PQC Function Evaluation

Carnegie Vacation Scholarship

David Amorim

Week 4
(22/07/2024 - 26/07/2024)

Table of Contents

Preliminary Definitions

- Consider a computational basis state, $|j\rangle$, in a p-qubit register:

$$|j\rangle = \bigotimes_{\alpha=0}^{p-1} |j_\alpha\rangle \,, \qquad |j_\alpha\rangle \in \{|0\rangle\,, |1\rangle\} \tag{1}$$

- Define

$$j_\alpha \equiv \begin{cases} 0 & \text{if } |j_\alpha\rangle = |0\rangle \\ 1 & \text{if } |j_\alpha\rangle = |1\rangle \end{cases} \tag{2}$$

- Two digitally encoded binary numbers can be associated with $|j\rangle$:

$$j \equiv \sum_{\alpha=0}^{p-1} j_\alpha 2^\alpha \qquad (0 \le j \le 2^p - 1), \tag{3}$$

$$j' \equiv \sum_{\alpha=0}^{p-1} j_\alpha 2^{\alpha-p} \qquad (0 \le j' \le 1) \tag{4}$$

Preliminary Definitions

- Consider an n-qubit input register and an m-qubit target register, denoted with subscripts i and t, respectively
- A computational basis state of the combined system, $|k\rangle_{i+t}$, can be decomposed into

$$|k\rangle_{i+t} = |j\rangle_i \otimes |l\rangle_t \,, \tag{5}$$

for computational basis states $|j\rangle_i$, $|l\rangle_t$ of the two registers

- Define

$$\text{input}(|k\rangle_{i+t}) \equiv |j\rangle_i \tag{6}$$

$$\text{target}(|k\rangle_{i+t}) \equiv |l\rangle_t \tag{7}$$

$$\tag{8}$$

- A general state of the two-register system is then

$$|z\rangle = \sum_{k=0}^{2^{n+m}-1} z_k \, |k\rangle_{i+t} \tag{9}$$

Preliminary Definitions

- For training in superposition, the two-register target state is

$$|y\rangle = \sum_{j=0}^{2^n-1} \frac{1}{\sqrt{2^n}} |j\rangle_i \, |\Psi'(j)\rangle_t \equiv \sum_{k=0}^{2^{n+m}-1} y_k \, |k\rangle_{i+t} \, , \tag{10}$$

with y_k

Preliminary Definitions

-

Improving WIM

- Recall the definition of WIM (WeIghted Mismatch):

$$\mathrm{WIM}(x, y) = \left| 1 - \sum_{k=0}^{2^{n+m}-1} \tilde{w}_k x_k y_k \right|, \tag{11}$$

  where
  - $|x\rangle = \sum_{k=0}^{2^{n+m}-1} x_k |k\rangle$ is the output state produced by the QCNN,
  - $|y\rangle = \sum_{k=0}^{2^{n+m}-1} y_k |k\rangle$ is the target state,
  - $\tilde{w}_k \in \mathbb{R}_+$ are weighting factors
-