QSIT Vortrag : Shor's Algorithm (Experimental Realization)

Kathrin Gerhard

1) Introduction

Paper:
→ first experimental realization of Shor's Algorithm using NMR techniques
→ By Vandersypen et al. at IBM Almaden Research Center, San Jose, California

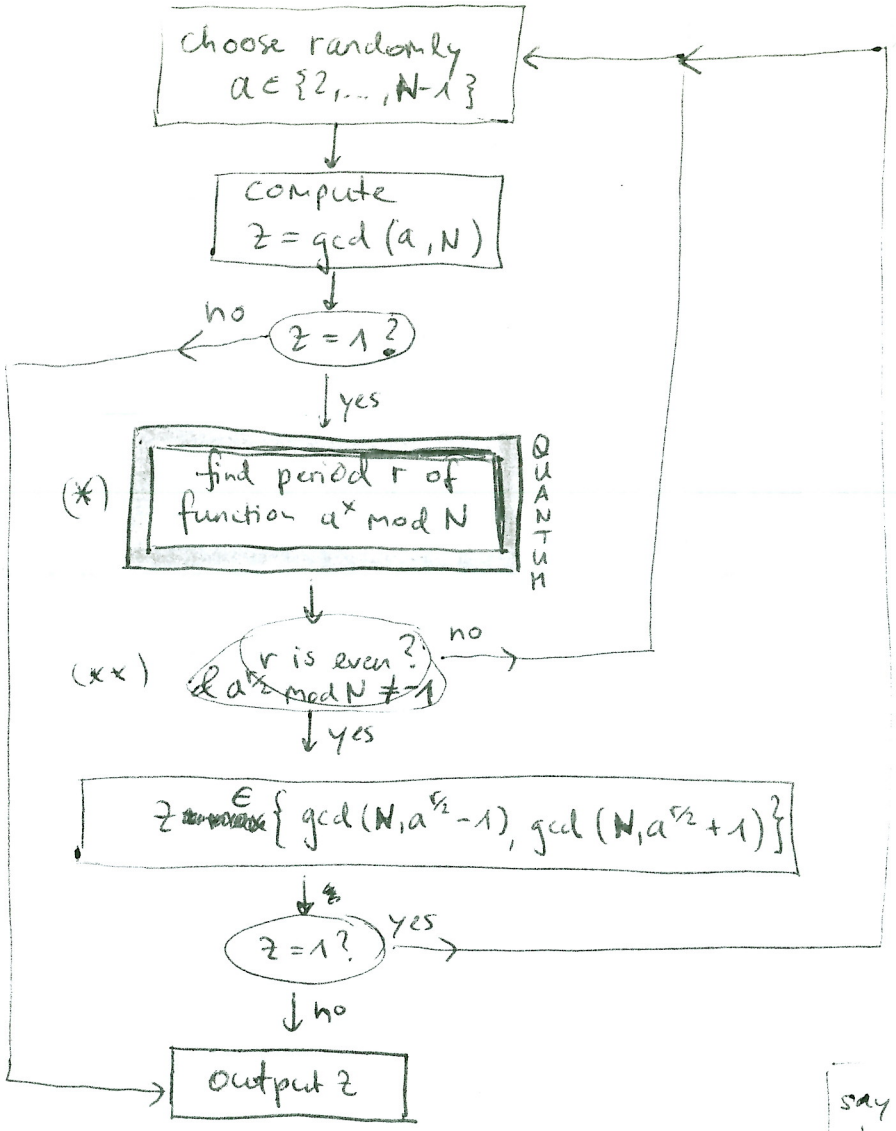
Factorizing integers → classically: $O(2^{L^{1/3}})$ exponential
→ quantum: $O(L^3)$ polynomial

→ paper gives implementation of simplest case: $N = 15$ to factorize.
using 7 qubits (spin-1/2 nuclei in a specific molecule)
where all experiments were performed at room temp.
and molecules solved in a liquid ("liquid state NMR")

→ Significance of NMR:
→ nuclear spins have long decoherence times (↔ couple little with environment)
→ could in principle use NMR qu. info. storage processes for large systems also
but though precise control needed, have again decoherence as the dominant source of error.

2. Shor's Algorithm

→ returns (with high probability) a nontrivial factor of any composite N



$\gcd(a,N) = 1$ $\hat{=}$ a, N "coprim"

→ computing gcd via the (classical) Euclid's Algorithm

say $a > b$. then $\gcd(a,b)$ determine by calculating k_1, r_1 s.t. $a = k_1 b + r$ and k_2, r_2 s.t. $b = k_2 r_1 + r_2$, etc up to some i for which $r_i = 0$. then s.t. and $\gcd(a,b) = \gcd(r_i,$ $= r_{i+1}$ ..

→ (*) order-finding subroutine:

$\hat{=}$ qu. algorithm to find the order of the function $a \bmod N$

order $\hat{=}$ the smallest possible integer r s.t. $a^r \bmod N = 1$

and thus $a^r = k \cdot N + 1$ for some k

$\Rightarrow a^{r+1} = k \cdot N \cdot a + a \Rightarrow a^{r+1} \pmod N = a \bmod N$

and r is the period of $f_N(x) = a^x \bmod N$, i.e.

$$f_N(x+r) = f_N(x)$$

Note: this shows ($r \leq N$) because $f_N(x)$ cannot assume more than N different values before repeating

→ (**) r even & $a^{r/2} \bmod N \neq -1 \Rightarrow \exists$ one nontrivial factor of N!

proof $y := a^{r/2}$

$y^2 \bmod N = a^r \bmod N = 1 \Rightarrow y^2 - 1$ is devided by N,

i.e., $(y+1)(y-1)$ is devided by N

⇒ N must have a common factor with $y+1$ or $y-1$

but this factor can't be N, since $y \bmod N \neq -1$

⇒ neither $y+1$ nor $y-1$ is a multiple of N

(if it were, then $a^{r/2} \bmod N = 1$ and the order would be $\frac{r}{2}$, not r)

⇒ the common factor we are looking for must be $\in \{\gcd(N, a^{r/2}+1), \gcd(N, a^{r/2}-1)\}$!!

Note:

Any step but the order-finding step can be efficiently performed on a classical computer!

→ that is why, when implementing Shor's Algorithm, the crucial part is to give an (quantum!) implementation of the order-finding subroutine. Once this has been achieved, we are done!

Note also: For $N = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ $(m \geq 2)$, i.e., N is a "odd composite number", from number theory:

$$\Pr(r \text{ even and } a^{r/2} \bmod N \neq -1) \geq 1 - \frac{1}{2^m} \geq \frac{3}{4}$$

⇒ for each time we calculate the order of $a \bmod N$, we have a chance of better than 75% to find a non-trivial prime factor of N!

→ chance of finding a prime factor (if one exists!) can thus be arbitrarily close to 1

→ still: Shor's alg. is a probabilistic algorithm ...

3. Quantum Circuit of the Order-finding algorithm

3.1 Brief Review of Quantum Fourier Transform (QFT)

→ have ONB $|0\rangle, \dots, |N-1\rangle$

→ QFT is defined to be a linear operator that acts like

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i jk}{N}} |k\rangle \quad , j = 0, \dots, N-1$$

on the basis states $|j\rangle = |j_1, j_2, \dots j_n\rangle$ if we take $N = 2^{(n)}$ ← some integer

↑ binary repr. ($\rightarrow j = j_1 2^{n-1} + \dots + j_n 2^0$)

→ action on arbitrary state:

$$\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{QFT} \sum_{k=0}^{N-1} y_k |k\rangle \quad \text{with} \quad y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i jk}{N}}$$

↑ Fourier transformed of amplitudes x_j

discrete Fourier transform of a vector of complex numbers $x_0, \dots, x_{N-1}$ (length N, fixed)

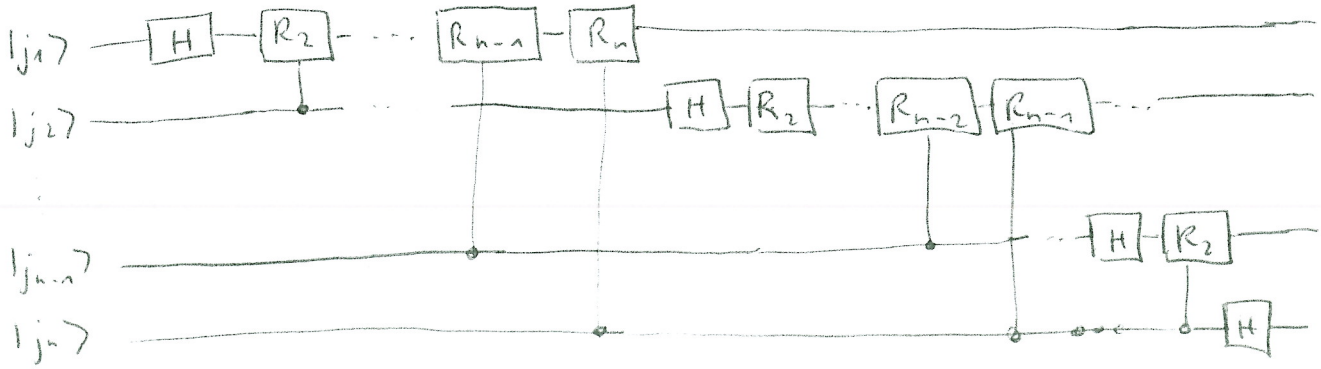
→ Notation: $0.j_\ell j_{\ell+1} \cdots j_m = \frac{j_\ell}{2} + \frac{j_{\ell+1}}{4} + \dots + \frac{j_m}{2^{m-\ell+1}}$ "binary fraction"

→ arrive at

product representation of QFT

$$|j_1, \dots j_n\rangle \longrightarrow \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

→ makes it easy to implement (rough picture)



with $R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$

Note: Swap operations (not shown) are used to reverse the order of the qubits ...

(see Nielsen & Chuang for details)

3.2. Phase Estimation

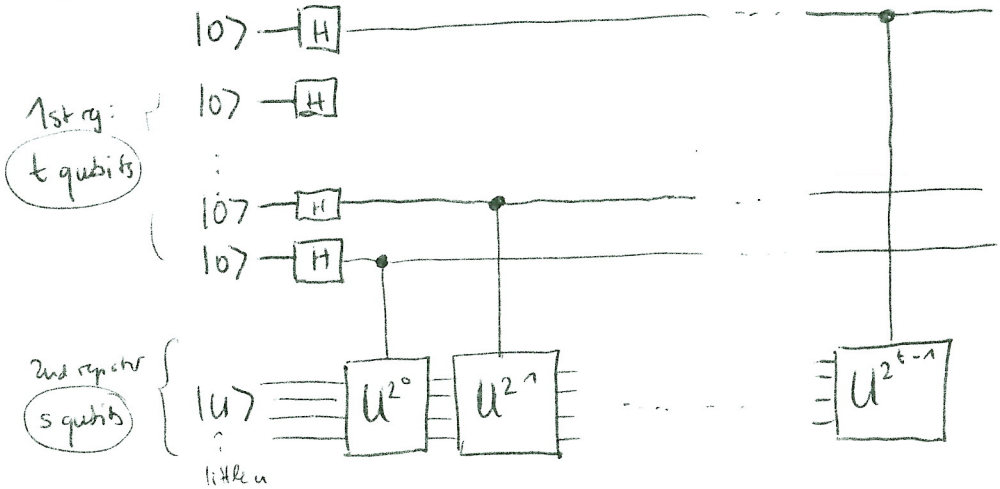
→ **The Problem:** Suppose unitary operator U has eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$, φ unknown. (i.e. $U|u\rangle = e^{2\pi i\varphi}|u\rangle$)

→ **Goal:** estimate φ!

→ **Assumption:** have ideal "black boxes" capable of preparing the state $|u\rangle$ and performing the controlled U^{2^j} operation (for suitable $j \geq 0$ integer)

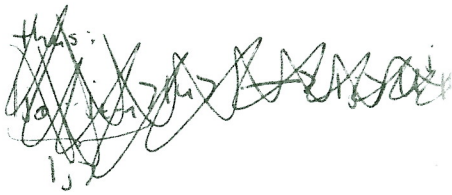
↝ in applications of this procedure, a description of how these black boxes operations are performed is given

→ **Circuit: First part:**



→ apply H transform to first register

→ apply controlled-U operations on the second register



note: t depends on # of digits of accuracy we wish to have in our estimate for φ
& with what prob. we wish the phase estim. procedure to be successful
s = # qubits necessary to store $|u\rangle$

final state of first register:

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} |k\rangle \qquad (\Delta)$$

→ ideal case

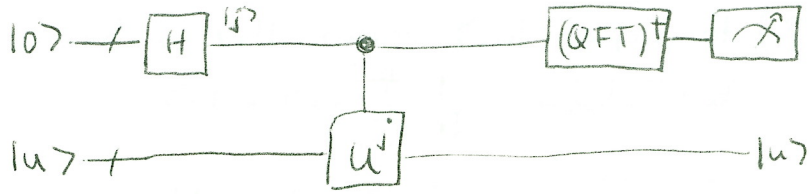
suppose $\varphi = 0.\varphi_1 \cdots \varphi_t$ (i.e., φ may be expressed in exactly t bits)

then (Δ) is just $\frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i \cdot 0.\varphi_t}|1\rangle\right) \otimes \cdots \left(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\cdots\varphi_t}|1\rangle\right)$

which is just the Fourier transformed state of a state $|\varphi_1 \ldots \varphi_t\rangle$!

⇒ applying the inverse FT gives us the phase $|\varphi\rangle$!!

→ the whole circuit for phase estimation:



and $\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \varphi j} |j\rangle |u\rangle \xrightarrow{QFT^\dagger} |\tilde{\varphi}\rangle |u\rangle$

↑
state that is a good estimator for φ when measured.
(even if φ not expressable in exactly t bits...)
→ see Nielsen/Chuang for details

($|\tilde{\varphi}\rangle = |\varphi\rangle$ in ideal case)

3.3. Order-finding algorithm

→ remender: want to find r s.t. $a^r \pmod N = 1$ for $a < N$ given.
↑ ↑
coprime.

→ $M = \lceil \log N \rceil$ = # bits needed to specify N → 2nd register
= # qubits initialized to $|1\rangle$
→ $n = 2\lceil \log N \rceil + 1$ = # qubits initialized to $|0\rangle$ → 1st register

here: $U = a \bmod N$
now:
and $U|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle$ with $|u_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |a^k \bmod N\rangle$

for $s = 0, \ldots, r-1$

→ so the quantum algorithm for order-finding is just the phase estimation algorithm applied to the unitary operator $U = a \bmod N$ with $U|y\rangle = |a\, y \pmod N\rangle$, $y \in \{0,1\}^m$ ($|y\rangle$ = state of target bits)

→ allows us to obtain, with high accuracy, the corresponding eigenvalues $e^{\frac{2\pi i s}{r}}$ from which we can obtain r.

→ need: 1) efficient procedure to implement a controlled-U^{2^j} operation for any j

oh! can use modular exponentiation

↳ see later with example how it works

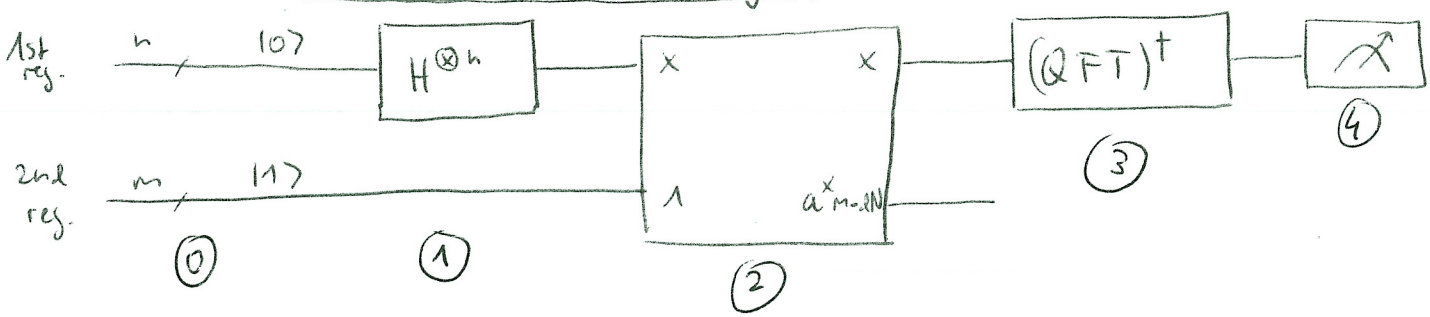
2) to prepare $|u_s\rangle$ requires that we know r → impossible.

but: observe: $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$

so: using $n = 2\lceil \log N \rceil + 1$ qubits in 1st register and prepare the second register in the state $|1\rangle$, it follows that

for each s $(0 \le s \le r-1)$ we will obtain an estimate of the phase $\varphi \approx \frac{s}{r}$

Algorithm: Quantum Order-Finding:



Inputs: a) black box $U_{a,N}$ performing $|j\rangle|k\rangle \to |j\rangle|a^j k \bmod N\rangle$

b) $n = 2\lceil \log N \rceil + 1$ qubits initialized to $|0\rangle$

$m = \lceil \log N \rceil$ qubits initialized to $|1\rangle$

Output: the least integer $r > 0$ s.t. $a^r = 1 \pmod N$.

Runtime: $O(n^3)$ operations. Succeeds with probability $O(1)$.

Procedure:

(0) initial state → $|0\rangle|1\rangle$

(1) create superposition → $\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|1\rangle$

(2) apply $U_{a,N}$ → $\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|a^j \bmod N\rangle \approx \frac{1}{\sqrt{r2^n}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^n-1} e^{\frac{2\pi i s j}{r}} |j\rangle|u_s\rangle$

(3) $(QFT)^\dagger$ to 1st register → $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{s/r}\rangle|u_s\rangle$

(4) measure first register (measure y) → $\tilde{s/r}$

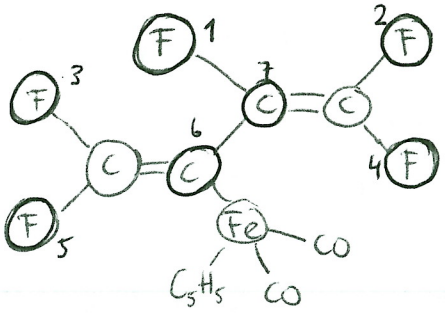
(5) → r (by continued fraction algorithm)

interference causes only terms $|y\rangle$ with $y = c\frac{2^n}{r}$ (for integer c) to have a substantial amplitude (notation from the paper)

4. NMR Implementation of Shor's Algorithm

4.1 Qubit Implementation

→ custom-designed molecule with five ^{19}F and two ^{13}C nuclear spins.
(fluorine)



"perfluorobutadienyl iron complex"

→ solve in liquid

→ $T = 30°C$

→ $B_0 = 11{,}7\ T$ ⇒ transition frequency values

↳ all different for the 7 nuclei (large range!)

⌈ chemical shift (~ kHz), $\frac{\omega_i}{2\pi}$ is $(i = 1, \dots, 7)$

given relative to a reference frequency
ca ~ 470 MHz for ^{19}F and ~ 125 MHz for ^{13}C.

fast gating of qubits ⇒

allows for single-qubit gate switching times of the order of 1 millisecond.

→ both ^{19}F and ^{13}C have long decoherence times (~ second)

→ each qubit is coupled to every other spin

(J-coupling, ~ Hz)

↓ interaction is pairwise!

→ large number of coupling constants ⇒ complicated spectrum!

~ $2^6 = 64$ resonance lines per spin (every spin coupled to six other spins)

and: for every gate, most of the couplings must be refocused

↳ unwanted couplings between qubits can be eliminated (apply pulse to one of the spins for example)

4.2. Initialisation

source $n=3$ target $m=4$

→ Desired initial state for the Algorithm : $|\psi_1\rangle = |0000001\rangle$

→ But: have thermal equilibr., spins have random orientation, i.e., they are in a statistical mixture of $|0\rangle$ and $|1\rangle$ (see fig. 3a) $k_B T \gg \hbar\omega_i$

↳ readout pulse on spin i → tipps spin from $|0\rangle$ ($+\hat{z}$) or $|1\rangle$ ($-\hat{z}$) into x-y plane → voltage oscillation at $\omega_i + \sum_j \frac{J}{2\pi}(\pm)$ detected

sign depends on other spin

⇒ Bring NMR system to "pseudopure" state. (or "effective pure state")

by temporal averaging: → ensemble of molecules

→ populations of the possible states

Bsp: $i=1,2$ → possible state: $|00\rangle$, $|10\rangle$, $|01\rangle$, $|11\rangle$

each have a population ≙ # molecules in this state

→ to obtain equal population of three levels (z.B. $|01\rangle$, $|10\rangle$, $|11\rangle$) to make one level ($|00\rangle$) stand out, we cyclically permute the populations and add the results. (averaging)

→ here: 7 qubits → do 36 experiments & average over them

→ but: this process results in loosing signal by destroying polarization (which increases exponentially with # qubits)

→ problem for scalability

↳ one restriction of usefulness of liquid-state NMR qu. computing

→ result (fig. 3b) → system in pure (or pseudo-pure) state,

each spin should have a well defined frequency, i.e., only one of the resonance lines that are generated by spin-spin couplings appears

→ position of the line depends on strength & sign of the J-couplings

good!

here: transition corresponds to all other states in $|0\rangle$

→ source register: initiated in the state $|0\rangle$

target: initially in state $|1\rangle$ (≙ first set to $|0\rangle$ and then flip bit 7)

→ have now initial state $\rho_1 = |\psi_1\rangle\langle\psi_1|$ (apply a NOT)

→ apply Hadamard transformation to generate superposition of all spin states of qubits 1 to 3 by spin-selective $\frac{\pi}{2}$ pulses on the first three qubits

4.3. Computation

- → want to calculate $f(x) = a^x \bmod N$ for 2^n values in parallel
  ↳ d.h. in one step.
  → use $a^x = a^{2^{n-1}x_{n-1}} \cdots a^{2x_1} a^{x_0}$ for x_k binary digits of x
  and $a^x \bmod N = \left(a^{x_{n-1}2^{n-1}} \bmod N\right) \cdot \ldots \cdot \left(a^{x_0 2^0} \bmod N\right)$.
  $x_k \in \{0, 1\}$.

  ⇒ Modular exponentiation consists of serial multiplication of $a^{2^k} \bmod N$ for all $0 \le k \le n-1$ for which $|x_k\rangle = |1\rangle$
  (compute these beforehand & classically (repeated squaring of a))

→ $N = 15$ ⇒ $a = 2, 4, 7, 8, 11, 13$ or 14 ($a < N$ & coprime with N)

- for $a = 2, 7, 8, 13$ → a^4 period $\bmod 15 = 1$ ⇒ all $a^{2^k} \bmod N = 1$ for $k \ge 2$
  ⇒ $f(x)$ simplifies to multiplications controlled by just x_0 and x_1

  for $a = 4, 11, 14$ ⇒ a^2 period $\bmod 15 = 1$ ⇒ only x_0 needed

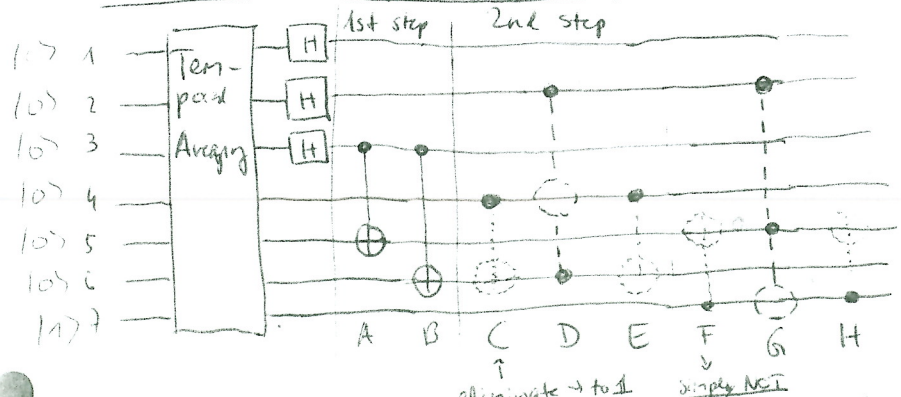
⇒ 1st register can be $n = 2$ qubits small.
here: they used $n = 3$ bits for encoding x (the additional qubit may be used for test purposes).

→ $m = \lceil \log N \rceil = 4$ qubits needed to encode $f(x)$

- ⇒ 7 qubits in total.

(Bsp) $a = 7$ → $f(x) = \left(a^{x_0} \bmod N\right)\left(a^{2x_1} \bmod N\right)$

Detailed circuit for this case (multiplication step)



→ C → unity
→ omit E, H
→ D, G can be simplified
→ F → NOT

qubit 4, 5, 6, 7
↓
|0000⟩

- 1st step: multiplication of target register (in state $|1\rangle$) by $a^{x_0} \bmod 15$ (if $x_0 = 1$). equivalent to adding $(a-1) \bmod 15$, which can be done by two operations: CNOT(3,5) CNOT(3,6), i.e., if $x_0 = 1$, qubits 5 and 6 are changed from $|0\rangle$ to $|1\rangle$ → $|0111\rangle$

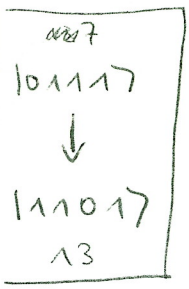
$|0001\rangle \rightarrow |0111\rangle$

2nd step: multiplication with $a^{2x_1} \pmod{15}$, controlled by qubit 2 (i.e., by q_{x_1}).

$\rightsquigarrow 7^2 \bmod 15 = 4$ $\rightsquigarrow$ need to multiply (mod 15) by 4, which can be done by SWAP operations of 4 with 6 and 5 with 7 (controlled by qubit 2)

$\rightarrow$ gives target register state $|1101\rangle = |13\rangle = |(4 \cdot 7) \bmod 15\rangle$ ☺

$\rightarrow$ can decompose each SWAP operation into 3 CNOT operations "CDE" and "FGH", D and G are "CCNOT" (controlled SWAP).



Note: Vandersypen et al. used a number of simplifications ("compiler optimizations") to simplify or eliminate specific gates (dotted in figure)

$\rightarrow$ Bsp: Gate C can be eliminated (be reduced to unity operation) since the control qubit is zero

$\rightarrow$ And: doubly controlled D and G gates act on target bits that are in basis states (not superposition states) which allows their replacement by simpler gates ($\rightarrow$ denoted by dashed lines)

$\rightarrow$ Gate F can be simplified to a NOT operation (since control qubit 7 is always 1)

$\rightarrow$ Gates E and H can be omitted (since they act on qubits that are no longer accessed afterwards and therefore do not affect the result

Now: Inverse QFT:

$\rightarrow$ H and phase gates (z.B. π-rotations) of 45 and 90 degrees, which are in practice mostly turned into rotations of the coord. axes

4.4. Readout

→ Information is stored in the populations of the spin state.

Note: all spins in an NMR qubit register must have different Larmor frequencies ($\omega_{\frac{1}{2\pi}}$) to allow addressability for logical operations.

This implies that their precession frequencies during detection are different!

→ Thus, when applying an RF pulse to measure the populations, the total signal obtained is generally the sum over all qubits, but, when Fourier transformed to obtain a spectrum, the individual contributions from different qubits (in freq. space) show up.

→ **a = 11 case** resulting state of three qubits form compact $\rho \sim \sum_c w_c \left| c\frac{2^3}{r} \right\rangle \left\langle c\frac{2^3}{r} \right|$

→ Spectra contain only positive lines for 1 and 2
→ these are in state $|0\rangle$ at the end of computation

→ one pos./one neg. line for 3 → 3 is in (equal) superposition $|0\rangle \pm |1\rangle$.

⇒ Resulting state: a mixture of $|\overset{3}{1}\overset{2}{0}\overset{1}{0}\rangle = |4\rangle$
and $|0\,0\,0\rangle = |0\rangle$
binary decimal

⇒ period of the probability (amplitude) of $|y\rangle$ is 4 $\Rightarrow r = \frac{2^n}{4} = 2$

$\left(y = c\frac{2^3}{r} \ldots \right)$

⇒ $\gcd(15, a^{\frac{r}{2}} \pm 1)$
$= \gcd(15, a \pm 1) = 3, 5$
$= \gcd(15, 11 \pm 1) = 3, 5$ ☺

a = 7 case

→ both 2 and 3 are in superposition states
→ 1 is in $|0\rangle$
⇒ possible results are $|\overset{3}{1}\overset{2}{0}\overset{1}{0}\rangle = |0\rangle$
$|0\,1\,0\rangle = |2\rangle$
$|1\,0\,0\rangle = |4\rangle$
$|1\,1\,0\rangle = |6\rangle$

⇒ period of amplitude of $|y\rangle$ is 2
$\Rightarrow r = \frac{8}{2} = 4$
$\Rightarrow \gcd(15, 7^{\frac{4}{2}} \pm 1)$
$= \gcd(15, 49 \pm 1) = 3, 5$

⇒ data indicate successful execution of Shor's Alg.!

5. Errors / Decoherence modelling

→ compare measured to ideal spectra:

errors most notably in case $a = 7$ (difficult case).

→ used ~ 300 rf pulses to implement the algorithm of which most were used to compensate for unwanted effects

(e.g. spin-spin coupling, magnetic field inhomogeity)

→ the overall sequence lasted almost 1 second, which is longer than some of the relevant relaxation times (= decoherence times)

⇒ significant loss of information ⇝ deviations from ideal to measured case

→ confirmed by modelling the decoherence processes

→ see fig 3 botton traces

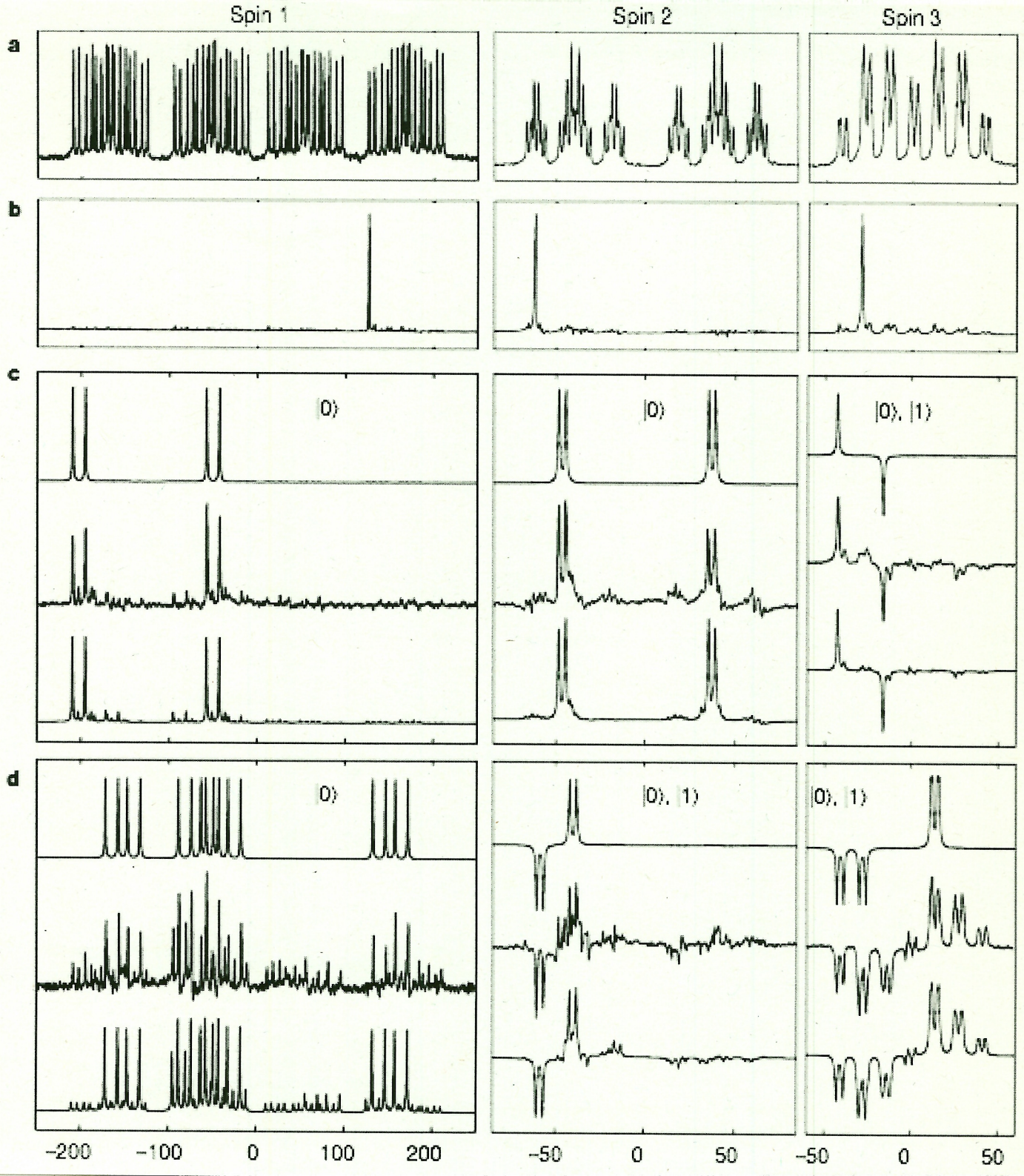
References

→ Nielsen & Chuang: Quantum Computation and Quantum Information

→ Stolze, Suter: Quantum Computing: A Short Course from Theory to Experiment

Fig. 3

Output Spectra



thermal eq.

(pseudo) pure State

a = 11

ideal case

meas.

model

a = 7

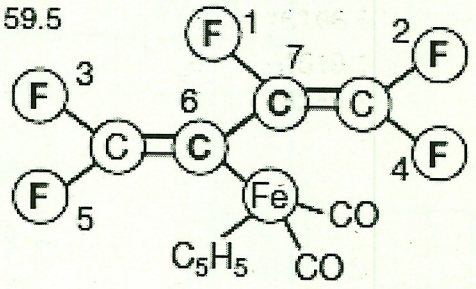
ideal case

meas.

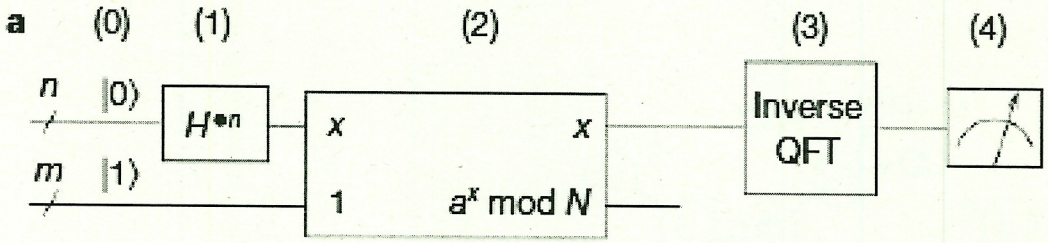
model

Transition freq., decoherence times, couplings of the 7 qubits

qubit	[Hz]	[s]	[s]	[Hz]					
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						



Quantum Circuit
Shor's Alg.



Detailed Circuit
for a=7