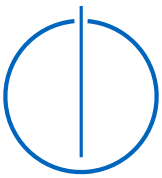
SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

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

- Quantum mechanics explained, jump to quantum computing. (Quantum Computing: Progress and Prospects) [1] - Quantum algorithms are better for specific tasks. (Quantum Advantage papers) [2, 3, 4] - Shor's algorithm breaks current asymmetric cryptographic implementations. (Shor) [2]

1.1 Motivation

- These quantum algorithms can't be run due to noise. (NISQ) [5] - Error mitigation and fault tolerance (Quantum computing) [6], improving hw, is important and still being researched. (NISQ) [5] - Intro to machine learning, its uses and widespread popularity. Presents possible risks and challenges. (On the opportunities and risks of foundational models) [7] - What is QML and why are people doing it? (Machine Learning with Quantum Computers) [8]

- Adversarial attacks can be crafted to force a ML model to missclassify an input. (Intriguing properties of NN) [9] - Adversarial attacks can be transferred in between models. (Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples) [10] - Adversarial training as a defense for adversarial attacks enhancing generalization. (Explaining and harnessing | intriguing properties of NN) [11, 9] - Present the limitations of adversarial training in large-scale systems. (AML at scale) [12] - Describe the potential uses of noise in QML as a potential increase in robustness. (QML a classical perspective) [13]

TODO: - Could we claim that noise in QML might also be a defense against data poisoning attacks? (AML at scale) [12]

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

2.1 Fundamentals of Quantum Computing

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

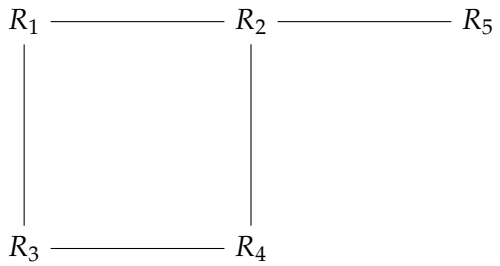


Figure 4.1: An example for a simple drawing.

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

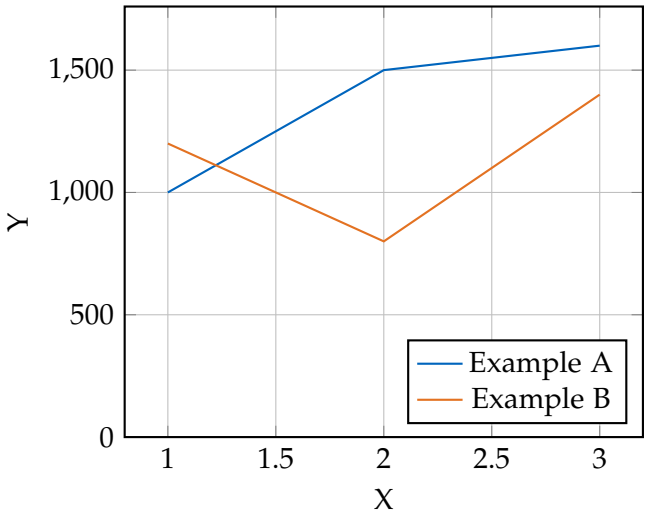


Figure 4.2: An example for a simple plot.

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

Figure 4.3: An example for a source code listing.

Abbreviations

TUM Technical University of Munich

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] 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].

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

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

[8] 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.

[9] 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].

[10] 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].

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

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

[13] 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.