GROVER AND SHOR ALGORITHMS IN NMR

Attila Fülöp

Henning Hammar

Outline

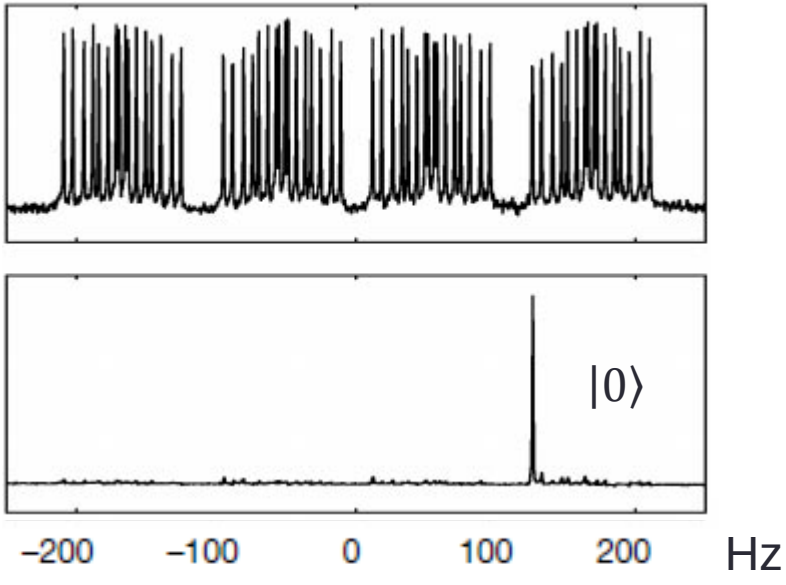
- Introduction
- Nuclear Magnetic Resonance
- Shor
- Grover
- Conclusion

Introduction

- Shor’s algorithm
  - Factorizing
  - Experimental realization
    - Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Vandersypen et al, 2001
- Grover’s algorithm
  - Search
  - Experimental realization
    - Implementation of a quantum search algorithm on a quantum computer, Jones, Mosca & Hansen, 1998

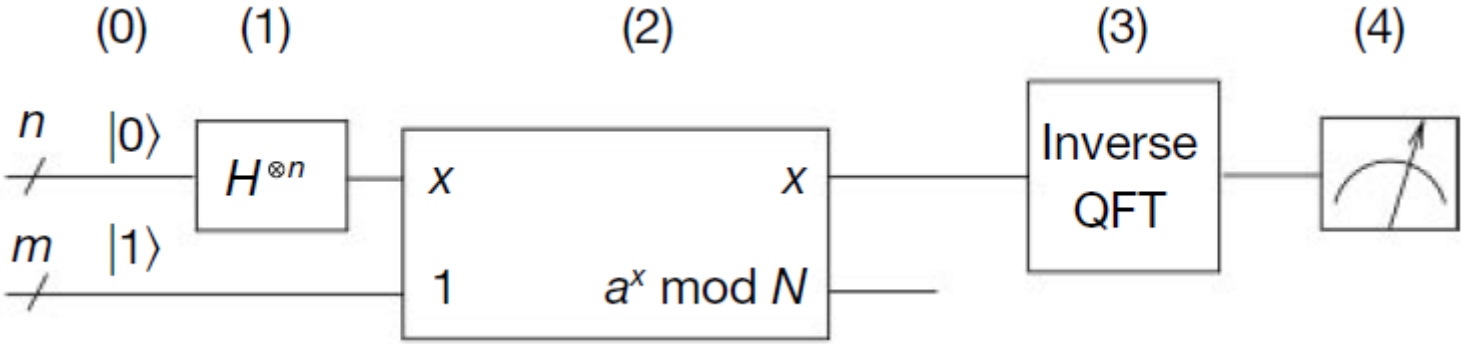
NMR recap

- Ensemble of atoms in room temperature
- Qubits: Spin states of atoms in a molecule (static magnetic field)
- Control: Radiofrequency (RF) pulses, spin-spin (J-coupling)
- Initialize state: Temporal averaging to create effective pure state



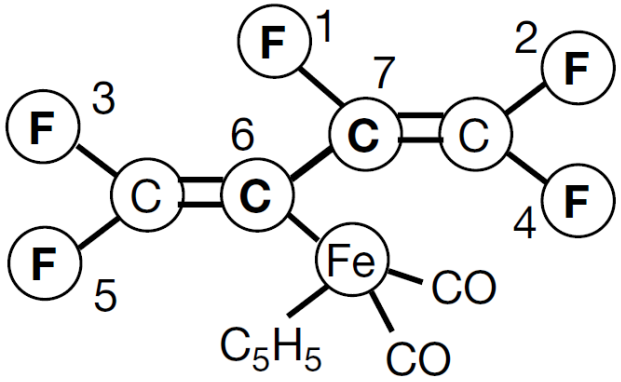
Theory – Shor's algorithm

- Prime factorization
- Scales polynomially with the number of digits.
- Factorizing N.
  - 0 & 1: Initialize qubits into the states we want them in.
  - 2: Multiply second register with $a^x \bmod N$. $a < N$ shares no factors with N (can be found on classical computer).
  - 3: Inverse quantum Fourier transform.
  - 4: Readout, find periodicity of $a^x \bmod N$ and do gcd classically.



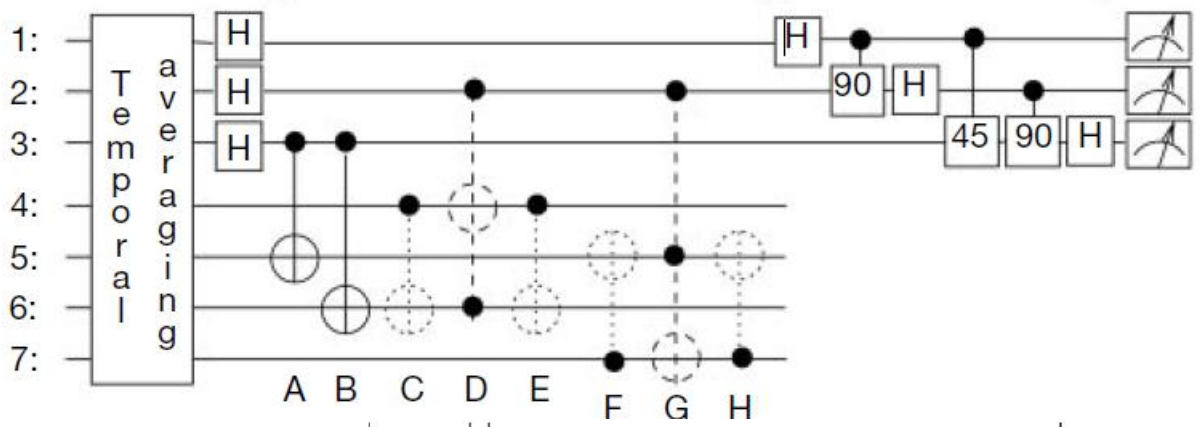
Implementation of Shor's algorithm

- Choosing qubits
  - $a^x = a^{2^{n-1}x_{n-1}} \dots a^{2x_1}a^{x_0}$
    - Pick a wisely!
  - Implemented with $a = 11$ and $a = 7$.
    - $a = 11 \Rightarrow a^x \bmod 15 = a^{x_0} \bmod 15$
    - $a = 7 \Rightarrow a^x \bmod 15 = a^{2x_1}a^{x_0} \bmod 15$
  - $n = 3$ qubits is enough in the first register.
  - Second register consists of $m = \lceil \log_2 15 \rceil = 4$ qubits.

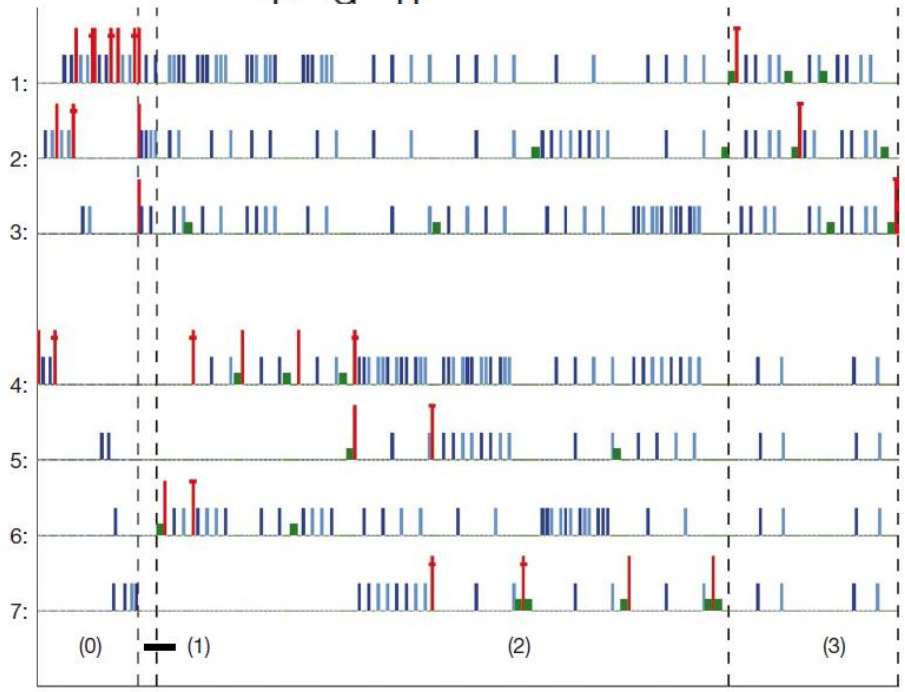


Implementation of Shor's algorithm

- More detailed circuit for $a = 7$



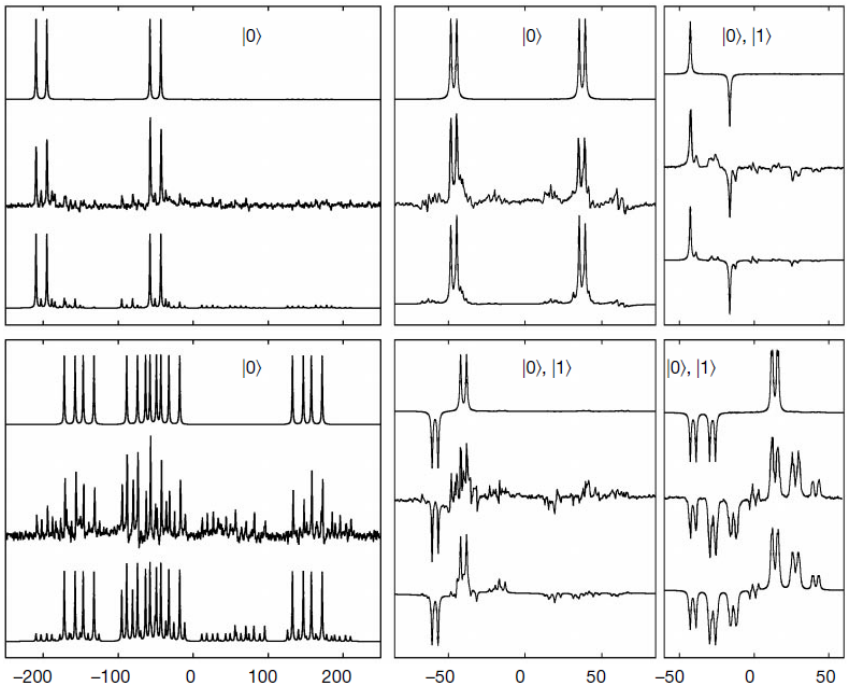
- ~300 r.f. pulses
  - Pulse scheme



- For large N
  - Continued fractions algorithm
  - Requires additional qubits

Results for Shor's algorithm

- For $a = 11$
  - Mix of $|000\rangle$ and $|100\rangle$ ($|0\rangle$ and $|4\rangle$)
  - $r = 2^n/4 = 2$
  - $\gcd\left(11^{2/2} \pm 1, 15\right) = 3, 5$
- For $a = 7$
  - Mix of $|000\rangle$, $|010\rangle$, $|100\rangle$ and $|110\rangle$ ($|0\rangle$, $|2\rangle$, $|4\rangle$ and $|6\rangle$)
  - $r = 2^n/2 = 4$
  - $\gcd\left(7^{4/2} \pm 1, 15\right) = 3, 5$

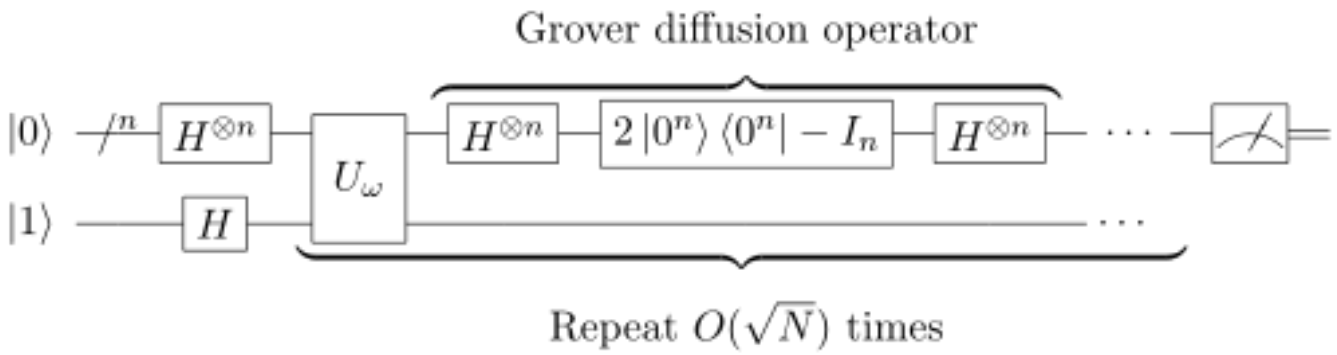


Theory – Grover's algorithm

- Quantum search

- Concept:
  - n-qubits used for a $N = 2^n$ element list
  - Initialize n-qubits in superpositioned states $|\psi\rangle = |0 \dots 0\rangle + \dots + |x\rangle + \dots + |1 \dots 1\rangle$
  - Do grover iteration $O(\sqrt{N})$ times:
    - Change sign on the element wanted, $U|x\rangle \rightarrow -|x\rangle$
    - Apply Hadamard gate
    - Change sign on all except $|0\rangle$ state
    - Apply Hadamard gate

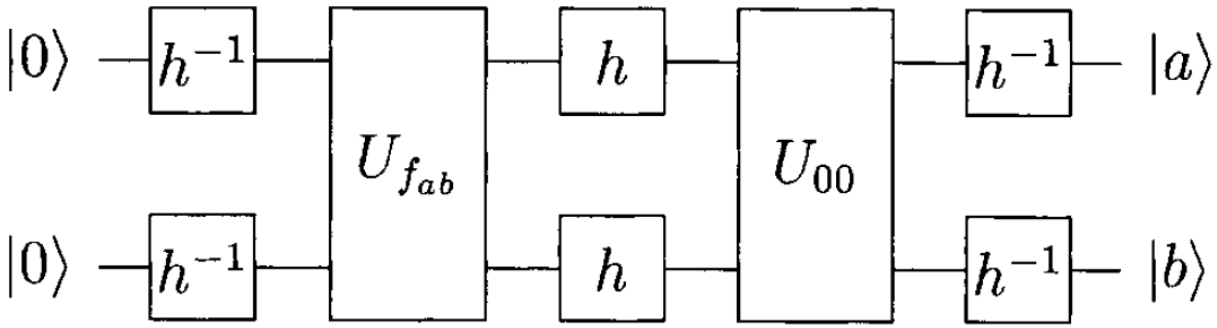
    Summary $G = (H^{\otimes n}(2|0\rangle\langle 0| - 1)H^{\otimes n})U$
  - Final state is in $|x\rangle$ (Position of element wanted)



Algorithm used in experiment

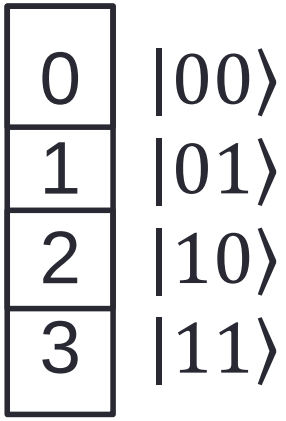
$$h = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = e^{\frac{i\pi}{2}I_y}$$

- 2-qubit computer:
  - Start in state $|00\rangle$
  - h^{-1} (inverse pseudo-Hadamard gates)
  - $U_{f_{ab}}$ unitary operation replacing eigenstate $|ab\rangle$ by $-|ab\rangle$
  - h (pseudo-Hadamard gate)
  - U_{00} unitary operation replacing eigenstate $|00\rangle$ by $-|00\rangle$
  - h^{-1} (inverse pseudo-Hadamard gates)
  - End with $|ab\rangle$, the state we searched for



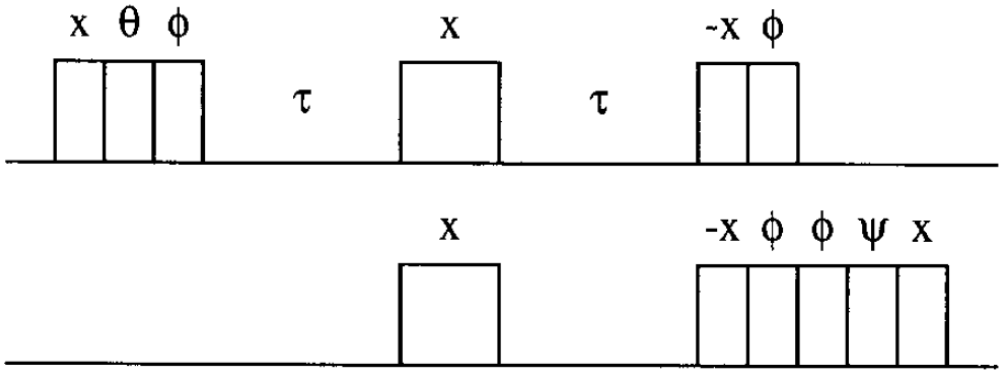
Example

- Search for state $|01\rangle$
  - $|\psi\rangle = |00\rangle$
  - $|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$
  - $U_{f_{01}}|\psi\rangle = |00\rangle - |01\rangle + |10\rangle + |11\rangle$
  - ...
  - $|\psi\rangle = |01\rangle$

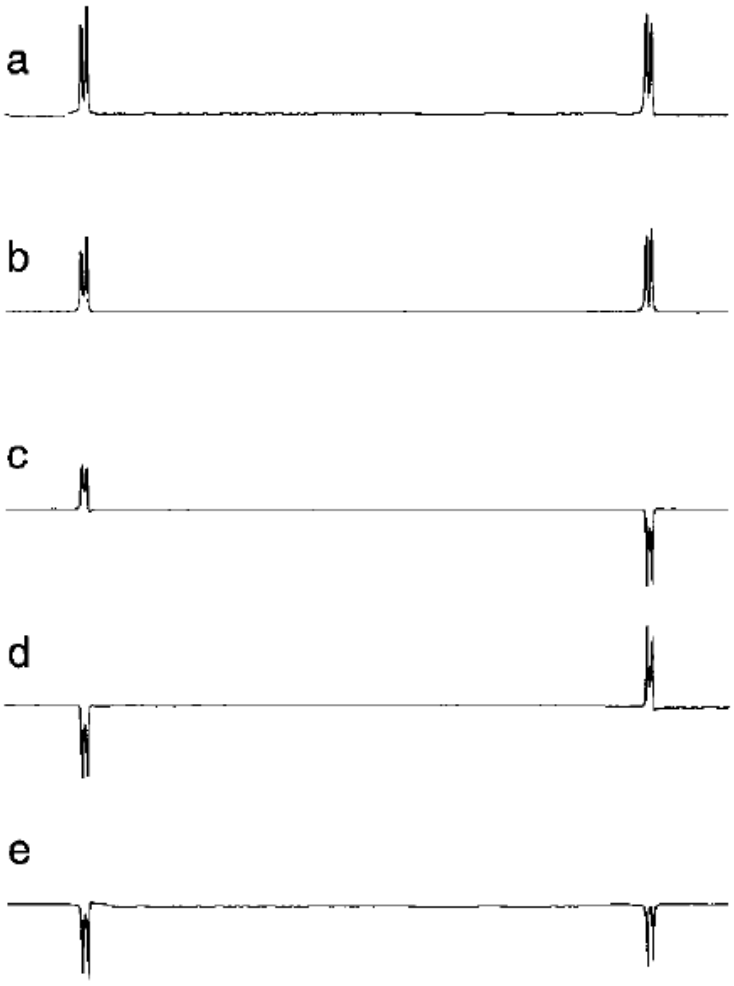


Implementation of Grover's algorithm

- System:
  - Qubits: 2 H nuclei in a magnetic field
  - Logic gates: Radiofrequency(RF) and spin-spin coupling
- Algorithm:
  - Initialize effective pure state
  - Pseudo Hadamard gate by $90^o{}_y$ pulses
  - $U_{f_{ab}}$ implemented by a pulse scheme, ex f_{00}; $\theta = +y, \phi = +x,$ $\psi = -y$



Output in experiment



- Reference spectrum $|00\rangle$
- $|00\rangle$
- $|01\rangle$
- $|10\rangle$
- $|11\rangle$

Conclusion

- Realization of multi-qubit algorithms is possible with NMR, but:
  - More qubits ⇒ bigger, more complex molecules
- Demonstrated implementations are “proof-of-concept”
  - Designed with the specific problems in mind
  - Not general

References

- Jones, Mosca, Hansen, et al. Implementation of a quantum search algorithm on a quantum computer, Nature 393, 344 (1998)
- Vandersypen, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature 414, 883 (2001)