Finite state verifiers with both private and public coins

M. Utkan Gezer A.C. Cem Say

Department of Computer Engineering, Boğaziçi University
Bebek 34342, İstanbul, Turkey

ICTCS 2023

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say Department of Computer Engineering, Boğaziçi University, 34342, Istanbul, Turkey

Motivation

- Previously, by [Con89; GKR15]:

$$\mathrm{IP}(\text{log-space}, \text{poly-public-coins}, \text{poly-time}) = \mathrm{P}$$

- Based on this, our main result:

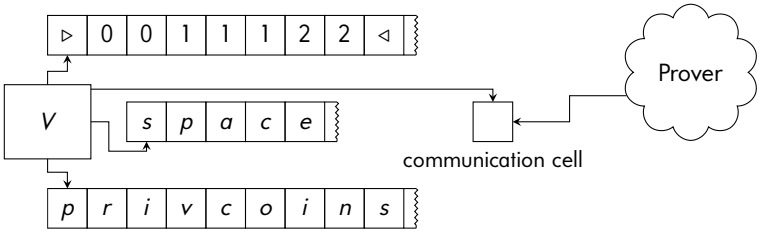
$$\mathrm{IP}(\text{con-space}, \text{con-private-coins}, \text{poly}^*\text{-public-coins}, \text{poly}^*\text{-time}) = \mathrm{P}$$

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey]

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say Department of Computer Engineering, Boğaziçi University, 34342, İstanbul, Turkey

Definitions and notation

- Interactive Proof System
  - Verifier: responsibility and authority to decide membership
  - Prover: interactive advocate of membership
- IP(...-space, ...-private-coins, ...-public-coins, ...-time)
  - Resource budgets of the verifier
  - Absent: unavailable



Definitions and notation

- Interactive Proof System
  - Verifier: responsibility and authority to decide membership
  - Prover: interactive advocate of membership
- $\mathrm{IP}(\ldots\text{-space}, \ldots\text{-private-coins}, \ldots\text{-public-coins}, \ldots\text{-time})$
  - Resource budgets of the verifier
  - Absent: unavailable
- Related examples and **shorthand notations**
  - $\mathrm{IP}(\text{log-space}, \text{poly-public-coins}, \text{poly-time})$

$\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$

  - $\mathrm{IP}(\text{con-space}, \text{con-private-coins}, \text{poly}^*\text{-public-coins}, \text{poly}^*\text{-time})$

$\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

- "*": 'expected budget' — expected consumption should be at most this much

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342, İstanbul, Turkey]

Definitions and notation

- Interactive Proof System
  - Verifier: responsibility and authority to decide membership
  - Prover: interactive advocate of membership
- IP(...-space, ...-private-coins, ...-public-coins, ...-time)
  - Resource budgets of the verifier
  - Absent: unavailable
- Related examples and **shorthand notations**
  - IP(log-space, poly-public-coins, poly-time)

$\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$

  - IP(con-space, con-private-coins, poly*-public-coins, poly*-time)

$\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, *)$

- "*": 'expected budget' — expected consumption should be at most this much

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey]

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say Department of Computer Engineering, Boğaziçi University, 34342, Istanbul, Turkey

Main result

$$\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*) = \text{P}$$

- $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) = \text{P}$ [Con89; GKR15]
- $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) = \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$
  - A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$
  - B) $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{log-space})$

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 İstanbul, Turkey]

Main result

A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

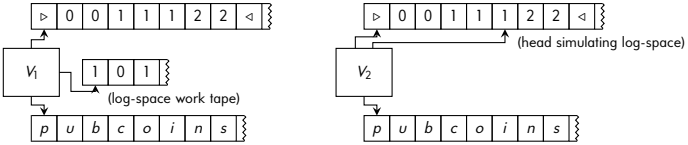
1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$
   [···]
2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$
   [···]

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342, Istanbul, Turkey]

Main result

A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$
   - Direct simulation via encoding $\log(n)$-bit memory into head positions [Har72]
   - $O(n)$ time overhead



2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

[···]

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey]

Main result

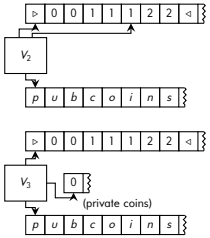
A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$

   [···]

2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

   - Simulate
     1. Pick head i with pr. p_i.
     2. Simulate the 'story' of k heads, tracing and verifying ith head.
     3. Interactivity is passed on.



M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 İstanbul, Turkey]

Main result

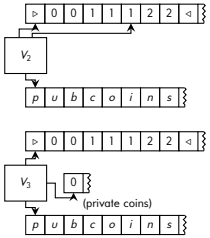
A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$

   [···]

2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

   - Repeat for m rounds:
     - Simulate
       1. Pick head i with pr. p_i.
       2. Simulate the 'story' of k heads, tracing and verifying ith head.
       3. Interactivity is passed on.



M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 İstanbul, Turkey]

Main result

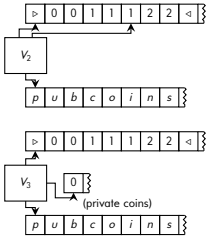
A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$

   [···]

2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

   - Repeat for m rounds:
     - Simulate with pr. $p_{\text{simulation}} = \sum_i p_i$.
       1. Pick head i with pr. p_i.
       2. Simulate the 'story' of k heads, tracing and verifying ith head.
       3. Interactivity is passed on.
     - Time the 'story' with the remaining high pr., p_{timer}. [GS22]



M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey]

Main result

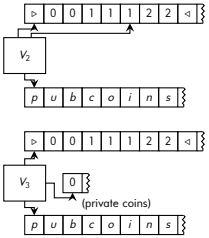
A) $\mathcal{IP}_{\text{pub-ran}}(\text{log-space}) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$

   [···]

2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$

   - Repeat for m rounds:
     - Simulate with pr. $p_{\text{simulation}} = \sum_i p_i$.
       1. Pick head i with pr. p_i.
       2. Simulate the 'story' of k heads, tracing and verifying ith head.
       3. Interactivity is passed on.
     - Time the 'story' with the remaining high pr., p_{timer}. [GS22]
       1. Random walk t times.
       2. Abort and *reject* if all end on $\triangleleft$. Else, repeat.
          - Markov analysis: $O(n^{t+2})$ expected; almost always more than $O(n^{t+1})$



M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, Bebek, 34342, Istanbul, Turkey]

Main result

B) $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{log-space})$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$
   [···]
2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$
   [···]

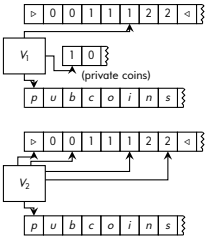
M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342, İstanbul, Turkey]

Main result

B) $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*) \subseteq \mathcal{IP}_{\text{pub-ran}}(\log\text{-space})$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$
   - r random bits $\rightsquigarrow$ 2^r heads to parallelly simulate 2^r probable executions
     - 2^r interactions multiplexed
     - Verify: sims that interacted identically are responded the same
   - t more heads to limit runtime to $O(n^t)$, deterministically
   - Decide by a randomly chosen sim
2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\log\text{-space})$

   [···]

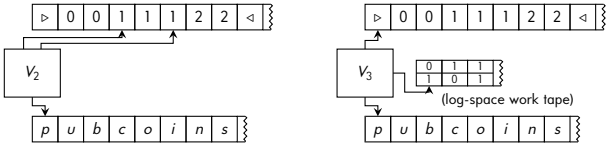


M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey

Main result

B) $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*) \subseteq \mathcal{IP}_{\text{pub-ran}}(\text{log-space})$

1. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, \text{con-private-coins}, ^*)$ to $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$
   [···]
2. $\mathcal{IP}_{\text{pub-ran}}(\text{con-space}, k\text{-head})$ to $\mathcal{IP}_{\text{pub-ran}}(\text{log-space})$
   - Direct simulation by keeping head indices in $\log(n)$-bit memory [Har72]
   - $O(n)$ time overhead, can be improved to $O(n/\log n)$



M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 Bebek, İstanbul, Turkey]

Main result (precise)

$$\mathrm{P} = \mathrm{IP}\big(\text{log-space, poly-public-coins, poly-time}\big) = \mathrm{IP}\big(\text{con-space, con-private-coins, poly}^*\text{-public-coins, poly}^*\text{-time}\big)$$

For any $t > 1$:

A) $$\mathrm{IP}\big(\text{log-space}, O(n^t)\text{-public-coins}, O(n^t)\text{-time}\big) \subseteq \mathrm{IP}\big(\text{con-space, con-private-coins}, O(n^{t+2})^*\text{-public-coins}, O(n^{t+2})^*\text{-time}\big)$$

B) $$\mathrm{IP}\big(\text{con-space, con-private-coins}, O(n^t)^*\text{-public-coins}, O(n^t)^*\text{-time}\big) \subseteq \mathrm{IP}\big(\text{log-space}, O(n^{\lceil t\rceil+1})\text{-public-coins}, O(n^{\lceil t\rceil+1})\text{-time}\big)$$

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say [Department of Computer Engineering, Boğaziçi University, 34342 İstanbul, Turkey]

Side result

$$\mathrm{NC} \subseteq \mathrm{IP}\big(\text{con-space}, \text{con-private-coins}, O(n^4)^*\text{-public-coins}, O(n^4)^*\text{-time}\big)$$

- $\mathrm{NC} \subseteq \mathrm{IP}\big(\log\text{-space}, O(n \log^2 n)\text{-public-coins}, O(n \log^2 n)\text{-time}\big)$ [FL93]
  - Thus, $\mathrm{NC} \subseteq \mathrm{IP}\big(\log\text{-space}, O(n^2)\text{-public-coins}, O(n^2)\text{-time}\big)$
- Result follows from "A)"

M. Utkan Gezer [utkangezer@gmail.com], A.C. Cem Say Department of Computer Engineering, Boğaziçi University, Bebek, 34342, Istanbul, Turkey

References

[Con89] Anne Condon. *Computational Models of Games*. MIT Press, 1989.

[FL93] Lance Fortnow and Carsten Lund. "Interactive proofs and alternating time-space complexity". In: *Theoretical Computer Science* 113 (1993), pp. 55–73.

[GKR15] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. "Delegating Computation: Interactive Proofs for Muggles". In: *J. ACM* 62.4 (Sept. 2015).

[GS22] M. Utkan Gezer and A. C. Cem Say. "Constant-space, constant-randomness verifiers with arbitrarily small error". In: *Information and Computation* 288 (2022), p. 104744.

[Har72] Juris Hartmanis. "On non-determinancy in simple computing devices". en. In: *Acta Informatica* 1.4 (1972), pp. 336–344.