Le Lemme de Composition.

January 16, 2026

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

$$V(G_f) = \mathbb{Z}_n, \quad E(G_f) = \{(v, f(v)) \colon v \in \mathbb{Z}_n\}. \tag{1}$$

The functional directed graph G_f of a function $f \in \mathbb{Z}_n^{\mathbb{Z}_n}$ is graceful if there exists a bijection $\sigma \in \mathrm{S}_n \subset \mathbb{Z}_n^{\mathbb{Z}_n}$ such that

$$\{|\sigma f \sigma^{-1}(i) - i| \colon i \in \mathbb{Z}_n\} = \mathbb{Z}_n. \tag{2}$$

We shall say that the function f itself is graceful. If $\sigma = \mathrm{id}$ (the identity function), then G_f (by extension f itself) is gracefully labeled. The set of distinct gracefully labeled functional directed graphs isomorphic to G_f is

$$\mathrm{GrL}(G_f) := \left\{ G_{\sigma f \sigma^{-1}} \colon \begin{array}{c} \sigma \text{ is a representative of a coset in } {}^{\mathrm{S}_n}\!/_{\mathrm{Aut}(G_f)} \text{ and} \\ \mathbb{Z}_n = \{|\sigma f \sigma^{-1}(i) - i| \colon i \in \mathbb{Z}_n\} \end{array} \right\}. \tag{3}$$

Fix $n \geq 2$, let $\mathcal{T}_n \subseteq \mathbb{Z}_n^{\mathbb{Z}_n}$ denote the semigroup defined as follows

$$\mathcal{T}_n := \{f \in \mathbb{Z}_n^{\mathbb{Z}_n} \colon f(i) > i \; \forall\, i \in \mathbb{Z}_{n-1}, \text{ and } f(n-1) = n-1\}.$$

Part I. Linear Algebra Setup (matrices, kernels, and a normalized solver)

For an arbitrary $h \in \mathbb{Z}_n^{\mathbb{Z}_n}$ let $A_h \in \{0,1\}^{n \times n}$ denote the adjacency matrix of G_h.

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

Let $L_h := (A_{\mathrm{id}} - A_h)$ denote the signed incidence matrix. Also let $\mathbf{e}_i$ denote the i-th standard basis vector (i.e. the i-th column of A_{id}) and

$$U := \{\mathbf{u} \in \mathbb{F}^{n \times 1} \colon \mathbf{u}[n-1] = 0\} = (\mathrm{Span}(\mathbf{e}_{n-1}))^{\perp}, \qquad H := (A_{\mathrm{id}} - \mathbf{e}_{n-1} \cdot \mathbf{e}_{n-1}^{\top}),$$

so that H is the orthogonal projector onto U.

Lemma 0.1 (*Rank and kernels of L_h*)**.** *For any $h \in \mathbb{Z}_n^{\mathbb{Z}_n}$, $\dim \ker(L_h)$ equals the number of connected components of G_h. Consequently*

$$\mathrm{rank}(L_h) = n - \#\{\text{connected components of } G_h\}.$$

In particular if $f \in \mathcal{T}_n$ then G_f is connected, hence $\mathrm{rank}(L_f) = n - 1$. Moreover for all $f \in \mathcal{T}_n$ one has

$$\ker(L_f) = \mathrm{Span}(1_{n \times 1}), \qquad \ker(L_f^{\top}) = \mathrm{Span}(\mathbf{e}_{n-1}).$$

Proof. $L_h \cdot \mathbf{x} = 0_{n \times 1}$ means $x_i = x_{h(i)}$ for all i, hence $\mathbf{x}$ is constant on each component; conversely any choice of constants on components gives a solution. This proves that the dimension of $\ker(L_h) = \#\{\text{connected components of } G_h\}$.

For $f \in \mathcal{T}_n$, every vertex flows to $n-1$, so the functional digraph is connected and by the rank-nullity theorem $\mathrm{rank}(L_f) = n - 1$. Also $L_f \cdot 1_{n \times 1} = 0_{n \times 1}$ is immediate, and any $\mathbf{x}$ with $L_f \cdot \mathbf{x} = 0_{n \times 1}$ must be constant on the unique component, so $\mathbf{x} \in \mathrm{Span}(1_{n \times 1})$. Finally $L_f^{\top} \cdot \mathbf{e}_{n-1} = 0$ because the last row of L_f is $0_{1 \times n}$, and the dimension of $\ker(L_f^{\top}) = 1$ since $\mathrm{rank}(L_f^{\top}) = \mathrm{rank}(L_f) = n - 1$. $\square$

Lemma 0.2 (*Normalized path-solvers $\mathbf{c}_{f,u,v}$*)*. Fix $f \in \mathcal{T}_n$. For each ordered pair (u,v) where $0 \leq u < v < n$ there exists a unique vector*

$$\mathbf{c}_{f,u,v} \in \{-1,0,1\}^{n \times 1} \subset U$$

such that

$$\mathbf{c}_{f,u,v}^\top \cdot L_f = (\mathbf{e}_v - \mathbf{e}_u)^\top \qquad \textit{equivalently} \qquad (\mathbf{c}_{f,u,v}^\top \cdot L_f \cdot \mathbf{x}) = x_v - x_u. \tag{4}$$

Proof. The vector $\mathbf{c}_{f,u,v}$ is obtained by telescoping vertices along the unique path in G_f spanning the vertex pair (u,v). If $\mathbf{c}, \mathbf{c}'$ are solutions then $(\mathbf{c} - \mathbf{c}')^\top \cdot L_f = 0$, hence $(\mathbf{c} - \mathbf{c}') \in \ker(L_f^\top) = \mathrm{Span}(\mathbf{e}_{n-1})$. Imposing $\mathbf{c} \in U$ (i.e. last coordinate of the vector $\mathbf{c}$ is 0) forces uniqueness. $\square$

Fix once and for all any basis $B = [\mathbf{b}_0 \ \cdots \ \mathbf{b}_{n-2}]$ for the subspace U. Over the field $\mathbb{F}$ of characteristic $\neq 2$ there exists a left inverse B^+ such that $B^+ \cdot B = I_{n-1}$ (e.g. the Moore–Penrose pseudoinverse). Define the coordinate vector

$$\boldsymbol{\alpha}_{f,B,u,v} := B^+ \cdot \mathbf{c}_{f,u,v} \in \mathbb{F}^{(n-1) \times 1}, \quad \text{so that} \quad \mathbf{c}_{f,u,v} = B \cdot \boldsymbol{\alpha}_{f,B,u,v}.$$

Part II. Polynomial f-certificates

Introduce indeterminates $x_0, \ldots, x_{n-1}$ entries of $\mathbf{x}$ and also treat the rows

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

as formal row-vector variables (y is a scalar indeterminate).

Define the *f-certificate (expanded with respect to the basis B)* by

$$P_{B,f}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right) := \prod_{0 \leq u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}^\top \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^\top \otimes L_f) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}}_{z_w} \right) \times$$

$$\prod_{\substack{0 \leq i < j < n \\ k \in \mathbb{Z}_2}} \left(\begin{pmatrix} \mathbf{e}_j + (-1)^k \mathbf{e}_i \\ 0_{(n^2-n) \times 1} \end{pmatrix}^\top \cdot (\mathbf{e}_0 \otimes \mathbf{e}_0^\top \otimes L_f) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_u \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right). \tag{5}$$

Equivalently written when no confusion arises from dependence of terms on the basis B as

$$P_{B,f}(\mathbf{x}, y) := \prod_{0 \leq u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{((y\mathbf{b}_w)^\top \cdot L_f \cdot \mathbf{x})}_{z_w} \right) \prod_{\substack{0 \leq i < j < n \\ k \in \mathbb{Z}_2}} \left((\mathbf{e}_j + (-1)^k \mathbf{e}_i) \cdot L_f \cdot \mathbf{x} \right). \tag{6}$$

Define also the *basis-free f-certificate* by

$$P_f(\mathbf{x}, y) := y^{\binom{n}{2}} \prod_{0 \leq u < v < n} \left((x_v - x_u)\big((x_{f(v)} - x_v)^2 - (x_{f(u)} - x_u)^2\big) \right). \tag{7}$$

Lemma 0.3 (*Basis-independence* of the f-certificates)**.** *For every $f \in \mathcal{T}_n$ and every choice of basis B of U,*

$$P_{B,f}(\mathbf{x}, y) = P_f(\mathbf{x}, y).$$

Equivalently,

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

hence $P_{B,f}$ is independent of the chosen expansion basis (even though (5) features rows $(y\,\mathbf{b}_0)^\top, \ldots, (y\,\mathbf{b}_{n-2})^\top$).

Proof. By (4), for each pair (u, v) subject to $0 \le u < v < n$ we have

$$\left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\left((y\mathbf{b}_w)^\top \cdot L_f \cdot \mathbf{x}\right)}_{z_w}\right) = \left(y\,(B \cdot \boldsymbol{\alpha}_{f,B,u,v})^\top \cdot L_f \cdot \mathbf{x}\right) = \left(y\,\mathbf{c}_{f,u,v}^\top \cdot L_f \cdot \mathbf{x}\right) = y(x_v - x_u).$$

Multiplying over all $0 \le u < v < n$ gives the vertex Vandermonde factor $y^{\binom{n}{2}} \prod_{0 \le u < v < n} (x_v - x_u)$. The edge factor

$$\prod_{\substack{0 \le i < j < n \\ k \in \mathbb{Z}_2}} \left((\mathbf{e}_j + (-1)^k \mathbf{e}_i) \cdot L_f \cdot \mathbf{x}\right)$$

is already expressed in a basis independent fashion, and equals

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

Therefore $P_{B,f}(\mathbf{x}, y) = P_f(\mathbf{x}, y)$ as claimed. $\qquad\square$

Remark (integrality for later and vertex Vandermonde symmetry). The right-hand side in Lemma 0.3 has *integer coefficients*. Thus, when we later reduce modulo a prime p, we reduce this integer-coefficient form (and do not need to interpret B^+ over $\mathbb{F}_p$). For the reader's benefit we have encapsulated in the variables z_w bilinear parts found in the vertex Vandermonde factor. For all $w \in \mathbb{Z}_{n-1}$

$$z_w = (y\,\mathbf{b}_w)^\top \cdot L_f \cdot \mathbf{x} = \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}^\top \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^\top \otimes L_f) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, \tag{8}$$

which will subsequently be key to expressing symmetries of the vertex Vandermonde factor to certain linear transformations.

Part III. Change of variables: relating f- and $f^{(2)}$-certificates

Let $M_f := (A_{\text{id}} + A_f)$. Note that $A_{f^{(2)}} = A_f^2$.

Lemma 0.4 (*Incidence factorization*)**.** *For $f \in \mathcal{T}_n$ one has*

$$L_{f^{(2)}} = (A_{\text{id}} - A_{f^{(2)}}) = (A_{\text{id}} - A_f^2) = (A_{\text{id}} - A_f) \cdot (A_{\text{id}} + A_f) = (A_{\text{id}} + A_f) \cdot (A_{\text{id}} - A_f) = L_f \cdot M_f = M_f \cdot L_f.$$

Proof. $A_{f^{(2)}} = A_f^2$ holds because following two edges in the functional digraph is composition. Then

$$(A_{\mathrm{id}} - A_f^2) = (A_{\mathrm{id}} - A_f) \cdot (A_{\mathrm{id}} + A_f) = (A_{\mathrm{id}} + A_f) \cdot (A_{\mathrm{id}} - A_f)$$

since A_f commutes with any polynomial in A_f. □

Lemma 0.5 (*Invertibility of M_f*)**.** *For $f \in \mathcal{T}_n$, $M_f = (A_{\mathrm{id}} + A_f)$ is upper triangular with diagonal entries $1, \ldots, 1, 2$. Hence* $\det(M_f) = 2$ *and* $M_f \in \mathrm{GL}_n(\mathbb{F}_p)$ *for all primes $p \neq 2$ (in particular for $p > 2n - 2$).*

Proof. For $i < n - 1$, $f(i) > i$ makes A_f strictly upper triangular on the first $n - 1$ rows, and $f(n-1) = n - 1$ contributes the bottom-right entry 1 in A_f, hence 2 in $A_{\mathrm{id}} + A_f$. □

We now describe the change of variables that we consider throughout this note. Consider the linear map

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

which in our setting is indistinguishable from the map

$$\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_w \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \mapsto \left(M_f \oplus \left(I_{n-1} \otimes \left(H \cdot (M_f^\top)^{-1} \right) \right) \right) \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_w \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}. \tag{9}$$

We work over a field of characteristic $\neq 2$ (so that M_f is invertible). The linear transformation is equivalently prescribed as a simultaneous linear maps

$$\mathbf{x} \longmapsto M_f \cdot \mathbf{x}, \qquad (y\mathbf{b}_w)^\top \longmapsto (y\mathbf{b}_w)^\top \cdot M_f^{-1} \qquad (w \in \mathbb{Z}_{n-1}),$$

which in our setting is indistinguishable from simultaneous maps

$$\mathbf{x} \longmapsto M_f \cdot \mathbf{x}, \qquad (y\mathbf{b}_w)^\top \longmapsto (y\mathbf{b}_w)^\top \cdot M_f^{-1} \cdot H \qquad (w \in \mathbb{Z}_{n-1}).$$

Lemma 0.6 (*Corrected transpose computation*)**.** *For every (u, v) pair subject to $0 \leq u < v < n$ and every $\mathbf{x}$,*

$$\mathbf{c}_{f,u,v}^\top \cdot M_f^{-1} \cdot L_{f^{(2)}} \cdot \mathbf{x} = (x_v - x_u).$$

Proof. Using Lemma 0.4 in the form $L_{f^{(2)}} = M_f \cdot L_f$, we get

$$\mathbf{c}_{f,u,v}^\top \cdot M_f^{-1} \cdot L_{f^{(2)}} \cdot \mathbf{x} = \mathbf{c}_{f,u,v}^\top \cdot M_f^{-1} \cdot M_f \cdot L_f \cdot \mathbf{x} = \mathbf{c}_{f,u,v}^\top \cdot L_f \cdot \mathbf{x} = (x_v - x_u).$$

by (4). □

Define the transformed basis in U by

$$B' := H \cdot (M_f^\top)^{-1} \cdot B \iff \mathbf{b}'_w := H \cdot (M_f^\top)^{-1} \cdot \mathbf{b}_w, \quad (w \in \mathbb{Z}_{n-1}).$$

(We project with H so that the transformed vectors remain in U.)

Lemma 0.7 (*Transport of the solvers and coordinates*). *For every (u,v) pair subject to $0 \le u < v < n$*

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

Consequently, the coordinate vectors are preserved:

$$\boldsymbol{\alpha}_{f^{(2)},B',u,v} = \big((B')^+ \cdot \mathbf{c}_{f^{(2)},u,v}\big) = (B^+ \cdot \mathbf{c}_{f,u,v}) = \boldsymbol{\alpha}_{f,B,u,v}.$$

Proof. Set $\tilde{\mathbf{c}} := H \cdot (M_f^\top)^{-1} \cdot \mathbf{c}_{f,u,v} \in U$. Then

$$\tilde{\mathbf{c}}^\top L_{f^{(2)}} = \mathbf{c}_{f,u,v}^\top \cdot M_f^{-1} \cdot H \cdot L_{f^{(2)}}.$$

But $(L_{f^{(2)}} \cdot \mathbf{x}) \in U$ for all $\mathbf{x}$ because the last row of $L_{f^{(2)}}$ is $0_{1 \times n}$ (since $f^{(2)}(n-1) = n-1$). Hence $H \cdot L_{f^{(2)}} = L_{f^{(2)}}$, and by Lemma 0.6 we have

$$\tilde{\mathbf{c}}^\top \cdot L_{f^{(2)}} = \big(\mathbf{c}_{f,u,v}^\top \cdot M_f^{-1} \cdot L_{f^{(2)}}\big) = (\mathbf{e}_v - \mathbf{e}_u)^\top.$$

By the uniqueness in Lemma 2 (applied to $f^{(2)}$), $\tilde{\mathbf{c}} = \mathbf{c}_{f^{(2)},u,v}$.

For the coordinate statement, note $\mathbf{c}_{f,u,v} = B \cdot (B^+ \mathbf{c}_{f,u,v})$ and apply $H \cdot (M_f^\top)^{-1}$ to obtain

$$\mathbf{c}_{f^{(2)},u,v} = B' \cdot \underbrace{(B^+ \cdot \mathbf{c}_{f,u,v})}_{\boldsymbol{\alpha}_{f,B,u,v}},$$

so $\boldsymbol{\alpha}_{f,B,u,v} = (B^+ \cdot \mathbf{c}_{f,u,v})$ is a valid coordinate vector of $\mathbf{c}_{f^{(2)},u,v}$ with respect to the basis B', hence

$$\boldsymbol{\alpha}_{f,B,u,v} = (B^+ \cdot \mathbf{c}_{f,u,v}) = \big((B')^+ \cdot \mathbf{c}_{f^{(2)},u,v}\big) = \boldsymbol{\alpha}_{f^{(2)},B',u,v}.$$

$\square$

Lemma 0.8 (*Certificate covariance under the change of variables*). *Under the substitution* (9)*, the expanded f-certificate $P_{B,f}$ transforms into the expanded $f^{(2)}$-certificate $P_{B',f^{(2)}}$ written in the transformed basis B' defined above. Let T_f denote the $n^2 \times n^2$ matrix defined by*

$$T_f := M_f \oplus \Big(I_{n-1} \otimes \big(H \cdot (M_f^\top)^{-1}\big)\Big).$$

We have

$$P_{B,f}\left(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right) = P_{B',f^{(2)}}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0' \\ \vdots \\ y\,\mathbf{b}_i' \\ \vdots \\ y\,\mathbf{b}_{n-2}' \end{pmatrix}\right)$$

In particular

$$P_{B,f}\left(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right) = P_{f^{(2)}}(\mathbf{x}, y).$$

5

126 *Proof.* Invoking the definition (5) yields

127
$$P_{B,f}(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) = \prod_{0 \le u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\left(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right)^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}}_{z'_w} \right) \times$$

128

129
$$\prod_{\substack{0 \le i < j < n \\ k \in \mathbb{Z}_2}} \left(\left(\begin{pmatrix} \mathbf{e}_j + (-1)^k \mathbf{e}_i \\ 0_{(n^2-n) \times 1} \end{pmatrix}^{\top} \cdot (\mathbf{e}_0 \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_u \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right) \right),$$

130 by the argument which relates B to B' in the proof of Lemma 0.7

131
$$\implies P_{B,f}(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) = \prod_{0 \le u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\begin{pmatrix} M_f \cdot \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix}^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot \begin{pmatrix} M_f \cdot \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix}}_{z'_w} \right) \times$$

132

133
$$\prod_{\substack{0 \le i < j < n \\ k \in \mathbb{Z}_2}} \left(\left(\begin{pmatrix} \mathbf{e}_j + (-1)^k \mathbf{e}_i \\ 0_{(n^2-n) \times 1} \end{pmatrix}^{\top} \cdot (\mathbf{e}_0 \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot \begin{pmatrix} M_f \cdot \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right) \right),$$

134 written alternatively

135
$$\implies P_{B,f}(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) = \prod_{0 \le u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\left((y\mathbf{b}'_w)^{\top} \cdot L_f \cdot M_f \cdot \mathbf{x} \right)}_{z'_w} \right) \prod_{\substack{0 \le i < j < n \\ k \in \mathbb{Z}_2}} \left((\mathbf{e}_j + (-1)^k \mathbf{e}_i) \cdot L_f \cdot M_f \cdot \mathbf{x} \right)$$

136 by Lemma 0.4

137
$$\implies P_{B,f}(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) = \prod_{0 \le u < v < n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \underbrace{\left((y\mathbf{b}'_w)^{\top} \cdot L_{f^{(2)}} \cdot \mathbf{x} \right)}_{z'_w} \right) \prod_{\substack{0 \le i < j < n \\ k \in \mathbb{Z}_2}} \left((\mathbf{e}_j + (-1)^k \mathbf{e}_i) \cdot L_{f^{(2)}} \cdot \mathbf{x} \right).$$

6

by the last equality in the proof of Lemma 0.7

$$\implies P_{B,f}\left(T_f\cdot\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\right)=\prod_{0\le u<v<n}\left(\sum_{w\in\mathbb{Z}_{n-1}}\boldsymbol{\alpha}_{f^{(2)},B',u,v}[w]\underbrace{\left((y\mathbf{b}'_w)^\top\cdot L_{f^{(2)}}\cdot\mathbf{x}\right)}_{z'_w}\right)\prod_{\substack{0\le i<j<n\\k\in\mathbb{Z}_2}}\left((\mathbf{e}_j+(-1)^k\mathbf{e}_i)\cdot L_{f^{(2)}}\cdot\mathbf{x}\right).$$

$$\implies P_{B,f}\left(T_f\cdot\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\right)=\prod_{0\le u<v<n}\Big(\sum_{w\in\mathbb{Z}_{n-1}}\boldsymbol{\alpha}_{f^{(2)},B',u,v}[w]\underbrace{\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}'_0\\\vdots\\y\,\mathbf{b}'_i\\\vdots\\y\,\mathbf{b}'_{n-2}\end{pmatrix}^\top\cdot(\mathbf{e}_w\otimes\mathbf{e}_0^\top\otimes L_{f^{(2)}})\cdot\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}'_0\\\vdots\\y\,\mathbf{b}'_i\\\vdots\\y\,\mathbf{b}'_{n-2}\end{pmatrix}}_{z'_w}\Big)\times$$

$$\prod_{\substack{0\le i<j<n\\k\in\mathbb{Z}_2}}\left(\begin{pmatrix}\mathbf{e}_j+(-1)^k\mathbf{e}_i\\0_{(n^2-n)\times1}\end{pmatrix}^\top\cdot(\mathbf{e}_0\otimes\mathbf{e}_0^\top\otimes L_{f^{(2)}})\cdot\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}'_0\\\vdots\\y\,\mathbf{b}'_i\\\vdots\\y\,\mathbf{b}'_{n-2}\end{pmatrix}\right).$$

$$\implies P_{B,f}\left(T_f\cdot\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\right)=P_{B',f^{(2)}}\left(\begin{pmatrix}\mathbf{x}\\y\,\mathbf{b}'_0\\\vdots\\y\,\mathbf{b}'_i\\\vdots\\y\,\mathbf{b}'_{n-2}\end{pmatrix}\right).$$

as claimed. $\qquad\square$

Remark: Since in the next to last equality the basis B' in $\boldsymbol{\alpha}_{f^{(2)},B',u,v}$ is align with vectors $(y\,\mathbf{b}'_0)^\top,\dots,(y\,\mathbf{b}'_{n-2})^\top$ it follows that $P_{B',f^{(2)}}$ is invariant to basis B' change.

Part IV. The $\mathbb{Z}_n$–grid ideal and canonical remainders (base ring made explicit)

Throughout Parts IV–VI we work in polynomial rings in the variables

$$\mathbf{x}=(x_0,\dots,x_{n-1})$$

with coefficients in a *coefficient ring* K (e.g. $K=\mathbb{Q}$ or $K=\mathbb{F}_p$), possibly enlarged by adjoining auxiliary indeterminates (such as y and the formal rows $(y\mathbf{b}_w)^\top$). Whenever an integer $j\in\mathbb{Z}$ appears inside K, we mean its image under the canonical map $\mathbb{Z}\to K$.

For such a ring K write $K[\mathbf{x}]:=K[x_0,\dots,x_{n-1}]$ and define the $\mathbb{Z}_n$–grid ideal over K by

$$\mathcal{I}_n^{(K)}:=\left\langle\prod_{j\in\mathbb{Z}_n}(x_i-j)\colon i\in\mathbb{Z}_n\right\rangle\subset K[\mathbf{x}].$$

If S is any K–algebra (for instance $S=K[y]$ or $S=K[y,\{(y\mathbf{b}_w)[i]\}]$), we write again $\mathcal{I}_n^{(K)}$ for its extension $\mathcal{I}_n^{(K)}S[\mathbf{x}]\subset S[\mathbf{x}]$.

7

In this part we take $K = \mathbb{Q}$ and, to simplify notation, we set

$$\mathcal{I}_n := \mathcal{I}_n^{(\mathbb{Q})} \subset \mathbb{Q}[\mathbf{x}],$$

and we also write $\mathcal{I}_n$ for its extension to $\mathbb{Q}[y][\mathbf{x}]$ (and to any larger $\mathbb{Q}$–algebra obtained by adjoining auxiliary indeterminates). Write $\overline{F}$ for the canonical remainder of a polynomial $F \in (\mathbb{Q}[y])[\mathbf{x}]$ modulo $\mathcal{I}_n$ (with respect to the variables $x_0, \ldots, x_{n-1}$).

Lemma 0.9 (*Remainder detects graceful labelings*). *For $f \in \mathcal{T}_n$, the remainder $\overline{P_f}$ is a $\mathbb{Z}$-linear combination of Lagrange basis polynomials on $(\mathbb{Z}_n)^{n \times 1}$, with coefficients $P_f(\mathbf{v}, y)$ for $\mathbf{v} \in (\mathbb{Z}_n)^{n \times 1}$. Given by*

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

In particular

$$\overline{P_f} \text{ is identically zero} \iff P_f(\mathbf{v}, y) = 0 \text{ for all } \mathbf{v} \in (\mathbb{Z}_n)^{n \times 1} \iff \mathrm{GrL}(G_f) = \varnothing.$$

Proof. Modulo the ideal $\mathcal{I}_n$, every polynomial is uniquely represented by its multivariate Lagrange interpolation remainder on the grid $(\mathbb{Z}_n)^n$. Thus $\overline{P_f}$ is identically zero iff all grid values $P_f(\mathbf{v}, y)$ vanish. The claimed expansion follows from the equality

$$\overline{P_f}(\mathbf{x}, y) = y^{\binom{n}{2}} \sum_{\sigma \in \mathrm{S}_n} \prod_{0 \leq u < v < n} \left(\sigma(v) - \sigma(u) \right) \left(\left(\sigma(v) - \sigma f(v) \right)^2 - \left(\sigma(u) - \sigma f(u) \right)^2 \right) \prod_{i \in \mathbb{Z}_n} \left(\prod_{j_i \in \mathbb{Z}_n \setminus \{\sigma(i)\}} \frac{x_i - j_i}{\sigma(i) - j_i} \right).$$

By Lemma 0.3, $P_f(\mathbf{v}, y)$ features the factor $\prod_{0 \leq i < j < n} (v_j - v_i)$, hence vanishes unless entries of $\mathbf{v}$ yields a permutation of $\mathbb{Z}_n$; such $\mathbf{v}$ correspond to $\sigma \in \mathrm{S}_n$ via the equality $v_i = \sigma(i)$ for all $i \in \mathbb{Z}_n$. Thus the edge Vandermonde factor is nonzero iff

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

in other words iff $\sigma f \sigma^{-1}$ is gracefully labeled. This is exactly the condition $\mathrm{GrL}(G_f) \neq \varnothing$. $\qquad\square$

Part V. Finite field variants over $\mathbb{F}_p$ and (f, r)–certificates

A direct use of Lemma 0.8 over the $\mathbb{Z}_n$-*grid* is obstructed because the linear map $\mathbf{x} \mapsto M_f \cdot \mathbf{x}$ does not preserve the lattice $(\mathbb{Z}_n)^{n \times 1}$. We therefore pass to a prime field $\mathbb{F}_p$ and a grid ideal stable under linear changes.

Fix a prime $p > 2(n-1)$. In particular, $p \neq 2$ and all integers $1, 2, \ldots, 2n-2$ are nonzero in $\mathbb{F}_p$.

We will use the coefficientwise reduction map

$$\pi_p : \mathbb{Z}[\mathbf{x}, y] \longrightarrow \mathbb{F}_p[\mathbf{x}, y],$$

and for any integer-coefficient polynomial F we write $F^{(p)} := \pi_p(F)$. By Lemma 0.3 the basis-free certificates $P_f(\mathbf{x}, y)$ lie in $\mathbb{Z}[\mathbf{x}, y]$, so $P_f^{(p)}$ is well-defined. (The expanded form $P_{B,f}$ may involve denominators coming from B^+, but we never need to reduce those denominators modulo p thanks to basis-independence.)

Because any permutation labeling uses the value 0 exactly once, it is convenient to slice by the index r where the label 0 occurs.

Definition 0.10 (*Expanded cutoff polynomial $\mathcal{C}_{f,r,B}$*). *Fix $f \in \mathcal{T}_n$, a basis $B = [\mathbf{b}_0 \ \ldots \ \mathbf{b}_{n-2}]$ of U, and $r \in \mathbb{Z}_n$. For*

$\mathbf{x} \in \mathbb{F}_p^{n \times 1}$ *we impose* $x_r = 0$ *and define*

$$
\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y\right) := \prod_{i<r} \prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \left(\sum_{w \in \mathbb{Z}_{n-1}} (-\boldsymbol{\alpha}_{f,B,i,r}[w]) \underbrace{\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot \begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}}_{z_{w,r}} - y\,j \right) \times
$$

$$
\prod_{i>r} \prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \left(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,r,i}[w] \underbrace{\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_f) \cdot \begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}}_{z_{w,r}} - y\,j \right).
$$

$$(10)$$

Definition 0.11 (*Basis-free cutoff polynomial* $\mathcal{C}_r$). *Fix* $r \in \mathbb{Z}_n$ *and define*

$$
\mathcal{C}_r(\mathbf{x}, y) := \prod_{i \in \mathbb{Z}_n \setminus \{r\}} \left(\prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \big(y\,(x_i - x_r) - y\,j \big) \right).
$$

Lemma 0.12 (*Basis-independence of the cutoff polynomial*). *For every* $f \in \mathcal{T}_n$, *every basis* B *of* U, *and every* $r \in \mathbb{Z}_n$,

$$
\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y\right) = \mathcal{C}_r\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y \right).
$$

9

In particular, $\mathcal{C}_{f,r,B}$ does not depend on the choice of basis B, nor on $f \in \mathcal{T}_n$.

Proof. Exactly as in the proof of Lemma 0.3, for every pair (u, v) with $0 \leq u < v < n$ we have

$$\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,u,v}[w] \left(\underbrace{(y \mathbf{b}_w)^\top \cdot L_f \cdot \mathbf{x}}_{z_w} \right) = y(x_v - x_u).$$

In (10) we always apply this identity with $v = r$ and with $x_r = 0$. Recall that

$$z_{w,r} = \left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y \, \mathbf{b}_0 \\ \vdots \\ y \, \mathbf{b}_i \\ \vdots \\ y \, \mathbf{b}_{n-2} \end{pmatrix} \right)^\top \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^\top \otimes L_f) \cdot \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y \, \mathbf{b}_0 \\ \vdots \\ y \, \mathbf{b}_i \\ \vdots \\ y \, \mathbf{b}_{n-2} \end{pmatrix}.$$

For $i < r$ we use the coefficients $-\boldsymbol{\alpha}_{f,B,i,r}$, hence

$$\sum_{w \in \mathbb{Z}_{n-1}} \left(-\boldsymbol{\alpha}_{f,B,i,r}[w] \right) z_{w,r} = -y \left(x_r - x_i \right) = y \left(x_i - x_r \right),$$

and for $i > r$ we use $\boldsymbol{\alpha}_{f,B,r,i}$, hence

$$\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f,B,r,i}[w] \, z_{w,r} = y \left(x_i - x_r \right).$$

Therefore every factor in (10) is exactly $\left(y \left(x_i - x_r \right) - y\,j \right)$ with $j \in \mathbb{Z}_p \setminus \mathbb{Z}_n$. Multiplying over $i < r$ and $i > r$ yields

$$\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \mathbf{x} \\ y \, \mathbf{b}_0 \\ \vdots \\ y \, \mathbf{b}_i \\ \vdots \\ y \, \mathbf{b}_{n-2} \end{pmatrix}, y \right) = \prod_{i \in \mathbb{Z}_n \setminus \{r\}} \left(\prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \left(y(x_i - x_r) - y\,j \right) \right) = \mathcal{C}_r(\mathbf{x}, y),$$

which is the desired equality. $\square$

Definition 0.13 (*The (f,r)–certificate*). *For $r \in \mathbb{Z}_n$, define*

$$\mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) := P_{B,f}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right)\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right).$$

Note that we have imposed $x_r = 0$.

Lemma 0.14 (*Evaluation meaning of (f,r)–certificates*). *For any assignment $\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \in (\mathbb{F}_p)^{n\times 1}$ one has*

$$\mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) \neq 0 \Leftrightarrow \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} \sigma(0) \\ \vdots \\ \sigma(r-1) \\ \sigma(r) = 0 \\ \sigma(r+1) \\ \vdots \\ \sigma(n-1) \end{pmatrix} \text{ for some } \sigma \in S_n \text{ and } \sigma f \sigma^{-1} \text{ is gracefully labeled.}$$

210   *Consequently,*

$$\mathrm{GrL}(G_f) \neq \varnothing \iff \exists\, r \in \mathbb{Z}_n \text{ such that } \mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) \text{ is not identically zero on } \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \in \mathbb{F}_p^{n \times 1}.$$

212   *Proof.* If $x_r = 0$ and some $x_i \notin \mathbb{Z}_n$, then $x_i - x_r \notin \mathbb{Z}_n$ and $\mathcal{C}_r\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y\right) = 0$, so

$$213 \qquad \mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) = 0.$$

214   Thus nonvanishing forces $x_i \in \mathbb{Z}_n$ for all i, i.e. $\mathbf{x} \in (\mathbb{Z}_n)^{n \times 1}$ with $x_r = 0$.

215   On $(\mathbb{Z}_n)^{n \times 1}$, Lemma 0.3 and Lemma 0.9 show $P_f\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y\right) \neq 0$ precisely on permutations which yield graceful

labelings, and the additional factors $\mathcal{C}_r\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix}, y\right)$ are nonzero for such points (since all values lie in $\mathbb{Z}_n$). The final

equivalence follows because every graceful labeling has a unique r with label 0. $\qquad\square$

Part VI. A stable $\mathbb{F}_p$–grid ideal and the pullback step

Fix the prime $p > 2(n-1)$ from Part V and set $K := \mathbb{F}_p$. Let S denote any K–algebra obtained by adjoining auxiliary indeterminates (in particular y and the formal rows $(y\mathbf{b}_w)^\top$). We work in the polynomial ring $S[\mathbf{x}] = S[x_0, \dots, x_{n-1}]$ in the variables $\mathbf{x} = (x_0, \dots, x_{n-1})$.

We now use the *full $\mathbb{F}_p$–grid ideal*

$$\mathcal{J}_p := \langle x_i^p - x_i : i \in \mathbb{Z}_n \rangle \subset \mathbb{F}_p[\mathbf{x}],$$

and, by abuse of notation, we also write $\mathcal{J}_p$ for its extension $\mathcal{J}_p S[\mathbf{x}] \subset S[\mathbf{x}]$. The key facts are:

Lemma 0.15 (*The ideal $\mathcal{J}_p$ is the vanishing ideal of $\mathbb{F}_p^n$*)**.** *Let S be a $K = \mathbb{F}_p$–algebra and consider $S[\mathbf{x}] = S[x_0, \dots, x_{n-1}]$. A polynomial $F \in S[\mathbf{x}]$ vanishes at every point of $\mathbb{F}_p^n$ (i.e. $F(\mathbf{a}) = 0$ for all $\mathbf{a} \in \mathbb{F}_p^n$) if and only if $F \in \mathcal{J}_p$ (viewed as the extended ideal $\mathcal{J}_p S[\mathbf{x}]$). In particular, if $F \in \mathcal{J}_p$ then F vanishes on $\mathbb{F}_p^n$.*

Proof. Reducing successively in each variable using the relations $x_i^p \equiv x_i \pmod{x_i^p - x_i}$ yields a canonical remainder $\overline{F}$ such that $F - \overline{F} \in \mathcal{J}_p$ and $\deg_{x_i}(\overline{F}) < p$ for all i. If F vanishes on $\mathbb{F}_p^n$ then so does $\overline{F}$. Fix all variables except x_0 and view $\overline{F}$ as a polynomial in x_0 of degree $< p$ with coefficients in $S[x_1, \dots, x_{n-1}]$; vanishing at all p values of $x_0 \in \mathbb{F}_p$ forces all these coefficients to vanish (the $p \times p$ Vandermonde matrix on $\mathbb{F}_p$ is invertible over $\mathbb{F}_p \subset S$). Iterating this argument over $x_1, \dots, x_{n-1}$ shows $\overline{F} = 0$, hence $F \in \mathcal{J}_p$. The converse direction is immediate since each generator $x_i^p - x_i$ vanishes on $\mathbb{F}_p$. $\qquad\square$

Lemma 0.16 (*Grid ideal stability under linear maps*)**.** *Let S be a $K = \mathbb{F}_p$–algebra and view $\mathcal{J}_p$ as an ideal of $S[\mathbf{x}]$. Let M be an $n \times n$ matrix with entries in $\mathbb{F}_p$. Then the substitution $\mathbf{x} \longmapsto M \cdot \mathbf{x}$ preserves $\mathcal{J}_p$. In particular, if $P(\mathbf{x}) \in \mathcal{J}_p$ then $P(M \cdot \mathbf{x}) \in \mathcal{J}_p$.*

Proof. Write $(M \cdot \mathbf{x})[i] = \sum_{j \in \mathbb{Z}_n} M[i,j]\, x_j$. Over $\mathbb{F}_p$ the Frobenius map satisfies $\left(\sum_{j \in \mathbb{Z}_n} a_j x_j\right)^p = \sum_{j \in \mathbb{Z}_n} a_j^p x_j^p = \sum_{j \in \mathbb{Z}_n} a_j x_j^p$. Hence

$$\big((Mx)_i\big)^p - (Mx)_i = \sum_{j \in \mathbb{Z}_n} M_{ij}(x_j^p - x_j) \in \mathcal{J}_p,$$

so $\mathcal{J}_p$ is preserved. $\qquad\square$

Lemma 0.17 (*Change of variables for $\mathcal{C}_r$*)**.** *Let $r \in \mathbb{Z}_n$. Under the substitution* (9)*, the cutoff polynomial $\mathcal{C}_r$ remains*

13

unchanged:

$$
\mathcal{C}_{f,r,B}\left(T_f \cdot \begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y \right) = \mathcal{C}_{f^{(2)},r,B'}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \end{pmatrix}, y \right) = \mathcal{C}_{f,r,B}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y \right),
$$

where $T_f := M_f \oplus \left(I_{n-1} \otimes \left(H \cdot (M_f^\top)^{-1} \right) \right)$.

Proof. The proof proceed similarly to the proof of Lemma 0.8 as follows. Invoking Equation (10) and skipping some of the steps carrying out the linear transformation we write

$$
\mathcal{C}_{f,r,B}\left(T_f \cdot \begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y \right) =
$$

14

$$\prod_{i<r}\prod_{j\in\mathbb{Z}_p\backslash\mathbb{Z}_n}\Big(\sum_{w\in\mathbb{Z}_{n-1}}(-\boldsymbol{\alpha}_{f,B,i,r}[w])\left(T_f\cdot\begin{pmatrix}\begin{pmatrix}x_0\\\vdots\\x_{r-1}\\0\\x_{r+1}\\\vdots\\x_{n-1}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\end{pmatrix}\right)^{\top}\cdot(\mathbf{e}_w\otimes\mathbf{e}_0^{\top}\otimes L_f)\cdot T_f\cdot\underbrace{\begin{pmatrix}\begin{pmatrix}x_0\\\vdots\\x_{r-1}\\0\\x_{r+1}\\\vdots\\x_{n-1}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\end{pmatrix}}_{z'_{w,r}}-y\,j\Big)\times$$

$$\prod_{i>r}\prod_{j\in\mathbb{Z}_p\backslash\mathbb{Z}_n}\Big(\sum_{w\in\mathbb{Z}_{n-1}}\boldsymbol{\alpha}_{f^{(2)},B',r,i}[w]\left(T_f\cdot\begin{pmatrix}\begin{pmatrix}x_0\\\vdots\\x_{r-1}\\0\\x_{r+1}\\\vdots\\x_{n-1}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\end{pmatrix}\right)^{\top}(\mathbf{e}_w\otimes\mathbf{e}_0^{\top}\otimes L_f)\cdot T_f\cdot\underbrace{\begin{pmatrix}\begin{pmatrix}x_0\\\vdots\\x_{r-1}\\0\\x_{r+1}\\\vdots\\x_{n-1}\\y\,\mathbf{b}_0\\\vdots\\y\,\mathbf{b}_i\\\vdots\\y\,\mathbf{b}_{n-2}\end{pmatrix}\end{pmatrix}}_{z'_{w,r}}-y\,j\Big),$$

$$= \prod_{i<r} \prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \Big(\sum_{w \in \mathbb{Z}_{n-1}} (-\boldsymbol{\alpha}_{f^{(2)},B',i,r}[w]) \underbrace{\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right)^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_{f^{(2)}}) \cdot \left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right)}_{z'_{w,r}} - y\,j \Big) \times$$

$$\prod_{i>r} \prod_{j \in \mathbb{Z}_p \setminus \mathbb{Z}_n} \Big(\sum_{w \in \mathbb{Z}_{n-1}} \boldsymbol{\alpha}_{f^{(2)},B',r,i}[w] \underbrace{\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right)^{\top} \cdot (\mathbf{e}_w \otimes \mathbf{e}_0^{\top} \otimes L_{f^{(2)}}) \cdot \left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right)}_{z'_{w,r}} - y\,j \Big),$$

$$= \mathcal{C}_{f^{(2)},r,B'}\left(\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \right), y \right) = \mathcal{C}_{f,r,B}\left(\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right), y \right).$$

as claimed. $\square$

Lemma 0.18 (*No accidental modulo–p zeros on the $\mathbb{Z}_n$–grid*)**.** *Assume $p > 2(n-1)$ is prime and view $\mathbb{Z}_n = \{0,\dots,n-1\}$ as a subset of $\mathbb{F}_p$. Let $f \in \mathcal{T}_n$ and let $\mathbf{v} \in (\mathbb{Z}_n)^{n \times 1}$. Write*

$$\Delta_i(\mathbf{v}) := v_{f(i)} - v_i \in \{-(n-1),\dots,n-1\} \subset \mathbb{Z}.$$

Define the integer

$$Q_f(\mathbf{v}) := \prod_{0 \le u < v < n} (v_v - v_u) \prod_{0 \le u < v < n} \left(\Delta_v(\mathbf{v})^2 - \Delta_u(\mathbf{v})^2 \right) \in \mathbb{Z}.$$

Then, reducing modulo p, one has

$$Q_f(\mathbf{v}) \equiv 0 \pmod{p} \quad \Longleftrightarrow \quad Q_f(\mathbf{v}) = 0 \ in \ \mathbb{Z}.$$

Equivalently, since $P_f(\mathbf{x}, y) = y^{\binom{n}{2}} Q_f(\mathbf{x})$ has integer coefficients,

$$P_f(\mathbf{v}, y) \equiv 0 \ in \ \mathbb{F}_p[y] \quad \Longleftrightarrow \quad P_f(\mathbf{v}, y) = 0 \ in \ \mathbb{Z}[y].$$

Proof. If an integer a satisfies $|a| < p$ and $a \equiv 0 \pmod{p}$, then $a = 0$. For the first product, each factor $v_j - v_i$ lies in $\{-(n-1), \ldots, n-1\}$, hence is either 0 or a unit modulo p. For the second product, each $\Delta_i(\mathbf{v})$ lies in $\{-(n-1), \ldots, n-1\}$, so for any pair $u < v$ we have

$$\left(\Delta_j(\mathbf{v}) \right)^2 - \left(\Delta_i(\mathbf{v}) \right)^2 = \left(\Delta_j(\mathbf{v}) - \Delta_i(\mathbf{v}) \right) \left(\Delta_j(\mathbf{v}) + \Delta_i(\mathbf{v}) \right),$$

where both factors lie in $\{-(2n-2), \ldots, 2n-2\}$ and hence have absolute value $< p$. Thus p divides $\left(\Delta_j(\mathbf{v}) \right)^2 - \left(\Delta_i(\mathbf{v}) \right)^2$ if and only if $\left(\Delta_j(\mathbf{v}) - \Delta_i(\mathbf{v}) \right) = 0$ or $\left(\Delta_j(\mathbf{v}) + \Delta_i(\mathbf{v}) \right) = 0$ as integers, i.e. if and only if $\left(\Delta_j(\mathbf{v}) \right)^2 = \left(\Delta_i(\mathbf{v}) \right)^2$ in $\mathbb{Z}$. Therefore each factor in the definition of $Q_f(\mathbf{v})$ is either 0 in $\mathbb{Z}$ or a unit modulo p, so the whole product is 0 modulo p if and only if it is 0 in $\mathbb{Z}$. The final equivalence follows from $P_f(\mathbf{v}, y) = y^{\binom{n}{2}} Q_f(\mathbf{v})$. $\qquad \square$

Lemma 0.19 (*Covariance for (f, r)–certificates*). *For all $f \in \mathcal{T}_n$,*

$$P_{B,f}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right) \in \mathcal{I}_n \implies P_{B', f^{(2)}}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0' \\ \vdots \\ y\,\mathbf{b}_i' \\ \vdots \\ y\,\mathbf{b}_{n-2}' \end{pmatrix} \right) \in \mathcal{I}_n,$$

where $\mathcal{I}_n = \mathcal{I}_n^{(\mathbb{Q})}$ is the $\mathbb{Z}_n$–grid ideal over $\mathbb{Q}$ (extended to the ambient polynomial ring). Equivalently, the basis-free certificates satisfy $P_f \in \mathcal{I}_n \Rightarrow P_{f^{(2)}} \in \mathcal{I}_n$.

Proof. Assume $P_{B,f} \in \mathcal{I}_n$. By Lemma 0.3 we have the identity of polynomials $P_{B,f}(\mathbf{x}, y) = P_f(\mathbf{x}, y)$ with $P_f \in \mathbb{Z}[\mathbf{x}, y]$. By Lemma 0.9, the assumption $P_f \in \mathcal{I}_n$ is equivalent to

$$P_f(\mathbf{v}, y) = 0 \quad \text{in } \mathbb{Z}[y] \quad \text{for all } \mathbf{v} \in (\mathbb{Z}_n)^{n \times 1}.$$

Fix $r \in \mathbb{Z}_n$. Consider the (f, r)–certificate

$$\mathcal{P}_{B,f,r}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y \right) = P_{B,f}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \right) \cdot \mathcal{C}_{f,r,B}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y \right),$$

with the specialization $x_r = 0$. By Lemmas 0.3 and 0.12 this equals the basis-free product

$$\mathcal{P}_{B,f,r}(\mathbf{x}, y) = P_f(\mathbf{x}, y)\, \mathcal{C}_r(\mathbf{x}, y) \quad \text{in } \mathbb{F}_p[y][\mathbf{x}],$$

with x_r specialized to 0.

17

We claim that $\mathcal{P}_{B,f,r}$ vanishes on $\mathbb{F}_p^n$; by Lemma 0.15 this is equivalent to $\mathcal{P}_{B,f,r} \in \mathcal{J}_p$ (viewed as an ideal of $S[\mathbf{x}]$). Indeed, let $\mathbf{a} \in \mathbb{F}_p^n$ with $a_r = 0$. If some coordinate $a_i \notin \mathbb{Z}_n$ then a_i equals some $j \in \mathbb{Z}_p \setminus \mathbb{Z}_n$, so the corresponding cutoff factor $y(a_i - a_r) - yj = y(a_i - j)$ vanishes and hence $\mathcal{C}_r(\mathbf{a}, y) = 0$. Otherwise $\mathbf{a} \in (\mathbb{Z}_n)^{n \times 1}$ and by the assumption above $P_f(\mathbf{a}, y) = 0$ in $\mathbb{Z}[y]$, hence also in $\mathbb{F}_p[y]$. In either case $\mathcal{P}_{B,f,r}(\mathbf{a}, y) = 0$ in $\mathbb{F}_p[y]$. Since x_r is specialized to 0 in $\mathcal{P}_{B,f,r}$, the polynomial does not depend on x_r and therefore vanishes on all of $\mathbb{F}_p^n$. By Lemma 0.15, this implies $\mathcal{P}_{B,f,r} \in \mathcal{J}_p$.

Apply the change of variables from Lemma 0.8 together with Lemma 0.17. For each r we obtain

$$\mathcal{P}_{B,f,r}\left(T_f \cdot \begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) = \mathcal{P}_{B',f^{(2)},r}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right).$$

Since $\mathcal{P}_{B,f,r} \in \mathcal{J}_p$ and $\mathcal{J}_p$ is stable under linear substitutions in the $\mathbf{x}$–variables (Lemma 0.16), we conclude

$$\forall\, r \in \mathbb{Z}_n, \quad \mathcal{P}_{B',f^{(2)},r} \in \mathcal{J}_p.$$

Hence, for each r, the polynomial $\mathcal{P}_{B',f^{(2)},r}$ vanishes on $\mathbb{F}_p^n$, and in particular on every permutation point $\mathbf{v} \in (\mathbb{Z}_n)^{n \times 1}$ with $v_r = 0$. For such a point we have in $\mathbb{F}_p[y]$:

$$0 = \mathcal{P}_{B',f^{(2)},r}(\mathbf{v}, y) = P_{f^{(2)}}(\mathbf{v}, y)\,\mathcal{C}_r(\mathbf{v}, y),$$

where we also used basis-independence $P_{B',f^{(2)}} = P_{f^{(2)}}$. Moreover $\mathcal{C}_r(\mathbf{v}, y)$ is a nonzero element of $\mathbb{F}_p[y]$ (it is a nonzero scalar multiple of $y^{(n-1)(p-n)}$), so we must have $P_{f^{(2)}}(\mathbf{v}, y) \equiv 0$ in $\mathbb{F}_p[y]$. By Lemma 0.18, this congruence forces $P_{f^{(2)}}(\mathbf{v}, y) = 0$ in $\mathbb{Z}[y]$, i.e. $P_{f^{(2)}}$ vanishes (over $\mathbb{Q}$) on every permutation point of $(\mathbb{Z}_n)^n$. Non-permutation points already yield $P_{f^{(2)}}(\mathbf{v}, y) = 0$ because of the vertex Vandermonde factor. Therefore $P_{f^{(2)}}(\mathbf{v}, y) = 0$ for all $\mathbf{v} \in (\mathbb{Z}_n)^{n \times 1}$, and Lemma 0.9 gives $P_{f^{(2)}} \in \mathcal{I}_n$, as claimed. $\qquad\square$

Remark: The assertion $\mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \end{pmatrix} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) \in \mathcal{J}_p$ for a specific $r \in \mathbb{Z}_n$ holds iff G_f admits no graceful labeling

subject to the vertex labeled r in G_f being assigned the label 0. Recall that

$$\mathcal{P}_{B,f,r}\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right) := P_{B,f}\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right)\mathcal{C}_{f,r,B}\left(\begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right).$$

Thus changing $r \in \mathbb{Z}_n$ amounts to considering evaluation points $\mathbf{x} \in (\mathbb{F}_p)^{n \times 1}$ (where we partition $(\mathbb{F}_p)^{n \times 1}$ into n disjoint

classes) of the same polynomial $P_{B,f}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right)$ i.e. the first factor of $\mathcal{P}_{B,f,r}$. By contrast the second factor i.e. the cutoff

polynomial $\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right)$ changes considerably for distinct $r \in \mathbb{Z}_n$. Observe that for a fixed $r \in \mathbb{Z}_n$, assigning to

x_r a value $v \in \mathbb{Z}_p \backslash \{0\}$ result in the vanishing of the said cutoff polynomial. Furthermore for a fixed $r \in \mathbb{Z}_n$, our chosen linear

map globally fixes the cutoff factor $\mathcal{C}_{f,r,B}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}, y\right)$ see Lemma 0.17. Thus the linear transformation effects for the

first factor the following map

$$\forall r \in \mathbb{Z}_n, \; P_{B,f}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}\right) \longmapsto P_{B',f^{(2)}}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \end{pmatrix}\right).$$

By the ideal stability result if for some $r \in \mathbb{Z}_n$, $\mathcal{P}_{B',f^{(2)},r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix} \end{pmatrix}, y\right) \notin \mathcal{J}_p$ then $P_{B',f^{(2)}}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix}\right) \notin \mathcal{I}_n$ which in

turn implies that there must some $r \in \mathbb{Z}_n$ such that $\mathcal{P}_{B,f,r}\left(\begin{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{r-1} \\ 0 \\ x_{r+1} \\ \vdots \\ x_{n-1} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix} \end{pmatrix}, y\right) \notin \mathcal{J}_p$ and incidentally $P_{B,f}\left(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}\right) \notin$

$\mathcal{I}_n$.

Lemma 0.20 (*Composition Lemma*)**.** *Fix $n \geq 2$ and let*

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

If $G_{f^{(2)}}$ is graceful for some $f \in \mathcal{T}_n$, then G_f is graceful; equivalently

$$\mathrm{GrL}(G_{f^{(2)}}) \neq \varnothing \implies \mathrm{GrL}(G_f) \neq \varnothing.$$

Proof. $G_{f^{(2)}}$ is graceful implies that $P_{B',f^{(2)}}(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix}) \notin \mathcal{I}_n$ by Lemma 0.9. The contrapositive of Lemma 0.19 yields

$$P_{B',f^{(2)}}(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}'_0 \\ \vdots \\ y\,\mathbf{b}'_i \\ \vdots \\ y\,\mathbf{b}'_{n-2} \end{pmatrix}) \notin \mathcal{I}_n \implies P_{B,f}(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) \notin \mathcal{I}_n.$$

Finally $P_{B,f}(\begin{pmatrix} \mathbf{x} \\ y\,\mathbf{b}_0 \\ \vdots \\ y\,\mathbf{b}_i \\ \vdots \\ y\,\mathbf{b}_{n-2} \end{pmatrix}) \notin \mathcal{I}_n$ implies G_f is graceful by which

$$\mathrm{GrL}(G_{f^{(2)}}) \neq \varnothing \implies \mathrm{GrL}(G_f) \neq \varnothing,$$

as claimed. $\qquad\square$

The Graceful Tree Labeling Theorem.

Theorem 0.21. *[Tree Labeling Theorem] Fix $n \geq 2$ and recall that*

$$\mathcal{T}_n := \big\{ f \in \mathbb{Z}_n^{\mathbb{Z}_n} : f(i) > i \;\forall i \in \mathbb{Z}_{n-1}, \text{ and } f(n-1) = n-1 \big\}.$$

For all $f \in \mathcal{T}_n$, we have $\mathrm{GrL}(G_f) \neq \varnothing$.

Proof. For an arbitrary $f \in \mathcal{T}_n$, consider the sequence of iterates of f of total length $1+\ell$ where $\ell = \lceil \log_2(n-1) \rceil$. The initial member of the sequence is f. Each subsequent member of the sequence is obtained by iterating the previous member of the sequence. In other words the sequence is $(g_0, \ldots, g_\ell)$ where $g_i \in \mathcal{T}_n$ for all $i \in \mathbb{Z}_{1+\ell}$. The initial condition for the sequence is

$$g_0 = f^{(2^0)} = f.$$

The recurrence relation prescribing all other members of the sequence indexed by $0 < i < \ell$ is:

$$g_{i+1} = g_i \circ g_i = g_i^{(2)}.$$

The sequence is therefore of the form:

$$(g_0 = f^{(2^0)}, \ldots, g_k = f^{(2^k)}, \ldots, g_\ell = f^{(2^\ell)} = f^{(n-1)}).$$

Observe that $g_\ell(\mathbb{Z}_n) = \{n-1\}$ by which we see that g_ℓ is graceful. By repeatedly invoking the Composition Lemma 0.20, we have we have $\mathrm{GrL}(G_f) \neq \varnothing$ as claimed. $\qquad\square$

21