Ranged Polynomial Protocols

Ariel Gabizon
Aztec
(Based on work with Zachary J. Williamson)
“traditional” approach (QAP/r1cs/..)

- Program
  - Constraints in some language
    - Polynomials
      - Proof
Recently..¹ (similar in spirit to [..,BCGGHJ17,Arya,..]):

```
Program

Constraints / polynomials

Proof
```

¹https://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: $H \subset \mathbb{F}$. 
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 $\mathcal{I}$. Must be $f_i \in \mathbb{F}_d[X]$. 
Ranged polynomials protocols

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

Protocol:

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

2. At end, $\mathcal{V}$ asks $\mathcal{I}$ if some identity holds between $\{f_1, \ldots, f_\ell, g_1, \ldots, g_t\}$ on $H$. 
D := max degree of identity C checked in exec with honest P.

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

\(^2\)similar statements in Marlin/Fractal/Supersonic
\[ D := \text{max degree of identity } C \text{ checked in exec with honest } P. \]

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

**Thm:**\(^2\) Can compile to “real” protocol in Algebraic Group Model, where prover complexity \( \vartheta(P) \).

\(^2\)similar statements in Marlin/Fractal/Supersonic
$$D := \text{max degree of identity } C \text{ checked in exec with honest } P.$$ 

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

**Thm:** Can compile to “real” protocol in Algebraic Group Model, where prover complexity $$\mathcal{d}(P).$$ 

**Proof sketch:** Use [KZG] polynomial commitment scheme. $$P$$ commits to all polys and $$C/Z_H.$$ $$V$$ checks identity at random challenge point.

---

2 similar statements in Marlin/Fractal/Surpersonic
Multiset equality check

Given $\mathbf{a}, \mathbf{b} \in \mathbb{F}^3$, want to check

$\{b_1, b_2, b_3\} \overset{?}= \{a_1, a_2, a_3\}$
Multiset equality check

Given $a, b \in \mathbb{F}^3$, want to check

$\{b_1, b_2, b_3\} \overset{?}{=} \{a_1, a_2, a_3\}$

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

$$(a_1+\gamma)(a_2+\gamma)(a_3+\gamma) \overset{?}{=} (b_1+\gamma)(b_2+\gamma)(b_3+\gamma)$$

If $a, b$ different as sets then w.h.p products different.
Multiset equality check

Given $a, b \in \mathbb{F}^3$, want to check
\[{b_1, b_2, b_3} = {a_1, a_2, a_3}\]

Choose random $\gamma \in \mathbb{F}$. Check
\[(a_1+\gamma)(a_2+\gamma)(a_3+\gamma) = (b_1+\gamma)(b_2+\gamma)(b_3+\gamma)\]

If $a, b$ different as sets then w.h.p products different.
Multiset equality check

Given \( \mathbf{a}, \mathbf{b} \in \mathbb{F}^3 \), want to check
\[
\{ b_1, b_2, b_3 \} \overset{?}{=} \{ a_1, a_2, a_3 \}
\]

Choose random \( \gamma \in \mathbb{F} \). Check
\[
(a_1 + \gamma)(a_2 + \gamma)(a_3 + \gamma) \overset{?}{=} (b_1 + \gamma)(b_2 + \gamma)(b_3 + \gamma)
\]

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

\[ \{ f(x) \}_{x \in \mathbb{H}} = \{ g(x) \}_{x \in \mathbb{H}} \] as multisets
Multiplicative subgroups:

\[ H = \{ \alpha, \alpha^2, \ldots, \alpha^n = 1 \} \].

\( L_i \) is i’th lagrange poly of \( H \):

\[ L_i(\alpha^i) = 1, \quad L_i(\alpha^j) = 0, \quad j \neq i \]
Reduces to:

\[ H = \{ \alpha, \alpha^2, \ldots, \alpha^n \} \].

\( \mathcal{P} \) has sent \( f, g \in \mathbb{F}_n[X] \).

Wants to prove:

\[
\prod_{i \in [n]} f(\alpha^i) = \prod_{i \in [n]} g(\alpha^i)
\]
Checking products with $\mathcal{H}$-ranged protocols [GWC19]

1. $\mathcal{P}$ computes $Z$ with
   
   \[ Z(\alpha) = 1, \quad Z(\alpha^i) = \prod_{j<i} f(\alpha^j)/g(\alpha^j). \]

2. Sends $Z$ to $\mathcal{I}$. 

Checking products with $\mathcal{H}$-ranged protocols \cite{GWC19}

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

We get $d(P) = n + 2n - |H| = 2n.$
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: \([1..M] \subset \{f(x)\}_{x \in H}\)
Example 2: Range checks

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

Protocol:

1. \(P\) computes ”sorted version of \(f\)“: \(s \in F_n[X]\) with \(\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}\), \(s(\alpha^i) \leq s(\alpha^{i+1})\).
Example 2: Range checks

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

Protocol:

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

2. \(\mathcal{P}\) sends \(s\) to \(\mathcal{I}\).
Example 2: Range checks

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

Protocol:

1. $P$ computes "sorted version of $f"$; $s \in F_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) \leq s(\alpha^{i+1})$.

2. $P$ sends $s$ to $I$.

3. $V$ checks that
   3.1 Mutli-set equality between $s$ and $f$. 
Example 2: Range checks

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

Protocol:

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

2. $P$ sends $s$ to $I$.

3. $V$ checks that
   \begin{align*}
   3.1 & \text{ Mutli-set equality between } s \text{ and } f. \\
   3.2 & \text{ } s(\alpha) = 1 \\
   3.3 & \text{ } s(\alpha^n) = M
   \end{align*}
Example 2: Range checks

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

**Protocol:**

1. $P$ computes "sorted version of $f$": $s \in F_{<n}[X]$ with $\{s(x)\}_{x \in H} = \{f(x)\}_{x \in H}$, $s(\alpha^i) \leq s(\alpha^{i+1})$.
2. $P$ sends $s$ to $I$.
3. $V$ checks that
   
   3.1 Multi-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. \( P \) computes ”sorted version of \( f \“: \ s \in \mathbb{F}_n[X]
   with \( \{ s(x) \}_{x \in H} = \{ f(x) \}_{x \in H} \),
   \( s(\alpha^i) \leq s(\alpha^{i+1}) \).

2. \( P \) sends \( s \) to \( I \).

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

Open question: get almost same complexity for larger range e.g. $[1..M^2]$