PQC Function Evaluation

Carnegie Vacation Scholarship

David Amorim

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

Table of Contents

Aims

- Continue work on WIM (develop a distance measure taking into account Ψ, e.g. $w_j \sim L_\Psi(x, y) = \sum_j 2^{j-m}|x_j - y_j|$)
- Change IL structure (all-to-all...)
- Keep parameters fixed for each layer

Table of Contents

Keeping Parameters Fixed

- Implemented the option to fix parameters for each layer type
- This means that each IL, neighbour-to-neighbour CL, and all-to-all CL use the same set of parameters
- This reduces the overall number of parameters to $n + m + \frac{1}{2} m * (m-1)$

ADDED FUNCTIONALITY, TEST !!! (does it make a difference?) – definitely works in terms of parameters – not sure yet if makes a difference w.r.t. mismatch MAKES PERFORMANCE WORSE – should at least speed things up? but apparently not ... DOES NOT SPEED THINGS UP...

Table of Contents

Improving IL Structure

– added shifts to successive ILs (test effects..): seems to give slight improvements! – added functionality for AA layers (test later)..

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 $|j\rangle$:

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

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

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 $y_k = 0$ if target$(|k\rangle_{i+t})$

Preliminary Definitions

- FIND GOOD NOTATION FOR ALL THIS !!!
- THINK ABOUT THIS ALL MORE DEEPLY! MAYBE HAVE TO SWITCH TO WEIGHTED L1/2 LOSS INSTEAD? (WILL)

Improving WIM

- Recall the definition of WIM (WeIghted Mismatch):

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

  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
- .... calculate w_k
- $\tilde{w}$