$$\mathrm{eq}(\mathbf{x}, \mathbf{y}) = \prod_{i \in [0,k)} (x_i \cdot y_i + (1 - x_i) \cdot (1 - y_i))$$

From this follows

- $\mathrm{eq}(\mathbf{x}, \mathbf{y}) = \mathrm{eq}(\mathbf{y}, \mathbf{x})$
- $\mathrm{eq}(0, y) = 1 - y$
- $\mathrm{eq}(1, y) = y$
- $\sum_{\mathbf{b} \in \{0,1\}^k} \mathrm{eq}(\mathbf{x}, \mathbf{b}) \cdot \mathrm{eq}(\mathbf{b}, \mathbf{y}) = \mathrm{eq}(\mathbf{x}, \mathbf{y})$

1 Inner Product Arithmetization

Definition 1 (IPCS): A **inner product commitment scheme** (IPCS) over a finite field $\mathbb{F}$ has operations

- $\mathsf{commit}(\mathbf{x}) \mapsto C_{\mathbf{x}}$ takes a vector $\mathbf{x} \in \mathbb{F}^n$ and outputs a commitment $C_{\mathbf{x}}$.
- $\mathsf{open}(\mathbf{x}, C_{\mathbf{x}}, \mathbf{w}, s) \to \pi$ proves the value of $\mathbf{x} \cdot \mathbf{w} = s$.
- $\mathsf{verify}(C_{\mathbf{x}}, \mathbf{w}, s, \pi)$ verifies the proof π.

where $C_{\mathbf{x}}$ is constant sized. If the size of π is sublinear in n we call it succinct in proof size.

Examples are WHIR and Ligerito.

In conventional sumcheck based protocols, we require $n = 2^k$ and the verifier only needs $\mathbf{w}$ to compute $w(\boldsymbol{r})$ with $\boldsymbol{r} \in \mathbb{F}^k$ and w given by:

$$w(\boldsymbol{r}) = \sum_{\boldsymbol{b} \in \{0,1\}^k} \mathbf{w}_{\boldsymbol{b}} \cdot \mathrm{eq}(\boldsymbol{b}, \boldsymbol{r})$$

If w can be computed sublinearly in n, we call it succinctly verifiable.

Lemma 1 (MLE): An IPCS can succinctly verify an MLE evaluation in $\mathbf{y} \in \mathbb{F}^k$ using

$$w(\mathbf{r}) = \mathrm{eq}(\mathbf{y}, \mathbf{r})$$

Proof: Consider the vector $\mathbf{x}$ as values on the hypercube $\{0,1\}^k$. Take f to be the multilinear extension of $\mathbf{x}$, then an evaluation $f(\boldsymbol{p})$ for $\boldsymbol{p} \in F^k$ can be done by setting $\boldsymbol{w}$.

$$w(\mathbf{r}) = \sum_{\boldsymbol{b} \in \{0,1\}^k} \mathrm{eq}(\boldsymbol{y}, \boldsymbol{b}) \cdot \mathrm{eq}(\boldsymbol{b}, \boldsymbol{r}) = \mathrm{eq}(\mathbf{y}, \boldsymbol{r})$$

□

Lemma 2 (Univariate): Consider the vector $\mathbf{x}$ as evaluations of a polynomial $f(x)$ on $\left(\omega_{2^k}^i\right)_{i \in [0,n)}$. An IPCS can succinctly verify an univariate evaluation in $y \in \mathbb{F}$ using

$$w(\mathbf{r}) = \mathrm{eq}\left(\left(1, y, y^2, y^4, ..., y^{2^k}\right), \mathbf{r}\right)$$

From here we can go further and make make treat the vector as an polynomial on an arbitrary basis

$$\boldsymbol{\omega}_n = \left(\omega_{n_0}^i\right)_{i \in [0,n_0)}$$

$$\left(\omega_{n_0}^i\right)_{i \in [0,n_0)} \times \left(\omega_{n_1}^i\right)_{i \in [0,n_1)} \times \cdots$$

for an arbitrary factorization $n = n_0 \cdot n_1 \cdot \ldots$. Of course, since $n = 2^k$ all factors will be powers of two.

2 Fibonacci

The classic demonstration or AIR style constraint systems is the fibonacci sequence. Given a vector

$$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...)$$

We want the following constraints:

- $x_0 = 1$
- $x_1 = 1$
- $x_i = x_{i-1} + x_{i-2}$ for $i \in [2, n-1]$
- x_{n-1} is the claimed value

This requires pointwise constraints, repeated constraints and constraints containing offsets.

https://hackmd.io/@aztec-network/plonk-arithmetiizati on-air#fn1

Q: Can we have succinct verification of every 2^l sized block in the witness?

3 Karatsuba

Multiplication in $\mathbb{F}_{p^2}$ can be done in three $\mathbb{F}_p$ multiplications:

$$(a_0 + a_1 \cdot \mathrm{i}) \cdot (b_0 + b_1 \cdot \mathrm{i}) =$$
$$a_0 \cdot b_0 - a_1 \cdot b_1 + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot \mathrm{i}$$

Multiplication in F_q^3 can be done in 5 operations $\mathbb{F}_{p^2}$ multiplications:

4 Zero check

[BDT24], [Gru24], [Wei+25]

Given MLEs $a, b, c \in \mathbb{F}_p[x^k]$ we want to prove that for all $\mathbf{x} \in \{0,1\}^k$ we have $a(\mathbf{x}) \cdot b(\mathbf{x}) = c(\mathbf{x})$. In zero-check we do this by proving

$$\sum_{\mathbf{b} \in \{0,1\}^k} \mathrm{eq}(\mathbf{r}, \mathbf{b}) \cdot (a(\mathbf{x}) \cdot b(\mathbf{x}) - c(\mathbf{x})) = 0$$

where $\mathbf{r} \in \mathbb{F}_p^k$ is randomly drawn. This works when $|\mathbb{F}_p| > 2^\lambda$. Furhtermore, sumcheck itself only works when $|\mathbb{F}_p| > 2^\lambda$.

5 General results on finite field embeddings

Question: Embedding of the Hadamard Product?

Lemma 3 (Dot Product Embedding): Given a field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ represented by $\mathbb{F}_q[X]/(X^n - m_1 \cdot X - m_0)$, we can construct an embedding of the $\mathbb{F}_q^n$ inner product in $\mathbb{F}_{q^n}$ in the monomial basis where one vector is transformed with the matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & m_0^{-1} \\ \vdots & \vdots & \iddots & 0 \\ 0 & m_0^{-1} & \cdots & 0 \end{pmatrix}$$

Proof: Since $X^n - m_1 \cdot X - m_0$ is irreducible we have $m_0 \neq 0$ and hence m_0^{-1} exists. The embedding of vectors $(a_0, a_1, \ldots, a_{n-1})$ and $(b_0, b_1, \ldots, b_{n-1})$ 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 and X^n contribute to the constant term. To see this, consider a term X^{n+k} with $k \in [1, n-2]$.

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

and since $k > 0$ and $k + 1 < n$ these do not contribute to the constant term. Thus the constant term is given by

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

which is the dot product as intended. □

Lemma 4 (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)

Lemma 5: Given a field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with $n = 2^k$ for some k, we can construct an embedding of the $\mathbb{F}_q^n$ dot product in $\mathbb{F}_{q^n}$.

Proof: Consider $\mathbb{F}_{q^n}$ as a tower of quadratic extension over F_q. Each quadratic extension has an irreducible polynomial of the form $X^2 - m_1 \cdot X - m_0$ and hence an embedding by Lemma 3. By Lemma 4 we can compose these embeddings to obtain an embedding for F_{q^n}. □

The follwing is a theorem, first conjectured in [HM92] and subsequently proven in [Wan97], [HM98].

Theorem 6 (Hansen–Mullen): Given a field $\mathbb{F}_q$ and positivie integer $n \geq 2$. Fix an $i \in [0, n)$ and $c \in \mathbb{F}_q$, then there exist an irreducible monic polynomial $X^n + \sum_{i \in [0,n)} c_i X^i$ in $F_q[X]$ with $c_i = c$, except when

1. $i = 0$, and $c = 0$, or
2. $q = 2^k$, $n = 2$, $i = 1$, and $c = 0$

The exceptions are natural: any polynomial with $c_0 = 0$ is divisible by X and hence not irreducible. Furthermore in characteristic 2 every value is a square and $x^2 + c_0$ factors as $\left(x + \sqrt{c_0}\right)^2$.

From Theorem 6 follows that for $n = 3$ there always exists an irreducible polynomial $X^3 + m_1 X + m_0$, and hence Lemma 3 applies. Combined with Lemma 4, this gives us embeddings for any $n = 2^k \cdot 3^l$.

Bibliography

[BDT24] S. Bagad, Y. Domb, and J. Thaler, "The Sum-Check Protocol over Fields of Small Characteristic." [Online]. Available: https://eprint.iacr.org/2024/1046

[Gru24] A. Gruen, "Some Improvements for the PIOP for ZeroCheck." [Online]. Available: https://eprint.iacr.org/2024/108

[Wei+25] Y. Wei *et al.*, "Packed Sumcheck over Fields of Small Characteristic with Application to Verifiable FHE." [Online]. Available: https://eprint.iacr.org/2025/719

[HM92] T. Hansen and G. L. Mullen, "Primitive polynomials over finite fields," *Math. Comp. 59 (1992), 639-643*, 1992, doi: https://doi.org/10.1090/S0025-5718-1992-1134730-7.

[Wan97] D. Wan, "Generators and irreducible polynomials over finite fields," *Math. Comp. 66 (1997), 1195-1212*, 1997, doi: http://dx.doi.org/10.1090/S0025-5718-97-00835-1.

[HM98] K. H. Ham and G. L. Mullen, "Distribution of irreducible polynomials of small degree over finite fields," *Math. Comp. 67 (1998), 337-341*, 1998, doi: https://doi.org/10.1090/S0025-5718-98-00904-1.