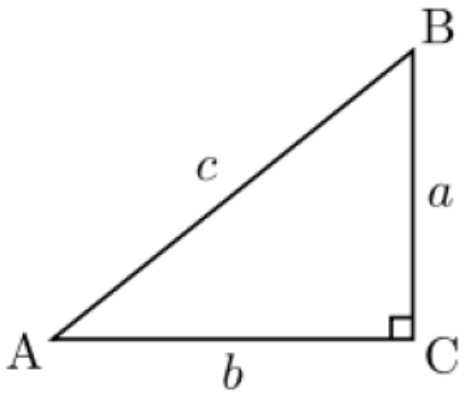
PROVAS

Grandes Ideias da Computação Teórica

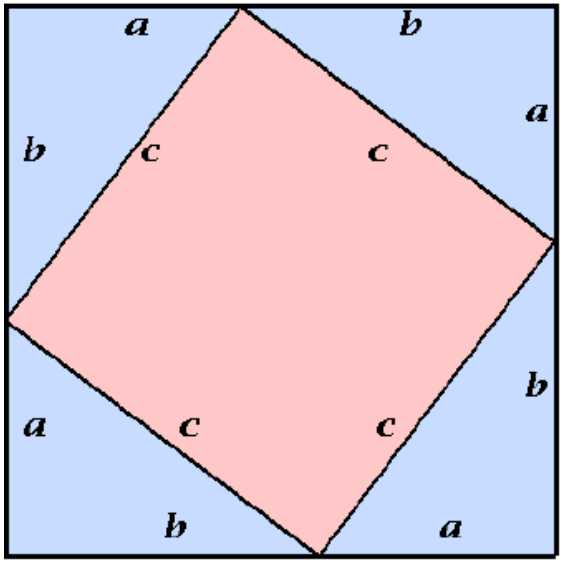
Prof. André Vignatti

Provas da Antiguidade

O Teorema de Pitágoras:

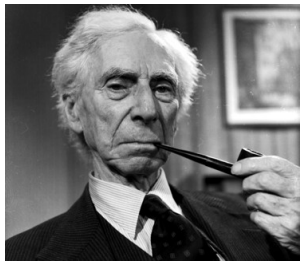


$$a^2 + b^2 = c^2$$



Como a área é $(a+b)^2 = a^2 + b^2 + 2ab$, temos que $c^2 = a^2 + b^2$.

Então veio Russel



Russel, junto de outros, buscou formalizar o conceito de prova. Relembramos a simples demonstração de que $1 + 1 = 2$

$*54{\cdot}43. \quad \vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54{\cdot}26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[*51{\cdot}231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$

$[*13{\cdot}12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . *11{\cdot}11{\cdot}35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . *11{\cdot}54 . *52{\cdot}1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Agora provas poderiam ser verificadas mecanicamente.

Provas para um cientista da computação

A classe **NP**

NP é a classe de todos os problemas de decisão para os quais existe um algoritmo V de tempo polinomial tal que:

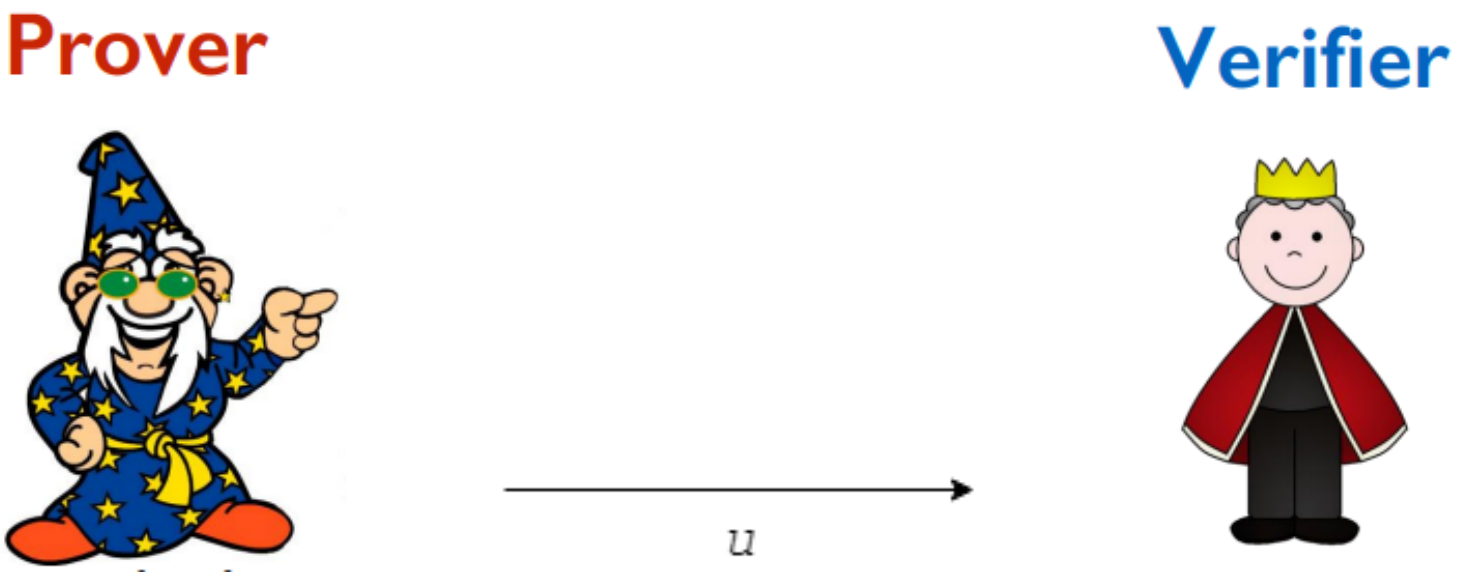
$$x \text{ é uma instância verdadeira } \leftrightarrow \exists_u \mid V(x, u) = 1.$$

Provas para um cientista da computação

A classe **NP**

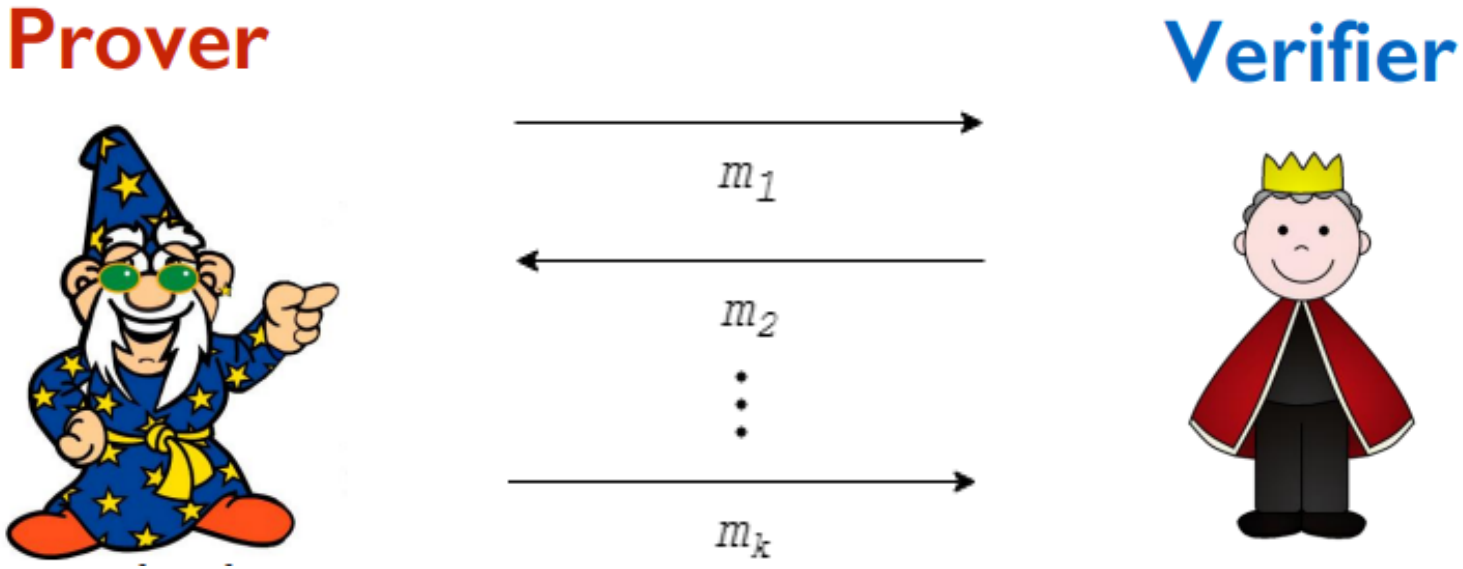
NP é a classe de todos os problemas de decisão para os quais existe um algoritmo V de tempo polinomial tal que:

$$x \text{ é uma instância verdadeira } \leftrightarrow \exists_u \mid V(x,u) = 1.$$



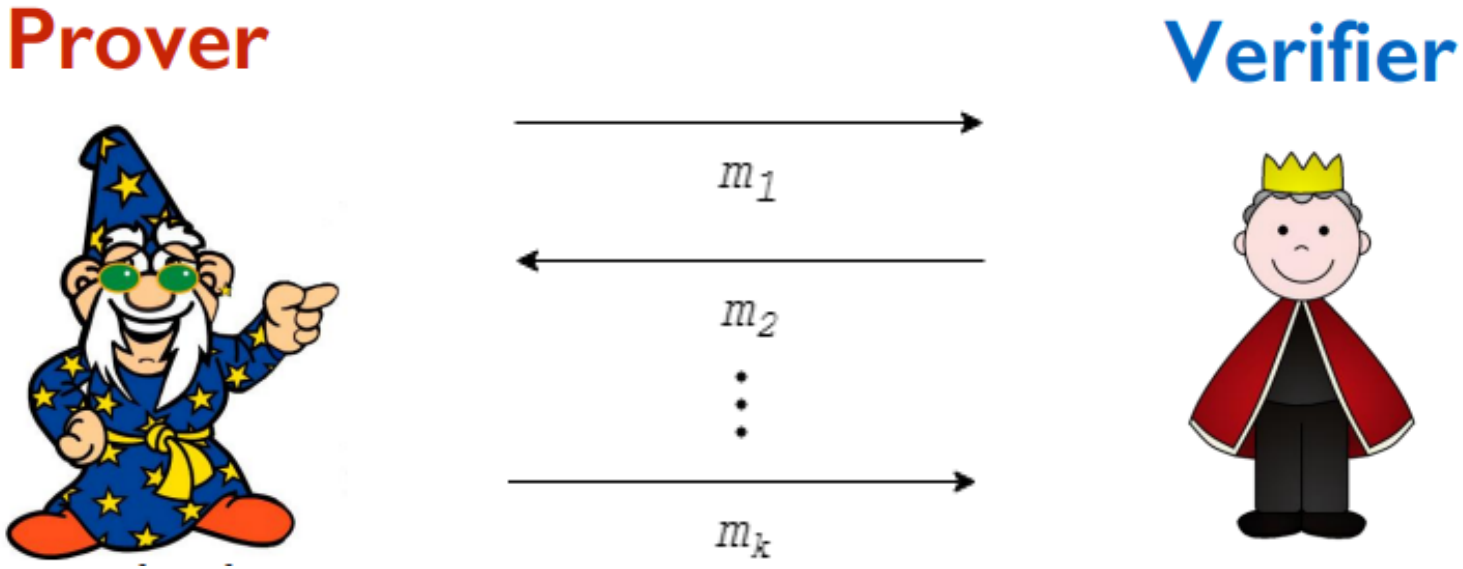
Provas Interativas

E se ao invés de apenas uma mensagem, ocorresse uma interação entre P e V, será que muda alguma coisa? Definimos a classe **dIP**.



Provas Interativas

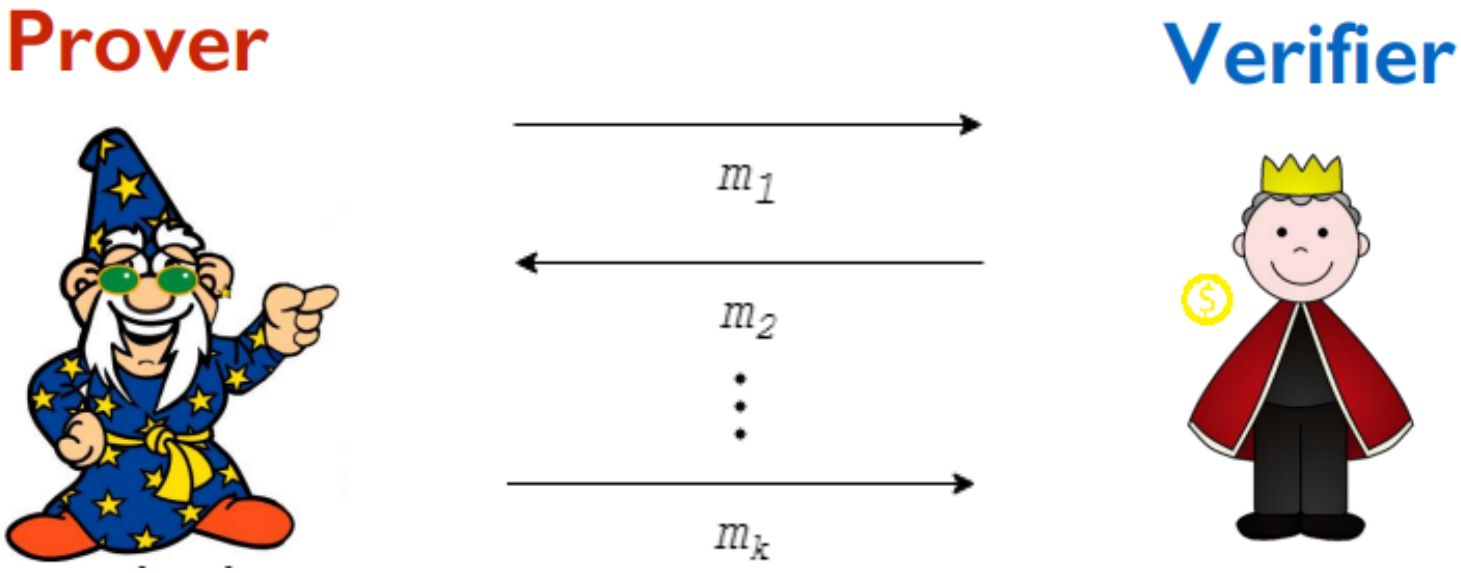
E se ao invés de apenas uma mensagem, ocorresse uma interação entre P e V, será que muda alguma coisa? Definimos a classe **dIP**.



Não... Pois nesse caso P poderia ter mandado todas as suas mensagens logo no início! **Exercício** para o aluno empenhado, prove que **NP** $=$ **dIP** [AB09].

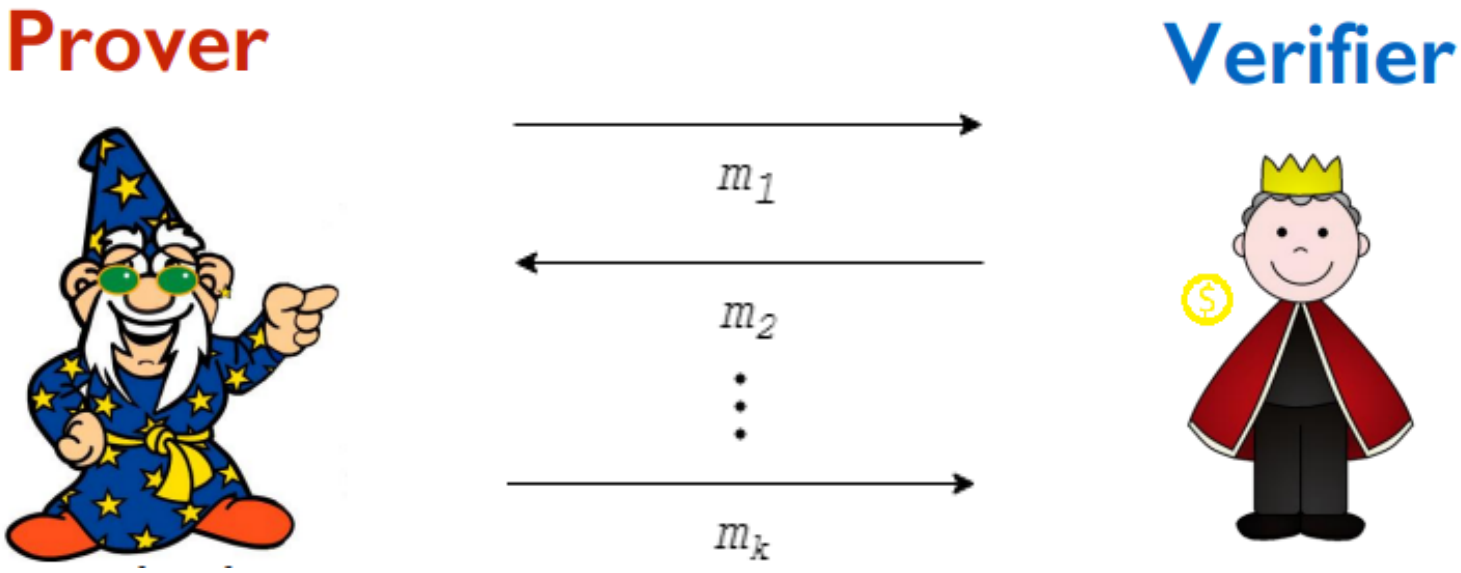
Provas Interativas

Grande ideia #1: E se, além da interação, imaginarmos que V é probabilístico? Definimos a classe **IP** [GMR89].



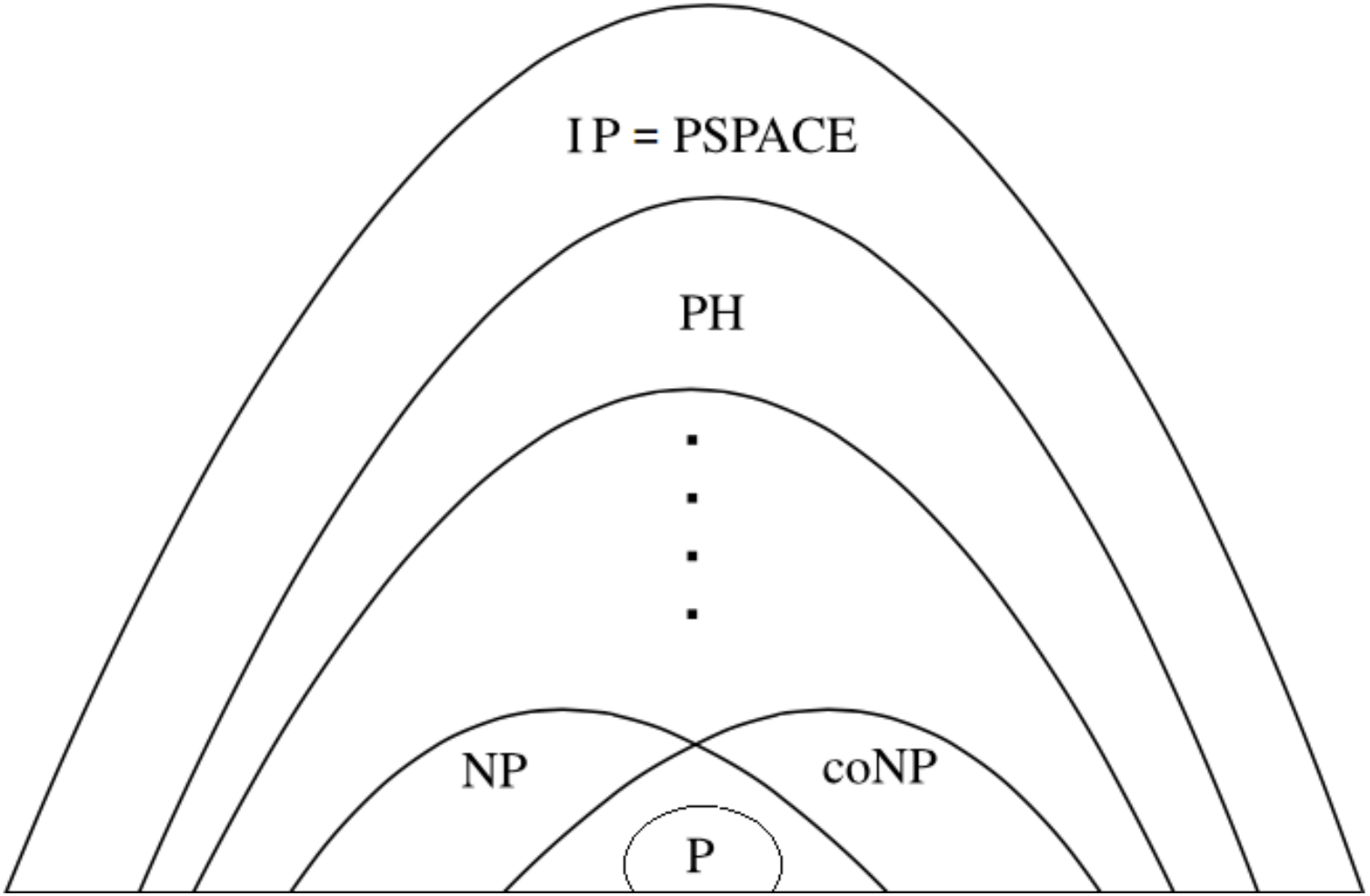
Provas Interativas

Grande ideia #1: E se, além da interação, imaginarmos que V é probabilístico? Definimos a classe **IP** [GMR89].



O poder de reconhecimento de V aumentou e muito! **IP** $=$ **PSPACE**.

IP = PSPACE



Um exemplo prático

Teorema: Coca-Cola $\neq$ Pepsi.

1. V: Joga uma moeda. Se cara, coloca Coca-Cola em um copo (escondido), se coroa, coloca Pepsi. Entrega o copo para P.
2. P: Experimenta e diz para V qual foi a bebida colocada no copo.
3. V: Aceita se e somente se P acertar a bebida.

Formalizando um pouco as coisas

Um sistema de prova interativa precisa obedecer a três condições

- **(Eficiência)**. O sistema é polinomialmente limitado.

Formalizando um pouco as coisas

Um sistema de prova interativa precisa obedecer a três condições

- **(Eficiência)**. O sistema é polinomialmente limitado.
- **(Integralidade)**. Se a instância é verdadeira, então V aceita com probabilidade 1.

Formalizando um pouco as coisas

Um sistema de prova interativa precisa obedecer a três condições

- **(Eficiência)**. O sistema é polinomialmente limitado.
- **(Integralidade)**. Se a instância é verdadeira, então V aceita com probabilidade 1.
- **(Corretude)**. Se a instância é falsa, então para qualquer estratégia de prova P^*, V rejeita com probabilidade maior ou igual a $1/2$.

Não-Isomorfismo de Grafos

Apesar de parecer uma brincadeira simples, o protocolo para distinguir bebidas é uma adaptação de um protocolo para um problema computacional importante. O de não-isomorfismo de grafos.

Não-Isomorfismo de Grafos

Apesar de parecer uma brincadeira simples, o protocolo para distinguir bebidas é uma adaptação de um protocolo para um problema computacional importante. O de não-isomorfismo de grafos.

Teorema: Os grafos G_0 e G_1 não são isomorfos. Mostramos um protocolo para provar esse tipo de afirmação

Não-Isomorfismo de Grafos

Apesar de parecer uma brincadeira simples, o protocolo para distinguir bebidas é uma adaptação de um protocolo para um problema computacional importante. O de não-isomorfismo de grafos.

Teorema: Os grafos G_0 e G_1 não são isomorfos. Mostramos um protocolo para provar esse tipo de afirmação

1. V: Sorteia um grafo G dentre G_0 e G_1 e uma permutação π, faz $H = \pi(G)$ e envia H para P.
2. P: Se $H \cong G_0$, responde G_0, senão responde G_1.
3. V: Aceita se e somente se P acertar o grafo usado para construir H.

Não-Isomorfismo de Grafos

Apesar de parecer uma brincadeira simples, o protocolo para distinguir bebidas é uma adaptação de um protocolo para um problema computacional importante. O de não-isomorfismo de grafos.

Teorema: Os grafos G_0 e G_1 não são isomorfos. Mostramos um protocolo para provar esse tipo de afirmação

1. V: Sorteia um grafo G dentre G_0 e G_1 e uma permutação π, faz $H = \pi(G)$ e envia H para P.
2. P: Se $H \cong G_0$, responde G_0, senão responde G_1.
3. V: Aceita se e somente se P acertar o grafo usado para construir H.

Exercício para o aluno empenhado: prove que o protocolo apresentado para não-isomorfismo de grafos é um sistema de prova interativo.

Provas de Conhecimento Zero

Grande ideia #2: E se V, no fim da interação com P, não aprender nada além do fato de que x é uma instância verdadeira? [GMR89]

Provas de Conhecimento Zero

Grande ideia #2: E se V, no fim da interação com P, não aprender nada além do fato de que x é uma instância verdadeira? [GMR89]

Provas de conhecimento zero capturam essa noção, mas como podemos fazer para provar que V não aprende nada? O que é "conhecimento" nesse caso?

Provas de Conhecimento Zero

Grande ideia #2: E se V, no fim da interação com P, não aprender nada além do fato de que x é uma instância verdadeira? [GMR89]

Provas de conhecimento zero capturam essa noção, mas como podemos fazer para provar que V não aprende nada? O que é "conhecimento" nesse caso?

Provas de conhecimento zero possuem uma condição extra:

- **(Conhecimento Zero)**. Existe um simulador S para qualquer verificador probabilístico de tempo polinomial V^* que produz mensagens parecidas com as que V^* e a estratégia de prova P produziriam ao interagir.

Provas de Conhecimento Zero

Parecidas? Como assim?

Provas de Conhecimento Zero

Parecidas? Como assim? Podemos definir três tipos de conhecimento zero.

1. Conhecimento Zero **Perfeito**: as mensagens são **idênticas**. Classe **PZK**.
2. Conhecimento Zero **Estatístico**: as mensagens possuem pequena **distância estatística**. Classe **SZK**.
3. Conhecimento Zero **Computacional**: as mensagens são **computacionalmente indistinguíveis**. Classe **CZK**.

Provas de Conhecimento Zero

Parecidas? Como assim? Podemos definir três tipos de conhecimento zero.

1. Conhecimento Zero **Perfeito**: as mensagens são **idênticas**. Classe **PZK**.
2. Conhecimento Zero **Estatístico**: as mensagens possuem pequena **distância estatística**. Classe **SZK**.
3. Conhecimento Zero **Computacional**: as mensagens são **computacionalmente indistinguíveis**. Classe **CZK**.

Qual a relação entre as classes vistas até o momento?
PZK ? **SZK** ? **CZK**.
CZK ? **IP**.

Provas de Conhecimento Zero

Parecidas? Como assim? Podemos definir três tipos de conhecimento zero.

1. Conhecimento Zero **Perfeito**: as mensagens são **idênticas**. Classe **PZK**.
2. Conhecimento Zero **Estatístico**: as mensagens possuem pequena **distância estatística**. Classe **SZK**.
3. Conhecimento Zero **Computacional**: as mensagens são **computacionalmente indistinguíveis**. Classe **CZK**.

Qual a relação entre as classes vistas até o momento?
PZK $\subseteq$ **SZK** $\subseteq$ **CZK**.
CZK $=$ **IP**. "Everything provable is provable in zero-knowledge" - [BOGG+90]

Um simulador para o primeiro protocolo

Quais são as mensagens trocadas no caso do nosso exemplo?

Um simulador para o primeiro protocolo

Quais são as mensagens trocadas no caso do nosso exemplo?

Simulador

1. Joga uma moeda. Se cara, coloca Coca-Cola em um *copo*, se coroa, coloca Pepsi.
2. Seja *bebida* a bebida colocada no copo.
3. Responde (*copo*, *bebida*).

Qual a qualidade dessa simulação?

Um simulador para o primeiro protocolo

Quais são as mensagens trocadas no caso do nosso exemplo?

Simulador

1. Joga uma moeda. Se cara, coloca Coca-Cola em um *copo*, se coroa, coloca Pepsi.
2. Seja *bebida* a bebida colocada no copo.
3. Responde (*copo*, *bebida*).

Qual a qualidade dessa simulação? Existe algum verificador que pode extrair informação extra?

Um simulador para o primeiro protocolo

Quais são as mensagens trocadas no caso do nosso exemplo?

Simulador

1. Joga uma moeda. Se cara, coloca Coca-Cola em um *copo*, se coroa, coloca Pepsi.
2. Seja *bebida* a bebida colocada no copo.
3. Responde (*copo*, *bebida*).

Qual a qualidade dessa simulação? Existe algum verificador que pode extrair informação extra?

Exercício para o aluno empenhado: prove que o protocolo que vimos para não-isomorfismo de grafos é de conhecimento zero (para o verificador V).

Outro tipo de prova

Vimos nesta aula provas que são:

- Interativas.
- Aleatorizadas.
- De conhecimento zero.

Outro tipo de prova

Vimos nesta aula provas que são:

- Interativas.
- Aleatorizadas.
- De conhecimento zero.

Há um outro tipo de prova, conhecida como **PCP** (provas probabilisticamente checáveis, em inglês). Nesse tipo de prova, V só precisa olhar para alguns pedaços da demonstração para se convencer.

Referências

- Sanjeev Arora and Boaz Barak, *Computational complexity: A modern approach*, 1st ed., Cambridge University Press, New York, NY, USA, 2009.
- Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway, *Everything provable is provable in zero-knowledge*, Advances in Cryptology — CRYPTO' 88 (New York, NY) (Shafi Goldwasser, ed.), Springer New York, 1990, pp. 37–56.
- S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof systems*, SIAM J. Comput. **18** (1989), no. 1, 186–208.