ETH zürich

NMR: Shor algorithm - Experimental realization

Patrik Caspar, Fadri Grünenfelder

Outline

Motivation

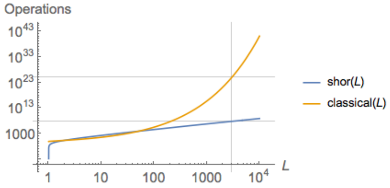
- Shor's algorithm in general:

Motivation

- Shor's algorithm in general:
  - Goal: Efficient prime factorization of L bit number N

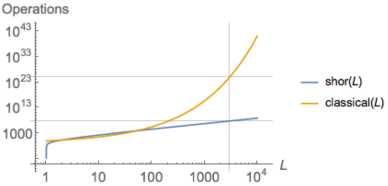
Motivation

- Shor's algorithm in general:
  - Goal: Efficient prime factorization of *L* bit number *N*
  - Speedup compared to classical algorithm:



Motivation

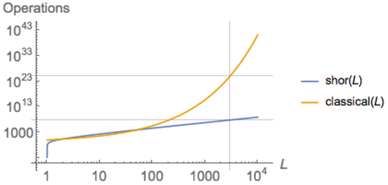
- Shor's algorithm in general:
  - Goal: Efficient prime factorization of L bit number N
  - Speedup compared to classical algorithm:



  - Tool for breaking public key cryptosystems

Motivation

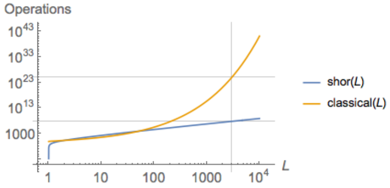
- Shor's algorithm in general:
  - Goal: Efficient prime factorization of L bit number N
  - Speedup compared to classical algorithm:



  - Tool for breaking public key cryptosystems
- NMR implementation:

Motivation

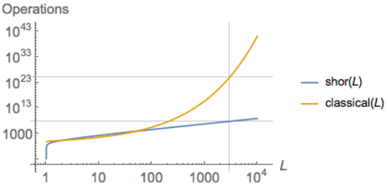
- Shor's algorithm in general:
  - Goal: Efficient prime factorization of *L* bit number *N*
  - Speedup compared to classical algorithm:



  - Tool for breaking public key cryptosystems
- NMR implementation:
  - Demonstration of experimental techniques for quantum computation with NMR

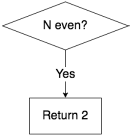
Motivation

- Shor's algorithm in general:
  - Goal: Efficient prime factorization of L bit number N
  - Speedup compared to classical algorithm:

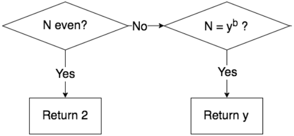


  - Tool for breaking public key cryptosystems
- NMR implementation:
  - Demonstration of experimental techniques for quantum computation with NMR
  - Implementation of Shor's algorithm for $N = 15$

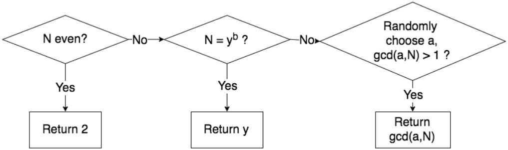
Recapitulation: Shor's algorithm



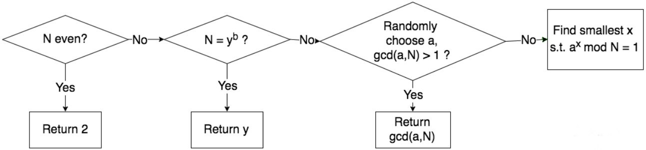
Recapitulation: Shor's algorithm



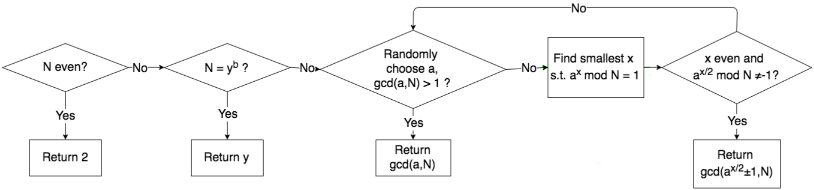
Recapitulation: Shor's algorithm



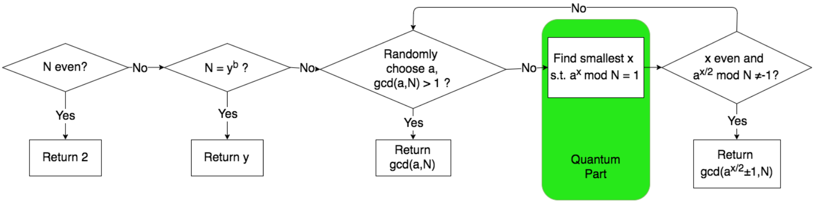
Recapitulation: Shor's algorithm



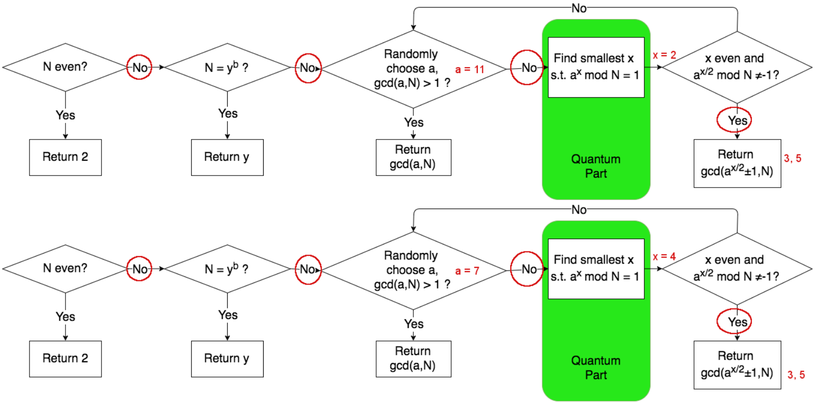
Recapitulation: Shor's algorithm



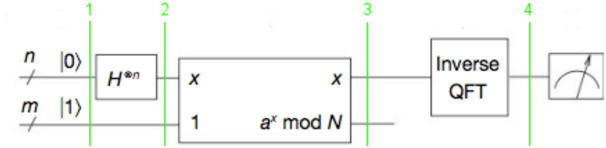
Recapitulation: Shor's algorithm



Examples: $N = 15$, $a = 11, 7$



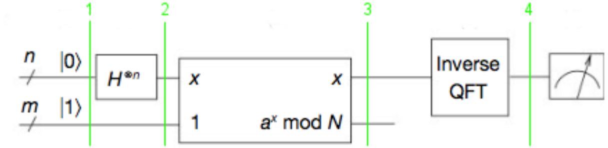
Shor's Algorithm - Quantum Part



$$|\psi_1\rangle = |0\rangle_n |1\rangle_m$$

L. M. K. Vandersypen *et al.*, *Nature* **414**,883 (2001)

Shor's Algorithm - Quantum Part

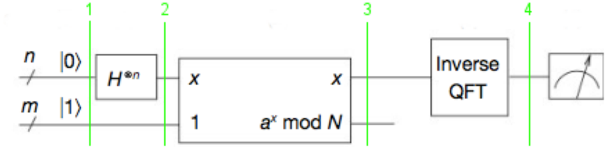


$$|\psi_1\rangle = |0\rangle_n |1\rangle_m$$

$$|\psi_2\rangle = \frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^{\otimes n} |1\rangle_m = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n |1\rangle_m$$

L. M. K. Vandersypen *et al.*, *Nature* **414**,883 (2001)

Shor's Algorithm - Quantum Part



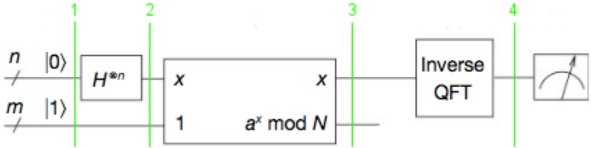
$$|\psi_1\rangle = |0\rangle_n |1\rangle_m$$

$$|\psi_2\rangle = \frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^{\otimes n} |1\rangle_m = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n |1\rangle_m$$

$$|\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n |a^k \bmod N\rangle_m$$

L. M. K. Vandersypen *et al.*, *Nature* **414**,883 (2001)

Shor's Algorithm - Quantum Part



$$|\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n |a^k \bmod N\rangle_m$$

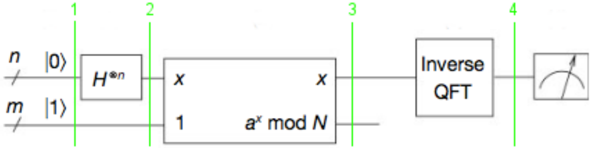
Basis change:

$$|u_s\rangle_m := \frac{1}{\sqrt{x}} \sum_{k=0}^{x-1} \exp\left(\frac{-2\pi isk}{x}\right) |a^k \bmod N\rangle_m$$

$$|a^k \bmod N\rangle_m = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} \exp\left(\frac{2\pi isk}{x}\right) |u_s\rangle_m$$

L. M. K. Vandersypen *et al.*, *Nature* **414**,883 (2001)

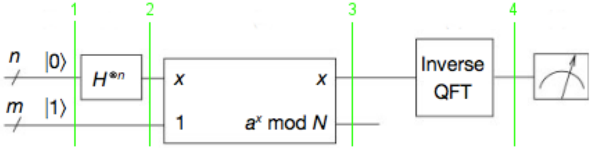
Shor's Algorithm - Quantum Part



Therefore: $|\psi_3\rangle = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n \exp\left(\frac{2^{n+1}\pi isk}{2^n x}\right) |u_s\rangle_m$

L. M. K. Vandersypen *et al.*, *Nature* **414**, 883 (2001)

Shor's Algorithm - Quantum Part



Therefore: $|\psi_3\rangle = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |k\rangle_n \exp\left(\frac{2^{n+1}\pi i s k}{2^n x}\right) |u_s\rangle_m$

$$|\psi_4\rangle = \frac{1}{\sqrt{x}} \sum_{s=0}^{x-1} |2^n s/x\rangle_n |u_s\rangle_m$$

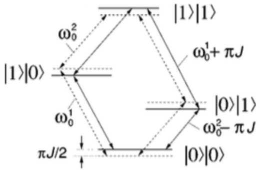
Measurement outcome: $2^n s/x$ for some s in 0, ..., $x - 1$

L. M. K. Vandersypen *et al.*, *Nature* **414**, 883 (2001)

NMR techniques

Manipulation:

$$H = -\sum_{i=1}^{N} \hbar\omega_0^i I_z^i - \sum_{i<j} 2\pi J_{ij} I_z^i I_z^j$$
$$- \sum_{i=1}^{N} \hbar\gamma_i B_1 [\cos(\omega_{\text{rf}} t + \phi) I_x^i - \sin(\omega_{\text{rf}} t + \phi) I_y^i]$$



L. M. K. Vandersypen and I. L. Chuang, *Reviews of modern Physics* **76**,1037 (2004)

NMR techniques

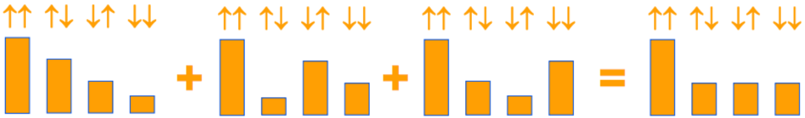
2 Qubit effective pure state:

$$\alpha_i = \hbar\omega_i / k_B T \approx 10^{-5}$$

$$\rho \propto \exp(\omega_i I_z^i / k_B T)$$

$$\rho = \frac{\mathbb{1}}{4} + \rho_\Delta = \frac{\mathbb{1}}{4} + \frac{1}{4}\begin{pmatrix} \alpha_1 + \alpha_2 & 0 & 0 & 0 \\ 0 & \alpha_1 - \alpha_2 & 0 & 0 \\ 0 & 0 & -\alpha_1 + \alpha_2 & 0 \\ 0 & 0 & 0 & -\alpha_1 - \alpha_2 \end{pmatrix}$$

Sum over permutations of the diagonal elements:

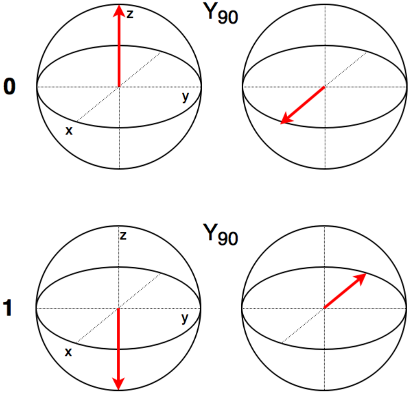


A. Wallraff, *Lecture Notes QSIT* (2016)

NMR techniques

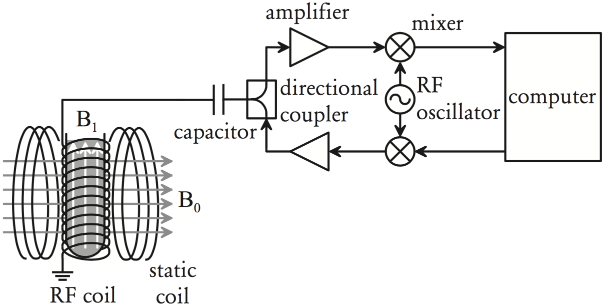
Readout:

We can measure: $\langle \mu_x + i\mu_y \rangle = \hbar\gamma \, \mathrm{Tr}[\rho_\Delta (I_x + iI_y)]$



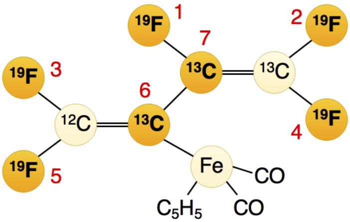
Experimental setup

$B_0 = 11.7$ T



I. L. Chuang *et al., Proceedings of the Royal Society A* **454**, pp. 447-467 (1998).

Quantum computer molecule



L. M. K. Vandersypen *et al., Nature* **414**, 883 (2001)

Quantum computer molecule

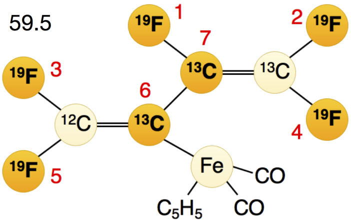
i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	–22052.0	5.0	1.3	–221.0	37.7	6.6	–114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	–3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	–13.5	41.6	12.9		
4	–4918.7	10.0	1.7	54.1	–5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	–4519.1	45.4	2.0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

At B_0 = 11.7 T:

$\omega_{0,F}/2\pi$ = 470 MHz

$\omega_{0,C}/2\pi$ = 125 MHz

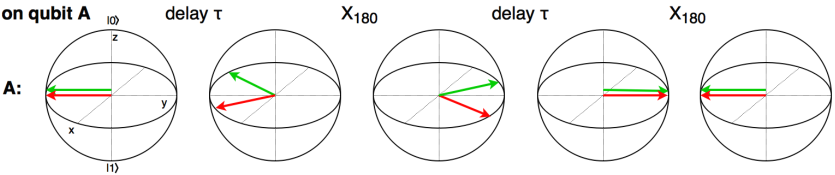
$[\omega_i/2\pi]$ = Hz, $[T]$ = s, $[J]$ = Hz



L. M. K. Vandersypen *et al.*, *Nature* **414**, 883 (2001)

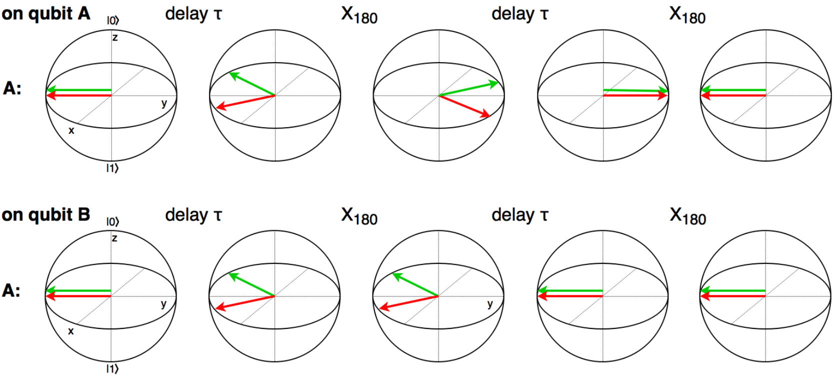
Refocusing

In rotating frame of qubit A



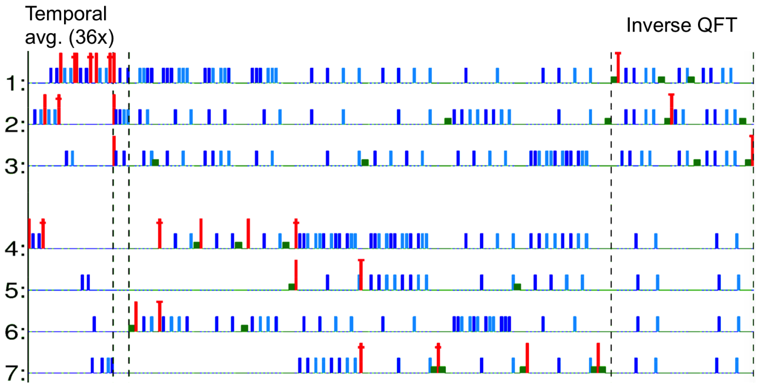
Refocusing

In rotating frame of qubit A



Pulse sequence

For a = 7: ∼300 pulses (0.22 - 2 ms), total ∼720 ms

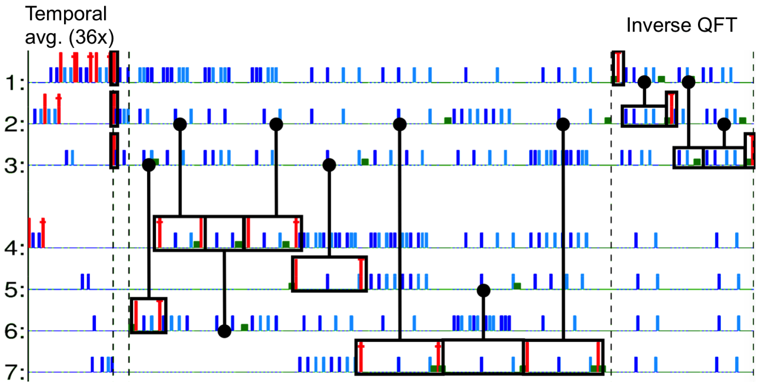


$\frac{\pi}{2}$ X-/Y-rotations, π −X-rotations (refocusing), Z-rotations

L. M. K. Vandersypen *et al.* (2001)

Pulse sequence

For a = 7: $\sim$300 pulses (0.22 - 2 ms), total $\sim$720 ms



$\frac{\pi}{2}$ X-/Y-rotations, π –X-rotations (refocusing), Z-rotations

L. M. K. Vandersypen *et al.* (2001)

Decoherence

Operator sum representation:

$$\rho \to \sum_k E_k \rho E_k^\dagger, \qquad \left(\sum_k E_k^\dagger E_k = I \right)$$

L. M. K. Vandersypen *et al., Nature* **414**, 883 (2001)

Decoherence

Operator sum representation:

$$\rho \to \sum_k E_k \rho E_k^\dagger, \qquad \left(\sum_k E_k^\dagger E_k = I \right)$$

Generalized amplitude damping (T_1): $p = \frac{1}{2} + \frac{\hbar\omega}{4k_B T}, \quad \gamma = 1 - e^{-t/T_1}$

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \qquad E_1 = \sqrt{p}\begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

$$E_2 = \sqrt{1-p}\begin{pmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_3 = \sqrt{1-p}\begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix}$$

L. M. K. Vandersypen *et al., Nature* **414**, 883 (2001)

Decoherence

Operator sum representation:

$$\rho \rightarrow \sum_k E_k \rho E_k^\dagger, \qquad \left(\sum_k E_k^\dagger E_k = I \right)$$

Generalized amplitude damping (T_1): $p = \frac{1}{2} + \frac{\hbar\omega}{4k_B T}, \quad \gamma = 1 - e^{-t/T_1}$

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix}, \qquad E_1 = \sqrt{p}\begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

$$E_2 = \sqrt{1-p}\begin{pmatrix} \sqrt{1-\gamma} & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_3 = \sqrt{1-p}\begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix}$$

Phase damping (T_2): $\lambda \sim \frac{1}{2}(1 + e^{-t/T_2})$

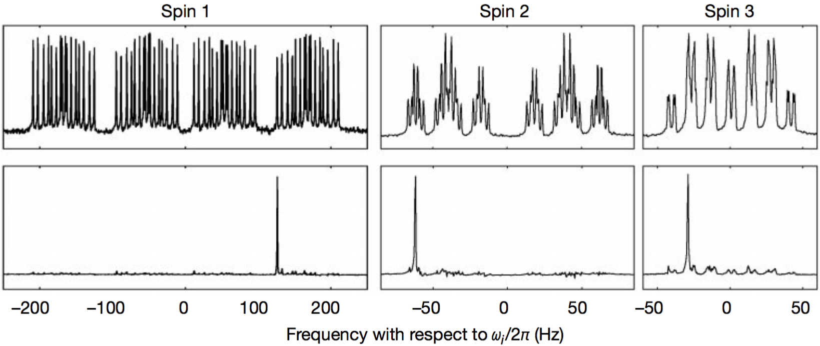
$$E_0 = \sqrt{\lambda}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad E_1 = \sqrt{1-\lambda}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

L. M. K. Vandersypen *et al., Nature* **414**, 883 (2001)

Readout

Thermal equilibrium state

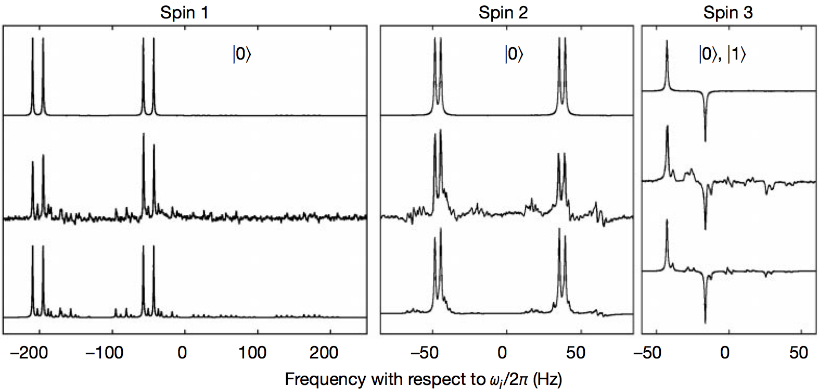
Effective pure ground state by adding multiple experiments



L. M. K. Vandersypen *et al.* (2001)

Readout

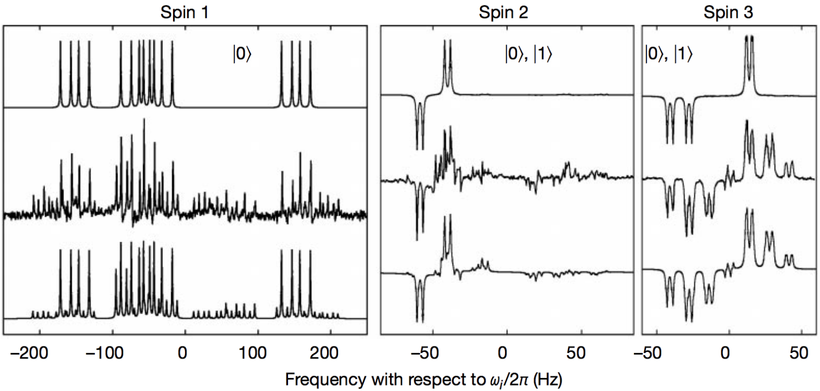
for a = 11



L. M. K. Vandersypen *et al.* (2001)

Readout

for a = 7



L. M. K. Vandersypen *et al.* (2001)

Further experiments

- 2009: Photonic chip (4 qubits)
- 2012: Josephson phase qubit quantum processor (4 qubits)

Summary

- First experimental realization of Shor’s factoring algorithm
- Advantages:
  - long coherence times
  - high degree of control
- Problems:
  - scaling
  - constant coupling

References

1. Vandersypen, L. M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883 (2001).
2. Gershenfeld, N. A. and Chuang, I. L. Bulk Spin-Resonance Quantum Computation. *Science* **275**, 350 (1997).
3. Vandersypen L. M. K. and Chuang, I. L. NMR techniques for quantum control and computation. *Review of Modern Physics* **76**, 1037 (2004).
4. Lucero, E. et al. Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics* **8**, 719 (2012).
5. Politi, A., Matthews, J. C. F. and O'Brien, J. L. Shor's Quantum Factoring Algorithm on a Photonic Chip. *Science* **325**, 1221 (2009).
6. Chuang, I. L., Gershenfeld, N., Kubinec, M. G. and Leung, D. W. Bulk Quantum Computation with Nuclear Magnetic Resonance: Theory and Experiment. *Proceedings of the Royal Society A* **454**, pp. 447-467 (1998).