ETH zürich

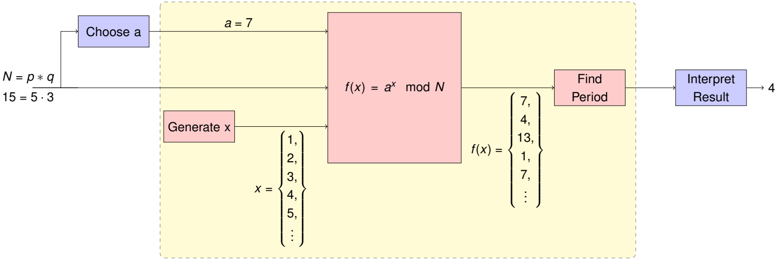
Factoring 15 using NMR

Amadé Bortis, Samuel Gyger

Outline

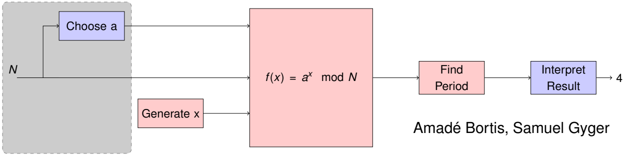
- Shor algorithm
  - Basics
  - Example
- Requirements
- Quantum circuit
- Results

Shor algorithm



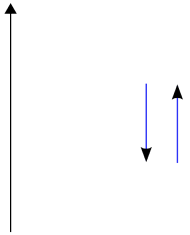
Qubit requirements

- Pick $a = 2, 7, 8, 13 \Rightarrow a^4 \bmod 15 = 1 \Rightarrow a^{2^k} \bmod 15 = 1$ for $k \geq 2$
- Pick $a = 4, 11, 14 \Rightarrow a^2 \bmod 15 = 1 \Rightarrow a^{2^k} \bmod 15 = 1$ for $k \geq 1$
- $f(x)$ simplifies to multiplications controlled by 2 bits (x_0, x_1)
- First register has to contain only 2 qubits
- 4 qubits needed to hold $f(x)$ $(2^4 = 16)$ (second register)

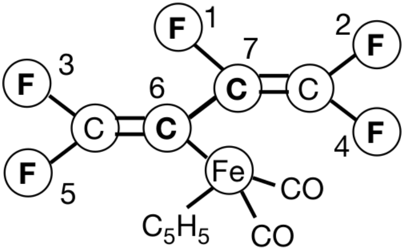


Molecule

- Experiment T = 303 K (30 °C)

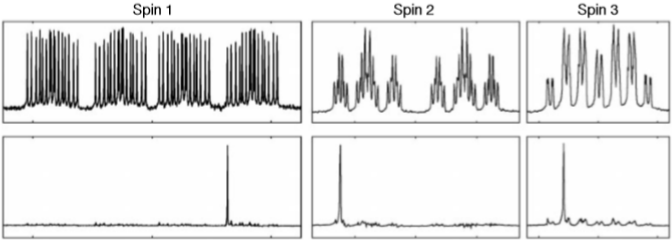


B=11.7T



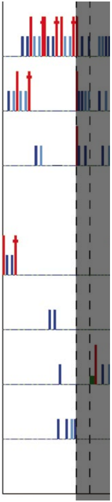
Initialization

- Desired inital state: $|\psi_1\rangle = |0000001\rangle$
- Use temporal averaging to create effective pure state $|\psi_1\rangle$
- $\rho^{pure} = \sum_i U_i^\dagger \rho U_i$



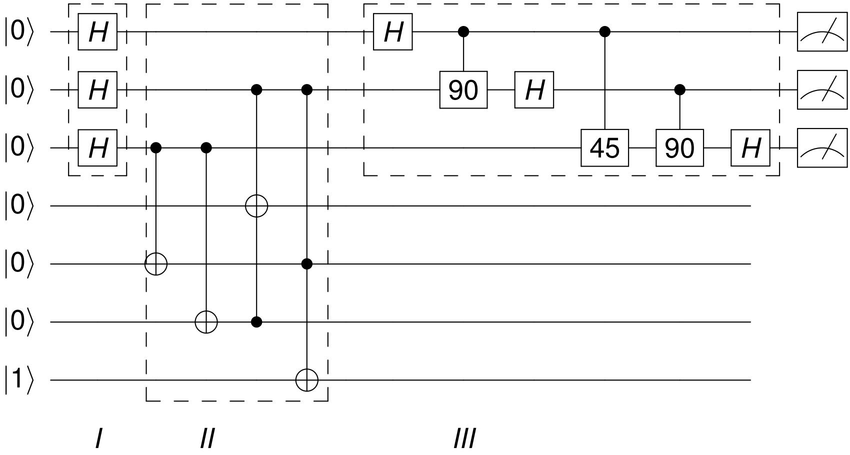
Quantum gates with NMR

- Using RF pulses
- Single Quantum Gates
  - 90° Pulse for a Hadamard Gate
- Coupling between different Atoms allows 2 Quantum Gates.
  - 90° Pulses and free Evolution Time
  - Refocusing undoes spin-spin interaction on target

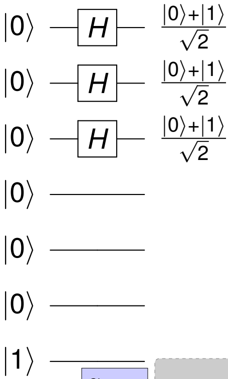


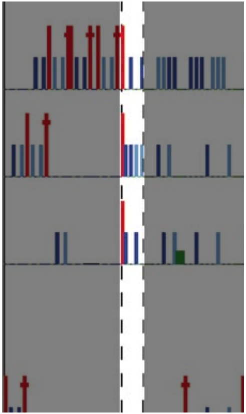
Run the Quantum circuit

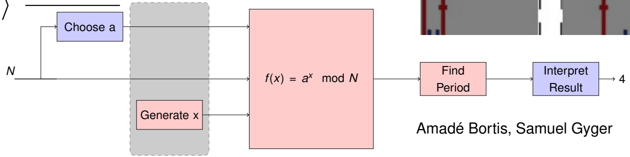
- Factorize N = 15 by finding Period of $f(x) = 7^x \bmod 15$



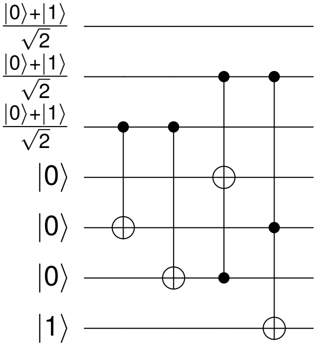
Step 1: The Hadamard gate



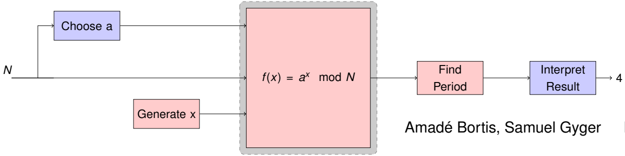




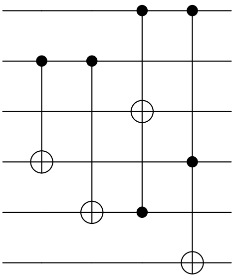
Step 2: Evaluate the function

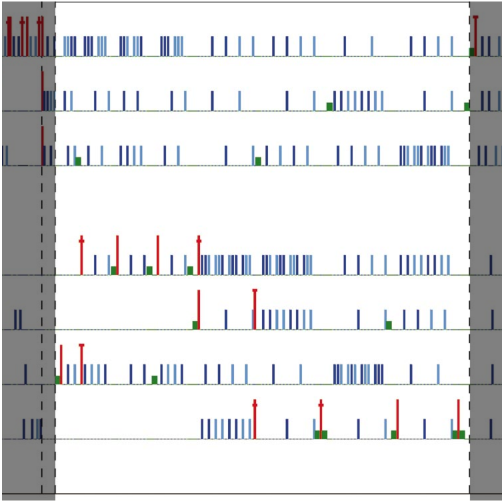


Step 2 creates a superposition in register 2, containing all possible values for $f(x) = a^x \bmod N$

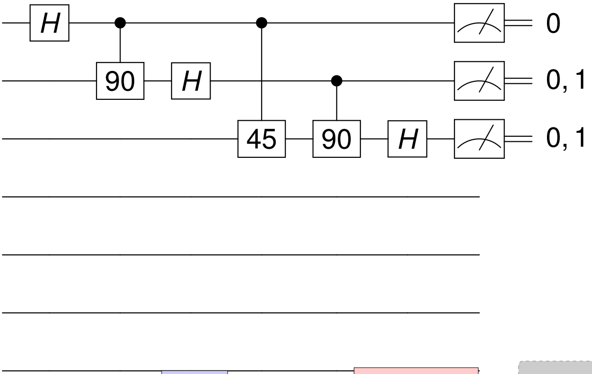


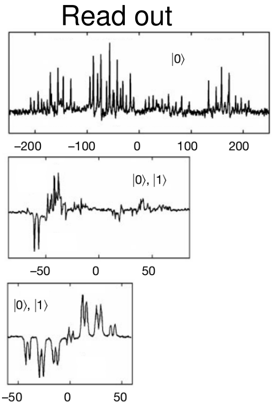
Step 2: Evaluate the function

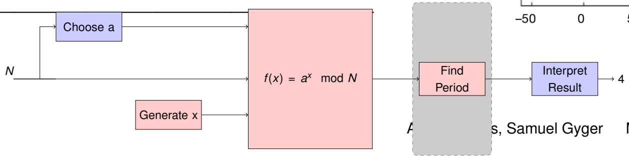




Step 3: Quantum Fourier Transform (QFT)

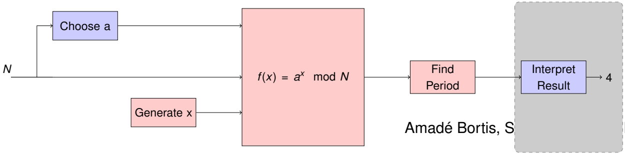






Calculating the Prime Factors

- All possible permutations of the Spin States are $|000\rangle$ (0), $|010\rangle$ (2), $|100\rangle$ (4), $|110\rangle$ (6).
- The smallest periodicity leads to $|2\rangle$ and therefore to $\gcd(7^{4/2} \pm 1, 15) = 3, 5$.



Outlook

- NMR not suited to factorize large numbers
- Similar experiments have been conducted with
  - Photonic Systems (Politi et al., 2009)
  - Superconducting Circuits (Lucero et al., 2012)

Literature

Lucero, E., Barends, R., Chen, Y., Kelly, J., Mariantoni, M., Megrant, A., O'Malley, P., Sank, D., Vainsencher, A., Wenner, J., White, T., Yin, Y., Cleland, A. N., and Martinis, J. M. (2012). Computing prime factors with a Josephson phase qubit quantum processor. *Nature Physics*, 8(10):719–723.

Politi, A., Matthews, J. C. F., and O'Brien, J. L. (2009). Shor's Quantum Factoring Algorithm on a Photonic Chip. *Science*, 325(5945):1221–1221.

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887.