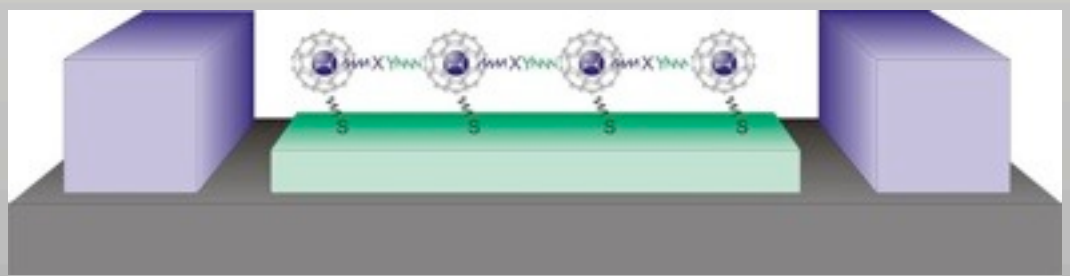
lecture WS ’15

Quantum Computers
- how to make them work -
Shor’s algorithm

C. Meyer, C.M. Schneider



prime factorization

algorithm found by Peter Shor 1994

prime factorization

algorithm found by Peter Shor 1994

prime factorization

algorithm found by Peter Shor 1994

generalized to an algorithm for order finding

prime factorization

algorithm found by Peter Shor 1994

generalized to an algorithm for order finding

key step is the quantum Fourier transform (QFT)

discrete Fourier transform (DFT)

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

DFT

unitary transform that converts a string of N complex numbers x_j to a string of N complex numbers y_k

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, \mathbf{e}^{i2\pi jk/N}$$

inverts periodicity (input string period r, output string N/r)

1 0 0 0 1 0 0 0 ⟶ 1 0 1 0 1 0 1 0

converts off-sets into phase factors

0 1 0 0 0 1 0 0 ⟶ 1 0 -i 0 -1 0 i 0

quantum Fourier transform

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

number of qubits $n = \log_2 N$ (for N=8, three qubits)

amplitude of $|000\rangle$ represents first complex number, $|001\rangle$ the 2nd

states $|000\rangle, |001\rangle, \ldots, |111\rangle$ are labelled $|0\rangle, |1\rangle, \ldots, |7\rangle$

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

0 1 0 0 0 1 0 0 ⟶ 1 0 -i 0 -1 0 i 0

$(|1\rangle + |5\rangle)\sqrt{2} \longrightarrow (|0\rangle - i|2\rangle - |4\rangle + i|6\rangle)/2$

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

$$|j_1 j_2 j_3\rangle \rightarrow \frac{1}{2^{n/2}} \left[\left(|0\rangle + e^{2\pi i\, 0.j_3} |1\rangle \right) \left(|0\rangle + e^{2\pi i\, 0.j_2 j_3} |1\rangle \right) \left(|0\rangle + e^{2\pi i\, 0.j_1 j_2 j_3} |1\rangle \right) \right]$$

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

reverse order of output qubits: $j_1^{in} = j_3^{out}$, $j_3^{in} = j_1^{out}$

$$|j_1 j_2 j_3\rangle \rightarrow \frac{1}{2^{n/2}} \left[\left(|0\rangle + e^{2\pi i\, 0.j_1} |1\rangle \right) \left(|0\rangle + e^{2\pi i\, 0.j_2 j_1} |1\rangle \right) \left(|0\rangle + e^{2\pi i\, 0.j_3 j_2 j_1} |1\rangle \right) \right]$$

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

reverse order of output qubits: $j_1^{in} = j_3^{out}$, $j_3^{in} = j_1^{out}$

$$|j_1 j_2 j_3\rangle \rightarrow \frac{1}{2^{n/2}} \left[\underbrace{\left(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\right)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} j_3^{in}} \left(|0\rangle + e^{2\pi i\, 0.j_2 j_1}|1\rangle\right) \left(|0\rangle + e^{2\pi i\, 0.j_3 j_2 j_1}|1\rangle\right) \right]$$

H

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

reverse order of output qubits: $j_1^{in} = j_3^{out}$, $j_3^{in} = j_1^{out}$

$$|j_1 j_2 j_3\rangle \rightarrow \frac{1}{2^{n/2}} \Big[\underbrace{\Big(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\Big)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} j_3^{in}} \underbrace{\Big(|0\rangle + e^{2\pi i\, 0.j_2 j_1}|1\rangle\Big)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} j_2^{in}} \Big(|0\rangle + e^{2\pi i\, 0.j_3 j_2 j_1}|1\rangle\Big) \Big]$$

H H

quantum Fourier transform

Nielsen/Chuang S. 218

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{i2\pi jk/N} |k\rangle$$

$j = j_1 2^2 + j_2 2^1 + j_3 2^0$ (short: $j = j_1 j_2 j_3$) $0.j_1 j_2 j_3 = j_1/2 + j_2/4 + j_3/8$

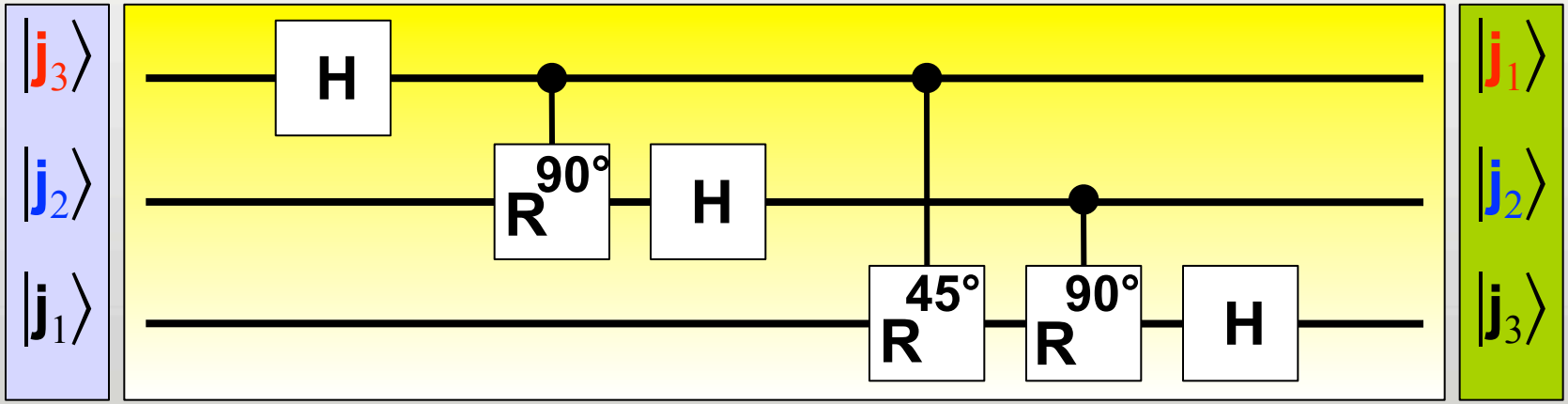
reverse order of output qubits: $j_1^{in} = j_3^{out}$, $j_3^{in} = j_1^{out}$

$$|j_1 j_2 j_3\rangle \rightarrow \frac{1}{2^{n/2}} \left[\underbrace{\left(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\right)}_{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} j_3^{in}} \underbrace{\left(|0\rangle + e^{2\pi i\, 0.j_2 j_1}|1\rangle\right)}_{j_3^{in}=1 \quad \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/2}\end{pmatrix} j_2^{in}} \left(|0\rangle + e^{2\pi i\, 0.j_3 j_2 j_1}|1\rangle\right) \right] \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} j_2^{in}$$

H | $R_{23}^{90°}$ | H

QFT quantum circuit

Weinstein et al.: quant-ph/99060059v1 (1999)



$$H = e^{\frac{i}{\hbar}\pi I_x} e^{\frac{i}{\hbar}\frac{\pi}{2} I_y}$$

$$R_1 = e^{-\frac{i}{\hbar}\phi I_z} = \begin{pmatrix} e^{-i\frac{\phi}{2}} & \\ & e^{i\frac{\phi}{2}} \end{pmatrix}$$

$$R_{jk} = e^{-\frac{i}{\hbar}\frac{\pi}{2} I_y^{j,k}} e^{\frac{i}{\hbar}\phi I_x^{j,k}} e^{\frac{i}{\hbar}\frac{\pi}{2} I_y^{j,k}}$$

$$e^{\frac{i}{\hbar}\pi I_\theta{}^j} e^{\frac{i}{\hbar} J t I_z^j I_z^k} e^{\frac{i}{\hbar}\pi I_\theta{}^j}$$

$$= e^{-\frac{i}{\hbar}\frac{\pi}{2} I_y} e^{\frac{i}{\hbar}\phi I_x} e^{\frac{i}{\hbar}\frac{\pi}{2} I_y}$$

QFT implementation

Weinstein et al.: Phys. Rev. Lett. 86,1889 (2001)

- ^{13}C labeled spins of Alanine as qubits (T_1>1.5s, T_2>400ms)
- Preparation of pseudo-pure state $|000\rangle$

$|111\rangle\langle 000|$

$|000\rangle\langle 000|$

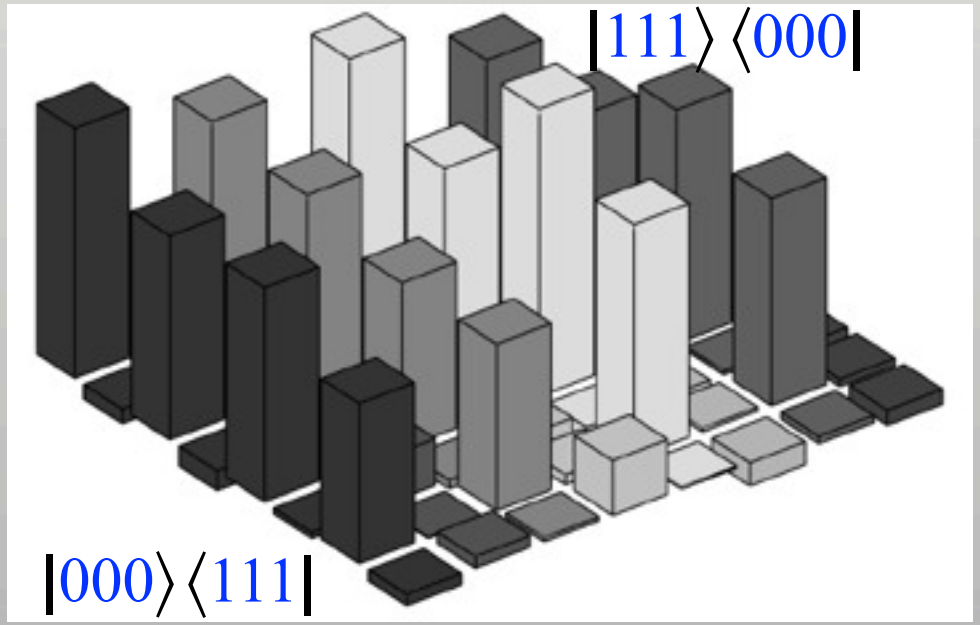
$|111\rangle\langle 111|$

$|000\rangle\langle 111|$

QFT implementation

Weinstein et al.: Phys. Rev. Lett. 86,1889 (2001)

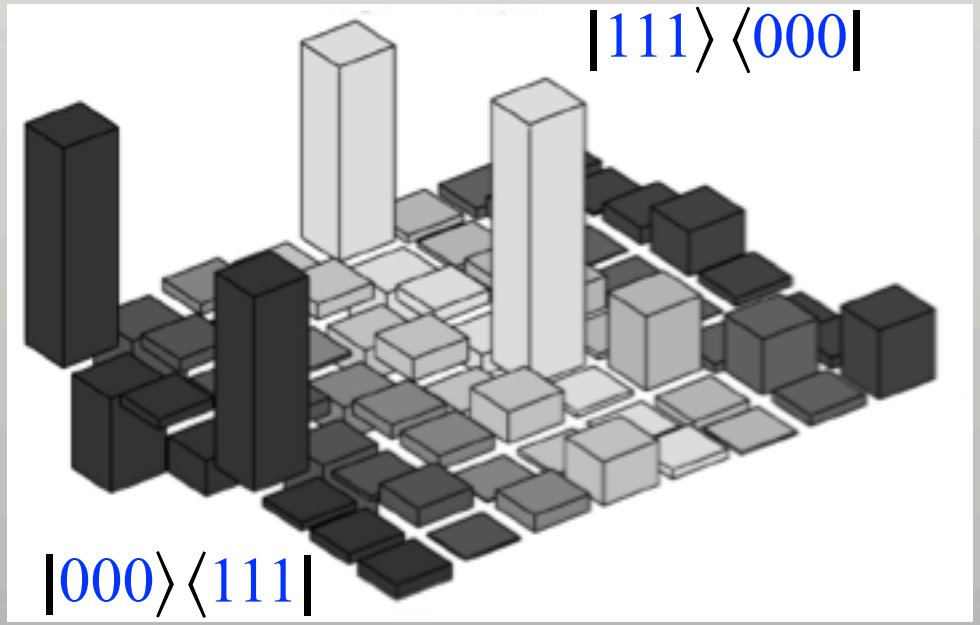
- ^{13}C labeled spins of Alanine as qubits (T_1>1.5s, T_2>400ms)
- Preparation of pseudo-pure state $|000\rangle$
- Preparation of input state $|000\rangle+|010\rangle+|100\rangle+|110\rangle$



QFT implementation

Weinstein et al.: Phys. Rev. Lett. 86,1889 (2001)

- ^{13}C labeled spins of Alanine as qubits (T_1>1.5s, T_2>400ms)
- Preparation of pseudo-pure state $|000\rangle$
- Preparation of input state $|000\rangle+|010\rangle+|100\rangle+|110\rangle$
- Apply QFT => $|000\rangle+|001\rangle$ and SWAP => $|000\rangle+|100\rangle$



Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

Order finding

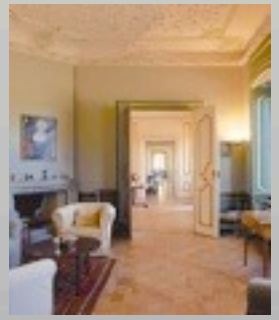
Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit





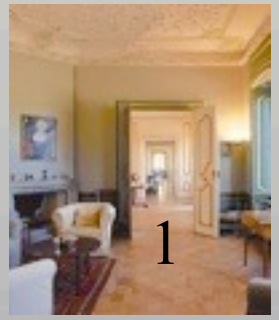





Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit



Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit
- Connected by subcycles

Order finding

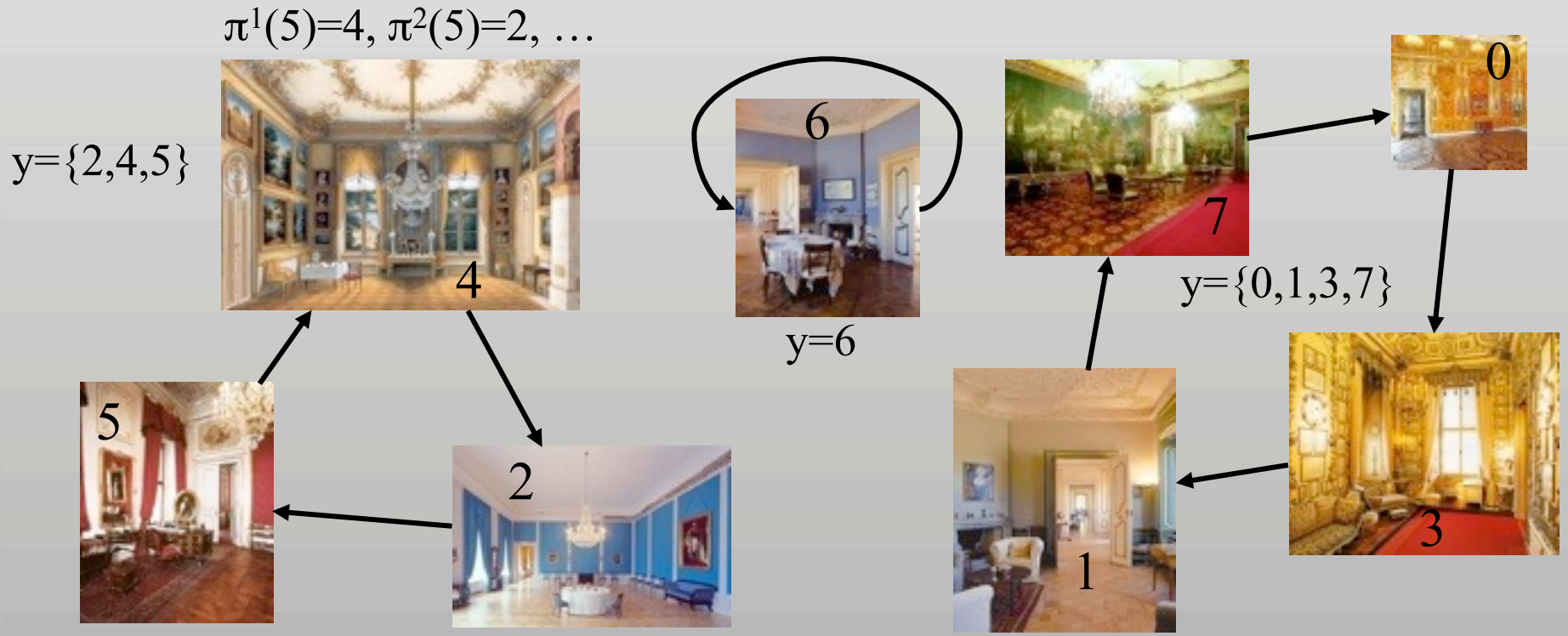
Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit
- Connected by subcycles

Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit
- Connected by subcycles

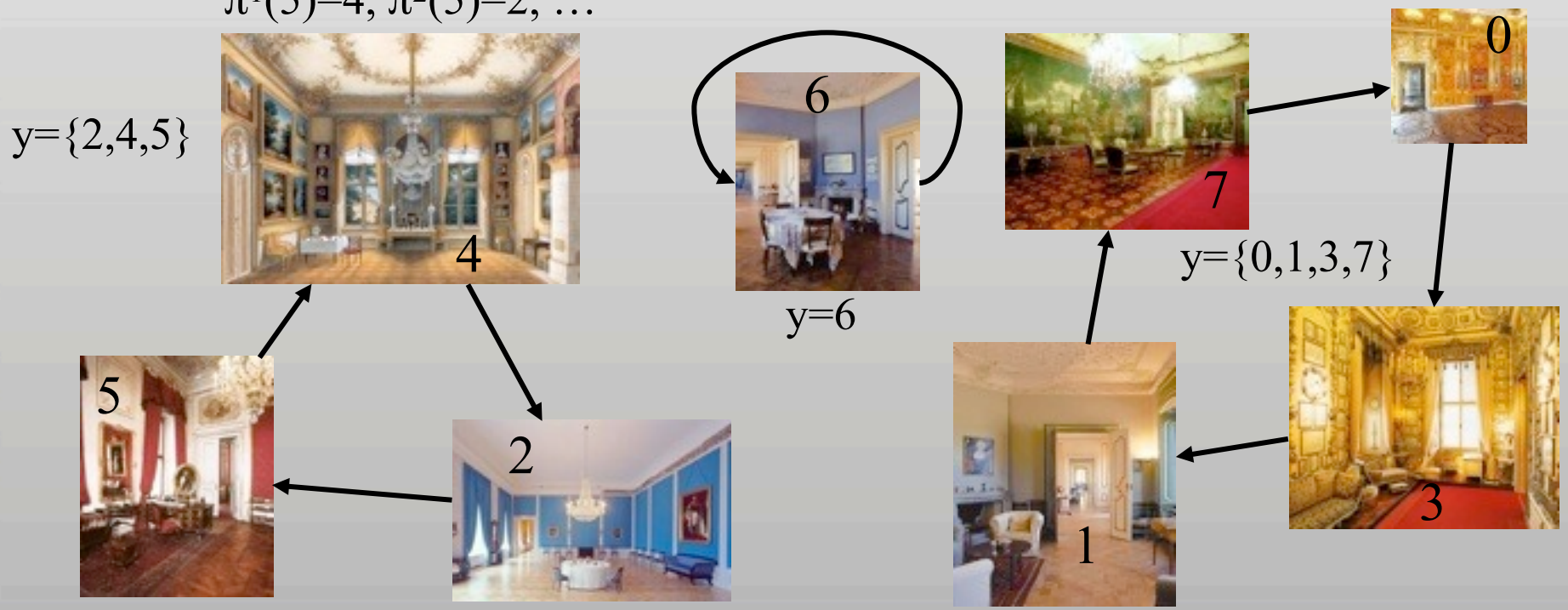


Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit
- Connected by subcycles
- How often to change room until back at start?

$\pi^1(5)=4$, $\pi^2(5)=2$, …

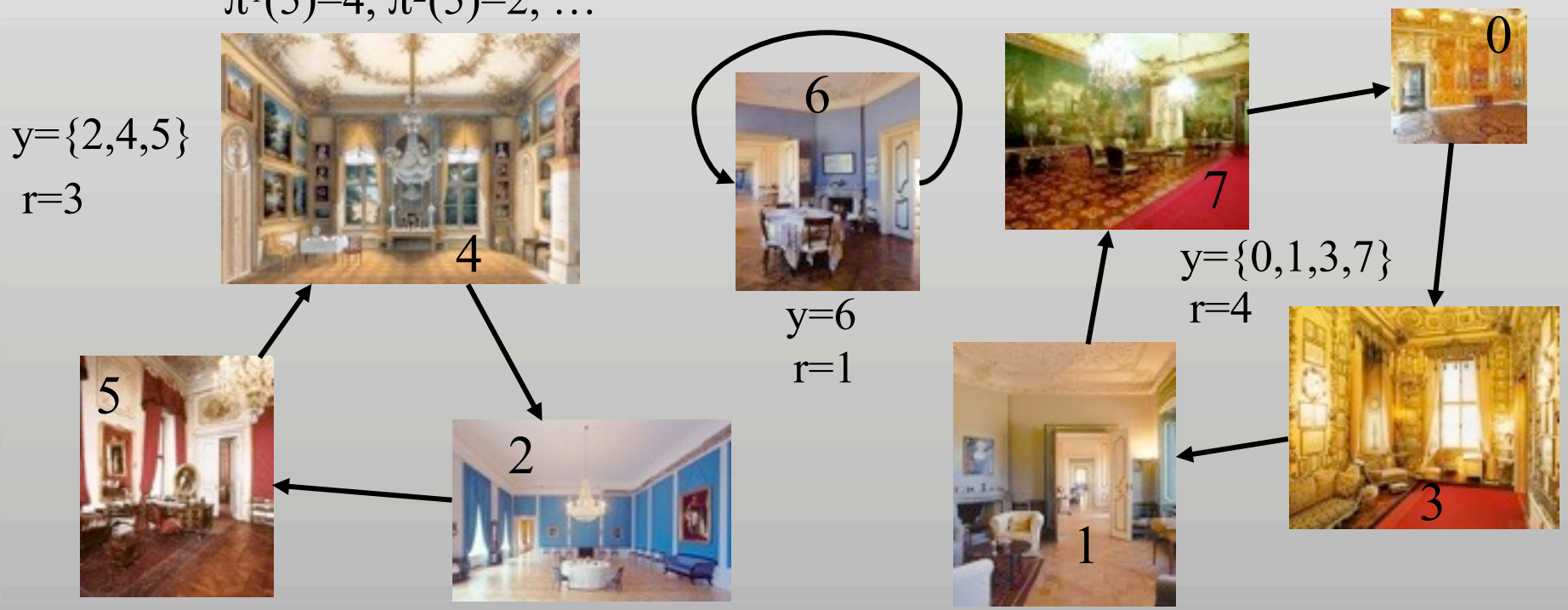


Order finding

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

- M rooms with one entrance and one exit
- Connected by subcycles
- How often to change room until back at start?

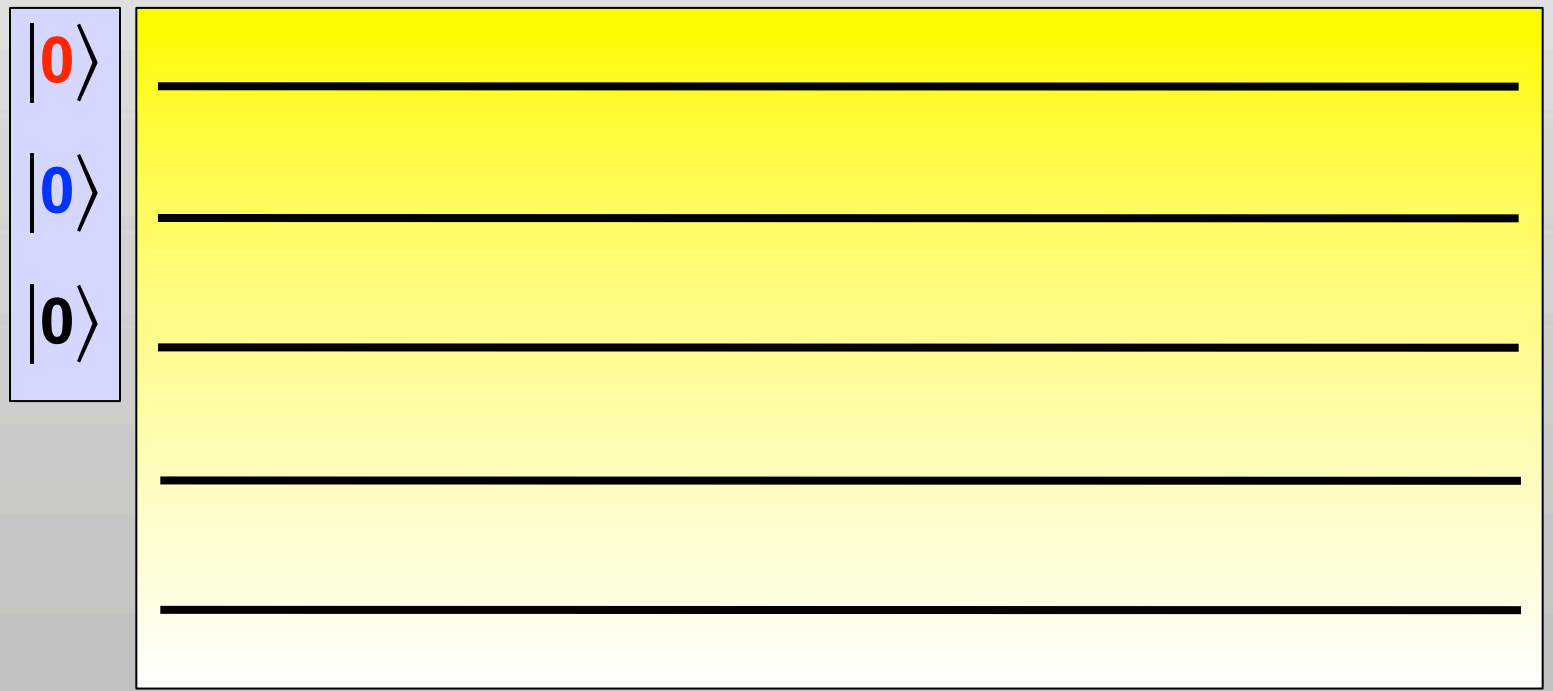
$\pi^1(5)=4$, $\pi^2(5)=2$, …



Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$

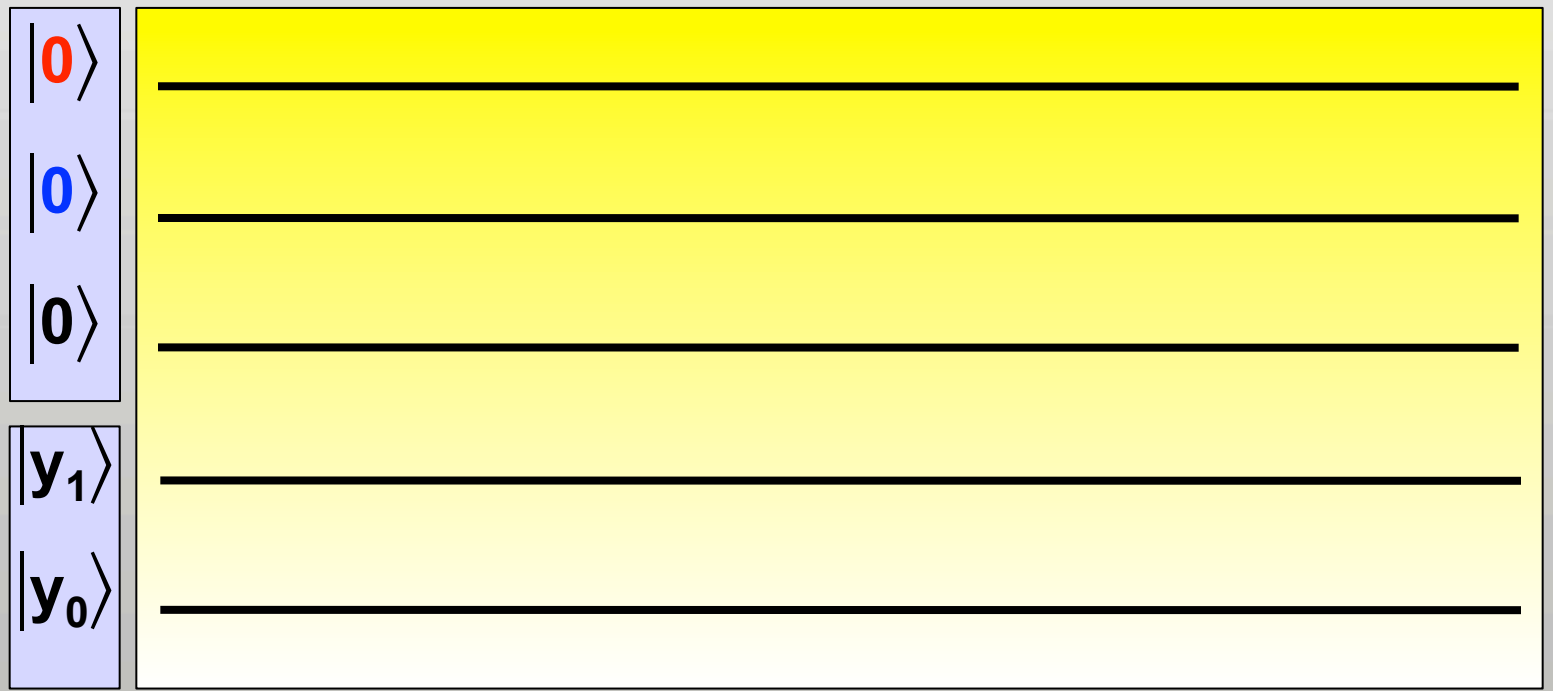


Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$

$M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

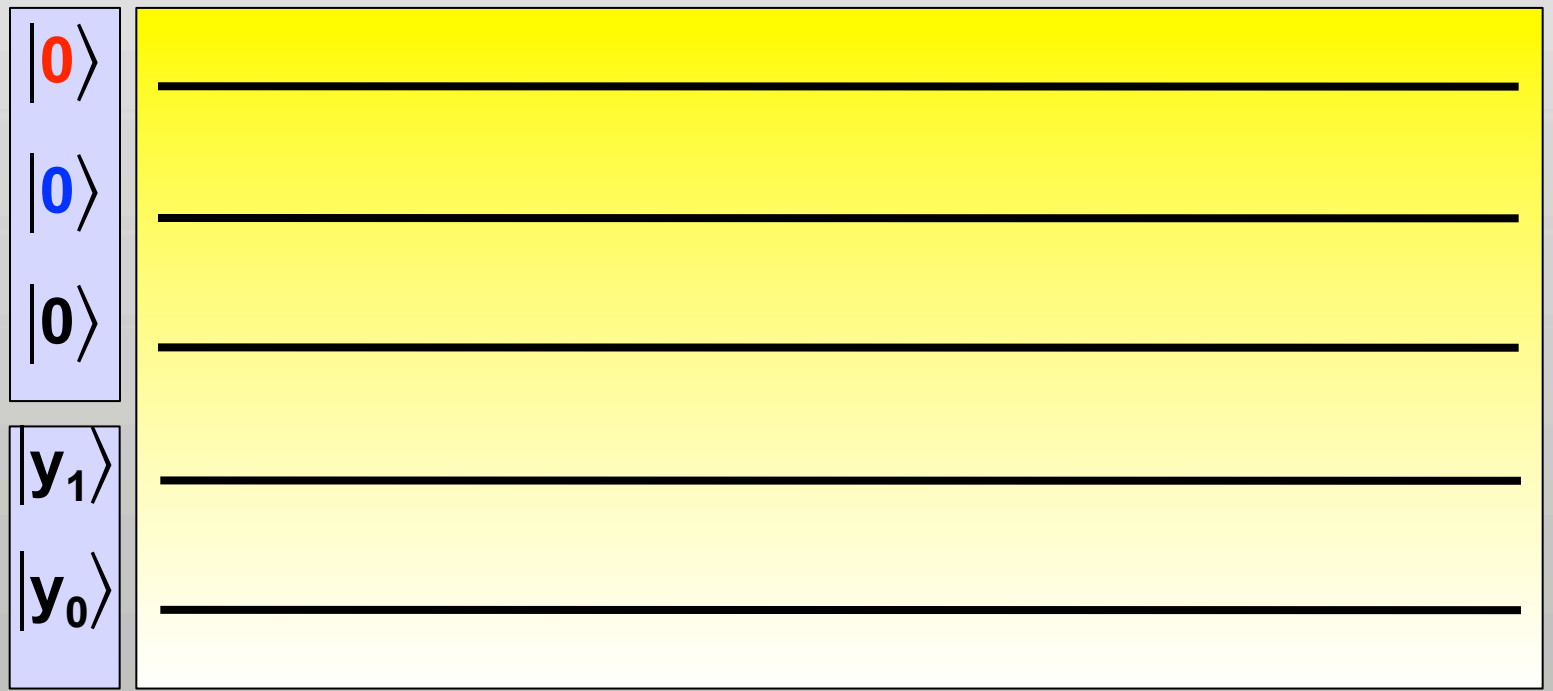


Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$



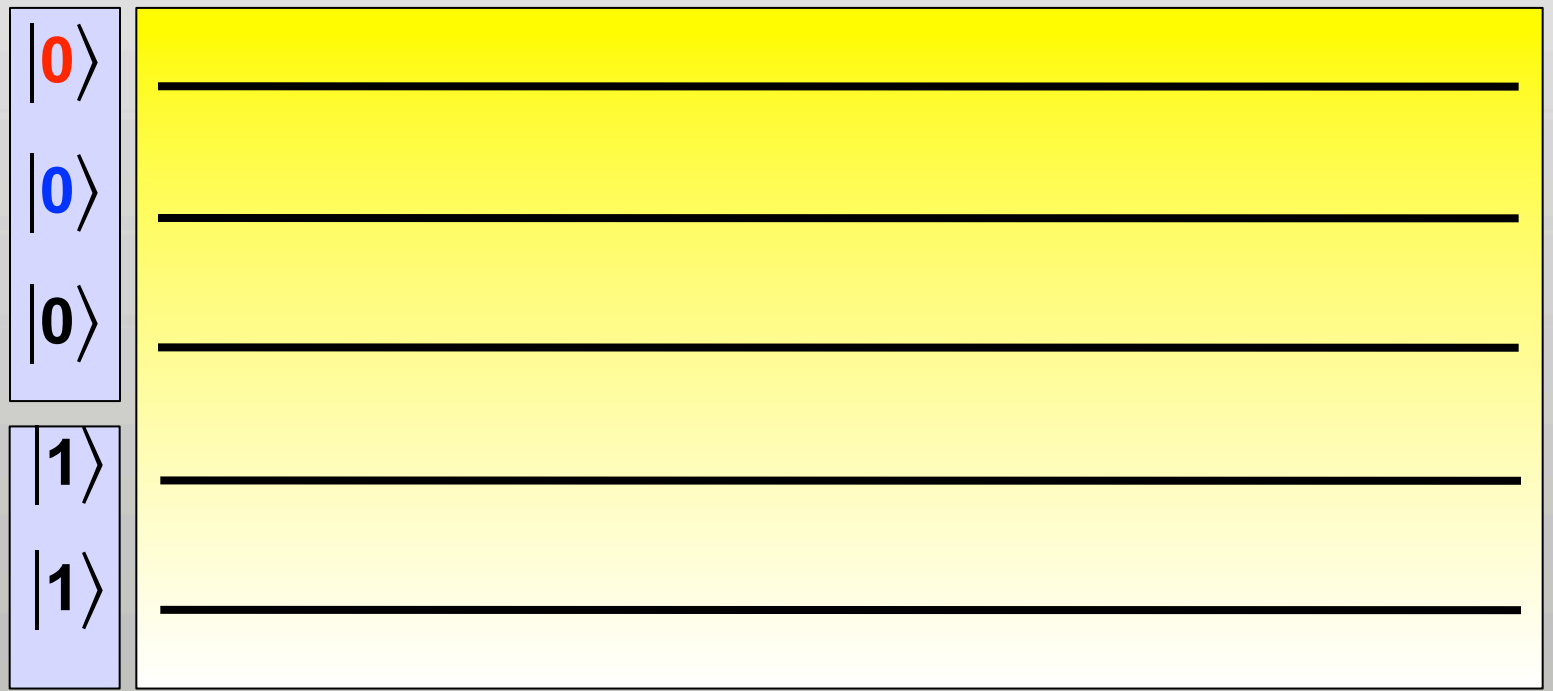
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$



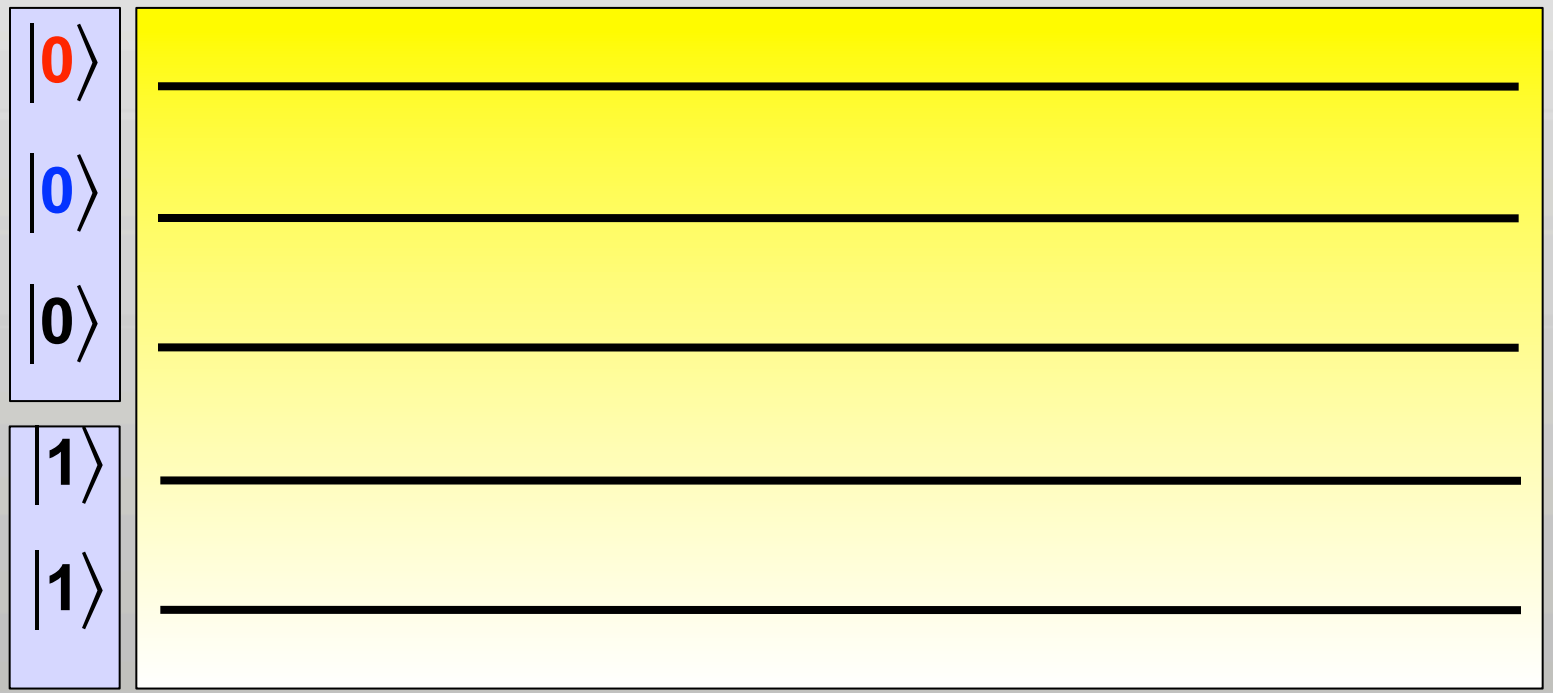
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$



$|\psi_0\rangle = |000\rangle|11\rangle$

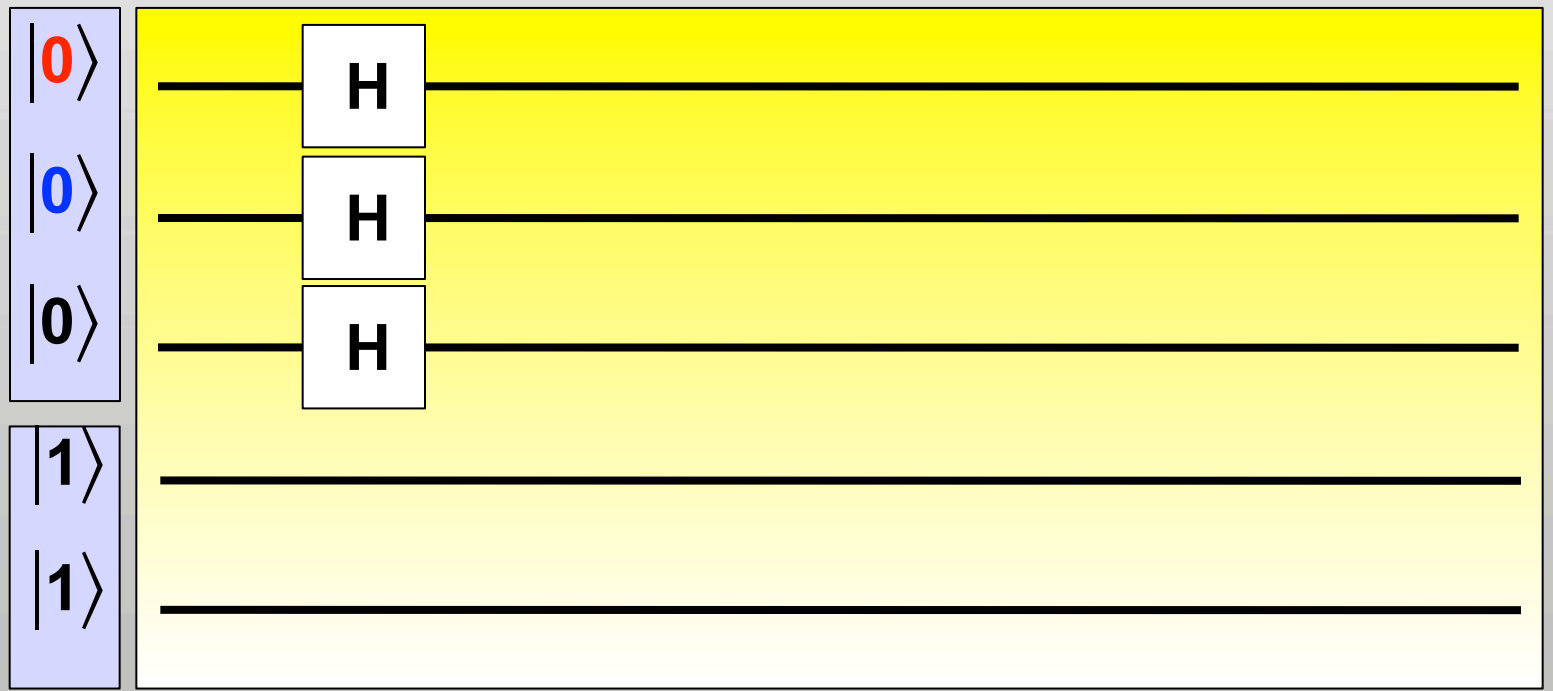
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$



$$|\psi_1\rangle = (|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)|11\rangle$$

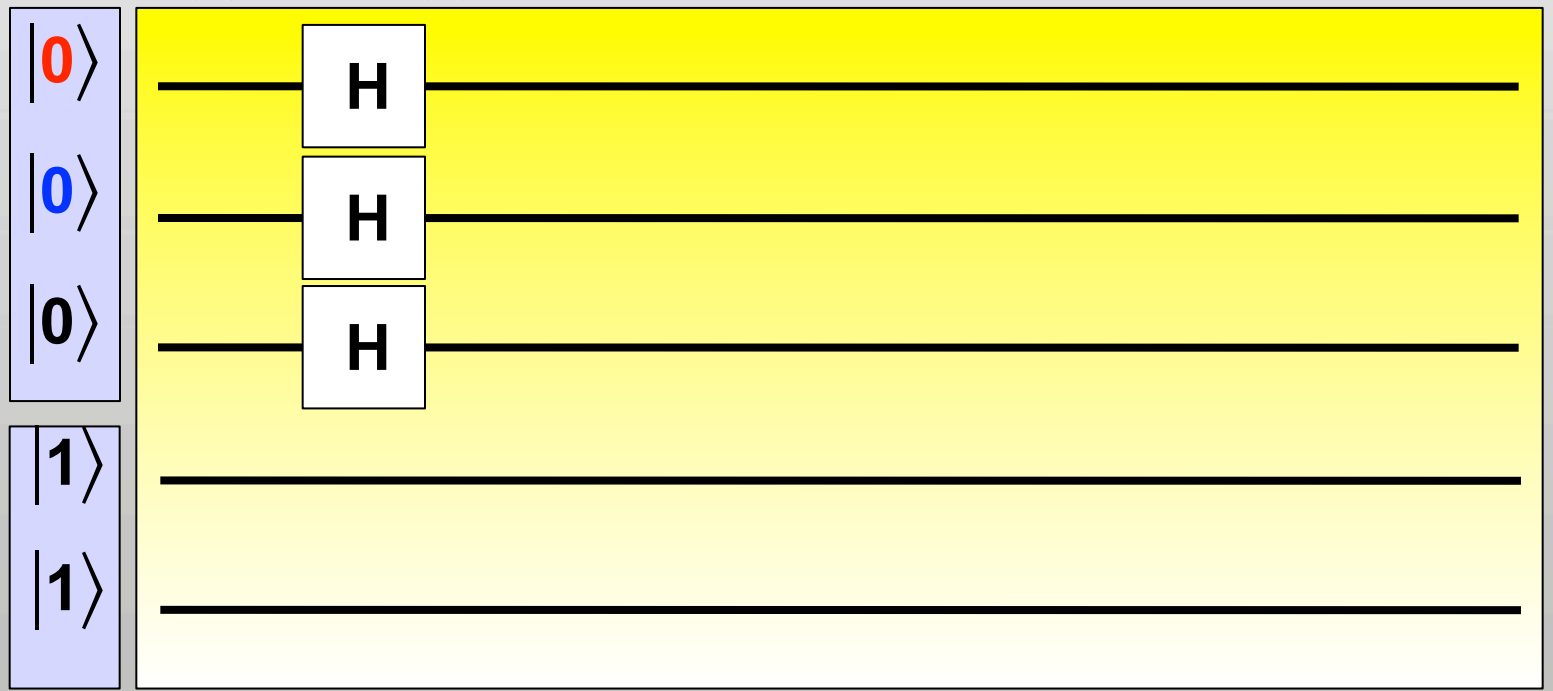
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$ $\quad \pi^1(3)=1,\ \pi^2(3)=3,\ \ldots$



$$|\psi_1\rangle = (|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle)|11\rangle$$

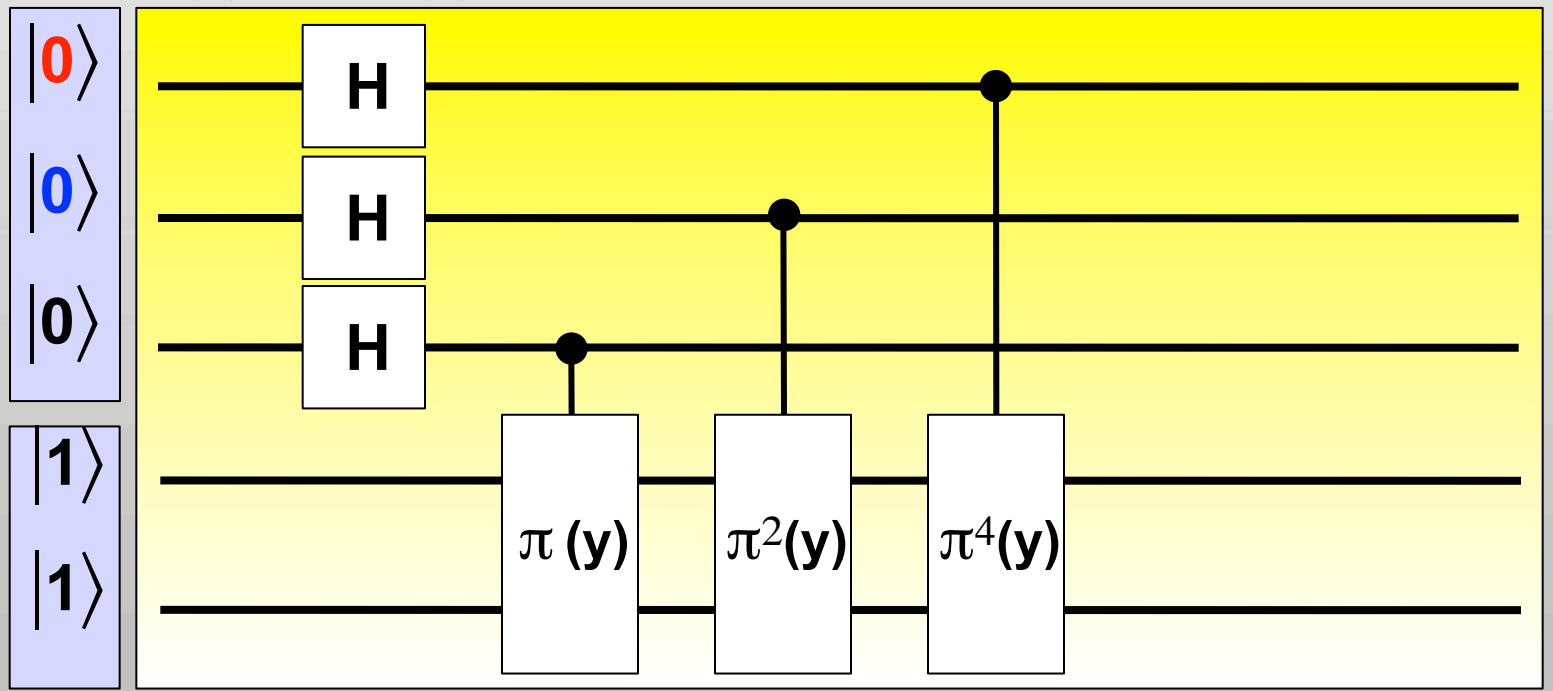
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$ $\quad \pi^1(3)=1,\ \pi^2(3)=3,\ \ldots$



$$|\psi_2\rangle = (|0\rangle + |2\rangle + |4\rangle + |6\rangle)|1\rangle + (|1\rangle + |3\rangle + |5\rangle + |7\rangle)|3\rangle$$

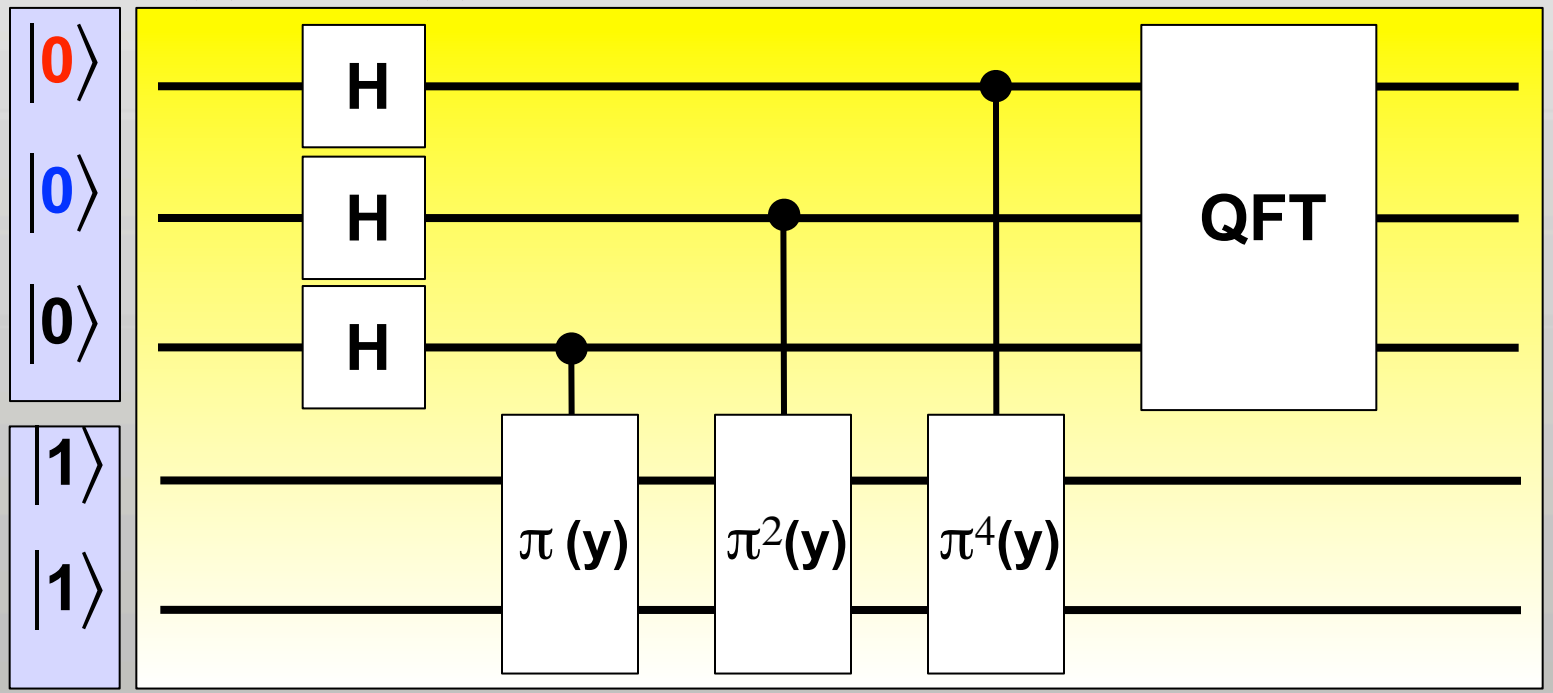
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$ $\quad \pi^1(3)=1,\ \pi^2(3)=3,\ \ldots$



$$|\psi_3\rangle = (|0\rangle + |4\rangle)|1\rangle + (|0\rangle - |4\rangle)|3\rangle$$

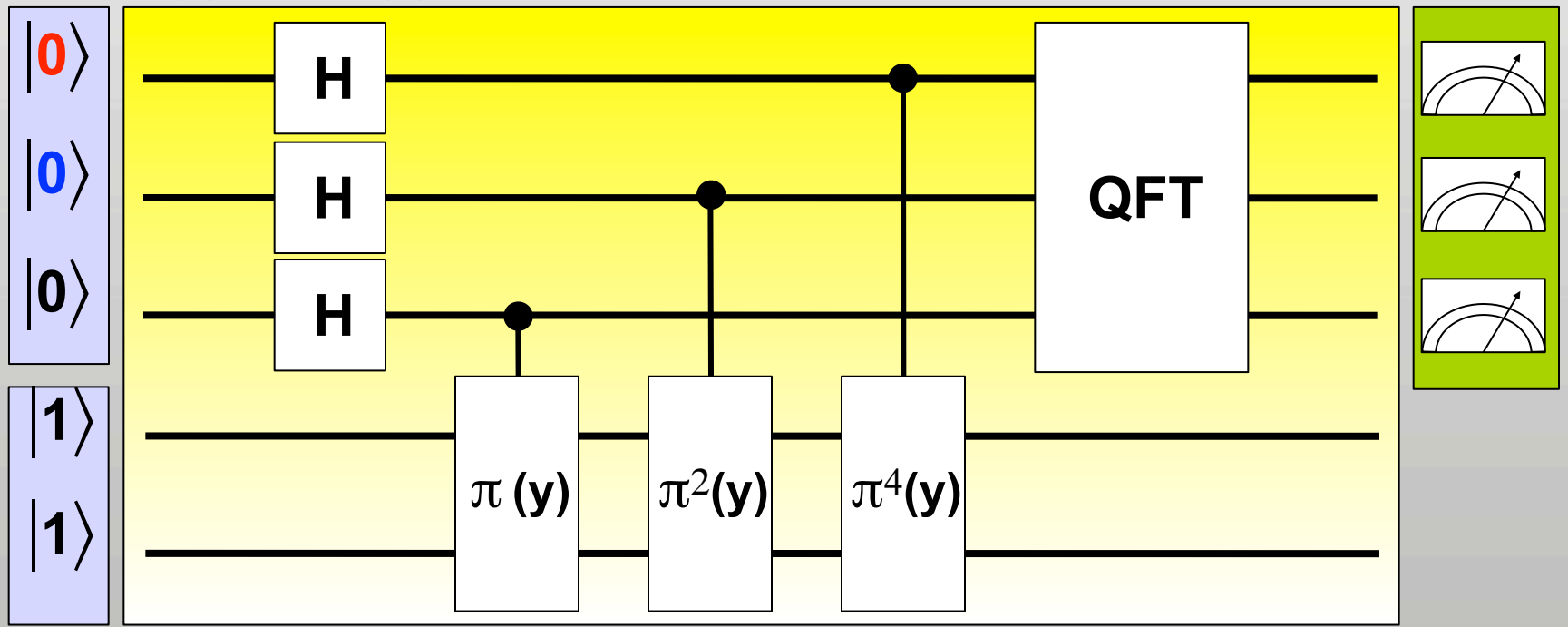
Order finding: quantum circuit

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

$|x\rangle = |x_2 x_1 x_0\rangle$, $x = 4x_2 + 2x_1 + x_0$ $\qquad$ $M=4$, $|y_1 y_0\rangle = |y\rangle$, $y \in M\text{-}1$

$|x\rangle|y\rangle \rightarrow |x\rangle|\pi^x(y)\rangle = |x\rangle|\pi^{4x_2}(y)\rangle|\pi^{2x_1}(y)\rangle|\pi^{x_0}(y)\rangle$

$y=3$ $\quad \pi^1(3)=1,\ \pi^2(3)=3,\ \ldots$



$|\psi_3\rangle = (|0\rangle + |4\rangle)|1\rangle + (|0\rangle - |4\rangle)|3\rangle$

measurement yields multiple of $2^n/r \Rightarrow r=2$

Order finding for n qubits

Lieven Vandersypen, PhD thesis: http://arxiv.org/abs/quant-ph/0205193

register 1 number of transitions between "rooms"

register 2 number of starting room

1) $|0\rangle|0\rangle$

2) $H^{\otimes n} \rightarrow \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|0\rangle$

3) $f(j)=\pi^j(0) \rightarrow \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle|f(j)\rangle$

4) QFT r1 $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \sum_{k=0}^{2^n-1} e^{i2\pi jk/N} |k\rangle|f(j)\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} e^{i2\pi jk/N} |k\rangle|f(j)\rangle$

5) Measure the amplitude of $|k\rangle \rightarrow \left(\sum_{j=0}^{2^n-1} e^{i2\pi jk/N} \right)^2$ (large for k=c*N/r)

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

$f(x,y)=\pi^x(y)=a^x y \bmod N$

one factor is $\gcd(a^{r/2}\pm 1,N)$
(probability >0.5)

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is gcd($a^{r/2}\pm1$,N)
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is gcd($a^{r/2}\pm1$,N)
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is gcd($a^{r/2}\pm1$,N)
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is $\gcd(a^{r/2}\pm 1, N)$
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$

$a^4 \bmod 15 = 1,\ a \in \{2,7,8,13\} \Rightarrow a^{2k} \bmod 15 = 1,\ k \geq 2$

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is $\gcd(a^{r/2}\pm 1, N)$
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$

f(x) needs x_0 only

$a^4 \bmod 15 = 1,\ a \in \{2,7,8,13\} \Rightarrow a^{2^k} \bmod 15 = 1,\ k \geq 2$

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is $\gcd(a^{r/2}\pm 1, N)$
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$

$a^4 \bmod 15 = 1,\ a \in \{2,7,8,13\} \Rightarrow a^{2^k} \bmod 15 = 1,\ k \geq 2$

f(x) needs x_0 only

f(x) needs x_0 and x_1

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is gcd($a^{r/2}\pm1$,N)
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$ f(x) needs x_0 only

$a^4 \bmod 15 = 1,\ a \in \{2,7,8,13\} \Rightarrow a^{2^k} \bmod 15 = 1,\ k \geq 2$
f(x) needs x_0 and x_1

register 2 needs 4 qubits $m=(\log_2 N)$

Shor's algorithm

L. Vandersypen et al.: Nature 414, 883 (2001)

number to factorize: N
(e.g. N=15)

one factor is $\gcd(a^{r/2}\pm 1, N)$
(probability >0.5)

integer a does NOT divide N
(a=2,4,7,8,11,13,14)

"easy"

$f(x,y)=\pi^x(y)=a^x y \bmod N$

"easy?"

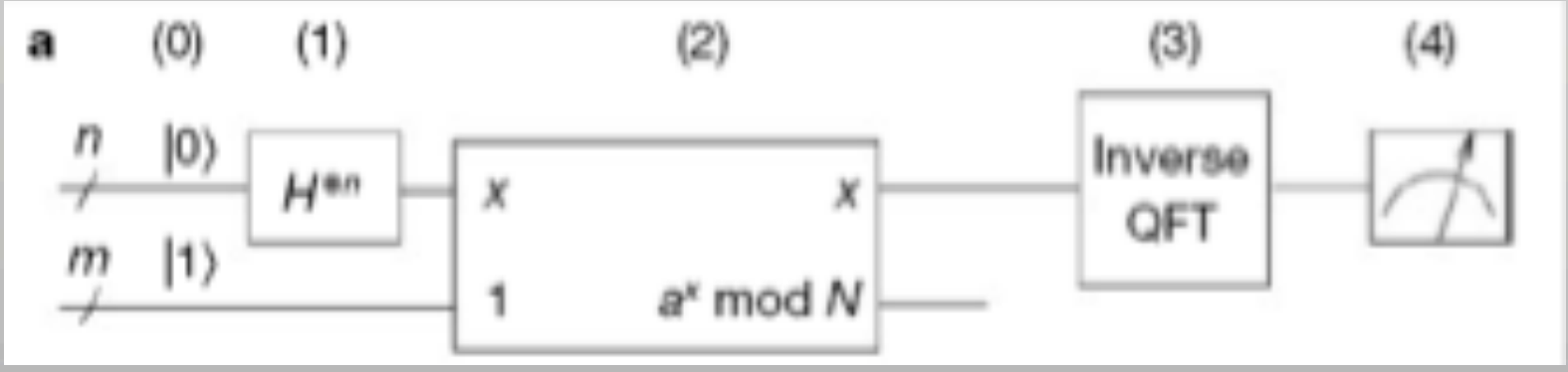
$a^2 \bmod 15 = 1,\ a \in \{4,11,14\}$ f(x) needs x_0 only

$a^4 \bmod 15 = 1,\ a \in \{2,7,8,13\} \Rightarrow a^{2^k} \bmod 15 = 1,\ k \geq 2$
f(x) needs x_0 and x_1

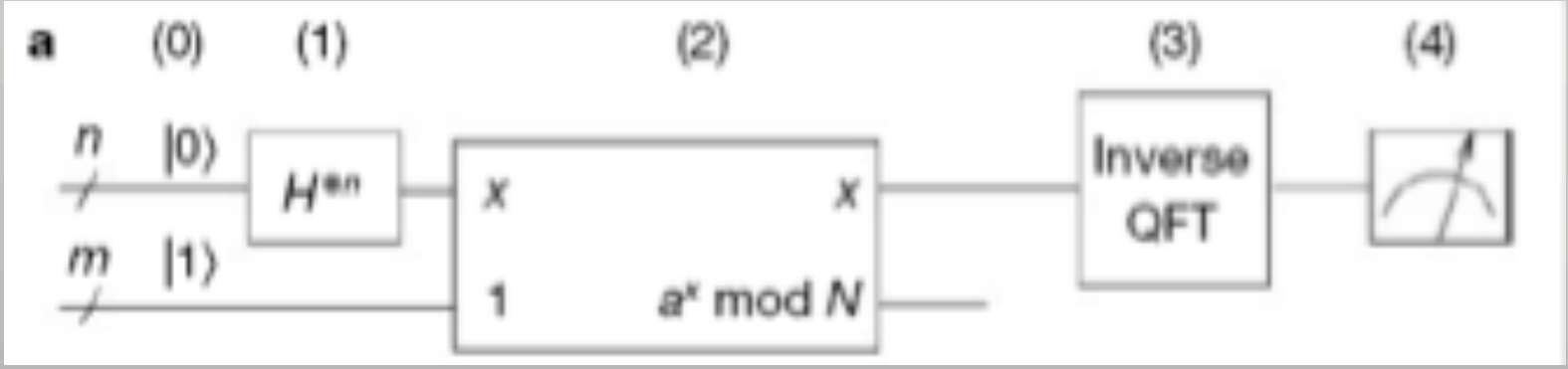
register 1 needs 2 qubits (take 3) $n=2m$

register 2 needs 4 qubits $m=(\log_2 N)$

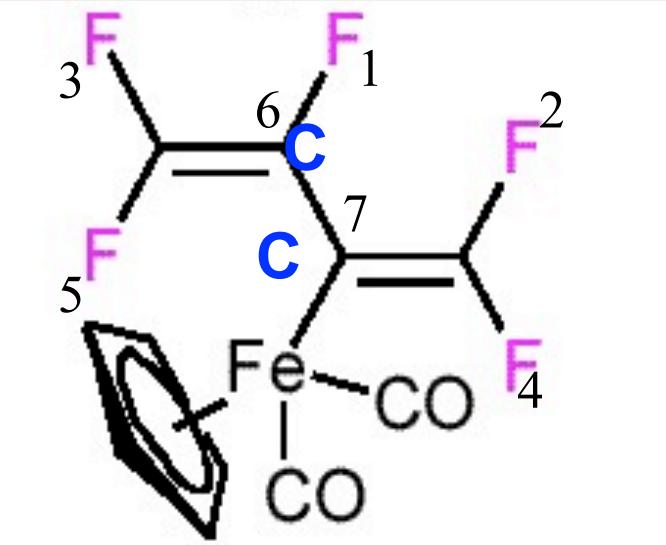
Implementation of Shor's

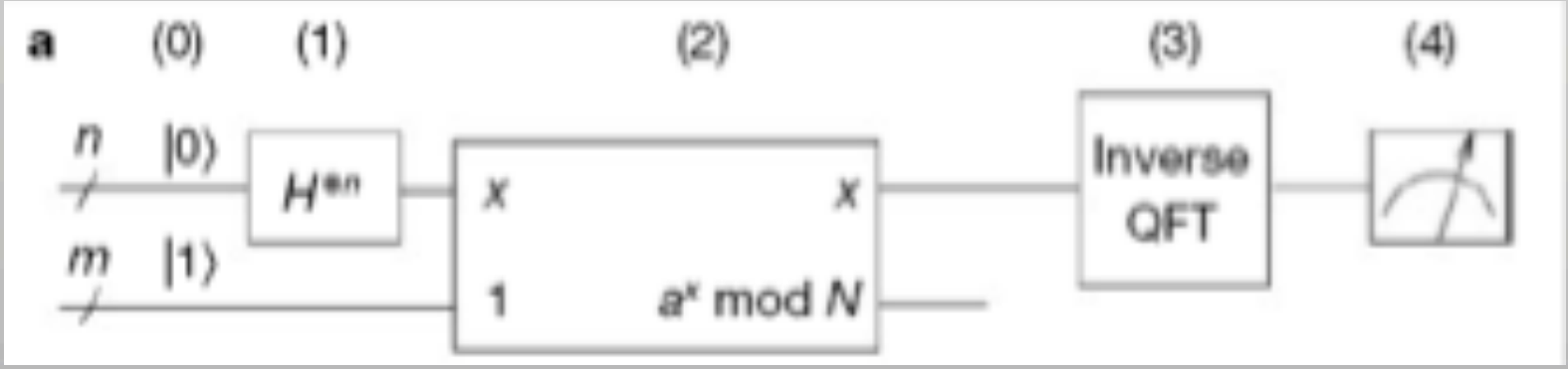


Implementation of Shor's

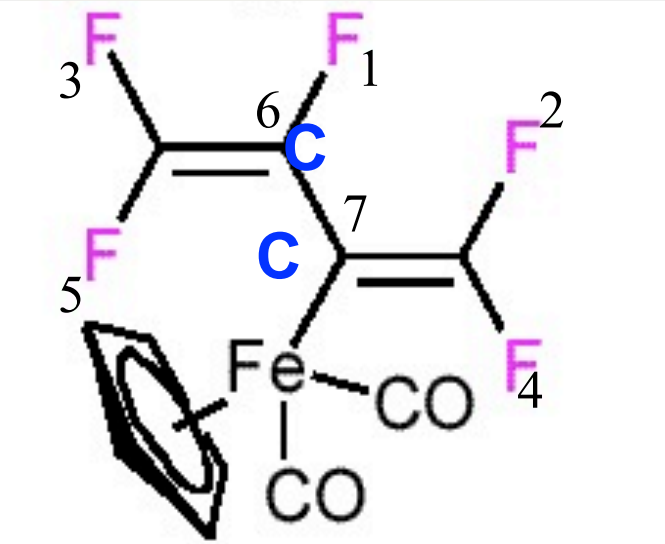


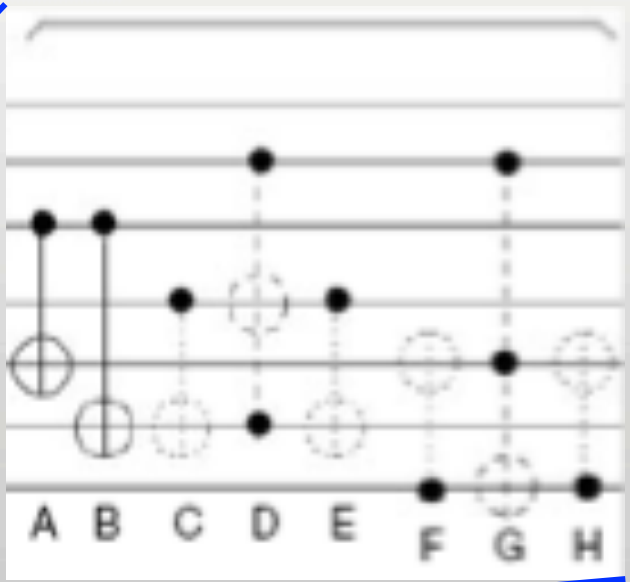
Implementation of Shor's

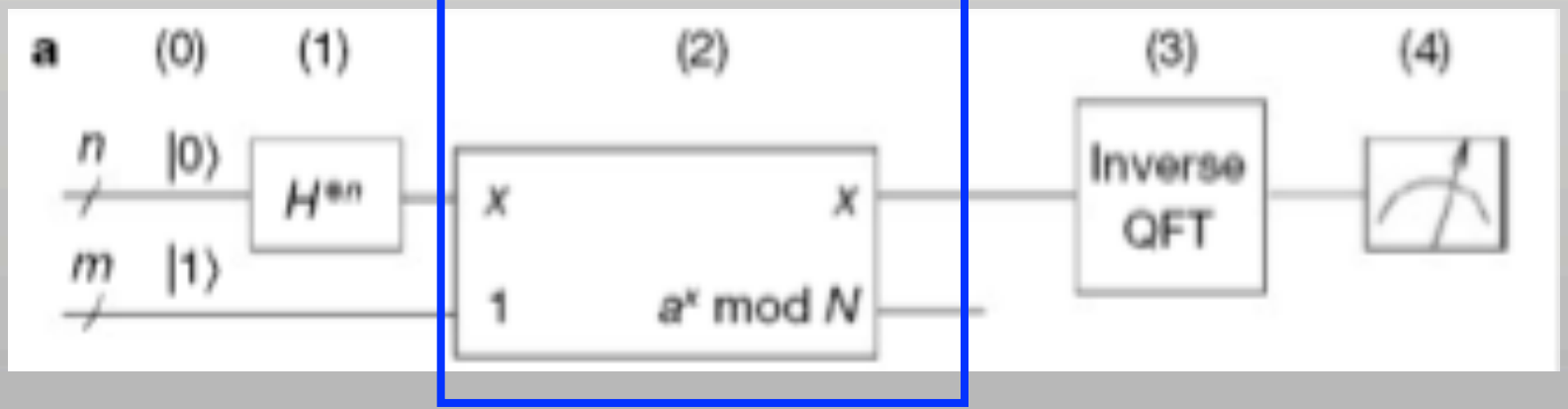




Implementation of Shor's

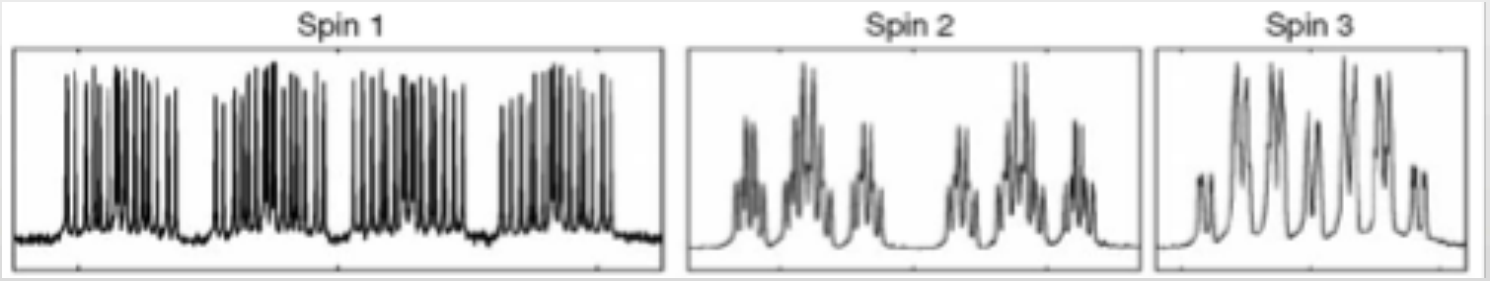




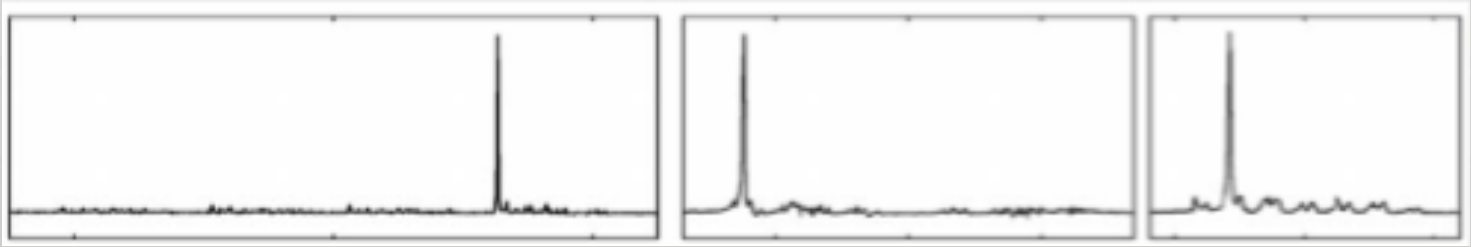


Measurement

thermal spectra

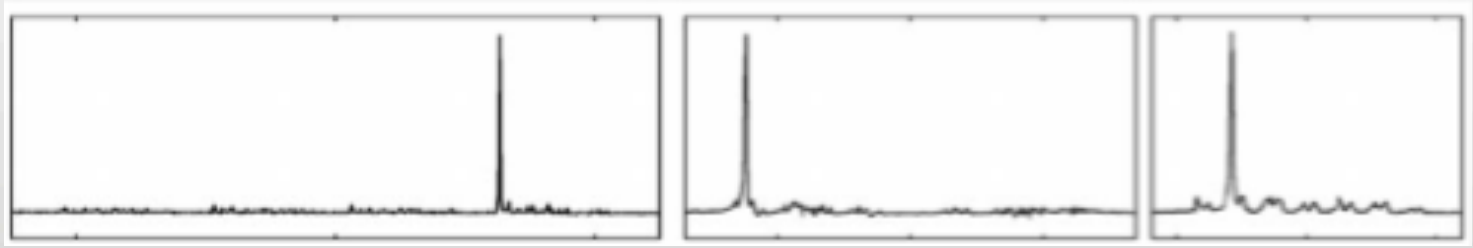


effective pure state

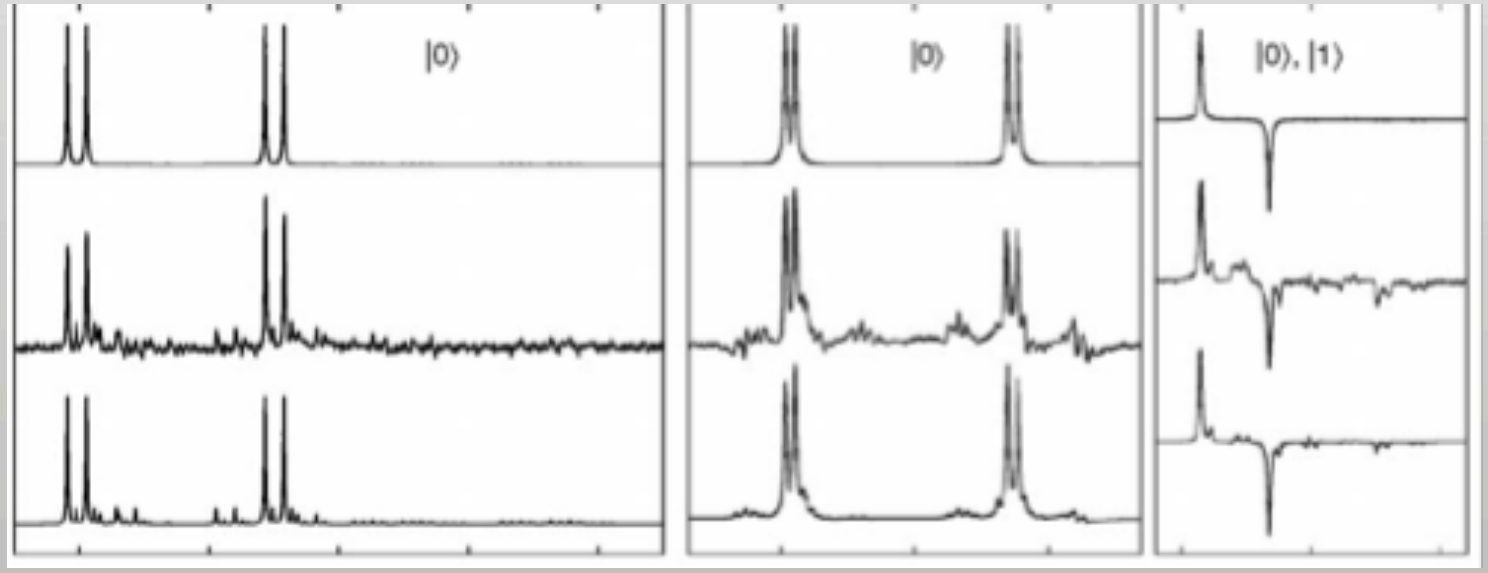


Measurement

effective pure state

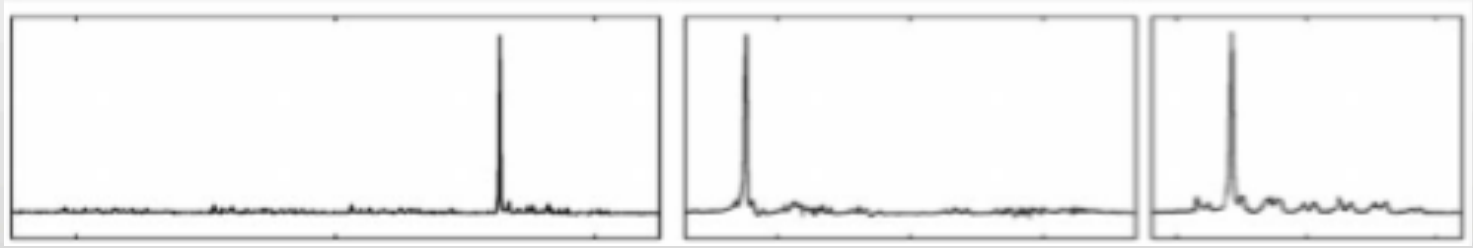


a=11

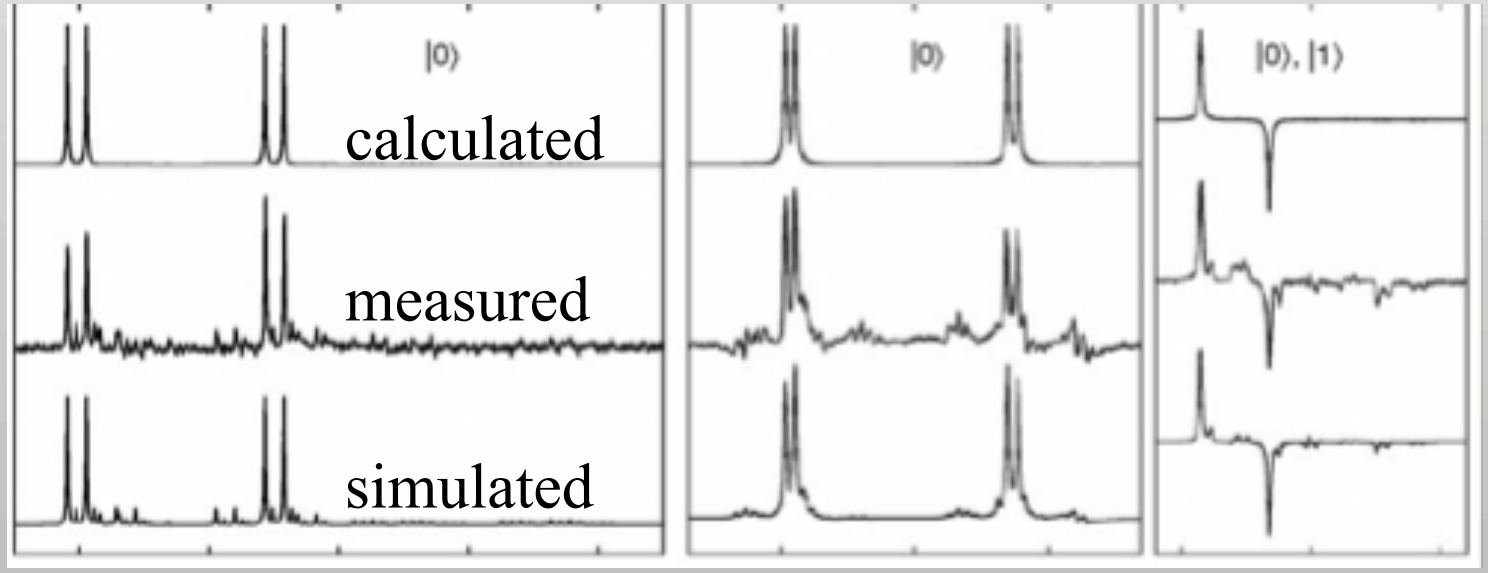


Measurement

effective pure state

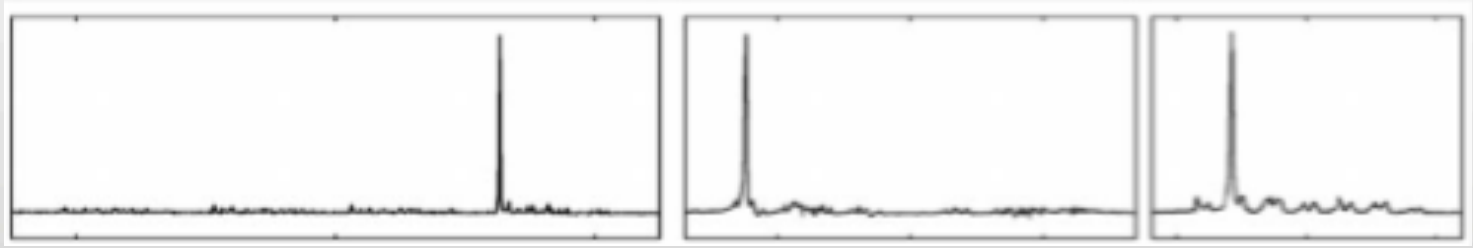


a=11

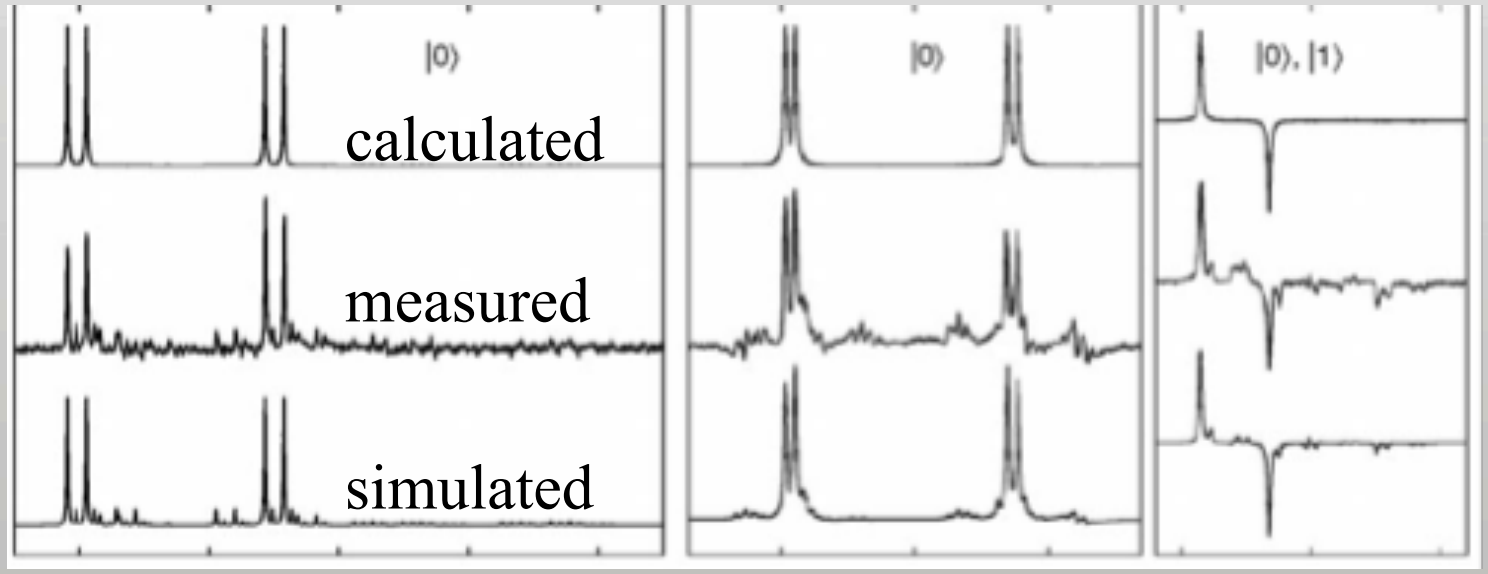


Measurement

effective pure state



a=11

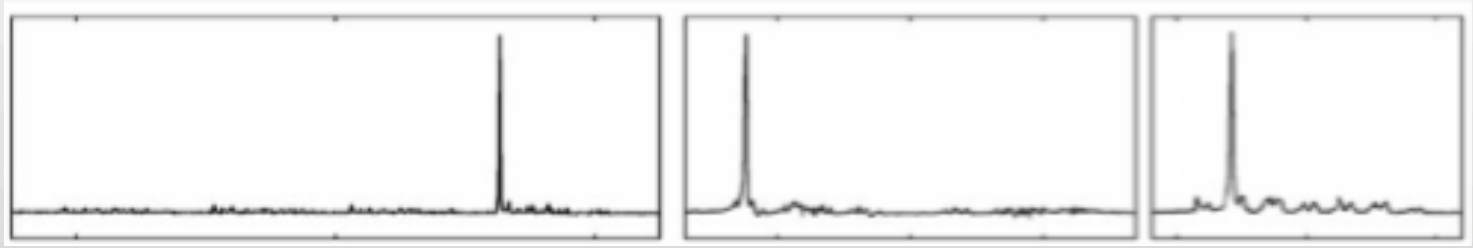


$x_0=0$ $x_1=0$ $x_2=|0\rangle+|1\rangle$

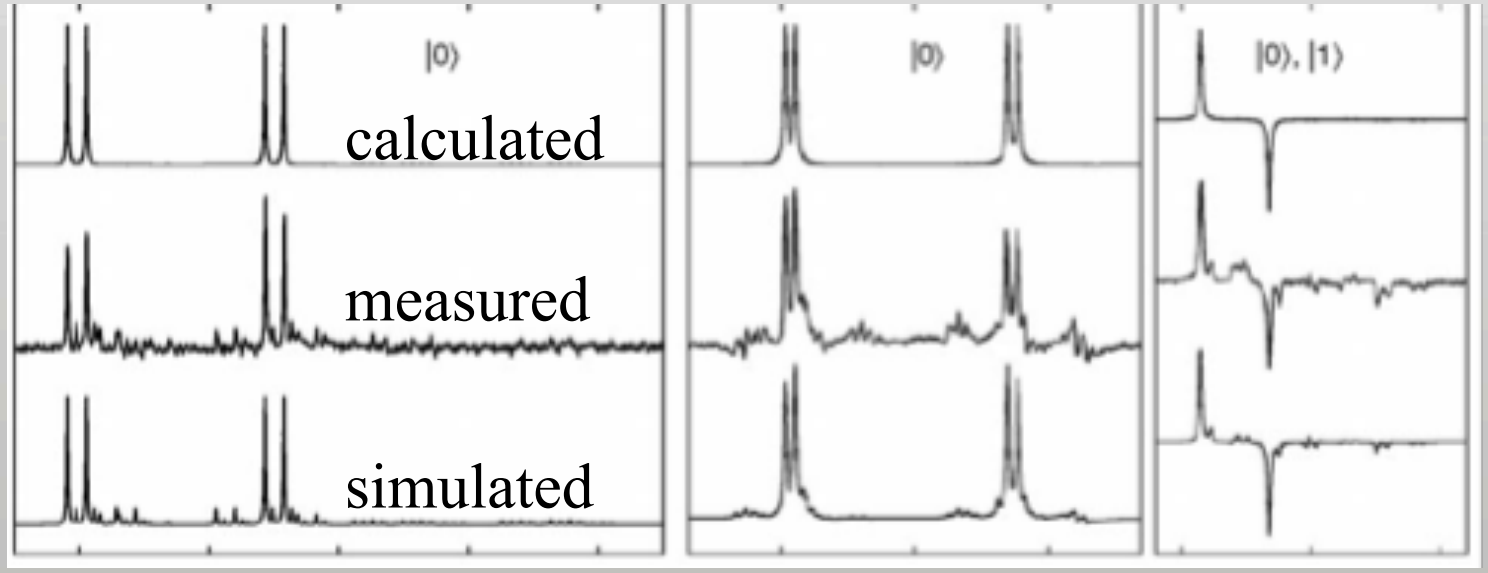
$x=|000\rangle+|100\rangle$

Measurement

effective pure state



a=11

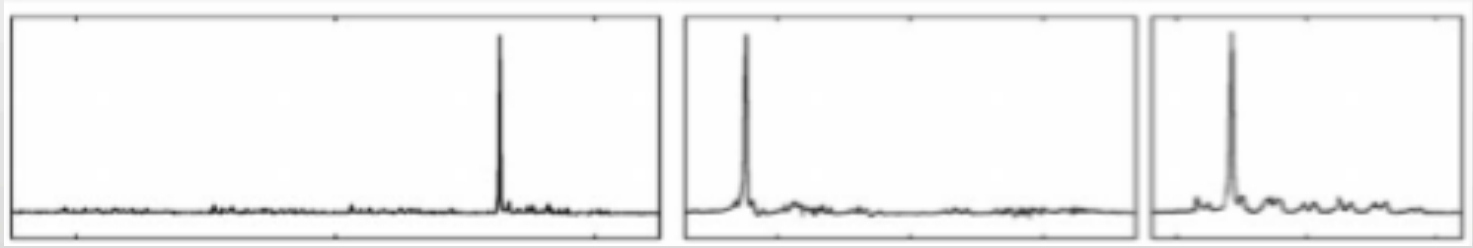


$x_0=0$ $x_1=0$ $x_2=|0\rangle+|1\rangle$

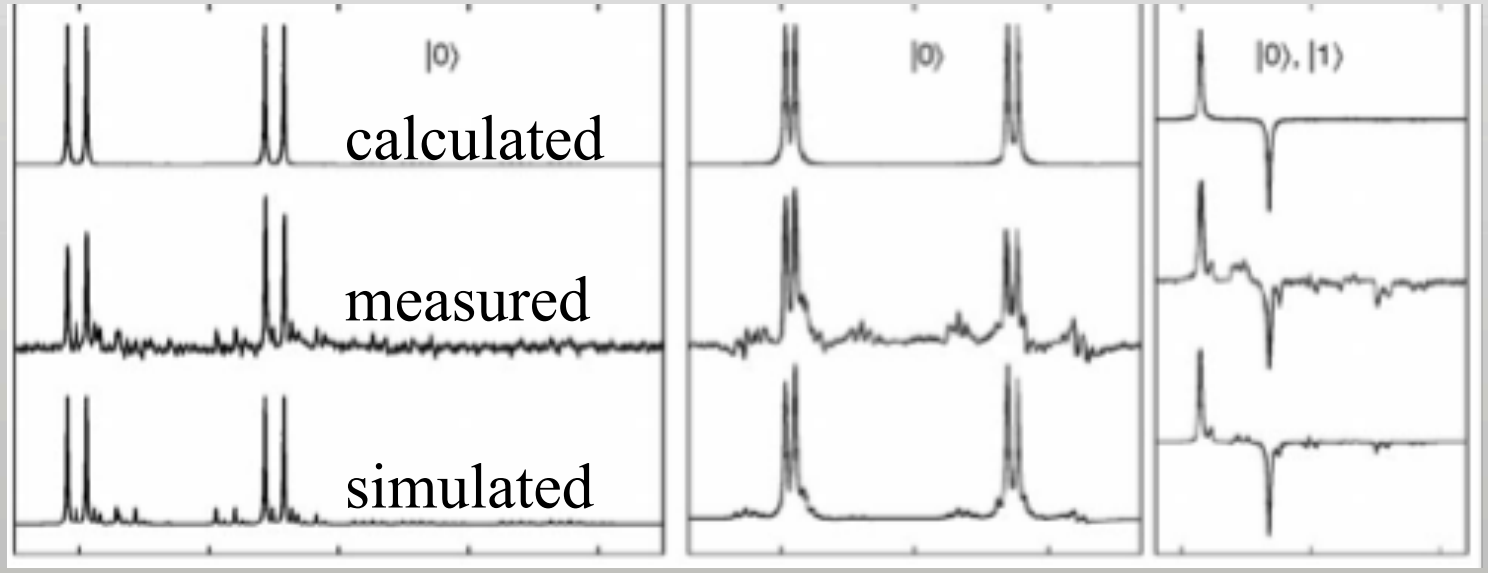
$x=|000\rangle+|100\rangle = |0\rangle+|4\rangle$

Measurement

effective pure state



a=11

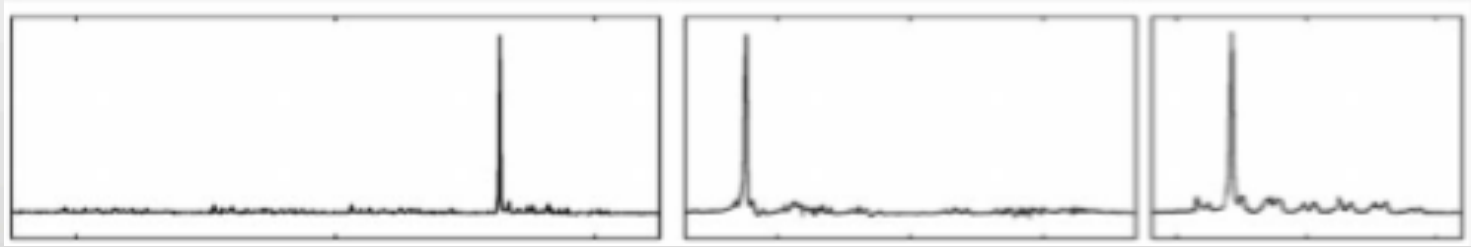


$x_0=0$ $x_1=0$ $x_2=|0\rangle+|1\rangle$

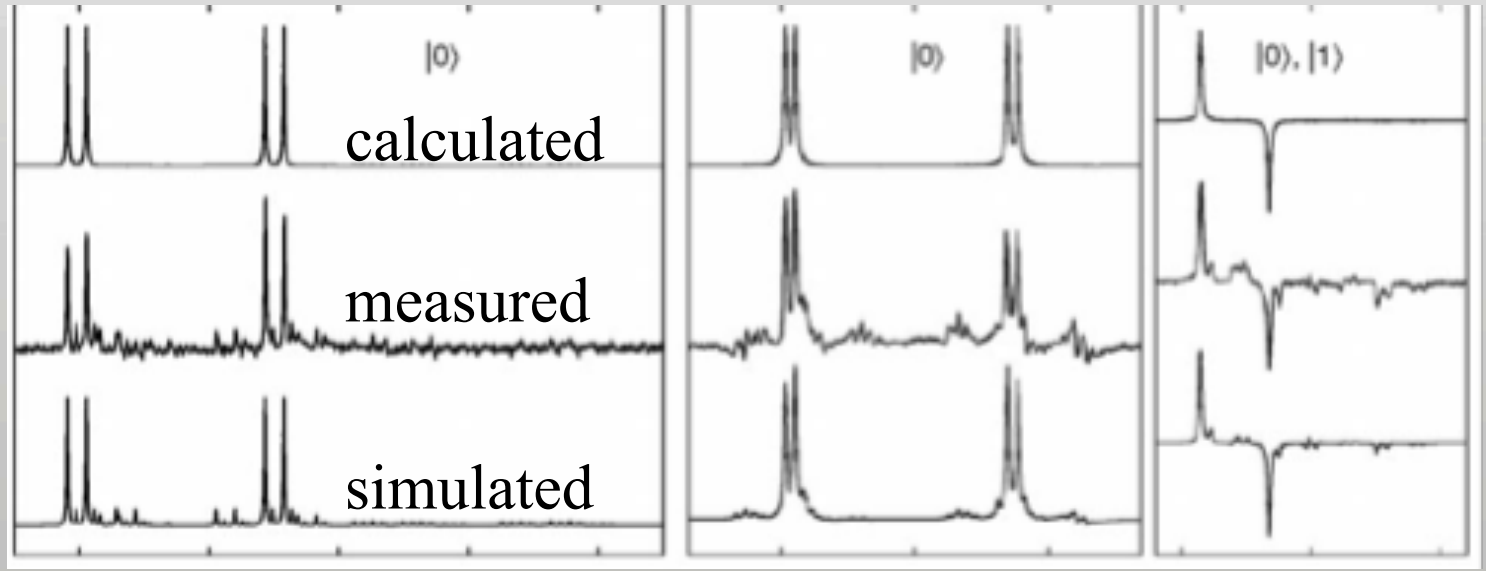
$x=|000\rangle+|100\rangle = |0\rangle+|4\rangle \Rightarrow r=2^n/4=2$

Measurement

effective pure state



a=11

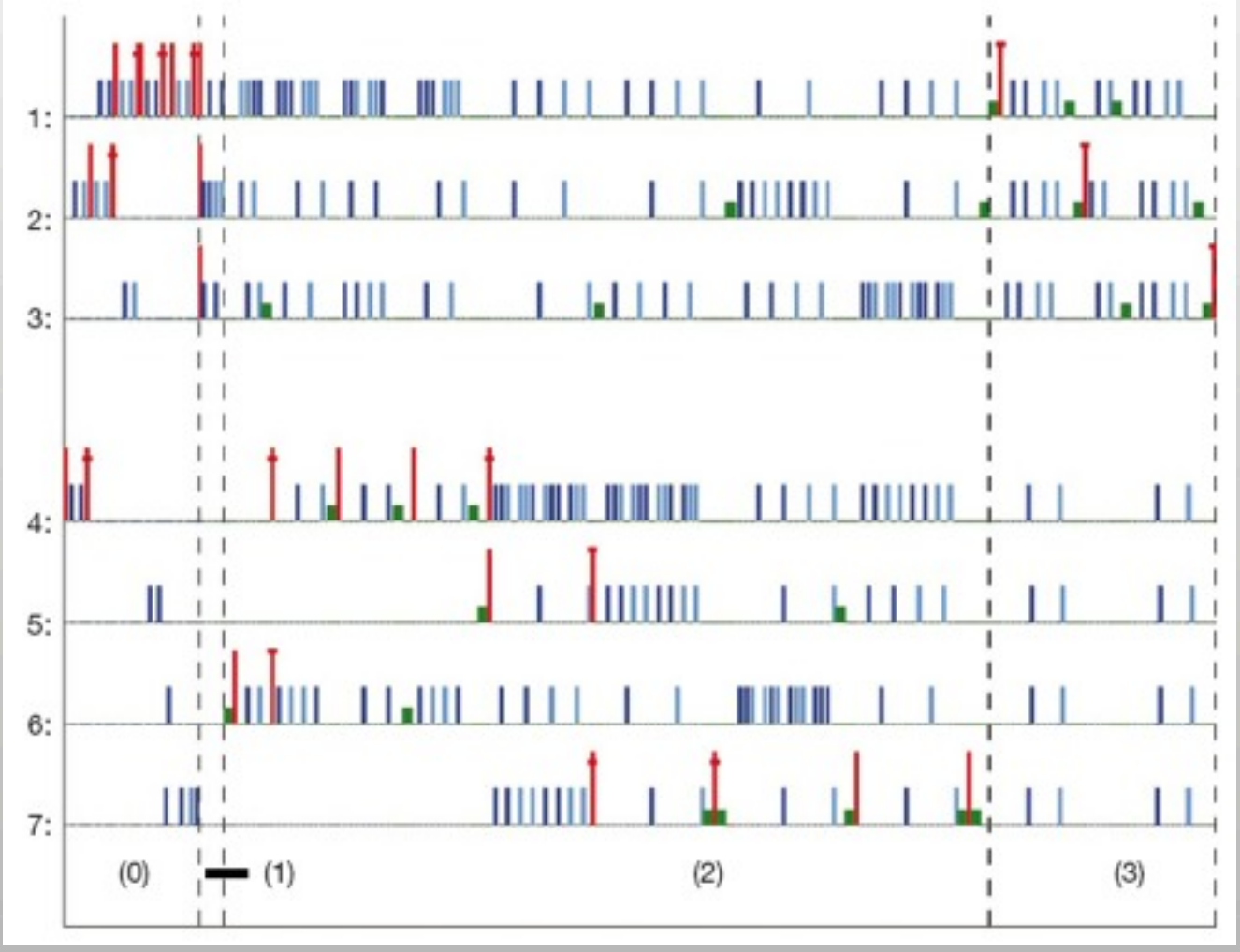


$x_0=0$ $x_1=0$ $x_2=|0\rangle+|1\rangle$

$x=|000\rangle+|100\rangle = |0\rangle+|4\rangle \Rightarrow r=2^n/4=2$ $\gcd(11^{2/2}\pm1,15)=3,5$

Pulse sequence

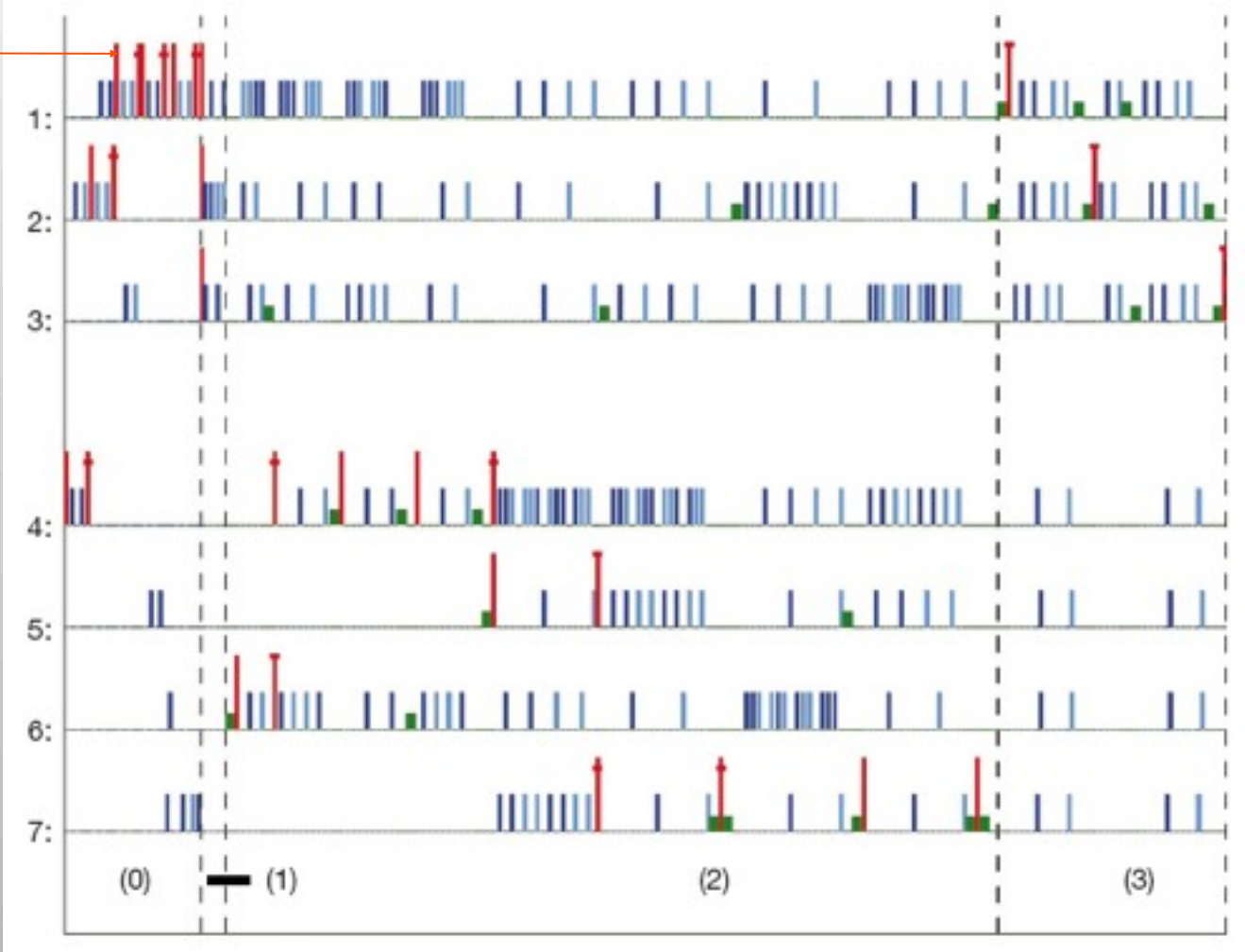
total ~300 pulses



Pulse sequence

total ~300 pulses

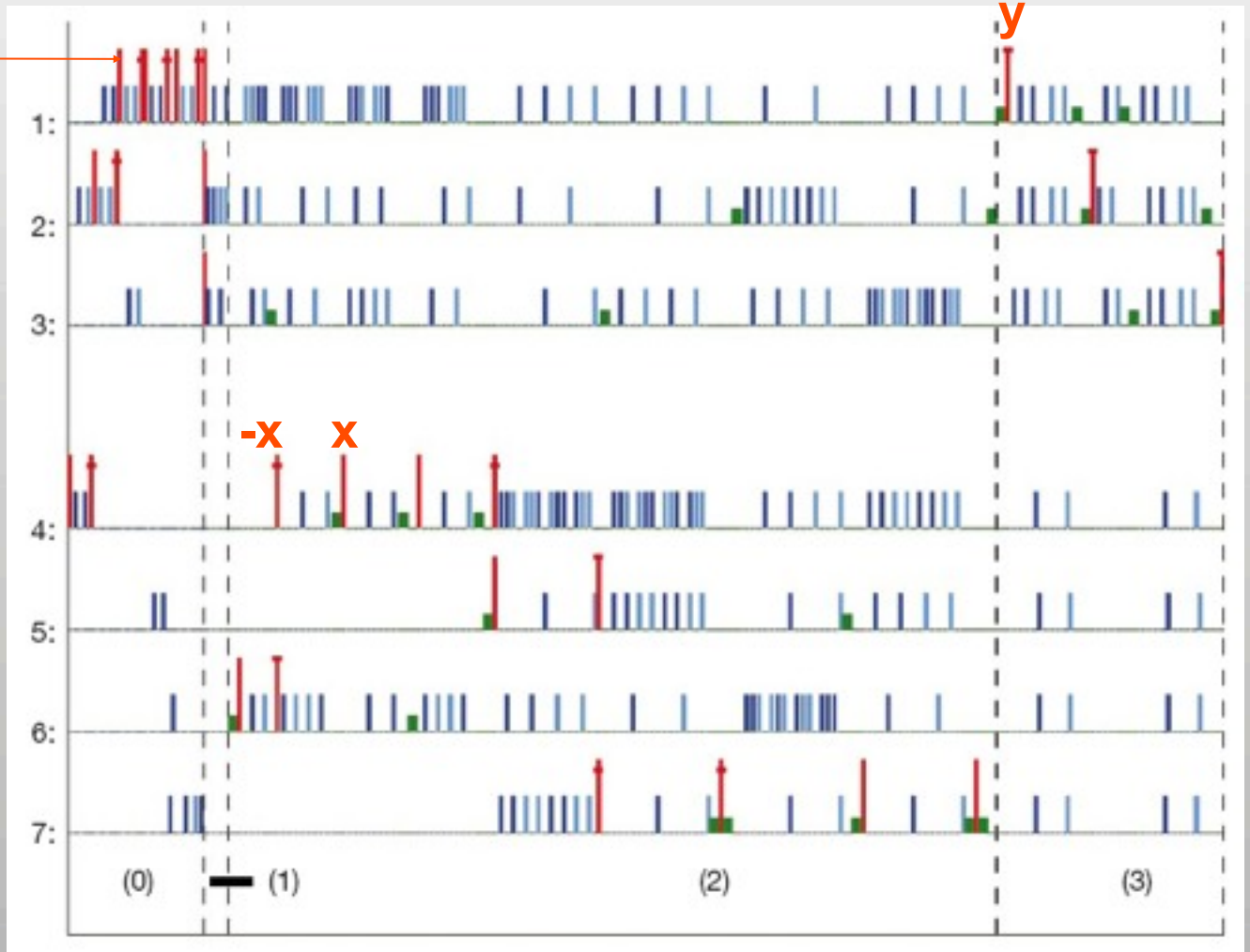
90°pulse



Pulse sequence

total ~300 pulses

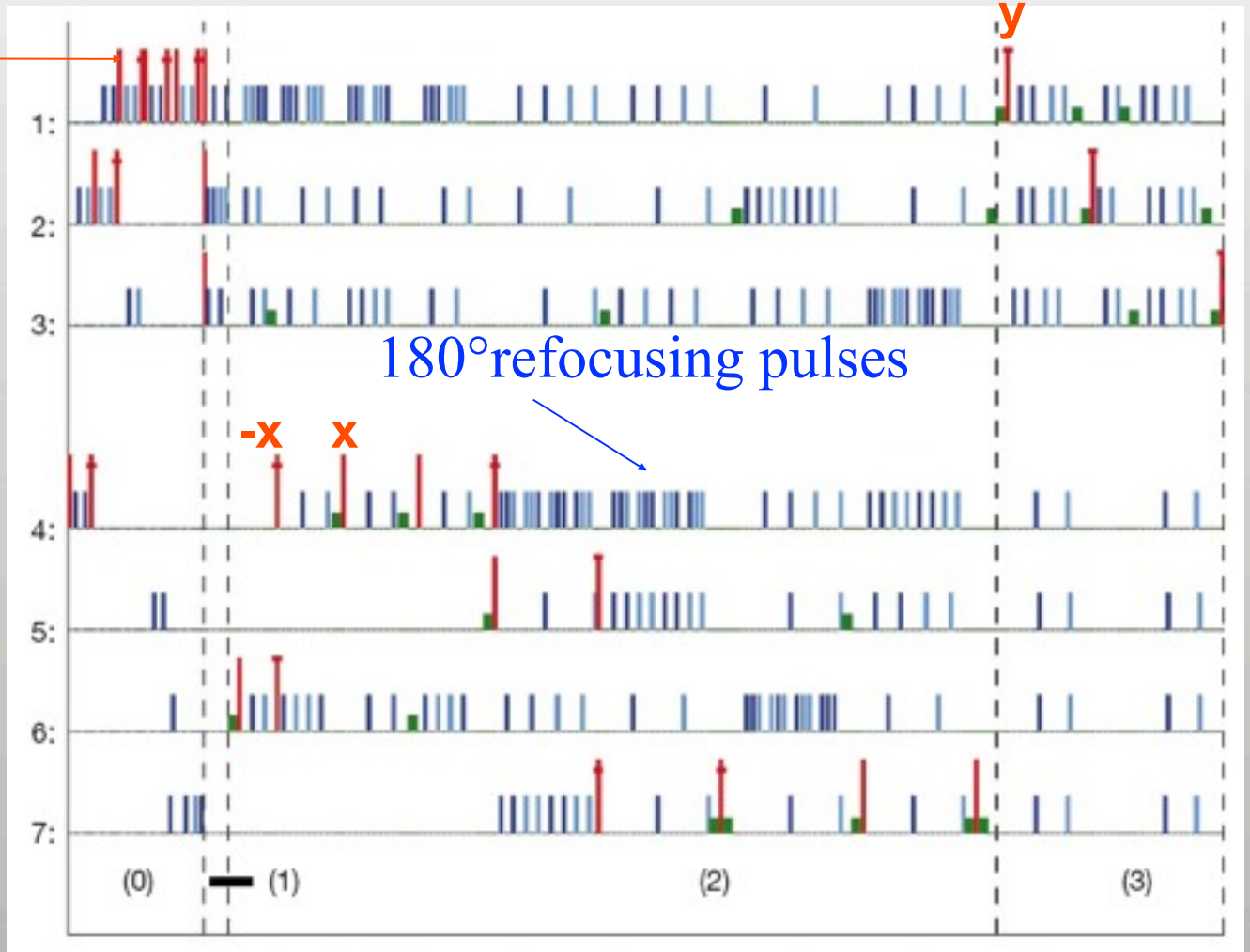
90°pulse



Pulse sequence

total ~300 pulses

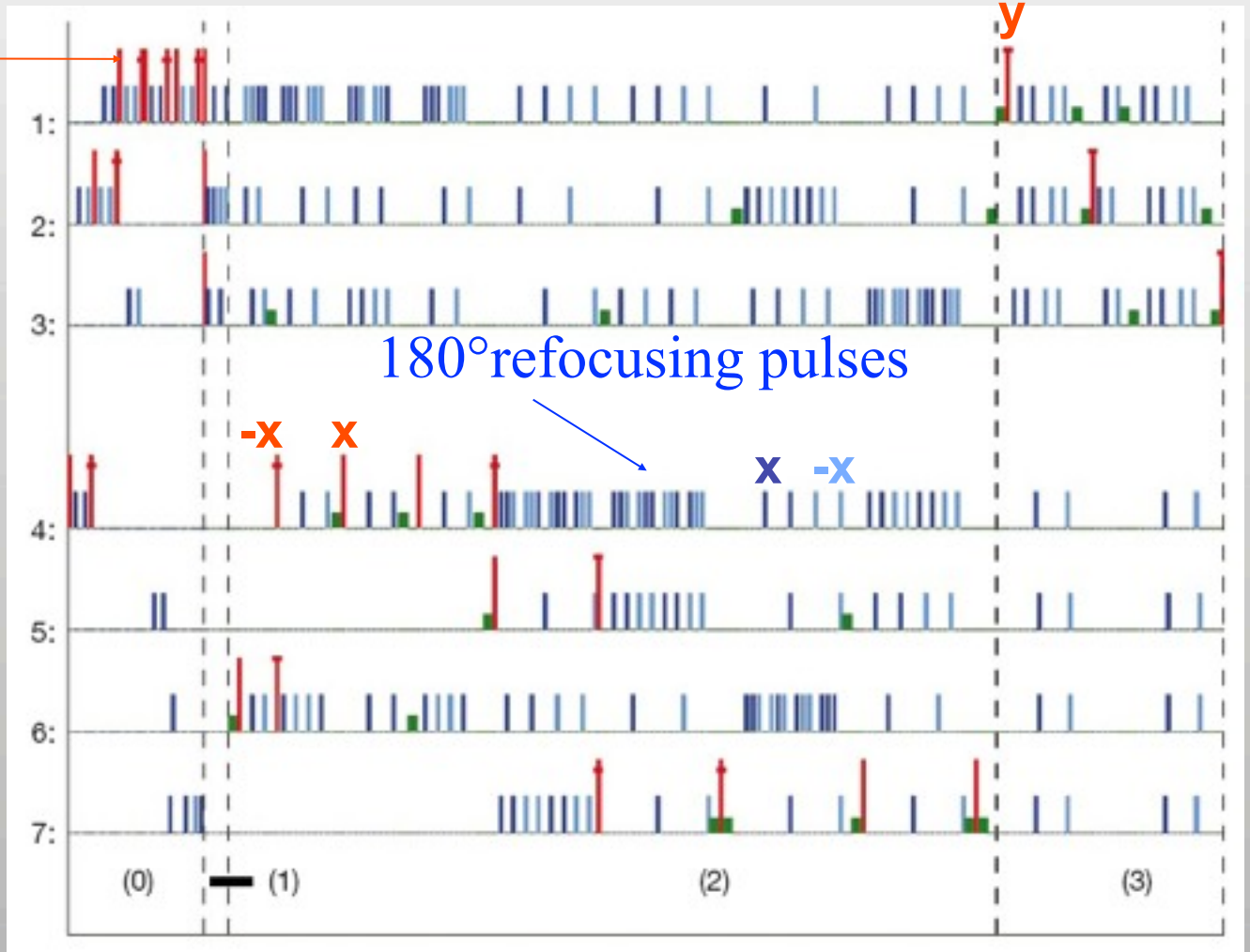
90°pulse



Pulse sequence

total ~300 pulses

90°pulse



Pulse sequence

total ~300 pulses

90°pulse