Randomized complexity classes

Today: Sipser’s coding lemmas, and consequences
Today

- 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.
Sipser’s coding lemmas
Hash tables

- Store elements of type $\sigma$ (e.g. strings)
  In general, associative array $\sigma \rightarrow \tau$

- **Hash-table** = table of size $N$
  **Hash function** $h : \sigma \rightarrow [0, N-1]$
  Each datum $x$ stored at position $h(x)$

- **Collision**: element $x$ of $\sigma$
  such that there is an element $x' \neq x$ of $\sigma$
  with $h(x) = h(x')$
Collisions

- In practice, one avoids collisions by:
  - storing **lists** of data \( x \) with the same \( h \) value instead of just elements
  - **resizing** the table (increasing \( N \)) in case of collisions

- But how can we ensure that \( N \) is large enough so that there are **no** collisions? How do we choose \( h \)?
Collisions

❖ In practice, one avoids collisions by:
— storing lists of data $x$ with the same $h$ value instead of just elements
— resizing the table (increasing $N$) in case of collisions
— using several hash functions $h_1, \ldots, h_\ell$

❖ Still, how can we ensure that $N$ is large enough so that there are no collisions? How do we choose $H \equiv (h_1, \ldots, h_\ell)$?
Carter and Wegman realized that you could draw $H \overset{\text{def}}{=} (h_1, \ldots, h_l)$ at random from certain so-called universal classes...

and there are very simple such classes!
Linear hash functions

- Let $\Sigma=\{0,1\} = \mathbb{Z}/2\mathbb{Z}$

- A **linear** hash function $h : \Sigma^{m} \rightarrow \Sigma^{m'}$
  is just a linear map between vector spaces (over $\mathbb{Z}/2\mathbb{Z}$)

- ... i.e., $h$ is given by a **matrix of bits** $B = (b_{ij})_{i=1..m', j=1..m}$:
  $$h(x_1, \ldots, x_m) = (b_{i1}x_1 + \ldots + b_{im}x_m)_{i=1..m'}$$

- For computer geeks, each row $(b_{i1}, \ldots, b_{im})$ is a **mask**
  and $b_{i1}x_1 + \ldots + b_{im}x_m$ is a **parity check**
  = exclusive or of the bits $x_j$ at those positions $j / b_{ij}=1$
Linear hash functions

❖ It is easy to draw $h$ at random uniformly: just draw $mm'$ bits independently, uniformly, at random.

❖ Let $X$ be the set of data to be stored. Sipser realized that:

❖ **(Coding lemma I):** if $X$ is sufficiently small, then drawing $H^{\equiv}(h_1, \ldots, h_l)$ at random, with high probability there will be no collision in $X$.

❖ **(Coding lemma II):** if $X$ is too large, then whichever $H^{\equiv}(h_1, \ldots, h_l)$ you take, there will definitely be a collision in $X$.

---

A linear hash function $h : \Sigma^m \rightarrow \Sigma^{m'}$ is just a linear map between vector spaces (over $\mathbb{Z}/2\mathbb{Z}$).

... i.e., $h$ is given by a matrix of bits $B = (b_{ij})_{i=1..m', j=1..m}$:

$$h(x_1, \ldots, x_m) = (b_{i1}x_1 + \ldots + b_{im}x_m)_{i=1..m'}$$
The definition of collisions

- A collision \( x \) for \( H = (h_1, \ldots, h_c) : \sum^m \rightarrow \sum^{m'} \) in \( X \) is a point:
  - in \( X \)
  - such that there are points \( y_1, \ldots, y_c \)
    - all in \( X \)
    - all distinct from \( x \)
    - but \( h_1(x) = h_1(y_1), \ldots, h_c(x) = h_c(y_c) \).
  - If such an \( x \) exists, we say that \( X \) has a collision for \( H \).
Lemma (3.15). Let $X \subseteq \Sigma^m$. Assume $|X| \leq 2^{m' - 1}$. Let $\ell \geq m'$.
Then $\Pr_H(X \text{ has a collision for } H) \leq 1/2^{\ell - m' + 1}$.

Proof (1/5). We start by proving:

Claim. For every non-zero $y \in \Sigma^m$,
$$\Pr_z(z \cdot y = 0) = \Pr_z(z \cdot y = 1) = 1/2.$$ 

Indeed, $y$ has a non-zero coordinate $y_i$ (hence $y_i = 1$)
Let $t \equiv (0, \ldots, 0, 1, 0, \ldots, 0)$ with the only 1 at position $i$.
Then $z \mapsto z \oplus t$ (flip bit $i$) is a bijection
of $\{z \in \Sigma^m \mid z \cdot y = 0\}$ onto $\{z \in \Sigma^m \mid z \cdot y = 1\}$. 

A collision $x$ for $H^d(h_1, \ldots, h_d)$ in $X$ is a point:
— in $X$
— such that there are points $y_1, \ldots, y_d$
— all in $X$
— all distinct from $x$
— but $h_1(x) = h_1(y_1), \ldots, h_d(x) = h_d(y_d)$. 

Sipser’s coding lemma I ($X$ small)
Lemma (3.15). Let \( X \subseteq \Sigma^m \). Assume \( |X| \leq 2^{m' - 1} \). Let \( \ell \geq m' \).

Then \( \Pr_H(X \text{ has a collision for } H) \leq 1 / 2^{\ell - m' + 1} \).

Proof (2/5). Recap:

Claim. For every non-zero \( y \in \Sigma^m \),
\[
\Pr_z(z \cdot y = 0) = \Pr_z(z \cdot y = 1) = 1/2.
\]

In particular, if \( x \neq y_j \), then \( \Pr_z(z \cdot x = z \cdot y_j) = 1/2 \)
(take \( y \overset{\text{def}}{=} x - y_j \)).
Lemma (3.15). Let \( X \subseteq \Sigma^m \). Assume \( |X| \leq 2^{m'-1} \). Let \( \ell \geq m' \).

Then \( \Pr_H(X \text{ has a collision for } H) \leq 1/2^{\ell-m'+1} \).

Proof (3/5). Recap:

If \( x \neq y_j \), then \( \Pr_z(z . x = z . y_j) = 1/2 \)

Hence \( \Pr_h(h(x) = h(y_j)) \)

\[ = \Pr_B(m' \times m) \text{ matrix}(B . x = B . y_j) \]

\[ = \Pr_B(m' \times m) \text{ matrix}(\forall \text{row } z \text{ of } B, z . x = z . y_j) = 1/2^{m'} \]
Lemma (3.15). Let $X \subseteq \Sigma^m$. Assume $|X| \leq 2^{m'-1}$. Let $\ell \geq m'$. Then $\Pr_H(X \text{ has a collision for } H) \leq 1/2^{\ell-m'+1}$.

Proof (4/5).
$\Pr_h(h(x)=h(y_j)) = 1/2^{m'}$ (recap).

$\Pr_H(x \text{ is a collision for } H \text{ in } X)$
$= \Pr_H(\exists y_1, \ldots, y_\ell \in X-\{x\}, \land_{j=1}^\ell h_j(x)=h_j(y_j))$

$\leq \sum_{y_1, \ldots, y_\ell \in X-\{x\}} \prod_{j=1}^\ell \Pr_h(h(x)=h(y_j))$ (sum bound+independence)

$\leq (|X|-1)^\ell / 2^{\ell m'} < 1/2^\ell$
Lemma (3.15). Let \( X \subseteq \Sigma^m \). Assume \( |X| \leq 2^{m'-1} \). Let \( \ell \geq m' \).
Then \( \Pr_H(X \text{ has a collision for } H) \leq 1/2^{\ell-m'+1} \).

Proof (5/5). Recap:
\[ \Pr_H(x \text{ is a collision for } H \text{ in } X) < 1/2^\ell \]
\[ \Pr_H(X \text{ has a collision for } H) = \Pr_H(\exists x \in X, \ x \text{ is a collision for } H \text{ in } X) \]
\[ \leq |X|/2^\ell \leq 1/2^{\ell-m'+1}. \square \]
Lemma (3.16). Let $X \subseteq \sum^m$. Assume $|X| > \ell \cdot 2^{m'}$. Then $X$ (definitely) has a collision for $H$.

Proof. A collision $x$ for $H$ in $X$ is a point in $X$ / $\forall j (1 \leq j \leq \ell), \exists y (\neq y_j) \in X \setminus \{x\}, h_j(x) = h_j(y)$

Hence, if $X$ has no collision for $H$, then for each $x \in X$, there is a $j (1 \leq j \leq \ell) / \forall y \in X \setminus \{x\}, h_j(x) \neq h_j(y)$

For each $x \in X$, let $\kappa(x) \triangleq$ the least such $j$.

Then $x \in X \rightarrow (j, h_j(x))$ where $j = \kappa(x)$ is injective

... since otherwise $\exists y \in X \setminus \{x\}, j = \kappa(x) = \kappa(y))$ and $h_j(x) = h_j(y)$

Hence $\text{card } X \leq \ell \cdot \text{card } \sum^{m'} = \ell \cdot 2^{m'}$. $\square$
Assume you are given a set $R$, which is either large or small. Let the gap be $\text{size}(\text{large}) / \text{size}(\text{small})$. We now have two techniques to better decide whether $R$ is large or small.

**Lautemann:** (as used in Babai’s theorem, Lemma 3.11)
- $R$ large $\Rightarrow \forall r_1, \ldots, r_k, \exists r', r' \oplus r_i \in R$
- $R$ small $\Rightarrow \Pr_{r_1, \ldots, r_k}(\exists r', r' \oplus r_i \in R)$ small

**Sipser:**
- $R$ large $\Rightarrow \forall H, \exists$ collision for $H$ in $R$
- $R$ small $\Rightarrow \Pr_H(\exists$ collision for $H$ in $R)$ small

- No error if $R$ large
- Requires gap $(1-1/2^n)/(1/2^n) \sim 2^n$
- No error if $R$ large
- Only needs gap $\ell 2^{m'}/2^{m'-1} = 2\ell = \text{poly}(n)$
Lautemann or Sipser?

- Sipser will have a real advantage over Lautemann only later, when we show that GNI is in AM, not just in IP[1]
- … and in principle when we show the Goldwasser-Sipser theorem (later)
- For now, we will use Sipser to show that AM ⊆ \Pi^p_2 and Lautemann would be just as practical here
- We start by showing that for every language \(L \in AM\), we can require perfect soundness (=no error if \(x \in L\)).
\( \text{AM} \subseteq \Pi^p_2 \)
AM with perfect soundness (1/4)

- Let $L$ be in AM. For some $D \in \text{P}$,
  - if $x \in L$ then $(\exists r, \exists y, x \# r \# y \in D) \geq 1 - 1/2^n$ (« large »)
  - if $x \notin L$ then $(\exists r, \exists y, x \# r \# y \in D) \leq 1/2^n$ (« small »)
- Let $R \equiv \{ r \in \sum^{m} | \exists y, x \# r \# y \in D \}$ (either large or small)
- Arthur draws $H \equiv (h_1, \ldots, h_l)$ at random uniformly ($mm'\ell$ bits)
- Merlin answers a (claimed) collision $r$ in $R$
- We check that this is a collision.
  - if $x \in L$ then $\forall H, \exists \text{collision for } H \text{ in } R$ (perfect soundness!)
  - if $x \notin L$ then $\Pr_H(\exists \text{collision for } H \text{ in } R) \leq 1/2^{\ell-m'+1}$

Can we really do this in polynomial time?
AM with perfect soundness (2/4)

- \(m=q(n)\) (assume \(m \geq n\)): determine \(m', \ell\)

- Use Sipser I and II:
  - To apply Sipser I, need \(|R| \leq 2^{m'-1}\) if \(x \notin L\) ⇒ e.g., require \(m'-1 \geq m-n\) (1)
  - To apply Sipser II, need \(|R| > \ell 2^{m'}\) if \(x \in L\) ⇒ e.g., require \(m' + \log_2 \ell < m-1\) (2)
  - We wish error to be \(\leq 1/2^{g(n)}\) ⇒ require \(\ell-m'+1 \geq g(n)\) (3)
  - Other constraints: \(\ell \geq m'\) (4), both polynomial in \(n\).

- Let \(L\) be in AM. For some \(D \in \mathbb{P}\),
  - if \(x \in L\) then \((E_r, \exists y, x \# r \# y \in D) \geq 1 - 1/2^n\) (« large »)
  - if \(x \notin L\) then \((E_r, \exists y, x \# r \# y \in D) \leq 1/2^n\) (« small »)
- Let \(R \equiv \{ r \in \Sigma^m \mid \exists y, x \# r \# y \in D\}\) (either large or small)
- Arthur draws \(H=h_1, \ldots, h_d\) at random uniformly (\(mm'\) bits)
- Merlin answers a (claimed) collision \(r\) in \(R\)
- We check that this is a collision.
  - if \(x \in L\) then \(\forall H, \exists\) collision for \(H\) in \(R\) (perfect soundness)
  - if \(x \notin L\) then \(\Pr[H(\exists\) collision for \(H\) in \(R\)\)] \leq 1/2^{\ell-m'+1}

- E.g., \(m' \equiv m-n+1\) (for (1)), \(\ell \equiv m'+g(n)\) (for (3), (4))
  - (2) OK for \(n\) large enough, otherwise tabulate
Now $m, m', t = \text{poly}(n)$ Can we check that $r$ is a collision in $R$ in poly time?

No: just checking that $r$ is in $R$ is an NP problem…

Instead…
We require Merlin to give us:

- a claimed collision \( r \)
- a proof \( y \) that \( r \in R \) (i.e., Merlin claims that \( x \# r \# y \in D \))
- points \( r_1, \ldots, r_\ell \)
- proofs \( y_j \) that each \( r_j \) is in \( R \)

And we check that \( x \# r \# y \in D \),
\[
x \# r_j \# y_j \in D \text{ for each } j=1..\ell,
\]
\( r \neq r_j \) and \( h_j(r) = h_j(r_j) \) for each \( j=1..\ell \). \( \square \)
We have proved:

**Prop (3.18).** Every $L \in \text{AM}$ can be decided with an AM game with perfect soundness (no error if $x \in L$).

Hence:

**Thm (3.19).** $\text{AM} \subseteq \Pi^p_2$.

Proof. $x \in L$ iff $\forall H, \exists \text{collision for } H \text{ in } R$ (with proofs!) and proofs of collisions can be checked in poly time. $\square$
Graph Non-Isomorphism is in AM
Reminder: Graph **Non-Isomorphism**

- **GNI** $\overset{\text{def}}{=} \text{complement of GI}$: in $\text{coNP}$, not known to be in $\text{P}$ or $\text{coNP}$-complete

- **Prop.** GNI is in $\text{IP}[1]$.  

  **Algorithm.**
  — Arthur draws $i \in \{1, 2\}$, $\pi \in S_N$ at random uniformly, sends $q \overset{\text{def}}{=} \pi.G_i$
  — Merlin answers $j \in \{1, 2\}$
  — We accept if $i=j$, reject otherwise.

---

**GI**

**INPUT:** 2 graphs $G_1=(V, E_1)$, $G_2=(V, E_2)$ (with the same $V$)

**QUESTION:** are $G_1, G_2$ isomorphic?

Note: it is crucial here that $i$ remains secret! This is not an AM game
GNI is in AM

- **Idea:** (that fails, but we will fix this later)
  Let $X_i \triangleq \{\text{graphs } G \text{ on } V \text{ such that } G \equiv G_i\}$,
  $X \triangleq X_1 \cup X_2$
- Imagine $|X_1| \approx |X_2| \approx K$
- If $(G_1, G_2) \in \text{GNI}$, i.e. if $G_1 \not\equiv G_2$ then $|X| \approx 2K$ ($X$ is large)
- Otherwise $|X| \approx K$ ($X$ is small)
- We test which is the case using Sipser (All random bits in $H$ are public $\Rightarrow$ in AM.)

Oops, gap is only 2: not enough for Sipser, but we will see later how to increase it.
Building sets of uniform size

- $X_i$ is the orbit of $G_i$ under the group action of $S_N$ on $G_N$
- Let $\phi_i \triangleq \{\pi \in S_N \mid \pi.G_i = G_i\}$
- The orbit-stabilizer thm:
  $|\text{orbit}| \times |\text{stabilizer}| = \text{order of the group } S_N$
- I.e., $|X_i \times \phi_i| = N!$
- ... independently of $i$.

GI
INPUT: 2 graphs $G_1=(V, E_1)$, $G_2=(V, E_2)$ (with the same $V$)
QUESTION: are $G_1$, $G_2$ isomorphic?

- Let $V = \{1, \ldots, N\}$ set of vertices,
  $G_N \cong$ directed graphs on $V$,
  $S_N \cong$ group of permutations of $V$.
- $S_N$ acts on $G_N$ by: $\forall \pi \in S_N, \forall G=(V,E) \in S_N$,
  $\pi.G = (V, \{(\pi(u), \pi(v)) \mid (u, v) \in E\}$
- Two graphs $G_1=(V, E_1)$, $G_2=(V, E_2)$ (with the same $V$)
  are isomorphic $(G_1 \cong G_2)$ iff $\exists \pi \in S_N, \pi.G_1=G_2$. 
Building sets of uniform size

- Hence let $X'_i \overset{def}{=} X_i \times \phi_i = \{(G, \pi) \mid G \equiv G_i \text{ et } \pi.G_i = G_i\}$,
  $X \overset{def}{=} X'_1 \cup X'_2$

- If $(G_1, G_2) \in \text{GNI}$, i.e.
  if $G_1 \not\equiv G_2$ then $|X| = 2N$

- Otherwise $|X| = N$

- Good... but gap is still only 2.
The power trick (repeating experiments virtually)

- Hence let $X'_i \overset{\text{def}}{=} X_i \times \phi_i = \{(G, \pi) \mid G \cong G_i \text{ et } \pi.G_i = G_i\}$, 
  $X \overset{\text{def}}{=} (X'_1 \cup X'_2)^k$

- If $(G_1, G_2) \in \text{GNI}$, i.e. 
  if $G_1 \not\cong G_2$ then $|X| = (2N!)^k$

- Otherwise $|X| = (N!)^k$

- Gap is now $2^k$. 
  Now take $k$ so large that this exceeds $2^\ell$. 

**GI**

INPUT: 2 graphs $G_1=(V, E_1)$, $G_2=(V, E_2)$ (with the same $V$) 
QUESTION: are $G_1$, $G_2$ isomorphic?

- $X_i$ is the orbit of $G_i$ under the group action of $S_N$ on $G_N$
- Let $\phi_i \overset{\text{def}}{=} \{\pi \in S_N \mid \pi.G_i = G_i\}$ stabilizer of $G_i$
- The orbit-stabilizer thm: $|X_i \times \phi_i| = N!$
GNI is in AM

- Arthur draws $H \overset{\text{def}}{=} (h_1, \ldots, h_{\ell})$ at random uniformly ($mm'\ell$ bits)
- Merlin answers a (claimed) collision $x$ in $X$ (with proofs!)
- We check (the proofs) that this is a collision.
  — if $(G_1, G_2) \in \text{GNI}$ then $\forall H$, $\exists$ collision for $H$ in $X$
  — if $(G_1, G_2) \notin \text{GNI}$ then
    $$\Pr_H(\exists \text{collision for } H \text{ in } R) \leq 1/2^{\ell-m'+1}$$

Let $X'_{i} \equiv X_{i} \times \phi_{i} = \{(G,\pi) \mid G \equiv G_{i} \text{ et } \pi.G_{i} = G_{i}\}$, $X \equiv (X'_{1} \cup X'_{2})^{k}$

We need to tune $m, m', \ell$ and $k$ so that the error is $\leq 1/2^{3(n)}$
Determining $m, m', \ell, \text{ and } k$

Note: size(graph)=$N^2$ (adjacency matrix)
size(input)=$n=2N^2$

- $m = k \times \text{ (size(graph)}+\text{size(permutation)})$
  $= O(k(N^2+N \log N)) = O(kN^2) = O(kn)$

- Use Sipser I and II:

  **Lemma (3.15).** Let $X \subseteq \Sigma^m$. Assume $|X| \leq 2^{m-1}$. Let $\ell \geq m'$.
  Then $\Pr_H(X \text{ has a collision for } H) \leq 1/2^{\ell-m'+1}$.

  **Lemma (3.16).** Let $X \subseteq \Sigma^m$. Assume $|X| > \ell \cdot 2^{m'}$, where $\ell \geq m'$.
  Then $X$ (definitely) has a collision for $H$.

- Sipser I: need $|X| \leq 2^{m'-1}$ if $(G_1, G_2) \notin \text{ GNI}$ ⇒ require $m'-1 \geq k \log_2(N!)$ (1)

- Sipser II: need $|X| > \ell \cdot 2^{m'}$ if $(G_1, G_2) \in \text{ GNI}$ ⇒ require $m'+\log_2 \ell < k(1+\log_2(N!))$ (2)

- We wish error to be $\leq 1/2^g(n)$ ⇒ require $\ell - m' + 1 \geq g(n)$ (3)

- Other constraints: $\ell \geq m'$ (4), all of $m, m', \ell, k$ polynomial in $n$.

E.g., $k \equiv N, m' \equiv 1+k \log_2(N!)$ (for 1), $\ell \equiv m'+g(n)$ (for 3, 4)
(2) OK for $n$ large enough, otherwise tabulate
Checking (proofs of) collisions

- Explicitly, Merlin sends:
  - an element $x$
  - a proof that $x$ is in $X$
  - elements $x_1, \ldots, x_\ell$
  - proofs that each $x_j$ is in $X$

- Then we will check the proofs
  $+ x \neq x_j$ and $h_j(x) = h_j(x_j)$ for each $j=1..\ell$.

- A proof that $x \equiv ((G_1',\pi_1),\ldots,(G_k',\pi_k))$ is in $X$ is:
  - for each $i=1..k$, a permutation $\pi'_i / \pi_i$. $G'_i = G_1$ or $G_2$
  - Checking it means checking $\pi'_i.G'_i = G_1$ or $G_2$,
    and also $\pi_i.G'_i = G'_i$, for each $i$.

Let $X'_i \equiv X_i \times \phi_i = \{(G,\pi) \mid G \equiv G_i \text{ et } \pi.G_i = G_i\}$,
$X \equiv (X'_1 \cup X'_2)^k$
We have proved:

**Prop (3.17).** GNI is in AM (not just IP[1]).

In fact:

**Thm (3.25; Goldwasser-Sipser).** For every $k \geq 1$, $\text{IP}[k] \subseteq \text{AM}[k+1]$.

I will omit the proof, see the lecture notes.

So $\text{AM} \subseteq \text{IP}[1] \subseteq \ldots \subseteq \text{IP}[k] \subseteq \text{AM}[k+1] = \text{AM}$.

**Corl.** For every $k \geq 1$, $\text{IP}[k] = \text{AM}[k] = \text{AM}$. (!)
The Boppana-Håstad-Zachos theorem

Babai (1985) and Goldwasser, Micah and Rackoff (1985) introduced two probabilistic extensions of the complexity classes NP and co-NP. The two complexity classes, denoted AM(γ) and IP(γ) respectively, are defined using randomized interactive proofs. Babai (1985) proved that the two classes are equal. We prove that if a complexity class co-NP is contained in IP[k] for some constant k (i.e., if every language in co-NP has a short interactive proof), then the polynomial-time hierarchy collapses to the second level. As a corollary, we show that if the Graph Isomorphism problem is NP-complete, then the polynomial-time hierarchy collapses.


Keywords: Interactive Proofs, Complexity Classes, Graph Isomorphism.
The Boppana-Håstad-Zachos theorem

Thm (3.20). If coNP ⊆ AM then PH collapses at level 2.

Proof. Let \( L \in \Sigma_{p2} \). We will show that \( L \) is in \( \Pi_{p2} \).
\[
L = \{ x \mid \exists y, (x,y) \in L' \}, \text{ for some } L' \in \text{ coNP}.
\]

Hence \( L' \in \text{ AM} \). There is a \( D \) in \( P \) such that:
— if \( (x,y) \in L' \) then \( (E_r, \exists z, x\#y\#r\#z \in D) \) large
— if \( (x,y) \not\in L' \) then \( (E_r, \exists z, x\#y\#r\#z \in D) \) small

— if \( x \in L \) then \( (\exists y, E_r, \exists z, x\#y\#r\#z \in D) \) large
— if \( x \not\in L \) then \( (\exists y, E_r, \exists z, x\#y\#r\#z \in D) \) small

Hence \( L \in \text{ MAM} = \text{ AM (Babai)} \subseteq \Pi_{p2} \). \( \square \)
Corl (3.21). If GI is \textbf{NP}-complete then \textbf{PH} collapses at level 2.

\textit{Proof.} \textbf{AM} is closed under poly time reductions.

Remember that \textbf{GNI} is in \textbf{AM}, as we have just shown.

Hence if GI is \textbf{NP}-complete, then \textbf{GNI} is \textbf{coNP}-complete, hence \textbf{coNP} \subseteq \textbf{AM}.

Now apply the previous theorem. □
Graph Isomorphism

- Corl (3.21). If GI is \textbf{NP}-complete then \textbf{PH} collapses at level 2.

- Remember that GI is not known to be in \textbf{P}, and not known to be \textbf{NP}-complete.

- The BHZ theorem shows that the latter is unlikely.

- Note: Babai gave a super polynomial time algo for GI in 2015 (still does not solve the question, but what a progress!); builds on a lot of things, including BHZ.
Next time...
IP and PSPACE

- IP and AM with polynomially many rounds (the classes IP and ABPP)
- Shamir’s theorem: ABPP=IP=PSPACE (!)