IOP of Proximity to Algebraic Geometry codes

Sarah Bordage    Jade Nardi

LIX, Ecole Polytechnique, Institut Polytechnique de Paris
Inria

November 19, 2020
https://eccc.weizmann.ac.il/report/2020/165/
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 \( \text{Supp}(D) := \{ P \in \mathcal{C} \mid n_P \neq 0 \} \).

\( D \leq D' \) if \( n_P \leq n'_P \) for every \( P \).

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

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

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

**AG codes**

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

We always choose \( D \) so that \( \text{ev} \) is injective: \( \mathbb{F}^n \hookrightarrow \mathbb{F}^P \) and

\[
C(\mathcal{C}, \mathcal{P}, D) = \{ f : \mathcal{P} \to \mathbb{F} \mid f \text{ coincides with a fct in } \mathcal{L}_\mathcal{C}(D) \}.
\]
Group action and Kani’s splitting of Riemann-Roch spaces

Let $C$ 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 $C$ s.t. $\gcd(m, |\mathbb{F}|) = 1$. Set the projection map $\pi : C \to C' := C/\Gamma$. Take $\zeta \in \overline{\mathbb{F}}$ a primitive $m^{th}$ root of unity.

- $\Gamma$ acts on the functions on $C$: $\gamma \cdot f = f \circ \gamma$ for any fct $f$ on $C$.
- There exists a function $\mu$ on $C$ s.t. $\gamma \cdot \mu = \zeta \mu$ [Kani’86].

For any $\Gamma$-invariant divisor $D$ on $C$, the action of $\Gamma$ on $L_C(D)$ gives

$$L_C(D) = \bigoplus_{j=0}^{m-1} L_C(D)_j$$

where $L_C(D)_j := \{g \in L_C(D) \mid \gamma \cdot g = \zeta^j g\}$.

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

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

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

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

2 / 10
Kani’s result on $\mathcal{C} = \mathbb{P}^1$

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

**FRI context:** For evaluation domain $\mathcal{P} = \langle [1 : \omega] \rangle$ where $\omega$ 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 $\text{RS}[\mathbb{F}, \mathcal{P}, d+1]$ viewed as the AG code $C = C(\mathbb{P}^1, \mathcal{P}, d\mathcal{P}_\infty)$, where $P_\infty = [0 : 1]$.

**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 polynomial $f$ of degree $\leq d$ can be written $f(x) = f_0(x^2) + xf_1(x^2)$ with $\begin{bmatrix} \deg f_0 \leq \left\lfloor \frac{d}{2} \right\rfloor, \\
\deg f_1 \leq \left\lfloor \frac{d-1}{2} \right\rfloor \end{bmatrix}$.

→ **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 $\Gamma \cong \mathbb{Z}/m\mathbb{Z}$, with the projection map $\pi : \mathcal{C} \to \mathcal{C}/\Gamma$.

**FRI’s idea:** proximity to an AG-code $\mathcal{C} = \mathcal{C}(\mathcal{C}, \mathcal{P}, D)$ reduced to proximity to an AG-code $\mathcal{C}’ = \mathcal{C}(\mathcal{C}/\Gamma, \mathcal{P}’, D’)$

We need:

- a $\Gamma$-invariant divisor $D$ (Kani'86) such that $f = \sum_{j=1}^{m-1} \mu^j f_j \circ \pi$.

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

Take $\mathcal{P}’ = \pi(\mathcal{P})$ ($|\mathcal{P}’| = |\mathcal{P}|/m$) and $D’$ is a divisor on $\mathcal{C}/\Gamma$ such that $L_{\mathcal{C}/\Gamma}(D’) \supseteq L_{\mathcal{C}/\Gamma}(E_j)$.

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 $\text{Fold} [f, z] : \mathcal{P}’ \to \mathbb{F}$ such that $\text{Fold} [f, z] = \sum_{j=0}^{m-1} z^j f_j$.

   $\rightarrow \text{Fold} [\cdot, z] (\mathcal{C}) \subseteq \mathcal{C}’$
The folding operator

(First attempt) If we define $\text{Fold} [f, z] = \sum_{j=0}^{m-1} z^j f_j$:

- **Completeness:** $\text{Fold} [\cdot, z] (C) \subseteq C'$.
- **Locality:** For any $P \in \mathcal{P}'$, compute $\text{Fold} [f, z] (P)$ with $m$ queries to $f$. Interpolate the set of $m$ points $\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\}$.
- **Distance preservation:** If $\Delta(f, C) > \delta$, then $\Delta(\text{Fold} [f, z], C') > \delta'$ (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 $\text{Fold} [f, z] = \sum_{j=0}^{m-1} z^j f_j$:

- **Completeness:** $\text{Fold} [\cdot, z] (C) \subseteq C'$.
- **Locality:** For any $P \in \mathcal{P}'$, compute $\text{Fold} [f, z] (P)$ with $m$ queries to $f$. Interpolate the set of $m$ points $\{(\mu(Q), f(Q)) \mid Q \in \pi^{-1}(\{P\})\}$.
- **Distance preservation:** If $\Delta(f, C) > \delta$, then $\Delta(\text{Fold} [f, z], C') > \delta'$ (w.h.p.).

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

Define **balancing functions** $\nu_j \in \mathbb{F}(C/\Gamma)$ 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 $\nu_j \in \mathbb{F}(C/\Gamma)$ such that $(\nu_j)_\infty = D' - E_j$. (for simplicity, take $D' = E_0$.)

$\rightarrow$ Need to carefully define $D'$, otherwise such functions $\nu_j$ may not exist.
The folding operator

(First attempt) If we define $\text{Fold} [f, z] = \sum_{j=0}^{m-1} z^j f_j$:

- **Completeness:** $\text{Fold} [\cdot, z] (C) \subseteq C'$.
- **Locality:** For any $P \in \mathcal{P}'$, compute $\text{Fold} [f, z] (P)$ with $m$ queries to $f$.
- **Distance preservation:** If $\Delta(f, C) > \delta$, then $\Delta(\text{Fold} [f, z], C') > \delta'$ (w.h.p.).

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

Define balancing functions $\nu_j \in \mathbb{F}(C/\Gamma)$ 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 $\nu_j \in \mathbb{F}(C/\Gamma)$ such that $(\nu_j)_{\infty} = D' - E_j$. (for simplicity, take $D' = E_0$.)

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

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

$$\text{Fold} [f, (z_1, z_2)] = \sum_{j=0}^{m-1} z_1^j f_j + \sum_{j=1}^{m-1} z_2^j \nu_j f_j.$$
An AG code $C_0 = C(C_0, \mathcal{P}_0, D_0)$ is said to be **foldable** if we can **repeat** the previous process:

1. There exists a large solvable group $G \in \text{Aut}(C_0)$ acting **freely** on $\mathcal{P}_0$, $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1$

   → $\Gamma_i := G_i/G_{i+1} \simeq \mathbb{Z}/p_i\mathbb{Z}$

   → **Sequence of curves** $(C_i)$ s.t. $C_{i+1} := C_i/\Gamma_i$

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

2. There exists a “nice” **sequence of divisors** $(D_i)$, i.e. for each $i$:
   - $D_i$ is supported by $\Gamma_i$-fixed points,
   - for every $0 \leq j < p_i$, $E_{i,j} \leq D_{i+1}$, \quad ([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 $\nu_{i+1,j} \in \mathbb{F}(C_{i+1})$ s.t. $(\nu_{i+1,j})_\infty = D_{i+1} - E_{i,j}$.

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

\[ f_0 \]

\[ (F, C_0, P_0, D_0) \]

**COMMIT Phase**

\[ z_0 \leftarrow F^2 \]

\[ f_1 \]

\[ z_1 \leftarrow F^2 \]

\[ f_2 \]

\[ \vdots \]

\[ z_{r-1} \leftarrow F^2 \]

\[ f_r \]

\[ f_1 = \text{Fold}[f_0, z_0] \]

\[ f_2 = \text{Fold}[f_1, z_1] \]

\[ \vdots \]

\[ f_r = \text{Fold}[f_{r-1}, z_{r-1}] \]
Overview of the AG-IOPP

**QUERY Phase**

**Round consistency tests:**
Sample $Q_0 \in \mathcal{P}_0$, Define query path $(Q_1, \ldots, Q_r)$ s.t. $Q_{i+1} = \pi_i(Q_i)$.

\[
\begin{align*}
  f_1(Q_1) & \overset{?}{=} \text{Fold}[f_0, z_0](Q_1) \\
  f_2(Q_2) & \overset{?}{=} \text{Fold}[f_1, z_1](Q_2) \\
  & \vdots \\
  f_r(Q_r) & \overset{?}{=} \text{Fold}[f_{r-1}, z_{r-1}](Q_r)
\end{align*}
\]

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

Completeness:
If $f_0 \in \mathcal{C}_0$, $V$ accepts with proba 1.

Soundness:
(relies on [BKS18] and [BGKS19]) If $f_0$ is $\delta$-far from $\mathcal{C}_0$, $V$ accepts with proba $\text{err}(\delta) < \text{err}_{\text{commit}} + (\text{err}_{\text{query}}(\delta))^{\alpha^\alpha}$.

α: repetition parameter
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 $\delta$-far from $C_0$, $\mathcal{V}$ accepts with proba
$err(\delta) < err_{\text{commit}} + (err_{\text{query}}(\delta))^\alpha$

$\alpha$ : repetition parameter
A family of foldable codes on Kummer curves

Assume \( \gcd(N, d) = 1 \) and \( \gcd(N, |F|) = 1 \).

The group \( \mathbb{Z}/N \mathbb{Z} \) acts on \( C_0 \) \((x, y) \mapsto (x, \zeta y)\) for \( \zeta^N = 1 \) and is solvable. Write \( N = \prod_{i=0}^{r-1} p_i \) and \( N_i = \prod_{j=0}^{r-1} p_{ij} \)

\[
\mathbb{Z}/N \mathbb{Z} \triangleright \mathbb{Z}/N_1 \mathbb{Z} \triangleright \mathbb{Z}/N_2 \mathbb{Z} \triangleright \cdots \triangleright \mathbb{Z}/N_{r-1} \mathbb{Z} \triangleright 1
\]

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

Sequence of divisors \((D_i)\) supported by \( \Gamma_i \)-fixed points:

\( P_\ell := (\alpha_\ell, 0) \) and \( P_i^\infty \) (unique point at \( \infty \))

Any fct \( f \in L_{C_i}(D_i) \) can be written \((\mu_i = y as \gamma_i : y = \zeta_i y)\)

\[
f(x, y) = \sum_{j=0}^{p_i-1} y^j f_j(x, y^{p_i}) \text{ with } f_j \in L_{C_i+1} \left( \left[ \frac{\pi_i^*(D) - jdP_i^{\infty+1} + j \sum P_\ell}{p_i} \right] \right).
\]

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

Existence of the balancing functions \( \checkmark \)
Main properties

Proximity testing to \( C_0 = C(C_0, P_0, D_0) \) of length \( n \) with \( C_0 \) a Kummer curve
\[
C_0 : y^N = f(x), \quad N > n^\varepsilon, \varepsilon \in (0, 1).
\]

- 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 \( k = \deg(D_0)/N + 1 < n/N \).

<table>
<thead>
<tr>
<th>Proof length</th>
<th>(&lt; n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round complexity</td>
<td>(&lt; \log n)</td>
</tr>
<tr>
<td>Query complexity</td>
<td>(O(n^{1-\varepsilon}))</td>
</tr>
<tr>
<td>Prover complexity</td>
<td>(\tilde{O}(n))</td>
</tr>
<tr>
<td>Verifier complexity</td>
<td>(O(n^{1-\varepsilon}))</td>
</tr>
</tbody>
</table>

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

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

\[
C_0 : y^N = f(x), \quad N > n^\varepsilon, \quad \varepsilon \in (0,1).
\]

- 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 \( \alpha, \ p_{max} := \max p_i \) |
| Prover complexity | \( O(n) + \tilde{O}(n/N) \) |
| Verifier complexity | \( O(\log n) + \tilde{O}(k) \) |

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

Recall **final test** “\( f_r \notin C_r \)” : the length \( n/N \) of the last code \( C_r \) is **not constant**.

\(~\rightarrow\) 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.
<table>
<thead>
<tr>
<th>Remarks and open questions</th>
</tr>
</thead>
</table>

**Remarks and open questions**

### FRI vs. AG-IOPP

<table>
<thead>
<tr>
<th></th>
<th>FRI</th>
<th>AG-IOPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of rounds</td>
<td>as many as needed</td>
<td>limited by the size of $\mathcal{G}$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unless $C_r \simeq \mathbb{P}^1$</td>
</tr>
<tr>
<td>Commit error</td>
<td>$\text{err}_{\text{commit}} \leq \frac{\cdots}{</td>
<td>\mathbb{F}</td>
</tr>
<tr>
<td></td>
<td>divided by $\approx</td>
<td>\mathbb{P}^1(\mathbb{F})</td>
</tr>
<tr>
<td></td>
<td></td>
<td>points of the curves?</td>
</tr>
</tbody>
</table>

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

**Other foldable codes?**

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