ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Algorithms in NMR Experiments

- 25th May 2012
- Ling LIN & Michael Loretz

Contents

Introduction to Shor's algorithm

- Given an integer N, find its prime factors.
- Classically, prime factorization takes $O(\exp[1.9(\log N)^{1/3}(\log \log N)^{2/3}])$ operations.
- On a quantum computer, it runs in polynomial time, taking only $O((\log N)^3)$ operations. Much faster!
- With a sufficient number of qubits, Shor's algorithm can be used to break public-key cryptography schemes such as the widely used RSA scheme.
- Shor's algorithm consists of two parts:
  - Classical part:
    A reduction of the factoring problem to the order-finding problem, which can be done on a classical computer.
  - Quantum part:
    A quantum algorithm is used to solve the order-finding problem.

Shor's algorithm (classical part)

- Task:
  - Given an integer N, find its prime factors
  - Calculate $a^x \bmod N = 1$; find period r (order of a) of $f_{N,a}(x)=a^x \bmod N$

- Procedure:
  - $a^2 \bmod N = 1 \Leftrightarrow (a + 1)(a - 1) = 0 \bmod N$
  - If neither (a + 1) nor (a - 1) multiple of N, than at least one factor of N is in (a + 1) and also in (a - 1)

- Algorithm:
  - Choose a ϵ {2, ..., N - 1}
  - y := gcd(a, N), check y = 1
  - r := ord(a), check r = 2k
  - z := max{gcd(ar/2 - 1, N), gcd(ar/2 + 1, N)}

Shor's algorithm (classical part)

- Task:
  - Given an integer N, find its prime factors
  - Calculate $a^x \bmod N = 1$; find period r (order of a) of $f_{N,a}(x)=a^x \bmod N$

- Procedure:
  - $a^2 \bmod N = 1 \Leftrightarrow (a + 1)(a - 1) = 0 \bmod N$
  - If neither (a + 1) nor (a - 1) multiple of N, than at least one factor of N is in (a + 1) and also in (a - 1)

- Algorithm:
  - Choose $a \in \{2, ..., N - 1\}$
  - y := gcd(a, N), check y = 1
  - r := ord(a), check r = 2k
  - $z := \max\{\gcd(a^{r/2} - 1, N), \gcd(a^{r/2} + 1, N)\}$

Example: to factorize 21:

Choose a=13

gcd(13,21)=1 ok.

ord(13): $13^2 \bmod 21 = 1 \Rightarrow r=2$ ok.

gcd(12,21)=3, gcd(14,21)=7

=> 21=3*7

Shor's algorithm (quantum part)

1. *Initialization*

$$Q^{-1/2}\sum_{x=0}^{Q-1}|x\rangle|0\rangle$$

2. *Construction*

$$Q^{-1/2}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle$$

3. *Transformation*

$$Q^{-1}\sum_{x}\sum_{y}\omega^{xy}|y\rangle|f(x)\rangle$$

$$\sum_{x:f(x)=f(x_0)}\omega^{xy}=\sum_{b}\omega^{(x_0+r_b)y}=\omega^{x_0y}\sum_{b}\omega^{rby}$$

Shor's algorithm (quantum part)

1. *Initialization*

$$Q^{-1/2}\sum_{x=0}^{Q-1}|x\rangle|0\rangle$$

a superposition of Q states

2. *Construction*

$$Q^{-1/2}\sum_{x=0}^{Q-1}|x\rangle|f(x)\rangle$$

f(x) as a quantum function and apply it to the above state

3. *Transformation*

$$Q^{-1}\sum_{x}\sum_{y}\omega^{xy}|y\rangle|f(x)\rangle$$

apply the quantum Fourier transform, and leads to the final state

$$\sum_{x:f(x)=f(x_0)}\omega^{xy}=\sum_{b}\omega^{(x_0+r_b)y}=\omega^{x_0y}\sum_{b}\omega^{rby}$$

Shor's algorithm (quantum part)

4.*Measurement*

$$\left| Q^{-1} \sum_{x:f(x)=f(x_0)} \omega^{xy} \right|^2 = Q^{-2} \left| \sum_b \omega^{(x_0+r_b)y} \right|^2 = Q^{-2} \left| \sum_b \omega^{rby} \right|^2$$

Shor's algorithm (quantum part)

4.*Measurement*

$$\left| Q^{-1} \sum_{x:f(x)=f(x_0)} \omega^{xy} \right|^2 = Q^{-2} \left| \sum_b \omega^{(x_0+r_b)y} \right|^2 = Q^{-2} \left| \sum_b \omega^{rby} \right|^2$$

-Perform Continued Fraction Expansion on y/Q to make an approximation, and produce some c/r' by it that satisfies two conditions:

A: r' < N

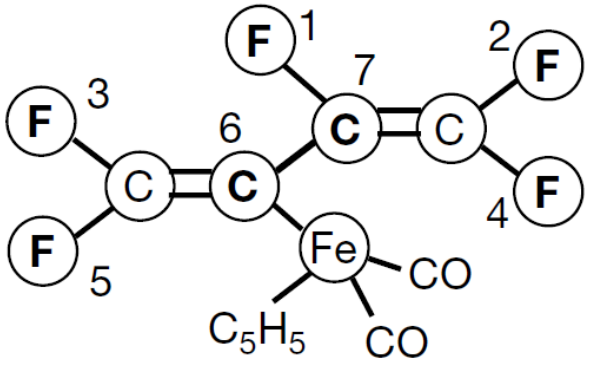
B: |y/Q - c/r'| < 1/2Q

r' would be the appropriate period r with high probability.

-Check if f(x) = f(x + r') <=> a^r = 1 (mod N); if so, done.

-Otherwise, obtain more candidates for r near y.

Qubit system: nuclear spins in a molecule



Perfluorobutadienyl molecule with 7 nuclear spins

- ^{19}F and ^{13}C are spin half nuclei
- 2 level system due to Zeeman splitting in static magnetic field

$$H = -\sum_i^n \bar{h}\,\omega_{0i} I_{iz} \qquad \omega_{0i} = \frac{g\mu_i B_0}{\bar{h}}$$

- ω_{0i} Transition frequency between $|0\rangle$ &$|1\rangle$

$$11.7\,T \rightarrow \begin{matrix} ^{13}C\ \omega_{0i} = 125\,MHz \\ ^{19}F\ \omega_{0i} = 470\,MHz \end{matrix}$$

Spin properties

- Chemical shifts in molecule causes inhomogenities in magnetic field, well separated frequencies for each qubit

$$\omega_{0i} = (1 - \sigma_i)\frac{g\mu_i B_0}{\bar{h}}$$

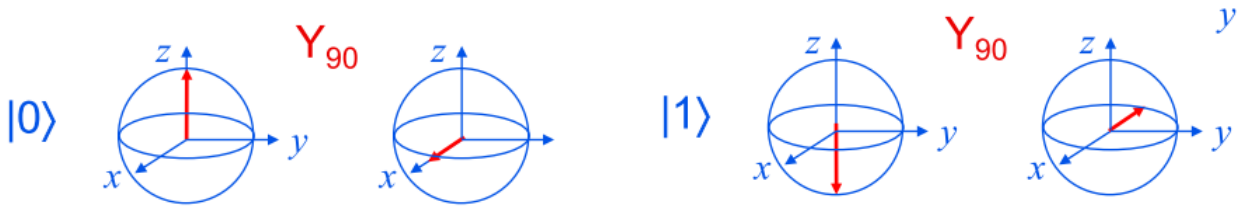
- Longitudinal and transvers coherence times T_1 and T_2 in order of seconds
- Pairwise J coupling between spins

$$H_J = \sum_{i<j} 2\pi\bar{h} J_{ij}\, I_{iz} I_{jz}$$

i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	–22052.0	5.0	1.3	–221.0	37.7	6.6	–114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	–3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	–13.5	41.6	12.9		
4	–4918.7	10.0	1.7	54.1	–5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	–4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						

Experimental realization

- RF coil in xy plane for applying RF pulses to manipulate spins
- Spin state is detected by rotating about y-axis by 90°
  - 10^{23} nuclei produce measurable RF field in the coil (ensemble measurement)



- Qubit system of the molecule fullfils the DiVincenzo criteria
  - For proper initialization temporal averaging can be used
  - Long enough coherence times
  - Pairwise J coupling of spins allows to implement gates
  - Readout of spin states possible

Shor's algorithm applied to 15

For N=15 have to consider 3 cases:

i. $a = 3,5,6,10 \rightarrow \gcd(a, 15) = 3 \; or \; 5$

no quantum computation step needed

ii. $a = 4,11,14 \rightarrow \gcd(a, 15) = 1$

$f(2) = a^2 mod 15 = 1$

iii. $a = 2,7,8,13 \rightarrow \gcd(a, 15) = 1$

$f(4) = a^4 mod 15 = 1$

Periodicity is either r=2 or 4

r is even

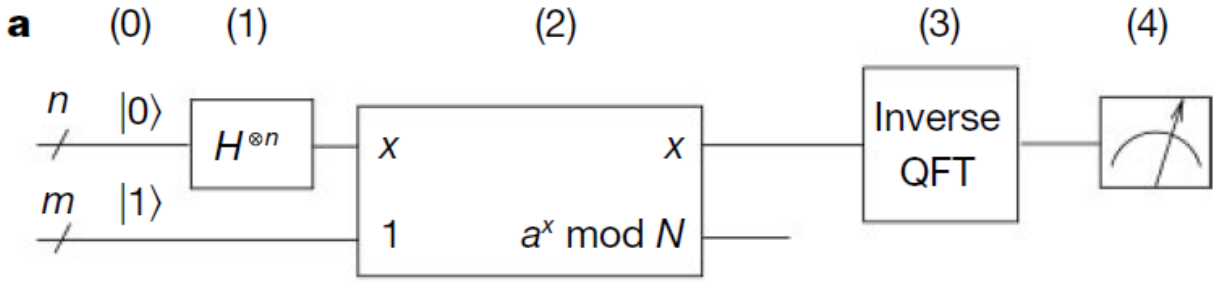
$a^{r/2} \neq -1 mod 15$

- First register has n=3 qubits to hold the periode r

  (two would be sufficient to represent 2 and 4, but there is one additional for possible higher periods)

- Second register has m=4 qubits to hold $f(x) = a^x mod 15$

Quantum circuit



0) Initialize first register to $|0\rangle = |000\rangle$ and the second to $|1\rangle = |0001\rangle$

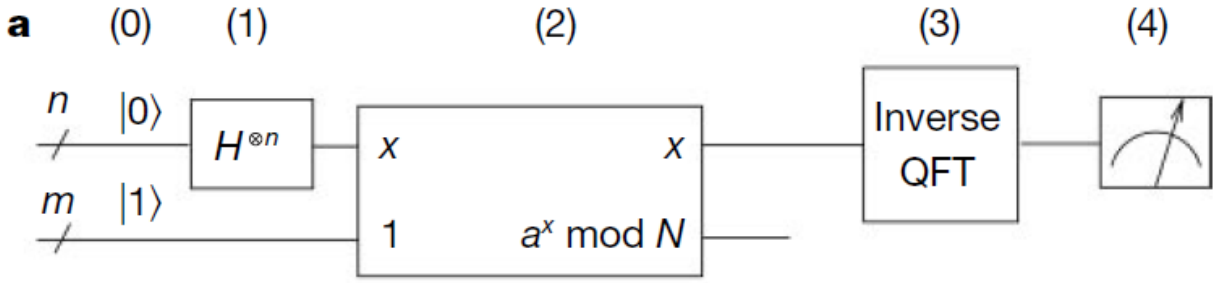
1) Hadamard gate on first register creates superposition

$$|\Psi_1\rangle = \sum_{x=0}^{7} \frac{1}{\sqrt[2]{8}} |x\rangle |1\rangle$$

2) Multiply second register with $f(x) = a^x mod N$

$$|\Psi_2\rangle = \sum_{x=0}^{7} \frac{1}{\sqrt[2]{8}} |x\rangle |1\rangle \langle a^x mod N\rangle$$

Quantum circuit II



3) Perform invers QFT on first register

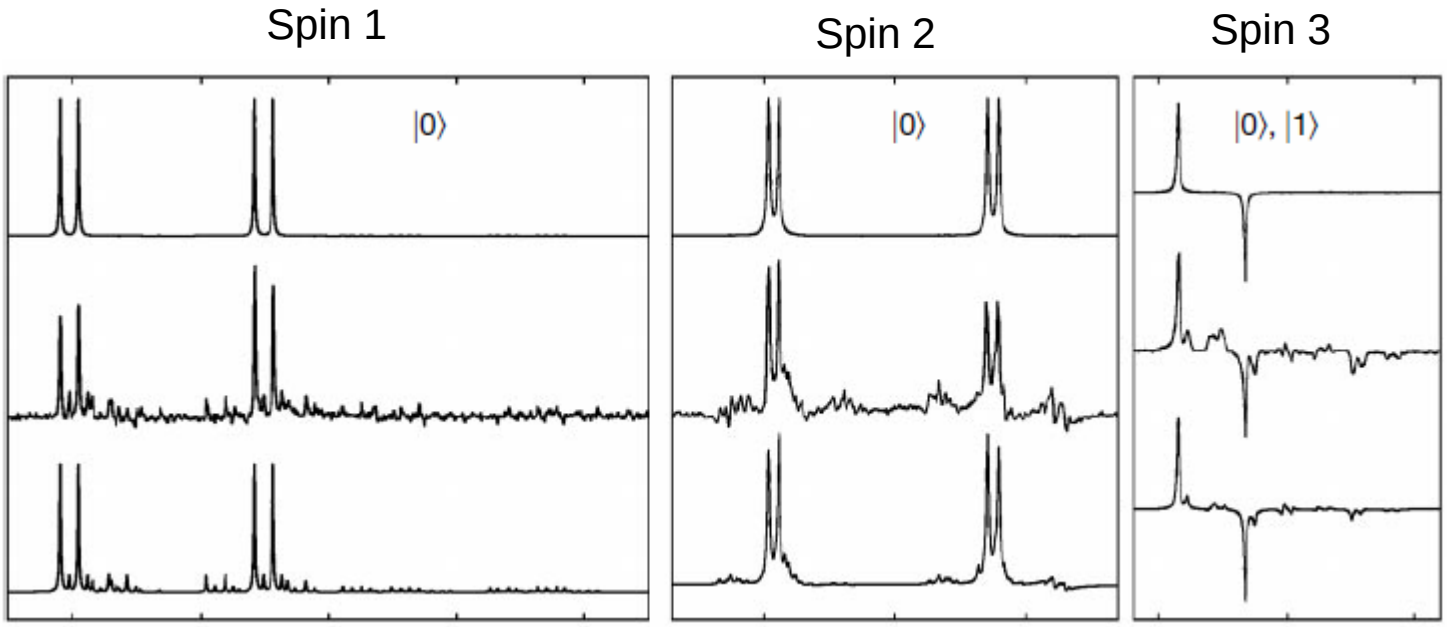
$$|\Psi_3\rangle = \sum_{y=0}^{7} \sum_{x=0}^{7} \frac{e^{2\pi i x y/8}}{\sqrt{8}} |y\rangle |a^x mod N\rangle$$

Sum over y reduces due to periodicity of f(x) to terms with $y = \frac{2^n c}{r}$, with c a constant and r the period of f(x)

4) Measuring the spin states of the first register with the pick up coil

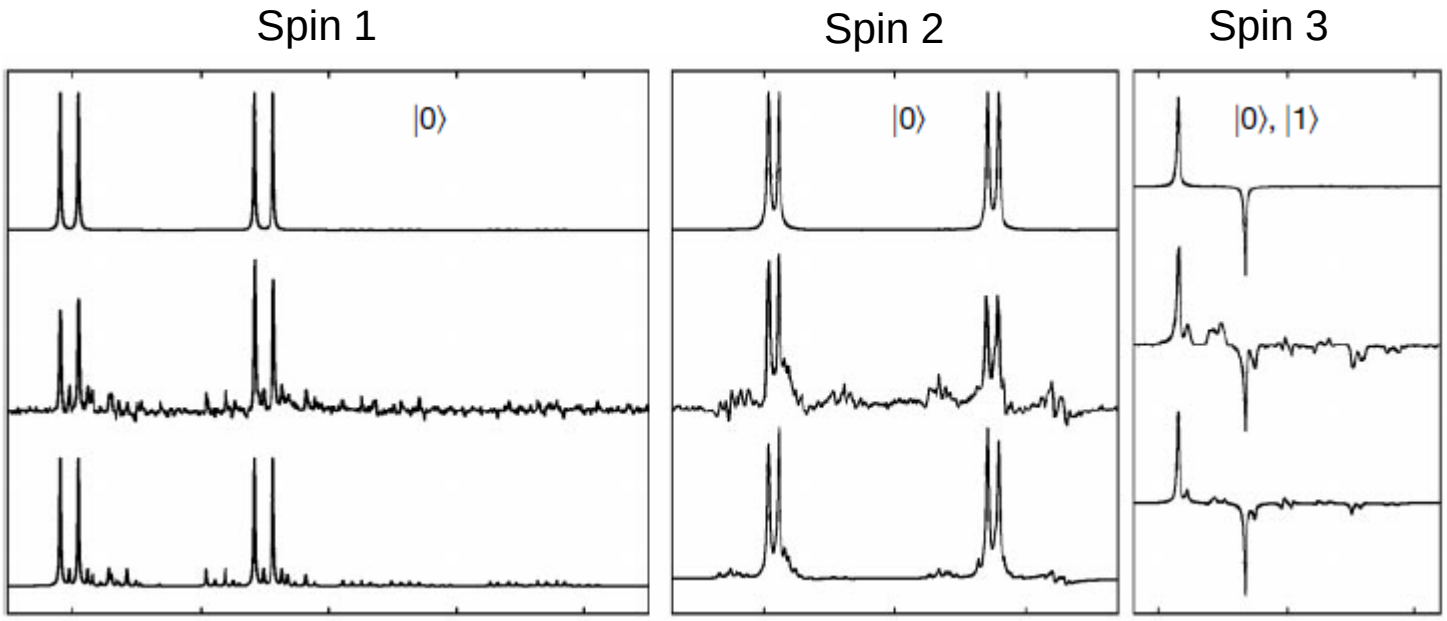
Initialization, manipulation and the measurement processes require about 300 RF pulses within 750 ms.

Experimental result a=11 (simple case)



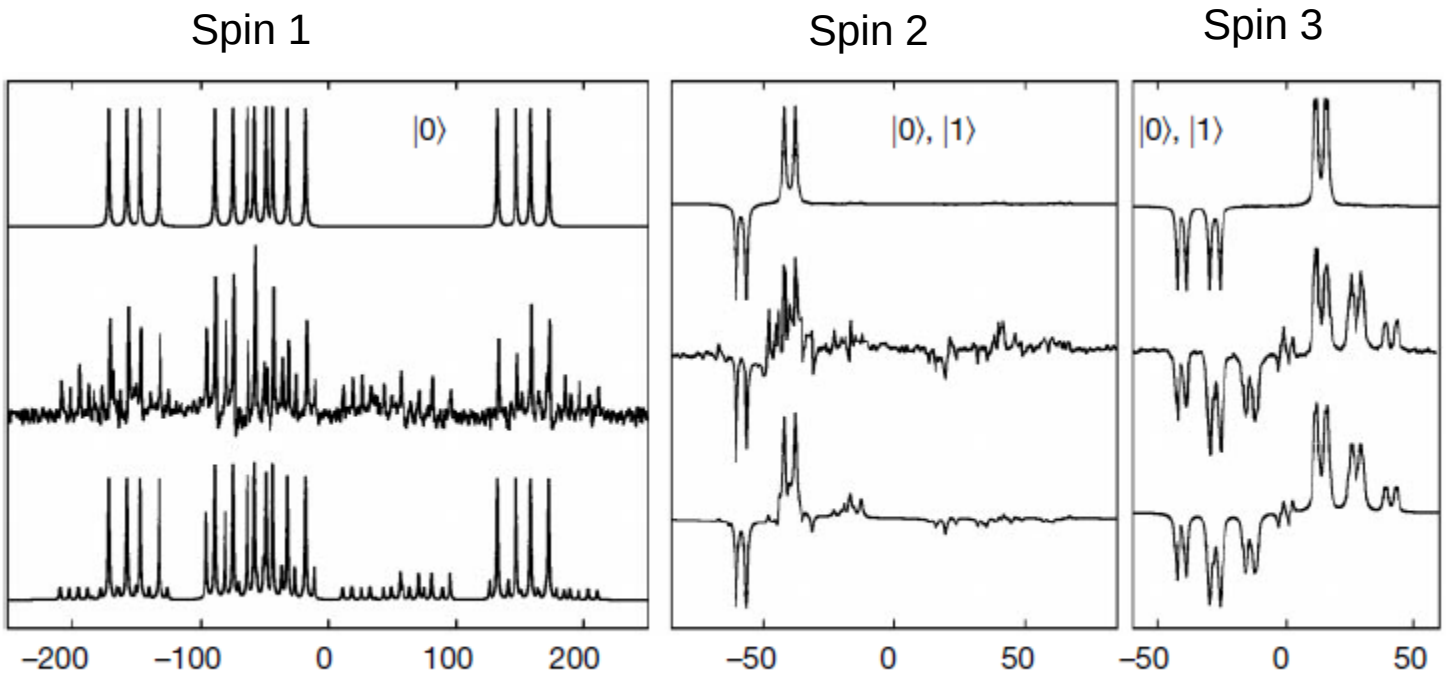
- Frequency vs. Phase plot for each spin
  - Positive peaks correspond to $|0\rangle$ and negative peaks to $|1\rangle$
- Simple case because just one qubit in a mixted state
- Multiple peaks in the spectra arise due to crosstalk of the spins

Experimental result a=11 (simple case)



- Mixture of states $|000\rangle$ and $|100\rangle$ or in decimal notation $|0\rangle$ and $|4\rangle$
- Period of y is $4 \rightarrow r = 2^3/4 = 2$
- $\gcd\left(11^{2/2} \pm 1{,}15\right) = 3 \;\&\; 5$

Experimental result a=7 (difficult case)



Theoretical simulation

Measured signal

Simulation with decoherence

- Mixture of states $|000\rangle$, $|010\rangle$, $|100\rangle$ and $|110\rangle$ or in decimal notation $|0\rangle$, $|2\rangle$, $|4\rangle$ and $|6\rangle$
- Period of y is 2 $\rightarrow r = 2^3/2 = 4$
- $\gcd\left(11^{4/2} \pm 1{,}15\right) = 3 \;\&\; 5$

References

- Shor Pieter W.
  Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

- Vandersypen, LMK: et al
  Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Conclusion

- Shor algorithm provides a solution for factoring number in polynominal time using a quantum computer
- Successful implementation of Shor‘s factoring algorithm in an NMR quantum computer
- Good agreement between measured and simulated spectra, discrepancies can be attributed to decoherence
- First quantum computation experiment for which decoherence is the dominant source of errors

Outlook

- The experiment shows the limits of NMR quantum computers
  - For N>15 a molecule with more spins is needed
  - Problems of single spin accessibility, spin interactions and shorter coherence times
- Hard to find error correction schemes for quantum computers to overcome imprecision and decoherence
- Proof for powerful every day applications of quantum computers is missing
- Task of the on going research to find other qubit systems and new quantum computation algorithms