# Basic elements of quantum computing

Nuclear TALENT course on quantum computing

Monday June 23, 2025

# Overview of Monday June 23 and plans for the second week

1. Simple Hamiltonian matrices, one and two-qubit examples
2. Introducing the Variational Quantum Eigensolver algorithm
3. Parametrized quantum circuits
4. Introducing the Lipkin model (nuclear structure classic)
5. Tuesday to Friday we plan to discuss more realistic nuclear physics Hamiltonians, the Jordan-Wigner transformation, time evolution, Quantum Fourier transforms, Quantum Phase estimation, quantum state preparation, quantum error propagation and more

# Hamiltonians, one-qubit example

As an initial test, we consider a simply $2 \times 2$ real Hamiltonian consistend of a diagonal part $H_0$ and off-diagonal part $H_I$, playing the roles of a non-interactive one-body and interactive two-body part respectively. Defined through their matrix elements, we express them in the Pauli basis $|0\rangle$ and $|1\rangle$

$$H = H_0 + H_I$$

$$H_0 = \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix}, \qquad H_I = \lambda \begin{bmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{bmatrix}$$

Where $\lambda \in [0, 1]$ is a coupling constant parameterizing the strength of the interaction.

# Rewriting in terms of Pauli matrices

Defining

$$E_+ = \frac{E_1 + E_2}{2}, \qquad E_- = \frac{E_1 - E_2}{2}$$

we see that by combining the identity and $Z$ Pauli matrix, this can be expressed as

$$H_0 = E_+ I + E_- Z$$

For $H_1$ we use the same trick to fill the diagonal, defining $V_+ = (V_{11} + V_{22})/2, V_- = (V_{11} - V_{22})/2$. From the hermiticity requirements of $H$, we note that $V_{12} = V_{21} \equiv V_o$, which simplifies the problem to a simple $X$. This gives

$$H_I = V_+ I + V_- Z + V_o X$$

# Measurement basis

For this system we note that the Pauli $X$ matrix can be rewritten in terms of the Hadamard matrices and the Pauli $Z$ matrix (exercises from Monday-Tuesday of week 1), that is

$$X = HZH.$$

# Second Hamiltonian matrix problems, two-qubit case

The second case is defined as a $4 \times 4$ real Hamiltonian. This can be viewed as two composite systems where each system is represented by a two-level system. In the product basis $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ (our computational basis) we define the one-body part as

$$H_0|ij\rangle = \epsilon_{ij}|ij\rangle,$$

with a two-body interaction defined as

$$\begin{aligned} H_I &= H_x X \otimes X + H_z Z \otimes Z \\ &= \begin{bmatrix} H_z & 0 & 0 & H_z \\ 0 & -H_z & H_x & 0 \\ 0 & H_x & -H_z & 0 \\ H_x & 0 & 0 & H_z \end{bmatrix}. \end{aligned}$$

Here $H_x$ and $H_z$ are coupling constants.

# Rewriting

For the $4 \times 4$ case, the interacting part of the Hamiltonian is already written in terms of Pauli matrices. On the other hand, we need to rewrite the diagonal term. We define

$$\epsilon_{\pm 0} = \frac{\epsilon_{00} \pm \epsilon_{01}}{2}, \qquad \epsilon_{\pm 1} = \frac{\epsilon_{10} \pm \epsilon_{11}}{2}.$$

We note that the energies $\epsilon_{00}$ and $\epsilon_{01}$ can be repeated on the diagonal. This is also the case for $\epsilon_{10}$ and $\epsilon_{11}$

$$D_0 = \epsilon_{+0} I \otimes I + \epsilon_{-0} I \otimes Z,$$
$$D_1 = \epsilon_{+0} I \otimes I + \epsilon_{-1} I \otimes Z.$$

# Further manipulations

Using the Pauli $Z$ matrix and the identity matrix $I$ we define

$$P_{\pm} = \frac{1}{2}(I \pm Z),$$

which we use to project out the first and last to two elements the of $4 \times 4$ matrix

$$P_0 = P_+ \otimes I, \qquad P_0 = P_- \otimes I.$$

Adding $D_0$ and $D_1$, we get

$$H_0 = P_0 D_0 + P_1 D_1 = \alpha_+ I \otimes I + \alpha_- Z \otimes I + \beta_+ I \otimes Z + \beta_- Z \otimes Z,$$

where we have defined

$$\alpha_{\pm} = \frac{\epsilon_{+0} \pm \epsilon_{+1}}{2}, \quad \beta_{\pm} = \frac{\epsilon_{-0} \pm \epsilon_{+1}}{2}$$

# The Lipkin model, more details below

For the Lipkin model, we recommend strongly the work of LaRose and collaborators, see https://journals.aps.org/prc/abstract/10.1103/PhysRevC.106.024319, see in particular section 3.
For codes, feel free to be inspired and/or reuse the codes at https://github.com/CompPhysics/QuantumComputingMachineLearning/tree/gh-pages/doc/Programs/LipkinModel.

# States, gates and measurements, reminder from last week

Mathematically, quantum gates are a series of unitary operators in the operator space defined by our Hamiltonian $\mathcal{H}$ and operators $\mathcal{O}$ which evolve a given initial state. The unitary nature preserves the norm of the state vector, ensuring the probabilities sum to unity. Since not all gates correspond to an observable, they are not all necessarily hermitian.

# Single qubit gates

The Pauli matrices (and gate operations following therefrom) are defined as

$$\boldsymbol{X} \equiv \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \boldsymbol{Y} \equiv \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \boldsymbol{Z} \equiv \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

# Pauli-X gate

The Pauli-$\boldsymbol{X}$ gate is also known as the **NOT** gate, which flips the state of the qubit.

$$\boldsymbol{X}|0\rangle = |1\rangle,$$
$$\boldsymbol{X}|1\rangle = |0\rangle.$$

The Pauli-$\boldsymbol{Y}$ gate flips the bit and multiplies the phase by $i$.

$$\boldsymbol{Y}|0\rangle = i|1\rangle,$$
$$\boldsymbol{Y}|1\rangle = -i|0\rangle.$$

The Pauli-$\boldsymbol{Z}$ gate multiplies only the phase of $|1\rangle$ by $-1$.

$$\boldsymbol{Z}|0\rangle = |0\rangle,$$
$$\boldsymbol{Z}|1\rangle = -|1\rangle.$$

# Hadamard gate

The Hadamard gate is defined as

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

It creates a superposition of the $|0\rangle$ and $|1\rangle$ states.

$$\boldsymbol{H}|0\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + |1\rangle \right), \tag{1}$$

$$\boldsymbol{H}|1\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle - |1\rangle \right). \tag{2}$$

Note that we will use $H$ as symbol for the Hadamard gate while we will reserve the notation $\mathcal{H}$ for a given Hamiltonian.

# Phase Gates

The phase gate is usually denoted as $S$ and is defined as

$$\boldsymbol{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

It multiplies only the phase of the $|1\rangle$ state by $i$.

$$\boldsymbol{S}|0\rangle = |0\rangle,$$
$$\boldsymbol{S}|1\rangle = i|1\rangle.$$

# The inverse of the $S$-gate

The inverse

$$S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$$

is known as the $S^\dagger$ gate which applies an $i$ phase shift to $|1\rangle$.

$$S^\dagger|0\rangle = |0\rangle,$$
$$S^\dagger|1\rangle = -i|1\rangle.$$

# Two-qubit gates

The CNOT gate is a two-qubit gate which acts on two qubits, a control qubit and a target qubit. The CNOT gate is defined as

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

It is often used to perform linear entanglement on qubits.

$$\begin{aligned} \text{CNOT}|00\rangle &= |00\rangle, \\ \text{CNOT}|01\rangle &= |01\rangle, \\ \text{CNOT}|10\rangle &= |11\rangle, \\ \text{CNOT}|11\rangle &= |10\rangle. \end{aligned}$$

# The SWAP gate

The SWAP gate is a two-qubit gate which swaps the state of two qubits. It is defined as

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$$\begin{aligned} \mathrm{SWAP}|00\rangle &= |00\rangle, \\ \mathrm{SWAP}|01\rangle &= |10\rangle, \\ \mathrm{SWAP}|10\rangle &= |01\rangle, \\ \mathrm{SWAP}|11\rangle &= |11\rangle. \end{aligned}$$

# Pauli Strings

A Pauli string, such as $\boldsymbol{XIYZ}$ is a tensor product of Pauli matrices acting on different qubits. The Pauli string $\boldsymbol{XIYZ}$ is defined as (from qubit one to qubit four, from left to right)

$$\boldsymbol{XIYZ} \equiv \boldsymbol{X}_0 \otimes \boldsymbol{I}_1 \otimes \boldsymbol{Y}_2 \otimes \boldsymbol{Z}_3.$$

Hamiltonians are often rewritten or decomposed in terms of Pauli string as they can be easily implemented on quantum computers.

# Variational Quantum Eigensolver

An important algorithm to estimate the eigenenergies of a quantum Hamiltonian is quantum phase estimation. In it, one encodes the eigenenergies, one binary bit at a time (up to $n$ bits), into the complex phases of the quantum states of the Hilbert space for $n$ qubits. It does this by applying powers of controlled unitary evolution operators to a quantum state that can be expanded in terms of the Hamiltonian's eigenvectors of interest. The eigenenergies are encoded into the complex phases in such a way that taking the inverse quantum Fourier transformation (see Hundt sections 6.1-6.2) of the states into which the eigen-energies are encoded results in a measurement probability distribution that has peaks around the bit strings that represent a binary fraction which corresponds to the eigen-energies of the quantum state acted upon by the controlled unitary operators. We will discuss the QPE on Wednesday this week.

# The VQE

While quantum phase estimation (QPE) is provably efficient, non-hybrid, and non-variational, the number of qubits and length of circuits required is too great for our NISQ era quantum computers. Thus, QPE is only efficiently applicable to large, fault-tolerant quantum computers that likely won't exist in the near, but the far future.

Therefore, a different algorithm for finding the eigen-energies of a quantum Hamiltonian was put forth in 2014 called the variational quantum eigensolver, commonly referred to as VQE. The algorithm is hybrid, meaning that it requires the use of both a quantum computer and a classical computer. It is also variational, meaning that it relies, ultimately, on solving an optimization problem by varying parameters and thus is not as deterministic as QPE. The variational quantum eigensolver is based on the variational principle:

# Rayleigh-Ritz variational principle

Our starting point is the Rayleigh-Ritz variational principle states that for a given Hamiltonian $H$, the expectation value of a trial state or just ansatz $|\psi\rangle$ puts a lower bound on the ground state energy $E_0$.

$$\frac{\langle\psi|\mathcal{H}|\psi\rangle}{\langle\psi|\psi\rangle} \geq E_0.$$

# The ansatz

The ansatz is typically chosen to be a parameterized superposition of basis states that can be varied to improve the energy estimate, $|\psi\rangle \equiv |\psi(\boldsymbol{\theta})\rangle$ where $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_M)$ are the $M$ optimization parameters.

# Expectation value of Hamiltonian and the variational principle

The expectation value of a Hamiltonian $\mathcal{H}$ in a state $|\psi(\theta)\rangle$ parameterized by a set of angles $\theta$, is always greater than or equal to the minimum eigen-energy $E_0$. To see this, let $|n\rangle$ be the eigenstates of $\mathcal{H}$, that is

$$\mathcal{H}|n\rangle = E_n|n\rangle.$$

# Expanding in the eigenstates

We can then expand our state $|\psi(\theta)\rangle$ in terms of the eigenstates

$$|\psi(\theta)\rangle = \sum_n c_n |n\rangle,$$

and insert this in the expression for the expectation value (note that we drop the denominator in the Rayleigh-Ritz ratio)

$$\langle\psi(\theta)|\mathcal{H}|\psi(\theta)\rangle = \sum_{nm} c_m^* c_n \langle m|\mathcal{H}|n\rangle = \sum_{nm} c_m^* c_n E_n \langle m|n\rangle = \sum_{nm} \delta_{nm} c_m^* c_n E_n$$

which implies that we can minimize over the set of angles $\theta$ and arrive at the ground state energy $E_0$

$$\min_\theta \langle\psi(\theta)|\mathcal{H}|\psi(\theta)\rangle = E_0.$$

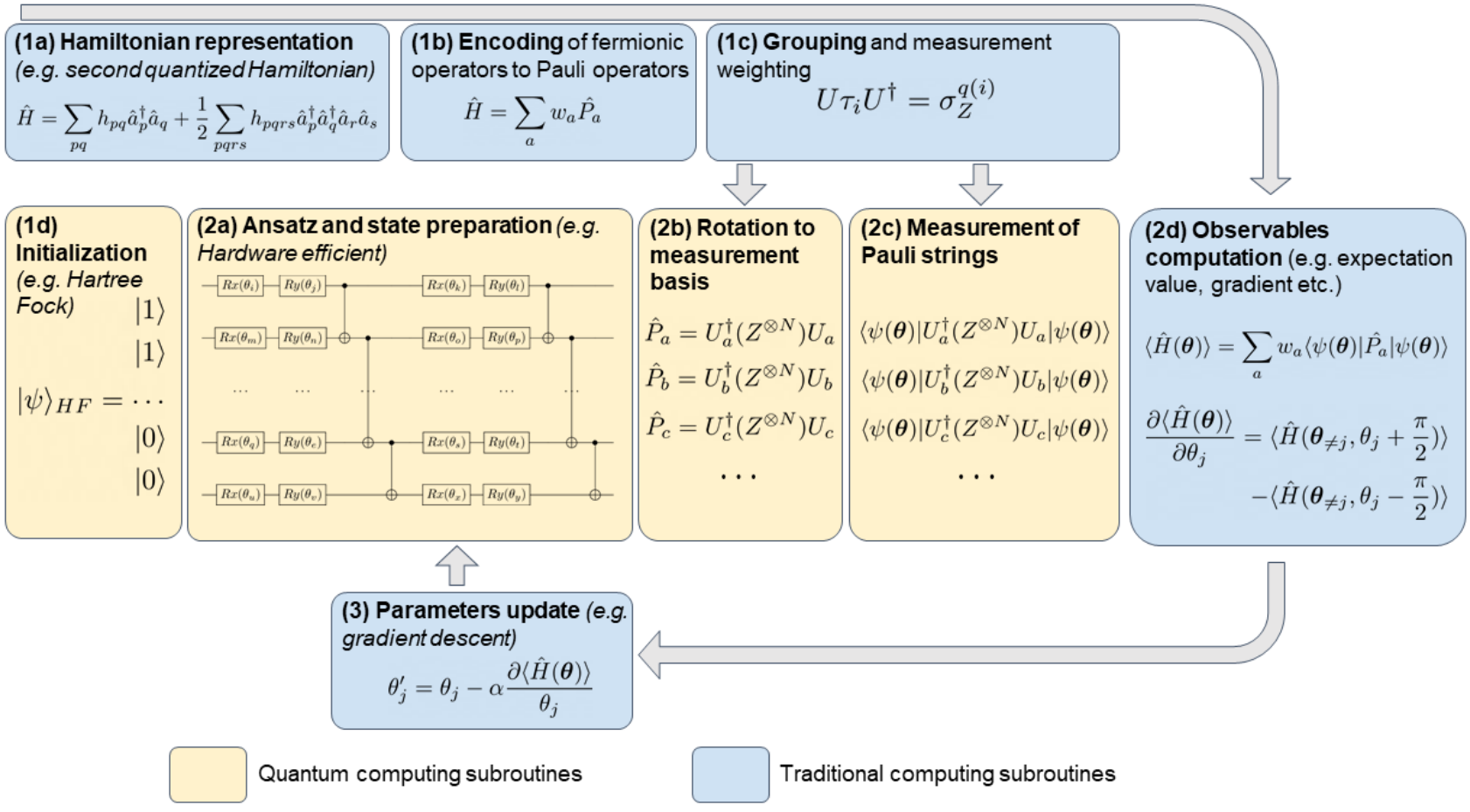
# Basic steps of the VQE algorithm

Using this fact, the VQE algorithm can be broken down into the following steps

1. Prepare the variational state $|\psi(\theta)\rangle$ on a quantum computer.
2. Measure this circuit in various bases and send these measurements to a classical computer
3. The classical computer post-processes the measurement data to compute the expectation value $\langle\psi(\theta)|\mathcal{H}|\psi(\theta)\rangle$
4. The classical computer varies the parameters $\theta$ according to a classical minimization algorithm and sends them back to the quantum computer which runs step 1 again.

This loop continues until the classical optimization algorithm terminates which results in a set of angles $\theta_{\text{min}}$ that characterize the ground state $|\phi(\theta_{\text{min}})\rangle$ and an estimate for the ground state energy $\langle\psi(\theta_{\text{min}})|\mathcal{H}|\psi(\theta_{\text{min}})\rangle$.

# VQE overview



# Rotations

To have any flexibility in the ansatz $|\psi\rangle$, we need to allow for a given parametrization. The most common approach is to employ the so-called rotation operations given by $R_x$, $R_z$ and $R_y$, where we apply chained operations of rotating around the various axes by $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_Q)$ of the Bloch sphere and CNOT operations. Applications of say the $y$-rotation specifically ensures that our coefficients always remain real, which often is satisfactory when dealing with many-body systems.

# Measurements and more

After the ansatz has been constructed, the Hamiltonian must be applied. The Hamiltonian must be written in terms of Pauli strings in order to perform measurements properly.
To obtain the expectation value of the ground state energy, one can measure the expectation value of each Pauli string,

$$E(\boldsymbol{\theta}) = \sum_i w_i \langle \psi(\boldsymbol{\theta}) | P_i | \psi(\boldsymbol{\theta}) \rangle \equiv \sum_i w_i f_i,$$

where $f_i$ is the expectation value of the Pauli string $i$.

# Collecting data

This is estimated statistically by considering measurements in the appropriate basis of the operator in the Pauli string.
With $N_0$ and $N_1$ as the number of 0 and 1 measurements respectively, we can estimate $f_i$ since

$$f_i = \lim_{N \to \infty} \frac{N_0 - N_1}{N},$$

where $N$ as the number of shots (measurements).
Each Pauli string requires its own circuit, where multiple measurements of each string is required. Adding the results together with the corresponding weights, the ground state energy can be estimated. To optimize with respect to $\boldsymbol{\theta}$, a classical optimizer is often applied.

# Ansatzes

Every possible qubit wavefunction $|\psi\rangle$ can be presented as a vector:

$$|\psi\rangle = \begin{bmatrix} \cos(\theta/2) \\ e^{i\varphi} \cdot \sin(\theta/2) \end{bmatrix},$$

where the numbers $\theta$ and $\varphi$ define a point on the unit three-dimensional sphere, the so-called Bloch sphere.
For a random one qubit Hamiltonian, a *good* quantum state preparation circuit should be able to generate all possible states on the Bloch sphere.

# Preparing the states

Before quantum state preparation, our qubit is in the $|0\rangle$ state. This corresponds to the vertical position of the vector in the Bloch sphere. In order to generate any possible $|\psi\rangle$ we will apply $R_x(t_1)$ and $R_y(t_2)$ gates on the $|0\rangle$ initial state

$$R_y(\phi)R_x(\theta)\,|0\rangle = |\psi\rangle\,.$$

The rotation $R_x(\theta)$ corresponds to the rotation in the Bloch sphere around the $x$-axis and $R_y(\phi)$ the rotation around the $y$-axis.

# Rotations used

These two gates with there parameters ($\theta$ and $\phi$) will generate for us the trial (ansatz) wavefunctions. The two parameters will be in control of the Classical Computer and its optimization model.

# Implementing using qiskit

```
import numpy as np
from random import random
from qiskit import *
def quantum_state_preparation(circuit, parameters):
    q = circuit.qregs[0] # q is the quantum register where the info ab
    circuit.rx(parameters[0], q[0]) # q[0] is our one and only qubit X
    circuit.ry(parameters[1], q[0])
    return circuit
```

# Expectation values

To execute the second step of VQE, we need to understand how expectation values of operators can be estimated via quantum computers by post-processing measurements of quantum circuits in different basis sets. To rotate bases, one uses the basis rotator $R_\sigma$ which is defined for each Pauli gate $\sigma$ to be (using the Hadamard rotation $H$ and Phase rotation $S$) for a Pauli-$\boldsymbol{X}$ matrix

$$\boldsymbol{X} = \boldsymbol{R}_\sigma \boldsymbol{Z} \boldsymbol{R}_\sigma = \boldsymbol{H}\boldsymbol{Z}\boldsymbol{H}$$

for a Pauli-$\boldsymbol{Y}$ matrix

$$\boldsymbol{Y} = \boldsymbol{R}_\sigma \boldsymbol{Z} \boldsymbol{R}_\sigma = \boldsymbol{H}\boldsymbol{S}^\dagger \boldsymbol{Z}\boldsymbol{H}\boldsymbol{S},$$

and

$$\boldsymbol{Z} = \boldsymbol{R}_\sigma \boldsymbol{Z} \boldsymbol{R}_\sigma = \boldsymbol{I}\boldsymbol{Z}\boldsymbol{I} = \boldsymbol{Z}.$$

# Measurements of eigenvalues of the Pauli operators

We can show that these rotations allow us to measure the eigenvalues of the Pauli operators. The eigenvectors of the Pauli $\boldsymbol{X}$ gate are

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}},$$

with eigenvalues $\pm 1$. Acting on the eigenstates with the rotation gives

$$\boldsymbol{H}|+\rangle = +1|0\rangle,$$

and

$$\boldsymbol{H}|-\rangle = -1|1\rangle.$$

# Single-qubit states

Any single-qubit state can be written as a linear combination of these eigenvectors,

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle.$$

We then have the following expectation value for the Pauli $\boldsymbol{X}$ operator

$$\langle|X|\rangle = \langle\psi|X|\psi\rangle = |\alpha|^2 - |\beta|^2.$$

However, we can only measure the qubits in the computational basis. Applying the rotation to our state gives

$$H|\psi\rangle = \alpha|0\rangle - \beta|1\rangle.$$

# Measurements and computational basis

We have seen how to rewrite the above sinple $2 \times 2$ eiegenvalue problem in terms of a Hamiltonian defined by Pauli $\boldsymbol{X}$ and $\boldsymbol{Z}$ matrices, and the identity matrix $\boldsymbol{I}$. Let us make this Hamiltonian that involves only one qubit somewhat more general

$$\langle\psi|\,\mathcal{H}\,|\psi\rangle = a\cdot\langle\psi|\,\boldsymbol{I}\,|\psi\rangle + b\cdot\langle\psi|\,\boldsymbol{Z}\,|\psi\rangle + c\cdot\langle\psi|\,\boldsymbol{X}\,|\psi\rangle + d\cdot\langle\psi|\,\boldsymbol{Y}\,|\psi\rangle\,.$$

# Expectation value of $\boldsymbol{I}$

For the $\boldsymbol{I}$ operator the expectation value is always unity:

$$\langle\psi|\,\boldsymbol{I}\,|\psi\rangle = 1.$$

Its contribution to the overall expectaction value is thus given by the constant $a$.

# The Pauli matrices

For the rest of the Pauli operators, we make the following remark: every one qubit quantum state $|\psi\rangle$ can be represented via different sets of basis vectors:

$$|\psi\rangle = c_1^z \cdot |0\rangle + c_2^z \cdot |1\rangle = c_1^x \cdot |+\rangle + c_2^x \cdot |-\rangle = c_1^y \cdot |+i\rangle + c_2^y \cdot |-i\rangle \,.$$

# In more detail

We have

$$\text{Z-eigenvectors} \qquad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

# For the other two matrices

X-eigenvectors $\quad |+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix},$

Y-eigenvectors $\quad |+i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, \qquad |-i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}.$

# Analyzing these equations

The first presented eigenvectors for each Pauli operator have eigenvalues equal to $+1$: $Z|0\rangle = +1|0\rangle$, $X|+\rangle = +1|+\rangle$, $Y|+i\rangle = +1|+i\rangle$, respectively.
The second eigenvectors for each Pauli operator have eigenvalues equal to $-1$: $Z|1\rangle = -1|1\rangle$, $X|-\rangle = -1|-\rangle$, $Y|-i\rangle = -1|-i\rangle$, respectively

# Explicit eigenvalues

Now, let us calculate the expectation values of these Pauli operators:

$$\langle\psi|\,\boldsymbol{Z}\,|\psi\rangle = \left(c_1^{z*}\cdot\langle 0| + c_2^{z*}\cdot\langle 1|\right) Z\left(c_1^{z}\cdot|0\rangle + c_2^{z}\cdot|1\rangle\right) = |c_1^z|^2 - |c_2^z|^2,$$

$$\langle\psi|\,\boldsymbol{X}\,|\psi\rangle = \left(c_1^{x*}\cdot\langle +| + c_2^{x*}\cdot\langle -|\right) X\left(c_1^{x}\cdot|+\rangle + c_2^{x}\cdot|-\rangle\right) = |c_1^x|^2 - |c_2^x|^2,$$

$$\langle\psi|\,\boldsymbol{Y}\,|\psi\rangle = \left(c_1^{y*}\cdot\langle +i| + c_2^{y*}\cdot\langle -i|\right) Y\left(c_1^{y}\cdot|+i\rangle + c_2^{y}\cdot|-i\rangle\right) = \left|c_1^y\right|^2 - \left|\right.$$

# Computational basis

The above equations require that we can make measurements in the chosen basis sets.
However, this may not be possible. The difficulty comes from the fact that one may have the possibility to measure only in the $\boldsymbol{Z}$-basis. To solve this difficulty we still do a $\boldsymbol{Z}$-basis measurement, but, before that, we apply specific operators to the $|\psi\rangle$ state.

# Unitary transformation of $\boldsymbol{X}$

If we use the Hadamard gate

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

we can rewrite

$$\boldsymbol{X} = \boldsymbol{HZH}.$$

The Hadamard gate/matrix is a unitary matrix with the property that $\boldsymbol{H}^2 = \boldsymbol{I}$.

# Generalizing

For the one-qubit Hamiltonian we have toyed with till now, we can thus rewrite in an easy way the Hamiltonian so that we can perform measurements using our favorite computational basis.
The transformation of the Pauli-$\boldsymbol{X}$ matrix can be generalized, as we will see in more detail below for the two-qubit Hamiltonian and next week for the Lipkin model, to the following expression

$$\mathcal{P} = \boldsymbol{U}^{\dagger}\boldsymbol{M}\boldsymbol{U},$$

where $\mathcal{P}$ represents some combination of the Pauli matrices and the identity matrix, $\boldsymbol{U}$ is a unitary matrix and $\boldsymbol{M}$ represents the gate/matrix which performs the measurements, often represented by a Pauli-$\boldsymbol{Z}$ gate/matrix.

# Interpretations

This tells us that we are able to estimate $|\alpha|^2$ and $|\beta|^2$ (and hence the expectation value of the Pauli $\boldsymbol{X}$ operator) by using a rotation and measure the resulting state in the computational basis. We can show this for the Pauli $\boldsymbol{Z}$ and Pauli $\boldsymbol{Y}$ similarly.

# Reminder on rotations

Note the following identity of the basis rotator

$$\boldsymbol{R}_\sigma^\dagger \boldsymbol{Z} \boldsymbol{R}_\sigma = \boldsymbol{\sigma},$$

which follows from the fact that $\boldsymbol{HZH} = \boldsymbol{X}$ and $\boldsymbol{SXS}^\dagger = \boldsymbol{Y}$.

# Why do we measure on one qubit? First consideration

In quantum computing, measurements are typically performed on one qubit at a time due to a combination of theoretical, practical, and algorithmic considerations:

## Algorithmic Requirements:

1. Adaptive Processing: Many quantum algorithms, such as quantum teleportation or error correction, require mid-circuit measurements. The outcomes determine subsequent operations, necessitating sequential measurements to adapt the circuit dynamically.
2. Partial Information Extraction: Algorithms often need only specific qubits' results (e.g., in Shor's algorithm), making full-system measurements unnecessary.

# Why do we measure on one qubit? Second consideration

## Quantum Mechanical Principles:

1. Collapse and Entanglement: Measuring a qubit collapses its state, potentially affecting entangled qubits. Sequential measurements allow controlled extraction of information while managing entanglement.
2. Measurement Basis: Most algorithms use the computational basis (individual qubit measurements). Joint measurements in entangled bases are possible but require complex setups and are not always needed.

# Why do we measure on one qubit? Third consideration

## Practical Hardware Limitations:

1. Crosstalk and Noise: Simultaneous measurements risk disturbing neighboring qubits due to hardware imperfections, especially in noisy intermediate-scale quantum (NISQ) devices.
2. Readout Constraints: Physical implementations (e.g., superconducting qubits) may have limited readout bandwidth, forcing sequential measurements.

# Why do we measure on one qubit? Fourth consideration

## Resource Management:

1. Qubit Reuse: Ancilla qubits (e.g., in error correction) are measured, reset, and reused, requiring sequential handling to avoid disrupting computational qubits.

## Conclusion:

While joint measurements are theoretically possible, the dominant practice of measuring one qubit at a time stems from algorithmic adaptability, hardware limitations, and the need to minimize quantum state disturbance. This approach balances efficiency, practicality, and the constraints of current quantum systems.

# Arbitrary Pauli gate

With this, we see that the expectation value of an arbitrary Pauli-gate $\sigma$ in the state $|\psi\rangle$ can be expressed as a linear combination of probabilities

$$\begin{aligned} E_\psi(\sigma) &= \langle\psi|\sigma|\psi\rangle \\ &= \langle\psi|R_\sigma^\dagger Z R_\sigma|\psi\rangle = \langle\phi|Z|\phi\rangle \\ &= \langle\phi| \left( \sum_{x\in\{0,1\}} (-1)^x |x\rangle\langle x| \right) |\phi\rangle \\ &= \sum_{x\in\{0,1\}} (-1)^x |\langle x|\phi\rangle|^2 \\ &= \sum_{x\in\{0,1\}} (-1)^x P(|\phi\rangle \to |x\rangle), \end{aligned}$$

where $|\phi\rangle = |R_\sigma\phi\rangle$ and $P(|\phi\rangle \to |x\rangle$ is the probability that the state $|\phi\rangle$ collapses to the state $|x\rangle$ when measured.

# Arbitrary string of Pauli operators

This can be extended to any arbitrary Pauli string: consider the string of Pauli operators $P = \bigotimes_{p \in Q} \sigma_p$ which acts non-trivially on the set of qubits $Q$ which is a subset of the total set of $n$ qubits in the system. Then

$$
\begin{aligned}
E_\psi(P) &= \langle\psi| \left( \bigotimes_{p \in Q} \sigma_p \right) |\psi\rangle \\
&= \langle\psi| \left( \bigotimes_{p \in Q} \sigma_p \right) \left( \bigotimes_{q \notin Q} I_q \right) |\psi\rangle \\
&= \langle\psi| \left( \bigotimes_{p \in Q} R_{\sigma_p}^\dagger Z_p R_{\sigma_p} \right) \left( \bigotimes_{q \notin Q} I_q \right) |\psi\rangle \\
&= \langle\psi| \left( \bigotimes_{p \in Q} R_{\sigma_p}^\dagger \right) \left( \bigotimes_{p \in Q} Z_p \right) \left( \bigotimes_{q \notin Q} I_q \right) \left( \bigotimes_{p \in Q} R_{\sigma_p} \right) |\psi\rangle
\end{aligned}
$$

# This gives us

$$
\begin{aligned}
E_\psi(P) &= \langle\phi| \left(\bigotimes_{p\in Q} Z_p\right) \left(\bigotimes_{q\notin Q} I_q\right) |\phi\rangle \\
&= \langle\phi| \left(\bigotimes_{p\in Q} \sum_{x_p\in\{0_p,1_p\}} (-1)^{x_p} |x_p\rangle\langle x_p|\right) \left(\bigotimes_{q\notin Q} \sum_{y_q\in\{0_q,1_q\}} |y_q\rangle\langle y_q|\right) |\phi \\
&= \langle\phi| \left(\sum_{x\in\{0,1\}^n} (-1)^{\sum_{p\in Q} x_p} |x\rangle\langle x|\right) |\phi\rangle \\
&= \sum_{x\in\{0,1\}^n} (-1)^{\sum_{p\in Q} x_p} |\langle x||\phi\rangle|^2 \\
&= \sum_{x\in\{0,1\}^n} (-1)^{\sum_{p\in Q} x_p} P(|\phi\rangle \to |x\rangle),
\end{aligned}
$$

where $|\phi\rangle = |\bigotimes_{p\in Q} R_{\sigma_p}\psi\rangle$.

# Final observables

Finally, because the expectation value is linear

$$E_\psi\left(\sum_m \lambda_m P_m\right) = \sum_m \lambda_m E_\psi(P_m),$$

one can estimate any observable that can be written as a linear combination of Pauli-string terms.

# Measurement

To estimate the probability $P(|\phi\rangle \to |x\rangle)$ from the previous results, one prepares the state $|\phi\rangle$ on a quantum computer and measures it, and then repeats this process (prepare and measure) several times. The probability $P(|\phi\rangle \to |x\rangle)$ is estimated to be the number of times that one measures the bit-string $x$ divided by the total number of measurements that one makes; that is

$$P(|\phi\rangle \to |x\rangle\rangle \approx \sum_{m=1}^{M} \frac{x_m}{M},$$

where $x_m = 1$ if the result of measurement is $x$ and 0 if the result of measurement is not $x$.

# Law of large numbers aka Bernoulli's theorem

By the law of large numbers the approximation approaches equality as $M$ goes to infinity

$$P(|\phi\rangle \to |x\rangle) = \lim_{M\to\infty} \sum_{m=1}^{M} \frac{x_m}{M}.$$

As we obviously do not have infinite time nor infinite quantum computers (which could be run in parallel), we must truncate our number of measurement $M$ to a finite, but sufficiently large number. More precisely, for precision $\epsilon$, each expectation estimation subroutine within VQE requires $\mathcal{O}(1/\epsilon^2)$ samples from circuits with depth $\mathcal{O}(1)$.