Mirror modular cloning and fast quantum associative retrieval

M. Cristina Diamantini

Nips laboratory, INFN and Department of Physics and Geology, University of Perugia

Coll: **Carlo A. Trugenberger, SwissScientific**

arXiv:2206.01644

ICNFP 2022

Kolymbari, August 30, 2022 - September 11, 2022

Associative Memory

traditional computers: retrieval of information requires precise knowledge of the memory address

associative memories:

- recall of information is done on the basis of a partial knowledge of its content
- not based on the knowledge of the storage location

person number 12345
that I met in my life

associative memory

incomplete or corrupetd inputs

- v_i^{μ} $\equiv$ p binary patterns containing n bits of information (i =1…n ; μ = 1….p) and take value 0,1

- when a new pattern m_i is presented the memory recalls the stored pattern v_i^{λ} that more strongly resembles n_i $\Longrightarrow$ $H_{\mu} = \sum_I (m_i - v_i^{\mu})^2$ $\equiv$ Hamming distance, minimal for μ=λ

- $S_i = 2m_i - 1$; $\sigma_i = 2 v_i - 1$ that take value ± 1

- $H_{\mu} \Longrightarrow \sum_I \sigma_i^{\mu} s_i + \text{const}$ minimization of the scalar product

- stored patterns are attractors for the network dynamics

paradigmatic example: **Hopfield model**:

- $\alpha = p/n < 0.138$ the network works as an associative memory; stored patterns are attractors for the dynamics
- $\alpha = p/n > 0.138$ phase transition to a spin glass, memory is lost

in general maximum number of stored patterns $p_{max} = O(n)$

Quantum memory

quantum memory: quantum-mechanical version of ordinary computer memory

- classical memory stores information as binary states
- quantum memory stores a quantum state for later retrieval

No-Cloning Theorem:

Theorem: Given a qubit in an arbitrary unknown state $|\phi_1\rangle$ and another qubit in an initial state $|\phi_2\rangle$, there does not exist any unitary operator U (i.e., any quantum mecahnical evolution) such that

$$U(|\phi_1\rangle \otimes |\phi_2\rangle) = e^{i\chi}|\phi_1\rangle \otimes |\phi_1\rangle$$

for all possible input $|\phi_1\rangle$.

(W. Wootters and W. Zurek, Nature 299, 802 (1982))

base of quantum cryptography

- error corrections (Shor 1995 Kitaev 1997)
- if memory state is measured memory state is lost

still possible that we can copy a quantum state approximately or probabilistically

Probabilistic Quantum Associative Memory

(C.A. Trugenberger, Phys.Rev. Lett. 89, 067901 (2001); Quantum Inf. Process 1, 471 (2002))

- store p binary patterns of n bits in a quantum superposition of the corresponding subset of the computational basis of n qubits → number of binary patterns that can be stored is exponential in the number n of qubits, $\mathbf{p_{max} = O(2^n)}$

- all binary patterns that can be formed with n bits can be stored → **optimal**

- information retrieval mechanism: memory quantum state rotated within the subspace defined by the stored patterns ⇒ amplitudes peaked on the stored patterns closest in Hamming distance to the input

- measurement of the rotated memory quantum state provides the output pattern, state collapse ⚠

- original retrieval algorithm, threshold T to classify an input as not recognized ⚠

Quantum Associative Memory in HEP Track Pattern Recognition

Illya Shapoval[1,*] and *Paolo* Calafiura[1,**]

[1]Lawrence Berkeley National Laboratory

Abstract. We have entered the Noisy Intermediate-Scale Quantum Era. A plethora of quantum processor prototypes allow evaluation of potential of the Quantum Computing paradigm in applications to pressing computational problems of the future. Growing data input rates and detector resolution foreseen in High-Energy LHC (2030s) experiments expose the often high time and/or space complexity of classical algorithms. Quantum algorithms can potentially become the lower-complexity alternatives in such cases. In this work we discuss the potential of Quantum Associative Memory (QuAM) in the context of LHC data triggering. We examine the practical limits of storage capacity, as well as store and recall errorless efficiency, from the viewpoints of the state-of-the-art IBM quantum processors and LHC real-time charged track pattern recognition requirements. We present a software prototype implementation of the QuAM protocols and analyze the topological limitations for porting the simplest QuAM instances to the public IBM 5Q and 14Q cloud-based superconducting chips.

- storage: Trugenberger’s algorithm
- retrieval: Grover’s based algorithm

(arXiv:1902.004982)

Mirror modular cloning

(C.A. Trugenberger and MCD, arXiv: 2206.01644)

- for quantum associative memories perfect cloning of a single state is **not necessary**

- cloning up to a global **NOT operation** sufficient
  state → mirror image

- **mirror modular cloning** performed by a (2×2) unitary transformation that depends on a single parameter of the state

- **exponentially faster** than the address-based Grover retrieval albeit at the price of possible retrieval errors due to its probabilistic nature

Storage

$$|M\rangle = \frac{1}{\sqrt{p}} \sum_{i=1}^{p} |p^i\rangle$$

NOT$|p_i\rangle = |\bar{p}_i\rangle$ $\Rightarrow$

$$|\bar{M}\rangle = \frac{1}{\sqrt{p}} \sum_{i=1}^{p} |\bar{p}^i\rangle$$

quantum memory states superposition on n entangled qubits; encodes p binary patterns $|p^i\rangle = |p^i_1 \ldots p^i_n\rangle$ of n qubits and their mirrors

- measure $< M|\bar{M} >$ (Stolze and Zenchuk, Phys.Lett. A383, 125978 (2019))
- add a normalized ancillary register of *n* qubits prepared in state $|\Sigma\rangle$ and a further ancilla qubit in state $|0\rangle$
- if ∃ a 2x2 unitary matrix U :

$$U(|M\rangle|\Sigma\rangle|0\rangle) = \sqrt{\gamma}|M\rangle|M\rangle|0\rangle + \sqrt{\bar{\gamma}}|M\rangle|\bar{M}\rangle|1\rangle \quad \Rightarrow$$

$$U\left(|\bar{M}\rangle|\Sigma\rangle|0\rangle\right) = \sqrt{\bar{\gamma}}|\bar{M}\rangle|\bar{M}\rangle|0\rangle + \sqrt{\gamma}|\bar{M}\rangle|M\rangle|1\rangle$$

$\Rightarrow$ **U perfectly clones the memory state up to a mirror modular transformation**
$|M>$ with probability γ
$|\bar{M}>$ with probability $\bar{\gamma}$
the two results being distinguished by the value of the ancilla qubit

theorem: given two sets of states $|\psi_i\rangle$, $|\varphi_i\rangle$ such that $\langle\psi_i|\psi_j\rangle = \langle\varphi_i|\varphi_j\rangle$ for all i, j = 1 . . . m ⇒ ∃ unitary transformation U such that $U|\psi_i\rangle = |\varphi_i\rangle$ (L.M. Duan and G.C. Guo, Phys.Rev. Lett 80 4999 (1998))

$|M>|\Sigma>|0>$
$|\bar{M}>|\Sigma>|0>$ ⇒ $U(|M\rangle|\Sigma\rangle|0\rangle)$, $U\left(|\bar{M}\rangle|\Sigma\rangle|0\rangle\right)$ ∃ U if

$$\gamma + \bar{\gamma} = 1\,, \qquad \sqrt{\gamma\bar{\gamma}} = \frac{1}{\langle M|\bar{M}\rangle + \langle\bar{M}|M\rangle}\,.$$

one parameter γ

Retrieval

- add: n qubit register with an input pattern $|I\rangle = |i_1 \ldots i_n\rangle$;
  b control qubits prepared in state $|O\rangle = |c_1 \ldots c_b\rangle = |0, \ldots, 0\rangle$

$$|\psi_0\rangle = \sqrt{\gamma}|I\rangle|M\rangle|O\rangle|0\rangle + \sqrt{\bar{\gamma}}|I\rangle|\overline{M}\rangle|O\rangle|1\rangle$$

- measure the **Hamming distance $d_H(i,p^k)$** between the input and the stored pattern or the **Hamming distance $\bar{d}_H(i,p^k)$, $\bar{d}_H = n - d_H$** between the input and the mirror of the stored pattern
- measure the ancilla qubit and amplitude amplification to rotate onto the "good" subspace
- measure memory register, two possibilities:

1. closest (in Hamming distance) pattern p_k
2. most distant pattern p_k

- probabilty:

$$P\left(i, p^k\right) = \frac{1}{p}\cos^{2b}\left(\frac{\pi}{2n} d_H\left(i, p^k\right)\right)$$

it does not matter if one obtains the closest or the most distant pattern

Complexity

mainly influenced by the amplitude amplification step:
number of applications C of the basic amplitude amplification rotation is given by the square root of the inverse probability of measuring the “good” subspace

$$C = \sqrt{\frac{p}{\sum_{k=1}^{p} \cos^{2b}\left(\frac{\pi}{2n} d_H\left(i, p^k\right)\right)}}$$

- polynomial in n
- independent on p, only pattern distribution matters
- depends on accuracy parameter b

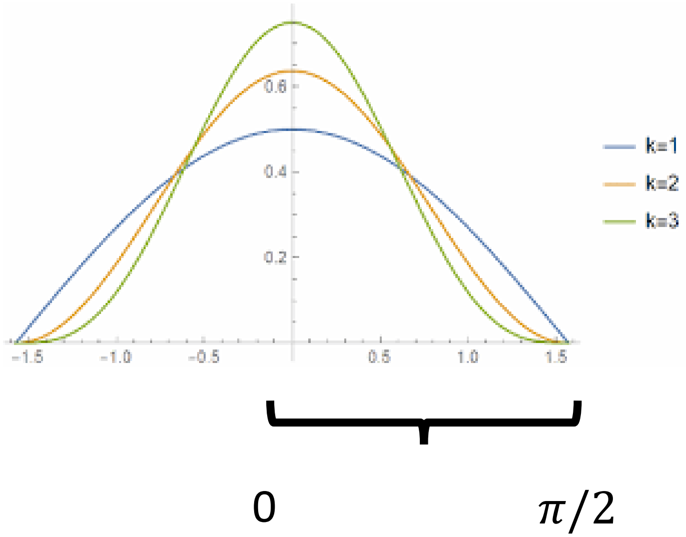
Grover’s algorith complexity $\sqrt{N} \Rightarrow$ **exponential speed up but probabilistic** need to estimate:

- amplitude estimation, C repetitions of the algorithm
- compute C for some typical inputs and repeat amplitude amplification a few times varying the number of oracle calls around this initial estimate

approximately uniform pattern distribution

$$C \approx n(\pi b)^{1/4}$$

trade-off between complexity and accuracy:
higher b ⇒ retrieval probability peaked on the correct pattern
higher b⇒ higher computational complexity



$$\frac{\cos^k x}{\int_{-\pi/2}^{\pi/2} \cos^k(x)\, dx}$$

k= 2b

Conclusions

- for quantum associative memories perfect cloning of a single state is **not necessary** cloning up to a global **NOT operation** sufficient
- **exponentially faster** than the address-based Grover retrieval

THANK YOU!!!!

Storage

- single-qubit gates

  NOT = σ^1 ; Hadamard H = $1/\sqrt{2}$ $(\sigma^1 + \sigma^3)$; σ^i Pauli matrices

- two-qubits gates

  XOR (CNOT) = diag (I, σ^1) performs a NOT on the second qubit iff the first one is in state $|1\rangle$

$$CS^i = |0\rangle\langle 0| \otimes 1 + |1\rangle\langle 1| \otimes S^i \ ,$$

$$S^i = \begin{pmatrix} \sqrt{\frac{i-1}{i}} & \frac{1}{\sqrt{i}} \\ \frac{-1}{\sqrt{i}} & \sqrt{\frac{i-1}{i}} \end{pmatrix} \ ,$$

i = 1,...,p ;
two-qubit controlled gates
central operation of the storing algorithm
separates out the new pattern to be stored

- three-qubits gate

  Toffoli 2XOR = diag (1, 1, σ^1) performs a NOT on the third qubit iff the first two are both in $|1\rangle$

- nXOR = generalization to n control qubits