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

- Rigetti
- Microsoft
- IONQ
- QCI
QUANTUM SIMULATION
NUMBER OF VARIABLES

- 30 particles – $2^{30} \approx 1,000,000,000$.  
- 100 particles – $2^{100} \approx 1,000 \ldots 000$. 

30 zeros
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.

Paul Dirac, 1929
QUANTUM CHEMISTRY

A substantial application for HPC

\[
H | \Psi \rangle = E | \Psi \rangle
\]

\[
H = \sum_{p,q} t_{pq} c^+_p c_q + \sum_{p,q,r,s} V_{pqrs} c^+_p c^+_q c_r c_s
\]
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.
FACTORYING AND CODE-BREAKING
FACTORYING

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);

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
THE SOURCE OF QUANTUM ADVANTAGE?
QUANTUM SYSTEM

Current state: i with amplitude $\alpha_i$.

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

\[ \begin{align*}
\alpha_1 & \quad 1 \\
\alpha_2 & \quad 2 \\
\alpha_3 & \quad 3 \\
\cdots & \\
\alpha_{1,000,000} & \quad 1,000,000 \\
\end{align*} \]

\[ \begin{align*}
F(1) & \quad \alpha_1 \\
F(2) & \quad \alpha_2 \\
F(3) & \quad \alpha_3 \\
\cdots & \\
F(1,000,000) & \quad \alpha_{1,000,000} \\
\end{align*} \]
WHAT CAN WE DO WITH SUCH STATE?

\[ F(1), F(2), F(3), \ldots, F(1,000,000) \]

\[ \alpha_1, \alpha_2, \alpha_3, \alpha_{1,000,000} \]

Measurement

\[ F(3) \]

Other values are lost!
QUANTUM INTERFERENCE

\[ F(1), F(2), F(3), \ldots, F(1,000,000) \]

\[ \alpha_1, \alpha_2, \alpha_3, \alpha_{1,000,000} \]

Result that depends on all values \( F(1), F(2), \ldots \)

Example: quantum Fourier transform finds periods quickly
QUANTUM COMPUTERS WILL PROVIDE BIG SPEEDUPS FOR **SOME BUT NOT ALL** COMPUTATIONAL TASKS
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

• N states.

• Is there a marked state?

• Random walk: at each step move to a randomly chosen vertex.

• Finds a marked vertex in $\sqrt{N}$ [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: $O\left(\sqrt{N \log N} \right)$

[A, Kempe, Rivosh, 2005]
### Application 3: Element Distinctness

Are there 2 equal numbers?

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

[A, 2004]

| 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 |
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.

Finite "tail"
ALGORITHM

Start state
WHAT HAPPENS?

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

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

More difficult than simple exhaustive search.
• 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 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

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

Unknown, irregular structure
• 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 $O(N^{1/2+o(1)})$. 
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)?