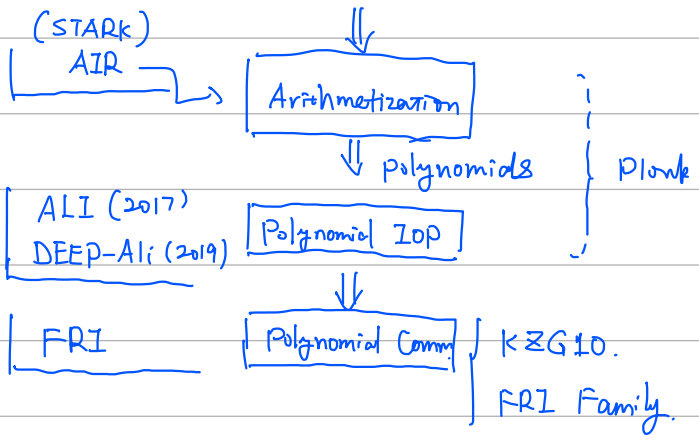
FRI Overview

1. Plonk & PCS.

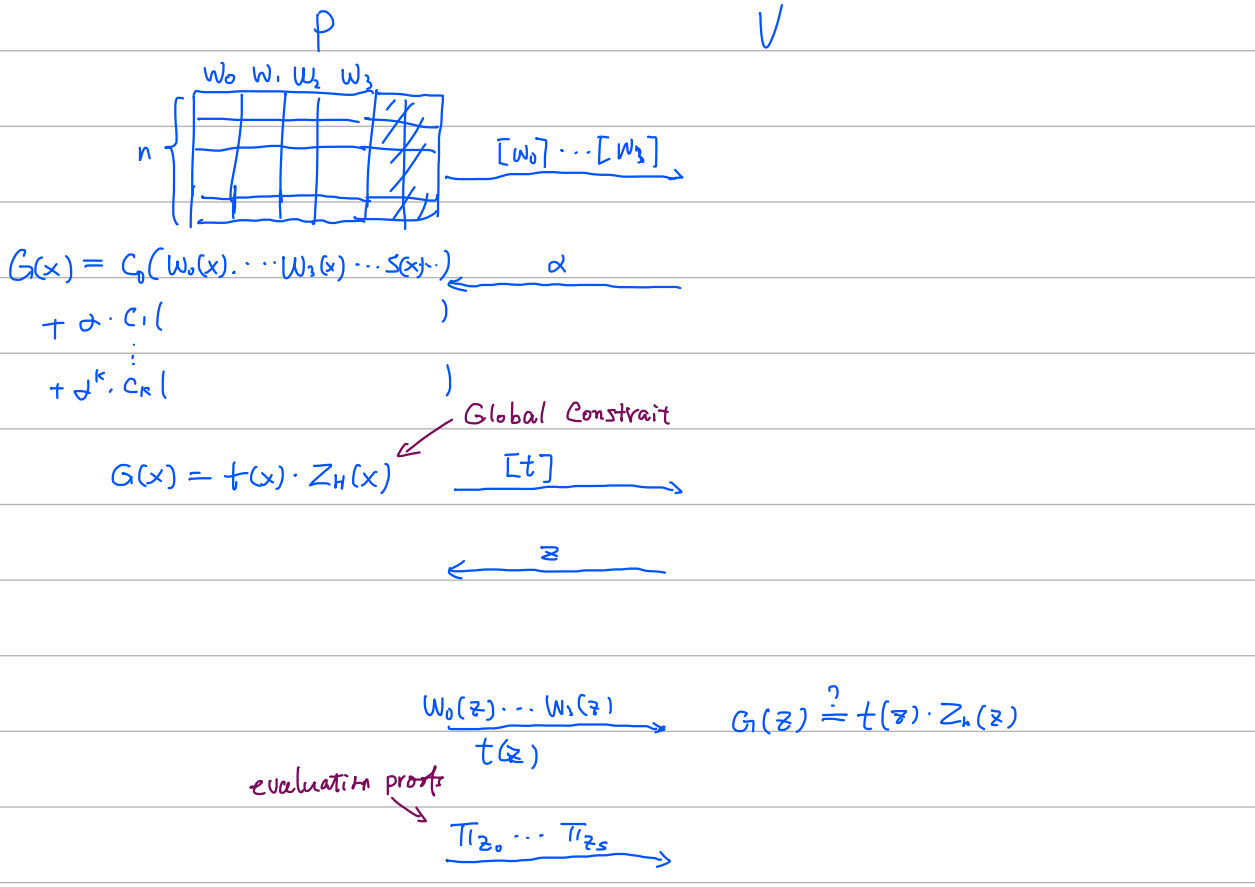
AIR vs. Plonkish

~~STARK vs. SNARK~~

FRI vs. KZG10.



#2. FRI as PCS (polynomial commitment scheme)



#3. KZG10 vs. FRI

FRI: Small Fields ($\mathbb{F}_p$: 64bit (or 32bit) ~ constraits.)

($\mathbb{K}$ (extension field) over $\mathbb{F}_p$. >128bit = ($\mathbb{F}_p \cdots \mathbb{F}_p$))

FRI : batching.

FRI : recursion-friendly. (hash-based commitment)

non-homomorphism. ~~[f] + [g]~~

#4. FRI protocol as PCS

evaluation proof : $f_i(z) = v_i$ $\quad i \in \{\cdots\}$

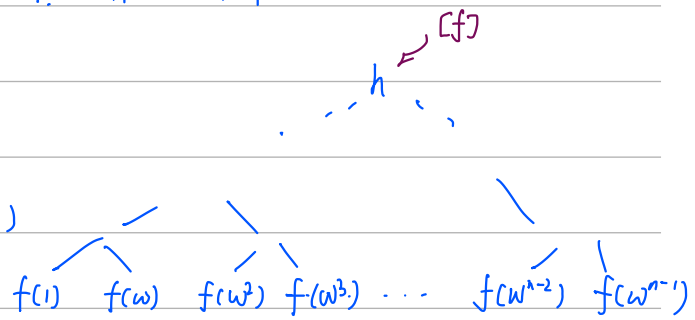
[f]: commitment. (merkle tree)

Domain $D \subset \mathbb{F}_p$. D is smooth multiplicative subgroup.

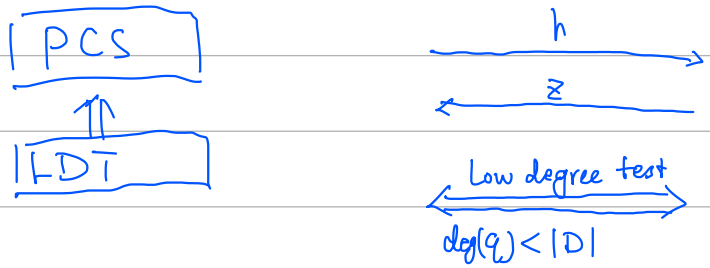
$D = \langle \omega \rangle = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$ $\quad n = 2^k$, for some k

$\bar{f} = \{f(x) \mid x \in D\}$.

$\begin{cases} z \in D. \times & z \in \mathbb{K} \setminus D \\ z \notin D. & z \in \mathbb{K} \quad (\text{DEEP Method}) \end{cases}$



P V

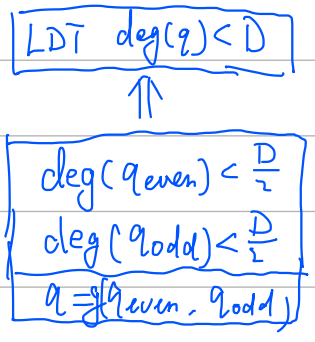


$\frac{f(x) - v}{x - z} = q(x)$

$\sum_i \lambda^i \frac{f_i(x) - v_i}{x - z} = q(x)$ (batched)

#5. Low degree test (FRI) ← FFT over finite fields

$$q(x) = c_0 + c_1 \cdot x + c_2 \cdot x^2 + \cdots + c_{n-1} \cdot x^{n-1}$$
$$= (c_0 + c_2 \cdot x^2 + \cdots + c_{n-2} \cdot x^{n-2}) + x \cdot (c_1 + c_3 \cdot x^2 + \cdots + c_{n-1} \cdot x^{n-2})$$
$$= q_{even}(x^2) + x \cdot q_{odd}(x^2)$$



✡ FRI - Commit phase (split and fold)

P V

β_0 ←

$q^{(1)}(x) = q_{even}(x) + \beta_0 \cdot q_{odd}(x)$

$[q^{(1)}]$ →

$\deg(q^{(1)}) < \frac{D}{2}$

β_1 ←

$[q^{(2)}]$ →

⋮

β_{k-1} ←

$q^{(k)}(x) = c'$

c' →

$c' \stackrel{?}{=}$ constant

✡ FRI - Query phase

$u_0\ u_1 \cdots u_s$ ←

open $([q], [q^{(1)}] \cdots [q^{(k)}])$ →

#6. Code Theory. (Reed-Solomon Code)

Enc Dec

↖ FFT (NTT) over FF.

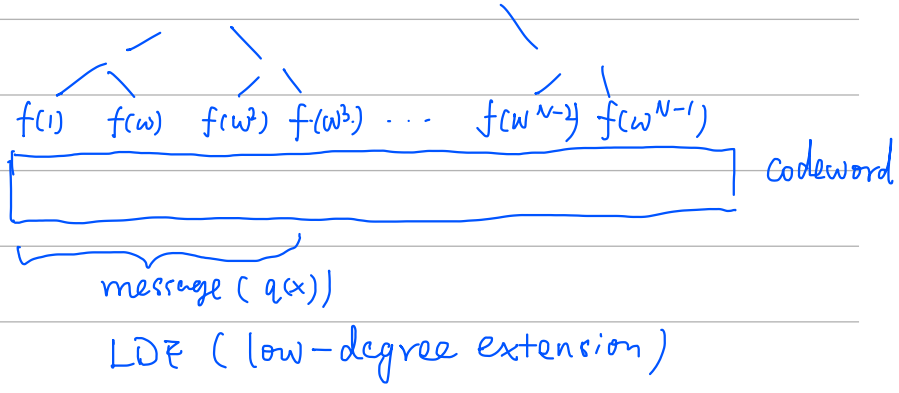
code-rate: $\rho < 1$, $\frac{\text{message}}{\text{codeword}}$

blowup factor = 8 ~ 32

$N = R \cdot n$, $n = \deg(q)$

$|L| = N$

coset $\gamma \cdot D$ ... h ... $[f]$



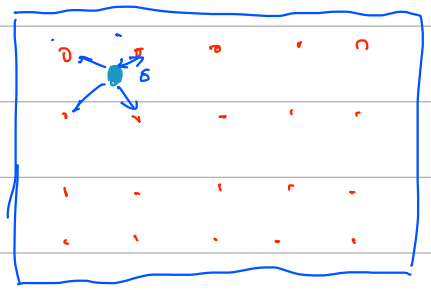
LDE (low-degree extension)

proximity (proof of proximity)

$\Delta(f, q) < \delta$. f is δ-closed to q

δ

list-decoding



#7. FRI History.

[BBHR18] : $\delta < \frac{1-3\rho}{4}$

[BKS18] : $\delta < 1-\sqrt[4]{\rho}$

[BGKS20] (Deep-fri) : $\delta < 1-\sqrt[3]{\rho}$

* [BCIKS20] : $\delta < 1-\sqrt{\rho}$ (Johnson bound) $\log n$ $\boxed{\delta < 1-\rho}$

[ACFY24] : (STIR) : $\delta < 1-\sqrt{\rho}$. query: $\log\log n$

#8. FRI Family.

{ Basefold , Fri-binius. (multivariate polynomials)
:

#9. 1. { Additive FRI (BBHR18) $D = \langle \beta_0 \cdots \beta_k \rangle$ over $\mathbb{F}_{2^m}$ $q: x \mapsto x\cdot(x+1)$ (subspace polynomial)
Multiplicative FRI ✓ * $D = \{1, \omega, \omega^2 \cdots \omega^{N-1}\}$, $q: x \mapsto x^2$

2. Code Theory Basics

3. Read the code !