Quantum Computing with imperfect quantum computers

(I) Gate accuracy

(→ universal quantum gates)

(II) Quantum error correction

(III) Fault tolerant quantum computing

(I) Gate accuracy

to which accuracy must quantum gates be physically implemented s.t. quantum computing still works ?

Recall: DFT use controlled phase shifts $R_k = \begin{pmatrix} 1 & \\ & e^{2\pi i/2^k} \end{pmatrix}$ up to $k = n$ (= number of qubits)

e.g. $n = 100$:

$$R_{100} = \begin{pmatrix} 1 & \\ & e^{2\pi i/2^{100}} \end{pmatrix}$$

$$= \mathbb{1}_2 + 10^{-30} \begin{pmatrix} 0 & \\ & 2\pi i \end{pmatrix} !$$

↑ necessary / irrelevant ?

Def.:

U approximates U' with accuracy ε

$:\Leftrightarrow \quad \| U - U' \|_{op} \leq \varepsilon$

$$\| A \|_{op} := \max_{|\psi|=1} |A\psi|$$

useful because of

(i) $\| U - U' \|_{op} \leq \varepsilon$

$\Rightarrow \forall |\varphi\rangle, |\psi\rangle : \big| |\langle\varphi|U|\psi\rangle|^2 - |\langle\varphi|U'|\psi\rangle|^2 \big| \leq 2\varepsilon$

$|\langle\varphi|U|\psi\rangle|^2 = p$, $|\langle\varphi|U'|\psi\rangle|^2 = p'$

p, p' ↖ ↗ transition probabilities

according to "ideal" and "real" gate transformations U and U'

we will also show:

(ii)

$$U = U_n U_{n-1} \cdots U_2 U_1$$

$$U' = U_n' U_{n-1}' \cdots U_2' U_1'$$

with $\| U_i - U_i' \|_{op} \leq \varepsilon$

$$\Rightarrow \quad \| U - U' \|_{op} \leq n\varepsilon$$

↑ linear growth with number of factors

implications:

poly. time generated circuit family $\{Q_n\}_{n \in \mathbb{N}}$

→ number T_n of elementary gates T_n in Q_n polynomially bounded:

$$T_n = O(n^d)$$

- bounded error-probability (BQP) requires $|p - p'| \leq O(1)$;

i.e.

$$\| Q_n - Q_n' \| \leq O(1)$$

Q_n and Q_n' results from T_n elementary gate transf.s:

$$Q_n = G_{T_n} G_{T_{n-1}} \cdots G_2 G_1$$
$$Q_n' = G_{T_n}' G_{T_{n-1}}' \cdots G_2' G_1'$$

with individ. accuracy $\| G_i - G_i' \| \leq \varepsilon$.

$\rightarrow \| Q_n - Q_n' \| \leq 2 T_n \varepsilon = O(n^2 \varepsilon)$

$\rightarrow$ to achieve $p - p' \leq O(1)$ we need individual gate errors

$$\boxed{\varepsilon \leq n^{-2}}$$

⊕ non-exponential !

⊖ not constant !

Moderate polynomial decrease with n physically feasible ?

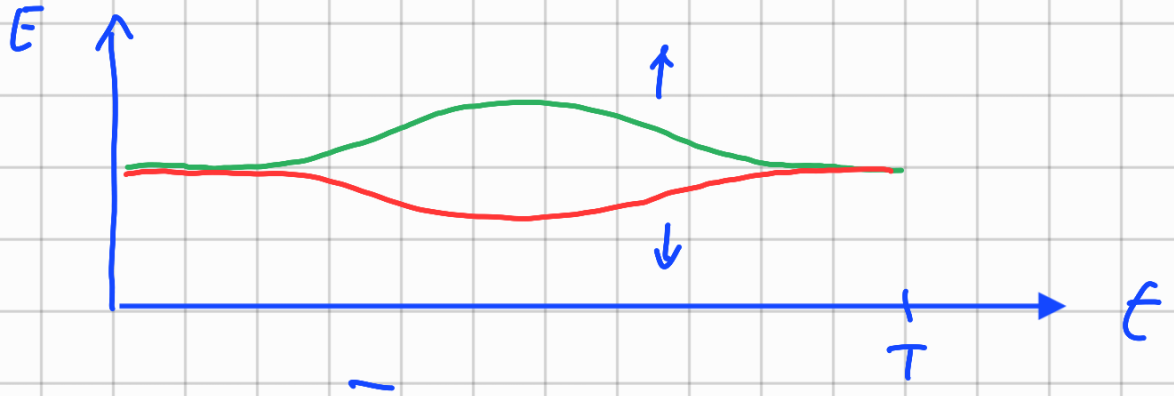
e.g. for Shor's algorithm with $n \approx 10^3$ qubits: $T_n \approx n^2 = 10^6$

$\rightarrow$ $\varepsilon \approx 10^{-6}$!

Example: phase-shift ($\uparrow e^{i\varphi}$)

on qubit = spin 1/2 by time-dependent mag. field $B(t)\,\vec{e}_z$,

$\rightarrow \quad E_{\uparrow/\downarrow} = E_0 \pm \mu_0 B(t)$



$$\varphi = \int_0^T dt\ \mu_0 B(t) \quad ;$$

with relative error $\frac{\Delta\varphi}{\varphi} \lesssim 10^{-6}$;

physically challenging !!

(control of phase-shifts φ by quantum state of other qubit even more challenging ...)

Rmk.: Use of operator-norm (= maximum-norm) corresponds to worst-case behaviour and therefore might overestimate required gate accuracy; however: alternative analysis based on 2-norm for average behaviour leads to similar results (cf. problem-sheet Nr. 5).

Proofs for relations (i) and (ii):

(i): $U' = V$, $P_\varphi = |\varphi\rangle\langle\varphi|$:

$$|p - p'| = \big|\,|\langle\varphi, U\psi\rangle|^2 - |\langle\varphi, V\psi\rangle|^2\,\big|$$

$$= |\langle\psi, U^+ P_\varphi U\psi\rangle - \langle\psi, U^+ V U\psi\rangle|$$

$$= |\langle\psi, U^+ P_\varphi \underbrace{(U-V)\psi}_{=:|x\rangle}\rangle + \underbrace{\langle\psi, (U-V)^+}_{=\langle x|} P_\varphi\,\psi\rangle|$$

$$= \left| \langle \psi, U^+ \varphi \rangle \langle \varphi, X \rangle + \langle X, \varphi \rangle \langle \varphi, V \psi \rangle \right|$$

$$\leq \quad 2 \left| \langle \varphi, X \rangle \right| = 2 \left| \langle \varphi, (U - V) \psi \rangle \right|$$

$$\leq \quad 2 \, \| U - V \|_{op} \quad \leq \quad 2 \varepsilon$$

(ii): by induction: $n = 1$ ✓

$n-1 \to n$: $\quad U = U_n \tilde{U}, \quad \tilde{U} = U_{n-1} \cdots U_1$

$$V = V_n \tilde{V}, \quad \tilde{V} = V_{n-1} \cdots V_1$$

with $\| U_n - V_n \|_{op} \leq \varepsilon$,

$\| \tilde{U} - \tilde{V} \|_{op} \leq (n-1) \varepsilon$;

$$\| U - V \| = \| U_n \tilde{U} - V_n \tilde{V} \| = \max_{\psi} \left| (U_n \tilde{U} - V_n \tilde{V}) \psi \right|$$

$$= \left| (U_n \tilde{U} - V_n \tilde{V}) \psi_0 \right| = \left| \{ (U_n - V_n) \tilde{U} + V_n (\tilde{U} - \tilde{V}) \} \psi_0 \right|$$

$$\leq \underbrace{\| U_n - V_n \|_{op}}_{\leq \varepsilon} + \underbrace{\| \tilde{U} - \tilde{V} \|_{op}}_{\leq (n-1)\varepsilon} \leq n \varepsilon$$

Universal quantum gates

Recall: any boolean function can be implemented by circuit made of elementary gates from a universal set as eg. $\{NAND, BRANCH\}$ or $\{CCNOT\}$.

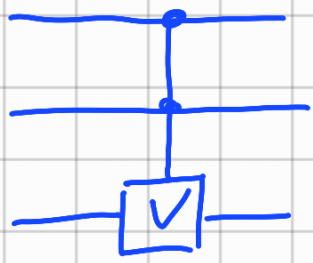
Does the same holds for quantum gates and circuits ?

Yes: Thm.: $\{CC[U], CC[W]\}$ with $U = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$, $W = \begin{pmatrix} 1 & \\ & e^{i\alpha} \end{pmatrix}$, where α/π irrational, is a universal set of quantum gates:

any unitary V can be implemented to any accuracy $\varepsilon > 0$ with a

a quantum circuit made of finitely many $CC[U]$ and $CC[W]$.

Remks.:

- $CC[V] \;\hat{=}\;$ 

$\hat{=} \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & V_{00} & V_{01} \\ & & & & V_{10} & V_{11} \end{pmatrix}$

- a better universal set with one 2-qubit gate and two 1-qubit gates is

$$\left\{ CNOT,\; H,\; T = \begin{pmatrix} 1 & \\ & e^{i\pi/4} \end{pmatrix} \right\};$$

however: proof of universality for $\{CC[U], CC[W]\}$ easier →

Proof in 3 stages:

I: $$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$ and

$$P_\theta = \begin{pmatrix} 1 & e^{i\theta} \end{pmatrix}$$

can be approximated by $U = R_\alpha$ and $W = P_\alpha$ to any accuracy:

$$\forall \varepsilon > 0 \quad \exists n: \quad \| R_\theta - U^n \| \leq \varepsilon$$

$$\| P_\theta - W^n \| \leq \varepsilon$$

(clear, because α/π irrational!)

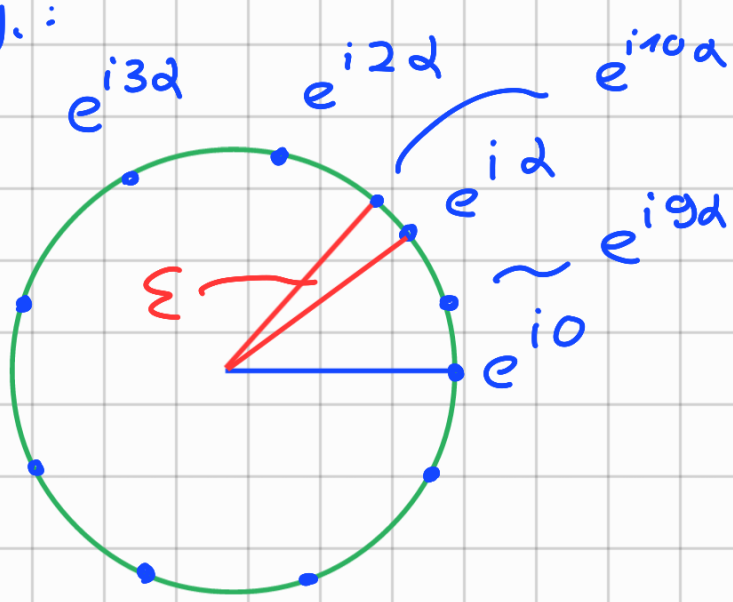
in more detail:

α/π irrational $\rightarrow$ for any $n \neq m$

$$e^{in\alpha} \neq e^{im\alpha}$$

$\rightarrow \{ e^{i\alpha n} \}_{n=0,1,\dots N}$ dividies

the unit-circle $S_1 \subset \mathbb{C}$ in to $N+1$ sectors (e.g.:



)

with $\varepsilon := \min \{ \delta_{lm} \} \overset{!}{\leq} \frac{2\pi}{N}$

$\rightsquigarrow \exists\ 1 \leq l \leq N : \quad e^{i\alpha l} = e^{i\varepsilon}$

$\rightsquigarrow \quad | e^{i\theta} - e^{i\alpha n_\theta} | \leq \varepsilon$

$\uparrow\ n_\theta = \lfloor \theta/\varepsilon \rfloor \cdot l$

„ Largest integer less than ... "

$\rightsquigarrow \quad \| P_\theta - W^{n_\theta} \| \leq \varepsilon$

$\| R_\theta - U^{n_\theta} \| \leq \varepsilon$

→ $CC[R_\theta]$ and $CC[P_\theta]$ can be approximated by $CC[U]$ and $CC[W]$ as well;

particularly $R_{\pi/2} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y$

$P_\pi = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} = \sigma_z$

→ $R_{\pi/2} P_\pi = -i\sigma_y \sigma_x = \sigma_x = NOT$

i.e CCNOT can be approximated and thus - by the classical universality of $\{CCNOT\}$ - all unitaries that represent boolean functions!

II: approximation of an arbitrary unitary $U \in U(8)$:

U : eigenvalues: $e^{i\Theta_j}$

eigenvectors: $|\psi_j\rangle$ $\quad j = 0, \dots, 7$

$$\rightarrow \text{with} \quad V_j := \sum_{k=0}^{7} e^{i\Theta_j} \delta_{kj} P_j$$

$$U = V_7 V_6 \cdots V_1 V_0 \quad ;$$

approximation of V_k as follows:

$$|\psi_k\rangle \xrightarrow{D_k} |111\rangle \xrightarrow[P_{\Theta_k}]{} e^{i\Theta_k} |111\rangle \xrightarrow{D_k^{-1}} e^{i\Theta_k} |\psi_k\rangle$$

$$\rightarrow V_k = D_k^{-1} P_{\Theta_k} D_k$$

approx. of D_k step-by-step:

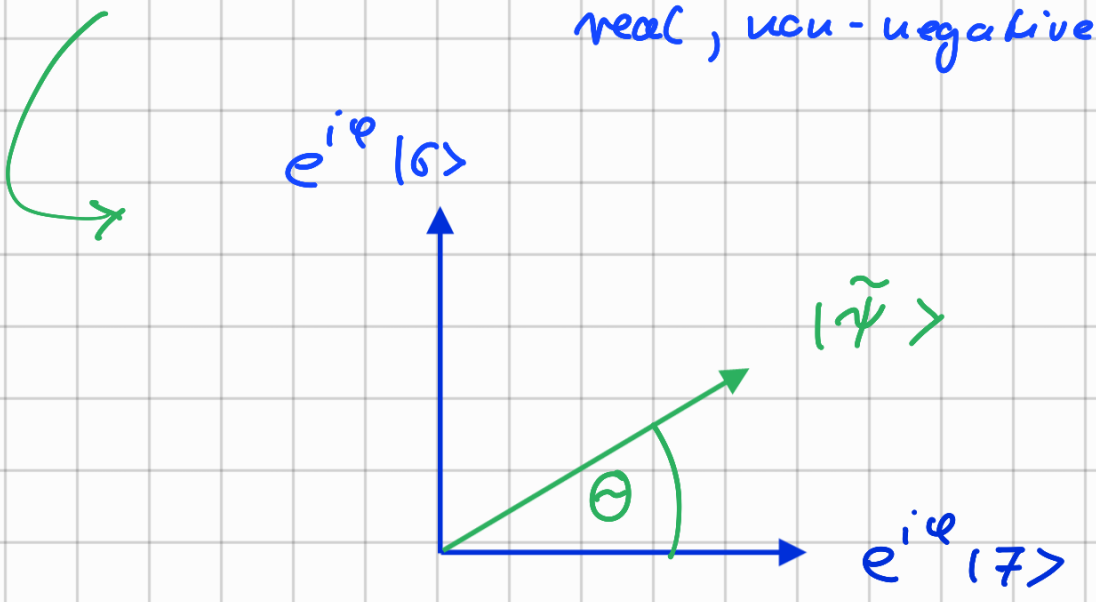
(a) $|\psi_k\rangle = \sum c_k |k\rangle \rightarrow |\psi'\rangle = \sum c_k' |k\rangle$

with $c_k' \stackrel{!}{=} 0$: $\rightarrow$

apply $CC[P_\chi]$ for suitable χ s.t.

$$\tilde{\lambda}_6 = r_6 e^{i\varphi}, \quad \tilde{\lambda}_7 = r_7 e^{i\varphi}$$

↑ real, non-negative !



applying $CC[R_{-\theta}]$ results in

$$|\psi'\rangle = \sum_\ell \lambda'_\ell |\ell\rangle \quad \text{with} \quad \lambda'_6 = 0 \; !$$

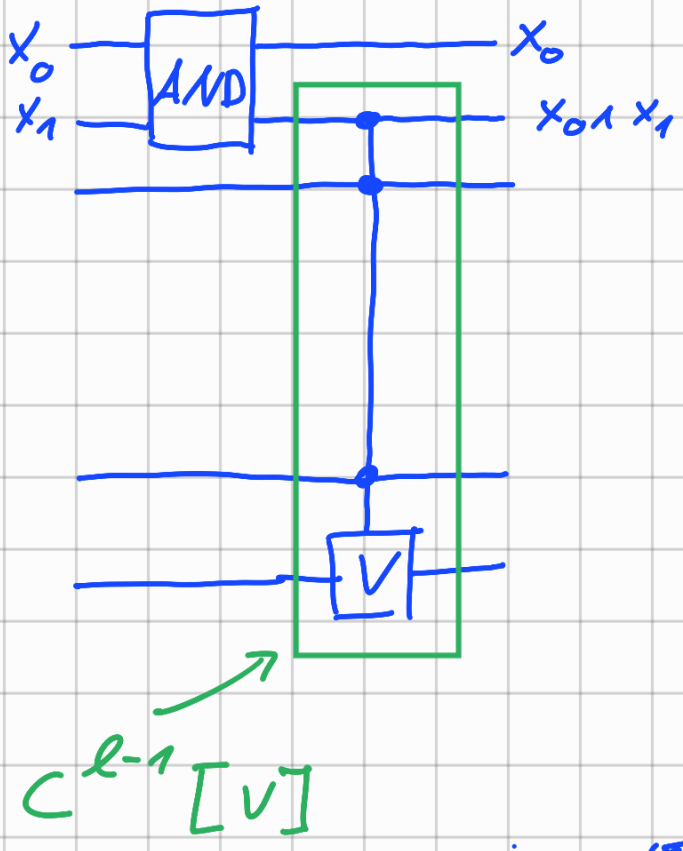
The same procedure after suitable permutations ($5 \leftrightarrow 6$, $4 \leftrightarrow 6$, ..., $0 \leftrightarrow 6$, with classically universal CCNOT !)

eventually results in D_h that rotates $|4\rangle$ to $|111\rangle$. ✓

III: approximation of general $U \in U(2^m)$ in the same manner with $(m-1)$-fold controlled V-gates, which in turn can be recursively reduced to $CC[V]$ and AND gates:

$C^\ell[V] \mathrel{\hat{=}}$

$\mathrel{\hat{=}}$



∎