Composition Lemma

Edinah Gnang

Parikshit Chalise

Contents

Chapter 1. Composition Lemma 5
1.1. Overview 5
1.2. Functional Directed Graphs 5
1.3. Quotient-Remainder Theorem and Lagrange Interpolation 6
1.4. The Composition Lemma 10

Bibliography 21

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 [**Gna20**] by Gnang. A further developed series of papers resolving the same conjecture again appeared in [**Gna22**] and [**Gna23**]. Recently, the same method has been applied to settle other longstanding conjectures in [**CCG24a**] and [**CCG24b**]. 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.,

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

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

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

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 $\mathrm{Aut}\,(G_f)$, is defined as follows:

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

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

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

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

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

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.,*

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

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

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

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

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

where for notational convenience $P(\alpha_g) := P(\alpha_{g(0)}, \ldots, \alpha_{g(m-1)})$. 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 $\big(q(x_0),\, r(x_0)\big) \in \mathbb{C}[x_0] \times \mathbb{C}[x_0]$ 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 $F \in \mathbb{C}\left[x_0, \ldots, x_{m-1}\right]$, we have

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

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 $H \in \mathbb{C}[x_0, \ldots, x_m]$. We view H as a univariate polynomial in the variable x_m whose coefficients lie in the field of fraction $\mathbb{C}(x_0, \ldots, x_{m-1})$. The univariate quotient-remainder theorem over the field of fractions $\mathbb{C}(x_0, \ldots, x_{m-1})$ asserts that there exit a unique quotient-remainder pair

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

subject to

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

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

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

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

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

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

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

Therefore, we have

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

Applying the induction hypothesis to coefficients

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

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

Proposition 1.3.15 (Ring Homomorphism). *For an arbitrary $H\in\mathbb{C}\left[x_0,\ldots,x_{n-1}\right]$, 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 $\overline{H}(\boldsymbol{\alpha}_g)=H(\boldsymbol{\alpha}_g)$.*
(ii) *If $H=H_0+H_1$, where $H_0,H_1\in\mathbb{C}\left[x_0,\ldots,x_{n-1}\right]$, then $\overline{H_0}+\overline{H_1}=\overline{H}$.*
(iii) *If $H=H_0\cdot H_1$, where $H_0,H_1\in\mathbb{C}\left[x_0,\ldots,x_{n-1}\right]$, 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

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

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

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

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. □

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

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

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

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

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

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

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

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

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

Observe that by the expansions in 1.3.22 and 1.3.24,

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

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

is congruent to

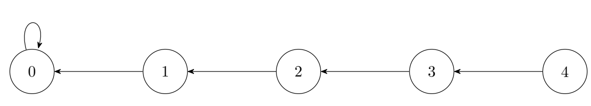
$$\prod_{v \in \mathbb{Z}_n} (v!)^2 \frac{(n-1+v)!}{(2v)!} \sum_{\substack{\sigma \in \mathrm{S}_n \\ \text{s.t.} \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma\, |\sigma f - \sigma|) \prod_{\substack{i \in \mathbb{Z}_n \\ j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}}} \left(\frac{x_i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

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

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

thus establishing the desired claim. □

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* $\left|f^{(n-1)}(\mathbb{Z}_n)\right| = 1$. *The following statements are equivalent:*

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

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

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

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

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

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

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

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 $0 \le \kappa < \lg(n-1)$ such that

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

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*

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

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

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

Recall that $\mathbb{Z}_n$ denote the smallest set of consecutive n non-negative integers. Let $\mathcal{T}_n \subset \mathbb{Z}_n^{\mathbb{Z}_n}$ denotes the semigroup of functions whose n (x, y)–coordinate graph points lie above the line $y = x$ with the exception of an intercept at $x = n-1$. In other words

$$\mathcal{T}_n := \left\{h \in \mathbb{Z}_n^{\mathbb{Z}_n} : h(i) > i, \ \forall\, i \in \mathbb{Z}_{n-1} \text{ and } h(n-1) = n-1\right\}. \tag{1.4.12}$$

We prove the C.L. via the polynomial method.

Part I. Linear-algebra setup (matrices, kernels, and pseudoinverse). Associate with an arbitrary $h \in \mathbb{Z}_n^{\mathbb{Z}_n}$ the adjacency matrix $A_h \in \{0,1\}^{n\times n}$ of G_h (the functional directed graph of h):

$$A_h[i,j] = \begin{cases} 1 & \text{if } j = h(i) \\ 0 & \text{otherwise} \end{cases}, \quad \forall\, (i,j) \in \mathbb{Z}_n \times \mathbb{Z}_n. \tag{1.4.13}$$

The signed incidence matrix of G_h is $(A_{\text{id}} - A_h) \in \{-1, 0, 1\}^{n\times n}$. Observe that generally for all $h \in \mathbb{Z}_n^{\mathbb{Z}_n}$, the rank of $(A_{\text{id}} - A_h)$ is equal to n minus the number of connected component of G_h. In fact each basis vector for the Nullspace of $(A_{\text{id}} - A_h)$ is prescribed by the vertex indicator vector of a corresponding connected component. Observe that adjacency matrices of functional graphs of members of $\mathcal{T}_n$ are all upper-triangular matrices and their incidence matrices are in Row Echelon Form. Furthermore, incidence matrices of functional directed graphs of members of $\mathcal{T}_n$ all have the same Reduced Row Echelon Form matrix. Namely

$$\text{RREF}(A_{\text{id}} - A_h) = A_{\text{id}} - A_{h^{(n-1)}}, \quad \forall\, h \in \mathcal{T}_n. \tag{1.4.14}$$

Observe that for all $h \in \mathcal{T}_n$, the function $h^{(n-1)}$ is the same identically constant function. Namely the function which maps every member of $\mathbb{Z}_n$ to $n-1$. For all $h \in \mathcal{T}_n$, the left and right kernel of $A_{\text{id}} - A_h$ are respectively $A_{\text{id}}[n-1, :]$ and $1_{n\times 1}$. Recall that a solution exist to the equation in the unknown vector $\mathbf{z}$

$$B \cdot \mathbf{z} = \mathbf{c} \tag{1.4.15}$$

where $\mathbf{c} \in \text{Column Space}(B)$. We adopt the following notation convention for expressing solutions in the unknown vector $\mathbf{z}$

$$\mathbf{z} \in B^{+} \cdot \mathbf{c} + \text{Null Space}(B), \tag{1.4.16}$$

where $B^{+} = (B^{\top} \cdot B)^{-1} B^{\top}$.

Part II. Polynomial f-certificate. Injectively assign to members of $\mathcal{T}_n$, a polynomial which expresses a function of n input vectors $\mathbf{x}$, $\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}$ as follows

$$P_f(\mathbf{x},\, y\mathbf{b}_0,\, \ldots,\, y\mathbf{b}_{n-2}) =$$

$$\prod_{0\le u<v<n} \Big(\sum_{w\in\mathbb{Z}_{n-1}} (B^+ \cdot \mathbf{c}_{f,u,v})_w \, y\mathbf{b}_w^\top \cdot (A_{\text{id}} - A_f)\cdot \mathbf{x}\Big) \prod_{t\in\mathbb{Z}_2} \Big(\big(A_{\text{id}}[v,:]\cdot (A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[u,:]\cdot(A_{\text{id}} - A_f)\big)\cdot \mathbf{x}\Big), \tag{1.4.17}$$

where $(B^+ \cdot \mathbf{c}_{f,u,v})_w$ denotes the entry w of the vector $(B^+ \cdot \mathbf{c}_{f,u,v})$. Crucially vectors column vectors $\big\{B[:,0] = \mathbf{b}_0, \ldots, B[:,n-2] = \mathbf{b}_{n-2}\big\}$ forms a basis for the $(n-1)$-dimensional subspace: (Span of $A_{\text{id}}[:,n-1])^\perp \subset \mathbb{Q}^{n\times 1}$
For each one of the $\binom{n}{2}$ vertex pair $(u,v)\in\mathbb{Z}_n\times\mathbb{Z}_n$ where $0\le u<v<n$, the vector $\mathbf{c}_{f,u,v}\in\{-1,0,1\}^{n\times 1}$ denotes the unique vector subject to

$$\mathbf{c}_{f,u,v}^\top \cdot (A_{\text{id}} - A_f)\cdot\mathbf{x} = (x_v - x_u). \tag{1.4.18}$$

Let H denote the projection matrix

$$H = (A_{\text{id}} - A_{\text{id}}[:,n-1]\cdot A_{\text{id}}[n-1,:]) \tag{1.4.19}$$

We call the expression of P_f above an expansion of the f-certificate with respect to an arbitrarily chosen basis vectors $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$ for (Span of $A_{\text{id}}[:,n-1])^\perp$. Recall that

$$\left(\text{Vandermonde}\begin{pmatrix} y\,x_0\\ \vdots\\ y\,x_u\\ \vdots\\ y\,x_{n-1}\end{pmatrix}\right)[i,j] = (y\,x_i)^j,\quad \forall\, 0\le i,j<n \implies \det\left(\text{Vandermonde}\begin{pmatrix} y\,x_0\\ \vdots\\ y\,x_u\\ \vdots\\ y\,x_{n-1}\end{pmatrix}\right) = y^{\binom{n}{2}} \prod_{0\le i<j<n}(x_j - x_i), \tag{1.4.20}$$

and

$$\det\left(\text{Vandermonde}\begin{pmatrix} (x_0 - x_{f(0)})^2\\ \vdots\\ (x_u - x_{f(u)})^2\\ \vdots\\ (x_{n-1} - x_{f(n-1)})^2\end{pmatrix}\right) = \prod_{0\le u<v<n}\big((x_v - x_{f(v)})^2 - (x_u - x_{f(u)})^2\big). \tag{1.4.21}$$

By construction, for any choices of basis vectors $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$ for (Span of $A_{\text{id}}[:,n-1])^\perp$ the following f-certificate equality holds

$$P_f(\mathbf{x}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2}) = \det\left(\text{Vandermonde}\begin{pmatrix} y\,x_0\\ \vdots\\ y\,x_u\\ \vdots\\ y\,x_{n-1}\end{pmatrix}\right)\det\left(\text{Vandermonde}\begin{pmatrix} (x_0 - x_{f(0)})^2\\ \vdots\\ (x_u - x_{f(u)})^2\\ \vdots\\ (x_{n-1} - x_{f(n-1)})^2\end{pmatrix}\right). \tag{1.4.22}$$

Part III. Change of variables and the relation between the f-certificate and the $f^{(2)}$-certificate. Consider the linear transformation prescribed by simultaneous maps:

$$\mathbf{x}\mapsto (A_{\text{id}} + A_f)\cdot\mathbf{x},\quad y\mathbf{b}_u^\top \mapsto y\mathbf{b}_u^\top\cdot (A_{\text{id}} + A_f)^{-1}, \forall\, u\in\mathbb{Z}_{n-1}, \tag{1.4.23}$$

rewritten simply using $M_f := (A_{\text{id}} + A_f)$ as

$$\mathbf{x}\mapsto M_f\cdot\mathbf{x},\quad y\mathbf{b}_u^\top\mapsto y\mathbf{b}_u^\top\cdot M_f^{-1}, \forall\, u\in\mathbb{Z}_{n-1}. \tag{1.4.24}$$

The simultaneous maps are more conveniently summarized via the single action of an invertible $n^2 \times n^2$ matrix as follows:

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \mapsto \left(M_f \oplus \left(I_{n-1} \otimes (M_f^\top)^{-1}\right)\right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}. \tag{1.4.25}$$

Part III.a. Rewrites of the vertex and edge factors of the f-certificate. Observe that for each triplet u, v, w where $0 \le u < v < n$ and $w \in \mathbb{Z}_{n-1}$, the following bilinear form equality holds in the expression of the vertex Vandermonde factor

$$(B^+ \cdot \mathbf{c}_{f,u,v})_w \cdot y\mathbf{b}_w^\top \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x} = \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}^\top \cdot \left(A_{\text{id}}[:,w] \cdot A_{\text{id}}[0,:]\right) \otimes \left((B^+ \cdot \mathbf{c}_{f,u,v})_w \, (A_{\text{id}} - A_f)\right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, \tag{1.4.26}$$

Similarly for all $u \in \mathbb{Z}_n$, the following equality holds in the expression of the edge Vandermonde factor

$$A_{\text{id}}[u,:] \cdot (A_{\text{id}} - A_f) \cdot \mathbf{x} = \left(A_{\text{id}}[:,0] \otimes A_{\text{id}}[:,u]\right)^\top \cdot \left((A_{\text{id}}[:,0] \cdot A_{\text{id}}[0,:]) \otimes (A_{\text{id}} - A_f)\right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}. \tag{1.4.27}$$

The two families of equalities described immediately above articulate the fact that the f-certificate may be viewed as function the $n^2 \times 1$ vector

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}$$

For further notational convenience we subsequently write M to denote M_f. We now show that applying the said linear transformation

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \mapsto \left(M_f \oplus \left(I_{n-1} \otimes (M_f^\top)^{-1}\right)\right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, \tag{1.4.28}$$

maps the expansion of a f-certificate with respect to the basis $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$ of (Span of $A_{\text{id}}[:, n-1]$)$^\perp$ denoted

$$P_f(\mathbf{x},\, y\,\mathbf{b}_0,\, \ldots,\, y\,\mathbf{b}_{n-2})$$

to the expansion of a $f^{(2)}$-certificate with respect to the basis

$$\left\{\mathbf{b}'_0 = H(M^\top)^{-1}\mathbf{b}_0, \ldots, \mathbf{b}'_i = H(M^\top)^{-1}\mathbf{b}_i, \ldots, \mathbf{b}'_{n-2} = H(M^\top)^{-1}\mathbf{b}_{n-2}\right\}, \tag{1.4.29}$$

of (Span of $A_{\text{id}}[:, n-1])^{\perp}$, denoted $P_{f^{(2)}}(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2})$. Thus establishing that

$$P_{f^{(2)}}(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2}) = \det\left(\text{Vandermonde}\begin{pmatrix} y\,x_0 \\ \vdots \\ y\,x_u \\ \vdots \\ y\,x_{n-1}\end{pmatrix}\right)\det\left(\text{Vandermonde}\begin{pmatrix} (x_0 - x_{f^{(2)}(0)})^2 \\ \vdots \\ (x_u - x_{f^{(2)}(u)})^2 \\ \vdots \\ (x_{n-1} - x_{f^{(2)}(n-1)})^2\end{pmatrix}\right). \tag{1.4.30}$$

Part III.b. Proof of Expansion of $f^{(2)}$ certificate in the transformed basis. Recall that an expansion of the $f^{(2)}$-certificate with respect to the basis $\left\{\mathbf{b}'_0, \ldots, \mathbf{b}'_{n-2}\right\}$ forms a basis of (Span of $A_{\text{id}}[:, n-1])^{\perp}$ is given by

$$P_{f^{(2)}}(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2}) = \prod_{0 \le u < v < n}\left(\sum_{w \in \mathbb{Z}_{n-1}}\left((B')^{+}\cdot\mathbf{c}_{f^{(2)},u,v}\right)_w y(\mathbf{b}'_w)^{\top}\cdot(A_{\text{id}} - A_{f^{(2)}})\cdot\mathbf{x}\right)\times$$

$$\prod_{0\le u<v<n}\prod_{t\in\mathbb{Z}_2}\left(\left(A_{\text{id}}[v,:]\cdot(A_{\text{id}} - A_{f^{(2)}}) + (-1)^t A_{\text{id}}[u,:]\cdot(A_{\text{id}} - A_{f^{(2)}})\right)\cdot\mathbf{x}\right). \tag{1.4.31}$$

where $B' = H(M^{\top})^{-1}B$

$$= \prod_{0 \le u < v < n}\left(\sum_{w \in \mathbb{Z}_{n-1}}\left((B')^{+}\cdot\mathbf{c}_{f^{(2)},u,v}\right)_w y\mathbf{b}_w^{\top}\cdot M^{-1}\cdot(A_{\text{id}} - A_f)\cdot M\cdot\mathbf{x}\right)\times$$

$$\prod_{0\le u<v<n}\prod_{t\in\mathbb{Z}_2}\left(\left(A_{\text{id}}[v,:]\cdot(A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[u,:]\cdot(A_{\text{id}} - A_f)\right)\cdot M\cdot\mathbf{x}\right). \tag{1.4.32}$$

Recall that $\mathbf{c}_{f,u,v}$ is the unique vector in (Span of $A_{\text{id}}[:, n-1])^{\perp}$ subject to

$$\mathbf{c}_{f,u,v}^{\top}(A_{\text{id}} - A_f)\mathbf{x} = (x_v - x_u), \tag{1.4.33}$$

Observe that

$$\mathbf{c}_{f,u,v}^{\top}M^{-1}(A_{\text{id}} - A_{f^{(2)}})\mathbf{x} = \mathbf{c}_{f,u,v}^{\top}(M^{\top})^{-1}(A_{\text{id}} - A_f)M\mathbf{x} = (x_v - x_u), \tag{1.4.34}$$

However $(M^{\top})^{-1}\mathbf{c}_{f,u,v}$ does not necessarily lie in (Span of $A_{\text{id}}[:, n-1])^{\perp}$. Since $(A_{\text{id}}[:, n-1])^{\top}$ lies in the left kernel of $(A_{\text{id}} - A_{f^{(2)}})$ adding a multiple of $A_{\text{id}}[:, n-1]$ to $\mathbf{c}_{f,u,v}^{\top}M^{-1}$ does not affect the equality immediately above. Thus for all $0 \le u < v < n$ we have

$$\mathbf{c}_{f^{(2)},u,v} = H(M^{\top})^{-1}\mathbf{c}_{f,u,v}. \tag{1.4.35}$$

Now fix a basis matrix $B = [\mathbf{b}_0 \cdots \mathbf{b}_{n-2}]$ of the subspace (Span of $A_{\text{id}}[:, n-1])^{\perp}$ and define the transformed basis matrix to be

$$B' := H\,M^{-T}B = [\mathbf{b}'_0 \cdots \mathbf{b}'_{n-2}] \quad \text{with} \quad \mathbf{b}'_w := H(M^{\top})^{-1}\mathbf{b}_w \in (\text{Span of } A_{\text{id}}[:, n-1])^{\perp}. \tag{1.4.36}$$

$$\implies (B')^{+}\mathbf{c}_{f^{(2)},u,v} = B^{+}\mathbf{c}_{f,u,v}. \tag{1.4.37}$$

$$P_{f^{(2)}}\left(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2}\right) = \prod_{0 \le u < v < n}\left(\sum_{w \in \mathbb{Z}_{n-1}}(B^{+}\cdot\mathbf{c}_{f,u,v})_w\, y\mathbf{b}_w^{\top}\cdot M^{-1}\cdot(A_{\text{id}} - A_f)\cdot M\cdot\mathbf{x}\right)\times$$

$$\prod_{0\le u<v<n}\prod_{t\in\mathbb{Z}_2}\left(\left(A_{\text{id}}[v,:]\cdot(A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[u,:]\cdot(A_{\text{id}} - A_f)\right)\cdot M\cdot\mathbf{x}\right). \tag{1.4.38}$$

We see that the right hand side of the equality immediately above is devised from the expansion of the f-certificate with respect to the chosen basis $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$ by carrying the linear transformation

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \mapsto \left(M \oplus \left(I_{n-1} \otimes (M^\top)^{-1} \right) \right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}. \tag{1.4.39}$$

Part III.c. Remark on scalars vs basis change. We emphasize to the reader that the said linear transformation does not affect scalars

$$\{(B^+ \cdot \mathbf{c}_{f,u,v})_w \,:\, w \in \mathbb{Z}_{n-1}\}. \tag{1.4.40}$$

Thus the map prescribed by

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \mapsto \left(I_n \oplus \left(I_{n-1} \otimes (M^\top)^{-1} \right) \right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \tag{1.4.41}$$

in this particular setting does not equate to a base change in the expansion of the f-certificate with respect to the basis $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$. For we know that a change of basis must also affect scalars

$$\{(B^+ \cdot \mathbf{c}_{f,u,v})_w \,:\, w \in \mathbb{Z}_{n-1}\}, \tag{1.4.42}$$

in that they change to coefficients with respect to the new chosen basis vectors.

Part IV. Canonical representatives modulo the "grid" ideal forcing $x_i \in \mathbb{Z}_n$. Canonical representatives (i.e. remainders) of $P_f(\mathbf{x}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2})$ and $P_{f^{(2)}}(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2})$ modulo the polynomial ideal generated by $\{\prod_{j \in \mathbb{Z}_n} (x_i - j) :$ $i \in \mathbb{Z}_n\}$ are respectively

$$\overline{P_f(\mathbf{x}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2})} = y^{\binom{n}{2}} \prod_{v \in \mathbb{Z}_n} \left((v!)^2 \frac{(n-1+v)!}{(2v)!}\right) \sum_{\substack{\sigma \in \mathrm{S}_n \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma \circ |\sigma f - \sigma|) \prod_{i \in \mathbb{Z}_n} \Big(\prod_{j_i \in \mathbb{Z}_n \backslash \{\sigma(i)\}} \Big(\frac{x_i - j_i}{\sigma(i) - j_i}\Big)\Big), \tag{1.4.43}$$

and

$$\overline{P_{f^{(2)}}(\mathbf{x}, y\mathbf{b}'_0, \ldots, y\mathbf{b}'_{n-2})} =$$

$$y^{\binom{n}{2}} \prod_{v \in \mathbb{Z}_n} \left((v!)^2 \frac{(n-1+v)!}{(2v)!}\right) \sum_{\substack{\sigma \in \mathrm{S}_n \\ |\sigma f^{(2)} - \sigma| \in \mathrm{S}_n}} \mathrm{sgn}(\sigma \circ |\sigma f^{(2)} - \sigma|) \prod_{i \in \mathbb{Z}_n} \Big(\prod_{j_i \in \mathbb{Z}_n \backslash \{\sigma(i)\}} \Big(\frac{x_i - j_i}{\sigma(i) - j_i}\Big)\Big). \tag{1.4.44}$$

Observe from the expression immediately above of the canonical representative that non-vanishing evaluations over the lattice $\mathbb{Z}_n^{\mathbb{Z}_n}$ of P_f and $P_{f^{(2)}}$ are all equal up to sign and congruent to zero modulo n.

Part V. Finite field variant of f-certificate over $\mathbb{F}_p$ (to avoid the mod-n degeneracy). In the subsequent part of the argument we bypass investigations of ring homomorphisms (induced by taking the quotient of the ring $\mathbb{Q}[x_0, \ldots, x_{n-1}]$ modulo the ideal generated by members of $\big\{\prod_{j \in \mathbb{Z}_n} (x_i - j) \,:\, i \in \mathbb{Z}_n\big\}$) by switching the ground field from $\mathbb{Q}$ (i.e. rational numbers) to the Galois field of order $p = \lceil 2n-1 \rceil_{\mathbb{P}}$ (i.e. the smallest prime number greater than $2n-2$). We point out to the reader that any prime $p > 2n-2$ would work just as well in the our argument. We proceeds with the following variant of the f-certificate given by

$$\mathcal{P}_f(\mathbf{x}) = \left(\prod_{0\le u<v<n}(x_v-x_u)\right)\left(\prod_{0\le u<v<n}\Big((x_{f(v)}-x_v)^2-(x_{f(u)}-x_u)^2\Big)\right)\left(\prod_{i\in\mathbb{Z}_n}\Big(\prod_{j_i\in\mathbb{Z}_p\backslash\mathbb{Z}_n}(x_i-j_i)\Big)\right). \tag{1.4.45}$$

and the congruence class of interest is

$$\mathcal{P}_f\big(\mathbf{x}\big) \mod \Big\{\prod_{j\in\mathbb{Z}_p}(x_i-j) : i\in\mathbb{Z}_n\Big\}. \tag{1.4.46}$$

Note that every non vanishing evaluation point occurs at a lattice point of $\mathbb{Z}_n^{\mathbb{Z}_n}$ having exactly one zero entry. By construction the congruence class immediately above vanishes identically if and only if for all $r\in\mathbb{Z}_n$ the congruence class

$$\Bigg(\prod_{\substack{0\le u<v<n\\ r\notin\{u,v\}}}(x_v-x_u)\Bigg)\Bigg(\prod_{w\in\mathbb{Z}_n\backslash\{r\}}x_w\Bigg)\left(\prod_{i\in\mathbb{Z}_n\backslash\{r\}}\Big(\prod_{j_i\in\mathbb{Z}_p\backslash\mathbb{Z}_n}(x_i-j_i)\Big)\right)\times$$

$$\prod_{0\le u<v<n}\Bigg(\prod_{t\in\mathbb{Z}_2}\big(A_{\mathrm{id}}[v,:](A_{\mathrm{id}}-A_f)+(-1)^tA_{\mathrm{id}}[u,:](A_{\mathrm{id}}-A_f)\big)\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\Bigg) \mod \Big\{\prod_{j\in\mathbb{Z}_p}(x_i-j) : i\in\mathbb{Z}_n\backslash\{r\}\Big\} \tag{1.4.47}$$

vanishes identically. We make sense of the linear transformation by defining the expansion of a slight variant of the f-certificate that we call the (f,r)-certificate relative to an arbitrarily chosen basis $\{\mathbf{b}_0,\,\ldots,\,\mathbf{b}_{n-2}\}$ of (Span of $A_{\mathrm{id}}[:,n-1])^{\perp}$ and for some arbitrary $r\in\mathbb{Z}_n$ as follows:

$$\mathcal{P}_{f,r}\Bigg(\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}, y\mathbf{b}_0,\ldots,y\mathbf{b}_{n-2}\Bigg) = \prod_{0\le u<v<n}\Bigg(\sum_{w\in\mathbb{Z}_{n-1}}(B^{+}\mathbf{c}_{f,u,v})_w\,y\mathbf{b}_w^{\top}(A_{\mathrm{id}}-A_f)\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\Bigg)\times$$

$$\prod_{i<r}\Bigg(\prod_{j\in\mathbb{Z}_p\backslash\mathbb{Z}_n}\Big(-\sum_{w\in\mathbb{Z}_{n-1}}(B^{+}\mathbf{c}_{f,i,r})_w y\mathbf{b}_w^{\top}(A_{\mathrm{id}}-A_f)\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}-yj\Big)\Bigg)\prod_{i>r}\Bigg(\prod_{j\in\mathbb{Z}_p\backslash\mathbb{Z}_n}\Big(\sum_{w\in\mathbb{Z}_{n-1}}(B^{+}\mathbf{c}_{f,r,i})_w y\mathbf{b}_w^{\top}(A_{\mathrm{id}}-A_f)\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}-yj\Big)\Bigg)$$

$$\prod_{0\le u<v<n}\Bigg(\prod_{t\in\mathbb{Z}_2}\big(A_{\mathrm{id}}[v,:](A_{\mathrm{id}}-A_f)+(-1)^tA_{\mathrm{id}}[u,:](A_{\mathrm{id}}-A_f)\big)\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\Bigg). \tag{1.4.48}$$

Just as in the previous setting, for all basis vectors $\{\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}\}$ of (Span of $A_{\text{id}}[:, n-1])^{\perp}$ we have

$$\mathcal{P}_{f,r}\Big(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2}\Big) = y^{\binom{n}{2}+(n-1)(p-n)}\Bigg(\prod_{\substack{0 \le u < v < n \\ r \notin \{u,v\}}} (x_v - x_u)\Bigg)\Big(\prod_{w \in \mathbb{Z}_n \setminus \{r\}} x_w\Big)\Bigg(\prod_{i \in \mathbb{Z}_n \setminus \{r\}} \Big(\prod_{j_i \in \mathbb{Z}_p \setminus \mathbb{Z}_n} (x_i - j_i)\Big)\Bigg) \times$$

$$\prod_{0 \le u < v < n} \Bigg(\prod_{t \in \mathbb{Z}_2} \big(A_{\text{id}}[v,:](A_{\text{id}} - A_f) + (-1)^t A_{\text{id}}[u,:](A_{\text{id}} - A_f)\big)\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}\Bigg). \tag{1.4.49}$$

Part V.a. Explicit expression of (f,r)-certificates in terms of the f-certificate. By construction

$$\mathcal{P}_{f,r}\Big(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2}\Big) =$$

$$\Bigg(\prod_{\substack{i > r \\ j_i \in \mathbb{Z}_p \setminus \mathbb{Z}_n}} (y\,x_i - y\,x_r - j_i y) \prod_{\substack{i < r \\ j_i \in \mathbb{Z}_p \setminus \mathbb{Z}_n}} \big(-(y\,x_r - y\,x_i) - j_i y\big)\, P_f(\mathbf{x}, y\mathbf{b}_0, \ldots, y\mathbf{b}_{n-2}) \mod x_r\Bigg) \tag{1.4.50}$$

its canonical representative is

$$y^{\binom{n}{2}+(n-1)(p-n)} \prod_{v \in \mathbb{Z}_n} \Big((v!)^2 \frac{(n-1+v)!}{(2v)!}\Big) \prod_{v \in \mathbb{Z}_n \setminus \{r\}} \Big(\prod_{u \in \mathbb{Z}_p \setminus \mathbb{Z}_n} (v-u)\Big) \sum_{\substack{\sigma \in \mathrm{S}_n \\ \sigma(r) = 0 \\ |\sigma f - \sigma| \in \mathrm{S}_n}} \operatorname{sgn}(\sigma \circ |\sigma f - \sigma|) \prod_{i \in \mathbb{Z}_n \setminus \{r\}} \Big(\prod_{j_i \in \mathbb{Z}_p \setminus \{\sigma(i)\}} \Big(\frac{x_i - j_i}{\sigma(i) - j_i}\Big)\Big). \tag{1.4.51}$$

Part V.b. Compatibility of (f,r)-certificate with the same change of variables. Similarly to the previous setting, we consider for all $r\in\mathbb{Z}_n$ the linear transformation prescribed by the map

$$\begin{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\\ y\,\mathbf{b}_0\\ \vdots\\ y\,\mathbf{b}_i\\ \vdots\\ y\,\mathbf{b}_{n-2}\end{pmatrix}\mapsto\Big(M\oplus\big(I_{n-1}\otimes(M^\top)^{-1}\big)\Big)\cdot\begin{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\\ y\,\mathbf{b}_0\\ \vdots\\ y\,\mathbf{b}_i\\ \vdots\\ y\,\mathbf{b}_{n-2}\end{pmatrix}. \tag{1.4.52}$$

The latter linear transformation maps the (f,r)-certificate relative to an arbitrarily chosen basis $\{\mathbf{b}_0,\,\dots,\,\mathbf{b}_{n-2}\}$ of (Span of $A_{\mathrm{id}}[:,n-1]$)$^\perp$

$$\mathcal{P}_{f,r}\big(\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix},y\mathbf{b}_0,\dots,y\mathbf{b}_{n-2}\big)$$

to the $(f^{(2)},r)$-certificate relative to the basis $\left\{\mathbf{b}'_0,\dots,\mathbf{b}'_{n-2}\right\}$ of (Span of $A_{\mathrm{id}}[:,n-1]$)$^\perp$

$$\mathcal{P}_{f^{(2)},r}\big(\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix},y\mathbf{b}'_0,\dots,y\mathbf{b}'_{n-2}\big)=\prod_{0\le u<v<n}\big(\sum_{w\in\mathbb{Z}_{n-1}}(B^+\mathbf{c}_{f,u,v})_w\,y\mathbf{b}_w^\top M^{-1}(A_{\mathrm{id}}-A_f)M\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\big)\times$$

$$\prod_{i<r}\Big(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n}\big(-\sum_{w\in\mathbb{Z}_{n-1}}(B^+\mathbf{c}_{f,i,r})_w\,y\mathbf{b}_w^\top M^{-1}(A_{\mathrm{id}}-A_f)M\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}-yj\big)\Big)\times$$

$$\prod_{i>r}\Big(\prod_{j\in\mathbb{Z}_p\setminus\mathbb{Z}_n}\big(\sum_{w\in\mathbb{Z}_{n-1}}(B^+\mathbf{c}_{f,r,i})_w\,y\mathbf{b}_w^\top M^{-1}(A_{\mathrm{id}}-A_f)M\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}-yj\big)\Big)\times$$

$$\prod_{0\le u<v<n}\left(\prod_{t\in\mathbb{Z}_2}\big(A_{\mathrm{id}}[v,:](A_{\mathrm{id}}-A_f)+(-1)^t A_{\mathrm{id}}[u,:](A_{\mathrm{id}}-A_f)\big)M\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\right). \tag{1.4.53}$$

Part VI. Final implication and conclusion (invertible change preserves identically-zero polynomials). The latter (f,r)-certificate and $(f^{(2)},r)$-certificate favorably compare to the previous f-certificate and $f^{(2)}$-certificate in the sense that their non-vanishing evaluations over $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}_n}$ are not congruent to zero modulo p. We conclude the proof by showing that the vanishing identically of the (f,r)-certificate over $\mathbb{Z}/p\mathbb{Z}$ for all $r\in\mathbb{Z}_n$ implies the vanishing identically of the $(f^{(2)},r)$-certificate over $\mathbb{Z}/p\mathbb{Z}$ for all $r\in\mathbb{Z}_n$. The transformation prescribed by the action

$$\begin{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\\ y\,\mathbf{b}_0\\ \vdots\\ y\,\mathbf{b}_i\\ \vdots\\ y\,\mathbf{b}_{n-2}\end{pmatrix}\mapsto\Big(M\oplus\big(I_{n-1}\otimes(M^\top)^{-1}\big)\Big)\cdot\begin{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix}\\ y\,\mathbf{b}_0\\ \vdots\\ y\,\mathbf{b}_i\\ \vdots\\ y\,\mathbf{b}_{n-2}\end{pmatrix}. \tag{1.4.54}$$

is alternatively carried out by an action of some larger induced invertible matrix on the coefficient vector of the polynomial. By invertibility, such an action necessarily maps each identically vanishing (f,r)-certificate to an identically vanishing $(f^{(2)},r)$-certificate. Thereby resulting in the contrapositive of the assertion of the Composition Lemma.

$$\left(\mathcal{P}_{f,r}\Big(\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix},\,y\mathbf{b}_0,\,\dots,\,y\mathbf{b}_{n-2}\Big)\equiv 0,\;\forall\,r\in\mathbb{Z}_n\right)\implies\left(\mathcal{P}_{f^{(2)},r}\Big(\begin{pmatrix}x_0\\ \vdots\\ x_{r-1}\\ 0\\ x_{r+1}\\ \vdots\\ x_{n-1}\end{pmatrix},y\mathbf{b}'_0,\dots,y\mathbf{b}'_{n-2}\Big)\equiv 0,\;\forall\,r\in\mathbb{Z}_n\right). \tag{1.4.55}$$

For each $r\in\mathbb{Z}_n$, congruence classes above are taken modulo the ideal generated by $\big\{\prod_{j\in\mathbb{Z}_p}(x_i-j)\,:\,i\in\mathbb{Z}_n\backslash\{r\}\big\}$. Or equivalently we have

$$\left(\mathcal{P}_f(\mathbf{x})\equiv 0\mod\Big\{\prod_{j\in\mathbb{Z}_p}(x_i-j):i\in\mathbb{Z}_n\Big\}\right)\implies\left(\mathcal{P}_{f^{(2)}}(\mathbf{x})\equiv 0\mod\Big\{\prod_{j\in\mathbb{Z}_p}(x_i-j):i\in\mathbb{Z}_n\Big\}\right) \tag{1.4.56}$$

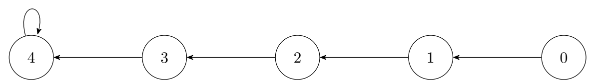
Thus

$$\big(\mathrm{GrL}(G_f)=\varnothing\implies\mathrm{GrL}(G_{f^{(2)}})=\varnothing\big)\iff\big(\mathrm{GrL}(G_{f^{(2)}})\neq\varnothing\implies\mathrm{GrL}(G_f)\neq\varnothing\big). \tag{1.4.57}$$

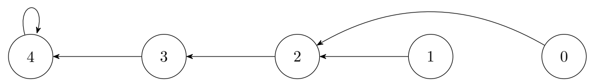
$\square$

Example 1.4.58. 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

[CCG24a] Parikshit Chalise, Antwan Clark, and Edinah K. Gnang. Every tree on n edges decomposes $k_{nx,nx}$ and k_{2nx+1}, 2024.

[CCG24b] Parikshit Chalise, Antwan Clark, and Edinah K. Gnang. A proof of the tree packing conjecture, 2024.

[Gna20] Edinah K. Gnang. On graceful labelings of trees, 2020.

[Gna22] Edinah K. Gnang. On the composition lemma, 2022.

[Gna23] Edinah K. Gnang. A proof of the kotzig-ringel-rosa conjecture, 2023.