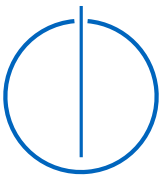
SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

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

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 computes have become very powerful, they still struggle to compute 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. This algorithm 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 algorithms, they still can not be executed in current quantum computers due to noise [6]. This noise occurs from the fact that 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 required 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

- Introduce the qubit 2.1

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

- Introduce superposition - Introuce Bloch sphere - Introduce entanglement - Introduce quantum gates - Introduce quantum circuits - Introduce quantum algorithms

i. Introduce the required quantum concepts for the reader to understand noise in quantum computing.

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

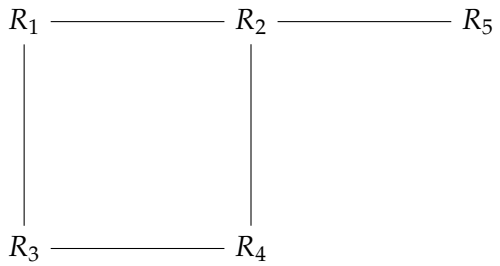


Figure 4.1: An example for a simple drawing.

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

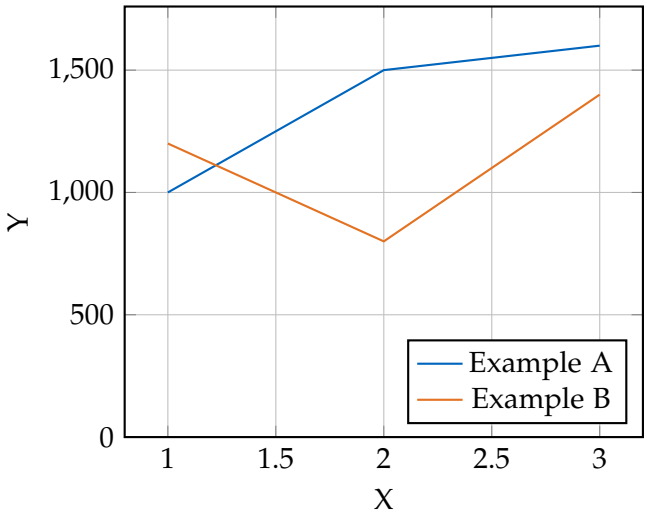


Figure 4.2: An example for a simple plot.

```
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

List of Tables

Bibliography

[1] E. National Academies of Sciences and Medicine. *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.