Interactive Oracle Proofs of Proximity to Codes on Graphs

Hugo Delavenne, Tanguy Medevielle, Élina Roussel

ISIT 2025, Ann Arbor

Thursday 26th June 2025

1. Interactive Oracle Proofs of Proximity
2. Flowering protocol

1 Interactive Oracle Proofs of Proximity

2 Flowering protocol

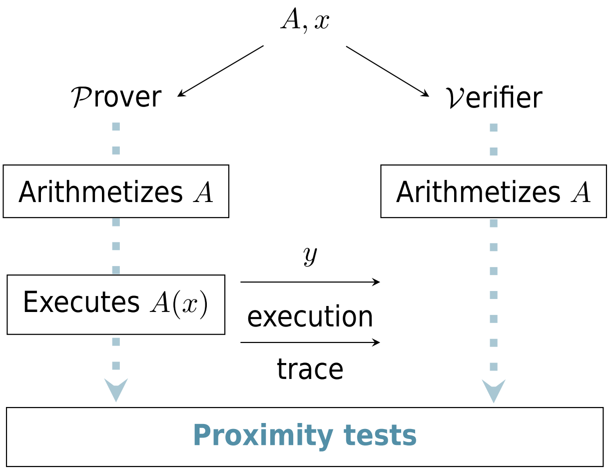
- Interactive Oracle Proof of Proximity
- Fast Reed-Solomon IOPP

SNARK means

- **S**uccinct
- **N**on-interactive
- **AR**gument of
- **K**nowledge

Goal: $\mathcal{P}$ convices $\mathcal{V}$ that

$$y = A(x)$$



Definition **Locally-testable code**

$C \subseteq \mathbb{F}^N$ is (ℓ, δ, s)-locally-testable if there is $\mathcal{V}$ with only ℓ **queries** to u such that

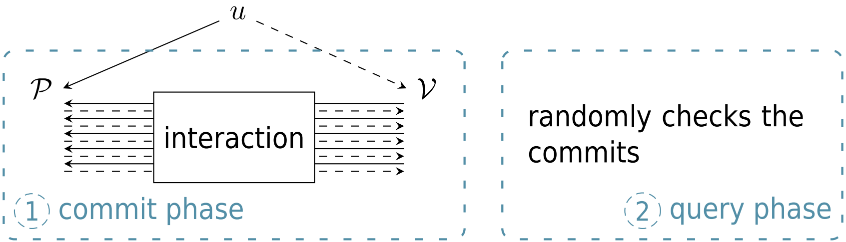
- **Completeness:** if $u \in C$ then $\mathbb{P}(\mathcal{V}^u \text{ accepts}) = 1$
- **Soundness:** if $\Delta(u, C) > \delta$ then $\mathbb{P}(\mathcal{V}^u$ **accepts**$) \leqslant s$

C has **locality** ℓ if C is (ℓ, δ, s)-locally-testable for $\delta, s < 1$.

Example **Reed-Solomon codes are not locally-testable**

RS$[\mathcal{L}, K] := \{f : \mathcal{L} \to \mathbb{F} \mid f \in \mathbb{F}[X]_{\leqslant K-1}\}$ does **not** have locality $\ell \leqslant K$.

Proof.
Any K values correspond to a degree $\leqslant K - 1$ polynomial by interpolation.



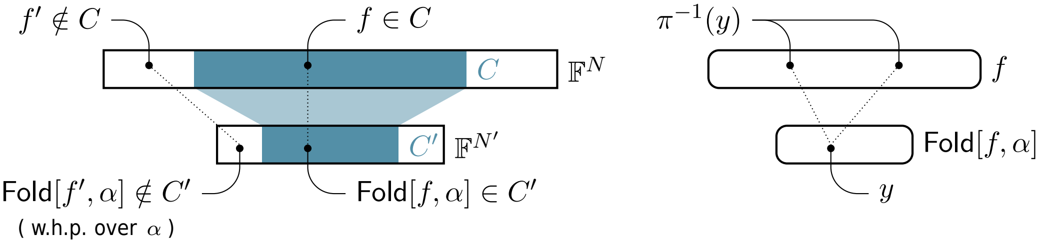
- **Completeness:** if $u \in C$ then $\mathbb{P}(\mathcal{V}^{u,\leftrightarrow\mathcal{P}}$ accepts$) = 1$
- **Soundness:** if $\Delta(u, C) > \delta$ then for any $\mathcal{P}$, $\mathbb{P}(\mathcal{V}^{u,\leftrightarrow\mathcal{P}}$ **accepts**$) \leqslant s$

[BCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive Oracle Proofs.
In *Theory of Cryptography: 14th International Conference, TCC 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part II 14*, pages 31–60. Springer, 2016

Definition **Folding operator**

Let $C \subseteq \mathbb{F}^N$, $C' \subseteq \mathbb{F}^{N'}$. **Fold** : $\mathbb{F}^N \times \mathbb{F} \to \mathbb{F}^{N'}$ must satisfy for $f \in \mathbb{F}^N$

- **Completeness:** If $f \in C$ then $\mathrm{Fold}[f, \alpha] \in C'$
- **Soundness:** If $\Delta(f, C) > \delta$ then $\Delta(\mathrm{Fold}[f, \alpha], C') > \delta - \varepsilon$ w.h.p. over α
- **Locality:** $\mathcal{V}$ computes $\mathrm{Fold}[f, \alpha](y)$ with only queries to $f(\pi^{-1}(y))$



Folding polynomials

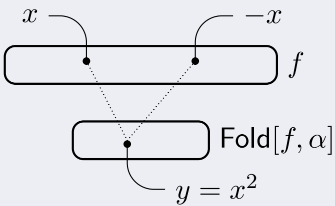
Idea: Test even and odd parts $f(X) =: f_{\text{even}}(X^2) + X f_{\text{odd}}(X^2)$

Definition **Folding**

Let $\mathcal{L}_1 := \{x^2 \mid x, -x \in \mathcal{L}_0\}$.

Define $\mathbf{Fold}[f, \alpha] : \mathcal{L}_1 \to \mathbb{F}$

$$\begin{aligned}\text{Fold}[f,\alpha](x^2) &:= f_{\text{even}}(x^2) + \alpha f_{\text{odd}}(x^2)\\ &= \frac{f(x)+f(-x)}{2} + \alpha \frac{f(x)-f(-x)}{2x}\end{aligned}$$



Field restriction: repeated foldings require $\approx |\mathcal{L}_0|$th roots of unity

e.g. $\mathbb{F}_p$ with $p = 2^{64} - 2^{32} + 1$ has 2^{32}th roots of unity

[BBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. In *45th international colloquium on automata, languages, and programming (ICALP 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018

$$f_0 : \mathcal{L}_0 \to \mathbb{F}$$

$\mathcal{P}$ $\mathcal{V}$

$$\alpha_0 \xleftarrow{\$} \mathbb{F}$$

$$f_1 : \mathcal{L}_1 \to \mathbb{F}$$

$$f_1 = \mathsf{Fold}[f_0, \alpha_0]$$

$$\vdots$$

$$\alpha_{r-1} \xleftarrow{\$} \mathbb{F}$$

$$f_r : \mathcal{L}_r \to \mathbb{F}$$

$$f_r = \mathsf{Fold}[f_{r-1}, \alpha_{r-1}]$$

1 commit phase

$$x_0 \xleftarrow{\$} \mathcal{L}_0,\ x_1 := x_0^2$$

$$f_1(x_1) \stackrel{?}{=} \mathsf{Fold}[f_0, \alpha_0](x_1)$$

$$\vdots$$

$$x_r := x_{r-1}^2$$

$$f_r(x_r) \stackrel{?}{=} \mathsf{Fold}[f_{r-1}, \alpha_{r-1}](x_r)$$

repeat m times

$$f_r \stackrel{?}{\in} \mathsf{RS}[\mathcal{L}_r, K/2^r]$$

2 query phase

[BBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. In *45th international colloquium on automata, languages, and programming (ICALP 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018

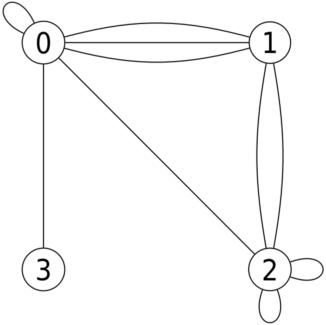
1 Interactive Oracle Proofs of Proximity

2 Flowering protocol

- Codes on graphs
- Folding graphs
- Flowering protocol
- Graphs considered

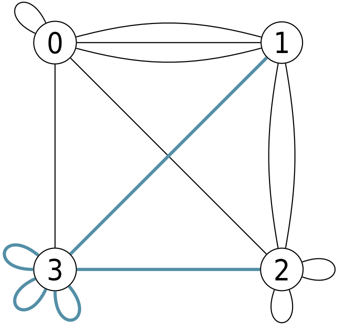
$\Gamma = (V, E)$ is a n-RIM:

- **Multigraph:** multiple edges and loops



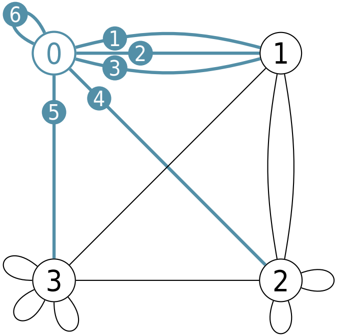
$\Gamma = (V, E)$ is a n-RIM:

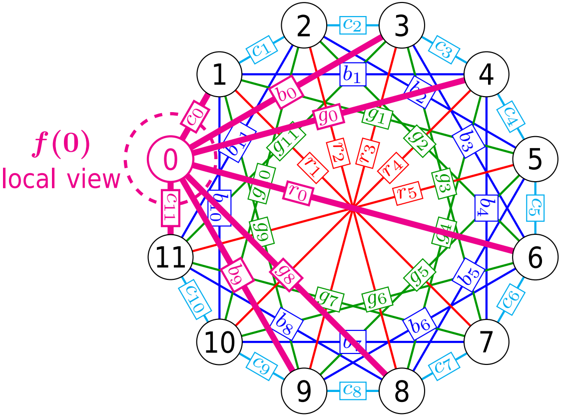
- ▷ **Multigraph:** multiple edges and loops
- ▶ **Regular:** same number n of edges



$\Gamma = (V, E)$ is a n-RIM:

- **Multigraph:** multiple edges and loops
- **Regular:** same number n of edges
- **Indexed:** edge is $(v, \ell) \in V \times [n]$
  Write $E(v, \ell) \in V$ the neighbor of v by ℓ





Word $f : V \times [n] \to \mathbb{F}$ on a graph Γ

Definition **Code $\mathcal{C}[\Gamma, C_0]$**

Given Γ a n-RIM and $C_0 \subseteq \mathbb{F}^n$,

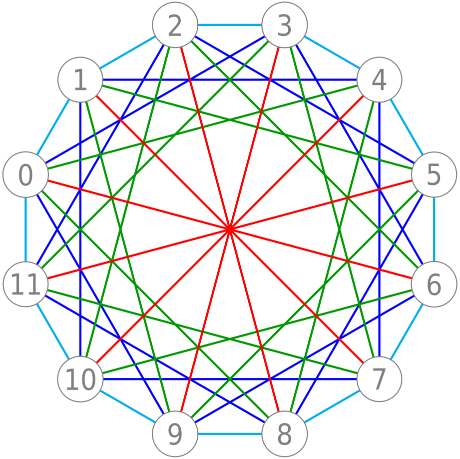
$$f \in \mathcal{C}[\Gamma, C_0] \iff \forall v,\ f(v) \in C_0.$$

We'll only use $C_0 = \mathsf{RS}[n, k]$.

Example

For $v = 0$, being a codeword requires $(c_0, b_0, g_0, r_0, g_8, b_9, c_{11}) \in \mathsf{RS}[7, k]$.

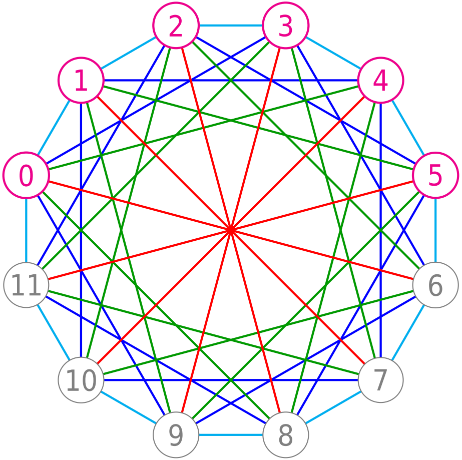
Cut-graph $\Gamma' = \mathrm{Cut}[\Gamma, V']$:



[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Cut-graph $\Gamma' = \mathsf{Cut}[\Gamma, V']$:

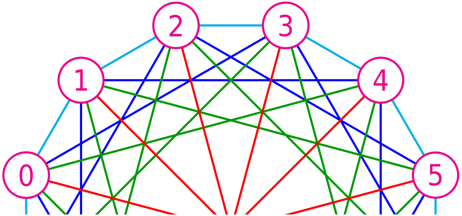
- Choose vertices $V' \subseteq V$



[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Cut-graph $\Gamma' = \mathsf{Cut}[\Gamma, V']$:

- Choose vertices $V' \subseteq V$
- Cut the rest

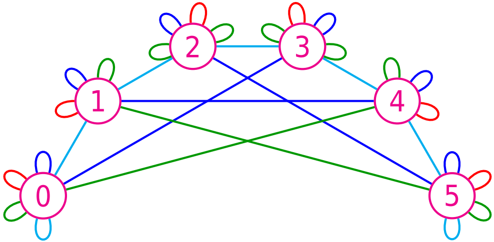


[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Cut-graph $\Gamma' = \text{Cut}[\Gamma, V']$:

- ▷ Choose vertices $V' \subseteq V$
- ▷ Cut the rest
- ▶ Turn cut edges into petals

$$E_{V'}(v, \ell) = \begin{cases} E(v, \ell) & \text{if } E(v, \ell) \in V' \\ v & \text{otherwise} \end{cases}$$

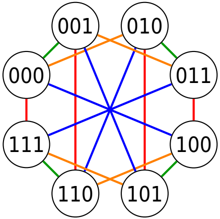


[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Definition RIM isomorphism

A bijection $\varphi : V' \to V''$ is an **isomorphism** $\Gamma' \to \Gamma''$ if

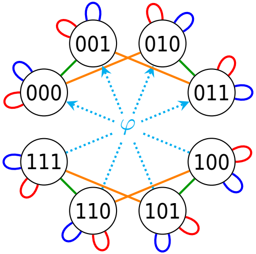
$$\forall (v', \ell) \in V' \times [n], \quad \varphi(E'(v', \ell)) = E''(\varphi(v'), \ell).$$



Definition Flowering cut

With $V'' = V \setminus V'$, if Cut$[\Gamma, V'] \sim$ Cut$[\Gamma, V'']$, the cut is **flowering**.

The cut-word Cut$[f, V']$ is the restriction $f_{|V' \times [n]}$.

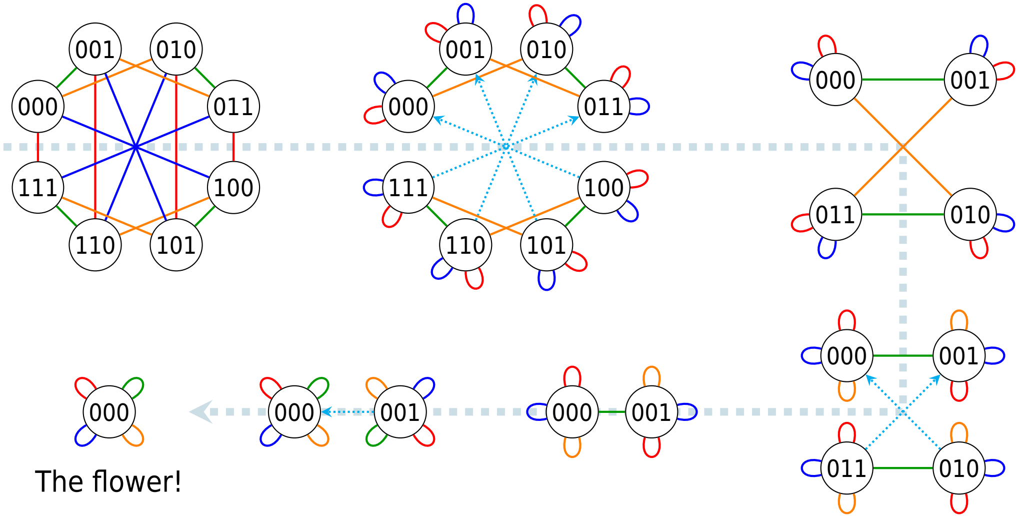


Definition Folding

For $\alpha \in \mathbb{F}$, $(v', \ell) \in V' \times [n]$,

$$\text{Fold}[f, \alpha](v', \ell) := \text{Cut}[f, V'](v', \ell) + \alpha \text{Cut}[f, V''](\varphi^{-1}(v'), \ell).$$

[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work


001
010
000
011
111
100
110
101
001
010
000
011
111
100
110
101
000
001
011
010
000
001
011
010
000
001
000
001
000

The flower!

$f_0 : V_0 \times [n] \to \mathbb{F}$

$\mathcal{P}$ $\mathcal{V}$

$\alpha_0 \xleftarrow{\$} \mathbb{F}$

$f_1 : V_1 \times [n] \to \mathbb{F}$

$f_1 = \mathsf{Fold}[f_0, \alpha_0]$

$\vdots$

$\alpha_{r-1} \xleftarrow{\$} \mathbb{F}$

$f_r : V_r \times [n] \to \mathbb{F}$

$f_r = \mathsf{Fold}[f_{r-1}, \alpha_{r-1}]$

1 commit phase

$v_0 \xleftarrow{\$} V_0, \ v_1 := \pi_1(v_0)$

$f_1(v_1) \stackrel{?}{=} \mathsf{Fold}[f_0, \alpha_0](v_1)$

$\vdots$

$v_r := \pi_r(v_{r-1})$

$f_r(v_r) \stackrel{?}{=} \mathsf{Fold}[f_{r-1}, \alpha_{r-1}](v_r)$

$f_r \stackrel{?}{\in} \mathsf{RS}[n, k]$

repeat m times

2 query phase

[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Let $C = \mathsf{RS}[N, K]$ or $\mathcal{C}[\Gamma, \mathsf{RS}[n, k]]$.

Proposition **FRI & Flowering complexities [BBHR18, DMR25]**

FRI and **Flowering** with m repetitions have complexities:

Protocol	FRI	Flowering
Prover	$< 8N$	$< 3N$
Verifier	$< 2m \log K$	$< 4m \log^2 N$
Query	$2m \log K$	$< 2m \log^2 N$
Round	$\log K$	$< \log N$

[BBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Fast Reed-Solomon Interactive Oracle Proofs of Proximity. **In *45th international colloquium on automata, languages, and programming (ICALP 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018**

[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025. **This work**

Let $C = \mathsf{RS}[N, K]$ or $\mathcal{C}[\Gamma, \mathsf{RS}[n, k]]$.

Theorem **FRI & Flowering completeness and soundness [BCI+23, DMR25]**

- **Completeness:** If $f \in C$ then $\mathcal{V}$ accepts with probability 1.
- **Soundness:** If $\Delta(f, C) > \delta$ then for any $\mathcal{P}$, $\mathcal{V}$ accepts with probability

$$\leqslant \frac{10^7 N^{3.5} \log K}{K^{1.5} |\mathbb{F}|} + \left(1 - \min\left(\delta, 1 - 1.05\sqrt{K/N}\right)\right)^m \qquad \textbf{(FRI)}$$

$$\leqslant \frac{N \log N}{|\mathbb{F}|} + (1 - \delta + \log N/N)^m . \qquad \textbf{(Flowering)}$$

[BCI+23] Eli Ben-Sasson, Dan Carmon, Yuval Ishai, Swastik Kopparty, and Shubhangi Saraf. Proximity Gaps for Reed–Solomon Codes. ***J. ACM*, 70(5), October 2023**

[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025. **This work**

Cayley graphs

Definition **Cayley graph Cay(G, S)**

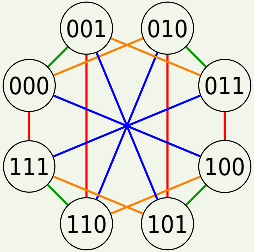
Fix $(G, \cdot)$. Let $S \subseteq G$ symmetric generating. Define $\Gamma = (G, E)$ where $E(g, s) = g{\cdot}s$.

We take

- $G = (\mathbb{F}_2^r, +)$
- $S \subseteq G$ of size n
- $\Gamma = \text{Cay}[G, S]$
- $C = \mathcal{C}[\Gamma, \text{RS}[n, k]]$

Example

With $G = (\mathbb{F}_2^3, +)$ and $S = \{100, 010, 001, 111\}$,



[Cay78] Arthur Cayley. Desiderata and Suggestions: No. 2. The Theory of Groups: Graphical Representation. ***American Journal of Mathematics***, **1(2):174–176, 1878**

Using S the columns of a parity check matrix of a $[n, n-r, d]_2$ binary code

Proposition **Parameters of the code**

- $N = n2^{r-1}$
- $\mathrm{rate}\, C \geqslant \frac{2k}{n} - 1$
- $\frac{1}{2}\delta \leqslant \Delta(C) \leqslant \delta$, with $\delta = \mathbf{2^{d-r-1}} \left(1 - \frac{k-1}{n}\right)$

If $d \ll r$ (i.e. far from MDS), δ is **terrible** ($O(1/N)$).

[DMR25] Hugo Delavenne, Tanguy Medevielle, and Élina Roussel. Interactive Oracle Proofs of Proximity to Codes on Graphs, 2025.
This work

Competing parameters with FRI

- Better soundness
- Complexity to improve
- No field restriction

New cuts, new graphs (work in progress)

- 2 disjoint cuts V', V'' $\rightarrow$ m covering cuts $V_1, V_2, ..., V_m$
- Flowering any Cayley graph $\rightarrow$ expander codes, constant minimal distance

Thank you!