Introduction to quantum computing

dirac notation, measurements, unitary transformations, density matrix formalism

Max (max@noppelmax.online)

August 31, 2019

Übersicht

Negative probabilities / 2-Norm[1]

- Nature ist not described by probabilities but by *amplitudes* which can be positiv, **negative** or even complex
- Could have be invented by mathematicians
- Say $(p_1 \dots p_N)$
- 1-Norm of $(p_1 \dots p_N) = \sum_{i=0}^{N} p_i = 1$
- 2-Norm/Euclidean Norm is $\sum_{i=0}^{N} p_i^2 = 1$

Qubits

- A quantumbit is 1 and 0 at the same time.
- By measuring it, the superposition collapses and the qubit is one of the measurementbases.
- In quantum theory is it common to write states with parenthesis like $|\cdot\rangle$.
- This notation is called *Bra-Ket Notation* or *Dirac-Notation*[1]

[1] Physiciest Paul Dirac (1902 - 1984), Nobelprice together with Schroedinger 1933

Qubits in Dirac-Notation

Qubit

A Quantumbit or *Qubit* is in state

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

Where α and β are *Amplitudes* and $\alpha, \beta \in \mathbb{C}$ with

$$|\alpha|^2 + |\beta|^2 = 1$$

Reminder: complex numbers

- Length $|a|$ of a complex vector a is $\sqrt{\overline{a}a}$
- where $\overline{a}$ is the complex conjugate of a: $a + ib \rightarrow a - ib$

Examples for Qubits

- A qubit could be $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$
- or like the *classical* bit $0 \cdot |0\rangle + 1 \cdot |1\rangle = |1\rangle$

Interpretation as vector space

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2 = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix} = \alpha\cdot|0\rangle + \beta\cdot|1\rangle$$

- Basis of the vector space is $\{|0\rangle, |1\rangle\}$ so the superposition is getting a linearcombination of the basiselements.
- Valid vectors must fulfill $|\alpha|^2 + |\beta|^2 = 1$

Quantum registers

$$
\begin{aligned}
R &= |x_1\rangle\,|x_2\rangle \\
&= |x_1 x_2\rangle \\
&= (\beta_0\,|0\rangle + \beta_1\,|1\rangle) \cdot (\gamma_0\,|0\rangle + \gamma_1\,|1\rangle) \\
&= \beta_0\gamma_0\,|00\rangle + \beta_0\gamma_1\,|01 + \beta_1\gamma_0\,|10\rangle + \beta_1\gamma_1\,|11\rangle\rangle \\
&= \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle
\end{aligned}
$$

- aus $|\beta_0|^2 + |\beta_1|^2 = 1$ und $|\gamma_0|^2 + |\gamma_1|^2 = 1)$ folgt[2] $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$

Quantum registers

- States of a quantum register with n bits are vectors in a 2^n dimensional complex vector space
- Example for 2 bit:

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix},$$

Übersicht

Bra-Ket notation (Dirac)[3][4]

- Kets like $|0\rangle$ denote column vectors and are typically used to describe quantum states.
- $\{|0\rangle, |1\rangle\}$ represent $\{(1,0)^T, (0,1)^T\}$
- Bra, $\langle x|$ denotes the conjugate transpose of $|x\rangle$.
- Combining $\langle x|$ and $|y\rangle$ as in $\langle x||y\rangle$, also written as $\langle x|y\rangle$, denotes the **inner product** of two vectors.
- The notation $|x\rangle\langle y|$ is the **outer product** of $|x\rangle$ and $\langle y|$.

Reminder: Dot product, scalar product

$$\langle \vec{a}, \vec{b} \rangle = \vec{a} \cdot \vec{b} = \vec{b}^T \vec{a} = (a_0, a_1) \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = \sum_{i=0}^{n} a_i b_i$$

- Inner product for Euclidian spaces

Examples

- Since $|0\rangle$ is a unit vector $\langle 0|0\rangle = 1$
- Since $|0\rangle$ and $|1\rangle$ are orthogonal we have $\langle 0|1\rangle = 0$

Outer product/Tensorproduct

$$\vec{u} \otimes \vec{v} = \vec{u}\vec{v}^T = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} \begin{pmatrix} v_1 & v_2 & v_3 \end{pmatrix} = \begin{pmatrix} u_1 v_1 & u_1 v_2 & u_1 v_3 \\ u_2 v_1 & u_2 v_2 & u_2 v_3 \\ u_3 v_1 & u_3 v_2 & u_3 v_3 \\ u_4 v_1 & u_4 v_2 & u_4 v_3 \end{pmatrix}$$

- Combining a m-dimensional vector with a n-dimensional vector results in a $m \times n$-matrix
- $|0\rangle \langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (0, 1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

Übersicht

Two types of operations

- measurement
- quantum state transformation

Measuring

If we measure a qubit in state $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ the superposition is collapses (in another superposition). After measurement the qubit is with probability $|\alpha|^2$ in state $|0\rangle$ and with probability $|\beta|^2$ in state $|1\rangle$.

Übersicht

Conjugate transpose

$$A = (a_{ji}) \in \mathbb{C}^{m \times n}$$

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

$$A^* = A^\dagger = \overline{A}^T = \overline{A^T} = \begin{pmatrix} \overline{a}_{11} & \dots & \overline{a}_{m1} \\ \vdots & \ddots & \vdots \\ \overline{a}_{1n} & \dots & \overline{a}_{mn} \end{pmatrix} \in \mathbb{C}^{n \times m}$$

Unitary transformations

- M^* or $M^\dagger$ denotes the conjugate transpose / Hermitian transpose of the matrix M

Unitary operator

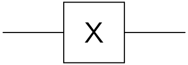
Matrix M is unitary if $MM^* = M^*M = I$

- Unitary transformations are rotations or mirrorings in complex vector space
- Unitary transformations are reversible
- Unitary transformations are length-preserving $||U\,|x\rangle\,|| = ||\,|x\rangle\,||$
- For finite dimensional vector spaces $M^*M = 1$ implies $MM^* = 1$

Übersicht

Single qubit quantum state transformations / Pauli-gates

$$
\begin{aligned}
I: \quad & |0\rangle \to |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
& |1\rangle \to |1\rangle & \\
\text{Pauli-X, Bitflip}: \quad & |0\rangle \to |1\rangle & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
& |1\rangle \to |0\rangle & \\
\text{Pauli-Y}: \quad & |0\rangle \to -|1\rangle & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
& |1\rangle \to |0\rangle & \\
\text{Pauli-Z, Phaseflip}: \quad & |0\rangle \to |0\rangle & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
& |1\rangle \to -|1\rangle &
\end{aligned}
$$



Hadamard[2] Transformation

Hadamard matrix

Matrix

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

is unitary and is called Hadamard Matrix

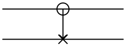
$$\begin{aligned} H: \quad |0\rangle &\to \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\to \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

[2] Mathematicians Jacques Hadamard (1865-1963)

controlled-NOT gate (C_{not})[5]

$$C_{not}: \quad \begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- C_{not} is unitary since $C_{not}^* = C_{not}$ and $C_{not}^* C_{not} = I$
- C_{not} cannot be decomposed into a tensorproduct of two single-bit transformations



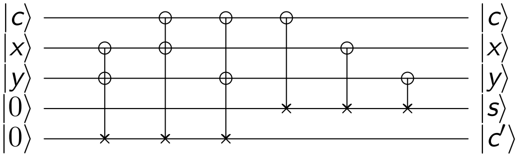
- Three bit controlled-controlled-NOT gate (Toffoli gate)[3][4]
  $T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{not}$
- Swap operation
  $S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$
- Controlled swap (Fredkin gate)
  $F = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S$

[3] Shi[6] had shown that the Hadamard and Toffoli gate already constitute a *universal set of quantum gates*.[1, p134]

[4] Can be used to construct AND and NOT operators, 1-bit full adder

Übersicht

1-bit full adder



with $|x\rangle$ and $|y\rangle$ being the databits, $|s\rangle$ being the sum, $|c'\rangle$ being the outcoming carrybit and $|c\rangle$ being the incoming carrybit.

The Toffoli-gate is sufficient to construct arbitrary combinatorial circuit.

Übersicht

Deutsch-Jozsa Problem

Give a function $f\colon \{0,1\} \to \{0,1\}$, say if f is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$). Running f is expensive.

Classical solution

Deutsch-Jozsa Problem

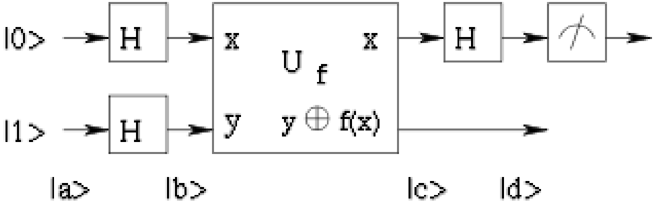
Give a function $f\colon \{0,1\} \to \{0,1\}$, say if f is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$). Running f is expensive.

Running f two times and compare the results.

Solution with quantum computing

Deutsch-Jozsa Problem

Give a function $f\colon \{0,1\} \to \{0,1\}$, say if f is constant ($f(0) = f(1)$) or balanced ($f(0) \neq f(1)$). Running f is expensive.



Deutsch-algorithm, 1985

Literatur I

S. Aaronson, *Quantum Computing Since Democritus*. Cambridge University Press, 2013.

M. Homeister, *Quantum Computing verstehen*. Springer Fachmedien WiesbadenGmbH, 2018.

P. A. M. Dirac, "A new notation for quantum mechanics," vol. 35, no. 3, p. 416.

B. Zwiebach, "DIRAC's BRA AND KET NOTATION," p. 15.

E. G. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists,"

Literatur II

Y. Shi, “Both toffoli and controlled-not need little help to do universal quantum computation,”