Basefold-02

X_0	X_1	X_2
0	0	0
1	0	0
0	1	0
1	1	0
0	0	1
1	0	1
0	1	1
1	1	1

$d = 3$ for our understanding

$$\Rightarrow \tilde{f}(X_0, X_1, \ldots, X_{d-1}) = \tilde{f}(X_0, X_1, X_2) = f_0 + f_1 X_0 + f_2 X_1 + f_3 X_0 X_1 + f_4 X_2 + f_5 X_0 X_2 + f_6 X_1 X_2 + f_7 X_0 X_1 X_2$$

- d unknowns $\Rightarrow$ length of coeff. vector $= 2^d$
- we use Lexicographic order of sorting

So, we encode coeff. vector f of $\tilde{f}(X)$

$\Downarrow$

codeword $C_f = \mathrm{Enc}(f)$, which has length $n_d = n_3$

$\Downarrow$

we use Hash-Based Merkle Tree to generate commitment

$\Downarrow$

$$\mathrm{cm}(f) = \mathrm{Merklize}\left(\mathrm{Enc}(f_0, f_1, \ldots, f_7)\right)$$

Similar to FRI, Basefold-IOPP is used to prove that a commitment

$$\pi_d = \mathrm{cm}(f)$$

is with high probability "close" to a vector encoded by C_d.

Proximity Gap

If two vectors π, π' are both far from any valid codeword, then random linear combination of them (like $\pi + \alpha \cdot \pi'$) is also far from a codeword — with very high probability.

$$\boxed{\Pr_{\alpha \in F}\left[\Delta(\pi + \alpha\pi', C_i) \le \delta\right] \le \epsilon << 1}$$

$\Downarrow$

"The probability over α chosen uniformly at random from the field F, that the dist. b/w $\pi + \alpha\pi'$ and the codeword C_i is less than or equal to δ, is at most ϵ, which is much less than 1."

Commit-Phase

$d = 3$ $\qquad$ $\pi_d \Rightarrow$ encoded coeff. vector with length n_d $\quad (\pi_3, n_3)$

$\Downarrow$

prover performs multiple folding

$\Downarrow$

(π_2, π_1, π_0) with length (n_2, n_1, n_0)

Since, it's interactive protocol with $d (= 3)$ rounds of interaction

→ for $0 \le i < d$; Prover folds π_{i+1} based on random scalar α_i sent by the verifier to obtain a new codeword π_i

$\Downarrow$ after d $(=3)$ rounds

Prover obtains a codeword of length n_0 denoted as π_0

$\Downarrow$

Prover commits to $(\pi_3, \pi_2, \pi_1, \pi_0)$

$\Downarrow$

Sends $cm(\pi_3)$, $cm(\pi_2)$, $cm(\pi_1)$, $cm(\pi_0)$ as o/p of IOPP. Commit

Now,

$$\Pi_{i+1} = (c_0, c_1, c_2, \dots, c_{n_{i+1}-1})$$

i from 2 → 0

here i = 2

⇓

$$\Pi_3 = (c_0, c_1, \dots, c_{n_3-1})$$

↓ we split it into

$$\left(c_0 \quad c_1 \quad \dots \quad c_{n_2-1} \;\middle\|\; c_{n_2}, c_{n_2+1}, \dots, c_{n_3-1} \right)$$

verifier provides a random scalar $\alpha^{(i)}$

⇓ we perform random linear combination of the two rows, or in other words

$$\Pi_2 = \left(\text{fold}_{\alpha_2}(c_0, c_{n_2}), \text{fold}_{\alpha_2}(c_1, c_{n_2+1}) \dots, \text{fold}_{\alpha_2}(c_{n_2-1}, c_{n_3-1}) \right)$$