Student Presentation

Factorization of 15 on an NMR quantum computer

Based on

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

Motivation

- Prime Factorization
  - Classically $O(2^{l/3})$
  - Shor $O(l^3)$
- Factorization of large primes (such as encryption keys) feasible on an *ideal* quantum computer
- What about Shor's algorithm on actual quantum computers?

  $\Rightarrow$ 15 factorized using *compiled* algorithms
  - 2001: Nuclear spins on a molecule [1]
  - 2009: Photons integrated on a chip [2]
  - 2012: Phase of Josephson junctions [3]

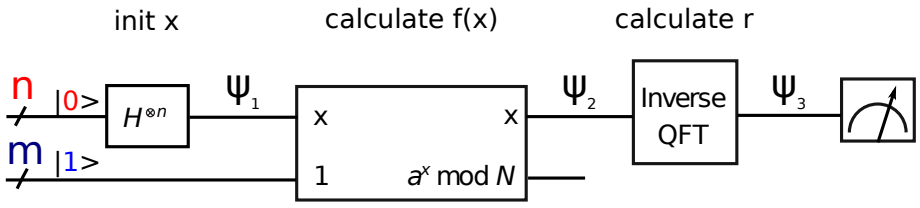
  $\Rightarrow$ as well as 21
  - 2012: Photons [4]

Factorization of 15 using Shor's algorithm

1. $f(x) = a^x \mod 15$
   - Possible $a = [2, \ , 4, \ , \ , 7, 8, \ , \ , 11, \ , 13, 14]$
2. Find period r in x of $f(x)$
   - $a^2 \mod 15 = 1$ for $a = [4, 11, 14]$
     $\Rightarrow r = 2$
   - $a^4 \mod 15 = 1$ for $a = [2, 7, 8, 13]$
     $\Rightarrow r = 4$
3. $\gcd(a^{\frac{r}{2}} \pm 1, 15)$
   - $\gcd(11^{\frac{2}{2}} \pm 1, 15) = [\gcd(10, 15), \gcd(12, 15)] = [5, 3]$
   - $\gcd(\ 2^{\frac{4}{2}} \pm 1, 15) = [\gcd(\ 3, 15), \gcd(\ 5, 15)] = [3, 5]$

$\Rightarrow$ Largest period of r is 4

Quantum Implementation



- Period finding in x by inverse QFT
- Parallelization
  - Qbits in superposition states to store x and $f(x)$
  - Exponential scaling of Hilbert space

⇒ Classically exponential problem runs in polynomial time

Example:
N = 15, a = 11 ⇒ r = 2
3 qbits for n, 4 qbits for m

$$\psi_1 \propto |0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle$$

$$\begin{aligned}\psi_2 \propto\ & |0\rangle|1\rangle + |1\rangle|11\rangle + |2\rangle|1\rangle + |3\rangle|11\rangle \\ & + |4\rangle|1\rangle + |5\rangle|11\rangle + |6\rangle|1\rangle + |7\rangle|11\rangle \\ =\ & \{|0\rangle + |2\rangle + |4\rangle + |6\rangle\}|1\rangle \\ & + \{|1\rangle + |3\rangle + |5\rangle + |7\rangle\}|11\rangle\end{aligned}$$

$$\begin{aligned}\psi_3 \propto\ & \{|0\rangle + |4\rangle\}|1\rangle \quad | \text{ delta comb} \Leftrightarrow \text{delta comb} \\ & + \{|0\rangle - |4\rangle\}|11\rangle \quad | \text{ sample shift} \Leftrightarrow \text{linear phase}\end{aligned}$$

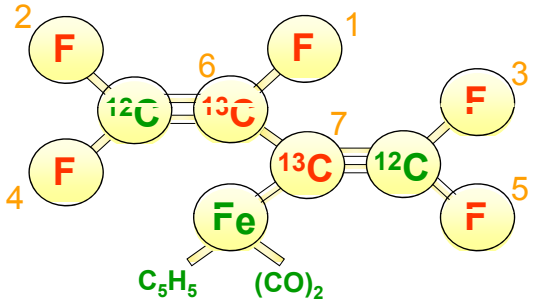
Readout of ψ_3 on n results in superposition of $|0\rangle$ and $|4\rangle$, i.e. $|000\rangle$ and $|100\rangle$

see also lecture notes (the last few slides, but values above for m represent actual f(x) value.)

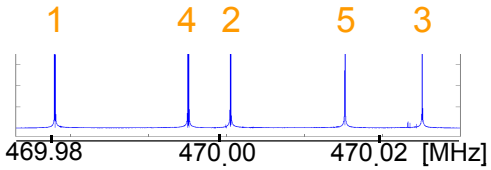
NMR Quantum Computation

Basics [5]

- Qbits
  - Ensemble of distinguishable and coupled nuclear spins
  - Coherence times > 1 sec
  - Highly mixed ground state, $\frac{\Delta E}{kT} \ll 1$
- Gates
  - Single Qbit
    - Spin-selective RF pulses, σ_x, σ_y or combination, 0.2 - 2 ms (and composite σ_z)
  - Double Qbit
    - Controlled phase by evolution under J for $t = \frac{1}{2J} \approx 5 - 10$ ms
- Readout
  - Weak ensemble measurement of σ_x and σ_y

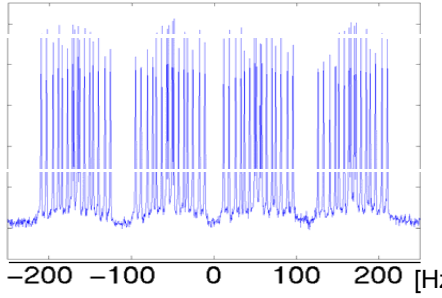


F spectrum



→ Zeeman terms + chem. shift

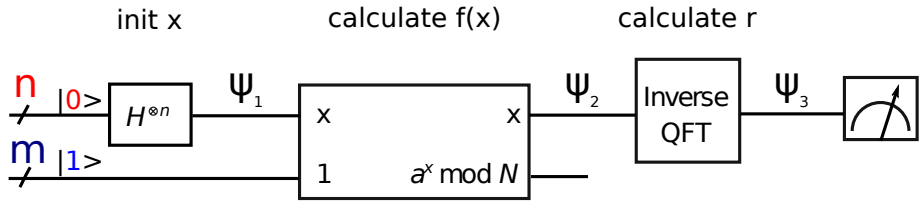
J couplings on 1

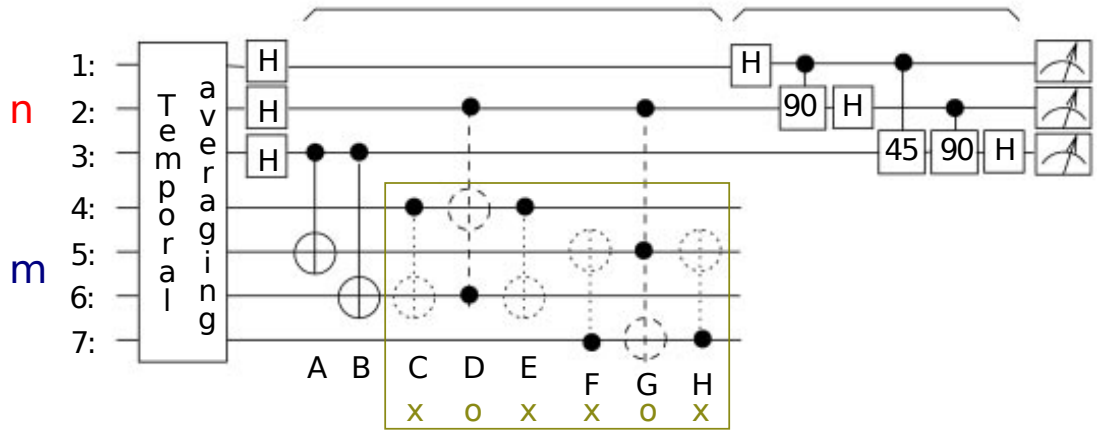


→ Interspin terms

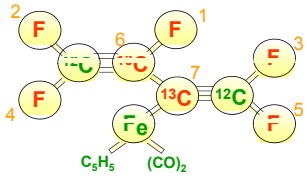
Quantum Circuit for NMR

- Qbit assignment (N = 15)
  - $r_{max} = 4$ requires $x = 0...3$
  - ⇒ 2 qbits for n sufficient, 3 qbits chosen for exp
  - m requires $\lceil \log_2(N) \rceil$ qbits
- Initialization
  - Temporal averaging for pseudopure state
- Optimizations
  - Gates reduced for $f(x) = a^x \mod N$
  - ⇒ compiled circuits for $a = 11$ and $a = 7$

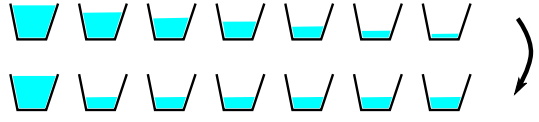




Specific optimizations to reduce gates



Temporal averaging: Creation of pseudopure state

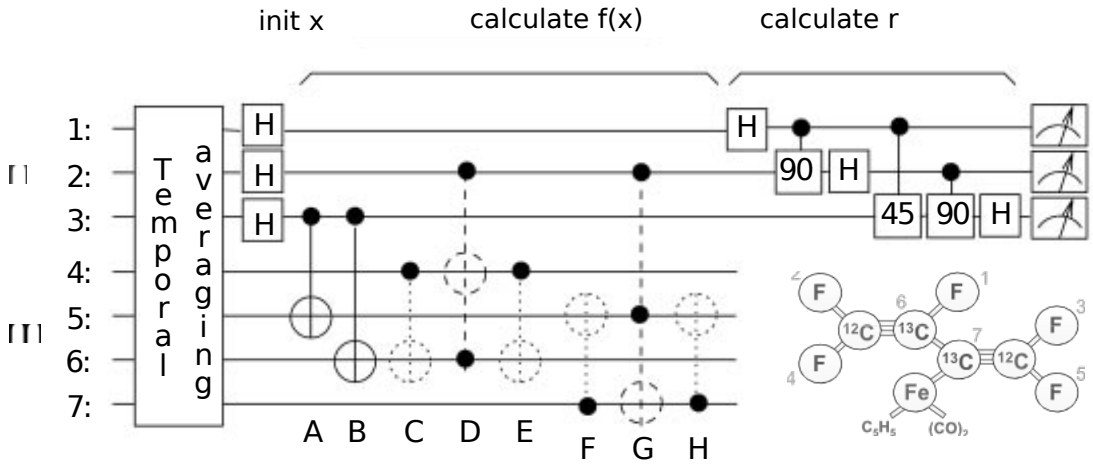


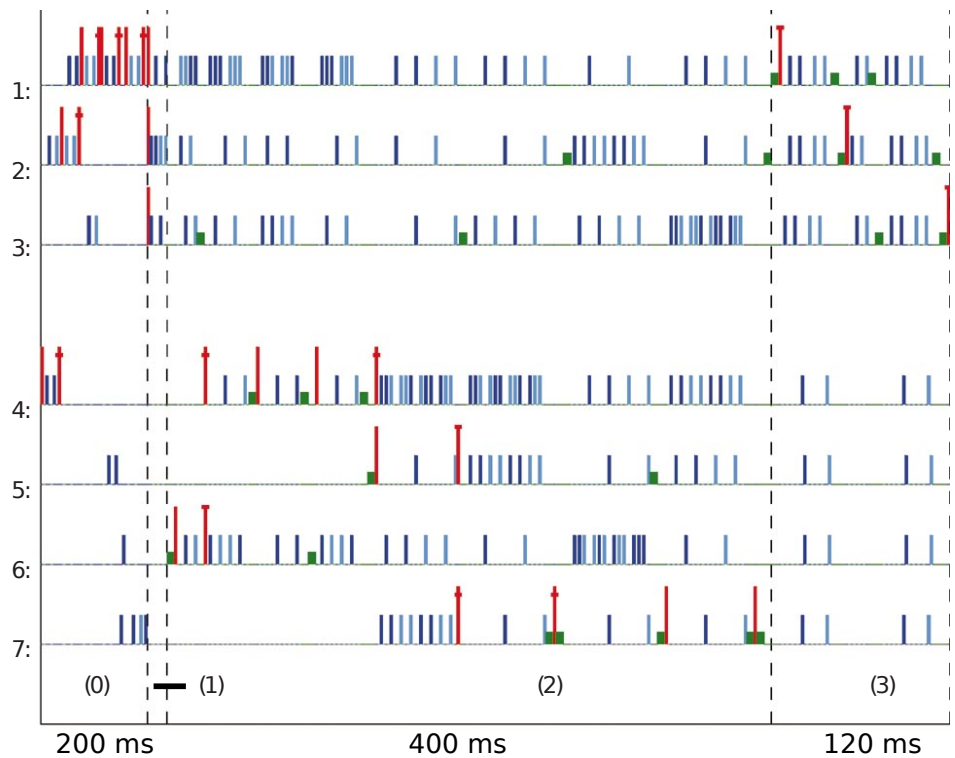
qbit swapping + averaging

36 x

Pulse Sequence

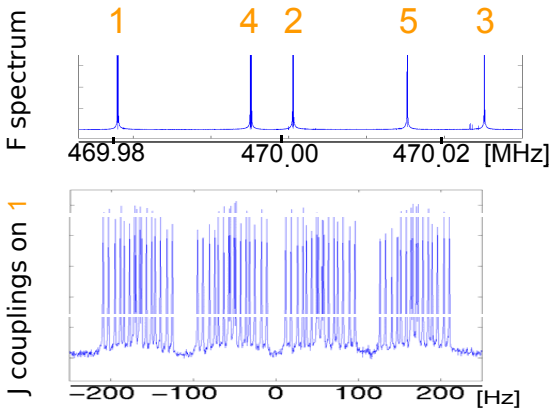
- 300+ pulses
  - $\frac{\pi}{2}$-pulses
    - Gaussian-shaped profile
    - Compensation of J
    - $\Rightarrow$ Selective excitation
    - either H or CNOT = H-CPHASE-H
  - π-pulses
    - Hermite-shaped profile
    - Compensation of J
    - $\Rightarrow$ Selective refocusing
    - to rewind J, where unwanted
  - z-rotations
    - Used for f(x) and iQFT





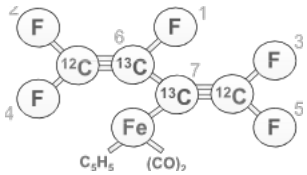
Pulse Sequence

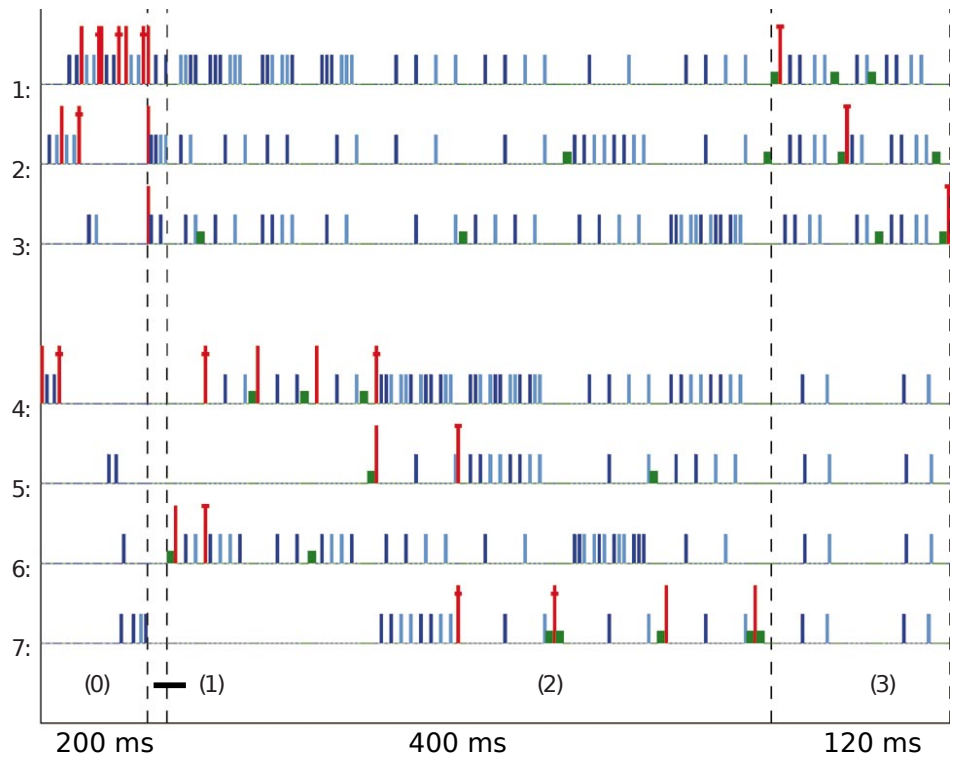
- 300+ pulses
  - $\frac{\pi}{2}$-pulses
    - Gaussian-shaped profile
    - Compensation of J
    - $\Rightarrow$ Selective excitation
    - either H or CNOT = H-CPHASE-H
  - π-pulses
    - Hermite-shaped profile
    - Compensation of J
    - $\Rightarrow$ Selective refocusing
    - to rewind J, where unwanted
  - z-rotations
    - Used for f(x) and iQFT



→ J refocused during free evolution

→ J compensated under RF pulse





Results for $a = 11$

Expected result:

$$\psi_2 \propto \{|0\rangle + |2\rangle + |4\rangle + |6\rangle\}\,|1\rangle + \{|1\rangle + |3\rangle + |5\rangle + |7\rangle\}\,|11\rangle$$

$$\psi_3 \propto \{|0\rangle + |4\rangle\}\,|1\rangle + \{|0\rangle - |4\rangle\}\,|11\rangle$$

Analysis of Spectra:

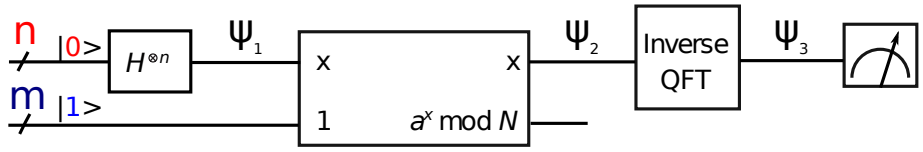
For two spins I and S in pseudo-pure states a and b, upon a $\frac{\pi}{2}$ pulse to I

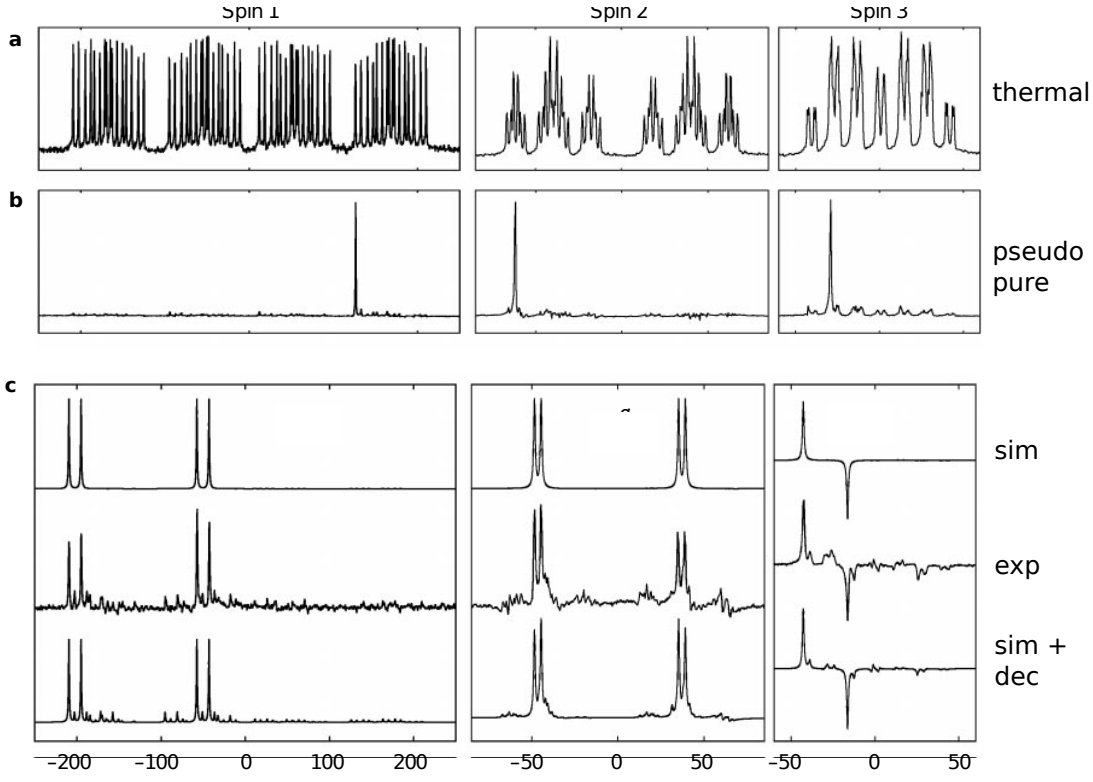
$$obs \propto (-1)^a (I_x + (-1)^b 2 I_x S_z)$$

$\Rightarrow$ spectral phase reveals state of observer spin
$\Rightarrow$ actual spectral line depends on state of coupled spin

here: several spectral peaks due to multiple spins
detection of observer spin state via spectral phase

$\Rightarrow$ desired superposition of $|000\rangle$ and $|100\rangle$, i.e. $|0\rangle$ and $|4\rangle$
+ artefacts





Results for $a = 7$

Expected result:

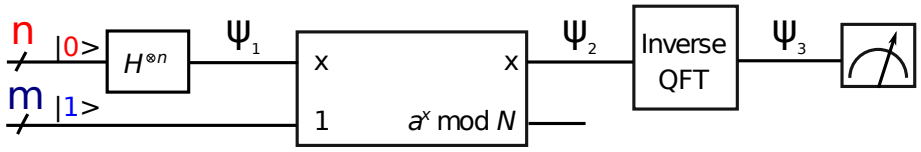
$$\psi_2 \propto \{|0\rangle + |4\rangle\}|1\rangle + \{|1\rangle + |5\rangle\}|7\rangle + \{|2\rangle + |6\rangle\}|4\rangle + \{|3\rangle + |7\rangle\}|13\rangle$$

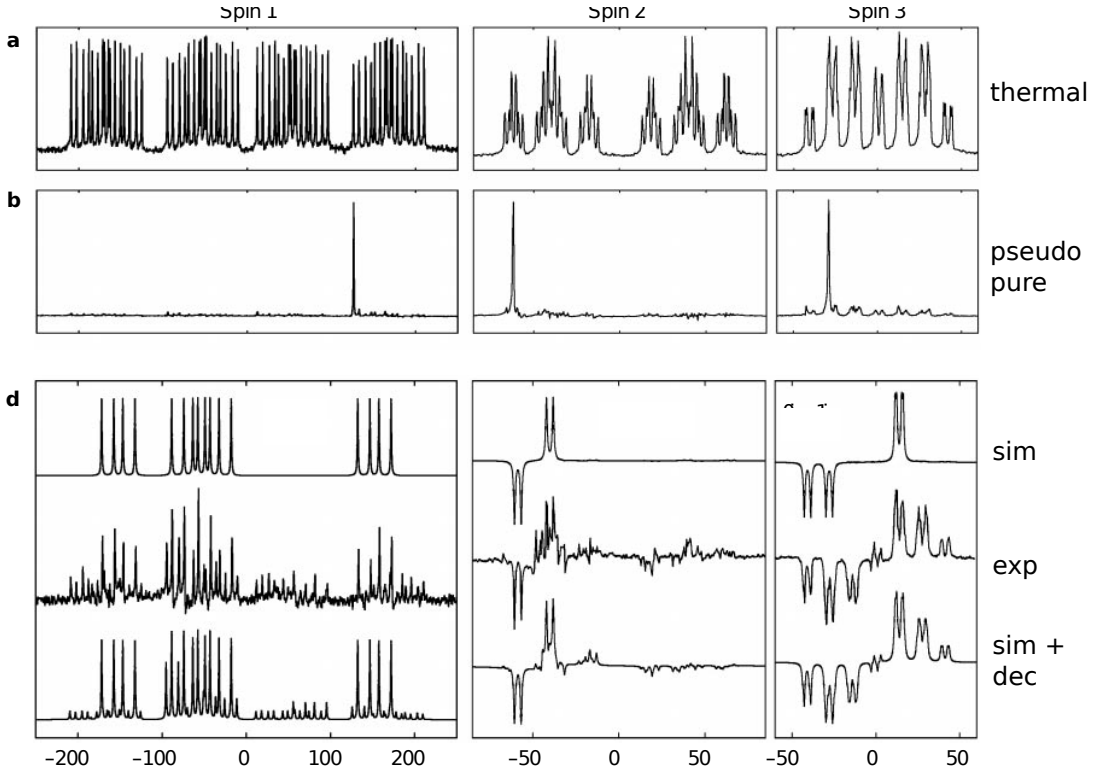
$$\psi_3 \propto \{|0\rangle + |2\rangle + |4\rangle + |6\rangle\}|1\rangle + \{|0\rangle - i|2\rangle - |4\rangle + i|6\rangle\}|7\rangle + \{|0\rangle - |2\rangle + |4\rangle - |6\rangle\}|4\rangle + \{|0\rangle + i|2\rangle - |4\rangle - i|6\rangle\}|13\rangle$$

Analysis of Spectra:

detection of observer spin state via spectral phase

$\Rightarrow$ desired superposition of
$|000\rangle$
$|010\rangle$
$|100\rangle$
$|110\rangle$
i.e. $|0\rangle$, $|2\rangle$, $|4\rangle$, $|6\rangle$
+ even more pronounced artefacts





Summary

- Successful *in-principle* demonstration
- Calculation of $f(x) = a^x \mod N$ expensive

$\Rightarrow$ Compiled/optimized algoritm, based on known a and r

- Simplest case already prone to decoherence

$\Rightarrow$ Experimental realization very demanding

- Main reasons:
  - Number of qbits
    - $3\log_2(N)$ for full-scale implementation
  - Number of gates
    - $n(n+1)/2$ for iQFT
      plus way more for modular exponentiation

(Factorization of N = 21 using photons [4] was achieved by an iterative decomposition of the iQFT. The execution time was therefore increased, whereas only one qbit was required for n)

References

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

[2] A. Politi, J. C. F. Matthews, J. L. O'Brien, Shors quantum factoring algorithm on a photonic chip, Science 325 (5945) (2009) 1221.

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

[4] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, J. L. O'Brien, Experimental realization of Shor's quantum factoring algorithm using qubit recycling, Nat Photon 6 (2012) 773 – 776.

[5] J. A. Jones, Quantum computing with NMR, Prog Nucl Magn Res Sp 59 (2) (2011) 91 – 120.

Figures adopted from [1] or lecture slides

Questions?