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 $(1, \mathrm{i}, \mathrm{j}, \mathrm{i} \cdot \mathrm{j}, \mathrm{j}^2, \mathrm{i} \cdot \mathrm{j}^2)$.

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 $\left\lceil \frac{n}{6} \right\rceil$ large field multiplications.

Applying Lemma 1 we find embedding matrices for the degree 2 and 3 extensions. Composing these using Lemma 2 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 $\left\lceil \frac{n}{6} \right\rceil$ elements of $\mathbb{F}_{p^6}$.

Applying this to WHIR, we can commit to a $\left\lceil \frac{n}{6} \right\rceil$ 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.

General results on finite field inner product embeddings

Lemma 1: Given a field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ represented by $\mathbb{F}_q[X]/(X^n - \alpha)$, 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

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

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

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

The constant term of the reduced product $a \cdot b$ is given by the $X^0 = 1$ and $X^n = \alpha$ terms:

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

which is the dot product as intended. ∎

Lemma 2 (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.

Lemma 2: Towers

(Proof TBD)