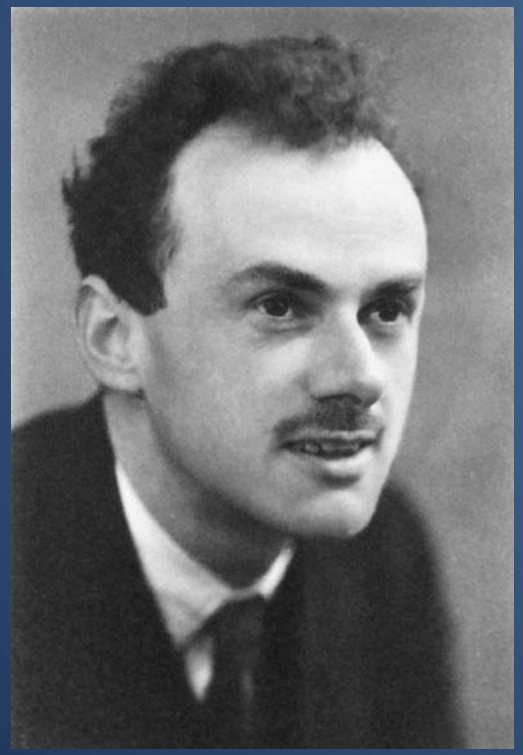
QUANTUM ALGORITHMS FOR SEARCH AND OPTIMIZATION

ANDRIS AMBAINIS

UNIVERSITY OF LATVIA

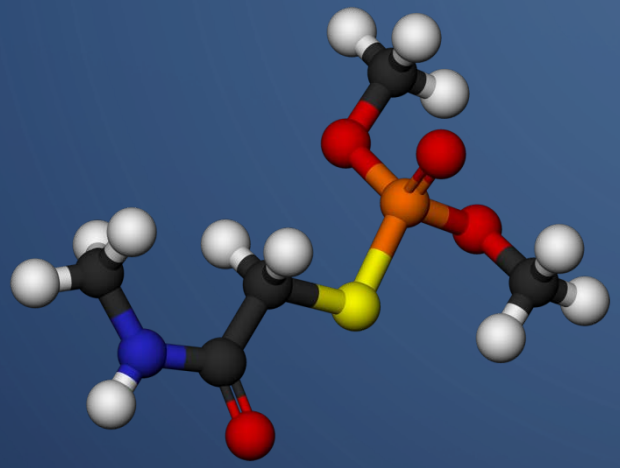
WHAT CAN WE DO WITH A QUANTUM COMPUTER?



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



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

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

A substantial application for HPC

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

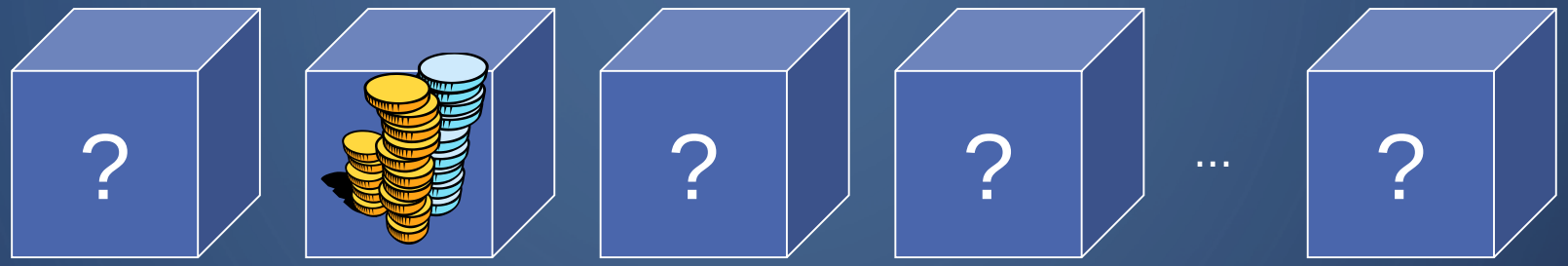
- RSA and other cryptosystems based on factoring/discrete log broken by quantum computers.
- Quantum algorithms for other crypto-related problems:
  - Pell's equation [Hallgren, 2002],
  - ideal class group [Biasse, Song, 2016],
  - principal ideal problem [Hallgren, 2002, Biasse, Song, 2016].

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 Post Quantum Crypto Standardization project (2nd stage now, 26 candidates).

SEARCH

QUANTUM SEARCH



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

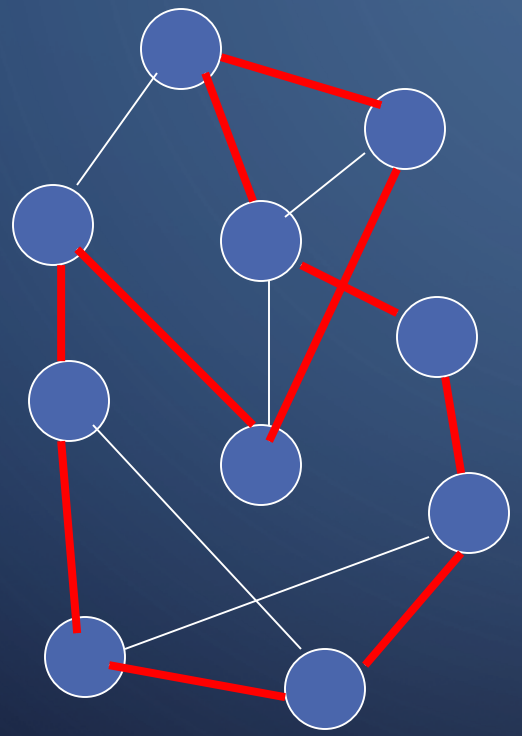
Grover, 1996: $O(\sqrt{N})$ quantum steps.

Who has the number 67033706?

Usual computer: N = 1,000,000 steps

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

APPLICATION: TRAVELING SALESMAN PROBLEM



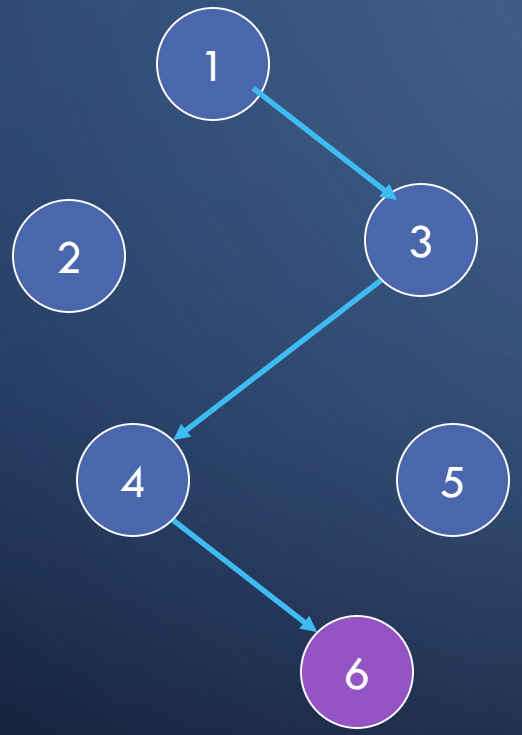
Find the best route through all the cities.

Quantum algorithm:

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

QUANTUM SPEEDUP FOR SMART SEARCH?

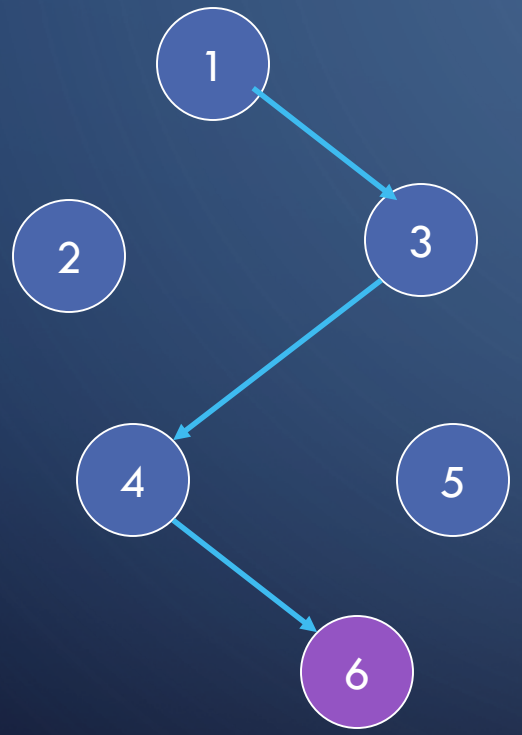
QUANTUM WALK SEARCH [SZEGEDY, 04]



- 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

Theorem Assume that a marked state is reached in expected time at most T.

A quantum algorithm can find a marked state in time $\tilde{O}(\sqrt{T})$.

Quadratic speedup for a variety of problems.

[Szegedy, 2004, A, Gilyen, Jeffery, Kokainis, 2018]

MAIN RESULT

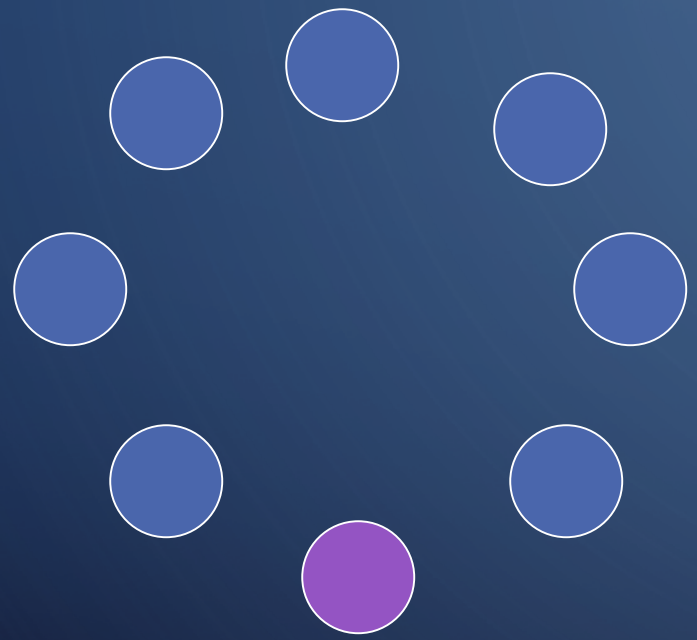
Theorem Assume that a marked state is reached in expected time at most T.

A quantum algorithm can find a marked state in time $\tilde{O}(\sqrt{T})$.

Quadratic speedup for a variety of problems.

[Szegedy, 2004, A, Gilyen, Jeffery, Kokainis, 2018]

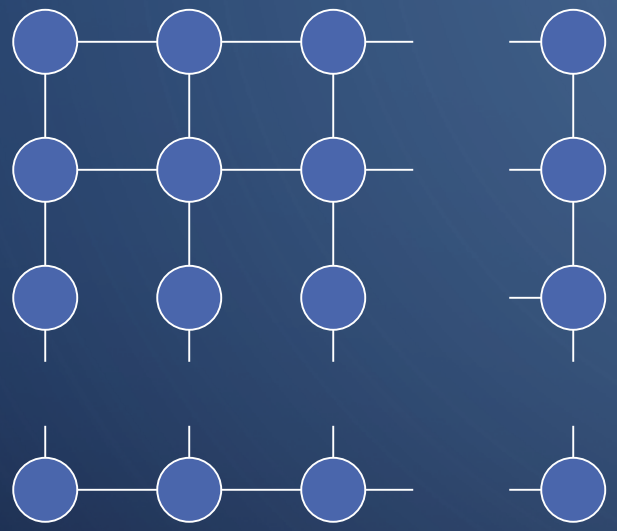
APPLICATION 1



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

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

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: $O\left(\sqrt{N \log N}\right)$

[A, Kempe, Rivosh, 2005]

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

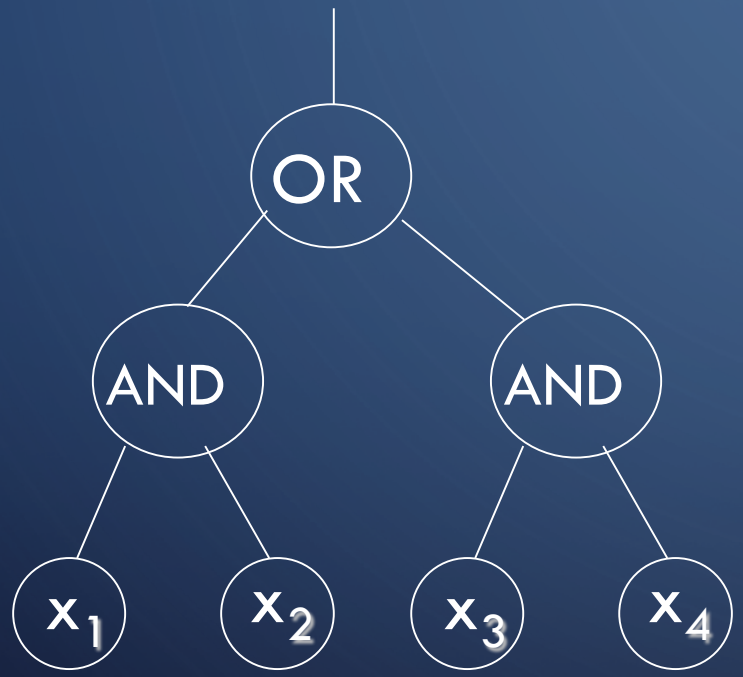
- Are there 2 equal numbers?

- Usual algorithms: N steps.
- Quantum algorithms: $O(N^{2/3})$.

[A, 2004]

QUANTUM ALGORITHMS FOR LOGIC FORMULAS

EVALUATING AND-OR TREES

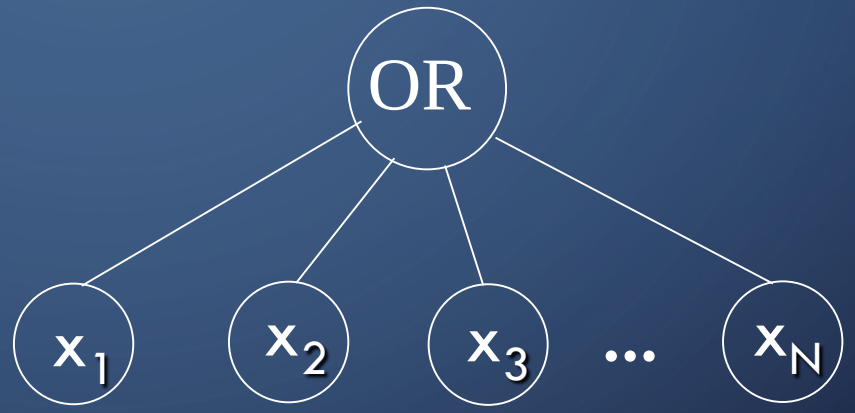


- Variables x_i accessed by queries to a black box:
  - Input i;
  - Black box outputs x_i.

- Evaluate T with the smallest number of queries.

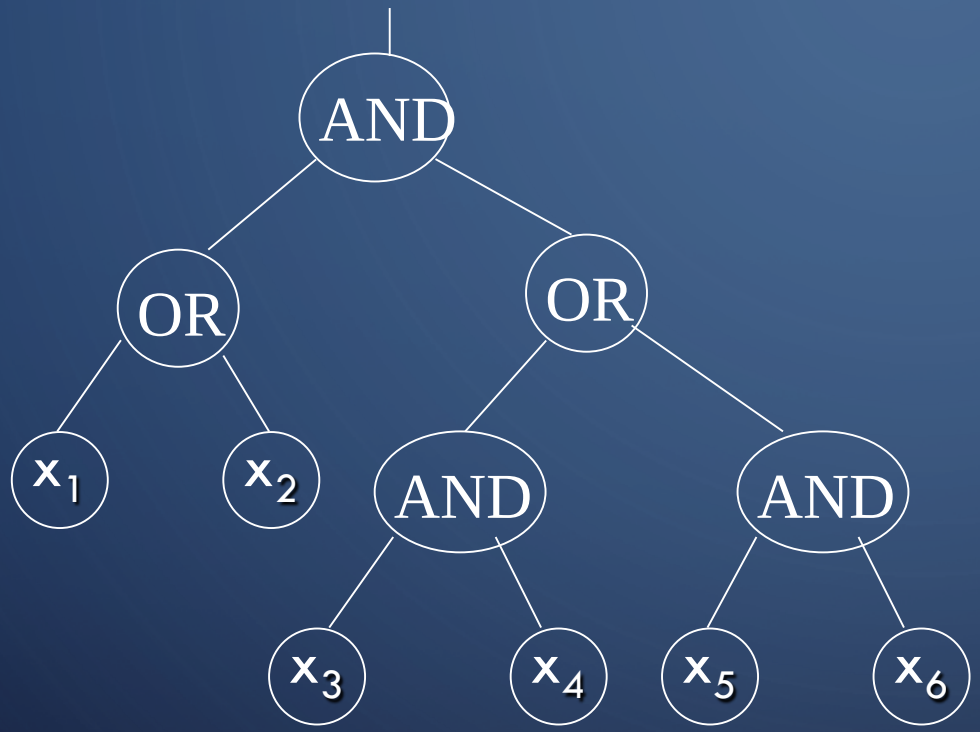
SEARCH AS FORMULA EVALUATION

Is there i: $x_i=1$?



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

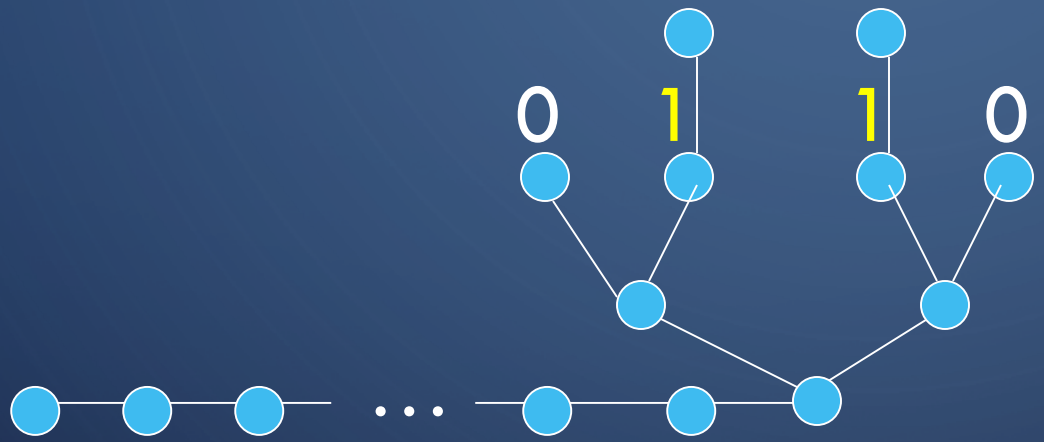
LOGIC FORMULAS



- Formula size: N.
- Quantum: $\Theta(\sqrt{N})$ queries.

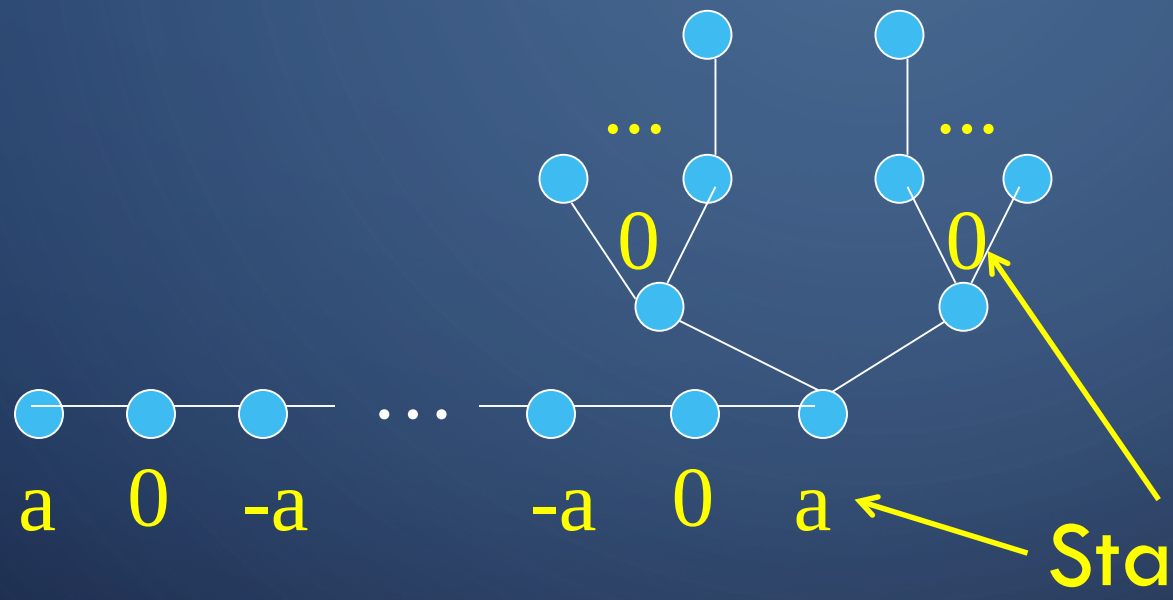
[Farhi, Gutman, Goldstone, 2007,
A, Childs, Špalek, Reichardt, Zhang, 2007, Reichardt, 2010]

FORMULA TREE

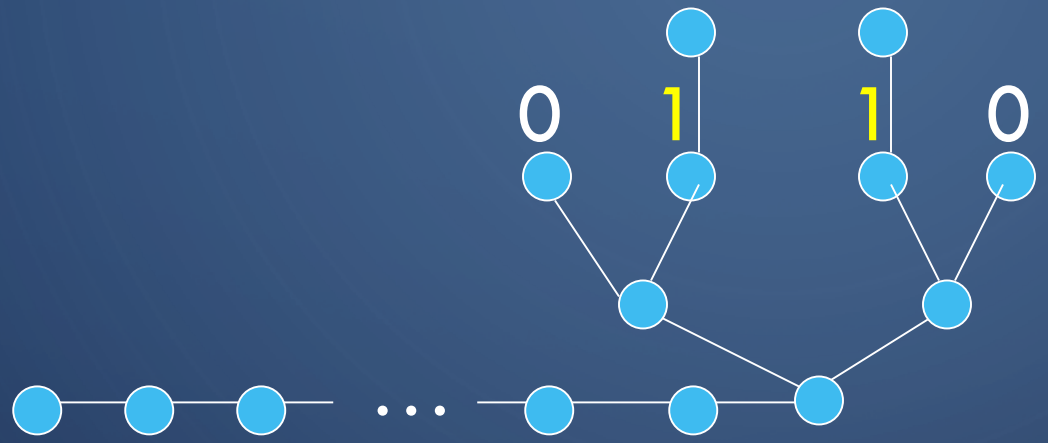


Finite “tail”

ALGORITHM



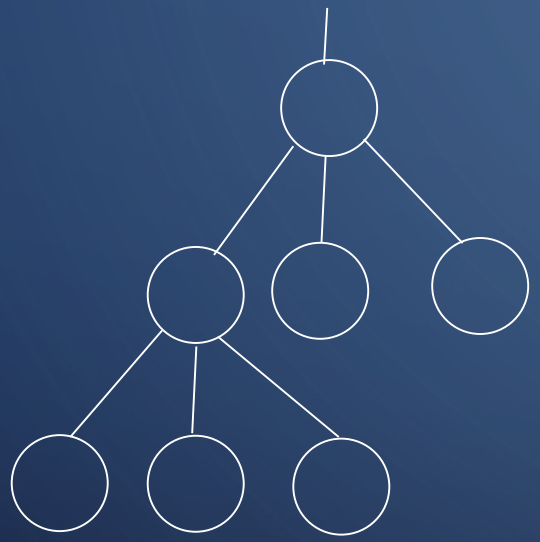
WHAT HAPPENS?



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

QUANTUM SEARCH ON TREES

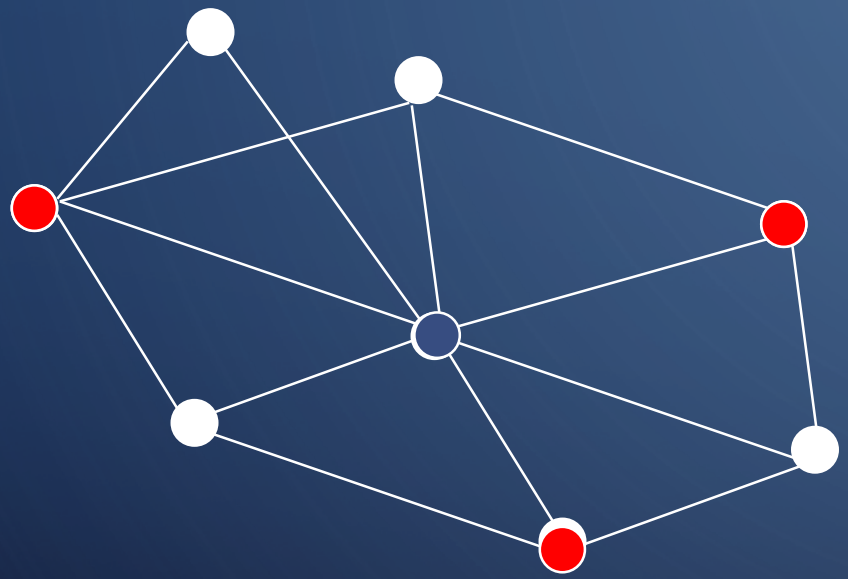
BACKTRACKING



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

More difficult than simple exhaustive search.

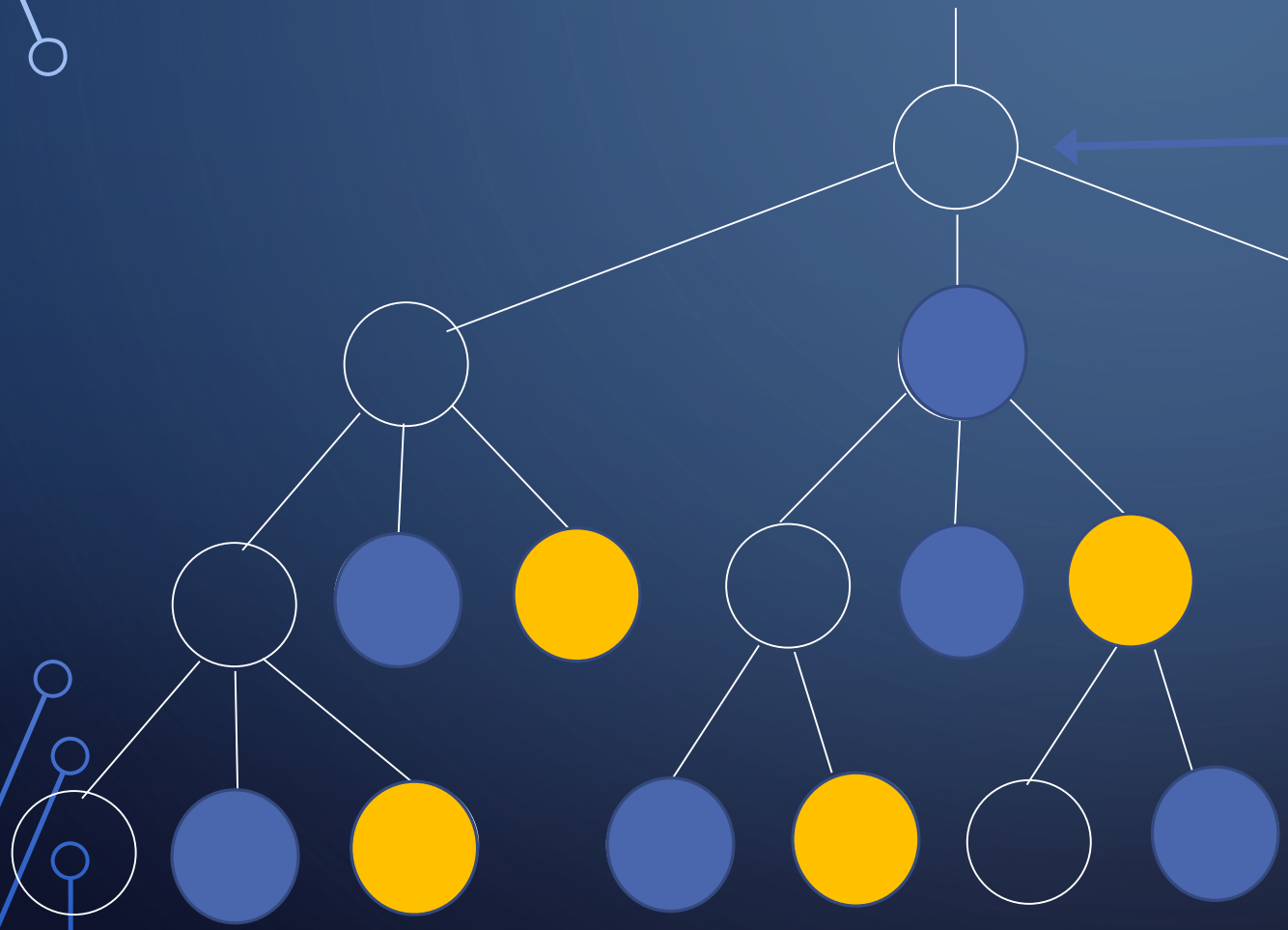
EXAMPLE



- 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



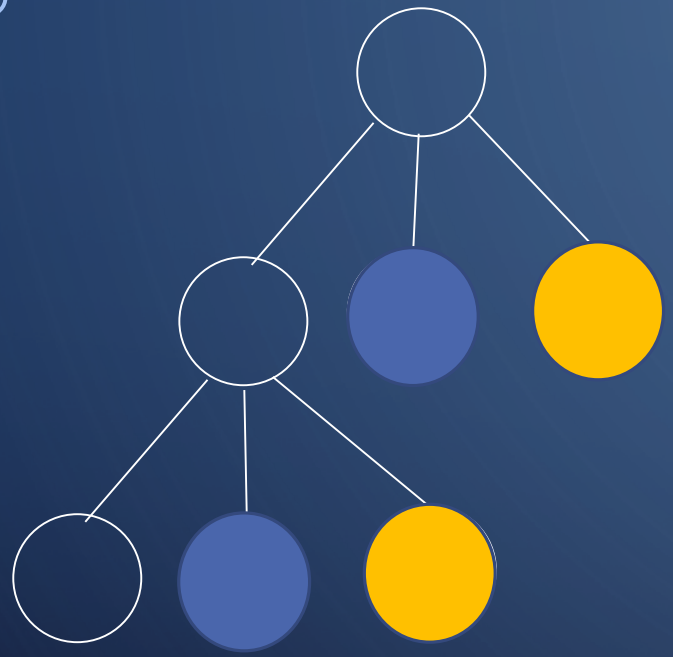
No vertices coloured

vertex 1 coloured

vertices 1, 2 coloured

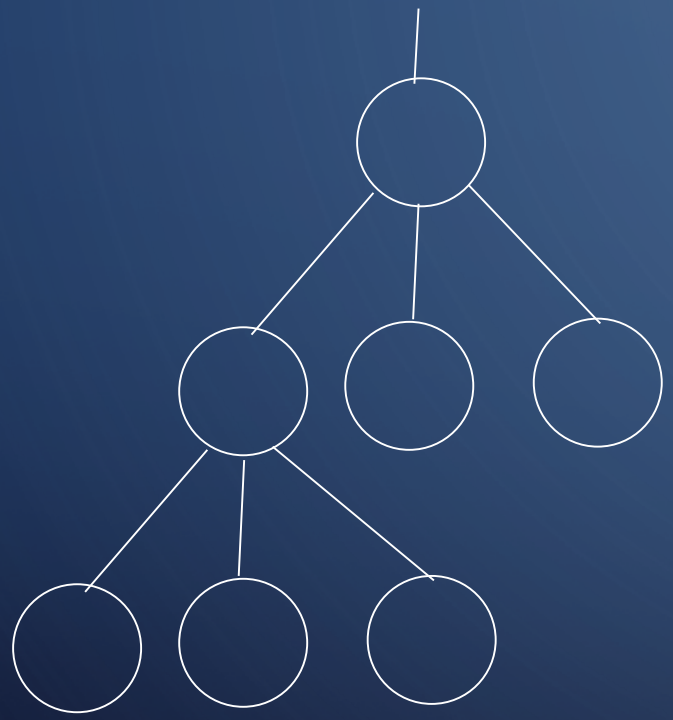
vertices 1, 2, 3 coloured

STANDARD QUANTUM SEARCH?



- Grover requires:
  - being able to index search space;
- Irregular structure:
  - Some vertices have more children;
  - Some branches stop early.

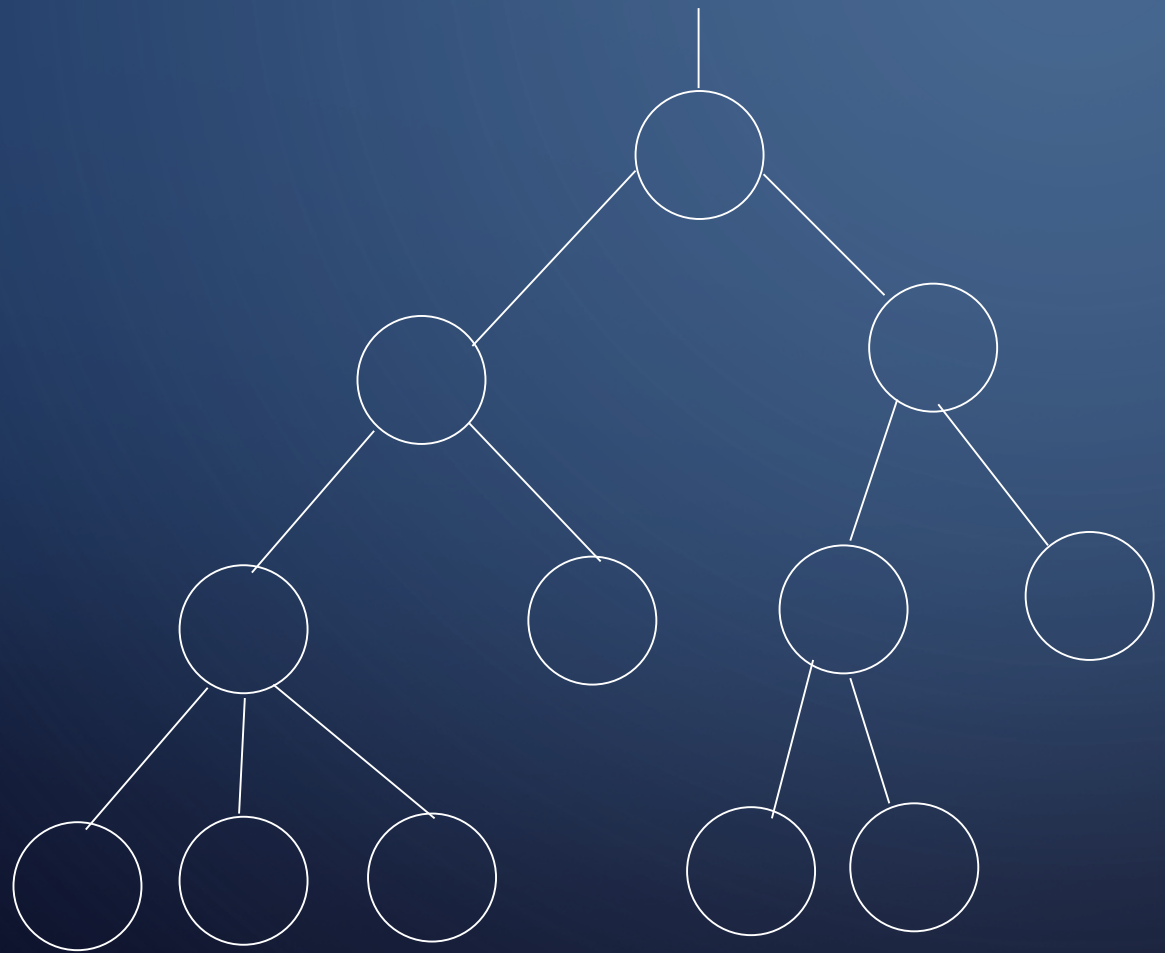
QUANTUM ALGORITHM



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

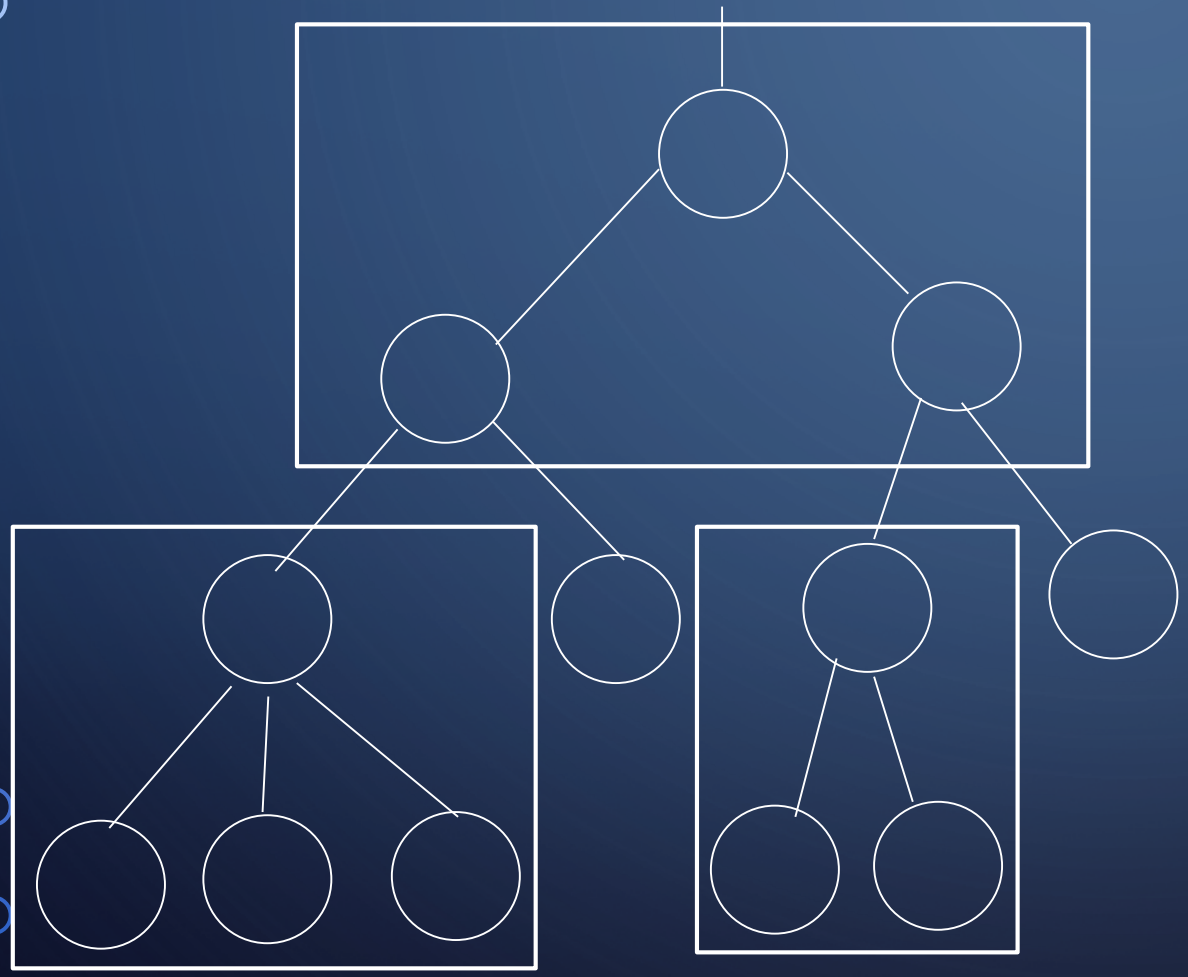
[Montanaro, 2015, A, Kokainis, 2017]

QUANTUM WALK (MONTANARO, 2015)



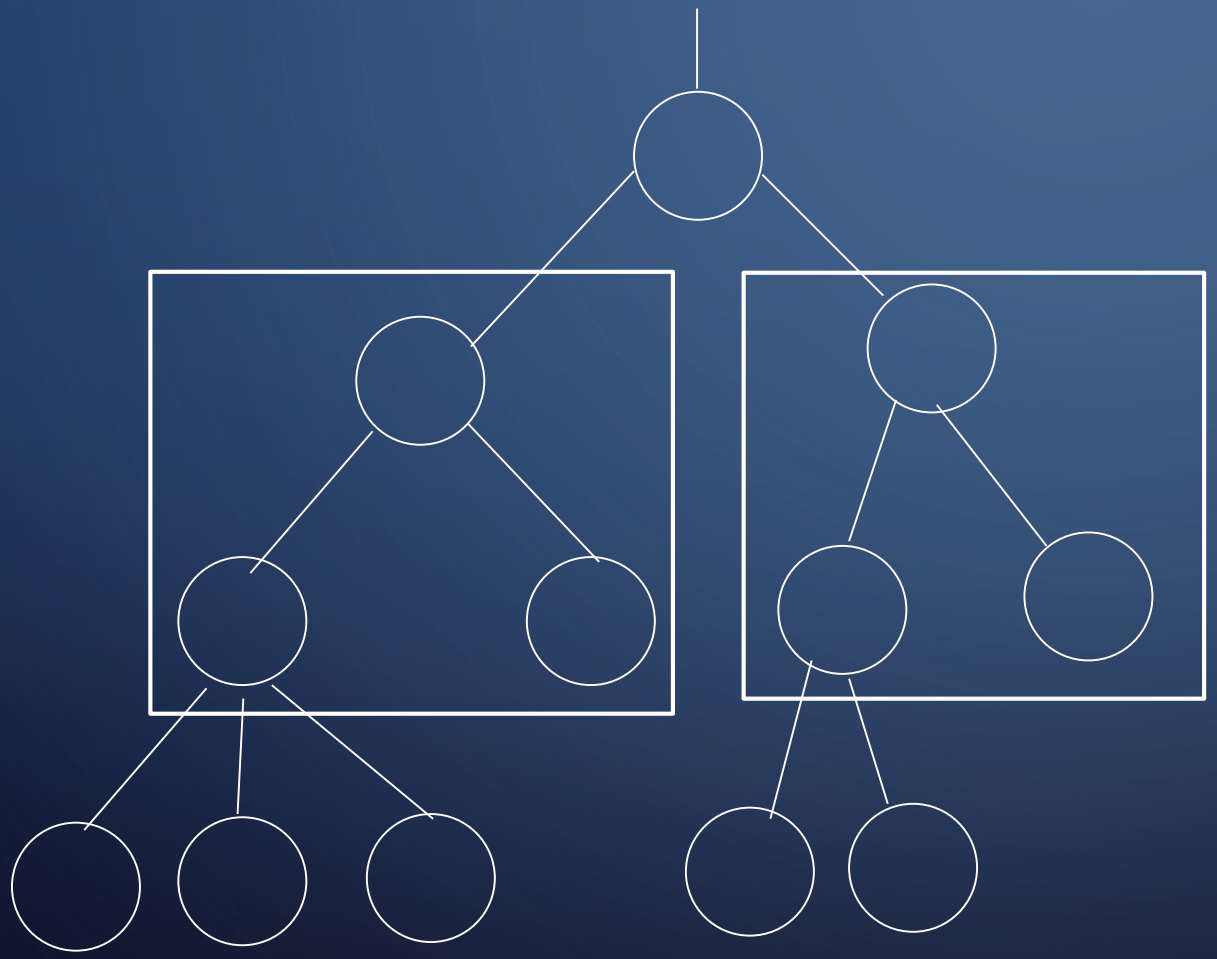
- Basis states: $|u\rangle$.
- Different transformations at odd, even steps.

ODD STEPS



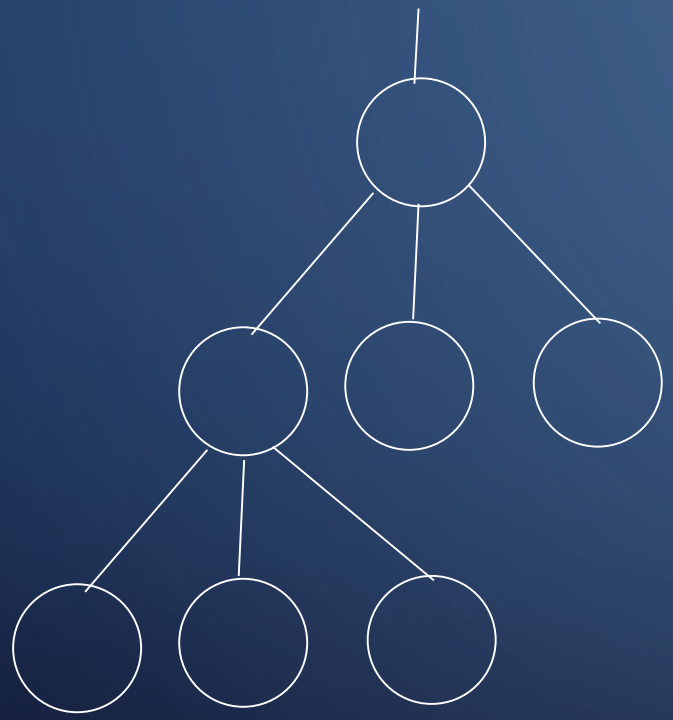
- S_v : odd-level vertex v with all its children.
- Transformation C_v on $|u\rangle$, $u \in S_v$.
- If v – leaf, C_v depends on whether v marked.

EVEN STEPS



- S_v : even-level vertex v with all its children.
- Transformation C_v on $|u\rangle$, $u \in S_v$.
- If v – leaf, C_v depends on whether v marked.

RESULT

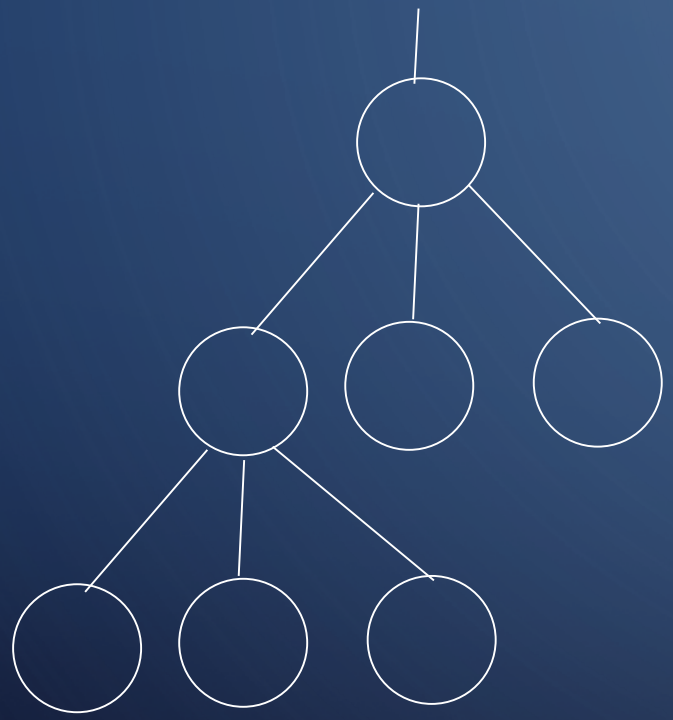


Starting state $|r\rangle$, r – root.

Marked vertex exists

There is a stationary state close to $|r\rangle$

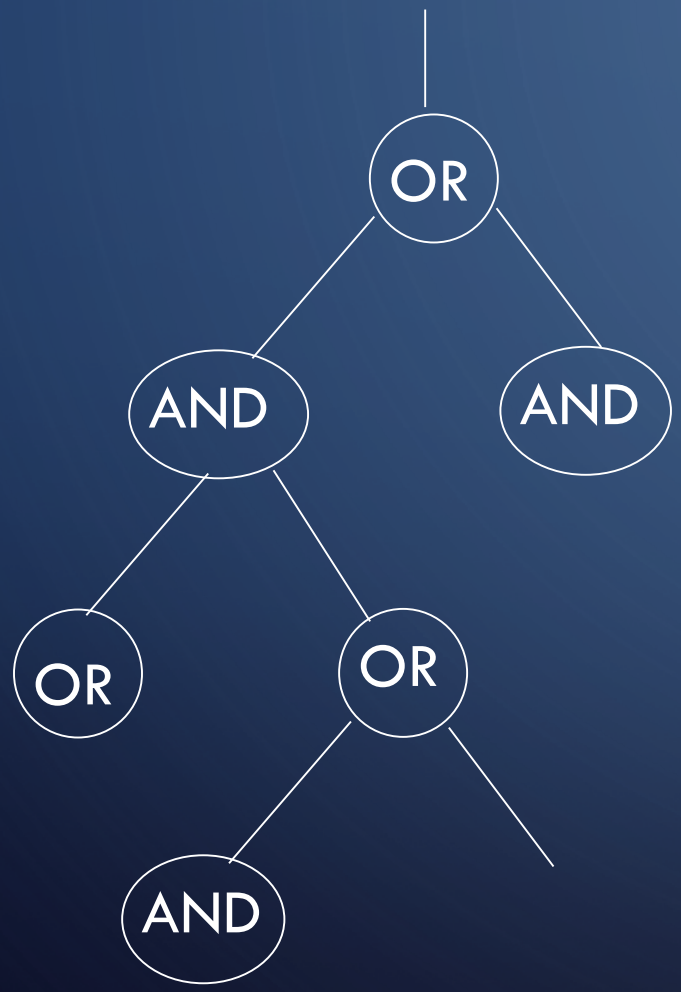
SHORT TERM EXPERIMENT?



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

SEARCHING GAME TREES

POSITION TREE



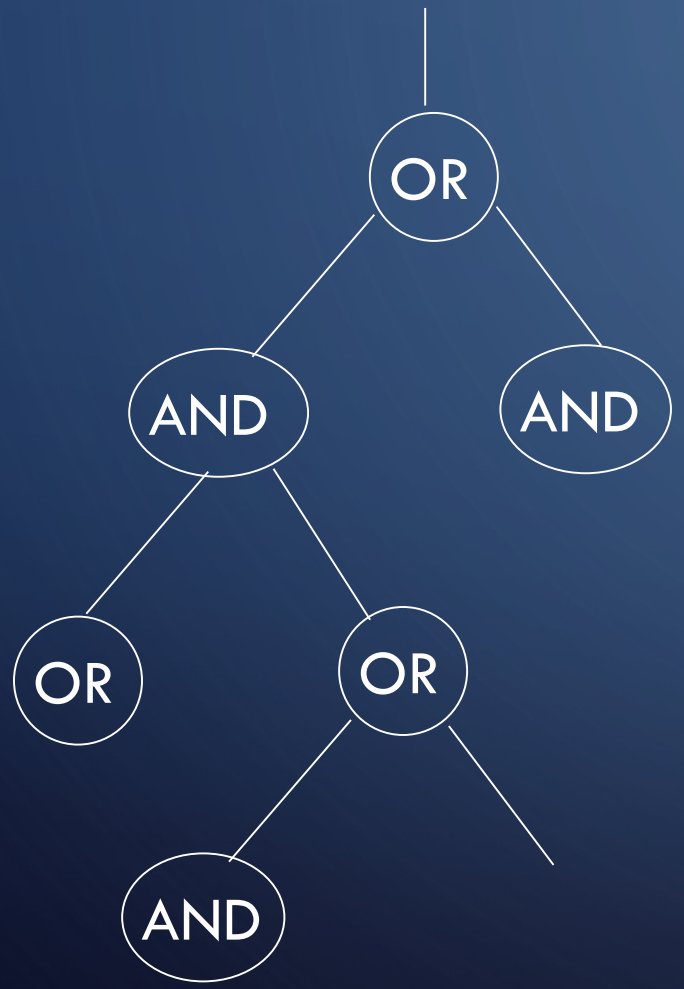
1st player

2nd player

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

Unknown, irregular structure

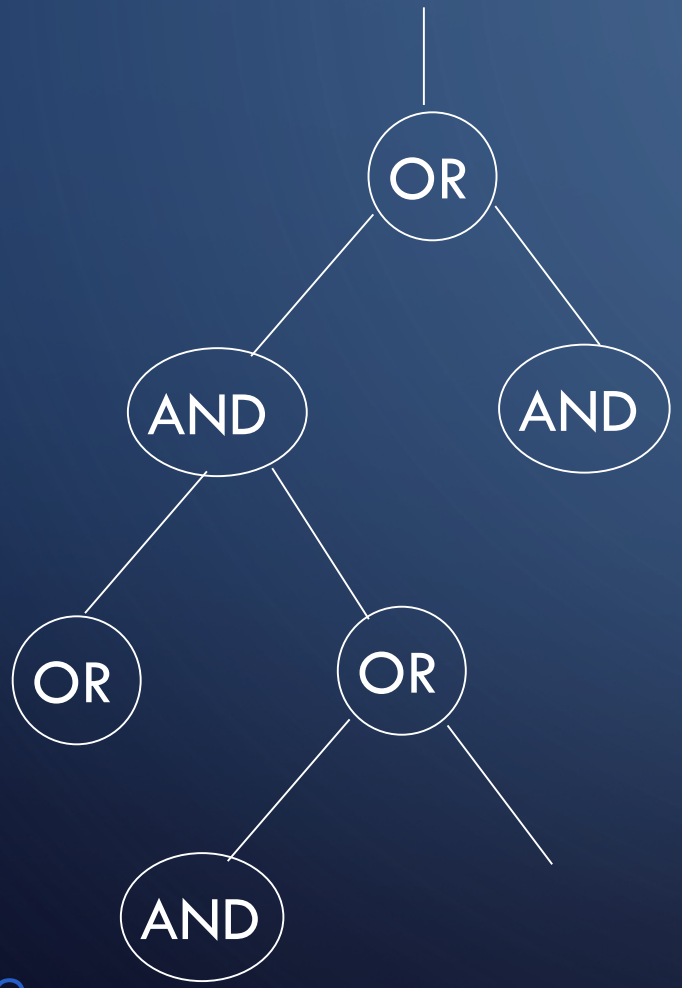
POSITION TREE



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

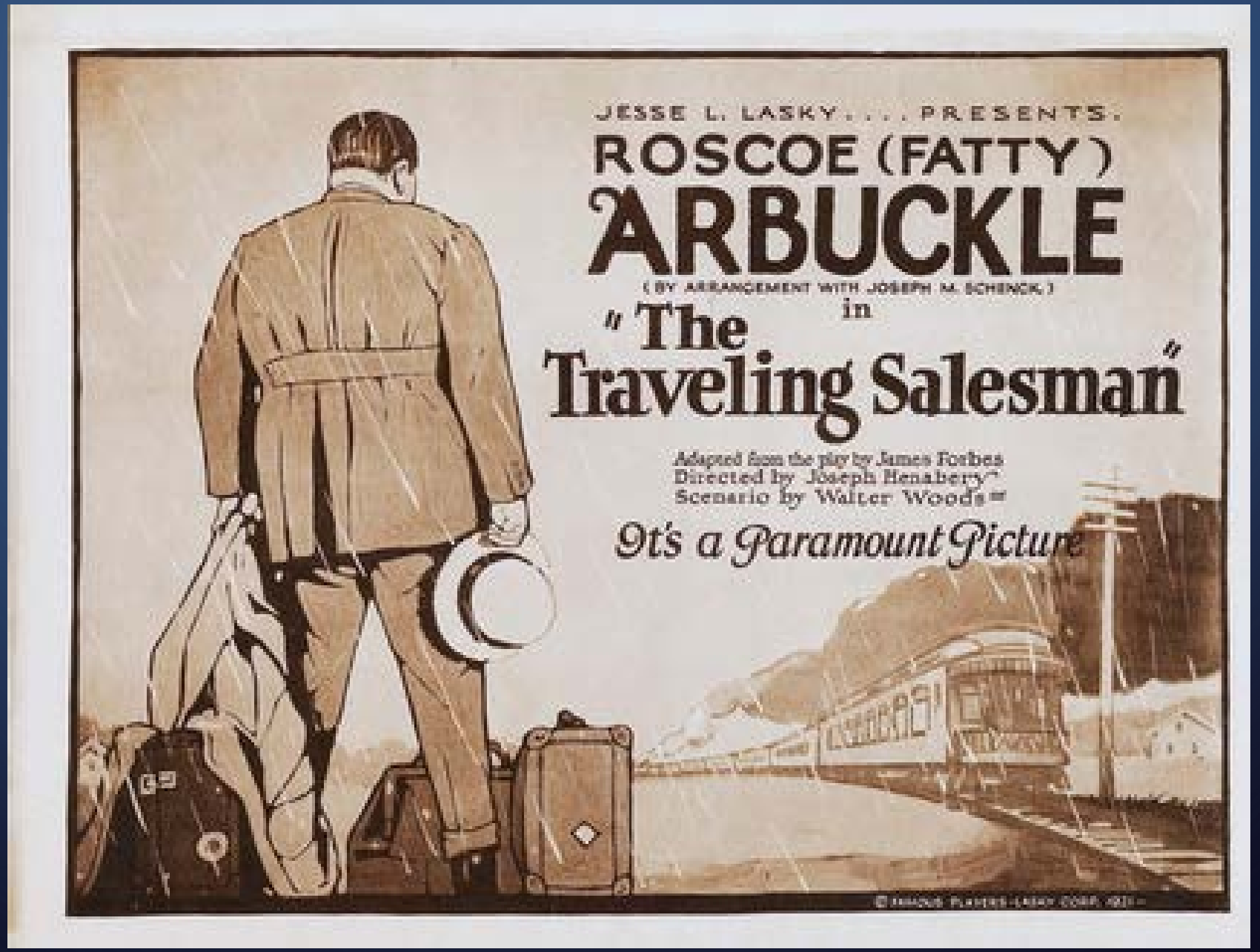
- Model: structure of formula known, inputs unknown.

A, KOKAINIS, 2017

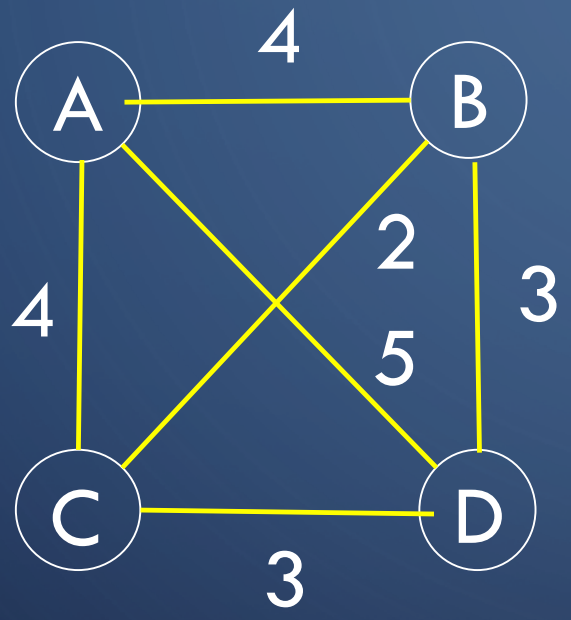


- AND-OR formula of unknown structure.

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


JESSE L. LASKY. . . . PRESENTS.
ROSCOE (FATTY)
ARBUCKLE
(BY ARRANGEMENT WITH JOSEPH M. SCHENCK)
in
"The Traveling Salesman"
Adapted from the play by James Forbes
Directed by Joseph Henabery
Scenario by Walter Woods
It's a Paramount Picture

TRAVELLING SALESMAN PROBLEM



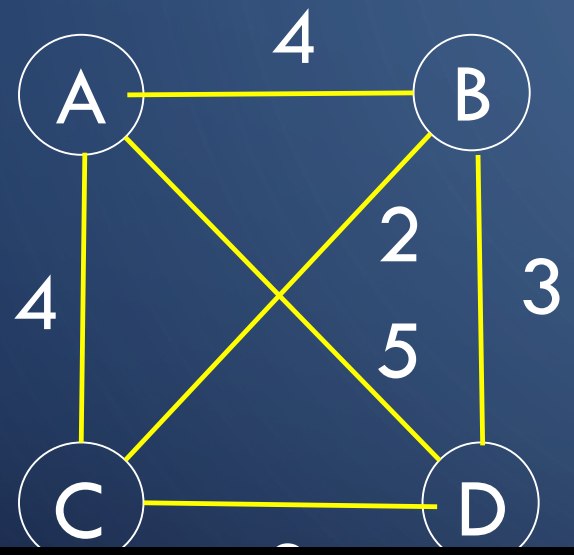
N cities, find the best route visiting all cities;

N! candidate routes;

Classically, $O(2^N)$ time!

Quantum search: $O(\sqrt{N!})$

BEST CLASSICAL ALGORITHM

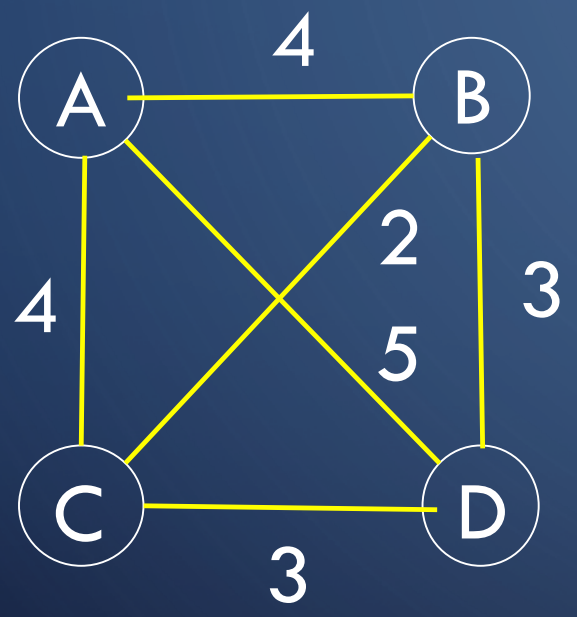


- Find the shortest route through every subset of cities S.
- Order: from smaller S to larger S.

Combine with quantum search!

- Time $\approx 2^N$.

QUANTUM ALGORITHM



- Find the shortest routes through small sets of cities S classically.
- Quantum search to find the best way to combine these routes.

CLASSICAL PART

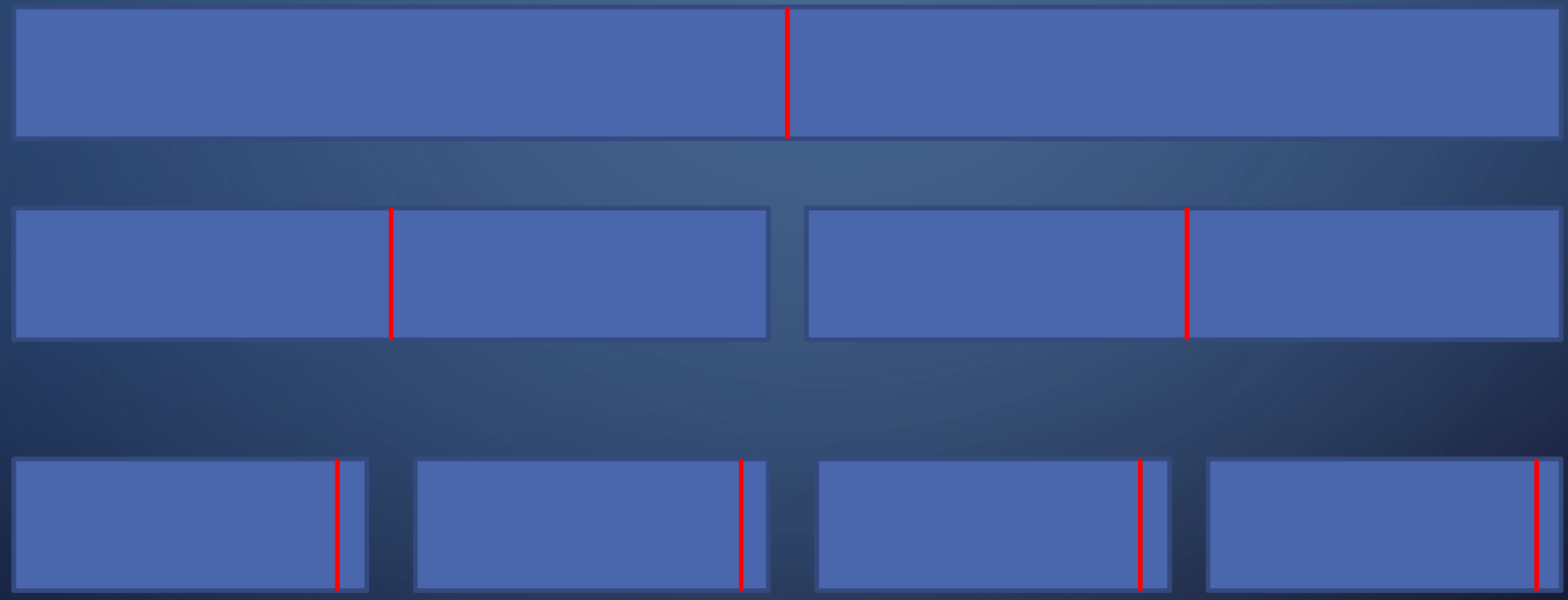
- Find the shortest route through every S, $|S| \leq \alpha N$.
- Time:

$$\binom{N}{0} + \binom{N}{1} + \ldots + \binom{N}{\alpha N} = O\left(2^{H(\alpha)N}\right)$$

- For α=0.24...,

$$O(1.73\ldots^{N})$$

DIVIDE AND CONQUER



DIVIDE AND CONQUER

- Classical search for the best split:

$$O\left(\binom{N}{N/2}\binom{N/2}{N/4}\binom{N/4}{0.24\,N}\right).$$

- Quantum search:

$$O\left(\sqrt{\binom{N}{N/2}\binom{N/2}{N/4}\binom{N/4}{0.24\,N}}\right) = O(1.73\ldots^{N}).$$

OPEN PROBLEM

- Quantum algorithm with small memory?
- Ideally, $O(N^c)$, N – number of cities.

SUMMARY

- 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 general search strategies?
- Quantum machine learning?
- Algorithms for first quantum computers (100 qubits, quite noisy)?