Interactive proofs of Proximity to Algebraic Geometry codes

Sarah Bordage **Jade Nardi**

January 12, 2021

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

LIX, Ecole Polytechnique, Institut Polytechnique de Paris
Inria

Motivation: Verifiable Computing[1]

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)

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

Motivation: Verifiable Computing[1]

Please, run program F on input x for me.

I want to quickly check if your result is correct.

Powerful Prover

(eg. a server)

outputs result y and

proof of correctness π

$$\xrightarrow{\quad y,\ \pi \quad}$$

Weak Verifier

(eg. a client)

checks validity of π

for statement "$y = F(x)$"

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

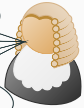
Applications: cloud computing, cryptocurrencies, blockchains

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

Motivation: Verifiable Computing[1]

Please, run program F on input x for me.

I want to quickly check if your result is correct.



Powerful Prover
(eg. a server)
outputs result y and
proof of correctness π

$\xrightarrow{y,\ \pi}$

Weak Verifier
(eg. a client)
checks validity of π
for statement "$y = F(x)$"

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

Applications: cloud computing, cryptocurrencies, blockchains

Arithmetization

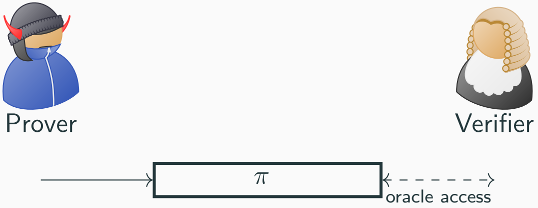
Proximity to a code C

Prover produces a word

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

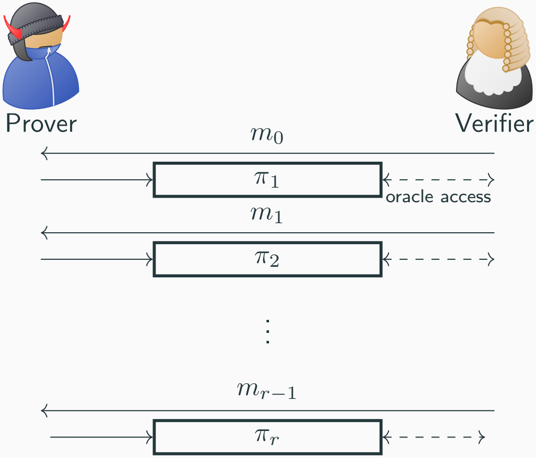
[1] Most of this slide is kindly provided by Sarah Bordage.

PCP model (Probabilistically Checkable Proofs) [2]



[2] This slide is kindly provided by Sarah Bordage.

IOP Model (Interactive Oracle Proofs)[2]



[Ben–Sasson-Chiesa-Spooner'16, Reingold-Rothblum^2'16]

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
  $|\pi_1| + \ldots + |\pi_r|$

[2] This slide is kindly provided by Sarah Bordage.

Proximity test to RS codes
Univariate low-degree testing

FRI: Prover-efficient RS IOPP (IOP of Proximity)[3]

[Ben–Sasson-Bentov-Horesh-Riabzev'18]

Reed-Solomon Proximity Testing

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

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

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

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

Δ relative Hamming distance

[3] This 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 $f : \mathcal{P} \to \mathbb{F}$ 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 $f : \mathcal{P} \to \mathbb{F}$ satisfies $\deg f < d$?

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

Check if $\deg f_0 < d/2$ and $\deg f_1 < d/2$. $\to$ 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 $f : \mathcal{P} \to \mathbb{F}$ satisfies $\deg f < d$?

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

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

Make 1 test: For $z \in \mathbb{F}$, define **Fold** $[f, z] : \mathcal{P}' \to \mathbb{F}$ 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 $f : \mathcal{P} \to \mathbb{F}$ satisfies $\deg f < d$?

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

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

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

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

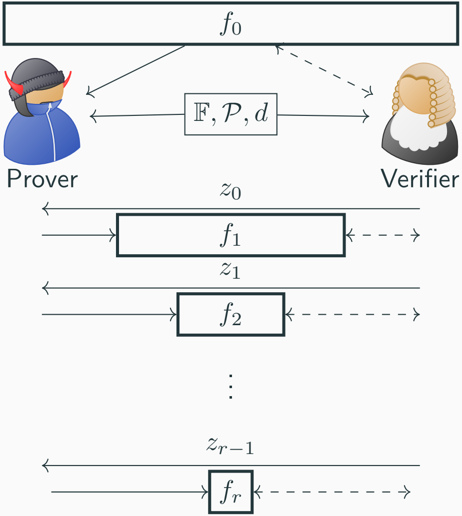
$\deg$ **Fold** $[f, -1] < 1$ but $\deg f \geq 2$

- ✔ **Completeness:** **Fold** $[\cdot, z]\,(\mathrm{RS}[\mathcal{P}, d]) \subseteq \mathrm{RS}[\mathcal{P}', d/2]$.
- ✔ **Locality:** compute a value of **Fold** $[f, z]$ on $\mathcal{P}'$ with only **2 queries** to f.

  Fold $\left[f, \pm\sqrt{y}\right](y) = f_0 \pm \sqrt{y} f_1 = f(\pm\sqrt{y})$
- ✔ **Distance preservation:** if $\Delta(f, \mathrm{RS}[\mathcal{P}, d]) > \delta$, then $\Delta($**Fold** $[f, z], \mathrm{RS}[\mathcal{P}', d/2]) > \delta'$ (w.h.p.).

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

FRI Protocol: Commit Phase[4]



Honest prover computes:

$$f_1 = \textbf{Fold}\left[f_0, z_0\right]$$

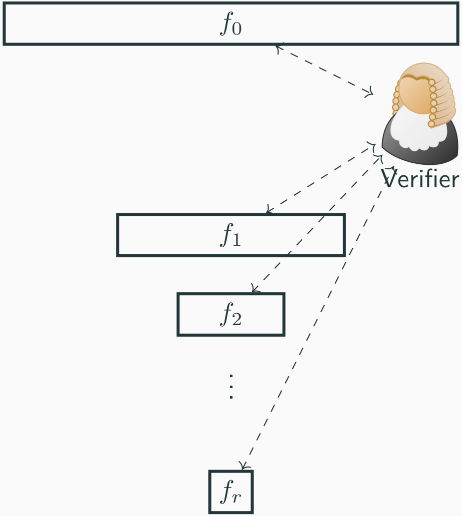
$$f_2 = \textbf{Fold}\left[f_1, z_1\right]$$

$$\vdots$$

$$f_r = \textbf{Fold}\left[f_{r-1}, z_{r-1}\right]$$

[4] This slide is kindly provided by Sarah Bordage.

FRI Protocol: Query Phase[5]



Check consistency at random locations

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

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

$$\vdots$$

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

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

[5] This slide is kindly provided by Sarah Bordage.

Soundness of the FRI Protocol [6]

Completeness: If $f \in \mathrm{RS}[\mathcal{P}, d]$, then $\exists P$ $\Pr[\text{V accepts P}] = 1$.
Soundness: If $\Delta(f, \mathrm{RS}[\mathcal{P}, d]) > \delta$, then $\forall \tilde{P}$ $\Pr[\text{V accepts } \tilde{\text{P}}] < \mathrm{err}(\delta)$.

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

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

Theorem

Assuming $\delta < 1 - \sqrt{\rho}$ (ρ is code rate), $\mathrm{err}(\delta) < err_{commit} + (err_{query})^{\alpha}$

$$< \mathrm{negl}(\kappa) + (1-\delta)^{\alpha}$$

security parameter

To get error $\mathrm{err}(\delta) = \mathrm{negl}(\kappa)$, 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").

[6] This content is kindly provided by Sarah Bordage.

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 $\mathrm{Supp}(D) := \{P \in \mathcal{C} \mid n_p \neq 0\}$.
- $D \leq D'$ 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 $\operatorname{Supp}(D) := \{P \in \mathcal{C} \mid n_p \neq 0\}$.
$D \leq D'$ 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 $\operatorname{Supp}(D) := \{P \in \mathcal{C} \mid n_p \neq 0\}$.
$D \leq D'$ 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. $\operatorname{Supp}(D) \cap \mathcal{P} = \emptyset$, the **AG code** $C = C(\mathcal{C}, \mathcal{P}, D)$ is defined as the image by $\mathbf{ev} : L_{\mathcal{C}}(D) \to \mathbb{F}^n$.

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

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

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

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 $\pi : \mathcal{C} \to \mathcal{C}' := \mathcal{C}/\Gamma$.

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

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 $\pi : \mathcal{C} \to \mathcal{C}' := \mathcal{C}/\Gamma$.

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] $L_{\mathcal{C}}(D)_j \simeq \mu^j \pi^* \left(L_{\mathcal{C}'}(E_j)\right)$ where $E_j := \left\lfloor \frac{1}{m}\pi_*(D + j(\mu)) \right\rfloor$[7] 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. $f = \sum_{j=0}^{m-1} \mu^j f_j \circ \pi$.

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

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

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

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 $\pi : \mathbb{P}^1 \to \mathbb{P}^1$ 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 $((x) = [1:0] - P_\infty)$

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

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

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

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

Kani's result on a Kummer curve

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

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

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

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

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

Kani's result on a Kummer curve

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

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

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

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 $f(x,y) = \sum_{j=0}^{N-1} y^j f_j(x, y^N)$ $\qquad (\mu = y$ as $\gamma \cdot y = \zeta y)$

where $f_j \in L_{\mathbb{P}^1}\left(\left\lfloor \frac{\pi_*(D) - j\left(\sum P_\ell - dP_\infty\right)}{N}\right\rfloor\right)$, 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 $\pi : \mathcal{C} \to \mathcal{C}/\Gamma$.

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 $D \overset{\text{[Kani'86]}}{\Longrightarrow} \underset{L_{\mathcal{C}}(D)}{\underset{\Cap}{f}} = \sum_{j=1}^{m-1} \mu^j \underset{L_{\mathcal{C}/\Gamma}(E_j)}{\underset{\Cap}{f_j}} \circ \pi.$

– 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 $\mathcal{C}/\Gamma$ 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 $\pi : \mathcal{C} \to \mathcal{C}/\Gamma$.

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 $\overset{\text{[Kani'86]}}{\Longrightarrow}$ $\underset{L_{\mathcal{C}}(D)}{\underset{\cap}{f}} = \sum_{j=1}^{m-1} \mu^j \underset{L_{\mathcal{C}/\Gamma}(E_j)}{\underset{\cap}{f_j}} \circ \pi.$

– 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 $\mathcal{C}/\Gamma$ 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** $[\cdot, z] : \mathbb{F}^{\mathcal{P}} \to \mathbb{F}^{\mathcal{P}'}$ 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 $\left\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\right\}$.
- ✖ **Distance preservation** $\Delta(f, C) > \delta \not\Rightarrow \Delta(\textbf{Fold}\,[f, z]\,, C') > \delta'$ 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: $L_{\mathcal{C}/\Gamma}(E_j) \subsetneq L_{\mathcal{C}/\Gamma}(D')$**!** 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 $D' = E_0$.

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

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

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

Such functions ν_j may not exist! (Weierstrass gaps)

$\rightarrow$ 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 $\gamma_i : (x, y) \mapsto (x, \zeta_i y)$ $(\zeta_i^{p_i} = 1)$

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

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 $d \equiv -1 \mod N$ guarantees the existence of the balancing functions.

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

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.

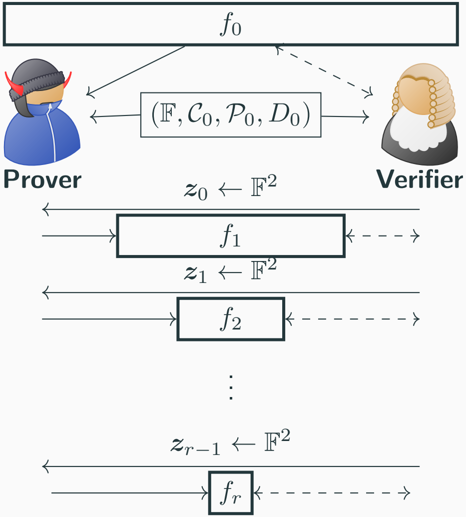
Proposition [Bordage, N.]

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

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

Proximity test to $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ of length n → 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-IOPP[8]



COMMIT Phase

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

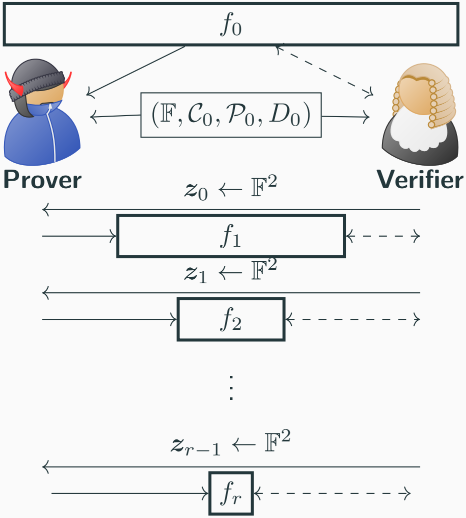
$$f_2 = \textbf{Fold}\,[f_1, z_1]$$

$$\vdots$$

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

[8] This slide is kindly provided by Sarah Bordage.

Overview of the AG-IOPP[8]



QUERY Phase

Round consistency tests:

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

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

$$f_1(Q_1) \stackrel{?}{=} \textbf{Fold}\left[f_0, \boldsymbol{z}_0\right](Q_1)$$

$$f_2(Q_2) \stackrel{?}{=} \textbf{Fold}\left[f_1, \boldsymbol{z}_1\right](Q_2)$$

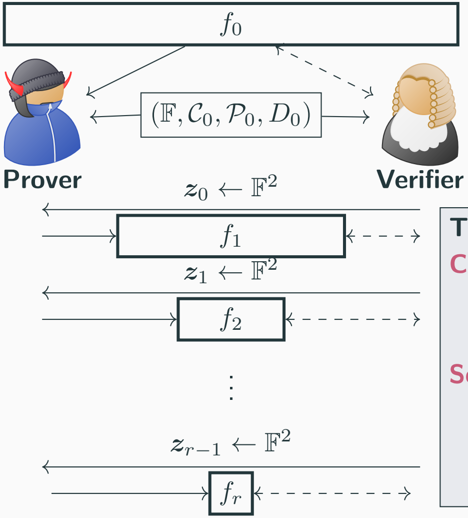
$$\vdots$$

$$f_r(Q_r) \stackrel{?}{=} \textbf{Fold}\left[f_{r-1}, \boldsymbol{z}_{r-1}\right](Q_r)$$

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

[8] This slide is kindly provided by Sarah Bordage.

Overview of the AG-IOPP[8]



Theorem [Bordage, N.]

Completeness:

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

Soundness: (relies on [BKS18] and [BGKS19])

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

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

α : repetition parameter

[8] This slide is kindly provided by Sarah Bordage.

Ingredients to fold several times: intermediary cyclic quotients

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

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

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

$$\begin{tikzcd} \mathcal{C}_0 \arrow[r, two heads, "\pi_0"] \arrow[loop above, "\Gamma_0"] & \mathcal{C}_1 \arrow[r, two heads, "\pi_1"] \arrow[loop above, "\Gamma_1"] & \cdots \arrow[r, two heads, "\pi_i"] & \mathcal{C}_i \arrow[r, two heads, "\pi_{i+1}"] \arrow[loop above, "\Gamma_i"] & \mathcal{C}_{i+1} \arrow[r, two heads] \arrow[loop above, "\Gamma_{i+1}"] & \cdots \arrow[r, two heads, "\pi_{r-1}"] & \mathcal{C}_r \end{tikzcd}$$

Ingredients to fold several times: intermediary cyclic quotients

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

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

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

$$\begin{tikzcd} \mathcal{C}_0 \arrow[loop above, "\Gamma_0"] \arrow[r, two heads, "\pi_0"] & \mathcal{C}_1 \arrow[loop above, "\Gamma_1"] \arrow[r, two heads, "\pi_1"] & \cdots \arrow[r, two heads, "\pi_i"] & \mathcal{C}_i \arrow[loop above, "\Gamma_i"] \arrow[r, two heads, "\pi_{i+1}"] & \mathcal{C}_{i+1} \arrow[loop above, "\Gamma_{i+1}"] \arrow[r, two heads] & \cdots \arrow[r, two heads, "\pi_{r-1}"] & \mathcal{C}_r \end{tikzcd}$$

   $\rightarrow$ **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.

$\rightarrow$ 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 $\underbrace{\mathcal{G} = \mathcal{G}_0 \triangleright \mathcal{G}_1 \triangleright \cdots \triangleright \mathcal{G}_r = 1}_{\text{composition series}}$ with $\Gamma_i := \mathcal{G}_i/\mathcal{G}_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$.

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

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

$$\begin{tikzcd} \mathcal{C}_0 \arrow[loop above, "\Gamma_0"] \arrow[r, two heads, "\pi_0"] & \mathcal{C}_1 \arrow[loop above, "\Gamma_1"] \arrow[r, two heads, "\pi_1"] & \cdots \arrow[r, two heads, "\pi_i"] & \mathcal{C}_i \arrow[loop above, "\Gamma_i"] \arrow[r, two heads, "\pi_{i+1}"] & \mathcal{C}_{i+1} \arrow[loop above, "\Gamma_{i+1}"] \arrow[r, two heads] & \cdots \arrow[r, two heads, "\pi_{r-1}"] & \mathcal{C}_r \end{tikzcd}$$

   $\rightarrow$ **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.

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

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

$\rightarrow$ Proximity test to C_0 reduced to *membership* test to C_r

Main properties

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

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

	$N > n^{\varepsilon}$, $\varepsilon \in (0,1)$	$N > n/\log n$
Proof length	$< n$	$< n$
Round complexity	$< \log n$	$< \log n$
	$\mathcal{C}_0/\mathcal{G} \simeq \mathbb{P}^1$ and $C_r =$ RS	
Query complexity	$O(n^{1-\varepsilon})$	$< \alpha \cdot p_{max} \cdot \log n$
Prover complexity	$\widetilde{O}(n)$	$O(n)$
Verifier complexity	$O(n^{1-\varepsilon})$	$O(\log n)$

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

Recall **final test "$f_r \overset{?}{\in} C_r$"** 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 might be substituted by FRI.

Remarks and open questions

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? Good candidates from asymptotically good towers of curves

$\rightsquigarrow$ "nice" sequence of divisors?

Thank you for your attention!

Distance preservation by folding (?)

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

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

Strategy (by converse): Assume $\Delta($**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 $L_{\mathcal{C}/\Gamma}(E_j)$ are not the same.

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

Strategy (by converse): Assume $\Delta(\textbf{Fold}\,[f, z]\,, C') \leq \delta'$ 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 $u_0, u_1, \ldots, u_{m-1} \in \mathbb{F}^n$.

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

If $\Delta(\textbf{Fold}\,[f, z]\,, C') < \delta'$ w.h.p. on z, then $\exists\, \tilde{f}_j \in C' = L_{\mathcal{C}/\Gamma}(D')$ 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 $\tilde{f} \notin C = L_{\mathcal{C}}(D)$!

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

Fixing the folding operator to ensure distance preservation

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

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 $D' = E_0$.

Fixing the folding operator to ensure distance preservation

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

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 $D' = E_0$.

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

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

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

Such functions ν_j may not exist! (Weierstrass gaps)

$\rightarrow$ Need to choose carefully D.