Notes on FRI

arnaucube

February 2023

Abstract

Notes taken from Vincenzo Iovino explainations and while reading about FRI [1], [2].

Usually while reading papers I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1 Preliminaries

1.1 Low degree testing

V wants to ensure that $deg(f(x)) \leq d$.

We are in the IOP setting, V asks on a point, P sends back the opening at that point.

TODO

1.1.1 General degree d test

Query at points $\{x_i\}_0^{d+1}$, z (with rand $z \overset{R}{\in} \mathbb{F}$). Interpolate $p(x)$ at $\{f(x_i)\}_0^{d+1}$ to reconstruct the unique polynomial p of degree d such that $p(x_i) = f(x_i)\ \forall i = 1, \ldots, d+1$.

V checks $p(z) = f(z)$, if the check passes, then V is convinced with high probability.

This needs $d + 2$ queries, is linear, $\mathcal{O}(n)$. With FRI we will have the test in $\mathcal{O}(\log d)$.

2 FRI protocol

Allows to test if a function f is a poly of degree $\leq d$ in $\mathcal{O}(\log d)$.

Note: "P *sends* $f(x)$ to V", "*sends*", in the ideal IOP model means that all the table of $f(x)$ is sent, in practice is sent a commitment to $f(x)$.

2.1 Intuition

V wants to check that two functions $g,\ h$ are both polynomials of degree $\leq d$.

Consider the following protocol:

1. V sends $\alpha \in \mathbb{F}$ to P. P sends $f(x) = g(x) + \alpha h(x)$ to V.
2. P sends $f(x) = g(x) + \alpha h(x)$ to V.
3. V queries $f(r),\ g(r),\ h(r)$ for rand $r \in \mathbb{F}$.
4. V checks $f(r) = g(r) + \alpha h(r)$. (Schwartz-Zippel lema). If holds, V can be certain that $f(x) = g(x) + \alpha h(x)$.
5. P proves that $deg(f) \leq d$.
6. If V is convinced that $deg(f) \leq d$, V belives that both g, h have $deg \leq d$.

With high probablility, α will not cancel the coeffs with $deg \geq d + 1$.

Let $g(x) = a \cdot x^{d+1},\ \ h(x) = b \cdot x^{d+1}$, and set $f(x) = g(x) + \alpha h(x)$. Imagine that P can chose α such that $ax^{d+1} + \alpha \cdot bx^{d+1} = 0$, then, in $f(x)$ the coefficients of degree $d + 1$ would cancel.

Here, P proves $g,\ h$ both have $deg \leq d$, but instead of doing $2 \cdot (d+2)$ queries ($d + 2$ for g, and $d + 2$ for h), it is done in $d + 2$ queries (for f). So we halved the number of queries.

2.2 FRI

Both P and V have oracle access to function f.

V wants to test if f is polynomial with $deg(f) \leq d$.

Let $f_0(x) = f(x)$.

Each polynomial $f(x)$ of degree that is a power of 2, can be written as

$$f(x) = f^L(x^2) + xf^R(x^2)$$

for some polynomials $f^L,\ f^R$ of degree $\frac{deg(f)}{2}$, each one containing the even and odd degree coefficients as follows:

$$f^L(x) = \sum_{0}^{\frac{d+1}{2}-1} c_{2i}x^i, \quad f^R(x) = \sum_{0}^{\frac{d+1}{2}-1} c_{2i+1}x^i$$

eg. for $f(x) = x^4 + x^3 + x^2 + x + 1$,

$$\left.\begin{array}{l} f^L(x) = x^2 + x + 1 \\ f^R(x) = x + 1 \end{array}\right\} \ f(x) = f^L(x^2) + x \cdot f^R(x^2)$$
$$= (x^2)^2 + (x^2) + 1 + x \cdot ((x^2) + 1)$$
$$= x^4 + x^2 + 1 + x^3 + x$$

1. V sends to P some $\alpha_0 \in \mathbb{F}$. Let
$$f_0(x) = f_0^L(x^2) + x f_0^R(x^2) \qquad (A_0)$$
2. P sends
$$f_1(x) = f_0^L(x) + \alpha_0 f_0^R(x) \qquad (B_0)$$
to V.
(remember that "sends" in IOP model is that P commits to it)
3. V sends to P some $\alpha_1 \in \mathbb{F}$. Let
$$f_1(x) = f_1^L(x^2) + x f_1^R(x^2) \qquad (A_1)$$
4. P sends
$$f_2(x) = f_1^L(x) + \alpha_1 f_1^R(x) \qquad (B_1)$$
to V.
5. Keep repeating the process, eg. let
$$f_2(x) = f_2^L(x^2) + x f_2^R(x^2) \qquad (A_2)$$
until $f_i^L,\ f_i^R$ are constant (degree 0 polynomials).
6. Once $f_i^L,\ f_i^R$ are constant, P sends them to V.

Notice that at each step, $deg(f_i)$ halves.

Query phase

1. V sends rand $z \in \mathbb{F}$ to P
2. P sends $\{f_i(z^{2^i}), f_i(-z^{2^i})\}$ to V.
   eg. $f_0(z),\ f_0(-z),\ f_1(z^2),\ f_1(-z^2),\ f_2(z^4),\ f_2(-z^4),\ f_3(z^8),\ f_3(-z^8),\ \ldots$
3. V checks $f_i(a) = f_i^L(a^2) + a f_i^R(a^2)$ for $a = \{z, -z\}$

$$\begin{pmatrix} 1 & z \\ 1 & -z \end{pmatrix} \begin{pmatrix} f_i^L(z^2) \\ f_i^R(z^2) \end{pmatrix} = \begin{pmatrix} f_i(z) \\ f_i(-z) \end{pmatrix}$$

The number of queries needed is $2 \cdot log(d)$.

3 FRI as polynomial commitment

[WIP. Unfinished document]

References

[1] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Fast reed-solomon interactive oracle proofs of proximity, 2018. `https://eccc.weizmann.ac.il/report/2017/134/`.

[2] Ulrich Haböck. A summary on the fri low degree test. Cryptology ePrint Archive, Paper 2022/1216, 2022. `https://eprint.iacr.org/2022/1216`.