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 first n natural numbers, 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:

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

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

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

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

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

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

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

then for an arbitrary $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ the complementary labeling involution is defined as the map

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

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

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

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

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

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. □

For notational convenience, we denote by $L_g(\mathbf{x})$ the Lagrange basis polynomial associated with $g\in\mathbb{Z}_n^{\mathbb{Z}_n}$

$$L_g(\mathbf{x}) := \prod_{i\in\mathbb{Z}_n}\left(\prod_{j_i\in\mathbb{Z}_n\setminus\{g(i)\}}\left(\frac{x_i-\alpha_{j_i}}{\alpha_{g(i)}-\alpha_{j_i}}\right)\right)$$

and for any $S\subseteq\mathbb{Z}_n$ we denote by $L_g(\mathbf{x}|_S)$ the factor of $L_g(\mathbf{x})$ which only features variables indexed by S as follows

$$L_g(\mathbf{x}|_S) := \prod_{i\in S}\left(\prod_{j_i\in\mathbb{Z}_n\setminus\{g(i)\}}\left(\frac{x_i-\alpha_{j_i}}{\alpha_{g(i)}-\alpha_{j_i}}\right)\right)$$

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

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

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

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

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 $(x_j)^{\underline{n}}$, 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 $\{d(x_i): i\in\mathbb{Z}_n\}$.

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

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

Lemma 1.3.17 (Symmetrization Lemma). *Let $P,\, F \in \mathbb{Q}[x_0, \dots, x_{n-1}]$ and distinct subsets $\mathcal{S}_u \subseteq \mathbb{Z}_n$ for all $u \in \mathbb{Z}_m$. For positive integers $\{D_u : u \in \mathbb{Z}_m\}$, let*

$$P(\mathbf{x}) = F(\mathbf{x}) \sum_{j\in\mathbb{Z}_m} \Big(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} (x_i)^{g(i)} \Big), \tag{1.3.18}$$

such that for some integer κ, $F(\alpha_{f\tau^{-1}}) = (-1)^\kappa F(\alpha_f)$ for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$, where τ denotes a transposition which exchanges a pair of variables. If $F(\alpha_f) = 0$ for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n} \backslash S_n$ and none of the non-vanishing orbits

$$\left\{ \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) F(\alpha_\sigma) L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\overline{\mathcal{S}_j}}) \not\equiv 0 : \begin{array}{c} (\sigma, h_j) \in S_n \times (\mathbb{Z}_n)^{\mathcal{S}_j} \\ \textit{where} \\ \sigma|_{\mathcal{S}_j} = h_j \end{array} \right\}$$

is fixed by τ when $\mathcal{S}_j \subseteq \mathbb{Z}_n$ indexes only one of the variables exchanged by τ. Then

$$\tau \in \mathit{Aut}(\,\overline{P}(\mathbf{x})) \implies \tau \in \mathit{Aut}\left(\sum_{\sigma\in S_n} F(\alpha_\sigma) \sum_{j\in\mathbb{Z}_m} \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) \right)$$

Proof. Observe that

$$\sum_{j\in\mathbb{Z}_m} \Big(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} (x_i)^{g(i)} \Big) \equiv \sum_{j\in\mathbb{Z}_m} \sum_{h_j\in\mathbb{Z}_n^{\mathcal{S}_j}} \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{h_j(i)}\right)^{g(i)} \right) L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}).$$

By our premise $\overline{F}(\alpha_{f\tau^{-1}}) = -\overline{F}(\alpha_f)$ for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ or alternatively $\overline{F}(\alpha_{f\tau^{-1}}) = \overline{F}(\alpha_f)$ for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$. Furthermore by the premise that $F(\alpha_f)$ vanishes for all $f \in \mathbb{Z}_n^{\mathbb{Z}_n} \backslash \mathrm{S}_n$,

$$\overline{P} \equiv \Big(\sum_{\sigma\in\mathrm{S}_n} F(\alpha_\sigma)\, L_\sigma(\mathbf{x}) \Big) \sum_{j\in\mathbb{Z}_m} \sum_{h_j\in\mathbb{Z}_n^{\mathcal{S}_j}} \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{h_j(i)}\right)^{g(i)} \right) L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}) =$$

$$\sum_{j\in\mathbb{Z}_m} \sum_{(\sigma,h_j)\in\mathrm{S}_n\times\mathbb{Z}_n^{\mathcal{S}_j}} \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{h_j(i)}\right)^{g(i)} \right) F(\alpha_\sigma)\, L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}),$$

where $\overline{\mathcal{S}_j} := \mathbb{Z}_n \setminus \mathcal{S}_j$. Recall that $\mathrm{Aut}(L_\sigma(\mathbf{x})) = \{\mathrm{id}\}$ for all $\sigma \in \mathrm{S}_n$. Each summamnd in the latter sum above of the form

$$\left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{h_j(i)}\right)^{g(i)} \right) F(\alpha_\sigma) L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\overline{\mathcal{S}_j}}),$$

is either congruent to zero in which case the said summand play no role in ascertaining $\mathrm{Aut}(\overline{P})$. Alternatively the said summand is not congruent to zero and is a member of a non-vanishing orbit of summands:

$$\left\{ \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) F(\alpha_\sigma) \underbrace{L_{h_j}(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\overline{\mathcal{S}_j}})}_{\equiv L_\sigma(\mathbf{x})} \not\equiv 0 : \begin{array}{c} (\sigma, h_j) \in \mathrm{S}_n \times (\mathbb{Z}_n)^{\mathcal{S}_j} \\ \text{where} \\ \sigma|_{\mathcal{S}_j} = h_j \end{array} \right\}$$

which by contrast imposes non-trivial constraints on permutations which lie in the automorphism group of $\overline{P}$. Therefore the remainder of such summand must be accounted for when determining $\mathrm{Aut}(\overline{P})$. If τ lies in the automorphism group of $\overline{P}$ then there are two cases to consider for each indexing set $\mathcal{S}_j$. In the first case both variables interchanged by the transposition τ either lie in $\mathcal{S}_j$ or both lie in its complement $\overline{\mathcal{S}_j}$. In this setting the non-vanishing orbit of summands

$$\left\{ \left(\sum_{g\in(1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i\in\mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) F(\alpha_\sigma)\, L_\sigma(\mathbf{x}) : \begin{array}{c} (\sigma, h_j) \in \mathrm{S}_n \times (\mathbb{Z}_n)^{\mathcal{S}_j} \\ \text{where} \\ \sigma|_{\mathcal{S}_j} = h_j \end{array} \right\}$$

is up to signed fixed by the transposition τ. Otherwise, in the setting where $\mathcal{S}_j$ indexes only one of the variables exchanged by τ, by our premise, τ induces a transposition of the non-vanishing orbit of summands

$$\left\{ \left(\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) F(\alpha_\sigma)\, L_\sigma(\mathbf{x}) : \begin{array}{c} (\sigma, h_j) \in \mathrm{S}_n \times (\mathbb{Z}_n)^{\mathcal{S}_j} \\ \text{where} \\ \sigma|_{\mathcal{S}_j} = h_j \end{array} \right\}$$

with some other non-vanishing orbit of summands say

$$\left\{ \left(\sum_{g \in (1+\mathbb{Z}_{D_k})^{\mathcal{S}_k}} c_{k,g} \prod_{i \in \mathcal{S}_k} \left(\alpha_{\gamma(i)}\right)^{g(i)} \right) F(\alpha_\gamma) L_\gamma(\mathbf{x}) : \begin{array}{c} (\gamma, h_k) \in \mathrm{S}_n \times (\mathbb{Z}_n)^{\mathcal{S}_k} \\ \text{where} \\ \gamma|_{\mathcal{S}_k} = h_k \end{array} \right\}.$$

Thus pairing by this interchange $\mathcal{S}_j$ with $\mathcal{S}_k$ and vice versa, where $\tau(\mathcal{S}_j) = \mathcal{S}_k$. Observe that

$$\overline{P}(\mathbf{x}) = \sum_{\sigma \in \mathrm{S}_n} F(\alpha_\sigma) \sum_{j \in \mathbb{Z}_m} \left(\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\overline{\mathcal{S}_j}}) \tag{1.3.19}$$

and the associated symmetrized polynomial is

$$\sum_{\sigma \in \mathrm{S}_n} F(\alpha_\sigma) \sum_{j \in \mathbb{Z}_m} \left(\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) \sum_{h \in \mathbb{Z}_n^{\overline{\mathcal{S}_j}}} L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_h(\mathbf{x}|_{\overline{\mathcal{S}_j}}).$$

Note that to obtain the symmetrized polynomial, for each $\sigma \in \mathrm{S}_n$, in equation (1.3.19) within the j-th summand for each $j \in \mathbb{Z}_m$, we have replaced the Lagrange basis

$$L_\sigma(\mathbf{x}) = L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_\sigma(\mathbf{x}|_{\overline{\mathcal{S}_j}})$$

with the sum over Lagrange bases polynomials

$$\sum_{f \in \mathbb{Z}_n^{\overline{\mathcal{S}_j}}} L_\sigma(\mathbf{x}|_{\mathcal{S}_j}) L_f(\mathbf{x}|_{\overline{\mathcal{S}_j}}).$$

Each such sum over Lagrange bases is taken as a block. Observe the blocks are themselves subject to the same orbit pairing argument described above. Thus τ also fixes the symmetrized polynomial. By properties of Lagrange basis polynomials it follows that the symmetrized polynomial equals

$$\sum_{\sigma \in \mathrm{S}_n} F(\alpha_\sigma) \sum_{j \in \mathbb{Z}_m} \left(\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} \left(\alpha_{\sigma(i)}\right)^{g(i)} \right) L_\sigma(\mathbf{x}|_{\mathcal{S}_j}).$$

By which we conclude that the desired claim holds. □

Remark: Note that for a summand

$$\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} (x_i)^{g(i)},$$

it is possible that its evaluations be τ-invariant over non-vanishing evaluations points of F despite $\mathcal{S}_j$ indexing only one of the variables exchanged by τ. This τ-invariance of evaluation implies that the associated orbit is also τ-invariant. For instance take

$$F = \frac{(x_0 + x_1 - 1)(x_0 + x_1 - 2)(x_0 + x_1 - 3)(x_0 + x_1 - 4)}{(5-1)\,(5-2)\,(5-3)\,(5-4)} \prod_{0 \le i < j < 4} (x_j - x_i)^2.$$

Let the chosen summand taken from the second factor be such that

$$\left(\sum_{g \in (1+\mathbb{Z}_{D_j})^{\mathcal{S}_j}} c_{j,g} \prod_{i \in \mathcal{S}_j} (x_i)^{g(i)} \right) = x_0^2 - 5x_0.$$

By construction the factor F is non vanishing over S_4 if and only if is $x_0 + x_1 = 5$. Let τ denote the transposition which exchanges 0 and 1. We see that the subset $\mathcal{S}_j = \{0\}$, indexes only the variable x_0. However evaluations of the summand are τ-invariant over points in S_4 where F is non-vanishing. This fact obstructs the variable restriction in this summand. The observation also explain the need for the premise that each orbits be non-trivially transposed by τ. In practice, however one easily by gets around this obstacle. We avoid this particular obstruction to the restriction by exploiting the τ-invariance of F. Averaging the summand over the τ-action enables us to replace the summand within the second factor with a τ-invariant polynomial which no longer obstruct the restriction. Crucially this substitution preserves evaluations of the summand. As a result of this substitution, the new polynomial reflects the τ-invariance of the summand and no longer obstructs the variable restriction. In our example we can replace the polynomial $x_0^2 - 5x_0$ with the polynomial $\frac{(x_0^2-5x_0)+(x_1^2-5x_1)}{2}$. The replacement results in partner summand associated with $\mathcal{S}'_j = \{1\}$. In summary if we effect the replacement described above to all summands whose orbit are fixed by τ and whose set indexes only one of the variables exchanged by τ, then the resulting polynomial remains congruent to P and is such that the variable restrictions described in the lemma can be applied to all its summands.

Definition 1.3.20 (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:

$$P_f(\mathbf{x}) := \underbrace{\prod_{0\le u<v<n} (x_v - x_u)}_{V(x_0,\dots,x_{n-1})} \underbrace{\prod_{0\le u<v<n} \left((x_{f(v)} - x_v)^2 - (x_{f(u)} - x_u)^2\right)}_{E_f(x_0,\dots,x_{n-1})}. \tag{1.3.21}$$

Definition 1.3.22 (Congruence class). For polynomials $P, Q \in \mathbb{C}[x_0, \dots, x_{n-1}]$, if

$$P(\mathbf{x}) \equiv\ Q(\mathbf{x}) \quad \mathrm{mod} \left\{ \prod_{j\in\mathbb{Z}_n} (x_i - j) : i \in \mathbb{Z}_n \right\}, \tag{1.3.23}$$

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 1.3.24 (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.,

$$V(\mathbf{x}) = \sum_{\theta\in \mathrm{S}_n} \mathrm{sgn}(\theta) \prod_{i\in\mathbb{Z}_n} (x_i)^{\theta(i)} = \prod_{v\in\mathbb{Z}_n} (v!) \sum_{\theta\in \mathrm{S}_n} \mathrm{sgn}(\theta) \prod_{\substack{i\in\mathbb{Z}_n \\ j_i\in\mathbb{Z}_n\setminus\{\theta(i)\}}} \left(\frac{x_i - j_i}{\theta(i) - j_i}\right), \tag{1.3.25}$$

where

$$\mathrm{sgn}(\theta) := \prod_{0\le u<v<n} \left(\frac{\theta(v) - \theta(u)}{v-u}\right), \quad \forall\, \theta \in \mathrm{S}_n. \tag{1.3.26}$$

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

$$E_f(\mathbf{x}) = \sum_{l\in\mathbb{Z}_m} q_l(\mathbf{x}) \prod_{k\in\mathbb{Z}_n} (x_l - k) + \prod_{v\in\mathbb{Z}_n} (v!) \frac{(n-1+v)!}{(2v)!} \sum_{\substack{g\,\in\, \mathbb{Z}_n^{\mathbb{Z}_n} \\ |gf-g|\,\in\, \mathrm{S}_n}} \mathrm{sgn}(|gf-g|) \prod_{\substack{i\in\mathbb{Z}_n \\ j_i\in\mathbb{Z}_n\setminus\{g(i)\}}} (\frac{x_i - j_i}{g(i) - j_i}). \tag{1.3.27}$$

Observe that by the expansions in 1.3.25 and 1.3.27,

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

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

is congruent to

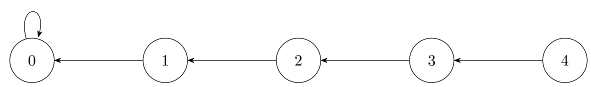
$$\prod_{v\in\mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \sum_{\substack{\sigma\in\mathrm{S}_n \\ \text{s.t.} \\ |\sigma f-\sigma|\in\mathrm{S}_n}} \mathrm{sgn}(\sigma\, |\sigma f - \sigma|) \prod_{\substack{i\in\mathbb{Z}_n \\ j_i\in\mathbb{Z}_n\setminus\{\sigma(i)\}}} (\frac{x_i - j_i}{\sigma(i) - j_i}), \tag{1.3.28}$$

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 1.3.29. 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.

PROPOSITION 1.3.30 (Complementary Labeling Symmetry). *Let $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ and the remainder of P_f be*

$$\overline{P}_f(\mathbf{x}) := \prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \sum_{\substack{\sigma \in S_n \\ s.t. \\ |\sigma f - \sigma| \in S_n}} sgn(\sigma\,|\sigma f - \sigma|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \backslash \{\sigma(i)\}}} \left(\frac{x_i - j_i}{\sigma(i) - j_i}\right). \tag{1.3.31}$$

The complementary labeling map $x_i \mapsto x_{n-1-i}$, for all $i \in \mathbb{Z}_n$, fixes $\overline{P}_f$ up to sign.

PROOF. For notational convenience, let $\mathbf{x}_\varphi := (x_{\varphi(0)}, \dots, x_{\varphi(i)}, \dots, x_{\varphi(n-1)})$. Observe that for any permutation $\varphi \in \mathrm{S}_n$, the action of φ on P_f yields equalities

$$\begin{aligned} P_f(\mathbf{x}_\varphi) &= \prod_{0 \le u < v < n} (x_{\varphi(v)} - x_{\varphi(u)})\big((x_{\varphi f(v)} - x_{\varphi(v)})^2 - (x_{\varphi f(u)} - x_{\varphi(u)})^2\big), \\ &= \prod_{0 \le \varphi^{-1}(i) < \varphi^{-1}(j) < n} (x_j - x_i)\big((x_{\varphi f \varphi^{-1}(j)} - x_j)^2 - (x_{\varphi f \varphi^{-1}(i)} - x_i)^2\big). \end{aligned}$$

The last equality above features the indexing change of variable $u = \varphi^{-1}(i)$ and $v = \varphi^{-1}(j)$. If $\varphi \in \mathrm{Aut}\left(G_f\right)$ then $P_f(x_{\varphi(0)}, \dots, x_{\varphi(n-1)})$ is up to sign equal to $P_{\varphi f \varphi^{-1}}$, in accordance with Definition 1.3.20. Furthermore, by the proof of Proposition 1.3.24, the action of φ on P_f yields the congruence identity

$$P_f(\mathbf{x}_\varphi) \equiv \overline{P}_f(\mathbf{x}_\varphi).$$

Hence,

$$\begin{aligned} \overline{P}_f(\mathbf{x}_\varphi) &= \prod_{v \in \mathbb{Z}_n} \left((v!)^2 \frac{(n-1+v)!}{(2v)!}\right) \sum_{\substack{\sigma \in \mathrm{S}_n \\ \mathrm{s.t.} \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma\,|\sigma f - \sigma|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \backslash \{\sigma(i)\}}} \left(\frac{x_{\varphi(i)} - j_i}{\sigma(i) - j_i}\right), \\ &= \mathrm{sgn}(\varphi) \prod_{v \in \mathbb{Z}_n} \left((v!)^2 \frac{(n-1+v)!}{(2v)!}\right) \sum_{\substack{\sigma \in \mathrm{S}_n \\ \mathrm{s.t.} \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma\,|\sigma f - \sigma|\,\varphi^{-1}) \prod_{\substack{u \in \mathbb{Z}_n \\ v_u \in \mathbb{Z}_n \backslash \{\sigma\varphi^{-1}(u)\}}} \left(\frac{x_u - v_u}{\sigma\varphi^{-1}(u) - v_u}\right). \end{aligned}$$

If $\varphi = n - 1 - \mathrm{id}$, then, by the complementary labeling symmetry, we have

$$G_{\sigma f \sigma^{-1}} \in \mathrm{GrL}\left(G_f\right) \iff G_{\sigma \varphi^{-1} f (\sigma \varphi^{-1})^{-1}} \in \mathrm{GrL}\left(G_f\right)$$

Let $\mathfrak{G}$ denote the subrgoup of S_n whose members are $\{\mathrm{id},\ \varphi\}$. We write

$$\overline{P}_f(\mathbf{x}_\varphi) =$$

$$\prod_{v \in \mathbb{Z}_n} \left((v!)^2 \frac{(n-1+v)!}{(2v)!}\right) \sum_{\substack{\sigma \in \mathrm{S}_n / \mathfrak{G} \\ \gamma = |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma\gamma) \left(\mathrm{sgn}(\varphi^{-1}) \prod_{\substack{u \in \mathbb{Z}_n \\ v_u \in \mathbb{Z}_n \backslash \{\sigma(u)\}}} \left(\frac{x_u - v_u}{\sigma(u) - v_u}\right) + \prod_{\substack{u \in \mathbb{Z}_n \\ v_u \in \mathbb{Z}_n \backslash \{\sigma\varphi^{-1}(u)\}}} \left(\frac{x_u - v_u}{\sigma\varphi^{-1}(u) - v_u}\right)\right).$$

Similarly,

$$\overline{P}_f(\mathbf{x}) =$$

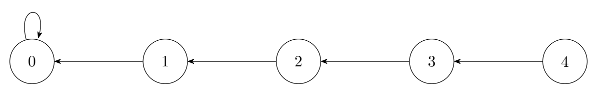
$$\prod_{v\in\mathbb{Z}_n}((v!)^2\frac{(n-1+v)!}{(2v)!})\sum_{\substack{\sigma\in\mathrm{S}_n/\mathfrak{G}\\ \gamma=|\sigma f-\sigma|\in\mathrm{S}_n}}\mathrm{sgn}(\sigma\gamma)\left(\prod_{\substack{i\in\mathbb{Z}_n\\ j_i\in\mathbb{Z}_n\backslash\{\sigma(i)\}}}(\frac{x_i-j_i}{\sigma(i)-j_i})+\mathrm{sgn}(\varphi^{-1})\prod_{\substack{i\in\mathbb{Z}_n\\ j_i\in\mathbb{Z}_n\backslash\{\sigma\varphi^{-1}(i)\}}}(\frac{x_i-j_i}{\sigma\varphi^{-1}(i)-j_i})\right).$$

We conclude that the complementary labeling symmetry yields the equality

$$\overline{P}_f(\mathbf{x})=\mathrm{sgn}(\varphi)\,\overline{P}_f(\mathbf{x}_\varphi)=\overline{P}_{\varphi f\varphi^{-1}}(\mathbf{x}),$$

thus establishing the desired claim. □

Example 1.3.32. We present an example of a path on 5 vertices.



Run the SageMath script `ex1328.sage` to verify.

Lemma 1.3.33 (Variable Dependency). *Let $P\in\mathbb{Q}[x_0,\dots,x_{n-1}]$ and $S\subsetneq\mathbb{Z}_n$. If*

$$P(\mathbf{x})=\sum_{g\in\mathbb{Z}_n^S}c_g\prod_{i\in S}(x_i)^{g(i)},\tag{1.3.34}$$

where $c_g\in\mathbb{C}$ for all $g\in\mathbb{Z}_n^S$, then for any positive integer m, the polynomial $\left(P(\mathbf{x})\right)^m$ admits a quotient-remainder expansion of the form

$$\left(P(x_0,\dots,x_{n-1})\right)^m=\sum_{j\in S}q_j(x_0,\dots,x_{n-1})\prod_{k\in\mathbb{Z}_n}(x_j-\alpha_k)+\sum_{g\in\mathbb{Z}_n^S}a_g\prod_{i\in S}(x_i)^{g(i)}\tag{1.3.35}$$

where $\alpha_k,a_g\in\mathbb{C}$ for all $k\in\mathbb{Z}_n$ such that $n=\left|\{\alpha_k:k\in\mathbb{Z}_n\}\right|$and $g\in\mathbb{Z}_n^S$.

Proof. By the premise, the polynomial $P(\mathbf{x})$ is of degree at most $n-1$ in its variables. Thus by Proposition 1.3.1, the polynomial $P(\mathbf{x})$ is equal to its remainder, i.e.,

$$P(\mathbf{x})\;=\;\sum_{g\in\mathbb{Z}_n^S}c_g\prod_{i\in S}(x_i)^{g(i)}\;=\;\sum_{g\in\mathbb{Z}_n^S}P(g)\prod_{\substack{i\in S\\ j_i\in\mathbb{Z}_n\backslash\{g(i)\}}}\left(\frac{x_i-\alpha_{j_i}}{\alpha_{g(i)}-\alpha_{j_i}}\right).\tag{1.3.36}$$

The remainder of $(P(\mathbf{x}))^m$ is obtained by repeatedly replacing each occurrence of $(x_i)^n$ with $(x_i)^n-\prod_{k\in\mathbb{Z}_n}(x_i-\alpha_k)$, followed by expanding the resulting polynomials, starting from the expanded form of

$$\left(\sum_{g\in\mathbb{Z}_n^S}c_g\prod_{i\in S}(x_i)^{g(i)}\right)^m,\tag{1.3.37}$$

until we obtain a polynomial of degree at most $n-1$ in each variable. The transformation never introduces a variable indexed by a member of the complement of S. We obtain that

$$\left(\sum_{g\in\mathbb{Z}_n^S}c_g\prod_{i\in S}(x_i)^{g(i)}\right)^m=\sum_{j\in\mathbb{Z}_m}q_j(\mathbf{x})\prod_{k\in\mathbb{Z}_n}(x_j-\alpha_k)+\sum_{g\in\mathbb{Z}_n^S}\left(P(g)\right)^m\prod_{\substack{i\in S\\ j_i\in\mathbb{Z}_n\backslash\{g(i)\}}}\left(\frac{x_i-\alpha_{j_i}}{\alpha_{g(i)}-\alpha_{j_i}}\right)$$

by which it follows that

$$\left(\sum_{g\in\mathbb{Z}_n^S}c_g\prod_{i\in S}(x_i)^{g(i)}\right)^m=\sum_{j\in\mathbb{Z}_m}q_j(\mathbf{x})\prod_{k\in\mathbb{Z}_n}(x_j-\alpha_k)+\sum_{g\in\mathbb{Z}_n^S}a_g\prod_{i\in S}(x_i)^{g(i)},\tag{1.3.38}$$

where $\alpha_k,a_g\in\mathbb{C}$ for all $k\in\mathbb{Z}_n$ and $n=\left|\{\alpha_k:k\in\mathbb{Z}_n\}\right|$ as claimed. □

Lemma 1.3.39 (Monomial support). *Let $P\in\mathbb{Q}[x_0,\dots,x_{n-1}]$ be such that it is not identically constant. If*

$$P(\mathbf{x})\;=\;\sum_{\sigma\in S_n}a_\sigma\prod_{\substack{i\in\mathbb{Z}_n\\ j_i\in\mathbb{Z}_n\backslash\{\sigma(i)\}}}\left(\frac{x_i-j_i}{\sigma(i)-j_i}\right),\tag{1.3.40}$$

then there exist a minimal non-empty set $\mathcal{M}_P \subset \mathbb{Z}_n^{\mathbb{Z}_n}$ *subject to* $\left|f^{-1}\left(\{0\}\right)\right| \le 1$ *for all* $f \in \mathcal{M}_P$ *such that*

$$P(\mathbf{x}) = \sum_{f \in \mathcal{M}_P} c_f \prod_{i \in \mathbb{Z}_n} x_i^{f(i)}, \tag{1.3.41}$$

where $c_f \in \mathbb{Q} \setminus \{0\}$.

Proof. Stated otherwise, every term in the expanded form of P is a multiple of at least $n-1$ distinct variables. Consider a Lagrange basis polynomial associated with an arbitrary $\sigma \in \mathrm{S}_n$:

$$L_\sigma(\mathbf{x}) = \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}}} \left(\frac{x_i - j_i}{\sigma(i) - j_i}\right) = \prod_{\substack{i \in \mathbb{Z}_n \setminus \{\sigma^{-1}(0)\} \\ j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}}} \left(\frac{x_i - j_i}{\sigma\left(i\right) - j_i}\right) \prod_{j_{\sigma^{-1}(0)} \in \mathbb{Z}_n \setminus \{0\}} \left(\frac{x_{\sigma^{-1}(0)} - j_{\sigma^{-1}(0)}}{0 - j_{\sigma^{-1}(0)}}\right).$$

On the right-hand side of the second equal sign immediately above, the univariate polynomial in $x_{\sigma^{-1}(0)}$ encompassed within the scope of the second Π indexed by $j_{\sigma^{-1}(0)} \in \mathbb{Z}_n \setminus \{0\}$ has (in its expanded form) a non-vanishing constant term equal to one. However, the constant term vanishes within the expanded form of each univariate factor

$$\prod_{j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}} \left(\frac{x_i - j_i}{\sigma\left(i\right) - j_i}\right)$$

encompassed within the scope of the first Π indexed by $i \in \mathbb{Z}_n \setminus \left\{\sigma^{-1}\left(0\right)\right\}$. Indeed, we have

$$L_\sigma(\mathbf{x}) = \underbrace{\prod_{\substack{i \in \mathbb{Z}_n \setminus \{\sigma^{-1}(0)\} \\ j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}}} \left(\frac{x_i - j_i}{\sigma\left(i\right) - j_i}\right)}_{\text{does not feature the variable } x_{\sigma^{-1}(0)}} \left(\frac{(x_{\sigma^{-1}(0)})^{n-1} + \ldots + (-1)^{n-1}(n-1)!}{(-1)^{n-1}(n-1)!}\right).$$

Observe that each summand term in the expanded form of the Lagrange basis polynomial $L_\sigma(\mathbf{x})$ above which is a non-vanishing monomial multiple of $x_{\sigma^{-1}(0)}$ is a multiple of every variable in $\{x_0, \ldots, x_{n-1}\}$. By contrast, every non-vanishing monomial summand term which is not a multiple of $x_{\sigma^{-1}(0)}$ is a multiple of every other variables, i.e., variables in the set $\{x_0, \ldots, x_{n-1}\} \setminus \left\{x_{\sigma^{-1}(0)}\right\}$. Applying the same argument to each $\sigma \in \mathrm{S}_n$ yields the desired claim. □

1.4. The Composition Lemma

Lemma 1.4.1 (Transposition Invariance). *Let* $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ *be such that its functional directed graph* G_f *has at least two sibling leaf nodes, i.e.,* G_f *has vertices* $u, v \in \mathbb{Z}_n$ *such that* $f^{-1}(\{u, v\}) = \emptyset$ *and* $f(u) = f(v)$. *If the transposition* $\tau \in S_n$ *exchanges* u *and* v, *i.e.,*

$$\tau(i) = \begin{cases} v & \textit{if } i = u \\ u & \textit{if } i = v \\ i & \textit{otherwise} \end{cases} \quad \forall\, i \in \mathbb{Z}_n.$$

Then

$$\tau \in \mathit{Aut}\left(P_f(\mathbf{x})\right), \tag{1.4.2}$$

where P_f *is the polynomial certificate of grace as defined in 1.3.20.*

Proof. Stated otherwise, the claim asserts that the polynomial P_f is fixed by a transposition of any pair of variables associated with sibling leaf vertices. By construction of $P_f\left(\mathbf{x}\right)$, the changes in its Vandermonde factors induced by the action of τ are as follows:

$$P_f(x_{\tau(0)}, \ldots, x_{\tau(i)}, \ldots, x_{\tau(n-1)}) = \prod_{0 \le i < j < n} (x_{\tau(j)} - x_{\tau(i)}) \prod_{0 \le i < j < n} ((x_{\tau f(j)} - x_{\tau(j)})^2 - (x_{\tau f(i)} - x_{\tau(i)})^2). \tag{1.4.3}$$

Note that there is a bijection

$$x_i \mapsto (x_{f(i)} - x_i)^2, \quad \forall\, i \in \mathbb{Z}_n. \tag{1.4.4}$$

Hence, the transposition $\tau \in \mathrm{Aut}\left(G_f\right)$ of the leaf nodes induces a transposition τ of the corresponding leaf edges outgoing from the said leaf nodes. More precisely, the maps

$$\left(\begin{array}{ccccc} x_0 & ,\dots, & x_i & ,\dots, & x_{n-1} \\ \downarrow & & \downarrow & & \downarrow \\ x_{\tau(0)} & ,\dots, & x_{\tau(i)} & ,\dots, & x_{\tau(n-1)} \end{array}\right)$$

and

$$\left(\begin{array}{ccccc} (x_{f(0)}-x_0)^2 & ,\dots, & (x_{f(i)}-x_i)^2 & ,\dots, & (x_{f(n-1)}-x_{n-1})^2 \\ \downarrow & & \downarrow & & \downarrow \\ (x_{\tau f(0)}-x_{\tau(0)})^2 & ,\dots, & (x_{\tau f(i)}-x_{\tau(i)})^2 & ,\dots, & (x_{\tau f(n-1)}-x_{\tau(n-1)})^2 \end{array}\right)$$

prescribe the same permutation τ of the vertex variables and induced edges label binomials respectively. Observe that

$$P_f(x_{\tau(0)},\dots,x_{\tau(i)},\dots,x_{\tau(n-1)}) =$$

$$\left(\prod_{0\le i<j<n}\frac{x_{\tau(j)}-x_{\tau(i)}}{x_j-x_i}\prod_{0\le i<j<n}(x_j-x_i)\right)\left(\prod_{0\le i<j<n}\frac{(x_{\tau f(j)}-x_{\tau(j)})^2-(x_{\tau f(i)}-x_{\tau(i)})^2}{(x_{f(j)}-x_j)^2-(x_{f(i)}-x_i)^2}\prod_{0\le i<j<n}((x_{f(j)}-x_j)^2-(x_{f(i)}-x_i)^2)\right)$$

$$=\left(\mathrm{sgn}(\tau)\prod_{0\le i<j<n}(x_j-x_i)\right)\left(\mathrm{sgn}(\tau)\prod_{0\le i<j<n}((x_{f(j)}-x_j)^2-(x_{f(i)}-x_i)^2)\right)$$

$$=\left((-1)\prod_{0\le i<j<n}(x_j-x_i)\right)\left((-1)\prod_{0\le i<j<n}((x_{f(j)}-x_j)^2-(x_{f(i)}-x_i)^2)\right)$$

$$\implies P_f(x_{\tau(0)},\dots,x_{\tau(n-1)}) = P_f(x_0,\dots,x_{n-1}), \tag{1.4.5}$$

thus establishing the desired claim.

□

PROPOSITION 1.4.6 (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)
$$\max_{\sigma\in S_n}\left|\left\{\left|\sigma f^{(2)}\sigma^{-1}(i)-i\right| : i\in\mathbb{Z}_n\right\}\right| \le \max_{\sigma\in S_n}\left|\left\{\left|\sigma f\sigma^{-1}(i)-i\right| : i\in\mathbb{Z}_n\right\}\right|.$$

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

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

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

$$n = \max_{\sigma\in \mathrm{S}_n}\left|\left\{\left|\sigma f\sigma^{-1}(i)-i\right| : i\in\mathbb{Z}_n\right\}\right| \iff P_f(\mathbf{x})\not\equiv 0 \iff \mathrm{GrL}(G_f)\ne\emptyset. \tag{1.4.7}$$

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 the assertions

$$n = \max_{\sigma\in \mathrm{S}_n}\left|\left\{|\sigma f^{(2)}\sigma^{-1}(i)-i| : i\in\mathbb{Z}_n\right\}\right| \text{ and } n = \max_{\sigma\in \mathrm{S}_n}\left|\left\{|\sigma f\sigma^{-1}(i)-i| : i\in\mathbb{Z}_n\right\}\right| \tag{1.4.8}$$

indeed implies the inequality

$$\max_{\sigma\in \mathrm{S}_n}\left|\left\{|\sigma f^{(2)}\sigma^{-1}(i)-i| : i\in\mathbb{Z}_n\right\}\right| \le \max_{\sigma\in \mathrm{S}_n}\left|\left\{|\sigma f\sigma^{-1}(i)-i| : i\in\mathbb{Z}_n\right\}\right|. \tag{1.4.9}$$

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

$$n > \max_{\sigma\in \mathrm{S}_n}\left|\left\{|\sigma f^{(2)}\sigma^{-1}(i)-i| : i\in\mathbb{Z}_n\right\}\right|, \tag{1.4.10}$$

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

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

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

$$n = \max_{\sigma\in \mathrm{S}_n} \left|\left\{|\sigma f^{(\lceil 2^{\lg(n-1)}\rceil)}\sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|, \tag{1.4.12}$$

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

$$\max_{\sigma\in \mathrm{S}_n} \left|\left\{|\sigma f^{(\lceil 2^{\kappa}\rceil)}\sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right| > \max_{\sigma\in \mathrm{S}_n} \left|\left\{|\sigma f^{(\lceil 2^{\kappa-1}\rceil)}\sigma^{-1}(i) - i| : i \in \mathbb{Z}_n\right\}\right|. \tag{1.4.13}$$

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

$$P_{f^{(\lceil 2^{\lg(n-1)}\rceil)}}(\mathbf{x}) \not\equiv 0. \tag{1.4.14}$$

$\square$

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

$$\max_{\sigma\in \mathrm{S}_n} \left|\left\{\left|\sigma f^{(2)}\sigma^{-1}(i) - i\right| : i \in \mathbb{Z}_n\right\}\right| \le \max_{\sigma\in S_n} \left|\left\{\left|\sigma f\sigma^{-1}(i) - i\right| : i \in \mathbb{Z}_n\right\}\right|. \tag{1.4.16}$$

PROOF. Owing to Proposition 1.4.6, 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. Given that the diameter of G_f is greater than 2, we may assume without loss of generality that $f^{-1}(\{n-1\}) = \emptyset$ and $f^{(2)}(n-1) \ne f(n-1)$. Let the contractive map $g \in \mathbb{Z}_n^{\mathbb{Z}_n}$ be devised from f such that

$$g(i) = \begin{cases} f^{(2)}(i) & \text{if } i \in f^{-1}(\{f(n-1)\}) \\ f(i) & \text{otherwise} \end{cases}, \ \forall\, i \in \mathbb{Z}_n. \tag{1.4.17}$$

We show that

$$P_g(\mathbf{x}) \not\equiv 0 \implies P_f(\mathbf{x}) \not\equiv 0. \tag{1.4.18}$$

Note that the assertion immediately above generalizes the composition lemma since, the function f is only partially iterated. More precisely, f is iterated only on the restriction $f^{-1}(\{f(n-1)\}) \subset \mathbb{Z}_n$. Iterating this slight generalization of the composition lemma yields that all functional trees are graceful, which in turn implies that the *Composition Lemma* as stated in Lemma 1.4.16 holds. For notational convenience, we assume without loss of generality that

$$f(n-1) = n - \left|f^{-1}(\{f(n-1)\})\right| - 1 \ \text{ and } \ f^{-1}(\{f(n-1)\}) = \mathbb{Z}_n \setminus \mathbb{Z}_{1+f(n-1)}. \tag{1.4.19}$$

If the conditions stated above are not met, we relabel the vertices of G_f to ensure that such is indeed the case. Note that such a relabeling does not affect the property we seek to prove. We prove the contrapositive claim

$$P_f(\mathbf{x}) \equiv 0 \implies P_g(\mathbf{x}) \equiv 0. \tag{1.4.20}$$

By construction, the polynomial

$$\begin{aligned} P_f(\mathbf{x}) = & \prod_{0\le i<j<n} (x_j - x_i) \times \\ & \prod_{\substack{0 \le u < v \le f(n-1) \\ t \in \{0,1\}}} \left(x_{f(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t\in\{0,1\}}} \left(x_{f(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \\ t\in\{0,1\}}} \left(x_{f(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right), \end{aligned} \tag{1.4.21}$$

differs only slightly from

$$\begin{aligned} P_g(\mathbf{x}) = & \prod_{0\le i<j<n} (x_j - x_i) \times \\ & \prod_{\substack{0 \le u < v \le f(n-1) \\ t \in \{0,1\}}} \left(x_{f(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t\in\{0,1\}}} \left(x_{f^{(2)}(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \\ t\in\{0,1\}}} \left(x_{f^{(2)}(v)} - x_v + (-1)^t (x_{f^{(2)}(u)} - x_u) \right). \end{aligned} \tag{1.4.22}$$

We setup a variable *telescoping* within each induced edge label binomial $(x_{f^{(2)}(v)} - x_v)$ where $v \in f^{-1}(\{f(n-1)\})$ (i.e. induced edge binomials of edges outgoing from the subset of vertices where f is iterated) as follows:

$$\underbrace{(x_{f^{(2)}(v)} - x_v)}_{x_v \longrightarrow x_{f^{(2)}(v)}} = \underbrace{(x_{f(v)} - x_v)}_{x_v \longrightarrow x_{f(v)}} + \underbrace{(x_{f^{(2)}(v)} - x_{f(v)})}_{x_{f(v)} \longrightarrow x_{f^{(2)}(v)}} .$$

The telescoping enables us to express induced edge binomials of edges outgoing from the subset of vertices where f is iterated in terms of induced edge binomials which feature in E_f. Note that

$$(x_{f^{(2)}(v)} - x_v) = \left((x_{f^{(2)}(v)} - x_{f(v)}) + (x_{f(v)} - x_v) \right) = (x_{f^{(2)}(n-1)} - x_{f(n-1)}) + (x_{f(v)} - x_v),$$

given that $f(v) = f(n-1)$ for all $v \in f^{-1}(\{f(n-1)\})$. Thus

$$P_g = \prod_{0 \le i < j < n} (x_j - x_i) \times$$
$$\prod_{\substack{0 \le u < v \le f(n-1) \\ t \in \{0,1\}}} \left(x_{f(v)} - x_v + (-1)^t (x_{f(u)} - x_u) \right) \times$$
$$\prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\}}} \left((x_{f^{(2)}(n-1)} - x_{f(n-1)}) + (x_{f(v)} - x_v) + (-1)^t (x_{f(u)} - x_u) \right) \times$$
$$\prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \\ t \in \{0,1\}}} \left((x_{f^{(2)}(n-1)} - x_{f(n-1)}) + (x_{f(v)} - x_v) + (-1)^t \left((x_{f^{(2)}(n-1)} - x_{f(n-1)}) + (x_{f(u)} - x_u) \right) \right).$$

For notational convenience, we set induced edge binomials to be $b_u := \left(x_{f(u)} - x_u \right)$ for all $u \in \mathbb{Z}_n$ we write

$$(1.4.23) \qquad \begin{aligned} P_g = & \prod_{0 \le i < j < n} (x_j - x_i) \times \\ & \prod_{0 \le u < v \le f(n-1)} ((b_v)^2 - (b_u)^2) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\}}} \left(b_{u,v,t} + b_{f(n-1)} \right) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v}} \left(b_v - b_u + 0\, b_{f(n-1)} \right) \left(b_v + b_u + 2\, b_{f(n-1)} \right) \end{aligned}$$

where chromatic induced edge label binomial expressions are

$$b_{f(n-1)} := (x_{f^{(2)}(n-1)} - x_{f(n-1)}),$$

$$b_i := (x_{f(i)} - x_i), \quad \forall\, i \in f^{-1}(\{f(n-1)\}),$$

and

$$b_{u,v,t} := b_v + (-1)^t\, b_u = ((x_{f(v)} - x_v) + (-1)^t (x_{f(u)} - x_u)), \quad \forall \substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\}.}$$

Note that in equation 1.4.23, we have successfully re-expressed the edge label Vandermonde factor E_g exclusively in terms of induced edge label binomials from G_f. We re-write the expression of P_f in equation (1.4.21) using the shorthand notation for induced edge binomials as follows:

$$(1.4.24) \qquad \begin{aligned} P_f = & \prod_{0 \le i < j < n} (x_j - x_i) \times \\ & \prod_{0 \le u < v \le f(n-1)} ((b_v)^2 - (b_u)^2) \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\}}} b_{u,v,t} \times \\ & \prod_{\substack{v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v}} (b_v - b_u)(b_v + b_u). \end{aligned}$$

Invoking the multi-binomial identity on the two bichromatic factors of P_g in equation (1.4.23) yields equalities

$$\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} \left(b_v + b_u + 2b_{f(n-1)}\right) =$$

$$\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v + b_u) + \sum_{\substack{r_{u,v}\in\{0,1\}\\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v + b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}}.$$

and

$$\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} \left(b_{u,v,t} + b_{f(n-1)}\right) =$$

$$\prod_{\substack{t\in\{0,1\}\\ v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)}} b_{u,v,t} + \sum_{\substack{s_{u,v,t}\in\{0,1\}\\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} \left(b_{u,v,t}\right)^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}}.$$

Substituting equalities immediately above into equation (1.4.23) yields an expression of P_g of the form

$$P_g = P_f + R_{f,g}. \tag{1.4.25}$$

The monochromatic red expressions in the multi-binomial expansion collect to result in P_f as written in equation (1.4.24). The second part denoted $R_{f,g}$ simply collects the remaining bichromatic summands and is given by

$$R_{f,g} = \prod_{0\le i<j<n} (x_j - x_i) \prod_{0\le u<v\le f(n-1)} \left((b_v)^2 - (b_u)^2\right) \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v - b_u)\times$$
$$\Bigg[\Bigg(\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v + b_u)\Bigg)\Bigg(\sum_{\substack{s_{u,v,t}\in\{0,1\}\\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} \left(b_{u,v,t}\right)^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}}\Bigg)+$$
$$\Bigg(\prod_{\substack{t\in\{0,1\}\\ v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)}} b_{u,v,t}\Bigg)\Bigg(\sum_{\substack{r_{u,v}\in\{0,1\}\\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v + b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}}\Bigg)+$$
$$\Bigg(\sum_{\substack{s_{u,v,t}\in\{0,1\}\\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} \left(b_{u,v,t}\right)^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}}\Bigg)\Bigg(\sum_{\substack{r_{u,v}\in\{0,1\}\\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v + b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}}\Bigg)\Bigg].$$

The color scheme above is meant to help track the location of telescoping variables. We now proceed with the main contradiction argument. Assume for the sake of establishing a contradiction that the claim (1.4.20) is false, i.e., for some f subject to conditions described in our premise, we have

$$0 \equiv P_f \text{ and } 0 \not\equiv P_g. \tag{1.4.26}$$

Then by equation (1.4.25), we obtain

$$P_g \equiv R_{f,g} \not\equiv 0 \iff \overline{P}_g = \overline{R}_{f,g} \not\equiv 0. \tag{1.4.27}$$

Observe that every summand in $R_{f,g}$ is a multiple of a positive power of the induced edge label binomial

$$b_{f(n-1)} = \left(x_{f^{(2)}(n-1)} - x_{f(n-1)}\right)$$

We focus in particular on the summand within $R_{f,g}$ which is a multiple of the largest possible power of the blue induced edge label binomial $b_{f(n-1)}$, namely the summand associated with binary exponent assignments

$$s_{u,v,t} = 0, \text{ for all } \begin{array}{c} v\in f^{-1}\left(\{f(n-1)\}\right)\\ 0\le u\le f(n-1)\\ t\in\{0,1\}\end{array} \text{ as well as } r_{u,v}=0, \text{ for all } \begin{array}{c} v\in f^{-1}\left(\{f(n-1)\}\right)\\ 0\le u\le f(n-1)\end{array}. \tag{1.4.28}$$

The said summand is

$$c \prod_{0\le i<j<n} (x_j - x_i) \left(\prod_{0\le u<v\le f(n-1)} ((b_v)^2 - (b_u)^2) \right) \left(\prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ f(n-1)<u<v}} (b_v - b_u) \right) \left(b_{f(n-1)} \right)^m,$$

where

$$m = \left| \left\{ \begin{array}{c} v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \end{array} \right\} \right| + \left| \left\{ \begin{array}{c} v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\} \end{array} \right\} \right| \text{ and } c = 2^{\left| \left\{ \begin{array}{c} v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \end{array} \right\} \right|}. \tag{1.4.29}$$

It follows from the premise $0 \not\equiv P_g$ that the remainder of the chosen summand is non–vanishing. Observe that the factor

$$\prod_{0\le i<j<n} (x_j - x_i) \left(\prod_{0\le u<v\le f(n-1)} ((b_v)^2 - (b_u)^2) \right) \left(\prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ f(n-1)<u<v}} (b_v - b_u) \right) \tag{1.4.30}$$

is a common factor to every summand in $R_{f,g}$. We factor out from the said common factor a smaller factor up to sign invariant to the transposition τ which exchanges the variable x_{n-1} with $x_{f(n-1)}$. We write

$$\begin{aligned} R_{f,g} = & \prod_{0\le i<j<n} (x_j - x_i) \prod_{0\le u<v<f(n-1)} ((b_v)^2 - (b_u)^2) \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\setminus\{n-1\} \\ f(n-1)<u<v}} (b_v - b_u) \times \\ & \prod_{0\le u<f(n-1)} ((b_{f(n-1)})^2 - (b_u)^2) \prod_{f(n-1)<u<n-1} (b_{n-1} - b_u) \times \\ & \left[\left(\prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ f(n-1)<u<v}} (b_v + b_u) \right) \left(\sum_{\substack{s_{u,v,t}\in\{0,1\} \\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ 0\le u\le f(n-1) \\ t\in\{0,1\}}} \left(b_{u,v,t}\right)^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}} \right) + \right. \\ & \left(\prod_{\substack{t\in\{0,1\} \\ v\in f^{-1}(\{f(n-1)\}) \\ 0\le u\le f(n-1)}} b_{u,v,t} \right) \left(\sum_{\substack{r_{u,v}\in\{0,1\} \\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ f(n-1)<u<v}} (b_v + b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}} \right) + \\ & \left. \left(\sum_{\substack{s_{u,v,t}\in\{0,1\} \\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ 0\le u\le f(n-1) \\ t\in\{0,1\}}} \left(b_{u,v,t}\right)^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}} \right) \left(\sum_{\substack{r_{u,v}\in\{0,1\} \\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\}) \\ f(n-1)<u<v}} (b_v + b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}} \right) \right]. \end{aligned}$$

Thus

$$R_{f,g}(\mathbf{x}) = \left(\prod_{0\le i<j<n} (x_j - x_i) \prod_{0\le u<v<f(n-1)} ((b_v)^2 - (b_u)^2) \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\setminus\{n-1\} \\ f(n-1)<u<v}} (b_v - b_u) \right) Q_{f,g}(\mathbf{x}),$$

where

$$Q_{f,g}(\mathbf{x}) = \prod_{0\le u<f(n-1)} ((b_{f(n-1)})^2-(b_u)^2) \prod_{f(n-1)<u<n-1} (b_{n-1}-b_u)\times$$
$$\left[\left(\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v+b_u)\right)\left(\sum_{\substack{s_{u,v,t}\in\{0,1\}\\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} (b_{u,v,t})^{s_{u,v,t}} (b_{f(n-1)})^{1-s_{u,v,t}}\right)+\right.$$
$$\left(\prod_{\substack{t\in\{0,1\}\\ v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)}} b_{u,v,t}\right)\left(\sum_{\substack{r_{u,v}\in\{0,1\}\\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v+b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}}\right)+$$
$$\left.\left(\sum_{\substack{s_{u,v,t}\in\{0,1\}\\ 0=\prod s_{u,v,t}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ 0\le u\le f(n-1)\\ t\in\{0,1\}}} (b_{u,v,t})^{s_{u,v,t}} \left(b_{f(n-1)}\right)^{1-s_{u,v,t}}\right)\left(\sum_{\substack{r_{u,v}\in\{0,1\}\\ 0=\prod r_{u,v}}} \prod_{\substack{v\in f^{-1}(\{f(n-1)\})\\ f(n-1)<u<v}} (b_v+b_u)^{r_{u,v}} \left(2b_{f(n-1)}\right)^{1-r_{u,v}}\right)\right].$$

Let

$$\Phi(g) := \left\{\theta\in \mathrm{S}_n : G_{\theta g\theta^{-1}} \in \mathrm{GrL}(G_g)\right\}.$$

By Proposition 1.3.1, the premise $\overline{P}_g = \overline{R}_{f,g}$ implies

$$(1.4.31)\qquad P_g(h) = R_{f,g}(h) = v_h\, Q_{f,g}(h) = \begin{cases} \mathrm{sgn}(h\;|hg-h|)\prod_{v\in\mathbb{Z}_n}(v!)^2\,\frac{(n-1+v)!}{(2v)!} & \text{if } h\in\Phi(g)\\ \\ 0 & \text{otherwise}\end{cases},\ \forall\, h\in\mathbb{Z}_n^{\mathbb{Z}_n}.$$

Recall that $Q_{f,g}$ is the remaining factor of $R_{f,g}$ after we exclude the invariant common factor (up to sign invariant to the transposition τ) equal to

$$\prod_{0\le i<j<n}(x_j-x_i)\prod_{0\le u<v<f(n-1)}((b_v)^2-(b_u)^2)\prod_{\substack{v\in f^{-1}\left(\{f(n-1)\}\right)\setminus\{n-1\}\\ f(n-1)<u<v}}(b_v-b_u)$$

Specifically, $Q_{f,g}$ is a polynomial resulting from the sum over chromatic summands resulting from the multibinomial expansions. Let us view $Q_{f,g}$ as a sum of $|\Sigma|$ summands (each of which is symmetrized as needed to reflect τ-invariance of evaluations when it holds) and denote by $Q^{[s]}_{f,g}$ the summands $1\le s\le|\Sigma|$ of $Q_{f,g}$. By Proposition 1.3.15, we can write the remainder of $R_{f,g}$ as follows:

$$\overline{R}_{f,g} = \sum_{1\le s\le|\Sigma|}\left(\sum_{\sigma\in\Phi(g)} v_\sigma\cdot Q^{[s]}_{f,g}(\sigma)\cdot L_\sigma(\mathbf{x})\right),$$

Let us denote by I_s the set of indices associated with variables featured in $Q^{[s]}_{f,g}$. Recall that $L_\sigma\left(\mathbf{x}|_{I_s}\right)$ denotes the factor of $L_\sigma(\mathbf{x})$ which only features variables indexed by I_s. Note that if any permutation τ lies in the automorphism group of the polynomial

$$\overline{R}_{f,g} = \sum_{1\le s\le|\Sigma|}\left(\sum_{\sigma\in\Phi(g)} v_\sigma\cdot Q^{[s]}_{f,g}(\sigma)\cdot L_\sigma(\mathbf{x}|_{I_s})\cdot L_\sigma(\mathbf{x}|_{\mathbb{Z}_n\setminus I_s})\right),$$

then, by Lemma 1.3.17, τ also lies in the automorphism group of the polynomial

$$\sum_{1\le s\le|\Sigma|}\left(\sum_{\sigma\in\Phi(g)} v_\sigma\cdot Q^{[s]}_{f,g}(\sigma)\cdot L_\sigma(\mathbf{x}|_{I_s})\right).$$

By Lemma 1.4.1, the premise $\overline{P}_g = \overline{R}_{f,g}$ implies that the transposition τ fixes $\overline{R}_{f,g}$. That is to say, we obtain

$$\tau\in\mathrm{Aut}\left(\sum_{1\le s\le|\Sigma|}\left(\sum_{\sigma\in\Phi(g)} v_\sigma\cdot Q^{[s]}_{f,g}(\sigma)\cdot L_\sigma(\mathbf{x}|_{I_s})\right)\right)$$

As a consequence of the multi-binomial expansion, the sum expressing $Q_{f,g}$ features as one of its summand a unique monochromatic blue binomial summand, say $Q_{f,g}^{[1]}$, given by

$$Q_{f,g}^{[1]} = c\,(b_{n-1})^{n-1-f(n-1)-2}(b_{f(n-1)})^{\ell}.$$

where

$$\ell = \left|\left\{\begin{array}{c} v \in f^{-1}(\{f(n-1)\}) \\ f(n-1) < u < v \end{array}\right\}\right| + \left|\left\{\begin{array}{c} v \in f^{-1}(\{f(n-1)\}) \\ 0 \le u \le f(n-1) \\ t \in \{0,1\} \end{array}\right\}\right| + 2f(n-1).$$

So that we are interested in

$$\left(\prod_{0\le i<j<n}(x_j - x_i)\prod_{0\le u<v<f(n-1)}\left((b_v)^2-(b_u)^2\right)\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\setminus\{n-1\}\\ f(n-1)<u<v}}(b_v - b_u)\right)Q_{f,g}^{[1]} =$$

$$\left(\prod_{0\le i<j<n}(x_j - x_i)\prod_{0\le u<v<f(n-1)}\left((b_v)^2-(b_u)^2\right)\prod_{\substack{v\in f^{-1}(\{f(n-1)\})\setminus\{n-1\}\\ f(n-1)<u<v}}(b_v - b_u)\right)c\,(b_{n-1})^{n-1-f(n-1)-2}(b_{f(n-1)})^{\ell}$$

Note that b_{n-1} is up to sign invariant to the transposition τ. By the premise that G_g is graceful, the chosen summand is non-vanishing if we interchange values assigned to variables x_{n-1} and $x_{f(n-1)}$ doing so changes the absolute induced edge label assigned to $b_{f(n-1)}$ but fixes the absolute induced edge label assigned to all other edges. Therefore non-zero evaluations of the chosen summand are not τ-invariant. Consequently the non-vanishing orbit associated with the chosen summand is not fixed by τ. By Lemmas 1.3.33 and 1.3.17, the invariance of $Q_{f,g}^{[1]}$ to the transposition τ is predicated upon the τ-invariance up to sign of the polynomial

$$c\sum_{\sigma\in\Phi(g)}\left(\sigma f^{(2)}(n-1) - \sigma f(n-1)\right)^{\ell}\times$$

$$\prod_{j_{f^{(2)}(n-1)}\in\mathbb{Z}_n\setminus\{\sigma f^{(2)}(n-1)\}}\left(\frac{x_{f^{(2)}(n-1)} - j_{f^{(2)}(n-1)}}{\sigma f^{(2)}(n-1) - j_{f^{(2)}(n-1)}}\right)\prod_{j_{f(n-1)}\in\mathbb{Z}_n\setminus\{\sigma f(n-1)\}}\left(\frac{x_{f(n-1)} - j_{f(n-1)}}{\sigma f(n-1) - j_{f(n-1)}}\right),$$

which is seen to be up to sign asymmetric to the transposition τ. Let us now focus on the action of the transposition τ on individual summands of some polynomial resulting from an arbitrary but fixed partition of its non-vanishing monomial terms. There are exactly three distinct ways that a candidate transposition of a pair of variables can lie in the automorphism group of a given polynomial. Assume that we reason about a particular summand denoted as S.

(i) Option 1: The candidate transposition of a pair of variables fixes the chosen summand S. This occurs when S is symmetric in the chosen pair of variables being transposed.

(ii) Option 2: The candidate transposition of the chosen pair of variables does not fix S (i.e., Option 1 does not apply) but induces in turn a transposition which exchanges the chosen summand S with some other summand from the partition say, S'. This occurs, for instance, if we consider the sum $S + S'$ where $S = (x_0)^2\,x_1$ and $S' = x_0\,(x_1)^2$. In this example, we see that the transposition which exchanges variables x_0 with x_1 does not fix S, but it induces a transposition which exchanges the summand S with the summand S'.

(iii) Option 3: The candidate transposition of a pair of variables neither fixes S nor does it induce a transposition which exchanges S with some other summand (i.e., neither Option 1 nor Option 2 applies). Instead, S is such that a symmetry broadening cancellation occurs. Such a cancellation must involve interactions between the non-vanishing monomials within the monomial support of S with the non-vanishing monomials within the support of other summands. Option 3 occurs, for instance, if we take $S = -x_1$ and $S' = x_0 + 2x_1$. We see that in this example neither Option 1 nor Option 2 applies when the candidate transposition is the transposition which exchanges variables x_0 with x_1. However $S + S' = x_0 + x_1$ is symmetric and thus admits the said transposition in its automorphism group. This fact is due to the symmetry broadening cancellation of like terms : $-x_1 + 2x_1$.

We have already established that $Q_{f,g}^{[1]}$ is not up to sign fixed by the transposition $\tau \in \mathrm{S}_n$. This first observation accounts for Option 1. Also note that the remainder of the chosen summand $Q_{f,g}^{[1]}$ does not exchange with the remainder of any other summands when we exchange $x_{f(n-1)}$ with x_{n-1} since by Lemma 1.3.39, when discounting the τ-invariant (up to sign) factor edge binomial b_{n-1}, the non-vanishing remainders of other bi-chromatic summand in $Q_{f,g}$ depends on 3 or more variables. This second observation accounts for Option 2. We now account for Option 3 and show that there are no symmetry-broadening cancellations which adjoin τ to the automorphism group. Again by Lemma 1.3.39, such a symmetry broadening cancellation can occur only for Lagrange bases

$$\prod_{j_{f^{(2)}(n-1)}\in\mathbb{Z}_n\setminus\{\sigma f^{(2)}(n-1)\}}\left(\frac{x_{f^{(2)}(n-1)}-j_{f^{(2)}(n-1)}}{\sigma f^{(2)}\left(n-1\right)-j_{f^{(2)}(n-1)}}\right)\prod_{j_{f(n-1)}\in\mathbb{Z}_n\setminus\{\sigma f(n-1)\}}\left(\frac{x_{f(n-1)}-j_{f(n-1)}}{\sigma f\left(n-1\right)-j_{f(n-1)}}\right).$$

where $\sigma\in\Phi(g)$ is subject to $\sigma\left(n-1\right)=0$ and G_f is such that $1=\left|f^{-1}\left(\left\{f\left(n-1\right)\right\}\right)\right|$. In that setting, non-vanishing monomials occurring in the expanded form of said Lagrange bases summands possibly cancel out non-vanishing monomials occurring in the expanded form of Lagrange bases expressing remainders of bi-chromatic summands in $Q_{f,g}$ of the form

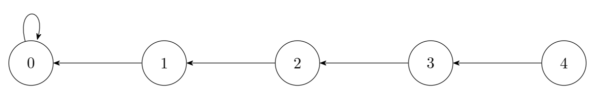
$$\left(b_{f(n-1),n-1,t}\right)^r\left(b_{f(n-1)}\right)^s=\left(b_{n-1}+(-1)^t b_{f(n-1)}\right)^r\left(b_{f(n-1)}\right)^s$$

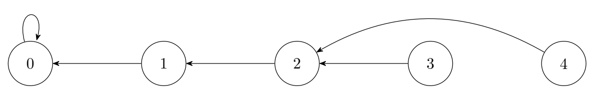
However, the restriction imposed by $\sigma\in\Phi(g)$ where $\sigma\left(n-1\right)=0$ breaks the complementary-labeling symmetry. Indeed by Proposition 1.3.30, the remainder is up to sign invariant to the involution prescribed by the map: $x_i\mapsto x_{n-1-i}$ for all $i\in\mathbb{Z}_n$. But the complementary labeling involution maps any Lagrange basis associated with $\sigma\in\Phi(g)$ such that $\sigma\left(n-1\right)=0$ to different Lagrange basis associated $\sigma'\in\Phi(g)$ such that $\sigma'\left(n-1\right)=n-1$ and thus negates the symmetry broadening cancellations. We see that a symmetry broadening cancellation which adjoins τ to the automorphism group of the remainder of $R_{f,g}$ would break the complementary labeling symmetry, thereby resulting in the contradiction

$$\tau=(f(n-1),n-1)\notin\operatorname{Aut}(\overline{R}_{f,g}).$$

We conclude that the desired claim $P_g(\mathbf{x})\not\equiv 0\implies P_f(\mathbf{x})\not\equiv 0$. holds. □

Example 1.4.32. We present a verification of Lemma 1.4.15 with an example of a path on 5 vertices.

G_f :


G_g :


Run the SageMath script `ex1434.sage` to verify.

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.