Problem Statement

Consider a polynomial $f(x)$

over a finite-field $\mathbb{F}_q$

defined by its evaluations $f_i = f(\omega^i)$

, where ω

is the n

-th root of unity of $A(x) = x^n - 1 = 0$

. The Lagrange interpolation of $f(x)$

based on Barycentric formula is

$A'(x) = nx^{n-1}$

$$\begin{align} f(x) & = A(x)\sum_{i=0}^{n-1} \frac{f(\omega^i)}{A'(\omega^i)} \frac{1}{x - \omega^i} \\ & = \frac{x^n - 1}{n} \sum_{i=0}^{n-1} \frac{f_i }{\omega^{i(n-1)}(x - \omega^i)} \\ & = \frac{x^n - 1}{n} \sum_{i=0}^{n-1} \frac{f_i \omega^i}{x - \omega^i} \end{align}$$

Now given $m = 2^l \leq n$

, we want to check that the degree of $f(x)$

is less than m

. Note that for $m = \frac{n}{2}$

, Dankrad has proposed a check [here]

Low Degree Check

Suppose ω_i

's are the roots of unity ordered by reverse bit order. E.g., if $n = 8$

, then $[\omega_0, ..., \omega_7] = [\omega^0, \omega^4, \omega^2, \omega^6, \omega^1, \omega^5, \omega^3, \omega^7]$

. Further, let us define $y_i = f(\omega_i)$

, which is the reverse-bit ordered version of f_i

. Then, we define $\Omega = \{\omega_0, …, \omega_{m-1}\}$

, and the coset $H_i = h_i \Omega$

with $h_i = \omega^i$

. For each coset H_i

, we have

$B_i(x) = \prod_{x_i \in H_i} (x - x_i) = x^m-h_i^{m}$

$B_i'(x) = mx^{m-1}$

$$\begin{align} f_i(x)& =B_i(x)\sum_{j = i m}^{(i+1)m - 1} \frac{f(\omega_j)}{B'_i(\omega_j)}\frac{1}{x-\omega_j} \\ & = \frac{x^m - h_i^m}{m } \sum_{j=im}^{(i+1)m - 1} \frac{y_j}{\omega_j^{m-1}(x - \omega_j)} \\ & = \frac{x^m - h_i^m}{m h_i^m} \sum_{j=im}^{(i+1)m - 1} \frac{y_j \omega_j}{x - \omega_j} \end{align}$$

To check if $f(x)$

's degree is less than m

, we sample a random point r

and verify that

$$\begin{align} f_i(r) = f_j(r), \forall i,j \end{align}$$

(Equation (7))

Note that if $m = n/2$

, the check will be exactly the same as Dankrad's.

Proof and Code

See [Dankrad's Notes]() and https://github.com/ethereum/research/pull/138

Application to FRI Low Degree Check

The FRI (Fast Reed-Solomon Interactive Oracle Proofs of Proximity) aims to provide a proof of a close

low degree of a polynomial $f(x)$

given its evaluations f_i

over roots of unity ω^i

(see https://vitalikblog.w3eth.io/general/2017/11/22/starks_part_2.html and https://vitalikblog.w3eth.io/general/2018/07/21/starks_part_3.html). The basic idea is to re-interpret $f(x) = q(x, x^m)$

, where m

is a power of 2 (commonly use $m = 4$

) and $q(x, y)$

is a 2D polynomial, whose degree in x

is less than m

, and degree in y

is less than $\frac{deg(f(x))}{m}$

. If $deg(f(x))$

is less than N

, then $f'(y) = q(r, y)$

will have degree $< \frac{N}{m}$

, where r

is a random evaluation point. Therefore, we just need to verify the degree of $f'(y)$

, which can be further done recursively. To build $f'(y)$

, we have the following proposition:

Proposition

: Given reversed ordered n-th roots of unity ω_i

, $i = 0, …, n-1$

, and the evaluations $y_i = f(\omega_i)$

, the reversed ordered $\frac{n}{m}$

th roots of unity $\phi_i = \omega^{m}_{im}$

, $i = 0, …, \frac{n}{m}-1$

, and the evaluations of $y'_i = f'(\phi_i) = f_i(r)$

.

Proof

: It is trivial to prove $\phi_i = \omega^{m}_{im}$

. For y'_i

, we have

$y'_i = f'(\phi_i) = q(r, \omega^m_{im})$.

Note that for $q(x, y)$

, if y

is fixed, $r(x) = q(x, y)$

is a polynomial with degree $< m$

. Let $y = \omega^m_{im}$

, the roots of y

is $\omega_{im +j}, 0 \leq j < m$

, then we can find m

distinct evaluations of $r(x)$

at m

positions $\omega_{im +j}, 0 \leq j < m$

, with $r(\omega_{im+j}) = q(\omega_{im+j}, \omega^m_{im+j}) = f(\omega_{im+j}) = y_{im+j} = f_i(\omega_{im+j})$

. Since $deg(f_i(x)) < m$,

this means that given $y = \omega^m_{im}$

, $r(x) = f_i(x)$

, and thus we have

$q(r, \omega^m_{im}) =f_i(r)$.

Q.E.D.

A couple of interesting comments here:

- Using Barycentric formula, we could find the evaluations of $f'(y)$

in linear complexity without Lagrange interpolation in https://vitalikblog.w3eth.io/general/2018/07/21/starks_part_3.html whose complexity is $N \log(m)$

. The code for FRI can be found at [FRI uses barycentric formula to evaluate poly by qizhou · Pull Request #140 · ethereum/research · GitHub]()

- If $m = N$

, then the FRI low degree check is the same as the exact check in Eq. (7), where $f'(y)$

becomes a degree 0 polynomial.