Jean Goubault-Larrecq

Randomized complexity classes

Today: the Arthur vs. Merlin hierarchy **collapses**

Today

- Babai's theorem: $\mathbf{MA} \subseteq \mathbf{AM}$
- Also, $\mathbf{MAM} \subseteq \mathbf{AM}$
- A detour through promise problems
- The Arthur vs. Merlin hierarchy collapses.

MA is included in **AM**

Converting MA to AM

Why not just use « skolemization »?
(Hint: does not work.)

- **Prop (Lemma 3.11).** Let $F(x,y,r)$ be a predicate

  (x of size n, r of poly size $q(n)$, y of poly size $p(n)$) such that $\forall x$,

  — either (1): $(\exists y, \mathrm{E}r, F(x,y,r)) \geq 1\text{–}1/2^n$ (« huge »)

  — or (2): $(\exists y, \mathrm{E}r, F(x,y,r)) \leq 1/2^n$ (« tiny »)

  M A

- Then for every poly $g(n)$, and for n large enough,

  — in case (1), $F'(x) \geq 1\text{–}1/2^{g(n)}$ … =1, in fact!

  — in case (2), $F'(x) \leq 1/2^{g(n)}$

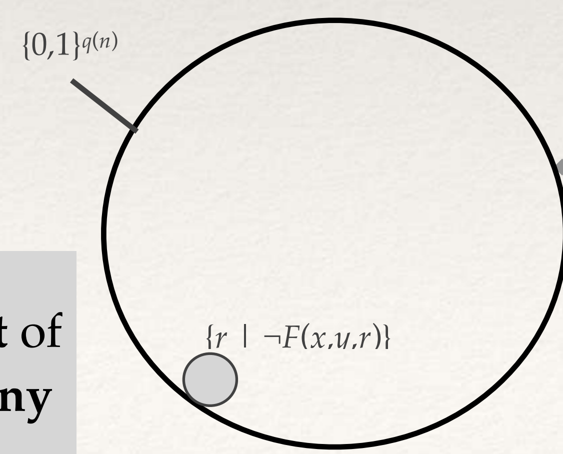
where $F'(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \ldots, r_k, \exists y, r', \bigwedge_{i=1}^k F(x,y,r'\oplus r_i)$.

and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$

A M

Permuting E over ∃, à la Lautemann

- In case (1) (« **huge** »), $(\mathrm{E}r,\ F(x,y,r)) \geq 1-1/2^n$ for some y. We fix that y.
- I.e., $\Pr_r(F(x,y,r)) \geq 1-1/2^n$
  ($F(x,y,r)$ is a **predicate**!)
  namely $\Pr_r(\neg F(x,y,r)) \leq 1/2^n$
- We claim that, in that case, for **all** $r_1, \ldots, r_k$, there is an r' / $\bigwedge_{i=1}^{k} F(x,y,r'\oplus r_i)$



The **complement** of $\{r \mid F(x,y,r)\}$ is **tiny**

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate
(x of size n, r of poly size $q(n)$, y of poly size $p(n)$) / $\forall x$,
⟹ — either (1): $(\exists y,\ \mathrm{E}r,\ F(x,y,r)) \geq 1-1/2^n$ (« huge »)
— or (2): $(\exists y,\ \mathrm{E}r,\ F(x,y,r)) \leq 1/2^n$ (« tiny »)
Then for every poly $g(n)$, and for n large enough,
— in case (1), $F'(x)=1$
— in case (2), $F'(x) \leq 1/2^{g(n)}$
where $F'(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \ldots, r_k, \exists y, r', \wedge_{i=1}^{k} F(x,y,r'\oplus r_i)$.
and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$

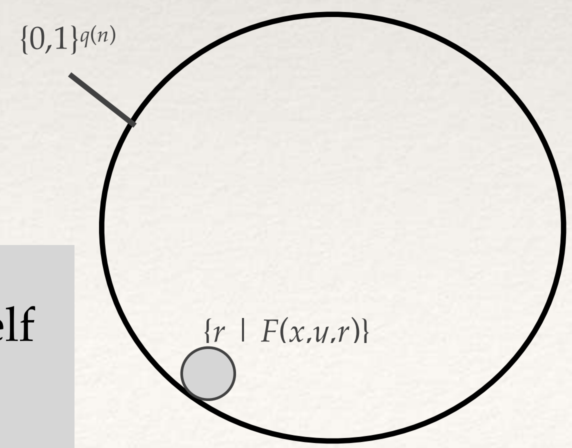
- Let $r_1, \ldots, r_k$ be arbitrary.
  $\Pr_{r'}(\neg \bigwedge_{i=1}^{k} F(x,y,r'\oplus r_i))$
  $\leq \Sigma_{i=1}^{k} \Pr_{r'}(\neg F(x,y,r'\oplus r_i))$
  $\leq k/2^n$
- Since $k=\mathrm{poly}(n)$, this is < 1 for n large enough.

Permuting E over ∃, à la Lautemann

- In case (2) (« **tiny** »), (Er, $F(x,y,r)$)≤$1/2^n$ for **every** y.
- $\Pr_r(F(x,y,r)) \leq 1/2^n$ for **every** y. ($F(x,y,r)$ is a **predicate**!)
- $\Pr_{r1,\ldots,rk}(\exists y,r', \bigwedge_{i=1}^k F(x,y,r'\oplus r_i))$
  $\leq \Sigma_{y,r'} \Pr_{r1,\ldots,rk}(\bigwedge_{i=1}^k F(x,y,r'\oplus r_i))$
  $= \Sigma_{y,r'} \prod_{i=1}^k \Pr_{ri}(F(x,y,r'\oplus r_i))$
  (independence)
- $\leq \Sigma_{y,r'} (1/2^n)^k$
  $= 2^{p(n)+q(n)-nk}$
  $\leq 1/2^{g(n)}$. □

⟹

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate
(x of size n, r of poly size $q(n)$, y of poly size $p(n)$) / ∀x,
— either (1): (∃y, Er, $F(x,y,r)$) ≥ 1–$1/2^n$ (« huge »)
— or (2): (∃y, Er, $F(x,y,r)$) ≤ $1/2^n$ (« tiny »)
Then for every poly $g(n)$, and for n large enough,
— in case (1), $F'(x) = 1$
— in case (2), $F'(x) \leq 1/2^{g(n)}$
where $F'(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \ldots, r_k, \exists y, r', \wedge_{i=1}^k F(x,y,r'\oplus r_i)$.
and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$



{r | $F(x,y,r)$} itself is **tiny**

$\mathbf{MA} \subseteq \mathbf{AM}$

- **Thm 3.12 (Babai). MA ⊆ AM.**
- *Proof.* Let $L \in \mathbf{MA}$.
  For some $D \in \mathbf{P}$,
  (logical characterization of **MA**)
  (1) if $x \in L$ then $(\exists y, \text{E}r, x\#y\#r \in D) \geq 1\text{–}1/2^n$
  (2) if $x \notin L$ then $(\exists y, \text{E}r, x\#y\#r \in D) \leq 1/2^n$.

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate
(x of size n, r of poly size $q(n)$, y of poly size $p(n)$) / $\forall x$,
— either (1): $(\exists y, \text{E}r, F(x,y,r)) \geq 1\text{–}1/2^n$ (« huge »)
— or (2): $(\exists y, \text{E}r, F(x,y,r)) \leq 1/2^n$ (« tiny »)
Then for every poly $g(n)$, and for n large enough,
— in case (1), $F'(x) = 1$
— in case (2), $F'(x) \leq 1/2^{g(n)}$
where $F'(x) \stackrel{\text{def}}{=} \text{E}r_1, \ldots, r_k, \exists y, r', \bigwedge_{i=1}^k F(x,y,r' \oplus r_i)$.
and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$

- Apply the Proposition to $F(x,y,r) \stackrel{\text{def}}{=} (x\#y\#r \in D)$
  (**predicate**!)
- Therefore L is in **AM**. ☐

Ah yes, case (2) only applies for n large enough.
For small values of n, tabulate.

MAM ⊆ AM

- **Lemma 3.11. MAM ⊆ AM.**
- *Proof* (1/2). Let $L \in$ **MAM**.
  For some $D \in$ **P**,

  (logical characterization of **MAM**)

  (1) if $x \in L$ then $(\exists y, \mathrm{E}r, \exists y', x\#y\#r\#y' \in D) \geq 1\text{–}1/2^n$
  (2) if $x \notin L$ then $(\exists y, \mathrm{E}r, \exists y', x\#y\#r\#y' \in D) \leq 1/2^n$.

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate
(x of size n, r of poly size $q(n)$, y of poly size $p(n)$) / $\forall x$,
— either (1): $(\exists y, \mathrm{E}r, F(x,y,r)) \geq 1\text{–}1/2^n$ (« huge »)
— or (2): $(\exists y, \mathrm{E}r, F(x,y,r)) \leq 1/2^n$ (« tiny »)
Then for every poly $g(n)$, and for n large enough,
— in case (1), $F'(x) = 1$
— in case (2), $F'(x) \leq 1/2^{g(n)}$
where $F'(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \ldots, r_k, \exists y, r', \bigwedge_{i=1}^{k} F(x,y,r'\oplus r_i)$.
and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$

- Apply the Proposition to $F(x,y,r) \stackrel{\text{def}}{=} (\exists y', x\#y\#r\#y' \in D)$
  (**predicate** again!)
- Then $F'(x) = \mathrm{E}r_1, \ldots, r_k, \exists y, r', \bigwedge_{i=1}^{k} \exists y', (x\#y\#(r'\oplus r_i)\#y' \in D) \ldots$

MAM ⊆ AM

- **Lemma 3.11. MAM ⊆ AM.**

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate
(x of size n, r of poly size $q(n)$, y of poly size $p(n)$) / $\forall x$,
— either (1): $(\exists y, \mathrm{E}r, F(x,y,r)) \geq 1-1/2^n$ (« huge »)
— or (2): $(\exists y, \mathrm{E}r, F(x,y,r)) \leq 1/2^n$ (« tiny »)
Then for every poly $g(n)$, and for n large enough,
— in case (1), $F'(x) = 1$
— in case (2), $F'(x) \leq 1/2^{g(n)}$
where $F'(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \ldots, r_k, \exists y, r', \bigwedge_{i=1}^k F(x,y,r'\oplus r_i)$.
and $k \stackrel{\text{def}}{=} \lceil m/n \rceil$, $m \stackrel{\text{def}}{=} p(n)+q(n)+g(n)$

- *Proof* (2/2).
- $F'(x) = \mathrm{E}r_1, \ldots, r_k, \exists y, r',$
$$\bigwedge_{i=1}^k \exists y', (x\#y\#(r'\oplus r_i)\#y' \in D)$$
- $= \mathrm{E}r_1, \ldots, r_k, \exists y, r', \underline{y'_1, \ldots, y'_k},$
$$\bigwedge_{i=1}^k (x\#y\#(r'\oplus r_i)\#y'_i \in D)$$
- Hence L is in **AM**. □

Intermission: promise problems

Promise problems: example

- Look back at, say, **SAT**:
  INPUT: a clause set *S*
  QUESTION: is *S* satisfiable?
- We silently assumed that this defined a language…
  but a language is a set of words, not of clause sets
- Some input words may **fail to parse** as clause sets.
- Hence, really, what we are interested in is…

Promise problems

- INPUT: a word w
  PROMISE: w parses as a clause set S
  QUESTION: is S satisfiable?
- Modeled as **two** languages:
  $L^+ \stackrel{\text{def}}{=} \{w \mid w \text{ parses as a satisfiable clause set } S\}$
  $L^- \stackrel{\text{def}}{=} \{w \mid w \text{ parses as an unsatisfiable clause set } S\}$
- In general, a **promise problem** is a pair of two disjoint languages:
  INPUT: a word w
  PROMISE: $w \in L^+ \cup L^-$
  QUESTION: is w in L^+?

Promise problems are often useless

- Testing the promise is usually easy (in **P**, sometimes even lower)
- Then there is no difference in complexity between L^+ and (the complement of) L^-
- E.g., for **SAT**, both are **NP**-complete.

- INPUT: a word w
  PROMISE: w parses as a clause set S
  QUESTION: is S satisfiable?
- Modeled as **two** languages:
  $L^+ \stackrel{\text{def}}{=} \{w \mid w$ parses as a satisfiable clause set $S\}$
  $L^- \stackrel{\text{def}}{=} \{w \mid w$ parses as an unsatisfiable clause set S
- In general, a **promise problem** is a pair of two disjoint languages:
  INPUT: a word w
  PROMISE: $w \in L^+ \cup L^-$
  QUESTION: is w in L^+?

Promise problems are sometimes useful

- Let **BPP′** be the promise version of **BPP**, i.e.:
  — if $x \in L^+$ then $\Pr_r(x\#r \in D) \geq 2/3$
  — if $x \in L^-$ then $\Pr_r(x\#r \in D) \leq 1/3$
  where D is a language in **P**.

- Then the following promise problem is **BPP′-complete**:
  $L^+ \stackrel{\text{def}}{=} \{\text{circuits } C \text{ that evaluate to 1 on} \geq 2/3 \text{ of their inputs}\}$
  $L^- \stackrel{\text{def}}{=} \{\text{circuits } C \text{ that evaluate to 1 on} \leq 1/3 \text{ of their inputs}\}$

- (There is no known **BPP**-complete problem.)

Promise versions of Arthur-Merlin games

- All the classes in the Arthur-Merlin hierarchy have analogues as **promise problems**:
  ε′, **A′**, **M′**, **MA′**, **AM′**, etc.

- Thm 3.12′. **MA′** $\subseteq$ **AM′**.
  Lemma 3.11′. MAM′ $\subseteq$ **AM′**.

(same proof as before!)

- $(L^+,L^-) \in$ **AMAM…′** iff
  for every polynomial $g(n)$,
  there is a poly time predicate P /
  — if $x \in L^+$, then $G(x) \geq 1 - 1/2^{g(n)}$
  — if $x \in L^-$ then $G(x) \leq 1/2^{g(n)}$
  where $G(x) \stackrel{\text{def}}{=} \mathrm{E}r_1, \exists y_1, \mathrm{E}r_2, \exists y_2, \ldots, \; P(x, r_1, y_1, r_2, y_2, \ldots)$

The Arthur-Merlin hierarchy collapses

The A-M' hierarchy collapses

- We will show by induction on the length of w that $\mathbf{w'} \subseteq \mathbf{AM'}$.
- Obvious if this length is 0.
- We will then look at the first letter of w, either `A` or `M`.

w' $\subseteq$ AM': (1) w starts with A

- Let $w \stackrel{\text{def}}{=} \mathrm{A}\, w_2$, and let $(L^+, L^-) \in \mathbf{w}'$… first, a useful lemma:
- **Square root lemma.** Let $0<\varepsilon<1$, and X be a non-negative real-valued random variable with finite expectation.
(i) If $E(X)\leq\varepsilon$ then $\Pr(X\leq\sqrt{\varepsilon})\geq 1-\sqrt{\varepsilon}$
(ii) If $E(X)\geq 1-\varepsilon$ then $\Pr(X\geq 1-\sqrt{\varepsilon})\geq 1-\sqrt{\varepsilon}$.

> **Theorem (Markov's inequality).**
> Let X be a **non-negative real-valued** ran
> with **finite** expectation $E(X)$. For eve
> $\Pr(X\geq a.E(X)) \leq 1/a$.

- *Proof.* (i) Let $a \stackrel{\text{def}}{=} 1/\sqrt{\varepsilon}$, so $a.E(X)\leq\sqrt{\varepsilon}$.

$$\Pr(X>\sqrt{\varepsilon}) \leq \Pr(X \geq \sqrt{\varepsilon}) \leq \Pr(X\geq a.E(X)) \leq \sqrt{\varepsilon}.$$

(ii) Use (i) with X replaced by $1-X$. □

I.e., if the expectation of X is **very large**,
then X is **large**, with **high probability**.

w' ⊆ AM': (1) w starts with A (1/5)

i.e., $(L^+,L^-) \in \mathbf{w}'$ is decided by a formula of the form $\underbrace{\text{E}r,\ \exists y_1,\ \text{E}r_2,\ \exists y_2,\ \ldots}_{F(x,r)}$

- Let $w \stackrel{\text{def}}{=} \mathtt{A}\, w_2$, and let $(L^+,L^-) \in \mathbf{w}'$.
  — if $x \in L^+$, then $(\text{E}r,\ F(x,r)) \geq 1-1/2^{2g(n)+2}$
  — if $x \in L^-$ then $(\text{E}r,\ F(x,r)) \leq 1/2^{2g(n)+2}$

We reduce the error preventively.
This will be needed.

- Beware: F is not a predicate, so expectation ≠ probability
- But, with high probability on r ($\geq 1-1/2^{g(n)+1}$),
  — if $x \in L^+$, then $F(x,r) \geq 1-1/2^{g(n)+1}$
  — if $x \in L^-$ then $F(x,r) \leq 1/2^{g(n)+1}$
  Why?

Square root lemma. Let $0<\varepsilon<1$, and X be a non-r
real-valued random variable with finite expectat
(i) If $E(X)\leq\varepsilon$ then $\Pr(X\leq\sqrt{\varepsilon})\geq 1-\sqrt{\varepsilon}$
(ii) If $E(X)\geq 1-\varepsilon$ then $\Pr(X\geq 1-\sqrt{\varepsilon})\geq 1-\sqrt{\varepsilon}$.

w' ⊆ AM': (1) w starts with A (2/5)

i.e., $(L^+,L^-) \in \mathbf{w}'$ is decided by a formula of the form $\underbrace{\mathrm{E}r,\ \exists y_1,\ \mathrm{E}r_2,\ \exists y_2,\ \ldots}_{F(x,r)}$

- Let $w \stackrel{\text{def}}{=} \mathtt{A}\, w_2$, and let $(L^+,L^-) \in \mathbf{w}'$.
  — if $x \in L^+$, then $(\mathrm{E}r,\ F(x,r)) \geq 1-1/2^{2g(n)+2}$
  — if $x \in L^-$ then $(\mathrm{E}r,\ F(x,r)) \leq 1/2^{2g(n)+2}$
- If $x \in L^+$, then by (ii) $\Pr_r(F(x,r) \geq 1-1/2^{g(n)+1}) \geq 1-1/2^{g(n)+1}$
- If $x \in L^-$, then by (i) $\Pr_r(F(x,r) \leq 1/2^{g(n)+1}) \geq 1-1/2^{g(n)+1}$

Square root lemma. Let $0<\varepsilon<1$, and X be a non-r
real-valued random variable with finite expectat
(i) If $\mathrm{E}(X) \leq \varepsilon$ then $\Pr(X \leq \sqrt{\varepsilon}) \geq 1-\sqrt{\varepsilon}$
(ii) If $\mathrm{E}(X) \geq 1-\varepsilon$ then $\Pr(X \geq 1-\sqrt{\varepsilon}) \geq 1-\sqrt{\varepsilon}$.

w' ⊆ AM': (1) w starts with A (3/5)

i.e., $(L^+,L^-) \in \mathbf{w}'$ is decided by a formula of the form $\underbrace{\mathrm{E}r, \exists y_1, \mathrm{E}r_2, \exists y_2, \ldots}_{F(x,r)}$

- Let $w \stackrel{\text{def}}{=} \mathtt{A}\, w_2$, and let $(L^+,L^-) \in \mathbf{w}'$.
  — if $x \in L^+$, then $(\mathrm{E}r, F(x,r)) \geq 1-1/2^{2g(n)+2}$
  — if $x \in L^-$ then $(\mathrm{E}r, F(x,r)) \leq 1/2^{2g(n)+2}$
- With high probability on r ($\geq 1-1/2^{g(n)+1}$),
  — if $x \in L^+$, then $F(x,r) \geq 1-1/2^{g(n)+1}$
  — if $x \in L^-$ then $F(x,r) \leq 1/2^{g(n)+1}$
- Let $D^+ \stackrel{\text{def}}{=} \{x\#r \mid F(x,r) \geq 1-1/2^{g(n)+1}\}$
  $D^- \stackrel{\text{def}}{=} \{x\#r \mid F(x,r) \leq 1/2^{g(n)+1}\}$
  (D^+,D^-) is a promise language in $\mathbf{w_2}'$.
- By induction hypothesis, (D^+,D^-) is in **AM′**.

This is where we need **promise languages**.

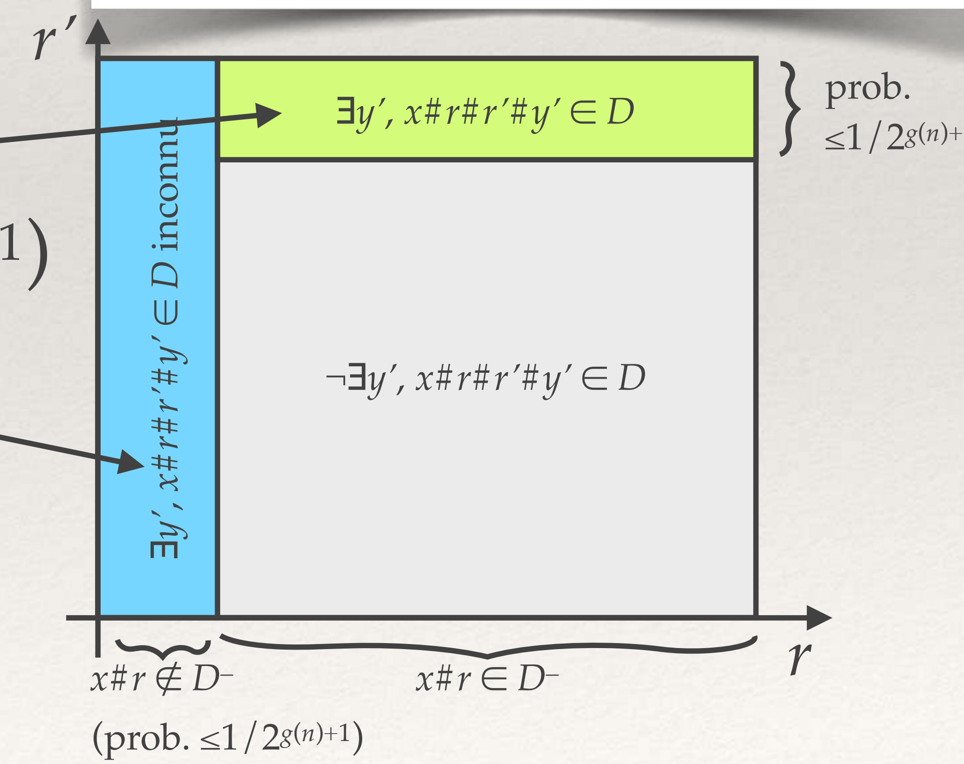
w' $\subseteq$ AM': (1) *w* starts with A (4/5)

- Since $(D^+,D^-) \in \mathbf{AM'}$, for some $D \in \mathbf{P}$:
  — if $x\#r \in D^+$, then
  $\Pr_{r'}(\exists y', x\#r\#r'\#y' \in D) \geq 1-1/2^{g(n)+1}$
  — if $x\#r \in D^-$, then
  $\Pr_{r'}(\exists y', x\#r\#r'\#y' \in D) \leq 1/2^{g(n)+1}$

- If $x \in L^-$ then $(\exists y', x\#r\#r'\#y' \in D)$ holds:
  — with prob. $\leq 1/2^{g(n)+1}$ (on r') if $x\#r \in D^-$,
  — and $x\#r \notin D^-$ happens (i.e., $F(x,r) > 1/2^{g(n)+1}$)
  with prob. $\leq 1/2^{g(n)+1}$ (on r)
  hence with prob. $\leq 1/2^{g(n)}$ total (on r, r')

- Hence $\Pr_{r,r'}(\exists y', x\#r\#r'\#y' \in D) \leq 1/2^{g(n)}$

- Let $w \stackrel{\text{def}}{=} \mathtt{A}\, w_2$, and let $(L^+,L^-) \in \boldsymbol{w'}$.
  — if $x \in L^+$, then $(\mathrm{E}r, F(x,r)) \geq 1-1/2^{2g(n)+2}$
  — if $x \in L^-$ then $(\mathrm{E}r, F(x,r)) \leq 1/2^{2g(n)+2}$
- With high probability on r ($\geq 1-1/2^{g(n)+1}$),
  — if $x \in L^+$, then $F(x,r) \geq 1-1/2^{g(n)+1}$
  — if $x \in L^-$ then $F(x,r) \leq 1/2^{g(n)+1}$
- Let $D^+ \stackrel{\text{def}}{=} \{x\#r \mid F(x,r) \geq 1-1/2^{g(n)+1}\}$
  $D^- \stackrel{\text{def}}{=} \{x\#r \mid F(x,r) \leq 1/2^{g(n)+1}\}$
  (D^+,D^-) is a promise language in $\boldsymbol{w_2'}$.
- By induction hypothesis, (D^+,D^-) is in $\mathbf{AM'}$.



$\mathbf{w'} \subseteq \mathbf{AM'}$: (1) w starts with $\mathtt{A}$ (5/5)

- In summary:
  — If $x \in L^-$ then $\Pr_{r,r'}(\exists y', x\#r\#r'\#y' \in D) \leq 1/2^{g(n)}$
  — If $x \in L^+$ then $\Pr_{r,r'}(\exists y', x\#r\#r'\#y' \in D) \geq 1 - 1/2^{g(n)}$
- Therefore (L^+, L^-) is in **AM′**.
- Since (L^+, L^-) was arbitrary in **w′**, $\mathbf{w'} \subseteq \mathbf{AM'}$.

w’ ⊆ AM’: (1) w starts with `M` (1/2)

- Let $w \stackrel{\text{def}}{=} \mathtt{M}\, w_2$, and let $(L^+,L^-) \in \mathbf{w}'$.
  — if $x \in L^+$, then for some y, $F(x,y) \geq 1-1/2^{g(n)}$
  — if $x \in L^-$ then for every y, $F(x,y) \leq 1/2^{g(n)}$
- Let $D^+ \stackrel{\text{def}}{=} \{x\#y \mid F(x,y) \geq 1-1/2^{g(n)}\}$
  $D^- \stackrel{\text{def}}{=} \{x\#y \mid F(x,y) \leq 1/2^{g(n)}\}$
- (D^+,D^-) is a promise language in $\mathbf{w_2}'$.

- By induction hypothesis, (D^+,D^-) is in **AM’**.

w' ⊆ AM': (1) w starts with `M` (2/2)

- Since $(D^+,D^-) \in \mathbf{AM'}$, for some $D \in \mathbf{P}$:
  — if $x\#y \in D^+$, then
  $(\mathrm{E}r', \exists y', x\#y\#r'\#y' \in D) \geq 1-1/2^{g(n)}$
  — if $x\#y \in D^-$, then
  $(\mathrm{E}r', \exists y', x\#y\#r'\#y' \in D) \leq 1/2^{g(n)}$

> - Let $w \stackrel{\text{def}}{=}$ `M` w_2, and let $(L^+,L^-) \in \mathbf{w'}$.
>   — if $x \in L^+$, then for some y, $F(x,y) \geq 1-1/2^{g(n)}$
>   — if $x \in L^-$ then for every y, $F(x,y) \leq 1/2^{g(n)}$
> - Let $D^+ \stackrel{\text{def}}{=} \{x\#y \mid F(x,y) \geq 1-1/2^{g(n)}\}$
> $D^- \stackrel{\text{def}}{=} \{x\#y \mid F(x,y) \leq 1/2^{g(n)}\}$
> - (D^+,D^-) is a promise language in $\mathbf{w_2'}$.
> - By induction hypothesis, (D^+,D^-) is in $\mathbf{AM'}$.

- If $x \in L^+$ then for some y, $x\#y \in D^+$, so
  $(\exists y, \mathrm{E}r', \exists y', x\#y\#r'\#y' \in D) \geq 1-1/2^{g(n)}$
- If $x \in L^-$ then for every y, $x\#y \in D^-$, so
  $(\exists y, \mathrm{E}r', \exists y', x\#y\#r'\#y' \in D) \leq 1/2^{g(n)}$
- Hence (L^+,L^-) is in **MAM'**… hence in **AM'**! □

The Arthur-Merlin hierarchy collapses

- We have proved: For every word w, **w′** ⊆ **AM′**
- If w_1 is a subword of w_2 (obtained by removing letters) then $\mathbf{w'_1} \subseteq \mathbf{w_2'}$
  E.g., **AM′** ⊆ **AAMAMMA′**, right?
- So, for every word w of the form $w_1\mathtt{A}w_2\mathtt{M}w_3$, **w′**=**AM′**.
- The remaining words are:
  — $w \in \mathtt{M}^+\mathtt{A}^+$: then **w′** = **MA′**
  — $w \in \mathtt{M}^+$: then **w′** = **M′** (=**NP′**)
  — $w \in \mathtt{A}^+$: then **w′** = **A′** (=**BPP′**)
  — $w = \varepsilon$: then **w′** = **P′**.

The Arthur-Merlin hierarchy collapses

- In summary:

AM′ (All other classes **w′** equal to **AM′**)

⊆

MA′

⊆ ⊇

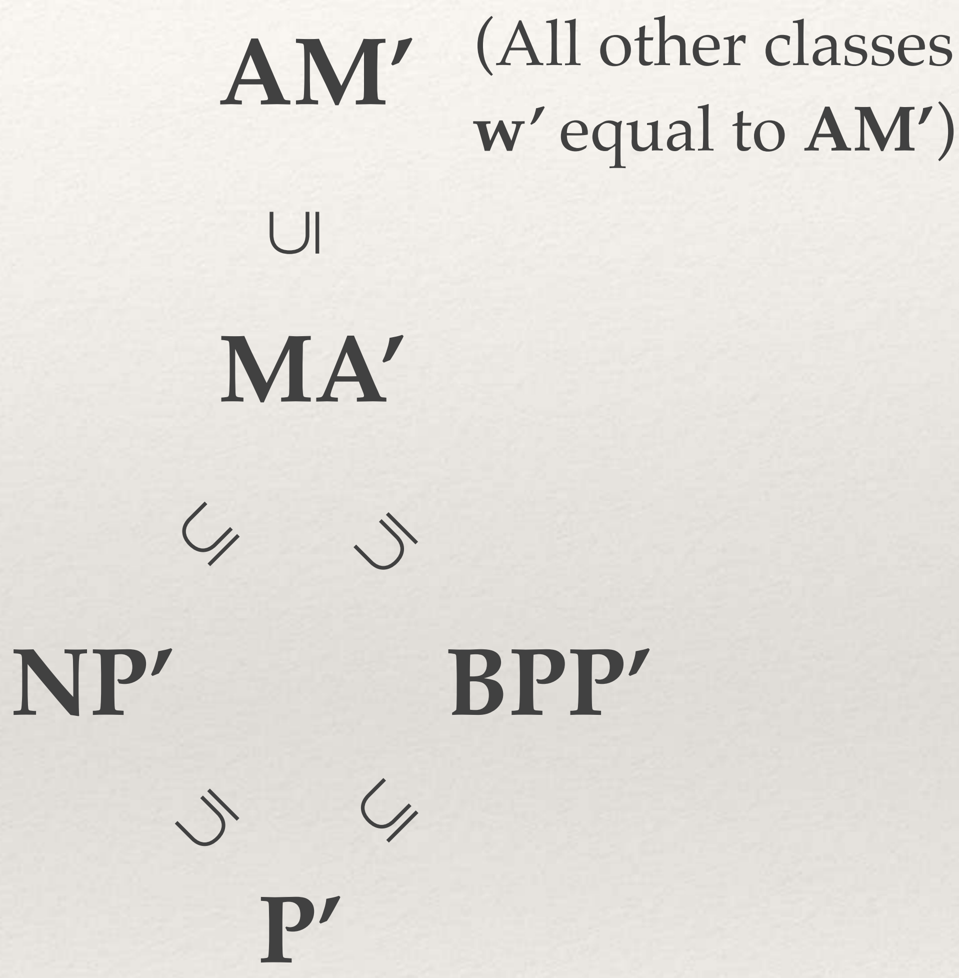
NP′ **BPP′**

⊇ ⊆

P′

The Arthur-Merlin hierarchy collapses

- We can equate a language L with the promise problem
  (L, complement of L)
- I.e., a promise problem (L^+,L^-) is a language iff
  L^+=complement of L^-
- Restricting to languages, we obtain…



The Arthur-Merlin hierarchy collapses

- **Thm 3.14 (Babai, Moran).**
  The A-M hierarchy collapses: there are no more than 5 different classes in the hierarchy.
- (No other relation known between these classes.)
- Note: the same technique shows that **AM**[$f(n)$+cst.] = **AM**[$f(n)$]… but no more.

(All other classes **w** equal to **AM**)

Variable number of turns $f(n)$… until now we only had a constant number of turns!

Next time…

Some more wonders!

- Sipser's coding lemmas
- **AM** is in the polynomial hierarchy
- The Goldwasser-Sipser theorem:
  public coins≡private coins
- The Boppana-Håstad-Zachos theorem:
  Graph Isomorphism is most certainly not **NP**-complete.