Experimental Realization of Shor’s Quantum Factoring Algorithm

M. Steffen\textsuperscript{1,2,3}, L.M.K. Vandersypen\textsuperscript{1,2}, G. Breyta\textsuperscript{1}, C.S. Yannoni\textsuperscript{1}, M. Sherwood\textsuperscript{1}, I.L. Chuang\textsuperscript{1,3}

\textsuperscript{1}IBM Almaden Research Center, San Jose, CA 95120
\textsuperscript{2}Stanford University, Stanford, CA 94305
\textsuperscript{3}MIT Media Laboratory, Cambridge, MA 02139

Outline

• Background
• Introduction to Quantum Computation
  ➢ Classical bits vs. Quantum bits
  ➢ Quantum Algorithms
• NMR Quantum Computation
• Shor’s algorithm and Factoring 15
  ➢ Shor’s Quantum circuit
  ➢ Molecule
  ➢ Results (spectra, innovations)
• Conclusions
The quantum limit

1 bit = 1 atom?

Can we exploit quantum mechanics for ultra-fast computation?
The promise of Quantum Computation

Searching databases
- unsorted list of N entries
- how many queries?

\[ O(N) \quad \Rightarrow \quad O(\sqrt{N}) \]

1 month \quad \rightarrow \quad 27 minutes

Factoring Integers
- \( N = pq \)
- \( N \) has L digits
- given \( N \), what are \( p \) and \( q \)?

\[ O(e^{L^{1/3}}) \quad \Rightarrow \quad O(L^3) \]

10 billion years \quad \rightarrow \quad 3 years

400 digits

Classical vs. Quantum

Classical bits
- transistors
- 0 or 1

Quantum bits
- quantum systems
- 0 or 1 or in-between

NAND, NOT, CNOT …

These quantum gates allow operations that are impossible on classical computers!
Quantum bits

One qubit:
\[ |\psi_1\rangle = a|0\rangle + b|1\rangle \quad |a|^2 + |b|^2 = 1 \]

Multiple qubits:
\[ |\psi_n\rangle = a_0|00...0\rangle + a_1|00...1\rangle + a_2^n|11...1\rangle \quad \sum_i |a_i|^2 = 1 \]

Evolution of quantum states:

Conservation of probabilities allows only reversible, unitary operations

\[ |\psi_{n,out}\rangle = U |\psi_{n,in}\rangle \quad U \text{ is a } 2^n \times 2^n \text{ unitary matrix, i.e. } UU^\dagger = I \]
Quantum bits cont’d

Let a function $f(x)$ (implemented by unitary transforms) act on an equal superposition:

$$|\psi_{n,\text{out}}\rangle = f(|00...0\rangle) + f(|00...1\rangle) + f(|11...1\rangle)$$

Parallel operation, **BUT** a measurement collapses the wave function to only one of the states with probability $|a_i|^2$
⇒ Need to design clever algorithms
Quantum Algorithms

Example: 2 qubit Grover search

1. Create equal superposition
   \[ |\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle \]

2. Mark special element
   \[ |\psi\rangle = |00\rangle + |01\rangle + |10\rangle - |11\rangle \]

3. Inversion about average
   \[ |\psi\rangle = |11\rangle \]

One query = marking & inversion
In general, need \( \sqrt{N} \) queries
Physical Realization of QCs

Requirements for Quantum Computers\textsuperscript{1}:

- A quantum system with qubits
- Individually addressable qubits
- Two qubit interactions (universal set of quantum gates)
- Long coherence times
- Initialize quantum system to known state
- Extract result from quantum system

Meeting all of these requirements \textit{simultaneously} presents a significant experimental challenge.

\Rightarrow \textbf{Nuclear Magnetic Resonance (NMR) techniques} largely satisfies these requirements and have enabled experimental exploration of small-scale quantum computers

\textsuperscript{1} DiVincenzo D.P., \textit{Fortschr. Physik}, 48 (9-11), 771 – 783 (2000)
NMR Quantum Computing $^{1,2}$

$$\psi_{\text{out}} = e^{-iHt} \psi_{\text{in}} = U \psi_{\text{in}}$$

Characterize all Hamiltonians

spin $\frac{1}{2}$ particle in magnetic field:

$$H_0 = -\frac{\gamma B_0 Z}{2} = -\frac{\omega_0 Z}{2} = \frac{\omega_0}{2} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

Multiple spin ½ nuclei

Heteronuclear spins:

<table>
<thead>
<tr>
<th>nucleus</th>
<th>$^1$H</th>
<th>$^2$H</th>
<th>$^{13}$C</th>
<th>$^{15}$N</th>
<th>$^{19}$F</th>
<th>$^{31}$P</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\omega_0$ [MHz]</td>
<td>500</td>
<td>77</td>
<td>126</td>
<td>-51</td>
<td>470</td>
<td>202</td>
</tr>
</tbody>
</table>

Homonuclear spins:

Chemical shift

\[
H_0 = -\sum_{i=1}^{n} \frac{\omega_0^i Z^i}{2}
\]
Spin-spin coupling

- Dipolar couplings (averaged away in liquids)
- J-coupling (through shared electrons)

\[ H_J \approx \sum_{i<j} \frac{\pi J_{ij} Z^i Z^j}{2} \]

\[ H = -\sum_{i=1}^{n} \frac{\hbar \omega_0 Z^i}{2} + \sum_{i<j} \frac{\pi J_{ij} Z^i Z^j}{2} \]

Lamour frequency of spin \( i \) shifts by \(-J_{ij}/2\) if spin \( j \) is in \(|0\rangle\) and by \(+J_{ij}/2\) if spin \( j \) is in \(|1\rangle\)
Single qubit rotations

Radio-frequency (RF) pulses tuned to $\omega_0$
Two qubit gates

Lamour frequency of spin $i$ shifts by $-J_{ij}/2$ if spin $j$ is in $|0\rangle$ and by $+J_{ij}/2$ if spin $j$ is in $|1\rangle$

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
</tr>
<tr>
<td>01</td>
<td>01</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
</tr>
</tbody>
</table>

2-bit CNOT
State initialization

Thermal Equilibrium: … highly mixed state

\[ \rho_{eq} \propto I + \sum_i \omega_0^i Z^i \]

Effective pure state: … still mixed but:

\[ \rho_{eq} \propto I + \varepsilon |00\cdots0\rangle\langle00\cdots0| \]

• Spatial Labeling
• Temporal Labeling
• Logical Labeling
• Schulman-Vazirani

\[
\begin{array}{cccc}
  a & b & c & d \\
  a & c & d & b \\
  a & d & b & c \\
  \hline
  3a & b+c+d & b+c+d & b+c+d
\end{array}
\]
NMR Setup
Shor’s Factoring Algorithm

Quantum circuit to factor an integer \( N \)

- \(|x\rangle\) \( n \) qubits
- \(|1\rangle\) \( m \) qubits
- \( f(x) = a^x \mod N \)
- \( \text{QFT} \)
- \( \gcd(a^{r/2} \pm 1, N) \)

- \( m = \log_2(N) \)
- \( n = 2m \)
- ‘a’ is randomly chosen and can’t have factors in common with \( N \).

The algorithm fails for \( N \) even or equal to a prime power (\( N=15 \) is smallest meaningful instance).
Factoring 15 ...

... sounds easy, but

Challenging experiment:

• synthesis of suitable 7 qubit molecule
• requires interaction between almost all pairs of qubits
• coherent control over qubits
Shor’s Factoring Algorithm

\[ a^x = a^{2^{n-1}x_{n-1}} \cdots a^{2x_1}a^{x_0} \]
where \( x_k \) are the binary digits of \( x \).

- \( a = 2, 7, 8, 13 \)
- \( a^4 \mod 15 = 1 \)
- “hard case”

- \( a = 4, 11, 14 \)
- \( a^2 \mod 15 = 1 \)
- “easy case”

Three qubits in the first register are sufficient to factor 15.
Factoring N = 15

- **a = 11**  
  ‘easy case’

- **a = 7**  
  ‘hard case’

Diagram showing the process of factoring N = 15 with operations labeled as **mod exp** and **QFT**.
The molecule

<table>
<thead>
<tr>
<th>i</th>
<th>Ω/2π</th>
<th>T1,i</th>
<th>T2,i</th>
<th>J7i</th>
<th>J6i</th>
<th>J5i</th>
<th>J4i</th>
<th>J3i</th>
<th>J2i</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15186.6</td>
<td>2.8</td>
<td>1.8</td>
<td>2.1</td>
<td>2.5</td>
<td>6.6</td>
<td>19.4</td>
<td>59.5</td>
<td>41.6</td>
</tr>
<tr>
<td>2</td>
<td>25088.3</td>
<td>3.0</td>
<td>2.5</td>
<td>12.9</td>
<td>3.9</td>
<td>14.5</td>
<td>1.0</td>
<td>-13.5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>-4519.1</td>
<td>45.4</td>
<td>2.0</td>
<td>-5.7</td>
<td>-3.9</td>
<td>37.7</td>
<td>68.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4244.3</td>
<td>31.6</td>
<td>2.0</td>
<td>54.1</td>
<td>18.6</td>
<td>-221</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-22052</td>
<td>25.0</td>
<td>1.3</td>
<td>-114.3</td>
<td>25.16</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>489.5</td>
<td>13.7</td>
<td>1.8</td>
<td>79.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>-4918.3</td>
<td>10.0</td>
<td>1.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Pulse Sequence

Init. mod. exp. QFT

~ 300 RF pulses || ~ 750 ms duration
Experimental detail and innovations

- Modified state initialization procedure
- Gaussian shaped $\pi/2$ pulses (220 – 900 μs)
- Hermite 180 shaped $\pi$ pulses (~ 2 ms)
- 4 channels, 7 spins: 6 spins always off resonance
- transient Bloch-Siegert shifts
- used technique for simultaneous soft pulses$^1$
- refocus T2* effects
- correct J-coupling during pulses

Results: Spectra

Mixture of $|0\rangle, |4\rangle$
$2^{3/2} = r = 4$
$\gcd(7^{4/2} \pm 1, 15) = 3, 5$

$15 = 3 \cdot 5$

Mixture of $|0\rangle, |2\rangle, |4\rangle, |6\rangle$
$2^{3/2} = r = 4$
$\gcd(7^{4/2} \pm 1, 15) = 3, 5$

$qubit 3$  $qubit 2$  $qubit 1$

$|0\rangle$

$a = 11$

$|0\rangle$

$a = 7$
Results: Predictive Decoherence Model

Operator sum representation: \( \rho \Rightarrow \sum_k E_k \rho E_k^\dagger \)

Generalized Amplitude Damping

\[ E_0 = \sqrt{p} \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \quad E_1 = \sqrt{p} \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \quad E_2 = \sqrt{1-p} \begin{bmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{bmatrix} \quad E_3 = \sqrt{1-p} \begin{bmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{bmatrix} \]

Phase Damping

\[ E_0 = \sqrt{\lambda} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad E_1 = \sqrt{1-\lambda} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \]
Decoherence Model cont’d

- GAD (and PD) acting on different spins commute
- $E_k$ for GAD commute with $E_k$ for PD on arb. Pauli matrices
- PD commutes with J-coupling, and z-rotations
- GAD (and PD) do NOT commute with RF pulses

- Pulse: time delay / GAD / PD / ideal pulse
Results: Circuit Simplifications

'Peephole' optimization

- control of C is $|0\rangle$
- control of F is $|1\rangle$
- E and H inconsequential to outcome
- targets of D and G in computational basis
Conclusions

• First experimental demonstration of Shor’s factoring algorithm
• Developed predictive decoherence model
• Methods for circuit simplifications