Efficient Sum-check and Lookup Argument for KZG-based Commitments

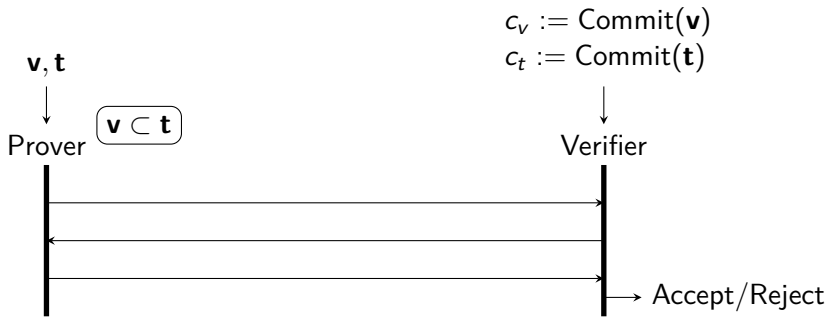
Yuncong Zhang, Shi-Feng Sun, Dawu Gu

Shanghai Jiao Tong University

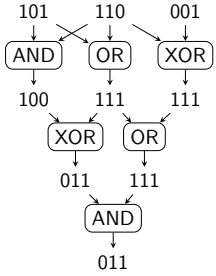
April 16, 2024

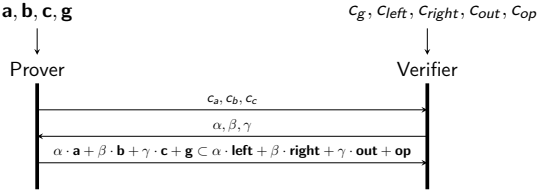
Outline

Lookup Argument



Example Application





a	b	c	g
101	110	100	0
101	110	111	1
110	001	111	2
100	111	011	2
111	111	111	1
011	111	011	0

$\subset$

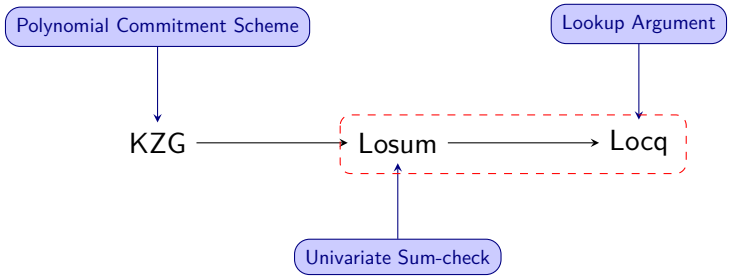
left	right	out	op
000	000	000	0
001	000	000	0
⋮	⋮	⋮	⋮
000	000	000	1
001	000	001	1
⋮	⋮	⋮	⋮
111	111	000	2

Lookup Arguments

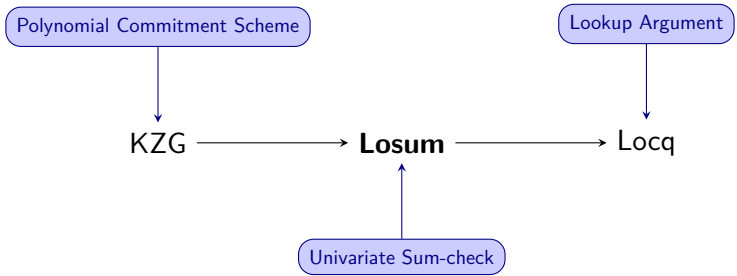
Name	Author	Preprocess	Prover	Verifier/Proof Size
Plookup	Gabizon, etc.	-	$O((m+N)\log(m+N))$	$O(1)$
Caulk	Vitalik and Maller, etc.	$O(N \log N)$	$O(m^2 + m \log N)$	$O(1)$
Caulk+	Posen and Kattis	$O(N \log N)$	$O(m^2)$	$O(1)$
Flookup	Gabizon, etc.	$O(N \log^2 N)$	$O(m \log^2 m)$	$O(1)$
cq	Eagen, Fiore, Gabizon	$O(N \log N)$	$O(m \log m)$	$O(1)$
cq+, cq++	Campanelli et al.	$O(N \log N)$	$O(m \log m)$	$O(1)$

$m = |\mathbf{v}|$ $N = |\mathbf{t}|$

This Work


Polynomial Commitment Scheme
Lookup Argument
KZG
Losum
Locq
Univariate Sum-check

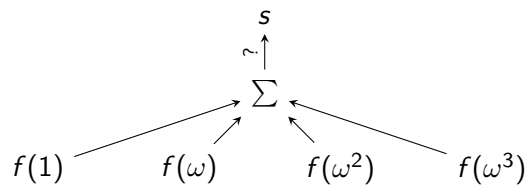
This Work


Polynomial Commitment Scheme
Lookup Argument
KZG
Losum
Locq
Univariate Sum-check

Univariate Sum-check

Given $[f(x)]_1$, check that

$$\sum_{h \in \mathbb{H}} f(h) = s$$



$$\mathbb{H} = \{ \quad 1 \quad \omega \quad \omega^2 \quad \omega^3 \quad \}$$

Univariate Sum-check

Observation

- Let $\mathcal{Z}$ be all polynomials of degree $< |\mathbb{H}|$ such that

$$\sum_{h \in \mathbb{H}} f(h) = 0$$

- $f(X) \in \mathcal{Z}, g(X) \in \mathcal{Z}$ then $f(X) + g(X) \in \mathcal{Z}$

$\mathcal{Z}$ is a linear space.

Linear Space Membership Check

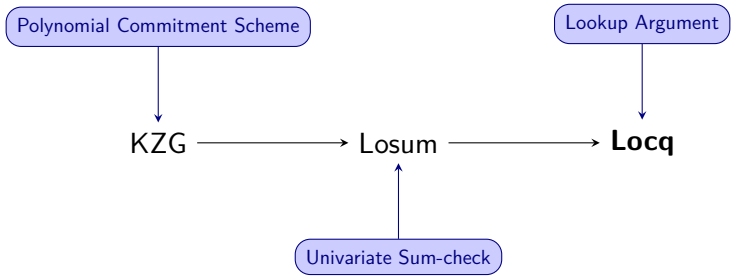
Basis Polynomials:	$b_1(X) \qquad b_2(X) \qquad b_3(X)$
Setup:	$\alpha \xleftarrow{\$} \mathbb{F} \qquad [\alpha b_1(x)]_1 \qquad [\alpha b_2(x)] \qquad [\alpha b_3(x)]$
Prove:	$\pi \leftarrow c_1[\alpha b_1(x)]_1 + c_2[\alpha b_2(x)]_1 + c_3[\alpha b_3(x)]_1$
Verify:	$e([f(x)]_1, [\alpha]_2) = e(\pi, [1]_2)$

Basis Choice for Univariate Sum-check

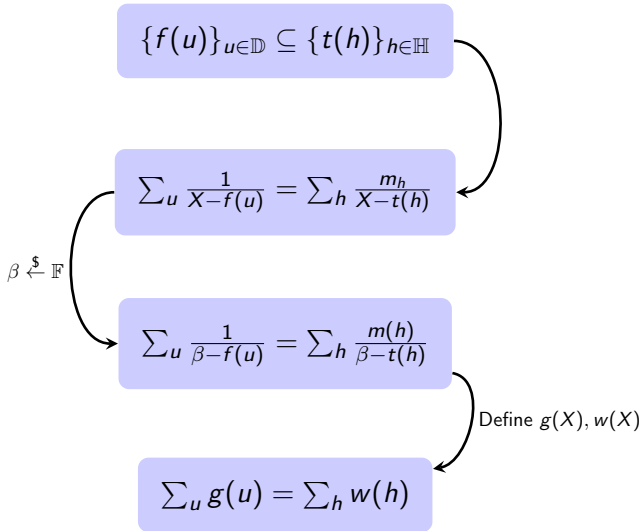
$b_1(X)$	$L_1(X) - L_{h^*}(X)$	1	0	0	-1	$\times f(1)$
$b_2(X)$	$L_\omega(X) - L_{h^*}(X)$	0	1	0	-1	$\times f(\omega)$
$b_3(X)$	$L_{\omega^2}(X) - L_{h^*}(X)$	0	0	1	-1	$\times f(\omega^2)$

$f(X)$	$f(1)$	$f(\omega)$	$f(\omega^2)$	$f(h^*)$

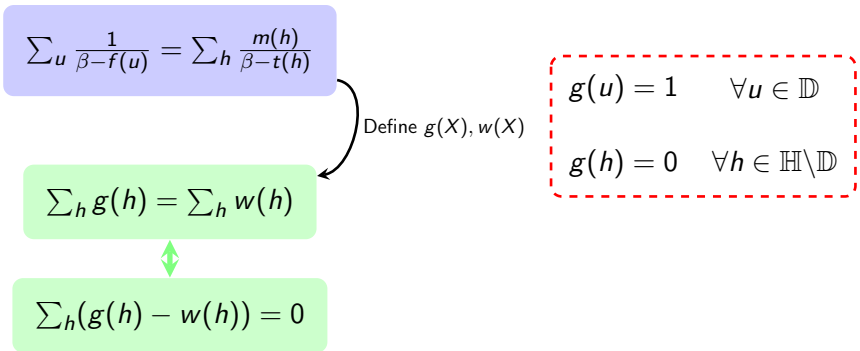
This Work


Polynomial Commitment Scheme
Lookup Argument
KZG
Losum
Locq
Univariate Sum-check

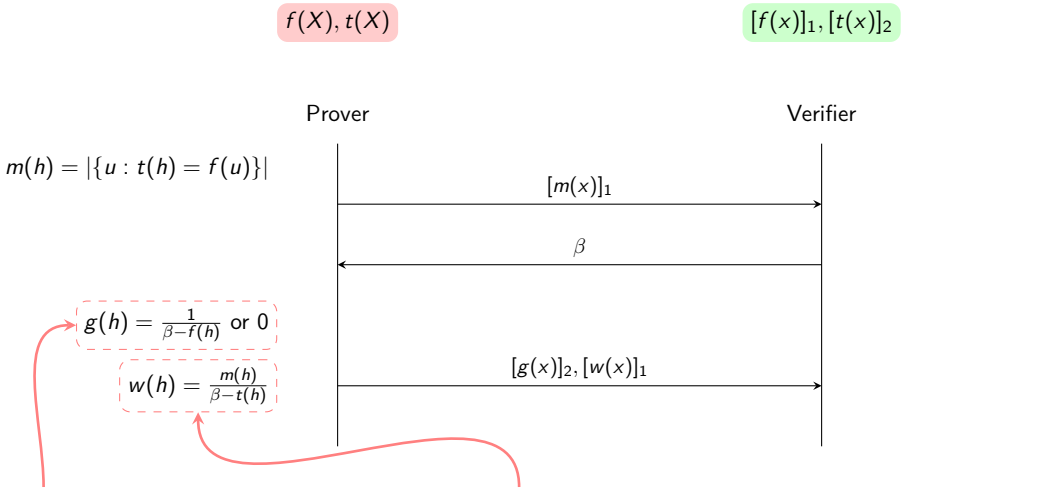
Recall: The cq Lookup Argument



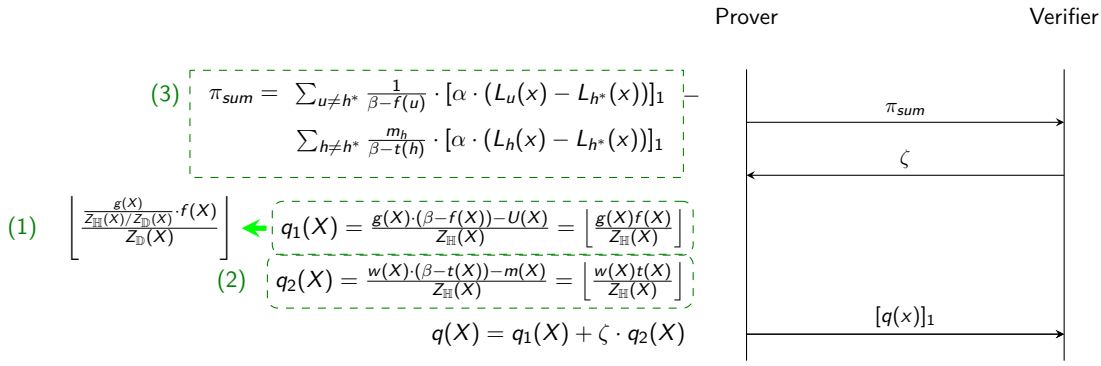
Locq


$\sum_u \frac{1}{\beta - f(u)} = \sum_h \frac{m(h)}{\beta - t(h)}$
Define $g(X), w(X)$
$g(u) = 1 \quad \forall u \in \mathbb{D}$
$g(h) = 0 \quad \forall h \in \mathbb{H} \backslash \mathbb{D}$
$\sum_h g(h) = \sum_h w(h)$
$\sum_h (g(h) - w(h)) = 0$

Locq


$f(X), t(X)$
$[f(x)]_1, [t(x)]_2$
Prover
Verifier
$m(h) = |\{u : t(h) = f(u)\}|$
$[m(x)]_1$
β
$g(h) = \frac{1}{\beta - f(h)}$ or 0
$w(h) = \frac{m(h)}{\beta - t(h)}$
$[g(x)]_2, [w(x)]_1$
(1) Prove correctness of $g(X)$
(2) Prove correctness of $w(X)$
(3) Prove $\sum(g(h) - w(h)) = 0$

Locq


Prover
Verifier
(3)
$\pi_{sum} = \sum_{u \neq h^*} \frac{1}{\beta - f(u)} \cdot [\alpha \cdot (L_u(x) - L_{h^*}(x))]_1 - \sum_{h \neq h^*} \frac{m_h}{\beta - t(h)} \cdot [\alpha \cdot (L_h(x) - L_{h^*}(x))]_1$
(1)
$\left\lfloor \frac{\frac{g(X)}{Z_{\mathbb{H}}(X)/Z_{\mathbb{D}}(X)} \cdot f(X)}{Z_{\mathbb{D}}(X)} \right\rfloor$
$q_1(X) = \frac{g(X) \cdot (\beta - f(X)) - U(X)}{Z_{\mathbb{H}}(X)} = \left\lfloor \frac{g(X) f(X)}{Z_{\mathbb{H}}(X)} \right\rfloor$
(2)
$q_2(X) = \frac{w(X) \cdot (\beta - t(X)) - m(X)}{Z_{\mathbb{H}}(X)} = \left\lfloor \frac{w(X) t(X)}{Z_{\mathbb{H}}(X)} \right\rfloor$
$q(X) = q_1(X) + \zeta \cdot q_2(X)$
π_{sum}
ζ
$[q(x)]_1$

Locq Verifier

- $$e(\pi_{sum}, [\alpha^{-1}]_2) = e(-[w(x)]_1, [1]_2) \cdot e([1]_1, [g(x)]_2).$$
- $$e(\beta \cdot [1]_1 - [f(x)]_1, [g(x)]_2) \cdot e(\zeta \cdot [w(x)]_1, \beta \cdot [1]_2 - [t(x)]_2) = e([U(x)]_1 + \zeta \cdot [m(x)]_1, [1]_2) \cdot e([q(x)]_1, [Z_{\mathbb{H}}(x)]_2).$$

Efficiency

Scheme	Prep.	Proof Size				Proving Cost	Vrf.	Hom.	ZK.
	$\mathbb{F}+\mathbb{G}_1$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{F}$	#Bits				
Caulk [ZBK+22]	$O(N\log N)$	14	1	4	7168	$O(m^2+m\log(N))(\mathbb{F}+\mathbb{G}_1)$	$4P$	✓	✓✓
Caulk+ [PK22]	$O(N\log N)$	7	1	2	3968	$O(m^2)(\mathbb{F}+\mathbb{G}_1)$	$3P$	✓	✓✓
Flookup [GK22]	$O(N\log^2 N)$	6	1	4	4096	$6m\mathbb{G}_1+m\mathbb{G}_2+O(m\log^2 m)\mathbb{F}$	$3P$	×	×
Baloo [ZGK+22]	$O(N\log N)$	12	1	4	6400	$13m\mathbb{G}_1+m\mathbb{G}_2+O(m\log^2 m)\mathbb{F}$	$5P$	✓	×
cq [EFG22]	$O(N\log N)$	8	-	3	3840	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$5P$	✓	×
cq+ [CFF+23]	$O(N\log N)$	7	-	1	2944	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$5P$	✓	×
cq++ [CFF+23]	$O(N\log N)$	6	-	1	2560	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$6P$	✓	×
cq+* [CFF+23]	$O(N\log N)$	8	-	1	3328	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$5P$	✓	✓
cq++* [CFF+23]	$O(N\log N)$	7	-	1	2944	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$6P$	✓	✓
zkcq+ [CFF+23]	$O(N\log N)$	9	-	1	3712	$8m\mathbb{G}_1+O(m\log m)\mathbb{F}$	$6P$	✓	✓✓
Locq (This work)	$O(N\log N)$	4	1	-	2304	$6m\mathbb{G}_1+m\mathbb{G}_2+O(m\log m)\mathbb{F}$	$4P$	✓	✓✓

Thanks

References I


Matteo Campanelli, Antonio Faonio, Dario Fiore, Tianyu Li, and Helger Lipmaa.
Lookup Arguments: Improvements, Extensions and Applications to Zero-Knowledge Decision Trees, 2023.


Liam Eagen, Dario Fiore, and Ariel Gabizon.
Cq: Cached quotients for fast lookups.
https://eprint.iacr.org/2022/1763, 2022.


Ariel Gabizon and Dmitry Khovratovich.
Flookup: Fractional decomposition-based lookups in quasi-linear time independent of table size.
https://eprint.iacr.org/2022/1447, 2022.

References II


Jim Posen and Assimakis A. Kattis.
Caulk+: Table-independent lookup arguments.
Cryptology ePrint Archive, 2022.
https://eprint.iacr.org/2022/957.


Arantxa Zapico, Vitalik Buterin, Dmitry Khovratovich, Mary Maller, Anca Nitulescu, and Mark Simkin.
Caulk: Lookup Arguments in Sublinear Time.
Technical Report 621, 2022.


Arantxa Zapico, Ariel Gabizon, Dmitry Khovratovich, Mary Maller, and Carla Ràfols.
Baloo: Nearly Optimal Lookup Arguments.
https://eprint.iacr.org/2022/1565, 2022.