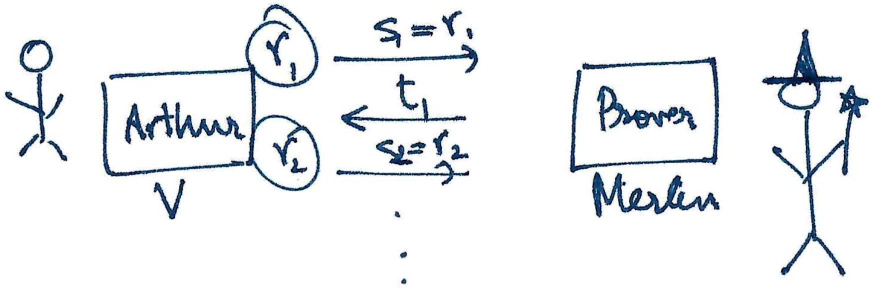
Arthur-Merlin Games



Prover/Merlin can see Arthur's random coins

Def: An Arthur-Merlin protocol is an IP where the verifier's messages are the random strings (r_i). There is no other randomness involved.

Merlin does not know random strings in advance.

Public Randomness

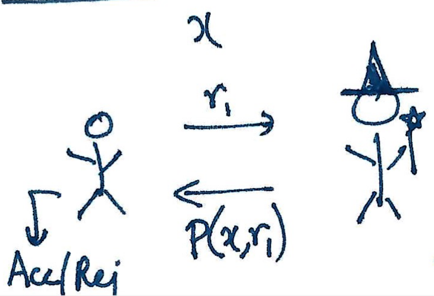
IP
private randomness

Def: $AM[k]$ is the class of languages decided by k-round Arthur Merlin protocols.

$$AM \neq \bigcup_{c \in \mathbb{N}} AM[n^c] \qquad IP = \bigcup_{c \in \mathbb{N}} IP[n^c]$$

$= AM[2]$

$AM[2] \qquad AMAM \qquad MA$



AM[2]

$L \in AM[2]$ if

$\exists$ poly time TM A s.t.

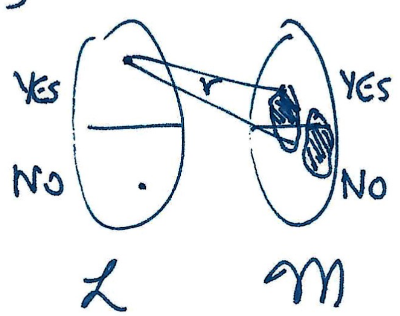
- If $x \in L \Rightarrow \exists$ fn P s.t. $\Pr_r[A(x, r, P(x,r)) \text{ accepts}] \geq 2/3$
- If $x \notin L \Rightarrow \forall$ fns P s.t. $\Pr_r[A(x, r, P(x,r)) \text{ accepts}] \leq 1/3$

Def: Randomized Reduction

A fn. $f:\{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ is a randomized reduction from language $\mathcal{L}$ to language $\mathcal{M}$ s.t.

$$\Pr_r\left[\mathcal{M}(f(x,r)) = \mathcal{L}(x)\right] \geq 2/3$$

The reduction is efficient if $|r| \leq p(n)$
$f(x,r)$ can be computed in poly time.



$\mathcal{L} \leq_r \mathcal{M}$ if there exists an efficient randomized reduction from $\mathcal{L}$ to $\mathcal{M}$.

$$\mathrm{BP}\cdot\mathrm{NP} = \{\mathcal{L} \mid \mathcal{L} \leq_r \mathrm{SAT}\}$$

Clm: $\mathrm{AM}[2] = \mathrm{BP}\cdot\mathrm{NP}$

Proof: $[\subseteq]$ $\mathcal{L} \in \mathrm{AM}[2]$. $\exists$ a 2-round Arthur-Merlin protocol.

Consider a randomized NTM R.

(1) Flip r (poly(n)) bits randomly
(2) Non-deterministically write down string $P(x,r)$
(3) Runs Arthur's computation $A(x,r,P(x,r))$

By Cook-Levin construction, there is a poly time computable formula $\cancel{\Phi(x,r)}$ $\Phi_{x,r}(v)$ s.t. $\Phi_{x,r}$ is satisfiable iff R accepts (when x,r are fixed).

$x \in \mathcal{L} \Rightarrow \exists$ fn P s.t. $\Pr_r[A(x,r,P(x,r)) \text{ accepts}] \geq 2/3$

For at least a $2/3$ fraction of all choices of $r \in \{0,1\}^{p(n)}$

$\exists$ a string P s.t. $A(x,r,P)$ accepts.

For at least $2/3$ fraction of choices of r, $R(x,r)$ accepts.

$\Pr_r[\Phi_{x,r} \in SAT] \geq 2/3$ $\qquad$ $\overset{|||}{\Phi_{x,r} \in SAT}$

$x \notin \mathcal{L} \Rightarrow \forall$ fns P s.t. $\Pr_r[A(x,r,P(x,r)) \text{ accepts}] \leq 1/3$

r is accepting seed if $A(x,r,P(x,r))$ accepts

rejecting seed if - - rejects.

For rejecting seed, $A(x,r,P(x,r))$ does NOT accept for any choice of $P(x,r)$

When machine R chooses a rejecting seed, R will not accept.

(non-det.)

$\Pr_r[\Phi_{x,r} \notin SAT] \geq 2/3$ $\qquad$ $\equiv \Phi_{x,r} \notin SAT$

$\blacksquare$

Public vs Private Randomness?

Thm [Goldwasser-Sipser 87]: $\forall k$ $\quad \mathbb{IP}[k] \subseteq \mathbb{AM}[k+2]$

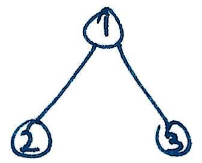
Thm [Babai-Moran 88]: $k \geq 2$ $\quad \mathbb{AM}[k+1] \subseteq \mathbb{AM}[k]$ (poly blow up)

$$\bigcup_{k \in \mathbb{N}} \mathbb{IP}[k] = \mathbb{AM}[2] = \mathbb{BP}\cdot\mathbb{NP} \quad !$$

Thm: $GNI \in AM[2]$ Input $\langle G_0, G_1 \rangle$

Proof: Key idea $S = \{ H \mid H \cong G_0 \text{ or } H \cong G_1 \}$

Suppose G_0 and G_1 have no non-trivial automorphism $Aut(G)$



$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$G_0 \xrightarrow{\pi(G_0)} H_{1,0}, H_{2,0}, \ldots, H_{n!,0}$ $n!$

$G_1 \xrightarrow{\pi(G_1)} H_{1,1}, H_{2,1}, \ldots, H_{n!,1}$

$$\boxed{\begin{array}{ll} \text{If } G_0 \not\cong G_1, & |S| = 2(n!) \\ \text{If } G_0 \equiv G_1 & |S| = n! \end{array}}$$

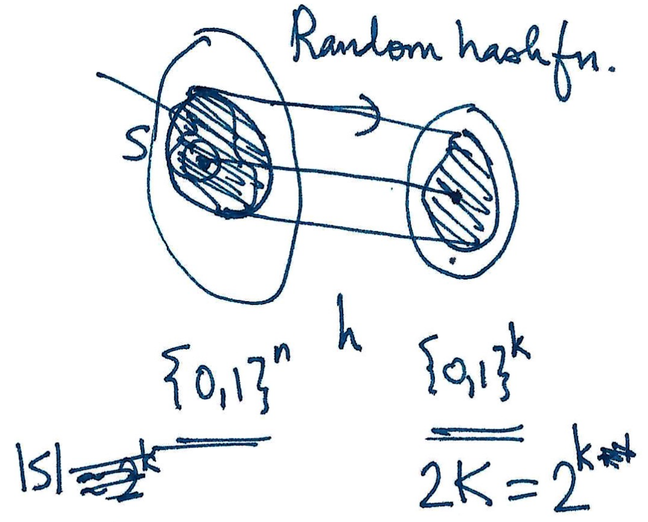
~~$S = \{ (H, aut(H))$~~ $\underline{\underline{S}} = \{ (H, \sigma) \mid H \cong G_0 \text{ or } H \cong G_1 \text{ and } \sigma \in Aut(H) \}$

There is a poly-sized efficiently ~~computable~~ verifiable certificate for membership in S. (The permutation leading to $H \cong G_0 / G_1$)

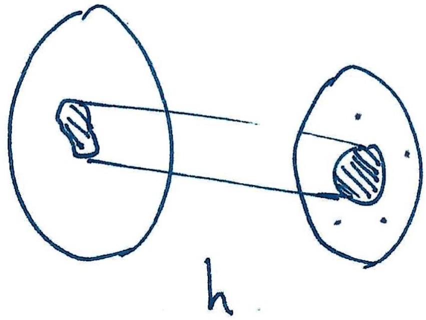
~~$x \in L$~~   There is a set S s.t. membership in S is efficiently verifiable $S \subseteq \{0,1\}^n$

$x \in L \Rightarrow |S| \geq 2K$ $x \notin L \Rightarrow |S| \leq K$

GS: <u>Set lower bound protocol</u>



YES



NO

Arthur : (1) Picks random hash fn. h

(2) Pick random y in range $\{0,1\}^k$

Asks Merlin "give me $x \in S$ s.t. $h(x) = y$ & give me certificate that $x \in S$."