- Exercise: Show that if Merlin errs then Arthur will detect it with high probability.

- Now we prove some lemmas to be used later.

Lemma (Babai, Fortnow, Nisan, Wigderson 1993):

$$\mathsf{EXP} \subseteq \mathsf{P/poly} \Rightarrow \mathsf{EXP} = \mathsf{MA}.$$

Proof:

- Suppose $\mathsf{EXP} \subseteq \mathsf{P/poly}$.
- We will first show that $\mathsf{EXP} \subseteq \Sigma_2$:

- Let $L \in \mathsf{EXP}$ & N be its exp-time TM.
- Since the j-th bit in the i-th configuration of $N(x)$ is computable in EXP, $\exists$ poly-sized circuit $C(x,i,j)$ computing it.
- Now, $x \in L \Leftrightarrow \exists C, \forall i, \forall j, [C(x,i,j) \rightarrow C(x,i+1,j)$ is a valid step of $N]$.

- This just means that $L \in \Sigma_2$.

$\Rightarrow \quad EXP \subseteq \Sigma_2$.

$\Rightarrow \quad EXP = \Sigma_2$.

- Also, $\Sigma_2 \subseteq Pspace = IP \subseteq EXP$.

$\Rightarrow \quad Pspace = IP = EXP \subseteq P/poly$.

- Thus, any $L \in EXP$ has an interactive protocol.

Moreover, Merlin can be seen as a Pspace-machine, hence, can be simulated by a poly-sized circuits family $\{C_n\}_n$.

- This suggest a single-round protocol to convince Arthur that $x \in L$:

(1) Merlin sends a circuit C, claiming to be C_n, $n := |x|$.

(2) Arthur runs the protocol on x, using C instead of Merlin.

$\Rightarrow L \in MA$

$\Rightarrow \quad EXP \subseteq MA \quad \Rightarrow \quad EXP = MA.$ $\square$

- The final lemma is the most advanced. We will prove it after we have covered pseudo-random generators.

__Lemma__ (Impagliazzo, Kabanets, Wigderson 2001):

$$NEXP \subseteq P/poly \Rightarrow NEXP = EXP.$$

- Finally, we can prove the PIT-theorem:

$$PIT \in P \Rightarrow NEXP \not\subseteq P/poly \text{ OR } per \notin alg\,P/poly.$$

__Proof:__

- Suppose $PIT \in P$, $NEXP \subseteq P/poly$.

  $\Rightarrow \quad NEXP = EXP = MA.$

- Also, $MA \subseteq PH \subseteq P^{per}$ [Toda's theorem]

  $\Rightarrow \quad NEXP \subseteq P^{per}.$

- Assuming $per \in P/poly$ implies $P^{per} \subseteq NP$.

$\Rightarrow$ $NEXP \subseteq NP$,
which contradicts the nondet.-time hierarchy.

- Thus, either $NEXP \not\subseteq P/poly$ OR $per \notin algP/poly$. $\square$

(Circuit) Lower bounds

- It is believed that $NP \neq P$.
  One way to prove that could be to show a <u>stronger</u> result: $SAT \notin P/poly$.
  It is a more algebraic question.

- This approach was tried in the 70/80s & lower bounds for special circuit models were obtained.
  Probabilistic methods were used!

<u>Definition</u>: • <u>AC^0</u> $:= \{L \subseteq \{0,1\}^* \mid \exists$ poly(n)-sized, $O(1)$-depth boolean circuits for $L\}$.

• <u>Modular gate</u> <u>mod_m</u> $: \{0,1\}^n \longrightarrow \{0,1\}$;

$$(x_1, \dots, x_n) \longmapsto \begin{cases} 1, & \text{if } \sum x_i \not\equiv 0 \pmod m, \\ 0, & \text{else}. \end{cases}$$

• <u>AC^0 with counters</u>, <u>$ACC^0[m]$</u> $:= \{L \subseteq \{0,1\}^* \mid$ $\exists$ poly(n)-sized, $O(1)$-depth boolean circuit family, using mod_m gates, solving $L\}$.

– We would suspect $mod_2 \notin AC^0$, and in general, $mod_p \notin ACC^0[q]$ for distinct primes p, q.

<u>Theorem</u> (Razborov '87, Smolensky '87): For primes $p \neq q$, $mod_p \notin ACC^0[q]$.

<u>Proof</u>:

• Idea - "Approximate" an $ACC^0[q]$ circuit by a polynomial over $\mathbb{F}_q$.

- We will exhibit the proof for $p=2, q=3$.

<u>Lemma 1</u>: Let C be a depth-d $ACC^0[3]$ circuit on n inputs and size-s.

allows us to make deg $\ll n$.

There is a polynomial in $\mathbb{F}_3[\bar{x}]$ of $\deg \leq (2\ell)^d$ which agrees with $C(\bar{x})$ on $\geq \left(1-\frac{s}{2^\ell}\right)$ fraction of the inputs.

<u>Lemma 2</u>: No polynomial in $\mathbb{F}_3[\bar{x}]$ of $\deg \leq \sqrt{n}$ can agree with mod_2 on ≥ 0.99 fraction of the inputs.

$\Rightarrow$ If mod_2 has a size-s $ACC^0[3]$ circuit then, by Lemma 1 for $\ell := \frac{1}{2} n^{1/2d}$, $\exists$ polynomial of $\deg \leq \sqrt{n}$ agreeing with mod_2 on $\geq \left(1-\frac{s}{2^\ell}\right)$ fraction of the inputs.

Now, by Lemma 2, $1-\frac{s}{2^\ell} < 0.99$