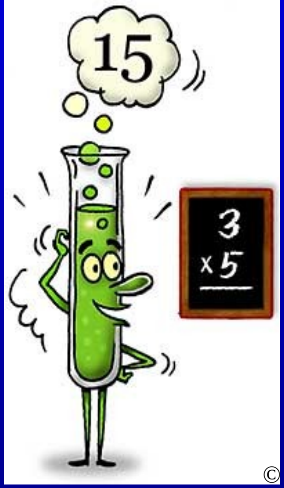
Experimental Realization of Shor's Quantum Factoring Algorithm[‡]



M. Steffen[1,2,3], L.M.K. Vandersypen[1,2], G. Breyta[1], C.S. Yannoni[1], M. Sherwood[1], I.L.Chuang[1,3]

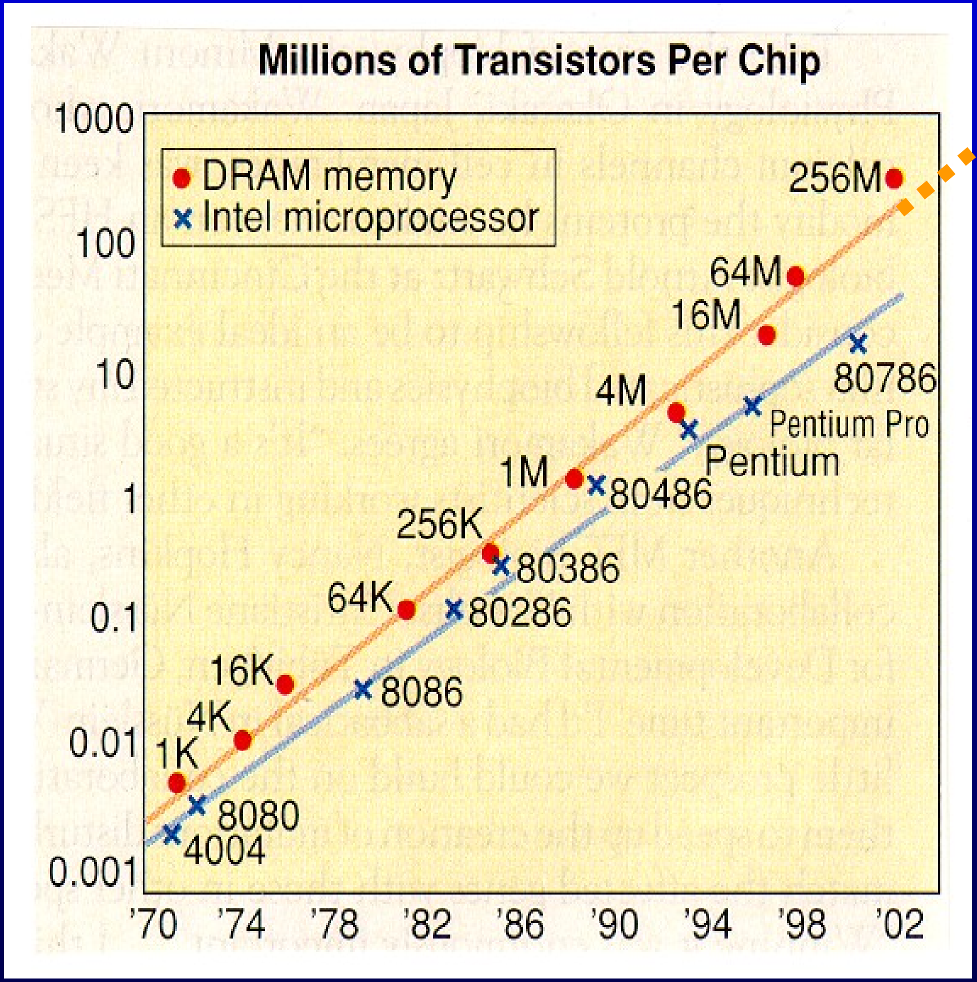
[1] IBM Almaden Research Center, San Jose, CA 95120
[2] Stanford University, Stanford, CA 94305
[3] MIT Media Laboratory, Cambridge, MA 02139

[‡]Vandersypen L.M.K, et al, *Nature*, v.414, pp. 883 – 887 (2001)

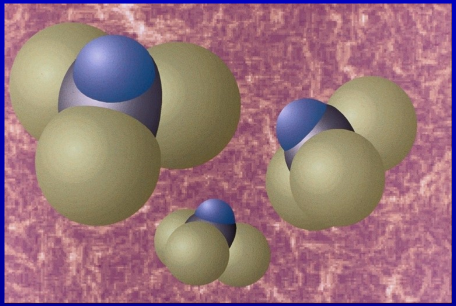
Outline

- 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



1bit = 1 atom ?



Can we exploit quantum mechanics for ultra-fast computation?

The promise of Quantum Computation

Searching databases[1]

- unsorted list of N entries
- how many queries?

$O(N)$ ⇨ $O(\sqrt{N})$

1 month — 27 minutes

Factoring Integers[2]

- N = pq
- N has L digits
- given N, what are p and q?

$O\left(e^{L^{1/3}}\right)$ ⇨ $O\left(L^{3}\right)$

10 billion years — 3 years

400 digits

[1] L.K. Grover, *PRL*, **79**, 4709 (1997)

[2] P. Shor, *Proc. 35th Ann. Symp. On Found. Of Comp. Sci.*, p.124 (1994)

Classical vs. Quantum

<u>Classical bits</u>

- transistors
- 0 or 1

NAND, NOT, CNOT …

<u>Quantum bits</u>

- quantum systems
- 0 or 1or <u>in-between</u>

NAND, NOT, CNOT …
Sqrt(NOT) …

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

Quantum bits

One qubit: $\left|\psi_1\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$ $\qquad |a|^2 + |b|^2 = 1$

Multiple qubits: $\left|\psi_n\right\rangle = a_0\left|00...0\right\rangle + a_1\left|00...1\right\rangle + a_{2^n}\left|11...1\right\rangle$ $\qquad \sum_i |a_i|^2 = 1$

Evolution of quantum states:

Conservation of probabilities allows only reversible, unitary operations

$\left|\psi_{n,out}\right\rangle = U\left|\psi_{n,in}\right\rangle$ $\qquad$ U is a 2^n x 2^n 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:*

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

Parallel operation, BUT a measurement collapses the wave function to only one of the states with probability $|a_i|^2$

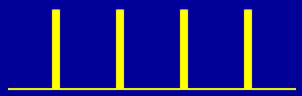
$\Rightarrow$ Need to design clever algorithms

Quantum Algorithms

Example: 2 qubit Grover search

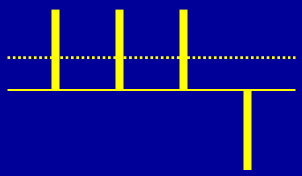
1. Create equal superposition

$$|\psi\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$



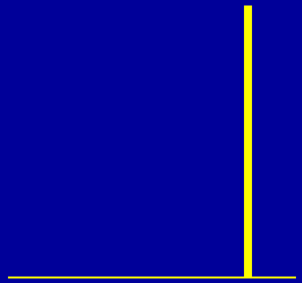
2. Mark special element

$$|\psi\rangle = |00\rangle + |01\rangle + |10\rangle - |11\rangle$$



3. Inversion about average

$$|\psi\rangle = |11\rangle$$



One query = marking & inversion

In general, need √N queries

Physical Realization of QCs

Requirements for Quantum Computers[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

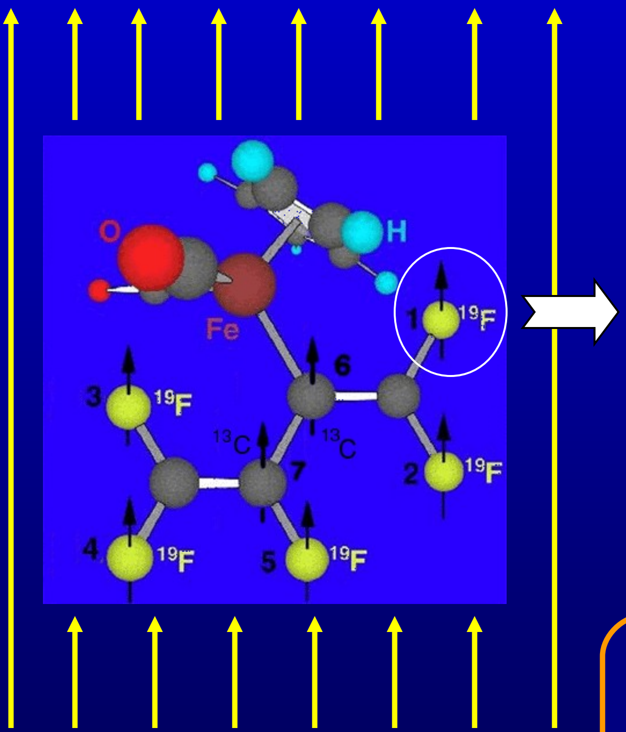
Meeting all of these requirements *simultaneously* presents a significant experimental challenge.

⇒ <u>Nuclear Magnetic Resonance (NMR) techniques</u> largely satisfies these requirements and have enabled experimental exploration of small-scale quantum computers

[1] DiVincenzo D.P., *Fortschr. Physik*, **48** (9-11), 771 – 783 (2000)

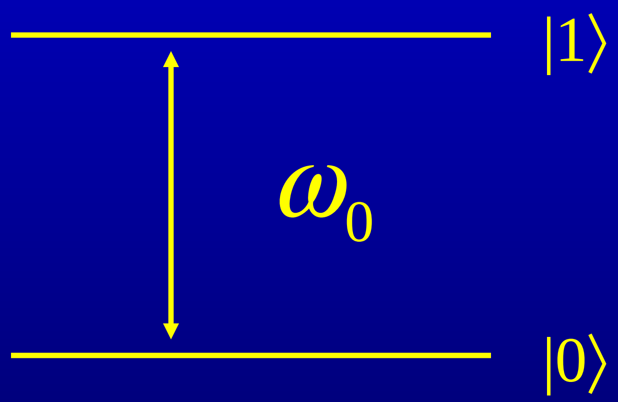
NMR Quantum Computing [1,2]

$$\left|\psi_{out}\right\rangle = e^{-iHt}\left|\psi_{in}\right\rangle = U\left|\psi_{in}\right\rangle$$ ⇨ Characterize all Hamiltonians



B_0

spin ½ particle in magnetic field:



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

[1] Gershenfeld, N. et al., *Science*, **275**, 350 – 356 (1997)
[2] Cory D. et al., *Proc. Natl. Acad. Sci.*, **94**, 1634 – 1639 (1997)

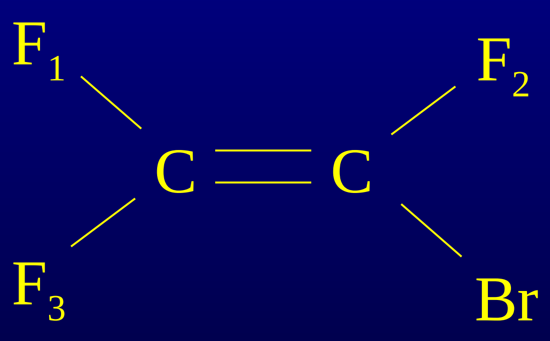
Multiple spin ½ nuclei

Heteronuclear spins:

nucleus	^{1}H	^{2}H	^{13}C	^{15}N	^{19}F	^{31}P
ω_0 [MHz]	500	77	126	-51	470	202

Homonuclear spins:

Chemical shift



nucleus	F_1	F_2	F_3
$\Delta\omega$ [kHz]	13	0	-9

$$\boxed{H_0 = -\sum_{i=1}^{n} \frac{\omega_0^i Z^i}{2}}$$

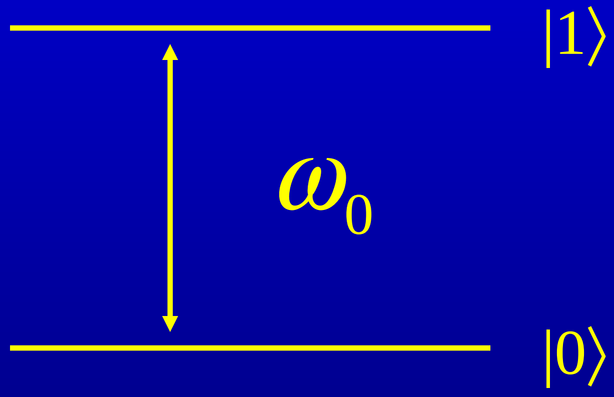
Spin-spin coupling

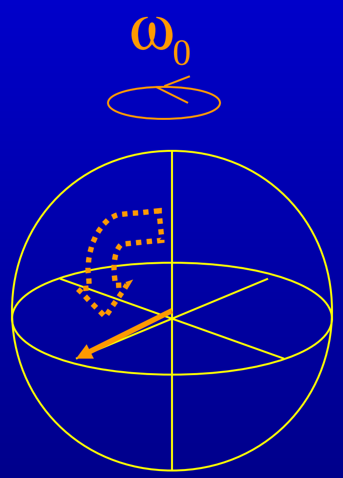
- Dipolar couplings (averaged away in liquids)
- J-coupling (through shared electrons)

$$H_J \approx \sum_{i<j}^{n} \frac{\pi J_{ij} Z^i Z^j}{2} \qquad H = -\sum_{i=1}^{n} \frac{\hbar \omega_0^i Z^i}{2} + \sum_{i<j}^{n} \frac{\pi J_{ij} Z^i Z^j}{2}$$

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 ω_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 $|1\rangle$

2-bit CNOT

Input	Output
00	00
01	01
10	11
11	10

Put video here

State initialization

Thermal Equilibrium: … highly mixed state

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

Effective pure state: … still mixed but:

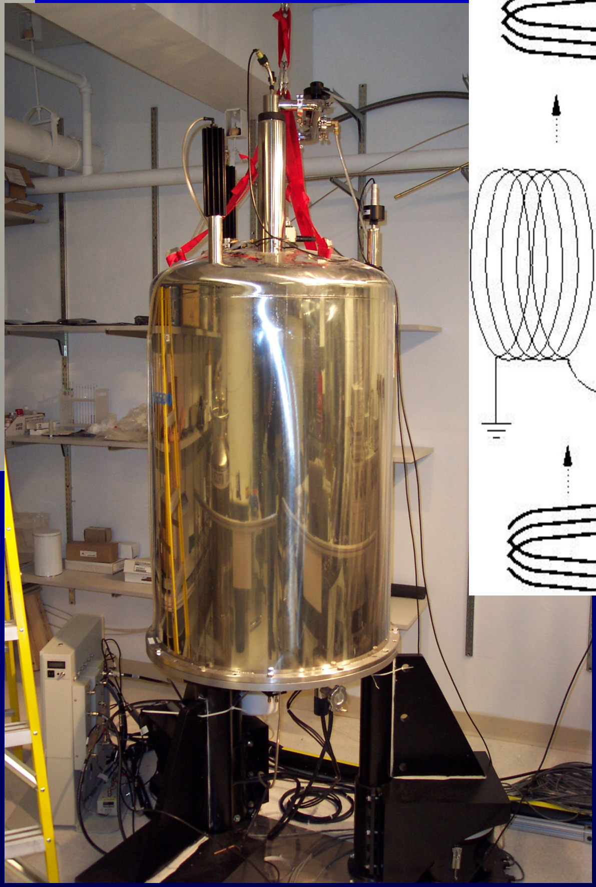
$$\rho_{eq} \propto I + \varepsilon |00\cdots0\rangle\langle00\cdots0|$$

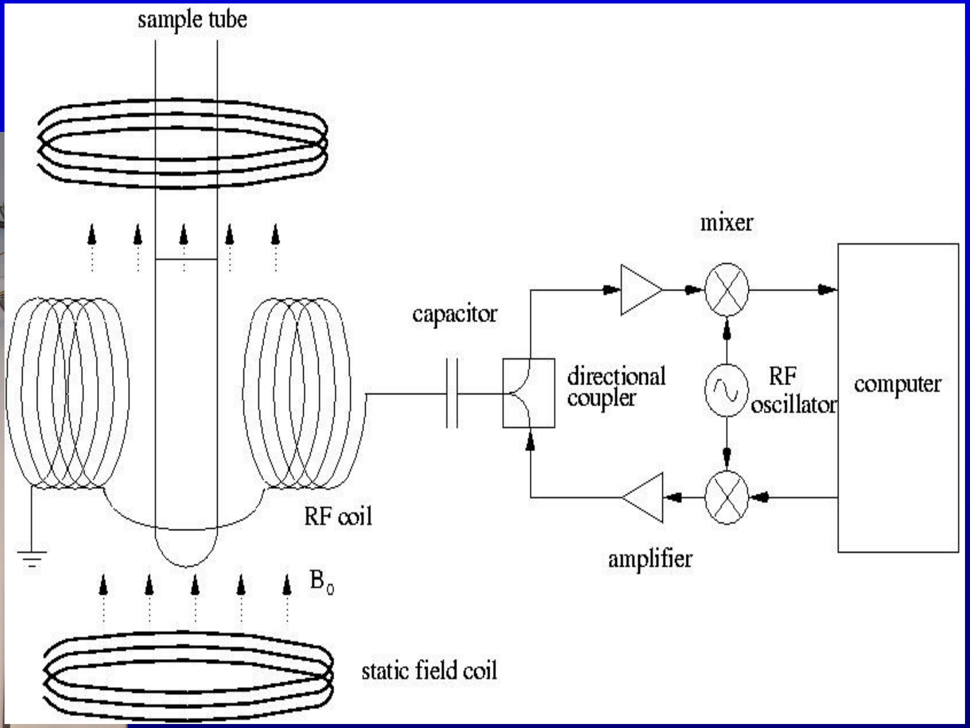
- Spatial Labeling
- Temporal Labeling
- Logical Labeling
- Schulman-Vazirani

$\Rightarrow$

a	b	c	d
a	c	d	b
a	d	b	c
3a	b+c+d	b+c+d	b+c+d

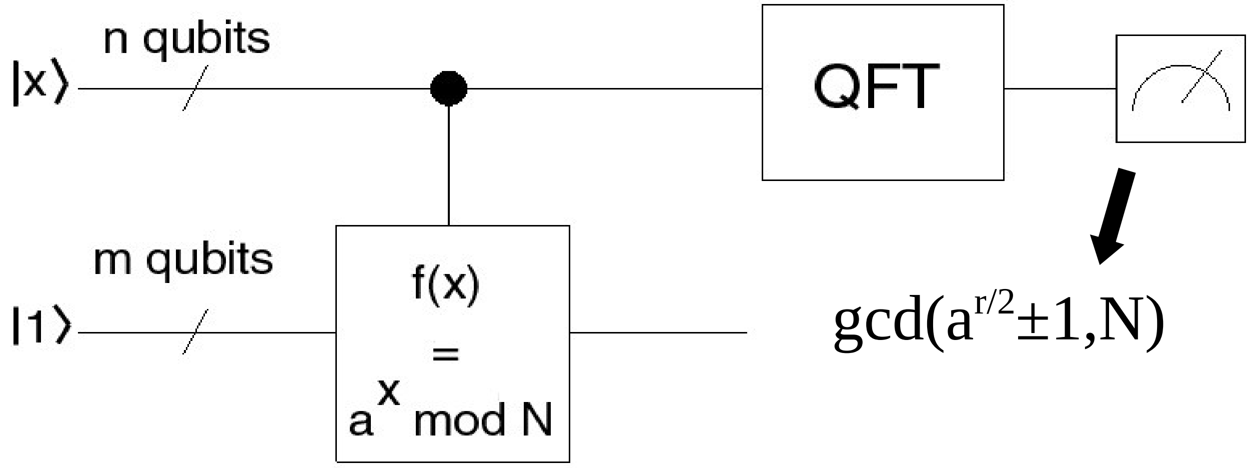
NMR Setup




sample tube
mixer
capacitor
directional coupler
RF oscillator
computer
RF coil
amplifier
B_0
static field coil

Shor's Factoring Algorithm

Quantum circuit to factor an integer 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

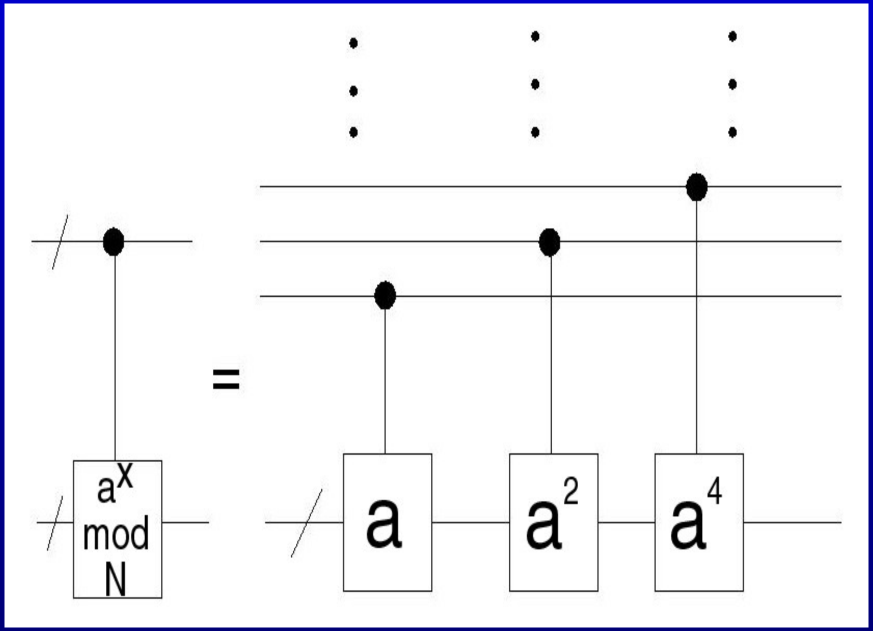
Shor's Factoring Algorithm

$a^x = a^{2^{n-1} x_{n-1}} \ldots a^{2 x_1} a^{x_0}$ where x_k are the binary digits of x.

a = 2, 7, 8, 13

$a^4 \bmod 15 = 1$

"hard case"



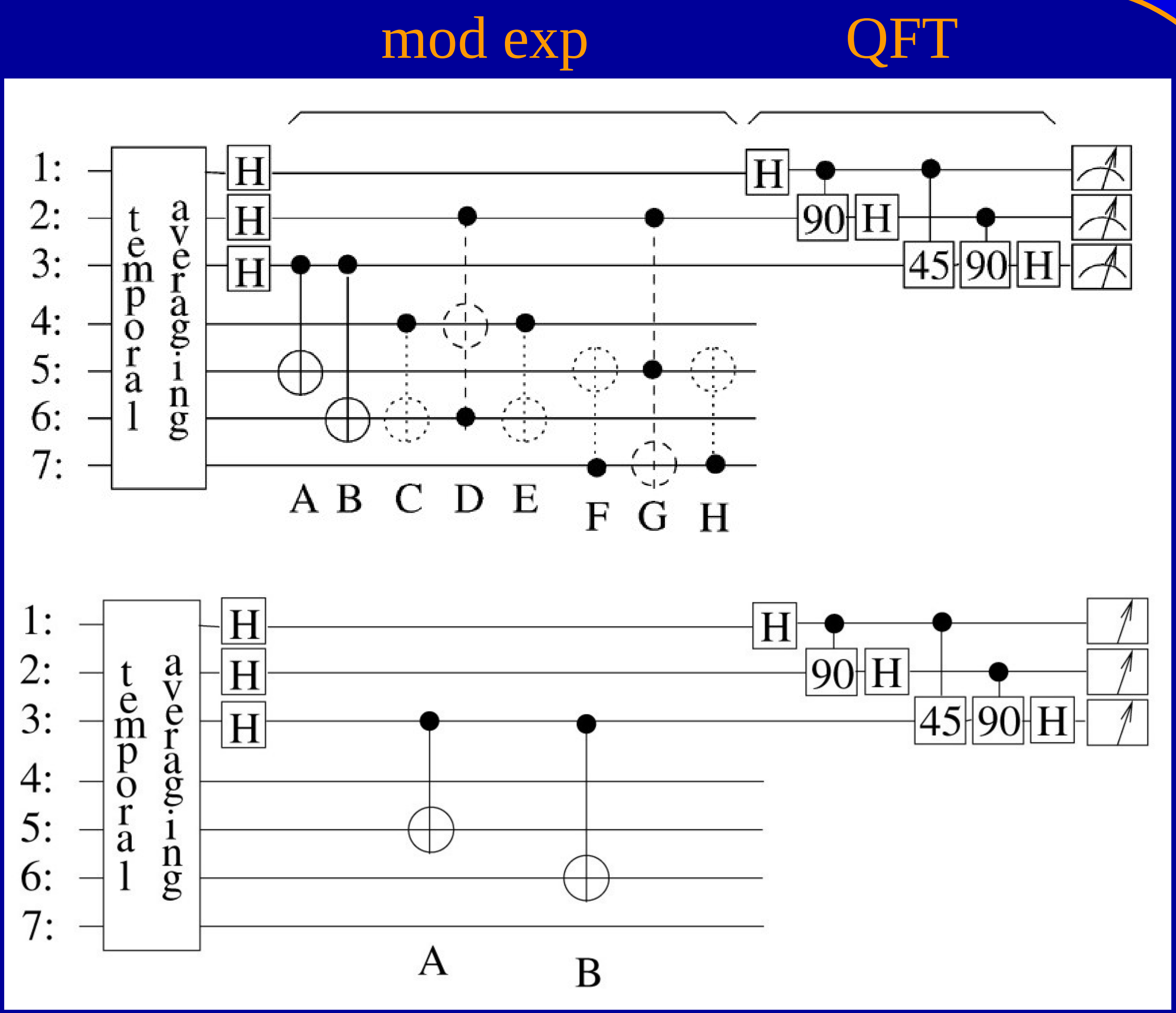
a = 4, 11, 14

$a^2 \bmod 15 = 1$

"easy case"

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

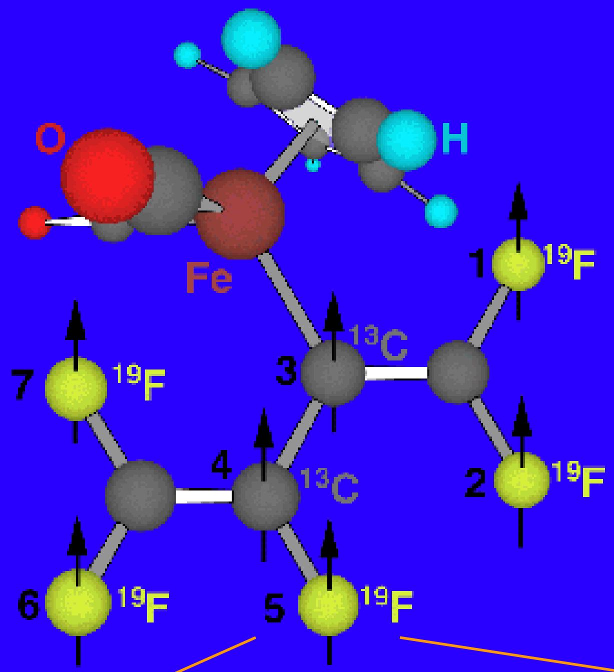
Factoring N = 15



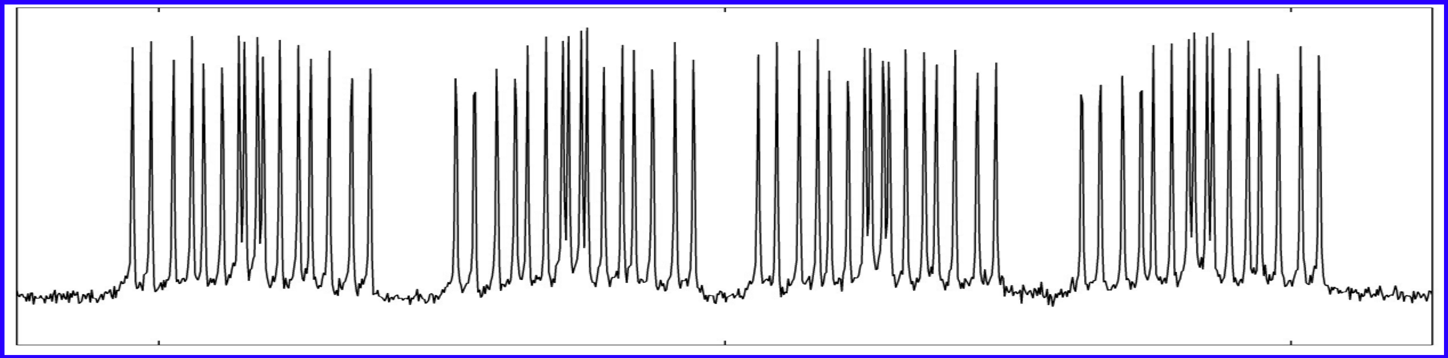
a = 7
'hard case'

a = 11
'easy case'

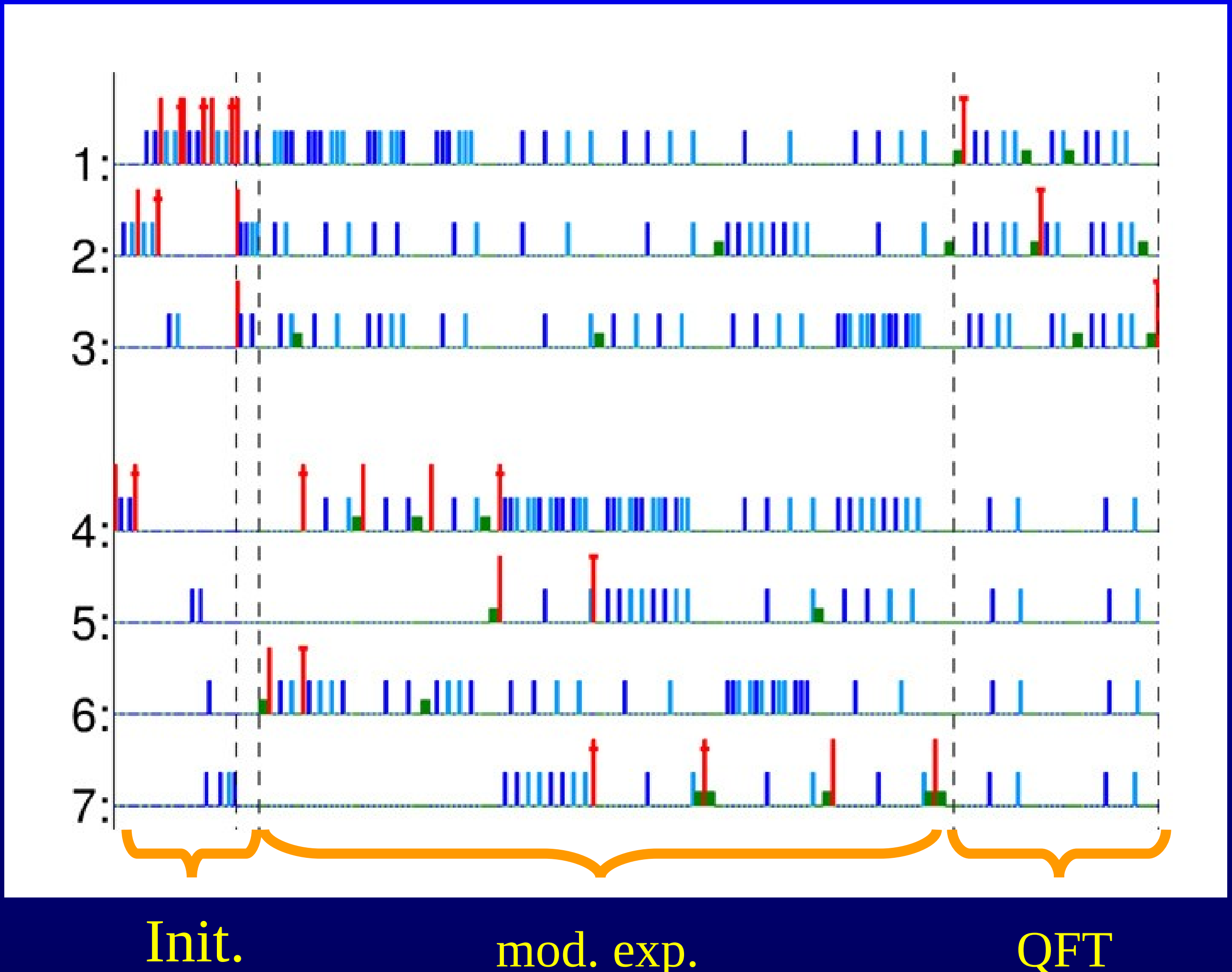
The molecule



i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	15186.6	2.8	1.8	2.1	2.5	6.6	19.4	59.5	41.6
2	25088.3	3.0	2.5	12.9	3.9	14.5	1.0	−13.5	
3	−4519.1	45.4	2.0	−5.7	−3.9	37.7	68.0		
4	4244.3	31.6	2.0	54.1	18.6	−221			
5	−22052	25.0	1.3	−114.3	25.16				
6	489.5	13.7	1.8	79.9					
7	−4918.3	10.0	1.7						



Pulse Sequence



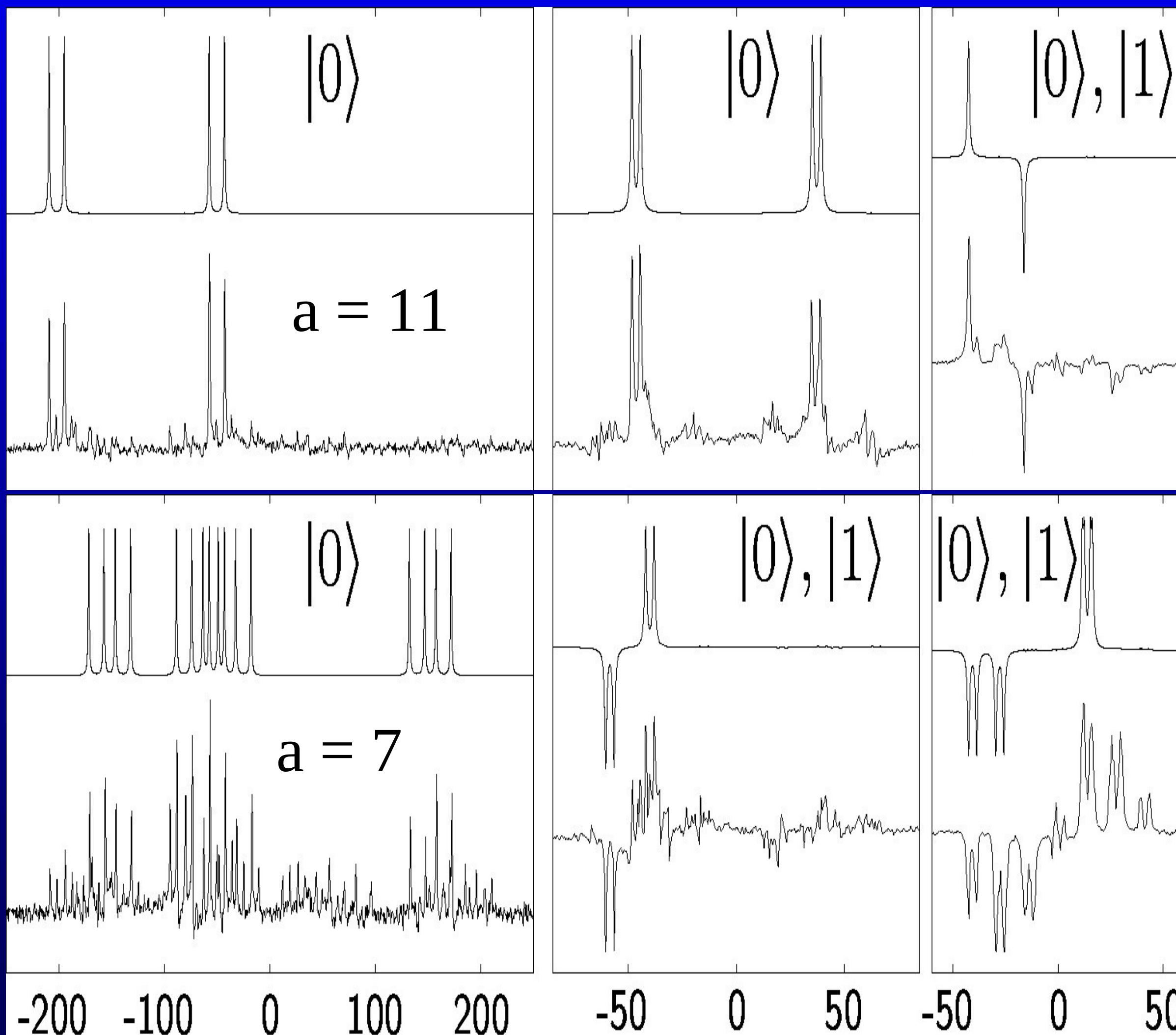
~ 300 RF pulses || ~ 750 ms duration

Experimental detail and innovations

- Modified state initialization procedure
- Gaussian shaped $\pi/2$ pulses (220 – 900 μs)
- Hermite 180 shaped π 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

[1] Steffen M., JMR, 146, 369 – 374 (2000)

Results: Spectra



qubit 3 qubit 2 qubit 1

Mixture of |0⟩,|4⟩
$2^3/4 = r = 2$
$\gcd(11^{2/2} \pm 1, 15) = 3, 5$

15 = 3 · 5

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

Results: Predictive Decoherence Model

Operator sum representation: $\rho \Rightarrow \sum_k E_k \, \rho \, E_k^{\dagger}$

Generalized Amplitude Damping

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

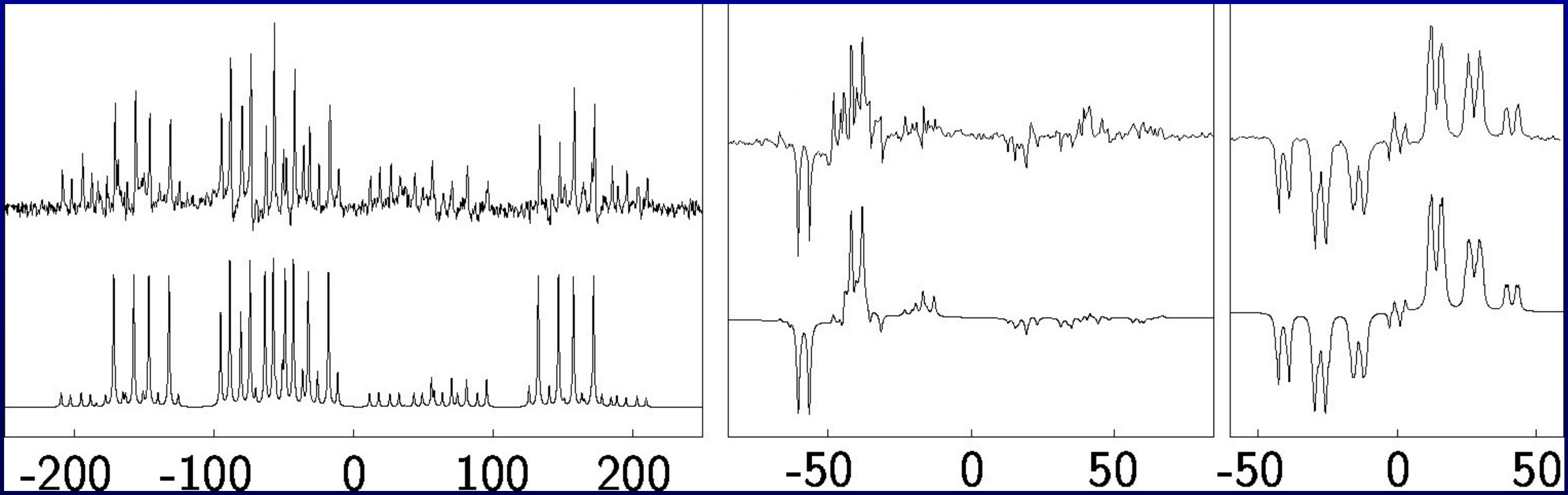
Phase Damping

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

Decoherence Model cont'd

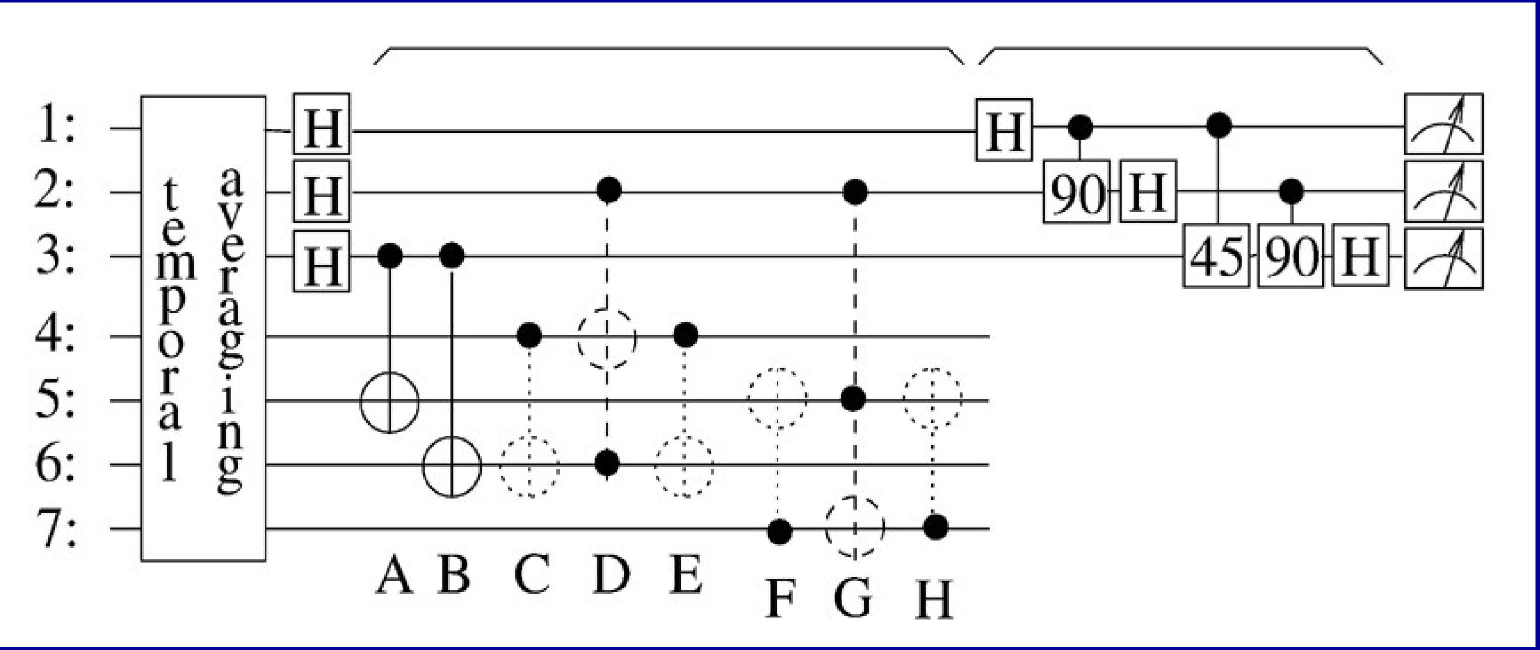
- GAD (and PD) acting on different spins commute
- E_k for GAD commute with E_k for PD on arb. Pauli matrices
- PD commutes with J-coupling, and z-rotations
- GAD (and PD) do *NOT* commute with RF pulses

- 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