Probabilistic Proof Systems

CS 6230: Topics in Information Security

Lecture 13: Retrospective

Prashant Nalini Vasudevan

Lecture Plan

1. What we saw
2. What we did not see

Non-Classical Proof Systems

- Studied by computer scientists since the 80’s
- New notions of what it means to “prove” something
- Vastly more “powerful” than classical proofs
- We will study some of these along with:
  - their applications,
  - connections to complexity theory and cryptography, and,
  - relevant tools from cryptography and TCS

Interactive Proofs

$$IP = PSPACE$$

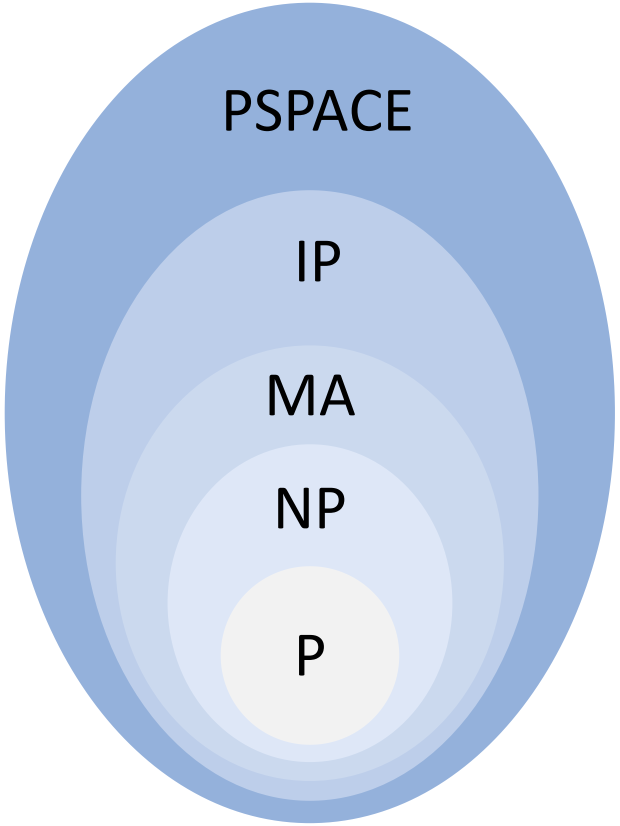
Sumcheck Protocol

Utility of Low-Degree Polynomials

Goldwasser-Sipser Set Lower Bound Protocol

Error Reduction, Round Reduction, etc.

Doubly Efficient IPs, the GKR Protocol, Delegation of Computation



Zero-Knowledge Proofs

Simulation-based definition

CZK for NP using commitments

SZK and distances between distributions

Completeness of the Statistical Closeness problem

Closure properties of SZK

Probabilistically Checkable Proofs

Definition with Proof oracle

Relation to IPs

The PCP Theorem

Hardness of Approximation

Hadamard PCP for systems of linear (and quadratic) equations

Linearity Testing

Arguments

Definition of Computational Soundness

Kilian's Construction of Succinct Arguments from PCPs

Collision-resistance and Merkle Hashing

Fiat-Shamir transformation to non-interactive arguments

Schnorr Identification (and Signature) Scheme using Discrete Log

Proof of Knowledge

Arguments

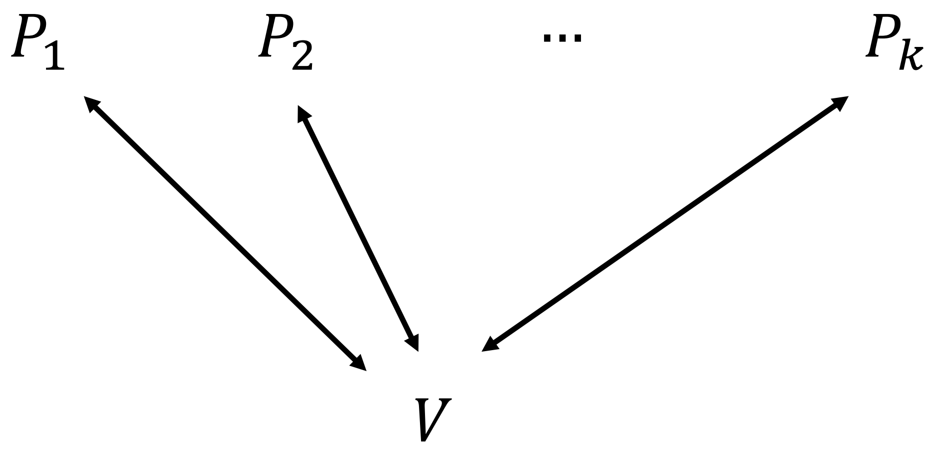
(See Justin Thaler's survey)

Information-Theoretic Proof System	+	Cryptography	$\xrightarrow{\text{Fiat-Shamir}}$	Succinct Non-Interactive Argument of Knowledge (SNARK)
PCP	+	Cryptographic Hash Functions		
IP Multi-Prover IP Interactive Oracle Proof	+	Polynomial Commitment Scheme		
Linear PCP	+	Homomorphic Encryption / Pairing-Based Cryptography		

Multi-Prover IP

[BenOr-Goldwasser-Kilian-Wigderson 88]

(no communication among P_i's)



Usual completeness and soundness requirements

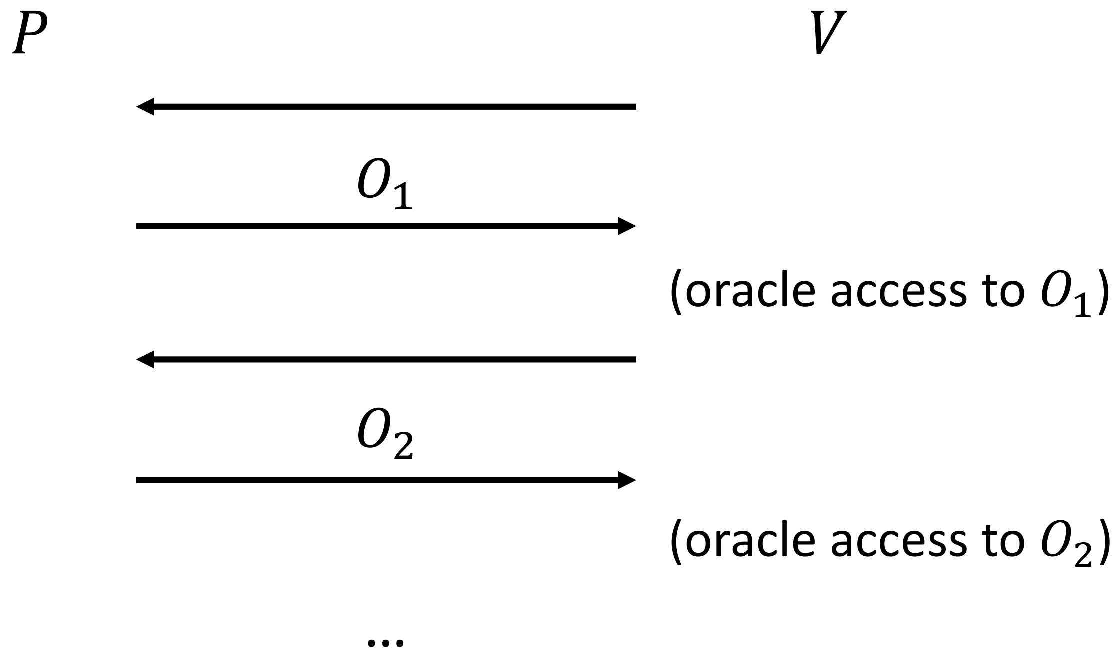
Can always decrease to two provers

Straightforward connection to PCPs

$$MIP = NEXP$$

Interactive Oracle Proof

[BenSasson-Chiesa-Spooner 16, Reingold-Rothblum-Rothblum 16]



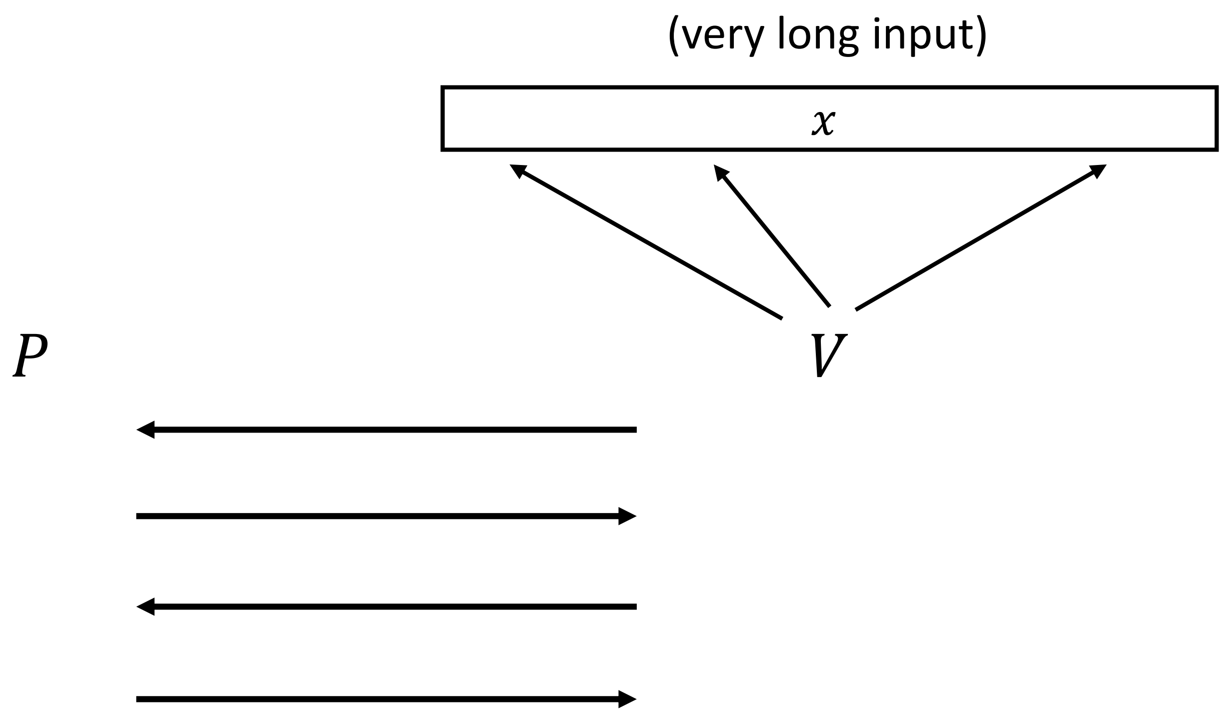
Usual completeness and soundness requirements

Generalisation of IPs and PCPs

Not natural, but useful for constructing SNARKs

Proof of Proximity

[Ergun-Kumar-Rubinfeld 04, Rothblum-Vadhan-Wigderson 13]



V runs in sub-linear time in $|x|$

Completeness: Accept if $x \in L$

Soundness: Reject if x is *far from* every $x' \in L$

Without a prover, called $property\ testing$
Eg: linearity testing, low-degree testing

Useful in constructing PCPs, IOPs

Batch Verification

[Ergun-Kumar-Rubinfeld 04, Rothblum-Vadhan-Wigderson 13]

Suppose L has IP with c bits of communication

How much communication needed to prove $x_1, \ldots, x_k$ are *all* in L?

Repeat IP k times: $k \cdot c$

Use $IP = PSPACE$: $c \cdot polylog(k)$
(but loses any interesting properties of original IP)

[RRR16,RR20]: Batching for UP while preserving prover efficiency

[KRRSV20,KRV21]: Batching for non-interactive SZK while preserving zero-knowledge

Entropy Difference

Another complete problem for SZK

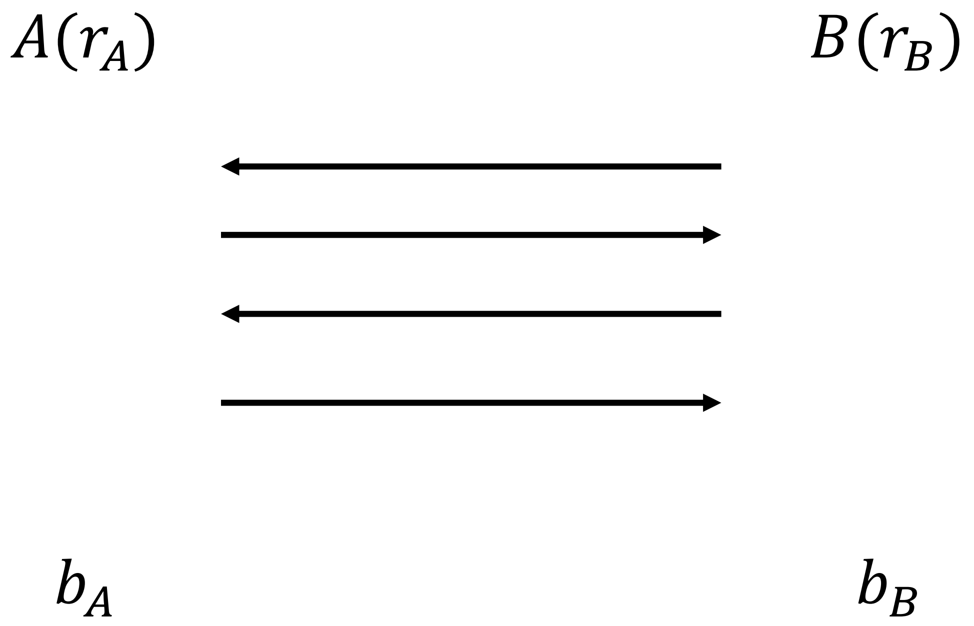
For circuit $C: \{0,1\}^m \to \{0,1\}^n$,
$H(C)$ - Shannon entropy of distribution of outputs on uniformly random input

Given C_0, C_1 such that $|H(C_0) - H(C_1)| > 1$,
decide whether $H(C_0) > H(C_1)$ or other way round

Reduces to Statistical Closeness using the Leftover Hash Lemma

Proof of completeness similar to what we saw for SC

Coin-Tossing Protocols



Agreement: When A and B are both honest,
$b_A = b_B$, distributed uniformly

Unbiasable: Irrespective of what B does,
b_A is almost uniform
(and vice versa)

Useful, e.g., in transforming public-coin HVZK proofs to malicious verifier ZK proofs

Many different notions of security studied,
Various constructions, impossibilities known

So Much More…

Secure Multi-Party Computation

Non-blackbox simulation in ZK proofs

Correlation Intractability and recent developments in the Fiat-Shamir methodology

In Conclusion

- Randomness and interaction are powerful
- Polynomials are amazing
- You never know what could be practical in twenty years