Cached quotients and lookups

Ariel Gabizon
Zeta Function Technologies

29. august 2023

Constraints vs Lookups

Example: Check $\mathbf{0 \leq x \leq 2^n - 1}$

Constraints vs Lookups

Example: Check $\mathbf{0 \leq x \leq 2^n - 1}$

Constraint approach:
Prover sends $\mathbf{b_0, \ldots, b_{n-1}}$. Shows:

- $\forall \mathbf{i}, \mathbf{b_i} \in \{\mathbf{0}, \mathbf{1}\}$
- $\sum_{\mathbf{i}} \mathbf{b_i 2^i} = \mathbf{x}$.

Constraints vs Lookups

Example: Check $\mathbf{0 \leq x \leq 2^n - 1}$

Constraint approach:
Prover sends $\mathbf{b_0, \ldots, b_{n-1}}$. Shows:

- $\forall \mathbf{i}, \mathbf{b_i} \in \{\mathbf{0}, \mathbf{1}\}$
- $\sum_{\mathbf{i}} \mathbf{b_i 2^i} = \mathbf{x}$.

Requires $\mathbf{n + 1}$ constraints.

Lookup approach

Preprocess table $\mathbf{T} = \{\mathbf{0}, \ldots, \mathbf{2^n - 1}\}$.Let $\mathbf{N} := |\mathbf{T}|$.
Devise protocol to check $x \in \mathbf{T}$.

Lookup approach

Preprocess table $\mathbf{T} = \{\mathbf{0}, \ldots, \mathbf{2^n - 1}\}$.Let $\mathbf{N} := |\mathbf{T}|$.
Devise protocol to check $x \in \mathbf{T}$.

Old results - good when amortized:
Thm[plookup]: Can check $\mathbf{m}$ different x's are in $\mathbf{T}$ in $\mathbf{O}(\mathbf{m} + \mathbf{N})$ constraints.

Lookup approach

Preprocess table $\mathbf{T} = \{\mathbf{0}, \ldots, \mathbf{2^n - 1}\}$.Let $\mathbf{N} := |\mathbf{T}|$. Devise protocol to check $\mathbf{x} \in \mathbf{T}$.

Old results - good when amortized:
Thm[plookup]: Can check $\mathbf{m}$ different $\mathbf{x}$'s are in $\mathbf{T}$ in $\mathbf{O}(\mathbf{m} + \mathbf{N})$ constraints.

New results - prover doesn't pay for table size!!
Thm [Caulk...$\mathfrak{cq}$]: After $\mathbf{O}(\mathbf{N} \log \mathbf{N})$ preprocessing, can check $\mathbf{x} \in \mathbf{T}$, in $\mathbf{O}(\mathbf{1})$ constraints.

Rest of talk: explain main technical component of new works - *cached quotients*

Rest of talk: explain main technical component of new works - *cached quotients*

First - a brief recap of polynomial commitment schemes..

The KZG Polynomial commitment scheme

$\mathbf{G}$ - generator of pairing friendly elliptic curve group.

$\mathbf{srs} := \mathbf{1 \cdot G, x \cdot G, \ldots, x^d \cdot G}$, for random $\mathbf{x} \in \mathbb{F}$.

The KZG Polynomial commitment scheme

$\mathbf{G}$ - generator of pairing friendly elliptic curve group.

$\mathbf{srs} := \mathbf{1} \cdot \mathbf{G}, x \cdot \mathbf{G}, \ldots, x^{\mathbf{d}} \cdot \mathbf{G}$, for random $x \in \mathbb{F}$.

For $\mathbf{f} \in \mathbb{F}[\mathbf{X}]$ of degree $\mathbf{d}$:

$$\mathbf{cm}(\mathbf{f}) := \mathbf{f}(x) \cdot \mathbf{G}$$

The KZG Polynomial commitment scheme

$\mathbf{G}$ - generator of pairing friendly elliptic curve group.

$\mathbf{srs} := \mathbf{1 \cdot G, x \cdot G, \ldots, x^d \cdot G}$, for random $x \in \mathbb{F}$.

For $f \in \mathbb{F}[X]$ of degree d:

$$\mathbf{cm}(f) := f(x) \cdot \mathbf{G}$$

Central Feature: Given $\mathbf{cm}(f)$ and any $\alpha \in \mathbb{F}$;
there is short proof for correctness of $z = f(\alpha)$.

The KZG Polynomial commitment scheme

$\mathbf{srs} := \mathbf{1 \cdot G, x \cdot G, \ldots, x^d \cdot G}$, for random $x \in \mathbb{F}$.

$\mathbf{cm(f) := f(x) \cdot G}$

Nice features:

The KZG Polynomial commitment scheme

$\mathbf{srs} := \mathbf{1} \cdot \mathbf{G}, x \cdot \mathbf{G}, \ldots, x^{\mathbf{d}} \cdot \mathbf{G}$, for random $x \in \mathbb{F}$.
$\mathbf{cm}(\mathbf{f}) := \mathbf{f}(x) \cdot \mathbf{G}$

Nice features:

- **Linearity:** $\mathbf{cm}(\mathbf{f} + \mathbf{g}) = \mathbf{cm}(\mathbf{f}) + \mathbf{cm}(\mathbf{g})$

The KZG Polynomial commitment scheme

$\mathbf{srs} := \mathbf{1} \cdot \mathbf{G}, \mathbf{x} \cdot \mathbf{G}, \ldots, \mathbf{x}^{\mathbf{d}} \cdot \mathbf{G}$, for random $\mathbf{x} \in \mathbb{F}$.
$\mathbf{cm}(\mathbf{f}) := \mathbf{f}(\mathbf{x}) \cdot \mathbf{G}$

Nice features:

- **Linearity:** $\mathbf{cm}(\mathbf{f} + \mathbf{g}) = \mathbf{cm}(\mathbf{f}) + \mathbf{cm}(\mathbf{g})$
- **Product checks:** Given $\mathbf{cm}(\mathbf{f_1}), \mathbf{cm}(\mathbf{f_2}), \mathbf{cm}(\mathbf{g_1}), \mathbf{cm}(\mathbf{g_2})$ can check $\mathbf{f_1}(\mathbf{X})\mathbf{f_2}(\mathbf{X}) \stackrel{?}{\equiv} \mathbf{g_1}(\mathbf{X})\mathbf{g_2}(\mathbf{X})$ via pairings. (Secure in the Algebraic Group Model)

Cached Quotients - a motivating example from **Caulk**[ZBKMN]

Cached Quotients - a motivating example from **Caulk**[ZBKMN]

$Z_T(X) = \prod_{a \in T}(X - a)$ a vanishing polynomial of a subset $T \subset \mathbb{F}$.

Cached Quotients - a motivating example from **Caulk**[ZBKMN]

$Z_T(X) = \prod_{a \in T}(X - a)$ a vanishing polynomial of a subset $T \subset \mathbb{F}$.

$\mathbf{cm}(Z_T), \mathbf{cm}(f)$ given to verifier.

Cached Quotients - a motivating example from **Caulk**[ZBKMN]

$Z_T(X) = \prod_{a \in T}(X - a)$ a vanishing polynomial of a subset $T \subset \mathbb{F}$.

$\mathbf{cm}(Z_T), \mathbf{cm}(f)$ given to verifier.
Prover wants to show $f = Z_S$ for some $S \subset T$.

Cached Quotients - a motivating example from **Caulk**[ZBKMN]

$\mathbf{Z_T(X) = \prod_{a \in T}(X - a)}$ a vanishing polynomial of a subset $\mathbf{T \subset \mathbb{F}}$.

$\mathbf{cm(Z_T), cm(f)}$ given to verifier.
Prover wants to show $\mathbf{f = Z_S}$ for some $\mathbf{S \subset T}$.

Can we do this in $\mathbf{O(|S|)}$ prover operations?(think $\mathbf{|S| \ll |T|}$)

Cached quotients idea:

The quotient $Z_{T\setminus S}(X) = \frac{Z_T(X)}{Z_S(X)}$ is a "witness" to $S \subset T$.

Cached quotients idea:

The quotient $Z_{T\setminus S}(X) = \frac{Z_T(X)}{Z_S(X)}$ is a "witness" to $S \subset T$.

- Enough to compute **commitment** to $Z_{T\setminus S}$.

Cached quotients idea:

The quotient $Z_{T\setminus S}(X) = \frac{Z_T(X)}{Z_S(X)}$ is a "witness" to $S \subset T$.

- Enough to compute **commitment** to $Z_{T\setminus S}$.
- This commitment is a **sparse combination** of commitments we can **precompute**.

details in next slide..

For each $i \in T$, let $g_i(X) := Z_{T \setminus \{i\}}(X)$.

For each $i \in T$, let $g_i(X) := Z_{T \setminus \{i\}}(X)$.

We have [Tomescu et. al]

$$Z_{T \setminus S}(X) = \sum_{i \in S} c_i \cdot g_i(X)$$

for some $c_i \in \mathbb{F}$.

For each $\mathbf{i} \in \mathbf{T}$, let $\mathbf{g_i(X) := Z_{T\setminus\{i\}}(X)}$.

We have [Tomescu et. al]

$$Z_{T\setminus S}(X) = \sum_{i\in S} c_i \cdot g_i(X)$$

for some $\mathbf{c_i} \in \mathbb{F}$.

We precompute $\mathbf{cm(Z_T), \{cm(g_i)\}_{i\in T}}$.

Prover then computes in $|S|$ operations:

$$\boldsymbol{\pi} := \mathbf{cm}(Z_{T \setminus S}) = \sum_{i \in S} \mathbf{c_i} \cdot \mathbf{cm}(\mathbf{g_i})$$

Prover then computes in $|S|$ operations:

$$\pi := \mathbf{cm}(Z_{T\setminus S}) = \sum_{i\in S} c_i \cdot \mathbf{cm}(g_i)$$

Verifier checks with pairing that:

$$e(\mathbf{cm}(f), \pi) = e(\mathbf{cm}(Z_T), 1 \cdot G)$$

Historical perspective: A trilogy of pairing-based SNARKs

Historical perspective: A trilogy of pairing-based SNARKs

1. **A new hope (for SNARKs, not the universe)** - [Groth10,**GGPR**,...,Groth16]

Historical perspective: A trilogy of pairing-based SNARKs

1. **A new hope (for SNARKs, not the universe)** - [Groth10,**GGPR**,...,Groth16]

2. **The polynomial commitment scheme strikes back** - [vsql,**Sonic**,Plonk,Marlin,...]

Historical perspective: A trilogy of pairing-based SNARKs

1. **A new hope (for SNARKs, not the universe)** - [Groth10,**GGPR**,...,Groth16]

2. **The polynomial commitment scheme strikes back** - [vsql,**Sonic**,Plonk,Marlin,...]

3. **Return of the pairing** - [Caulk,...,cq,..]

Other Application in Chapter 3: lincheck

Fixed $n \times n$ matrix M.

Other Application in Chapter 3: lincheck

Fixed $n \times n$ matrix M.

Prover has poly $f \in \mathbb{F}_{<n}[X]$. Verifier $\mathbf{cm}(f)$.
$a := f|_H$ for subgroup H of size n.

Other Application in Chapter 3: lincheck

Fixed $n \times n$ matrix M.

Prover has poly $f \in \mathbb{F}_{<n}[X]$. Verifier $\mathbf{cm}(f)$.
$a := f|_H$ for subgroup H of size n.

cq-lin: After preprocessing of M, prover can show $M \cdot a = \mathbf{0}$ *in* $O(n)$ *operations.*

Other Application in Chapter 3: lincheck

Fixed $n \times n$ matrix M.

Prover has poly $f \in \mathbb{F}_{<n}[X]$. Verifier $\mathbf{cm}(f)$.
$a := f|_H$ for subgroup H of size n.

cq-lin: After preprocessing of M, prover can show
$M \cdot a = \mathbf{0}$ *in* $O(n)$ *operations.*