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 (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 $\overline{\mathrm{GI}}$

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 $\mathrm{\overline{TAUT}}$: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 $\overline{\mathrm{TAUT}}$: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 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.

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.

GI is in IP(2)

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

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 $b_1 \cdots b_n$.

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.

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!

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 $H_i \simeq G_{b_i}$.

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.

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 $c_1 \cdots c_n$.

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

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.

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 $\frac{1}{2^n}$.

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) One can show show $\overline{\mathrm{GI}} \in \mathrm{AM}$. We will not do this.

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

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 $\mathrm{GI} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

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 $\mathrm{GI} \in \mathrm{AM}$, $\mathrm{TAUT} \in \mathrm{AM}$.

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 $\mathrm{NP} = \mathrm{co\text{-}NP}$? 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 co-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 $\mathrm{co\text{-}NP}$) 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

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

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

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

Σ_2 and Π_2

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

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

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

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

Examples

Σ_2 and Π_2

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

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

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

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

Examples

$\{\phi(\vec{x}, \vec{y}) : (\exists \vec{b})(\forall \vec{c})[\phi(\vec{b}, \vec{c})]$ In Σ_2.

Σ_2 and Π_2

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

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

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

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

Examples

$\{\phi(\vec{x}, \vec{y}) : (\exists \vec{b})(\forall \vec{c})[\phi(\vec{b}, \vec{c})]$ In Σ_2.

$\{\phi :\ \phi$ is the min sized fml for the function $\phi\}$ In Π_2 (Exercise)

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

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

If $\overline{GI}$ 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 $\overline{GI}$ 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.

If $\overline{GI}$ 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.

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.