Mersenne 31

Given $p = 2^{31} - 1$ and $\mathbb{F}_p$, construct the extensions

$$
\begin{aligned}
\mathbb{F}_{p^2} &= \mathbb{F}_p[\mathrm{i}]/(\mathrm{i}^2 + 1) \\
\mathbb{F}_{p^6} &= \mathbb{F}_{p^2}[\mathrm{j}]/(\mathrm{j}^3 - 5)
\end{aligned}
$$

Such that $\mathbb{F}_{p^6}$ has $\mathrm{i}^2 = -1$ and $\mathrm{j}^3 = 5$. We represent elements by the F_p coefficients in the basis $(1, \mathrm{i}, \mathrm{j}, \mathrm{i} \cdot \mathrm{j}, \mathrm{j}^2, \mathrm{i} \cdot \mathrm{j}^2)$.

TODO: An alternative not-cube is $j^3 = 2 + \mathrm{i}$, it's not immediately obvious which will lead to the most performant implementation, but at least the inner product embedding would become more dense.

Number Theoretic Transforms (NTTs)

In this tower we can do efficent NTTs since the multiplicative groups have small subgroups:

$$
\begin{aligned}
\left|\mathbb{F}_p^\times\right| &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331 \\
\left|\mathbb{F}_{p^2}^\times\right| &= 2^{32} \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331 \\
\left|\mathbb{F}_{p^6}^\times\right| &= 2^{32} \cdot 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 43^2 \cdot 79 \cdot 151 \cdot 331 \cdot 1381 \cdot 529510939 \cdot 1758566101 \cdot 2903110321
\end{aligned}
$$

In particular it has primitive 2^{32}-th roots of unity contained in the $\mathbb{F}_{p^2}$ subfield. The roots up to 8th order have low hamming weight structure:

$$
\begin{aligned}
\omega_8^0 &= 1 & \omega_8^1 &= 2^{15} \cdot (1 - \mathrm{i}) \\
\omega_8^2 &= -\mathrm{i} & \omega_8^3 &= -2^{15} \cdot (1 + \mathrm{i}) \\
\omega_8^4 &= -1 & \omega_8^5 &= -2^{15} \cdot (1 - \mathrm{i}) \\
\omega_8^6 &= \mathrm{i} & \omega_8^7 &= 2^{15} \cdot (1 + \mathrm{i})
\end{aligned}
$$

Embedding inner products

We are interested in computing inner products over $\mathbb{F}_p$, but for technical reasons we often need to work in $\mathbb{F}_{p^6}$ (the field needs to be large enough for cryptographic applications). The naive way of implementing $\mathbb{F}_p^n$ inner products in $\mathbb{F}_{p^6}$ results in n large field multiplications. We will construct an embedding of $\mathbb{F}_p^6$ inner products into $\mathbb{F}_{p^6}$ to reduce this to $\lceil \frac{n}{6} \rceil$ large field multiplications.

Applying Lemma 2 we find embedding matrices for the degree 2 and 3 extensions. Composing these using Lemma 3 we obtain an embedding for $\mathbb{F}_{p^6}$ in our chosen basis:

$$
\mathrm{B} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 5^{-1} & 0 \\
0 & 0 & 0 & 0 & 0 & -5^{-1} \\
0 & 0 & 5^{-1} & 0 & 0 & 0 \\
0 & 0 & 0 & -5^{-1} & 0 & 0
\end{pmatrix}
$$

Thus to compute the inner product of two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}_p^6$ we compute the $\mathbb{F}_{p^6}$ elements v, w. We compute v from the coefficient representation $\boldsymbol{v}$ and w from the coefficients $\mathrm{B} \cdot \boldsymbol{w}$. The inner product is then computed as the constant coefficient of $v \cdot w$. Because of linearity, this alows us to embed F_p^n inner products into an inner product over $\lceil \frac{n}{6} \rceil$ elements of $\mathbb{F}_{p^6}$.

Applying this to WHIR, we can commit to a $\lceil \frac{n}{6} \rceil$ sized witness vector in $\mathbb{F}_{p^6}$ and do opening proofs with weights in $\mathbb{F}_{p^6}$ to proof a witness-weight inner product over $\mathbb{F}_p^n$.

If we instead need to do an inner product between a witness in $\mathbb{F}_p^n$ and weights in $\mathbb{F}_{p^6}^n$ (which may be the case in an adaptation of GR1CS) then we can do this using 6 inner product over $\mathbb{F}_p^n$, which can be batched in the WHIR opening. (TODO: Is there a more efficient way to do this?)

TODO: Appropriate adaptation of GR1CS.

Equality function

Isomorphisms and representations of the vector space $\mathbb{F}^{2^k}$.

The boolean hypercube evaluation basis of size $n = 2^k$ is $\mathcal{B}_n = \{0,1\}^k$.

The an evaluation basis of size n is

The Fourier basis $\mathcal{F}_n = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ where ω is a primitive n-th root of unity.

Q: We have $\mathcal{B}_2 \neq \mathcal{L}_2$, but we could construct a $\mathcal{B}_2$ hypercube fine.

The basis functions for $\mathcal{B}_2$ are

$$x \cdot y + (x-1) \cdot (y-1)$$

The basis functions for $\mathcal{L}_n$ are

$$\frac{x^n - 1}{x - y}$$

Definition 1: Given a basis $\mathcal{B}$ for an $\mathbb{F}$ vector-space V define $\{\mathrm{eq}_{\boldsymbol{y}}\}_{\boldsymbol{y} \in \mathcal{B}}$ to be a basis of multivariate polynomial $\mathbb{F}[X^{\dim V}]$ where each $\mathrm{eq}_{\boldsymbol{y}}$ is a multivariate polynomial of minimal degree such that for all $\boldsymbol{x} \in V$

$$\mathrm{eq}_{\boldsymbol{y}}(\boldsymbol{x}) = \begin{cases} 1 \text{ if } \boldsymbol{x} = \boldsymbol{y} \\ 0 \text{ otherwise} \end{cases}$$

We will leave out $\mathcal{B}$ where it is clear from context.

Example 1: Given a basis of evaluation points $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ for $\mathbb{F}[X^{<n}]$ where ω is a primitive n-th root of unity, we have

$$\mathrm{eq}(x, y) = \frac{x^n - 1}{x - y}$$

Q: Why is this not symmetrical in x and y.

Example 2: Given a basis $\{0, 1\}$ where ω is a primitive n-th root of unity, we have

$$\mathrm{eq}(x, y) = \frac{x^n - 1}{x - y}$$

Lemma 1: Given a product basis $\mathcal{B} = \mathcal{B}_0 \times \mathcal{B}_1$ the $\mathrm{eq}_{\mathcal{B}}$ function factors as

$$\mathrm{eq}_{\mathcal{B}}(\boldsymbol{x_0} \times \boldsymbol{x_1}, \boldsymbol{y_0} \times \boldsymbol{y_1}) = \mathrm{eq}_{\mathcal{B}_0}(\boldsymbol{x_0}, \boldsymbol{y_0}) \cdot \mathrm{eq}_{\mathcal{B}_1}(\boldsymbol{x_1}, \boldsymbol{x_1})$$

Definition 2 (Extension): Given an ordered basis $\mathcal{B} = \{\boldsymbol{b}_0, ..., \boldsymbol{b}_{n-1}\}$ and a vector $\boldsymbol{f} \in \mathbb{F}^n$ define the *extension* $\hat{f}$ as.

$$\hat{f}(\boldsymbol{x}) = \sum_{i \in [0,n)} f_i \cdot \mathrm{eq}_{\mathcal{B}}(\boldsymbol{x}, \boldsymbol{b}_i)$$

General results on finite field inner product embeddings

Definition 3 (Embedding): Given a bilinear map $f : \mathbb{F}^n \times \mathbb{F}^m \to \mathbb{F}^k$ and a finite $\mathbb{F}$-algebra K, an *embedding of f in K* is a triplet of linear maps $(\mathrm{A}, \mathrm{B}, \mathrm{C})$ such that for all $\boldsymbol{x} \in \mathbb{F}^n, \boldsymbol{y} \in \mathbb{F}^m$

$$f(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{C}(\mathrm{A}(\boldsymbol{x}) \cdot_K \mathrm{B}(\boldsymbol{y}))$$

where $\mathrm{A} : \mathbb{F}^n \to K, \mathrm{B} : \mathbb{F}^m \to K$ and $\mathrm{C} : K \to \mathbb{F}^k$.

This is also called *packing*. Note that K is isomorphic to $\mathbb{F}^l$ for some l and given a representaion of K the $\mathrm{A}, \mathrm{B}, \mathrm{C}$ are represented by matrices.

Lemma 2: Given a field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ represented by $\mathbb{F}_q[X]/(X^n - m_1 \cdot X - m_0)$, there exist and embedding of the $\mathbb{F}_q^n$ dot product in $\mathbb{F}_{q^n}$ with $\mathrm{A} = \mathrm{I}$, $\mathrm{C} = (1, 0, ..., 0)$ and

$$\mathrm{B} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & m_0^{-1} \\ \vdots & \vdots & ⋰ & 0 \\ 0 & m_0^{-1} & \cdots & 0 \end{pmatrix}$$

Proof: The embedding of vectors $(a_0, a_1, ..., a_{n-1})$ and $(b_0, b_1, ..., b_{n-1})$ results in

$$a = a_0 + a_1 \cdot X + \cdots + a_{n-1} \cdot X^{n-1}$$
$$b = b_0 + m_0^{-1} \cdot (b_{n-1} \cdot X + \cdots + b_1 \cdot X^{n-1})$$

The product $a \cdot b$ has powers up to $X^{2 \cdot (n-1)}$. Note that in the quotient we have $X^n = m_0 + m_1 \cdot X$. Of the unreduced product, only $X^0 \wedge X^n$ contribute to the constant term of the reduced result. To see this, consider a term X^{n+k} with $k \in [1, n-2]$:

$$X^{n+k} = (m_0 + m_1 \cdot X) \cdot X^k = m_0 \cdot X^k + m_1 \cdot X^{\{k+1\}}$$

since $k > 0$ and $k + 1 < n$ this does not contribute to X^0. Thus the constant term is given by

$$c_0 = a_0 \cdot b_0 + m_0 \cdot \left(a_1 \cdot m_0^{-1} \cdot b_1 + \cdots + a_{n_1} \cdot m_0^{-1} \cdot b_{n-1}\right)$$

which is the dot product as intended. □

Lemma 3 (Towers): Given m, n and a $\mathbb{F}_q^m$ dot product embedding in $\mathbb{F}_{q^m}$ and an $\mathbb{F}_{q^m}^n$ dot product embedding in $\mathbb{F}_{q^{m \cdot n}}$, we can construct an $\mathbb{F}_q^{m \cdot n}$ dot product embedding in $\mathbb{F}_{q^{m \cdot n}}$ by taking the Kronecker product of the embedding matrics.

(Proof TBD)

Theorem 4 (Hansen-Muller):