Delegating Computation: A New Perspective

Yael Tauman Kalai
Microsoft Research
Interactive proofs

multi-prover interactive proofs

Probabilistically checkable proofs

[All powerful provers!]

[Interactive proofs] [GMR85]

[multi-prover interactive proofs] [BGKW88]

[Probabilistically checkable proofs] [FRS88, FGLSS91, BFLS91, AS92, ALMSS92]
Doubly Efficient Proofs

[GKR08]

Proofs for \textit{poly-time computations}:

- \textit{Prover runtime} \approx \textit{computation runtime}
- \textit{Verifier runtime} \approx |\text{input}|
Doubly Efficient Proofs

[GKR08]

Doubly efficient Interactive proofs for bounded depth

$O(depth)$ rounds
Summary of Delegation Under Standard Assumptions

- [GKR08]: Doubly efficient interactive proofs for bounded depth
- [KR09]: 2-message for bounded depth (under PIR)
- [Ki92, Mi94]: PCP/MIP
- [IKO07, BC12,...]: 4-message for NP (under CRH)
- [KRR14]: no-signaling PCP/MIP = P
- [KRR14]: 2-message for P (under PIR)

Doubly efficient interactive proof or argument

• RAM [KP15]
• Poly PIR [DNR16, BHK17]
• Adaptive security [BHK17]
• Amortized NP delegation [BHK17]
• Quasi-linear runtime, and additive space overhead [HR17]
Doubly efficient Interactive proofs for bounded space

2-message for bounded depth (under PIR)

Doubly efficient Interactive proofs for bounded depth

4-message for NP (under CRH)

PCP/MIP

2-message for P (under PIR)

Doubly efficient Interactive proofs for bounded space

no-signaling

PCP/MIP = P

RAM [KP15]
Poly PIR [DNR16, BHK17]
Adaptive security [BHK17]
Amortized NP delegation [BHK17]
Quasi-linear runtime, and additive space overhead [HR17]
We Will NOT Talk About:

2-message for $NP$ (non-falsifiable assumptions)  

2-message for $P$ ($iO$)  

Delegation in the Preprocessing Model  
Theoretical Results  Implementations

[GKR08] blue-print proved itself useful!

Main drawback: Only useful for low depth

Implementations
[CMT12, TRMP12, Thaler2013, VSBW13, WHGSW16, WJBSTWW17, ZGKPP17]
Today: Use GKR Blueprint Beyond Bounded Depth Delegation

Obtain previous theoretical results using GKR blueprint

Hope:

1. Lead to practical improvements
   Practical delegation for $P$ (and $NP$)

2. Shed light towards theoretical improvements
   2-message delegation for $NP$?
Doubly efficient Interactive proof bounded depth

[Goldwasser-K-Shelat17]

Doubly efficient Interactive argument for \( P \) (and \( NP \)) \((CRH/PIR)\)

[Better efficiency?]

- Simpler?
- \( NP \) ???

K-Rothblum17

no-signaling PCP/MIP = \( P \)

KRR14

2-message for \( P \) \((PIR)\)
Verifier can compute $v_d$ for local correctness:

If $v_d$ is not correct, then whp $v_{d-1}$ is not correct.

[Diagram showing a pentagon with vertices labeled $v_d$, $v_{d-1}$, and $x_1, x_2, x_3, \ldots, x_n$.]
Verifier can compute $v_d$

protocol for local correctness: If $v_{d-1}$ is not correct then whp $v_{d-2}$ is not correct

Verifier can compute $v_{d-1}$

Verifier can compute $v_{d-2}$

Linear ECC

GKR08 Blue Print
Verifier can compute Linear ECC

Verifier can compute Linear ECC

Verifier can compute Linear ECC

protocol for local correctness:
If $v_2$ is not correct then whp $v_1$ is not correct
protocol for **local correctness:**

**Sum-check**

- Verifier runtime \(\text{polylog}(S)\)
- Number of rounds \(\text{polylog}(S)\)
- Prover runtime \(\text{poly}(S)\)

Verifier runtime and communication grows with the depth
Eliminate Depth Restriction in GKR

Idea: Convert computation to low-depth circuit!

Run GKR on squashed circuit!
Verifiable needs to compute linear ECC

$LDE(x, c_1, ..., c_T, out)$
on a single point of his choice!
Squashed GKR

Verifier needs to compute linear ECC

\[ LDE(x, c_1, \ldots, c_T, \text{out}) \]

on a single point of his choice!
Squashed GKR

Verifier needs to compute linear ECC 
\[ LDE(x, c_1, \ldots, c_T, \text{out}) \]
on a single point of his choice!
Squashed GKR

Verifier needs to compute linear ECC

\[ LDE(x, c_1, ..., c_T, \text{out}) \]

on a single point of his choice!
Squashed GKR

[Chunk-K-Liu-Raz11]

Shrinking commitment using $Enc$

$LDE(x, c_1, ..., c_T, \text{out})$

Send the values of $P$ on the line $z \rightarrow z'$

$z' \in F^m$

decommit to $z'$
Squashed GKR

\[ \text{Commit}(LDE(x, c_1, ..., c_T, \text{out})) + \]

Low degree test

Linear ECC

\[ x \quad c_1 \quad c_T \quad \text{out} \]

\[ z' \in F^m \]

decommit to \( z' \)

Send the values of \( P \) on the line \( z \rightarrow z' \)
Soundness of Squashed GKR

Computationally bounded

\( P^* \)

\[ \text{Commit}(LDE(x, c_1, \ldots, c_T, \text{out})) \]

\[ + \]

Low degree test

Linear ECC

\[ x \quad c_1 \quad c_T \quad \text{out} \]

\[ z' \in F^m \]

decommitt to \( z' \)
Soundness of Squashed GKR

\[ LDE(x, \tilde{c}_1, ..., \tilde{c}_T, \tilde{\text{out}}) \]

Soundness is implied by soundness of GKR
Squashed GKR

\[ \text{Commit}(LDE(x, c_1, \ldots, c_T, \text{out})) + \]

Low degree test

Linear ECC

\(O(\log T')\) rounds

Theoretically, inferior to [Ki94], but more efficient

\[ z' \in F^m \]

decommitt to \( z' \)
Squashed GKR

Commit($LDE(x, c_1, ..., c_T, out)$) + Low degree

Linear ECC

$z' \in F^m$
decommit to $z'$

[Goldwasser-K-Shelat...17]
Squashed GKR

2-Message Argument

\[ \text{Commit}(LDE(x, c_1, ..., c_T, out)) \]

Low degree test

\[ r_0 \]
\[ a_0 \]
\[ r_1 \]
\[ a_1 \]
\[ r_\ell \]
\[ a_\ell \]

\[ \ell = O(\log T) \]

GKR on squashed circuit

Soundness?

\[ r_0 \]
\[ r_1 \]
\[ r_1, r_2 \]
\[ r_1, r_2, ..., r_\ell \]

\[ a_0 \]
\[ a_1 \]
\[ a_1, a_2 \]
\[ a_1, a_2, ..., a_\ell \]
Proof Pending

GKR on squashed circuit

Soundness?

Low degree test

$\ell = O(\log T)$

$\text{Commit}(LDE(x, c_1, \ldots, c_T, \text{out}))$

$\text{Commit}(LDE(x, c_1, \ldots, c_T, \text{out}))$

$P \xrightarrow{\text{Commit}(LDE(x, c_1, \ldots, c_T, \text{out}))} P$

$V \xrightarrow{r_0 \ldots r_\ell} V$

$\mathcal{P} \xrightarrow{V} \mathcal{P}$

$\mathcal{V}$

GKR on squashed circuit

$\mathcal{P}$

$\mathcal{V}$
Squashed GKR → 2-Message Argument

Interactive argument with no-signaling soundness

[KR09, KRR13] → Sound
Soundness

Interactive proof

No-signaling PCP/MIP

No-signaling interactive argument

2-message delegation

[KR09]

[KRR14]

[KR09, KRR13]

NP???
Summary

- Doubly efficient Interactive proof bounded depth
  - [GKR08]

- Interactive argument for $P$ with no-signaling soundness ($CRH/PIR$)
  - [Goldwasser-K-Shelat17]

- 2-message for $P$ ($PIR$)
  - [K-Rothblum17]

- More efficient?
- Simpler?
- $NP$???
THANK YOU