- The "physical" interpretation of these classes is by considering k-rounds of <u>interaction</u> between:
  the king <u>Arthur</u> (randomized verifier)
  his advisor <u>Merlin</u> (unreliable prover)

- AM[1]:

| Arthur | | Merlin |
|---|---|---|
| $x, y_1$ | | (not used) |

▷ AM[1] = BPP.

- MA[1]:

| Arthur | | Merlin |
|---|---|---|
| $x$ | $\xleftarrow{\ y_1\ }$ | |

▷ MA[1] = NP.

- MA[2]:

| Arthur | | Merlin |
|---|---|---|
| $x, y_2$ | $\xleftarrow{\ y_1\ }$ | |

⇒ like NP with a randomized verifier.

- This we also call <u>MA</u>.

- AM[2]:

| Arthur | | Merlin |
|---|---|---|
| $x, y_1$ | $\xleftarrow{\ y_2\ }$ | |

- This we also call <u>AM</u>.

<u>Definition</u>: If we make k a variable then we get $IP := \bigcup_{c \in \mathbb{R}_{>0}} AM[n^c]$.

(interactive protocol)

▷ All these classes are in Pspace.

<u>Theorem</u> (Shamir 1990): IP = Pspace.

<u>Pf sketch</u>:

- It suffices to show that Pspace $\subseteq$ IP.
- We pick a Pspace-complete problem — Quantified boolean formula (<u>QBF</u>):

$x_i \in \{0,1\} \rightarrow$ Given a formula $\psi := Q_1 x_1 \cdots Q x_n\, \phi(\bar{x})$, where $Q_i$'s are quantifiers $\{\exists, \forall\}$ & $\phi$ is a boolean formula. Test whether $\psi$ is true.

▷ QBF is Pspace-complete.

- We intend to show that QBF $\in$ IP.

This protocol will be <u>algebraic</u>.

- For the boolean formula $\phi$, we define an <u>arithmetized</u> version $P_\phi \in \mathbb{Q}[x_1, \ldots, x_n]$.

e.g. $\phi := (x_1 \vee x_2) \wedge (\overline{x}_2 \vee x_3 \vee x_4)$ arithmetizes to $T_\phi := \left(1-(1-x_1)(1-x_2)\right) \cdot \left(1 - x_2(1-x_3)(1-x_4)\right)$.

The key property being that $\phi(a_1, \ldots, a_n) = \text{true}$ iff $T_\phi(a_1, \ldots, a_n) = 1$.

- Clearly, arithmetization is <u>easy</u> to do.
- We extend this to quantifiers as:

$$\forall x_i \text{ converts to } \prod_{x_i \in \{0,1\}},$$

$$\exists x_i \quad \text{"} \quad \text{"} \quad \sum_{x_i \in \{0,1\}}$$

By going mod a <u>random</u> prime, wlog $P_\psi$ is an integer in $[0, 2^n]$

- Finally, $\psi := Q_1 x_1 \cdots Q_n x_n \, \phi(\overline{x})$ converts to $P_\psi := \tilde{Q}_1 \tilde{Q}_2 \cdots \tilde{Q}_n \, P_\phi(x_1, \ldots, x_n)$, where $\tilde{Q}_i$ is $\prod_{x_i}$ or $\sum_{x_i}$.

▷ $\psi$ is true iff $P_\psi \neq 0$.

- Now to convince Arthur that $\psi$ = true, Merlin will try to prove: $P_\psi = k \in [2^n]$ in $n$ rounds of interaction.

(Merlin sends partial polynomial related to $P_\psi$. Arthur does PIT.)

0) Merlin sends $k>0$, claiming $P_\psi = k$.

1) If $n=1$ then Arthur accepts iff:

$$Q_1 = \forall \ \& \ P_\phi(0) \cdot P_\phi(1) = k,$$
$$Q_1 = \exists \ \& \ P_\phi(0) + P_\phi(1) = k.$$

deg $s$ can be made small

2) If $n>1$ then Merlin sends $s(x_1)$, claiming it to be $\tilde{Q}_2 \tilde{Q}_3 \cdots \tilde{Q}_n P_\phi(x_1, \ldots, x_n)$.

3) Arthur tests: $Q_1 = \forall \ \& \ s(0) \cdot s(1) = k$,

$Q_1 = \exists \ \& \ s(0) + s(1) = k$,

and for a random $\alpha$, verifies

$$s(\alpha) = \tilde{Q}_2 \cdots \tilde{Q}_n P_\phi(\alpha, x_2, \ldots, x_n).$$

done recursively by interacting with Merlin

$\square$

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

- Now we prove some lemmas to be used later.

<u>Lemma</u> (Babai, Fortnow, Nisan, Wigderson 1993):

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

<u>Proof</u>:

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

- Let $L \in \mathrm{EXP}$ & $N$ 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, $x \in L \Leftrightarrow \exists C, \forall i, \forall j, [C(x,i,j) \to C(x,i+1,j)$ is a valid step of $N]$.