TEST BILD

PROBABILISTIC PROOF SYSTEMS

by

Oded GOLDREICH
WEIZMANN INSTITUTE
ISRAEL

www.wisdom.weizmann.ac.il/~oded/

pps.html
cc.html foc.html

Before going to probabilistic proof systems, let's review the traditional/deterministic ones

BACKGROUND: NP

- PROOF SYSTEM = VERIFICATION PROCEDURE
- EFFICIENT COMPUTATION
  = POLYNOMIAL-TIME (IN LEN' OF ASSERT')
- NP-PROOF SYSTEM
  = POLY-TIME VERIFICATION PROC'

E.G., G3C $\triangleq$ SET OF 3-COLORABLE GRAPHS.

ASSERTION: "$G(V,E) \in G3C$"

PROOF: $\varphi: V \to \{1,2,3\}$ ("NP-WITNESS")

VERIFICATION: FOR EVERY $(u,v) \in E$
VERIFY $\varphi(u) \neq \varphi(v)$

$S \in NP$ IF EXISTS POLY-TIME ALG', V, S.T.

(Completeness & soundness)

$x \in S \Leftrightarrow \exists \pi \; V(x,\pi) = 1$

$(x \notin S \Rightarrow \forall \pi \; V(x,\pi) \neq 1)$

↳ } completeness & soundness

→ ~~Why~~ Prob. Proof systems ? ("contraventrale")
— Because they are more powerful and yield results/phenomena not existing otherwise (in

PROBABILISTIC PROOF SYSTEMS: COMMON THEME

- EFFICIENT VERIFICATION (AS IN NP-PROOFS).
- PROBABILISTIC VERIFICATION PROCEDURE
  - "VERIFIER" TOSSES COINS, AND
  - "RULES BY STATISTICAL EVIDENCE".

  ⇒ ERROR PROB'
- ERROR PROBABILITY
  - EXPLICITLY BOUNDED
  - REDUCIBLE BY SUCCESIVE APPLICATIONS
- TYPES

  IP = INTERACTIVE PROOFS

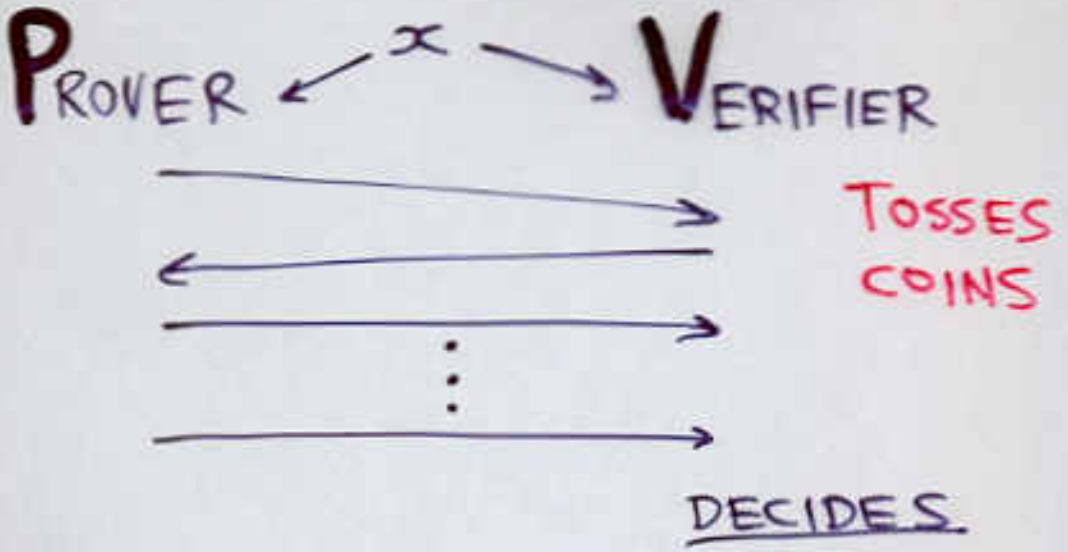
  ZK = ZERO-KNOWLEDGE PROOFS

  PCP = PROBABILISTICALLY CHECKABLE PROOFS

  MULTI-PROVER INTERACTIVE PROOFS (MIP).
  COMPUTATIONALLY-SOUND PROOFS.

AND others that did not fit the slide, like
- proof of knowledge
- NIZK

INTERACTIVE PROOFS – DEFINITION [GMR]



- VERIFIER RUNS IN (PROB') POLY(|x|)-TIME.
- PROVER IS COMPUTATIONALLY UNBOUNDED.
- COMPLETENESS (FOR S)

  $x \in S \Rightarrow \exists$ PROVER STRATEGY P

  $\text{PROB}(V \text{ ACC}') = 1$

- SOUNDNESS (FOR S)

  $x \notin S \Rightarrow \forall$ PROVER STRATEGY P

  $\text{PROB}(V \text{ ACC}') \leq \frac{1}{2}$

INTERACTIVE PROOF FOR S

INTERACTIVE PROOF FOR GRAPH NON-ISOMORPHISM [GMW]

- $G_1(V,E_1)$ & $G_2(V,E_2)$ ARE <u>ISOMORPHIC</u> IF

  $\exists \varphi: V \xrightarrow{1\text{-}1} V$ S.T. $(u,v) \in E_1 \Leftrightarrow (\varphi(u), \varphi(v)) \in E_2$

- INTERACTIVE PROOF FOR $G_1 \not\cong G_2$

  <u>VERIFIER</u>: $i \in_R \{1,2\}$

  H IS <u>RANDOM</u> ISOMORPHIC TO G_i

  <u>SEND</u> H TO PROVER.

  <u>PROVER</u>: FIND j S.T. $H \cong G_j$ (UNIQUE IFF $G_1 \not\cong G_2$)

  <u>SEND</u> j TO VERIFIER.

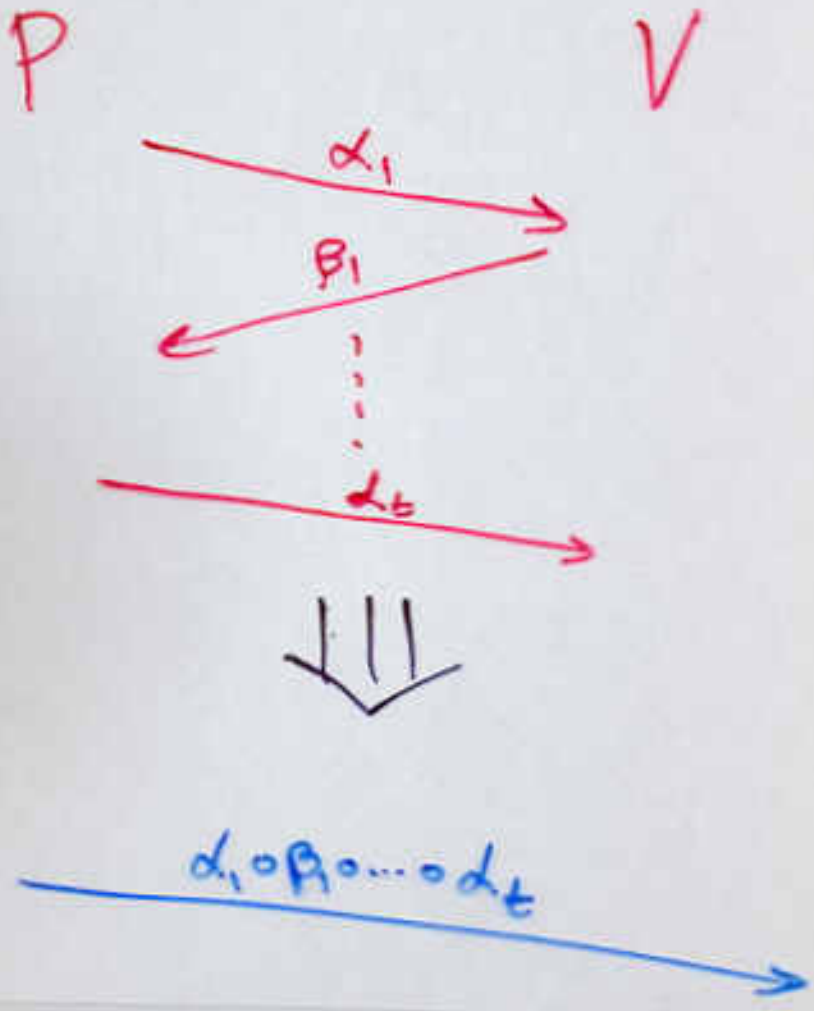
  <u>VERIFIER</u>: ACCEPT IFF $i = j$.

- IF $G_1 \not\cong G_2$ THEN $\text{PROB}(V \text{ ACC}') = 1$
- IF $G_1 \cong G_2$ THEN $\text{PROB}(V \text{ ACC}') \leq \frac{1}{2}$
- **NO NP-PROOF KNOWN.**

2nd mysterd (interaction)
Does not buy anything without RND

INTERACTIVE PROOFS WITHOUT RANDOMNESS

CLAIM: IF S HAS AN INTERACTIVE PROOF WITH A DETERMINISTIC VERIFIER THEN $S \in NP$.



MORAL: NO POINT TO LISTEN TO WEAK & PREDICTABLE CREATURES...

→ This, is NP-pro

TURNS OUT THAT I.P. IS VERY POWERFUL
AND CAN PROVE MEM' IN ANY PSPACE-S

THE POWER OF INTERACTIVE PROOFS [LFKN, S]

THM: $IP = PSPACE$

$\Longrightarrow$ $coNP \subseteq IP$

E.G. INTERACTIVE PROOF FOR SHOWING THAT A GRAPH IS NOT 3-COLORABLE.

WIDELY BELIEVED THAT $coNP \neq NP$

$\Rightarrow$ NO NP-PROOFS FOR NON-3-COLORABILITY.

$S \in coNP \iff \bar{S} \in NP$

PSPACE $\cong$ SETS DECIDABLE BY ALGORITHMS WITH POLYNOMIAL WORK SPACE.

Recall, ips allows to prove membership in more sets.
But do they also allow to prove it "more efficiently"?

IP: Some Recent Developments

[GVW] Evidence that (in general)

INTERACTIVE PROOFS CANNOT PROVIDE REDUCTION IN TOTAL PROOF LENGTH (OVER TRADITIONAL/NP PROOFS).

- TOTAL PROOF LEN. $\triangleq$ # BITS SENT BY THE PROVER.
- IN GENERAL $\triangleq$ Say, for NPC SETS.
- Evidence $\triangleq$ O.W., NP $\subseteq$ coAM[subexp]

STRONGER evidence for STRONGER REDUCTION.

e.g., #BITS = $\alpha(l)$ $\Rightarrow$ NP $\subseteq$ coAM/coNP.

ZERO-KNOWLEDGE PROOFS – DEFINITION [GMR]

AN INTERACTIVE PROOF IS ZERO-KNOWLEDGE IF WHATEVER THE VERIFIER CAN COMPUTE AFTER INTERACTING WITH THE PROVER CAN BE COMPUTED FROM THE ASSERTION ITSELF.

P IS ZERO-KNOWLEDE (ON S) IF

$\forall$ PROB' POLY-TIME V^* (A VERIFIER STRATEGY)

$\exists$ PROB' POLY-TIME M^* ("SIMULATOR")

S.T. $\{\langle P, V^* \rangle(x)\}_{x \in S} \overset{c}{\equiv} \{M^*(x)\}_{x \in S}$

$\{A(x)\} \overset{c}{\equiv} \{B(x)\}$ MAY BE

- EQUALITY
- STATISTICAL CLOSENESS
- COMPUTATIONAL INDISTINGUISH'

$\{A(x)\} \overset{c}{\equiv} \{B(x)\}$ ARE COMP' INDIST' IF $\forall$ EFFICIENT D

$$\text{PROB}(D(A(x))=1) \approx \text{PROB}(D(B(x))=1)$$

ZERO-KNOWLEDGE PROOF OF 3-COLORABILITY [GMW]

- $G(V,E)$ IS 3-COLORABLE IF $\exists \varphi: V \to \{1,2,3\}$ S.T. $\forall (u,v) \in E \quad \varphi(u) \neq \varphi(v)$
- ZKIP FOR 3-COLORABILITY OF $G(V,E)$

SUPPOSE φ IS A 3-COLORING OF G.

Repeat $O(|E|)$ times

PROVER: $\pi \in_R Sym(\{1,2,3\})$

COLOR G USING $\pi \circ \varphi(\cdot)$

PUT IN "SEALED BOXES" AND SEND TO V'

VERIFIER: SEND $(u,v) \in_R E$ TO PROVER.

PROVER: SEND KEYS TO BOXES u AND v.

VERIFIER: OPEN BOXES u AND v

AND CHECK THEY CONTAIN DIFFERENT COLORS $\in \{1,2,3\}$.

- G IS 3-COLORABLE $\Rightarrow$ V NEVER REJECTS
- G IS NOT 3-COLOR' $\Rightarrow$ V REJECT W.P $\geq \frac{1}{|E|}$
- SIMULATION IN ABSTRACT SETTING AND IN "REALITY".

THE POWER OF ZERO-KNOWLEDGE PROOFS [GMW]

THM [N,HILL]: IF ∃ ONE-WAY FUNCTIONS (E.G. IF "FACTORING") THEN "BOXES" CAN BE IMPLEMENTED.

THM [GMW]: (IF ∃ ONE-WAY FUNCTIONS THEN) $\forall S \in NP$ HAS A ZERO-KNOWLEDGE PROOF SYSTEM.

COR [GMW]: CAN "FORCE" (ALL) PARTIES IN PROTOCOLS TO FOLLOW THE PROTOCOL. (OR GET DETECTED).

THM [IY, B+6]: (IF ∃ ONE-WAY FUNCTIONS THEN)

$$ZKIP = IP.$$

RAND' ESS to power of ZK

ZERO-KNOWLEDGE WITHOUT RANDOMNESS

THM [GO]: IF S HAS A ZKIP WITH EITHER DETER' VERIFIER OR DETERMINIST' PROVER THEN $S \in BPP$.

(BPP = DECIDABLE IN PROB' POLY-TIME)

OBSERVE, EVERY $S \in BPP$ HAS A TRIVIAL ZKIP IN WHICH THE PROVER SENDS NOTHING (AND THE VERIFIER DECIDES BY ITSELF).

THUS, RANDOMNESS IS ESSENTIAL TO USEFULNESS OF ZERO-KNOWLEDGE.

ZK: Some Recent Developments

- CONCURRENT COMPOSITION
  - $\tilde{O}(\log n)$-ROUND PROTOCOLS (PROVEN ZK via BB simulation). [RK] [KP] [PRS]
  - $\tilde{\Omega}(\log n)$-ROUND ARE REQUIRED FOR BB SIMULATION OF CONC. ZK. [CKPR]

- USING the ADV's STRATEGY in the proof of SECURITY
  - Black-Box use of ADV's strategy is A SIGNIFICANT RESTRICTION!!!

$\Leftrightarrow$ $BBZK \subsetneq ZK$ [B]

↳ interesting cases!

e.g. $o(1)$-ROUND AM ARG.

& "BOUNDED CONC.-ZK"

$o(1)$-ROUND ZK THAT WITHSTAND n CONC. COMPOSITION

PROBABILISTICALLY CHECKABLE PROOFS [BGKW, FRS]

- VERIFIER IS PROB' POLY-TIME W/ ACCESS TO ORACLE.
- COMPLETENESS (FOR S')

$$x \in S' \Rightarrow \exists \Pi \quad \text{PROB}[V^{\Pi}(x)=1] = 1$$

- SOUNDNESS (FOR S')

$$x \notin S \Rightarrow \forall \Pi \quad \text{PROB}[V^{\Pi}(x)=1] \leq \frac{1}{2}$$

} PCP FOR S

- ADDITIONAL COMPEXITY MEASURES [FGLSS]
  - RANDOMNESS (# COINS TOSSED BY VERIFIER)
  - QUERY COMPLEX' (# QEURIES BY VERIFIER)
- NOTATION [AS]: $PCP(r(\cdot), q(\cdot))$

$r(\cdot)$: RANDOMNESS COMPLEXITY

$q(\cdot)$: QUERY COMPLEX'

THE POWER OF PCP [BFL, BFLS, FGLSS, AS, ALMSS]

THM: $NP = PCP(\alpha \log n), O(1))$

SIGNIFICANCE: $(\varphi, \pi) \rightleftharpoons (\varphi, \pi')$

- (φ, π): ASSERTION, NP-PROOF
- $\rightleftharpoons$: EFFICIENT TRANSFORM'
- (φ, π'): NP-PROOF W/ TRADE-OFF

TRADE-OFF BETWEEN

- CONFIDENCE (ERROR PROB' $\leq \varepsilon$)
- # QUERIES (HERE, $O(\log 1/\varepsilon)$) (+RANDOM)

e Application of TRANS. to "Robust NP-proofs" is its relation to approximation

PCP & APPROXIMATION

RECALL. **THM: $NP \subseteq PCP(O(\log n), 3)$**

IF $\varphi \in SAT$ THEN $\exists \Pi$

IF $\varphi \notin SAT$ THEN $\forall \Pi$

$V^{\Pi}_{r}(\varphi)$ IS A FUNCTION, $f_{\varphi, r}$, OF _ BITS IN Π.

Let $\Pi = \Pi_1, \ldots, \Pi_m$ $\quad \Pi_i \in \{0,1\}$

$$\varphi \longrightarrow \bigwedge_{r} f_{\varphi,r}(\Pi_{i_{R,1}}, \Pi_{i_{R,2}}, \Pi_{i_{R,3}}) \triangleq \varphi'$$

r COINS

FURTHERMORE, CAN BE WRITTEN IN 3CNF WITH 4 CLAUSES.

$\varphi \in SAT \rightarrow \varphi'$ IS SATISFIABLE

$\varphi \notin SAT \rightarrow \forall$ ASSIGN. TO Π SATISFIES $\leq 1 - \frac{1}{2} \cdot \frac{1}{4}$ OF CLAUSES OF φ'

RATIO 7/8

$\Rightarrow$ MAX3SAT IS HARD TO APPROX TO FACTOR 7/8

e Application of "Robust NP-proofs" is its relation to approximation

PCP & APPROXIMATION

RECALL. **THM: $NP \subseteq PCP(O(\log n), 3)$**

IF $\varphi \in SAT$ THEN $\exists \Pi$ $\quad \text{PROB}_R[V^{\Pi}_R(\varphi) = 1] = 1$

IF $\varphi \notin SAT$ THEN $\forall \Pi$ $\quad \text{PROB}_R[V^{\Pi}_R(\varphi) = 1] < \frac{1}{2}$

$V^{\Pi}_R(\varphi)$ IS A FUNCTION, $f_{\varphi,R}$, OF _ BITS IN Π.

Let $\Pi = \Pi_1, \ldots, \Pi_m$ $\quad \Pi_i \in \{0,1\}$

$$\varphi \longrightarrow \bigwedge_{R \text{ COINS}} f_{\varphi,R}(\Pi_{i_{R,1}}, \Pi_{i_{R,2}}, \Pi_{i_{R,3}}) \equiv \varphi'$$

FURTHERMORE, CAN BE WRITTEN IN 3CNF WITH 4 CLAUSES.

$\varphi \in SAT \rightarrow \varphi'$ IS SATISFIABLE

$\varphi \notin SAT \rightarrow \forall$ ASSIGN. TO Π SATISFIES $\leq 1 - \frac{1}{2} \cdot \frac{1}{4}$ OF CLAUSES OF φ'

RATIO 7/8

$\Rightarrow$ MAX3SAT IS HARD TO APPROX TO FACTOR 7/8

One Application of TRANS. to "Robust NP-proofs" is its relation to approximation

PCP & APPROXIMATION

RECALL. **THM: $NP \subseteq PCP(O(\log n), 3)$**

IF $\varphi \in SAT$ THEN $\exists \Pi$ $\quad |\{\underline{r} : V^{\Pi}_{\underline{r}}(\varphi) = 1\}| = \text{POLY}(|\varphi|)$

IF $\varphi \notin SAT$ THEN $\forall \Pi$ $\quad |\{\underline{r} : V^{\Pi}_{\underline{r}}(\varphi) = 1\}| < \frac{1}{2} \cdot \text{POLY}(|\varphi|)$

$V^{\Pi}_{\underline{r}}(\varphi)$ IS A FUNCTION, $f_{\varphi,\underline{r}}$, OF 3 BITS IN Π.

Let $\Pi = \Pi_1, \ldots, \Pi_m$ $\qquad \Pi_i \in \{0,1\}$

$$\varphi \longrightarrow \bigwedge_{\underline{r}\ \text{CONS}} f_{\varphi,r}(\Pi_{i_{r,1}}, \Pi_{i_{r,2}}, \Pi_{i_{r,3}}) \equiv \varphi'$$

FURTHERMORE, CAN BE WRITTEN IN 3CNF WITH 4 CLAUSES.

$\varphi \in SAT \rightarrow \varphi'$ IS SATISFIABLE

$\varphi \notin SAT \rightarrow \forall$ ASSIGN. TO Π SATISFIES $\leq 1 - \frac{1}{2} \cdot \frac{1}{4}$ OF CLAUSES OF φ'

RATIO 7/8

$\Rightarrow$ MAX3SAT IS HARD TO APPROX TO FACTOR 7/8

None of this is possible without RANDOMIZATION

PCP WITHOUT RANDOMNESS

$$PCP(0, q(\cdot)) \subseteq DTIME(poly(n) \cdot 2^{q(n)})$$

E.G., $PCP(0, \log n) = P$

- $NP \subseteq DTIME(2^n)$ IS "UNLIKELY".

(THUS, $NP \subseteq PCP(0, n)$ IS "UNLIKELY")

PCP: Some Recent Developments

How long should PCPs be?

Simple ANSWER: log. RANDOM. $\Rightarrow$ poly. LENGTH

Can we have linear length?

ANS: "ALMOST" [PS, GS+BSVW, BGHSV]

PCP: Some Recent Developments

How long should PCPs be?

Simple ANSWER: log. RANDOM. $\Rightarrow$ poly. LENGTH

Can we have linear length?

ANS: "ALMOST" [PS, GS+BSVW, BGHSV]

[PS]-"almost" $\triangleq$ $n^{1+1/o(q)}$ for q QUERIES

[GS+ BSVW]-"almost" $\triangleq$ $n \cdot 2^{\sqrt{\log n}} = n^{1+o(1)}$ (FOR 20 QUERIES)

[BGHSV]-"almost" $\triangleq$ $\begin{cases} n \cdot 2^{(\log n)^{1/o(q)}} & \text{for } q \text{ QUE.} \\ n \cdot 2^{(\log g n)^2} & \text{for } \log g = Q. \end{cases}$

CONJ: CAN GET $n \cdot \text{poly}(\log n)$ W. $O(1)$ QUE.

OPEN

Probladh → HARSHA

CONCLUSION

PROBABILISTIC PROOF SYSTEMS OFFER ADVANTAGES OVER DETERMINISTIC PROOF SYSTEMS.

A PRICE, HOWEVER, EXISTS :-

ERROR PROBABILITY

BUT, ERROR

- IS EXPLICITLY BOUNDED
- CAN BE REDUCED BY REPETIONS

http://wisdom.weizmann.AC.IL/~oded/pps.html