FRISoundness

Bolton Bailey

August 14, 2024

Overview

This Lean Blueprint seeks to be a guide towards the development of a formal proof of Theorem 8.2/8.3 of "Proximity Gaps for Reed Solomon Codes" by Ben-Sasson et al.:

Lemma 0.0.1 (8.2). *Let $V^{(0)} = \mathrm{RS}[\mathbb{F}, \mathcal{D}^{(0)}, k^{(0)}]$ where $\mathcal{D}^{(0)}$ is a coset of a 2-smooth multiplicative group, and $k^{(0)} + 1$ is a power of 2; set $\rho = (k^{(0)} + 1)/|\mathcal{D}^{(0)}|$.*

Let $F \subseteq \mathbb{F}^{\mathcal{D}^{(0)}}$ be a space of functions as defined in Eq. (8.3) whose correlated agreement density with $V^{(0)}$ is at most α. For integer $m \geq 3$, let

$$\alpha^{(0)}(\rho, m) = \max\{\alpha, \sqrt{\rho}(1 + 1/2m)\}.$$

Assume the FRI protocol is used with r rounds, and let $l^{(i)} = |\mathcal{D}^{(i)}|/|\mathcal{D}^{(i+1)}|$ denote the ratio between prover messages (oracles) i and $i + 1$. Let ϵ_Q denote the probability that the verifier accepts a single FRI QUERY invocation. Then,

$$\Pr_{x_1,\ldots,x_t,z^{(0)},\ldots,z^{(r-1)}}[\epsilon_Q > \alpha^{(0)}(\rho, m)] \leq \epsilon_C,$$

where

$$\epsilon_C = \frac{(m + \frac{1}{2})^7 \cdot |\mathcal{D}^{(0)}|^2}{2\rho^{3/2}|\mathbb{F}|} + \frac{(2m + 1) \cdot (|\mathcal{D}^{(0)}| + 1)}{\sqrt{\rho}} \cdot \frac{\sum_{i=0}^{r-1} l^{(i)}}{|\mathbb{F}|}.$$

In words: For any interactive FRI prover P^*, the probability that the oracles $f^{(0)}, \ldots, f^{(r)}$ sent by P^* will pass a single invocation of the batched FRI QUERY test with probability greater than $\alpha^{(0)}(\rho, m)$, is smaller than ϵ_C. The probability is over the random variables $x_1, \ldots, x_t$ used to sample $f^{(0)}$ from F and over the random messages $z^{(0)}, \ldots, z^{(r-1)}$ sent by the verifier during the COMMIT phase.

Theorem 0.0.2 (8.3). *Let $f_0^{(0)}, \ldots, f_t^{(0)} : \mathcal{D}^{(0)} \to \mathbb{F}$ be a sequence of functions and let $V^{(0)} = \mathrm{RS}[\mathbb{F}, \mathcal{D}^{(0)}, k^{(0)}]$ where $\mathcal{D}^{(0)}$ is a coset of a 2-smooth group of size $n^{(0)} = |\mathcal{D}^{(0)}|$, and $\rho = \frac{k^{(0)}+1}{n^{(0)}}$ satisfies $\rho = 2^{-R}$ for positive integer R. Let $\alpha = \sqrt{\rho}(1 + 1/2m)$ for integer $m \geq 3$ and ϵ_C be as defined in Lemma 8.2.*

Assume the FRI protocol is used with r rounds. Let $l^{(i)} = |\mathcal{D}^{(i)}|/|\mathcal{D}^{(i+1)}|$ denote the ratio between prover messages (oracles) i and $i + 1$. Assume furthermore that s is the number of invocations of the FRI QUERY step.

Suppose there exists a batched FRI prover P^* that interacts with the batched FRI verifier and causes it to output "accept" with probability greater than

$$\epsilon_{\mathrm{FRI}} := \epsilon_C + \alpha^s = \frac{\left(m + \frac{1}{2}\right)^7 \cdot |\mathcal{D}^{(0)}|^2}{2\rho^{3/2}|\mathbb{F}|} + \frac{(2m + 1) \cdot (|\mathcal{D}^{(0)}| + 1)}{\sqrt{\rho}} \cdot \frac{\sum_{i=0}^{r-1} l^{(i)}}{|\mathbb{F}|} + \left(\sqrt{\rho} \cdot \left(1 + \frac{1}{2m}\right)\right)^s.$$

Then $f_0^{(0)}, \dots, f_t^{(0)}$ *have correlated agreement with* $V^{(0)}$ *on a domain* $\mathcal{D}' \subset \mathcal{D}^{(0)}$ *of density at least* α.

I would like the blueprint to reflect the entire dependency tree of this theorem, including all the results from this paper and any critical results from other papers. Here is an intermediate result:

Theorem 0.0.3 (6.1)**.** *Suppose* $\delta \leq (1-\rho)/2$. *Let* $u_0, u_1, \dots, u_l : \mathcal{D} \to \mathbb{F}_q$ *be functions. Let*

$$S = \{z \in \mathbb{F}_q : \Delta(u_0 + zu_1 + \cdots + z^l u_l, V) \leq \delta\}$$

and suppose $|S| > l \cdot n$. *Then for all* $z \in \mathbb{F}_q$ *we have*

$$\Delta(u_0 + zu_1 + \cdots + z^l u_l, V) \leq \delta,$$

and furthermore there are $v_0, \dots, v_l \in V$ *such that for all* $z \in \mathbb{F}_q$,

$$\Delta(u_0 + zu_1 + \cdots + z^l u_l, v_0 + zv_1 + \cdots + z^l v_l) \leq \delta$$

and in fact

$$|\{x \in \mathcal{D} : (u_0(x), \dots, u_l(x)) \neq (v_0(x), \dots, v_l(x))\}| \leq \delta|\mathcal{D}|.$$