BILL AND NATHAN, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Graph Isomorphism Is Probably Not NPC

Graph Isomorphism: A History

Def **Graph Isomorphism (GI)** is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

Graph Isomorphism: A History

Def **Graph Isomorphism** ($\mathbf{GI}$) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions.

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

3) Over the years the following are shown.

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

3) Over the years the following are shown.
a) Degree or genus of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$.

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

3) Over the years the following are shown.
a) Degree or genus of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$.
b) Eigenvalue Mult of G_1, G_2 bounded $\rightarrow$ $\mathrm{GI} \in \mathrm{P}$ (Mount's PhD).

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

3) Over the years the following are shown.
a) Degree or genus of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$.
b) Eigenvalue Mult of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$ (Mount's PhD).
c) GI is in $n^{\log^k n}$ for some k (likely $k = 3$).

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions.
This is not a proof that GI is not NPC!.

3) Over the years the following are shown.
a) Degree or genus of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$.
b) Eigenvalue Mult of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$ (Mount's PhD).
c) GI is in $n^{\log^k n}$ for some k (likely $k = 3$).
c) $\rightarrow$ (GI NPC $\rightarrow \mathrm{NP} \subseteq \mathrm{DTIME}(n^{\log^{O(1)} n})$).

Graph Isomorphism: A History

Def Graph Isomorphism (GI) is, given two graphs, are they isomorphic, denoted $G_1 \simeq G_2$. GI is clearly in NP.

1) Since 1971 people tried hard to prove GI is NPC (There is a rumor that Levin thought GI is NPC and delayed publishing his paper since he wanted to include that result).

2) They did not manage it. Informally the reason is that GI is too rigid. That is, a very slight change in one of the graphs can send the (G_1, G_2) from GI to $\overline{\mathrm{GI}}$, which gets in the way of reductions. **This is not a proof that GI is not NPC!**.

3) Over the years the following are shown.
a) Degree or genus of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$.
b) Eigenvalue Mult of G_1, G_2 bounded $\rightarrow \mathrm{GI} \in \mathrm{P}$ (Mount's PhD).
c) GI is in $n^{\log^k n}$ for some k (likely $k = 3$).
c) $\rightarrow$ (GI NPC $\rightarrow \mathrm{NP} \subseteq \mathrm{DTIME}(n^{\log^{O(1)} n})$).

We show a different reason why GI NPC is unlikely.

An Interactive Protocol for $\overline{GI}$

Intuition: Why GI is Diff than SAT: SAT

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.

Alice could give Bob **The entire Truth Table For ϕ**.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.

Alice could give Bob **The entire Truth Table For ϕ**.

Can Alice give Bob **short proof** that $\phi \in \mathrm{TAUT}$? Discuss.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from $\mathbf{TAUT}$:$\mathbf{TAUT}$

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.
Alice could give Bob **The entire Truth Table For ϕ**.

Can Alice give Bob **short proof** that $\phi \in \mathrm{TAUT}$? Discuss.
We do not know; however, we think not.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.
Alice could give Bob **The entire Truth Table For ϕ**.

Can Alice give Bob **short proof** that $\phi \in \mathrm{TAUT}$? Discuss.
We do not know; however, we think not.

More precise We do not think $\mathrm{TAUT} \in \mathrm{NP}$.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.
Alice could give Bob **The entire Truth Table For ϕ**.

Can Alice give Bob **short proof** that $\phi \in \mathrm{TAUT}$? Discuss.
We do not know; however, we think not.

More precise We do not think $\mathrm{TAUT} \in \mathrm{NP}$.

Alice wants to convince Bob $(G_1, G_2) \in \overline{\mathrm{GI}}$. How? Discuss.

Intuition: Why GI is Diff than SAT: SAT

The title is not quite right. It should be

Intuition: Why $\overline{\mathrm{GI}}$ diff from TAUT:TAUT

Alice wants to convince Bob $\phi \in \mathrm{TAUT}$. How? Discuss.
Alice could give Bob **The entire Truth Table For ϕ**.

Can Alice give Bob **short proof** that $\phi \in \mathrm{TAUT}$? Discuss.
We do not know; however, we think not.

More precise We do not think $\mathrm{TAUT} \in \mathrm{NP}$.

Alice wants to convince Bob $(G_1, G_2) \in \overline{\mathrm{GI}}$. How? Discuss.
GOTO Next Page.

Intuition: why $\overline{\mathrm{GI}}$ is diff from $\mathrm{TAUT{:}GI}$

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$. That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

1) Bob sends Alice a challenge, Alice responds, Bob verifies.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

1) Bob sends Alice a challenge, Alice responds, Bob verifies.
2) Bob flips coins to decide what to send. He verifies in poly.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

1) Bob sends Alice a challenge, Alice responds, Bob verifies.
2) Bob flips coins to decide what to send. He verifies in poly.
3) We allow a probability of error.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$. That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

1) Bob sends Alice a challenge, Alice responds, Bob verifies.
2) Bob flips coins to decide what to send. He verifies in poly.
3) We allow a probability of error.
4) This is $\mathrm{IP}(2)$. 2 is for 2 rounds. We won't define formally.

Intuition: why $\overline{\mathrm{GI}}$ is diff from TAUT:GI

The following would be great but it is not known: $\overline{\mathrm{GI}} \in \mathrm{NP}$.
That would contrast TAUT. Alas don't know if this is true.

Alice wants to convince Bob that $(G_1, G_2) \in \overline{\mathrm{GI}}$.

We put several twists on **Alice sends short verifiable proof**.

1) Bob sends Alice a challenge, Alice responds, Bob verifies.
2) Bob flips coins to decide what to send. He verifies in poly.
3) We allow a probability of error.
4) This is $\mathrm{IP}(2)$. 2 is for 2 rounds. We won't define formally.
We show $\overline{\mathrm{GI}} \in \mathrm{IP}(2)$ on next slide.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \to$ Alice can tell $H_i \simeq G_{b_i}$.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can tell $H_i \simeq G_{b_i}$.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Alice is clueless. Uninformed guess possible.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can tell $H_i \simeq G_{b_i}$.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Alice is clueless. Uninformed guess possible.
5) Alice sends an n bit string $c_1 \cdots c_n$.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can tell $H_i \simeq G_{b_i}$.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Alice is clueless. Uninformed guess possible.
5) Alice sends an n bit string $c_1 \cdots c_n$.
6) $b_1 \cdots b_n = c_1 \cdots c_n \rightarrow$ Bob accepts, else Bob rejects.
Easy to show

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can tell $H_i \simeq G_{b_i}$.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Alice is clueless. Uninformed guess possible.
5) Alice sends an n bit string $c_1 \cdots c_n$.
6) $b_1 \cdots b_n = c_1 \cdots c_n \rightarrow$ Bob accepts, else Bob rejects.
Easy to show
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can send the correct string.

$\overline{GI}$ is in IP(2)

1) Alice and Bob are both looking at G_1, G_2 both on n vertices.
2) Bob flips a coin n times get a seq $b_1 \cdots b_n$.
3) For $1 \le i \le n$ Bob rand permutes vertices of G_{b_i} to get H_i.
4) Bob sends $H_1, \ldots, H_n$ to Alice. This is a challenge!
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can tell $H_i \simeq G_{b_i}$.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Alice is clueless. Uninformed guess possible.
5) Alice sends an n bit string $c_1 \cdots c_n$.
6) $b_1 \cdots b_n = c_1 \cdots c_n \rightarrow$ Bob accepts, else Bob rejects.
Easy to show
$(G_1, G_2) \in \overline{\mathrm{GI}} \rightarrow$ Alice can send the correct string.
$(G_1, G_2) \notin \overline{\mathrm{GI}} \rightarrow$ Prob Alice sends the correct string is $\frac{1}{2^n}$.

An Interactive Protocol for $\overline{GI}$ With Public Coins Set Up

Private Coins, Public Coins

IP(2) used **Private Coins**. Alice does not get to see Bob's coins.
Def A is in Arthur-Merlin (AM) if $A \in \mathrm{IP}(2)$ but Alice gets to see Bob's coin flips. We do not define this formally.

Private Coins, Public Coins

IP(2) used **Private Coins**. Alice does not get to see Bob's coins.
Def A is in Arthur-Merlin (AM) if $A \in \mathrm{IP}(2)$ but Alice gets to see Bob's coin flips. We do not define this formally.

1) Why called Arthur-Merlin? King Arthur gives Merlin a challenge openly, and Merlin the wizard (all powerful) responds.

Private Coins, Public Coins

IP(2) used **Private Coins**. Alice does not get to see Bob's coins.
Def A is in Arthur-Merlin (AM) if $A \in \mathrm{IP}(2)$ but Alice gets to see Bob's coin flips. We do not define this formally.

1) Why called Arthur-Merlin? King Arthur gives Merlin a challenge openly, and Merlin the wizard (all powerful) responds.

2) We will show $\overline{\mathrm{GI}} \in \mathrm{AM}$. We then show that this implies something unlikely happens. We discuss this in more detail later.

Needed Graph Theory

Notation Henceforth G_1, G_2 will be the pair of graphs Merlin and Arthur are looking at, and n will be the number of vertices on them.

Needed Graph Theory

Notation Henceforth G_1, G_2 will be the pair of graphs Merlin and Arthur are looking at, and n will be the number of vertices on them.

Notation S_n is the set of ALL permutations of $\{1, \ldots, n\}$. Let $\sigma \in S_n$. Then $\sigma(G) = (V, E')$ where

$$E' = \{(\sigma(x), \sigma(y)) : (x, y) \in E\}.$$

Needed Graph Theory

Notation Henceforth G_1, G_2 will be the pair of graphs Merlin and Arthur are looking at, and n will be the number of vertices on them.

Notation S_n is the set of ALL permutations of $\{1, \ldots, n\}$. Let $\sigma \in S_n$. Then $\sigma(G) = (V, E')$ where

$$E' = \{(\sigma(x), \sigma(y)) : (x, y) \in E\}.$$

Def Let G be a graph. An **Automorphism** is an isomorphism from G to itself. $\mathrm{AUT}(G)$ is the set of all automorphism. Note $\mathrm{AUT}(G) \subseteq S_n$.

Needed Graph Theory

Notation Henceforth G_1, G_2 will be the pair of graphs Merlin and Arthur are looking at, and n will be the number of vertices on them.

Notation S_n is the set of ALL permutations of $\{1, \ldots, n\}$. Let $\sigma \in S_n$. Then $\sigma(G) = (V, E')$ where

$$E' = \{(\sigma(x), \sigma(y)) : (x, y) \in E\}.$$

Def Let G be a graph. An **Automorphism** is an isomorphism from G to itself. $\mathrm{AUT}(G)$ is the set of all automorphism. Note $\mathrm{AUT}(G) \subseteq S_n$.

Fact (Do examples on whiteboard.)
If $\sigma \in S_n$ then $G \simeq \sigma(G)$.
If $\sigma \in \mathrm{AUT}(G)$ then $G = \sigma(G)$.

How Big is $\{\sigma(G) : \sigma \in S_n\}$?

Consider the set:

$$\{\sigma(G) : \sigma \in S_n\}$$

How Big is $\{\sigma(G) : \sigma \in S_n\}$?

Consider the set:

$$\{\sigma(G) : \sigma \in S_n\}$$

How big is it? Is it $n!$? No since some of the $\sigma(G)$ appear more than once.

How Big is $\{\sigma(G) : \sigma \in S_n\}$?

Consider the set:

$$\{\sigma(G) : \sigma \in S_n\}$$

How big is it? Is it $n!$? No since some of the $\sigma(G)$ appear more than once.

Goto Breakout Rooms and look at some simple graphs and try to derive it.

How Big is $\{\sigma(G) : \sigma \in S_n\}$?

Consider the set:

$$\{\sigma(G) : \sigma \in S_n\}$$

How big is it? Is it $n!$? No since some of the $\sigma(G)$ appear more than once.

Goto Breakout Rooms and look at some simple graphs and try to derive it.

Lem $|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$.
Proof on next slide.

$|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$

Let $\mathrm{AUT}(G) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. The multiset

$|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$

Let $\mathrm{AUT}(G) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. The multiset

$$B = \{\sigma(G) : \sigma \in S_n\}$$

has $n!$ elements in it: $G_1, \ldots, G_{n!}$.

$|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$

Let $\mathrm{AUT}(G) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. The multiset

$$B = \{\sigma(G) : \sigma \in S_n\}$$

has $n!$ elements in it: $G_1, \ldots, G_{n!}$.
$G_i = G_j$ iff $(\exists \tau \in \mathrm{AUT}(G)$ such that $\tau(G_i) = G_j$.

$|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$

Let $\mathrm{AUT}(G) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. The multiset

$$B = \{\sigma(G) : \sigma \in S_n\}$$

has $n!$ elements in it: $G_1, \ldots, G_{n!}$.
$G_i = G_j$ iff $(\exists \tau \in \mathrm{AUT}(G)$ such that $\tau(G_i) = G_j$.
Key Take G_1. It EQUALS all $|\mathrm{AUT}(G)|$ graphs in

$$\{\tau(G) : \tau \in \mathrm{AUT}(G)\}$$

Hence every graph appears **exactly** $|\mathrm{AUT}(G)|$ times.

$|\{\sigma(G) : \sigma \in S_n\}| = \frac{n!}{\mathrm{AUT}(G)}$

Let $\mathrm{AUT}(G) = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$. The multiset

$$B = \{\sigma(G) : \sigma \in S_n\}$$

has $n!$ elements in it: $G_1, \ldots, G_{n!}$.
$G_i = G_j$ iff $(\exists \tau \in \mathrm{AUT}(G)$ such that $\tau(G_i) = G_j$.
Key Take G_1. It EQUALS all $|\mathrm{AUT}(G)|$ graphs in

$$\{\tau(G) : \tau \in \mathrm{AUT}(G)\}$$

Hence every graph appears **exactly** $|\mathrm{AUT}(G)|$ times.
The result follows.

Three Important Sets

Let G, G_1, G_2 be graphs.
1) $Y(G) = \{(H, \sigma) : G \simeq H \wedge \sigma \in \mathrm{AUT}(G)\}$.

Three Important Sets

Let G, G_1, G_2 be graphs.
1) $Y(G) = \{(H, \sigma) : G \simeq H \wedge \sigma \in \mathrm{AUT}(G)\}$.
How big is $Y(G)$? $\frac{n!}{|AUT(G)|}$ choices for H, $|AUT(G)|$ choices for σ.
Hence $|Y(G)| = n!$.

Three Important Sets

Let G, G_1, G_2 be graphs.
1) $Y(G) = \{(H,\sigma) : G \simeq H \wedge \sigma \in \mathrm{AUT}(G)\}$.
How big is $Y(G)$? $\frac{n!}{|AUT(G)|}$ choices for H, $|AUT(G)|$ choices for σ.
Hence $|Y(G)| = n!$.

2) $Y(G_1, G_2) = Y(G_1) \cup Y(G_2)$.

$$|Y(G_1, G_2)| = \begin{cases} n! & \text{if } G_1 \simeq G_2 \\ 2n! & \text{if } G_1 \not\simeq G_2 \end{cases} \tag{1}$$

$n!$ vs $2n!$ is a size diff, but not a big enough one.

Three Important Sets

Let G, G_1, G_2 be graphs.
1) $Y(G) = \{(H, \sigma) : G \simeq H \wedge \sigma \in \mathrm{AUT}(G)\}$.
How big is $Y(G)$? $\frac{n!}{|AUT(G)|}$ choices for H, $|AUT(G)|$ choices for σ.
Hence $|Y(G)| = n!$.

2) $Y(G_1, G_2) = Y(G_1) \cup Y(G_2)$.

$$|Y(G_1, G_2)| = \begin{cases} n! & \text{if } G_1 \simeq G_2 \\ 2n! & \text{if } G_1 \not\simeq G_2 \end{cases} \tag{1}$$

$n!$ vs $2n!$ is a size diff, but not a big enough one.

3) Let $X(G_1, G_2) = Y(G_1, G_2) \times \cdots \times Y(G_1, G_2)$ (n times).

$$|X(G_1, G_2)| = \begin{cases} (n!)^n & \text{if } G_1 \simeq G_2 \\ 2^n(n!)^n & \text{if } G_1 \not\simeq G_2 \end{cases} \tag{2}$$

Merl Convinces Aut that $(H,\sigma) \in Y(G_1,G_2)$

Mini Goal Merlin will later send Authur some (H,σ) and a proof that $(H,\sigma) \in Y(G_1,G_2)$.

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

1. A number $i \in \{1, 2\}$. Merlin is saying that $(H, \sigma) \in Y_i$. ALSO

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

1. A number $i \in \{1, 2\}$. Merlin is saying that $(H, \sigma) \in Y_i$. ALSO
2. $\rho \in S_n$. Merlin is saying that ρ is an isom of H to G_i.

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

1. A number $i \in \{1, 2\}$. Merlin is saying that $(H, \sigma) \in Y_i$. ALSO
2. $\rho \in S_n$. Merlin is saying that ρ is an isom of H to G_i.

Given (i, ρ) Author an easily verify that ρ is an isom of H to G_i. Author can also verify that σ is an auto of G without any help from Merlin.

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

1. A number $i \in \{1, 2\}$. Merlin is saying that $(H, \sigma) \in Y_i$. ALSO
2. $\rho \in S_n$. Merlin is saying that ρ is an isom of H to G_i.

Given (i, ρ) Author an easily verify that ρ is an isom of H to G_i. Author can also verify that σ is an auto of G without any help from Merlin.

Mini Goal Merlin will later send Authur some

$$(H_1, \sigma_1), \cdots, (H_n, \sigma_n)$$

and a proof that

$$(H_1, \sigma_1), \cdots, (H_n, \sigma_n) \in X(G_1, G_2).$$

Merl Convinces Aut that $(H, \sigma) \in Y(G_1, G_2)$

Mini Goal Merlin will later send Authur some (H, σ) and a proof that $(H, \sigma) \in Y(G_1, G_2)$.

Merlin's proof that $(H, \sigma) \in Y(G_1, G_2)$ Proof is in two parts.

1. A number $i \in \{1, 2\}$. Merlin is saying that $(H, \sigma) \in Y_i$. ALSO
2. $\rho \in S_n$. Merlin is saying that ρ is an isom of H to G_i.

Given (i, ρ) Author an easily verify that ρ is an isom of H to G_i. Author can also verify that σ is an auto of G without any help from Merlin.

Mini Goal Merlin will later send Authur some

$$(H_1, \sigma_1), \cdots, (H_n, \sigma_n)$$

and a proof that

$$(H_1, \sigma_1), \cdots, (H_n, \sigma_n) \in X(G_1, G_2).$$

Just do the proof for each $(H_i, \sigma_i) \in Y(G_1, G_2)$.

Restate Merlin's Goal

Restate Merlin's Goal

$G_1 \simeq G_2 \to |X(G_1, G_2)| = (n!)^n$ which is **small**

Restate Merlin's Goal

$G_1 \simeq G_2 \to |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \to |X(G_1, G_2)| = 2^n (n!)^n$ which is **big**

Restate Merlin's Goal

$G_1 \simeq G_2 \rightarrow |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \rightarrow |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

Restate Merlin's Goal

$G_1 \simeq G_2 \rightarrow |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \rightarrow |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

How can Merlin convince Arthur that X is big? Discuss

Restate Merlin's Goal

$G_1 \simeq G_2 \rightarrow |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \rightarrow |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

How can Merlin convince Arthur that X is big? Discuss

Remember- we are computer scientists!

Restate Merlin's Goal

$G_1 \simeq G_2 \rightarrow |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \rightarrow |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

How can Merlin convince Arthur that X is big? Discuss
Remember- we are computer scientists!
We can use Hash Functions!

Restate Merlin's Goal

$G_1 \simeq G_2 \to |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \to |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

How can Merlin convince Arthur that X is big? Discuss
Remember- we are computer scientists!
We can use Hash Functions!

We use same math from the rand reduction of SAT to SAT_1.

Restate Merlin's Goal

$G_1 \simeq G_2 \rightarrow |X(G_1, G_2)| = (n!)^n$ which is **small**

$G_1 \not\simeq G_2 \rightarrow |X(G_1, G_2)| = 2^n(n!)^n$ which is **big**

Merlin needs to convince Arthur that $X(G_1, G_2)$ is big.

How can Merlin convince Arthur that X is big? Discuss
Remember- we are computer scientists!
We can use Hash Functions!

We use same math from the rand reduction of SAT to SAT_1.

We'll get to that later, we have other things to attend to now.

Representation of Potential Elements of $X(G_1, G_2)$

How to represent the elements in $X(G_1, G_2)$? How long is that representation?

Representation of Potential Elements of $X(G_1, G_2)$

How to represent the elements in $X(G_1, G_2)$? How long is that representation?

1. A graph takes $\Theta(n^2)$ bits to represent.

Representation of Potential Elements of $X(G_1, G_2)$

How to represent the elements in $X(G_1, G_2)$? How long is that representation?

1. A graph takes $\Theta(n^2)$ bits to represent.
2. An automorphism takes $\Theta(n \log n)$ bits to represent.

Representation of Potential Elements of $X(G_1, G_2)$

How to represent the elements in $X(G_1, G_2)$? How long is that representation?

1. A graph takes $\Theta(n^2)$ bits to represent.
2. An automorphism takes $\Theta(n \log n)$ bits to represent.
3. Every element in $Y(G_1, G_2)$ takes $\Theta(n^2 + n \log n) = \Theta(n^2)$ bits to represent.

Representation of Potential Elements of $X(G_1, G_2)$

How to represent the elements in $X(G_1, G_2)$? How long is that representation?

1. A graph takes $\Theta(n^2)$ bits to represent.
2. An automorphism takes $\Theta(n \log n)$ bits to represent.
3. Every element in $Y(G_1, G_2)$ takes $\Theta(n^2 + n \log n) = \Theta(n^2)$ bits to represent.
4. Every element in $X(G_1, G_2)$ takes $\Theta(n(n^2)) = \Theta(n^3)$ bits to represent.

An Interactive Protocol for $\overline{GI}$ With Private Coins: Hash Functions

Convention about Random Matrices

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.
Then

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.
Then

1. $E(S) = 2^{-k}|X|$

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.
Then

1. $E(S) = 2^{-k}|X|$
2. $Var(S) \le 2^{-k}|X|$.

Recall Lemma

Let $k, n \in \mathbb{N}$. Let $X \subseteq \{0,1\}^n$. Assume $0^n \notin X$.

Consider the following random variable:

Pick a random $k \times n$ 0-1 valued matrix M (all arith is mod 2).

$$S = |\{x \in X : M(x) = 0^k\}|.$$

Output S.
Then

1. $E(S) = 2^{-k}|X|$
2. $Var(S) \leq 2^{-k}|X|$.

Note $E(S)$ and $Var(S)$ do not depends on n, just on k and $|X|$.

Set Up Input for Hash Function

Notation

Set Up Input for Hash Function

Notation

1) N will be the length of the encoding of elements of $X(G_1, G_2)$.

Set Up Input for Hash Function

Notation

1) N will be the length of the encoding of elements of $X(G_1, G_2)$.

2) Recall $N = \Theta(n^3)$.

Set Up Input for Hash Function

Notation

1) N will be the length of the encoding of elements of $X(G_1, G_2)$.

2) Recall $N = \Theta(n^3)$.

3) We make sure $0^n \notin X(G_1, G_2)$.

Set Up Input for Hash Function

Notation

1) N will be the length of the encoding of elements of $X(G_1, G_2)$.

2) Recall $N = \Theta(n^3)$.

3) We make sure $0^n \notin X(G_1, G_2)$.

4) We pick k later.

Set Up Input for Hash Function

Notation

1) N will be the length of the encoding of elements of $X(G_1, G_2)$.
2) Recall $N = \Theta(n^3)$.
3) We make sure $0^n \notin X(G_1, G_2)$.
4) We pick k later.
5) Rand Var will be: Pick a rand $k \times N$ 0-1 matrix M, output

$$S = |\{z \in X(G_1, G_2) : M(z) = 0^k\}|.$$

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \leq (n!)^n/2^k$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \leq (n!)^n/2^k$.

If $G_1 \not\simeq G_2$ then

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \leq (n!)^n/2^k$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \leq (n!)^n/2^k$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.
2) $E(S) = 2^n(n!)^n/2^k$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \leq (n!)^n/2^k$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.
2) $E(S) = 2^n(n!)^n/2^k$.
3) $Var(S) \leq 2^n(n!)^n/2^k$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = (n!)^n/2^k$.
3) $Var(S) \le (n!)^n/2^k$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.
2) $E(S) = 2^n(n!)^n/2^k$.
3) $Var(S) \le 2^n(n!)^n/2^k$.

We pick k such that $2^k = (n!)^n$, so $k = \Theta(n^2 \log n)$.

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$
3) $Var(S) \leq 1$.

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$
3) $Var(S) \leq 1$.

If $G_1 \not\simeq G_2$ then

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$
3) $Var(S) \leq 1$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$
3) $Var(S) \leq 1$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n (n!)^n$.
2) $E(S) = 2^n$.

Plug in $2^k = (n!)^n$

If $G_1 \simeq G_2$ then
1) $|X(G_1, G_2)| = (n!)^n$.
2) $E(S) = 1$
3) $Var(S) \leq 1$.

If $G_1 \not\simeq G_2$ then
1) $|X(G_1, G_2)| = 2^n(n!)^n$.
2) $E(S) = 2^n$.
3) $Var(S) \leq 2^n$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \not\simeq G_2$ then $E(S) = 2^n$ and $Var(S) \leq 2^n$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \not\simeq G_2$ then $E(S) = 2^n$ and $Var(S) \leq 2^n$.
$\Pr(|S - 2^n| \geq a) < \frac{2^n}{a^2}$.

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \not\simeq G_2$ then $E(S) = 2^n$ and $Var(S) \leq 2^n$.
$\Pr(|S - 2^n| \geq a) < \frac{2^n}{a^2}$. Plug in $a = 2^{n-1}$ to get

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \not\simeq G_2$ then $E(S) = 2^n$ and $Var(S) \leq 2^n$.
$\Pr(|S - 2^n| \geq a) < \frac{2^n}{a^2}$. Plug in $a = 2^{n-1}$ to get
$\Pr(|S| \leq 2^{n-1}) < \frac{2^n}{2^{2n-2}} = \frac{1}{2^{n-2}}$, so

If $G_1 \simeq G_2$ then .... If $G_1 \not\simeq G_2$ then ...

In the protocol Arthur will challenge Merlin to produce n elements of $X(G_1, G_2)$.

Recall Chebyshev's Inequality:

$$\Pr(|S - E(S)| \geq a) < \frac{Var(S)}{a^2}.$$

Warning bounds below are overly generous.

If $G_1 \simeq G_2$ then $E(S) = 1$ and $Var(S) \leq 1$.
$\Pr(|S - 1| \geq a) < \frac{1}{a^2}$. Plug in $a = n$ to get
$\Pr(|S| \geq n) < \frac{1}{n^2}$

If $G_1 \not\simeq G_2$ then $E(S) = 2^n$ and $Var(S) \leq 2^n$.
$\Pr(|S - 2^n| \geq a) < \frac{2^n}{a^2}$. Plug in $a = 2^{n-1}$ to get
$\Pr(|S| \leq 2^{n-1}) < \frac{2^n}{2^{2n-2}} = \frac{1}{2^{n-2}}$, so
$\Pr(|S| \leq n - 1) \leq \frac{1}{2^{n-2}}$.

Final Protocol for $\overline{\mathrm{GI}} \in \mathrm{AM}$

AM Protocol for $\overline{\mathrm{GI}}$

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.
3. Mer sends Art $z_1, \ldots, z_n \in \{0,1\}^N$ and $(\forall i)$ proof that $z_i \in X(G_1, G_2)$.
   Mer intent is to prove to Art that $(\forall i)[z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k]$.

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.
3. Mer sends Art $z_1, \ldots, z_n \in \{0,1\}^N$ and $(\forall i)$ proof that $z_i \in X(G_1, G_2)$.
   Mer intent is to prove to Art that
   $(\forall i)[z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k]$.
4. $(\forall i)$ Art tries to verify $z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k$. If for any i either of these fails then output NO. Else output YES.

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.
3. Mer sends Art $z_1, \ldots, z_n \in \{0,1\}^N$ and $(\forall i)$ proof that $z_i \in X(G_1, G_2)$.
   Mer intent is to prove to Art that
   $(\forall i)[z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k]$.
4. $(\forall i)$ Art tries to verify $z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k$. If for any i either of these fails then output NO. Else output YES.

As shown in prior slide:

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.
3. Mer sends Art $z_1, \ldots, z_n \in \{0,1\}^N$ and $(\forall i)$ proof that $z_i \in X(G_1, G_2)$.
   Mer intent is to prove to Art that
   $(\forall i)[z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k]$.
4. $(\forall i)$ Art tries to verify $z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k$. If for any i either of these fails then output NO. Else output YES.

As shown in prior slide:

$G_1 \simeq G_2 \rightarrow$ Prob Merlin can send $z_1, \ldots, z_n$ is $\leq \frac{1}{2^n}$.

AM Protocol for $\overline{\mathrm{GI}}$

1. Input(G_1, G_2). (Mer and Art see this.) N, k as above. Both poly in n.
2. Art sends Mer a random $N \times k$ matrix of 0's and 1' M.
3. Mer sends Art $z_1, \ldots, z_n \in \{0,1\}^N$ and $(\forall i)$ proof that $z_i \in X(G_1, G_2)$.
   Mer intent is to prove to Art that
   $(\forall i)[z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k]$.
4. $(\forall i)$ Art tries to verify $z_i \in X(G_1, G_2) \wedge M(z_i) = 0^k$. If for any i either of these fails then output NO. Else output YES.

As shown in prior slide:

$G_1 \simeq G_2 \rightarrow$ Prob Merlin can send $z_1, \ldots, z_n$ is $\le \frac{1}{2^n}$.

$G_1 \not\simeq G_2 \rightarrow$ Prob Merlin cannot send $z_1, \ldots, z_n$ is $\le \frac{1}{2^n}$.

$\overline{\mathrm{GI}} \in \mathrm{AM}$

So What?

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{P} = \mathrm{NP}$?

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{P} = \mathrm{NP}$? No.

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{P} = \mathrm{NP}$? No.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{NP} = \text{co-NP}$?

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{P} = \mathrm{NP}$? No.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{NP} = \mathrm{co\text{-}NP}$? No.

Consequences of $\overline{\mathrm{GI}} \in \mathrm{AM}$

Recall that the original goal was to get

If GI is NPC then something unlikely happens

If GI is NPC then, since $\overline{\mathrm{GI}} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{P} = \mathrm{NP}$? No.

Does $\mathrm{TAUT} \in \mathrm{AM}$ imply $\mathrm{NP} = \text{co-NP}$? No.

To state what $\mathrm{TAUT} \in \mathrm{AM}$ implies, we need more definitions.

Reviewing NP

Recall

$A \in \mathrm{NP}$ if there exists poly p and set $B \in \mathrm{P}$ such that

$$A = \{x : (\exists y, |y| \leq p(|x|)[(x, y) \in B]\}.$$

Reviewing NP

Recall
$A \in \mathrm{NP}$ if there exists poly p and set $B \in \mathrm{P}$ such that

$$A = \{x : (\exists y, |y| \leq p(|x|)[(x, y) \in B]\}.$$

Notation We use $\exists^p$ and $\forall^p$ to mean the variable is bounded by poly in the length of an understood input.

Reviewing NP

Recall
$A \in \mathrm{NP}$ if there exists poly p and set $B \in \mathrm{P}$ such that

$$A = \{x : (\exists y, |y| \le p(|x|))[(x, y) \in B]\}.$$

Notation We use $\exists^p$ and $\forall^p$ to mean the variable is bounded by poly in the length of an understood input.

$A \in \mathrm{NP}$ if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

$A \in \Pi_1$ (also called $\mathrm{co\text{-}NP}$) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)[(x, y) \in B]\}.$$

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

$A \in \Pi_1$ (also called $\mathrm{co\text{-}NP}$) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)[(x, y) \in B]\}.$$

Examples

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

$A \in \Pi_1$ (also called $\mathrm{co\text{-}NP}$) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)[(x, y) \in B]\}.$$

Examples

1) $\mathrm{TAUT} = \{\phi : (\forall x)[\phi(x) = T]\}$

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x,y) \in B]\}.$$

$A \in \Pi_1$ (also called $\mathrm{co\text{-}NP}$) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)[(x,y) \in B]\}.$$

Examples

1) $\mathrm{TAUT} = \{\phi : (\forall x)[\phi(x) = T]\}$
2) $\overline{\mathrm{HAMC}} = \{G : (\forall \text{ cycles } C)[C \text{ is not Hamiltonian}]\}$

Σ_1 and Π_1

$A \in \Sigma_1$ (also called NP) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)[(x, y) \in B]\}.$$

$A \in \Pi_1$ (also called $\mathrm{co}\text{-}\mathrm{NP}$) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)[(x, y) \in B]\}.$$

Examples

1) $\mathrm{TAUT} = \{\phi : (\forall x)[\phi(x) = T]\}$
2) $\overline{\mathrm{HAMC}} = \{G : (\forall \text{ cycles } C)[C \text{ is not Hamiltonian}]\}$
3) If A is any set in NP then $\overline{A}$ in in Π_1.

Σ_2 and Π_2

$A \in \Sigma_2$ (also called Σ_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)(\forall^p z)[(x, y, z) \in B]\}.$$

Σ_2 and Π_2

$A \in \Sigma_2$ (also called Σ_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)(\forall^p z)[(x, y, z) \in B]\}.$$

Examples

Σ_2 and Π_2

$A \in \Sigma_2$ (also called Σ_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)(\forall^p z)[(x,y,z) \in B]\}.$$

Examples

1) $\{\phi(\vec{x}, \vec{y}) : (\exists \vec{b})(\forall \vec{c})[\phi(\vec{b}, \vec{c})]\}$

Σ_2 and Π_2

$A \in \Sigma_2$ (also called Σ_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)(\forall^p z)[(x, y, z) \in B]\}.$$

Examples

1) $\{\phi(\vec{x}, \vec{y}) : (\exists \vec{b})(\forall \vec{c})[\phi(\vec{b}, \vec{c})]\}$
2) $\{\phi :\ \phi$ is the min sized formula for the function ϕ $\}$
Exercise to put this in Σ_2 form.

Σ_2 and Π_2

$A \in \Sigma_2$ (also called Σ_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\exists^p y)(\forall^p z)[(x,y,z) \in B]\}.$$

Examples

1) $\{\phi(\vec{x},\vec{y}) : (\exists \vec{b})(\forall \vec{c})[\phi(\vec{b},\vec{c})]\}$
2) $\{\phi :\ \phi$ is the min sized formula for the function ϕ $\}$
Exercise to put this in Σ_2 form.

$A \in \Pi_2$ (also called Π_2^p) if there exists $B \in \mathrm{P}$ such that

$$A = \{x : (\forall^p y)(\exists^p)[(x,y) \in B]\}.$$

The Polynomial Hierarchy

The Polynomial Hierarchy

1) There are very few natural problems naturally in Σ_2 or Π_2.

The Polynomial Hierarchy

1) There are very few natural problems naturally in Σ_2 or Π_2.

2) Can define Σ_3, Π_3. The hierarchy is called Poly Hierarchy

The Polynomial Hierarchy

1) There are very few natural problems naturally in Σ_2 or Π_2.

2) Can define Σ_3, Π_3. The hierarchy is called Poly Hierarchy

3) $\Sigma_1 \subseteq \Sigma_2 \cdots$. Thought to be proper.

The Polynomial Hierarchy

1) There are very few natural problems naturally in Σ_2 or Π_2.

2) Can define Σ_3, Π_3. The hierarchy is called Poly Hierarchy

3) $\Sigma_1 \subseteq \Sigma_2 \cdots$. Thought to be proper.

4) $\Pi_1 \subseteq \Pi_2 \cdots$. Thought to be proper.

The Polynomial Hierarchy

1) There are very few natural problems naturally in Σ_2 or Π_2.
2) Can define Σ_3, Π_3. The hierarchy is called Poly Hierarchy
3) $\Sigma_1 \subseteq \Sigma_2 \cdots$. Thought to be proper.
4) $\Pi_1 \subseteq \Pi_2 \cdots$. Thought to be proper.
5) $\Sigma_i \subseteq \Pi_{i+1}$. Thought to be proper.

If $\overline{\mathrm{GI}}$ is NPC then ...

1) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_3 = \Pi_3$.

If $\overline{\mathrm{GI}}$ is NPC then ...

1) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_3 = \Pi_3$.

2) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_2 = \Pi_2$ (this takes more effort).

If $\overline{\mathrm{GI}}$ is NPC then ...

1) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_3 = \Pi_3$.

2) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_2 = \Pi_2$ (this takes more effort).

Most people thing that the poly hierarchy is proper and hence that $\Sigma_2 \neq \Pi_2$ and hence that $\overline{\mathrm{GI}}$ is not NPC.

If $\overline{\mathrm{GI}}$ is NPC then ...

1) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_3 = \Pi_3$.

2) From $\mathrm{TAUT} \in \mathrm{AM}$ can show that $\Sigma_2 = \Pi_2$ (this takes more effort).

Most people thing that the poly hierarchy is proper and hence that $\Sigma_2 \neq \Pi_2$ and hence that GI is not NPC.

I am not going to do these proofs. I have shown you the interesting algorithmic aspects of the problem, which is enough for this course.

My Prediction

My Prediction

1. P vs NP will be resolved in the year 2525.

My Prediction

1. P vs NP will be resolved in the year 2525.
2. We still won't know the status of GI.