

Recall From Last Time

Factoring natural numbers $\in \mathbf{NP} \cap \mathbf{co-NP}$

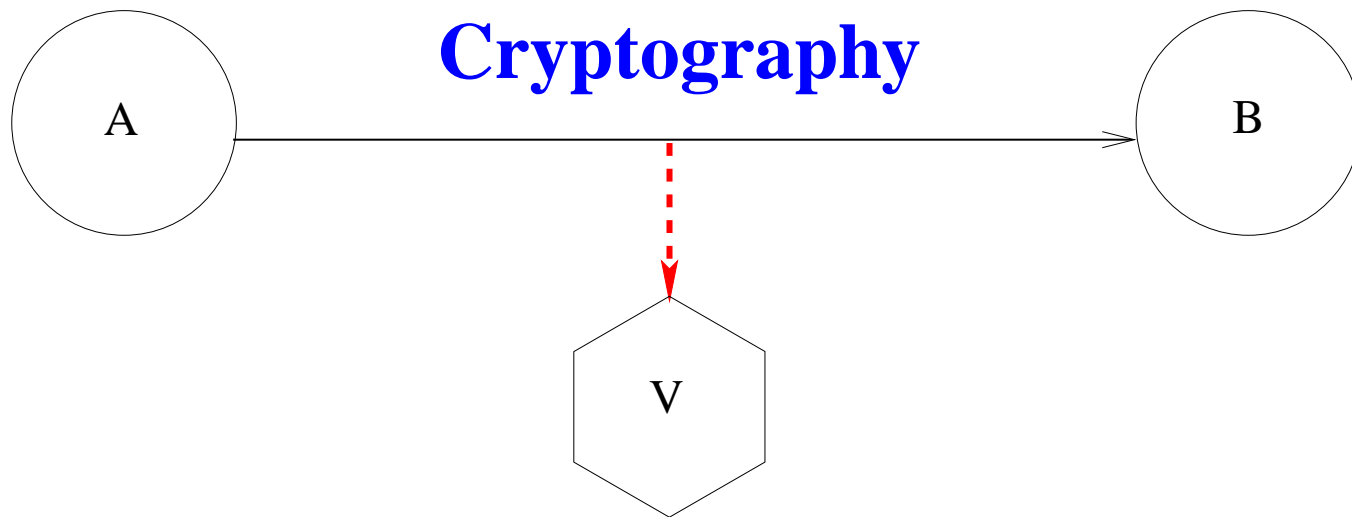
Definition of **BPP** and **BPL**

Thm: $\mathbf{PRIME} \in \mathbf{BPP}$

Thm: $\mathbf{UREACH} \in \mathbf{BPL}$

New Results:

- $\mathbf{PRIME} \in \mathbf{P}$ [Agrawal, Kayal, and Saxena, 2002]
- $\mathbf{UREACH} \in \mathbf{L}$ [Reingold, 2004]



One-Time Pad: $p \in \{0, 1\}^n$; $m \in \{0, 1\}^n$

$$E(p, x) = p \oplus x$$

$$D(p, x) = p \oplus x$$

$$D(p, E(p, m)) = p \oplus (p \oplus m) = m$$

One-Time Pad, Continued

p	0	1	1	0	0	1	0	1	0	1
m	0	0	0	0	1	1	1	1	0	0
$E(p, m)$	0	1	1	0	1	0	1	0	0	1
$D(p, E(p, m))$	0	0	0	0	1	1	1	1	0	0

Thm: If p is chosen at random and known only to A and B
Then $E(p, m)$ provides no information to E about m
except perhaps its length.

Better not use p more than once!

Public-Key Cryptography

Idea: [Diffie, Hellman, 1976] Using computational complexity, I may be able to publish a key for sending secret messages to me, that are intractable to decode. Example: Diffie-Hellman key exchange.

Realization: [Rivest, Shamir, Adleman, 1976] This is the Public-Key Algorithm that is used today in the SSL algorithm that lets your browser generate a key to send an order to Amazon.com without, **we believe**, divulging any **useful** information about your credit card number, or what you bought.

RSA

B chooses p, q n -bit primes, e , s.t. $\text{GCD}(e, \varphi(pq)) = 1$;

B publishes: pq, e ; keeps p, q secret.

Using Euclid's algorithm, B computes d, k , s.t.

$$ed + k\varphi(pq) = 1 \quad [\varphi(pq) = (p - 1)(q - 1)].$$

[Break message into pieces shorter than $2n$ bits]

$$\begin{aligned} E_B(x) &\equiv x^e \pmod{pq} \\ D_B(x) &\equiv x^d \pmod{pq} \\ D_B(E_B(m)) &\equiv (m^e)^d \pmod{pq} \\ &\equiv m^{1-k\varphi(pq)} \pmod{pq} \\ &\equiv m \cdot (m^{\varphi(pq)})^{-k} \pmod{pq} \\ &\equiv m \pmod{pq} \\ &\equiv E_B(D_B(m)) \pmod{pq} \end{aligned}$$

For sufficiently large n , [$n \geq 300$ bits is fine in 2005],

It is widely believed that: $E_B(m)$ divulges no useful information about m to anyone not knowing p, q , or d .

Message signing:

Let $m = "B \text{ promises to give } A \text{ } \$10 \text{ by } 5/17/05."$

Let $m' = m \circ r$ where r is nonce or current date and time

It is widely believed that: $D_B(m')$ could be produced only by B . Thus it can be used as a contract signed by B .

Useful for proving authenticity

Interactive Proofs

[Goldwasser, Micali, Rackoff], [Babai]

Decision problem: D ; input string: x

Two players:

Prover — Merlin is computationally all-powerful. Wants to convince **Verifier** that $x \in D$.

Verifier — Arthur: probabilistic polynomial-time TM. Wants to know the truth about whether $x \in D$.

Def: $D \in \mathbf{IP}$ iff there is a PTIME interactive protocol

1. If $x \in D$, then there exists a strategy for **M**

$$\text{Prob}\{\mathbf{A} \text{ accepts } x\} > \frac{2}{3}$$

2. If $x \notin D$, then for all strategies for **M**

$$\text{Prob}\{\mathbf{A} \text{ accepts } x\} < \frac{1}{3}$$

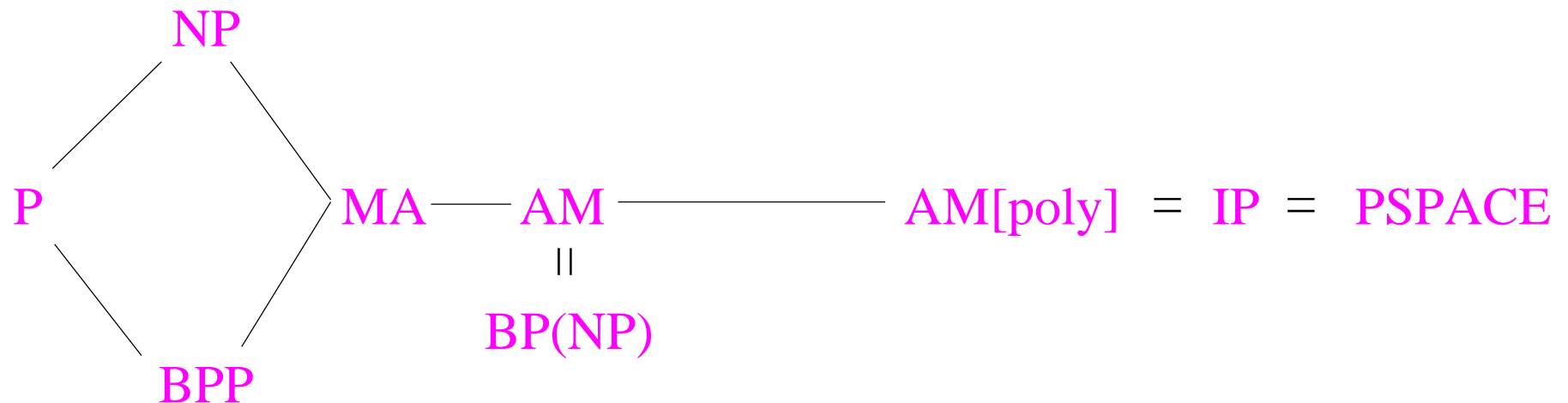
Observation: As for **BPP**, by iterating we can make probability of error exponentially small.

Def: **MA** is the set of decision problems admitting two step proofs where Merlin moves first.

AM is the set of decision problems admitting two step proofs where Arthur moves first. For $k \geq 2$,

$$\mathbf{AM}[k] = \underbrace{\mathbf{AMA} \cdots}_{k} \quad \square$$

Fact: [Babai] For all $k \geq 2$, $\mathbf{AM}[k] = \mathbf{AM}$.



Fact: [Goldwasser & Sipser] The power of interactive proofs is unchanged if **M** knows **A**'s coin tosses. For all k ,

- $\mathbf{IP}[k] = \mathbf{AM}[k]$

- $\mathbf{IP} = \mathbf{AM}[n^{O(1)}]$

Graph Isomorphism \in NP; Is it in co-NP?

Input = G_0, G_1 , $n = \|G_0\| = \|G_1\|$

0. **A** has G_0, G_1 **M** has G_0, G_1
1. flip $\kappa : \{1, \dots, r\} \rightarrow \{0, 1\}$
flip $\pi_1, \dots, \pi_r \in S_n$
 $\pi_1(G_{\kappa(1)}), \dots, \pi_r(G_{\kappa(r)}) \longrightarrow$
2. $\longleftarrow m_2 \in \{0, 1\}^r$
3. accept iff $\kappa = m_2$

Prop: Graph Isomorphism \in co-AM

Proof: If $G_0 \not\cong G_1$, then **A** will accept with probability 1.

If $G_0 \cong G_1$, then **A** will accept with probability $\leq 2^{-r}$. □

Shamir's Thm: $\mathbf{IP} = \mathbf{PSPACE}$

Rough idea of proof that $\mathbf{PSPACE} \subseteq \mathbf{IP}$:

Suffices to show that $\mathbf{QSAT} \in \mathbf{IP}$.

Let input to \mathbf{QSAT} be: $\varphi \equiv \exists x_1 \forall x_2 \cdots \exists x_{n-1} \exists x_n (\alpha)$

Arithmetize to equivalent: α' a polynomial of low degree

$$\varphi' \equiv \exists x_1 \in \mathbf{Z} \forall x_2 \in \mathbf{Z} \cdots \exists x_{n-1} \in \mathbf{Z} \exists x_n \in \mathbf{Z} (\alpha'(\bar{x}) = 0)$$

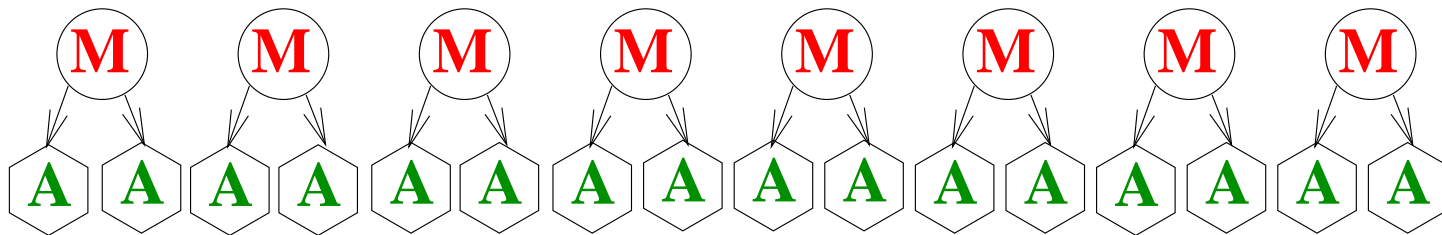
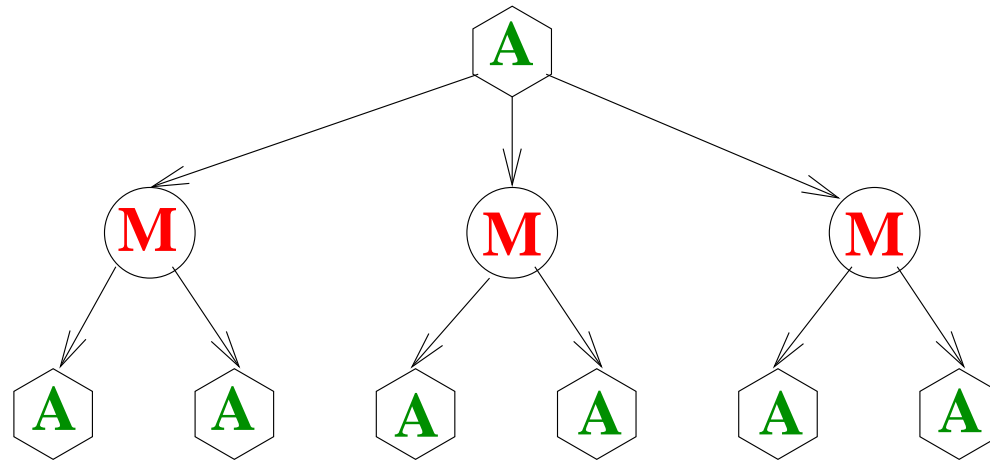
\mathbf{A} chooses prime, p ; \mathbf{M} must show in $\mathbf{Z}/p\mathbf{Z}$:

$$\exists x_1 \forall x_2 \cdots \exists x_{n-1} \exists x_n (\alpha'(\bar{x}) \equiv 0 \pmod{p})$$

\mathbf{M} produces $x_1 \in \mathbf{Z}/p\mathbf{Z}$; \mathbf{A} randomly chooses $x_2 \in \mathbf{Z}/p\mathbf{Z}$;

If $\varphi \notin \mathbf{QSAT}$ Then probability that \mathbf{A} accepts is exponentially small because it would imply that a value chosen by \mathbf{A} was the zero of a low-degree polynomial.

proof that $IP \subseteq PSPACE$: Evaluate the game tree.
For **M**'s moves choose the maximum value.
For **A**'s moves choose the average value.



Prop: $\mathbf{NP} \subseteq \mathbf{MA}$.

By adding randomness to the verifier, we can greatly restrict its computational power and the number of bits of Π that it needs to look at, while still enabling it to accept all of \mathbf{NP} .

Verifier \mathbf{A} is $(r(n), q(n))$ -**restricted** iff \mathbf{A} always uses at most $O(r(n))$ random bits and examines at most $O(q(n))$ bits of its proof, Π .

Let $\mathbf{PCP}[r(n), q(n)]$ be the set of boolean queries that are accepted by $(r(n), q(n))$ -restricted verifiers.

PCP Thm: $\mathbf{NP} = \mathbf{PCP}[\log n, 1]$

MAX-3-SAT: given a 3CNF formula, find a truth assignment that maximizes the number of true clauses.

$$(x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee x_4 \vee \overline{x_5}) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{x_4}) \wedge (x_2 \vee \overline{x_3} \vee \overline{x_4}) \\ \wedge (\overline{x_2} \vee x_3 \vee x_5) \wedge (\overline{x_3} \vee \overline{x_4} \vee \overline{x_5}) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3) \wedge (\overline{x_2} \vee \overline{x_4} \vee x_5)$$

Prop: MAX-3-SAT has a polynomial-time $\epsilon = \frac{1}{2}$ approximation algorithm.

Proof: Be greedy. □

Had Been Open for Years: Assuming $\mathbf{NP} \neq \mathbf{P}$ is there some ϵ , $0 < \epsilon < 1$, s.t. MAX-3-SAT has no PTIME ϵ -approximation algorithm?

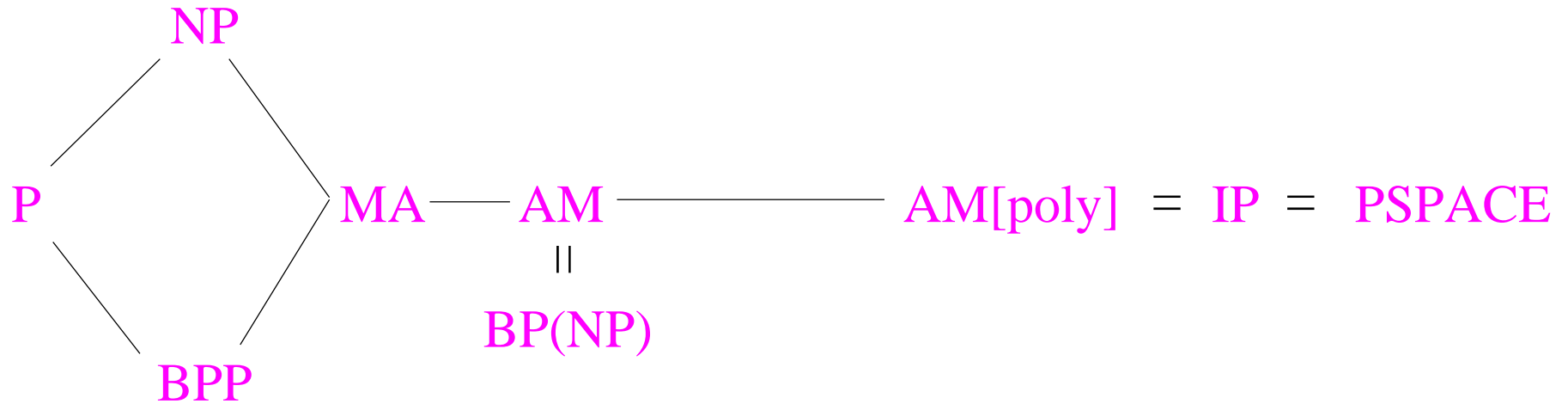
PCP Thm: $\mathbf{NP} = \mathbf{PCP}[\log n, 1]$

Cor: If $\mathbf{P} \neq \mathbf{NP}$, Then $\exists \epsilon . 0 < \epsilon < 1$, **MAX-3-SAT** has no ptime, ϵ -approximation algorithm.

Fact: **MAX-3-SAT** has a PTIME approximation algorithm with $\epsilon = \frac{1}{8}$ and no better ratio can be achieved unless $\mathbf{P} = \mathbf{NP}$.

Reference:

Sanjeev Arora, “The Approximability of **NP**-hard Problems”, STOC 98, www.cs.princeton.edu/~arora.



Prop: Graph Non-Isomorphism \in AM

Shamir's Thm: IP = PSPACE

PCP Thm: NP = PCP[log n , 1]

Cor: MAX-3-SAT has a PTIME approximation algorithm with $\epsilon = \frac{1}{8}$ and no better ratio can be achieved unless $P = NP$.