Introduction to Quantum Computing

June 2021

Overview:

I.) From bits to qubits: Dirac notation, density matrices, measurements, Bloch sphere

II.) Quantum circuits: basic single-qubit & two-qubit gates, multipartite quantum states

III.) Entanglement: Bell states, Teleportation, Q-sphere

I. From bits to qubits

- classical states for computation are either "0" or "1"
- in quantum mechanics, a state can be in superposition, i.e., simultaneously in "0" and "1"
  - → superpositions allow to perform calculations on many states at the same time
    - ⇒ quantum algorithms with exponential speed-up

BUT: once we measure the superposition state, it collapses to one of its states

(→ we can only get one "answer" and not all answers to all states in the superposition)

⇒ it is not THAT easy to design quantum algorithms, but we can use interference effects

(→ "wrong answers" cancel each other out, while the "right answer" remai

Dirac notation & density matrices

- used to describe quantum states: let $a, b \in \mathbb{C}^2$. (→ 2-dimensional vector with complex entries)
  - ket: $|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$
  - bra: $\langle b| = |b\rangle^{+} = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}^{+} = \begin{pmatrix} b_1^* & b_2^* \end{pmatrix}$ ← complex conjugated & transposed
  - bra-ket: $\langle b|a\rangle = a_0 b_0^* + a_1 b_1^* = \langle a|b\rangle^* \in \mathbb{C}$ (→ complex number) ← inner product
  - ket-bra: $|a\rangle\langle b| = \begin{pmatrix} a_0 b_0^* & a_0 b_1^* \\ a_1 b_0^* & a_1 b_1^* \end{pmatrix}$ (→ 2×2-matrix) ← not an "X" !!

- we define the pure states $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which are orthogonal: $\langle 0|1\rangle = 1 \cdot 0 + 0 \cdot 1 = 0$

  ↳ $|0\rangle\langle 0| = (1\ 0) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $|1\rangle\langle 1| = (0\ 1) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$$\Rightarrow \rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} = \rho_{00} \cdot |0\rangle\langle 0| + \rho_{01} |0\rangle\langle 1| + \rho_{10} |1\rangle\langle 0| + \rho_{11} |1\rangle\langle 1|$$

- all quantum states can be described by density matrices, i.e.,

  normalized positive Hermitian operators ρ : $tr(\rho) = 1$, $\rho \geq 0$, $\rho = \rho^+$

  $\Leftrightarrow$ for $\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}$: $tr(\rho) = \rho_{00} + \rho_{11} \overset{!}{=} 1$, $\langle \psi | \rho | \psi \rangle \geq 0 \ \forall |\psi\rangle \Leftrightarrow$ all eigenvalues ≥ 0, $\rho^+ = \begin{pmatrix} \rho_{00}^* & \rho_{10}^* \\ \rho_{01}^* & \rho_{11}^* \end{pmatrix} = \rho$
- all quantum states are normalized, i.e., $\langle \psi | \psi \rangle = 1$, e.g. $|\psi\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle) = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$
- spectral decomposition: for every density matrix ρ $\exists$ an orthonormal basis $\{|i\rangle\}_i$

  s.t. $\rho = \sum_i \lambda_i |i\rangle\langle i|$, where $|i\rangle$: eigenstates, λ_i : eigenvalues, $\sum_i \lambda_i = 1$
- a density matrix is pure, if $\rho = |\phi\rangle\langle\phi|$, otherwise it is mixed

  $\rightarrow$ if ρ is pure, one eigenvalue equals 1, all others are 0,

  i.e. $tr(\rho^2) = \sum_i \lambda_i^2 = 1$ if ρ is pure, otherwise $tr(\rho^2) < 1$
- examples: (i) $\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0|$ $\rightarrow$ pure , $\rho = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle\langle 1|$ $\rightarrow$ pure

  (ii) $\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|)$ $\rightarrow$ mixed

  (iii) $\rho = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2} (|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} (|0\rangle - |1\rangle)(\langle 0| - \langle 1|)$

  $\hookrightarrow$ pure

Measurements

- we choose orthogonal bases to describe & measure quantum states ($\rightarrow$ projective measurement)
- during a meas. onto the basis $\{|0\rangle, |1\rangle\}$, the state will collapse into either state

  $|0\rangle$ or $|1\rangle$ $\rightarrow$ as these are the eigenstates of σ_z, we call this a z-measurement
- there are infinitely many different bases, but other common ones are

  $\{ |+\rangle := \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), |-\rangle := \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \}$ and $\{ |+i\rangle := \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle), |-i\rangle := \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle) \}$,

  corresponding to the eigenstates of σ_x and σ_y, respectively.
- Born rule: the probability that a state $|\psi\rangle$ collapses during a projective meas. onto the

  basis $\{|x\rangle, |x^\perp\rangle\}$ to the state $|x\rangle$ is given by

  $P(x) = |\langle x | \psi \rangle|^2$, $\sum_i P(x_i) = 1$

· examples: - $|\psi\rangle = \frac{1}{\sqrt{3}}\left(|0\rangle + \sqrt{2}\,|1\rangle\right)$ is meas. in the basis $\{|0\rangle, |1\rangle\}$:

$$\rightarrow P(0) = \left|\langle 0|\tfrac{1}{\sqrt{3}}\left(|0\rangle + \sqrt{2}\,|1\rangle\right)\right|^2 = \left|\tfrac{1}{\sqrt{3}}\underbrace{\langle 0|0\rangle}_{1} + \sqrt{\tfrac{2}{3}}\underbrace{\langle 0|1\rangle}_{0}\right|^2 = \frac{1}{3} \rightarrow P(1) = \frac{2}{3}$$

- $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ is measured in the basis $\{|+\rangle, |-\rangle\}$:

$$\rightarrow P(+) = |\langle +|\psi\rangle|^2 = \left|\tfrac{1}{\sqrt{2}}\left(\langle 0| + \langle 1|\right)\cdot\tfrac{1}{\sqrt{2}}\cdot\left(|0\rangle - |1\rangle\right)\right|^2$$

$$= \frac{1}{4}\left|\underbrace{\langle 0|0\rangle}_{1} - \underbrace{\langle 0|1\rangle}_{0} + \underbrace{\langle 1|0\rangle}_{0} - \underbrace{\langle 1|1\rangle}_{1}\right|^2 = 0 \rightarrow \text{expected, as } \langle +|\psi\rangle = \underbrace{\langle +|-\rangle}_{\text{orthogonal}} = 0$$

$\hookrightarrow P(-) = |\langle -|-\rangle|^2 =$

Bloch sphere:

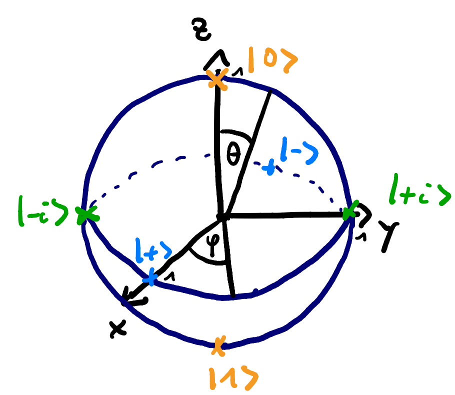
We can write any normalized (pure) state as $\quad |\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle$,

where $\varphi \in [0, 2\pi]$ describes the relative phase and $\theta \in [0, \pi]$ determines the probability to measure $|0\rangle$ / $|1\rangle$: $\quad p(|0\rangle) = \cos^2\frac{\theta}{2}$, $\ p(|1\rangle) = \sin^2\frac{\theta}{2}$.

⇒ all normalized pure states can be illustrated on the surface of a sphere with radius $|\vec{r}| = 1$, which we call the Bloch sphere

⇒ the coordinates of such a state are given by the Bloch vector: $\vec{r} = \begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix}$

<u>examples</u>:
- $|0\rangle$: $\theta = 0$, φ arbitrary $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$
- $|1\rangle$: $\theta = \pi$, φ arb. $\rightarrow \vec{r} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$
- $|+\rangle$: $\theta = \frac{\pi}{2}$, $\varphi = 0 \rightarrow \vec{r} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
- $|-\rangle$: $\theta = \frac{\pi}{2}$, $\varphi = \pi \rightarrow \vec{r} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$
- $|+i\rangle$: $\theta = \frac{\pi}{2}$, $\varphi = \frac{\pi}{2} \rightarrow \vec{r} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$
- $|-i\rangle$: $\theta = \frac{\pi}{2}$, $\varphi = \frac{3\pi}{2} \rightarrow \vec{r} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$



<u>Be careful</u>: On the Bloch sphere, angles are twice as big as in Hilbert space, e.g. $|0\rangle$ & $|1\rangle$ are orthogonal, but on the Bloch sphere their angle is 180°. For a general state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \ldots \rightarrow \theta$ is the angle on the Bloch sphere, while $\frac{\theta}{2}$ is the actual angle in Hilbert space!

⇒ Z-measurement corresponds to a projection onto the z-axis and analogously for X & Y!

II. Quantum Circuits

- "circuit model": sequence of building blocks that carry out elementary computations, called gates

input — $\boxed{\text{algorithm}}$ — output

Single qubit gates

- classical example: NOT 
- quantum examples: as quantum theory is unitary, quantum gates are represented by

unitary matrices: $U^{\dagger}U = \mathbb{1}$

recall Dirac notation: $U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} = u_{00}|0\rangle\langle 0| + u_{01}|0\rangle\langle 1| + u_{10}|1\rangle\langle 0| + u_{11}|1\rangle\langle 1|$

- $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$

  ↳ $\sigma_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$, Dirac notation ↓ $\sigma_x|1\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|) \cdot |1\rangle) = |0\rangle\underbrace{\langle 1|1\rangle}_{1} + |1\rangle\underbrace{\langle 0|1\rangle}_{0} = |0\rangle$

  ⇒ bit flip $\hat{=}$ NOT-gate, e.g. $|0\rangle - \boxed{\sigma_x} - |1\rangle$ ⇒ rotation around x-axis by π

- $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

  ↳ $\sigma_z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle$, $\sigma_z|-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \cdot \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  $= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

  ⇒ phase flip ⇒ rotation around z-axis by π

- $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i \cdot \sigma_x \cdot \sigma_z$ ⇒ bit & phase flip

  ⇒ σ_x, σ_y & σ_z are the so-called Pauli matrices and $\sigma_i^2 = \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (does nothing)

  ⇒ together with identity $\mathbb{1}$ they form a basis of 2x2 matrices

  (→ any 1-qubit rotation can be written as a linear combination of them)

- Hadamard gate: one of the most important gates for quantum circuits

  $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$

  ↳ $H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \cdot |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

  ⇒ creates superposition! also $H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$ ⇒ used to change between X & Z basis

- similarly, as $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ adds 90° to the phase φ: $S \cdot |+\rangle = |+i\rangle$, $S|-\rangle = |-i\rangle$

  ⇒ $S \cdot H$ is applied to change from Z to Y basis

Multipartite quantum states

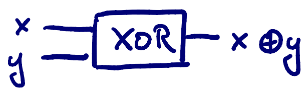
- we use tenser products to describe multiple states: $|a\rangle \otimes |b\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$
- example: system A is in state $|1\rangle_A$ and system B is in state $|0\rangle_B$

  $\Rightarrow$ the total (bipartite) state is $|10\rangle_{AB} := |1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$

  ↳ remark: states of this form are called uncorrelated, but there are also bipartite states that cannot be written as $|\psi\rangle_A \otimes |\varphi\rangle_B$. These states are correlated and sometimes even entangled (→very strong correlation), e.g. $|\psi^{(00)}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

  a so-called Bell state, used for teleportation, cryptography, Bell tests, etc.

Two-qubit gates

- classical example: XOR  →irreversible (→given the output we cannot recover the input)

  BUT: as quantum theory is unitary, we only consider unitary and therefore reversible gates

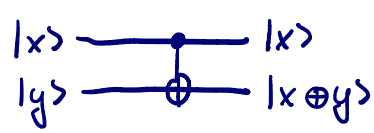
- quantum example:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

↳ $CNOT \cdot |00\rangle_{xy} = CNOT \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle_{xy}$, $\quad CNOT\,|10\rangle_{xy} = |11\rangle_{xy}$

$\Rightarrow$

input		output	
x	y	x	x⊕y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$\Rightarrow$ circuit: 

$\hat{=}$ reversible XOR

$\Rightarrow$ we can show that every function f can be described by a reversible circuit

$\Rightarrow$ quantum circuits can perform all functions that can be calculated classically

III. Entanglement

- If a pure state $|\Psi\rangle_{AB}$ on systems A, B cannot be written as $|\varphi\rangle_A \otimes |\Phi\rangle_B$, it is entangled

Bell states

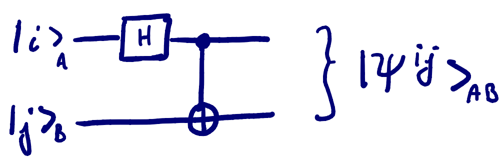
There are four so-called Bell states that are maximally entangled and build an orthonormal basis:

$$|\psi^{00}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \qquad |\psi^{01}\rangle := (|01\rangle + |10\rangle)$$

$$|\psi^{10}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad |\psi^{11}\rangle := (|01\rangle - |10\rangle)$$

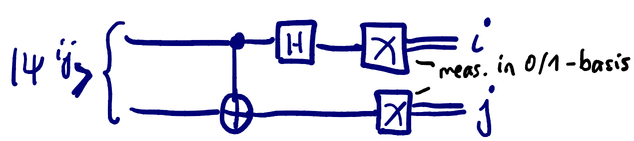
$\Rightarrow$ in general we can write $\quad |\psi^{ij}\rangle = (\mathbb{1} \otimes \sigma_x^j \cdot \sigma_z^i)|\psi^{00}\rangle$

Creation of Bell states



initial state $\|ij\rangle_{AB}$		$(H_A \otimes \mathbb{1}_B)\|ij\rangle_{AB}$		$\|\psi^{ij}\rangle$
$\|00\rangle$		$(\|00\rangle + \|10\rangle)/\sqrt{2}$		$(\|00\rangle + \|11\rangle)/\sqrt{2} = \|\psi^{00}\rangle$
$\|01\rangle$	$\xrightarrow{H_A}$	$(\|01\rangle + \|11\rangle)/\sqrt{2}$	$\xrightarrow{CNOT_{AB}}$	$(\|01\rangle + \|10\rangle)/\sqrt{2} = \|\psi^{01}\rangle$
$\|10\rangle$		$(\|00\rangle - \|10\rangle)/\sqrt{2}$		$(\|00\rangle - \|11\rangle)/\sqrt{2} = \|\psi^{10}\rangle$
$\|11\rangle$		$(\|01\rangle - \|11\rangle)/\sqrt{2}$		$(\|01\rangle - \|10\rangle)/\sqrt{2} = \|\psi^{11}\rangle$

$\rightarrow$ opposite direction: Bell measurement



$\Rightarrow$ classical outcomes i, j correspond to a meas. of the state $|\psi^{ij}\rangle$

Teleportation

- **Goal**: Alice wants to send her (unknown) state $|\phi\rangle_S := \alpha|0\rangle_S + \beta|1\rangle_S$ to Bob.

  She can only send him two classical bits though. They both share the maximally entangled state $|\Psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$.

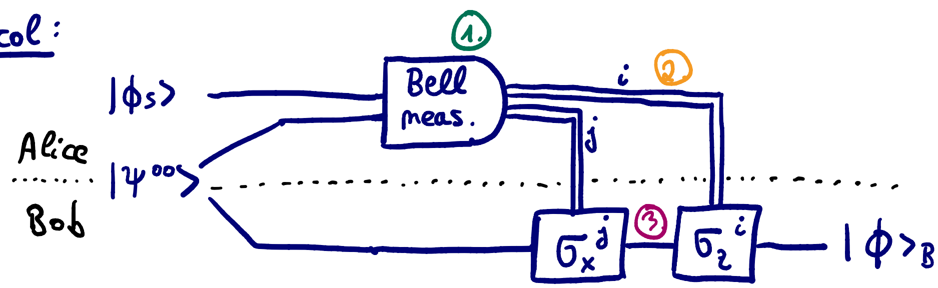
$\Rightarrow$ initial state of the total system:

$$|\phi\rangle_S \otimes |\Psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}\right)$$

$$= \frac{1}{2\sqrt{2}}\Big[(|00\rangle_{SA} + |11\rangle_{SA})\otimes(\alpha|0\rangle_B + \beta|1\rangle_B) + (|01\rangle_{SA} + |10\rangle_{SA})\otimes(\alpha|1\rangle_B + \beta|0\rangle_B)$$
$$+ (|00\rangle_{SA} - |11\rangle_{SA})\otimes(\alpha|0\rangle_B - \beta|1\rangle_B) + (|01\rangle_{SA} - |10\rangle_{SA})\otimes(\alpha|1\rangle_B - \beta|0\rangle_B)\Big]$$

$$= \frac{1}{2}\Big[|\Psi^{00}\rangle_{SA}\otimes|\phi\rangle_B + |\Psi^{01}\rangle_{SA}\otimes(\sigma_x|\phi\rangle_B)$$
$$+ |\Psi^{10}\rangle_{SA}\otimes(\sigma_z|\phi\rangle_B) + |\Psi^{11}\rangle_{SA}\otimes(\sigma_x\sigma_z|\phi\rangle_B)\Big]$$

- **Protocol**:



1. Alice performs a meas. on S & A in the Bell basis.
2. She sends her classical outputs i, j to Bob.
3. Bob applies $\sigma_z^i\sigma_x^j$ to his qubit and gets $|\phi\rangle$!

1. Alice's measurement		→ Bob's state	2. Alice sends $i\ j$	3. Bob applies	→ Bob's final state
$\lvert\Psi^{00}\rangle$		$\lvert\phi\rangle_B$	0 0	$\mathbb{1}$	$\lvert\phi\rangle_B$
$\lvert\Psi^{01}\rangle$	$\otimes$	$\sigma_x\lvert\phi\rangle_B$	0 1	σ_x	"
$\lvert\Psi^{10}\rangle$		$\sigma_z\lvert\phi\rangle_B$	1 0	σ_z	"
$\lvert\Psi^{11}\rangle$		$\sigma_x\sigma_z\lvert\phi\rangle_B$	1 1	$\sigma_z\sigma_x$	"

Note, that Alice's state collapsed during the measurement, so she does not have the initial state $|\phi\rangle$ anymore. This is expected due to the no-cloning theorem, as she cannot copy her state, but just send her state to Bob when destroying her own.