Uma Revisão sobre a Relação de BQP com outras Classes de Complexidade Computacional

Henrique Hepp[1], Murilo V. G. da Silva[1], Leandro M. Zatesko[2]
hhepp@inf.ufpr.br

20 de setembro de 2019

[1]UFPR, [2]UTFPR

WPCCG 2019

UNIVERSIDADE FEDERAL DO PARANÁ

Uma Revisão sobre a Relação de BQP com outras Classes de Complexidade Computacional

Introdução

Introdução

Classe de Complexidade

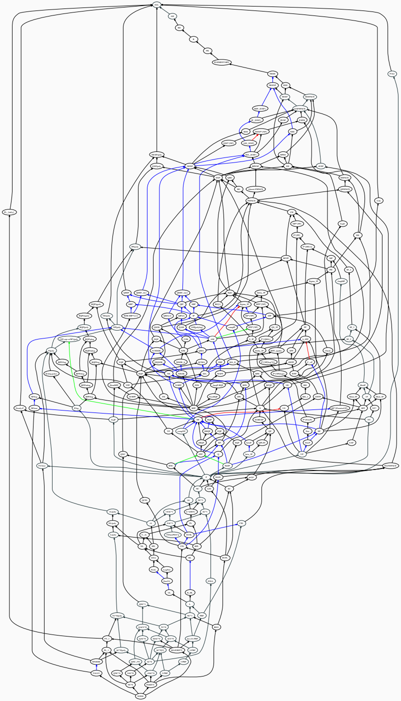
Classificação de problemas computacionais de acordo com os recursos, como tempo e espaço, necessários para resolvê-los.

Introdução

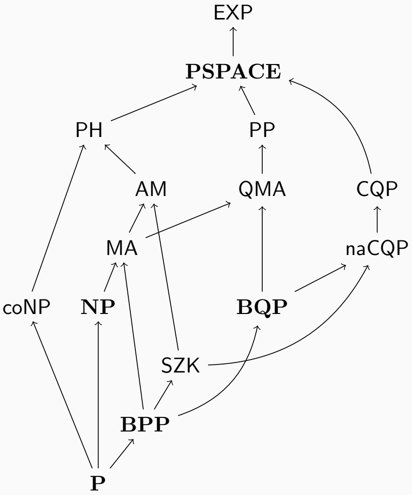
Classe de Complexidade

Classificação de problemas computacionais de acordo com os recursos, como tempo e espaço, necessários para resolvê-los.

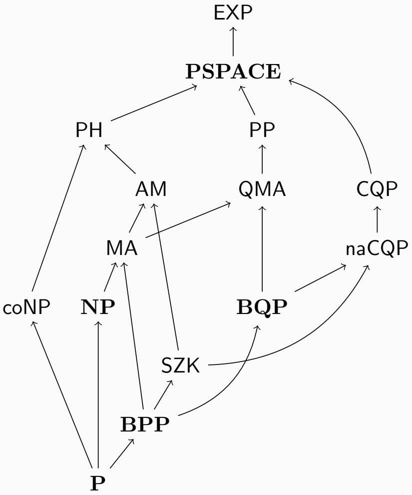
- Já foram definidas mais de 500 classes de complexidade.
- `https://complexityzoo.uwaterloo.ca/Complexity_Zoo`



Introdução

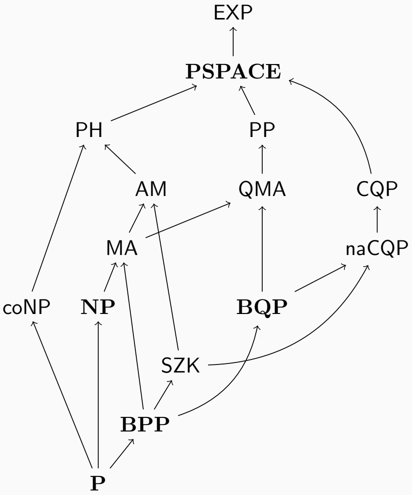


Introdução



- $\mathsf{NP} \stackrel{?}{=} \mathsf{P}$

Introdução



- NP $\stackrel{?}{=}$ P
- PSPACE $\stackrel{?}{=}$ P

Computação Quântica

- Vetor de Estado

$$|\Psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \text{ onde } \alpha_0, \cdots \alpha_{N-1} \in \mathbb{C} \text{ e } \sum_i |\alpha_i|^2 = 1$$

- Vetor de Estado

$$|\Psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \text{ onde } \alpha_0, \cdots \alpha_{N-1} \in \mathbb{C} \text{ e } \sum_i |\alpha_i|^2 = 1$$

$$|\Psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{N-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

- Vetor de Estado

$$|\Psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{bmatrix} \text{ onde } \alpha_0, \cdots \alpha_{N-1} \in \mathbb{C} \text{ e } \sum_i |\alpha_i|^2 = 1$$

$$|\Psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \alpha_{N-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$$

- Notação de Dirac:

$$|\Psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{N-1} |N-1\rangle$$

Computação Quântica

- Qubit

$$|\psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Computação Quântica

- Qubit

$$|\psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

Computação Quântica

- Qubit

$$|\psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

- 2 Qubits

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{bmatrix}$$

Computação Quântica

- Qubit

$$|\psi\rangle = \alpha_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

- 2 Qubits

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \beta_0 \\ \beta_1 \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{bmatrix}$$

$$|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$$

Computação Quântica

- n Qubits

$$|\Psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle + \cdots + \alpha_{2^n-1} |2^n - 1\rangle$$

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

$$\text{onde } \alpha_0, \cdots, \alpha_{2^n-1} \in \mathbb{C} \text{ e } \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

Operações na Computação Quântica

- Transformações Unitárias — Portas Quânticas

$$|\Psi'\rangle = U\,|\Psi\rangle$$

Operações na Computação Quântica

- Transformações Unitárias — Portas Quânticas

$$|\Psi'\rangle = U\,|\Psi\rangle$$

- Porta Not

$$|\psi'\rangle = X\,|0\rangle = |1\rangle$$

Operações na Computação Quântica

- Transformações Unitárias — Portas Quânticas

$$|\Psi'\rangle = U\,|\Psi\rangle$$

- Porta Not

$$|\psi'\rangle = X\,|0\rangle = |1\rangle$$

$$|\psi'\rangle = X\left(\frac{1}{\sqrt{3}}\,|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}\,|1\rangle\right) = \frac{\sqrt{2}}{\sqrt{3}}\,|0\rangle + \frac{1}{\sqrt{3}}\,|1\rangle$$

Operações na Computação Quântica

- Transformações Unitárias — Portas Quânticas

$$|\Psi'\rangle = U\,|\Psi\rangle$$

- Porta Not

$$|\psi'\rangle = X\,|0\rangle = |1\rangle$$

$$|\psi'\rangle = X\left(\frac{1}{\sqrt{3}}\,|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}\,|1\rangle\right) = \frac{\sqrt{2}}{\sqrt{3}}\,|0\rangle + \frac{1}{\sqrt{3}}\,|1\rangle$$

- Porta Hadamard

$$|\psi'\rangle = H\,|0\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

Operações na Computação Quântica

- Medições Quânticas
  - Ao se medir $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ o estado *colapsa* em $|i\rangle$ com probabilidade $|\alpha_i|^2$

Operações na Computação Quântica

- Medições Quânticas
  - Ao se medir $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ o estado *colapsa* em $|i\rangle$ com probabilidade $|\alpha_i|^2$
  - Exemplo:

$$M\left(\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle\right) = \begin{cases} |0\rangle, & \text{com probabilidade } \frac{1}{3} \\ |1\rangle, & \text{com probabilidade } \frac{2}{3} \end{cases}$$

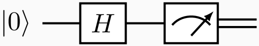
- Medições Quânticas
  - Ao se medir $|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ o estado *colapsa* em $|i\rangle$ com probabilidade $|\alpha_i|^2$
  - Exemplo:

$$M\left(\frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle\right) = \begin{cases} |0\rangle, & \text{com probabilidade } \frac{1}{3} \\ |1\rangle, & \text{com probabilidade } \frac{2}{3} \end{cases}$$

$$M\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \begin{cases} |0\rangle, & \text{com probabilidade } \frac{1}{2} \\ |1\rangle, & \text{com probabilidade } \frac{1}{2} \end{cases}$$

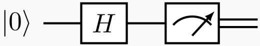
Circuito Quântico

$$MH\,|0\rangle$$

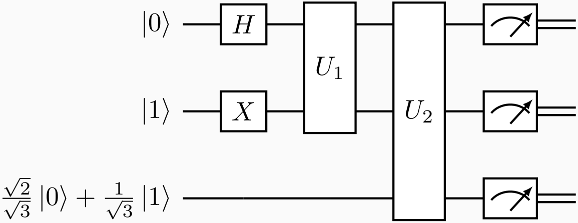


Circuito Quântico

$$MH\,|0\rangle$$



- Um circuito qualquer



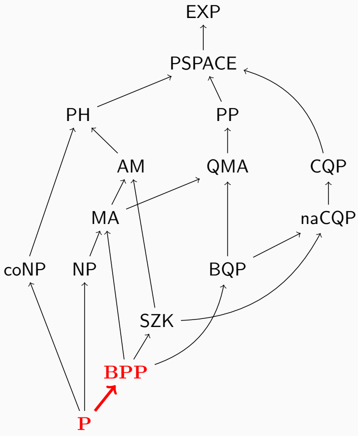
A Classe BQP

BQP é a classe de problemas de decisão que podem ser resolvidos por uma família uniforme de circuitos quânticos com tamanho polinomial.

Classes de Complexidade

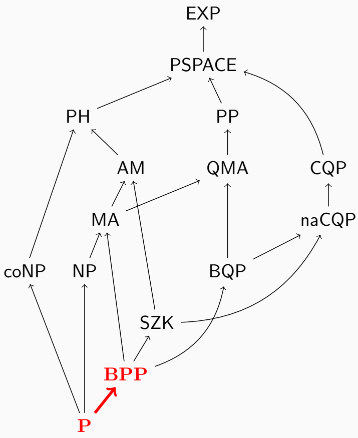
Classes de Complexidade

- P $\subseteq$ BPP



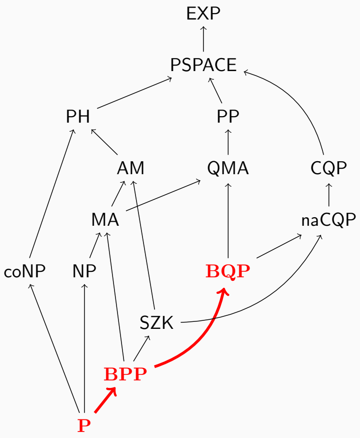
Classes de Complexidade

- P ⊆ BPP
  - BPP é P mais bits aleatórios



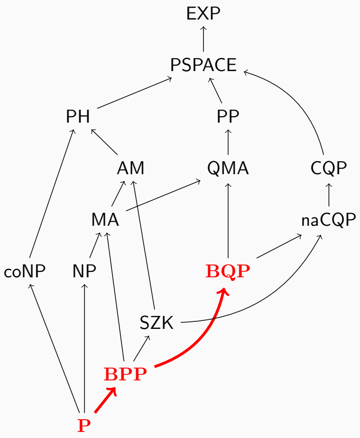
Classes de Complexidade

- P $\subseteq$ BPP
  - BPP é P mais bits aleatórios
- BPP $\subseteq$ BQP



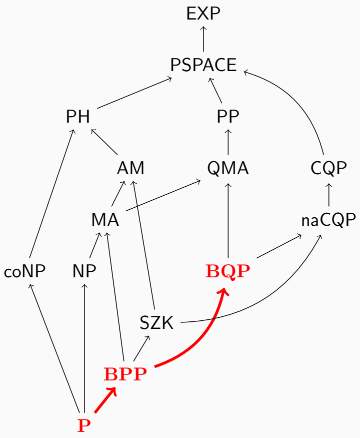
Classes de Complexidade

- $P \subseteq BPP$
  - BPP é P mais bits aleatórios
- $BPP \subseteq BQP$
  - BQP simula circuitos clássicos



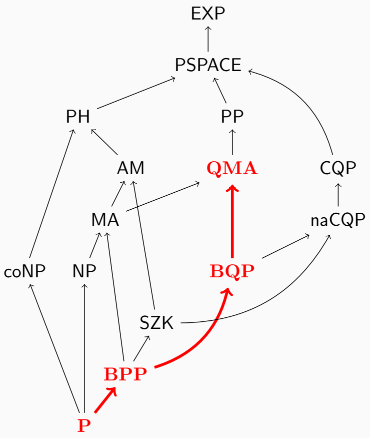
Classes de Complexidade

- P ⊆ BPP
  - BPP é P mais bits aleatórios
- BPP ⊆ BQP
  - BQP simula circuitos clássicos
  - BQP gera bits aleatórios



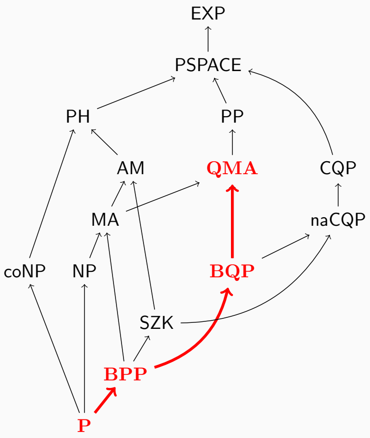
Classes de Complexidade

- P $\subseteq$ BPP
  - BPP é P mais bits aleatórios
- BPP $\subseteq$ BQP
  - BQP simula circuitos clássicos
  - BQP gera bits aleatórios
- BQP $\subseteq$ QMA



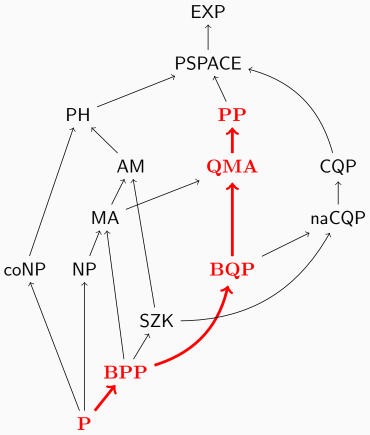
Classes de Complexidade

- P $\subseteq$ BPP
  - BPP é P mais bits aleatórios
- BPP $\subseteq$ BQP
  - BQP simula circuitos clássicos
  - BQP gera bits aleatórios
- BQP $\subseteq$ QMA
  - Análogo a P $\subseteq$ NP e a BPP $\subseteq$ MA



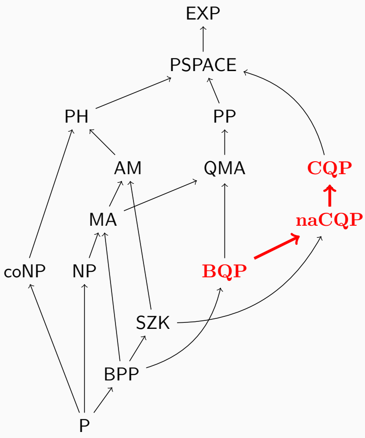
Classes de Complexidade

- $P \subseteq BPP$
  - BPP é P mais bits aleatórios
- $BPP \subseteq BQP$
  - BQP simula circuitos clássicos
  - BQP gera bits aleatórios
- $BQP \subseteq QMA$
  - Análogo a $P \subseteq NP$ e a $BPP \subseteq MA$
- $QMA \subseteq PP$



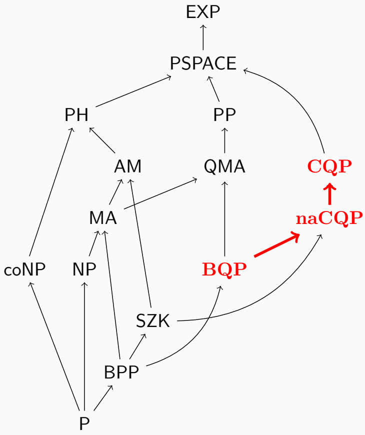
Classes de Complexidade

- BQP $\subseteq$ naCQP $\subseteq$ CQP



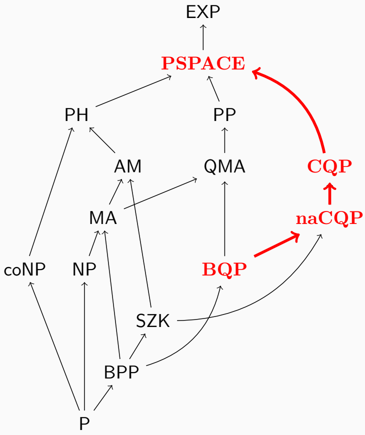
Classes de Complexidade

- BQP $\subseteq$ naCQP $\subseteq$ CQP
  - CQP é BQP com medidas sem colapso



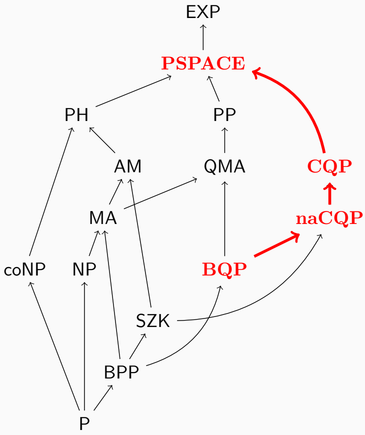
Classes de Complexidade

- BQP $\subseteq$ naCQP $\subseteq$ CQP
  - CQP é BQP com medidas sem colapso
- CQP $\subseteq$ PSPACE



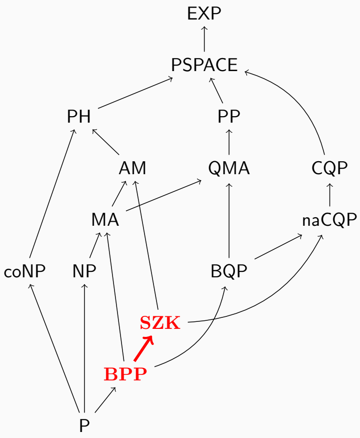
Classes de Complexidade

- BQP ⊆ naCQP ⊆ CQP
  - CQP é BQP com medidas sem colapso
- CQP ⊆ PSPACE
  - $\mathrm{BPP}^{\mathrm{PP}}$ simula circuitos CQP e $\mathrm{BPP}^{\mathrm{PP}} \subseteq$ PSPACE



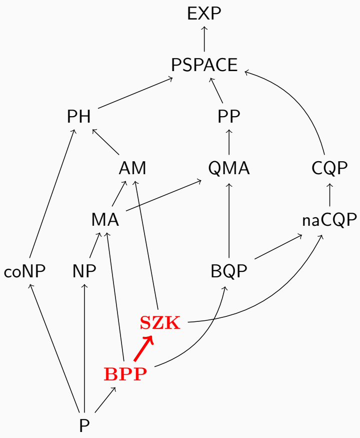
Classes de Complexidade

- BPP $\subseteq$ SZK



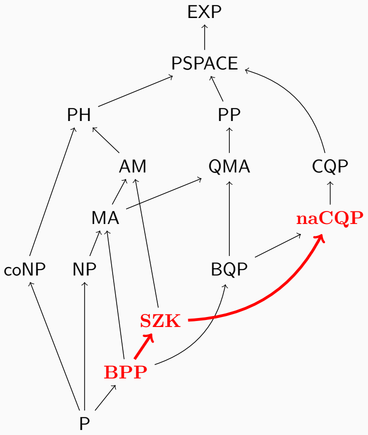
Classes de Complexidade

- BPP ⊆ SZK
  - SZK usa um verificador BPP



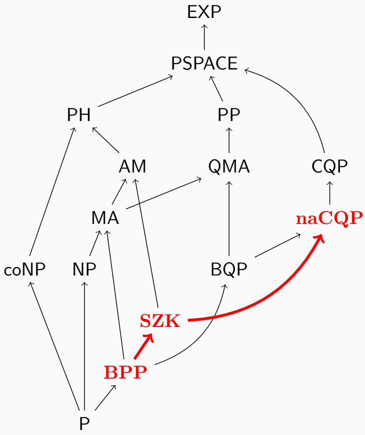
Classes de Complexidade

- BPP $\subseteq$ SZK
  - SZK usa um verificador BPP
- SZK $\subseteq$ naCQP



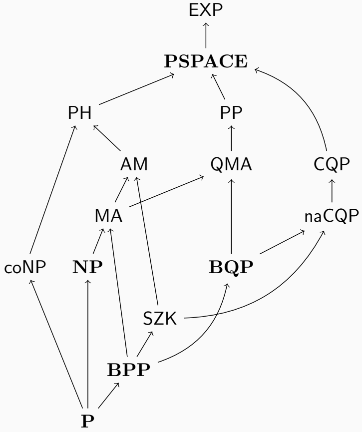
Classes de Complexidade

- BPP $\subseteq$ SZK
  - SZK usa um verificador BPP
- SZK $\subseteq$ naCQP
  - naCQP resolve problemas completos de SZK

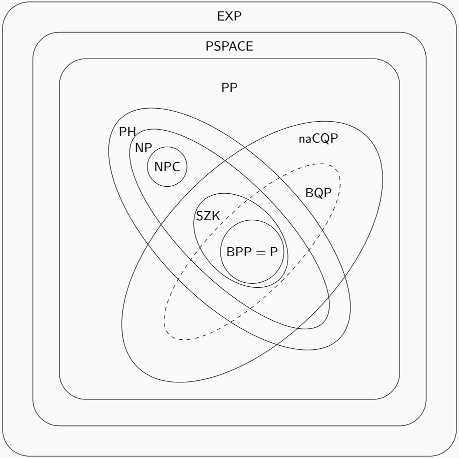


Classes de Complexidade

Relações confirmadas

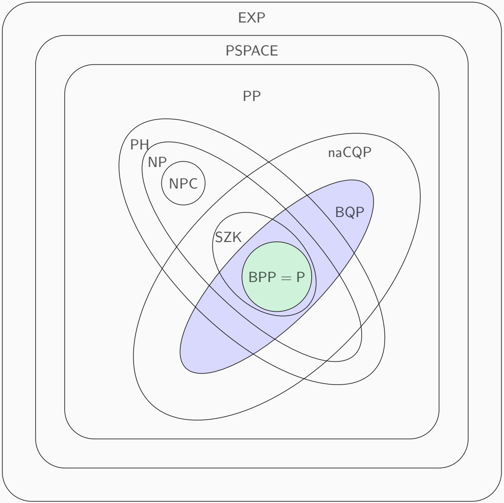


Relações conjecturadas



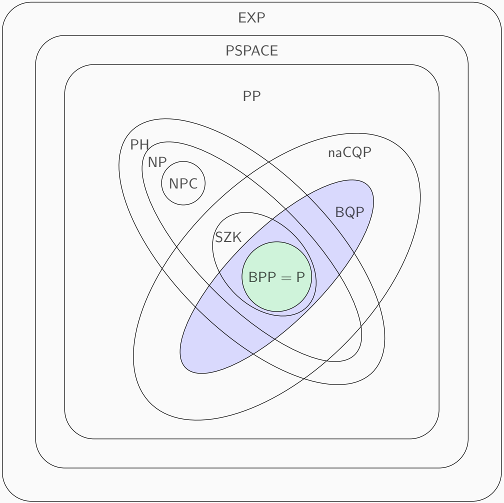
Classes de Complexidade: Relações Conjecturadas

- BPP = P



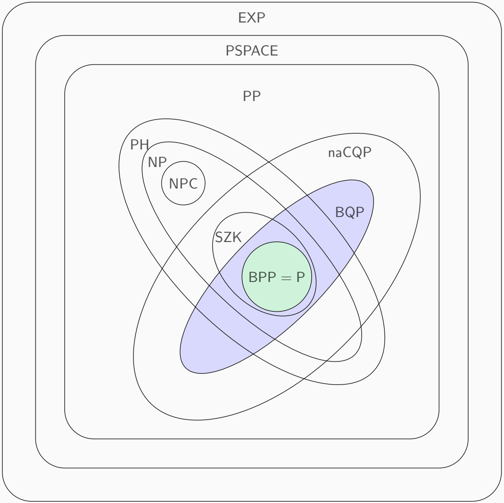
Classes de Complexidade: Relações Conjecturadas

- BPP $=$ P
- BPP $\subsetneq$ BQP



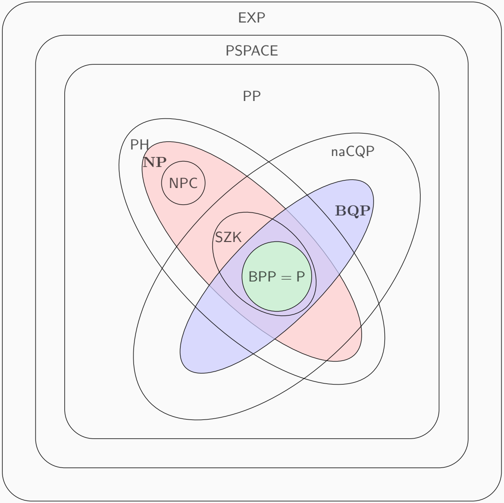
Classes de Complexidade: Relações Conjecturadas

- BPP $=$ P
- BPP $\subsetneq$ BQP
  - Algoritmo de Shor



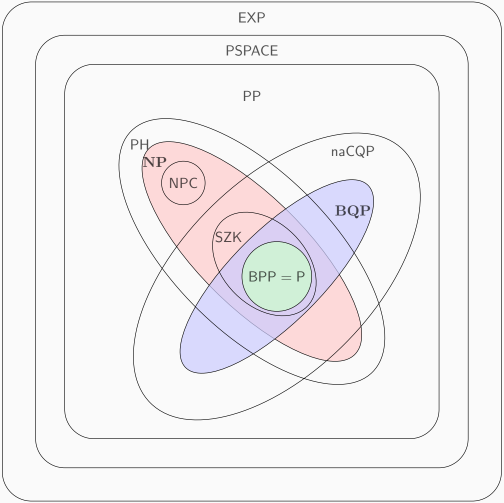
Classes de Complexidade: Relações Conjecturadas

- $BPP = P$
- $BPP \subsetneq BQP$
  - Algoritmo de Shor
- $NP \not\subset BQP$



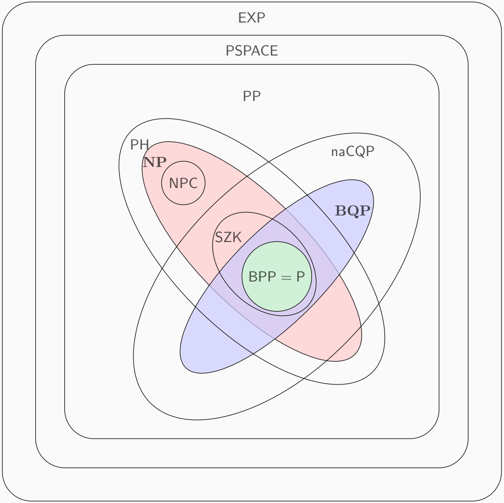
Classes de Complexidade: Relações Conjecturadas

- BPP $=$ P
- BPP $\subsetneq$ BQP
  - Algoritmo de Shor
- NP $\not\subset$ BQP
  - Busca no modelo "caixa-preta" dentre 2^n itens em $\Omega(2^{n/2})$



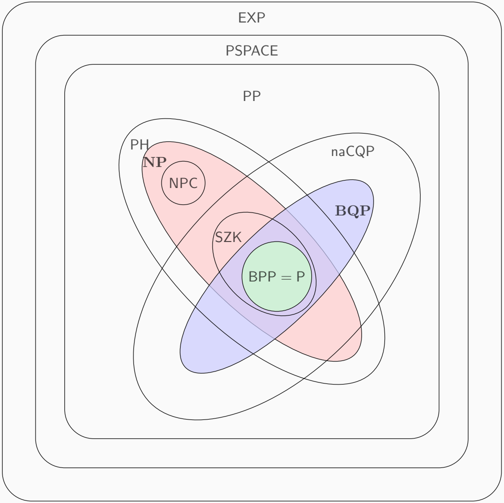
Classes de Complexidade: Relações Conjecturadas

- BPP $=$ P
- BPP $\subsetneq$ BQP
  - Algoritmo de Shor
- NP $\not\subset$ BQP
  - Busca no modelo "caixa-preta" dentre 2^n itens em $\Omega(2^{n/2})$
- BQP $\not\subset$ NP



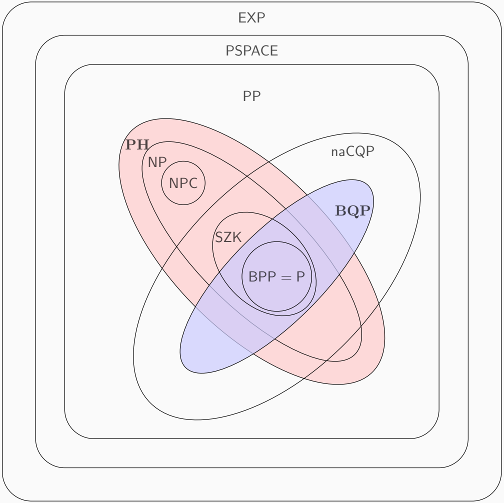
Classes de Complexidade: Relações Conjecturadas

- BPP $=$ P
- BPP $\subsetneq$ BQP
  - Algoritmo de Shor
- NP $\not\subset$ BQP
  - Busca no modelo "caixa-preta" dentre 2^n itens em $\Omega(2^{n/2})$
- BQP $\not\subset$ NP
  - $\mathsf{BQP}^A \not\subset \mathsf{NP}^A$



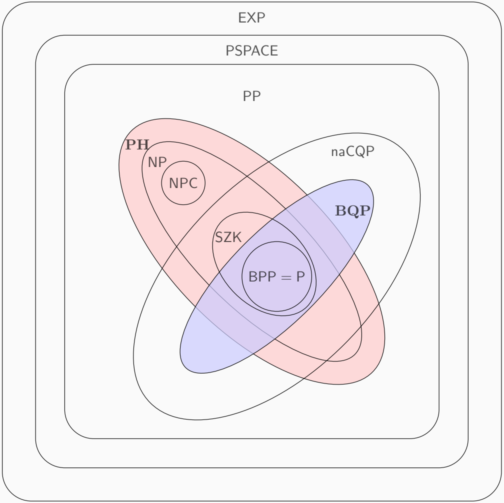
Classes de Complexidade: Relações Conjecturadas

- $\mathsf{PH} \not\subset \mathsf{BQP}$



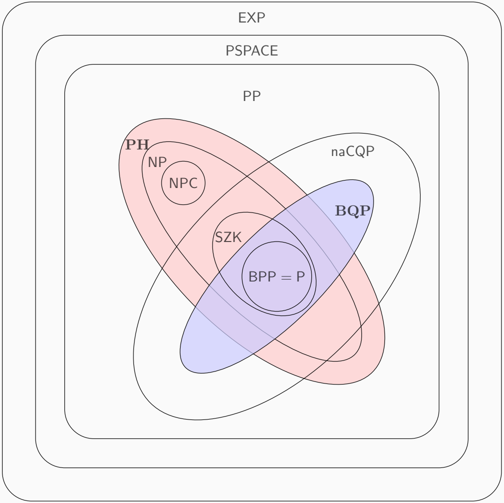
Classes de Complexidade: Relações Conjecturadas

- PH $\not\subset$ BQP
  - Muito mais improvável que NP $\not\subset$ BQP



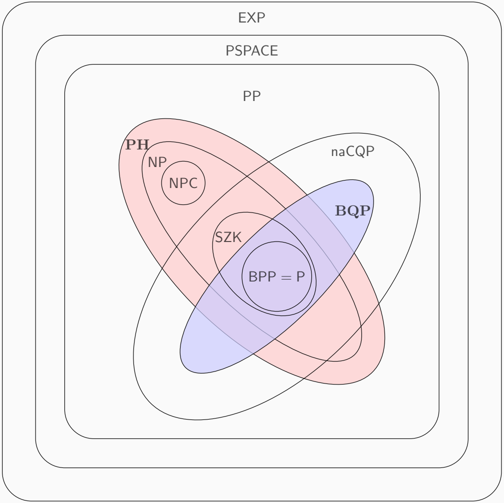
Classes de Complexidade: Relações Conjecturadas

- PH $\not\subset$ BQP
  - Muito mais improvável que NP $\not\subset$ BQP
- BQP $\not\subset$ PH



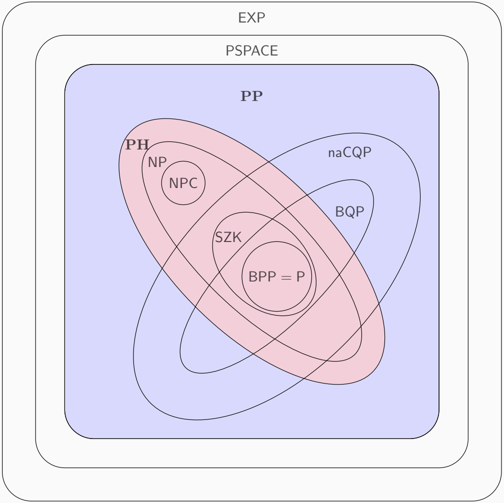
Classes de Complexidade: Relações Conjecturadas

- $\mathsf{PH} \not\subset \mathsf{BQP}$
  - Muito mais improvável que $\mathsf{NP} \not\subset \mathsf{BQP}$
- $\mathsf{BQP} \not\subset \mathsf{PH}$
  - $\mathsf{BQP}^A \not\subset \mathsf{PH}^A$



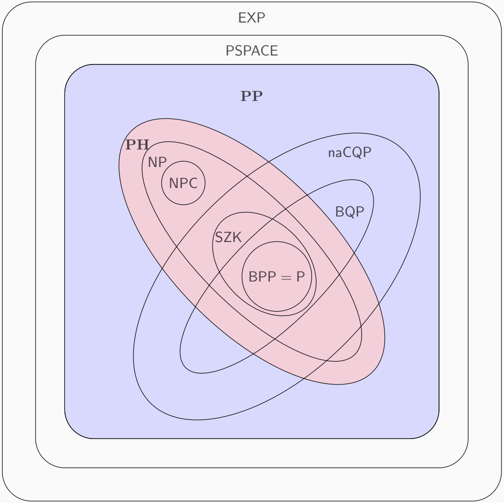
Classes de Complexidade: Relações Conjecturadas

- PH $\subset$ PP



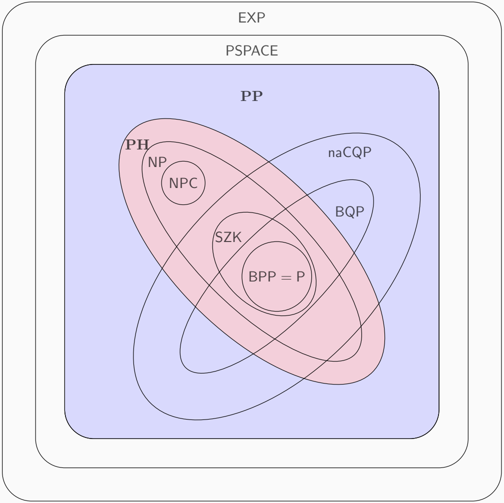
Classes de Complexidade: Relações Conjecturadas

- PH $\subset$ PP
  - Teorema de Toda implica: PH $\subseteq$ BP $\cdot$ PP



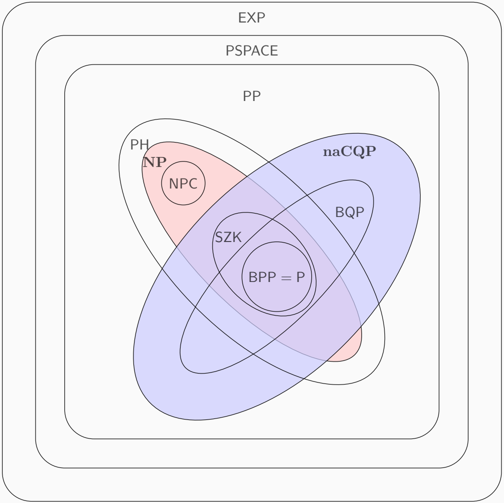
Classes de Complexidade: Relações Conjecturadas

- $\mathsf{PH} \subset \mathsf{PP}$
  - Teorema de Toda implica: $\mathsf{PH} \subseteq \mathsf{BP} \cdot \mathsf{PP}$
  - Com hipóteses de desaleatorização: $\mathsf{BP} \cdot \mathsf{PP} = \mathsf{PP}$



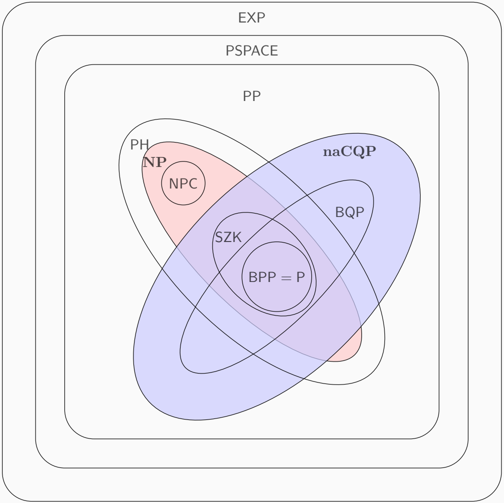
Classes de Complexidade: Relações Conjecturadas

- $\mathsf{NP} \not\subset \mathsf{naCQP}$



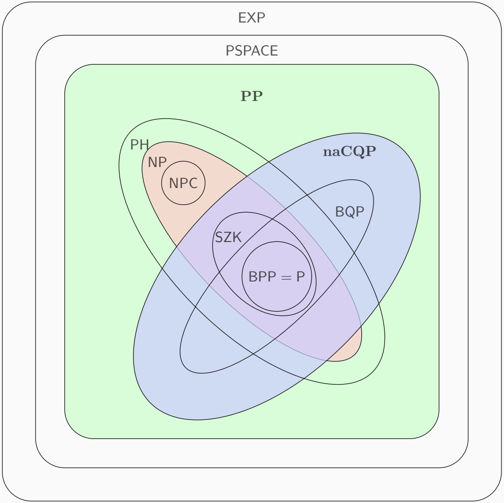
Classes de Complexidade: Relações Conjecturadas

- NP $\not\subset$ naCQP
  - Busca no modelo "caixa-preta" dentre 2^n itens em $\Omega(2^{n/4})$



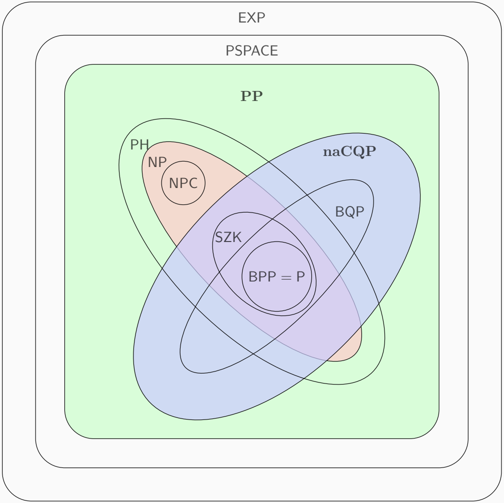
Classes de Complexidade: Relações Conjecturadas

- NP $\not\subset$ naCQP
    - Busca no modelo "caixa-preta" dentre 2^n itens em $\Omega(2^{n/4})$
- naCQP $\subset$ PP



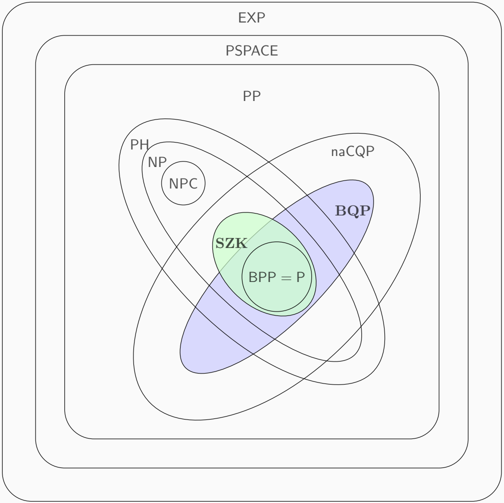
Classes de Complexidade: Relações Conjecturadas

- NP $\not\subset$ naCQP
  - Busca no modelo “caixa-preta” dentre 2^n itens em $\Omega(2^{n/4})$
- naCQP $\subset$ PP
  - Acredita-se que naCQP seja apenas um pouco maior que BQP



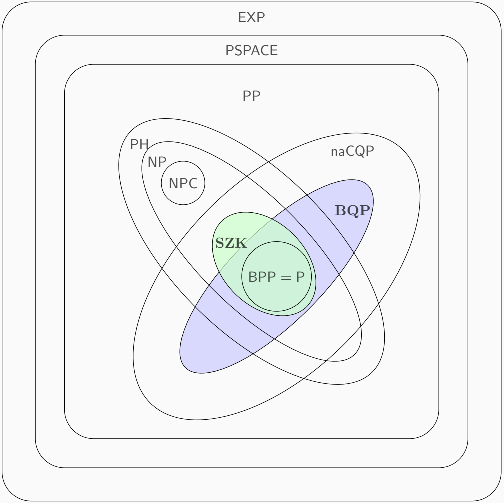
Classes de Complexidade: Relações Conjecturadas

- SZK $\not\subset$ BQP



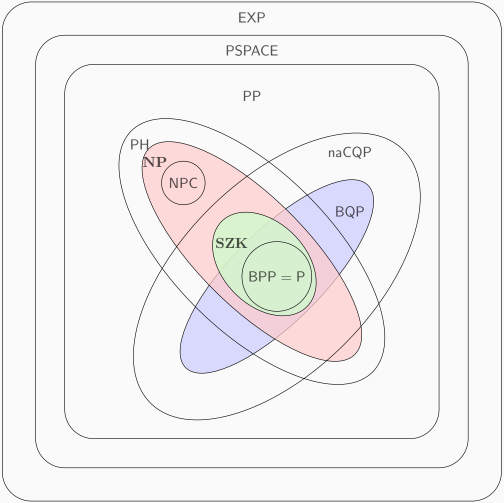
Classes de Complexidade: Relações Conjecturadas

- SZK $\not\subset$ BQP
  - $\text{SZK}^A \not\subset \text{BQP}^A$



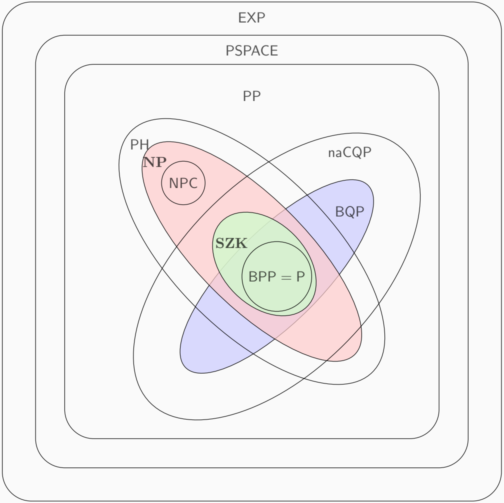
Classes de Complexidade: Relações Conjecturadas

- $\mathsf{SZK} \not\subset \mathsf{BQP}$
  - $\mathsf{SZK}^A \not\subset \mathsf{BQP}^A$
- $\mathsf{SZK} \subsetneq \mathsf{NP}$



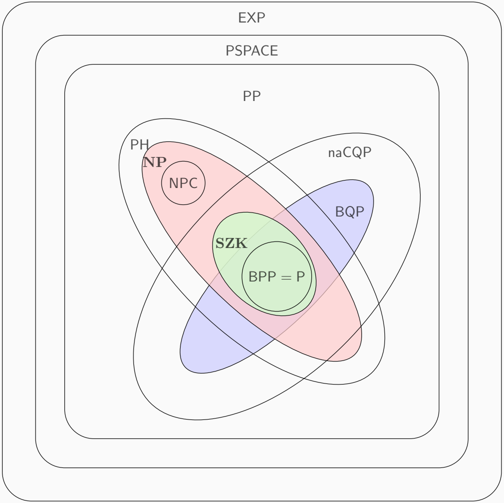
Classes de Complexidade: Relações Conjecturadas

- SZK $\not\subset$ BQP
    - $\text{SZK}^A \not\subset \text{BQP}^A$
- SZK $\subsetneq$ NP
    - Contém problemas como fatoração que está em NP



Classes de Complexidade: Relações Conjecturadas

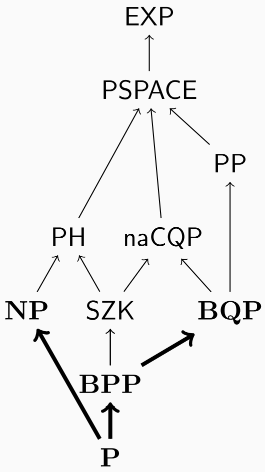
- SZK $\not\subset$ BQP
  - $\text{SZK}^A \not\subset \text{BQP}^A$
- SZK $\subsetneq$ NP
  - Contém problemas como fatoração que está em NP
  - Se NP $\subset$ SZK, PH colapsa.



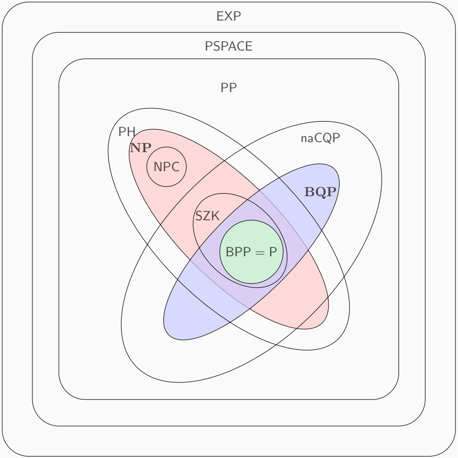
Conclusão

Conclusão

Relações confirmadas



Relações conjecturadas



Uma Revisão sobre a Relação de BQP com outras Classes de Complexidade Computacional

Henrique Hepp[1], Murilo V. G. da Silva[1], Leandro M. Zatesko[2]
hhepp@inf.ufpr.br

20 de setembro de 2019

[1]UFPR, [2]UTFPR

WPCCG 2019