Hauptseminar Quantum Information
WS 2022/23

0. Elements of network quantum computing

(A) what is information?

example: throwing a die

- if a die player tells you that he has thrown a "5" this is only an information for you if you didn't watch him throwing the die
- if he says he has thrown a number between 1 and 6 this is also no information

$\boxed{\text{information is a notion of a priori ignorance}}$

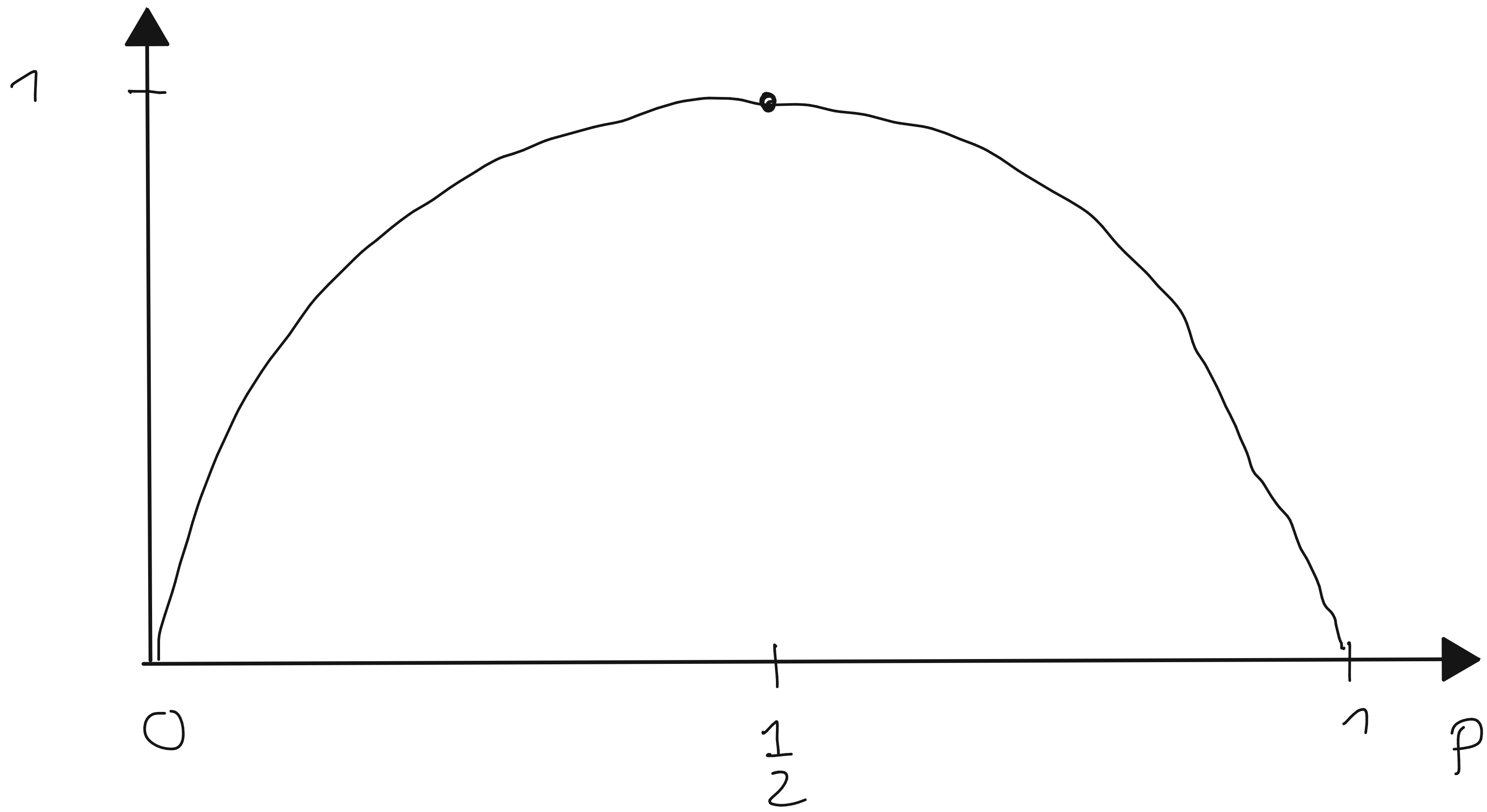
- elementary unit of information: binary alternative: "yes" or "no"

bit: 0 1

a-priori probability $p : 0$ $\quad 1-p : 1$

measure of information : Shannon entropy

$$(1) \qquad H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$$



multiple events

$$(2) \qquad \boxed{S_{Sh}(p_1, \dots, p_N) = -\sum_{j=1}^{N} p_j \log_2 p_j}$$

(B) Computation

general model of computation: Turing machine

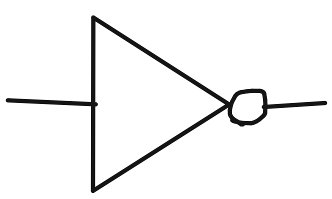
circuit model

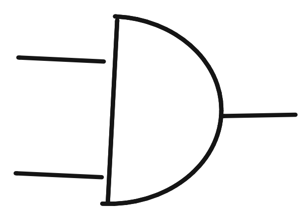
logic gate

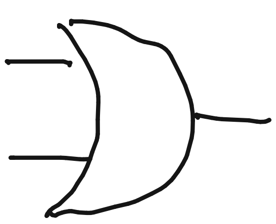
(3) $$\boxed{f : \{0,1\}^k \longrightarrow \{0,1\}^\ell}$$

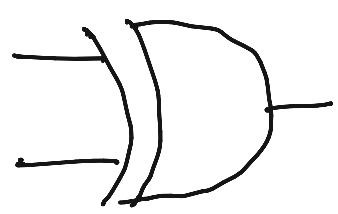
k : # of input bits $\qquad$ ℓ : # of output bits

- circuit is acyclic
- general circuit can be composed of elementary gates

NOT $\quad a$  $\bar{a}$

AND $\quad a, b$  $a \oplus b$

OR $\quad a, b$  $a \wedge b$

XOR $\quad a, b$  $\bar{a} \wedge b$

FANOUT $\quad a \to a, a$

CROSSOVER $\quad a, b \to b, a$

- combination of these gates allows to compute any function
- problem $\quad$ AND, OR, XOR not reversible

eq. (3) in general not reversible !

reversible computing $\hat{=}$ invertible function

$$f: \{0,1\}^n \longrightarrow \{0,1\}^n \tag{4}$$

- any function (3) can be turned into a symmetric one by addition of anzillas

$$\begin{aligned} f(x)&: \{0,1\}^k \longrightarrow \{0,1\}^\ell \\ \tilde{f}(x)&: \{0,1\}^{k+\ell} \longrightarrow \{0,1\}^{\ell+k} \end{aligned} \tag{5}$$

where

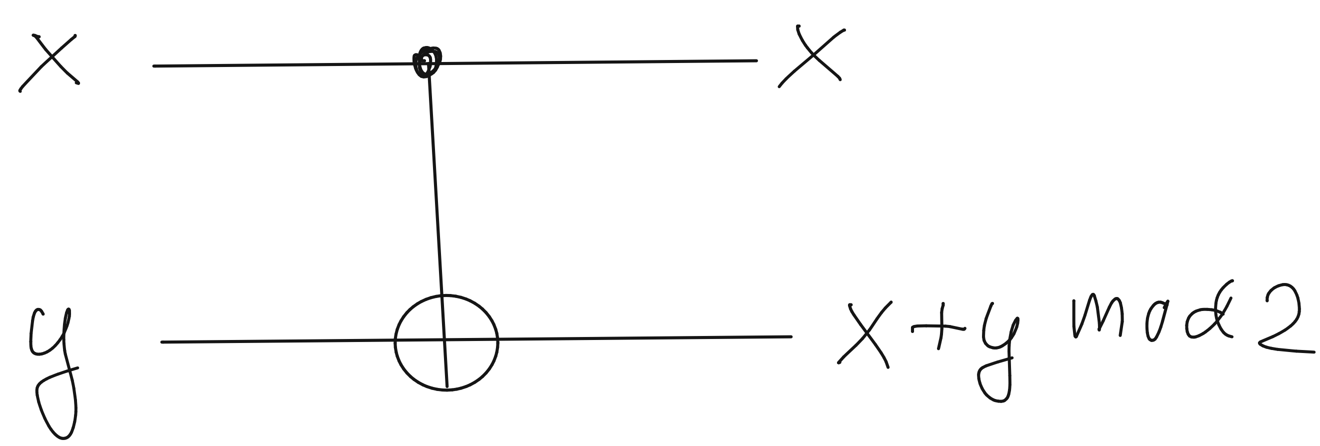
$$\boxed{\tilde{f}(x) = \tilde{f}(\underbrace{x}_{k\text{ bits}}, \underbrace{0,0,0\ldots0}_{\ell\text{ bits}}) = (x, f(x))} \tag{6}$$

control-not

$$\text{CNOT} \quad (x,y) \longrightarrow (x, x \oplus y \bmod 2) \tag{7}$$

control bit

target bit



matrix representation (addition modulo 2)

$$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix} \qquad (8)$$

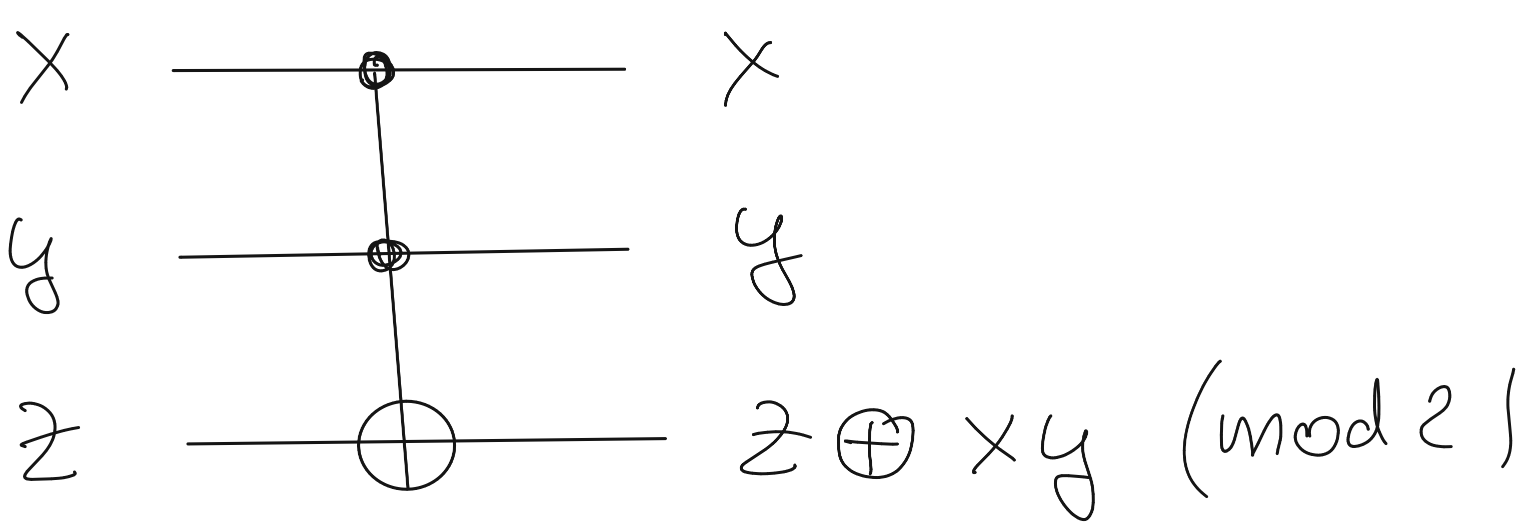
$$M^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

> reversible 1-bit and 2-bit gates are not universal since they are all linear

$\Rightarrow$ nonlinear function cannot be calculated

- for $n \geq 3$ reversible gates exists that correspond to a nonlinear mapping

Toffoli gate controlled-controlled NOT



(c) quantum network computer

input: string of classical bits

0 1 0 0 1 1 0 ·   bits

↓

factorized initial state

↓

$|0\rangle|1\rangle|0\rangle|0\rangle|1\rangle|1\rangle|0\rangle$ qubits

↓

gates: general unitary transformations

↓

von Neumann projection on a set of qubits to computational basis $\{|0\rangle, |1\rangle\}$

↓

output: string of classical bits with probabilities p_j

probabilistic in nature:

0	1	0	1	1 …
p_1	$(1-p_2)$	p_3	$(1-p_4)$	$(1-p_5)$

qubits

quantum system with Hilbert space of dimension $d=2$

- spin $1/2$
- two-level atom
- photon with two polarizations

computational basis $\{ |0\rangle, |1\rangle \}$

e.g. eigenstates of $\hat{\sigma}_z$

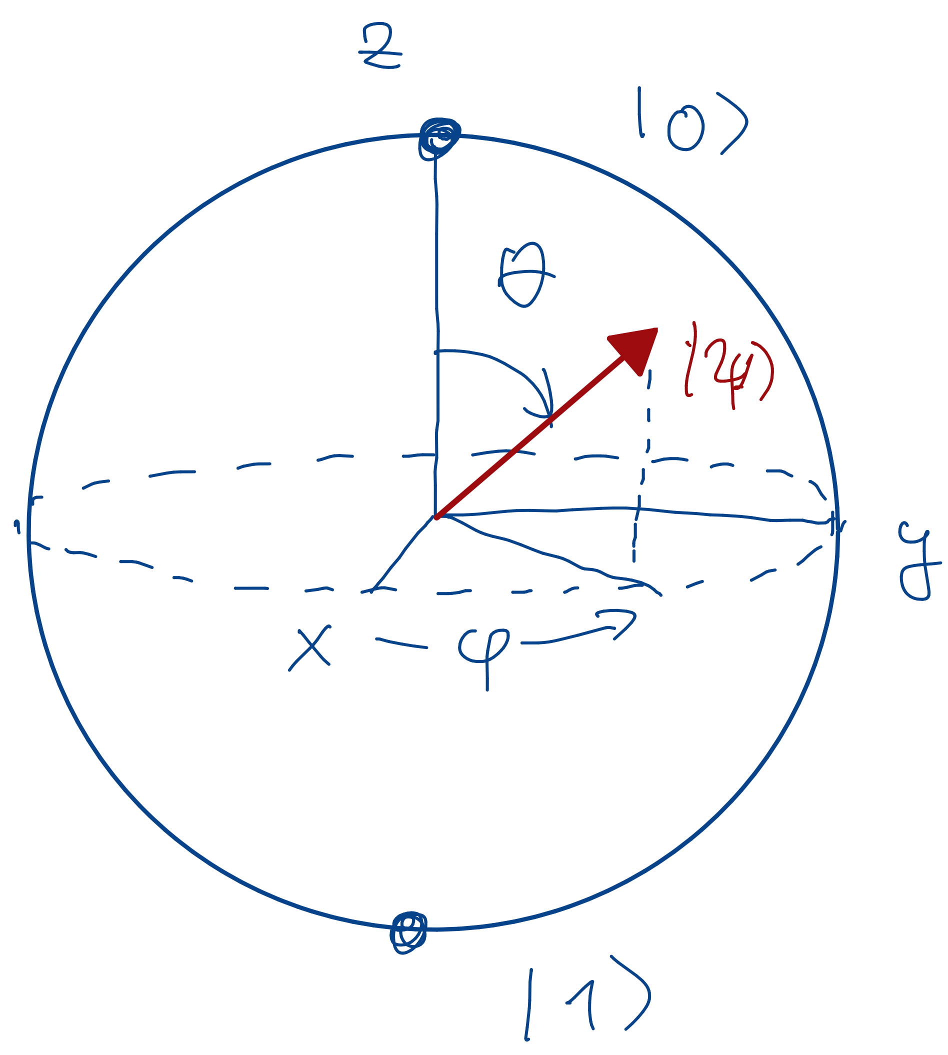
general state

$$|\psi\rangle = \cancel{e^{i\gamma}} \left(\cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2} |1\rangle \right) \tag{9}$$

$\uparrow$ irrelevant

(θ, φ) characterize state

Bloch sphere



peculiarities with qubits vs. bits

- arbitrary superpositions allowed!

does this mean we should associate to a qubit an infinite amount of information (continuous angles on ~~the~~ the Bloch sphere)? No!

$$\boxed{\text{An unknown quantum state of a qubit cannot be completely determined by a measurement}}$$

complete measurement

$$\hat{\Pi}_0 = |0\rangle\langle 0| \qquad \hat{\Pi}_1 = |1\rangle\langle 1| \qquad \hat{\Pi}_0 + \hat{\Pi}_1 = \mathbb{1} \tag{10}$$

$$\rho = |\psi\rangle\langle\psi| \quad \begin{cases} \nearrow \ \lambda = 0 \qquad \dfrac{\hat{\Pi}_0 \rho \hat{\Pi}_0}{Tr\{\Pi_0 \rho \Pi_0\}} \\[2ex] \searrow \ \lambda = 1 \qquad \dfrac{\hat{\Pi}_1 \rho \hat{\Pi}_1}{Tr\{\Pi_1 \rho \Pi_1\}} \end{cases} \tag{11}$$

only binary information

perhaps we can generate copies of $|\psi\rangle$ and then measure? No!

$$\boxed{\begin{array}{l}\text{An unknown quantum state (of a qubit) can in general not be duplicated} \\ \text{(no cloning theorem)}\end{array}}$$

general qubit state ρ; since $\rho = \rho^\dagger$ it can be diagonalized; eigenvalues are probabilities (in case of degeneracy ⇒ choose orthogonal basis) eigenstates $|x_j\rangle$ are orthogonal

(12) $$\rho = \sum_{j=0}^{1} p_j \, |x_j\rangle\langle x_j| \qquad p_0 + p_1 = 1$$

Information of ρ in p_j ⇒ Shannon $\hat{=}$ von Neumann

(13) $$\boxed{S_{Sh} = -\sum_j p_j \log p_j = -\mathrm{Tr}\{\rho \log \rho\} = S_N}$$

- unitary transformations can generate entanglement and entangled states can have "stronger" correlations than classically possible (see talk on Bell inequalities)

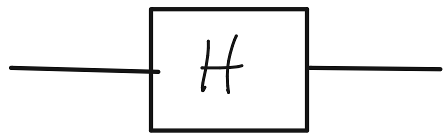
theorem of Deutsch (1985)

> any d-dimensional unitary matrix can be decomposed into $d(d-1)/2$ unitary 2×2 matrices

since the 2×2 matrices can also act in the 2 dim-space spanned by states of different qubits one- and two-qubit gates are needed in practice

important 1-qubit gates

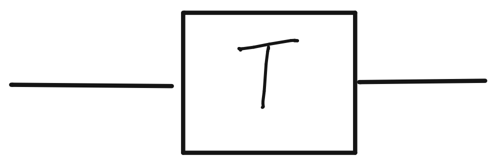
(14) **Hadamard**



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

$$\{|0\rangle, |1\rangle\} \xrightarrow{\quad H \quad} \left\{\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)\right\}$$

(15) **$\pi/8$**



$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

combination of Hadamard und $\pi/8$ gate allows to approximate any unitary operation on a single qubit with arbitrary precision

other single qubit gates

$\boxed{X}$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Pauli X

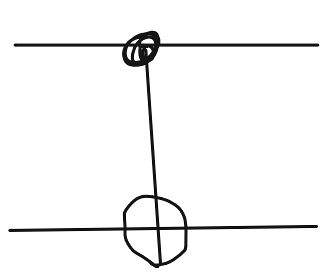
$\boxed{Y}$ $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Pauli Y

$\boxed{Z}$ $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Pauli Z

$\boxed{S}$ $\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ Phase

important 2-qubit gates

CNOT



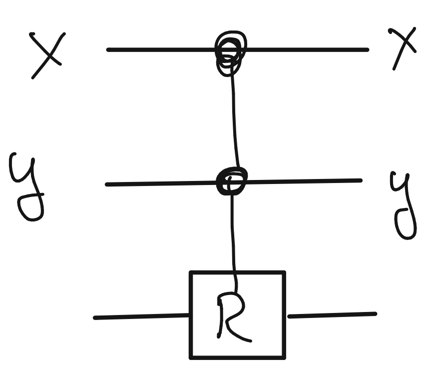
(16)

$$\begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array}$$
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\boxed{\text{arbitrary single qubit gates plus a CNOT gate are universal!}}$$

But a classical two-bit gate was not sufficient, how come?

universal 3-qubit gate (David Deutsch 1989)



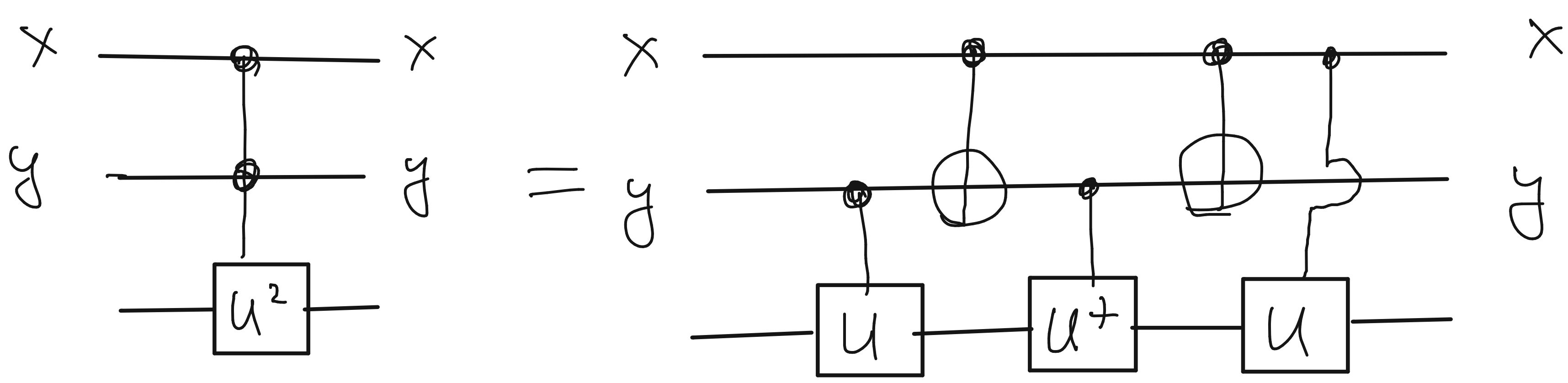
$$R = -i \exp\left\{ i \frac{\theta}{2} \sigma_x \right\}$$

iff 1st <u>and</u> 2nd qubit in $|1\rangle$

(a'la Toffoli)

this can be decomposed into 2 qubit gates

$$R = U^2$$



action on 3rd qubit

$$U^y U^{\dagger(x \oplus y)} U^x = U^{y - x \oplus y + x}$$

$$= U^{y-(x+y-2xy)+x} = U^{2xy} = R^{xy} \checkmark$$

(D) realizing unitaries

$$U = e^{iA} \qquad A = A^{+}$$

- single qubit $\quad U:\ 2\times 2$ matrix

$$A \in \{ \mathbb{1}, \sigma_x, \sigma_y, \sigma_z \}$$

$$\boxed{\begin{aligned} \exp(-i\theta\sigma_x/2) &= \cos\frac{\theta}{2}\,\mathbb{1} - i\sin\frac{\theta}{2}\,\sigma_x \\ \exp(-i\theta\sigma_y/2) &= \cos\frac{\theta}{2}\,\mathbb{1} - i\sin\frac{\theta}{2}\,\sigma_y \\ \exp(-i\theta\sigma_z/2) &= \cos\frac{\theta}{2}\,\mathbb{1} - i\sin\frac{\theta}{2}\,\sigma_z \end{aligned}} \tag{17}$$

$\Rightarrow$ unitary time evolution with π pulse

$$H = \hbar\frac{\Omega(\tau)}{2}\sigma_\mu \qquad U = \exp\left(-i\int_0^T d\tau\,\frac{\Omega(\tau)}{2}\sigma_\mu\right) \tag{18}$$

requirement

$$\int_0^T d\tau\,\Omega(\tau) \overset{!}{=} \pi \quad \Rightarrow \quad U = -i\,\sigma_\mu \tag{19}$$

more robust alternatives

- adiabatic qubit gates
- geometric qubit gates

- Controlled NOT

$$U = \exp\left\{ -i \underbrace{\int_0^T dt \, g}_{=\theta/2} \left(|0\rangle_1 \langle 0| \cdot \mathbb{1}_2 + |1\rangle_1 \langle 1| \sigma_2^x \right) \right\}$$

$$= \left(\cos\frac{\theta}{2} - i \sin\frac{\theta}{2} \right) |0\rangle_1 \langle 0| \, \mathbb{1}_2$$

(20)

$$+ \left(\cos\frac{\theta}{2} - i \sin\frac{\theta}{2} \right) |1\rangle_1 \langle 1| \, \sigma_2^x$$

$$\underset{\theta = \pi}{=} \quad -i \left(|0\rangle_1 \langle 0| \, \mathbb{1}_2 + |1\rangle \langle 1| \, \sigma_2^x \right)$$

$\Rightarrow$ requires strong interaction between spin 1 and 2