Perfect probabilistic storing and retrieving of unitary channels

Michal Sedlák
Institute of Physics
Slovak Academy of Sciences
Dúbravská cesta 9
845 11 Bratislava, Slovakia
michal.sedlak@savba.sk

Alessandro Bisio
QUIT group
Dipartimento di Fisica
INFN Sezione di Pavia
via Bassi 6, 27100 Paviav
Italy

Mário Ziman
Institute of Physics
Slovak Academy of Sciences
Dúbravská cesta 9
845 11 Bratislava, Slovakia

Any sequence of quantum gates on a set of qubits defines a multipartite unitary transformation. These sequences may correspond to some parts of a quantum computation or they may be used to encode classical/quantum information (e.g. in private quantum channels). If we have only limited access to such a unitary transformation, we may want to store it into a quantum memory and later perfectly retrieve it. Thus, once we cannot use the unitary transformation directly anymore, we could still apply it to any state with the help of the footprint kept in the quantum memory. This can be useful for speeding up some calculations or as an attack for process based quantum key distribution protocol or a communication scheme. We require the storing and retrieving protocol to perfectly reconstruct the unitary transformation, which implies non unit probability of success. We derive optimal probability of success for a qubit unitary transformation ($d = 2$) used N-times. The optimal probability of success has very simple form $\lambda = N/(N+3)$. We solved the problem also for one up to four uses of a d-dimensional unitary transformation and in all these cases we find that the probability of success goes to one as $N/(N-1+d^2)$.

1 Introduction

Soon after the first important quantum algorithms emerged [1, 2] also the questions of universal quantum devices were investigated. One can imagine having universal cloner [3, 4], processor[5] or a multimeter [6]. In such a device one part of quantum system would serve as the data register and the other as a program register, which determines an operation to be performed on the data. Universality simply means that the device works on all input states and can be programmed to any of the allowed transformations or measurements. Although such devices would be certainly very useful usually they are not allowed by quantum mechanics in their ideal form. For cloners we have the famous no cloning theorem [7], and linearity severely restricts also multimeters. For quantum processors Nielsen and Chuang [8] proved that perfect (error free) implementation of k distinct unitary transformations requires at least k dimensional program register, which is effectively a No-programming theorem. These restrictions imposed by quantum mechanics can be treated in two ways. Either we ask for approximate devices, which always produce an output, or we require the device to be probabilistic, but if it is successful it always produces a perfect (precise) output. Study of optimal cloners already proved to be quite useful and this motivates also the study of other universal devices.

Recently, cloning was considered also for quantum operations [9, 10]. This unveiled unexpected feature called super-replication [11, 12]. In this protocol one can deterministically generate with an exponentially small error up to N^2 copies of a single-qubit unitary operation U starting only from N copies. While studying cloning of unitary transformations it was realized there is a closely related task, which only differs in the causal order of available resources. While in cloning the cloned transformation

Submitted to:
QPL 2017

is available after we have the input states for the clones, one can consider also a task where the order is reversed.

Consider a set of unitary channels on the d dimensional Hilbert space $\mathscr{H}$. Suppose one of these channels, further denoted as $\mathscr{U}$, is chosen randomly and we have access only to N uses of it today. Our aim is to propose a strategy that contains channel $\mathscr{U}$ N-times and stores it in a state of a quantum memory. This phase of the task is called storing. Later, after we lost access to $\mathscr{U}$, we are requested to apply $\mathscr{U}$ on an unknown state ξ. Our goal is chose storing and retrieving strategy in such a way that we would be able to retrieve channel $\mathscr{U}$. This task was first considered in the approximative way by Bisio et.al. [13] and it was termed quantum learning. Our goal is to study the perfect probabilistic version of the problem, and we call the task *perfect probabilistic storing and retrieving of a unitary channel*. The main difference is that we want to retrieve the quantum channel from the quantum memory only without error and with highest possible probability.

In section 2 we summarize our main results. Section 3 quickly reviews the formalism of quantum combs used intensively in the whole paper. Section 4 contains the derivations valid for any dimension of the stored and retrieved transformation, while Section 4.1 presents our most explicit results in the qubit case.

2 Summary of the results

Our goal is to encode the unknown channel $\mathscr{U}$ into a state of a quantum memory while using it N times and then retrieve it exactly with the highest possible probability. Due to no-programming theorem of Nielsen and Chuang [8] the retrieving part of the strategy can not succeed with probability one, if the quantum memory is finite dimensional. Thus, the success of the retrieving part corresponds to a quantum operation $\mathscr{T}$, which is only proportional to the original unitary channel $\mathscr{U}$. Thus, if $\mathscr{U}(\xi) = U\xi U^\dagger$ then $\mathscr{T}(\xi) = \lambda U\xi U^\dagger$ and consequently $\lambda = Tr(\mathscr{T}(\xi))$, is the probability of successful retrieval and we require it to be the same for all unitary transformations $U \in SU(d)$.

We derived the following results with the use of the formalism of quantum combs [14], which is briefly summarized in the next section and it is very useful for solving this type of problems. We solved the perfect probabilistic storing and retrieving of a unitary channel completely for a qubit ($d = 2$) system and arbitrary number of channel uses N.

Theorem 1 *The optimal probability of success of perfect probabilistic storing and retrieving of a qubit unitary channel from its N uses is* $\lambda = N/(N+3)$.

We investigated also the qudit version of the problem (d arbitrary) and until now we were able to solve $N = 1$ up to $N = 4$ setting. All the results we have found can be described by the formula

$$\lambda = N/(N-1+d^2), \tag{1}$$

which suggests the conjecture that the formula (1) holds for N and d arbitrary. Very recently, we managed to reduce the general problem to a linear program for optimization of probability distributions and we believe that soon we will either verify or reject the above conjecture.

Nevertheless, already our current results have surprising features. Let us start by comparison with the approximate version of the problem (termed quantum learning). Optimal solution of the approximate version turns out to be a estimate and prepare strategy, thus quantum memory is not essentially needed. In contrast for our problem quantum memory can not be avoided. The goal of the quantum learning is to maximize the quantum channel fidelity between the stored and retrieved unitary channel. To optimal

infidelity scales roughly as $1/N^2$. In our case in case of success the retrieved channel has fidelity one, and the failure happens with probability roughly $1/N$. If we take the output of our protocol in case of success as well as in case of failure we would obtain the channel infidelity that scales roughly as $1/N$.

It is worh noting that the perfect probabilistic storing and retrieving of a qubit unitary channel is one of few optimal protocols, where a closed form formula was derived.

Our results have implication also for quantum processors. If we focus on probabilistic universal quantum processors one of the main questions is the relation between the dimension of the program register and the probability of success. This question although very important is still unsolved. One problem of addressing it lays in the relation between program states and implemented unitary transformations. Without assuming anything about this relation it is difficult to exclude existence of processors with high probability of success, but awfully complicated determination of a program state for the chosen unitary transformation U we would like to implement. To avoid this kind of additional complexity hidden in the above relation, it is natural to study quantum processors, where the relation of the program state to the implemented unitary transformation is specified by some representation $W(U)$ of the unitary group $U(d)$ and the success probability is the same for all unitaries. In the following we denote such processors as covariant. However, even if we restrict to universal covariant probabilistic processors, the relation between dimension of the program register and the success probability is not known. Although our goal was to solve a slightly different problem, it turns out we can derive the above relation in some special cases, with a conjecture also for the general setting.

For covariant processors we can always imagine the program state as a fixed state on which the representation $W(U)$ was applied. Later on, once the input register is ready the processor performs a big unitary transformation on program and data register followed by a measurement, which indicates whether the operation was successful or not. This is indirectly related to the above discussed perfect storing and retrieving problem. In particular our results, allow us to specify an achievable trade off between the dimension of the program register d_{prog} and the optimal success probability λ for the qubit universal covariant probabilistic processors. While optimizing perfect probabilistic storing and retrieving we show that it is optimal to use the unitary channels $\mathscr{U}$ in parallel, which mathematically corresponds to a reducible representation $U^{\otimes N}$ of $SU(2)$. Depending on the parity of N the decomposition of $U^{\otimes N}$ into irreducible representations (IRRs) of $SU(2)$ contains either even ($j = 0, 1, \ldots N/2$) or odd ($j = 1/2, 3/2, \ldots, N/2$) spin representations. The optimal solution specifies a state onto which $U^{\otimes} N \otimes I$ is applied. If it is not advantageous to use certain IRR the state would have zero amplitude in the subspace of that IRR and the dimension of the quantum memory (program register) could be reduced. It turns out that the optimal state uses all the IRRs (except for the highest spin) in the decomposition of $U^{\otimes N}$. By having optimal solution for every N we can think of having a list of all even (odd) representations up to spin $N/2$ and optimization of succes probability dictates to use all IRRs in the decomposition. We thus obtain a graph how big quantum memory (program register) is used to achieve given probability of success. On the other hand, our results imply that a probability of success $\widetilde{\lambda}$ cannot be achieved if the list of IRRs does not contain high enough spin $j_{\widetilde{\lambda}}$. This effectively introduces a lower bound on the dimension of the program register for a given $\widetilde{\lambda}$. Our findings are summarized in Figure 1.

3 Quantum networks and generalized instruments

The mathematical formalization of perfect probabilistic storing and retrieving of a unitary channel can be easily given within the framework of *quantum combs*. In this section we provide a small review of the subject and we refer to the literature [14, 15, 17] for a complete presentation.

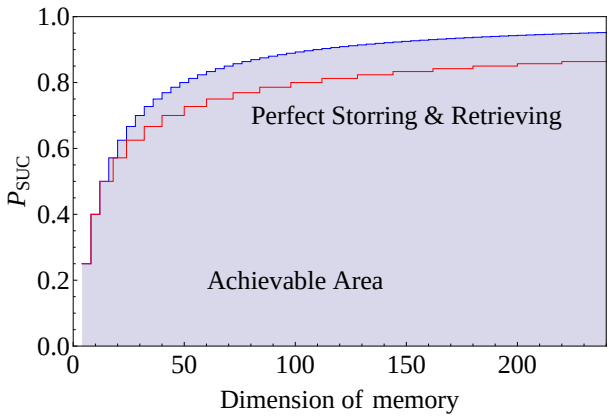


Figure 1: The figure shows the relation between the dimension of the program register (quantum memory) and the probability of success of a universal probabilistic covariant qubit processor. Our results imply a lower bound as well as an upper bound on the dimension for a given success rate.

We will start by introducing some notation. If $\mathscr{H}$ and $\mathscr{K}$ are finite-dimensional Hilbert spaces, then we denote with $\mathscr{L}(\mathscr{H})$ the set of linear operator on $\mathscr{H}$ and with $\mathscr{L}(\mathscr{H},\mathscr{K})$ the set of linear operator from $\mathscr{H}$ to $\mathscr{K}$. We will use the one-to-one correspondence between linear operators $A \in \mathscr{L}(\mathscr{H},\mathscr{K})$ and vectors $|A\rangle\rangle \in \mathscr{K}\otimes\mathscr{H}$ and given by

$$|A\rangle\rangle = \sum_{m=1}^{\dim(\mathscr{K})}\sum_{n=1}^{\dim(\mathscr{H})} \langle m|A|n\rangle |m\rangle|n\rangle, \tag{2}$$

where $\{|m\rangle\}_{m=1}^{\dim(\mathscr{K})}$ and $\{|n\rangle\}_{n=1}^{\dim(\mathscr{H})}$ are two fixed orthonormal bases for $\mathscr{K}$ and $\mathscr{H}$, respectively. For A,B and C operators on $\mathscr{H}$ one can verify the identity

$$A\otimes B|C\rangle\rangle = |ACB^T\rangle\rangle \tag{3}$$

where X^T denotes the transpose of X with respect to the orthonormal basis $|n\rangle$. A quantum operation $\mathscr{O}$ from $\mathscr{L}(\mathscr{H})$ to $\mathscr{L}(\mathscr{K})$ is a completely positive trace non increasing map which can be represented by its Choi operator $O \in \mathscr{L}(\mathscr{K}\otimes\mathscr{H})$. The operator O must satisfy

$$O \geq 0, \quad \mathrm{Tr}_{\mathscr{K}}[O] \leq I_{\mathscr{H}} \tag{4}$$

where $\mathrm{Tr}_{\mathscr{K}}$ denotes the partial trace on $\mathscr{K}$ and $I_{\mathscr{H}}$ the identity operator on $\mathscr{H}$. The two constraints in Eq. (4) correspond to the complete positivity and trace non increasing of the quantum operation $\mathscr{O}$. By making use of the notation in Eq. (2), the Choi operator for a unitary channel $\mathscr{U}$ can be written as the rank one projector $|U\rangle\rangle\langle\langle U|$.

The action of the quantum operation $\mathscr{O}$ on a quantum state $\rho \in \mathscr{L}(\mathscr{H})$ can be described in terms of the Choi operator O as follows

$$\mathscr{O}(\rho) = \mathrm{Tr}_{\mathscr{K}}[O(I_{\mathscr{K}}\otimes\rho^T)] =: O*\rho \tag{5}$$

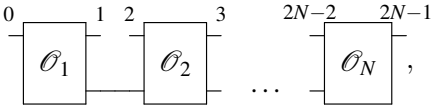
where we introduce the *link product* between the operators O and ρ. The composition of two quantum operations can be represented in terms of their Choi operators too. Let us consider two quantum operations $\mathscr{O},\mathscr{O}'$ with multipartite input and output, i.e. $\mathscr{O}$ goes from $\mathscr{L}(\mathscr{H}_1\otimes\mathscr{H}_2)$ to $\mathscr{L}(\mathscr{H}_3\otimes\mathscr{K})$ and $\mathscr{O}'$

goes from $\mathscr{L}(\mathscr{H}_4 \otimes \mathscr{K})$ to $\mathscr{L}(\mathscr{H}_5 \otimes \mathscr{H}_6)$. We can connect the output of $\mathscr{O}$ on $\mathscr{L}(\mathscr{K})$ with the input of $\mathscr{O}'$ on $\mathscr{L}(\mathscr{K})$ obtaining a new quantum operation from $\mathscr{L}(\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \mathscr{H}_4)$ to $\mathscr{L}(\mathscr{H}_3 \otimes \mathscr{H}_5 \otimes \mathscr{H}_6)$. The Choi operator of the resulting quantum operation is given by the link product of the two quantum operations, as follows:

$$O' * O = \mathrm{Tr}_{\mathscr{K}}[(O' \otimes I_{123})(I_{456} \otimes O^{T_{\mathscr{K}}})] \tag{6}$$

where $O^{T_{\mathscr{K}}}$ denotes the partial transposition of O on the Hilbert space $\mathscr{K}$ and I_{ijk} denotes the identity operator on $\mathscr{H}_i \otimes \mathscr{H}_j \otimes \mathscr{H}_k$. We can interpret Eq. (5) as an instance of Eq. (6).

A quantum network $\mathscr{R}$ consists of a sequence of multipartite quantum operations $\{\mathscr{O}_i, i = 1, \ldots N\}$ where some output of a $\mathscr{O}_i$ is connected to some input of the following quantum operation $\mathscr{O}_{i+1}$ as we illustrate in the following diagram:



(7)

where the floating wires correspond to the input and output systems of the quantum network. $\mathscr{R}$ is called a *deterministic* quantum network if all the quantum operations in Eq. (7) are trace preserving, and it is called a *probabilistic* quantum network otherwise.

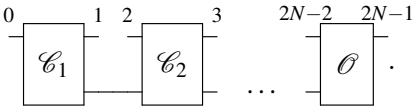
A quantum network can be represented by a Choi operator (commonly called *quantum comb*) which is given by the link product of all the component quantum operations. The Choi operator R of a deterministic quantum network $\mathscr{R}$ obeys the following constraints

$$\mathrm{Tr}_{2k-1}[R^{(k)}] = I_{2k-2} \otimes R^{(k-1)} \qquad k = 1, \ldots, N \tag{8}$$

where, referring to the diagram in Eq. (7), the Hilbert space of the wire labelled by j is $\mathscr{H}_j$, $R^{(N)} = R$, $R^{(0)} = 1$, $R^{(k)} \in \mathscr{L}(\mathscr{H}_{odd_k} \otimes \mathscr{H}_{even_k})$ with $\mathscr{H}_{even_k} = \bigotimes_{j=0}^{k-1} \mathscr{H}_{2j}$ and $\mathscr{H}_{odd_k} = \bigotimes_{j=0}^{k-1} \mathscr{H}_{2j+1}$. $R^{(k)}$ is the Choi operator of the reduced network $\mathscr{R}^{(k)}$ obtained by discarding the last $N-k$ teeth. The set of of positive operators satisfying Eq. (8) and the set of deterministic quantum networks are in one to one correspondence. On the other hand, a given deterministic quantum network $\mathscr{R}$ can be realized as a composition of quantum channels in many different ways. In the probabilistic case, the Choi operator of a probabilistic quantum network $\mathscr{T}$, must satisfy

$$0 \leq T \leq R \tag{9}$$

where R is the Choi operator of a deterministic quantum network. A given probabilitic quantum network $\mathscr{T}$ can be realised as a composition of quantum operations in many different ways. In particular, any probabilitic quantum network $\mathscr{T}$ can be realised by a composition of channels $\{\mathscr{C}\}$ and a final quantum operation $\mathscr{O}$ as follows:

$\mathscr{T} =$ 

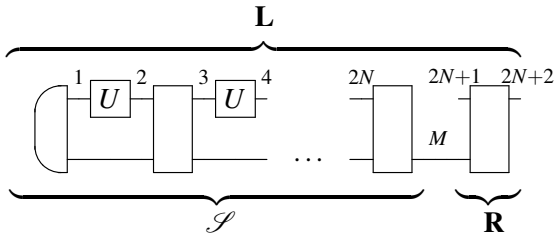
(10)

A set of probabilistic quantum networks $\mathbf{R} = \{\mathscr{R}_i\}$, with the same input and output wires, is called a *generalised quantum instrument* if the sum of their Choi operators $\sum_i R_i =: R$ is the Choi operator of a deterministic quantum network. As in the analogous case of a quantum instrument (i.e. a quantum measurement yielding both classical outcome and a post-measurement state), the index i which labels

the elements of a generalised quantum instrument represents the classical outcome which is available after the quantum network has been provided with an input. If the outcome i is obtained then it means that the probabilistic quantum network $\mathscr{R}_i$ happened. Any generalised quantum instrument can always be realised by a composition of channels followed by a final quantum instrument. We notice that for any probabilistic quantum network there exists a generalised quantum instrument to which it belongs.

4 Optimal Perfect Storing and Retrieving

As we discussed in the introduction, the perfect storing and retrieving of an unknown unitary transformation $\mathscr{U}$ consists of exploiting N uses of the unknown operation in order to be able to, at a later time, reproduce the action $U\xi U^\dagger$, $U \in SU(d)$ of $\mathscr{U}$ on an arbitrary input state ξ. The whole procedure can be described as two steps in a sequence: a *storing* phase and a *retrieving* phase. In the storing phase we use the N copies of the unknown $\mathscr{U}$ to produce some state $|\psi_U\rangle \in \mathscr{H}_M$. During the retrieving phase both the state $|\psi_U\rangle$ and the target state ξ are sent as inputs to a retrieving quantum instrument $\mathbf{R} = \{\mathscr{R}_s, \mathscr{R}_f\}$ whose output in the case of successful retrieving ($\mathscr{R}_s$) should be exactly $\mathscr{U}(\xi)$. Any possible way in which storing and retrieving can be done (parallel or sequential application of $\mathscr{U}$, or any other intermediate approach) is mathematically described by inserting the N uses of the unitary channel $\mathscr{U}$ into N open slots of a generalized quantum instrument $\mathbf{L} = \{\mathscr{L}_s, \mathscr{L}_f\}$ as follows:



(11)

where $\mathscr{S}$ denotes the (deterministic) storing network and $\mathbf{R}$ the retrieving quantum instrument. The output system of the storing network correspond to the Hilbert space $\mathscr{H}_M$ which carries the state $|\psi_U\rangle$. In the case of successful retrieving (i.e. observing outcome s corresponding to both $\mathscr{R}_s$ and $\mathscr{L}_s$) The resulting quantum operation from $\mathscr{L}(\mathscr{H}_{2N+1})$ to $\mathscr{L}(\mathscr{H}_{2N+2})$ is required to be proportional to the channel $\mathscr{U}$ i.e.

$$L_s * \left(\bigotimes_{i=1}^{N} |U\rangle\rangle\langle\langle U|_{2i-1,2i} \right) = \lambda |U\rangle\rangle\langle\langle U|_{2N+1,2N+2} \tag{12}$$

where we used the link product formalism reviewed in Section 3 and the Choi operator $L_s = S * R_s$ describes the successful operation of the storing and retrieving quantum network. Thus, in this case we know with certainty that final output of the network is the desired state $U\xi U^\dagger \in \mathscr{L}(\mathscr{H}_{2N+2})$. By expressing the link product in the above Eq. (12) explicitly the requirement of perfect probabilistic storing and retrieving can be stated as

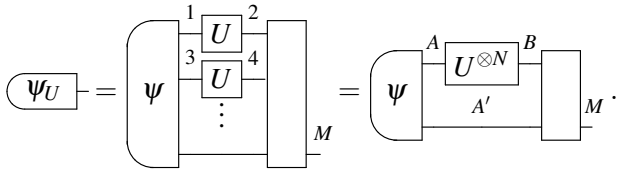
$$\langle\langle U^*|^{\otimes N} L_s |U^*\rangle\rangle^{\otimes N} = \lambda |U\rangle\rangle\langle\langle U| \qquad \forall U \in SU(d). \tag{13}$$

We stress that the probability of success, i.e. the value of λ is required to be the same for all $U \in SU(d)$. The aim of our analysis is to derive the optimal probabilistic quantum network L_s which obeys the constraint of Eq. (13) and maximizes the value of λ.

Our first observation is that the operator L_s could be chosen to satisfy the commutation relation

$$[L_s, U^{*\otimes N} \otimes V^{\otimes N} \otimes U_{2N+1} \otimes V^*_{2N+2}] = 0 \qquad \forall\, U, V \in SU(d). \tag{14}$$

The proof relies on the Holevo's averaging argument for covariant estimation [19]. As a consequence of Eq. (14), it was proved in [13] that the optimal storing phase is *parallel*, i.e. the N uses of the uknown unitary are applied in parallel on a quantum state $|\psi\rangle$ as shown in the following diagram:



(15)

Where we made a suitable relabeling of the Hilbert spaces. Let us now consider the decomposition of $U^{\otimes N} \in \mathscr{L}(\mathscr{H}_A)$ into irreducible representations

$$U^{\otimes N} = \bigoplus_j U^{(j)} \otimes I_{m_j} \tag{16}$$

where I_{m_j} denotes the identity operator on the multiplicity space. Eq. (16) induces the following decomposition of the Hilbert space $\mathscr{H}_A$

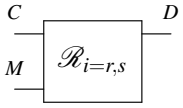
$$\mathscr{H}_A := \bigoplus_j \mathscr{H}_j \otimes \mathscr{H}_{m_j} \qquad \dim(\mathscr{H}_j) = d_j \quad \dim(\mathscr{H}_{m_j}) = m_j. \tag{17}$$

It was shown in [13] that the optimal state $|\psi\rangle$ for the storage can be taken of the following form

$$|\psi\rangle := \bigoplus_j \sqrt{\frac{p_j}{d_j}} |I_j\rangle\!\rangle \in \tilde{\mathscr{H}} \qquad p_j \geq 0,\ \sum_j p_j = 1 \tag{18}$$

where $\mathscr{H}_A \otimes \mathscr{H}_{A'} \supseteq \tilde{\mathscr{H}} := \bigoplus_j \mathscr{H}_j \otimes \mathscr{H}_j$ and I_j denotes the identity operator on $\mathscr{H}_j$. The optimal state $|\psi\rangle$ undergoes the action of the unitary channels and becomes $|\psi_U\rangle := \bigoplus_j \sqrt{\frac{p_j}{d_j}} |U_j\rangle\!\rangle$. Clearly, $|\psi_U\rangle$ belongs to $\mathscr{H}_M$ which is a subspace of $\mathscr{H}_B \otimes \mathscr{H}_{A'}$ isomorphic to $\tilde{\mathscr{H}}$.

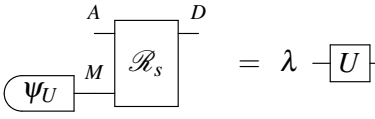
We can focus our attention to the retrieving quantum instrument $\{\mathscr{R}_s, \mathscr{R}_f\}$ from $\mathscr{L}(\mathscr{H}_C \otimes \mathscr{H}_M)$ to $\mathscr{L}(\mathscr{H}_D)$



(19)

The condition that the outcome s corresponds to the perfect learning becomes:

$$R_s * |\psi_U\rangle\langle\psi_U| = \mathrm{Tr}_M[R_s((|\psi_U\rangle\langle\psi_U|)^T \otimes I_{C,D})] = \langle\psi_U^*|R_s|\psi_U^*\rangle = \lambda |U\rangle\!\rangle\langle\!\langle U| \quad \forall U$$



(20)

where $|\psi_U^*\rangle = \bigoplus_j \sqrt{\frac{p_j}{d_j}}|U_j^*\rangle\rangle$. The optimal R_s can be chosen to satisfy the following commutation relation:

$$\begin{aligned} &\left[R_s, U'^* V' \otimes U_C \otimes V_D^*\right] = 0, \\ &U' := \bigoplus_j U_j \otimes I_j, \quad V' := \bigoplus_j I_j \otimes V_j. \end{aligned} \tag{21}$$

which is clearly the analog of Eq. (14) where $U^{\otimes N} \otimes V^{\otimes N}$ has been replaced by $U'V'$. Then, reminding that $U'|\psi\rangle = |\psi_U\rangle$ and $|\psi_I^*\rangle = |\psi\rangle$, from Eq. (21) we have

$$\langle\psi_U^*|R_s|\psi_U^*\rangle = \lambda\,|U\rangle\rangle\langle\langle U| \quad \forall U \iff \langle\psi|R_s|\psi\rangle = \lambda\,|I\rangle\rangle\langle\langle I|\,. \tag{22}$$

Let us now summarize what we discussed so far by giving a formal statement of the optimization problem for the probabilistic perfect learning:

$$\begin{aligned} \underset{|\psi\rangle, R_s}{\text{maximize}} \quad & \lambda = \frac{1}{d^2}\langle\langle I|\langle\psi|R_s|\psi\rangle|I\rangle\rangle \\ \text{subject to} \quad & \langle\psi|R_s|\psi\rangle = \lambda\,|I\rangle\rangle\langle\langle I| \\ & |\psi\rangle \text{ as in Eq. (18)} \\ & R_s \text{ obeys Eq. (21)} \\ & \mathrm{Tr}_D[R_s] \leq I\,. \end{aligned} \tag{23}$$

Let us now consider the decomposition

$$\begin{aligned} U_j^* \otimes U &= \bigoplus_{J \in \mathsf{J}_j} U_J \otimes I_{m_J^{(j)}} \\ \mathscr{H}_j \otimes \mathscr{H} &= \bigoplus_{J \in \mathsf{J}_j} \mathscr{H}_J \otimes \mathscr{H}_{m_J^{(j)}} \end{aligned} \tag{24}$$

where we remind that the index j labels the irreducible representations in the decomposition of $U^{\otimes N}$ and we denote with J_j the set of values of J such that U_J is in the decomposition of $U_j^* \otimes U$. It is important to notice that the multiplicity spaces $\mathscr{H}_{m_J^{(j)}}$ are one dimensional and therefore $I_{m_J^{(j)}}$ are rank one [1]. Then we have

$$\begin{aligned} U'V' \otimes U^* \otimes V^* &= \bigoplus_{JK} U_J \otimes V_K \otimes I_{m_{JK}} \\ \mathscr{H}_{m_{JK}} &= \bigoplus_{j \in \mathsf{j}_{JK}} \mathscr{H}_{m_J^{(j)}} \otimes \mathscr{H}_{m_K^{(j)}} \end{aligned} \tag{25}$$

where j_{JK} denotes the set of values of j such that $U_J \otimes V_K$ is in the decomposition of $U_j^* \otimes V_j \otimes U \otimes V^*$. Since $\dim(\mathscr{H}_{m_J^{(j)}}) = 1$ we stress that $\langle\langle I_{m_J^{(j)}}|I_{m_J^{(j')}}\rangle\rangle = \delta_{j,j'}$, $|\chi\rangle \in \mathscr{H}_{m_J^{(j)}} \otimes \mathscr{H}_{m_J^{(j)}} \Leftrightarrow |\chi\rangle \propto |I_{m_J^{(j)}}\rangle\rangle$ and $\mathscr{H}_{m_{JJ}} = \mathrm{span}(\{|I_{m_J^{(j)}}\rangle\rangle\}, j \in \mathsf{j}_{JJ})$.

[1] From the Schur-Weyl duality, any irreducible representation U_j of $SU(d)$ is in correspondence with a young diagram Y_j, the defining representation U being represented by a single box $\square$. One can verify that there cannot be two equivalent Young diagrams in the decomposition $Y_j \times \square = \sum_K Y_K$. For a more detailed treatment we refer to [18]

From Eq. (25) the commutation relation of Eq. (21) becomes

$$\left[R_s, \bigoplus_{JK} U_J \otimes V_K \otimes I_{m_{JK}}\right] = 0 \tag{26}$$

which, thanks to the Schur's lemma, gives

$$\begin{aligned} R_s &= \bigoplus_{J,K} I_J \otimes I_K \otimes s^{(JK)} \\ s^{(JK)} &\in \mathscr{L}\left(\mathscr{H}_{m_{JK}}\right) \ , s^{(JK)} \geq 0 \end{aligned} \tag{27}$$

From Eq. (27) we have that the quantum operation R_s is the sum of the positive operators $I_J \otimes I_K \otimes s^{(JK)}$. Therefore we have that

$$\langle\psi|R_s|\psi\rangle = \lambda |I\rangle\rangle\langle\langle I| \iff \langle\psi|I_J \otimes I_K \otimes s^{(JK)}|\psi\rangle = \lambda_{JK}|I\rangle\rangle\langle\langle I| \quad \forall J,K \tag{28}$$

since $|I\rangle\rangle\langle\langle I|$ is a rank one operator.

From the identity $I_j \otimes I = \bigoplus_{J \in \mathsf{I}_j} I_J \otimes I_{m_J^{(j)}}$ (we remid that $I_{m_J^{(j)}}$ has rank one), we obtain

$$|\psi\rangle|I\rangle\rangle = \bigoplus_j \bigoplus_{J \in \mathsf{J}_j} \sqrt{\frac{p_j}{d_j}} |I_J\rangle\rangle |I_{m_J^{(j)}}\rangle\rangle = \bigoplus_J \bigoplus_{j \in \mathsf{j}_{JJ}} \sqrt{\frac{p_j}{d_j}} |I_J\rangle\rangle |I_{m_J^{(j)}}\rangle\rangle = \bigoplus_J |I_J\rangle\rangle |\phi_J\rangle \tag{29}$$

$$|\phi_J\rangle := \bigoplus_{j \in \mathsf{j}_{JJ}} \sqrt{\frac{p_j}{d_j}} |I_{m_J^{(j)}}\rangle\rangle. \tag{30}$$

Using Eq. (27) into Eq. (23) we obtain

$$\lambda_{JK} = \delta_{JK}\lambda_J, \quad \lambda = \sum_J \lambda_J \tag{31}$$

$$\lambda_J = \frac{d_J}{d^2} \langle\phi_J|s^{(JJ)}|\phi_J\rangle \tag{32}$$

where the λ_{JK}'s were defined in Eq. (28). It is now easy to show that we can assume

$$R_s = \bigoplus_J I_J \otimes I_J \otimes s^{(J)} \tag{33}$$

$$s^{(J)} := \sum_{j,j' \in \mathsf{j}_{JJ}} s^{(J)}_{jj'} |I_{m_J^{(j)}}\rangle\rangle\langle\langle I_{m_J^{(j')}}| \tag{34}$$

Indeed, let $R'_s = \bigoplus_{JK} I_J \otimes I_K \otimes s'^{(JK)}$ be the optimal quantum operation and let us define the operators $R_s = \bigoplus_J I_J \otimes I_J \otimes s^{(J)}$ where $s^{(J)} = s'^{(JJ)}$ and $R''_s = \bigoplus_{J \neq K} I_J \otimes I_K \otimes s^{(JK)}$. Since both R_s and R''_s are positive and $R_s + R''_s = R'_s$, we have that $\mathrm{Tr}_D[R'_s] \leq I$ implies $\mathrm{Tr}_D[R_s] \leq I$ i.e. R_s is a quantum operation. Finally, from Eq. (31) we have that $\langle\psi|R_s|\psi\rangle = \langle\psi|R'_s|\psi\rangle$, thus proving that also $\{R_s, |\psi\rangle\}$ is an optimal solution of the optimization problem (23). Let us now consider the constraint $\mathrm{Tr}_D[R_s] \leq I$. Since R_s satisfies Eq. (21), we have

$$\left[\mathrm{Tr}_D[R_s], U'V' \otimes U_C^*\right] = 0 \implies \mathrm{Tr}_D[R_s] = \bigoplus_J \bigoplus_{j \in \mathsf{j}_{JJ}} I_J \otimes I_j s^{(J)}_{jj} \tag{35}$$

From Eq. (35) we have

$$\mathrm{Tr}_D[R_s] \leq I \Leftrightarrow \frac{d_J}{d_j} s_{jj}^{(J)} \leq 1 \;\; \forall J, \, \forall j \in \mathrm{j}_{JJ}. \tag{36}$$

If R_s is of the form of Eq. (33) we can express the constraint of Eq. (28) in terms of the operators $s^{(J)}$ as follows:

$$\langle \psi | R_s | \psi \rangle = \lambda \, |I\rangle\rangle\langle\langle I| \quad \Longleftrightarrow \quad 0 = \sum_{j,j' \in \mathrm{j}_{JJ}} \delta_{j,j'} \, d \, d_J \frac{p_j}{d_j^2} s_{jj}^{(J)} - \sqrt{\frac{p_j p_{j'}}{d_j d_{j'}}} s_{jj'}^{(J)} \;\; \forall J. \tag{37}$$

The proof of Eq. (37) is given in appendix A. It is now possible to restate the optimization problem of Eq. (23) in terms of the operators s^J:

$$\begin{array}{ll} \underset{|\psi\rangle, s^J}{\text{maximize}} & \lambda = \sum_J \lambda_J \\ \text{subject to} & |\psi\rangle \text{ as in Eq. (18)} , \\ & s^J \text{ obeys Eq. (37)} \;\; \forall J, \\ & \frac{d_J}{d_j} s_{jj}^{(J)} \leq 1 \;\; \forall J \, \forall j \in \mathrm{j}_{JJ} \, . \end{array} \tag{38}$$

where the λ_J's are given by Eq. (32).

At this point it is useful to introduce operators $r^{(J)} = \sum_{jj'} r_{jj'}^{(J)} |j\rangle\langle j'|$,

$$r_{jj'}^{(J)} \equiv \sqrt{\frac{p_j p_{j'}}{d_j d_{j'}}} s_{jj'}^{(J)}, \tag{39}$$

where we introduced new notation for the orthonormal basis $|j\rangle \equiv |I_{m_J^{(j)}}\rangle\rangle$, $j \in \mathrm{j}_{JJ}$ of the multiplicity space $\mathscr{H}_{m_{JJ}}$. Operators $r^{(J)}$ contain both the information about the state $|\psi\rangle$ as well as about operators $s^{(J)}$ and they correspond to the nondeterministic quantum network $\mathscr{L}_s$. As a consequence of $s^{(J)} \geq 0$ and $p_j \geq 0$ operators $r^{(J)}$ are positive semidefinite and in particular $r_{jj}^{(J)} \geq 0$. Let us also define

$$|\rho\rangle := \sum_j \sqrt{r_{jj}^{(J)}} |j\rangle \tag{40}$$

$$A := \sum_{j \in \mathrm{j}_{JJ}} \frac{d d_J}{d_j} r_{jj}^{(J)} |j\rangle\langle j| \tag{41}$$

The condition (37) of perfect storing and retrieving can be written as

$$\langle v | A - r^{(J)} | v \rangle = 0, \tag{42}$$

$$|v\rangle = \sum_{j \in \mathrm{j}_{JJ}} |j\rangle. \tag{43}$$

Let us assume that we have proved the identity

$$d d_J = \sum_{j \in \mathrm{j}_{JJ}} d_j. \tag{44}$$

This can be rigorously proved for $SU(d)$, but for the purpose of this submission we will show it only for $SU(2)$ once we restrict to the $d = 2$ case.

Matrix H_{ij} is positive semidefinite if and only if $|H_{ij}| \leq \sqrt{H_{ii}H_{jj}}\ \forall i,j$. Using this criterion and Eq. (44) one can easily show that both $A - r^{(J)}$ and $A - |\rho\rangle\langle\rho|$ are positive semidefinite matrices. Moreover, using $\Re(r^{(J)}_{jj'}) \leq |r^{(J)}_{jj'}| \leq \sqrt{r^{(J)}_{jj} r^{(J)}_{j'j'}}$ one can easily prove the inequality

$$\langle v|(A - r^{(J)})|v\rangle \geq \langle v|(A - |\rho\rangle\langle\rho|)|v\rangle. \tag{45}$$

which also gives

$$\langle v|(A - r^{(J)})|v\rangle = 0 \implies \langle v|(A - |\rho\rangle\langle\rho|)|v\rangle = 0, \tag{46}$$

due to $A - |\rho\rangle\langle\rho| \geq 0$. Moreover, let us rewrite expression $\langle v|A|v\rangle$ as

$$\langle v|A|v\rangle = \langle\rho|B|\rho\rangle \tag{47}$$

$$B := \sum_{j \in \mathrm{j}_{JJ}} \frac{dd_J}{d_j} |j\rangle\langle j| \tag{48}$$

As a consequence we have

$$\langle v|(A - |\rho\rangle\langle\rho|)|v\rangle = \langle\rho|(B - |v\rangle\langle v|)|\rho\rangle. \tag{49}$$

Thanks to Eq. (44) $B - |v\rangle\langle v|$ is a positive matrix, which has either trivial or one dimensional kernel. This allows us together with Eqs. (46),(49) to write a necessary condition for perfect storing and retrieving

$$\langle\rho|(B - |v\rangle\langle v|)|\rho\rangle = 0 \tag{50}$$

$$\implies B|\rho\rangle - |v\rangle\langle v|\rho\rangle = 0 \tag{51}$$

Explicitly solving the above equation we get the only possible solution

$$\frac{dd_J}{d_j}\sqrt{r^{(J)}_{jj}} = \frac{dd_J}{d_{j'}}\sqrt{r^{(J)}_{jj'}} \implies r^{(J)}_{jj} = \mu_J d_j^2, \tag{52}$$

which is unique up to a constant μ_J as we expected due to the rank one deficiency of $B - |v\rangle\langle v|$. Once the diagonal elements $r^{(J)}_{jj}$ respect Eq. (52) we have $\langle v|(A - |\rho\rangle\langle\rho|)|v\rangle = 0$, but to fulfill Eq. (46) we need also the saturation of the bound (45). This happens if and only if

$$r^{(J)}_{jj'} = \sqrt{r^{(J)}_{jj}}\sqrt{r^{(J)}_{j'j'}}. \tag{53}$$

Thus, fulfillment of Eqs. (52), (53) guarantees the perfect storing and retrieving of unitary transformations and we can rewrite the probability of success as

$$\lambda = \sum_J \lambda_J = \sum_J \sum_{j,j' \in \mathrm{j}_{JJ}} \frac{d_J}{d^2} \mu_J d_j d_{j'} = \sum_J d_J^3 \mu_J, \tag{54}$$

where we used Eqs. (32),(39) and (44).

Let us express the normalization conditions of the retrieving channel (36) via constants μ_J using on the way the Eq. (39)

$$\mu_J d_j^2 \leq \frac{p_j}{d_J} \tag{55}$$

Collecting Eqs.(54),(55) and (18) the optimization of perfect probabilistic storing and retrieving can be reduced to

$$\begin{aligned} &\underset{\mu_J, p_j}{\text{maximize}} && \lambda = \sum_J d_J^3 \mu_J, \\ &\text{subject to} && 0 \leq d_J \mu_J \leq \frac{p_j}{d_j^2} \quad \forall j \in \mathrm{j}_{JJ} \quad \forall J \\ & && p_j \geq 0 \quad \sum_j p_j = 1, \end{aligned} \tag{56}$$

which is a simple linear programming problem for variables μ_J and p_j. In order to numerically solve it one needs to know the list of representations labelled by indexes j,J, their dimensions and how they are related i.e. the sets j_{JJ}. Using Young diagram this can be done easily at least for small N. How difficult the problem really is for arbitrary N and dimension d is still an ope question.

4.1 Perfect probabilistic storing and retrieving of qubit unitary transformations

Our goal now is to restrict to $d = 2$, but to solve the problem for arbitrary number N of uses of the unknown unitary channel. We start by decomposing the representation $U^{\otimes N}$, that corresponds to parallel uses of the qubit unitary transformation U, into irreducible representations of $SU(2)$:

$$U^{\otimes N} = \bigoplus_{j=\langle\langle N/2 \rangle\rangle}^{N/2} U_j \otimes I_{m_j}, \tag{57}$$

where $\langle\langle x \rangle\rangle$ denotes the fractional part of x (i.e. $\langle\langle N/2 \rangle\rangle$ is 0 for N even and $1/2$ for N odd) and $m_j = \frac{2j+1}{N/2+j+1}\binom{N}{N/2+j}$ [20]. Here U_j denotes operators of IRR with spin j and dimension $d_j = 2j+1$. We note that value of the multiplicity m_j is unimportant as we argued in the previous sections.

We will study only even N in order to make the notation less cumbersome. The case of odd N is very similar, and we discuss its specifics in the Appendix. For the even N spin j can have the following values $j = 0, 1, \ldots, N/2$. Let us note that for $SU(2)$ the conjugated representation U_j^* is equivalent to the representation U_j. Thus, the decomposition of $U_j^* \otimes U$ from Eq. (24) is formally equivalent to the composition of spin j with spin $1/2$. As a consequence we can get either $J = j + 1/2$ or $J = j - 1/2$ and so $\mathrm{J}_j = \{j - 1/2, j + 1/2\}$. Althogether J can obtain values $J = 1/2, 3/2, \ldots (N+1)/2$.

Let us now study the validity of Eq. (44). For all values of J except for $J = (N+1)/2$ we have that J could have emerged only from $j = J \pm 1/2$. We can easily check that Eq. (44) is in this case satisfied

$$\sum_{j \in \mathrm{j}_{JJ}} d_j = d_{J-1/2} + d_{J+1/2} = 2J + 2J + 2 = 2(2J+1) = d d_J, \tag{58}$$

but it is not true for $J = N + 1/2$, because $d_{N/2} \neq 2 d_{(N+1)/2}$. It turns out that $J = N + 1/2$ cannot be used for perfect storing and retrieving i.e. $s^{\frac{N+1}{2}}$ must be zero, because ${}_{BA}\langle\langle I | I_{\frac{N+1}{2}} \otimes I_{\frac{N+1}{2}} \otimes s^{\frac{N+1}{2}} | I \rangle\rangle_{BA} \neq \lambda_{\frac{N+1}{2}} |I\rangle\rangle\langle\langle I|$. We are now in position to prove the following lemma.

Lemma 1 *The probability of success of perfect probabilistic storing and retrieving of a qubit unitary channel from its N uses is upper bounded by* $\frac{N}{N+3}$.

Proof 1 *Let us write two inequalities that are given by Eq. (55) for any j except for* $j = 0, N/2$

$$\mu_{j+1/2}\, d_j^2 d_{j+1/2} \leq p_j \tag{59}$$

$$\mu_{j-1/2}\, d_j^2 d_{j-1/2} \leq p_j \tag{60}$$

Let us note that for $j = 0$ *only Eq. (59) exists and similarly for* $j = N/2$ *only Eq. (60). We define coefficient* $f_j \in [0,1]$ *for* $j = 0, \ldots, \frac{N}{2}$ *via the formula*

$$f_j = \frac{1}{2}\frac{2j}{2j+1}\left(\frac{2j+2}{N}+1\right) \tag{61}$$

Since $f_0 = 0$ *and* $f_{N/2} = 1$ *we can multiply Eq. (59) by* $1 - f_j$ *and Eq. (60) by* f_j *sum them up for all j. We obtain*

$$\sum_{j=0}^{\frac{N}{2}} (1-f_j)\, \mu_{j+1/2}\, d_j^2 d_{j+1/2} + f_j\ \mu_{j-1/2}\, d_j^2 d_{j-1/2} \leq 1 \tag{62}$$

The above inequality can be rewritten as

$$\sum_{J=\frac{1}{2}}^{\frac{N-1}{2}} z_J \mu_J \leq 1, \tag{63}$$

where we defined

$$z_J \equiv d_J \left(d_{J-1/2}^2 (1 - f_{J-1/2}) + d_{J+1/2}^2\, f_{J+1/2} \right) \tag{64}$$

and we used $f_0 = 0$, $f_{\frac{N}{2}} = 1$. *By inserting explicit expression of* f_j *from Eq. (61) into definition of* z_J *a straightforward calculation yields*

$$z_j = d_J^3 \frac{N+3}{N} \tag{65}$$

Let us mention that the coefficient f_j *was intentionally chosen so that the J dependent part of* z_j *matches the coefficient in the expression for* λ_J *in Eq. (56). Thanks to this, inequality (63) actually reads*

$$\begin{aligned} \frac{N+3}{N} \sum_{J=\frac{1}{2}}^{\frac{N-1}{2}} d_J^3 \mu_J &\leq 1 \\ \frac{N+3}{N} \sum_{J=\frac{1}{2}}^{\frac{N-1}{2}} \lambda_J &\leq 1, \\ \lambda = \sum_{J=\frac{1}{2}}^{\frac{N+1}{2}} \lambda_J &\leq \frac{N}{N+3}, \end{aligned} \tag{66}$$

where we used that $\lambda_{\frac{N+1}{2}}$ *must be zero due to the condition of perfect storing and retrieving as we showed earlier. Since* λ *represents the probability of success of the perfect learning of a qubit unitary gate we proved the lemma.*

Proof 2 (Proof of Theorem 1) *Finally, we prove Theorem 1 by showing that the upper bound from Lemma 1 can be saturated. One can simply choose*

$$p_j = \frac{6}{(N+1)(N+2)(N+3)}(2j+1)^2 \tag{67}$$

$$\mu_{j+1/2} = \frac{6}{(N+1)(N+2)(N+3)}\frac{1}{2j+2} \tag{68}$$

and check that conditions in Eq. (56) are satisfied and $\lambda = N/(N+3)$. Knowledge of μ_J and p_j allows us to completely specify the state $|\psi\rangle$ and the retrieving operation $\mathscr{R}_s$ sufficient for building the complete storing and retrieving strategy.

A Proof of Eq. (37)

For any J the operator $R_s^{(J)} := I_J \otimes I_J \otimes s^{(J)}$ satisfies the commutation relation of Eq. (21). which implies

$$\begin{aligned}
&\langle\psi|R_s^{(J)}|\psi\rangle = \\
&= \langle\psi|(U'U'^* \otimes U^* \otimes U)R_s^{(J)}(U'U'^* \otimes U^* \otimes U)^\dagger|\psi\rangle \\
&= (U^* \otimes U)\langle\psi|R_s^{(J)}|\psi\rangle(U^* \otimes U)^\dagger \ \ \forall U
\end{aligned} \tag{69}$$

Thanks to the Schur's lemma Eq. (69) gives

$$\langle\psi|R_s^{(J)}|\psi\rangle = \lambda_J|I\rangle\rangle\langle\langle I| + \nu_J\left(I - \tfrac{1}{d}|I\rangle\rangle\langle\langle I|\right) \tag{70}$$

which implies that Eq. (28) is satisfied if $\nu_J = 0$ for all J. By taking the trace of Eq. (70) we have

$$\begin{aligned}
&\mathrm{Tr}[\langle\psi|R_s^{(J)}|\psi\rangle] = \langle\psi|\,\mathrm{Tr}_{CD}[R_s^{(J)}]|\psi\rangle = \\
&\langle\psi|\bigoplus_{j\in \mathrm{j}_{JJ}} I_j \otimes I_j q_j^{(J)}|\psi\rangle = \\
&\sum_{j\in \mathrm{j}_{JJ}} p_j q_j^{(J)} = \lambda_J d + \nu_J(d^2-1) \\
&\qquad\qquad q_j^{(J)} := \frac{d_J^2}{d_j^2} s_{jj}^{(J)}.
\end{aligned} \tag{71}$$

If we insert Eq. (30) into Eq. (32) we have

$$\lambda_J = \frac{d_J}{d^2}\sum_{j,j'\in \mathrm{j}_{JJ}} \sqrt{\frac{p_j p_{j'}}{d_j d_{j'}}} s_{jj'}^{(J)}. \tag{72}$$

From Eq. (71) and Eq. (71) we have

$$\begin{aligned}
&\nu_j = 0 \iff \\
&\sum_{j,j'\in \mathrm{j}_{JJ}} \delta_{j,j'}\, d\, d_J \frac{p_j}{d_j^2} s_{jj}^{(J)} - \sqrt{\frac{p_j p_{j'}}{d_j d_{j'}}} s_{jj'}^{(J)} = 0,
\end{aligned} \tag{73}$$

which proves the thesis.

B The case of odd N

The main difference is that the IRR's with minimum and maximum spin ($J = 0$ and $J = \frac{N+1}{2}$) have only multiplicity one. Also for N odd the investigation of the conditions of perfect learning reveals that $s^{\frac{N+1}{2}}$ has to be zero. On the other had for $J = 0$ can be involved in the perfect storing and retrieving. Other expressions remain identical, but now J is an integer. In particular, in the proof of Lemma 1 we choose f_J according to Eq. (61) and the whole proof goes on analogically to the case of even N.

References

[1] P. Shor, SIAM J. Computing 26 (1997), 1484-1509.

[2] Lov K. Grover, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219

[3] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996)

[4] V. Scarani, S. Iblisdir, N. Gisin, A. Acin, Rev. Mod. Phys. 77, 1225-1256 (2005)

[5] M. Hillery, V. Bužek,and M. Ziman, PHYSICAL REVIEW A, VOLUME 65, 022301 (2002)

[6] Miloslav Dušek and Vladimir Bužek Phys. Rev. A 66, 022112 (2002)

[7] W.K. Wootters and W.H. Zurek, Nature 299, 802 (1982)

[8] Programmable Quantum Gate Arrays M. A. Nielsen and Isaac L. Chuang, Phys. Rev. Lett. 79, 321 (1997)

[9] G. Chiribella, G.M. DAriano, and P. Perinotti, Phys. Rev. Lett. 101, 180504 (2008)

[10] A. Bisio, G.M. DAriano, P. Perinotti, and M. Sedlak, Phys. Lett. A 378, 1797 (2014)

[11] W. Dur, P. Sekatski, and M. Skotiniotis, Phys. Rev. Lett. 114, 120503 (2015).

[12] G. Chiribella, Y. Yang, and C. Huang, Phys. Rev. Lett. 114, 120504 (2015).

[13] A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, P. Perinotti, Phys. Rev. A 81, 032324 (2010)

[14] G. Chiribella, G. M. D'Ariano, P. Perinotti, Phys. Rev. A **80**, 022339 (2009).

[15] G. Chiribella, G. M. D'Ariano, P. Perinotti, Phys. Rev. Lett. **101**, 060401 (2008).

[16] G. Chiribella, G. M. D'Ariano, P. Perinotti, Europhysics Letters **83**, 30004 (2008).

[17] A. Bisio, G. Chiribella, G. M. D'Ariano, P. Perinotti, Acta Physica Slovaca 61, No.3, 273-390 (2011).

[18] W. Fulton, J. Harris, "Representation Theory: A First Course", Springer (2013)

[19] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory*, North-Holland, Amsterdam, (1982).

[20] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. 82, 4344 (1999).