IOP of Proximity to Algebraic Geometry codes

Sarah Bordage   Jade Nardi

November 19, 2020

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

LIX, Ecole Polytechnique, Institut Polytechnique de Paris
Inria

Algebraic Geometry (AG) codes

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

Divisors. A **divisor** D on $\mathcal{C}$ is a formal sum of 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** $(f) := \sum_P \underbrace{v_P(f)}_{\text{valuation}} P$.

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

Embedding of RR spaces: If $D \leq D'$, then $L_{\mathcal{C}}(D) \subset L_{\mathcal{C}}(D')$.

AG codes

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

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

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

Let $\mathcal{C}$ be a curve over a field $\mathbb{F}$ and let $\Gamma = \langle\gamma\rangle \simeq \mathbb{Z}/m\mathbb{Z}$ a group of automorphisms of $\mathcal{C}$ s.t $\gcd(m, |\mathbb{F}|) = 1$. Set the projection map $\pi : \mathcal{C} \to \mathcal{C}' := \mathcal{C}/\Gamma$. 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].

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

Splitting of Riemann-Roch spaces: $L_{\mathcal{C}}(D) = \bigoplus_{j=0}^{m-1} \mu^j \pi^* L_{\mathcal{C}'}\left(E_j\right)$

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

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

FRI context: For evaluation domain $\mathcal{P} = \langle [1:\omega]\rangle$ where ω has order 2^r.

- $\gamma : [X_0 : X_1] \mapsto [X_0 : -X_1]$ acts on $\mathbb{P}^1$ and $\langle \gamma \rangle \simeq \mathbb{Z}/2\mathbb{Z}$,
- Define projection $\pi : \mathbb{P}^1 \to \mathbb{P}^1$ by $\pi[X_0 : X_1] := [X_0^2 : X_1^2]$,

Consider the RS code RS$[\mathbb{F}, \mathcal{P}, d+1]$ viewed as the AG code $C = C(\mathbb{P}^1, \mathcal{P}, dP_\infty)$, where $P_\infty = [0:1]$.

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

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

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

$\to$ **Proximity to $C = C(\mathcal{C}, \mathcal{P}, D)$ reduced to proximity to** $C' = C(\mathbb{P}^1, \mathcal{P}', \left\lfloor \frac{d}{2} \right\rfloor P_\infty)$ where $\mathcal{P}' = \pi(\mathcal{P})$.

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.

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 an AG-code $C = C(\mathcal{C}, \mathcal{P}, D)$ reduced to proximity to an AG-code $C' = C(\mathcal{C}/\Gamma, \mathcal{P}', D')$

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. $L_{\mathcal{C}/\Gamma}(D') \supseteq L_{\mathcal{C}/\Gamma}(E_j)$.

1. Split $f : \mathcal{P} \to \mathbb{F}$ into m functions $f_j : \mathcal{P}' \to \mathbb{F}$.
2. For any $z \in \mathbb{F}$, define **folding** of f as the function **Fold** $[f, z] : \mathcal{P}' \to \mathbb{F}$ s.t. **Fold** $[f, z] = \sum_{j=0}^{m-1} z^j f_j$.

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

The folding operator

(First attempt) If we define **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 the set of m points $\left\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\right\}$.
- ✖ **Distance preservation:** If $\Delta(f, C) > \delta$, then $\Delta($**Fold** $[f, z], C') > \delta'$ (w.h.p.).
  We need to ensure that $f_j \notin L(D') \setminus L(E_j)$!

The folding operator

(First attempt) If we define **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 the set of m points $\left\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\right\}$.
- ✖ **Distance preservation:** If $\Delta(f,C) > \delta$, then $\Delta($**Fold** $[f,z], C') > \delta'$ (w.h.p.).
  We need to ensure that $f_j \notin L(D') \setminus L(E_j)$!

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

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

We assume there exists $\nu_j \in \mathbb{F}(\mathcal{C}/\Gamma)$ such that $(\nu_j)_\infty = D' - E_j$. (for simplicity, take $D' = E_0$.)

$\longrightarrow$ Need to carefully define D', otherwise such functions ν_j may not exist.

The folding operator

(First attempt) If we define **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 the set of m points $\left\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\right\}$.
- ✖ **Distance preservation:** If $\Delta(f, C) > \delta$, then $\Delta($**Fold** $[f, z], C') > \delta'$ (w.h.p.).

  We need to ensure that $f_j \notin L(D') \setminus L(E_j)$!

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

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

We assume there exists $\nu_j \in \mathbb{F}(\mathcal{C}/\Gamma)$ such that $(\nu_j)_\infty = D' - E_j$. (for simplicity, take $D' = E_0$.)

$\longrightarrow$ Need to carefully define D', otherwise such functions ν_j may not exist.

(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.

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

Foldable AG codes

An AG code $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ is said to be **foldable** if we can **repeat** the previous process:

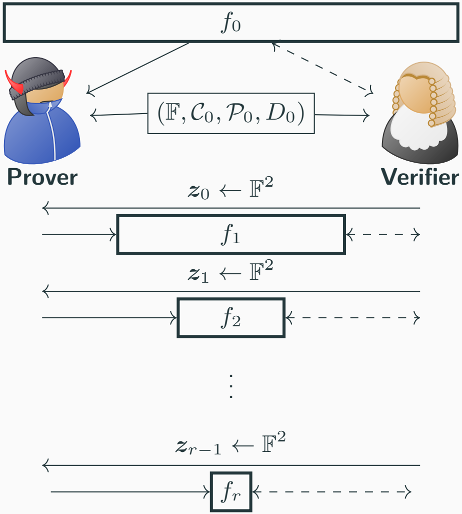
$$\overset{\Gamma_0}{\circlearrowright}\mathcal{C}_0 \xrightarrow{\pi_0} \overset{\Gamma_1}{\circlearrowright}\mathcal{C}_1 \xrightarrow{\pi_1} \cdots \xrightarrow{\pi_i} \overset{\Gamma_i}{\circlearrowright}\mathcal{C}_i \xrightarrow{\pi_{i+1}} \overset{\Gamma_{i+1}}{\circlearrowright}\mathcal{C}_{i+1} \longrightarrow \cdots \xrightarrow{\pi_{r-1}} \mathcal{C}_r$$

1. There exists a large solvable group $\mathcal{G} \in \mathrm{Aut}(\mathcal{C}_0)$ acting freely on $\mathcal{P}_0$, $\underbrace{\mathcal{G} = \mathcal{G}_0 \rhd \mathcal{G}_1 \rhd \cdots \rhd \mathcal{G}_r = 1}_{\text{composition series}}$
   $\rightarrow \Gamma_i := \mathcal{G}_i / \mathcal{G}_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$
   $\rightarrow$ **Sequence of curves** $(\mathcal{C}_i)$ s.t. $\mathcal{C}_{i+1} := \mathcal{C}_i / \Gamma_i$
   $\rightarrow$ **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), i.e. for each i:
   - D_i is supported by Γ_i-fixed points,
   - for every $0 \leq j < p_i$, $E_{i,j} \leq D_{i+1}$, ([Kani'86] $L(D_i)$ is split into p_i smaller spaces $L(E_{i,j})$)
   - for every $0 \leq j < p_i$, there exists $\nu_{i+1,j} \in \mathbb{F}(\mathcal{C}_{i+1})$ s.t. $(\nu_{i+1,j})_\infty = D_{i+1} - E_{i,j}$.

A foldable AG code $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ induces
a **sequence of AG codes** $(C_i = C(\mathcal{C}_i, \mathcal{P}_i, D_i))$.

Overview of the AG-IOPP



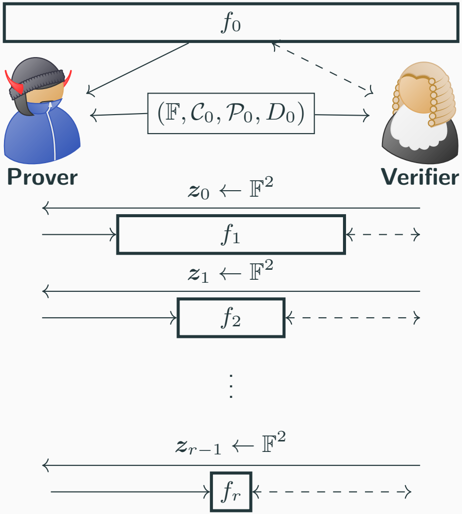
COMMIT Phase

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

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

$$\vdots$$

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



QUERY Phase

Round consistency tests:

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

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

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

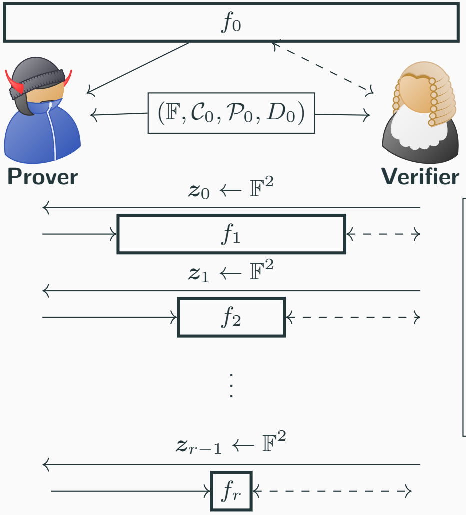
$$f_2(Q_2) \stackrel{?}{=} \textbf{Fold}\,[f_1, z_1]\,(Q_2)$$

$$\vdots$$

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

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

Overview of the AG-IOPP



Completeness:

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

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

If f_0 is δ-far from C_0, $\mathcal{V}$ accepts with proba $\mathrm{err}(\delta) < \mathrm{err}_{\mathrm{commit}} + (\mathrm{err}_{\mathrm{query}}(\delta))^{\alpha}$

α : repetition parameter

A family of foldable codes on Kummer curves

Assume $\gcd(N, d) = 1$ and $\gcd(N, |\mathbb{F}|) = 1$.

The group $\mathbb{Z}/N\mathbb{Z}$ **acts on** $\mathcal{C}_0$ ($(x, y) \mapsto (x, \zeta y)$ for $\zeta^N = 1$) and is **solvable**. Write $N = \prod_{i=0}^{r-1} p_i$ and $N_i = \prod_{j=i}^{r-1} p_j$

$$\mathbb{Z}/N\mathbb{Z} \rhd \mathbb{Z}/N_1\mathbb{Z} \rhd \mathbb{Z}/N_2\mathbb{Z} \rhd \cdots \rhd \mathbb{Z}/N_{r-1}\mathbb{Z} \rhd 1$$

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

Sequence of divisors (D_i) supported by Γ_i−fixed points:
$P_\ell := (\alpha_\ell, 0)$ and P_∞^i (unique point at ∞)

Any fct $f \in L_{\mathcal{C}_i}(D_i)$ can be written ($\mu_i = y$ as $\gamma_i \cdot y = \zeta_i y$)

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

$$f(x, y) = \sum_{j=0}^{p_i - 1} y^j f_j(x, y^{p_i}) \text{ with } f_j \in L_{\mathcal{C}_{i+1}}\left(\left\lfloor \frac{\pi_{i*}(D) - jdP_\infty^{i+1} + j\sum P_\ell}{p_i} \right\rfloor \right).$$

The code $C(\mathcal{C}, \mathcal{P}, D)$ is foldable for $D = \sum_{\ell=1}^{d} a_\ell P_\ell + bP_\infty^0$ if $N \mid a_\ell, b$ and $d \equiv -1 \mod N$.

Existence of the **balancing functions** ✔

Main properties

Proximity testing to $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ of length n with $\mathcal{C}_0$ a Kummer curve

$$\mathcal{C}_0 : y^N = f(x), \qquad N > n^\varepsilon,\ \varepsilon \in (0,1).$$

- Minimum distance of each code C_i is $\Delta(C_i) = \Delta(C_0) = 1 - \frac{\deg D_0}{n}$.
- Last code C_r is a RS code of length n/N and dimension $k = \deg(D_0)/N + 1 < n/N$.

Proof length	$< n$
Round complexity	$< \log n$
Query complexity	$O(n^{1-\varepsilon})$
Prover complexity	$\widetilde{O}(n)$
Verifier complexity	$O(n^{1-\varepsilon})$

Question: Why not **linear** prover time and **logarithmic** query and verifier complexities (as in FRI)?

Main properties

Proximity testing to $C_0 = C(\mathcal{C}_0, \mathcal{P}_0, D_0)$ of length n with $\mathcal{C}_0$ a Kummer curve

$$\mathcal{C}_0 : y^N = f(x), \qquad N > n^{\varepsilon},\ \varepsilon \in (0,1).$$

- Minimum distance of each code C_i is $\Delta(C_i) = \Delta(C_0) = 1 - \frac{\deg D_0}{n}$.
- Last code C_r is a RS code of length n/N and dimension $k = \deg(D_0)/N + 1 < n/N$.

Proof length	$< n$	
Round complexity	$< \log n$	
Query complexity	$< \alpha \cdot p_{max} \cdot \log n + k$	(repetition param α, $p_{max} := \max p_i$)
Prover complexity	$O(n) + \widetilde{O}(n/N)$	
Verifier complexity	$O(\log n) + \widetilde{O}(k)$	

Question: Why not **linear** prover time and **logarithmic** query and verifier complexities (as in FRI)?

Recall **final test "$f_r \overset{?}{\in} C_r$"** : the length n/N of the last code C_r is **not constant**.
$\rightsquigarrow$ One needs $N = |\mathcal{G}|$ to be **large enough** for better complexities.

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

Remarks and open questions

<table>
<tr><th></th><th>FRI</th><th>AG-IOPP</th></tr>
<tr><td>Number of rounds</td><td>as many as needed</td><td>limited by the size of $\mathcal{G}$
unless $\mathcal{C}_r \simeq \mathbb{P}^1$</td></tr>
<tr><td rowspan="2">Commit error</td><td colspan="2">$\mathsf{err}_{\mathsf{commit}} \leq \frac{\cdots}{|\mathbb{F}|}$</td></tr>
<tr><td>divided by $\approx \left|\mathbb{P}^1(\mathbb{F})\right|$</td><td>$|\mathcal{C}_i(\mathbb{F})| > |\mathbb{F}|$
Could we sample over the points of the curves?</td></tr>
</table>

On improving soundness: DEEP technique for AG codes? Proximity gaps?

Other foldable codes?

Good candidates from asymptotically good towers of curves ($\rightsquigarrow$ “nice” sequence of divisors?)