# IPA as sumcheck

Ariel Gabizon (based on work with Liam Eagen)
Aztec Labs

# Main Goal:

- Reduce linear verifier time from IPA

# Polynomials over $\mathbb{G}$

# Multilinears and vectors

$n = 2^k$.

$f = (f_0, \ldots, f_{n-1}) \in \mathbb{F}^n, z \in \mathbb{F}^k$

$$\hat{f}(z) := \sum_{i<n} \mathbf{eq}(i, z) f_i$$

# Multilinears and vectors

$n = 2^k$.

$f = (f_0, \ldots, f_{n-1}) \in \mathbb{F}^n, z \in \mathbb{F}^k$

$$\hat{f}(z) := \sum_{i<n} \mathbf{eq}(i, z) f_i$$

(can do same for $\mathbf{G} \in \mathbb{G}^n$)

# MLPCS based on IPA:

**Setup:** Chooose random non-zero
$\mathbf{G} = (\mathbf{G_0}, \ldots, \mathbf{G_{n-1}}) \in \mathbb{G}^{\mathbf{n}}, \mathbf{P} \in \mathbb{G}$.

# MLPCS based on IPA:

**Setup:** Chooose random non-zero
$\mathbf{G} = (\mathbf{G_0}, \ldots, \mathbf{G_{n-1}}) \in \mathbb{G}^n, \mathbf{P} \in \mathbb{G}$.

**Commitment:** $\mathbf{f} \in \mathbb{F}^n$, $\mathbf{com}(\mathbf{f}) = \sum_{i<n} \mathbf{f_i} \mathbf{G_i}$.

# MLPCS based on IPA:

**Setup:** Chooose random non-zero
$\mathbf{G} = (\mathbf{G_0}, \ldots, \mathbf{G_{n-1}}) \in \mathbb{G}^n, \mathbf{P} \in \mathbb{G}$.

**Commitment:** $\mathbf{f} \in \mathbb{F}^n$, $\mathbf{com}(\mathbf{f}) = \sum_{i<n} \mathbf{f_i G_i}$.

**Openings:** next slide.

Given $\mathbf{cm} \in \mathbb{G}, z \in \mathbb{F}^k, v \in \mathbb{F}$ want to prove $\mathbf{com}(\mathrm{f}) = \mathbf{cm}$ and $\hat{\mathrm{f}}(z) = v$.

Given $\mathbf{cm} \in \mathbb{G}, z \in \mathbb{F}^{k}, v \in \mathbb{F}$ want to prove $\mathbf{com}(\mathbf{f}) = \mathbf{cm}$ and $\hat{\mathbf{f}}(z) = v$.

Define the polynomial

$$A(\mathbf{X}) := \hat{\mathbf{f}}(\mathbf{X})\hat{\mathbf{G}}(\mathbf{X}) + \mathbf{eq}(\mathbf{X}, z)\hat{\mathbf{f}}(\mathbf{X})\mathbf{P}$$

Given $\mathbf{cm} \in \mathbb{G}, z \in \mathbb{F}^k, v \in \mathbb{F}$ want to prove $\mathbf{com}(f) = \mathbf{cm}$ and $\hat{f}(z) = v$.

Define the polynomial

$$A(X) := \hat{f}(X)\hat{G}(X) + eq(X, z)\hat{f}(X)P$$

When claim holds:

$$\sum_{b \in \{0,1\}^k} \hat{f}(b)\hat{G}(b) + eq(b, z)\hat{f}(b)P$$

$$= \sum_{i<n} f_i G_i + eq(i, z) f_i P = \mathbf{cm} + \hat{f}(z)P$$

Given $\mathbf{cm} \in \mathbb{G}, z \in \mathbb{F}^k, v \in \mathbb{F}$ want to prove $\mathbf{com}(f) = \mathbf{cm}$ and $\hat{f}(z) = v$.

Define the polynomial

$$A(X) := \hat{f}(X)\hat{G}(X) + \mathrm{eq}(X, z)\hat{f}(X)P$$

When claim holds:

$$\sum_{b \in \{0,1\}^k} \hat{f}(b)\hat{G}(b) + \mathrm{eq}(b, z)\hat{f}(b)P$$

$$= \sum_{i<n} f_i G_i + \mathrm{eq}(i, z) f_i P = \mathbf{cm} + \hat{f}(z)P$$

$\mathcal{P}$ and $\mathcal{V}$ will run sumcheck on $A$ with target value $\mathbf{cm} + v\mathbf{P}$.

$\mathcal{P}$ and $\mathcal{V}$ will run sumcheck on $\boldsymbol{A}$ with target value $\mathbf{cm} + \boldsymbol{v}\mathbf{P}$.

At end of sumcheck, $\mathcal{V}$ needs to evaluate $\boldsymbol{A}(\mathbf{r}) = \hat{\mathbf{f}}(\mathbf{r})\hat{\mathbf{G}}(\mathbf{r}) + \mathbf{eq}(\mathbf{r}, \boldsymbol{z})\hat{\mathbf{f}}(\mathbf{r})\mathbf{P}$ for some $\mathbf{r} \in \mathbb{F}^{\mathbf{k}}$.

$\mathcal{P}$ and $\mathcal{V}$ will run sumcheck on $\boldsymbol{A}$ with target value $\mathbf{cm} + \boldsymbol{v}\mathbf{P}$.

At end of sumcheck, $\mathcal{V}$ needs to evaluate $\boldsymbol{A}(\mathbf{r}) = \hat{\mathbf{f}}(\mathbf{r})\hat{\mathbf{G}}(\mathbf{r}) + \mathbf{eq}(\mathbf{r}, \boldsymbol{z})\hat{\mathbf{f}}(\mathbf{r})\mathbf{P}$ for some $\mathbf{r} \in \mathbb{F}^{\mathbf{k}}$.

**In IPA:** $\mathcal{V}$ computes $\mathbf{eq}(\mathbf{r}, \boldsymbol{z}), \hat{\mathbf{G}}(\mathbf{r})$. $\mathcal{P}$ *simply sends* $\boldsymbol{\alpha} = \hat{\mathbf{f}}(\mathbf{r})$.

$\mathcal{P}$ and $\mathcal{V}$ will run sumcheck on $\boldsymbol{A}$ with target value $\mathbf{cm} + \nu\mathbf{P}$.

At end of sumcheck, $\mathcal{V}$ needs to evaluate $\mathbf{A}(\mathbf{r}) = \hat{\mathbf{f}}(\mathbf{r})\hat{\mathbf{G}}(\mathbf{r}) + \mathbf{eq}(\mathbf{r}, z)\hat{\mathbf{f}}(\mathbf{r})\mathbf{P}$ for some $\mathbf{r} \in \mathbb{F}^{\mathbf{k}}$.

**In IPA:** $\mathcal{V}$ computes $\mathbf{eq}(\mathbf{r}, z), \hat{\mathbf{G}}(\mathbf{r})$. $\mathcal{P}$ *simply sends* $\mathbf{a} = \hat{\mathbf{f}}(\mathbf{r})$.

*The strange (and useful) thing:* When $\mathbb{G}$ has hard discrete-log this is sound!

$\mathcal{P}$ and $\mathcal{V}$ will run sumcheck on $A$ with target value $\mathbf{cm} + v\mathbf{P}$.

At end of sumcheck, $\mathcal{V}$ needs to evaluate $A(\mathbf{r}) = \hat{\mathbf{f}}(\mathbf{r})\hat{\mathbf{G}}(\mathbf{r}) + \mathbf{eq}(\mathbf{r}, z)\hat{\mathbf{f}}(\mathbf{r})\mathbf{P}$ for some $\mathbf{r} \in \mathbb{F}^k$.

**In IPA:** $\mathcal{V}$ computes $\mathbf{eq}(\mathbf{r}, z), \hat{\mathbf{G}}(\mathbf{r})$. $\mathcal{P}$ *simply sends* $a = \hat{\mathbf{f}}(\mathbf{r})$.

*The strange (and useful) thing:* When $\mathbb{G}$ has hard discrete-log this is sound!

*Drawback:* Computing $\hat{\mathbf{G}}(\mathbf{r})$ is $n$-size MSM for $\mathcal{V}$!

# Mitigation from Halo: defer MSM

Note

$$\hat{\mathbf{G}}(\mathbf{r}) = \sum_{\mathbf{i}<\mathbf{n}} \mathbf{eq}(\mathbf{i}, \mathbf{r})\mathbf{G}_{\mathbf{i}},$$

is the *commitment to* $\mathbf{eq}(\mathbf{X}, \mathbf{r})$*!*

# Mitigation from Halo: defer MSM

Note

$$\hat{\mathbf{G}}(\mathbf{r}) = \sum_{\mathbf{i}<\mathbf{n}} \mathbf{eq}(\mathbf{i}, \mathbf{r})\mathbf{G}_{\mathbf{i}},$$

is the *commitment to* $\mathbf{eq}(\mathbf{X}, \mathbf{r})$*!*

Can use this to reduce multiple evaluation claims $\mathbf{G}(\mathbf{r}_{\mathbf{i}}) = \mathbf{V}_{\mathbf{i}}$ into one.

# $\mathcal{P}$ proving correctness of $\hat{\mathbf{G}}(\mathbf{r})$

*Observation: If we have mlPCS for field-valued multilinears, where all ops on* $\mathbf{f}$*'s vals are* $\mathbb{F}$*-linear, can also use on group valued multilinear* $\mathbf{G}$*. - e.g. Basefold*

# Correlated agreement theorem: