VeriQR: A Robustness Verification Tool for Quantum Machine Learning Models

Yanling Lin[1,2], Ji Guan[2](✉)[⋆], Wang Fang[2], Mingsheng Ying[3], Zhaofeng Su[1]

[1] University of Science and Technology of China, Hefei 230026, China
[2] Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[3] Centre for Quantum Software and Information, University of Technology Sydney, NSW 2007, Australia

Adversarial noise attacks present a significant threat to quantum machine learning (QML) models, similar to their classical counterparts. This is especially true in the current Noisy Intermediate-Scale Quantum era, where noise is unavoidable. Therefore, it is essential to ensure the robustness of QML models before their deployment. To address this challenge, we introduce *VeriQR*, the first tool designed specifically for formally verifying and improving the robustness of QML models, to the best of our knowledge. This tool mimics real-world quantum hardware's noisy impacts by incorporating random noise to formally validate a QML model's robustness. *VeriQR* supports exact (sound and complete) algorithms for both local and global robustness verification. For enhanced efficiency, it implements an under-approximate (complete) algorithm and a tensor network-based algorithm to verify local and global robustness, respectively. As a formal verification tool, *VeriQR* can detect adversarial examples and utilize them for further analysis and to enhance the local robustness through adversarial training, as demonstrated by experiments on real-world quantum machine learning models. Moreover, it permits users to incorporate customized noise. Based on this feature, we assess *VeriQR* using various real-world examples, and experimental outcomes confirm that the addition of specific quantum noise can enhance the global robustness of QML models. These processes are made accessible through a user-friendly graphical interface provided by *VeriQR*, catering to general users without requiring a deep understanding of the counter-intuitive probabilistic nature of quantum computing.

VeriQR repository is available at https://github.com/Veri-Q/VeriQR.
Full Version: ArXiv:2407.13533

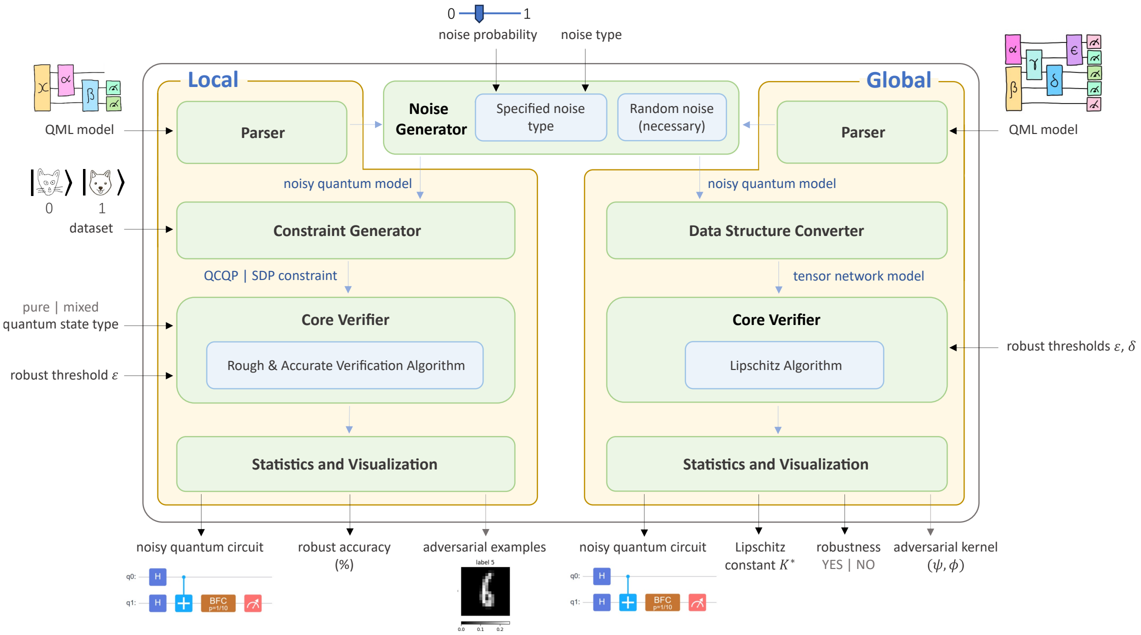

Fig. 1: An overview of the architecture of *VeriQR*.

[⋆] guanji1992@gmail.com