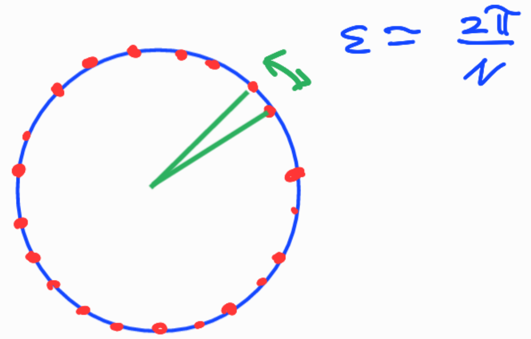
How <u>many</u> universal quantum gates do we need to approximate an arbitrary gate?

E.g. for appr. of $P_\theta = \begin{pmatrix} 1 & \\ & e^{i\theta} \end{pmatrix}$

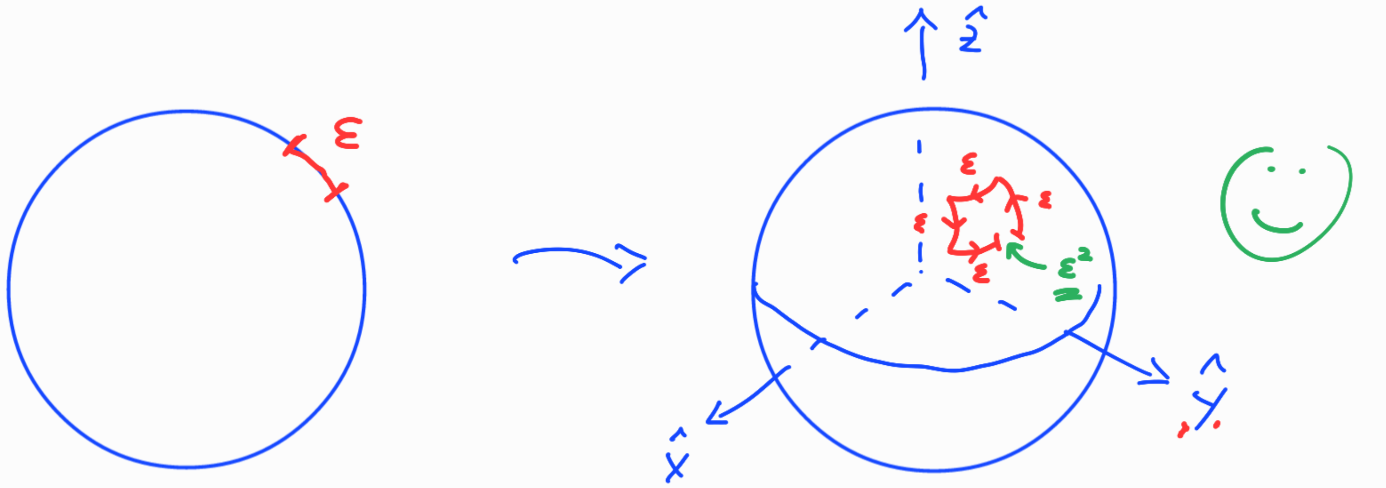
by $P_\alpha = \begin{pmatrix} 1 & \\ & e^{i\alpha} \end{pmatrix}$ :

acc. to proof of last lecture:




$\longrightarrow \quad \boxed{N_\varepsilon \sim \frac{1}{\varepsilon}}$

fortunately, one can do <u>much</u> better:




$S_1 \cong U(1)$ $\qquad$ $S_2 \cong SO_3 \cong SU(2)/\mathbb{Z}_2$

e.g. $U = e^{i\varepsilon\sigma_x}$, $V = e^{i\varepsilon\sigma_z}$

$$\rightarrow \underbrace{V^{-1}U^{-1}VU}_{\text{group-commutator of } V \text{ and } U} = e^{-\varepsilon^2 \underbrace{[\sigma_z,\sigma_x]}_{\text{commutator of the Lie-algebra}}} = e^{-2i\varepsilon^2\sigma_y}$$

$$\rightarrow \quad \varepsilon \rightarrow \varepsilon^2$$

in one step!

→ <u>Solovay - Kitaev thm:</u>

roughly: $N_\varepsilon = \mathcal{O}(\log^c 1/\varepsilon)$

→ $T$ gates can be approx. by $\mathcal{O}(T \log^c T)$ universal gates!

→ "universal set of gates" is a valid concept also in quantum comp.!

# Quantum Error Correction

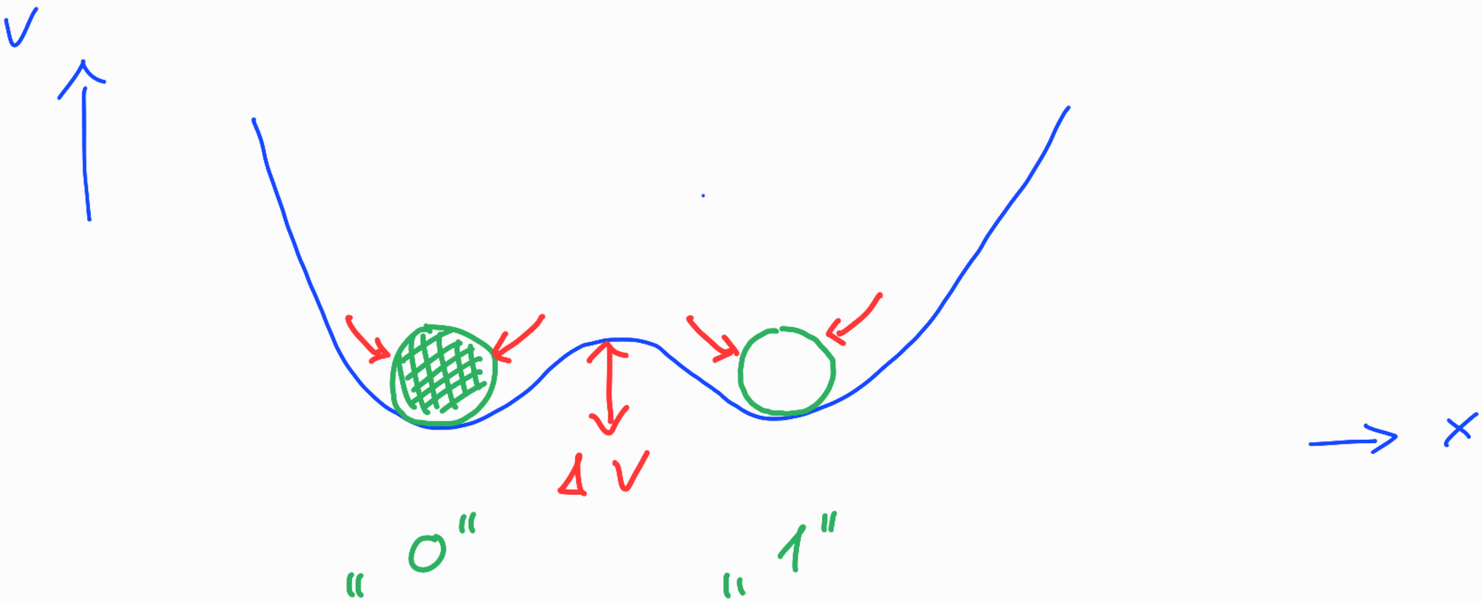
Error correction fundamental for quantum computation, whereas classical computer can do without error correction!

Why?

classical bit $\cong$ classical 2-state system

e.g. particle in a double well:

macroscopic!




classical bit is stabilized by dissipation!

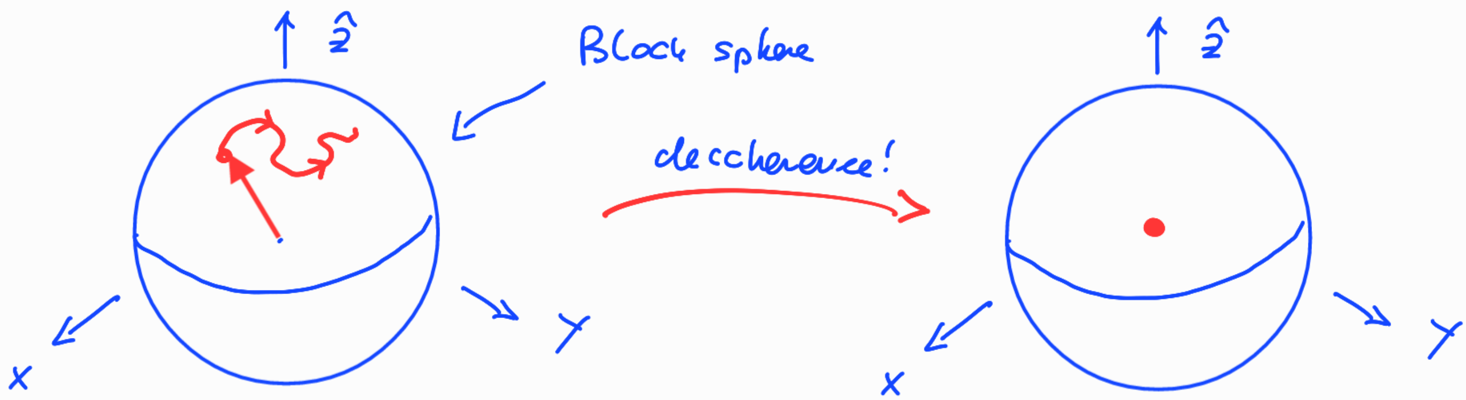
(as long as $k_B T \ll \Delta V$)

→ no need of active error correction!

→ non-perfect gates unproblematic!

<u>qubit</u> $\hat{=}$ quantum 2-state system

(e.g. spin $1/2$)




quantum bit sensitive

to any kind of external noise!

→ active quantum error-correction

indispensable!

( <u>if possible</u>: <u>poor</u> quantum gates useful!! )

prevailing opinion around 1995:

"QEC is never going to work!"

because

- "measurement (of error-syndrome) destroys qubit"
- "quantum errors are continuous"
- "decoherence can't be avoided" (Schrödinger-cats don't exist!)

these arguments were countered by Shor:

Suitable encoding of 1 logical qubit into 9 physical qubit allows for perfect recovery from total decoherence of any single (physical) qubit!

Shor's 1 - 9 encoding:

$$|0\rangle \longrightarrow |0_L\rangle = \frac{1}{\sqrt{8}}\left(|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3}\right)^{\otimes 3}$$

$$= \left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)/\sqrt{8}$$

$$|1\rangle \longrightarrow |1_L\rangle = \frac{1}{\sqrt{8}}\left(|0\rangle^{\otimes 3} - |1\rangle^{\otimes 3}\right)^{\otimes 3}$$

$$= \left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)/\sqrt{8}$$

## How does it work?

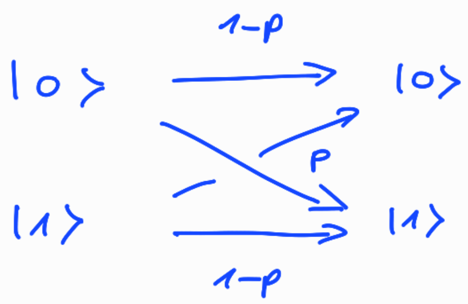
1st: elementary analysis (Shor)

2nd: general theory of QEC (later!)

Quantum error correction of bit-flips:

qubit (of a quantum register) flips with

probability $p$:



find encoding of 1 logical qubit into k physical qubits s.t. single bit-flip can be corrected!

$\rightsquigarrow$ 1–3 code: $|0\rangle \longrightarrow |0_L\rangle = |000\rangle$

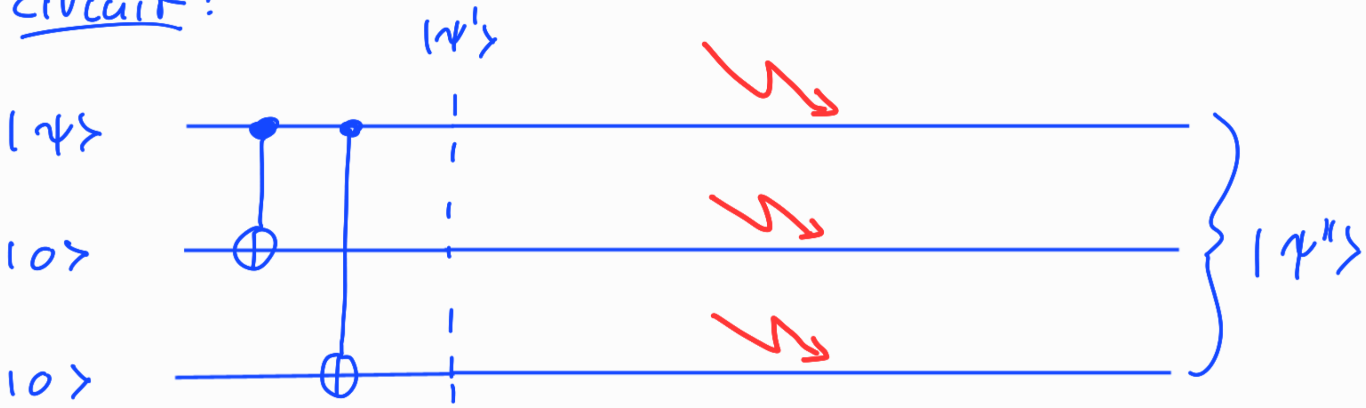
$|1\rangle \longrightarrow |1_L\rangle = |111\rangle$

$\rightarrow$ encoding of general state:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \rightarrow \quad |\psi'\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$$

$$= \alpha|000\rangle + \beta|111\rangle$$

circuit:




syndrom:

$$|\psi''\rangle = \begin{cases} |\psi_0\rangle = \alpha|000\rangle + \beta|111\rangle & : \quad - \\ |\psi_1\rangle = \alpha|100\rangle + \beta|011\rangle & : \quad 1 \\ |\psi_2\rangle = \alpha|010\rangle + \beta|101\rangle & : \quad 2 \\ |\psi_3\rangle = \alpha|001\rangle + \beta|110\rangle & : \quad 3 \end{cases}$$

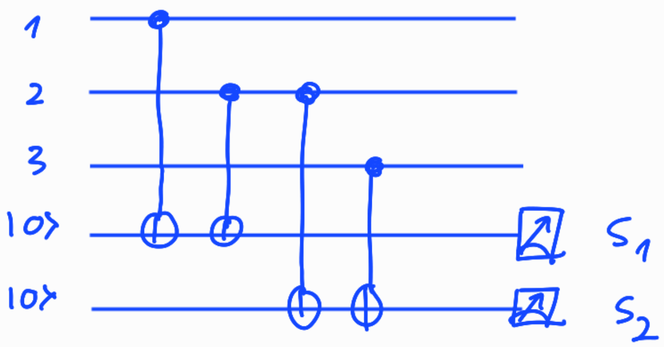
tricky point: measurement of error-syndrom without measurement of the logical qubit!

Solution: ideal measurement of $E_1 = Z_1 Z_2$, $E_2 = Z_2 Z_3$

| | $\vert\psi_0\rangle$ | $\vert\psi_1\rangle$ | $\vert\psi_2\rangle$ | $\vert\psi_3\rangle$ |
|---|---|---|---|---|
| $E_1$ : | 1 | -1 | -1 | 1 |
| $E_2$ : | 1 | +1 | -1 | -1 |
| Syn-drom : | – | 1 | 2 | 3 |

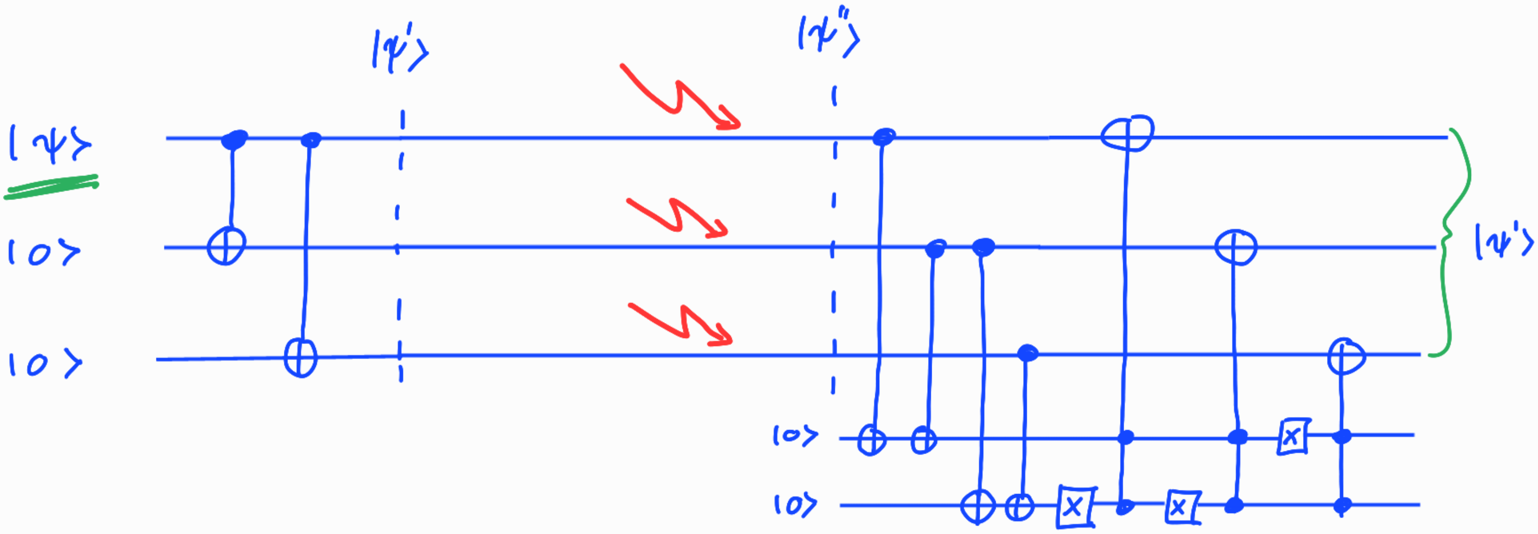
← eigenstates of $E_1$ and $E_2$

Circuit implementation:




| $S_2 S_1$ | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| Syndr. : | – | 1 | 3 | 2 |
| correct : | $\mathbb{1}$ | $X_1$ | $X_3$ | $X_2$ |

→ encoding, error-detection and -correction with following circuit :




Error correcting code for <u>phase-flips</u>:

$$|0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \xrightarrow{1-p} |1\rangle$$

$$\xrightarrow[p]{} -|1\rangle$$

( $\hat{=}$ apply $Z$ with prob. $p$ )

<u>idea</u>: <u>phase-flips</u> on $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} = H|0\rangle$

$$|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} = H|1\rangle$$

look like <u>bit-flips</u>: $Z|+\rangle = |-\rangle$

$$Z|-\rangle = |+\rangle$$

→ w.r.t. $|\pm\rangle$ basis phase-flip code

(as well as syndrom measurement, correction)

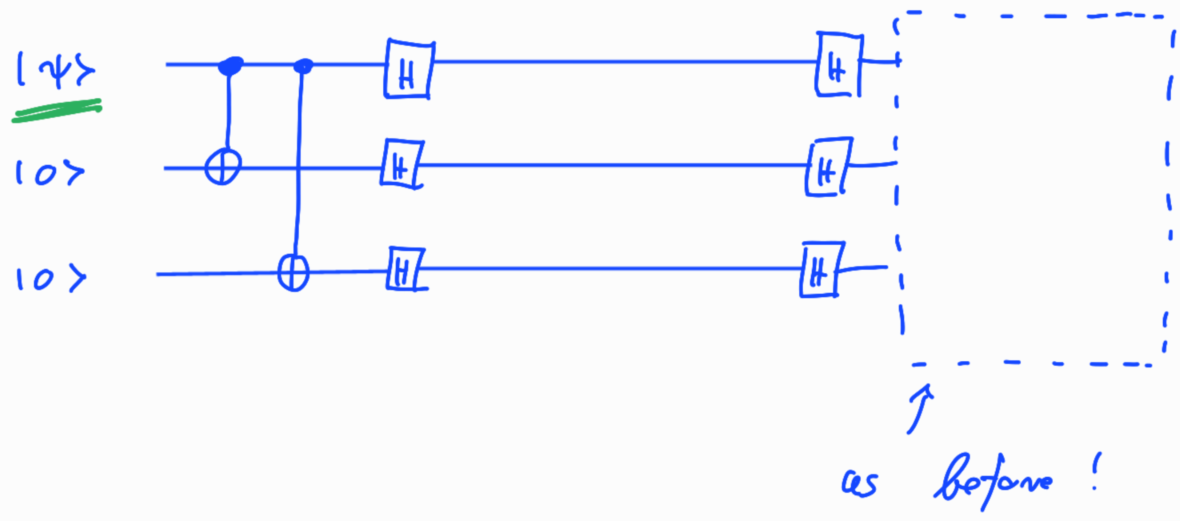
exactly as bit-flip code w.r.t. $|0\rangle, |1\rangle$

basis!

→ $|0\rangle \longrightarrow |0_L\rangle = |{+}{+}{+}\rangle$

$|1\rangle \longrightarrow |1_L\rangle = |{-}{-}{-}\rangle$

→ circuit:




concatenation of 1-3 bit-flip and

1-3 phase-flip code yields 1-9 Shor-code

that corrects simultaneous bit and phase-flips:

$$|0\rangle \to |+++\rangle = \underbrace{(|0\rangle+|1\rangle)}\underbrace{(|0\rangle+|1\rangle)}\underbrace{(|0\rangle+|1\rangle)}/\sqrt{8}$$

$$= (|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)/\sqrt{8}$$

$$= \left(|0\rangle^{\otimes 3}+|1\rangle^{\otimes 3}\right)^{\otimes 3}/\sqrt{8}$$

$$|1\rangle \longrightarrow \left(|0\rangle^{\otimes 3}-|1\rangle^{\otimes 3}\right)^{\otimes 3}/\sqrt{8}$$

Syndrom measurement:

$B_1^{(1)} = Z_1 Z_2$, $\quad B_1^{(2)} = Z_4 Z_5$, $\quad B_1^{(3)} = Z_7 Z_8$

$B_2^{(1)} = Z_2 Z_3$, $\quad B_2^{(2)} = Z_5 Z_6$, $\quad B_2^{(3)} = Z_8 Z_9$

for detection of bit-flips and

$P_1 = X_1 X_2 X_3 X_4 X_5 X_6$

$P_2 = X_4 X_5 X_6 X_7 X_8 X_9$

for detection of phase-flips.