THE CATHOLIC UNIVERSITY OF AMERICA

Quantum AI and Cybersecurity, An Overview

Daniel Sierra-Sosa, Ph.D.

Assistant Professor

Department of Computer Science

Quantum Machine Learning

Classical ML

Classical ML on quantum data

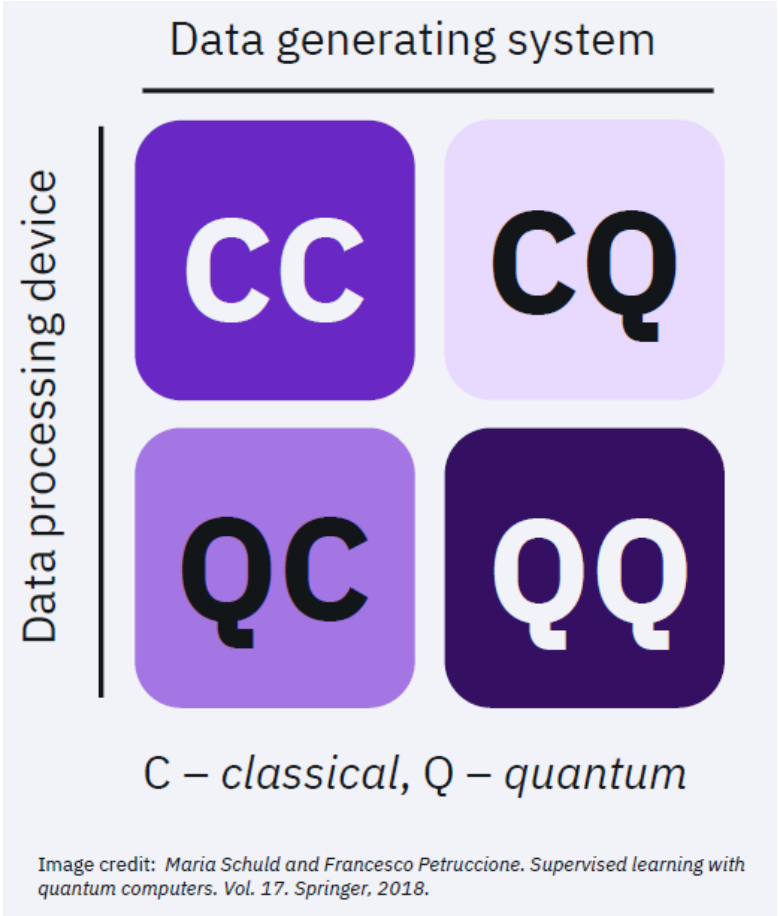


Image credit: *Maria Schuld and Francesco Petruccione. Supervised learning with quantum computers. Vol. 17. Springer, 2018.*

Quantum ML on classical data

Quantum ML on quantum data

Main Idea

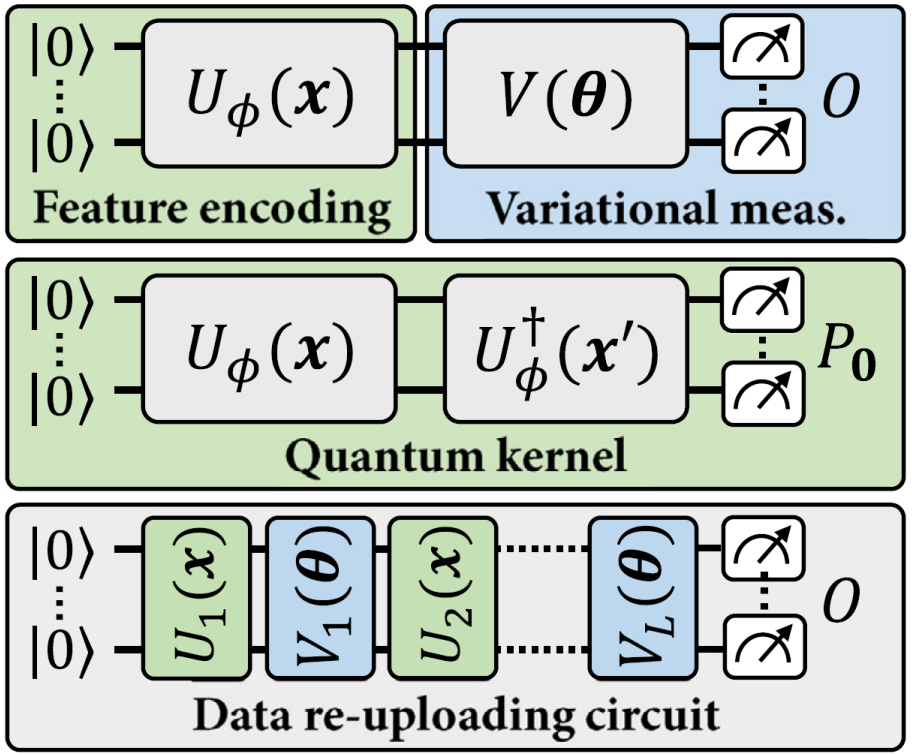
- **The Challenge:** Without assuming any particular mathematical structure in the input space, we must embed each data point into a Hilbert Space ($\mathcal{H}$)
- **The Opportunity:** The freedom to choose the embedding map allows us to design various similarity measures and machine learning algorithms.
- **The Promise:** Quantum Machine Learning (QML) aims to accelerate tasks with classical and quantum data.

WARNING!!!!

Very unlikely that QML will beat ML performance on classical data

Quantum Machine Learning Models

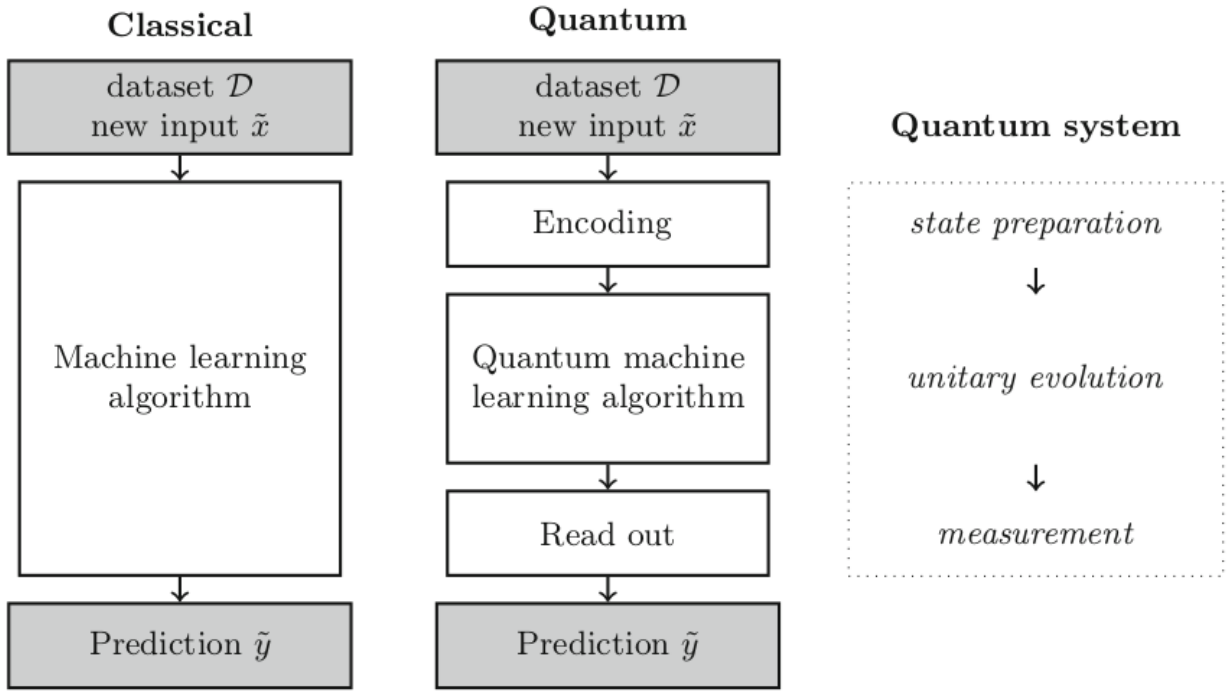
- QML models can be generalized into three main components
  - The collection and the **preparation of data** from source to *state preparation*
  - **The model** either quantum or a hybrid quantum-classical
    - A variational or parametric quantum circuit applied alone
    - A variational quantum circuit followed by a perceptron or any other layer
  - The **optimization**, activation, and loss
    - Recent work has shown that these steps performed in a classical device and benefit the quantum components



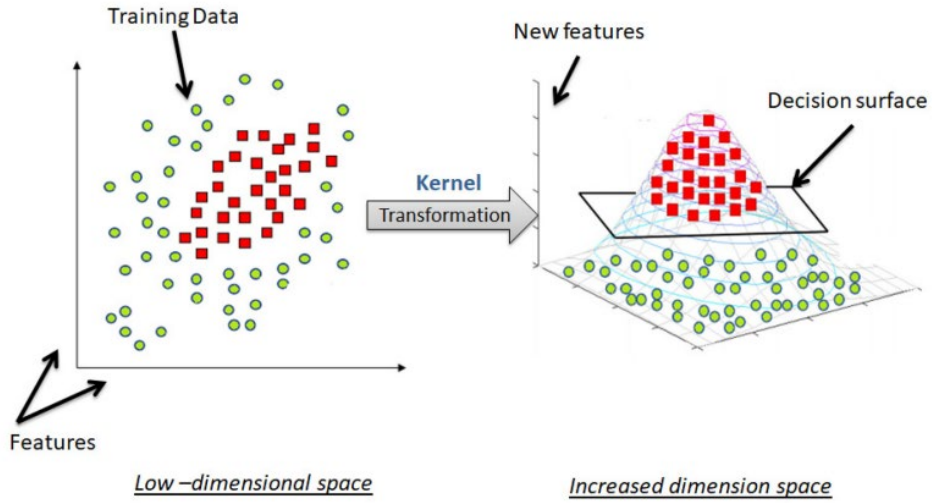
Jerbi, S., Fiderer, L. J., Poulsen Nautrup, H., Kübler, J. M., Briegel, H. J., & Dunjko, V. (2023). Quantum machine learning beyond kernel methods. *Nature Communications*, *14*(1), 517.

Quantum Embeddings

Design a procedure to transform data stored in a classical memory into a quantum state.



Taken from: Schuld, M., & Petruccione, F. (2018). Supervised learning with quantum computers (Vol. 17). Berlin: Springer.



Taken from: Tychola, K. A., Kalampokas, T., & Papakostas, G. A. (2023). Quantum Machine Learning—An Overview. Electronics, 12(11), 2379.

Quantum Embeddings

- The codification is feature-mapping from the original input space X to the quantum Hilbert space of qubits $\mathcal{H}_Q$, it changes the structure of the data in a non-trivial way, influencing the expressiveness of the models.
- The quantum feature map $\mathcal{U}: X \rightarrow \mathcal{H}_Q$, with a parameter dependence θ:

$$|0\rangle^{\otimes n} \rightarrow \mathcal{U}_\theta(x)|0\rangle^{\otimes n}$$

  where we can optimize the parameters of $\mathcal{U}_\theta$ to make the classes separable.
- There are ways to optimize and evaluate this mapping

Encoding

basis encoding of binary string $(1, 0)$, i.e. representing integer 2

Hamiltonian encoding of a matrix A

$$|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$$

$$U = e^{-iH_A t}$$

amplitude encoding of unit-length complex vector $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)$

time-evolution encoding of a scalar t

Source: Schuld, M., & Petruccione, F. (2021). Machine learning with quantum computers. Springer.

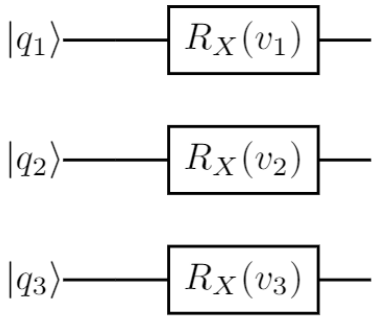
Encoding

Basis Encoding

$$|D\rangle = \frac{1}{\sqrt{2}}|0011\rangle + \frac{1}{\sqrt{2}}|1011\rangle$$

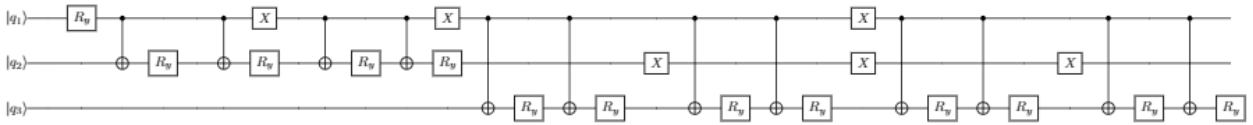
$$\alpha = \left(0,0,0,\frac{1}{\sqrt{2}},0,0,0,0,0,0,0,\frac{1}{\sqrt{2}},0,0,0,0\right)$$

Angle Encoding

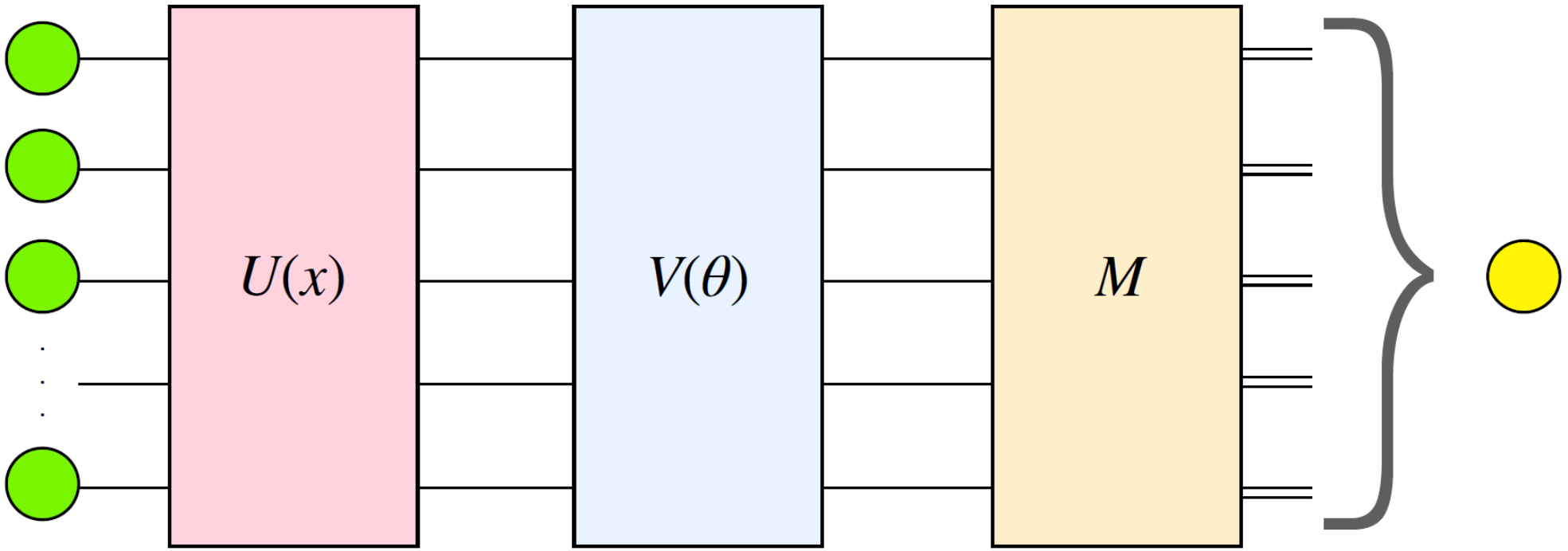


Amplitude Encoding

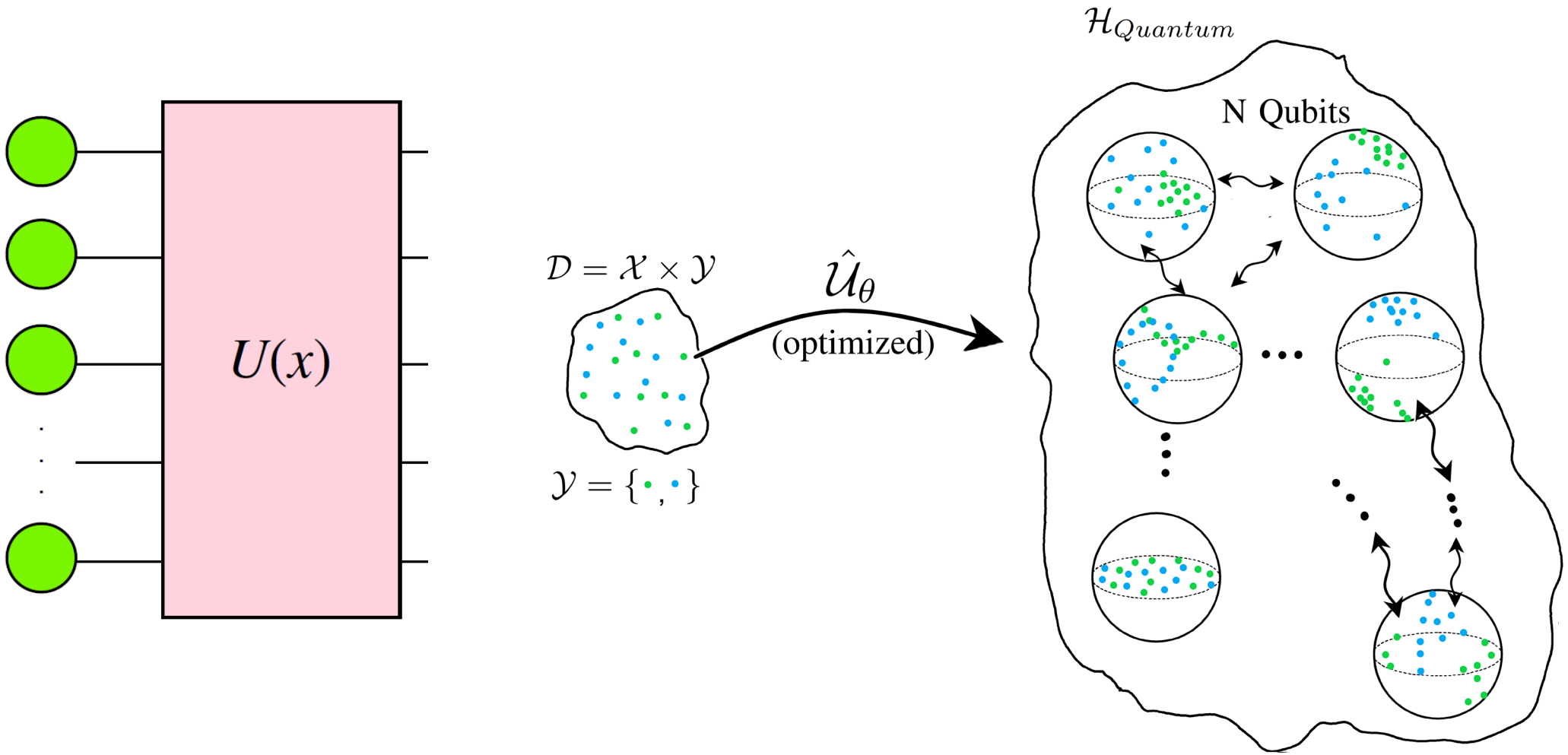
$$|\psi\rangle = R(v^i, \beta)|q_1 \dots q_{s-1}\rangle|q_s\rangle$$



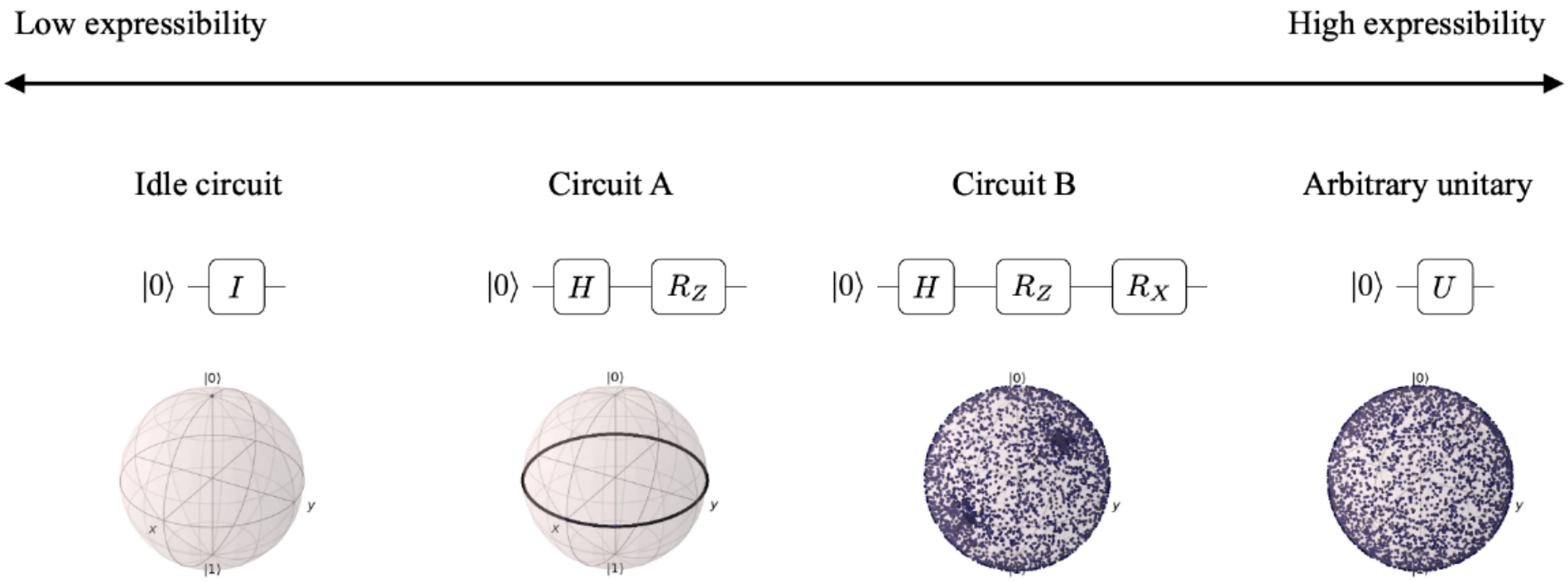
Parameterized Quantum Circuits



Parameterized Quantum Circuits



Expressibility



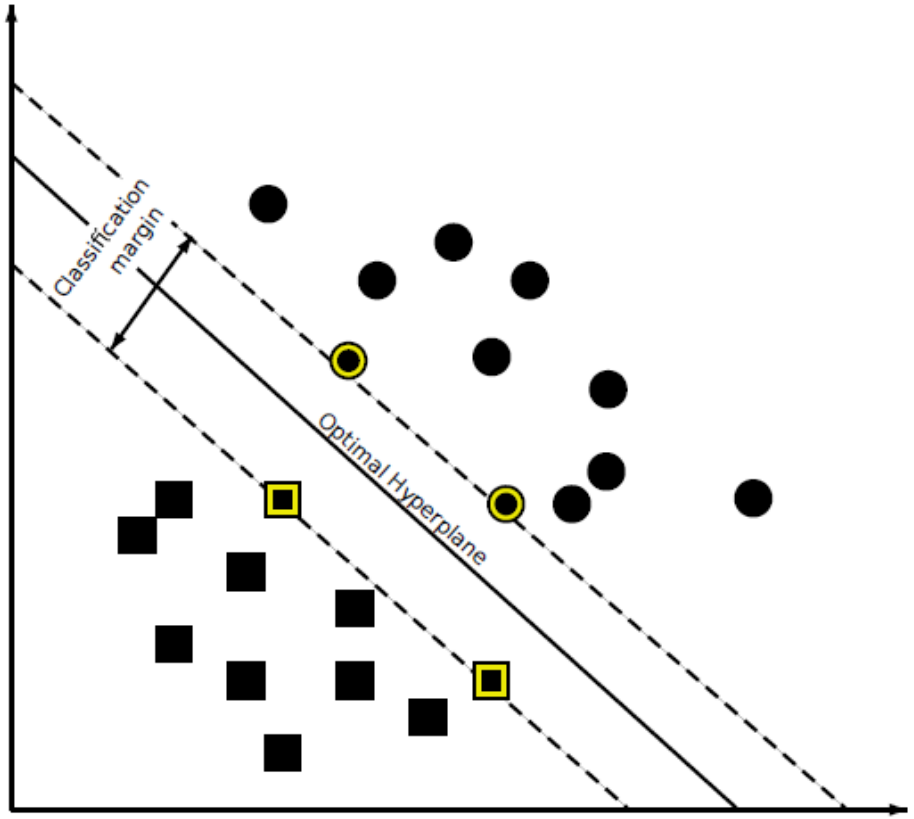
Source: Sim, Sukin, Peter D. Johnson, and Alán Aspuru-Guzik. "Expressibility and Entangling Capability of Parameterized Quantum Circuits for Hybrid Quantum-Classical Algorithms." Advanced Quantum Technologies 2.12 (2019): 1900070.

Quantum Support Vector Machine

The SVM algorithm is as follows:

1. Map the input data to a high dimensional feature space via some nonlinear mapping, chosen a priori.
2. Construct an optimal hyperplane in the high dimensional feature space that separates the classes

The optimal hyperplane is the one that maximizes the margin between the training points of the classes



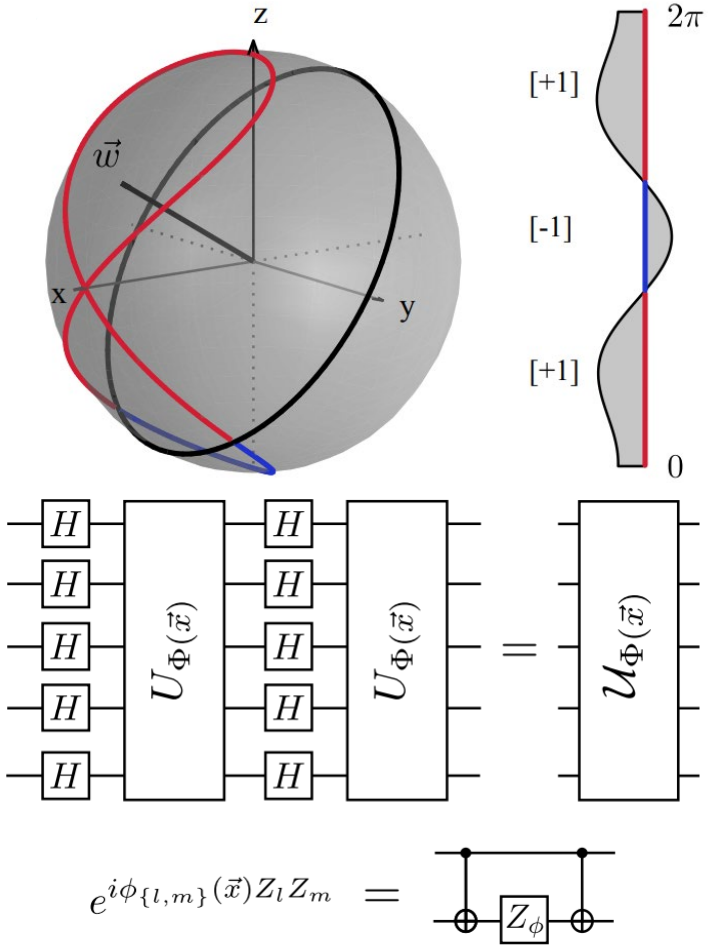
Quantum Support Vector Machine

QSVM thus follows naturally from SVM but with a quantum kernel executed on a quantum computer defined as:

$$k(x_i, x_j) = \left|\langle \psi(x_i) | \psi(x_j) \rangle\right|^2$$

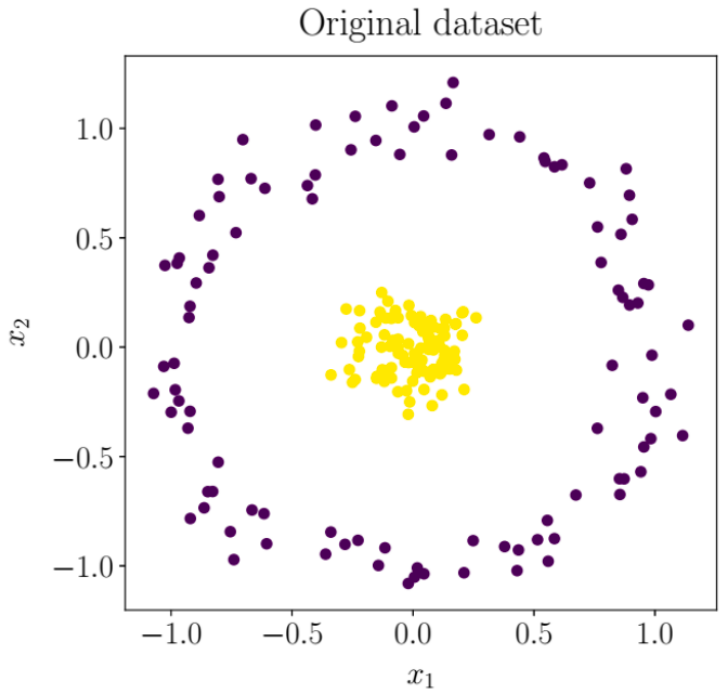
The input vector x_i has been encoded into a n-qubit quantum state $|\psi(x_i)\rangle$ by some unitary transformation $U_\psi(x_i)$ on the $|\psi(x_i)\rangle^{\otimes n}$ state.

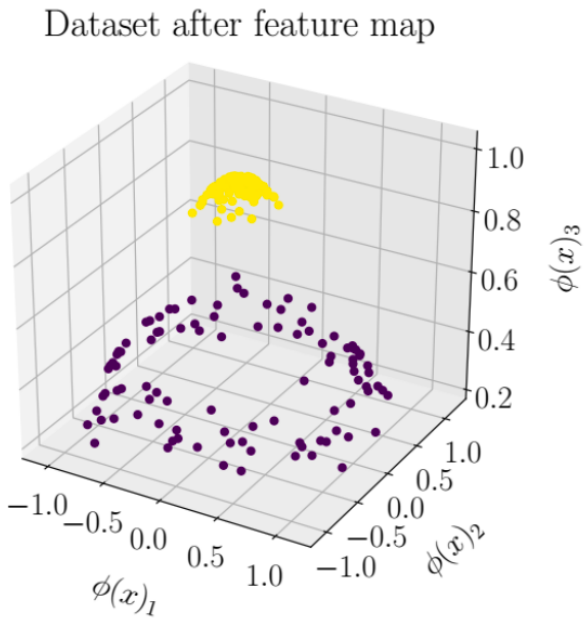
Once the kernel matrix has been computed, the QSVM can be trained similarly as the classical SVM.



Taken from: Supervised learning with quantum enhanced feature spaces

Feature Maps



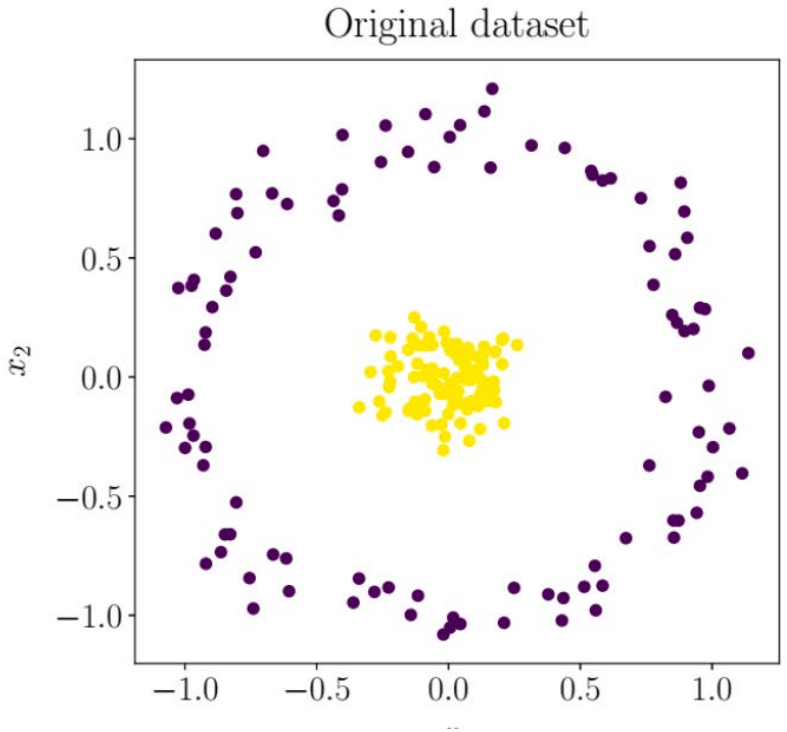


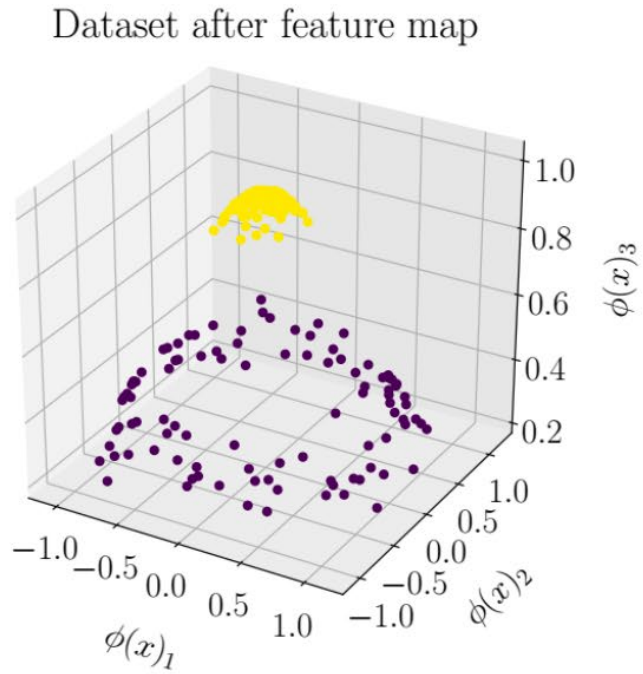
$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

$$\phi(x) = \begin{bmatrix} \phi(x_1) \\ \phi(x_2) \\ \phi(x_3) \end{bmatrix}$$

Mapping to a high-dimensional space could make classification easier

Kernel Methods





$$\kappa(x, x') = \text{similarity} \qquad \kappa(\phi(x), \phi(x')) = \text{similarity}$$

Quantum Kernel Functions

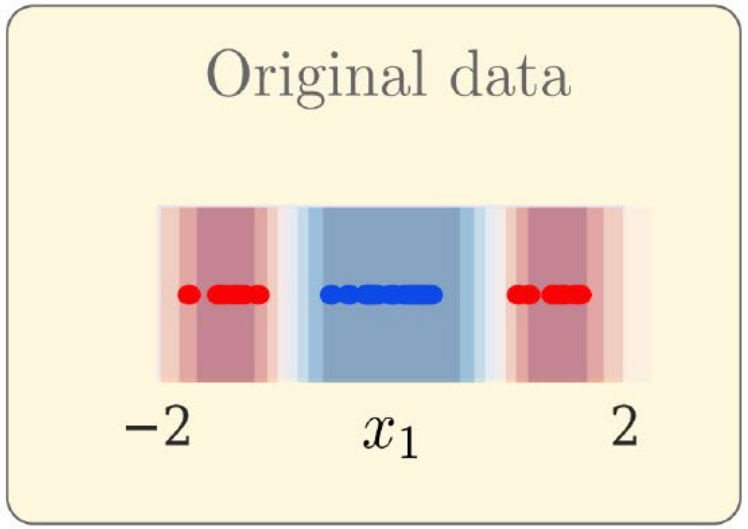
- Quantum Feature Map

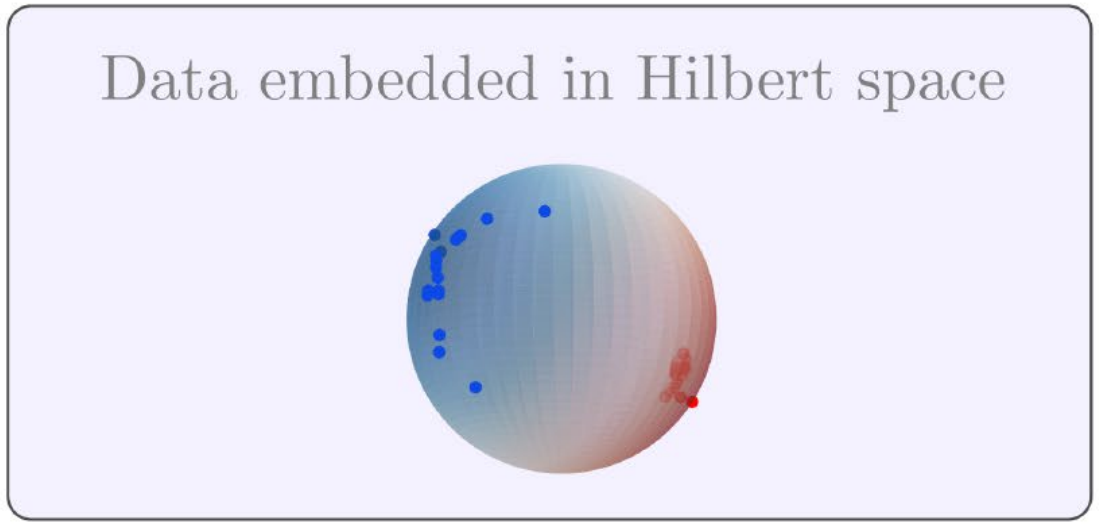
$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \longrightarrow |\phi(x)\rangle = \begin{bmatrix} \phi(x_1) \\ \phi(x_2) \\ \vdots \end{bmatrix}$$

- Quantum Kernel Function

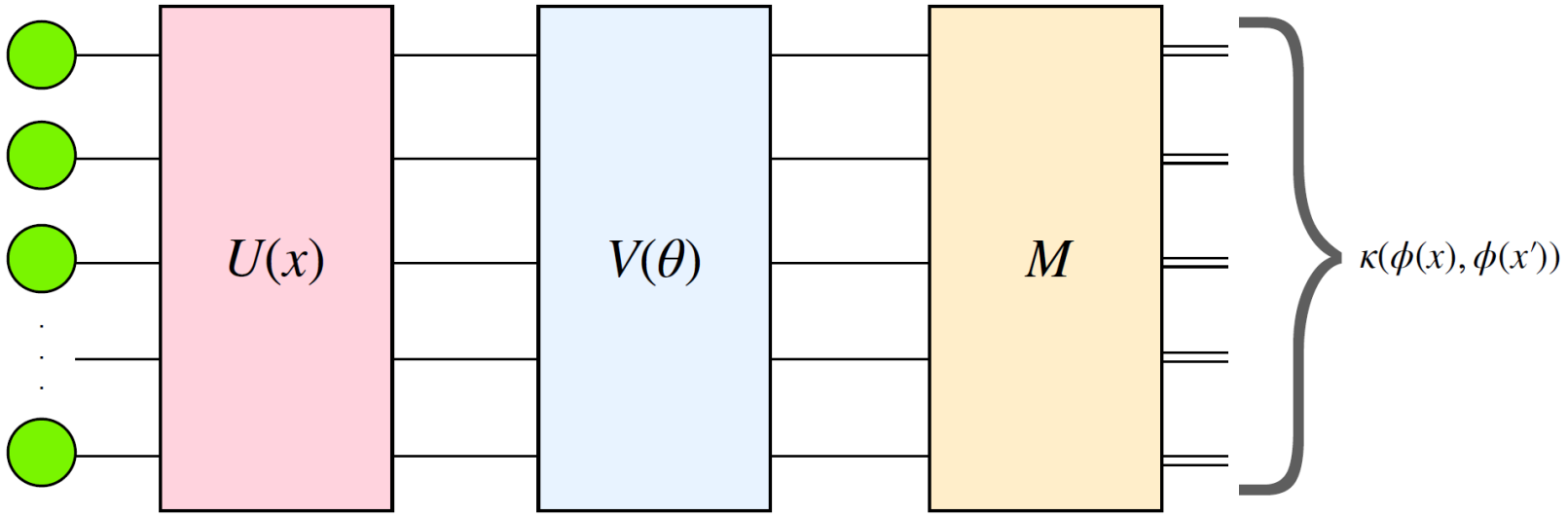
$$\kappa(\phi(x), \phi(x')) = \langle \phi(x) | \phi(x') \rangle$$

Quantum Kernel Functions

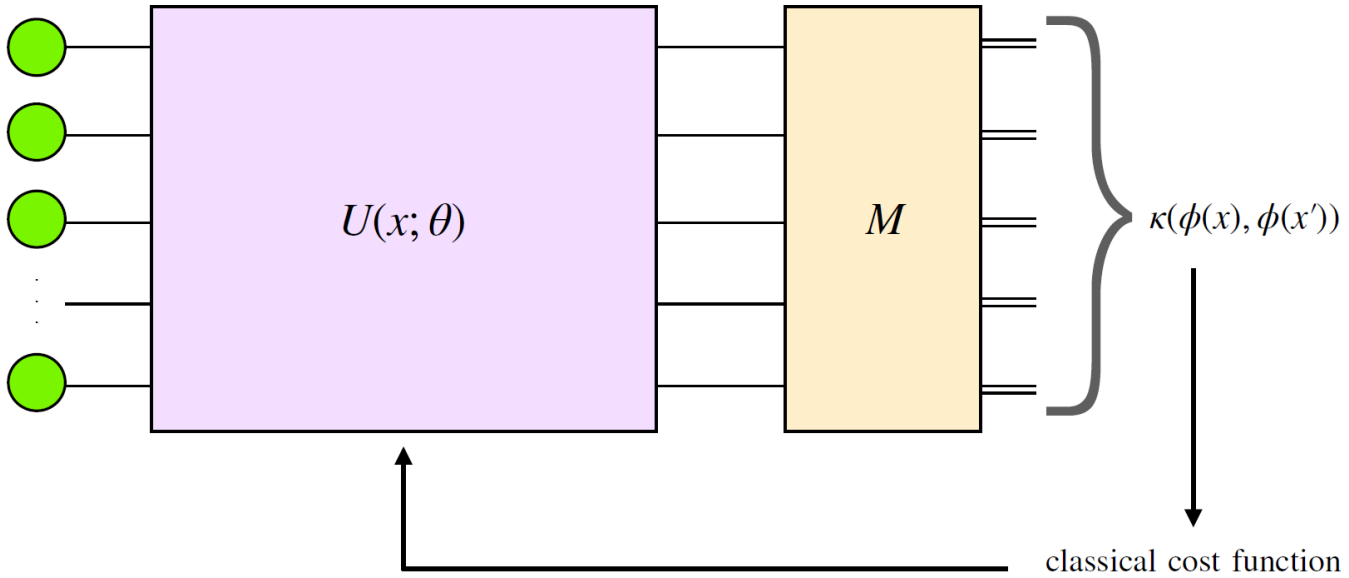




Source: Lloyd, Seth, et al. "Quantum embeddings for machine learning." arXiv preprint arXiv:2001.03622 (2020).

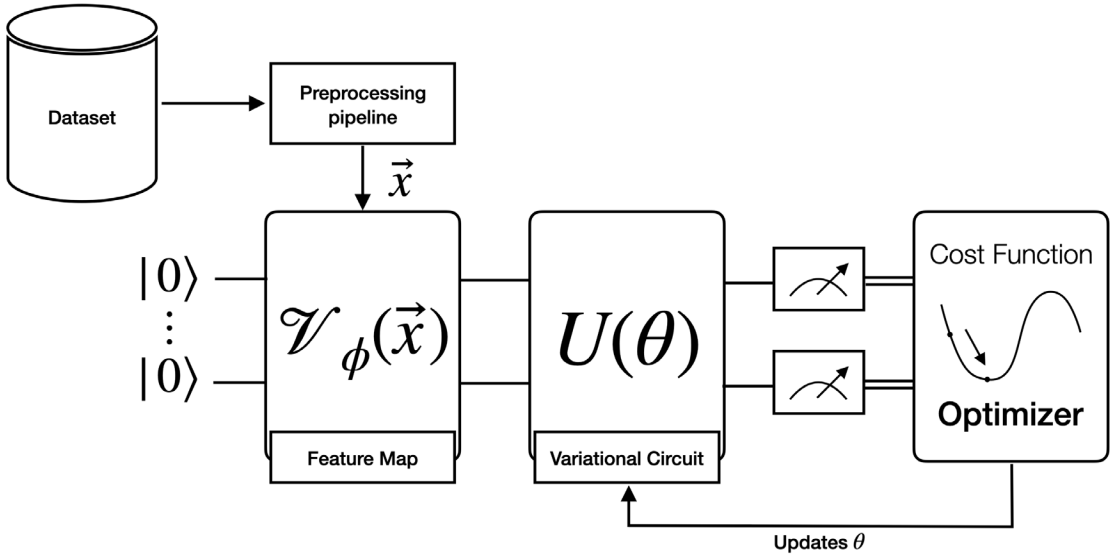


You can assume this block as one and then train!

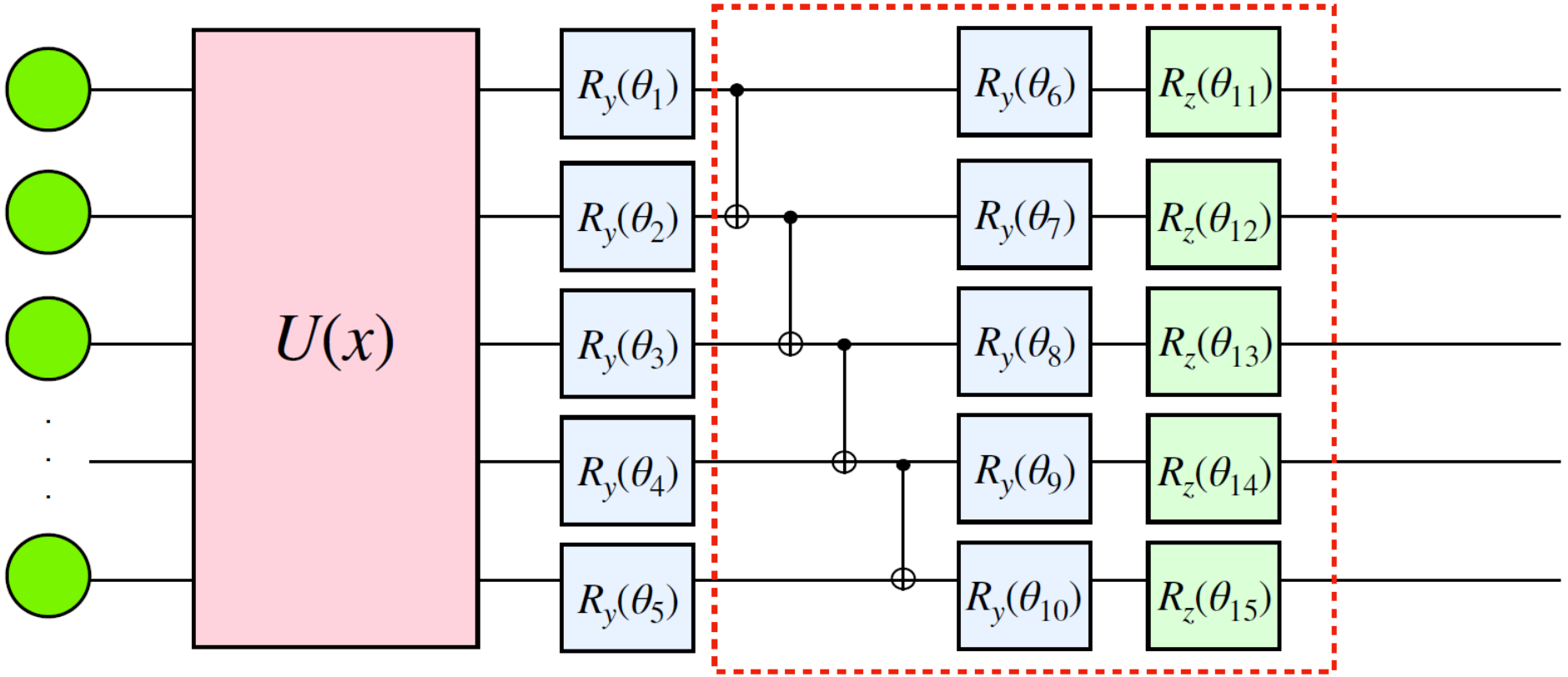


Variational Quantum Circuits

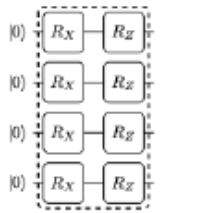
- A variational quantum circuit (VQC) is a quantum circuit that uses rotation function gates with random initialization to carry out a variety of computational tasks like approximation, optimization, and classification.
- VQC is comparable to artificial neural networks in that it closely resembles functions through parameter learning, but it differs owing to many QC properties.
  - Quantum circuits with multilayer topologies employ entanglement layers rather than activation functions because all quantum gate operations are reversible linear operations

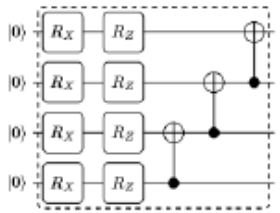


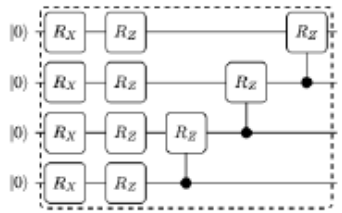
Variational Forms

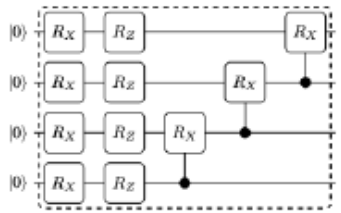


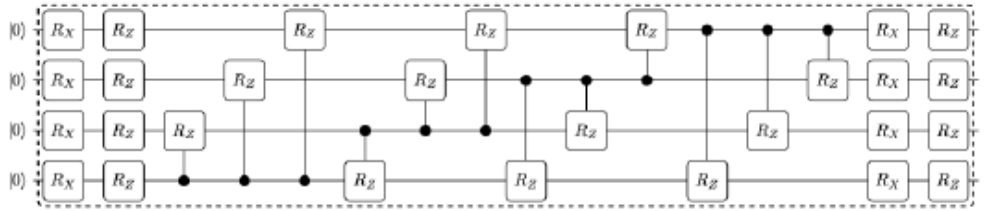
Variational Forms

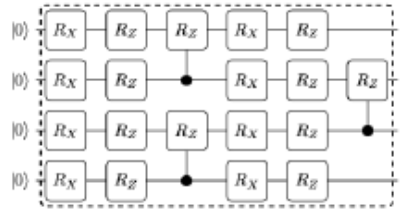

Circuit 1

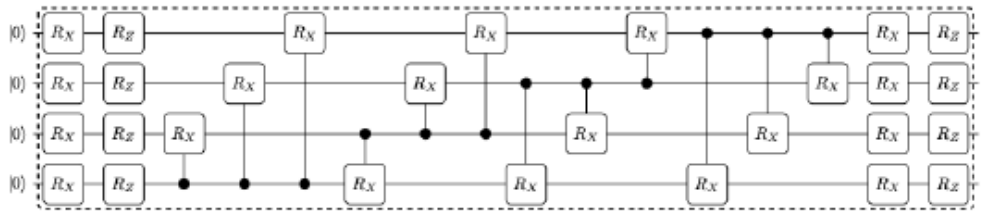

Circuit 2

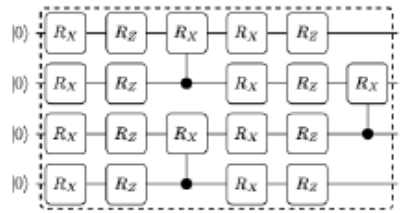

Circuit 3

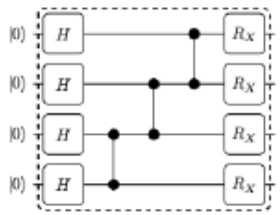

Circuit 4

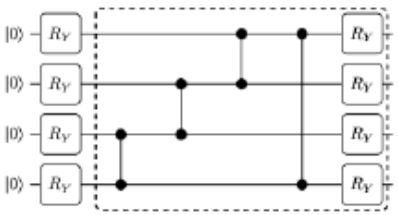

Circuit 5

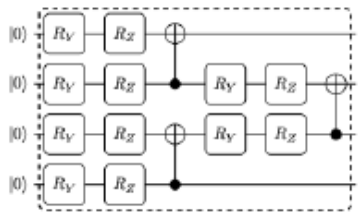

Circuit 7

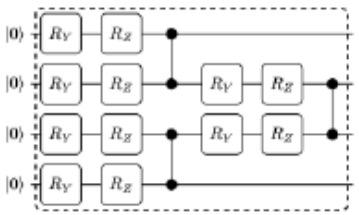

Circuit 6


Circuit 8

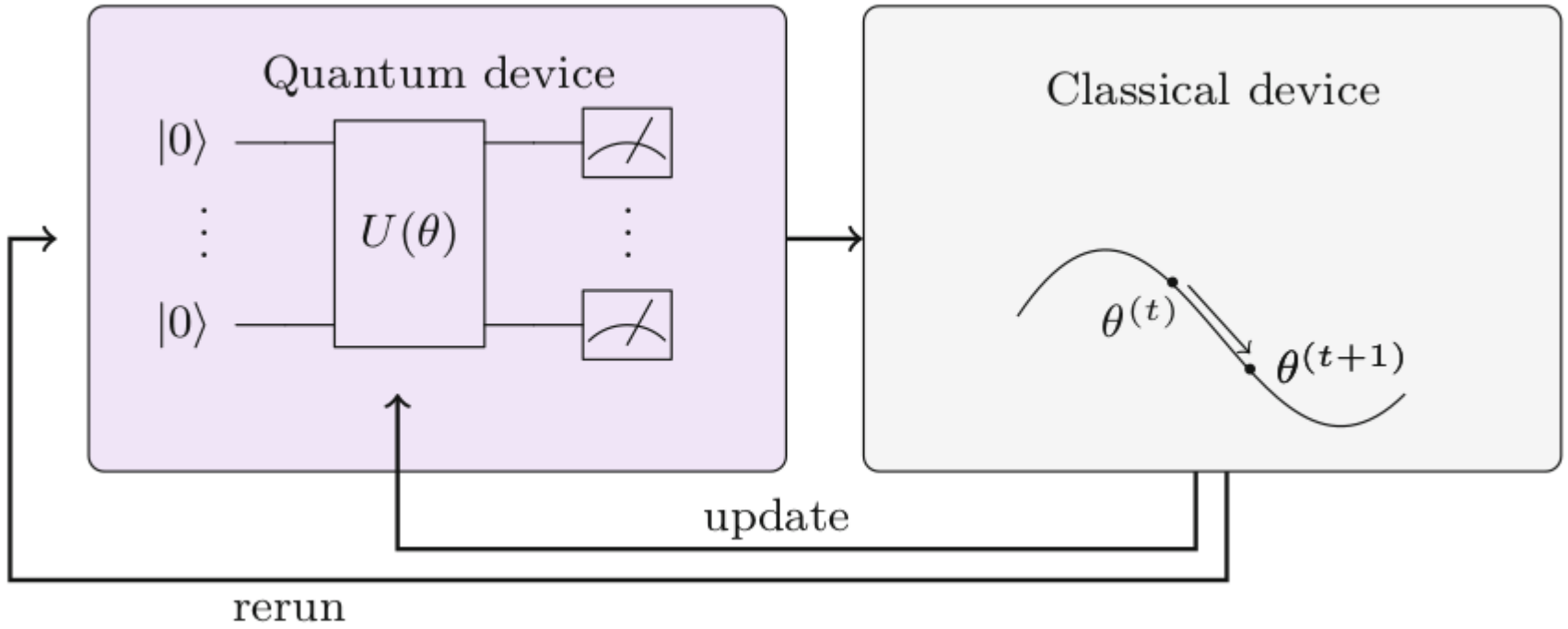

Circuit 9


Circuit 10


Circuit 11


Circuit 12

Variational Quantum Algorithm



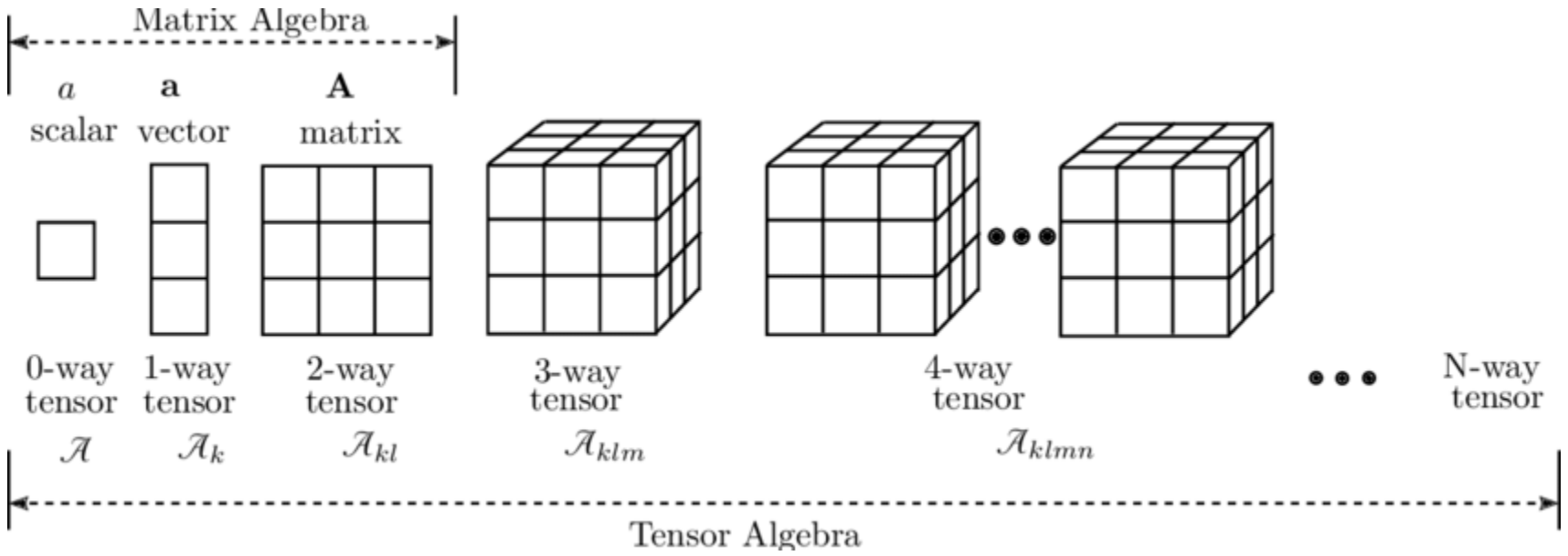
Adapted from 'Supervised Learning with Quantum Computers' by Schuld, M., Petruccione, F., 2018, Springer Nature Switzerland AG,p.225

Quantum Circuits: Tensor-Network

- Each quantum circuit can be represented as a network of tensors, with the link dimension dependent on the width and connectivity of the circuit.
- The connectivity of a network of tensors is related to how the entanglement is distributed and how the correlations propagate in the resulting quantum circuit of the network of tensors.

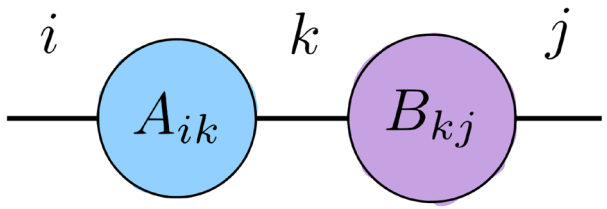
Tensor-networks

Tensors are multidimensional arrays of numbers. Intuitively, they can be interpreted as a generalization of scalars, vectors and matrices.



Tensor contraction

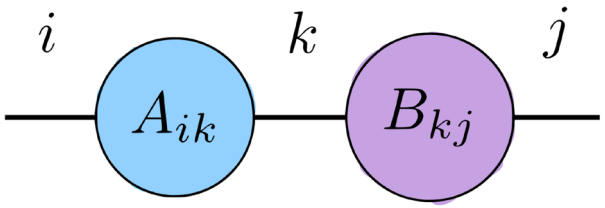
- Two or more tensors can be contracted by adding repeated indices.
- In schematic notation, repeated indices appear as lines connecting tensors.



Two range two tensors connected by a repeated index, *k*. The dimension of the repeated index is called the bond dimension.

Source: https://pennylane.ai/qml/demos/tutorial_tn_circuits.html#huggins

Tensor contraction



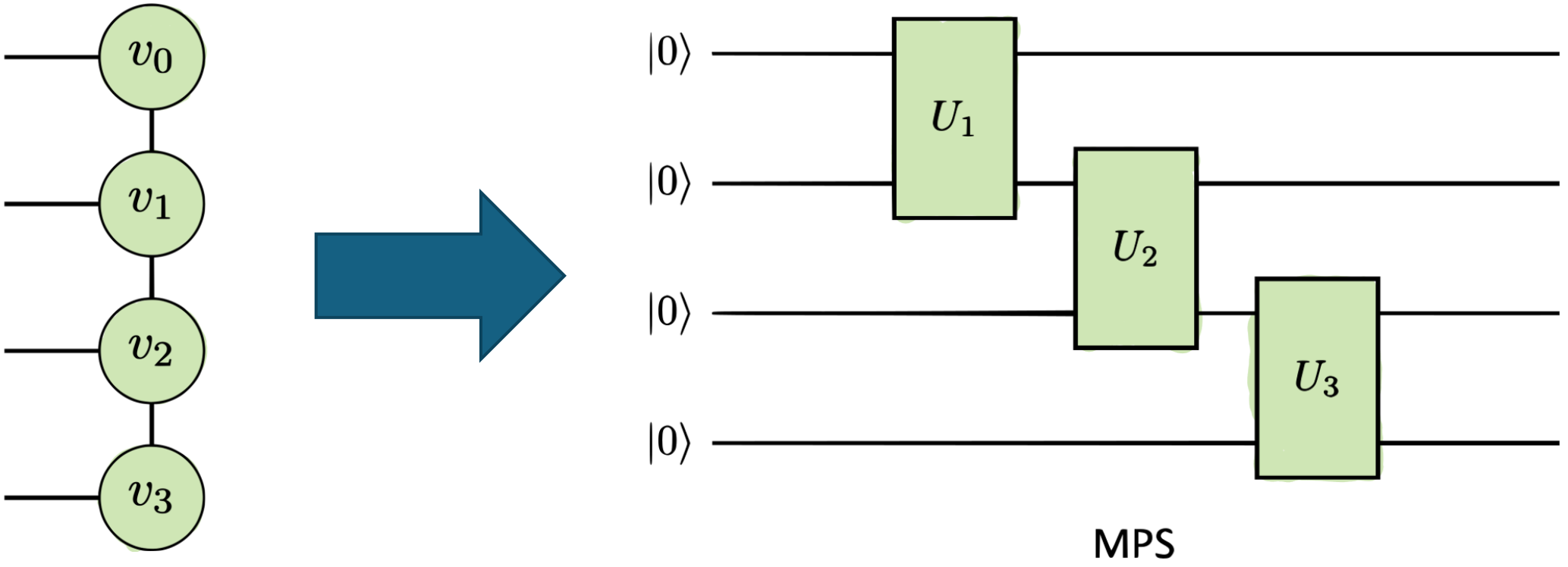
- The contraction of the above tensors is equivalent to the standard matrix multiplication formula and can be expressed as:

$$C_{ij} = \sum_{k} A_{ik} B_{kj}$$

- C_{ij} denotes the entry for the i-th row and the j-th column of the product $C = AB$
- A tensor network is a collection of tensors where a subset of all indices is contracted.
- Tensor networks can represent complicated operations involving several tensors with many indices contracted in sophisticated patterns

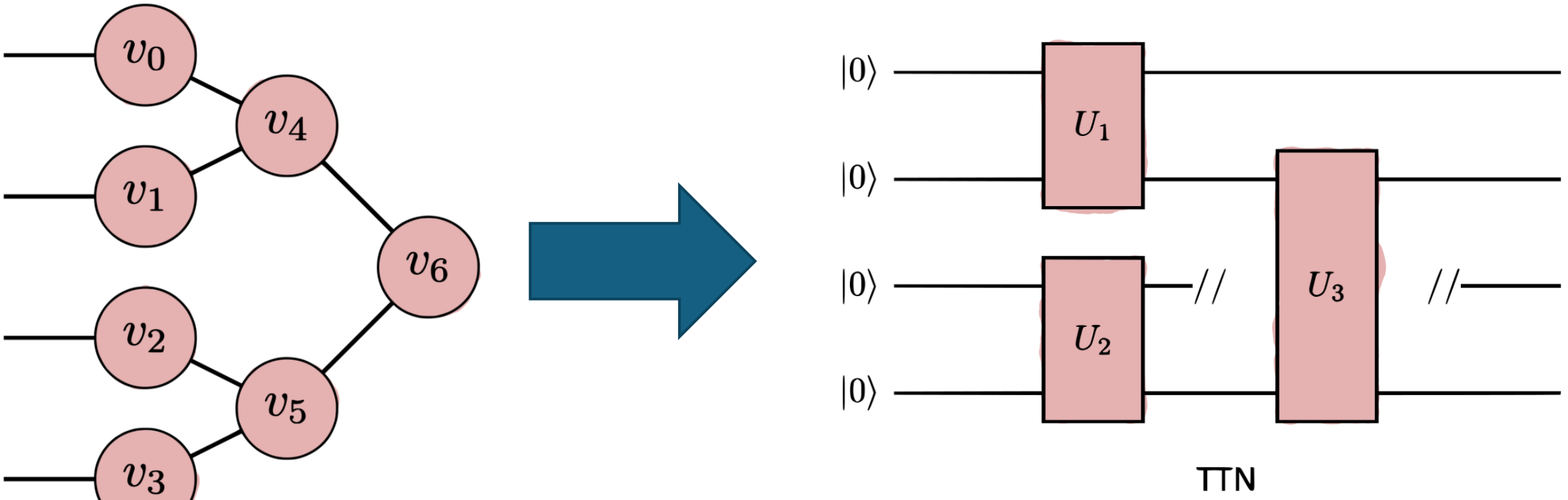
Source: https://pennylane.ai/qml/demos/tutorial_tn_circuits.html#huggins

Matrix Product State (MPS)



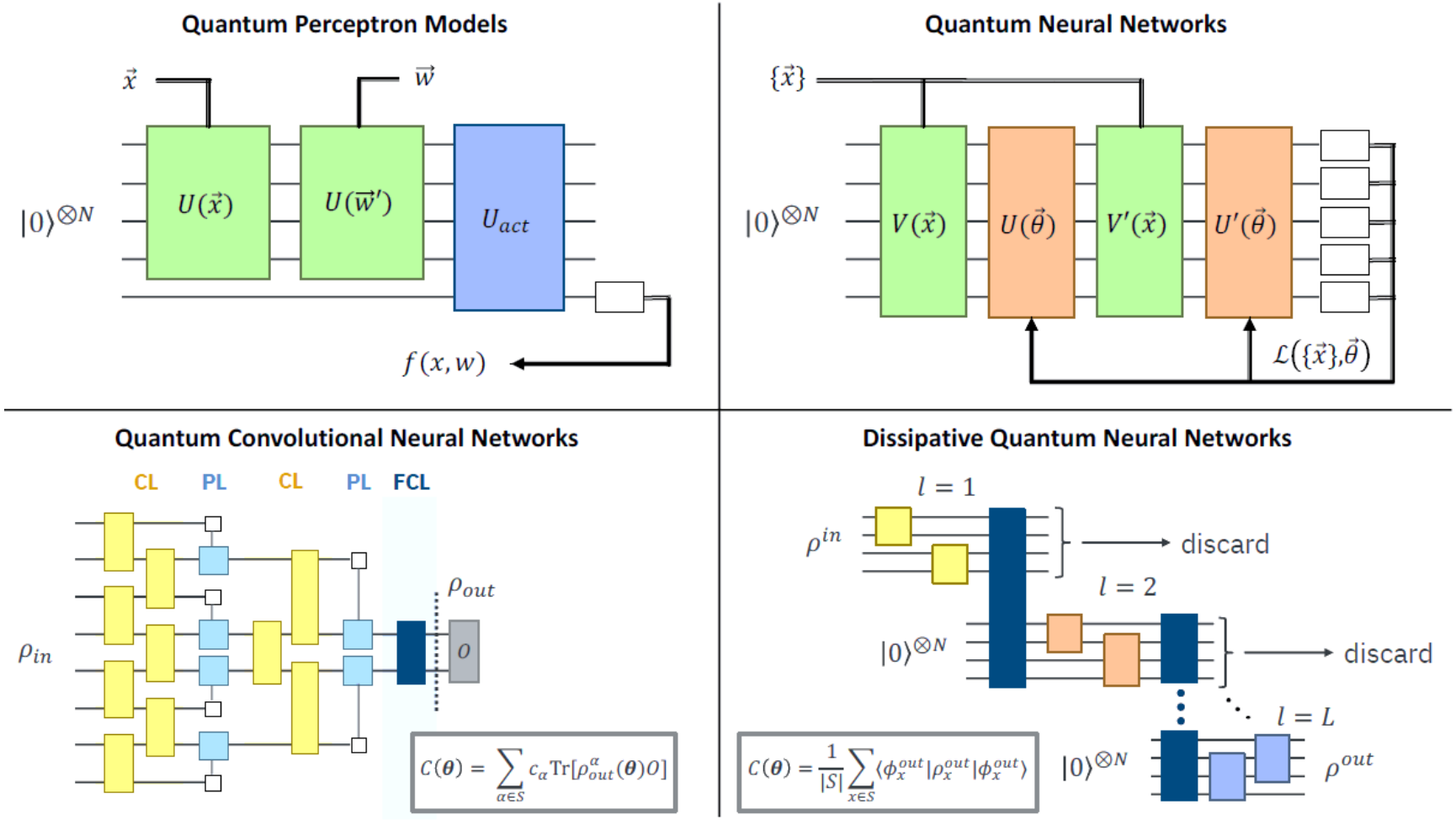
Source: https://pennylane.ai/qml/demos/tutorial_tn_circuits.html#huggins

Tree Tensor-Network (TTN)

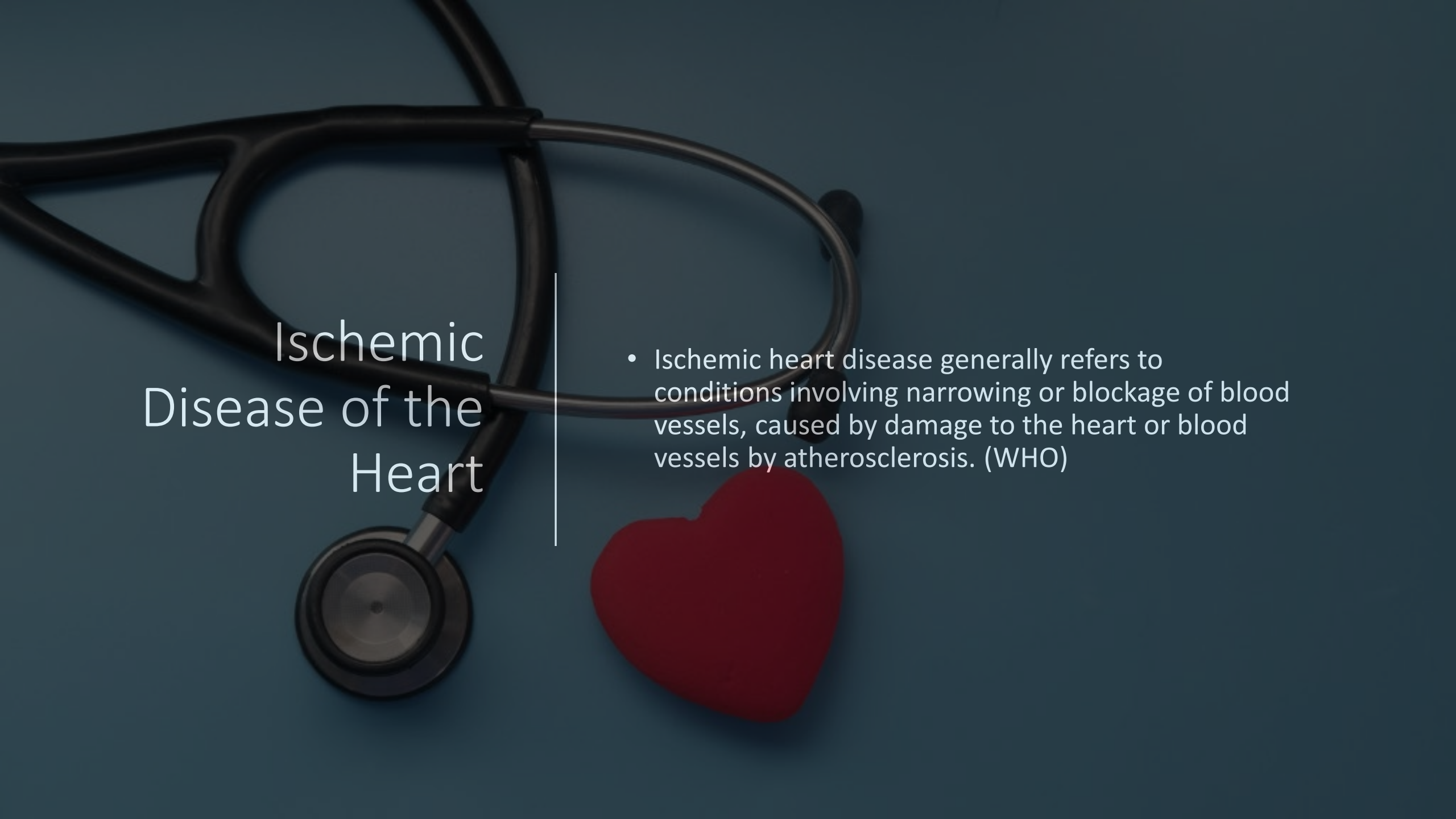


Source: https://pennylane.ai/qml/demos/tutorial_tn_circuits.html#huggins

Quantum neural network models

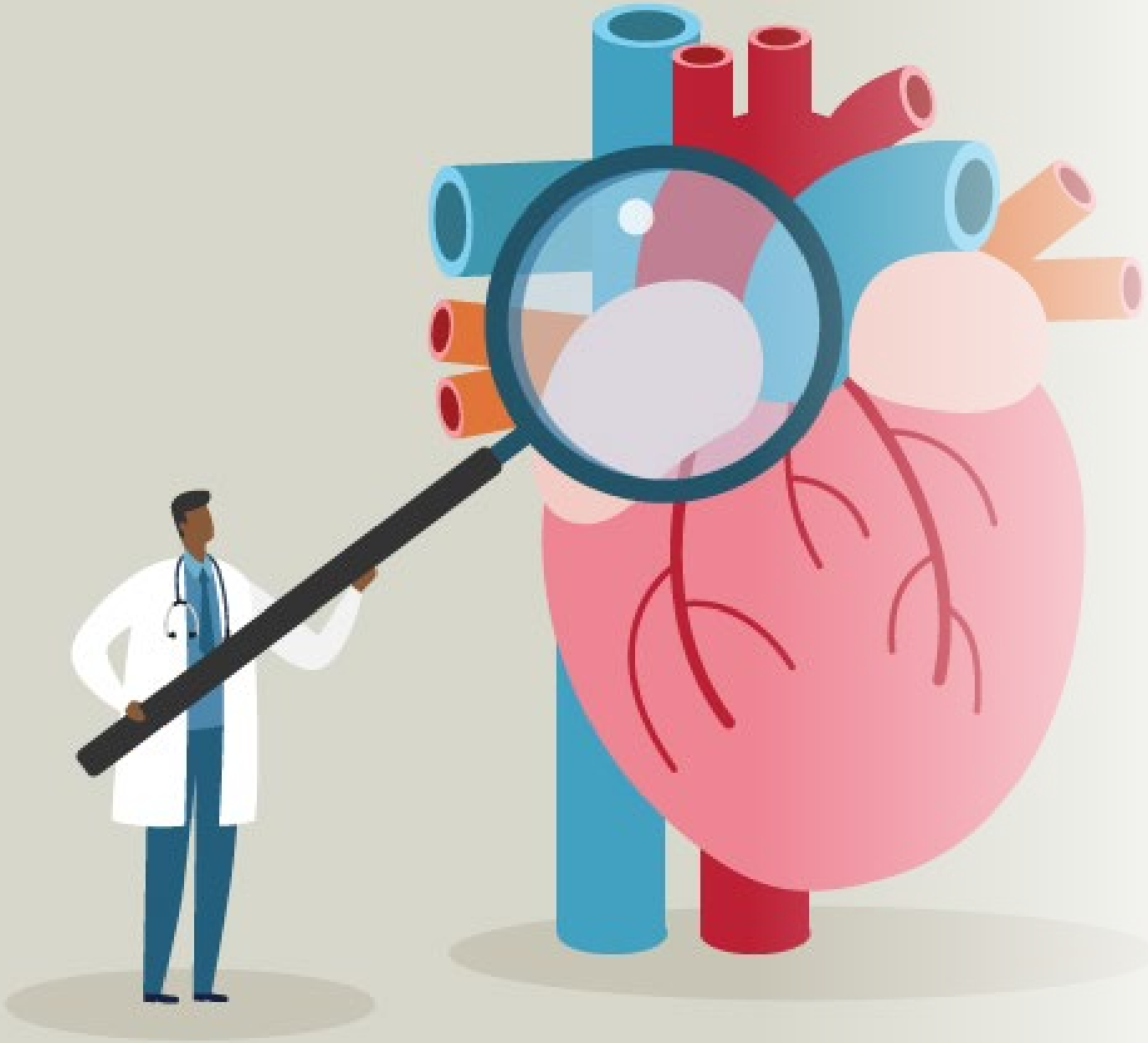


Case Study



Ischemic Disease of the Heart

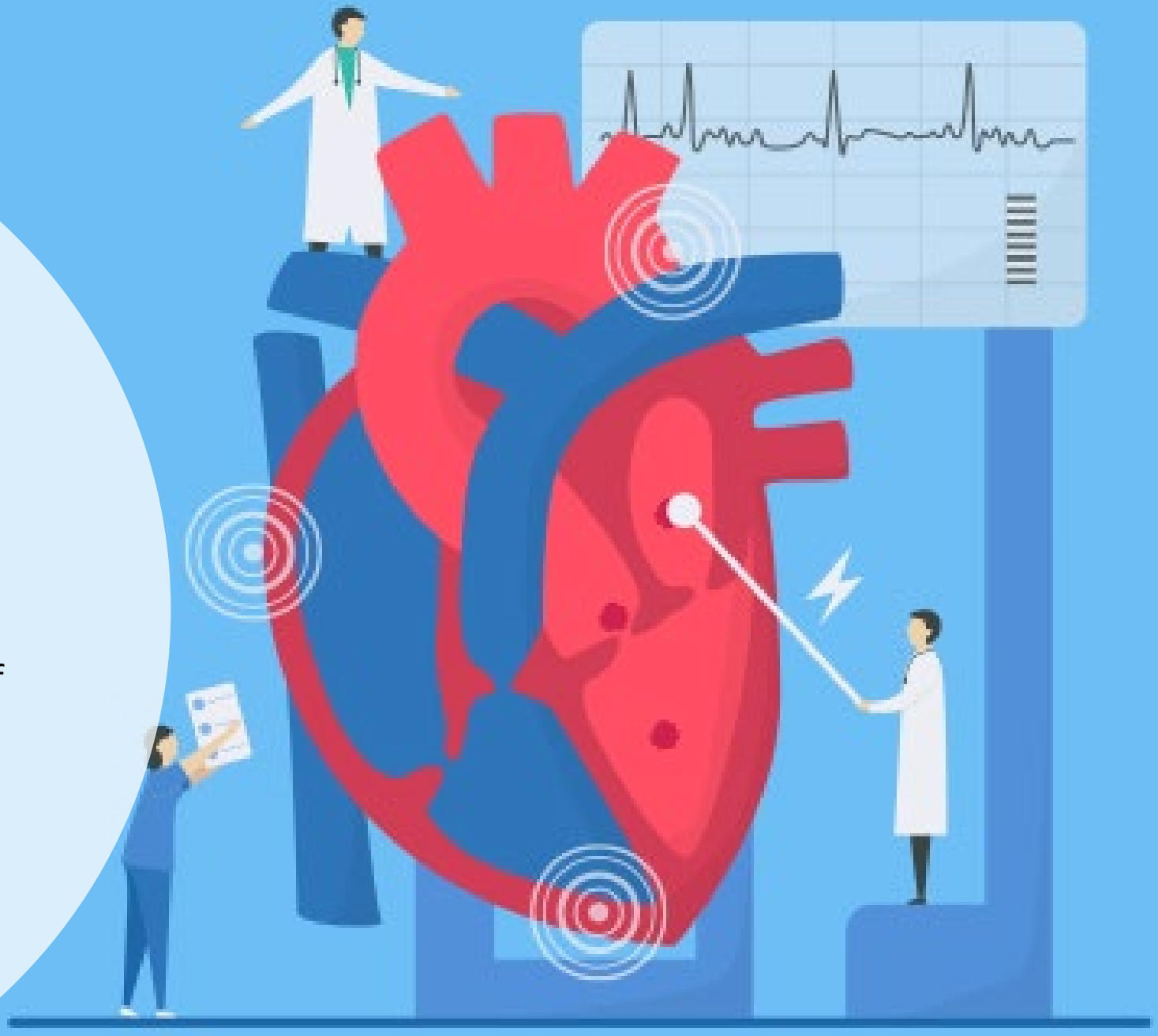
- Ischemic heart disease generally refers to conditions involving narrowing or blockage of blood vessels, caused by damage to the heart or blood vessels by atherosclerosis. (WHO)



Some people who have myocardial ischemia have no signs or symptoms

Motivation

- Cardiology has been one of the branches of medicine where more progress has been made in recent years. The high prevalence of cardiovascular pathologies has led to a constant development of new technologies for diagnosis and treatment.



Data - IEEE DataPort

- In this dataset, 5 independent subsets are combined based on 11 common features in 1,190 records, making it the largest coronary artery disease dataset available so far for research purposes. The five data sets used are:
  - Cleveland
  - Hungarian
  - Switzerland
  - Long Beach VA
  - Statlog (Heart) Data Set

Source: https://ieee-dataport.org/open-access/heart-disease-dataset-comprehensive

Diagnosis of heart disease (angiographic status):

- Value 0: < 50% diameter narrowing
- Value 1: > 50% diameter narrowing

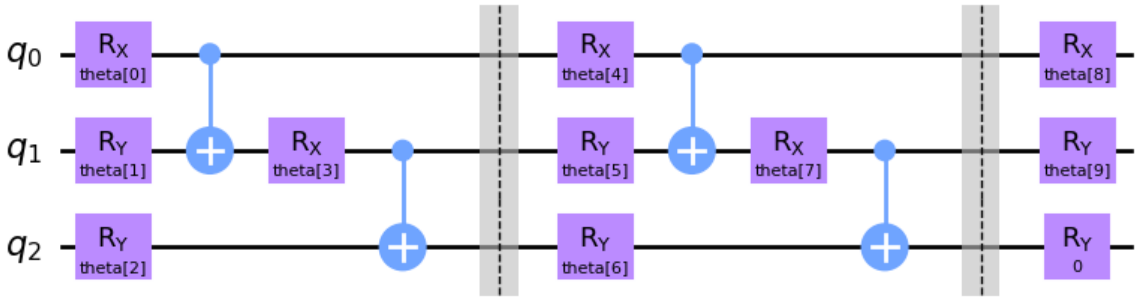
Attributes

Attribute	Units	Guy
Age	in years	Numeric
Gender	1, 0	Binary
Type of pain in the chest	1,2,3,4	Nominal
Resting blood pressure	in mm Hg	Numeric
Cholesterol	in mg/dl	Numeric
Fasting blood sugar	1,0 > 120 mg/dl	Binary
Resting electrocardiogram	0,1,2	Nominal
Maximum heart rate achieved	71–202	Numeric
Exercise-induced angina	0,1	Binary
Peak ST	depression	Numeric
Slope of ST segment (maximum exercise)	0,1,2	Nominal
Diagnostic	0,1	Binary

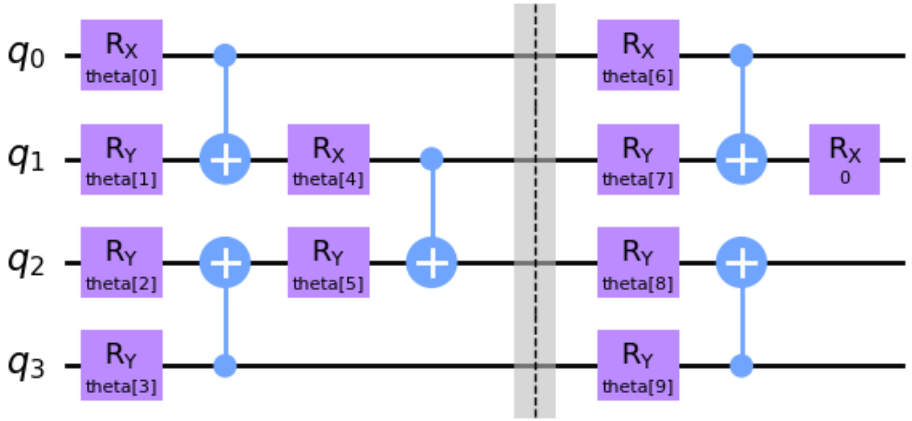
Results: VQC and QSVM

Technique	Accuracy	Precision_0	Precision_1	Recall_0	Recall_1	F1-Score_0	F1-Score_1
SVM	80.25%	82.30%	78.40%	77.50%	83.05%	79.83%	80.66%
Naive Bayes	78.99%	83.19%	75.20%	75.20%	83.19%	78.99%	78.99%
Logistic Regression	78.99%	81.42%	76.80%	76.03%	82.05%	78.63%	79.34%
Decision Tree	85.29%	84.07%	86.40%	84.82%	85.71%	84.44%	86.06%
Random Forest	88.24%	91.15%	85.60%	85.12%	91.45%	88.03%	88.43%
XGBoost	84.03%	87.61%	80.80%	80.49%	87.83%	83.90%	84.17%
QSVM	77.73%	75.00%	80.51%	79.65%	76.00%	77.25%	78.19%
VQC	73.95%	72.57%	75.20%	72.57%	75.20%	72.57%	75.20%

Tensor networks



MPS



TTN

Network	Accuracy	Precision_0	Precision_1	Recall_0	Recall_1	F1-Score_0	F1-Score_1
MPS	73.1%	68.7%	78.5%	79.6%	67.2%	73.8%	72.4%
TTN	66.0%	59.4%	82.4%	89.4%	44.8%	71.4%	58.0%

Cybersecurity??

- Let’s go hands-on!

https://github.com/HIVE-AI-Studio/QuantumDay

THE CATHOLIC UNIVERSITY OF AMERICA

Questions?