Abstract

Quantum cloning

The task is to take a quantum state and produce two (perfect) ‘clones’ of it (deterministically). The no-cloning theorem is a pillar of quantum mechanics and forbids this. However, if the ‘perfectness’ requirement of the cloned states is relaxed, we get approximate quantum cloning [1]. The ‘quality’ of clones is measured relative to local fidelity:

\[ F_l(\rho_{ideal}, \sigma_{clone}) = \left( \text{Tr} \sqrt{\sqrt{\rho_{ideal}} \sigma_{clone} \sqrt{\rho_{ideal}}} \right)^2 \]

Approximate cloning machines (unitaries: \(U_{clone}\)) come in two forms:

- **Universal:** E.g. clone all single qubit states.
- **State-dependent:** Restricted to specific families of states, \(S\) for example phase-covariant states:

\[ \sigma(\alpha) = \frac{1}{2} (|0\rangle + e^{i\alpha}|1\rangle)|0\rangle + \frac{1}{2} (|0\rangle + e^{i\alpha}|1\rangle)|1\rangle \]

Optimal achievable fidelity for clones [2]:

\[ F^U_{L,\text{opt}} = 5/6 \approx 0.833 \]

Optimal fidelity: \(F_{PC}^{\text{opt}} \approx 0.85 > 5/6\)

Quantum coin flipping protocols

Coin flipping is a cryptographic primitive that allows two parties (without mutual trust) to remotely agree on a random bit (\(y\)) without either party being able to bias the coin in its favour. A “biased coin” has one outcome (Heads/Tails) being more likely

Alice \[\begin{array}{c} (q, c) \end{array}\] Bob \[\begin{array}{c} a \end{array}\]

Alice and Bob may exchange quantum (\(q\)) and/or classical (\(c\)) information to perform the (strong) coin flipping protocol. Alice and Bob both contribute a bit, \(a\) or \(b\) respectively to the final coin.

Quantum coin flipping states:

Many coin flipping protocols use the following set of quantum states (fixed overlap states) to perform the protocol:

\[ \{\phi_{\alpha, \beta}\} = \{\phi_{\alpha, 0} = \cos \phi |0\rangle + (-1)^\alpha \sin \phi |1\rangle, \phi_{\alpha, 1} = \sin \phi |0\rangle + (-1)^{\beta \oplus \alpha} \cos \phi |1\rangle\} \]

The protocol of Aharonov et. al. [5]:

In this protocol, Alice utilises all 4 of the above states with the angle \(\phi \approx \frac{\pi}{2}\). She encodes her contribution to the coin (her bit, \(a\)) in the ‘basis’ information of the above states.

A dishonest party (Bob) can bias if learns the basis (i.e. he learns Alice’s bit, \(a\)).

Variational quantum cloning

Variational Quantum Cloning (VarQlone) is a variational quantum algorithm [2], suitable for NISQ computers and can be used to find short depth circuits for approximate cloning machines. We also extend to \(M \rightarrow N\) cloning, taking \(M\) copies of the input state and producing \(N\) output clones.

Cost functions:

We use local and global cost functions which serve different purposes, e.g. a local cost:

\[ C_l(\theta) := 1 - \frac{1}{N} \sum_{j=1}^{N} \left| \text{Tr} \left( \hat{V}_j (|\psi\rangle \langle \psi|) \rho_{ideal} \right) \right| \]

Faithfulness:

The cost functions are faithful - closeness to minimum implies closeness of each clone (\(j\)) to \(\rho_{ideal}\) (in some metric):

\[ |C_l(\theta) - C_l(\theta^*)| \leq \epsilon \rightarrow D(\rho_{ideal}, \rho_{opt}) \leq f(\epsilon) \]

\(\forall |\psi\rangle \in S, \forall j\)

Variational quantum cryptanalysis

Using VarQlone, we can build constructive attacks on quantum protocols whose security may reduce to quantum cloning (for example BB84 QKD, see Figure).

Eve can build an approximate cloning machine to attack Alice & Bobs communication. Eve’s goal is to create 2 clones of Alice’s state to gain information, using ancillary states, \(E^*\). She can achieve better performance using a state-dependent cloning if she has side information.

Explicitly, we derive a cloning based attack that Bob can implement coin flipping protocols to bias the coin. As an explicit example, we can prove:

**Theorem:** Using a local VarQlone cloning attack on the protocol, \(P\), Bob can achieve a bias:

\[ \varepsilon_{P, \text{VarQlone}} \approx 0.24 \]

Numerical results

VQC learning to find a ‘good’ circuit structure using the gate pool. Each iteration corresponds to a different circuit, whose parameters are then optimised by gradient descent using Adam’. Example shown for phase covariant cloning. After 50 iterations, a circuit has been found which achieves the cost function minimum.

Cloning phase covariant states in a BB84 like protocol. One clone goes to Bob and the other to Eve. (a) ‘Ideal’ circuit, (a, c) VQC learned circuits. VQC learns circuits which saturate theoretical optimal fidelity in simulator (QVM) and display higher fidelity on Rigetti Hardware (QPU).

Cost functions which serve different purposes, e.g. a local cost:

\[ C_l(\theta) := 1 - \frac{1}{N} \sum_{j=1}^{N} \left| \text{Tr} \left( \hat{V}_j (|\psi\rangle \langle \psi|) \rho_{ideal} \right) \right| \]

Faithfulness:

The cost functions are faithful - closeness to minimum implies closeness of each clone (\(j\)) to \(\rho_{ideal}\) (in some metric):

\[ |C_l(\theta) - C_l(\theta^*)| \leq \epsilon \rightarrow D(\rho_{ideal}, \rho_{opt}) \leq f(\epsilon) \]

\(\forall |\psi\rangle \in S, \forall j\)

**References:**