

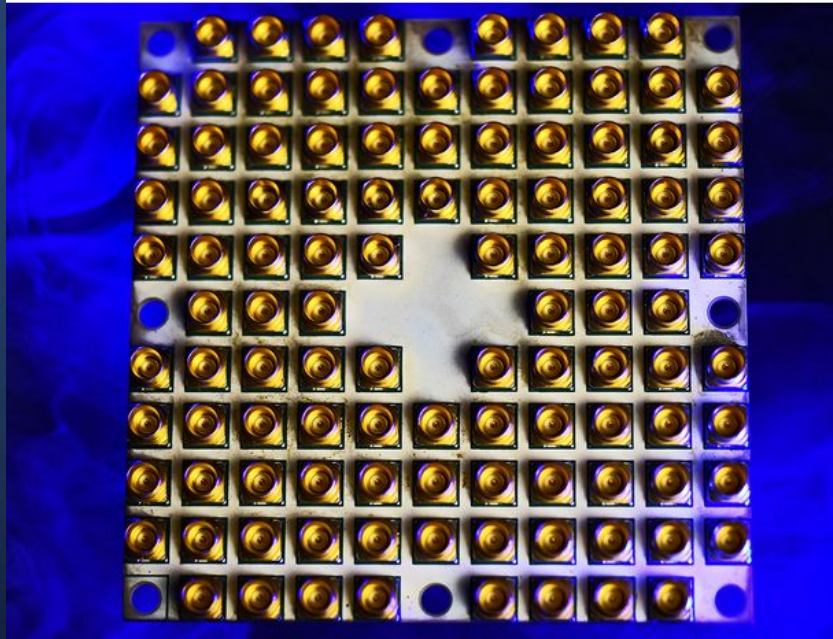
A decorative graphic on the left side of the slide, consisting of a network of light blue lines and small circles, resembling a circuit board or a quantum network, extending from the top to the bottom.

ALGORITHMS FOR QUANTUM COMPUTERS

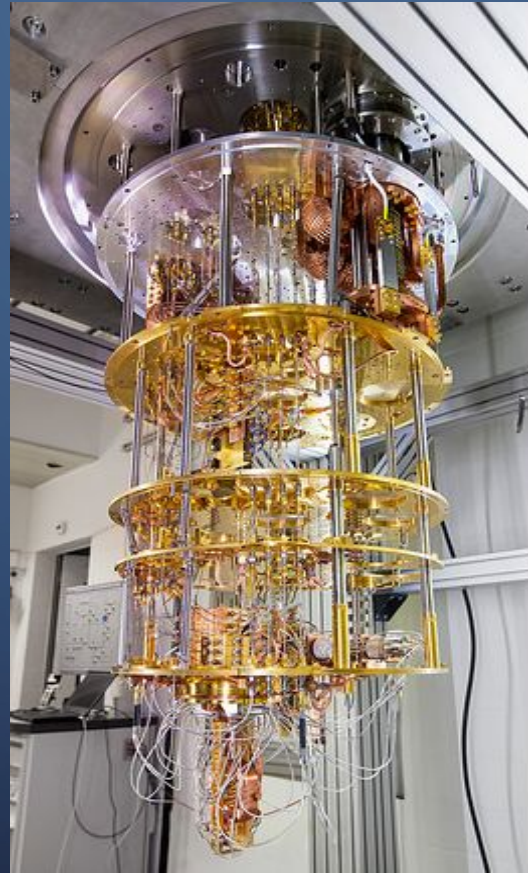
ANDRIS AMBAINIS

UNIVERSITY OF LATVIA

SMALL SCALE QUANTUM COMPUTERS



Intel, 49
qubits

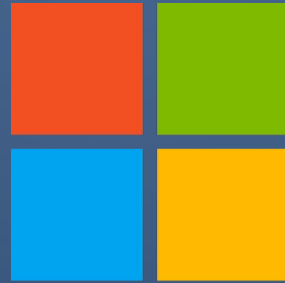


IBM, 50
qubits



Google, 72
qubits

OTHER QUANTUM COMPUTING EFFORTS

The logo for Rigetti, featuring the word "rigetti" in a lowercase, sans-serif font. The "ri" is in a teal color, and the "getti" is in a grey color.

Microsoft

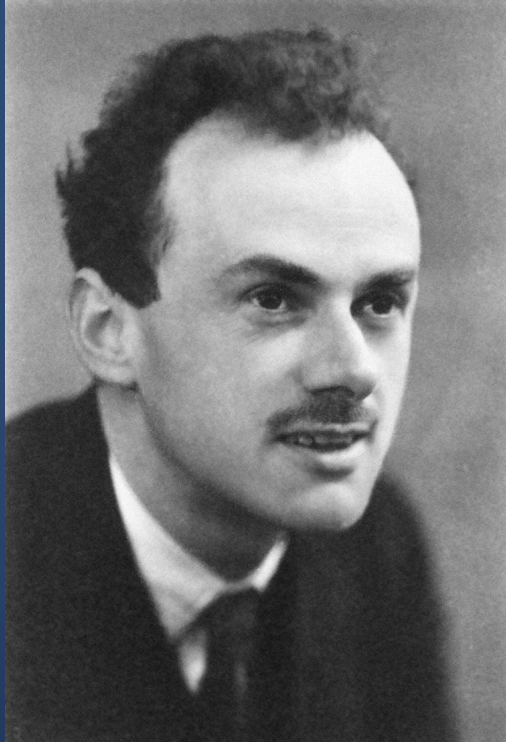


The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks. These elements consist of thin white lines that branch out and terminate in small white circles, creating a symmetrical, abstract pattern in each corner.

QUANTUM SIMULATION

NUMBER OF VARIABLES

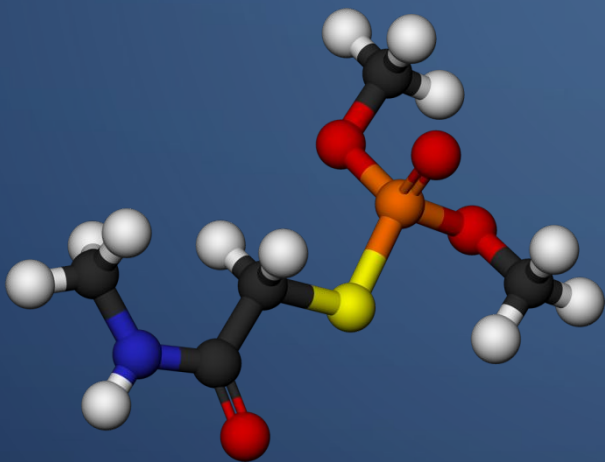
- 30 particles – $2^{30} \approx 1,000,000,000.$
- 100 particles – $2^{100} \approx \underbrace{1,000 \dots 000.}_{30 \text{ zeros}}$



Paul
Dirac,
1929

The underlying physical laws ...
for a large part of physics and
the whole chemistry are thus
completely known and the
difficulty is only that the exact
application of these laws leads
to equations much too
complicated to be soluble.

QUANTUM CHEMISTRY



$$H|\Psi\rangle = E|\Psi\rangle$$

$$H = \sum_{p,q} t_{pq} c_p^\dagger c_q + \sum_{p,q,r,s} V_{pqrs} c_p^\dagger c_q^\dagger c_r c_s$$

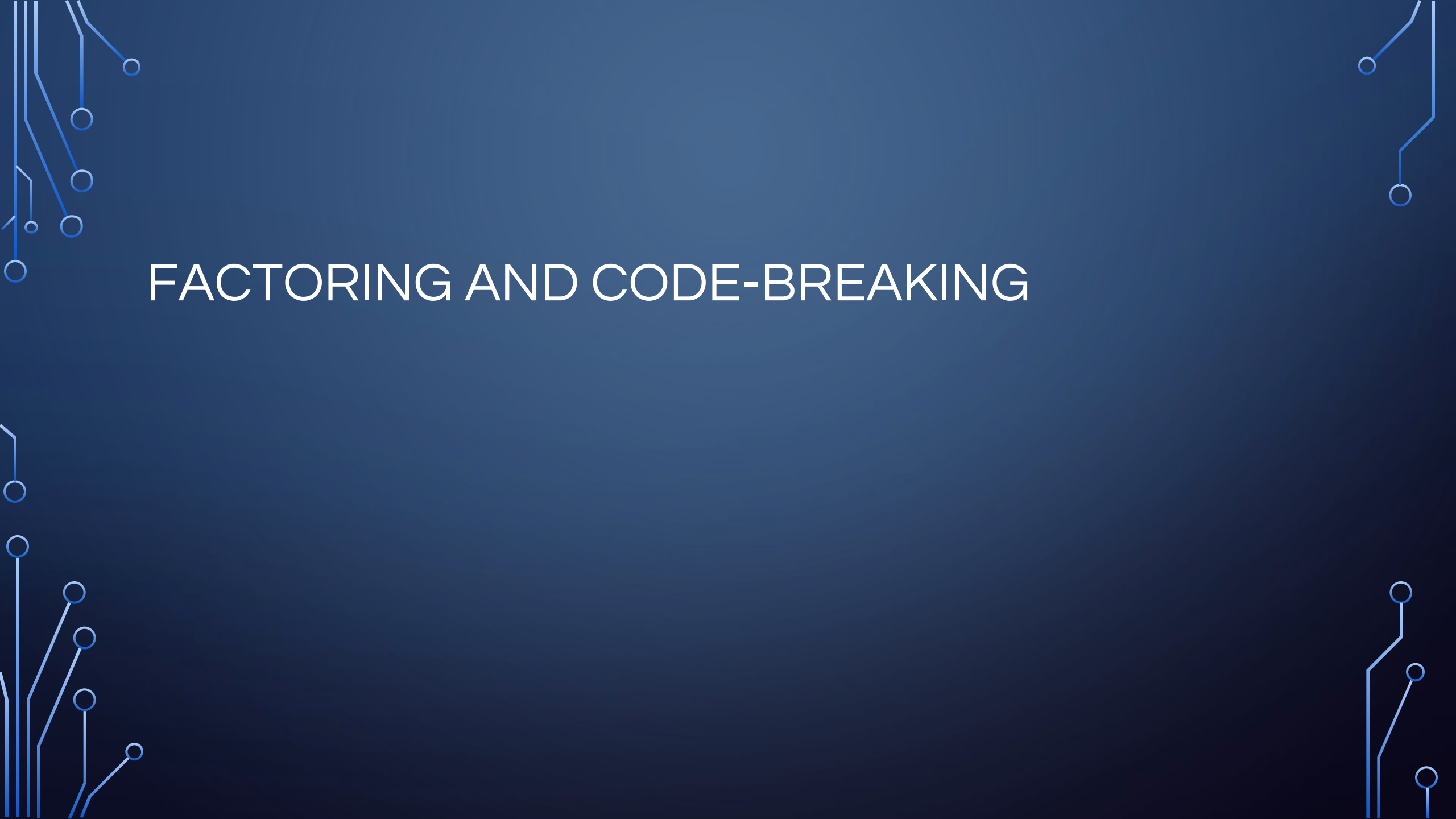
A substantial application for
HPC

EXAMPLE: NITROGEN FIXATION



- $\text{N}_2 \rightarrow 2 \text{NH}_3$.
- Performed at room temperature by nitrogenase enzyme in plants.
- The active site (**FeMoCo**) can be modelled with **110-2000** qubits.

Reiher et al., Elucidating reaction mechanisms on quantum computers, PNAS, 2017:201619152.

The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks. These elements consist of thin white lines that branch out and terminate in small white circles, creating a symmetrical, abstract pattern in each corner.

FACTORING AND CODE-BREAKING

FACTORING

$$6231540623 = 93599 * 66577.$$

Given 6231540623, find factors?

For large (300 digit) numbers conventional computers are too slow.

Shor, 1994: quantum computers can factor large numbers efficiently.

IMPLICATIONS

- RSA and other cryptosystems based on factoring/discrete log broken by quantum computers.
- Quantum algorithms for other crypto-related problems:
 - Pell's equation [Hallgren, 2002],
 - ideal class group [Biasse, Song, 2016],
 - principal ideal problem [Hallgren, 2002, Biasse, Song, 2016].

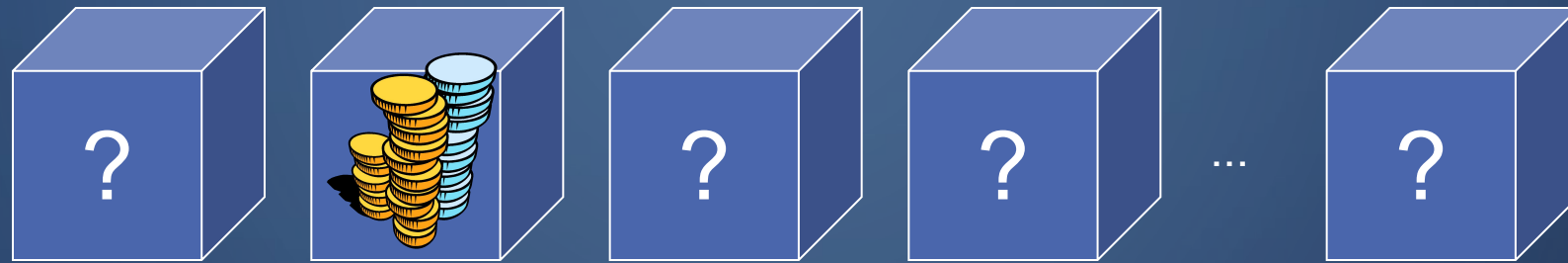
POST QUANTUM CRYPTOGRAPHY

- Classical schemes secure against quantum attacks:
 - Lattice based (e.g. NTRU, LWE);
 - Code based (e.g. McEliece);
 - Based on multivariate quadratic equations (oil-and-vinegar);
- NIST Call for Proposals for Post Quantum Crypto Standard: Nov 30, 2017.

The image features a dark blue gradient background. In the corners, there are decorative elements resembling circuit board traces or neural network connections. These consist of thin, light blue lines that branch out and terminate in small circles. The top-left and bottom-left corners have more complex, dense patterns of these lines, while the top-right and bottom-right corners have simpler, more sparse patterns.

SEARCH

QUANTUM SEARCH



- N objects;
- Find an object with a certain property.

Grover, 1996: $O(\sqrt{N})$ quantum steps.

Polskie Książki Telefoniczne

94/95

WARSZAWA
I WOJEWÓDZTWO WARSZAWSKIE

Spis firm w układzie branżowym i alfabetycznym
Telefony alarmowe, numery kierunkowe
Mapy województwa i centrum Warszawy
Przewodnik po centrum handlowym

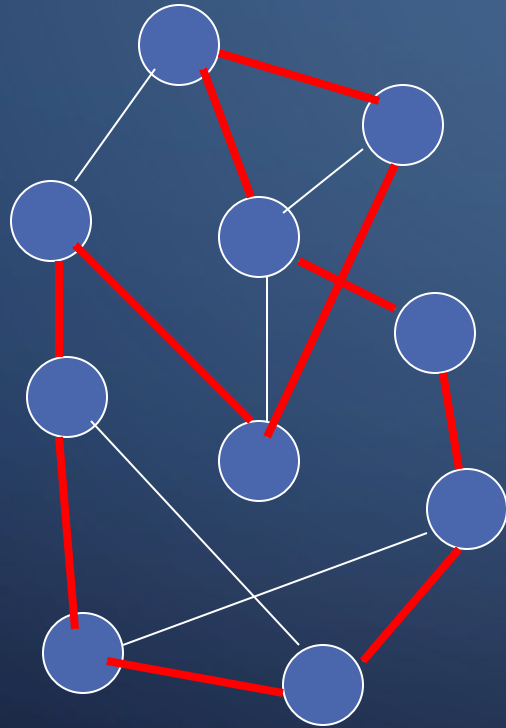
600 000 książek za darmo

Who has the
number
67033706?

Usual computer: $N = 1,000,000$
steps

Quantum computer: $\sqrt{N} = 1000$

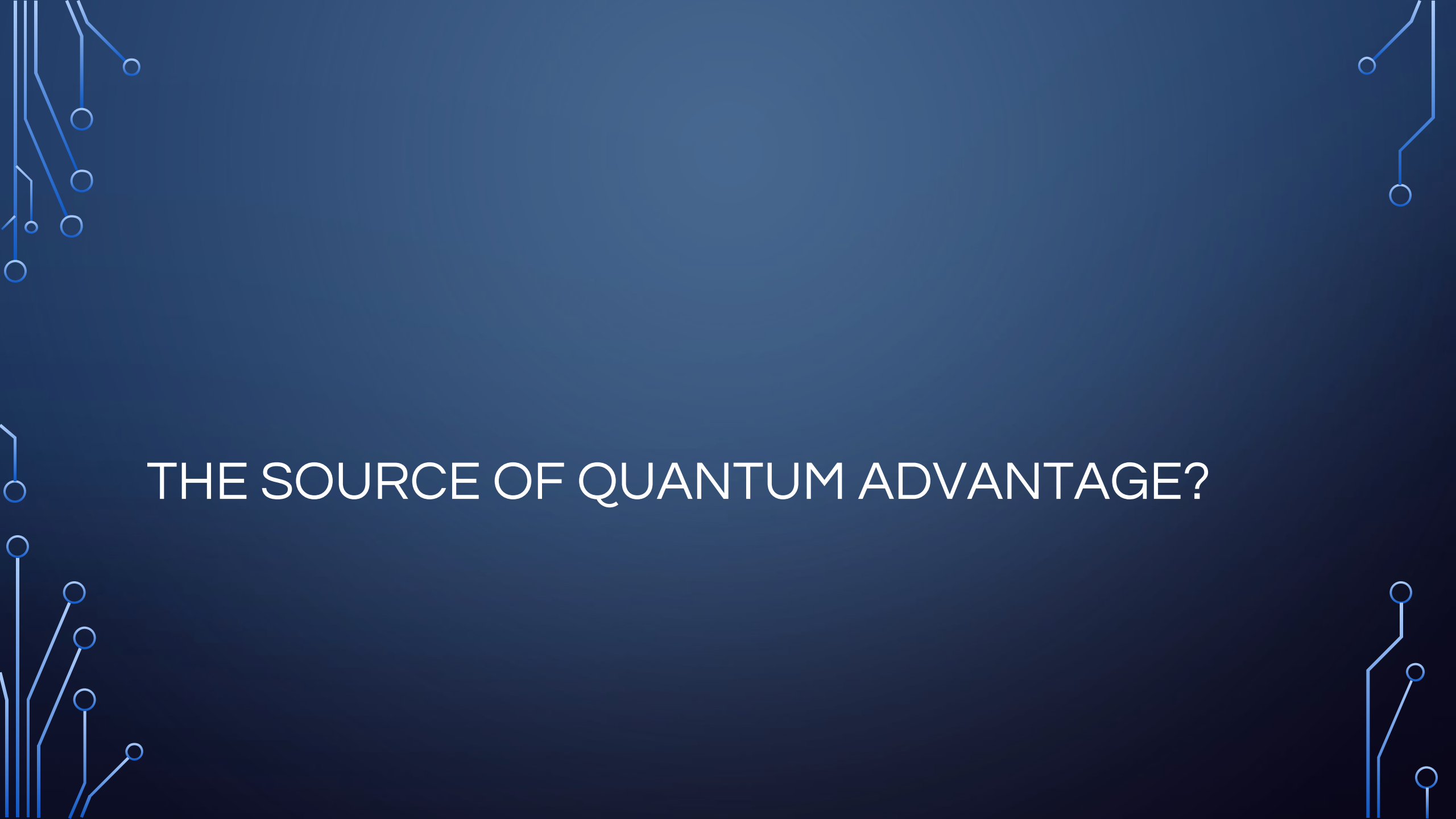
APPLICATION: TRAVELING SALESMAN PROBLEM



Find the best route through all the cities.

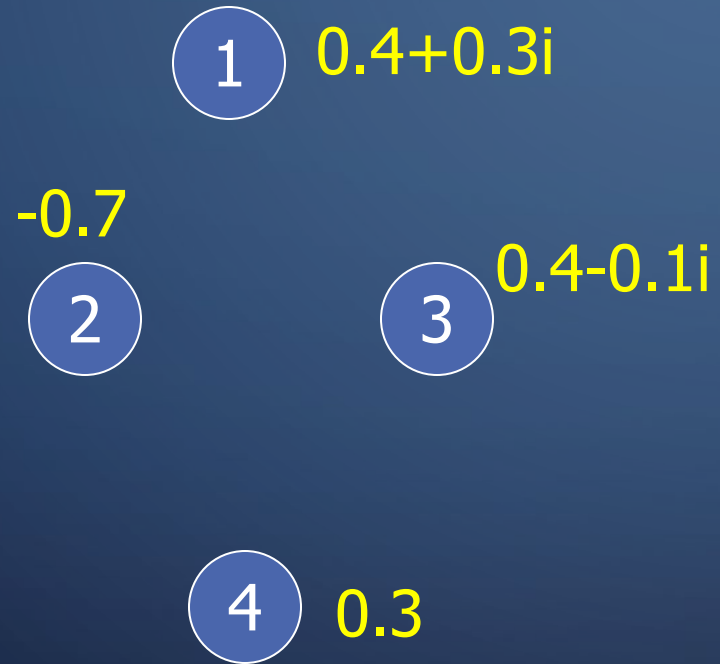
Quantum algorithm:

- 1,000,000 candidates;
- Time = 1,000

The image features a dark blue gradient background. In the corners, there are decorative elements resembling circuit board traces or neural network connections, consisting of thin white lines and small white circles.

THE SOURCE OF QUANTUM ADVANTAGE?

QUANTUM SYSTEM



Current state: i with amplitude α_i .

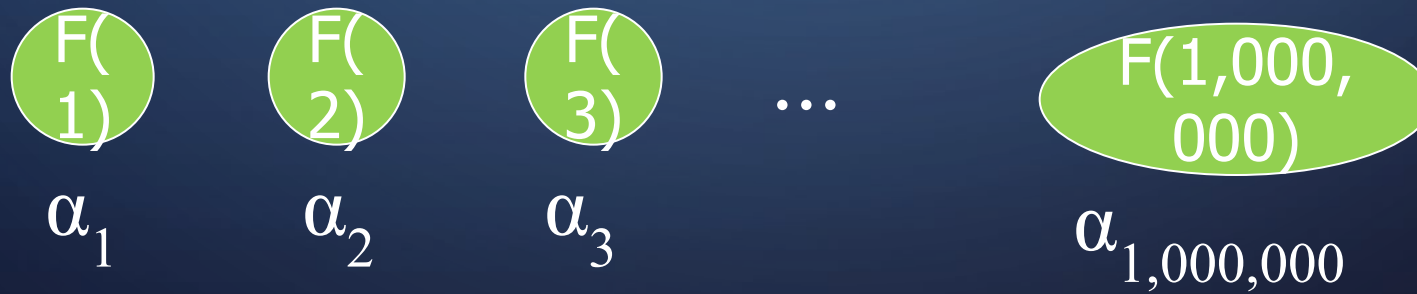
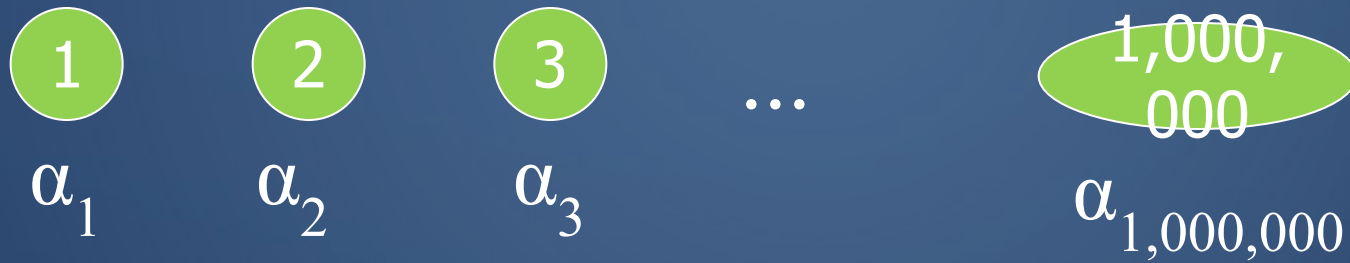
$$\sum_i |\alpha_i|^2 = 1$$



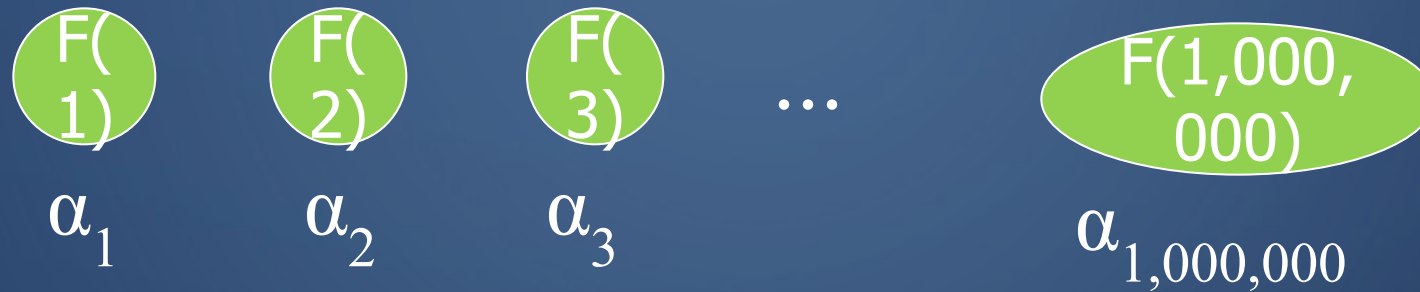
What is it [quantum mechanics] about? From my perspective, it's about information and probabilities and observables, and how they relate to each other.

/Scott Aaronson, MIT,
2005/

QUANTUM PARALLELISM



WHAT CAN WE DO WITH SUCH STATE?

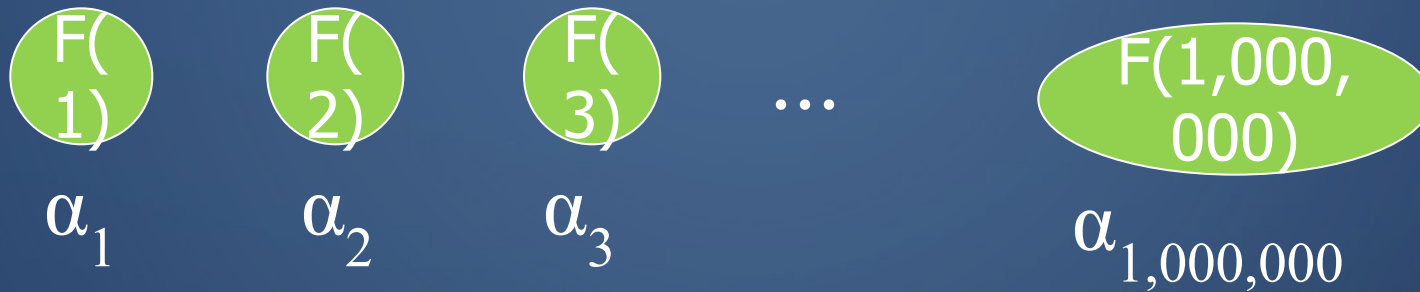


Measurement



Other values are
lost!

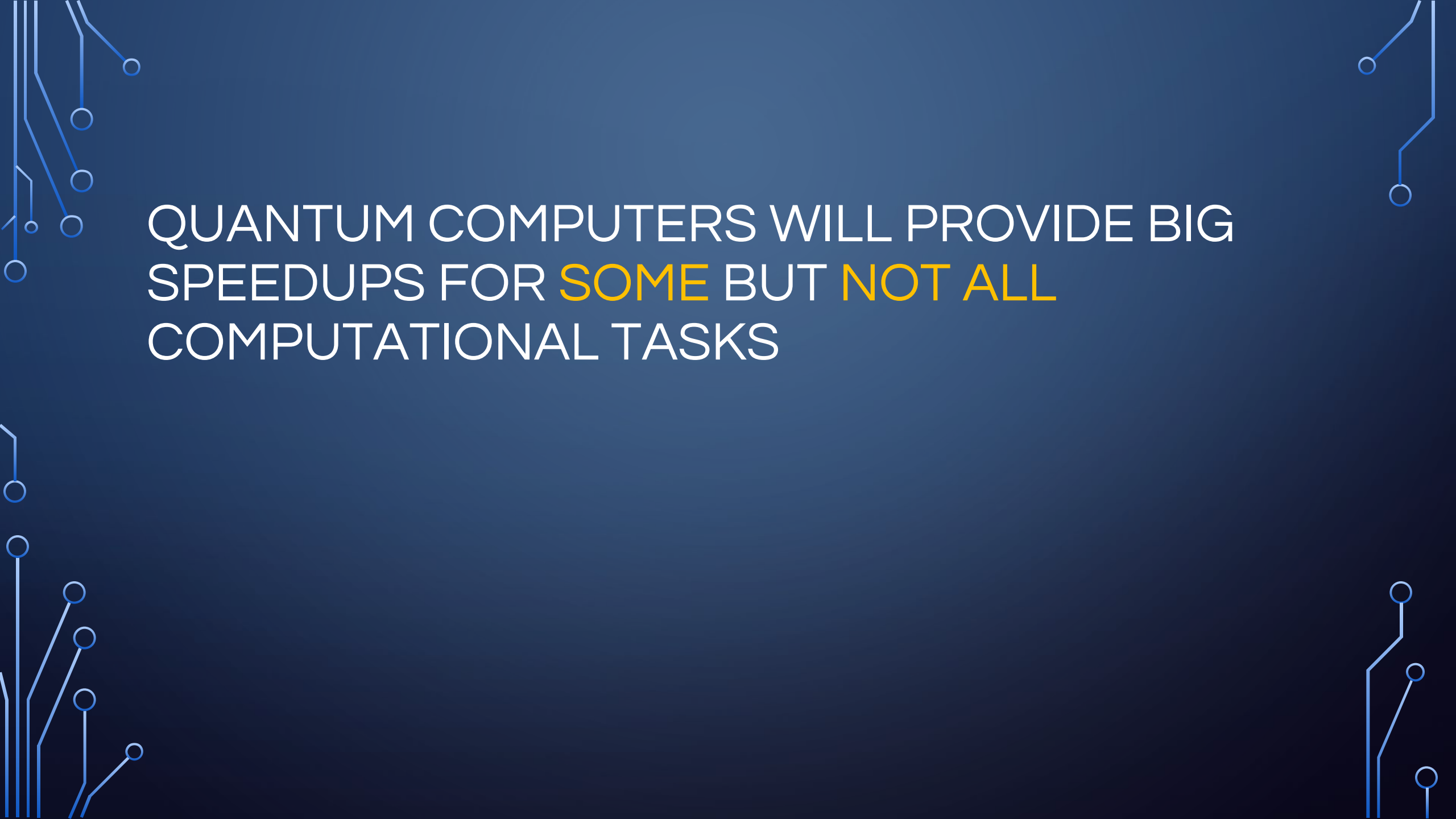
QUANTUM INTERFERENCE



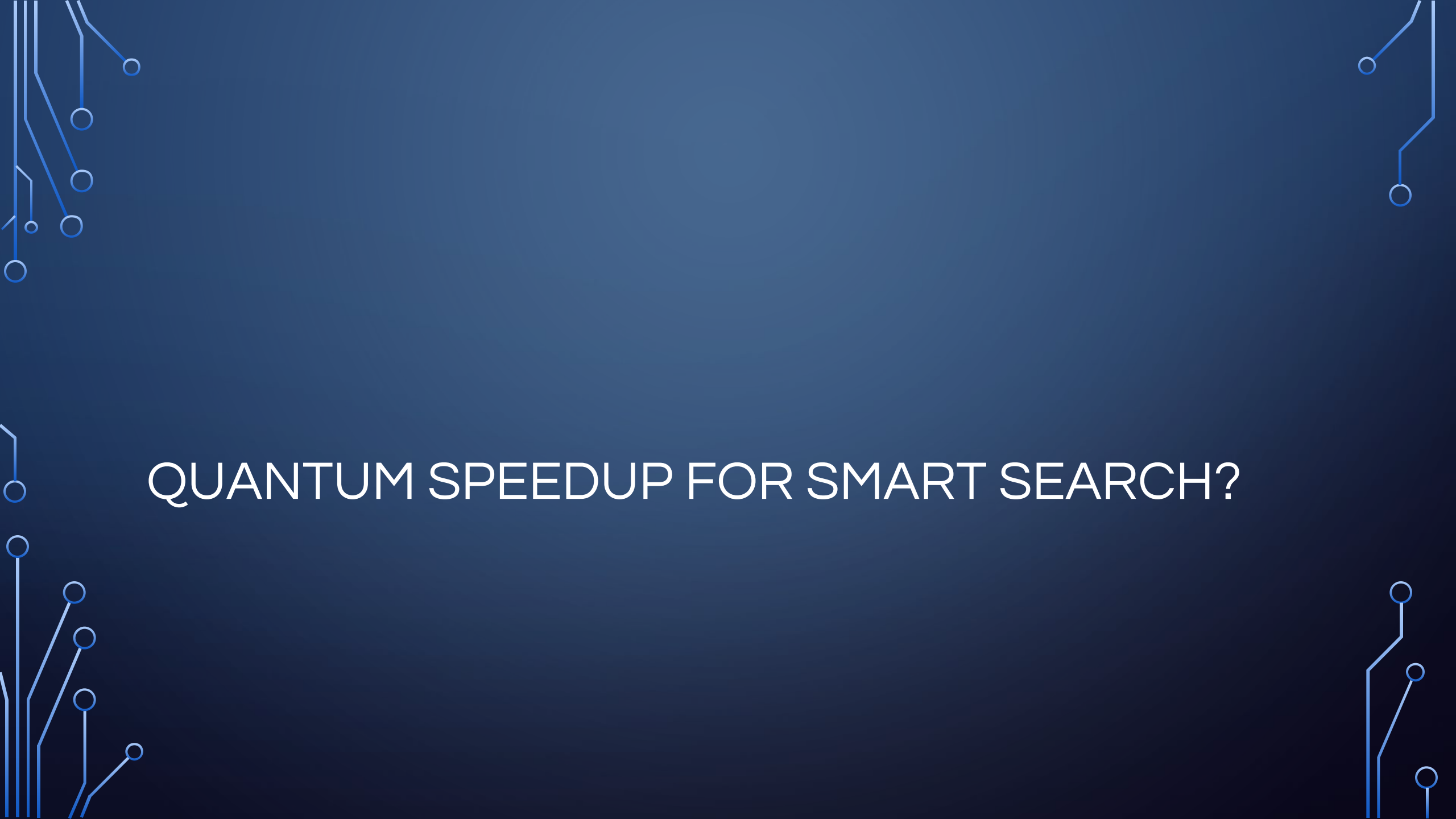
Result that depends on all
values

$F(1), F(2), \dots$

Example: quantum Fourier transform finds periods
quickly

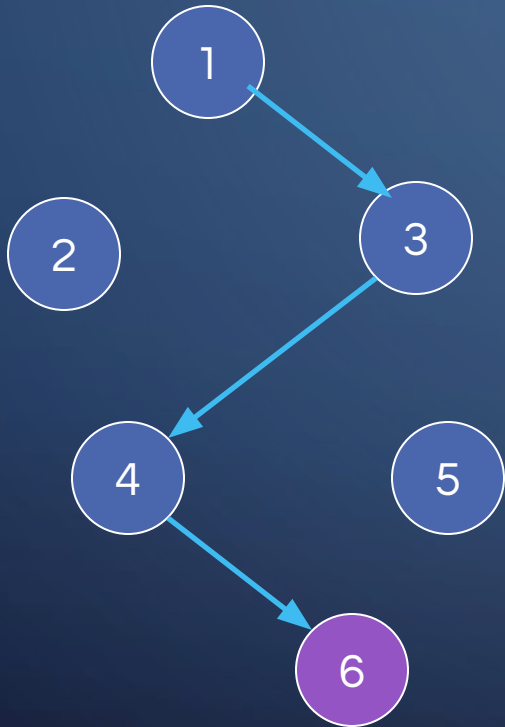
The background is a dark blue gradient. It features decorative white circuit-like lines with small circles at the ends, resembling a printed circuit board (PCB) layout. These lines are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

QUANTUM COMPUTERS WILL PROVIDE BIG
SPEEDUPS FOR **SOME** BUT **NOT ALL**
COMPUTATIONAL TASKS

The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural network connections. These include straight lines, right-angle turns, and small circles at the ends of the lines.

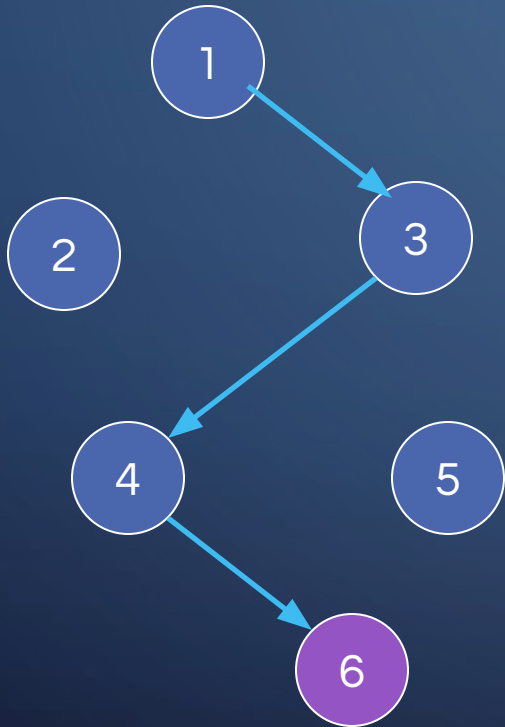
QUANTUM SPEEDUP FOR SMART SEARCH?

QUANTUM WALK SEARCH [SZEGEDY, 04]



- Finite search space.
- Some elements might be marked.
- Find a marked element!
 - Perform a random walk, stop after finding a marked element.

CONDITIONS ON MARKOV CHAIN



- Random walk must be symmetric: $p_{xy} = p_{yx}$.
- Start state = uniformly random state.
- T = expected time to reach marked state, if there is one.

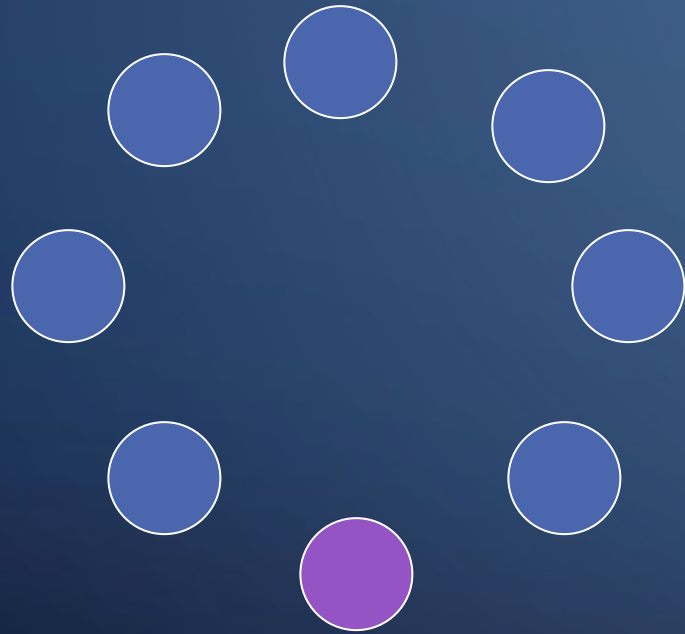
MAIN RESULT [SZEGEDY, 04]

Theorem Assume that:

1. There are no marked states, or
2. A marked state is reached in expected time at most T .

A quantum algorithm can distinguish the two cases in time $O(\sqrt{T})$.
Quadratic speedup for a variety of problems.

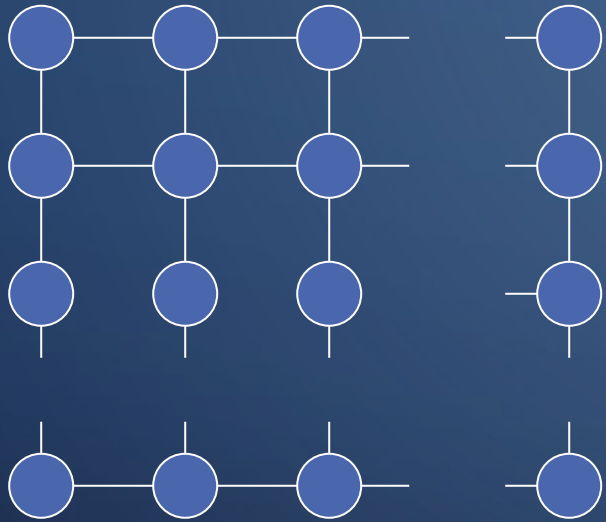
APPLICATION 1



Quantum: $O(\sqrt{N})$
steps

- N states.
- Is there a marked state?
- Random walk: at each step move to a randomly chosen vertex.
- Finds a marked vertex in N [Grover] expected steps.

APPLICATION 2: SEARCH ON GRIDS



- Random walk: at each step move to a random neighbour.
- Finding marked state: $O(N \log N)$ steps.

Quantum
algorithm:

[A, Kempe, Rivosh,
2005]

$$O(\sqrt{N \log N})$$

APPLICATION 3: ELEMENT DISTINCTNESS

31 40 75 71 93 32 47
11 70 37 78 79 36 63
40 48 98 23 41 16 66
75 38 27 42 55 77 19
45 15 53 22 91 37 90
58 13 10 25 29 25 56
68 12 11 51 23 77 15
17 24 88 56 42

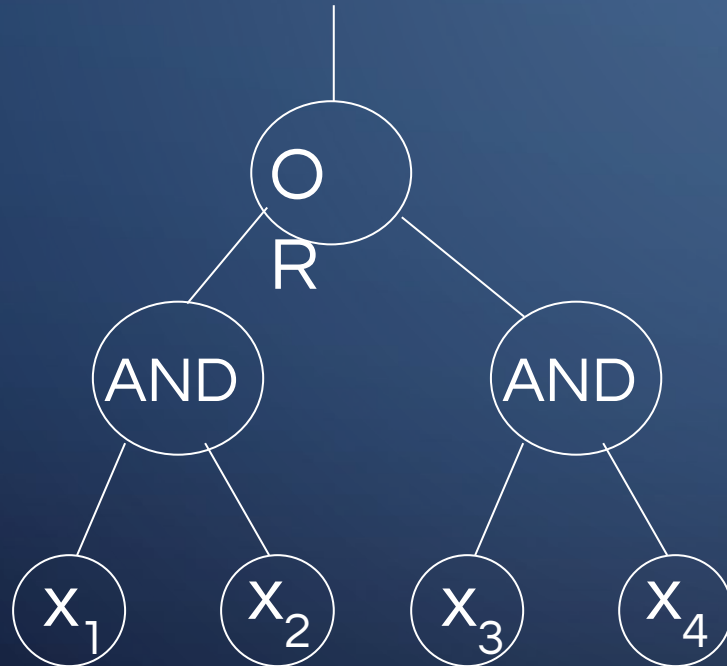
[A, 2004]

- Are there 2 equal numbers?
- Usual algorithms: N steps.
- Quantum algorithms: $O(N^{2/3})$.

The background is a dark blue gradient. In the corners, there are decorative white line art elements resembling circuit boards or neural networks. These elements consist of thin white lines that branch out and terminate in small white circles, creating a symmetrical, abstract pattern in each corner.

QUANTUM ALGORITHMS FOR LOGIC FORMULAS

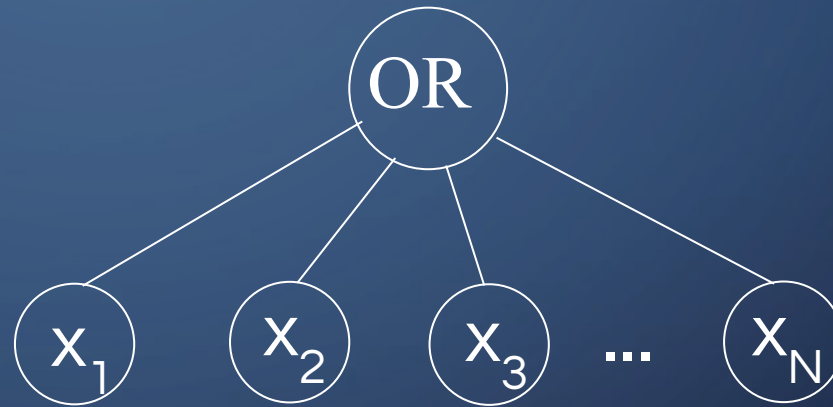
EVALUATING AND-OR TREES



- Variables x_i accessed by queries to a black box:
 - Input i ;
 - Black box outputs x_i .
- Evaluate T with the smallest number of queries.

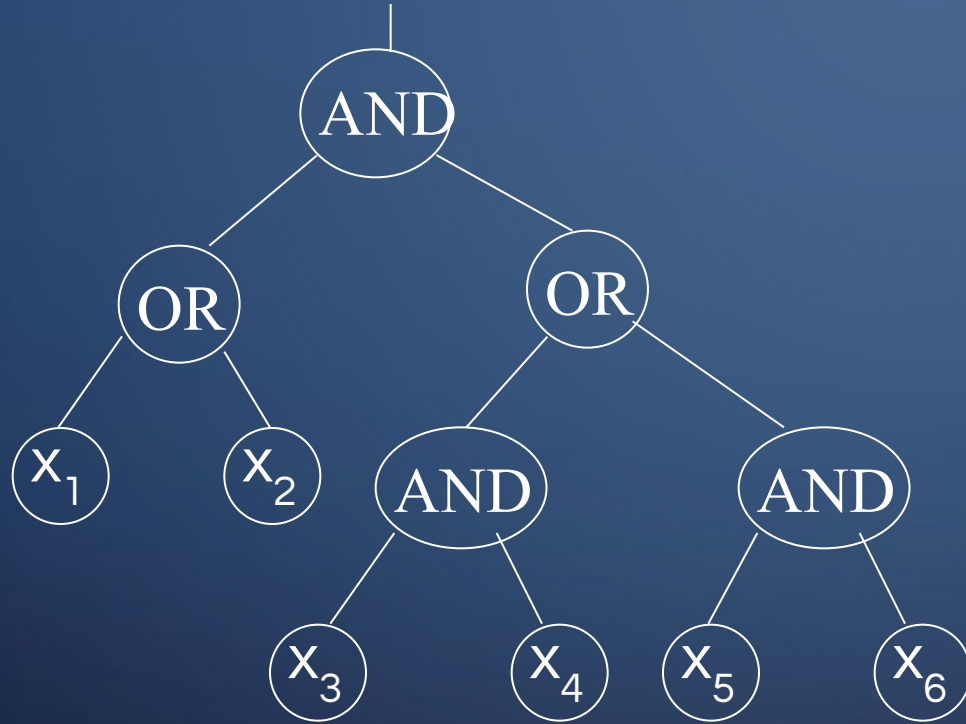
SEARCH AS FORMULA EVALUATION

- Is there $i: x_i = 1$?



Quantum algorithm with $O(\sqrt{N})$ queries.

LOGIC FORMULAS

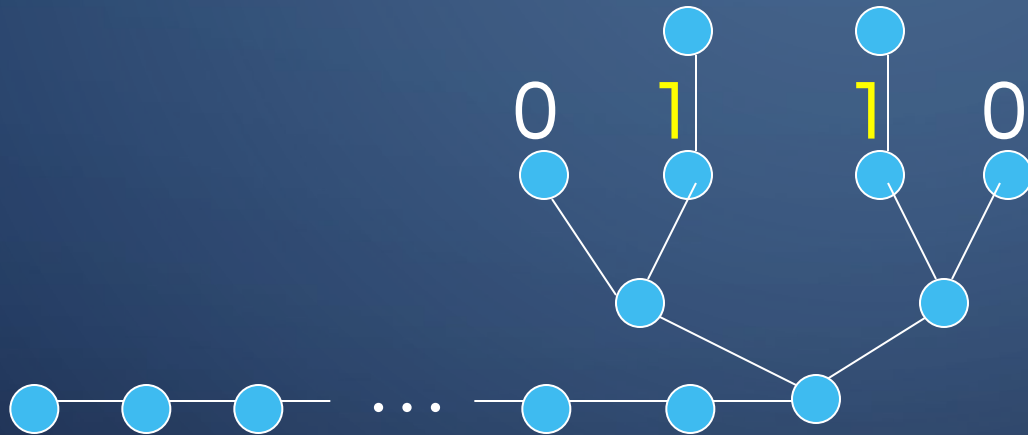


■ Formula size: N .

■ Quantum: $\Theta(\sqrt{N})$
queries.

*[Farhi, Gutman, Goldstone, 2007,
A, Childs, Špalek, Reichardt, Zhang, 2007, Reichardt, 2010]*

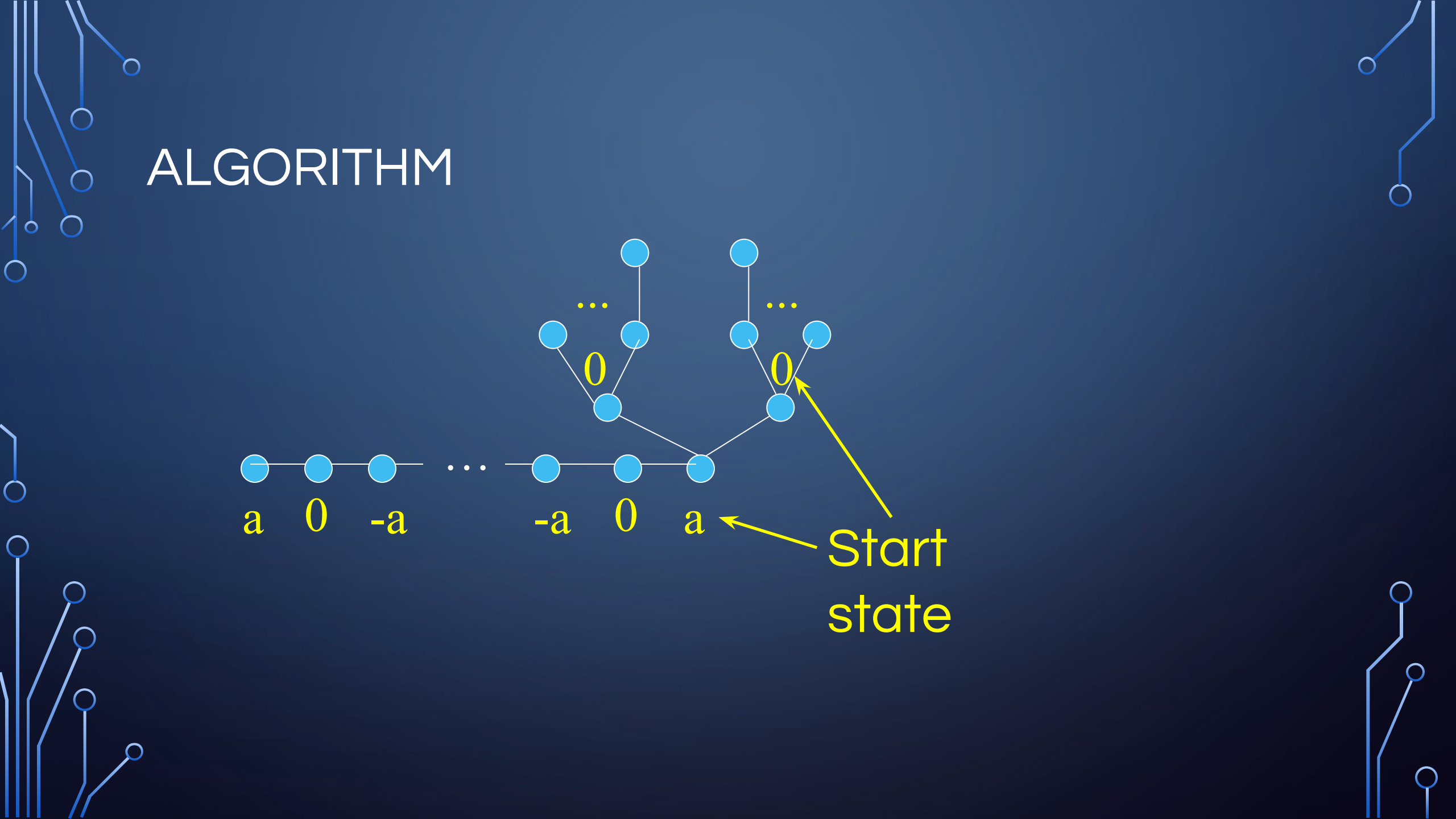
FORMULA TREE



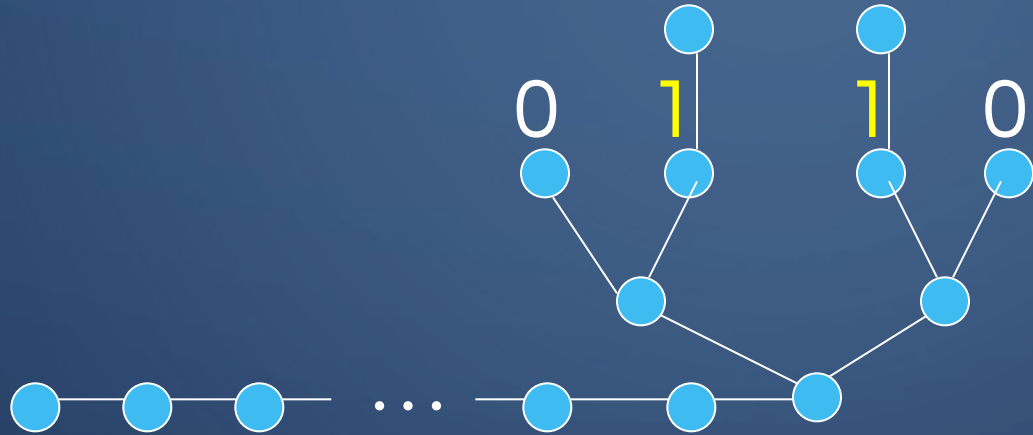
Finite
"tail"

ALGORITHM

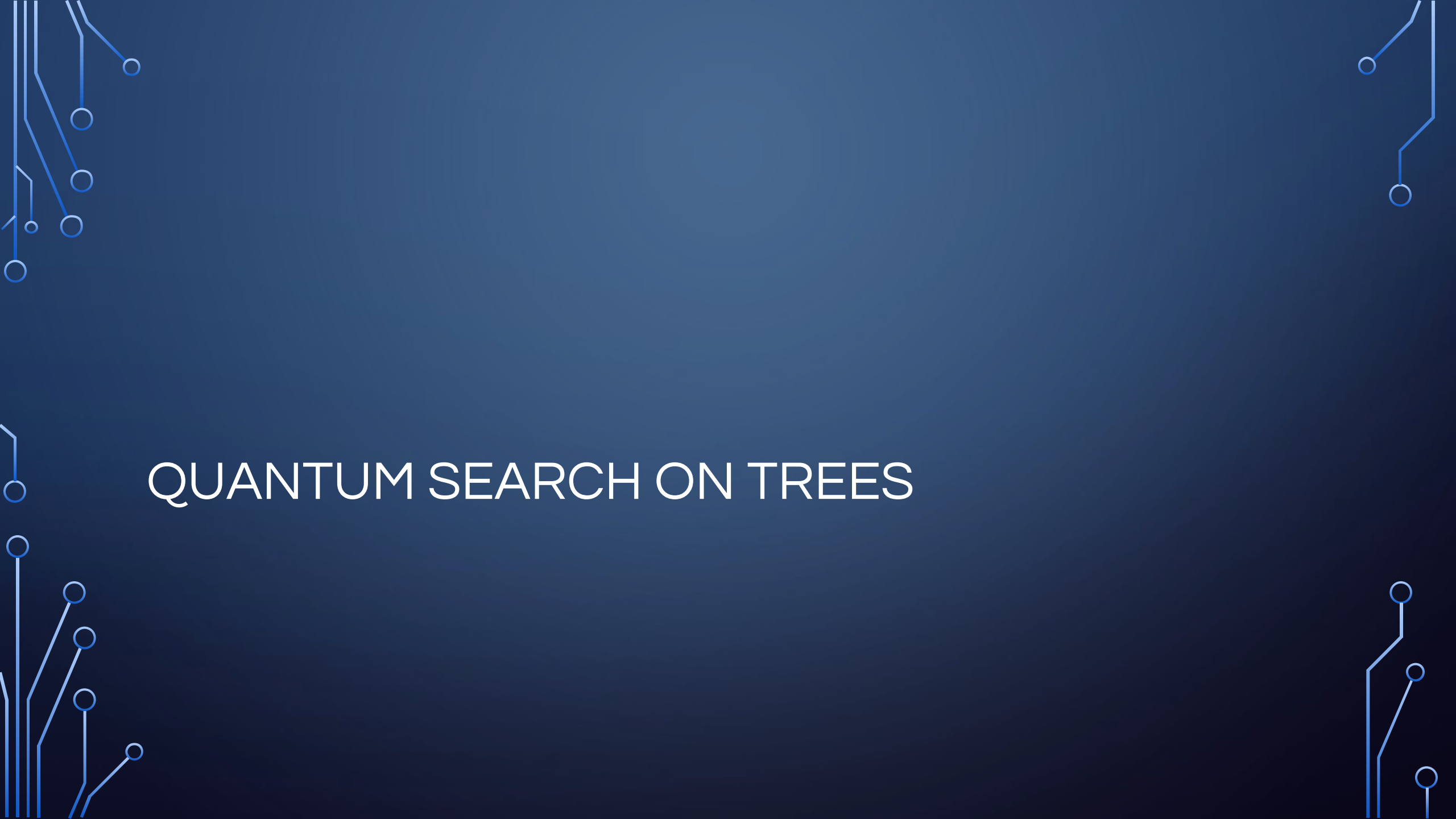
The diagram illustrates a quantum circuit for a 1D Ising model. It shows a chain of qubits with horizontal and vertical connections. The bottom row of qubits is labeled a , 0 , $-a$, followed by an ellipsis, then $-a$, 0 , a . The top row of qubits has two 0 labels. A yellow arrow points to the a qubit in the bottom row, labeled "Start state".



WHAT HAPPENS?

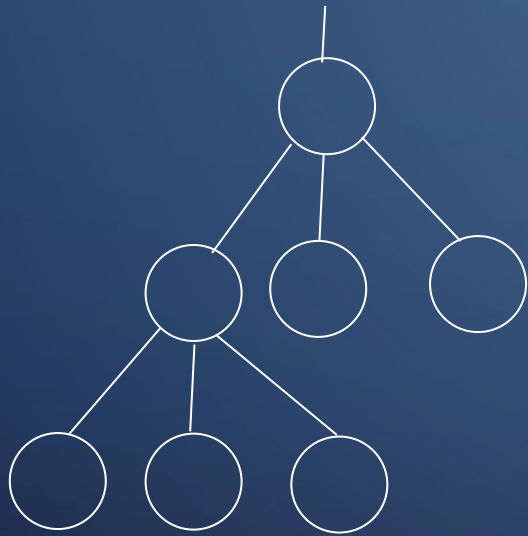


- If $F=0$, state is (almost) unchanged.
- If $F=1$, state «scatters» into the tree.

The background is a dark blue gradient. In the corners, there are decorative elements resembling circuit board traces or tree branches, composed of thin white lines and small white circles.

QUANTUM SEARCH ON TREES

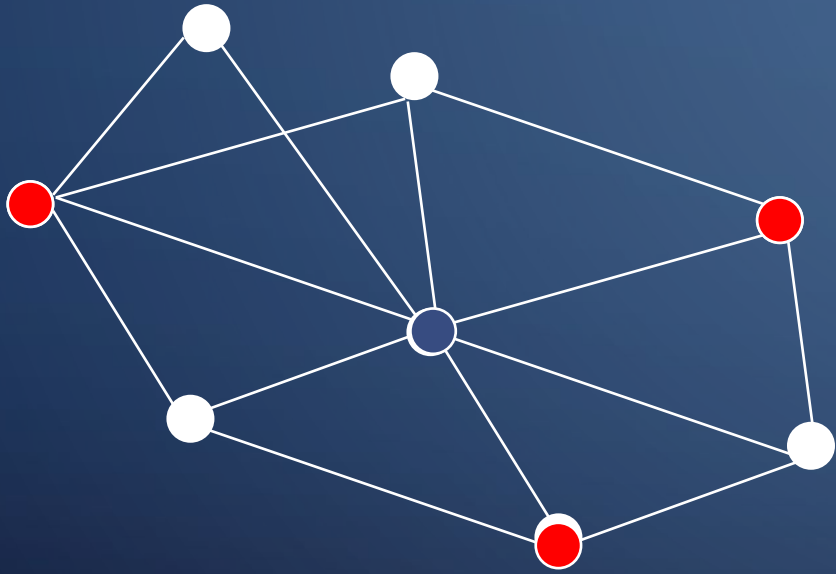
BACKTRACKING



- Start with a partial solution, try to expand it.
- Applications: SAT solvers, optimization, etc.

More difficult than simple exhaustive search.

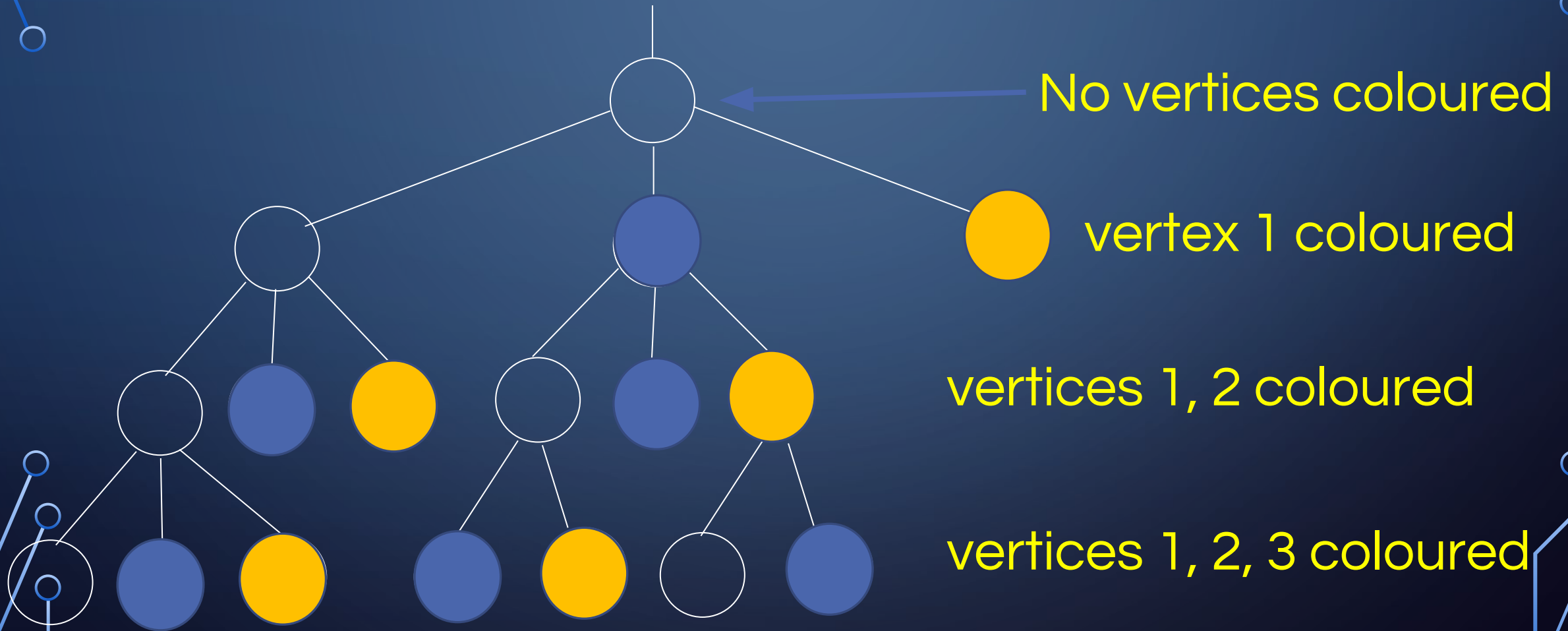
EXAMPLE



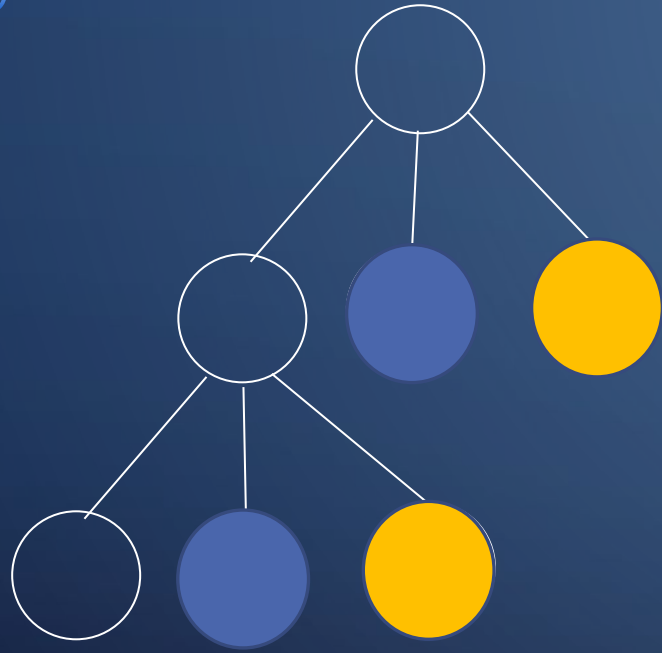
- 3-COLORING: Can we colour vertices with 3 colours so that no edge is monochromatic?
- NP-complete.

Algorithm: attempt to colour vertices one by one.

TREE OF PARTIAL COLORINGS

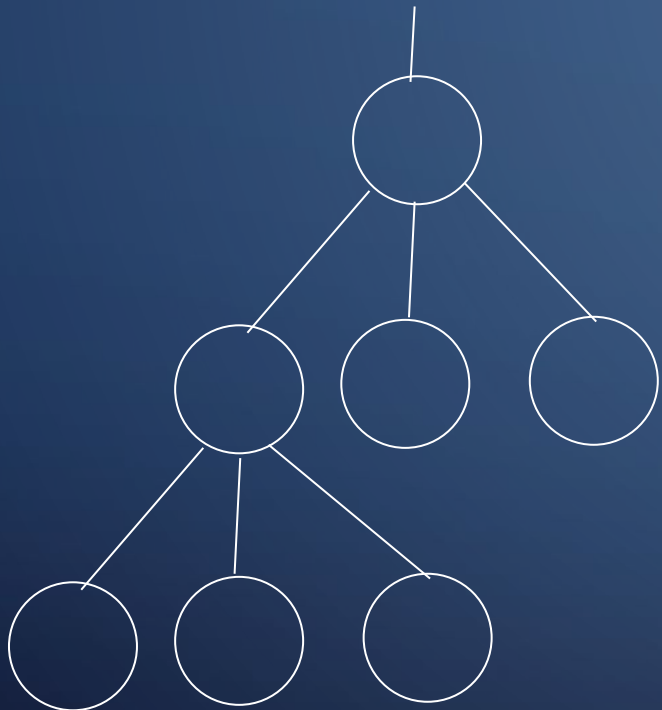


STANDARD QUANTUM SEARCH?



- Grover requires:
 - being able to enumerate search space;
 - being able to find i^{th} candidate solution.
- Because of irregular structure:
 - Some vertices have more children;

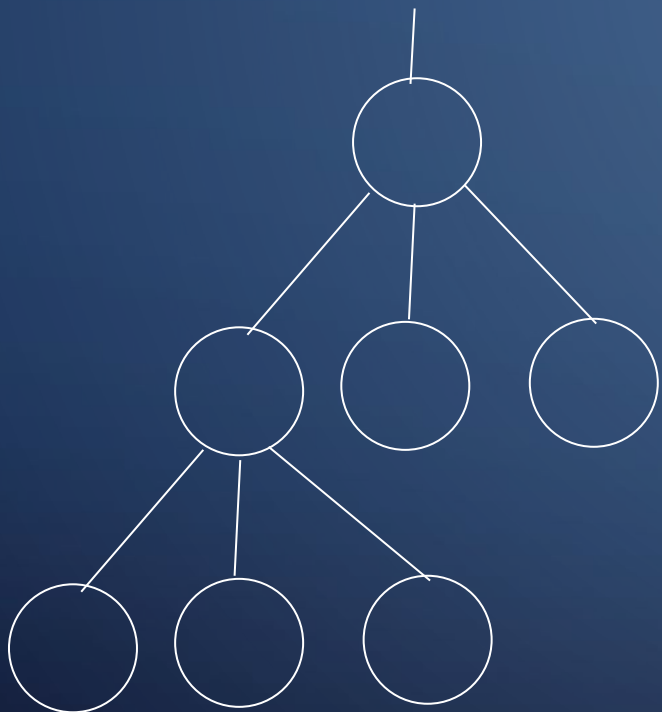
QUANTUM ALGORITHM



- Quantum algorithm for searching a tree in time $O(\sqrt{Tn})$,
 - T – size of the tree;
 - n – depth of the tree.
- Almost quadratic advantage.

[Montanaro, 2015, A, Kokainis, 2017]

SHORT TERM EXPERIMENT?

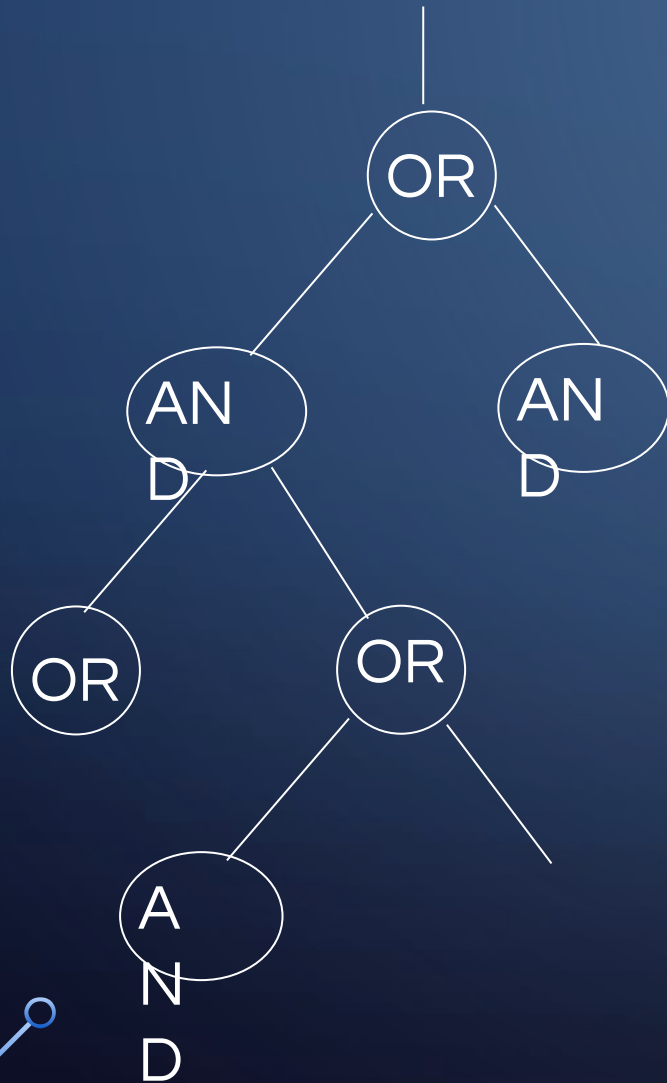


- Small memory requirements:
 - Basis states = vertices;
 - N vertex tree = $\log N$ qubits.

SEARCHING GAME TREES



POSITION TREE



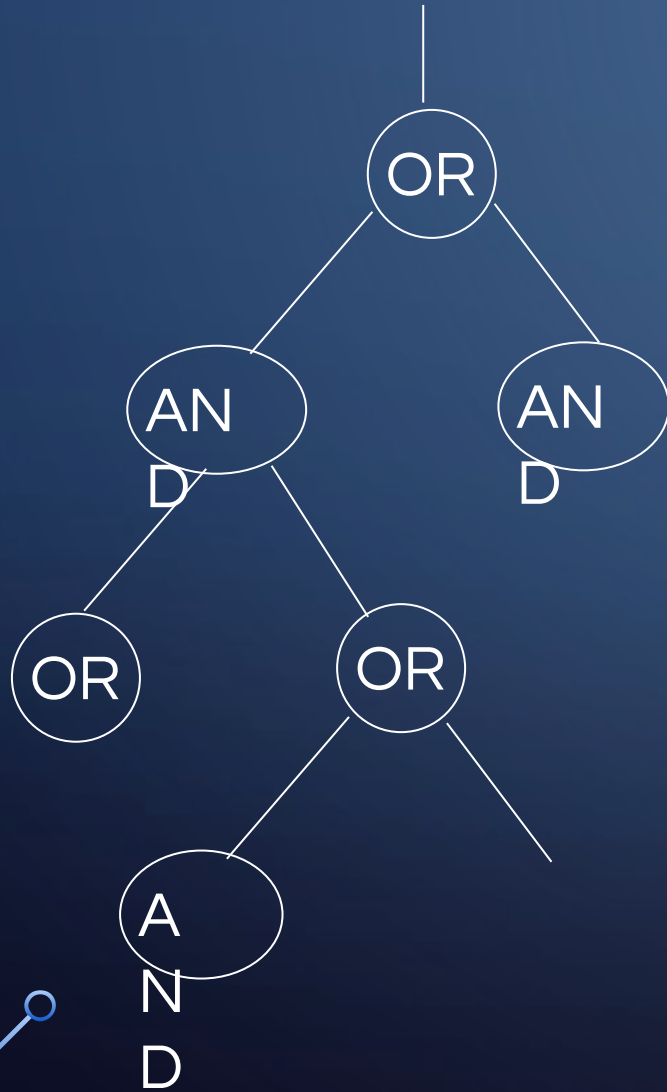
1st player

2nd player

Unknown, irregular structure

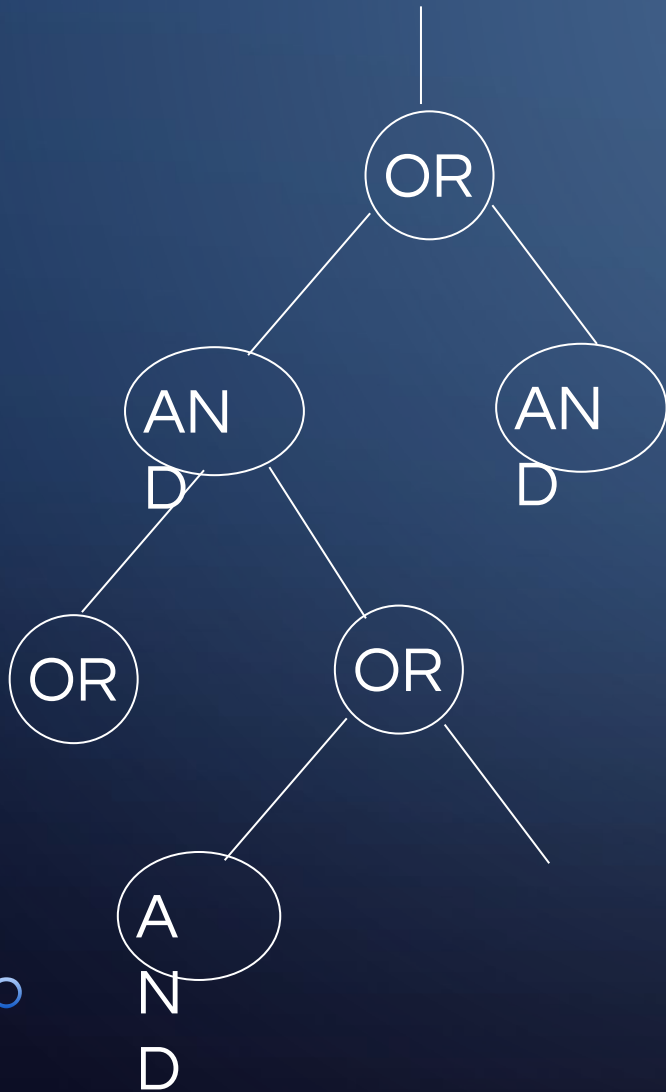
- Position tree = formula;
- Output = YES if 1st player wins;

POSITION TREE



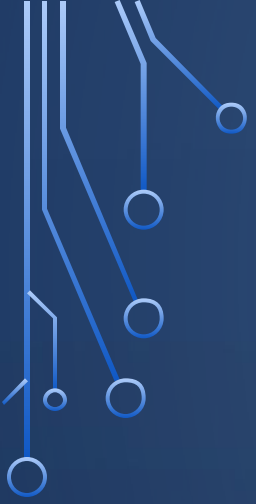
- AND/OR formula of size T can be evaluated by quantum algorithm in $O(\sqrt{T})$ steps [Reichardt, 2010].
- Model: structure of formula known, inputs unknown.

A, KOKAINIS, 2017



- AND-OR formula of unknown structure.

Theorem Formulas of size N and depth $N^{o(1)}$ can be evaluated in time $O(N^{1/2+o(1)})$.

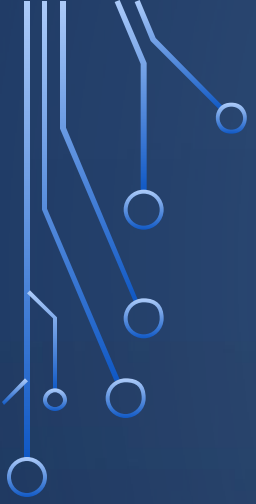


SUMMARY (1)

- Quantum computers may be useful for
 - Simulating physics;
 - Factoring/codebreaking;
 - Search;
- 
- 
- 

SUMMARY (2)

- Quantum advantage over many classical algorithms:
 - Simple exhaustive search;
 - Search by a random walk;
 - Nested search (formula evaluation);
 - Search on trees of unknown structure (backtracking).
- Usually, quadratic advantage but in very general settings.



CHALLENGES FOR FUTURE RESEARCH

- Speeding up dynamic programming?
 - Quantum machine learning?
 - Algorithms for first quantum computers (100 qubits, quite noisy)?
- 
- 