SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Influence of Noise in Quantum Machine Learning

Erick Ruben Quintanar Salas

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Influence of Noise in Quantum Machine Learning

Einfluss von Rauschen in Quantenmaschinen Lernen

Author:	Erick Ruben Quintanar Salas
Supervisor:	Prof. Dr. Claudia Eckert
Advisors:	M. Sc. Pascal Debus / M. Sc. Kilian Tscharke
Submission Date:	Submission date

I confirm that this master's thesis is my own work and I have documented all sources and material used.

Munich, Submission date Erick Ruben Quintanar Salas

Acknowledgments

Abstract

Contents

Acknowledgments **iii**

Abstract **iv**

1 Introduction **1**
1.1 Motivation 1
1.2 Research Goals 2
1.3 Outline 3

2 Theoretical Background **4**
2.1 Fundamentals of Quantum Computing 4
2.1.1 Qubit 4
2.1.2 Bloch Sphere 5
2.1.3 Multiple qubits 5
2.1.4 Quantum Gates 7
2.1.5 Density Operator 8
2.2 Quantum Noise 8
2.3 Quantum Machine Learning 8
2.4 Adversarial Machine Learning 8

3 Implementation **9**
3.1 Section 9

4 Style **10**
4.1 Section 10
4.1.1 Subsection 10

Abbreviations **12**

List of Figures **13**

List of Tables **14**

Bibliography **15**

1 Introduction

In recent years the interest on techniques to utilize quantum mechanics has been rising. One of the many applications is quantum computing, where devices based on the laws of quantum theory are exploited to process information [1]. Although current classical computers have become very powerful, they still struggle to process many applications that quantum computers can in theory easily solve.

Many quantum algorithms for quantum computers have been proposed that highly outperform a classical computer with the best known algorithms [2, 3, 4]. These quantum algorithms solve in polynomial time problems that quickly become intractable to solve in a classical computer, as they normally grow exponentially. The most famous algorithm is Shor's algorithm [2], which can find the prime factors of an integer. It is of special interest because if quantum devices were able to execute it, the current confidentiality and integrity guarantees that the RSA [5] cryptographic mechanism offers would be violated.

1.1 Motivation

Even though the previously mentioned quantum algorithms would surpass the performance of the best classical ones, they still can not be executed in current quantum computers due to noise [6]. This noise occurs because current quantum devices are not completely isolated from the environment and every time we perform an operation on them we introduce a disturbance. This type of device is known as Noisy Intermediate-Scale Quantum (NISQ), meaning that there will be significant noise when operating the quantum device.

In order to reduce the influence of noise in NISQ devices, either the precision in which quantum computers can be manipulated has to improve or error-correcting codes have to be implemented [7]. Currently both techniques are being heavily researched and in conjunction will lead to the next generation of quantum devices, namely fault-tolerant quantum computers.

A technology that right now has gained a bigger presence in our society is Machine Learning (ML). There have been many important breakthroughs for ML in the past few years, with uses in natural language processing, computer vision, anomaly detection, and many more fields [8]. Nowadays ML has a big impact in society, and even though it depicts big opportunities for improvement in society it also represents significant risks.

Quantum computing and ML are information processing techniques that have improved significantly in recent years. This lead to the natural desire of harnessing the advantages of both and to the emergence of a new field of study denominated Quantum Machine Learning (QML) [9]. QML explores several ideas like whether quantum devices are better at ML than classical computers or if quantum information adds new data that affects how machines recognize patterns.

Returning to the possible risks that ML might encounter, several attacks have been developed to force a ML model to missclassify an input [10]. These attacks are denominated adversarial attacks and are based on crafting specific input data that has been slightly modified to cause the model to erroneously classify the input. At the beginning, when the first adversarial attacks were developed, they needed to know the architecture of the model to be able to fool it. Nevertheless, it was proved that adversarial attacks are transferable between models with the same use case, without knowing the architecture of the model or the dataset it was trained on [11].

Adversarial training was developed in order to defend ML models against adversarial attacks [12, 10]. Adversarial training consists of including adversarial samples into the training of the ML model to better generalize its classification. This mechanism has a tradeoff, in which the accuracy of the model lowers, while increasing the resilience to adversarial attacks [13].

In classical ML noise in training has been shown to improve generalization performance and local optima avoidance [14]. This property from noise is particularly interesting in NISQ devices, as their inherent noise might be able to improve QML performance, accuracy and resilience against adversarial attacks.

TODO: - Could we claim that noise in QML might also be a defense against data poisoning attacks? (AML at scale) [13]

1.2 Research Goals

1. Test the effect of different types of noise in QML regarding robustness. 2. Test the effect of noise in different parts of the QML circuits. 3. Test the effect of noise between VQA and Kernel methods. 4. Test the models with different types of adversarial attacks (FGSM, CaW, PGD)

1.3 Outline

Write here what is the general structure of the thesis.

2 Theoretical Background

In Chapter 2 we will introduce the background information that is required to understand the main ideas of this thesis. First we introduce the basic concepts of quantum computing. Then we will describe advanced concepts regarding quantum noise. We assume some baseline ML knowledge, however, we will provide an outlook into QML. Finally, we present several types of adversarial machine learning and adversarial training as a defense mechanism.

2.1 Fundamentals of Quantum Computing

2.1.1 Qubit

The basic computing unit in quantum computing is the *qubit* [15]. Similar to the classical bit, a qubit also has a state. While a bit has either a *0* or *1* state, the qubit can have many more states. The quantum equivalent to the classical bit states would be $|0\rangle$ and $|1\rangle$ in Dirac notation [16] and they represent the orthonormal computational basis states in Equation 2.1.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

What makes the qubit different and more capable than the classical bit is that it can also have different states created by a linear combination or *superposition* from its basis states. The linear combination in Equation 2.2 is the complete representation of a qubit, where α and β are two complex numbers that are denominated *probability amplitudes*. The values α and β represent a distribution, in which with probability $|\alpha|^2$ we will observe a *0* value and with probability $|\beta|^2$ we will observe a *1* value. This distribution is determined by the Born rule [17] and states that $|\alpha|^2 + |\beta|^2 \overset{!}{=} 1$. The Born rule thus implies that a qubit state is a unitary vector in a two-dimensional complex vector space. Although the probability amplitudes can take on any complex value as long as they fulfill the Born rule, when we perform a measurement on the qubit it *collapses* to one of the two basis states.

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.2}$$

In the real physical world qubits can be implemented by several different small particles. However, the mathematical qubit abstraction helps establish a baseline computing unit for quantum computing independent of which particle it is being represented by [18]. While in this perfect mathematical description noise doesn't occur, there are different mechanisms to represent the noise that quantum computers suffer from, namely the density operator that will be introduced in Subsection 2.1.5.

2.1.2 Bloch Sphere

The qubit state from Equation 2.2 can be rewritten into Equation 2.3, where e is the Euler number, i is the imaginary number, and γ, φ, and θ are real numbers.

$$|\psi\rangle = e^{i\gamma} \left(\cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2}\beta |1\rangle \right) \tag{2.3}$$

Because for a single qubit the global phase $e^{i\gamma}$ has no observable effects, we can omit it and write the state of a qubit as:

$$|\psi\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\varphi} \sin\frac{\theta}{2}\beta |1\rangle \tag{2.4}$$

where θ and φ determine a point in the Bloch sphere [19]. The Bloch sphere (Fig. 2.1) is a helpful visual representation for understanding the state of a qubit. In Section 2.2 this representation will be utilized to show the effects of quantum noise on a quantum state. It can also be used to visualize the effect of the operations performed on quantum states, these operations are called *gates* and they will be introduced in Subsection 2.1.4.

2.1.3 Multiple qubits

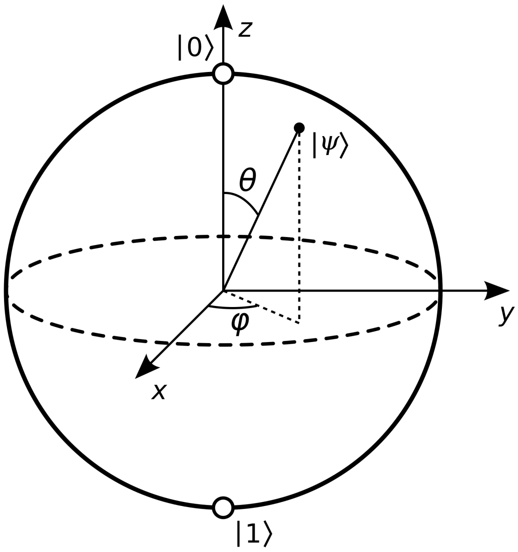


Figure 2.1: Bloch sphere representation of a qubit. Image taken from https://commons.wikimedia.org/wiki/File:Bloch_Sphere.svg under the Creative Commons Attribution-Share Alike 3.0 Unported license.

To describe multiple qubits we utilize the fundamentals presented in Subsection 2.1.1 and expand them. For two qubits $|00\rangle, |01\rangle, |10\rangle$, and $|11\rangle$ are the computational basis. A general representation for a two qubit system can be found in Equation 2.5, where all the probability amplitudes must follow the Born rule.

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{2.5}$$

Due to the Born rule the measurement results for $x = \{00, 01, 10, 11\}$ follow the probability distribution determined by $|\alpha_x|^2$. Similar to a single qubit, once a measurement on both qubits is performed, the state of the qubits will collapse to the measured computational basis. Nevertheless, with multiple qubits we are able to perform measurements on a subset of qubits. In the case of a two-qubit system, measuring the first qubit will collapse its value. However, the second's qubit state will remain. In the case of Eq. 2.5, if *0* was measured in the first qubit, the amplitudes α_{10} and α_{11} would disappear from the state as they are no longer possible. Furthermore, the remaining amplitudes must be normalized, such as in Eq. 2.6, to fulfill Born's rule.

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{2.6}$$

In Equation 2.7 we can find a general representation of a set of n qubits. For a system composed by n qubits there are 2^n amplitudes. If we tried to simulate a quantum system with $n = 50$, assuming that complex numbers require 8 bytes to be stored, a classical computer would need approximately 9000 terabytes to store the generated quantum state. This simple calculation shows the reason why quantum computers are so promising and also why classical computers are not able to process quantum information efficiently.

$$|\psi\rangle = \alpha_{00}|0\cdots 0\rangle + \cdots + \alpha_{2^{n-1}}|1\cdots 1\rangle \tag{2.7}$$

2.1.4 Quantum Gates

- Introduce quantum gates - Equate a gate with a unitary matrix - Pauli Gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad -\boxed{X}- \tag{2.8}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad -\boxed{Y}- \tag{2.9}$$

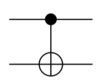
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad -\boxed{Z}- \tag{2.10}$$

- Hadamard Gate

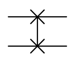
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad -\boxed{H}- \tag{2.11}$$

- Multiple qbits gates

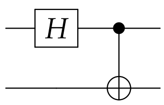
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.12}$$



$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.13}$$



- Introduce entanglement and bell states, 11,16



$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{2.14}$$

- Introduce quantum circuits - Introduce quantum measurement

2.1.5 Density Operator

- Introduce the density operator - Introduce quantum algorithms*
Todo: - Citation for hadamard gate, pauli gate.

2.2 Quantum Noise

i. Describe the types of noise that can occur. ii. Explain where can noise occur. iii. State how noise can be simulated.

2.3 Quantum Machine Learning

i. Present the difference between QML and classical ML. ii. Introduce variational quantum circuits. iii. Explain quantum kernel methods.

2.4 Adversarial Machine Learning

i. State generalization problems. ii. Present different attacks such as FGSM, C&W, and PGD. iii. Introduce adversarial training as defence mechanism against adversarial attacks. iv. Explain the relationship between general accuracy and adversarial resilience.

3 Implementation

3.1 Section

a. Introduce the used datasets and why they were chosen. b. Describe how the experiments have been chosen and created: i. Possible mixes with different types of noise, in different places, with different datasets and QML mechanisms.

4 Style

4.1 Section

Citation test [1]. Acronyms must be added in `main.tex` and are referenced using macros. The first occurrence is automatically replaced with the long version of the acronym, while all subsequent usages use the abbreviation.

E.g. `\ ac{tum}, \ ac{tum}` ⇒ Technical University of Munich (TUM), TUM

For more details, see the documentation of the `acronym` package[1].

4.1.1 Subsection

See Table 4.1, Figure 4.1, Figure 4.2, Figure 4.3.

Table 4.1: An example for a simple table.

A	B	C	D
1	2	1	2
2	3	2	3

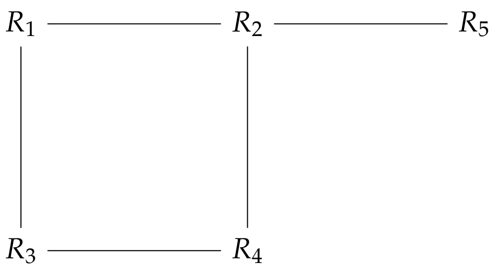


Figure 4.1: An example for a simple drawing.

[1] `https://ctan.org/pkg/acronym`

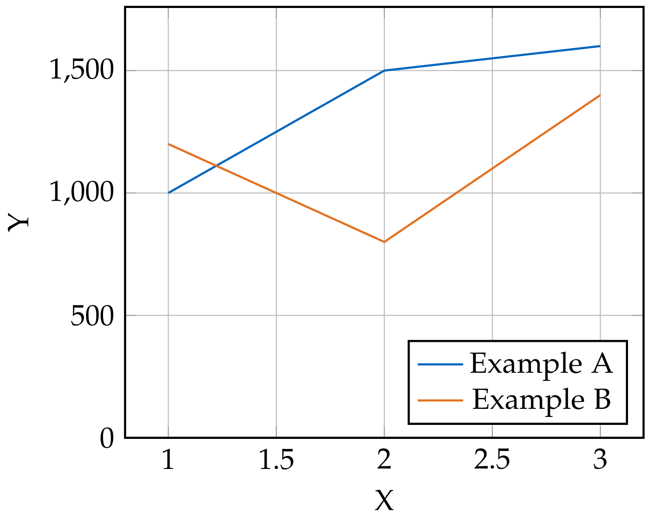


Figure 4.2: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 4.3: An example for a source code listing.

Abbreviations

TUM Technical University of Munich

NISQ Noisy Intermediate-Scale Quantum

ML Machine Learning

QML Quantum Machine Learning

List of Figures

2.1 Bloch sphere representation of a qubit. Image taken from https://commons.wikimedia.org/wiki/I
under the Creative Commons Attribution-Share Alike 3.0 Unported license. 6

4.1 Example drawing 10
4.2 Example plot 11
4.3 Example listing 11

List of Tables

4.1 Example table 10

Bibliography

[1]

bibinitperiod M. National Academies of Sciences Engineering. *Quantum Computing: Progress and Prospects*. Google-Books-ID: ATH3DwAAQBAJ. National Academies Press, Mar. 27, 2019. 273 pp. ISBN: 978-0-309-47972-1.

[2] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." In: *SIAM Journal on Computing* 26.5 (Oct. 1997). Publisher: Society for Industrial and Applied Mathematics, pp. 1484–1509. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172.

[3] W. Van Dam, S. Hallgren, and L. Ip. "Quantum Algorithms for Some Hidden Shift Problems." In: *SIAM Journal on Computing* 36.3 (Jan. 2006), pp. 763–778. ISSN: 0097-5397, 1095-7111. DOI: 10.1137/S009753970343141X.

[4] S. Hallgren. "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem." In: *Journal of the ACM* 54.1 (Mar. 2007), pp. 1–19. ISSN: 0004-5411, 1557-735X. DOI: 10.1145/1206035.1206039.

[5] R. L. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems." In: *Communications of the ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/359340.359342.

[6] J. Preskill. "Quantum Computing in the NISQ era and beyond." In: *Quantum* 2 (Aug. 6, 2018), p. 79. ISSN: 2521-327X. DOI: 10.22331/q-2018-08-06-79. arXiv: 1801.00862[cond-mat,physics:quant-ph].

[7] P. W. Shor. "Quantum Computing." In: *Documenta Mathematica - Extra Volume ICM 1998*, pp. 467–486.

[8] R. Bommasani, D. A. Hudson, E. Adeli, et al. *On the Opportunities and Risks of Foundation Models*. July 12, 2022. arXiv: 2108.07258[cs].

[9] M. Schuld and F. Petruccione. *Machine Learning with Quantum Computers*. Quantum Science and Technology. Cham: Springer International Publishing, 2021. ISBN: 978-3-030-83097-7 978-3-030-83098-4. DOI: 10.1007/978-3-030-83098-4.

[10] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus. *Intriguing properties of neural networks*. Feb. 19, 2014. arXiv: 1312.6199[cs].

[11] N. Papernot, P. McDaniel, and I. Goodfellow. *Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples*. May 23, 2016. arXiv: `1605.07277[cs]`.

[12] I. J. Goodfellow, J. Shlens, and C. Szegedy. *Explaining and Harnessing Adversarial Examples*. Mar. 20, 2015. arXiv: `1412.6572[cs,stat]`.

[13] A. Kurakin, I. Goodfellow, and S. Bengio. *Adversarial Machine Learning at Scale*. Feb. 10, 2017. arXiv: `1611.01236[cs,stat]`.

[14] C. Ciliberto, M. Herbster, A. D. Ialongo, M. Pontil, A. Rocchetto, S. Severini, and L. Wossnig. "Quantum machine learning: a classical perspective." In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 474.2209 (Jan. 2018), p. 20170551. ISSN: 1364-5021, 1471-2946. DOI: `10.1098/rspa.2017.0551`.

[15] B. Schumacher. "Quantum Coding." In: *Physical Review A* 51.4 (Apr. 1, 1995), pp. 2738–2747. ISSN: 1050-2947, 1094-1622. DOI: `10.1103/PhysRevA.51.2738`.

[16] P. a. M. Dirac. "A New Notation for Quantum Mechanics." In: *Mathematical Proceedings of the Cambridge Philosophical Society* 35.3 (July 1939), pp. 416–418. ISSN: 1469-8064, 0305-0041. DOI: `10.1017/S0305004100021162`.

[17] M. Born. "Quantenmechanik der Stoßvorgänge." In: *Zeitschrift für Physik* 38.11 (Nov. 1, 1926), pp. 803–827. ISSN: 0044-3328. DOI: `10.1007/BF01397184`.

[18] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Higher Education from Cambridge University Press. ISBN: 9780511976667 Publisher: Cambridge University Press. Dec. 9, 2010. DOI: `10.1017/CBO9780511976667`. URL: `https://www.cambridge.org/highereducation/books/quantum-computation-and-quantum-information/01E10196D0A682A6AEFFEA52D53BE9AE` (visited on 03/28/2024).

[19] F. Bloch. "Nuclear Induction." In: *Physical Review* 70.7 (Oct. 1, 1946), pp. 460–474. ISSN: 0031-899X. DOI: `10.1103/PhysRev.70.460`.