STIR : Shift To Improve Rate (Part 1)

rate $\Rightarrow$ proportion of true info contained in codeword

rate $\downarrow$ $\Rightarrow$ true infor. $\downarrow$ $\Rightarrow$ redundancy increases

$\Downarrow$

verifier's testing ability $\uparrow$

$\Downarrow$

verifier needs fewer queries to achieve target security

FRI v STIR

$L \subseteq F$ be the evaluation domain, $|L| = n$

$d \rightarrow$ degree bound (assume both $n = 2^k$, $d = 2^\ell$)

RS encoding space $RS[F, L, d]$ contains all functions $f: L \to F$ such that f is consistent with the evaluation of degree strictly less than $\underline{d}$ on L.

The rate $\rho = \dfrac{d}{|L|}$ ✓

Goal: Verifier can obtain a function $f: L \to F$ through queries. Verifier's goal is to query the values of $\underline{f}$ at as few locations as possible to distinguish which following cases f belongs to:

① $f \in RS[F, L, d]$

② f is δ-far from all codewords in $RS[F, L, d]$ in relative Hamming distance, i.e. $\Delta(f, RS[F, L, d]) > \delta$

FRI

$g_1 \in RS[F, L^k, d/k]$

$g_i \in RS[F, L^{k^i}, d/k^i]$

$\rho_i = \frac{d/k^i}{|L_i|} = \frac{d}{k^i} \cdot \frac{k^i}{n} = \frac{d}{n}$

$\rho_i = \rho$

STIR

$g_1' \in RS[F, L_1', d/k]$

$g_i' \in RS[F, L_i', d/k^i]$

$\rho_i = \frac{d/k^i}{|L_i'|} = \frac{d}{k^i} \cdot \frac{2^i}{n} = \left(\frac{2}{k}\right)^i \cdot \rho$

If $\frac{2}{k} < 1$ i.e. $k > 2$

$\Downarrow$

ρ_i decreases in each round

When compiling this IOPP into a SNARK, we use BCS transformation,

1. Merkle Commit the Prover's messages, and when the Verifier wants to query, open these commitments.
   Transforming IOPP into a succinct interactive argument.
2. Use Fiat-Shamir Transform to convert the succinct interactive argument of first step into non-interactive one.

Now, in BCS transformation, IOPP needs to have strong soundness called round-by-round soundness

$\downarrow$

requires IOPP to have a relatively small soundness error in each round

- let's assume the bound for round-by-round soundness error is $2^{-\lambda}$
- Each round can be queried t_i times repeatedly, and entire IOPP protocol goes through M rounds, so total query complexity of entire proof is

$$\sum_{i=0}^{M} t_i$$

For δ reaching the johnson bound, i.e. $\delta = 1 - \sqrt{\rho}$, we can calculate

① query complexity of FRI is:

$$O\left(\lambda \cdot \frac{\log d}{-\log \sqrt{\rho}}\right)$$

② query complexity of STIR is :

$$O\left(\lambda \cdot \log\left(\frac{\log d}{-\log \sqrt{\rho}}\right) + \log d\right)$$

Powerful Tools for RS-Encoding

Folding

$f: L \rightarrow F$, given $r \in F$, its k-fold function is

$$f_r := \text{Fold}(f, r) : L^k \rightarrow F$$

- it's defined as $\forall x \in L^k$, we can find k y in L satisfying $y^k = x$
- from k pairs $(y, f(y))$, we create polynomial $\hat{p}$ of degree less than k satisfying $\hat{p}(y) = f(y)$, then $\hat{p}(r)$ is the value of the function $f_r(x)$

This is consistent with FRI and has two good properties

↳ f before folding is $RS[F, L, d]$, then for random $r \in F$

$f_r \in RS[F, L^k, d/k]$

↳ for $\delta \in [0, 1-\sqrt{\rho})$, f is δ-far from $RS[F, L, d]$
$\Rightarrow$ f_r is δ-far from $RS[F, L^k, d/k]$ with prob. at least $1 - \text{poly}(|L|)/F$

How I understand $f_r(x)$

f_r is the rule "for any $x \in L^k$, take its k roots, interpolate a curve through the k points $(y, f(y))$, then evaluate that curve at $f_r(x)$"

Quotienting

$f: L \in F$ $\quad p: S \to F$ $\quad S \subseteq F$

$$\text{Quotient}(f, S, p)(x) := \frac{f(x) - \hat{p}(x)}{\prod_{a \in S}(X - a)}$$

p is the unique polynomial of degree less than $|S|$ satisfying

$$\hat{p}(a) = p(a) \quad \forall\, a \in S$$

We can see Consistency, Assuming S and L are disjoint, then

① if $f \in RS[F, L, d]$ is consistent with p on S, then
$\text{Quotient}(f, S, p) \in RS[F, L, d - |S|]$

② If for any $\hat{u}$ (deg $< d$) is δ-close to f, $\hat{u}$ is not consistent with p on S, then
$\text{Quotient}(f, S, p)$ is δ-far from $RS[F, L, d - |S|]$

Out of Domain Sampling

List decoding $\rightarrow$ unique decoding

for a function $f: L \rightarrow F$, Verifier randomly selects $\alpha \in F \setminus L$, and prover returns a value β.

Then in list of codewords $\text{List}(f, d, \delta)$ within δ range of f, with high probability, there is at most one codeword $\hat{u}$ satisfying

$$\hat{u}(\alpha) = \beta$$

Say $\hat{u}'$ and $\hat{u}$ are two different codewords with degree less than d, we have

$$\Pr_{\alpha \leftarrow F/L}\left[\hat{u}'(\alpha) = \hat{u}(\alpha)\right] \leq \frac{d-1}{|F| - |L|}$$

Suppose $RS[F, L, d]$ is (δ, ℓ) list-decodable, meaning there are at most ℓ codewords within δ range. $\Rightarrow \binom{\ell}{2}$ combinations

$\Rightarrow$ Total prob. for $\hat{u}'(\alpha) = \hat{u}(\alpha) \leq \binom{\ell}{2} \frac{d-1}{|F| - |L|}$

HOW TO CHECK $f(\alpha) = \beta$? $\rightarrow$ use Quotienting

One Iteration of the STIR protocol

Objective: • given a function f, we want to prove that it is in $RS[F, L, d]$, where $L = \langle \omega \rangle$

- After one iteration, prove that function $f' \in RS[F, L', d/k]$, $L' = \omega \cdot \langle \omega^2 \rangle$

i.e. $f^{\circledcirc}$ is k-folded $\Rightarrow$ degree $d \rightarrow d/k$
but domain L' of $f^{\circledcirc}$ f' is only reduced by 2 times

Say $\omega^8 = 1$

$L = \langle \omega \rangle$	ω^1	ω^2	ω^3	ω^4	ω^5	ω^6	ω^7	ω^8
$\langle \omega^2 \rangle$		ω^2		ω^4		ω^6		ω^8
$\omega \cdot \langle \omega^2 \rangle$	ω^1		ω^3		ω^5		ω^7	

Why do we choose $L' = \omega \cdot \langle \omega^2 \rangle$ as $\langle \omega^2 \rangle$ is also half the size?

suppose $k=4$ $\Rightarrow$ $L^4 = \{\omega^4, \omega^8\}$
$L' = \{\omega^1, \omega^3, \omega^5, \omega^7\}$

$\rightarrow L^4 \cap L' = \phi$

$\Downarrow$

we want to avoid FRI function which contains the intersect$^{\circledcirc}$ pts.