Ranged Polynomial Protocols

Ariel Gabizon
Aztec
(Based on work with Zachary J. Williamson)

"traditional" approach (QAP/r1cs/..)

Program

$\downarrow$

Constraints in some language

$\downarrow$

Polynomials

$\downarrow$

Proof

Recently..[1] (similar in spirit to [..,BCGGHJ17,Arya,..]):

$$\begin{array}{c}\text{Program}\\ \Big\downarrow \\ \text{Constraints /polynomials}\\ \Big\downarrow \\ \text{Proof}\end{array}$$

[1] https://ethresear.ch/t/using-polynomial-commitments-to-replace-state-roots/7095,plookup

Ranged polynomials protocols

Preprocessing/inputs: Predefined polynomials $g_1, \ldots, g_t \in \mathbb{F}_{<d}[X]$
Range: $H \subset \mathbb{F}$.

Ranged polynomials protocols

Preprocessing/inputs: Predefined polynomials $g_1, \ldots, g_t \in \mathbb{F}_{<d}[X]$
Range: $H \subset \mathbb{F}$.

Protocol:

1. $\mathcal{P}$'s msgs are to ideal party $\mathbf{I}$. Must be $f_i \in \mathbb{F}_{<d}[X]$.

Ranged polynomials protocols

Preprocessing/inputs: Predefined polynomials $g_1, \ldots, g_t \in \mathbb{F}_{<d}[X]$
Range: $H \subset \mathbb{F}$.

Protocol:

1. $\mathcal{P}$'s msgs are to ideal party $\mathbf{I}$. Must be $f_i \in \mathbb{F}_{<d}[X]$.
2. At end, $\mathcal{V}$ asks $\mathbf{I}$ if some identity holds between $\{f_1, \ldots, f_\ell, g_1, \ldots, g_t\}$ **on** H.

$\mathbf{D} :=$ max degree of identity $\mathbf{C}$ checked in exec with honest $\mathcal{P}$.

$\mathfrak{d}(\mathbf{P}) := \left(\sum_{i\in[t]} \deg(f_i) + 1\right) + \mathbf{D} - |\mathbf{H}|.$

[2] similar statements in Marlin/Fractal/Supersonic

$\mathbf{D}$:= max degree of identity $\mathbf{C}$ checked in exec with honest $\mathcal{P}$.

$$\mathfrak{d}(\mathbf{P}) := \left(\sum_{i\in[t]} \deg(\mathbf{f_i}) + 1\right) + \mathbf{D} - |\mathbf{H}|.$$

Thm:[2] Can compile to "real" protocol in Algebraic Group Model, where prover complexity $\mathfrak{d}(\mathbf{P})$.

[2]similar statements in Marlin/Fractal/Supersonic

$\mathbf{D}$:= max degree of identity $\mathbf{C}$ checked in exec with honest $\mathcal{P}$.

$$\mathfrak{d}(\mathbf{P}) := \left(\sum_{i\in[t]} \deg(f_i) + 1\right) + \mathbf{D} - |\mathbf{H}|.$$

Thm:[2] Can compile to "real" protocol in Algebraic Group Model, where prover complexity $\mathfrak{d}(\mathbf{P})$.

proof sketch: Use [KZG] polynomial commitment scheme. $\mathcal{P}$ commits to all polys and $\mathbf{C}/\mathbf{Z}_{\mathbf{H}}$. $\mathcal{V}$ checks identity at random challenge point.

[2] similar statements in Marlin/Fractal/Supersonic

Multiset equality check

Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} \stackrel{?}{=} \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$

Multiset equality check

Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check
$\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} \stackrel{?}{=} \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$

Choose random $\boldsymbol{\gamma} \in \mathbb{F}$. Check

$$(\mathbf{a}_1+\boldsymbol{\gamma})(\mathbf{a}_2+\boldsymbol{\gamma})(\mathbf{a}_3+\boldsymbol{\gamma}) \stackrel{?}{=} (\mathbf{b}_1+\boldsymbol{\gamma})(\mathbf{b}_2+\boldsymbol{\gamma})(\mathbf{b}_3+\boldsymbol{\gamma})$$

Multiset equality check

Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} \stackrel{?}{=} \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$

Choose random $\boldsymbol{\gamma} \in \mathbb{F}$. Check

$$(\mathbf{a}_1+\boldsymbol{\gamma})(\mathbf{a}_2+\boldsymbol{\gamma})(\mathbf{a}_3+\boldsymbol{\gamma}) \stackrel{?}{=} (\mathbf{b}_1+\boldsymbol{\gamma})(\mathbf{b}_2+\boldsymbol{\gamma})(\mathbf{b}_3+\boldsymbol{\gamma})$$

If $\mathbf{a}, \mathbf{b}$ different as sets then w.h.p products different.

Multiset equality check

Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check
$\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} \stackrel{?}{=} \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$

Choose random $\boldsymbol{\gamma} \in \mathbb{F}$. Check

$$(\mathbf{a}_1+\boldsymbol{\gamma})(\mathbf{a}_2+\boldsymbol{\gamma})(\mathbf{a}_3+\boldsymbol{\gamma}) \stackrel{?}{=} (\mathbf{b}_1+\boldsymbol{\gamma})(\mathbf{b}_2+\boldsymbol{\gamma})(\mathbf{b}_3+\boldsymbol{\gamma})$$

If $\mathbf{a}, \mathbf{b}$ different as sets then w.h.p products different.

Multiset equality check - polynomial version

Given $f, g \in \mathbb{F}_{<d}[X]$, want to check
$\{f(x)\}_{x \in H} \stackrel{?}{=} \{g(x)\}_{x \in H}$ as multisets

Multiplicative subgroups:

$\mathbf{H} = \{\alpha, \alpha^2, \ldots, \alpha^n = 1\}$.

$\mathbf{L_i}$ is i'th lagrange poly of $\mathbf{H}$:

$$\mathbf{L_i}(\alpha^i) = 1, \mathbf{L_i}(\alpha^j) = 0, j \neq i$$

Reduces to:

$$\mathbf{H} = \left\{\boldsymbol{\alpha}, \boldsymbol{\alpha}^2, \ldots, \boldsymbol{\alpha}^n\right\}.$$

$\mathcal{P}$ has sent $\mathbf{f}, \mathbf{g} \in \mathbb{F}_{<n}[\mathbf{X}]$.

Wants to prove:

$$\prod_{i \in [n]} \mathbf{f}(\boldsymbol{\alpha}^i) = \prod_{i \in [n]} \mathbf{g}(\boldsymbol{\alpha}^i)$$

Checking products with $\mathbb{H}$-ranged protocols [GWC19]

1. $\mathcal{P}$ computes Z with $Z(\alpha) = 1, Z(\alpha^i) = \prod_{j<i} f(\alpha^j)/g(\alpha^j)$.
2. Sends Z to $\mathbf{I}$.

Checking products with $\mathbf{H}$-ranged protocols [GWC19]

1. $\mathcal{P}$ computes $\mathbf{Z}$ with $\mathbf{Z}(\boldsymbol{\alpha}) = 1, \mathbf{Z}(\boldsymbol{\alpha}^{\mathbf{i}}) = \prod_{\mathbf{j}<\mathbf{i}} \mathbf{f}(\boldsymbol{\alpha}^{\mathbf{j}})/\mathbf{g}(\boldsymbol{\alpha}^{\mathbf{j}})$.
2. Sends $\mathbf{Z}$ to $\mathbf{I}$.
3. $\mathcal{V}$ checks following identities on $\mathbf{H}$.
   3.1 $\mathbf{L}_1(\mathbf{X})(\mathbf{Z}(\mathbf{X}) - 1) = 0$
   3.2 $\mathbf{Z}(\mathbf{X})\mathbf{f}(\mathbf{X}) = \mathbf{Z}(\boldsymbol{\alpha} \cdot \mathbf{X})\mathbf{g}(\mathbf{X})$

Checking products with $\mathbb{H}$-ranged protocols [GWC19]

1. $\mathcal{P}$ computes Z with $Z(\alpha) = 1, Z(\alpha^i) = \prod_{j<i} f(\alpha^j)/g(\alpha^j)$.
2. Sends Z to $\mathbf{I}$.
3. $\mathcal{V}$ checks following identities on $\mathbb{H}$.
   3.1 $L_1(X)(Z(X) - 1) = 0$
   3.2 $Z(X)f(X) = Z(\alpha \cdot X)g(X)$

We get $\mathfrak{d}(P) = n + 2n - |\mathbb{H}| = 2n$.

Example 2: Range checks

Integer $M < n$. Given $f \in \mathbb{F}_{<n}[X]$, want to check $f(x) \in [1..M]$ for each $x \in H$.

Example 2: Range checks

Integer $M < n$. Given $f \in \mathbb{F}_{<n}[X]$, want to check $f(x) \in [1..M]$ for each $x \in H$.
(most?) common SNARK operation

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{\mathbf{f}(x)\}_{x \in \mathbf{H}}$

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$

Protocol:

1. $\mathcal{P}$ computes ”sorted version of f“: $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x\in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x\in H} = \{f(x)\}_{x\in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
    1. Mutli-set equality between s and f.

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
   3.1 Mutli-set equality between s and f.
   3.2 $s(\alpha) = 1$
   3.3 $s(\alpha^n) = M$

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
   3.1 Mutli-set equality between s and f.
   3.2 $s(\alpha) = 1$
   3.3 $s(\alpha^n) = M$
   3.4 For each $x \in H \setminus \{1\}$,

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x\in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x\in H} = \{f(x)\}_{x\in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
   - 3.1 Mutli-set equality between s and f.
   - 3.2 $s(\alpha) = 1$
   - 3.3 $s(\alpha^n) = M$
   - 3.4 For each $x \in H \setminus \{1\}$,

$$(s(x\cdot\alpha) - s(x))^2 = s(x\cdot\alpha) - s(x)$$

We get $\mathfrak{d}(P) = 3n$

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$
Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
   3.1 Mutli-set equality between s and f.
   3.2 $s(\alpha) = 1$
   3.3 $s(\alpha^n) = M$
   3.4 For each $x \in H \setminus \{1\}$,
   $$(s(x \cdot \alpha) - s(x))^2 = s(x \cdot \alpha) - s(x)$$

We get $\mathfrak{d}(P) = 3n$
To remove assumption use preprocessed "table poly" t with $\{t(x)\}_{x \in H} = [1..M]$ increased $\mathfrak{d}(P)$ by $2M$

Example 2: Range checks

Simplyfing assumption: $[1..M] \subset \{f(x)\}_{x \in H}$

Protocol:

1. $\mathcal{P}$ computes "sorted version of f": $s \in \mathbb{F}_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) < s(\alpha^{i+1}$.
2. $\mathcal{P}$ sends s to $\mathbf{I}$.
3. $\mathcal{V}$ checks that
   3.1 Mutli-set equality between s and f.
   3.2 $s(\alpha) = 1$
   3.3 $s(\alpha^n) = M$
   3.4 For each $x \in H \setminus \{1\}$,

$$(s(x \cdot \alpha) - s(x))^2 = s(x \cdot \alpha) - s(x)$$

We get $\mathfrak{d}(P) = 3n$

To remove assumption use preprocessed "table poly" t with $\{t(x)\}_{x \in H} = [1..M]$ increased $\mathfrak{d}(P)$ by $2M$