

Introduction to Quantum Computing

Overview:

- I.) From bits to qubits: Dirac notation, 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" remains)

Dirac notation

- used to describe quantum states: let $a, b \in \mathbb{C}^2$. (→ 2-dimensional vector with complex entries)
 - ket: $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ ← complex conjugated & transposed
 - bra: $\langle b| = |b\rangle^+ = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^+ = (b_1^* \ b_2^*)$
 - bra-ket: $\langle b|a\rangle = a_1 b_1^* + a_2 b_2^* = \langle a|b\rangle^* \in \mathbb{C}$ (→ complex number)
 - ket-bra: $|a\rangle\langle b| = \begin{pmatrix} a_1 b_1^* & a_1 b_2^* \\ a_2 b_1^* & a_2 b_2^* \end{pmatrix}$ (→ 2×2 -matrix)
- we define the states $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, which are orthogonal: $\langle 0|1\rangle = 1 \cdot 0 + 0 \cdot 1 = 0$
- all quantum states are normalized, i.e., $\langle \psi|\psi\rangle = 1$, e.g. $|\Psi\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle) = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$

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 those are the eigenstates of $\hat{\sigma}_z$, we call this a z -measurement
- there are infinitely many different bases, but other common ones are

$$\{|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$
 corresponding to the eigenstates of $\hat{\sigma}_x$ and $\hat{\sigma}_y$, 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

$$P(x) = |\langle x | \psi \rangle|^2 \quad , \quad \sum_i P(x_i) = 1$$
- examples:
 - $|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle)$ is meas. in the basis $\{|0\rangle, |1\rangle\}$:

$$\rightarrow P(0) = \left| \langle 0 | \frac{1}{\sqrt{3}}(|0\rangle + \sqrt{2}|1\rangle) \right|^2 = \left| \frac{1}{\sqrt{3}} \underbrace{\langle 0 | 0 \rangle}_1 + \sqrt{\frac{2}{3}} \underbrace{\langle 0 | 1 \rangle}_0 \right|^2 = \frac{1}{3} \rightarrow P(1) = \frac{2}{3}$$
 - $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is measured in the basis $\{|+\rangle, |-\rangle\}$:

$$\begin{aligned} \rightarrow P(+)&= |\langle + | \psi \rangle|^2 = \left| \frac{1}{\sqrt{2}} (\langle 0 | + \langle 1 |) \cdot \frac{1}{\sqrt{2}} \cdot (|0\rangle - |1\rangle) \right|^2 \\ &= \frac{1}{4} \left| \underbrace{\langle 0 | 0 \rangle}_1 - \underbrace{\langle 0 | 1 \rangle}_0 + \underbrace{\langle 1 | 0 \rangle}_0 - \underbrace{\langle 1 | 1 \rangle}_1 \right|^2 = 0 \rightarrow \text{expected, as } \langle + | \psi \rangle - \langle + | - \rangle = 0 \\ &\hookrightarrow P(-) = \left| \langle - | \psi \rangle \right|^2 = \text{orthogonal} \end{aligned}$$

Bloch sphere:

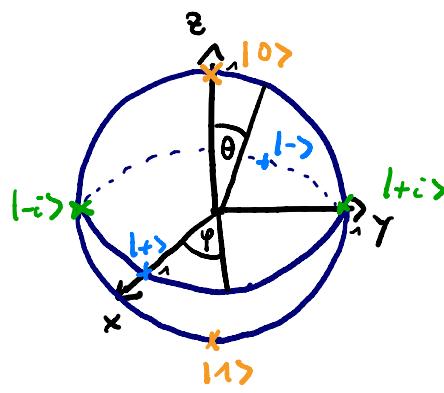
We can write any normalized (pure) state as $|\psi\rangle = \cos \frac{\Theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\Theta}{2} |1\rangle$,

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

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

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

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



Be careful: 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 $|+\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \dots \rightarrow \theta$ is the

angle on the Bloch sphere, while $\frac{\theta}{2}$ is the actual angle in Hilbert space!

\Rightarrow 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



Single qubit gates

- classical example: NOT $|1\rangle \rightarrow |0\rangle$
- quantum examples: as quantum theory is unitary, quantum gates are represented by

unitary matrices: $U^\dagger U = 1\!l$

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

$$-\quad \tilde{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

Dirac notation

$$\hookrightarrow \tilde{\sigma}_x|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \quad \tilde{\sigma}_x|1\rangle = \underbrace{(\tilde{\sigma}_x|0\rangle)}_{\downarrow} \cdot |1\rangle = |0\rangle$$

\Rightarrow bit flip $\hat{=}$ NOT-gate, e.g. $|0\rangle \xrightarrow{\tilde{\sigma}_x} |1\rangle \Rightarrow$ rotation around x-axis by π

$$-\quad \tilde{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

$$\hookrightarrow \tilde{\sigma}_z|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle, \quad \tilde{\sigma}_z|-\rangle = (|0\rangle\langle 0| - |1\rangle\langle 1|) \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

\Rightarrow phase flip \Rightarrow rotation around z-axis by π

$$= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle$$

$$-\quad \tilde{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i \cdot \tilde{\sigma}_x \cdot \tilde{\sigma}_z \quad \Rightarrow \text{bit \& phase flip}$$

$\Rightarrow \tilde{\sigma}_x, \tilde{\sigma}_y \& \tilde{\sigma}_z$ are the so-called Pauli matrices and $\tilde{\sigma}_i^2 = 1\!l = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (does nothing)

\Rightarrow together with identity $1\!l$ they form a basis of 2×2 matrices

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

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

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

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

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

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

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

Multipartite quantum states

- we use tensor 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 (bi-partite) 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 bi-partite states that cannot be written as $|\psi\rangle_A \otimes |\psi\rangle_B$. These states are **correlated** and sometimes even **entangled** (\rightarrow very strong correlation), e.g. $|\Psi\rangle_{AB}^{(0)} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$
 a so-called **Bell state**, used for teleportation, cryptography, Bell tests, etc.

Two-qubit gates

- classical example: XOR $\begin{array}{c} x \\ y \end{array} \xrightarrow{\text{XOR}} \begin{array}{c} x \oplus y \end{array} \quad \rightarrow \text{irreversible} \quad (\rightarrow \text{given the output we cannot recover the input})$
 BUT: as quantum theory is unitary, we only consider unitary and therefore **reversible** gates
- quantum example:
 $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$
 $\hookrightarrow CNOT \cdot |00\rangle_{xy} = CNOT \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle_{xy}, \quad CNOT \cdot |10\rangle_{xy} = |11\rangle_{xy}$
- $\begin{array}{c|cc} \text{input} & \text{output} \\ \hline x \ y & x \oplus y \\ \hline 0 \ 0 & 0 \ 0 \\ 0 \ 1 & 0 \ 1 \\ 1 \ 0 & 1 \ 1 \\ 1 \ 1 & 1 \ 0 \end{array} \Rightarrow \text{circuit: } \begin{array}{ccc} |x\rangle & \xrightarrow{\quad} & |x\rangle \\ |y\rangle & \xrightarrow{\oplus} & |x \oplus y\rangle \end{array}$
 $\hat{=} \text{reversible XOR}$

\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 $|\Psi_{AB}\rangle$ on systems A, B cannot be written as $|\psi_A\rangle \otimes |\phi_B\rangle$, it is entangled Bell states.

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

$$|\Psi^{00}\rangle := \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

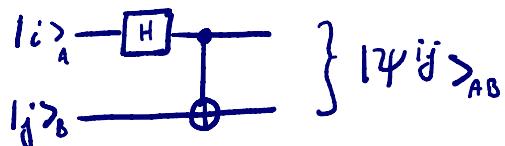
$$|\Psi^{01}\rangle := (|01\rangle + |10\rangle)$$

$$|\Psi^{10}\rangle := \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$|\Psi^{11}\rangle := (|01\rangle - |10\rangle)$$

→ in general we can write $|\Psi^{ij}\rangle = (I \otimes \sigma_x^j \cdot \sigma_z^i) |\Psi^{00}\rangle$

Creation of Bell states



initial state

$$|i,j\rangle_{AB}$$

$$(H_A \otimes I_B) |i,j\rangle_{AB}$$

$$|\Psi^{ij}\rangle$$

$$|00\rangle$$

$$(|00\rangle + |11\rangle)/\sqrt{2}$$

$$(|00\rangle + |11\rangle)/\sqrt{2} = |\Psi^{00}\rangle$$

$$|01\rangle$$

$$\xrightarrow{H_A}$$

$$(|01\rangle + |10\rangle)/\sqrt{2}$$

$$\xrightarrow{\text{CNOT}_{AB}}$$

$$(|01\rangle + |10\rangle)/\sqrt{2} = |\Psi^{01}\rangle$$

$$|10\rangle$$

$$(|00\rangle - |11\rangle)/\sqrt{2}$$

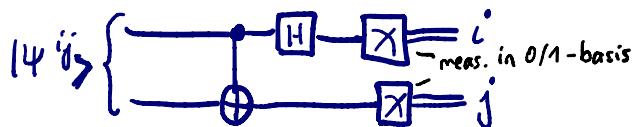
$$(|00\rangle - |11\rangle)/\sqrt{2} = |\Psi^{10}\rangle$$

$$|11\rangle$$

$$(|01\rangle - |10\rangle)/\sqrt{2}$$

$$(|01\rangle - |10\rangle)/\sqrt{2} = |\Psi^{11}\rangle$$

→ opposite direction: Bell measurement



→ 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.

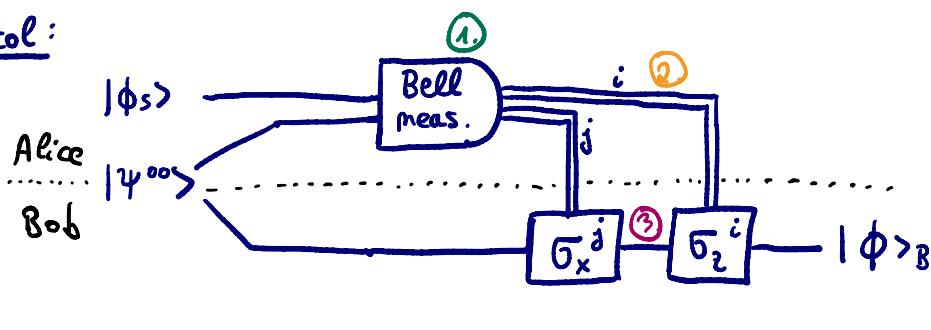
She can only send him two classical bits though. They both share the

maximally entangled state $|\Psi^{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$.

⇒ initial state of the total system:

$$\begin{aligned}
 |\phi\rangle_s \otimes |\Psi^{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(\alpha|000\rangle_{SAB} + \alpha|011\rangle_{SAB} + \beta|100\rangle_{SAB} + \beta|111\rangle_{SAB}) \\
 &= \frac{1}{2\sqrt{2}}[(|00\rangle_{SA} + |11\rangle_{SA}) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + (|01\rangle_{SA} + |10\rangle_{SA}) \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \\
 &\quad + (|00\rangle_{SA} - |11\rangle_{SA}) \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) + (|01\rangle_{SA} - |10\rangle_{SA}) \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)] \\
 &= \frac{1}{2} [|\Psi^{00}\rangle_{SA} \otimes |\phi\rangle_B + |\Psi^{01}\rangle_{SA} \otimes (\bar{\sigma}_x |\phi\rangle_B) \\
 &\quad + |\Psi^{10}\rangle_{SA} \otimes (\bar{\sigma}_z |\phi\rangle_B) + |\Psi^{11}\rangle_{SA} \otimes (\bar{\sigma}_x \bar{\sigma}_z |\phi\rangle_B)]
 \end{aligned}$$

- 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 $\bar{\sigma}_z^i \bar{\sigma}_x^j$ to his qubit and gets $|\phi\rangle_B$

1. Alice's measurement → Bob's state

$$\begin{array}{ll}
 |\Psi^{00}\rangle & |\phi\rangle_B \\
 |\Psi^{01}\rangle & \bar{\sigma}_x |\phi\rangle_B \\
 |\Psi^{10}\rangle & \bar{\sigma}_z |\phi\rangle_B \\
 |\Psi^{11}\rangle & \bar{\sigma}_x \bar{\sigma}_z |\phi\rangle_B
 \end{array}$$

2. Alice sends i, j

$$\begin{array}{ll}
 00 & 00 \\
 01 & 01 \\
 10 & 10 \\
 11 & 11
 \end{array}$$

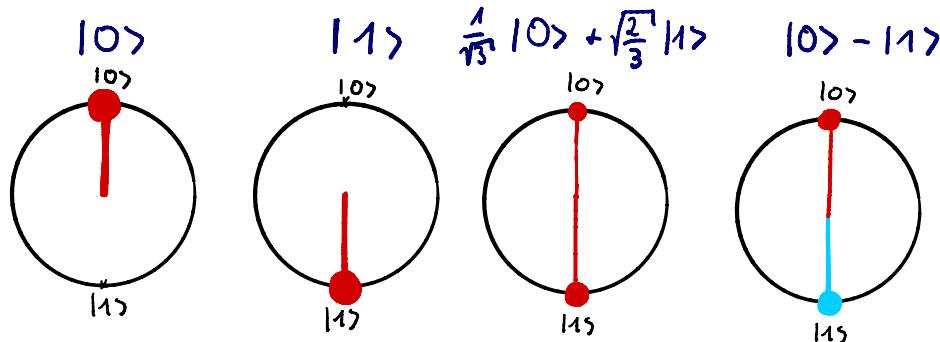
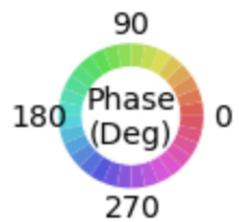
3. Bob applies → Bob's final state

$$\begin{array}{ll}
 00 & |\phi\rangle_B \\
 01 & \bar{\sigma}_x \\
 10 & \bar{\sigma}_z \\
 11 & \bar{\sigma}_z \bar{\sigma}_x
 \end{array}$$

Note, that Alice's state collapsed during the measurement, so she does not have the initial state $|\phi\rangle_s$ 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.

Q-Sphere

- Bloch sphere can only illustrate the state of 1 qubit \Rightarrow for multiple qubits: Q-sphere
- for one qubit: - the "north pole" represents state $|0\rangle$, the "south pole" state $|1\rangle$
 - the size of the blob is proportional to the prob. of measuring the respective state
 - the color indicates the relative phase compared to state $|0\rangle$



- for n qubits, there are 2^n basis states, e.g. for $n=3$ we have $000, 001, 010, 100, 011, 101, 110, 111$
 \Rightarrow we plot those basis states as equally distributed points on a sphere, with $0^{\otimes n}$ on the "north pole", $1^{\otimes n}$ on the "south pole" and all other states aligned on parallels, s.t. the number of "1"s on each latitude is constant and increasing from North to South

example: for $n=3$:

\rightarrow size & color of the blobs as before

e.g. $\frac{1}{2} \cdot (|000\rangle - |011\rangle + \sqrt{2} \cdot i \cdot |101\rangle)$

