Optimal probabilistic storage and retrieval of unitary channels

Michal Sedlák, 1,2 Alessandro Bisio, 3 and Mário Ziman 1,2

1 RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 84511 Bratislava, Slovakia
2 Faculty of Informatics, Masaryk University, Botanická 68a, 60200 Brno, Czech Republic
3 QUIT group, Dipartimento di Fisica, INFN Sezione di Pavia, via Bassi 6, 27100 Pavia, Italy

We address the question of a quantum memory storage of quantum dynamics. In particular, we design an optimal protocol for \( N \to 1 \) probabilistic storage-and-retrieval of unitary channels on \( d \)-dimensional quantum systems. If we may access the unknown unitary gate only \( N \)-times, the optimal success probability of perfect retrieval of its single use is \( N/(N - 1 + d^2) \). The derived size of the memory system exponentially improves the known upper bound on the size of the program register needed for probabilistic programmable quantum processors. Our results are closely related to probabilistic perfect alignment of reference frames and probabilistic port-based teleportation.

PACS numbers: 03.67.-a, 03.67.Ac, 03.65.Fd

**Introduction.** Since the discovery of the first quantum algorithms \[1,2\] and protocols \[3,4\] the information processing with quantum systems has challenged basic paradigms and existing limitations of computer science. In the last few decades we have discovered that quantum information cannot be cloned \[5\], its “logical value” cannot be inverted \[6\], quantum processors cannot be universally programmed \[7\], and universal multimeters do not exist \[8,9\]. No doubt, any of these programmable devices would represent a very useful piece of quantum technology, thus, their approximate realisations are of foundational interest \[8,12\]. The no-go restrictions imposed by quantum theory are treated in two ways. Either we ask for an approximate performance, or we allow that the perfect performance happens with some probability of failure.

Studies of optimal approximate cloners initiated by Hillery and Bužek \[10\] demonstrated that such non-ideal devices are of practical relevance and this motivated the study of other universal devices. In particular, it was shown that quantum theory limits the fidelity of \( 1 \to N \) clones of qubits to \( (2N + 1)/3N \) \[13\]. For quantum processors Nielsen and Chuang \[7\] proved that perfect (error free) implementation of \( k \) distinct unitary transformations requires at least \( k \) dimensional program register. Recently, the cloning was considered also for quantum transformations \[14,15\]. This unveiled an unexpected feature called super-replication \[16,17\]. In this protocol, starting with \( N \) copies of a qubit unitary transformation \( U \) one deterministically generates up to \( N^2 \) copies of \( U \) with an exponentially small error rate. While studying cloning of unitaries it was realized there is a closely related task of storage-and-retrieval (SAR), which only differs in the causal order of available resources. While in the cloning the cloned device is available after the input states are at the disposal, one can consider also a task where this order is reversed, thus, the device is available only before the input states. In such case, we need to learn \[18\] and somehow store the action of the device and retrieve it once the input states are available.

**Problem formulation.** The devices transforming states of \( d \)-dimensional quantum systems associated with Hilbert space \( \mathcal{H} \) are formalized as quantum channels, i.e. completely positive trace-preserving linear maps on the space \( L(\mathcal{H}) \) of linear operators on \( \mathcal{H} \). Suppose an unknown channel \( U \) is provided for experiments and we may access it \( N \) times. However, we are asked to apply \( U \) on an unknown state \( \xi \) only after we lost the access to this channel. Therefore, our aim is to find an optimal strategy that stores \( U \) in a state of a quantum memory (associated with Hilbert space \( \mathcal{H}_M \) ) and allows us to retrieve its action when needed. In the approximative settings this task (for unitary channels) was studied in Ref.\[19\].

Our goal is to investigate the probabilistic version of the SAR problem, in particular, we aim to find the optimal \( N \to 1 \) probabilistic storage and retrieval procedure (PSAR). Moreover, we require the retrieved channel to be implemented perfectly and with the same probability of success (“covariance” property) for all considered channels. We will design the strategy maximizing the probability for the set of unitary channels, i.e. \( U(\xi) = U\xi U\dagger \) for some unitary operator \( U \). Due to no-programming theorem \[7\], the retrieving part of any PSAR strategy cannot be deterministic. Thus, the successful retrieval is described by a trace-non-increasing completely positive linear map (quantum operation) \( T_U : L(\mathcal{H}) \to L(\mathcal{H}) \) proportional to the unknown unitary channel, \( T_U = \lambda_U U \).

Consequently, the success probability is \( \lambda_U = \text{tr}[T_U(\xi)] \) and the condition of covariance implies \( \lambda_U = \lambda \) for all \( U \).

**One-to-one probabilistic storage-and-retrieval.** In such
case the unknown unitary $U$ is applied on a suitably chosen state $|\psi\rangle$ (in general bipartite and entangled), which yields state $|\psi_U\rangle \in \mathcal{H}_M$ and concludes the storing phase. Afterwards, once we want to apply unitary $U$ on some state $\xi$, we employ a retrieving quantum instrument $\mathbf{R} = \{\mathcal{R}_s, \mathcal{R}_f\}$, which acts on $\xi \otimes |\psi_U\rangle/|\psi_U\rangle$ and in case of success outputs an sub-normalized state $\lambda U\xi U^\dagger$, i.e. $\mathcal{R}_s : \mathcal{L}(\mathcal{H}_{in} \otimes \mathcal{H}_M) \to \mathcal{L}(\mathcal{H}_{out})$ with $\mathcal{H}_i = \mathcal{H}_{in} = \mathcal{H}_{out}$.

The retrieving quantum instrument plays the role of a probabilistic programmable processor and the state $|\psi_U\rangle$ programs a unitary transformation $U$ to be performed on a state $\xi$.

Using the Choi isomorphism [20] we have that $\mathcal{R}_s(\xi \otimes |\psi_U\rangle/|\psi_U\rangle) = \text{tr}_{in,M}(I \otimes \xi^T \otimes |\psi_U\rangle/|\psi_U\rangle^T \mathcal{R}_s) = \lambda \text{tr}_{in}((I \otimes \xi^T)|U\rangle\langle U|) = \lambda U\xi U^\dagger$, where $\mathcal{R}_s \in \mathcal{L}(\mathcal{H}_{out} \otimes \mathcal{H}_{in} \otimes \mathcal{H}_M)$ and $|U\rangle = \sqrt{\alpha}(U \otimes I)|\psi_+\rangle$ with $|\psi_+\rangle = d^{-1/2} \sum_j |j\rangle \otimes |j\rangle$ (vectors $\{|j\rangle\}$) form an orthonormal basis of $\mathcal{H}_i = \mathcal{H}_{in} = \mathcal{H}_{out}$). Since the above identity must hold for any $\xi$ and $|\psi_U\rangle/|\psi_U\rangle^T = |\psi_U\rangle^T/|\psi_U\rangle^T$ (both the transposition and the conjugation are defined with respect to the same basis of $\mathcal{H}_M$) we obtain the following perfect retrieval condition

$$
(|\psi_U\rangle/|\psi_U\rangle^T)|\mathcal{R}_s|\psi_U\rangle = \lambda|U\rangle\langle U| \quad \forall U \in \text{SU}(d).
$$

(S.1)

Already this simple case shows that the maximization of probability of success $\lambda$ involves the simultaneous optimization of the storing phase (choice of $|\psi\rangle$) and the retrieving phase (choice of quantum instrument $\mathbf{R}$). It turns out that the optimal performance is achieved by the (incomplete) quantum teleportation protocol [3] that is a known example of a universal probabilistic quantum processor [21]. Let us note that this is similar to quantum gate teleportation invented by Gottesman and Nielsen [22], yet it is different, because PSAR must work perfectly for any unitary transformation. In particular, for the storing phase we set $|\psi\rangle = |\psi_\perp\rangle$. Then the optimal retrieval is achieved by a quantum teleportation of state $\xi$ using the stored state $|\psi_U\rangle = d^{-1/2}|U\rangle$ (see Fig. S.1). The generalized Bell measurement performed on $\xi$ and one part of $|\psi_U\rangle$ results in an outcome $k$ with probability $1/d^2$. In such case we are left with the second part of $|\psi_U\rangle$ in the state $U\sigma_k\xi\sigma_k U^\dagger$, where $\sigma_k$ are generalized Pauli operators. In case of $\sigma_k = I$ (associated with the Bell measurement projection onto $|\psi_+\rangle$) the stored unitary channel is successfully retrieved. For all the other outcomes, the unwanted $\sigma_k$ rotation can not be undone, because the unitary $U$ is unknown. In conclusion, the teleportation-based PSAR succeeds with probability $1/d^2$. Its optimality follows from our subsequent discussion of the optimal $N \to 1$ PSAR.

**N-to-one probabilistic storage-and-retrieval.**

The general PSAR strategy with $N$ uses of a channel in the storing phase involves all combinations of their parallel, successive and adaptive processing and corresponds to a quantum circuit with open slots, where the $N$ uses of a channel can be inserted. Such framework is described within the theory of quantum networks [11][13][24] and any quantum circuit with open slots is represented by a positive operator (see [27] for a short introduction). The storing network is described by an operator $S$. It accepts $N$ channels as its input and it outputs a memory state $|\psi_U\rangle \in \mathcal{H}_M$ (see Fig. S.2a). As in $1 \to 1$ case the retrieving phase is described by a two-valued instrument $\mathbf{R} = \{\mathcal{R}_s, \mathcal{R}_f\}$. The overall action of PSAR is a composition of $S$ and $\mathbf{R}$ determining a generalized quantum instrument $\mathbf{L} = \{\mathcal{L}_s, \mathcal{L}_f\}$. In the Choi picture the input of PSAR corresponds to $|U\rangle\langle U| \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $L_s \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_{out} \otimes \mathcal{H}_{in})$, where $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H} \otimes \mathcal{N}$. The perfect retrieval condition (similarly to Eq. (S.1)) is

$$
\langle U^\dagger | U \rangle \in \mathcal{L}(\mathcal{H}_M) \quad \forall U \in \text{SU}(d),
$$

(S.2)

where $\lambda$ gives the success probability. Let us stress that the probability of success, i.e. the value of $\lambda$, is required to be the same for all $U \in \text{SU}(d)$. Thanks to this assumption we can without loss of generality apply the methods of [19] to conclude that the optimal storing phase is parallel as illustrated in Fig. S.2b. Consider the decomposition $U \otimes N = \bigoplus_{j \in \text{Irr}(\mathcal{H} \otimes \mathcal{N})} U_j \otimes I_{m_j}$ into irreducible representations (IRRs), where $U_j$ is a unitary operator on $\mathcal{H}_j$ and $I_{m_j}$ denotes the identity operator on the multiplicity space. This corresponds to the following decomposition of the Hilbert space $\mathcal{H}_A := \bigoplus_{j \in \text{Irr}(\mathcal{H} \otimes \mathcal{N})} \mathcal{H}_j \otimes \mathcal{H}_{m_j}$, and we set $d_j = \dim(\mathcal{H}_j)$. The result of [19] implies that the memory state $|\psi\rangle$ can be taken of the following form

$$
|\psi\rangle := \bigoplus_j \sqrt{\frac{p_j}{d_j}} |I_j\rangle \in \mathcal{H}_M \quad p_j \geq 0, \sum_j p_j = 1,
$$

(S.3)

where $I_j$ denotes the identity operator on $\mathcal{H}_j$ and $\mathcal{H}_M := \bigoplus_{j \in \text{Irr}(\mathcal{H} \otimes \mathcal{N})} \mathcal{H}_j \otimes \mathcal{H}_j \subseteq \mathcal{H}_A \otimes \mathcal{H}_A$. The state $|\psi\rangle$ undergoes the action of the unitary channels and becomes
\[ |\psi_U\rangle := \bigoplus_j \sqrt{d_j} |U_j\rangle. \] Clearly, \(|\psi_U\rangle \in \mathcal{H}_M\) for any \(U\).

Let us now focus on the retrieving quantum instrument \(R\) from \(\mathcal{L}(\mathcal{H}_{in} \otimes \mathcal{H}_M)\) to \(\mathcal{L}(\mathcal{H}_{out})\), where in/out labels the system on which the retrieved channel is applied. The perfect retrieval condition is again given by Eq. (S.21) with \(|\psi_1^\ast\rangle = \bigoplus_j \sqrt{d_j} |U_j^\ast\rangle\). As a consequence of Eq. (S.22) the optimal Choi operator \(R_s\) can be chosen to satisfy the commutation relation

\[ [R_s, U'^\ast V' \otimes U_{in} \otimes V_{out}^\ast] = 0, \quad (S.4) \]

where \(U' := \bigoplus_j U_j \otimes I_j, \quad V' := \bigoplus_m I_j \otimes V_j\). Thanks to Eq. (S.21), \(U_j|\psi\rangle = |\psi_j\rangle\) and \(|\psi_j^\ast\rangle = |\psi\rangle\) the perfect retrieval condition becomes

\[ \langle\psi|R_s|\psi\rangle = \lambda|I\rangle\langle I| \quad (S.5) \]

and the success probability reads \(\lambda = \frac{1}{2^d} \langle I|\psi|R_s|\psi\rangle|I\rangle\).

Let us now consider the decomposition

\[ U_j^\ast \otimes U = \bigoplus_{j \in \text{Irr}(U_j^\ast \otimes U)} U_j \otimes I_{m_j^\ast}, \quad (S.6) \]

which induces the Hilbert space decomposition \(\mathcal{H}_J \otimes \mathcal{H} = \bigoplus_{j \in \text{Irr}(U_j^\ast \otimes U)} \mathcal{H}_J \otimes \mathcal{H}_{m_j^\ast}\). Let us denote by \(J, K\) the set of values of \(j\) such that \(U_j \otimes V_K\) is in the decomposition of \(U_j^\ast \otimes V_j \otimes U \otimes V^\ast\). Using Eqs. (S.21) and (S.22) we can assume \(S_j^\ast\) that \(R_j = \bigoplus_{j \in J} I_j \otimes I_j \otimes s_j^\ast\), where \(s_j^\ast := \sum_{j^\prime \in J} I_{j^\prime}^\ast |I_{m_j^\prime}\rangle\langle I_{m_j^\prime}|\). Given this left hand side of Eq. (S.22) reads

\[ \langle\psi|R_s|\psi\rangle = \sum_{j} \lambda_j |I\rangle\langle I| + \nu_j (I - \frac{1}{2^d}|I\rangle\langle I|), \quad (S.7) \]

where \(\nu_j\) are specified in (S.24), \(\lambda_j = \frac{d_j}{2^d} \langle \phi_j|s_j^\ast|\phi_j\rangle\) and \(|\phi_j\rangle = \bigoplus_{j \in I_{j^\prime}} \sqrt{d_j} |I_{m_j^\prime}\rangle\). Since \(R_s \geq 0\), the perfect learning condition of Eq. (S.22) holds only if \(\nu_j = 0\) for all \(J\). Then, the success probability \(\lambda = \sum_j \lambda_j\). The following result translates the optimisation of \(\lambda\) from an operator optimisation problem into a linear program.

**Theorem 1.** For optimal PSAR the success probability \(\lambda\) is given by the following linear programming problem:

\[ \begin{aligned} \text{maximize} & \quad \lambda = \sum_{j \in C} d_j^3 \mu_j, \\ \text{subject to} & \quad 0 \leq d_j \mu_j \leq \frac{p_j}{d_j^2} \quad \forall j \in J, J \quad \forall J \in C, \\ & \quad p_j \geq 0 \quad \sum_{j \in \text{Irr}(U^\ast \otimes U)} p_j = 1, \end{aligned} \quad (S.8) \]

where \(C = \{ J \in \text{Irr}(U^\otimes U^\ast) | dd_j = \sum_{j \in I_{j^\prime}} d_j\}\).

**Proof.** We will sketch only the key steps. The complete proof is in (S.27). First, one shows that \(J \notin C\) implies \(s_j^\ast\). Then, for any \(J \in C\) \(\nu_j = 0\) and \(s_j\) imply that \(|\psi_j\rangle = |\psi_j\rangle\), for some \(\mu_j \geq 0\). Thus, \(\lambda = \sum_{j \in C} \sum_{j \in I_{j^\prime}} d_j^3 \mu_j d_j = \sum_{j \in C} d_j^3 \mu_j\). The constraint that \(R_s\) is a quantum operation gives \(tr_{out}[R_s] \leq I\). Eq. (S.21) implies \(tr_{out}[R_s], U'V' \otimes U_{in}^\ast = 0\) and \(tr_{out}[R_s] = \bigoplus_{j \in I_{j^\prime}} I_j \otimes I_j |d_j^3 \rangle\langle d_j^3|\). Thus, \(d_j \mu_j d_j^3 \leq 1\) must hold for all \(j\) and \(j \in I_{j^\prime}\). Conditions on \(p_j\) are from Eq. (S.50).

**Case study: N → 1 PSAR for qubit channels.** In case of qubit (\(d = 2\)) the decomposition of \(U^\otimes N\) into IRRs of \(SU(2)\) reads \(U^\otimes N = \bigoplus_{j = (N/2)_{mod 2}}^{N/2} U_j \otimes I_m\), where \(m_j = \frac{2j+1}{2} (N/2\pm j)\) and \(U_j\) are the IRRs of spin \(j\) with dimension \(d_j = 2j + 1\). For convenience we work with even \(N\) (for odd \(N\) see (S.27)), \(j = 0, 1, \ldots, N/2\). For \(SU(2)\) the simplest conjugate representation \(U_j^\ast\) is equivalent to \(R_j\). Thus, in Eq. (S.23) we get either \(J = j + 1/2\) or \(J = j - 1/2\). Altogether, \(J\) can have values \(J = C = \{1/2, \ldots, (N - 1)/2\}\). Eq. (S.23) holds only for \(j = 0, 2\) and \(N/2\) can we multiply Eq. (S.7) by \(1 - f_j\) and Eq. (S.10) by \(f_j\), and take the sum for all \(j\). A straightforward calculation gives the upper bound:

\[ \frac{N + 3}{N} \sum_{j = 2}^{N - 1} d_j^3 \mu_j \leq 1 \quad \iff \quad \lambda \leq \frac{N}{N + 3}. \quad (S.11) \]

Finally, by choosing \(p_j = (2j + 1)^2/L, \mu_j + 1/2 = 1/(L(2j + 2))\) (where \(L = (N + 1)(N + 2)(N + 3)/6\)), one proves that that conditions in Eq. (S.50) are satisfied and the upper bound (S.11) is achieved. The knowledge of \(\mu_j\) and \(p_j\) completely specifies the state \(|\psi\rangle\) and the retrieving operation \(R_s\) which can be explicitly expressed (see Eq. (S.22)). Let \(|j, j_2\rangle \in \mathcal{H}_J\) with \(j_2 \in \{\pm j, \ldots, j\}\) be an orthonormal basis of the spin \(j\) IR. By definition \(|I_j\rangle = \sum_{j_2 = -j}^{j} |j, j_2\rangle\otimes |j, j_2\rangle\). Consequently, from Eq. (S.50), the dimension of the quantum memory is \(\dim H_M = \sum_{j_2 = 0}^{N/2} d_j^2 = L\) and the optimal input state for storage is \(|\psi\rangle = \bigoplus_{j = 0}^{N/2} \sqrt{2j + 1} |I_j\rangle\).

**Optimal PSAR for qudit unitary transformations.** The optimization of \(N \to 1\) PSAR of qudit channels follows similar steps as for the qubit case and it exploits a combinatorial identity (Proposition 3 in (S.28)) which was discovered and proved in a byproduct of this analysis.

**Theorem 2.** The optimal probability of success of \(N \to 1\) probabilistic storage and retrieval of a unitary channel \(U(\cdot) = UU^\dagger, U \in SU(d)\) equals \(\lambda = N/(N + 1 + d^2)\). The optimal state for storage is \(|\psi\rangle := \bigoplus_j \sqrt{d_j^3} |I_j\rangle\in \mathcal{H}_M\) where \(L := \sum j^2 d_j^3\) and \(j \in \text{Irr}(U^\otimes N)\).
The proof is given in [27]. Clearly, as $N$ goes to infinity $\lambda \sim 1 - \frac{d^2}{N}$, and $\lambda \approx \frac{1}{2}$ implies $N \approx d^2$. Reminding that a $d$-dimensional unitary transformation has $d^2$ parameters, we see that roughly one use per unknown parameter is needed for reliable storage and retrieval of the transformation. Let us note that the storage state in Theorem 3 is optimal also for the estimation of a group transformation in the maximum likelihood approach [30]. Further, it is worth to stress that the optimal PSAR protocol is achieved by a coherent retrieval, hence, the quantum memory is essential. In contrast, optimal approximate SAR [19] is equivalent to quantum estimation in the maximum fidelity approach and classical memory is sufficient as an output of the storing phase. Use of the optimal storage state in the design of an approximate SAR leads to fidelity that scales as $1 - O(N^{-1})$, however, for the optimal approximate SAR the fidelity scales as $1 - O(N^{-2})$ [19]. This $O(N)$ difference is the price to pay for the perfect retrieval in case of PSAR.

Alignment of reference frames (ARF). Let us note that the correction of alignment errors can be modeled as a PSAR protocol in which $N$ uses of an unknown $U$ are stored and the aim is to retrieve the inverse transformation $U^\dagger$. For $SU(2)$, we can show that, given $N$ uses of $U$, the inverse transformation $U^\dagger$ can be perfectly retrieved with the same optimal probability of success $\lambda$ (see Fig. S.3 and [27]). It follows that the success probability of the probabilistic ARF protocol [8] achieves the optimal scaling $O(N^{-1})$ (see [27]).

Probabilistic port-based teleportation (PPBT) As the first step of PPBT [32] Alice and Bob share $N$ suitably entangled pairs of quantum systems. Their goal is to teleport an unknown state $\xi$ to Bob in a way that this state appears in one of his systems (called ports [33, 34]). In order to achieve this goal (see also Fig. S.4) Alice performs a specific measurement resulting in $n \in \{0, 1, \ldots, N\}$ (0 labels the failure of the protocol), communicates this information to Bob who selects the system from the $n$th port to accomplish the teleportation. If Bob applies a channel $U$ on each of his ports (storing phase) and Alice starts the teleportation (retrieving phase) of $\xi$ afterwards, the $n$th port will output $U(\xi)$. Strictly speaking, we swap $n$th port into a fixed quantum system and effectively we achieve $N \to 1$ PSAR. Let us stress that while any PPBT protocol can be turned into a PSAR protocol, the converse does not hold. In a sense, PPBT scheme provides a structurally simple realization of an optimal PSAR protocol. Our results show that the optimal probability of PPBT [35] coincides with the optimal success probability of PSAR. However, the memory dimension $\dim \mathcal{H}_M$ of the optimal PSAR is exponentially smaller (see the following paragraph) in comparison with $2N$ qudits used in PPBT construction.

Implications for covariant probabilistic programmable processors. Up to now the best bound on the size of the program register for universal covariant probabilistic processors was provided by family of PPBT processors for which $\dim \mathcal{H}_M \approx (d^2-1)^{1/f}$, where $f = 1 - \lambda$ is the failure probability. In contrast, the retrieving phase of optimal $N \to 1$ PSAR defines a class of processors for which the program register size reads $\dim \mathcal{H}_M = \sum_{j \in \text{err}(U^{\otimes N})} d_j^2 = \left(\frac{N+d^2-1}{N}\right)$, where we used Schur’s result [36]. In terms of the failure probability it reads $\dim \mathcal{H}_M \propto (1/f)^{(d^2-1)}$, which is exponentially smaller (for fixed $d$ and $f \to 0$) in comparison with PPBT-based processors. This result can be viewed as a quantification of achievable tradeoffs imposed by the no-programming theorem [27] on universal covariant probabilistic processors. Although PSAR provides only an upper bound on the size of the program register, we conjecture that the lower bound will have the same scaling. However, this question remains open.

Summary. We showed that optimal probabilistic storage-and-retrieval of unknown unitary channels on $d$-dimensional quantum systems can be designed with success probability $\lambda = N/(N-1+d^2)$, where $N$ is the number of uses of the channel in the storing phase. This probability coincides with the success probability for probabilistic port-based teleportation [35], and, for the $SU(2)$ case, with the probability of success for probabilistic alignment of reference frames. Optimal PPBT can be rephrased as an optimal protocol for PSAR, but for the PSAR protocol designed here the storing memory system is exponentially smaller and optimal in this parameter. On the other hand, $N \to 1$ PPBT-based PSAR implements all quantum channels (not only unitary ones), thus, its performance is universal. The question of potential reduction of memory system while keeping the universality for all channels remains open.
Acknowledgments

MS and MZ acknowledge the support by the QuantERA project HIPHOP (project ID 731473), projects QETWORK (APVV-14-0878), MAXAP (VEGA 2/0173/17), GRUPIK (MUNI/G/1211/2017) and the support of the Czech Grant Agency (GAČR) project no. GA16-22211S. AB acknowledges the support of the John Templeton Foundation under the project ID# 60609 Causal Quantum Structures. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

[1] P. Shor, SIAM J. Computing 26 (1997), 1484-1509.
[2] L. K. Grover, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), May 1996, pages 212-219
[3] C. H. Bennett and G. Brassard, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8, New York, 1984
[4] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. 70, 18951899 (1993)
[5] W. K. Wootters and W. H. Zurek, Nature 299, 802 (1982)
[6] V. Bužek, M. Hillery, and R. F. Werner, Phys. Rev. A 60, R2626(R) (1999)
[7] M. A. Nielsen and Isaac L. Chuang, Phys. Rev. Lett. 79, 321 (1997)
[8] Miloslav Dušek and Vladimir Bužek Phys. Rev. A 66, 022112 (2002)
[9] J. Fiurášek, M. Dušek, and R. Filip Phys. Rev. Lett. 89, 190401 (2002)
[10] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996)
[11] V. Scarani, S. Iblisdir, N. Gisin, A. Acín, Rev. Mod. Phys. 77, 1225-1256 (2005)
[12] M. Hillery, V. Bužek, and M. Ziman, Phys. Rev. A 65, 022301 (2002)
[13] N. Gisin, S. Massar, Optimal Quantum Cloning Machines, Phys. Rev. Lett. 79, 2153-2156 (1997)
[14] G. Chiribella, G.M. D’Ariano, and P. Perinotti, Phys. Rev. Lett. 101, 180504 (2008)
[15] A. Bisio, G.M. D’Ariano, P. Perinotti, and M. Sedlák, Phys. Lett. A 378, 1797 (2014)
[16] W. Dur, P. Sekatski, and M. Skotiniotis, Phys. Rev. Lett. 114, 120503 (2015).
[17] G. Chiribella, Y. Yang, and C. Huang, Phys. Rev. Lett. 114, 120504 (2015).
[18] In the literature, the task of storage and retrieval is also called quantum learning.
[19] A. Bisio, G. Chiribella, G. M. D’Ariano, S. Facchini, P. Perinotti, Phys. Rev. A 81, 032324 (2010)
[20] M. Choi, Linear Algebra and its Applications, 10 (3): 285-290, (1975), A. Jamiolkowski, Rep. Math. Phys. 3, 275 (1972).
[21] T. Heinosaari, M. Ziman, The mathematical language og quantum theory, (Cambridge Universituy Press, 2012)
[22] D. Gottesman and I. Chuang, Nature 402, 390 (1999)
[23] G. Chiribella, G. M. D’Ariano, P. Perinotti, Phys. Rev. Lett. 101, 060401 (2008).
[24] G. Chiribella, G. M. D’Ariano, P. Perinotti, Europhysics Letters 83, 30004 (2008).
[25] G. Chiribella, G. M. D’Ariano, P. Perinotti, Phys. Rev. A 80, 022339 (2009).
[26] A. Bisio, G. Chiribella, G. M. D’Ariano, P. Perinotti, Acta Physica Slovaca 61, No.3, 273-390 (2011).
[27] see supplemental material
[28] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. 82, 4344 (1999).
[29] Michal Sedláček, Alessandro Bisio, "On some new hook-content identities”, arXiv:1809.02008
[30] Giulio Chiribella, Giacomo Mauro D’Ariano, Paolo Perinotti, and Massimiliano F. Sacchi Phys. Rev. A 70, 062105 (2004).
[31] Stephen D. Bartlett, Terry Rudolph, Robert W. Spekkens and Peter S. Turner, New J. Phys. 11, 063013 (2009).
[32] S. Ishizaka and T. Hiroshima, Phys. Rev. A 79, 042306 (2009)
[33] S. Ishizaka and T. Hiroshima, Phys. Rev. Lett. 101, 240501 (2008)
[34] M. Mozrzymas, M. Studziski, S. Strelchuk, and M. Horodecki, New J. Phys., Vol. 20, (2018)
[35] M. Studziski, S. Strelchuk, M. Mozrzymas, and M. Horodecki, Sci. Rep. Vol. 7, 10871 (2017)
[36] Issai Schur, ber eine Klasse von Matrizen, die sich einer gegebenen Matrix zuordnen lassen, Doctoral dissertation, Universitt Berlin, 1901; reprinted in Brauer k Rohrback [71, Band I, pp. 172 (1973).
I. SUPPLEMENTAL MATERIAL

This Supplemental Material provides a short introduction to theory of quantum networks, detailed proofs of Theorems 1,2 and more precise clarification of the relation of the presented work to the alignment of reference frames.

II. QUANTUM NETWORKS AND GENERALIZED INSTRUMENTS

The mathematical formalization of the perfect learning of a unitary channel can be easily given within the framework of quantum networks. In this section we provide a small review of the subject and we refer to the literature \cite{13} for a complete presentation.

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

\[
|A\rangle = \sum_{m=1}^{\dim(\mathcal{K})} \sum_{n=1}^{\dim(\mathcal{H})} (m|A|n)\langle m|n\rangle, \tag{S.12}
\]

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

\[
A \otimes B|C\rangle = |ABC^T\rangle \tag{S.13}
\]

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

\[
\mathcal{O}(\rho) = \mathcal{O} \otimes \rho =: O \otimes \rho \tag{S.15}
\]

where we introduce the link product between the operators \( O \) and \( \rho \). The composition of two quantum operations can be represented in terms of their Choi operators too. Let us consider two quantum operations \( \mathcal{O}, \mathcal{O}' \) with multipartite input and output, i.e. \( \mathcal{O} \) goes from \( \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2) \) to \( \mathcal{L}(\mathcal{H}_3 \otimes \mathcal{K}) \) and \( \mathcal{O}' \) goes from \( \mathcal{L}(\mathcal{H}_4 \otimes \mathcal{K}) \) to \( \mathcal{L}(\mathcal{H}_5 \otimes \mathcal{K}_6) \). We can connect the output of \( \mathcal{O} \) on \( \mathcal{L}(\mathcal{K}) \) with the input of \( \mathcal{O}' \) on \( \mathcal{L}(\mathcal{K}) \) obtaining a new quantum operation from \( \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_4) \) to \( \mathcal{L}(\mathcal{H}_3 \otimes \mathcal{H}_5 \otimes \mathcal{H}_6) \). The Choi operator of the resulting quantum operation is given by the link product of the two quantum operations, as follows:

\[
\mathcal{O}' * \mathcal{O} = \text{Tr}_K[(\mathcal{O}' \otimes I_{456})(I_{123} \otimes \mathcal{O}^{T_K})] \tag{S.16}
\]

where \( \mathcal{O}^{T_K} \) denotes the partial transposition of \( \mathcal{O} \) on the Hilbert space \( \mathcal{K} \) and \( I_{ijk} \) denotes the identity operator on \( \mathcal{H}_i \otimes \mathcal{H}_j \otimes \mathcal{H}_k \). We can interpret Eq. (S.15) as an instance of Eq. (S.16).

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

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\mathcal{O}_1 & \mathcal{O}_2 & \mathcal{O}_3 & \mathcal{O}_N \\
2N-2 & 2N-1 & \cdots & \end{array}
\]

where the floating wires correspond to the input and output systems of the quantum network. \( \mathcal{R} \) is called a deterministic quantum network if all the quantum operations in Eq. (S.17) 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 \( \mathcal{R} \) obeys the following constraints

\[
\text{Tr}_{2k-1}[R^{(k)}] = I_{2k-2} \otimes R^{(k-1)} \quad k = 1, \ldots, N \tag{S.18}
\]

where, referring to the diagram in Eq. (S.17), the Hilbert space of the wire labelled by \( j \) is \( \mathcal{H}_j \), \( R^{(j)} = R \), \( R^{(0)} = I \), \( R^{(k)} \in \mathcal{L}(\mathcal{H}_{odd5} \otimes \mathcal{H}_{even5}) \) with \( \mathcal{H}_{even5} = \bigotimes_{j=0}^{k-1} \mathcal{H}_{2j+1} \) and \( \mathcal{H}_{odd5} = \bigotimes_{j=0}^{k-1} \mathcal{H}_{2j} \). \( R^{(k)} \) is the Choi operator of the reduced network \( \mathcal{R}^{(k)} \) obtained by discarding the last \( N-k \) teeth. The set of positive operators satisfying Eq. (S.18) and the set of deterministic quantum networks are in one to one correspondence. On the other hand, a given deterministic quantum network \( \mathcal{R} \) 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 \( \mathcal{T} \), must satisfy

\[
0 \leq T \leq R \tag{S.19}
\]

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

$$\mathcal{T} = \begin{bmatrix} C_1 & 1 & 2 & 3 & 2N-2 & 2N-1 \end{bmatrix}. \quad (S.20)$$

A set of probabilistic quantum networks $\{\mathcal{R}_i\}$, with the same input and output wires, is called a generalised quantum instrument if the sum of their Choi operators $\sum_i \mathcal{R}_i =: \mathcal{R}$ is the Choi operator of a deterministic quantum network. As in the analogous case of quantum instruments, 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 some input. If the outcome $i$ is obtained then it means that the probabilistic quantum network $\mathcal{R}_i$ 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 which it belongs to.

### III. RELEVANT SUB-BLOCKS OF RETRIEVING OPERATION $R_s$

As we stated in the main text, Choi operator $R_s$ of the retrieving operation can be chosen to satisfy the commutation relation

$$[R_s, U'^* V' \otimes U_{in} \otimes V_{out}^*] = 0, \quad (S.21)$$

where $U' := \bigoplus_{j} U_j \otimes I_j, \quad V' := \bigoplus_{j} I_j \otimes V_j$. We remind also the perfect retrieving condition

$$\langle \psi | R_s | \psi \rangle = \lambda |\langle I \rangle| |\langle I \rangle|. \quad (S.22)$$

For convenience we placed here also the decomposition

$$U_j^* \otimes U = \bigoplus_{j \in \text{Irr}(U_j^* \otimes U)} U_j \otimes I_{m(j)}, \quad (S.23)$$

which induces the Hilbert space decomposition

$$\mathcal{H}_j \otimes \mathcal{H} = \bigoplus_{j \in \text{Irr}(U_j^* \otimes U)} \mathcal{H}_j \otimes \mathcal{H}_{m(j)}. \quad (S.24)$$

First, we notice that the multiplicity spaces $\mathcal{H}_{m(j)}$ and $\mathcal{H}_{m(j)}$ are one dimensional and therefore $I_{m(j)}$ are rank one. 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 $U$ is 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 [3]. Then we have that

$$U' V' \otimes U^* \otimes V^* = \bigoplus_{jK} U_j \otimes V_K \otimes I_{m(jK)} \quad (S.25)$$

induces decomposition $\mathcal{H}_{m(jK)} = \bigoplus_{jK} \mathcal{H}_{m(j)} \otimes \mathcal{H}_{m(j)}$, where $jK$ 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 $\dim(\mathcal{H}_{m(j)}) = 1$ we stress that $\langle I_{m(j)} | I_{m(j')} \rangle = \delta_{j,j'}$ and $\mathcal{H}_{m(j)} = \text{span}(\{|I_{m(j)}\}, j \in jK)$.

From Eq. (S.25) the commutation relation of Eq. (S.21) becomes $[R_s, \bigoplus_{jK} U_j \otimes V_K \otimes I_{m(j)}] = 0$, which, thanks to the Schur’s lemma, gives

$$R_s = \bigoplus_{jK} I_j \otimes I_K \otimes s^{(JK)}, \quad (S.26)$$

where $s^{(JK)} \in \mathcal{L} (\mathcal{H}_{m(jK)}), \quad s^{(JK)} \geq 0$. Due to $|\langle I \rangle|^{\langle I \rangle}$ being a rank one operator and $R_s$ being the sum of the positive operators from Eq. (S.26) we have that Eq. (S.22) holds if and only if

$$\langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle = \lambda_{jK} |\langle I \rangle| |\langle I \rangle| \quad \forall j, K. \quad (S.27)$$

From the identity $I_j \otimes I = \bigoplus_{jJ} \text{Irr}(U_j^* \otimes U_j) I_j \otimes I_{m(j)}$ (we remind that $I_{m(j)}$ has rank one), we obtain

$$|\langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle |^2 = \sum_j \lambda_{jK} \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \quad (S.28)$$

$|\langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle |^2 = \sum_j \lambda_{jK} \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \langle \psi | I_j \otimes I_K \otimes s^{(JK)} | \psi \rangle \quad (S.29)$

Using Eqs. (S.26), (S.28) into $\lambda = \frac{1}{d} |\langle I | \langle \psi | R_s | \psi \rangle | |\langle I \rangle| |\langle I \rangle|$ we obtain

$$\lambda = \sum_j \lambda_{jK} \quad \lambda_{jK} = \frac{d}{\sqrt{d}} \langle \phi_j | s^{(JK)} | \phi_j \rangle \quad (S.30)$$

where the $\lambda_{jK}$’s were defined in Eq. (S.27). It is now easy to show that we can assume

$$R_s = \bigoplus_{jK} I_j \otimes I_K \otimes s^{(JK)}, \quad (S.31)$$

where $s^{(J)} := \sum_{j,j'K} \delta_{j,j'} |\langle I_j \otimes I_K \otimes s^{(JK)} | I_{m(j')} \rangle|$. 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 $R_s = \bigoplus_{jK} I_j \otimes I_K \otimes s^{(JK)}$ where $s^{(J)} = s^{(JK)}$ and $R'_s = \bigoplus_{jK} I_j \otimes I_K \otimes s^{(JK)}$. Since both $R_s$ and $R'_s$ are positive and $R_s + R'_s = R_s$, we have that $\text{Tr}_D(R'_s) \leq I$ implies $\text{Tr}_D(R_s) \leq I$ i.e. $R_s$ is a quantum operation. Finally, from Eq. (S.28) 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 our optimization problem.

### IV. EXPLICIT FORM OF THE RETRIEVED CHANNEL

Due to commutation relation (S.21) and the form of $R_s$ given by Eq. (S.31) the retrieved channel has the
following Choi operator

$$\langle \psi | R_s | \psi \rangle = \sum_{j} \lambda_j |I\rangle \langle I| + \nu_j \left( I - \frac{1}{2} |I\rangle \langle I| \right). \quad (S.32)$$

As we stated in the main text the perfect retrieving condition is satisfied if and only if $\nu_j = 0$ for all $J$. This happens because positive-semidefiniteness of $R_s^{(j)} := I_j \otimes I_j \otimes s^{(j)}$ implies $\nu_j \geq 0$ and the requirement $\sum_j \nu_j = 0$ implies that all the terms must vanish. Let us study separately every operator $R_s^{(j)}$, which by definition satisfies the commutation relation of Eq. (S.21). We have that

$$\langle \psi | R_s^{(j)} | \psi \rangle =$$

$$\langle \psi | (U^*U^* \otimes U^* \otimes U) R_s^{(j)} (U^*U^* \otimes U^* \otimes U)^\dagger | \psi \rangle =$$

$$(U^* \otimes U) \langle \psi | R_s^{(j)} | \psi \rangle (U^* \otimes U)^\dagger \forall U \quad (S.33)$$

Thanks to the Schur’s lemma Eq. (S.33) gives

$$\langle \psi | R_s^{(j)} | \psi \rangle = \lambda_j |I\rangle \langle I| + \nu_j \left( I - \frac{1}{2} |I\rangle \langle I| \right). \quad (S.34)$$

By taking the trace of Eq. (S.34) we have

$$\text{Tr}[(\psi | R_s^{(j)} | \psi)] = \langle \psi | \text{Tr}_{out} \left[ R_s^{(j)} \right] | \psi \rangle =$$

$$\langle \psi | \sum_{j,j\in J} I_j \otimes I_j | \psi \rangle =$$

$$\sum_{j,j\in J} p_j q_j^{(j)} = \lambda_j d + \nu_j(d^2 - 1)$$

$$q_j^{(j)} := \frac{d_j^2}{d_j^2} s^{(j)}.$$  \hspace{1cm}(S.35)

If we insert Eq. (S.29) into Eq. (S.30) we have

$$\lambda_j = \frac{d_j}{d^2} \sum_{j,j\in J} \sqrt{p_j p_j'} s^{(j)}.$$  \hspace{1cm}(S.36)

From Eq. (S.35) and Eq. (S.36) we have

$$\nu_j = 0 \iff$$

$$\sum_{j,j'\in J} \delta_{j,j'} d_j \sqrt{p_j p_j'} s^{(j)} - \sqrt{p_j p_j'} s^{(j')} = 0,$$  \hspace{1cm}(S.37)

which is the most explicit form of the perfect retrieving condition that constrains the relation between the state $|\psi\rangle$ parametrized by probabilities $p_j$ and the structure of the retrieving operation parameterized by $s^{(j)}$.  

**Lemma 1.** Suppose a matrix $X = \sum_{j,j'} X_{jj'} |j\rangle \langle j'| \geq 0$ obeys $\sum_{j,j'} X_{jj'} = \sum_j \frac{1}{c_j} X_{jj}$, where $c_j > 0$ and $\sum_j c_j = 1$. This implies $X \propto |\chi\rangle \langle \chi|$, where $|\chi\rangle = \sum_j c_j |j\rangle$.

**Proof.** Let us define

$$|v\rangle := \sum_j |j\rangle$$ (S.38)

$$|\rho\rangle := \sum_j \sqrt{X_{jj}} |j\rangle$$ (S.39)

$$A := \sum_j \frac{1}{c_j} X_{jj} |j\rangle \langle j|$$ (S.40)

The condition $\sum_{j,j'} X_{jj'} = \sum_j \frac{1}{c_j} X_{jj}$ can be written as

$$\langle v | A - X | v \rangle = 0.$$  \hspace{1cm}(S.41)

Matrix $H_{ij}$ is positive semidefinite if and only if $H_{ij} \geq 0$ $\forall i$ and $|H_{ij}| \leq \sqrt{H_{ii} H_{jj}}$ $\forall i \neq j$. Using this criterion and $\sum_j c_j = 1$ one can easily show that both $A - |\rho\rangle \langle \rho|$ are positive semidefinite matrices. Moreover, using $\Re (X_{jj'}) \leq |X_{jj'}|$ $\leq \sqrt{X_{jj} X_{jj'}}$ one can easily prove the inequality

$$\langle v | (A - X) | v \rangle \geq \langle v | (A - |\rho\rangle \langle \rho|) | v \rangle,$$  \hspace{1cm}(S.42)

which also gives

$$\langle v | (A - X) | v \rangle = 0 \implies \langle v | (A - |\rho\rangle \langle \rho|) | v \rangle = 0,$$  \hspace{1cm}(S.43)

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

$$\langle v | A | v \rangle = \langle \rho | B | \rho \rangle$$  \hspace{1cm}(S.44)

$$B := \sum_j \frac{1}{c_j} |j\rangle \langle j|$$  \hspace{1cm}(S.45)

As a consequence we have

$$\langle v | (A - |\rho\rangle \langle \rho|) | v \rangle = \langle \rho | (B - |v\rangle \langle v|) | \rho \rangle.$$  \hspace{1cm}(S.46)

Thanks to $c_j > 0 \forall j$ we have that $B - |v\rangle \langle v|$ is a positive matrix, which has either trivial or one dimensional kernel. This together with Eqs. (S.33), (S.46) allows us to write a necessary condition for matrix $X$

$$\langle \rho | (B - |v\rangle \langle v|) | \rho \rangle = 0 \implies B |\rho\rangle - |v\rangle \langle v| \rho \rangle = 0.$$  \hspace{1cm}(S.47)

Explicitly solving the above equation we get the only possible solution

$$\frac{1}{c_j} \sqrt{X_{jj}} = \frac{1}{c_{j'}} \sqrt{X_{jj'}} \implies X_{jj} = \mu c_j^2,$$  \hspace{1cm}(S.49)

which is unique up to a constant $\mu$, as we expected due to the rank one deficiency of $B - |v\rangle \langle v|$. Once the diagonal elements $X_{jj}$ respect Eq. (S.49) we have

**V. N → 1 PSAR AS A LINEAR PROGRAMMING PROBLEM**

In this section we provide complete proof of Theorem 1 from the main text. First, we prove the following technical lemma, which will be needed.
\langle \psi | (A - |\langle \rho |) |\psi \rangle = 0, \text{ but to fulfill LHS of Eq. (S.43) we need also the saturation of the bound (S.42). This happens if and only if}
\[ X_{jj'} = \sqrt{X_{jj}} \sqrt{X_{jj'}}, \] (S.50)
which together with Eq. (S.49) proves the claim of the lemma.

Let us restate Theorem 1 from the main text.

**Theorem 3.** For optimal PSAR the success probability \( \lambda \) is given by the following linear programming problem:

\[
\begin{align*}
\text{maximize} & \quad \lambda = \sum_{\mu, \nu} d^j_{\mu, j}, \\
\text{subject to} & \quad 0 \leq d_{\mu, j} \leq \frac{p_j}{d_j} \quad \forall j \in J, j \in C \\
& \quad p_j \geq 0 \quad \sum_{j \in \text{Irr}(U^*)} p_j = 1,
\end{align*}
\]

where \( C = \{ J \in \text{Irr}(U^{\otimes N} \otimes U^*) | dd_j = \sum_{j \in j, j} d_j \} \).

**Proof.** We first need to examine relations between IRR’s that appear in the decomposition of \( U^{\otimes N} \) and those that appear in \( \bigoplus_{j \in \text{Irr}(U^{\otimes N})} U^{(j)} \otimes U^* \).

We remind that 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 \( U \) is represented by a single box \( \Box \) and \( \text{Irr} \) defined via \( U^* \) is represented by a column of \( d - 1 \) boxes.

Decomposition of \( U^{\otimes N} \) into IRRs can be obtained by collecting the decompositions of the tensor products \( U_k \otimes U \) of all Young diagrams \( k \) appearing with multiplicity \( m_k \) in the decomposition of \( U^{\otimes N-1} \) and putting together equivalent IRRs (those with the same Young diagram). This can be mathematically stated as follows. Let \( \text{Irr}(U^{\otimes N}) \) denote the set of Young diagrams that appear in the decomposition of \( U^{\otimes N} \) into IRRs of \( SU(d) \). We have that \( K \in \text{Irr}(U^{\otimes N}) \) if and only if \( \exists k \in \text{Irr}(U^{\otimes N-1}) \) such that \( K \in \text{Irr}(U_k \otimes U) \) and \( m_K = \sum_{k \in k} m_k \), where \( k \) denotes the set of values of \( k \) such that \( U_k \) is in the decomposition of \( U_k \otimes U \). On the other hand, thanks to Schur-Weyl duality the multiplicity \( m_K = \tilde{d}_K (m_k = \tilde{d}_k) \) is given by the dimension of the IRRs of the symmetric group \( S(N) \) (\( S(N - 1) \)) with the Young diagram \( K \) (\( k \)), respectively. Hence, we obtained a known identity \( \Box \)
\[
\tilde{d}_K = \sum_{k \in k} \tilde{d}_k, \] (S.52)
where \( k \) can be equivalently specified as those Young diagrams \( k \), which by addition of a single box become \( K \).

Next, we consider decomposition of \( U_j \otimes U^* \) (or more conveniently \( U^* \otimes U_j \)), where \( j \in \text{Irr}(U^{\otimes N}) \). We denote Young diagram \( Y_j \) with \( r \) rows and \( n_i \) boxes in the \( i \)-th row as \( (n_1, n_2, \ldots, n_r) \). A valid Young diagram of \( SU(d) \) IRR has \( r \leq d \), \( n_r > 0 \) and \( n_i \geq n_{i+1} \quad \forall i \) (we set \( n_{r+1} = 0 \)). Rows \( i \) in which \( n_i > n_{i+1} \) we call corners of \( (n_1, n_2, \ldots, n_r) \) and we denote the number of corners by \( s \) and we write \( i \in \text{Cor} \). Suppose \( Y_j \leftrightarrow (n_1, n_2, \ldots, n_r) \) has \( r \leq d - 1 \). Then the decomposition of \( U^{*} \otimes U_j \) contains \( s + 1 \) Young diagrams each with multiplicity one. One of them is given as Young diagram \( (n_1 + 1, n_2 + 1, \ldots, n_r + 1, 1, \ldots, 1) \) with \( d - 1 \) rows, which we denote \( Y_j \) and for each \( i \in \text{Cor} \) we have Young diagram \( Y_j \otimes U \leftrightarrow (n_1, n_2, \ldots, n_r) \). The above statement follows from the Littlewood-Richardson rules \( \Box \) if one realizes, that either one of the corner boxes completes the first column into \( d \) boxes (the remaining boxes can be only attached to the right in the original order) or the whole Young diagram is attached from the right to the column of \( d - 1 \) boxes. If \( Y_j \leftrightarrow (n_1, n_2, \ldots, n_r) \) has \( r = d \) the situation is the same except for the diagram \( Y_j \) not appearing in the decomposition, because it would not be a valid Young diagram. Let us note that Young diagram \( Y_j \) can emerge in our setting only from diagram \( Y_i \) where \( i = j \). We can also easily verify that \( dd_j \neq d_j \), which can be seen from the formula for the dimension of \( SU(d) \) IRRs \( \Box \) by calculating the fraction \( d_{ij} / d_j \) for a general \( j \). Therefore, we conclude that for \( J = \{ j \} \) Eq. (S.37) can be satisfied only if \( s_{ij} = 0 \), which in turn thanks to Eq. (S.30) implies \( \lambda_j = 0 \). Thus, Young diagrams \( C = \{ Y_{ij}, j \in \text{Irr}(U^{\otimes N}) \} \) correspond to those \( J \) that do not belong to the set \( C \) defined in the theorem.

On the other hand, consistently with the notation for \( \overline{C} \), we define \( C = \{ Y_{i}, j \in \text{Irr}(U^{\otimes N}), i \in \text{Cor} \} \). Let us remind that \( \text{Irr}(U^{\otimes N}) \) is exactly constituted by all Young diagrams consisting of \( N \) boxes and having at most \( d \) rows. This implies \( C = \{ \text{Irr}(U^{\otimes N-1}) \} \), because by removing in any possible way a single box from Young diagrams in \( \text{Irr}(U^{\otimes N}) \) we get all possible Young diagrams in \( \text{Irr}(U^{\otimes N-1}) \). More operationally, for any Young diagram \( J \in C \) we can add a box to the first row and get some element \( j \in \text{Irr}(U^{\otimes N}) \), which can be reversed to prove the claim.

Moreover, for every subset \( C_j = \{ Y_{i}, i \in \text{Cor} \} \) of \( C \) we have that
\[
\tilde{d}_j = \sum_{j \in C_j} \tilde{d}_j, \] (S.53)
which is just a reformulation of Eq. (S.52), because Young diagrams \( J \in C_j \) have \( N - 1 \) boxes and an addition of a single box changes them to Young diagram \( j \) consisting of \( N \) boxes.

Let us pick any element \( J \in C \). Let us now specify all the Young diagrams \( Y_j, j \in \text{Irr}(U^{\otimes N}) \), which contain \( J \) in the decomposition of \( U_j \otimes U^* \). We denote such set \( J \) and it coincides with \( j \) defined below Eq. (S.25). These are such Young diagrams \( j \) in which by removing one corner box we get \( Y_j \). This is the same as saying that \( j \) is the set of Young diagrams of \( SU(d) \) group that can be obtained from \( J \) by addition of a single box, because \( \text{Irr}(U^{\otimes N}) \) contains all possibly emerging Young diagrams. This implies that \( dd_j = \sum_{j \in j} d_j \), because this corresponds to the decomposition of an operator \( U_j \otimes U \),
which acts on $dd_J$ dimensional space. Thus, we proved that the set $C$ can be equivalently defined as

$$
C = \{ J \in \text{Irr}(U^\otimes N \otimes U^*) | dd_J = \sum_{j \in J} d_j \}
$$

$$
= \{ J \setminus \mu, J \in \text{Irr}(U^\otimes N), i \in \text{Cor}_J \}
$$

$$
= \text{Irr}(U^\otimes N^{-1})
$$

(S.54)

Furthermore, we showed that for $J \notin C$ $s^J = 0$ and consequently $\lambda_J = 0$.

In order to proceed we apply Lemma 1 for every $J \in C$. Expression $\sqrt{\frac{\mu_J p_j d_j}{p_j d_j}} s^{(J)}_{jj}$ plays the role of $X_{jj'}$, $c^j = \frac{d_j}{\mu_J}$ and the remaining assumption is guaranteed by Eq. (S.29). As a consequence, we get that the condition

$$
s_{jj'}^{(J)} = \mu_J \sqrt{\frac{d^2_j d^2_{j'}}{p_j p_{j'}}}, \quad \forall J \in C
$$

(S.55)

Thus, fulfillment of Eq. (S.55) guarantees the perfect retrieving of unitary transformations and we can rewrite the probability of success as

$$
\lambda = \sum_{J \in C} \sum_{j,j' \in J} \frac{d_j d_{j'}}{\mu_J d_j d_{j'}} = \sum_{J \in C} d_J^3 \mu_J,
$$

(S.56)

where we used Eqs. (S.25), (S.30) and the defining property of the set $C$.

The constraint that $R_s$ is a quantum operation translates into its Choi operator as $\text{Tr}_D[R_s] \leq I$. Since $R_s$ satisfies Eq. (S.21), we obtain $[\text{Tr}_D[R_s], U'V' \otimes U_2^\otimes] = 0$, which implies $\text{Tr}_D[R_s] = \bigoplus J \bigoplus e_{j,j}, J \otimes J \frac{d_j}{d_j} s_{jj'}^{(J)}$. This implies

$$
\text{Tr}_D[R_s] \leq I \iff \frac{d_j}{d_j} s_{jj'}^{(J)} \leq 1 \quad \forall J, \forall j \in J.J.
$$

(S.57)

Let us express the above condition via coefficients $\mu_J$ using Eq. (S.55)

$$
\mu_J d_j^2 \leq \frac{p_j}{d_j}, \quad \forall J, \forall j \in J.J.
$$

(S.58)

Let us remind the definition of state $|\psi\rangle$ from the main text.

$$
|\psi\rangle := \bigoplus J \sqrt{\frac{p_j}{d_j}} |I_j\rangle \in \tilde{H} \quad p_j \geq 0, \sum_j p_j = 1
$$

(S.59)

Collecting Eqs. (S.56), (S.55), (S.58) and (S.59) we see that the optimization of probabilistic storage and retrieval is reduced to a linear program stated in the Theorem 3.

VI. $N \rightarrow 1$ PSAR FOR QUBIT CHANNELS - THE CASE OF ODD $N$

All the steps are completely analogical to the derivation valid for even $N$ presented in the main text. 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. For odd $N$ (identically as for even $N$) the investigation of the conditions of perfect learning reveals that $s^{\frac{N-1}{2}}$ has to be zero. On the other hand, $J = 0$ can be involved in the perfect storing and retrieving. Other expressions remain identical, but now $J$ is an integer. In particular, we choose $f_J$ according to the same formula as in the main text

$$
f_J = \frac{1}{2} \frac{2j}{2j+1} \left( \frac{2j+2}{N} + 1 \right)
$$

(S.60)

and the whole proof goes on analogically to the case of even $N$.

VII. $N \rightarrow 1$ PSAR FOR QUDIT CHANNELS - THE GENERAL CASE OF $SU(d)$

The goal of this section is to prove Theorem 3 from the main text.

Theorem 4. The optimal probability of success of $N \rightarrow 1$ probabilistic storage and retrieval of a unitary channel $U(.) = U.U^\dagger, U \in SU(d)$ equals $\lambda = N/(N-1+d^2)$. The optimal state for storage is $|\psi\rangle := \bigoplus J \sqrt{\frac{d_j}{d_j}} |I_j\rangle \in \mathcal{H}$ where $L := \sum_j d_j^2$ and $j \in \text{Irr}(U^\otimes N)$.

Proof. The idea of the proof is analogous to the case of qubit unitary transformations. However, in the qudit case the relations between IRRs are more complicated and we will need some of the facts derived in the proof of Theorem 3 and a new combinatorial identities, which were derived in [6] by some of us.

Let us define positive function

$$
f(J, J) = \frac{\tilde{d}_J}{d_J},
$$

(S.61)

for all $j \in \text{Irr}(U^\otimes N)$, $J \in C_j$ or equivalently for all $J \in \text{Irr}(U^\otimes N^{-1})$, $j \in J J = j$. Let us note that thanks to Eq. (S.53) we have

$$
\sum_{J \in C_j} f(J, J) = 1 \quad \forall j \in \text{Irr}(U^\otimes N).
$$

(S.62)

For the proof of the main theorem we need a new theorem from combinatorics [6] and a technical lemma.

Theorem 5. For any Young diagram $J$ consisting of $N-1$ boxes it holds that

$$
\sum_{j \in J^3} (C_j - R_j)^2 \tilde{d}_j = N(N-1) \tilde{d}_J
$$

(S.63)
where the sum runs through all Young diagrams \( j \) that can be obtained from \( J \) by addition of a single box,

- \( \tilde{d}_j, \bar{d}_j \) are dimensions of IRRs of the symmetric group \( S(N-1), S(N) \), respectively
- \( C_j \) is the number of the column of the added box,
- \( R_j \) is the number of the row of the added box that leads from diagram \( J \) to the diagram \( j \).

**Lemma 2.** For any Young diagram \( J \in \text{Irr}(U^\otimes N^{-1}) \) the following identity for dimensions \( d_j, \bar{d}_j \) of IRRs of \( SU(d) \) group and for dimensions of \( \tilde{d}_j, \bar{d}_j \) of the symmetric group, holds

\[
\sum_{j \in jJ} \frac{d_j^2}{d_j} = \frac{N - 1 + d^2}{N} \sum_j \frac{\bar{d}_j}{\bar{d}_j}, \quad \forall J \in \text{Irr}(U^\otimes N^{-1}),
\]

where \( jJ = \{ j \in \text{Irr}(U^\otimes N) \mid J \in \text{Irr}(U^\otimes U^*) \} \).

**Proof.** Let us remind expressions for the dimensions of IRRs that are involved (for detailed explanation see [4]):

\[
d_j = \frac{l_j}{h_j}, \quad \bar{d}_j = \frac{l_j}{\bar{h}_j}, \quad \tilde{d}_j = \frac{N!}{h_j}, \quad (S.65)
\]

where \( h_j, \bar{h}_j \) denote the hook lengths factors and \( l_j \) is the number of the row (column) of the current box from the Young diagram \( j \). Using Eq. (S.65) we can write Eq. (S.64) as

\[
\sum_{j \in jJ} \frac{l_j^2 h_j}{l_j^2} \frac{\bar{h}_j}{\bar{h}_j} = d^2 + N - 1 \quad (S.66)
\]

Thus, proving Lemma 2 is equivalent to proving that Eq. (S.66) holds. We start by direct evaluation of the left hand side. We obtain:

\[
\sum_{j \in jJ} \frac{l_j^2 h_j}{l_j^2} \frac{\bar{h}_j}{\bar{h}_j} = \sum_{j \in jJ} (d - R_j + C_j)^2 \frac{h_j}{h_j}
\]

where \( R_j \) is the row number and \( C_j \) the column number of the additional box in Young diagram \( Y_j \) with respect to \( Y_J \). At this point it is useful to realize that for Young diagrams \( J \in \text{Irr}(U^\otimes N^{-1}) \) with \( d \)-rows, there is a difference between the set \( jJ = jJ \) and the set \( J \) of all Young diagrams that can be obtained from \( J \) by addition of a single box. The difference is exactly one Young diagram, which is obtained from \( J \) by adding the box into the \( d + 1 \)-th row, in the first column. Luckily, the bracket \( (d - R_j + C_j) \) for this diagram evaluates to zero \((d - (d + 1) + 1 = 0)\), so we can sum also through this term in Eq. (S.67) without changing its value. This is useful especially for \( d < N \), because later on we want to apply Theorem 5 where the summation runs through the set \( J \). Thus, left hand side of Eq. (S.66) can be equivalently rewritten as

\[
\sum_{j \in jJ} \frac{l_j^2 h_j}{l_j^2} \frac{\bar{h}_j}{\bar{h}_j} = \sum_{j \in jJ} (d - R_j + C_j)^2 \frac{h_j}{h_j} = F + G + H,
\]

where we expanded the square and we defined

\[
F = d^2 \sum_{j \in jJ} \frac{h_j}{h_j}, \quad G = \sum_{j \in jJ} (C_j - R_j)^2 \frac{h_j}{h_j}, \quad H = \sum_{j \in jJ} 2d(C_j - R_j) \frac{h_j}{h_j}.
\]

It is known [7] that

\[
\sum_{j \in jJ} \tilde{d}_j = N \tilde{d}_J, \quad \forall J \in \text{Irr}(U^\otimes N^{-1}), \quad (S.71)
\]

which can be using Eq. (S.65) equivalently rewritten as

\[
\sum_{j \in jJ} \frac{h_j}{h_j} = 1, \quad \forall J \in \text{Irr}(U^\otimes N^{-1}). \quad (S.72)
\]

Using the identity (S.72) we have that \( F = d^2 \). Moreover, we have

\[
\sum_{j \in jJ} (d - R_j + C_j) \frac{h_j}{h_j} = d \sum_{j \in jJ} \frac{h_j}{h_j} + \sum_{j \in jJ} (C_j - R_j) \frac{h_j}{h_j} = d, \quad (S.73)
\]

where we used Eq. (S.54) and the fact that \( d_j = 0 \) if \( j \) has more than \( d \) rows. On the other hand

\[
\sum_{j \in jJ} (d - R_j + C_j) \frac{h_j}{h_j} = d \sum_{j \in jJ} \frac{h_j}{h_j} + \sum_{j \in jJ} (C_j - R_j) \frac{h_j}{h_j} = d + \frac{1}{2d} H, \quad (S.74)
\]

and then \( H = 0 \). Combining the above considerations equation (S.68) reads

\[
\sum_{j \in jJ} \frac{l_j^2 h_j}{l_j^2} \frac{\bar{h}_j}{\bar{h}_j} = d^2 + \sum_{j \in jJ} (C_j - R_j)^2 \frac{h_j}{h_j}.
\]

Comparing Eq. (S.76) with Eq. (S.66) we conclude we still need to prove

\[
\sum_{j \in jJ} (C_j - R_j)^2 \frac{h_j}{h_j} = N - 1. \quad (S.77)
\]

Luckily, the above equation is exactly the claim of Theorem 5 written using Eq. (S.65). Thus, relying on Theorem 5 we conclude the proof.
Let us define $J$ and insert them into Eqs. (S.51). It is easy to see that the upper bound (S.81) can be saturated. One can choose $p_j$ as follows

\[
\lambda = \sum_{J \in \text{Irr}(U^{\otimes N}-1)} \sum_{j \in I(J)} \frac{d_j}{d_J} J_{-j} \mu_J
\]

and insert them into Eqs. (S.51). It is easy to see that requirements on $p_j$ are satisfied and inequalities between $p_j$ and $\mu_J$ are actually all saturated. Let us now evaluate $\lambda$. Inserting Eq. (S.82) into Eq. (S.51) we obtain

\[
\lambda = \sum_{J \in C} \frac{d_j^2}{d_J^2} \\sum_{k \in \text{Irr}(U^{\otimes N})} \frac{1}{d_k^2} \\sum_{j \in I(J)} \frac{d_j}{d_J^2} \mu_J
\]

where we used Lemma 2, exchanged the order of the sums and used the Eq. (S.62). Thanks to knowledge of $\mu_J$ and $p_j$ we can completely specify the state $|\psi\rangle$ and the retrieving operation $R_{\psi}$. Thus, we can build valid storing and retrieving strategy, which succeeds with probability $N/(N - 1 + d^2)$ saturating the upper bound (S.81) and concluding the proof.

\[\square\]

VIII. ALIGNMENT OF REFERENCE FRAMES

We now review the quantum protocol for the alignment of reference frames in a quantum communication scenario, as it was considered in Ref. [8]. Let us consider the scenario in which one party, called Alice, wants to send a qubit to another distant party, denoted as Bob. If the qubit is encoded into a spin-1/2 particle Bob can recover the quantum state $|\varphi\rangle$ if he and Alice share a reference frame for orientation. Otherwise, the lack of a shared frame amounts to having a noisy channel and retrieving strategy, which succeeds with probability $N/(N - 1 + d^2)$.

There are two differences between this protocol and the SAR we consider in our work. The first difference is that the token $|\psi\rangle$ plays the role of the storage state. $|\psi\rangle$ is a multipartite state $|\psi\rangle \in \mathcal{H}^{\otimes N}$.

\[\bullet\] The effect of the misalignment can be thought of as the storing phase in which the state $|\psi_U\rangle := U^{\otimes N} |\psi\rangle$ is created.

\[\bullet\] In the retrieving phase, Bob exploits the state $|\psi_U\rangle$ to retrieve the inverted channel $U^\dagger$ which is applied to the qubit $U |\varphi\rangle$.

There are two differences between this protocol and the SAR we consider in our work. The first difference is that $N$ uses of $U$ are given, but we are required to retrieve $U^\dagger$. However, for $U \in SU(2)$, we can show that our optimal PSAR protocol which stores $U^{\otimes N}$ and retrieves $U$, can be turned into a PSAR protocol which retrieves $U^\dagger$ with the same probability of success. If we had $|\psi_U\rangle$, then the retrieval phase of our optimal PSAR protocol would recover $U^\dagger$ with the optimal probability of success $\lambda$ (which is the same for any $U \in SU(2)$). In particular, for $U \in SU(2)$, the storage state $|\psi_U\rangle$ can be created by exploiting $N$ uses of $U$ as follows

\[
|\psi_U\rangle = U^{\otimes N} \otimes I |\psi\rangle = I \otimes U^{\star \otimes N} |\psi\rangle
\]

where $|\psi\rangle$ is the optimal state for storage.
The second difference between SAR and the alignment protocol is that we are not allowed to use an external reference system, i.e. the ancillary system $H_A'$ in our protocol, since it would correspond to a partially shared reference frame. Since our protocol is less constraint than the alignment protocol, the probability of success $\lambda$ of PSAR is an upper bound for the probability of success of perfect alignment. However, both the strategy of Ref. [8] and the optimal PSAR protocol achieve the same $O(N^{-1})$ scaling, which is then optimal.

[1] G. Chiribella, G. M. D’Ariano, P. Perinotti, Phys. Rev. Lett. 101, 060401 (2008).
[2] G. Chiribella, G. M. D’Ariano, P. Perinotti, Phys. Rev. A 80, 022339 (2009).
[3] A. Bisio, G. Chiribella, G. M. D’Ariano, P. Perinotti, Acta Physica Slovaca 61, No.3, 273-390 (2011).
[4] W. Fulton, J. Harris, "Representation Theory: A First Course", Springer (2013)
[5] R. P. Stanley, S. Fomin, Enumerative Combinatorics, Vol. 2 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1999. doi:10.1017/CBO9780511609589.
[6] Michal Sedlák Alessandro Bisio, "On some new hook-content identities", arXiv:1809.02008
[7] A. M. Vershik, Hook formula and related identities, Journal of Soviet Mathematics 59 (5) (1992) 1029-1040. doi:10.1007/BF01480684.
[8] Stephen D. Bartlett, Terry Rudolph, Robert W. Spekkens and Peter S. Turner, New J. Phys. 11, 063013 (2009).