Proof simultaneous verification using interleaved Reed-Solomon codes

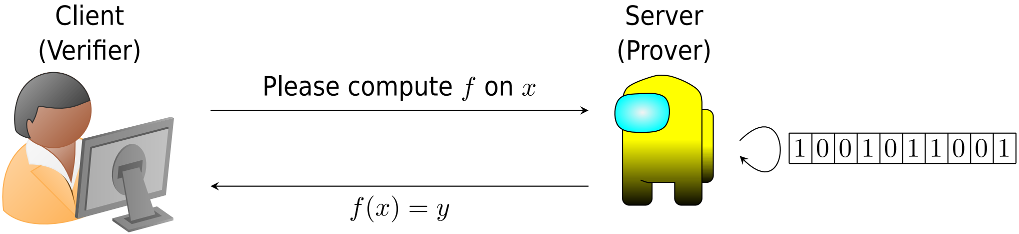
Hugo Delavenne

Grace – Groupe de travail

20 September 2022

Summary

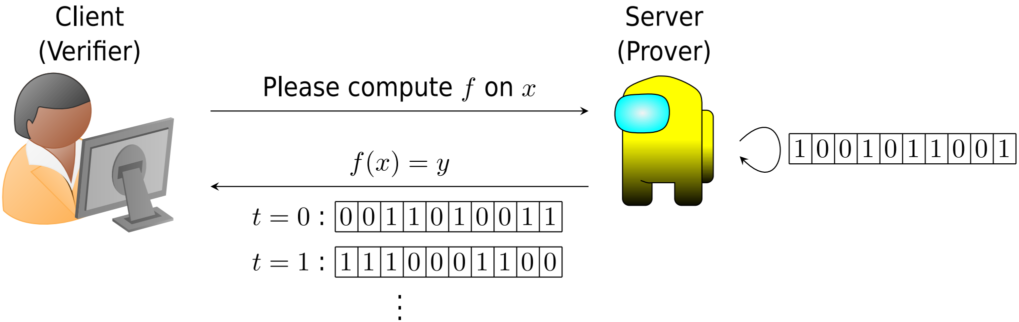
Introduction



Question

How can the client check that the server gives the correct answer?

The client checks the execution trace!



But naively checking the whole computation is as hard as computing.

Definition $\mathbf{PCP}$ **(Probabilistically Checkable Proof)**

$\mathcal{L} \subseteq \Sigma^*$ is in $\mathbf{PCP}[r(n), q(n)]$ if $\exists$ polynomial time V using $r(n)$ random bits and reading $q(n)$ bits of the proof, such that

- Perfect completeness: $\forall x \in \mathcal{L}, \exists \pi$ proof, $\mathbb{P}\big(V(x,\pi)$ accepts$\big) = 1$
- Soundness: $\exists s < 1/2, \forall x \notin \mathcal{L}, \forall \pi$ proof, $\mathbb{P}\big(V(x,\pi)$ accepts$\big) < s$.

- [BFLS91]: $\mathbf{PCP}[O(\log(n)), O(1)] = \mathbf{NP}$
- [BS08]: quasilinear-size PCP proofs

Definition IOP (Interactive Oracle Proof) [BCS16]

$\mathcal{L} \subseteq \Sigma^*$ is in $\mathbf{IOP}$ if $\exists$ polynomial time V interacting with a prover, such that

- Perfect completeness: $\forall x \in \mathcal{L}, \exists P$ prover, $\mathbb{P}\big(V(x, P(x))$ accepts$\big) = 1$
- Soundness: $\exists s < 1/2, \forall x \notin \mathcal{L}, \forall P$ prover, $\mathbb{P}\big(V(x, P(x))$ accepts$\big) < s$.

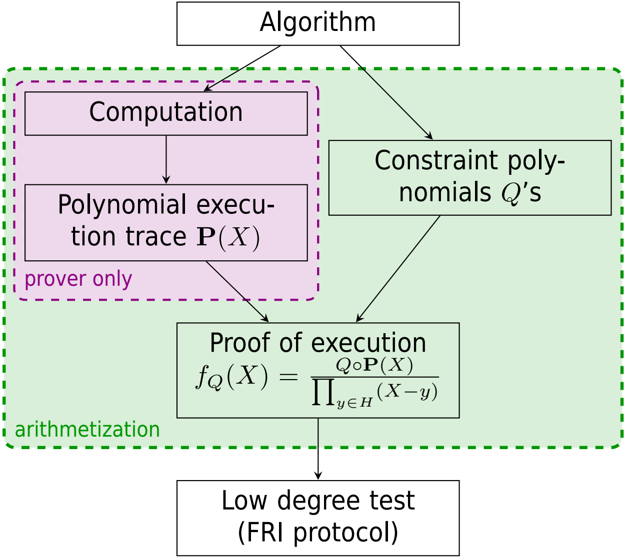
Theorem [BCS16]

$\mathbf{IOP} = \mathbf{NEXP}$

Without oracle, $\mathbf{IP} = \mathbf{PSPACE}$.

STARK protocols

- Arithmetization
- Reed-Solomon codes
- FRI protocol
- Proof of soundness



- $H = \langle g \rangle \subseteq \mathbb{F}^*$ of size $T + 1$
- R registers $r_i : H \to \mathbb{F}$
- $P_i(X) \in \mathbb{F}[X]$ interpolates r_i on H
- several transition constraints $Q(X_1, ..., X_R, Y_1, ..., Y_R)$
- $Q \circ \mathbf{P} := Q(\mathbf{P}(X), \mathbf{P}(gX))$ cancels on H iff valid computation

Consider $\begin{cases} f_0 = f_1 = 1 \\ f_{i+2} = f_{i+1}^2 + f_i^2 \mod 96769. \end{cases}$

There are 2 registers f_i and $g_i = f_{i-1}$ satisfying

$$f_{i+1} - f_i^2 - g_i^2 = 0 \qquad g_{i+1} - f_i = 0,$$

so the constraint polynomials are

$$Q_1(X_1, X_2, Y_1, Y_2) = Y_1 - X_1^2 - X_2^2 \qquad Q_2(X_1, X_2, Y_1, Y_2) = Y_2 - X_1.$$

Definition — **Reed-Solomon codes**

Given $\mathcal{D} \subseteq \mathbb{F}$ and $k < |\mathcal{D}|$,

$$\mathrm{RS}[\mathbb{F}, \mathcal{D}, k] := \{f : \mathcal{D} \to \mathbb{F} \mid \exists P(X) \in \mathbb{F}[X]_{<k}, P_{|\mathcal{D}} = f\}.$$

H	$\mathcal{D}$
execution trace ($\lvert H\rvert = k$)	codeword

Definition — **Hamming distance**

With $u, v \in \mathbb{F}^n$,

$$\Delta(u, v) := \frac{\#\{i \in [\![1, n]\!], u_i \neq v_i\}}{n}.$$

Lemma **Gap promise**

With $f(x) := \dfrac{Q \circ \mathbf{P}(x)}{\prod_{y \in H}(x-y)}$ a proof of execution,

- if $\prod_{y \in H}(X-y)$ divides $Q \circ \mathbf{P}(X)$ then $f \in \mathsf{RS}[\mathbb{F}, \mathcal{D}, k]$
- otherwise, $\Delta(f, \mathsf{RS}[\mathbb{F}, \mathcal{D}, k]) \geqslant 1 - \dfrac{k}{|\mathcal{D}|} \max(\deg Q, 2)$.

Consider the even and odd parts $f_0(Y) + X f_1(Y) = f(X)$ with $Y = X^2$.

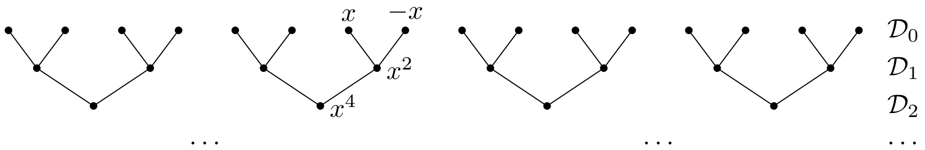
We check simultaneously the degree of a random folding.

Notation **Folding**

For $\alpha \in \mathbb{F}$ and $f : \mathcal{D} \to \mathbb{F}$, with f_0, f_1 even and odd parts of f,

$$\textbf{Fold}[f, \alpha] := f_0 + \alpha f_1.$$

- **Fold**$[f, \alpha] : \mathcal{D}' \to \mathbb{F}$ where $\mathcal{D}' = \{x^2 \mid x \in \mathcal{D}\}$.



- If $f \in \mathsf{RS}[\mathbb{F}, \mathcal{D}, k]$ then **Fold**$[f, \alpha] \in \mathsf{RS}[\mathbb{F}, \mathcal{D}', k/2]$.
- **Fold**$[f, \alpha](x^2) = \frac{f(x)+f(-x)}{2} + \alpha \frac{f(x)-f(-x)}{2x}$.

commit

Prover		Verifier
	α_0	$\alpha_0 \xleftarrow{\$} \mathbb{F}$
$f_1 : \mathcal{D}_1 \to \mathbb{F}$ $(f_1 = \textbf{Fold}[f_0, \alpha_0])$	f_1	
$\vdots$	$\vdots$	$\vdots$
	α_{r-1}	$\alpha_{r-1} \xleftarrow{\$} \mathbb{F}$
$f_r : \mathcal{D}_r \to \mathbb{F}$ $(f_r = \textbf{Fold}[f_{r-1}, \alpha_{r-1}])$	f_r	

query

Verifier chooses $s_0 \xleftarrow{\$} \mathcal{D}_0$, defines $s_{i+1} := s_i^2$ and accepts if

$$f_1(s_1) = \textbf{Fold}[f_0, \alpha_0](s_1)$$

$$\vdots$$

$$f_r(s_r) = \textbf{Fold}[f_{r-1}, \alpha_{r-1}](s_r).$$

m times

Theorem **Properties of FRI [Bor22]**

The FRI protocol on RS$[\mathbb{F}, \mathcal{D}, k]$ with m query phases has properties

- round complexity $\log k$
- proof length $< |\mathcal{D}|$
- query complexity $2m \log k + 1$
- prover complexity $< 8|\mathcal{D}|$
- verifier complexity $< 8m \log k$

Let $V_i := \mathrm{RS}[\mathbb{F}, \mathcal{D}_i, k/2^i]$.

$$\mathbb{P}(V \text{ accepts}) \leqslant \mathbb{P}\,(\text{gap reduction}) + \mathbb{P}\left(V \text{ accepts} \,\middle|\, \overline{\text{gap reduction}}\right)$$

Theorem — **Gap reduction probability [BKS18]**

Let $f_i : \mathcal{D}_i \to \mathbb{F}$ be an arbitrary function. Let $\varepsilon > 0$ and $\delta = \Delta(f_i, V_i)$.
Suppose $\delta \leqslant \delta_{\max}$. Then

$$\mathbb{P}_{\alpha \in \mathbb{F}}\left(\Delta\left(\textbf{Fold}[f_i, \alpha], V_{i+1}\right) \leqslant \delta - \varepsilon\right) \leqslant \frac{2}{\varepsilon^3 |\mathbb{F}|}.$$

Proposition — **Query soundness [BKS18]**

Let $\varepsilon > 0$ and $\delta := \Delta(f_0, V_0) > 0$. Suppose $\delta \leqslant \delta_{\max}$. Then

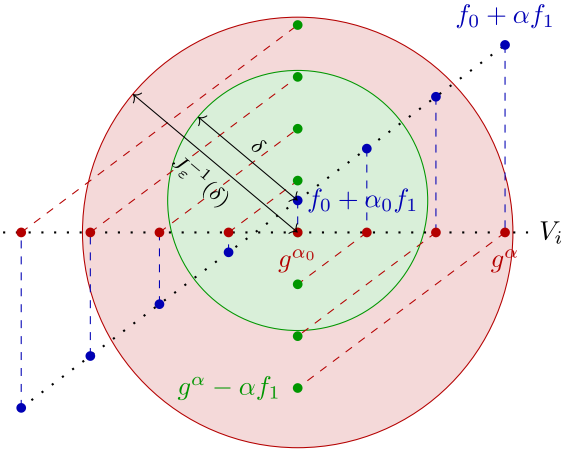
$$\mathbb{P}\left(V \text{ accepts} \,|\, \forall i, \Delta(\textbf{Fold}[f_i, \alpha], V_{i+1}) > \delta - \varepsilon\right) \leqslant \left(1 - \delta + \varepsilon \log k\right)^m.$$

Definition **List-decodability**

$S \subseteq \mathbb{F}^n$ is (μ, δ)-list-decodable if $\forall u \in \mathbb{F}^n, |B(u, \delta) \cap S| \leqslant \mu$.

Theorem **Johnson bound**

Let $J_\varepsilon(\delta) := 1 - \sqrt{1 - \delta(1 - \varepsilon)}$. Then $S \subseteq \mathbb{F}^n$ is $\left(\frac{1}{\varepsilon}, J_\varepsilon(\Delta(S))\right)$-list-decodable.



Let $A := \{\alpha \in \mathbb{F} \mid (\Delta\left(f_0 + \alpha f_1, V_{i+1}\right) \leqslant \delta - \varepsilon)\}$
Suppose $|A| > \frac{2}{\varepsilon^3}$.

$\rightarrow g_0, g_1 \in V_i$ s.t. $g_{0|T} = f_{0|T}$, $g_{0|T} = f_{0|T}$.

- $\rightarrow \alpha_0 \in \mathbb{F}, B \subseteq A$ such that $\forall \alpha \in B, \Delta(g^\alpha - \alpha f_1, g^{\alpha_0} - \alpha_0 f_1) < J_\varepsilon^{-1}(\delta)$.
- $\rightarrow g_1 \in V_i, C \subseteq B$ such that $\forall \alpha \in C, g_1 = \frac{1}{\alpha - \alpha_0}(g^\alpha - g^{\alpha_0})$.
- $\rightarrow g_0$, $\forall \alpha \in C, g_0 + \alpha g_1$ closest to $f_0 + \alpha f_1$.
- $\rightarrow |T| \geqslant (1-\delta)|\mathcal{D}|$...

Twice Johnson bound so $\delta \leqslant \delta_{\max} := J_\varepsilon(J_\varepsilon(\Delta(V_i)))$.

Using Interleaved Reed-Solomon codes

- Definition and properties
- Attempt with the FRI protocol
- DEEP-FRI protocol

Definition **Interleaved error-correcting code**

For $C \subseteq \mathbb{F}^n$, the ℓ-interleaved code associated is

$$\left\{ \begin{pmatrix} u_1 \\ \vdots \\ u_\ell \end{pmatrix} \middle| u_1, \ldots, u_\ell \in C \right\} \subseteq \mathbb{F}^{\ell \times n}.$$

The distance used is the same distance, but over $\mathbb{F}^\ell$.

Notation **Interleaved Reed-Solomon code**

IRS$[\mathbb{F}, \mathcal{D}, k, \ell]$ is the ℓ-interleaved code on RS$[\mathbb{F}, \mathcal{D}, k]$.

Definition **Probabilistic list-decoding**

Given $E \subseteq \mathcal{P}(\mathbb{F}^n)$, $S \subseteq \mathbb{F}^n$ is (E, p)-probabilistically (μ, δ)-list-decodable if

$$\forall U \in E, \underset{u \in U}{\mathbb{P}}\left(|B(u, \delta) \cap S| \leqslant \mu\right) \geqslant p.$$

Deterministic list-decoding use $p = 1$ and $E = \{\{u\} \mid u \in \mathbb{F}^n\}$.

Proposition **Probabilistic decoding of an IRS [Zap20]**

With $U_v := B\left(v, \frac{\ell}{\ell+1}(\Delta(V))\right)$ and $E := \{U_v \mid v \in \mathrm{IRS}[\mathbb{F}, \mathcal{D}, k, \ell]\}$, $V := \mathrm{IRS}[\mathbb{F}, \mathcal{D}, k, \ell]$ is

$$\left(E, 1 - \frac{\ell}{\ell+1}\frac{|\mathcal{D}|-k}{|\mathbb{F}|}\right)\text{-probabilistically } \left(1, \frac{\ell}{\ell+1}(\Delta(V))\right)\text{-list-decodable.}$$

Lemma **Gap reduction probability generalization**

Let $f : \mathcal{D}_i \to \mathbb{F}$ be an arbitrary function.
Let $\mu \in \mathbb{N}$ and $\delta, \varepsilon, \gamma > 0$ such that $\delta = \Delta(f, V_i)$.
Let f_1 be the odd part of f. Suppose that

$$|B(f_1, \gamma) \cap V_i| \leqslant \mu \tag{1}$$

$$\delta \leqslant \delta_{\max} := J_\varepsilon(\gamma). \tag{2}$$

Then

$$\mathbb{P}_{x \in \mathbb{F}}(\Delta(\textbf{Fold}[f, x], V_{i+1}) < \delta - \varepsilon) \leqslant \frac{\mu}{\mathbb{F}}.$$

- (1) requires V_i to be (μ, γ)-list-decodable, by worst case scenario
- thus in (2), $\delta_{\max}$ can't be improved.

commit

Prover		Verifier
	$\dots$	
	$\xleftarrow{\quad z_i \quad}$	$z_i \xleftarrow{\$} \mathbb{F}$
$B_{i+1,z_i} : \mathbb{F} \to \mathbb{F}$ $(B_{i+1,z_i}(X) = \textbf{Fold}[f_i, X](z_i))$	$\xrightarrow{\quad B_{i+1,z_i} \quad}$	
	$\xleftarrow{\quad \alpha_i \quad}$	$\alpha_i \xleftarrow{\$} \mathbb{F}$
$f_{i+1} : \mathcal{D}_{i+1} \to \mathbb{F}$ $(f_{i+1}(X) = \frac{\textbf{Fold}[f_i,\alpha_i](X) - B_{i+1,z_i}(\alpha_i)}{X - z_i})$	$\xrightarrow{\quad f_{i+1} \quad}$	
	$\dots$	

Theorem **Gap reduction probability [BGKS20]**

Let $f_i : \mathcal{D}_i \to \mathbb{F}$ be an arbitrary function. Let $\varepsilon > 0$ and $\delta = \Delta(f, V_i)$. Suppose that V_i is $(\mu, \delta_{\max})$-list-decodable and $\delta \leqslant \delta_{\max}$. Then

$$\mathbb{P}(\text{gap reduction}) \leqslant \eta_{\mu,k,\varepsilon,\mathbb{F}} := 2\mu \cdot \left(\frac{k}{|\mathbb{F}|} + \varepsilon \right)^{1/3} + \frac{4}{\varepsilon^2 |\mathbb{F}|}.$$

Hypothesis $(\mu, p, \delta_{\max})$**-hypothesis**

IRS$[\mathbb{F}, \mathcal{D}, k, \ell]$ is (E, p)-probabilistically $(\mu, \delta_{\max})$-list-decodable, with

$$E := \left\{\{f_0 + \alpha \cdot f_1 \mid \alpha \in \mathbb{F}^\ell\} \mid f_0, f_1 \in \mathbb{F}^{\ell \times n}\right\}$$

Theorem **DEEP-FII soundness**

Let $f : \mathcal{D}_i \to \mathbb{F}$ be an arbitrary function. Let $p, \varepsilon > 0$ and $\delta = \Delta(f, V_i)$.
Suppose that the $(\mu, p, \delta_{\max})$-hypothesis is valid and $\delta \leqslant \delta_{\max}$. Then

$$\mathbb{P}(\text{gap reduction}) \leqslant p \cdot \eta_{\mu,k,\varepsilon,\mathbb{F}} + 1 - p.$$

Conclusion

- I have not improved the soundness with probabilistic list-decoding.
- The results to prove to do so are more clearly identified.
- Studying arithmetization may give other tracks of study.

Bibliography

- Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev.
Fast Reed-Solomon Interactive Oracle Proofs of Proximity.
In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, 45th International Colloquium on Automata, Languages, and Programming (ICALP 2018), volume 107 of Leibniz International Proceedings in Informatics (LIPIcs), pages 14:1–14:17, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

- Eli Ben-Sasson, Dan Carmon, Yuval Ishai, Swastik Kopparty, and Shubhangi Saraf.
Proximity Gaps for Reed–Solomon Codes.
In 2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS), pages 900–909, 2020.

- Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner.
Interactive oracle proofs.
In Martin Hirt and Adam Smith, editors, Theory of Cryptography, pages 31–60, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

- László Babai, Lance Fortnow, Leonid A Levin, and Mario Szegedy.
Checking computations in polylogarithmic time.
In Proceedings of the twenty-third annual ACM symposium on Theory of computing, pages 21–32, 1991.

- Eli Ben-Sasson, Lior Goldberg, Swastik Kopparty, and Shubhangi Saraf.
DEEP-FRI: sampling outside the box improves soundness.
151:5:1–5:32, 2020.
https://eprint.iacr.org/2019/336.

- Eli Ben-Sasson, Swastik Kopparty, and Shubhangi Saraf.
Worst-Case to Average Case Reductions for the Distance to a Code.
In Rocco A. Servedio, editor, 33rd Computational Complexity Conference (CCC 2018), volume 102 of Leibniz International Proceedings in Informatics (LIPIcs), pages 24:1–24:23, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

- Eli Ben-Sasson and Madhu Sudan.
Short PCPs with Polylog Query Complexity.
SIAM Journal on Computing, 38(2):551–607, 2008.

- Ilaria Zappatore.
Primitivity of generalized translation based block ciphers.
PhD thesis, 2020.