Principles of Quantum Computation, a Physicist's View: Computation is a Physical Process!

Gerd Schön *Karlsruhe Institute of Technology*

- **Physics of 2-level quantum systems (spins)**
  - states: superposition, entangled states
  - unitary time evolution (spin rotation, phase shifts,…)
  - phase coherence, dephasing, measurement process

- **Elementary operations for quantum computation: "gates"**

  NOT, $\sqrt{\text{NOT}}$, U(φ), CNOT, CU(φ), ... reversible! (unitary time evolution)

  quantum parallelism ⇒ huge gain in speed

  reduction by measurement ⇒ huge loss of information

- **Examples of quantum computation**
  - discrete Fourier-transformation
  - Shor's algorithm for factorizing large integers
  - principles of error correction

- **Physical realizations of qubits and gates**

Spin-1/2 System:

- basis states $|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- superposition $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1$
- N spins: Hilbert space of 2^N dimensions
  - ‘simple’ states (product states)

$$|\psi\rangle = \left(\alpha_1|\uparrow\rangle_1 + \beta_1|\downarrow\rangle_1\right) \times \left(\alpha_2|\uparrow\rangle_2 + \beta_2|\downarrow\rangle_2\right) \times \ldots \left(\alpha_N|\uparrow\rangle_N + \beta_N|\downarrow\rangle_N\right)$$

  - ‘entangled’ states (cannot be written as product state)

e.g. spin singlet state: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right)$

arise as result of interaction

‘exotic’ $\Rightarrow$ Bell’s inequality, EPR paradox

- Operators: Pauli matrices σ_x, σ_y, σ_z

  e.g. spin in magnetic field $H = B_x\, \sigma_x + B_y\, \sigma_y + B_z\, \sigma_z$

- Time evolution described by Hamiltonian / unitary operation

  phase coherent, reversible

$$i\hbar \frac{\partial}{\partial t}\Psi(t) = H(t)\Psi(t) \quad \Leftrightarrow \quad \left|\psi(t)\right\rangle = U(0,t)\left|\psi(0)\right\rangle$$

$$U(0,t) = \mathrm{T}\exp\left(-\frac{i}{\hbar}\int_0^t dt'\, H(t')\right)$$

$$UU^{+} = 1$$

- Quantum statistics: density matrix $\rho(t)$

  pure state $\left|\psi\right\rangle = \alpha\left|\uparrow\right\rangle + \beta\left|\downarrow\right\rangle \quad \Rightarrow \rho = \left|\psi\right\rangle\left\langle\psi\right| = \begin{pmatrix} |\alpha|^2, & \alpha\beta^* \\ \alpha^*\beta, & |\beta|^2 \end{pmatrix}$

  ‘mixed states’ described only by $\rho(t)$

  dephasing $\Rightarrow$ off-diagonal elements decay (on time scale $T_2 = \tau_\varphi$)

  relaxation $\Rightarrow$ approach to thermal distribution (on time scale T_1)

Quantum computation:

- store information in spin state / qubit
- program: manipulate qubits by controlling Hamiltonian
- model Hamiltonian [switch on and off $B_\nu^i(t)$ and $J^{ij}(t)$]:

$$H(t) = -\sum_{i=1}^{N}\left[B_x^i(t)\,\sigma_x^i + B_z^i(t)\,\sigma_z^i\right] - \sum_{i<j} J^{ij}(t)\sigma_+^i\sigma_-^j + h.c.$$

allows "universal set of gates" (sufficient for all needed logic operations)

1. single-bit logic gate: spin rotation of spin *i*

$H(t) = -B_x^i\,\sigma_x^i$ for some time τ

$$U_x^i(\varphi) = \exp\left(i\,B_x^i\,\sigma_x^i\,\tau/\hbar\right) = \begin{pmatrix} \cos\varphi & i\sin\varphi \\ i\sin\varphi & \cos\varphi \end{pmatrix}, \quad \varphi = \frac{B_x^i\,\tau}{\hbar}$$

creates superposition of states, logic iNOT for $\varphi = \pi/2$, $\sqrt{\mathrm{iNOT}}$ for $\varphi = \pi/4$.

2. phase shift

$H(t) = -B_z^i\,\sigma_z^i$ for some time τ

$$U_z^i(\varphi) = \exp\left(i\,B_z^i\,\sigma_z^i\,\tau/\hbar\right) = \begin{pmatrix} \exp(i\varphi) & 0 \\ 0 & \exp(-i\varphi) \end{pmatrix}, \quad \varphi = \frac{B_z^i\,\tau}{\hbar}$$

3. two-bit gate: for spins *i* and *j*

$$H(t) = -J^{ij}\ \sigma_+^i \sigma_-^j + h.c.$$

for some time τ

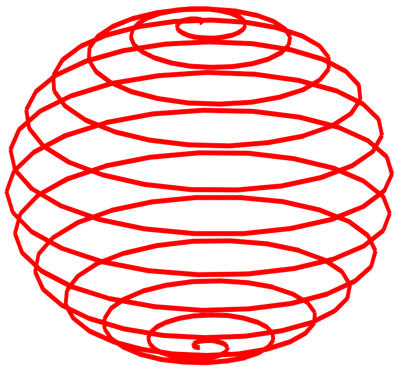
$$U_{2-bit}^{i}(\gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\gamma & i\sin\gamma & 0 \\ 0 & i\sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{in basis} \quad \begin{matrix} |\uparrow_i \uparrow_j\rangle \\ |\uparrow_i \downarrow_j\rangle \\ |\downarrow_i \uparrow_j\rangle \\ |\downarrow_i \downarrow_j\rangle \end{matrix}$$

$$\gamma = J^{ij}\ \tau / \hbar$$

creates entanglement, logic iSWAP for $\gamma = \pi/2$, $\sqrt{\text{iSWAP}}$ for $\gamma = \pi/4$, XNOT, ...

Spin rotation by Rabi oscillations

$$H = -\frac{1}{2}\hbar\omega_0\sigma_z - \frac{1}{2}\hbar\Omega_R(\cos\omega t\ \sigma_x + \sin\omega t\ \sigma_y)$$



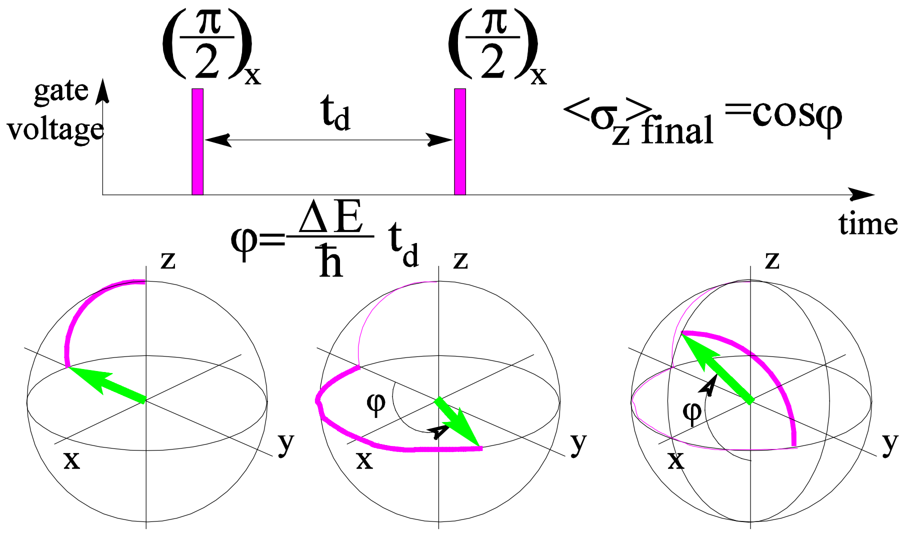
in lab frame

operate at resonance $\omega = \omega_0$

in rotating frame
(unitary transformation) $H' = -\frac{1}{2}\hbar\Omega_R\sigma_x$

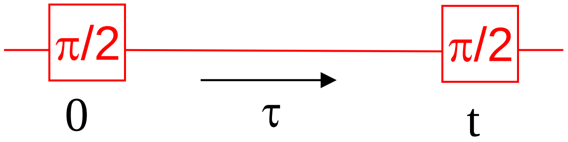
→ rotation around x'-axis

Coherent oscillations, Ramsey fringes

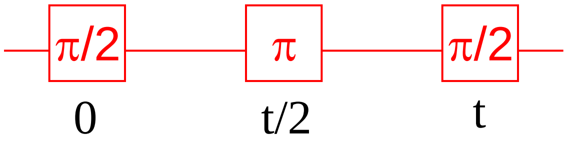


Echo experiment refocusing

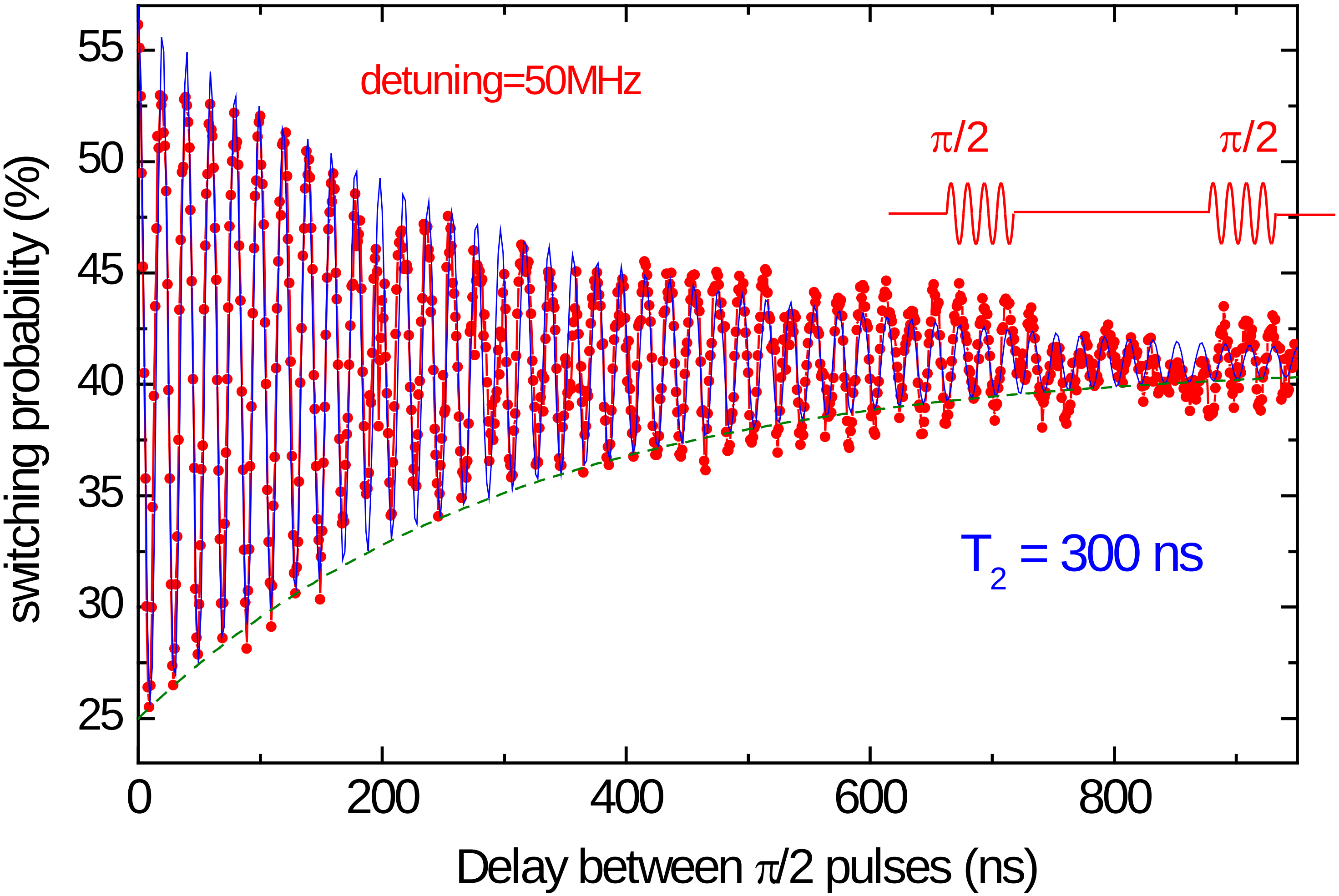
Free decay (Ramsey fringes)



Echo signal



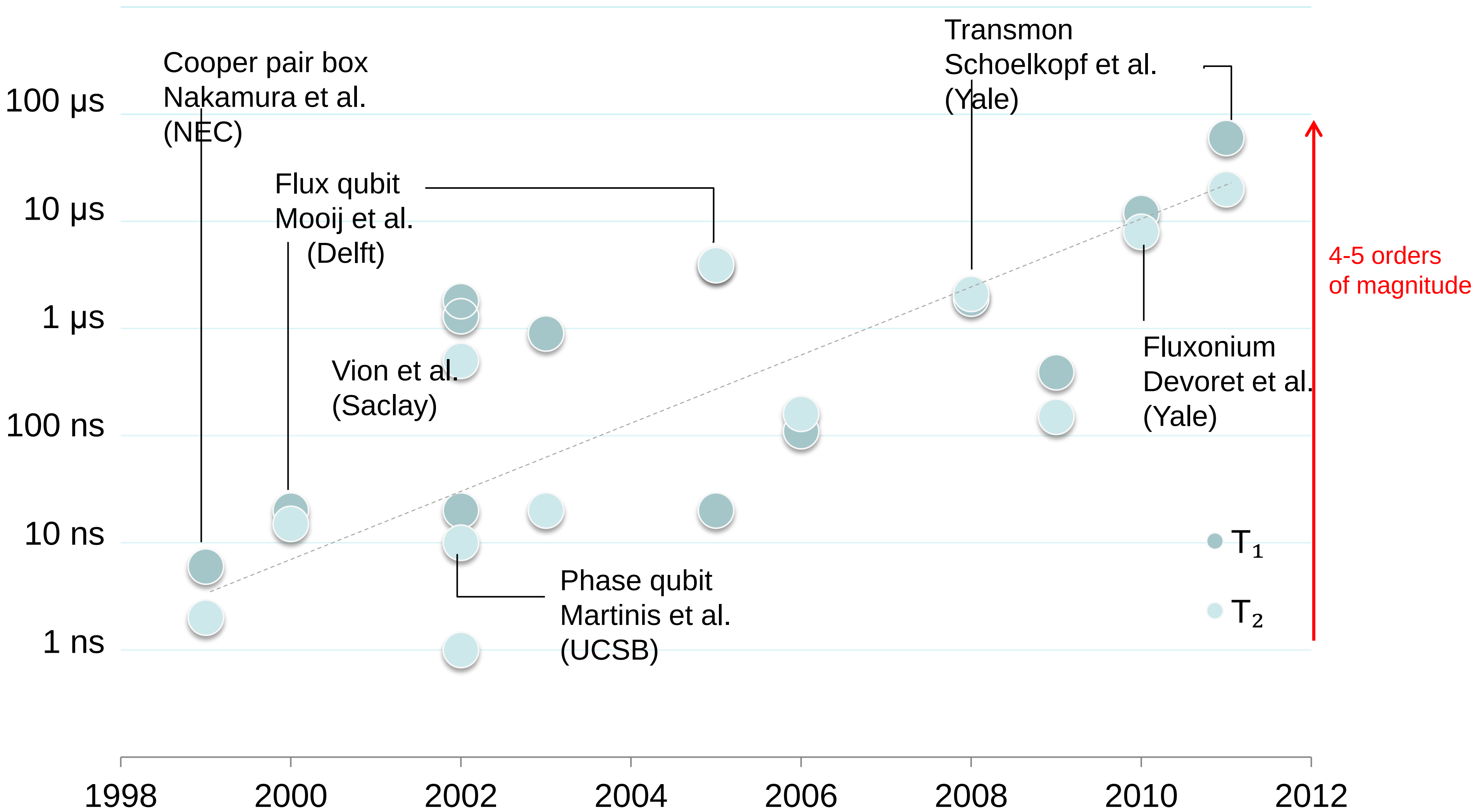
Decay of Ramsey fringes at optimal point



Vion et al. (Saclay), Science 02

Superconducting qubits: coherence times

Moore's law?



Courtesy of Jens Koch, Northwestern U.

Elements of quantum computation:

classical: bits, registers, elementary gate NAND is sufficient,
reset bits to zero (delete information, enhance entropy)
functions $x \rightarrow f(x)$, in general irreversible

quantum: qubits, quantum register, universal set of gates,
all steps (except measurement) phase coherent
functions $|x,0> \leftrightarrow |x, f(x)>$ reversible

2^N numbers represented by register of N qubits

$$|0\rangle = |\uparrow .. \uparrow\uparrow\uparrow\rangle$$
$$|1\rangle = |\uparrow .. \uparrow\uparrow\downarrow\rangle$$
$$...$$
$$|2^N - 1\rangle = |\downarrow .. \downarrow\downarrow\downarrow\rangle$$

Quantum Parallelism

Start with superposition of states (e.g. all integers $0 \leq x \leq 2^N$-1)

$$|\psi(t=0)\rangle = \frac{1}{2^{N/2}}(|\uparrow\rangle_1 + |\downarrow\rangle_1)(|\uparrow\rangle_2 + |\downarrow\rangle_2)...(|\uparrow\rangle_N + |\downarrow\rangle_N) = \frac{1}{2^{N/2}}\sum_{x=0}^{2^N-1}|x\rangle$$

perform unitary operations (= program) on all states simultaneously.

$$|\{x\},\{0\}\rangle \rightarrow |\{x\},\{f(x)\}\rangle$$

I.e. get whole function in one calculation.

$\Rightarrow$ **Massive parallel computation!**

Quantum Measurement:

At the end one can read out the state of N qubits.

N measurements provide much less information than contained in the quantum states (2^N amplitudes).

For some applications this is enough!

- Shor’s algorithm for factorization of large integers
- Grover’s algorithm for seeking a needle in a haystack
- Simulating quantum problems (time evolution, ground state,…)

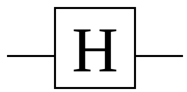
Examples of logic gates

Hadamard gate

acting on one qubit (*i*)

$$|\uparrow\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$$

$$|\downarrow\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right)$$



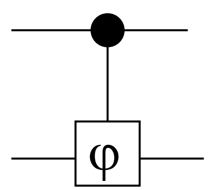
$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = i\exp\left(-i\frac{\pi}{2}\frac{\sigma_x^i + \sigma_z^i}{\sqrt{2}}\right)$$

Controlled phase shift gate

acting on 2 qubits (*i* and *j*)

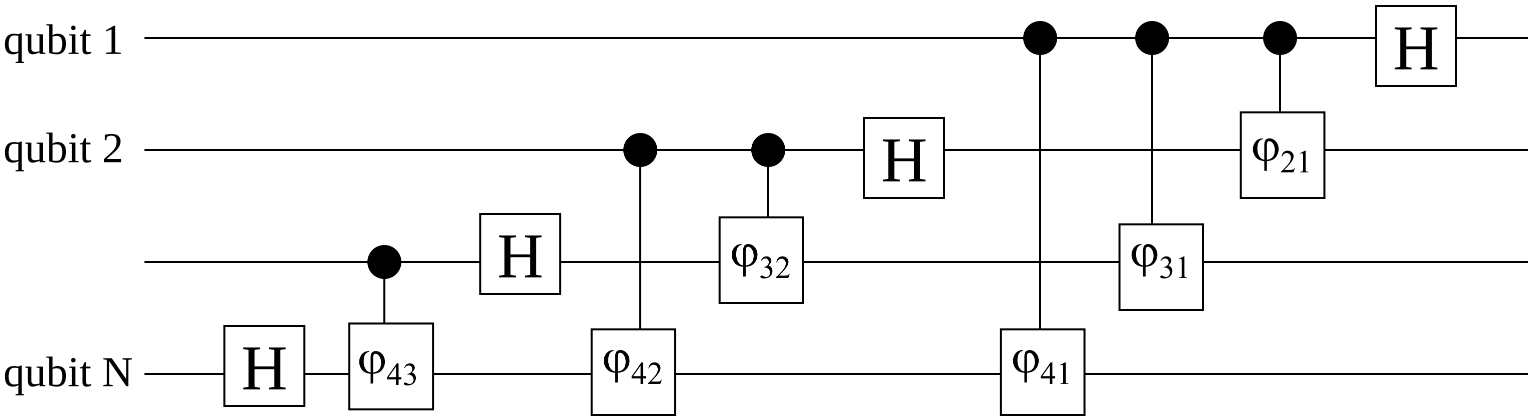
$$|\uparrow\uparrow\rangle \rightarrow |\uparrow\uparrow\rangle, \quad |\uparrow\downarrow\rangle \rightarrow |\uparrow\downarrow\rangle$$

$$|\downarrow\uparrow\rangle \rightarrow |\downarrow\uparrow\rangle, \quad |\downarrow\downarrow\rangle \rightarrow e^{i\varphi}|\downarrow\downarrow\rangle$$



$$\Leftrightarrow \exp\left(-i\varphi\left(\sigma_+^i\sigma_-^j + \sigma_-^i\sigma_+^j\right)\right)$$

Example: Fourier transformation



$\varphi_{ij} = \pi/2^{|i-j|}$

$$|0\rangle = |\uparrow..\uparrow\uparrow\uparrow\rangle$$
$$|1\rangle = |\uparrow..\uparrow\uparrow\downarrow\rangle$$
$$\ldots$$
$$|2^N - 1\rangle = |\downarrow..\downarrow\downarrow\downarrow\rangle$$

$$\sum_{x=0}^{2^N-1} a_x |x\rangle \quad \Rightarrow \quad \sum_{k=0}^{2^N-1} c_k |k\rangle$$

superposition
of all states

$$c_k = \frac{1}{2^N} \sum_{x=0}^{2^N-1} \exp\left(\frac{2\pi\, i\, k\, x}{2^N}\right) a_x$$

# of quantum gates ~ N^2 ⇔ classical FFT ~ 2^N

Factorization of large integers

The factorization of large integers with *N* digits is intractable on a **classical computer** (state of the art, best known algorithm):

$t \approx \exp[a\, N^{1/3}]$	$\approx$ 1 month CPU	for N =130 digits
exponential	$\approx 10^{10}$ years	for N =400 digits

quantum computer (Shor's algorithm):

$t \approx a\, N^3$	$\approx$ 1 month (e.g.)	for N =130 digits
polynomial	$\approx$ 3 years	for N =400 digits

High interest in the problem since RSA **cryptosystem**
(used by banks, Netscape, ...).
Relies on *assumption* that the factorization is difficult.

RSA cryptosystem

(Rivest, Shamir, Adleman '78)

Alice	public channel	Bob
		p,q large primes, $n = p\,q$
		$p=5,\ q=3$ $\quad$ $n= 15$
		$e > 1$ coprime with p -1,q -1
		e=3 no common divisor with 4, 2
	$\leftarrow$ ***n*,*e*: public key**	$e\,d = 1 \bmod (p-1)(q-1)$
	n=15,e=3	$3\,d = 1 \bmod 8 \rightarrow d=3$
		***n*,*d*: secret key**
message m	$\rightarrow s=m^e \bmod n$	$s^d \bmod n = m$
$m = 2$	$2^3 \bmod 15 = 8$	$8^3 \bmod 15 = 512 \bmod 15 = 2$
3	$3^3 \bmod 15 = 12$	$12^3 \bmod 15 = 1728 \bmod 15 = 3$
4	$4^3 \bmod 15 = 4$	$4^3 \bmod 15 = 4$
5	$5^3 \bmod 15 = 5$	$5^3 \bmod 15 = 5$

Shor's algorithm

1. Elements of number theory:

- find factors of n (= $p\,q$) $\Leftrightarrow$ find period r of $f_{a,n}(x) = a^x \bmod n$
  'intractable' on classical computer
  $x = 1,2,3,\ldots$ a random, coprime with n
  equally 'intractable'

- if r is even, and $r \bmod n \neq -1 \Leftrightarrow p,q = \gcd(a^{r/2} \pm 1, n)$

- greatest common divisor can be found in polynomial time *(Euclid, 300 BC)*

Example: $n = 15$

select $a = 2$

$x = 1,2,3,4,5,6,7,\ldots \Rightarrow f_{a,n}(x) = a^x \bmod n = 2,4,8,1,2,4,8,1,\ldots \Rightarrow$ period $r = 4$

$\Rightarrow a^{r/2} = 4$, $p = \gcd(3, 15) = 3$, $q = \gcd(5, 15) = 5$ $\Rightarrow n = 3 \times 5$

for $a = 7$ $\Rightarrow f_{a,n}(x) = a^x \bmod n = 7,4,13,1,7,4,13,\ldots \Rightarrow$ period $r = 4$

different function $f_{a,n}(x)$, but same period,

$\Rightarrow a^{r/2} = 49$, $p = \gcd(48, 15) = 3$, $q = \gcd(50, 15) = 5$ $\Rightarrow n = 3 \times 5$

for $a = 14$ $\Rightarrow f_{a,n}(x) = a^x \bmod n = 14,1,14,1,14,1,14\ldots \Rightarrow$ period $r = 2$

$\Rightarrow a^{r/2} = 14$, method fails

2. Exploit quantum parallelism:

compute $f_{a,n}(x) = a^x \bmod n$ for all x simultaneously

- initial state $|0^N\rangle|0^N\rangle$ (2N qubits)
- apply N Hadamard gates $H_1 H_2 \ldots H_N |0^N\rangle|0^N\rangle = \frac{1}{2^N} \sum_{x=0}^{2^N-1} |x\rangle|0^N\rangle$

  $\Rightarrow$ superposition of all x
- apply $U \Rightarrow |x\rangle|f_{a,n}(x)\rangle$ $\Rightarrow$ whole function is encoded in register!

This information cannot be read out! But we need only period!

- measure second register, obtain some value j,

  $\Rightarrow$ project onto subspace of those states $|x\rangle|j\rangle$ where $f_{a,n}(x) = j$

  example: n=15, a = 2

  measure $j = 2 \Rightarrow$ post measurement state = $(|1\rangle + |5\rangle + |9\rangle + \ldots)|2\rangle$

  measure $j = 4 \Rightarrow$ post measurement state = $(|2\rangle + |6\rangle + |10\rangle + \ldots)|4\rangle$

  ...

- different measurements yield different j, project onto different subspaces, all have same period r, but different offset k_j: $|\psi\rangle = \sum_{i=0}^{2^N/r} |i\, r+k_j\rangle|j\rangle$

3. Apply discrete Fourier transform to find r

$\Rightarrow$ factorization of large integer in polynomial time!

Error correction

- Classical digital computers are reliable (0.9 → 1, 0.1 → 0)
  usually need **no** error correction.
- If needed, do so by majority vote: 0 → (000), 1 → (111)
  single bit flip error, e.g. (001), can be detected and corrected.
- Quantum computer suffers from

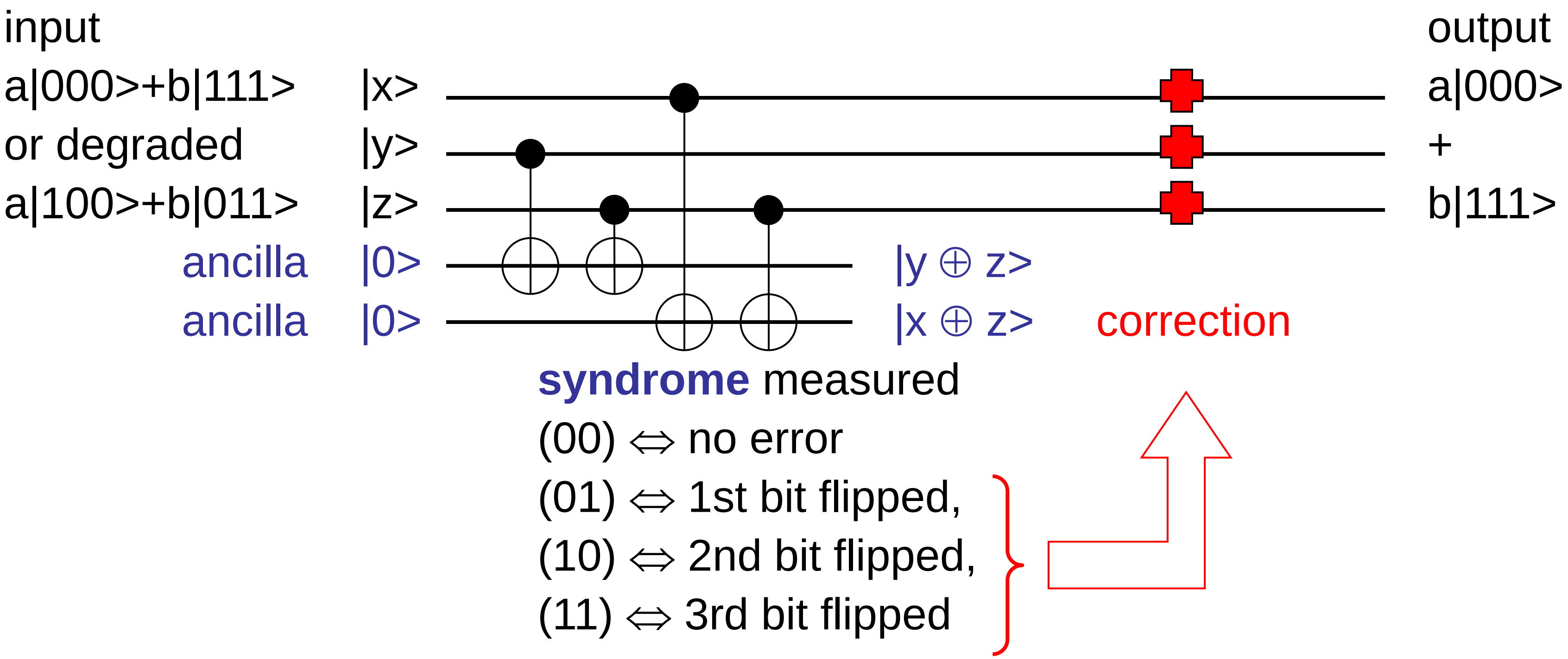
  - more errors: bit flip $|0\rangle \leftrightarrow |1\rangle$
    continuous errors $a\,|0\rangle + b\,|1\rangle \rightarrow a'\,|0\rangle + b'\,|1\rangle$
    phase errors $a\,|0\rangle + b\,|1\rangle \rightarrow a\,e^{i\beta}\,|0\rangle + b\,|1\rangle$

  - measurement interrupts quantum computation

  - cloning of quantum state is not possible

Quantum error correction: (example bit flips only)

- encode logical bits with 3 qubits |**0** > = |000>, |**1**> = |111>
- check by quantum non-demolition measurement whether spin flip occurred, read out syndrome (not the state!) and correct if needed.



All errors can be corrected by 9 qubit encoding *(Shor 95)*

5 qubit encoding *(DiVincenzo + Shor 96)*

Requirements for Quantum Information Systems

(DiVincenzo criteria)

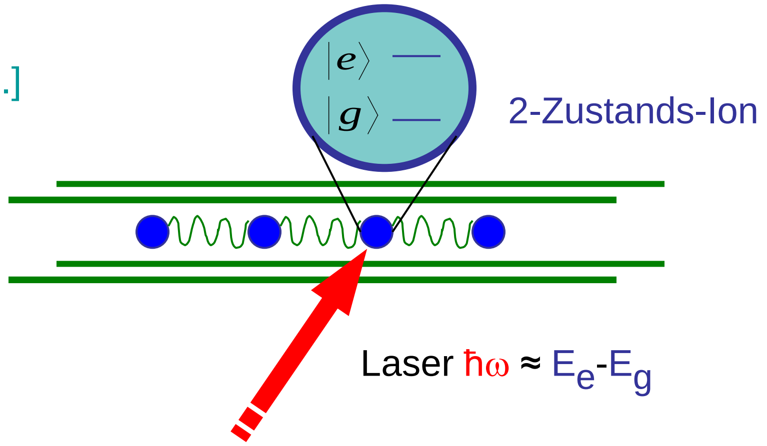
1. N well defined qubits, scalable to large *N*
2. preparation of well-defined initial state
3. all single-bit gates and some two-bit gates, forming universal set
4. long coherence time τ_φ (genauer $T_1, T_2 \geq 10^4\ \tau_{op}$)
5. read-out

Physikalische Realisierungen:

Ionen in Fallen

[Cirac und Zoller (96), Wineland et al., Blatt et al.]

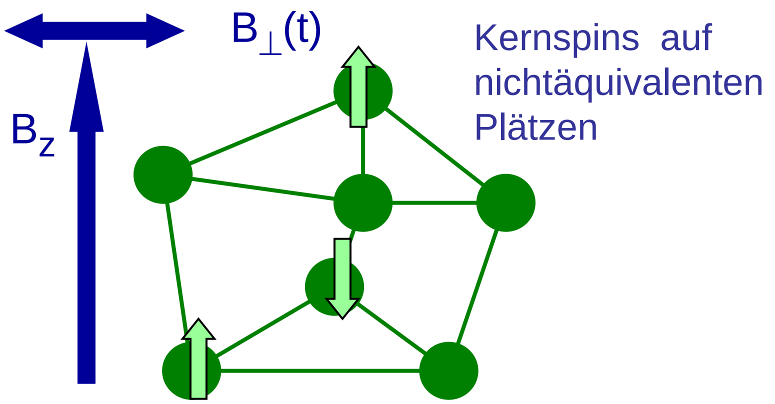
+ großartige Experimente
+ langes τ_φ
+ >10 gekoppelte qubits
– schwer in Elektronik integrierbar
– schwer zu großen N skalierbar



NMR

[Chuang et al., Vandersypen et al.]

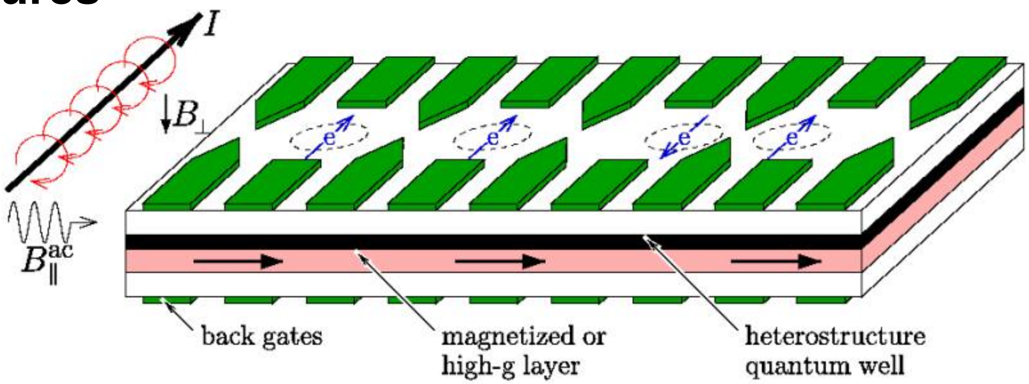
+ etablierte Technologie
+ langes τ_φ
+ 7 qubits gekoppelt
+ 15 = 3 x 5 demonstriert
– nicht zu großen N skalierbar
– sehr langsam



Electron spins in gated structures

[Loss & DiVincenzo, ...]

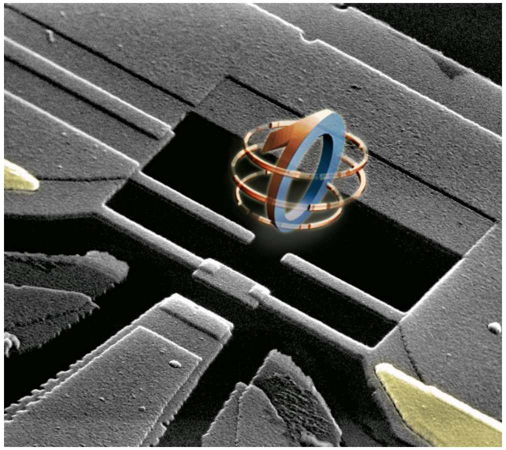
+ τ_φ for spins > τ_φ for charge
+ precisely 2 states
- experimental challenge



Josephson junction qubits

[Mooij, Shnirman&GS, Ustinov, ….]

+ technology available (SET, SQUID)
+ integrated into electronic circuit
+ scalable, 4 qubits coupled
- many sources of decoherence



Quantronium
(Saclay)

Dorit Aharonov, Quantum Computation
arXiv:quant-ph/9812037