# NP-completeness and physics

## NP-complete Problems and Physical Reality

## Scott Aaronson

**Saman Zarandioon**

**April 2007**

**With Acroread, CTRL-L switch between full screen and window mode**

# NP-completeness and physics

# NP-completeness and physics

## 1 – NP-Complete Problems

# NP-completeness and physics

## 1 – NP-Complete Problems

☞ Question: Can NP-complete problems be solved efficiently in the pysical universe?

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding
  - Quantum Mechanics

# NP-completeness and physics

## 1 – NP-Complete Problems

☞ Question: Can NP-complete problems be solved efficiently in the pysical universe?

- Soap Bubbles
- Protein Folding
- Quantum Mechanics
- Quantum Gravity

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding
  - Quantum Mechanics
  - Quantum Gravity
  - Relativistic Time Dilation

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding
  - Quantum Mechanics
  - Quantum Gravity
  - Relativistic Time Dilation
  - Analog Computing

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding
  - Quantum Mechanics
  - Quantum Gravity
  - Relativistic Time Dilation
  - Analog Computing
  - Anthropic Computing

# NP-completeness and physics

## 1 – NP-Complete Problems

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
  - Soap Bubbles
  - Protein Folding
  - Quantum Mechanics
  - Quantum Gravity
  - Relativistic Time Dilation
  - Analog Computing
  - Anthropic Computing
  - ...

# NP-completeness and physics

Grover's. Can. What is. Quan. Soap. NP-. NP-.

# NP-completeness and physics

☞ Question: Can NP-complete problems be solved efficiently in the pysical universe?

# NP-completeness and physics

- ☞ Question: Can NP-complete problems be solved efficiently in the pysical universe?
- ☞ Why to study this question?

# NP-completeness and physics

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
- Why to study this question?
  - We may find a way to solve our NP-complete problems efficiently (Not that much hope!)

# NP-completeness and physics

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
- Why to study this question?
  - We may find a way to solve our NP-complete problems efficiently (Not that much hope!)
  - To gain insight on NP-complete problems; (May help us to prove $P \neq NP$)

# NP-completeness and physics

- Question: Can NP-complete problems be solved efficiently in the pysical universe?
- Why to study this question?
  - We may find a way to solve our NP-complete problems efficiently (Not that much hope!)
  - To gain insight on NP-complete problems; (May help us to prove $P \neq NP$)
  - To better understand physics and universe

# NP-completeness and physics

# NP-completeness and physics

☞ How can this study help us to better understand universe?!

# NP-completeness and physics

- ☞ How can this study help us to better understand universe?!
  - ➾ Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.

# NP-completeness and physics

- How can this study help us to better understand universe?!
  - Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
  - In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)

# NP-completeness and physics

- How can this study help us to better understand universe?!
  - Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
  - In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)
  - Similar to what we do all the time in computer science (Esp. cryptography) ”Assuming $P \neq NP$, ...”

# NP-completeness and physics

- How can this study help us to better understand universe?!
  - Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
  - In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)
  - Similar to what we do all the time in computer science (Esp. cryptography) "Assuming $P \neq NP$, ..."
- Importance of $P vs. NP$ question: (some quotes:)

# NP-completeness and physics

- ☞ How can this study help us to better understand universe?!
  - ➾ Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
  - ➾ In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)
  - ➾ Similar to what we do all the time in computer science (Esp. cryptography) "Assuming $P \neq NP$, ..."
- ☞ Importance of $P vs. NP$ question: (some quotes:)
  - ➾ "deepest problems in all of mathematics." [51]

# NP-completeness and physics

☞ How can this study help us to better understand universe?!

- ➾ Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
- ➾ In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)
- ➾ Similar to what we do all the time in computer science (Esp. cryptography) "Assuming $P \neq NP$, ..."

☞ Importance of $Pvs.NP$ question: (some quotes:)

- ➾ "deepest problems in all of mathematics." [51]
- ➾ "that no one has any idea where to begin". [35]

# NP-completeness and physics

- How can this study help us to better understand universe?!
  - Persumed interactability of NP-complete problems might be taken as a useful constraint in the search for new physical theories.
  - In other words, we may be able to use $P \neq NP$ as a constraint in the search for new physical theories (like, impossibility of superluminal signaling, and Second Law of Thermodynamics)
  - Similar to what we do all the time in computer science (Esp. cryptography) "Assuming $P \neq NP$, ..."
- Importance of $P vs. NP$ question: (some quotes:)
  - "deepest problems in all of mathematics." [51]
  - "that no one has any idea where to begin". [35]
  - "that we have a pretty sophisticated idea of why we have no idea." [62]

# NP-completeness and physics

# NP-completeness and physics

☞ What do we know about this problem:

# NP-completeness and physics

- What do we know about this problem:
  - If there is no deterministic algorithm can we find a probabilistic or noneuniform algorithm? It is unlikely, Karp and Lipton showed that either of these would collapse polynomial hierarchy[53].

# NP-completeness and physics

☞ What do we know about this problem:

- ➾ If there is no deterministic algorithm can we find a probabilistic or noneuniform algorithm? It is unlikely, Karp and Lipton showed that either of these would collapse polynomial hierarchy[53].
- ➾ Also Impagliazzo and Wigderson gave strong evidence that P = BPP [50].

# NP-completeness and physics

- What do we know about this problem:
  - If there is no deterministic algorithm can we find a probabilistic or noneuniform algorithm? It is unlikely, Karp and Lipton showed that either of these would collapse polynomial hierarchy[53].
  - Also Impagliazzo and Wigderson gave strong evidence that P = BPP [50].
  - It is known that $P \neq NP$ in a "black box" or oracle setting. So, any efficient algorithm for an NP-complete problem would have to exploit the problems structure in a nontrivial way. Brute-force search won't solve the problem [11].

# NP-completeness and physics

## 2 – Soap Bubbles

# NP-completeness and physics

## 2 – Soap Bubbles

☞ Steiner tree is similar to minimum spanning tree but we are allowed to add new vertices (Steiner vertices) to make the total length minimum.

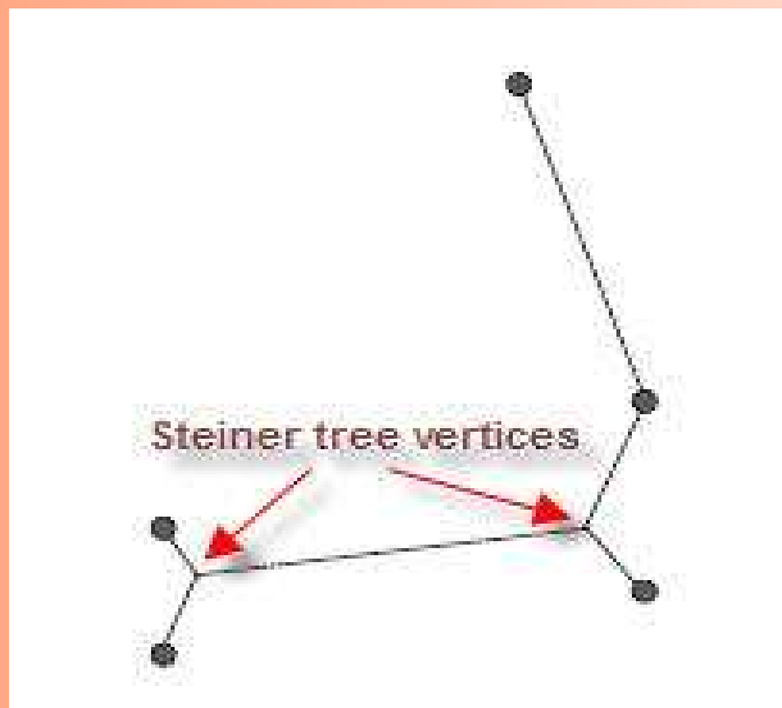


Figure 1: Steiner Tree

# NP-completeness and physics

# NP-completeness and physics

☞ Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)
- Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:

# NP-completeness and physics

☞ Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.

☞ It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)

☞ Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:

  ➾ Finding a Steiner tree is NP-hard

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)
- Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:
  - Finding a Steiner tree is NP-hard
  - Soap bubbles find a Steiner tree in polynomial time

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)
- Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:
  - Finding a Steiner tree is NP-hard
  - Soap bubbles find a Steiner tree in polynomial time
  - Soap bubbles are classical objects

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)
- Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:
  - Finding a Steiner tree is NP-hard
  - Soap bubbles find a Steiner tree in polynomial time
  - Soap bubbles are classical objects
  - Classical physics can be simulated by a Turing machine with polynomial slowdown

# NP-completeness and physics

- Garey, Graham, and Johnson [39] showed that finding Euclidean Steiner tree in NP-hard.
- It was known that if two glass plates with pegs between them are dipped into soapy water, then the soap bubbles will rapidly form a Steiner tree connecting the pegs.( Steiner tree is minimum-energy configuration.)
- Bringsjord and Taylor [24] in June 2004 put these two facts together and argued that $P = NP$:
  - Finding a Steiner tree is NP-hard
  - Soap bubbles find a Steiner tree in polynomial time
  - Soap bubbles are classical objects
  - Classical physics can be simulated by a Turing machine with polynomial slowdown
  - So, it follows that $P = NP$

# NP-completeness and physics

# NP-completeness and physics

☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.

# NP-completeness and physics

☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.

☞ He used some samples from the OR-Library website with 3 to 7 vertices.

# NP-completeness and physics

- ☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- ☞ He used some samples from the OR-Library website with 3 to 7 vertices.
- ☞ This is his result:

# NP-completeness and physics

- Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- He used some samples from the OR-Library website with 3 to 7 vertices.
- This is his result:
  - With 3 or 4 pegs, the optimum tree is usually found.

# NP-completeness and physics

- ☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- ☞ He used some samples from the OR-Library website with 3 to 7 vertices.
- ☞ This is his result:
  - ➾ With 3 or 4 pegs, the optimum tree is usually found.
  - ➾ Especially for more pegs, by no means it is always found.

Grover's.
Can.
What is.
Quan.
Soap.
NP-.
NP-.

# NP-completeness and physics

- ☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- ☞ He used some samples from the OR-Library website with 3 to 7 vertices.
- ☞ This is his result:
  - ➾ With 3 or 4 pegs, the optimum tree is usually found.
  - ➾ Especially for more pegs, by no means it is always found.
  - ➾ Sometimes the resulting configuration is not even of the correct form and it contains structures that can never happen in a Steiner tree. (local minima)

# NP-completeness and physics

- ☞ Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- ☞ He used some samples from the OR-Library website with 3 to 7 vertices.
- ☞ This is his result:
  - ➾ With 3 or 4 pegs, the optimum tree is usually found.
  - ➾ Especially for more pegs, by no means it is always found.
  - ➾ Sometimes the resulting configuration is not even of the correct form and it contains structures that can never happen in a Steiner tree. (local minima)
  - ➾ Result were highly nondeterministic. Different results in different experiments for the same structure.

# NP-completeness and physics

- Scott Aaronson conducted an experience to see if soap bubbles can really solve this NP-complete problem in poly-time.
- He used some samples from the OR-Library website with 3 to 7 vertices.
- This is his result:
  - With 3 or 4 pegs, the optimum tree is usually found.
  - Especially for more pegs, by no means it is always found.
  - Sometimes the resulting configuration is not even of the correct form and it contains structures that can never happen in a Steiner tree. (local minima)
  - Result were highly nondeterministic. Different results in different experiments for the same structure.
  - Sometimes the bubbles would start in a suboptimal configuration and then slowly ”relax” toward a better one. Even with 4 or 5 pegs, this process could take around ten seconds.

# NP-completeness and physics

# NP-completeness and physics

- There are some other proposed methods for solving NP-complete problems that involves relaxation to a minimum-energy state; for example, **protein folding**.

# NP-completeness and physics



- There are some other proposed methods for solving NP-complete problems that involves relaxation to a minimum-energy state; for example, **protein folding**.
  - All of these methods are subject to the same pitfalls of local optima and potentially long relaxation times.

# NP-completeness and physics



- There are some other proposed methods for solving NP-complete problems that involves relaxation to a minimum-energy state; for example, **protein folding**.
  - All of these methods are subject to the same pitfalls of local optima and potentially long relaxation times.
  - It seems that proteins are evolved in such a way that do not have local optima.

# NP-completeness and physics



- There are some other proposed methods for solving NP-complete problems that involves relaxation to a minimum-energy state; for example, **protein folding**.
  - All of these methods are subject to the same pitfalls of local optima and potentially long relaxation times.
  - It seems that proteins are evolved in such a way that do not have local optima.
  - But this means that protein folding mechanism may fail to solve a protein folding of an artificial protein that is generated from a 3SAT problem; so we can not use them to solve general NP-complete problems efficiently. (They are efficient only in solving especial instances of proteins - i.e. natural proteins.)

# NP-completeness and physics

## 3 – Quantum Computing



- Having constant number of parallel processor will not help us in to solve NP-complete problems. It can just improve running time by a constant factor.
- What if we had access to exponential units that are parallel?
- In quantum computers the state of n bits is maintained using $2^n$ hidden complex numbers. Could we exploit this exponentiality inherent in the nature to try out all $2^n$ possible solutions to an NP-complete problem in parallel?
- Can quantum computers efficiently compute anything that is not efficiently computable by machines that are built based on classical physics (Turing equivalent Machines)?

# NP-completeness and physics



## 4 – What is Quantum Computer?

- Quantum computers are proposed based on three basic principles in quantum mechanics:
  - The superposition principle: An n-bit quantum register that has $k = 2^n$ classical state, has a quantum state that is a linear combination (superposition) of all classical states with complex coefficients. Therefore the quantum state of this register can be represented by a k-dimensional complex vector. Using ket notation we can represent its states as:

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

    Where $\alpha_i$ is the complex amplitude corresponding to classical state $|i\rangle$ which is a vector that only its $i^{th}$ row is one and the rest is zero.
  - The measurement principle: The quantum state of a quantum register is hidden to us the only thing we can do is measuring it and we will

# NP-completeness and physics

get classical state $|i\rangle$ with probability $|\alpha_i|^2$ (So, length of quantum state vector should be unit, Hilbert space)

The weird thing is that measurements following the first measurement will result the same value that was obtained in the first measurement. (This property forms the basis of quantum cryptography.)

- Unitary evolution: Every operation on the quantum state vector is a unitary operation. Intuitively, a unitary operator is a rotation or reflection of the Hilbert space.

# NP-completeness and physics

## 5 – Can quantum computer efficiently solve 3SAT?

- Can we design a brute-force quantum algorithm that inspects all possible assignments and returns the one that satisfies the 3SAT? NO!
- In 1994 Bennett, Bernstein, Brassard, and Vazirani [17] showed that any quantum algorithm that searches an unordered database of N items ( $2^n$ assignments of 3SAT )for a single "marked" item (satisfying assignment) must query the database about $\sqrt{N}$ times.
- This follows that any brute-force algorithm needs at least $2^{n/2}$ steps.
- Therefore any potential efficient algorithm should exploit the structure of 3SAT formula.
- Why couldn't we use the inherent exponential parallelism in the quantum mechanics? All proves for this lower-bound exploit linearity of quantum operators which is the crucial property of quantum mechanics. Intuitively, if we think of the components of a superposition as "parallel universe," then linearity is what prevents the universe containing the marked item from simply "telling all the other universes about it."

# NP-completeness and physics

## 6 – Grover's Algorithm

# NP-completeness and physics

## 6 – Grover's Algorithm

- Ok, is there at least an algorithm that can find a solution to 3SAT formula $\Phi$ in $2^{n/2}$ steps?

# NP-completeness and physics

## 6 – Grover's Algorithm

- Ok, is there at least an algorithm that can find a solution to 3SAT formula $\Phi$ in $2^{n/2}$ steps?
- $2^{n/2}$ is much smaller than $2^n$ which is the number of steps in a brute-force algorithm in classical machines.

# NP-completeness and physics

## 6 – Grover's Algorithm

- Ok, is there at least an algorithm that can find a solution to 3SAT formula $\Phi$ in $2^{n/2}$ steps?
- $2^{n/2}$ is much smaller than $2^n$ which is the number of steps in a brute-force algorithm in classical machines.
- In 1996, Grover found a quantum algorithm with running time of $O(2^{n/2})$.

# NP-completeness and physics

## 6 – Grover's Algorithm

- Ok, is there at least an algorithm that can find a solution to 3SAT formula $\Phi$ in $2^{n/2}$ steps?
- $2^{n/2}$ is much smaller than $2^n$ which is the number of steps in a brute-force algorithm in classical machines.
- In 1996, Grover found a quantum algorithm with running time of $O(2^{n/2})$.
- Algorithm: WLG, assume function f has a single satisfying assignment **a**. Consider an n-qbit register and let **u** denote the uniform state vector of this register (i.e. **u**=$\frac{1}{2^{n/2}}\Sigma_{x\in\{0,1\}^n} |x\rangle$ ).

# NP-completeness and physics

## 6 – Grover's Algorithm

- Ok, is there at least an algorithm that can find a solution to 3SAT formula $\Phi$ in $2^{n/2}$ steps?
- $2^{n/2}$ is much smaller than $2^n$ which is the number of steps in a brute-force algorithm in classical machines.
- In 1996, Grover found a quantum algorithm with running time of $O(2^{n/2})$.
- Algorithm: WLG, assume function f has a single satisfying assignment **a**. Consider an n-qbit register and let **u** denote the uniform state vector of this register (i.e. **u**=$\frac{1}{2^{n/2}}\Sigma_{x\in\{0,1\}^n}|x\rangle$ ).
- Using property of inner product, $\langle \mathbf{u}, |a\rangle\rangle = \frac{1}{2^{n/2}} = cos(\pi/2-\theta)$, therefore $sin\theta = \frac{1}{2^{n/2}}$ and assuming n is sufficiently large, $\theta \geq \frac{1}{2.2^{n/2}}$ (since for small $\theta$, $sin\theta \sim \theta$).

# NP-completeness and physics

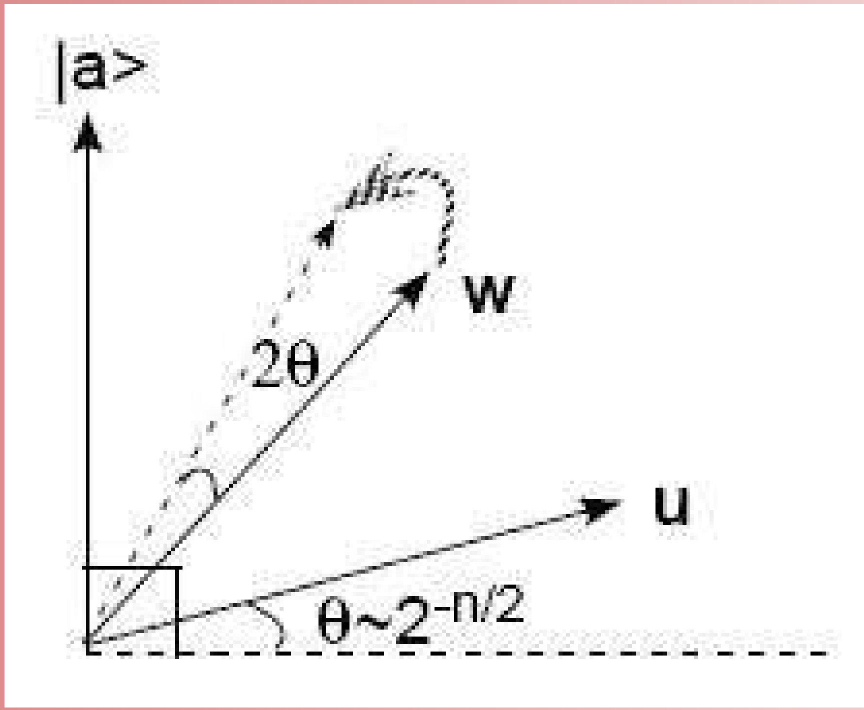


Figure 2: Get $2\theta$ closer to $|a\rangle$ at each step

- Start from state **u** at each step transform it to a state that is $2\theta$ closer to $|a\rangle$.
- So, in $O(1/\theta) = O(2^{n/2})$ steps it gets close enough to vector **a** so our measurement will yield a with high probability.

# NP-completeness and physics

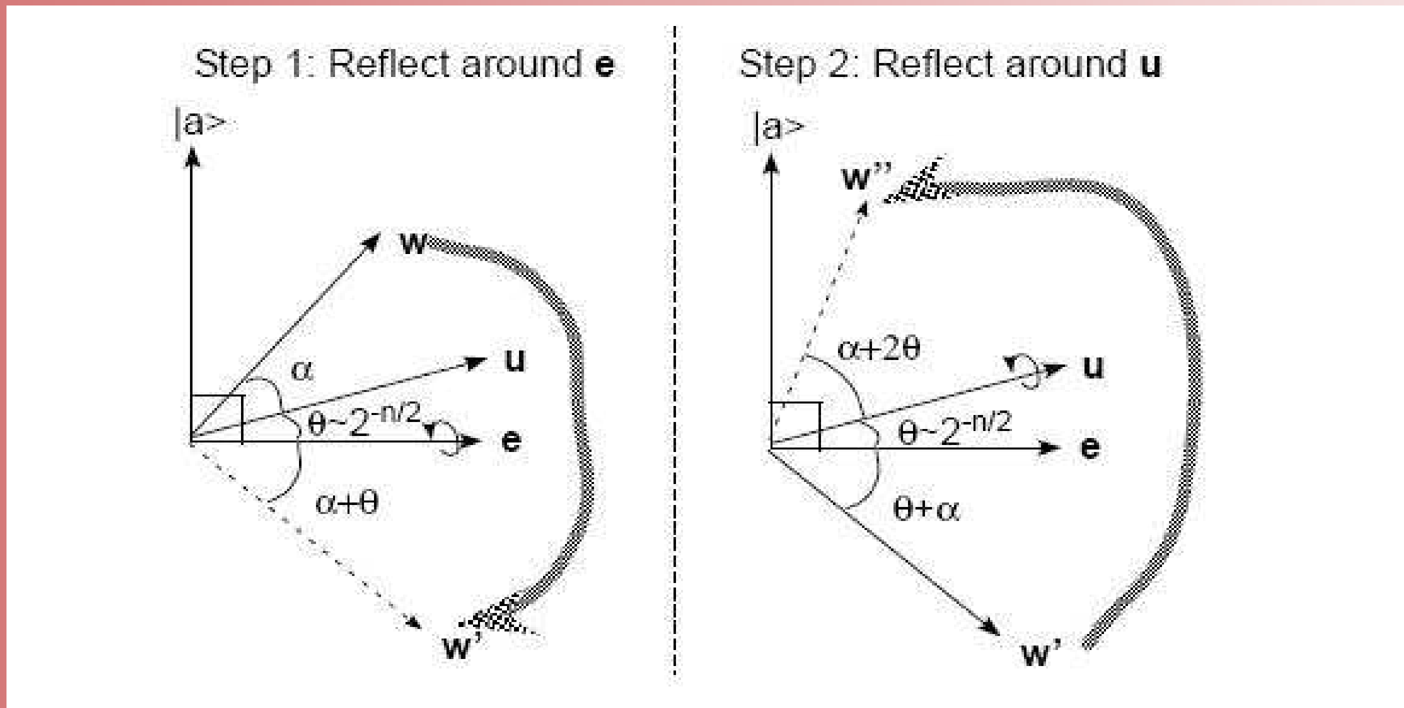


Figure 3: How to get $2\theta$ closer to $|a\rangle$

- Prove by picture: Figure 3 illustrates how by reflection around the vector **a** and the vector **e**$= \Sigma_{x\neq a} |a\rangle$ (**e** is the vector orthogonal to $|a\rangle$ in the plane spanned by **u** and $|a\rangle$.

# NP-completeness and physics

- Ok, so we can search a database faster, but is there anything that we cannot do in polynomial time in classical model that we can do in quantum computers?
- P. Shor in 1997 introduced an polynomial time quantum algorithm for factoring problem. Still we do not know any deterministic or probabilistic efficient algorithm for factoring in classical model.
- Also there is an efficient quantum algorithm for Discrete Log problem.
- If we cannot solve NP-complete problems using NP-complete problems, can we design a quantum algorithm that solves a SAT problem by exploiting its structure in a nontrivial way? We don't know! it is an open question.

# NP-completeness and physics

- Lets call the class of problems that can be solved by applying polynomial number of quantum operators BQP(Bounded error, Quantum, Polynomial time)
- Theorem: P $\subseteq$ BPP $\subseteq$ BQP $\subseteq$ $P^{\#P}$ $\subseteq$ PSPACE.

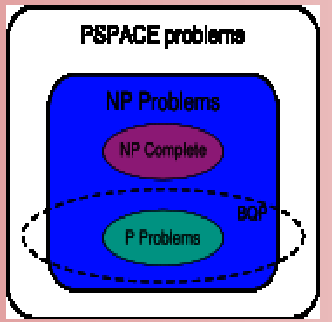


Figure 4: The suspected relationship of BQP to other problem spaces (Wikipedia)

- The fact that operators in quantum computers are linear makes them less powerful, otherwise the could solve PSPACE problems in polynomial time!