{\prod_{j\in\mathbb{Z}_n}(x_i - j) : i \in \mathbb{Z}_n\big\}\Big) \implies \Big(P_f(\mathbf{x}) \not\equiv 0 \mod \big\{\prod_{j\in\mathbb{Z}_n}(x_i - j) : i \in \mathbb{Z}_n\big\}\Big)$$

as claimed. □

Example 1.4.16. The figure below illustrates the local iteration described in the proof of Lemma 1.4.10 with an example of a path on 5 vertices.

G_f :


G_g :


Bibliography

[1] Parikshit Chalise, Antwan Clark, and Edinah K. Gnang. Every tree on n edges decomposes $k_{nx,nx}$ and k_{2nx+1}, 2024.
[2] Parikshit Chalise, Antwan Clark, and Edinah K. Gnang. A proof of the tree packing conjecture, 2024.
[3] Edinah K. Gnang. On graceful labelings of trees, 2020.
[4] Edinah K. Gnang. On the composition lemma, 2022.
[5] Edinah K. Gnang. A proof of the kotzig-ringel-rosa conjecture, 2023.