

Interactive proofs of Proximity to Algebraic Geometry codes

Sarah Bordage **Jade Nardi**

June 4, 2021

Séminaire C2

<https://eccc.weizmann.ac.il/report/2020/165/>

LIX, Ecole Polytechnique, Institut Polytechnique de Paris
Inria

Motivation: Verifiable Computing¹



Powerful Prover
(eg. a server)

Please, run program F on input x for me.

I want to **quickly** check if your result is correct.



Weak Verifier
(eg. a client)

¹Most of this slide is kindly provided by Sarah Bordage.

Motivation: Verifiable Computing¹



Powerful Prover

(eg. a server)

outputs result y and
proof of correctness π

Please, run program
 F on input x for me.

I want to quickly check
if your result is correct.

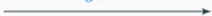


Weak Verifier

(eg. a client)

checks validity of π
for statement " $y = F(x)$ "

y, π



How to ensure
P cannot cheat?
Fast verification?
Short proofs?

Applications: cloud computing, cryptocurrencies, blockchains

¹Most of this slide is kindly provided by Sarah Bordage.

Motivation: Verifiable Computing¹



Powerful Prover

(eg. a server)

outputs result y and
proof of correctness π

Arithmetization

Proximity to
a code C

Please, run program
 F on input x for me.

I want to quickly check
if your result is correct.



Weak Verifier

(eg. a client)

checks validity of π
for statement " $y = F(x)$ "

y, π

How to ensure
P cannot cheat?
Fast verification?
Short proofs?

Applications: cloud computing, cryptocurrencies, blockchains

Prover produces a word

- $c \in C$ if the statement " $y = F(x)$ " holds,
- \tilde{c} which is **very far** from C otherwise.

¹Most of this slide is kindly provided by Sarah Bording.

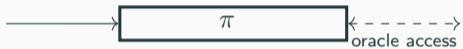
PCP model (Probabilistically Checkable Proofs) ²



Prover



Verifier



²This slide is kindly provided by Sarah Bordage.

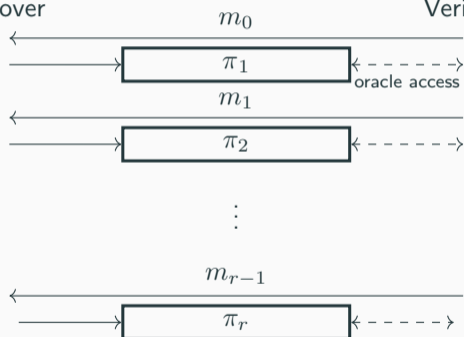
IOP Model (Interactive Oracle Proofs)²



Prover



Verifier



[Ben-Sasson-Chiesa-Spooner'16,
Reingold-Rothblum²'16]

IOPs generalize PCPs and IPs

public-coin IOP \rightarrow non-interactive proof
in the RO model (Fiat-Shamir paradigm)

with communication complexity:

- linear in query complexity of the IOP
- logarithmic in oracle proof length

$$|\pi_1| + \dots + |\pi_r|$$

²This slide is kindly provided by Sarah Bordage.

Proximity test to RS codes
Univariate low-degree testing

[Ben–Sasson–Bentov–Horesh–Riabzev'18]

Reed-Solomon Proximity Testing

Input code: $RS[\mathcal{P}, d] = \{f : \mathcal{P} \rightarrow \mathbb{F} \mid f \text{ coincides with polynomial of degree } < d\}$

Input oracle: $f : \mathcal{P} \rightarrow \mathbb{F}$

Completeness: If $f \in RS[\mathcal{P}, d]$, then $\exists P \Pr[V \text{ accepts } P] = 1$

Soundness: If $\Delta(f, RS[\mathcal{P}, d]) > \delta$, then $\forall \tilde{P} \Pr[V \text{ accepts } \tilde{P}] < \text{err}(\delta)$

Δ relative Hamming distance

³This slide is kindly provided by Sarah Bordage.

Halving the size of the problem by folding

On a finite field \mathbb{F} with $2 \nmid |\mathbb{F}|$, take $\omega \in \mathbb{F}^\times$ of order 2^k and $\mathcal{P} := \langle \omega \rangle$.

How to check if $f : \mathcal{P} \rightarrow \mathbb{F}$ satisfies $\deg f < d$?

Halving the size of the problem by folding

On a finite field \mathbb{F} with $2 \nmid |\mathbb{F}|$, take $\omega \in \mathbb{F}^\times$ of order 2^k and $\mathcal{P} := \langle \omega \rangle$.

How to check if $f : \mathcal{P} \rightarrow \mathbb{F}$ satisfies $\deg f < d$?

Write $f(x) = f_0(x^2) + x \cdot f_1(x^2)$, where $f_0, f_1 : \underbrace{\mathcal{P}'}_{=\langle \omega^2 \rangle} \rightarrow \mathbb{F}$ with $\deg f_0, \deg f_1 \leq \deg f / 2$.

Check if $\deg f_0 < d/2$ and $\deg f_1 < d/2$. \rightarrow 2 tests!

Halving the size of the problem by folding

On a finite field \mathbb{F} with $2 \nmid |\mathbb{F}|$, take $\omega \in \mathbb{F}^\times$ of order 2^k and $\mathcal{P} := \langle \omega \rangle$.

How to check if $f : \mathcal{P} \rightarrow \mathbb{F}$ satisfies $\deg f < d$?

Write $f(x) = f_0(x^2) + x \cdot f_1(x^2)$, where $f_0, f_1 : \underbrace{\mathcal{P}'}_{=\langle \omega^2 \rangle} \rightarrow \mathbb{F}$ with $\deg f_0, \deg f_1 \leq \deg f / 2$.

Check if $\deg f_0 < d/2$ and $\deg f_1 < d/2$. \rightarrow 2 tests!

Make 1 test: For $z \in \mathbb{F}$, define **Fold** $[f, z] : \mathcal{P}' \rightarrow \mathbb{F}$ by **Fold** $[f, z] = f_0 + z f_1$.

May fail: take $f(x) = 1 + x^2 + x(x^2 + 2)$. Then **Fold** $[f, -1] = 1 + x - (x + 2) = -1$.

\deg **Fold** $[f, -1] < 1$ but $\deg f \geq 2$

Halving the size of the problem by folding

On a finite field \mathbb{F} with $2 \nmid |\mathbb{F}|$, take $\omega \in \mathbb{F}^\times$ of order 2^k and $\mathcal{P} := \langle \omega \rangle$.

How to check if $f : \mathcal{P} \rightarrow \mathbb{F}$ satisfies $\deg f < d$?

Write $f(x) = f_0(x^2) + x \cdot f_1(x^2)$, where $f_0, f_1 : \underbrace{\mathcal{P}'}_{=\langle \omega^2 \rangle} \rightarrow \mathbb{F}$ with $\deg f_0, \deg f_1 \leq \deg f / 2$.

Check if $\deg f_0 < d/2$ and $\deg f_1 < d/2$. \rightarrow 2 tests!

Make 1 test: For $z \in \mathbb{F}$, define **Fold** $[f, z] : \mathcal{P}' \rightarrow \mathbb{F}$ by **Fold** $[f, z] = f_0 + z f_1$.

May fail: take $f(x) = 1 + x^2 + x(x^2 + 2)$. Then **Fold** $[f, -1] = 1 + x - (x + 2) = -1$.

\deg **Fold** $[f, -1] < 1$ but $\deg f \geq 2$

✓ **Completeness:**

Fold $[\cdot, z] (\text{RS}[\mathcal{P}, d]) \subseteq \text{RS}[\mathcal{P}', d/2]$.

✓ **Locality:**

compute a value of **Fold** $[f, z]$ on \mathcal{P}' with only **2 queries** to f .

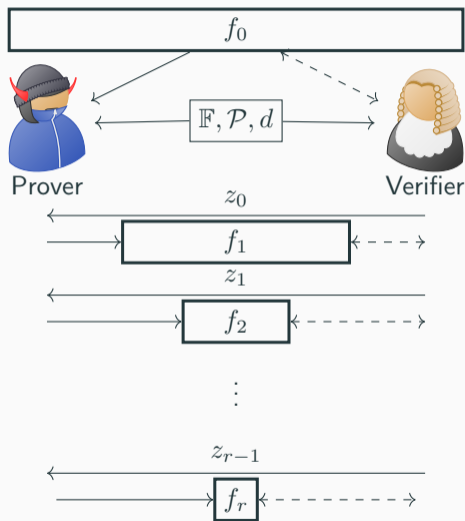
$$\text{Fold} [f, \pm\sqrt{y}] (y) = f_0 \pm \sqrt{y} f_1 = f(\pm\sqrt{y})$$

✓ **Distance preservation:**

if $\Delta(f, \text{RS}[\mathcal{P}, d]) > \delta$, then $\Delta(\text{Fold} [f, z], \text{RS}[\mathcal{P}', d/2]) > \delta'$ (w.h.p.).

\rightarrow **Proximity to** $\text{RS}[\mathcal{P}, d]$ **reduced to proximity to** $\text{RS}[\mathcal{P}', d/2]$ (probabilistically).

FRI Protocol: Commit Phase⁴



Honest prover computes:

$$f_1 = \mathbf{Fold} [f_0, z_0]$$

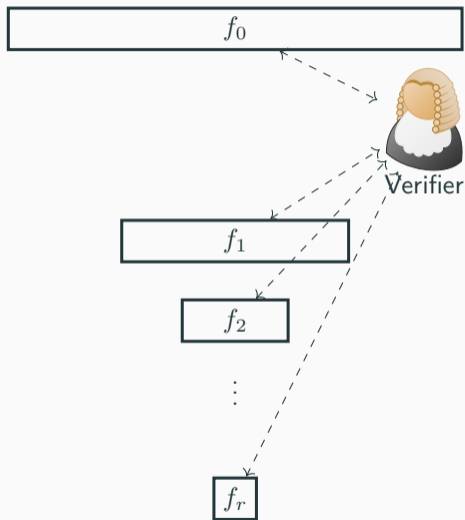
$$f_2 = \mathbf{Fold} [f_1, z_1]$$

\vdots

$$f_r = \mathbf{Fold} [f_{r-1}, z_{r-1}]$$

⁴This slide is kindly provided by Sarah Bordage.

FRI Protocol: Query Phase⁵



Check consistency
at random locations

$$f_1(s_1) \stackrel{?}{=} \mathbf{Fold} [f_0, z_0] (s_1)$$

$$f_2(s_2) \stackrel{?}{=} \mathbf{Fold} [f_1, z_1] (s_2)$$

\vdots

$$f_r(s_r) \stackrel{?}{=} \mathbf{Fold} [f_{r-1}, z_{r-1}] (s_r)$$

Final test: $f_r \stackrel{?}{\in} \mathbf{RS}_r$

⁵This slide is kindly provided by Sarah Bordage.

Soundness of the FRI Protocol ⁶

Completeness: If $f \in \text{RS}[\mathcal{P}, d]$, then $\exists P \Pr[\text{V accepts } P] = 1$.

Soundness: If $\Delta(f, \text{RS}[\mathcal{P}, d]) > \delta$, then $\forall \tilde{P} \Pr[\text{V accepts } \tilde{P}] < \text{err}(\delta)$.

FRI Protocol [Ben-Sasson-Bentov-Horesh-Riabzev'18]

- ✓ linear prover time
- ✓ logarithmic query complexity
- ✓ linear (interactive) proof length
- ✓ logarithmic verifier time

Theorem

Assuming $\delta < 1 - \sqrt{\rho}$ (ρ is code rate), $\text{err}(\delta) < \text{err}_{\text{commit}} + (\text{err}_{\text{query}})^\alpha$
 $< \text{negl}(\kappa) + (1 - \delta)^\alpha$
security parameter

To get error $\text{err}(\delta) = \text{negl}(\kappa)$, repeat query phase enough time (α times).

Building-block of succinct ZK proofs

with no trusted setup, PQ security, succinct verification (see e.g. "ZK-STARKs").

⁶This content is kindly provided by Sarah Bordage.

Proximity test for AG codes

Algebraic Geometry (AG) codes

Let \mathcal{C} be an algebraic curve defined over a finite field \mathbb{F} .

Divisors. A (rational) **divisor** D on \mathcal{C} is a formal sum of \mathbb{F} -points $D = \sum n_P P$.

Its **degree** is $\deg D := \sum n_P$ and **support** is $\text{Supp}(D) := \{P \in \mathcal{C} \mid n_P \neq 0\}$.

$D \leq D'$ if $n_P \leq n'_P$ for every P

A function f on \mathcal{C} defines a **principal divisor** $(f) := \sum_P \underbrace{v_P(f)}_{\text{valuation}} P$.

Algebraic Geometry (AG) codes

Let \mathcal{C} be an algebraic curve defined over a finite field \mathbb{F} .

Divisors. A (rational) **divisor** D on \mathcal{C} is a formal sum of \mathbb{F} -points $D = \sum n_P P$.

Its **degree** is $\deg D := \sum n_P$ and **support** is $\text{Supp}(D) := \{P \in \mathcal{C} \mid n_P \neq 0\}$.

$D \leq D'$ if $n_P \leq n'_P$ for every $P \Rightarrow L_{\mathcal{C}}(D) \subset L_{\mathcal{C}}(D')$.

A function f on \mathcal{C} defines a **principal divisor** $(f) := \sum_P \underbrace{v_P(f)}_{\text{valuation}} P$.

Riemann-Roch space of D . $L_{\mathcal{C}}(D) = \{f \in \mathbb{F}(\mathcal{C}) \mid (f) \geq -D\} \cup \{0\}$.

Algebraic Geometry (AG) codes

Let \mathcal{C} be an algebraic curve defined over a finite field \mathbb{F} .

Divisors. A (rational) **divisor** D on \mathcal{C} is a formal sum of \mathbb{F} -points $D = \sum n_P P$.

Its **degree** is $\deg D := \sum n_P$ and **support** is $\text{Supp}(D) := \{P \in \mathcal{C} \mid n_P \neq 0\}$.

$D \leq D'$ if $n_P \leq n'_P$ for every $P \Rightarrow L_{\mathcal{C}}(D) \subset L_{\mathcal{C}}(D')$.

A function f on \mathcal{C} defines a **principal divisor** $(f) := \sum_P \underbrace{v_P(f)}_{\text{valuation}} P$.

Riemann-Roch space of D . $L_{\mathcal{C}}(D) = \{f \in \mathbb{F}(\mathcal{C}) \mid (f) \geq -D\} \cup \{0\}$.

AG codes

Given $\mathcal{P} \subset \mathcal{C}(\mathbb{F})$ of size $n := |\mathcal{P}|$ and a divisor D on \mathcal{C} s.t. $\text{Supp}(D) \cap \mathcal{P} = \emptyset$, the **AG code** $C = C(\mathcal{C}, \mathcal{P}, D)$ is defined as the image by $\mathbf{ev} : L_{\mathcal{C}}(D) \rightarrow \mathbb{F}^n$.

Example: $C = C(\mathbb{P}^1, \mathcal{P}, dP_{\infty})$, with $P_{\infty} = [0 : 1]$, is Hamming-eq. to $\text{RS}[\mathcal{P}, d+1]$.

We always choose D so that \mathbf{ev} is injective: $\mathbb{F}^n \xleftrightarrow{\mathbf{ev}} \mathbb{F}^{\mathcal{P}}$ and

$$C(\mathcal{C}, \mathcal{P}, D) = \{f : \mathcal{P} \rightarrow \mathbb{F} \mid f \text{ coincides with a fct in } L_{\mathcal{C}}(D)\}.$$

Group action and Kani's splitting of Riemann-Roch spaces

Let \mathcal{C} be a curve over \mathbb{F} and let $\Gamma = \langle \gamma \rangle \simeq \mathbb{Z}/m\mathbb{Z}$ a group of automorphisms of \mathcal{C} s.t. $\gcd(m, |\mathbb{F}|) = 1$. Take $\zeta \in \overline{\mathbb{F}}$ a primitive m^{th} root of unity.

- Γ acts on the functions on \mathcal{C} : $\gamma \cdot f = f \circ \gamma$ for any fct f on \mathcal{C} .
- There exists a function μ on \mathcal{C} s.t. $\gamma \cdot \mu = \zeta \mu$ [Kani'86].

Set the projection map $\pi : \mathcal{C} \rightarrow \mathcal{C}' := \mathcal{C}/\Gamma$.

⁷Notation: $\lfloor \frac{1}{n} D \rfloor := \sum \lfloor \frac{n_P}{n} \rfloor P$, for a divisor $D = \sum n_P P$ and integer $n > 0$.

Group action and Kani's splitting of Riemann-Roch spaces

Let \mathcal{C} be a curve over \mathbb{F} and let $\Gamma = \langle \gamma \rangle \simeq \mathbb{Z}/m\mathbb{Z}$ a group of automorphisms of \mathcal{C} s.t. $\gcd(m, |\mathbb{F}|) = 1$. Take $\zeta \in \overline{\mathbb{F}}$ a primitive m^{th} root of unity.

- Γ acts on the functions on \mathcal{C} : $\gamma \cdot f = f \circ \gamma$ for any fct f on \mathcal{C} .
- There exists a function μ on \mathcal{C} s.t. $\gamma \cdot \mu = \zeta \mu$ [Kani'86].

Set the projection map $\pi : \mathcal{C} \rightarrow \mathcal{C}' := \mathcal{C}/\Gamma$.

For any Γ -invariant divisor D on \mathcal{C} , the action of Γ on $L_{\mathcal{C}}(D)$ gives

$$L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} L_{\mathcal{C}}(D)_j \text{ where } L_{\mathcal{C}}(D)_j := \{g \in L_{\mathcal{C}}(D) \mid \gamma \cdot g = \zeta^j g\}.$$

[Kani'86] $L_{\mathcal{C}}(D)_j \simeq \mu^j \pi^* (L_{\mathcal{C}'}(E_j))$ where $E_j := \lfloor \frac{1}{m} \pi_* (D + j(\mu)) \rfloor$ is a divisor on \mathcal{C}' .

\rightsquigarrow For every $f \in L_{\mathcal{C}}(D)$, there exist m fcts $f_j \in L_{\mathcal{C}'}(E_j)$ s.t. $f = \sum_{j=0}^{m-1} \mu^j f_j \circ \pi$.

⁷Notation: $\lfloor \frac{1}{n} D \rfloor := \sum \lfloor \frac{n_P}{n} \rfloor P$, for a divisor $D = \sum n_P P$ and integer $n > 0$.

Kani's result on $\mathcal{C} = \mathbb{P}^1$

$$[\text{Kani}'86]: L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{\mathcal{C}'} \left(\left[\frac{1}{m} \pi_* (D + j(\mu)) \right] \right).$$

The AG code $C = C(\mathbb{P}^1, \mathcal{P}, dP_{\infty})$, with $P_{\infty} = [0 : 1]$, corresponds to RS $[\mathcal{P}, d + 1]$.

Consider the **action** on \mathbb{P}^1 of $\gamma : [X_0 : X_1] \mapsto [X_0 : -X_1]$. Then $\langle \gamma \rangle = \mathbb{Z}/2\mathbb{Z}$.

Projection map $\pi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ by $\pi[X_0 : X_1] := [X_0^2 : X_1^2]$.

Kani's result on $\mathcal{C} = \mathbb{P}^1$

$$[\text{Kani}'86]: L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{\mathcal{C}'} \left(\left[\frac{1}{m} \pi_* (D + j(\mu)) \right] \right).$$

The AG code $C = C(\mathbb{P}^1, \mathcal{P}, dP_{\infty})$, with $P_{\infty} = [0 : 1]$, corresponds to RS $[\mathcal{P}, d + 1]$.

Consider the **action** on \mathbb{P}^1 of $\gamma : [X_0 : X_1] \mapsto [X_0 : -X_1]$. Then $\langle \gamma \rangle = \mathbb{Z}/2\mathbb{Z}$.

Projection map $\pi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ by $\pi[X_0 : X_1] := [X_0^2 : X_1^2]$.

Kani's result with $\mu = x := \frac{X_1}{X_0}$ ($\gamma \cdot x = -x$) yields to $((x) = [1 : 0] - P_{\infty})$

$$L_{\mathbb{P}^1}(dP_{\infty}) = \pi^* L_{\mathbb{P}^1} \left(\left[\frac{d}{2} \right] P_{\infty} \right) + x \pi^* L_{\mathbb{P}^1} \left(\left[\frac{d-1}{2} \right] P_{\infty} \right),$$

i.e. any pol. f of degree $\leq d$ can be written $f(x) = f_0(x^2) + x f_1(x^2)$ with $\begin{cases} \deg f_0 \leq \lfloor \frac{d}{2} \rfloor, \\ \deg f_1 \leq \lfloor \frac{d-1}{2} \rfloor. \end{cases}$

FRI: For $z \in \mathbb{F}$, define **Fold** $[f, z] = f_0 + z f_1$.

Remark: For **odd** d , $\lfloor \frac{d}{2} \rfloor = \lfloor \frac{d-1}{2} \rfloor$, i.e. $L_{\mathbb{P}^1}(dP_{\infty})$ is split into 2 "copies" of the **same** space.

Kani's result on a Kummer curve

$$[\text{Kani}'86]: L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{\mathcal{C}'} \left(\left[\frac{1}{m} \pi_* (D + j(\mu)) \right] \right).$$

Assume $\gcd(N, d) = 1$ and $\gcd(N, |\mathbb{F}|) = 1$. Take ζ a primitive N^{th} root of unity.

$$\mathcal{C} : y^N = f(x) = \prod_{\ell=1}^d (x - \alpha_{\ell})$$

Kani's result on a Kummer curve

$$[\text{Kani}'86]: L_C(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{C'} \left(\left[\frac{1}{m} \pi_* (D + j(\mu)) \right] \right).$$

Assume $\gcd(N, d) = 1$ and $\gcd(N, |\mathbb{F}|) = 1$. Take ζ a primitive N^{th} root of unity.

$$\begin{array}{ccc} \langle \gamma : (x, y) \mapsto (x, \zeta y) \rangle \simeq \mathbb{Z}/N\mathbb{Z} \curvearrowright \mathcal{C} : y^N = f(x) = \prod_{\ell=1}^d (x - \alpha_\ell) & & \\ \pi : (x, y) \rightarrow (x, y^N) \downarrow & & \\ \mathbb{P}^1 \simeq \mathcal{C}' : y = f(x) & & \end{array}$$

Kani's result on a Kummer curve

$$[\text{Kani}'86]: L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{\mathcal{C}'}, \left(\left\lfloor \frac{1}{m} \pi_* (D + j(\mu)) \right\rfloor \right).$$

Assume $\gcd(N, d) = 1$ and $\gcd(N, |\mathbb{F}|) = 1$. Take ζ a primitive N^{th} root of unity.

$$\begin{aligned} \langle \gamma : (x, y) \mapsto (x, \zeta y) \rangle &\simeq \mathbb{Z}/N\mathbb{Z} \curvearrowright \mathcal{C} : y^N = f(x) = \prod_{\ell=1}^d (x - \alpha_{\ell}) \\ \pi : (x, y) &\rightarrow (x, y^N) \downarrow \\ &\mathbb{P}^1 \simeq \mathcal{C}' : y = f(x) \end{aligned}$$

Take $D = \alpha P_{\infty}$ where P_{∞} is the unique point at ∞ on \mathcal{C} . Write $P_{\ell} = (\alpha_{\ell}, 0)$.

Any fct $f \in L_{\mathcal{C}}(D)$ can be written $f(x, y) = \sum_{j=0}^{N-1} y^j f_j(x, y^N)$ ($\mu = y$ as $\gamma \cdot y = \zeta y$)

where $f_j \in L_{\mathbb{P}^1} \left(\left\lfloor \frac{\pi_*(D) - j(\sum P_{\ell} - dP_{\infty})}{N} \right\rfloor \right)$, i.e. f_j is a pol. of degree $\leq \left\lfloor \frac{\alpha - jd}{N} \right\rfloor \leq \left\lfloor \frac{\alpha}{N} \right\rfloor$.

Using Kani's result to fold

Let \mathcal{C} be a curve over a field \mathbb{F} on which acts $\Gamma \simeq \mathbb{Z}/m\mathbb{Z}$, with the projection map $\pi : \mathcal{C} \rightarrow \mathcal{C}/\Gamma$.

FRI's idea: proximity to $C = C(\mathcal{C}, \mathcal{P}, D)$ reduced to proximity to $C' = C(\mathcal{C}/\Gamma, \mathcal{P}', D')$

We need: – a Γ -invariant divisor $D \xrightarrow{[\text{Kani}'86]} f = \sum_{j=1}^{m-1} \mu^j f_j \circ \pi.$
$$\underset{L_{\mathcal{C}}(D)}{\cap} \quad \underset{L_{\mathcal{C}/\Gamma}(E_j)}{\cap}$$

– an evaluation set $\mathcal{P} =$ **union of Γ -orbits of size $|\Gamma|$** (Γ acts freely on \mathcal{P}).

Take $\mathcal{P}' = \pi(\mathcal{P})$ ($|\mathcal{P}'| = |\mathcal{P}|/m$) and D' is a divisor on \mathcal{C}/Γ s.t. $L_{\mathcal{C}/\Gamma}(D') \supseteq L_{\mathcal{C}/\Gamma}(E_j)$.

Using Kani's result to fold

Let \mathcal{C} be a curve over a field \mathbb{F} on which acts $\Gamma \simeq \mathbb{Z}/m\mathbb{Z}$, with the projection map $\pi : \mathcal{C} \rightarrow \mathcal{C}/\Gamma$.

FRI's idea: proximity to $C = C(\mathcal{C}, \mathcal{P}, D)$ reduced to proximity to $C' = C(\mathcal{C}/\Gamma, \mathcal{P}', D')$

We need: – a Γ -invariant divisor $D \xrightarrow{[\text{Kani}'86]} f = \sum_{j=1}^{m-1} \mu^j f_j \circ \pi$.

$\bigcap_{L_{\mathcal{C}}(D)} \qquad \qquad \qquad \bigcap_{L_{\mathcal{C}/\Gamma}(E_j)}$

– an evaluation set $\mathcal{P} =$ **union of Γ -orbits of size $|\Gamma|$** (Γ acts freely on \mathcal{P}).

Take $\mathcal{P}' = \pi(\mathcal{P})$ ($|\mathcal{P}'| = |\mathcal{P}|/m$) and D' is a divisor on \mathcal{C}/Γ s.t. $L_{\mathcal{C}/\Gamma}(D') \supseteq L_{\mathcal{C}/\Gamma}(E_j)$.

For any $z \in \mathbb{F}$, define the *folding operator* **Fold** $[\cdot, z] : \mathbb{F}^{\mathcal{P}} \rightarrow \mathbb{F}^{\mathcal{P}'}$ by **Fold** $[f, z] = \sum_{j=0}^{m-1} z^j f_j$.

✓ **Completeness:**

Fold $[\cdot, z](C) \subseteq C'$.

✓ **Locality:**

For any $P \in \mathcal{P}'$, compute **Fold** $[f, z](P)$ with m queries to f .

interpolate on the geometric progression $\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\}$.

✗ **Distance preservation**

$\Delta(f, C) > \delta \not\Rightarrow \Delta(\mathbf{Fold}[f, z], C') > \delta'$ w.h.p.

Distance preservation by folding (?)

Problem: $L_{\mathcal{C}/\Gamma}(E_j) \subsetneq L_{\mathcal{C}/\Gamma}(D')$! All the $L_{\mathcal{C}/\Gamma}(E_j)$ are not the same.

We need to know if a function lies in $L_{\mathcal{C}/\Gamma}(E_j)$, not only in $L_{\mathcal{C}/\Gamma}(D')$.

Define **balancing functions** $\nu_j \in \mathbb{F}(\mathcal{C}/\Gamma)$ s.t. $h \in L_{\mathcal{C}/\Gamma}(E_j)$ iff $h, \nu_j h \in L_{\mathcal{C}/\Gamma}(D')$.

(on \mathbb{P}^1 : if $\deg \nu = 1$, then $\deg h \leq d - 1$ iff $\deg h, \deg \nu h \leq d$)

To avoid C' to be too large, we want D' to be one of the E_j . For simplicity, assume $D' = E_0$.

Distance preservation by folding (?)

Problem: $L_{C/\Gamma}(E_j) \subsetneq L_{C/\Gamma}(D')$! All the $L_{C/\Gamma}(E_j)$ are not the same.

We need to know if a function lies in $L_{C/\Gamma}(E_j)$, not only in $L_{C/\Gamma}(D')$.

Define **balancing functions** $\nu_j \in \mathbb{F}(C/\Gamma)$ s.t. $h \in L_{C/\Gamma}(E_j)$ iff $h, \nu_j h \in L_{C/\Gamma}(D')$.

(on \mathbb{P}^1 : if $\deg \nu = 1$, then $\deg h \leq d - 1$ iff $\deg h, \deg \nu h \leq d$)

To avoid C' to be too large, we want D' to be one of the E_j . For simplicity, assume $D' = E_0$.

(Final attempt) For any $(z_1, z_2) \in \mathbb{F}^2$, define **Fold** $[f, (z_1, z_2)] : \mathcal{P}' \rightarrow \mathbb{F}$ s.t.

$$\mathbf{Fold} [f, (z_1, z_2)] = \sum_{j=0}^{m-1} z_1^j f_j + \sum_{j=1}^{m-1} z_2^j \nu_j f_j.$$

Lemma: ν_j is a balancing function iff $(\nu_j)_\infty = D' - E_j$.

Such functions ν_j may not exist! (Weierstrass gaps)

→ Need to choose carefully D .

Let us fold several times! Back to Kummer curves.

Write $N = \prod_{i=0}^{r-1} p_i$ and $N_i = \prod_{j=i}^{r-1} p_j$

$\Gamma_i := \langle \gamma_i \rangle \simeq \mathbb{Z}/p_i\mathbb{Z}$ where $\gamma_i : (x, y) \mapsto (x, \zeta_i y)$ ($\zeta_i^{p_i} = 1$)

$$\begin{array}{l} \mathbb{Z}/p_0\mathbb{Z} \curvearrowright \mathcal{C}_0 : y^N = f(x) = \prod_{\ell=1}^d (x - \alpha_\ell) \\ \quad \downarrow \pi_0 \\ \mathbb{Z}/p_1\mathbb{Z} \curvearrowright \mathcal{C}_1 : y^{\frac{N}{p_0}} = f(x) \\ \quad \downarrow \pi_1 \\ \quad \vdots \\ \mathbb{Z}/p_i\mathbb{Z} \curvearrowright \mathcal{C}_i : y^{N_i} = f(x) \\ \quad \downarrow \pi_i : (x, y) \mapsto (x, y^{p_i}) \\ \quad \vdots \\ \mathbb{P}^1 \simeq \mathcal{C}_r : y = f(x) \end{array}$$

Let us fold several times! Back to Kummer curves.

Write $N = \prod_{i=0}^{r-1} p_i$ and $N_i = \prod_{j=i}^{r-1} p_j$

$\Gamma_i := \langle \gamma_i \rangle \simeq \mathbb{Z}/p_i\mathbb{Z}$ where $\gamma_i : (x, y) \mapsto (x, \zeta_i y)$ ($\zeta_i^{p_i} = 1$)

We want a **sequence of divisors** (D_i) supported by Γ_i -fixed points ($P_\ell := (\alpha_\ell, 0)$ and P_∞^i (pt at ∞)) that ensure *distance preservation* at each step.

Proposition [Bordage, N.]

Taking $D_0 = \sum a_\ell P_\ell + bP_\infty^0$ with $N \mid a_\ell, b$ and $d \equiv -1 \pmod N$ guarantees the existence of the balancing functions.

$$\begin{aligned} \mathbb{Z}/p_0\mathbb{Z} \curvearrowright \mathcal{C}_0 : y^N &= f(x) = \prod_{\ell=1}^d (x - \alpha_\ell) \\ &\downarrow \pi_0 \\ \mathbb{Z}/p_1\mathbb{Z} \curvearrowright \mathcal{C}_1 : y^{\frac{N}{p_0}} &= f(x) \\ &\downarrow \pi_1 \\ &\vdots \\ \mathbb{Z}/p_i\mathbb{Z} \curvearrowright \mathcal{C}_i : y^{N_i} &= f(x) \\ &\downarrow \pi_i : (x, y) \mapsto (x, y^{p_i}) \\ &\vdots \\ \mathbb{P}^1 &\simeq \mathcal{C}_r : y = f(x) \end{aligned}$$

Let us fold several times! Back to Kummer curves.

Write $N = \prod_{i=0}^{r-1} p_i$ and $N_i = \prod_{j=i}^{r-1} p_j$

$\Gamma_i := \langle \gamma_i \rangle \simeq \mathbb{Z}/p_i\mathbb{Z}$ where $\gamma_i : (x, y) \mapsto (x, \zeta_i y)$ ($\zeta_i^{p_i} = 1$)

We want a **sequence of divisors** (D_i) supported by Γ_i -fixed points ($P_\ell := (\alpha_\ell, 0)$ and P_∞^i (pt at ∞)) that ensure *distance preservation* at each step.

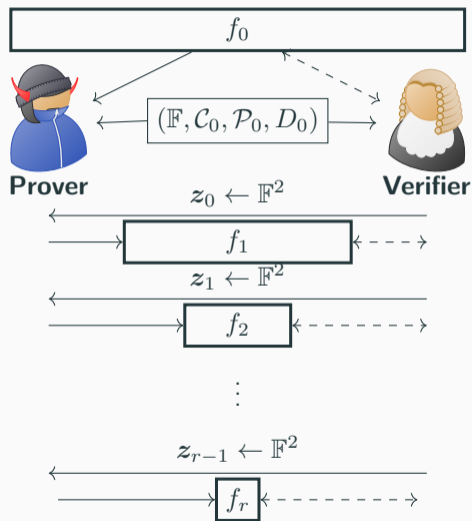
Proposition [Bordage, N.]

Taking $D_0 = \sum a_\ell P_\ell + b P_\infty^0$ with $N \mid a_\ell, b$ and $d \equiv -1 \pmod N$ guarantees the existence of the balancing functions.

$$\begin{aligned} \mathbb{Z}/p_0\mathbb{Z} \curvearrowright \mathcal{C}_0 : y^N &= f(x) = \prod_{\ell=1}^d (x - \alpha_\ell) \\ &\downarrow \pi_0 \\ \mathbb{Z}/p_1\mathbb{Z} \curvearrowright \mathcal{C}_1 : y^{\frac{N}{p_0}} &= f(x) \\ &\downarrow \pi_1 \\ &\vdots \\ \mathbb{Z}/p_i\mathbb{Z} \curvearrowright \mathcal{C}_i : y^{N_i} &= f(x) \\ &\downarrow \pi_i : (x, y) \mapsto (x, y^{p_i}) \\ &\vdots \\ \mathbb{P}^1 &\simeq \mathcal{C}_r : y = f(x) \end{aligned}$$

Proximity test to $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ of length $n \rightarrow$ membership test to RS $\left[\pi(\mathcal{P}_0), \left\lfloor \frac{\pi_*(D_0)}{N} \right\rfloor \right]$ of $\left[\frac{n}{N}, \frac{\deg(D_0)}{N} + 1 \right]$ and relative minimum distance $1 - \frac{\deg D_0}{n}$.

Overview of the AG-IOPP⁸



COMMIT Phase

$$f_1 = \mathbf{Fold}[f_0, z_0]$$

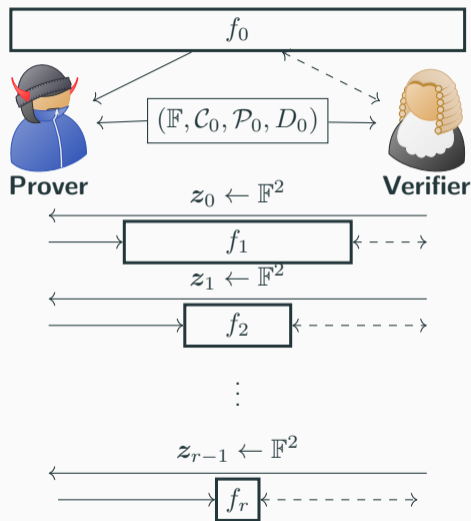
$$f_2 = \mathbf{Fold}[f_1, z_1]$$

\vdots

$$f_r = \mathbf{Fold}[f_{r-1}, z_{r-1}]$$

⁸This slide is kindly provided by Sarah Bordage.

Overview of the AG-IOPP⁸



QUERY Phase

Round consistency tests:

Sample $Q_0 \in \mathcal{P}_0$,

Define query path (Q_1, \dots, Q_r) s.t. $Q_{i+1} = \pi_i(Q_i)$.

$$f_1(Q_1) \stackrel{?}{=} \mathbf{Fold}[f_0, z_0](Q_1)$$

$$f_2(Q_2) \stackrel{?}{=} \mathbf{Fold}[f_1, z_1](Q_2)$$

\vdots

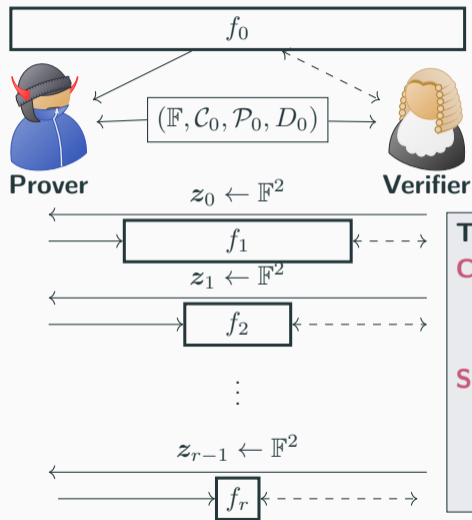
\vdots

$$f_r(Q_r) \stackrel{?}{=} \mathbf{Fold}[f_{r-1}, z_{r-1}](Q_r)$$

Final test: $f_r \stackrel{?}{\in} C(\mathcal{C}_r, \mathcal{P}_r, D_r)$

⁸This slide is kindly provided by Sarah Bordage.

Overview of the AG-IOPP⁸



Theorem [Bordage, N.]

Completeness:

If $f_0 \in C_0$, V accepts with probability 1.

Soundness:

(relies on [BKS18] and [BGKS19])

If f_0 is δ -far from C_0 , V accepts with proba

$$\text{err}(\delta) < \text{err}_{\text{commit}} + (\text{err}_{\text{query}}(\delta))^\alpha$$

α : repetition parameter

⁸This slide is kindly provided by Sarah Bordage.

Ingredients to fold several times: intermediary cyclic quotients

A group \mathcal{G} is solvable if $\mathcal{G} = \mathcal{G}_0 \triangleright \mathcal{G}_1 \triangleright \cdots \triangleright \mathcal{G}_r = 1$ with $\Gamma_i := \mathcal{G}_i/\mathcal{G}_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$.
composition series

1. Assume $\mathcal{G} \in \text{Aut}(\mathcal{C}_0)$ is a **large solvable** group acting **freely** on \mathcal{P}_0 ,

→ **Sequence of curves** (\mathcal{C}_i) s.t. $\mathcal{C}_{i+1} := \mathcal{C}_i/\Gamma_i$

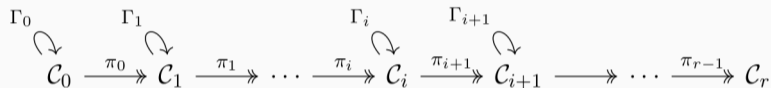
$$\begin{array}{ccccccc} \Gamma_0 & & \Gamma_1 & & \Gamma_i & & \Gamma_{i+1} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{C}_0 & \xrightarrow{\pi_0} \twoheadrightarrow & \mathcal{C}_1 & \xrightarrow{\pi_1} \twoheadrightarrow & \cdots & \xrightarrow{\pi_i} \twoheadrightarrow & \mathcal{C}_i & \xrightarrow{\pi_{i+1}} \twoheadrightarrow & \mathcal{C}_{i+1} & \longrightarrow \twoheadrightarrow & \cdots & \xrightarrow{\pi_{r-1}} \twoheadrightarrow & \mathcal{C}_r \end{array}$$

Ingredients to fold several times: intermediary cyclic quotients

A group \mathcal{G} is solvable if $\mathcal{G} = \mathcal{G}_0 \triangleright \mathcal{G}_1 \triangleright \cdots \triangleright \mathcal{G}_r = 1$ with $\Gamma_i := \mathcal{G}_i/\mathcal{G}_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$.
composition series

1. Assume $\mathcal{G} \in \text{Aut}(\mathcal{C}_0)$ is a **large solvable** group acting **freely** on \mathcal{P}_0 ,

→ **Sequence of curves** (\mathcal{C}_i) s.t. $\mathcal{C}_{i+1} := \mathcal{C}_i/\Gamma_i$



→ **Sequence of evaluation points** (\mathcal{P}_i) s.t. $\mathcal{P}_{i+1} = \pi_i(\mathcal{P}_i) \rightsquigarrow |\mathcal{P}_{i+1}| = |\mathcal{P}_i|/p_i$

2. There exists a “nice” **sequence of divisors** (D_i) that ensure distance preservation at each step.

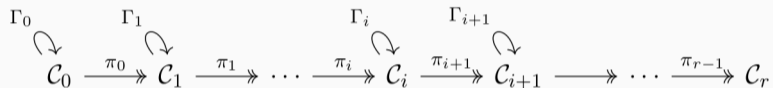
→ The AG code $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ is said to be **foldable**.

Ingredients to fold several times: intermediary cyclic quotients

A group \mathcal{G} is solvable if $\mathcal{G} = \mathcal{G}_0 \triangleright \mathcal{G}_1 \triangleright \cdots \triangleright \mathcal{G}_r = 1$ with $\Gamma_i := \mathcal{G}_i/\mathcal{G}_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$.
composition series

1. Assume $\mathcal{G} \in \text{Aut}(\mathcal{C}_0)$ is a **large solvable** group acting **freely** on \mathcal{P}_0 ,

→ **Sequence of curves** (\mathcal{C}_i) s.t. $\mathcal{C}_{i+1} := \mathcal{C}_i/\Gamma_i$



→ **Sequence of evaluation points** (\mathcal{P}_i) s.t. $\mathcal{P}_{i+1} = \pi_i(\mathcal{P}_i) \rightsquigarrow |\mathcal{P}_{i+1}| = |\mathcal{P}_i|/p_i$

2. There exists a “nice” **sequence of divisors** (D_i) that ensure distance preservation at each step.

→ The AG code $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ is said to be **foldable**.

→ **Sequence of AG codes** $C_i = C(\mathcal{C}_i, \mathcal{P}_i, D_i)$ with length and dimension ↘

→ Proximity test to C_0 reduced to *membership* test to C_r

Main properties

Assume the code $C(C_0, \mathcal{P}_0, D_0)$ of length n is **foldable** thanks to the action of \mathcal{G} on C_0 .

Set $|\mathcal{G}| := N$.

	General case	$C_0/\mathcal{G} \simeq \mathbb{P}^1$
Group size	$N > n^\varepsilon, \varepsilon \in (0, 1)$	no assumption
Proof length	$< n$	$< n$
Round complexity	$< \log n$	$< \log n$
Query complexity	$O(n^{1-\varepsilon})$	$< \alpha \cdot p_{max} \cdot \log n$
Prover complexity	$\tilde{O}(n)$	$O(n)$
Verifier complexity	$O(n^{1-\varepsilon})$	$O(\log n)$

(repetition param $\alpha, p_{max} := \max p_i$)

Recall **final test** “ $f_r \stackrel{?}{\in} C_r$ ” of length n/N (code C_r **constant** in FRI).

\rightsquigarrow One needs \mathcal{G} to be **large enough** for good complexities.

However, if C_r is a RS code, membership test to C_r can be substituted by FRI.

Number of rounds

- as many as needed in FRI,
- limited by the size of \mathcal{G} unless $\mathcal{C}_r \simeq \mathbb{P}^1$ here.

Soundness: Improved in FRI using DEEP technique and Proximity gaps.

What about with AG-codes?

Other foldable codes?

- from maximal curves (long codes, well-know geometry)
- from asymptotically good towers of curves (similar setting)

Thank you for your attention!

Distance preservation by folding (?)

Problem: all the $L_{C/\Gamma}(E_j)$ are not the same.

Define $\mathbf{Fold}[f, z] = \sum_{j=0}^{m-1} z^j f_j$. We want to prove that $\Delta(f, C) > \delta \Rightarrow \Delta(\mathbf{Fold}[f, z], C') > \delta'$
with high probability on z .

Strategy (by converse): Assume $\Delta(\mathbf{Fold}[f, z], C') \leq \delta'$ and exhibit $\tilde{f} \in C$ s.t. $\Delta(f, \tilde{f}) \leq \delta$.

Distance preservation by folding (?)

Problem: all the $L_{C/\Gamma}(E_j)$ are not the same.

Define $\mathbf{Fold}[f, z] = \sum_{j=0}^{m-1} z^j f_j$. We want to prove that $\Delta(f, C) > \delta \Rightarrow \Delta(\mathbf{Fold}[f, z], C') > \delta'$
with high probability on z .

Strategy (by converse): Assume $\Delta(\mathbf{Fold}[f, z], C') \leq \delta'$ and exhibit $\tilde{f} \in C$ s.t. $\Delta(f, \tilde{f}) \leq \delta$.

Proposition [Ben-Sasson-Kopparty-Saraf'18]

Let $V \subset \mathbb{F}^n$ be a \mathbb{F} -vector space. Let $u_0, u_1, \dots, u_{m-1} \in \mathbb{F}^n$.

If $\Delta(\sum z^i u_i, V) < \delta'$ w.h.p. on z , then for every i , $\Delta(u_i, V) < \delta$.

If $\Delta(\mathbf{Fold}[f, z], C') < \delta'$ w.h.p. on z , then $\exists \tilde{f}_j \in C' = L_{C/\Gamma}(D')$ s.t. $\Delta(f_j, \tilde{f}_j) < \delta$.

Set $\tilde{f} = \sum \mu^j \tilde{f}_j \circ \pi$. Then $\Delta(f, \tilde{f}) < \delta$ **but we cannot ensure $\tilde{f} \notin C = L_C(D)$!**

If $\deg f \leq 4$, then for $f(x) = f_0(x^2) + x f_1(x^2)$, $\deg f_0 \leq 2$ and $\deg f_1 \leq 1$.

But if $\deg \tilde{f}_0, \tilde{f}_1 \leq 2$, setting $\tilde{f}(x) = \tilde{f}_0(x^2) + x \tilde{f}_1(x^2)$, we just have $\deg \tilde{f} \leq 5$.

We need $\tilde{f}_j \in L_{C/\Gamma}(E_j) \subsetneq L_{C/\Gamma}(D)$!

Fixing the folding operator to ensure distance preservation

We need $\tilde{f}_j \in L_{C/\Gamma}(E_j) \subsetneq L_{C/\Gamma}(D')$!

Define **balancing functions** $\nu_j \in \mathbb{F}(C/\Gamma)$ s.t. $h \in L_{C/\Gamma}(E_j)$ iff $h, \nu_j h \in L_{C/\Gamma}(D')$.

(on \mathbb{P}^1 : if $\deg \nu = 1$, then $\deg h \leq d - 1$ iff $\deg h, \deg \nu h \leq d$)

To avoid C' to be too large, we want D' to be one of the E_j . For simplicity, assume $D' = E_0$.

Fixing the folding operator to ensure distance preservation

We need $\tilde{f}_j \in L_{C/\Gamma}(E_j) \subsetneq L_{C/\Gamma}(D')$!

Define **balancing functions** $\nu_j \in \mathbb{F}(C/\Gamma)$ s.t. $h \in L_{C/\Gamma}(E_j)$ iff $h, \nu_j h \in L_{C/\Gamma}(D')$.

(on \mathbb{P}^1 : if $\deg \nu = 1$, then $\deg h \leq d - 1$ iff $\deg h, \deg \nu h \leq d$)

To avoid C' to be too large, we want D' to be one of the E_j . For simplicity, assume $D' = E_0$.

(Final attempt) For any $(z_1, z_2) \in \mathbb{F}^2$, define **Fold** $[f, (z_1, z_2)] : \mathcal{P}' \rightarrow \mathbb{F}$ s.t.

$$\mathbf{Fold} [f, (z_1, z_2)] = \sum_{j=0}^{m-1} z_1^j f_j + \sum_{j=1}^{m-1} z_2^j \nu_j f_j.$$

Lemma: ν_j is a balancing function iff $(\nu_j)_\infty = D' - E_j$.

Such functions ν_j may not exist! (Weierstrass gaps)

→ Need to choose carefully D .