General Structure 🫡

Commitment to $f(x)$ (degree ≤ 2^k)

- $\boxed{\text{Merkle-commitment to } f(\omega)_{\omega \in \Omega}}$
  - $\mathbb{F}_p \supset \Omega$ = [$2^{k\rho}$th roots of unity] (typically, $\rho \in \{2,4,8,16\}$)
- 🪄 + low degree proof “if I **fold** this polynomial in half k times, it’s degree 0”

Opening proof for $f(u) = v$

- Proof that $(x - u) \mid (f - v)$ by proving that $\deg((f(x) - v)/(x - u)) \leq 2^k - 1$

🪄 Folding

- Given polynomial f of degree d
- 🎯 Goal: split and fold into polynomial h of degree $d/2$.
- 🖖 Split: $f(x) = f_{\text{even}}(x^2) + x \cdot f_{\text{odd}}(x^2)$

$$f_0(x) = 19 + 56x + 34x^2 + 48x^3 + 43x^4 + 37x^5 + 10x^6 + 0x^7$$

We've turned one polynomial with 8 coefficients…

…into 2 polynomials with 4 coefficients.

$$= 19 + 34x^2 + 43x^4 + 10x^6 + 56x + 48x^3 + 37x^5 + 0x^7$$

$$f_{0,even}(x) = 19 + 34x + 43x^2 + 10x^3$$

$$f_{0,odd}(x) = 56 + 48x + 37x^2 + 0x^3$$

- 🪭 Fold: $h = f_{\text{even}} + r \cdot f_{\text{odd}}$ for random challenge r (from verifier/FS)

🤨 Checking the folding

- Prover Merkle-RS-commits to original polynomial f and to folded polynomial h
  - Merkle$((f(\omega))_{\omega\in\Omega})$ and Merkle$((h(\omega))_{\omega\in\Omega^2})$
    - $\Omega^2 =$ squared roots of unity (i.e. half)
- How to check $h = f_{\text{even}} + r \cdot f_{\text{odd}}$?
  - “Locally”, without looking at full polynomial.

To check $h(\omega^2)$
First, note:

$$2 \cdot f_{\text{even}}(\omega^2) = f(\omega) + f(-\omega)$$
$$2\omega \cdot f_{\text{odd}}(\omega^2) = f(\omega) - f(-\omega)$$

So from two queries to Merkle(f), can compute $f_{\text{even}}(\omega^2), f_{\text{odd}}(\omega^2)$

Then check

$$h(\omega^2) = f_{\text{even}}(\omega^2) + r \cdot f_{\text{odd}}(\omega^2)$$

Spot-checking a few ω^2 suffices (RS)