6.2
Introduction to quantum information processing

6.2 Introduction to information processing

Information

→ General concept (similar to energy)
→ Many forms: Mechanical, thermal, electric, ...
→ Can be packed into equivalent forms:

0 1 ↓ ↑

→ Information is physical (Landauer 1991)
- Ink on paper
- Charge on capacitor
- Currents in leads
- Spins
- …

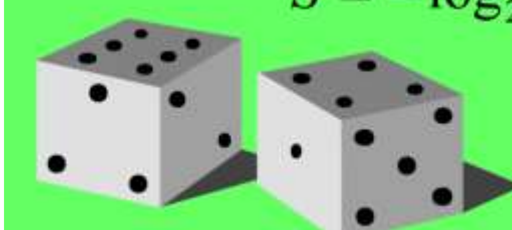
Information has uncertainty!
→ Shannon entropy
→ Measure of this uncertainty

Can be **quantified:** The random variable X distributed according to $p(x)$ contains the information

$$S[p(x)] = -\sum_x p(x)\log_2 p(x)$$

E.g., in the process of throwing a dice one may gain the information

$$S = -\log_2(1/6)$$



Konrad Zuse (1945)

→ Built the first binary digital computer („Z1“) in 1938.

→ First programmable electromechanical computer („Z3“) completed in 1941.

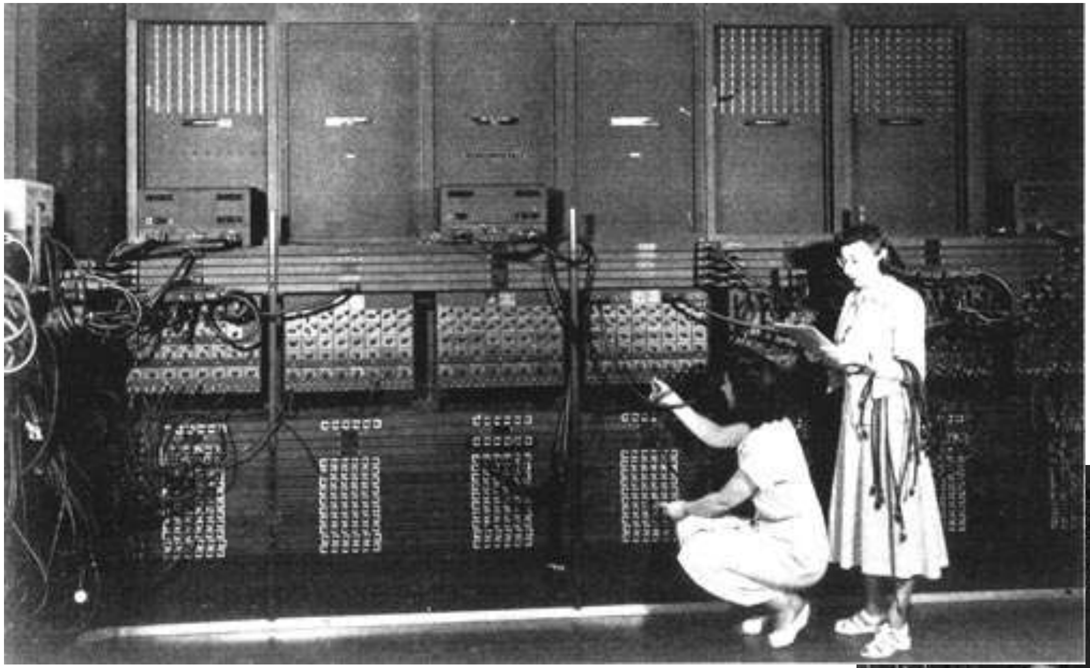
→ Developed the first algorithmic programming language („Plankalkül“).

6.2 Introduction to information processing

John von Neumann (1945)

→ Proposed the EDVAC computer in 1945.

→ Introduced the concept of a computer that is controlled by a stored program.



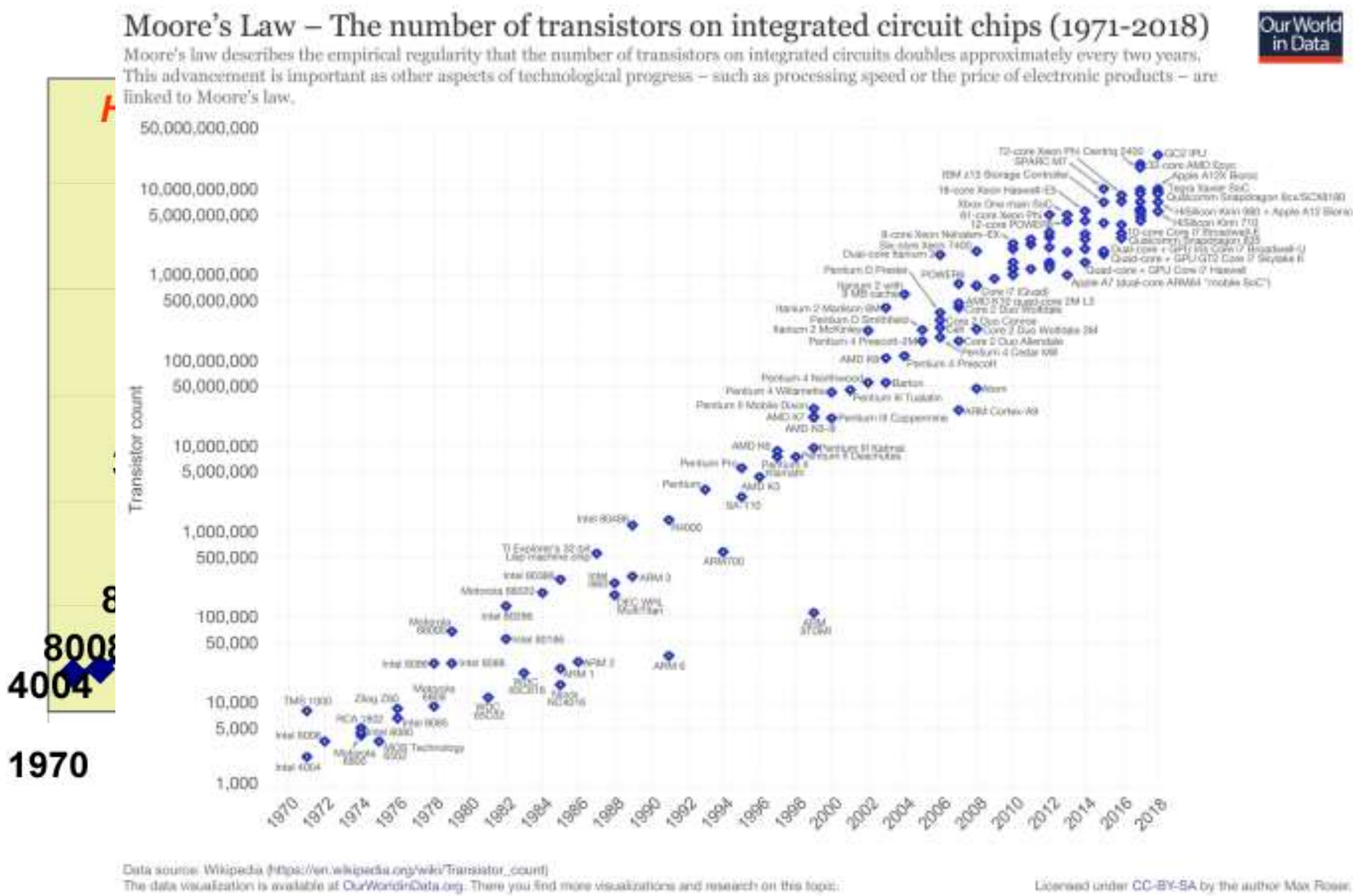
The „electronic numerical integrator and computer“ (ENIAC, 1946)

→ Built at the University of Pennsylvania
→ 18.000 vacuum tubes
→ Weight of 30 tons
→ Space of 160 m²
→ Required 6 operators

Left to right:
H.Wexler, J. von Neumann, M. H. Frankel,
J. Namias, J. C. Freeman, R. Fjortoft,
F. W. Reichelderfer, and J. G. Charney.

Moore‘s law

In 1965, Moore observed an **exponential growth** in the number of transistors per integrated circuit → Prediction: trend continues



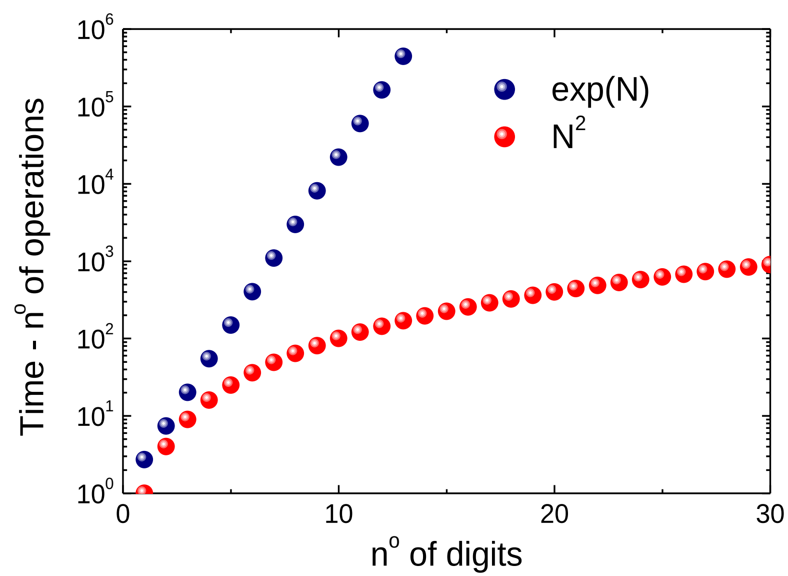
Complexity of a „yes/no“-problem

Example: Is m a prime number?

→ Expressed in terms of required resourses (memory space & computing time) as a function of the problem size N

→ Prime number factorization → $N = \log_2 m$ (number of bits)

L	Logarithmic memory space	$\mathcal{O}(\ln N)$
PSPACE	Polynomial memory space Chess computer	$\mathcal{O}(\ln N^k)$
P, QP	Polynominal execution time Multiply two numbers → $\mathcal{O}(N^2)$	$\mathcal{O}(N^k)$
NP	Not solvable in polynominal time Travelling salesman problem	
EXP	Exponential execution time Simple factorization ~ $2^{N/2}$ Easy: 7919 x 17 389 = ? Hard: 137 703 491 = ?	$\mathcal{O}(k^N)$

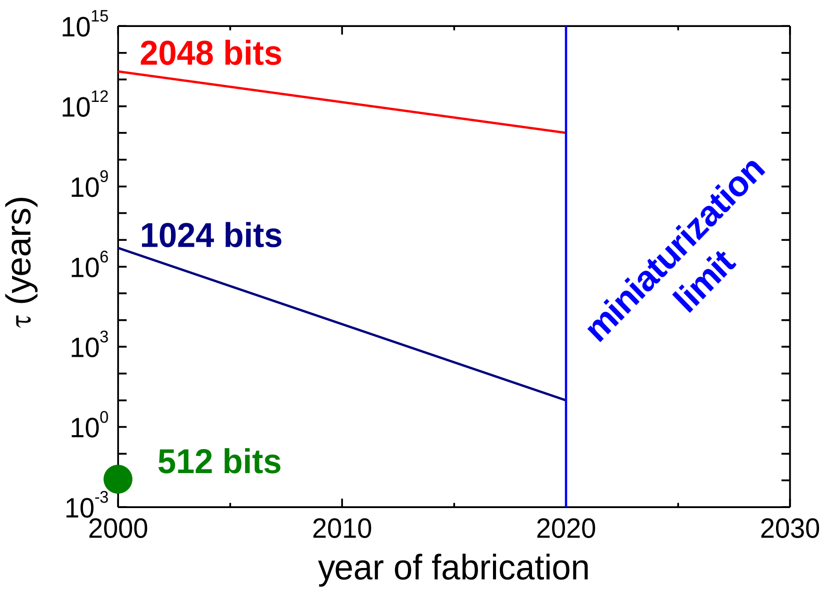


Known relations between the complexity classes → $\mathrm{L} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$

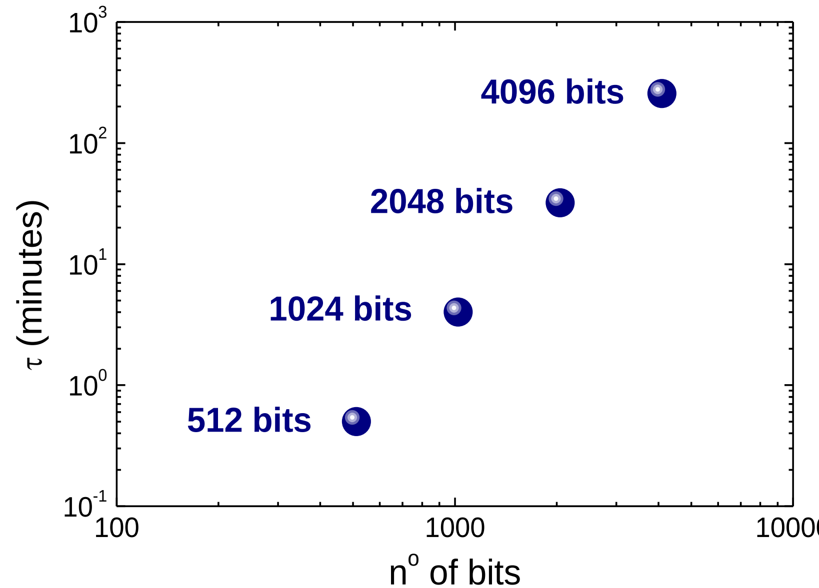
6.2.1 Computational complexity: Factorization

Integer factorization → NP hard on classical computer!

Classical computer



Quantum computer
(clock 100 MHz)



☹ Algorithm is known, but it takes too long

☺ Exponential speedup by quantum algorithm (Shor)

6.2.1 Computational complexity: Factorization

Integer factorization

Best known classical algorithm (number field sieve)

→ Required time $\propto \exp\left[2(\ln m)^{\frac{1}{3}}(\ln(\ln m))^{\frac{2}{3}}\right]$

→ Exponential in bit number $N \equiv \log_2 m$

→ Factorization of 400-digit decimal takes $\simeq 10^{10}$ years

Peter W. Shor

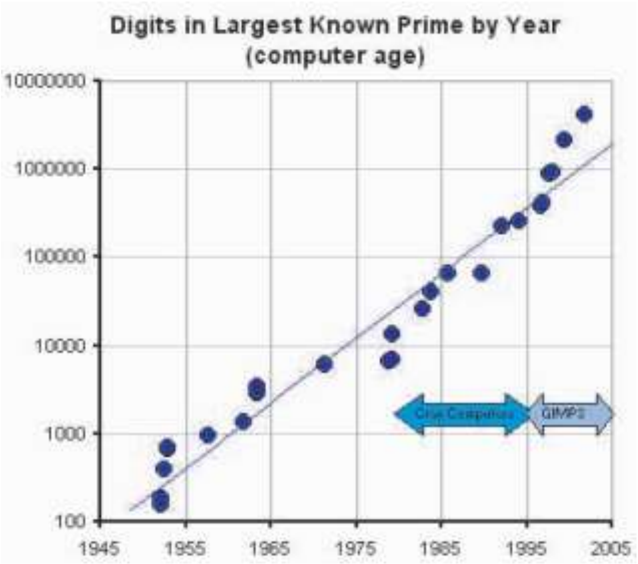
Shor quantum algorithm (Peter Shor, 1994)

→ Required time $\propto (\ln m)^3$

→ Factorization of 400-digit decimal takes a few years

Largest known prime number (2017):

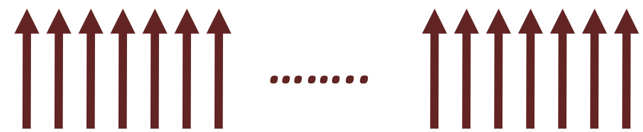
$2^{74207281}$-1 → 22 338 618 - digit decimal



→ Quantum algorithms can reduce the execution time to human timescales, where classical algorithms would take „forever“ in terms of these timescales!

6.2.1 Computational complexity: Quantum simulation

Example: N interacting spins (S = ½)



$N = 1000$ → Dimension of Hilbert space $= 2^{1000} >$ number of atoms in universe

Richard Feynman (1981):

"… nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem because it doesn't look so easy."

Quantum simulation → Encode the dynamics of a difficult-to-access quantum system in another quantum system, which can be more easily accessed

Example → Dirac dynamics of a relativistic electron in (nonrelativistic) trapped ion system (Nature **463**, 68-71, 2010)

Advantage → Less demanding than a universal quantum computer

6.2.2 Improvement of IP systems

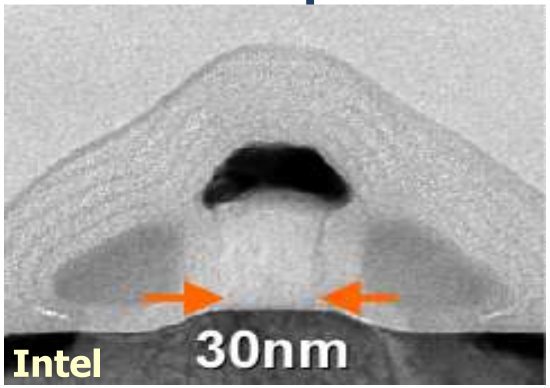
Exploitation of new functionalities

field	*electronics*	*opto electronics*	*fluxonics*	*mechatronics*	*spintronics*
degree of freedom	charge	charge + optical degree of freedom	charge + fluxonic degree of freedom	charge + mechanical degree of freedom	charge + spin degree of freedom

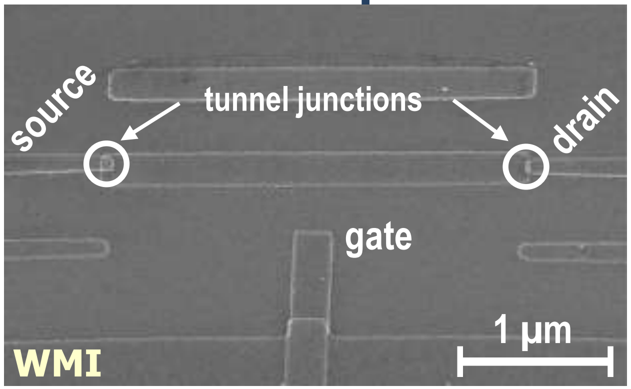
RSFQ-Logic
ultrafast AD-converters
.....

MRAM
GMR read heads
spin transistor
.....

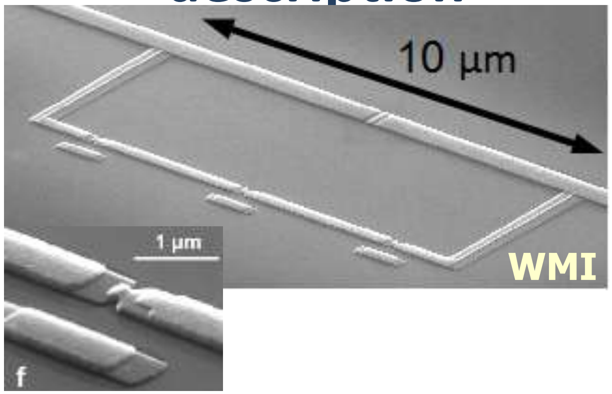
today	near future	far future
multi	**single**	**quantum**
electron, spin, fluxon, photon **devices**	***electron, spin, fluxon, photon*** **devices**	***electron, spin, fluxon, photon*** **devices**
classical description	quantifiable, but not quantum	quantum description



65 nm process 2005

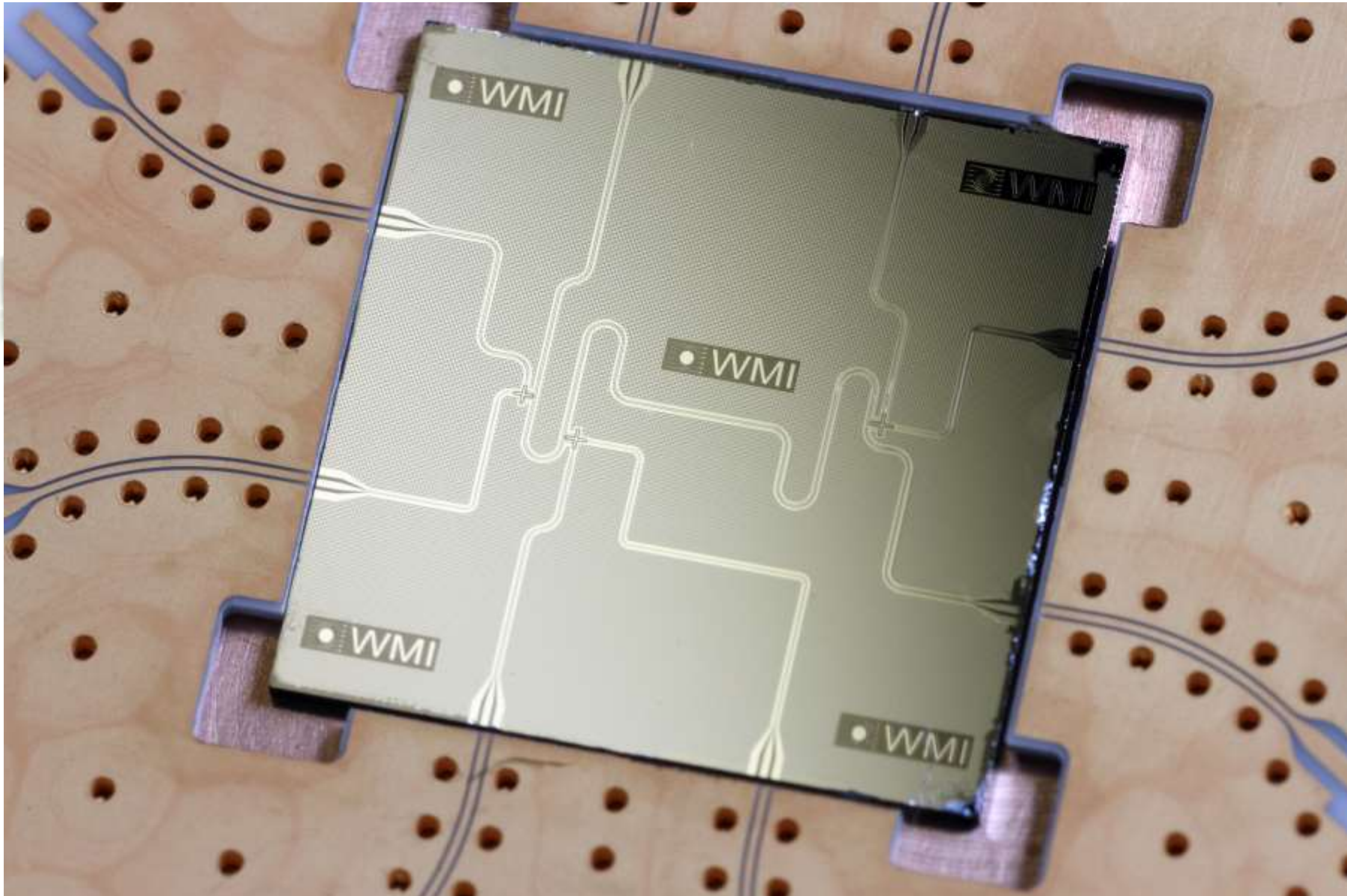


single electron transistor



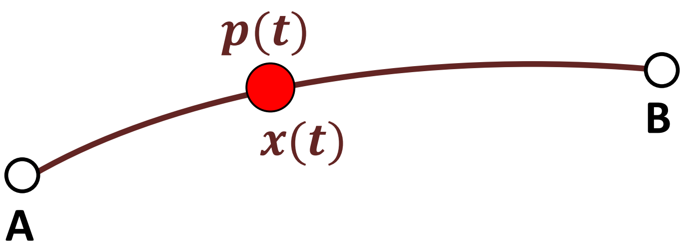
superconducting qubit

6.2.2 Improvement of IP systems



6.2 Introduction to QIP

Classical



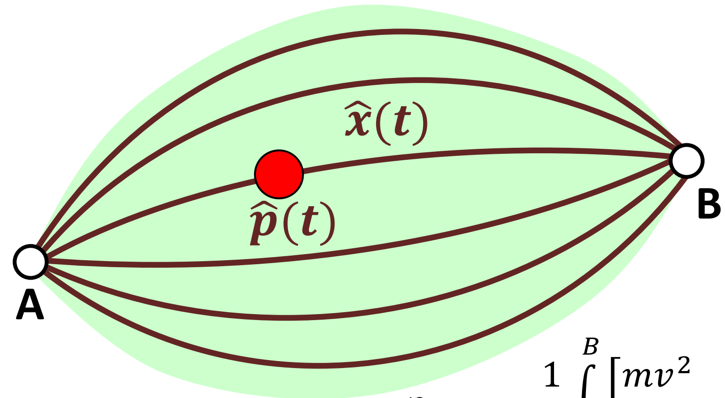
Point on a classical trajectory

$x(t)$ and $p(t)$ can be measured simultaneously at arbitrary precisions

No noise → $(\Delta x) = (\Delta p) = 0$

Classical noise
→ Probability distribution
→ Nonnegative

Quantum mechanical



$$\varphi_{path} = \frac{1}{\hbar}\int_A^B \left[\frac{mv^2}{2} - V(r)\right] dt$$

$$\Psi_B = \sum_{paths} \exp[i\varphi_{path}]\Psi_A$$

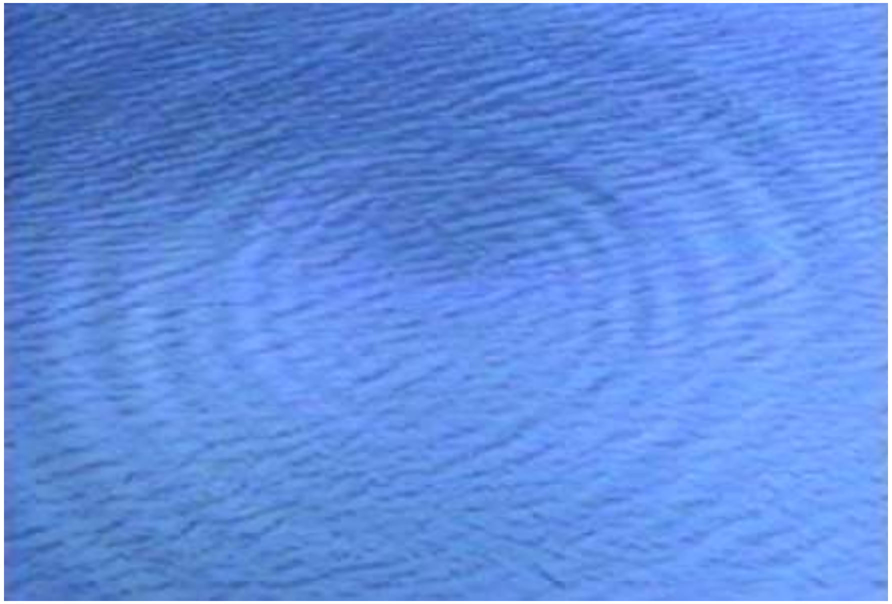
Quantum parallelism
→ Superposition of states
→ Entanglement of states

Vacuum noise (quantum)
→ $(\Delta x)(\Delta p) \geq \hbar/2$
→ Quasiprobability distribution
→ Can become negative (e.g., Fock states)

Ruth Bloch, bronze, 27" (2000)

Superposition of (basis) states

A quantum degree of freedom is described through a wave function.



Entanglement between states

Two quantum degrees of freedom can exhibit stronger correlations than any classical system.
("Superposition between Hilbert spaces")

Not entangled, separable (product) states: $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$

(Quantum) Entanglement $|\Psi\rangle \neq |\Psi_1\rangle \otimes |\Psi_2\rangle$

Uniquely quantum mechanical property of a composite system

No/restricted knowledge on subsystems despite perfect knowledge on combined system

→ Quantum correlations

Entanglement between spatially separate subsystems

→ Quantum teleportation

→ Quantum communication

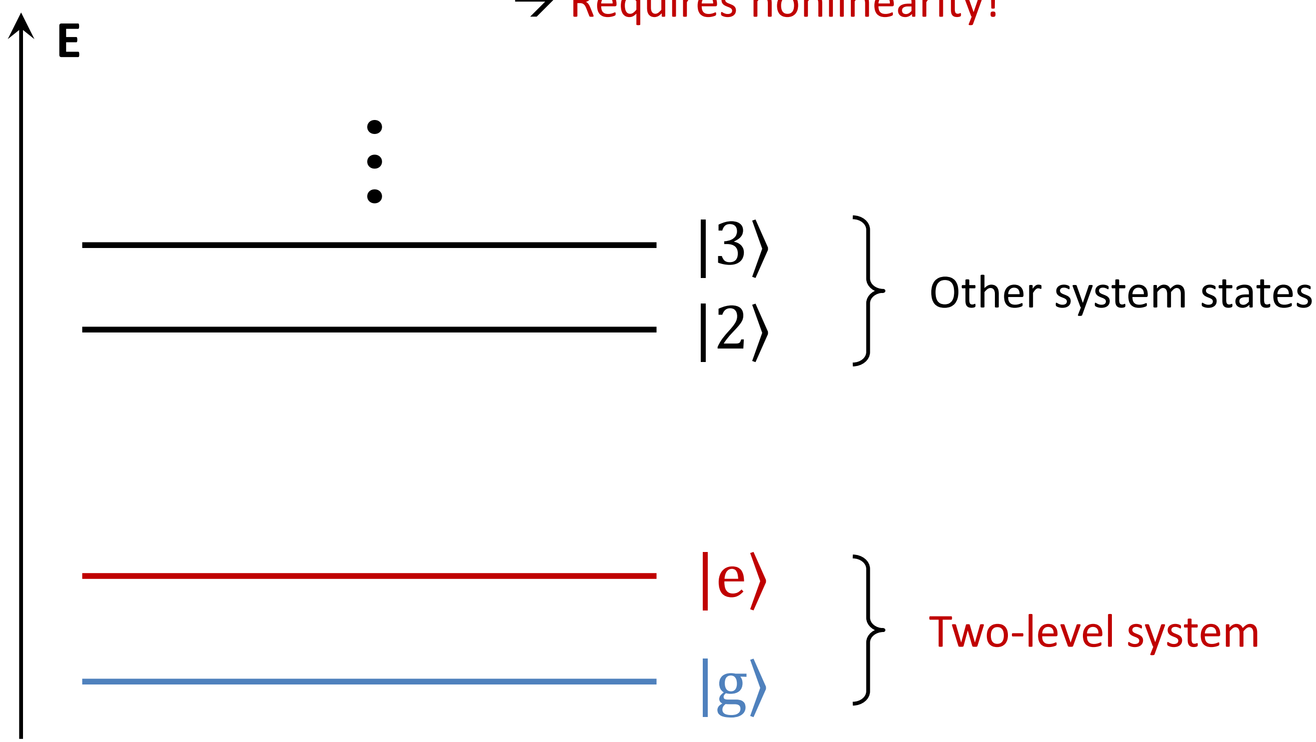
→ Quantum illumination (radar)

→ Quantum cryptography

Realization of a quantum two-level system

Natural systems:
→ Natural spins $|\downarrow\rangle$, $|\uparrow\rangle$
→ Orthogonally polarized light $|\updownarrow\rangle$, $|\leftrightarrow\rangle$

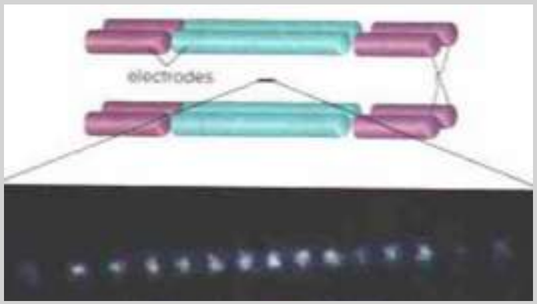
Effective systems:
→ Isolate two levels from a manifold structure
Mechanisms: Energy separation, selection rules, …
→ Requires nonlinearity!



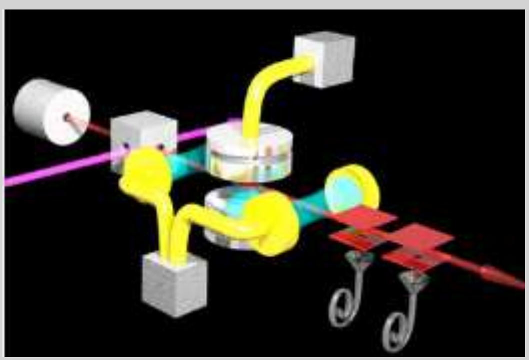
6.2 Introduction to QIP

microscopic

quantum optics
trapped ions

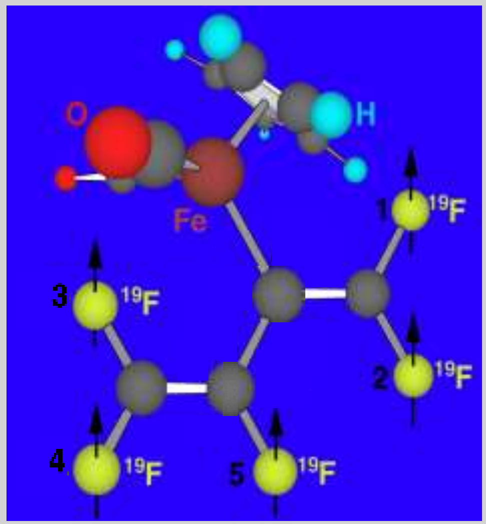


NIST, Innsbruck, Munich



ENS Paris

NMR

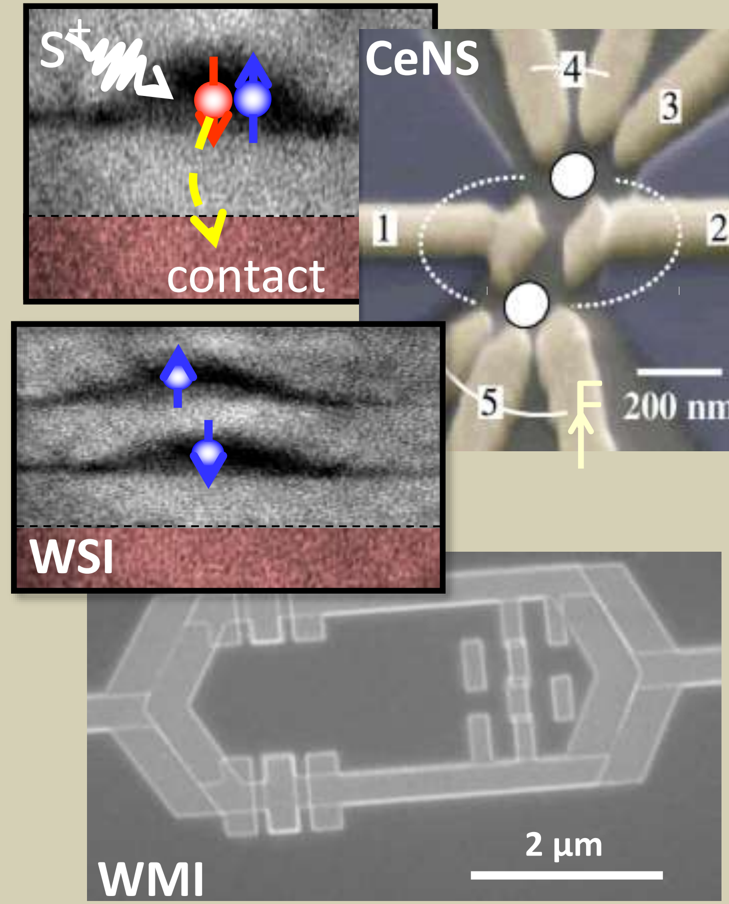


Oxford, Stanford,
IBM,MIT…

**easily quantum,
but difficult to scale**

meso- and macroscopic

solid state devices

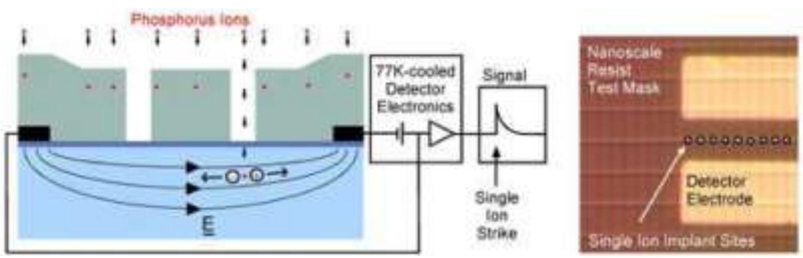


**scalable,
but not easily quantum**

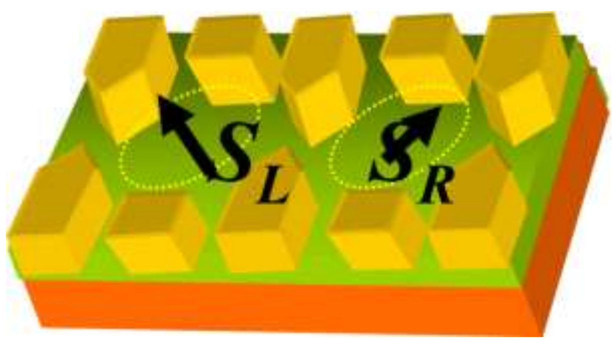
6.2 Introduction to QIP

single particle states
semiconductors

• nuclear spins of P in Si (Kane)



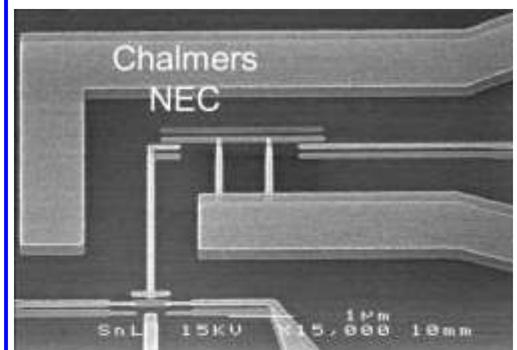
• electron spins in quantum dots

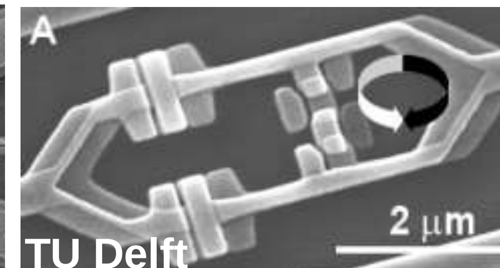


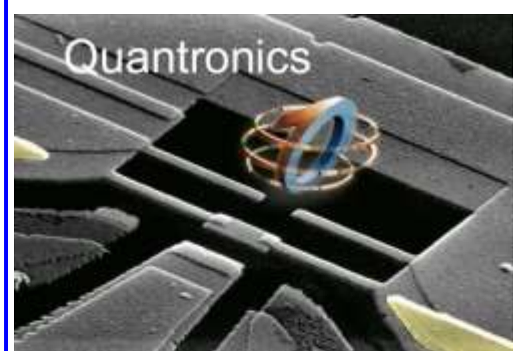
• ……

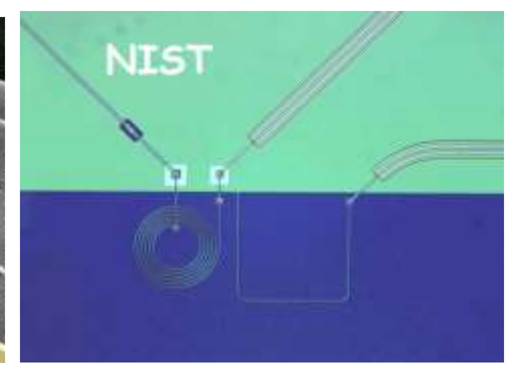
global states
superconductors

• superconducting flux, charge, phase, charge-phase qubits







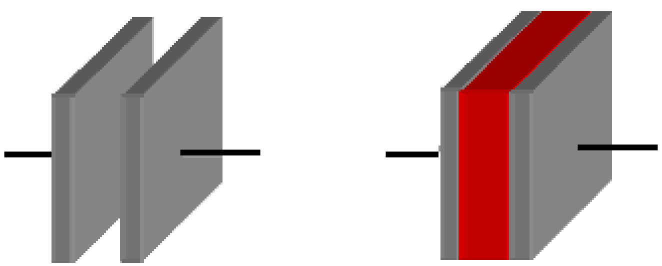


6.2 Introduction to QIP

Classical bits

0,1

E.g., implementation by charge states



0: Q = 0 **1: Q = Q_0**

Basic gates:

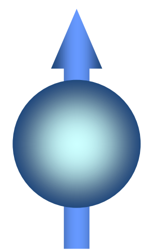
Single-bit-gate: NOT

Two-bit-gates: AND, OR

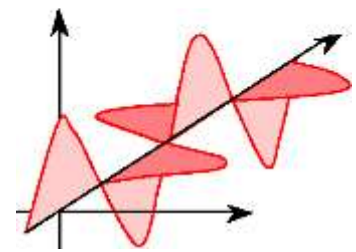
Quantum bits

$$|\Psi(t)\rangle = \cos\left(\frac{\theta}{2}\right)|e\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|g\rangle$$

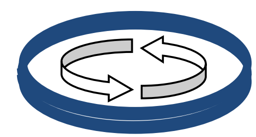
Implementation by any quantum two-level system



Spin



Polarization



Persistent current

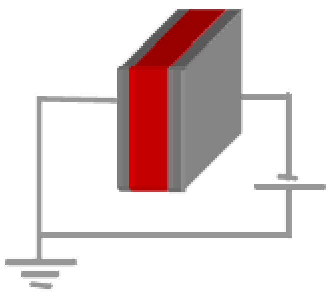
Basic gates:

Single-qubit-gate: rotations, Hadamard

Two-qubit-gates: C-NOT

6.2 Introduction to QIP

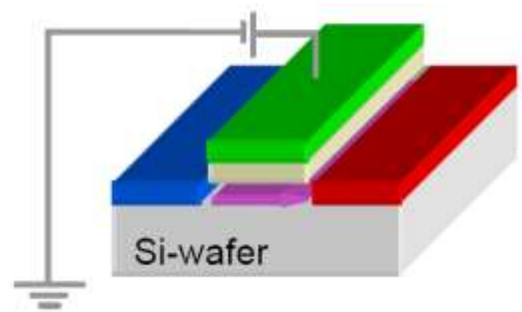
Classical computer: Bits & gates



Bits → Capacitors

$V = 0 \rightarrow 0$

$V > 0 \rightarrow 1$

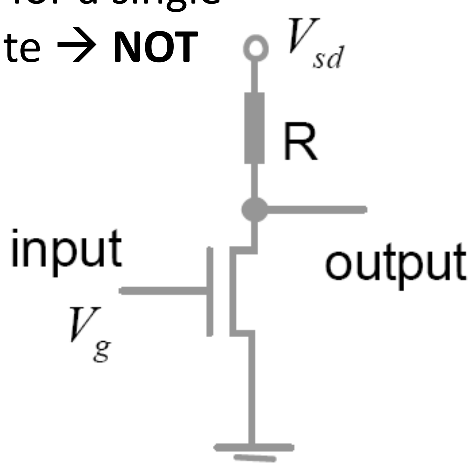


Gates → transistors

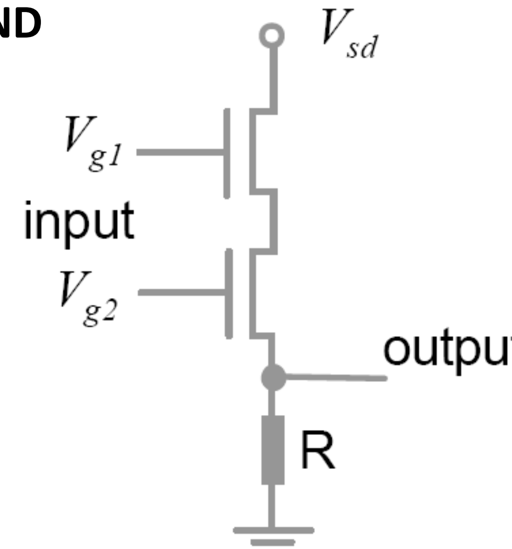
$V_g = 0 \quad \rightarrow$ closed

$V_g > 0 \quad \rightarrow$ open

Example for a single-bit gate → **NOT**



Example for a two-bit gate → **AND**



6.2 Introduction to QIP

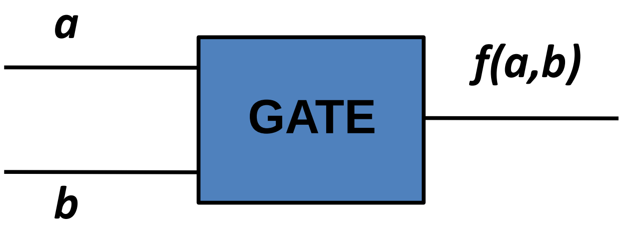
Universality theorem

A small number of Single-bit gates (e.g., NOT) and two-bit gates allows for any manipulation on classical bits (universal set)

Truth tables for various 2-bit gates

(a,b)	AND	NAND	OR	NOR	EQUIV	XOR
0 0	0	1	0	1	1	0
0 1	0	1	1	0	0	1
1 0	0	1	1	0	0	1
1 1	1	0	1	0	1	0

universal



Examples

$$\left.\begin{aligned} a \text{ OR } b &= (a \text{ NAND } a) \text{ NAND } (b \text{ NAND } b) \\ a \text{ AND } b &= (a \text{ NAND } b) \text{ NAND } (a \text{ NAND } b) \\ \text{NOT } a &= a \text{ NAND } a \end{aligned}\right\} \quad \text{OR, AND, NOT also form universal set}$$

Irreversible classical logic (1940 - current):

Logical irreversibility

→ No ability to reconstuct the input from the output

Physical irreversibility

→ Heat dissipated during a gate operation

Intimate connection

→ Increase of entropy due to loss of 1 bit of information, $\Delta S = k_B \ln 2$

→ Dissipative heat → Irreversibility

Si-based computers

→ Way above the ideal limit by a factor

→ 10^{10} (transistor)

→ 100 (DNA copying mechanism in human cell)

→ Discussion somewhat academic

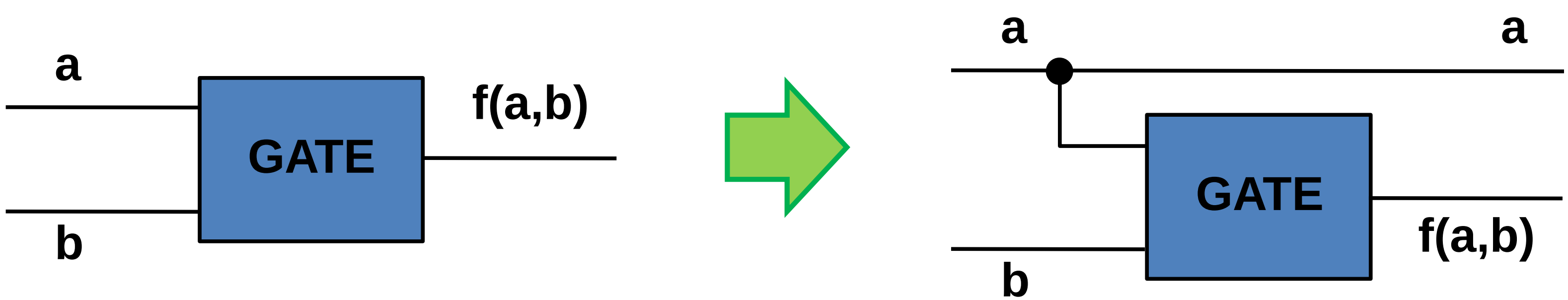
Reversible classical logic (Bennett, 1973)

Conditions

→ Absence of physical dissipation

→ Number of output bits equals to number of inputs

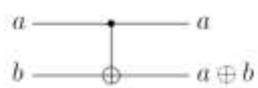
→ Gate produces all input combinations at output



(a,b)	(a, a NAND b)	(a, a XOR b)
(0,0)	(0,1)	(0,0)
(0,1)	(0,1)	(0,1)
(1,0)	(1,1)	(1,1)
(1,1)	(1,0)	(1,0)

	Intrinsically irreversible	Logically reversible

CNOT gate (reversible XOR)



a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

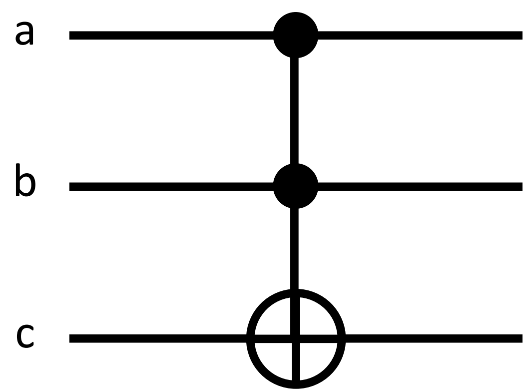
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Three-bit gates (Bennett, 1973)

Universality → Reversible logic requires three-bit gates

Toffoli gate → Controlled CNOT gate (CCNOT)

→ Applies a NOT to bit c when both bit a and bit b are "1"



→ Some two-bit gates are intrinsically irreversible (e.g., NAND)

→ Third bit required to store input safely

Definition of a quantum bit

Classical bit → Deterministic, either in ground state "g" or in excited state "e"

Quantum bit (qubit) → Superposition of two computational basis states

$$|\Psi(t)\rangle = a(t)|\mathrm{g}\rangle + b(t)|\mathrm{e}\rangle$$

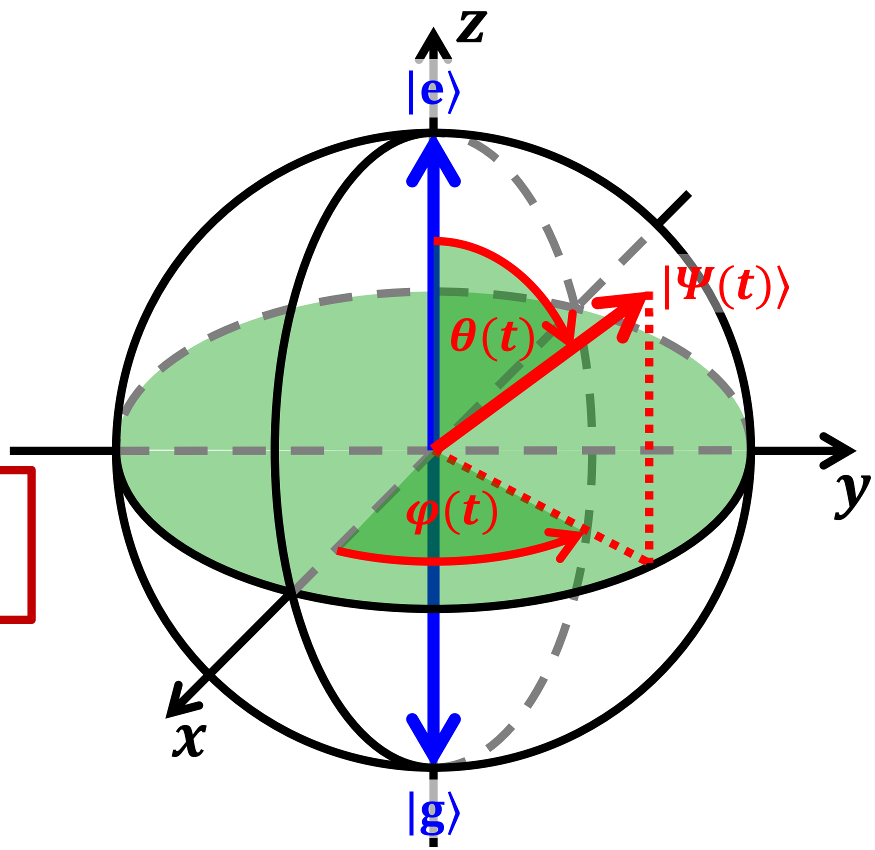
$a(t), b(t) \in \mathbb{C}$ with $|a(t)|^2 + |b(t)|^2 = 1$

→ All states can be visualized on the surface of a sphere

Global phase unobservable

→ Bloch sphere representation

$$\boxed{|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|\mathrm{e}\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|\mathrm{g}\rangle}$$



Bloch angles

$\theta(t)$ → Amplitude → Energy, population

$\varphi(t)$ → Phase → Coherence

Linear algebra notation of operators and state vectors

Qubit states can be written as vectors

$$a|\mathrm{e}\rangle + b|\mathrm{g}\rangle \quad \rightarrow \quad \mathrm{a}\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix}$$

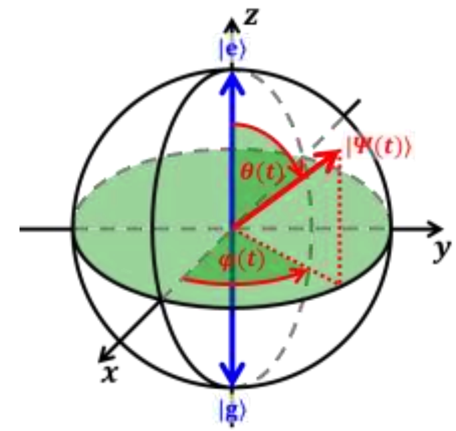
Qubit operators (gates) can be written as matrices

$$a|\mathrm{e}\rangle\langle\mathrm{e}| + b|\mathrm{g}\rangle\langle\mathrm{g}| + c|\mathrm{e}\rangle\langle\mathrm{g}| + d|\mathrm{g}\rangle\langle\mathrm{e}|$$

$$\rightarrow a\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} + c\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} + a\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}a & c\\d & b\end{pmatrix}$$

Pseudo spin and Pauli matrices

$$|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|\mathrm{e}\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|\mathrm{g}\rangle$$



Pseudo spin

→ $|\Psi\rangle$ equivalent to spin wavefunction in external magnetic field

Unitary operations

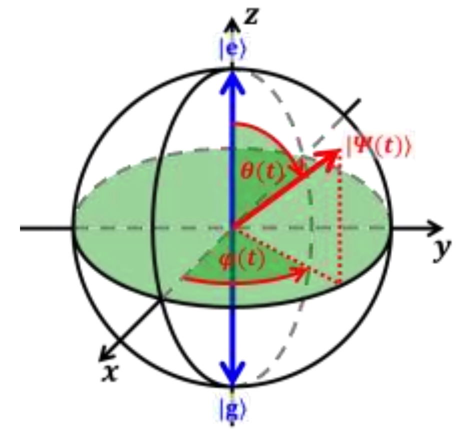
→ $\hat{U}|\Psi\rangle$ expressed via the Hermitian Pauli spin matrices $\hat{1}$, $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$

$$\hat{1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\sigma}_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$|\mathrm{g}\rangle$ and $|\mathrm{e}\rangle$ are the eigenvectors of $\hat{\sigma}_z$

Conventions: Pauli matrices and Bloch sphere

$$\hat{1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\sigma}_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



$$|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|\mathrm{e}\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|\mathrm{g}\rangle$$

These definitons contain several conventions, such as

→ The global scaling factor
→ The positon of the minus sign in σ_z
→ Here, we show two examples with fixed σ_z

→ Physics convention → $|\mathrm{g}\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|\mathrm{e}\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

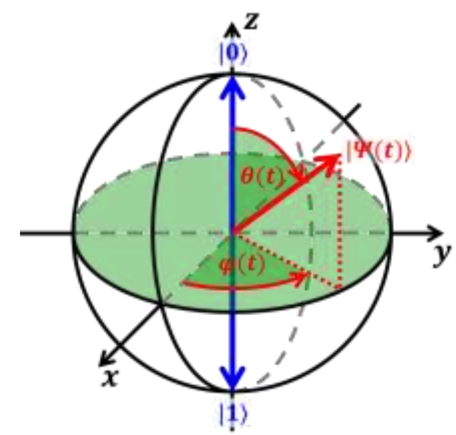
→ Ground state energy negative (more „physical“)

Information theory (IT) convention

→ M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press

→ $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

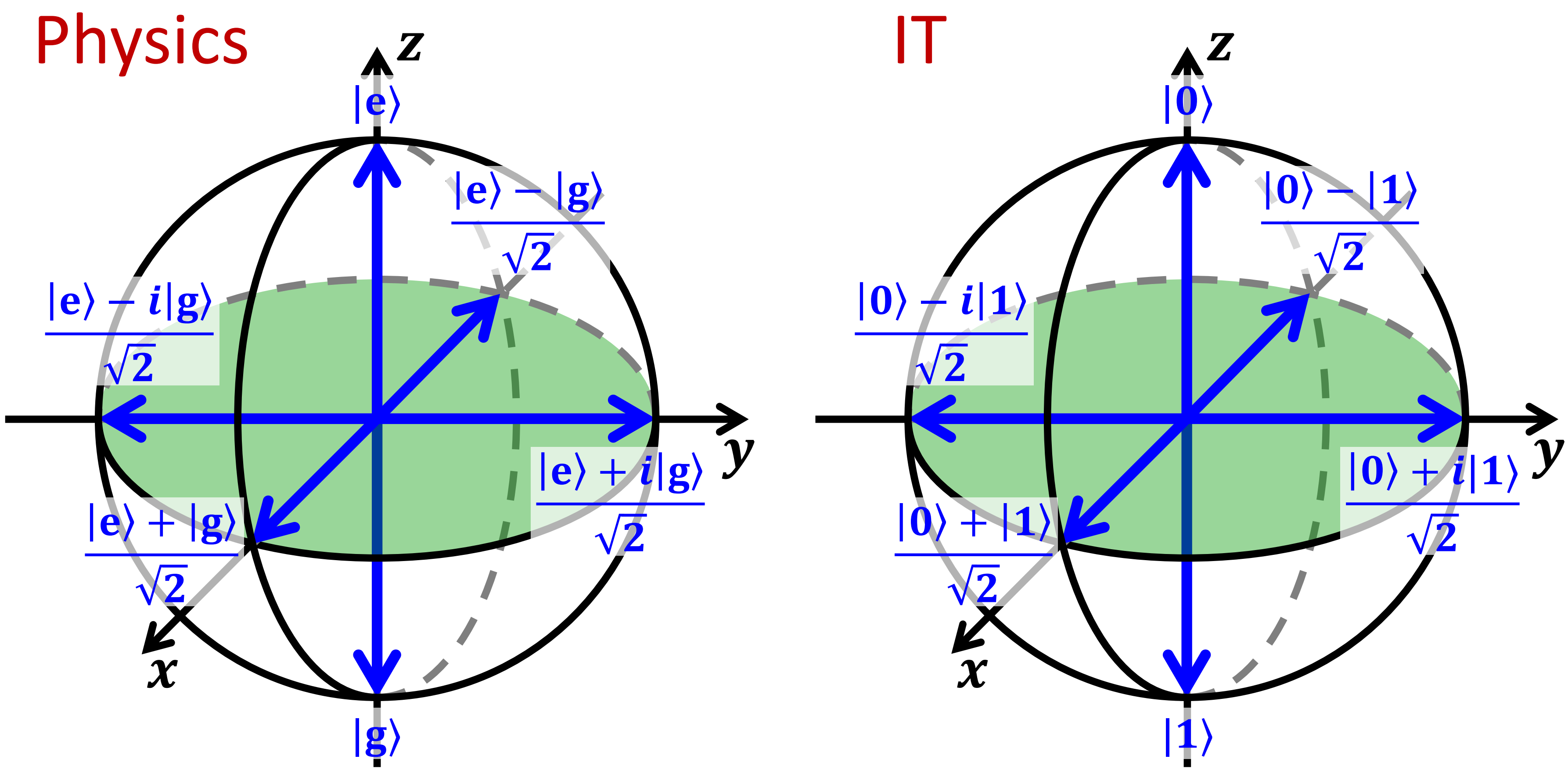
→ Ground state energy positive („unphysical“)
→ Easily generalized, more „logical”



$$|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|0\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|1\rangle$$

→ Unless otherwise mentioned → Physics convention!
→ Formal resolution → Equate $|\mathrm{g}\rangle$ to $|1\rangle$ and $|\mathrm{e}\rangle$ to $|0\rangle$ → Used in this lecture!

Important states on the Bloch sphere



$$|\Psi(t)\rangle = \cos\left(\frac{\theta}{2}\right)|\mathrm{e}\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|\mathrm{g}\rangle$$

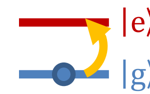
$$|\Psi(t)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Interpretation of the Pauli matrices

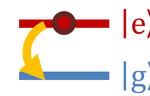
$$\hat{1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\sigma}_x \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

→ The Pauli matrices can expressed in terms of projection operators

$\hat{\sigma}_+ = |\mathrm{e}\rangle\langle\mathrm{g}|$ → Puts an excitation into the qubit



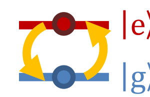
$\hat{\sigma}_- = |\mathrm{g}\rangle\langle\mathrm{e}|$ → Removes an excitation from the qubit



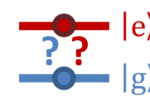
$\hat{\sigma}_x = \hat{\sigma}_- + \hat{\sigma}_+$

$\hat{\sigma}_y = i(\hat{\sigma}_- - \hat{\sigma}_+)$

→ Induce transitions between $|\mathrm{g}\rangle$ and $|\mathrm{e}\rangle$



$\hat{\sigma}_z = |\mathrm{e}\rangle\langle\mathrm{e}| - |\mathrm{g}\rangle\langle\mathrm{g}|$ → $\langle\hat{\sigma}_z\rangle$ gives the qubit population



$\hat{1} = |\mathrm{g}\rangle\langle\mathrm{g}| + |\mathrm{e}\rangle\langle\mathrm{e}|$ → Reflects normalization

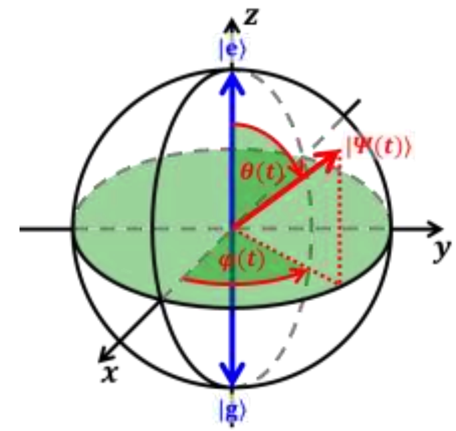
→ Combination of basis definition and operator description in terms of projection operators → Matrix from of operators

→ In this lecture, we fix the matrix definitions of the Pauli matrices

→ "Physical" intuition in $\{|\mathrm{g}\rangle, |\mathrm{e}\rangle\}$-notation

→ Notation consistent with Nielsen & Chuang and most physics papers!

Definition of a single qubit gate



Single qubit gate

→ Unitary operation $\widehat{U}$ on state $|\Psi\rangle$

→ Described by rotations on Bloch sphere + global phase

Rotation matrices

→ Around x-axis → $\hat{R}_x(\alpha) \equiv e^{-\frac{i\alpha\hat{\sigma}_x}{2}} = \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$

→ Around y-axis → $\hat{R}_y(\alpha) \equiv e^{-\frac{i\alpha\hat{\sigma}_y}{2}} = \begin{pmatrix} \cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$

→ Around z-axis → $\hat{R}_z(\alpha) \equiv e^{-\frac{i\alpha\hat{\sigma}_z}{2}} = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix}$

Why? General unitary expressed by rotations

→ $\widehat{U} = e^{i\varepsilon}\hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta)$ with $\varepsilon, \beta, \gamma, \delta \in \mathbb{R}$

→ Z-Y decomposition (others possible)

→ ε is a global phase (unobservable)

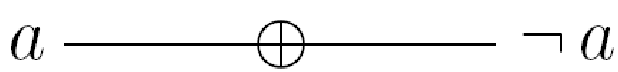
6.2 Introduction to QIP

Examples for 1-qubit gates

Identität	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\sqrt{\mathrm{NOT}}$	$\sqrt{X}$	$\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$
NOT	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Hadamard	H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli-Y	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Phase $(\sqrt{Z})$	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
Pauli-Z	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\pi/8\ (\sqrt{S})$	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

Graphical representation example

NOT



Matrix representation (taken from QI theory books) typically follow IT convention!

Hadamard gate $\widehat{H}$ is of particular importance

→ Applied to one of the basis states $|\mathrm{g}\rangle$ or $|\mathrm{e}\rangle$, it results in a superposition state of the basis states

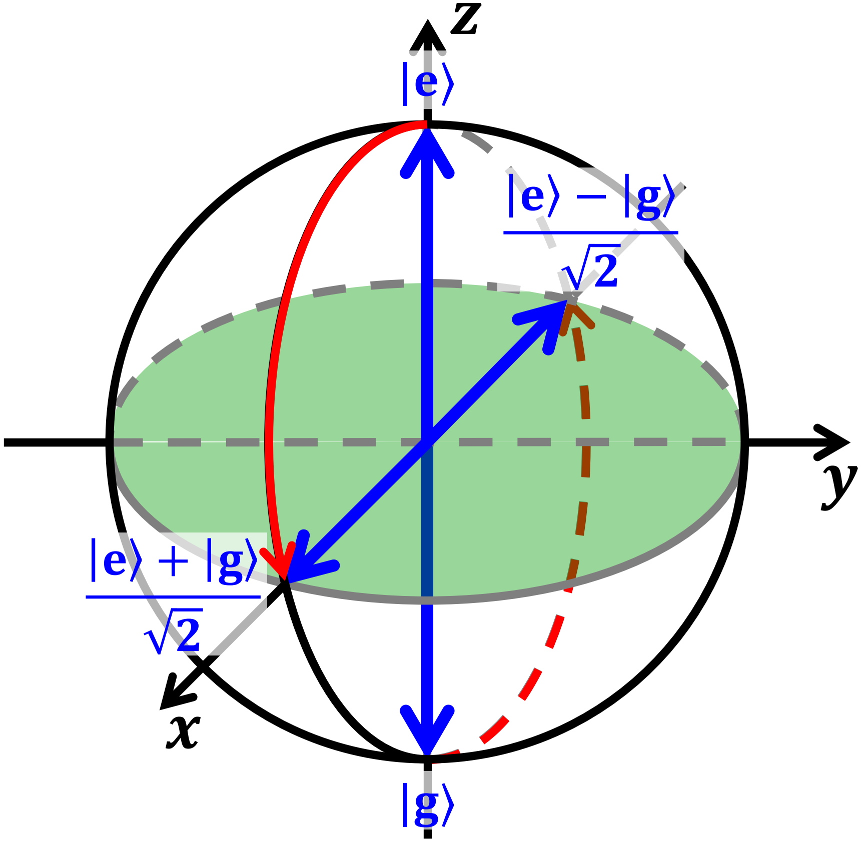
$$\widehat{H} \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$$

→ Physics convention

$$\widehat{H} = \frac{1}{\sqrt{2}}(|\mathrm{e}\rangle\langle\mathrm{e}| - |\mathrm{g}\rangle\langle\mathrm{g}| + |\mathrm{e}\rangle\langle\mathrm{g}| + |\mathrm{g}\rangle\langle\mathrm{e}|)$$

$$\widehat{H}|\mathrm{g}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{e}\rangle - |\mathrm{g}\rangle)$$

$$\widehat{H}|\mathrm{e}\rangle = \frac{1}{\sqrt{2}}(|\mathrm{e}\rangle + |\mathrm{g}\rangle)$$

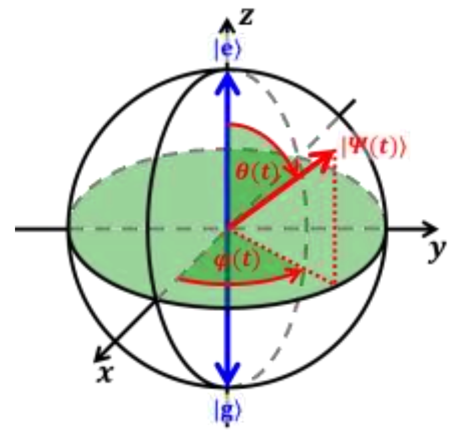


Quantum coherence

$$|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|\mathrm{e}\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|\mathrm{g}\rangle$$

$\theta(t)$ → Amplitude → Energy, population

$\varphi(t)$ → Phase → Coherence



Ideal quantum system

→ Completely isolated
→ In reality, however, …

Environment must interact with $|\Psi(t)\rangle$ for control

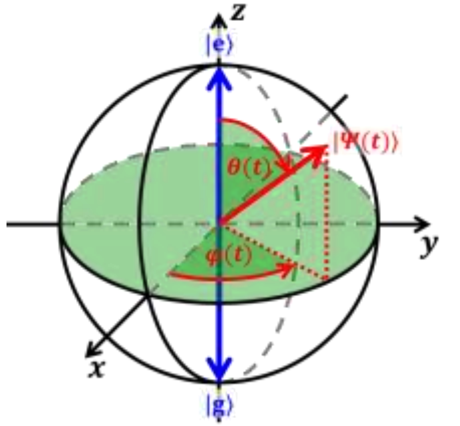
→ Uncontrolled interactions (noise) also exist
→ Quantum effects (population oscillations, quantum interference, superpositions, entanglement) unobservable after characteristic time
→ Decoherence time T_{dec}
→ After T_{dec}, quantum effects have decayed to $^1/_e$ of their original level
→ T_{dec} is a time scale rather than a strict time
→ Term “decoherence” originally only referred to phase
→ Nowadays sloppily comprises both phase and amplitude effects

Energy and phase relaxation

$$|\Psi(t)\rangle = \cos\left(\frac{\theta(t)}{2}\right)|\mathrm{e}\rangle + e^{i\varphi(t)}\sin\left(\frac{\theta(t)}{2}\right)|\mathrm{g}\rangle$$

$\theta(t)$ → Amplitude → Energy, population

$\varphi(t)$ → Phase → Coherence



Population
→ Energy relaxation time T_1 or T_r
→ $k_\mathrm{B}T \ll \hbar\omega_\mathrm{ge}$ → decay from |e⟩ to |g⟩
→ Nonadiabatic (irreversible) processes
→ Induced by high-frequency fluctuations ($\omega \approx \omega_\mathrm{ge}$)

Phase
→ Pure dephasing time T_φ
→ Adiabatic (reversible) processes
→ Induced by low-frequency fluctuations ($\omega \to 0$)
→ Often encountered: 1/f-noise
→ Real measurements always contain T_1-effects

$$T_2^{-1} = (2T_1)^{-1} + \mathrm{T}_\varphi^{-1}$$

Nomenclature is not very consistent in literature!

From single to multi-qubit systems

Single qubit (IT) →

$$0 \equiv |0\rangle \equiv \binom{1}{0}$$

$$1 \equiv |1\rangle \equiv \binom{0}{1}$$

$$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle$$

Two qubits (IT) → $|\Psi\rangle = c_1|00\rangle + c_2|10\rangle + c_3|01\rangle + c_4|11\rangle$

$$|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |01\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

Tensor product

$$|10\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |11\rangle = \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Two-qubit operators

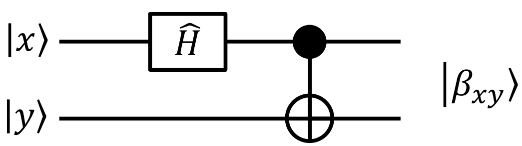
$$A \otimes B = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \otimes \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} = \begin{pmatrix} A_{11}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} & A_{12}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \\ A_{21}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} & A_{22}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \end{pmatrix}$$

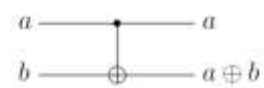
→ Tensor product (blockwise product) of single qubit operators

6.2 Introduction to QIP

The Bell states

→ The Bell states are of particular importance in many QIP protocols
→ Created via a Hadamard and a CNOT gate





a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$|00\rangle$ $$|\beta_{00}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$|01\rangle$ $$|\beta_{01}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$|10\rangle$ $$|\beta_{10}\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$|11\rangle$ $$|\beta_{11}\rangle \equiv \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$\hat{H} \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Einstein-Podolsky-Rosen (EPR) paradoxon

Example: Two spins

Alice  Bob

Uncorrelated: 4 product states $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle, |\downarrow\downarrow\rangle$

Correlated: Linear combination of product states
→ Entanglement

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle\right)$$

→ Alice and Bob perform measurements in z-direction on the entangled spins

→ Suppose: Alice first measures her spin and finds $|\uparrow\rangle$ (50% chance)

→ Then: Bob always measures his spin $|\downarrow\rangle$ (100%), although he may be far away from Alice → Quantum mechanics is nonlocal !

→ Repetition of the experiment
  → Always the same result → The two entangled spins are fully correlated

→ Heisenberg relation violated if conjugate quantites measured by Alice and Bob („EPR paradox“)?
  → No, Bob‘s measurements in x- or y-direction yield equal probabilities

→ Superluminal information exchange?
  → Only if quantum copying („cloning“) was allowed

No-cloning theorem

Classical bits can be copied easily: C → CC

Quantum bits (quantum states) cannot be copied → No-cloning theorem

→ Proof: Assume that there is a unitary transformation $\widehat{U}$ producing copies of $|\alpha\rangle$ and $|\beta\rangle$

$$\widehat{U}|\alpha 0\rangle = |\alpha\alpha\rangle \text{ and } \widehat{U}|\beta 0\rangle = |\beta\beta\rangle$$

→ However, the quantum copying machine fails in copying state

$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$$

$$\widehat{U}|\gamma 0\rangle = \frac{1}{\sqrt{2}}(|\alpha\alpha\rangle + |\beta\beta\rangle) \neq |\gamma\gamma\rangle$$

Combination of the EPR paradox and the no-cloning theorem

→ Rescues the consistency between quantum mechanics and special relativity

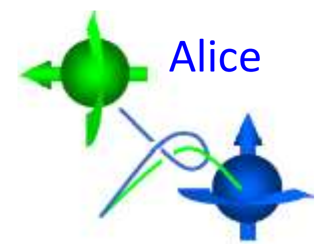
→ No superliminal communication!

6.2 Introduction to QIP

Quantum teleportation

→ No-cloning theorem forbids copying state $|\phi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$
→ However, vanishing at one place and reappearing at another is allowed
→ Teleportation
→ Teleporting a quantum state (qubit) requires that Alice and Bob share an entangled state $|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$ ("EPR pair")

Teleportation protocol



1. Alice entangles her spin $|\uparrow\rangle$ with the unknown state $|\phi\rangle$

2. Alice measures what state her two spins are and tells Bob, which of the four possible results she has found
   → Classical communication

$\uparrow\uparrow, \uparrow\downarrow, \downarrow\uparrow, \downarrow\downarrow$

3. Bob carries out the appropriate rotation of his spin $|\uparrow\rangle$ by π

4. As a result, Bob ends up with his spin in the state $|\phi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$

Quantum gates

Intrinsically reversible

→ Any irreversible manipulation would be associated with heat dissipation
→ Destruction of quantum coherence

→ Universal set of gates → E.g., single qubit rotations and CNOT

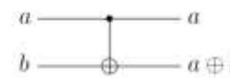
→ Three-qubit Toffoli is required (also important for quantum error correction)

Represented by unitary transformations

→ Normalization → length of state vector (on Bloch sphere) stays constant

→ Reversibility requires that matrix can be inverted

→ Complex matrix elements, since components of spinor are complex

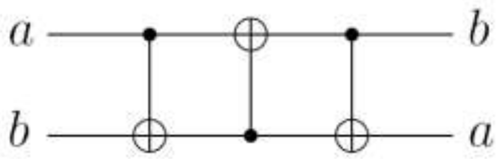


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

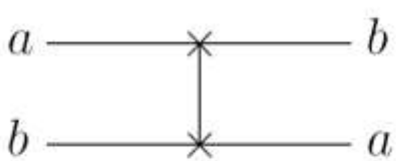
CNOT gate

SWAP gate



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

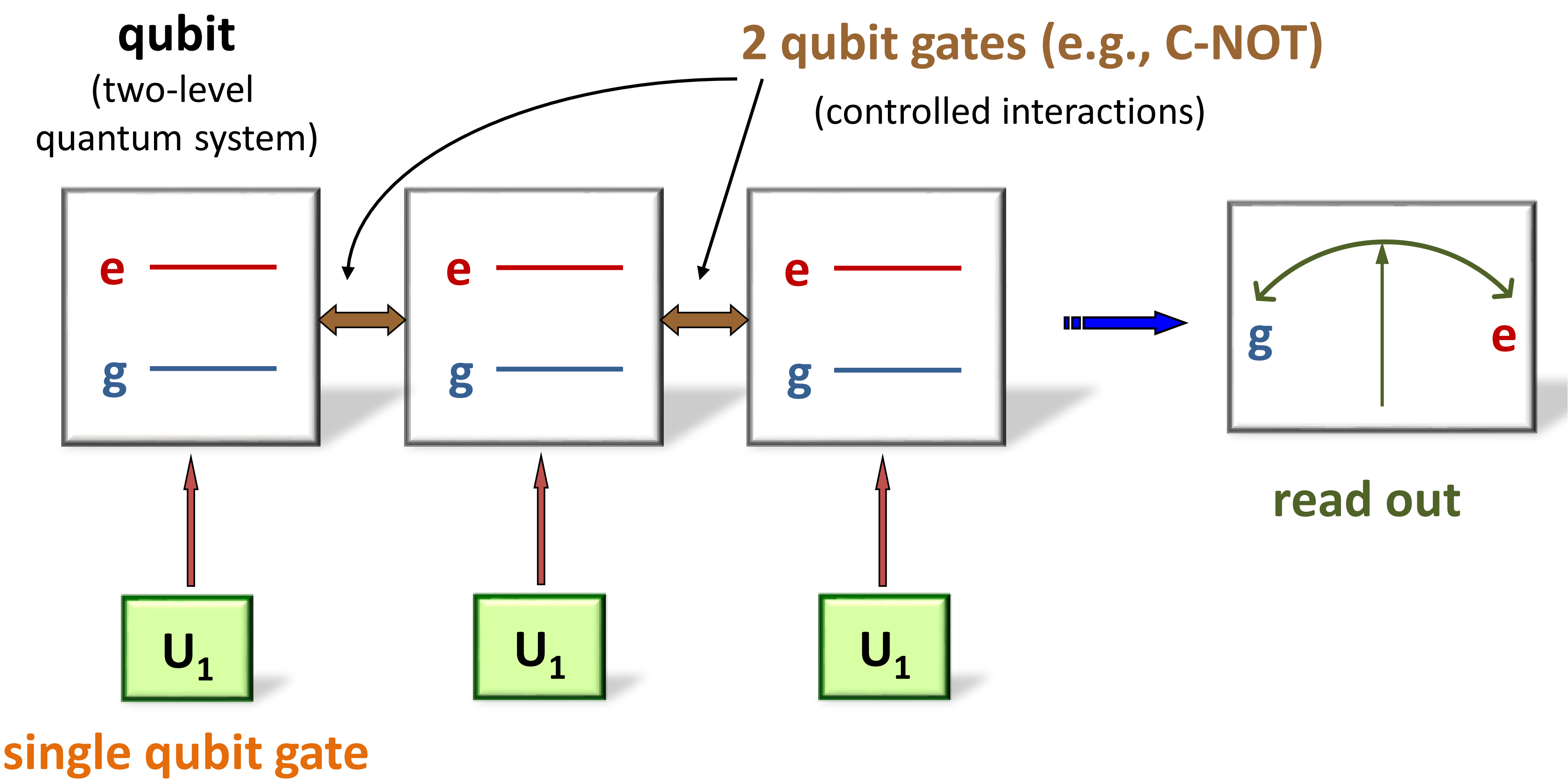
resp.



a	b	a'	b'
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Interchange of a and b

Universal quantum processor: Required elements

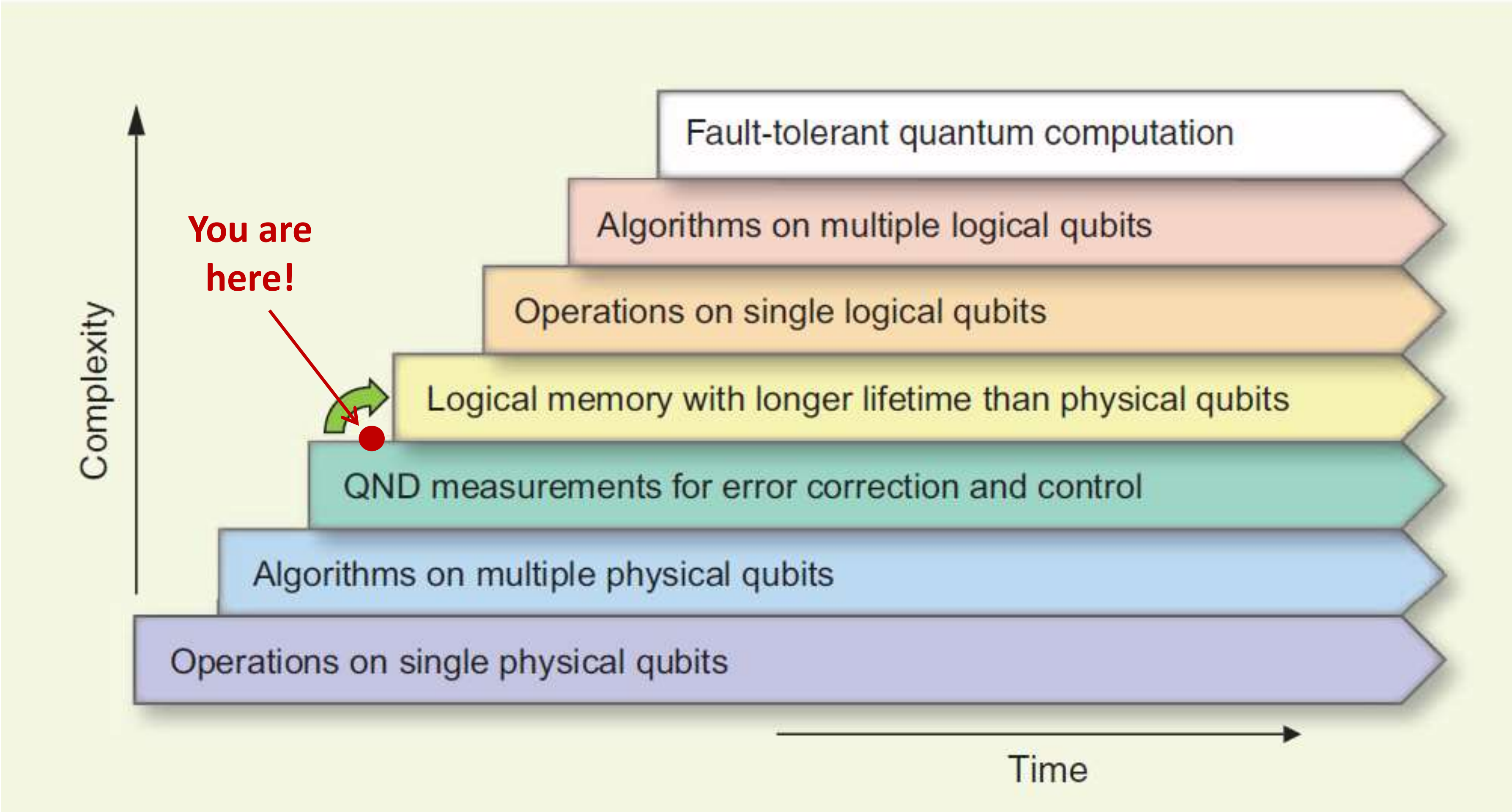


Initialization	$\|0\rangle \otimes \|0\rangle \otimes \ldots. \otimes \|0\rangle \otimes$	
Preparation of superposition states Example: 3 bit system	$\|0\rangle + \|1\rangle \otimes \|0\rangle + \|1\rangle \otimes \ldots. \otimes \|0\rangle + \|1\rangle$ $\|Y\rangle = a\|000\rangle + b\|001\rangle + c\|010\rangle + d\|100\rangle +$ $e\|011\rangle + f\|101\rangle + g\|110\rangle + h\|111\rangle$	
Computational steps → Unitary transformations → Single-qubit gates → Two-qubit gates → Program → Parameters		Quantum algorithm → Factorization (Shor) → Database search (Grover) → …
Quantum error correction		E.g., Shor, Steane, surface code, cat code
Readout	**Final state**	

DiVincenzo criteria for scalable QIP

- **Qubits:**
  The system has to provide a well defined two-level quantum system
- **Preparation of the initial state**:
  It must be possible to prepare the initial state with sufficient accuracy
- **Decoherence**:
  The phase coherence time must be long enough to allow for a sufficiently large number (typically >10^4) of coherent manipulations
- **Quantum gates:**
  There must be sufficient control over the qubit Hamiltonian to perform the necessary unitary transformations, i.e., single- and two-qubit operations
- **Quantum measurement:**
  For read-out of the quantum information a quantum measurement is needed
- **Scalability:**
  There should be the possibility to increase to number of qubits

D. DiVincenzo, *The physical implementation of quantum computation,* Fortschr. Phys. **48, 771 (2000).**



M. H. Devoret and R. J. Schoelkopf, *Science* **339**, 1169 (2013); DOI:10.1126/science.1231930