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
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): $(\exists y, E_r, F(x,y,r)) \geq 1 - 1/2^n$ (« huge »)
— or (2): $(\exists y, E_r, F(x,y,r)) \leq 1/2^n$ (« tiny »)

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

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

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

and $k \overset{\text{def}}{=} \lceil \frac{m}{n} \rceil$, $m \overset{\text{def}}{=} M(n) + \sigma(n)$

Why not just use « skolemization »?
(Hint: does not work.)
Permuting $E$ over $\exists$, à la Lautemann

- In case (1) (« huge »), $(E_r, F(x,y,r)) \geq 1 - 1/2^n$ 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 $r' / \wedge_{i=1}^k F(x,y,r' \oplus r_i)$

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): $(\exists y, \exists r, F(x,y,r)) \geq 1 - 1/2^n$ (« huge ») — or (2): $(\exists y, \exists r, F(x,y,r)) \leq 1/2^n$ (« tiny »)
Then for every poly $o(n)$, and for $n$ large enough, — in case (1), $F'(x)=1$ — in case (2), $F'(x) \leq 1/2^{o(n)}$
where $F'(x) \equiv E_{r_1, \ldots, r_k} \exists y, r', \wedge_{i=1}^k F(x,y,r' \oplus r_i)$ and $k \equiv m/n^\gamma, m \equiv p(n)+q(n)+g(n)$

- Let $r_1, \ldots, r_k$ be arbitrary. $\Pr_r(\neg \wedge_{i=1}^k F(x,y,r' \oplus r_i)) \\
\leq \sum_{i=1}^k \Pr_r(\neg F(x,y,r' \oplus r_i)) \\
\leq k / 2^n$
- Since $k=poly(n)$, this is $< 1$ for $n$ large enough.
Permuting $E$ over $\exists$, à la Lauteemann

- In case (2) (« tiny »),
  $(E_r, F(x,y,r)) \leq 1/2^n$ for every $y$.
- $\Pr_r(F(x,y,r)) \leq 1/2^n$ for every $y$. $(F(x,y,r)$ is a predicate!)
- $\Pr_{r_1,\ldots,r_k}(\exists y, r', \wedge_{i=1}^k F(x,y,r' \oplus r_i))$
  $\leq \sum_{y,r'} \Pr_{r_1,\ldots,r_k}(\wedge_{i=1}^k F(x,y,r' \oplus r_i))$
  $= \sum_{y,r'} \prod_{i=1}^k \Pr_{r_i}(F(x,y,r' \oplus r_i))$
  (independence)

$\Rightarrow$

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): $(\exists y, E_r, F(x,y,r)) \geq 1 - 1/2^n$ (« huge »)
- or (2): $(\exists y, E_r, F(x,y,r)) \leq 1/2^n$ (« 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 $F'(x) \equiv E_{r_1, \ldots, r_k} \exists y, r', \wedge_{i=1}^k F(x,y,r' \oplus r_i)$.

and $k \equiv \lceil m/n \rceil$, $m \equiv p(n)+q(n)+g(n)$

$\leq \sum_{y,r'} (1/2^n)^k$
$= 2^{p(n)+q(n)-nk}$
$\leq 1/2^{g(n)}$. $\square$
Thm 3.12 (Babai). $\text{MA} \subseteq \text{AM}$.

Proof. Let $L \in \text{MA}$.
For some $D \in \text{P}$,

(logical characterization of $\text{MA}$)
(1) if $x \in L$ then $(\exists y, E_r, x \# y \# r \in D) \geq 1 - 1/2^n$
(2) if $x \notin L$ then $(\exists y, E_r, x \# y \# r \in D) \leq 1/2^n$.

Prop (Lemme 3.11). Let $F(x,y,r)$ be a predicate

(1) if $x \in L$ then $(\exists y, E_r, x \# y \# r \in D) \geq 1 - 1/2^n$ (« huge »)
(2) if $x \notin L$ then $(\exists y, E_r, x \# y \# r \in D) \leq 1/2^n$ (« 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 $F'(x) \equiv E_r \land \cdots \land E_r \land (\exists y, r', \land_i F(x,y,r') \lor r_i)$.
and $k \equiv \lceil m/n \rceil$, $m \equiv p(n)+q(n)+g(n)$

Therefore $L$ is in $\text{AM}$. □

Ah yes, case (2) only applies for $n$ large enough. For small values of $n$, tabulate.
Lemma 3.11. MAM ⊆ AM.

Proof (1/2). Let $L \in \text{MAM}$.

For some $D \in \mathbb{P},$

(logical characterization of MAM)

(1) if $x \in L$ then $(\exists y, \text{Er}, \exists y', x \# y \# r \# y' \in D) \geq 1 - 1/2^n$

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

Applying the Proposition to $F(x,y,r) \equiv (\exists y', x \# y \# r \# y' \in D)$

(piadicate again!)

Then $F'(x) = \text{Er}_1, \ldots, r_k, \exists y, r', \wedge_{i=1}^{k} \exists y', (x \# y \# (r' \oplus r_i) \# y' \in D) \ldots$
Lemma 3.11. MAM $\subseteq$ AM.

Proof (2/2).

$F'(x) = E r_1, \ldots, r_k, \exists y, r', 
\land_{i=1}^k \exists y', (x \# y \# (r' \oplus r_i) \# y' \in D)$

$= E r_1, \ldots, r_k, \exists y, r', y'_1, \ldots, y'_k, 
\land_{i=1}^k (x \# y \# (r' \oplus r_i) \# y'_i \in D)$

Hence $L$ is in AM.  \(\square\)
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:
   \( \mathcal{L}^+ \overset{\text{def}}{=} \{ w \mid w \text{ parses as a satisfiable clause set } S \} \)
   \( \mathcal{L}^- \overset{\text{def}}{=} \{ w \mid w \text{ parses as an unsatisfiable clause set } S \} \)

❖ In general, a **promise problem** is a pair of two disjoint languages:
   INPUT: a word \( w \)
   PROMISE: \( w \in \mathcal{L}^+ \cup \mathcal{L}^- \)
   QUESTION: is \( w \) in \( \mathcal{L}^+ \)?
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:
  $L^+ = \{w \mid w$ parses as a satisfiable clause set $S\}$
  $L^- = \{w \mid w$ 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 $\text{BPP}'$ be the promise version of $\text{BPP}$, i.e.:
  - if $x \in L^+$ then $\Pr_r(x \not\in D) \geq 2/3$
  - if $x \in L^-$ then $\Pr_r(x \not\in D) \leq 1/3$
  where $D$ is a language in $\text{P}$.

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

- (There is no known $\text{BPP}$-complete problem.)
Promise versions of Arthur-Merlin games

- All the classes in the Arthur-Merlin hierarchy have analogues as **promise problems**: $\varepsilon', A', M', MA', AM'$, etc.

- $(L^+, L^-) \in \text{AMAM}...'$ 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 $G(x) \triangleq E_{r_1}, \exists y_1, E_{r_2}, \exists y_2, \ldots, P(x, r_1, y_1, r_2, y_2, \ldots)$

- **Thm 3.12'**. $\text{MA'} \subseteq \text{AM'}$.
- **Lemma 3.11'**. $\text{MAM'} \subseteq \text{AM'}$.
  (same proof as before!)
The Arthur-Merlin hierarchy collapses
The A-M’ hierarchy collapses

- We will show by induction on the length of $w$ that $w' \subseteq A M'$.
- Obvious if this length is 0.
- We will then look at the first letter of $w$, either A or M.
**w′ ⊆ AM′**: (1) *w* starts with *A* (1/5)

- Let *w* ≝ *A* *w*₂, and let (*L*, *L*⁻) ∈ *w*′.
  - if *x* ∈ *L*, then (Er, *F*(*x*, *r*)) ≥ 1 − 1/2²ᵍ⁻²
  - if *x* ∈ *L*⁻ then (Er, *F*(*x*, *r*)) ≤ 1/2²ᵍ⁻²

- Beware: *F* is not a predicate, so expectation ≠ probability

- But, with high probability on *r* (≥ 1 − 1/2⁸⁻₁),
  - if *x* ∈ *L*, then *F*(*x*, *r*) ≥ 1 − 1/2⁸⁻¹
  - if *x* ∈ *L*⁻ then *F*(*x*, *r*) ≤ 1/2⁸⁻¹

Why?

We reduce the error preventively. This will be needed.
Let $w \triangleq A w_2$, and let $(L^+, L^-) \in w'$.
- if $x \in L^+$, then $(\mathbb{E}r, F(x, r)) \geq 1 - 1/2^{2g(n)+2}$
- if $x \in L^-$ then $(\mathbb{E}r, F(x, r)) \leq 1/2^{2g(n)+2}$

We use Markov's inequality on:

- $X \triangleq F(x, \_)$ if $x \in L^-$: $\Pr_r(F(x, r) > 1/2^{g(n)+1}) \leq 1/2^{g(n)+1}$
  i.e., $\Pr_r(F(x, r) \leq 1/2^{g(n)+1}) \geq 1 - 1/2^{g(n)+1}$

- $X \triangleq 1-F(x, \_)$ if $x \in L^+$: $\Pr_r(1-F(x, r) > 1/2^{g(n)+1}) \leq 1/2^{g(n)+1}$
  i.e., $\Pr_r(F(x, r) \geq 1-1/2^{g(n)+1}) \geq 1-1/2^{g(n)+1}$
Let $w \equiv A w_2$, and let $(L^+, L^-) \in w'$.
- if $x \in L^+$, then $(E_r, F(x, r)) \geq 1 - 1/2^{2g(n)+2}$
- if $x \in L^-$, then $(E_r, F(x, r)) \leq 1/2^{2g(n)+2}$

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 $D^+ \equiv \{ x\#r \mid F(x, r) \geq 1 - 1/2^{g(n)+1} \}$
$\quad D^- \equiv \{ x\#r \mid F(x, r) \leq 1/2^{g(n)+1} \}$
$(D^+, D^-)$ is a promise language in $w_2'$.

By induction hypothesis, $(D^+, D^-)$ is in $\text{AM}'$.

This is where we need promise languages.
(We could hack our way without here, but we won’t be able to next time.)
$w' \subseteq AM'$: (1) $w$ starts with $A$ (4/5)

- Since $(D^+, D^-) \in AM'$, for some $D \in P$:
  - 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 $x \# r \not\in D^-$ 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 $w = A w_2$, and let $(L^+, L^-) \in w'$.
  - if $x \in L^+$, then $(Er, F(x, r)) \geq 1 - 1/2^g(n+1)$
  - if $x \in L^-$ then $(Er, F(x, r)) \leq 1/2^g(n+1)$

- 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 $D^+ = \{x \# r \mid F(x, r) \geq 1 - 1/2^g(n+1)\}$
  $D^- = \{x \# r \mid F(x, r) \leq 1/2^g(n+1)\}$
  $(D^+, D^-)$ is a promise language in $w_2$.

- By induction hypothesis, $(D^+, D^-)$ is in $AM'$.
$w' \subseteq \text{AM'}$: (1) $w$ starts with $A$ (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 $\text{AM'}$.

- Since $(L^+, L^-)$ was arbitrary in $w'$, $w' \subseteq \text{AM'}$. 
\( w' \subseteq \text{AM}' : (1) \ w \text{ starts with } M \ (1/2) \)

- Let \( w \overset{\text{def}}{=} Mw_2 \), and let \( (L^+, L^-) \in w' \).
  - 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 \( D^+ \overset{\text{def}}{=} \{ x\#y \mid F(x, y) \geq 1 - 1/2^{g(n)} \} \)
  \( D^- \overset{\text{def}}{=} \{ x\#y \mid F(x, y) \leq 1/2^{g(n)} \} \)
- \((D^+, D^-)\) is a promise language in \( w_2' \).
- By induction hypothesis, \((D^+, D^-)\) is in \text{AM}'.

This is much simpler!

This is where we need promise languages. No way we could use a single language \( D^+ = D^- \)
\[ w' \subseteq \text{AM'}: (1) \ w \text{ starts with } M \ (2/2) \]

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

- If \(x \in L^+\) then for some \(y, x \# y \in D^+\), so
  \[(\exists y, E r', \exists y', x \# y \# r' \# y' \in D) \geq 1 - 1/2^g(n)\]

- If \(x \in L^-\) then for every \(y, x \# y \in D^-\), so
  \[(\exists y, E r', \exists y', x \# y \# r' \# y' \in D) \leq 1/2^g(n)\]

- Hence \((L^+, L^-)\) is in \(\text{MAM'}\)… hence in \(\text{AM'}\)!

- Let \(w \equiv M w_2\), and let \((L^+, L^-) \in w'\):
  - 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 \(D^+ \equiv \{x \# y \mid F(x,y) \geq 1 - 1/2^g(n)\}\)
  \[D^- \equiv \{x \# y \mid F(x,y) \leq 1/2^g(n)\}\]

- \((D^+, D^-)\) is a promise language in \(w_2'\).

- By induction hypothesis, \((D^+, D^-)\) is in \(\text{AM'}\).
The Arthur-Merlin hierarchy collapses

- We have proved: For every word $w$, $w' \subseteq AM'$
- If $w$ is a subword of $w'$ (obtained by removing letters) then $w \subseteq w'$
  E.g., $AM' \subseteq AAMAMMA'$, right?
- So, for every word $w$ of the form $w_1Aw_2Mw_3$, $w' = AM'$.
- The remaining words are:
  - $w \in M^+A^+$: then $w' = MA'$
  - $w \in M^+$: then $w' = M'$ (=NP')
  - $w \in A^+$: then $w' = A'$ (=BPP')
  - $w = \epsilon$: then $w' = P'$. 
The Arthur-Merlin hierarchy collapses

In summary:

$\subseteq P' \subseteq BPP' \subseteq NP' \subseteq MA' \subseteq AM'$

(All other classes $w'$ equal to $AM'$)
The Arthur-Merlin hierarchy collapses

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

$(\text{AM}')$ (All other classes $w'$ equal to AM')
$(\text{MA}')$
$(\text{NP}')$
$(\text{BPP}')$
$(\text{P}')$
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 $\text{AM}[f(n)+\text{cst.}] = \text{AM}[f(n)]$... but no more.

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
- \textbf{AM} is in the polynomial hierarchy
- The Goldwasser-Sipser theorem: public coins $\equiv$ private coins
- The Boppana-Håstad-Zachos theorem: Graph Isomorphism is most certainly not \textbf{NP}-complete.