A QCNN for Quantum State Preparation

Carnegie Vacation Scholarship

David Amorim

Weeks 7-8
(12/08/2024 - 23/08/2024)

Aims for the Week

The following aims were set at the last meeting (14/08/2024):

New Phase Encoding Approach

Investigate a new approach to phase encoding using linear piecewise phase functions without explicit function evaluation.

Handover

Hand over the slides, documentation, code and the poster for the Carnegie Trust.

Table of Contents

Preliminaries

- Consider an n-qubit register with computational basis states $|j\rangle = |j_0 j_1 ... j_{n-1}\rangle$ representing n-bit strings
- Let p of the register qubits be precision qubits so that

$$j = \sum_{k=0}^{n-1} j_k 2^{k-p} \tag{1}$$

- Now consider a phase function Ψ over the domain $\mathcal{D} = \{j\}$ and construct an M-fold partition sub-domains $\mathcal{D}_u$:

$$\mathcal{D} = \bigcup_{u=1}^{M} \mathcal{D}_u, \quad \mathcal{D}_u \cap \mathcal{D}_v = \emptyset, \tag{2}$$

- Take $M = 2^m$ with $m \leq n$ and let the sub-domains be equally sized ($|\mathcal{D}_u| = |\mathcal{D}_v|$)

Preliminaries

Aim

Construct an appropriate operator to transform

$$|j\rangle \mapsto e^{i\Psi(j)}\,|j\rangle \tag{3}$$

via the linear piecewise approximation

$$|j\rangle \mapsto e^{i(\alpha_u j+\beta_u)}\,|j\rangle \quad (j \in \mathcal{D}_u) \tag{4}$$

Initial Remarks

- The 2^m pairs of coefficients (α_u, β_u) require 2^m independent operators $\hat{O}_u$ to implement the mapping $|j\rangle \mapsto e^{i(\alpha_u j+\beta_u)} |j\rangle$
- Each operator $\hat{O}_u$ will generally involve controlled rotations on all n qubits in the register, with m qubits acting as controls
- Thus, the expected lower bound for controlled rotations is $\sim \Omega(2^m n)$
- Note that m-controlled operations require $\Theta(m^2)$ CNOT gates [*Barenco 1995*[1], Cor 7.6] or $\Theta(m)$ CNOT gates when using ancillae [*Barenco 1995*, Cor 7.12]
- To avoid this additional factor in the gate count and meet the lower bound only single-controlled operations will be employed, leading to a more complex control architecture

[1] `https://arxiv.org/pdf/quant-ph/9503016`

Constructing $\hat{O}_u$

- Consider the single-qubit operators

$$\hat{P}^{(k)}(\varphi) = \begin{pmatrix} e^{i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix}, \quad \hat{R}^{(k)}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \tag{5}$$

  each acting on the kth qubit
- Now define

$$\hat{U}_u^{(k)} \equiv \hat{P}^{(k)}(\beta_u/n)\hat{R}^{(k)}(\alpha_u 2^{k-p}) \tag{6}$$

- Then

$$\hat{O}_u \equiv \bigotimes_{k=0}^{n-1} \hat{U}_u^{(k)} \tag{7}$$

  transforms

$$|j\rangle \mapsto \exp\left[i\left(\sum_{k=0}^{n-1} \alpha_u j_k 2^{k-p} + \beta_u\right)\right]|j\rangle = e^{i(\alpha_u j + \beta_u)}|j\rangle \tag{8}$$

The Control Structure

- It is straight-forward to construct $\hat{O}_u$ for each of the sub-domains $\mathcal{D}_u$
- More challenging is applying the correct $\hat{O}_u$ based on the sub-domain corresponding to each $|j\rangle$, which requires controlling on the first m qubits
- In order to achieve this with only single-controlled operations a control structure similar to *Barenco 1995* Lemmas 6.1, 7.1 is chosen
- This involves defining 2^m auxiliary operators $\hat{V}_q^{(k)}$ which give the $\hat{U}_u^{(k)}$ when multiplied in appropriate combinations
- Since a product of rotation operators corresponds to a sum of rotation angles, the $\hat{V}_q^{(k)}$ can be constructed by solving the appropriate linear system in the $\hat{U}_u^{(k)}$
- The following two slides show examples of the control structure for 'target qubits', i.e. the $n-m$ qubits that do not act as controls

The Case $m = 2$ $(M = 4)$

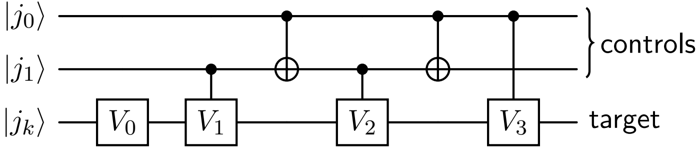

Figure 1: Control structure for $m = 2$ $(M = 4)$ with $2 \leq k < n$. The number of controlled operations is $2^{m+1} - 3 = 5$

$(j_0 j_1)$	Operation	Equiv. $\hat{U}$	$(j_0 j_1)$	Operation	Equiv. $\hat{U}$
(00)	$\hat{V}_0$	$\hat{U}_0$	(10)	$\hat{V}_3 \hat{V}_2 \hat{V}_0$	$\hat{U}_2$
(01)	$\hat{V}_2 \hat{V}_1 \hat{V}_0$	$\hat{U}_1$	(11)	$\hat{V}_3 \hat{V}_1 \hat{V}_0$	$\hat{U}_3$

Table 1: Operations applied to $|j_k\rangle$ for various control states

The Case $m = 3$ ($M = 8$)

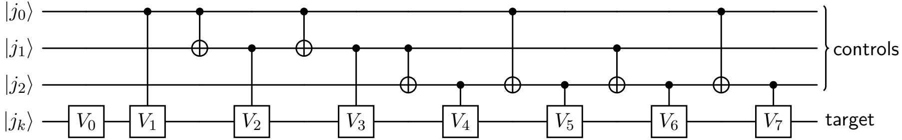

Figure 2: Control structure for $m = 3$ ($M = 8$) with $3 \leq k < n$. The number of controlled operations is $2^{m+1} - 3 = 13$

$(j_0 j_1 j_2)$	Operation	Equiv. $\hat{U}$	$(j_0 j_1 j_2)$	Operation	Equiv. $\hat{U}$
(000)	$\hat{V}_0$	$\hat{U}_0$	(100)	$\hat{V}_6\hat{V}_5\hat{V}_2\hat{V}_1\hat{V}_0$	$\hat{U}_4$
(001)	$\hat{V}_7\hat{V}_4\hat{V}_0$	$\hat{U}_1$	(101)	$\hat{V}_7\hat{V}_4\hat{V}_2\hat{V}_1\hat{V}_0$	$\hat{U}_5$
(010)	$\hat{V}_5\hat{V}_4\hat{V}_2\hat{V}_0$	$\hat{U}_2$	(110)	$\hat{V}_6\hat{V}_4\hat{V}_3\hat{V}_1\hat{V}_0$	$\hat{U}_6$
(011)	$\hat{V}_7\hat{V}_6\hat{V}_3\hat{V}_2\hat{V}_0$	$\hat{U}_3$	(111)	$\hat{V}_7\hat{V}_5\hat{V}_3\hat{V}_1\hat{V}_0$	$\hat{U}_7$

Table 2: Operations applied to $|j_k\rangle$ for various control states

The Control Structure

- The control structure required to apply the appropriate $\hat{U}_u^{(k)}$ to the k-th target qubit requires $2^{m+1} - 3$ CNOT gates
- As there are $n - m$ target qubits this brings the CNOT count due to the targets to $(n - m)(2^{m+1} - 3)$
- Handling the control structure for the m 'control qubits' requires slightly more care as the operator to be applied to the l-th control qubit is conditional on $|j_l\rangle$ itself
- This problem can be addressed by introducing an ancilla $|0\rangle_a$ and following the procedure:
  a. Apply a CNOT gate to the ancilla, controlled by $|j_l\rangle$
  b. Apply the same control structure as for the target qubits, with the ancilla as the target
  c. Apply a SWAP gate between the ancilla and $|j_l\rangle$
  d. Apply a CNOT gate to the ancilla, controlled by $|j_l\rangle$
- The final step clears the ancilla, allowing it to be re-used for all m controls

Gate Cost

- Thus, encoding the phase on each control qubit requires the same structure as before but with an additional 5 CNOT gates per control qubit (3 of are part of the SWAP)
- The m control qubits thus require $m2^{m+2}$ CNOT gates in addition to the $(n-m)(2^{m+1}-3)$ CNOTs for the targets

Overall Complexity

The CNOT cost of the algorithm presented here is

$$C(n,m) = 2^{m+1}(n+m) - 3(n-m), \quad (9)$$

corresponding to the lower bound $\mathcal{O}(n2^m)$ on the complexity

Additional Remarks

- Generally, when applying a controlled phase gate, the resulting phase shift cannot be unambiguously attributed to either the control or the target
- Here, this does not pose an issue as only the overall phase of the n-qubit register matters
- *Barenco 1995* omits the explicit construction of the control structure for general m, only pointing towards the generalisation of the cases $m = 2, 3$ shown here
- Circuit structure may be simplified by using SWAP gates and the ancilla for all n qubits, at the cost of incurring $6(n - m)$ additional CNOT gates

Comparison with the Previous Approach

- The phase encoding in *Hayes 2023*[2] uses n_l label qubits (with $2^{n_l} = M$) as well as n_c coefficient qubits
- The overall gate cost has contributions from the label operation ($\mathcal{O}(2^{n_l} n)$), the addition and multiplication operations ($\mathcal{O}(n^2 + n_c^2)$), as well as loading the coefficients ($\mathcal{O}(n_c 2^{n_l} n_l^2)$):

$$C_{\text{Hayes}}(n, n_c, n_l) = \mathcal{O}(n^2 + 2^{n_l}[n + n_l^2 n_c] + n_c^2) \tag{10}$$

Complexity Comparison

The new approach results in a quadratic complexity reduction in n, from $\mathcal{O}(n^2)$ to $\mathcal{O}(n)$. The $\mathcal{O}(Mn)$ term remains while the number of ancillae is reduced from $n_c + n_l$ to 1

[2] https://arxiv.org/pdf/2306.11073

Table of Contents

Handover

The code, documentation, slides, and poster are all available on GitHub:

`https://github.com/david-f-amorim/PQC_function_evaluation`

- The source code is found in the directory `pqcprep`
- The slides and poster are found in the directory `slides`
- The documentation is hosted externally here, which is also linked on GitHub