General Structure

Commitment to f(x) (degree $\leq 2^k$)

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

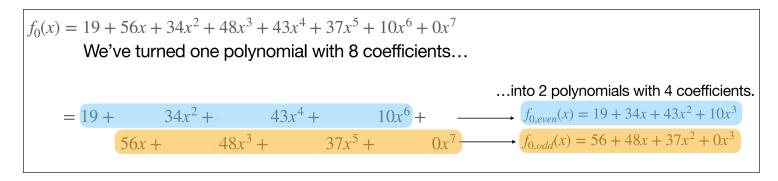
Opening proof for f(u) = v

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



- Given polynomial f of degree d
- If Goal: split and fold into polynomial h of degree d/2.

•
$$\checkmark$$
 Split: $f(x) = f_{\text{even}}(x^2) + x \cdot f_{\text{odd}}(x^2)$



• Fold: $h = f_{even} + r \cdot f_{odd}$ 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 $Merkle((h(\omega))_{\omega \in \Omega^2})$
 - Ω^2 = squared roots of unity (i.e. half)
- How to check $h = f_{even} + r \cdot f_{odd}$?
 - "Locally", without looking at full polynomial.

To check $h(\omega^2)$ First, note: $2 \cdot f_{even}(\omega^2) = f(\omega) + f(-\omega)$ $2\omega \cdot f_{odd}(\omega^2) = f(\omega) - f(-\omega)$

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

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)