Perfect probabilistic storage and retrieval of phase gates

Michal Sedlák
RCQI, Institute of Physics,
Slovak Academy of Sciences,
Dúbravská cesta 9,
84511 Bratislava, Slovakia
Centre of Excellence IT4Innovations,
Faculty of Information Technology,
Brno University of Technology,
Božetěchova 2/1,
612 00 Brno, Czech Republic

Mário Ziman
RCQI, Institute of Physics,
Slovak Academy of Sciences,
Dúbravská cesta 9,
84511 Bratislava, Slovakia
Faculty of Informatics,
Masaryk University,
Botanická 68a,
60200 Brno, Czech Republic

Probabilistic storage and retrieval (PSR) of unitary dynamics is possible with exponentially small failure probability if we count the number of systems used as quantum memory [PRL 122, 170502 (2019)]. For $N \to 1$ PSR of qubit phase gates we derive improved optimal success probability $N/(N+1)$ due to prior knowledge that the gate rotates the qubit by an unknown angle a round Z axis. Using programmable phase gate [PRL 88, 047905 (2002)] we propose optimal $(2^k - 1) \to 1$ phase gate PSR using k CNOT gates.

1 Introduction

Discovery of Shor's algorithm [1] boosted research investigating capabilities of quantum systems for computation and information processing. In analogy with classical computers people envisioned a quantum computer, which would have at its heart a quantum processor realizing a fixed unitary transformation on data and program quantum bits (qubits). Ideally the transformation should be universal, i.e. by choice of the state of the program register the machine could be programmed to perform any desired (unitary) transformation on the data qubits. However, Nielsen and Chuang [2] 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. Quantum mechanics is intrinsically random and we anyway expect to design probabilistic algorithms. Thus, one could still hope that very good approximate processors can be found, or one can consider heralded operation of the device, i.e. the device either performs the desired operation exactly or it signalizes that it failed. Since we can look at any part of a quantum algorithm as on quantum processor detailed knowledge of their limits is vital for our understanding of the limits of quantum information processing. Although some upper bounds on the achievable performance of approximate or probabilistic processors exist [3] there are still gaps between them and performance of the processors that were found so far.

The task of storage and retrieval of unitary transformations studies how quantum dynamics can be stored into a quantum state and later retrieved. In our previous paper [4] we investigated probabilistic storage and retrieval of unitary transformations, which allowed us to find covariant probabilistic universal quantum processors with exponentially smaller program register than those known before. In the present submission we would like to see how the situation changes under different prior knowledge of the transformation to be stored and we aim at presenting also practical description of how such probabilistic processors can be implemented in practice using elementary quantum gates.

More precisely, 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 uniformly randomly and we have access only to

Submitted to:
QPL 2020

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 part of the task is called storage. Later, after we lost access to $\mathscr{U}$, we are requested to apply $\mathscr{U}$ on an unknown state ξ. Our goal is chose storage and retrieval 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. [5] and it was termed quantum learning. Perfect probabilistic version of the problem, termed *probabilistic storage and retrieval of a unitary channel*(PSR) was considered by Sedlák et. al. [4]. The main difference is that we want to retrieve the quantum channel from the quantum memory only without error and with highest possible probability, which was found to be $\lambda = N/(N-1+d^2)$. In this submission we study how this optimal success probability changes if we have some a priori knowledge about the unitary transformation to be stored. In particular, we study PSR of qubit phase gates, i.e. qubit unitary transformations, which in computation basis acts as

$$U_\varphi = |0\rangle\langle 0| + e^{i\varphi}|1\rangle\langle 1|. \tag{1}$$

After finding the optimal success probability and the description of the protocol on the abstract level, we will also search for some efficient realization of the PSR protocol in terms of quantum circuit composed from elementary quantum gates.

The rest of the submission is organized as follows. We use formalism of quantum combs in section 2 for derivation of the optimal protocol and its description on the level of overall transformations. We find that the optimal success probability increases from $N/(N+3)$ for PSR of an arbitrary qubit unitary transformation to $N/(N+1)$ for PSR of phase gates. Section 3 shows how a single use of a phase gate can be optimally stored and retrieved using just a single qubit storage, one CNOT gate and a single qubit measurement for retrieval. Section 4 gathers observations from previous two sections to describe circuit realization of the optimal protocol via a ancillary qudit and controlled shift gate followed be a measurement of the qudit. Section 5 specializes on $2 \to 1$ PSR of phase gates, i.e. a case, where the gate can be accessed twice in the storage phase. For this we minimized the CNOT gate count by hand and we present a 3-qubit quantum circuit containing 8 CNOTs. Finally, in section 6 we show that proposal of Vidal, Masanes and Cirac [9] for realization of programmable phase gate can be turned into $(2^k-1) \to 1$ PSR of phase gates in such a way that it performs optimally and requires only k CNOT gates, while having exponentially small failure probability in k. It seems that as a consequence of our results on PSR of phase gates we can close an longstanding open question Vidal, Masanes and Cirac had [9] about optimality of their programmable phase gate for arbitrary k, because such problem can be understood as a single point of a bigger set in which we are optimizing over.

2 Optimal Probabilistic Storage and Retrieval of phase gates

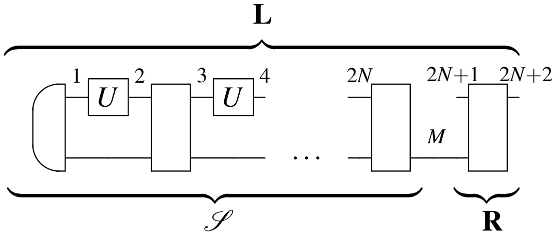
From mathematical perspective the calculations here follow exactly the same steps as in [4], however here the transformation is not chosen completely randomly from $U(2)$, but rather from its $U(1)$ subgroup. Therefore, the structure of the irreducible subspaces changes and effectively this paves the way to higher success probability. The main aim of this section is to prove the following theorem.

Theorem 1. *The optimal probability of success of $N \to 1$ probabilistic storage and retrieval of an unknown qubit phase gate U_φ equals $\lambda = N/(N+1)$.*

Proof

The whole storage and retrieval protocol can be described as follows. In the storing phase we use the N copies of the unknown U_φ to produce some state $|\psi_\varphi\rangle \in \mathscr{H}_M$. During the retrieving phase both the state

$|\psi_\varphi\rangle$ 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 $\mathscr{U}_\varphi(\xi) = U_\varphi(\xi)U_\varphi^\dagger$. Any possible way in which storing and retrieving can be done (parallel or sequential application of U_φ, or any other intermediate approach) is mathematically described by inserting the N uses of the unitary channel $\mathscr{U}_\varphi$ into N open slots of a generalized quantum instrument (see supplementary material of [4] for a short review, or [6, 7, 8]) $\mathbf{L} = \{\mathscr{L}_s, \mathscr{L}_f\}$:



(2)

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 $|\psi_\varphi\rangle$. 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 $\mathscr{U}_\varphi$ i.e.

$$L_s * \left(\bigotimes_{i=1}^{N} |U_\varphi\rangle\rangle\langle\langle U_\varphi|_{2i-1,2i} \right) = \lambda |U_\varphi\rangle\rangle\langle\langle U_\varphi|_{2N+1,2N+2} \qquad (3)$$

where we used the link product formalism reviewed in Section **??** 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 $U_\varphi \xi U_\varphi^\dagger \in \mathscr{L}(\mathscr{H}_{2N+2})$. By expressing the link product in the above Eq. (3) explicitly the requirement of perfect probabilistic storing and retrieving can be stated as

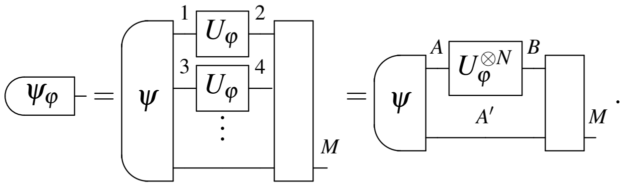
$$\langle\langle U_\varphi^*|^{\otimes N} L_s |U_\varphi^*\rangle\rangle^{\otimes N} = \lambda |U_\varphi\rangle\rangle\langle\langle U_\varphi| \qquad \forall \varphi \in [0, 2\pi]. \qquad (4)$$

We stress that the probability of success, i.e. the value of λ is required to be the same for all $\varphi \in [0, 2\pi]$. The aim of our analysis is to derive the optimal probabilistic quantum network L_s, which obeys the constraint of Eq. (4) and maximizes the value of λ.

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

$$[L_s, U_\varphi^{\otimes N} \otimes U_\vartheta^{\otimes N} \otimes (U_\varphi^*)_{2N+1} \otimes (U_\vartheta^*)_{2N+2}] = 0 \qquad \forall \varphi, \vartheta \in [0, 2\pi]. \qquad (5)$$

This can be proven by showing that any optimal strategy can be made covariant, while keeping the same success probability. As a consequence of Eq. (5), it was proved in [5] that the optimal storing phase is *parallel*, i.e. the N uses of the unknown unitary are applied in parallel on a quantum state $|\psi\rangle$ as shown in the following diagram:



(6)

Where we made a suitable relabeling of the Hilbert spaces. Let us now consider the decomposition of $U_\varphi^{\otimes N} \in \mathscr{L}(\mathscr{H}_A)$ into irreducible representations (irreps) of $U(1)$

$$U_\varphi^{\otimes N} = \bigoplus_{j=0}^{N} e^{ij\varphi} \otimes I_{m_j} \tag{7}$$

where I_{m_j} denotes the identity operator on the multiplicity space. Let us remind that all irreps of $U(1)$ are one dimensional ($\dim(\mathscr{H}_j) = 1$) and $e^{ij\varphi}$ represents the element $e^{i\varphi} \in U(1)$. Eq. (7) induces the following decomposition of the Hilbert space $\mathscr{H}_A$

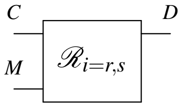
$$\mathscr{H}_A := \bigoplus_j \mathscr{H}_j \otimes \mathscr{H}_{m_j} \qquad \dim(\mathscr{H}_{m_j}) = m_j. \tag{8}$$

It was shown in [5] that the optimal state $|\psi\rangle$ for the storage can be taken of the following form

$$|\psi\rangle := \bigoplus_j \sqrt{p_j} |I_j\rangle\rangle \in \tilde{\mathscr{H}} \qquad p_j \geq 0,\ \sum_j p_j = 1 \tag{9}$$

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 $|\psi_\varphi\rangle := \bigoplus_j \sqrt{p_j} e^{ij\varphi} |I_j\rangle\rangle$. Clearly, $|\psi_\varphi\rangle$ belongs to $\mathscr{H}_M$ which is a subspace of $\mathscr{H}_B \otimes \mathscr{H}_{A'}$ isomorphic to $\tilde{\mathscr{H}}$.

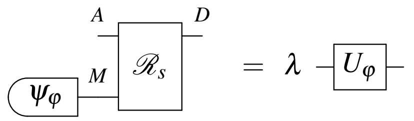
We can focus our attention to the retrieving quantum instrument $\{\mathscr{R}_s, \mathscr{R}_f\}$ from $\mathscr{L}(\mathscr{H}_C \otimes \mathscr{H}_M)$ to $\mathscr{L}(\mathscr{H}_D)$



. (10)

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

$$\begin{aligned} R_s * |\psi_\varphi\rangle\langle\psi_\varphi| &= \mathrm{Tr}_M[R_s((|\psi_\varphi\rangle\langle\psi_\varphi|)^T \otimes I_{C,D})] \\ &= \langle\psi_\varphi^*|R_s|\psi_\varphi^*\rangle = \lambda |U_\varphi\rangle\rangle\langle\langle U_\varphi| \quad \forall\varphi \in [0, 2\pi] \end{aligned} \tag{11}$$



, (12)

where $|\psi_\varphi^*\rangle = \bigoplus_j \sqrt{p_j} e^{-ij\varphi} |I_j\rangle\rangle$. The optimal R_s can be chosen to satisfy the following commutation relation:

$$\left[R_s, U'_\varphi U'_\vartheta \otimes (U_\varphi^*)_C \otimes (U_\vartheta)_D^*\right] = 0, \qquad U'_\varphi := \bigoplus_j e^{ij\varphi}\, I_j \otimes I_j. \tag{13}$$

which is clearly the analog of Eq. (5) where $U_\varphi^{\otimes N} \otimes U_\vartheta^{\otimes N}$ has been replaced by $U'_\varphi U'_\vartheta$. Then, reminding that $U'_\varphi|\psi\rangle = |\psi_\varphi\rangle$ and $|\psi^*\rangle = |\psi\rangle$, from Eq. (13) we have

$$\langle\psi_\varphi^*|R_s|\psi_\varphi^*\rangle = \lambda |U_\varphi\rangle\rangle\langle\langle U_\varphi| \quad \forall\varphi \iff \langle\psi|R_s|\psi\rangle = \lambda |I\rangle\rangle\langle\langle I|\,. \tag{14}$$

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

$$\begin{aligned} \underset{|\psi\rangle,R_s}{\text{maximize}} \quad & \lambda = \frac{1}{4}\langle\langle I|\langle\psi|R_s|\psi\rangle|I\rangle\rangle \\ \text{subject to} \quad & \langle\psi|R_s|\psi\rangle = \lambda|I\rangle\rangle\langle\langle I| \\ & |\psi\rangle \text{ as in Eq. (9)} \\ & R_s \text{ obeys Eq. (13)} \\ & \mathrm{Tr}_D[R_s] \leq I\ . \end{aligned} \tag{15}$$

Let us now consider the decomposition

$$e^{ij\varphi}I_j\otimes U^*_\varphi = \bigoplus_{J\in\mathsf{J}_j} e^{iJ\varphi}I_J\otimes I_{m_J^{(j)}} \qquad \mathscr{H}_j\otimes\mathscr{H} = \bigoplus_{J\in\mathsf{J}_j}\mathscr{H}_J\otimes\mathscr{H}_{m_J^{(j)}} \tag{16}$$

where we remind that the index j labels the irreducible representations in the decomposition of $U_\varphi^{\otimes N}$ and we denote with J_j the set of values of J such that $e^{iJ\varphi}$ is in the decomposition of $e^{ij\varphi}I_j\otimes U^*_\varphi$. 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. Then we have

$$U'_\varphi U'_\vartheta\otimes U^*_\varphi\otimes U^*_\vartheta = \bigoplus_{J,K=-1}^{N} e^{iJ\varphi}I_J\otimes e^{iK\vartheta}I_K\otimes I_{m_{JK}} \qquad \mathscr{H}_{m_{JK}} = \bigoplus_{j\in\mathsf{j}_{JK}}\mathscr{H}_{m_J^{(j)}}\otimes\mathscr{H}_{m_K^{(j)}} \tag{17}$$

where j_{JK} denotes the set of values of j such that $e^{iJ\varphi}e^{iK\vartheta}$ is in the decomposition of $e^{ij\varphi}I_j\otimes e^{ij\vartheta}I_j\otimes U^*_\varphi\otimes U^*_\vartheta$. 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 $\mathscr{H}_{m_{JJ}} = \mathrm{span}(\{|I_{m_J^{(j)}}\rangle\rangle\}, j\in\mathsf{j}_{JJ})$.

From Eq. (17) the commutation relation of Eq. (13) becomes

$$\left[R_s, \bigoplus_{J,K=-1}^{N} e^{iJ\varphi}I_J\otimes e^{iK\vartheta}I_K\otimes I_{m_{JK}}\right] = 0 \tag{18}$$

which, thanks to the Schur's lemma, gives

$$R_s = \bigoplus_{J,K=-1}^{N} I_J\otimes I_K\otimes s^{(JK)} \qquad s^{(JK)}\in\mathscr{L}(\mathscr{H}_{m_{JK}})\ , s^{(JK)}\geq 0 \tag{19}$$

From Eq. (19) 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

$$\langle\psi|R_s|\psi\rangle = \lambda|I\rangle\rangle\langle\langle I| \iff \langle\psi|I_J\otimes I_K\otimes s^{(JK)}|\psi\rangle = \lambda_{JK}|I\rangle\rangle\langle\langle I| \quad \forall J,K \tag{20}$$

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

From the identity $I_j\otimes I = \bigoplus_{J=j-1}^{j} I_J\otimes I_{m_J^{(j)}}$ (we remind that $I_{m_J^{(j)}}$ has rank one), we obtain

$$\begin{aligned} |\psi\rangle|I\rangle\rangle &= \bigoplus_{j=0}^{N}\bigoplus_{J=j-1}^{j}\sqrt{p_j}|I_J\rangle\rangle|I_{m_J^{(j)}}\rangle\rangle = \bigoplus_{J=-1}^{N}\bigoplus_{j\in\mathsf{j}_{JJ}}\sqrt{p_j}|I_J\rangle\rangle|I_{m_J^{(j)}}\rangle\rangle = \bigoplus_{J=-1}^{N}|I_J\rangle\rangle|\phi_J\rangle \\ |\phi_J\rangle &:= \bigoplus_{j\in\mathsf{j}_{JJ}}\sqrt{p_j}|I_{m_J^{(j)}}\rangle\rangle. \end{aligned} \tag{21}$$

Using Eq. (19) into Eq. (15) we obtain

$$\lambda_{JK} = \delta_{JK}\lambda_J, \qquad \lambda = \sum_{J=-1}^{N} \lambda_J \qquad \lambda_J = \frac{1}{4}\langle \phi_J | s^{(JJ)} | \phi_J \rangle \tag{22}$$

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

$$R_s = \bigoplus_J I_J \otimes I_J \otimes s^{(J)} \qquad s^{(J)} := \sum_{j,j' \in \mathrm{j}_{JJ}} s^{(J)}_{jj'} |I_{m_J^{(j)}}\rangle\rangle\langle\langle I_{m_J^{(j')}}| \tag{23}$$

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. (22) 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 (15).

If R_s is of the form of Eq. (23) we can express the constraint of Eq. (**??**) in terms of the operators $s^{(J)}$ as follows:

$$s^{(J)}_{j,j'} = \frac{\mu_J}{\sqrt{p_j p_{j'}}} \quad J = 0, \ldots, N-1, \quad s^{(-1)} = s^{(N)} = 0, \tag{24}$$

where μ_J is some number, which must be non-negativite due to positive-semidefinitness of R_S. The proof of Eq. (24) is given in appendix A.

Fulfillment of Eq. (24) guarantees the perfect storing and retrieving of phase gates and we can rewrite the probability of success as

$$\lambda = \sum_{J=-1}^{N} \lambda_J = \sum_{J=0}^{N-1} \frac{1}{4} \sum_{j,j' \in \mathrm{j}_{JJ}} \sqrt{p_j} \frac{\mu_J}{\sqrt{p_j p_{j'}}} \sqrt{p_{j'}} = \sum_{J=0}^{N-1} \mu_J, \tag{25}$$

where we used Eqs. (22), (24).

Let us now consider the constraint $\mathrm{Tr}_D[R_s] \leq I$. Since R_s satisfies Eq. (13), we have that $\left[\mathrm{Tr}_D[R_s], U'_\varphi U'_\vartheta \otimes (U^*_\varphi)_C\right] = 0$ implies

$$\mathrm{Tr}_D[R_s] = \bigoplus_{J=-1}^{N} \bigoplus_{j \in \mathrm{j}_{JJ}} I_J \otimes I_j s^{(J)}_{jj} \tag{26}$$

From Eq. (26) we have

$$\mathrm{Tr}_D[R_s] \leq I \Leftrightarrow s^{(J)}_{jj} \leq 1 \;\; J = -1, \ldots, N, \; \forall j \in \mathrm{j}_{JJ}. \tag{27}$$

Thanks to Eq. (24) the above can be expressed as inequalities between μ_J and p_j as

$$\mu_J \leq p_j \quad \forall j \in \mathrm{j}_{JJ} \;\; J = 0, \ldots, N-1 \tag{28}$$

Collecting Eqs.(25),(28) and (9) the optimization of perfect probabilistic storing and retrieving can be reduced to

$$\begin{array}{ll} \underset{\mu_J, p_j}{\text{maximize}} & \lambda = \displaystyle\sum_{J=0}^{N-1} \mu_J, \\ \text{subject to} & 0 \leq \mu_J \leq p_j \quad \forall j \in \mathrm{j}_{JJ} \;\; J = 0, \ldots, N-1 \\ & p_j \geq 0 \quad \displaystyle\sum_j p_j = 1, \end{array} \tag{29}$$

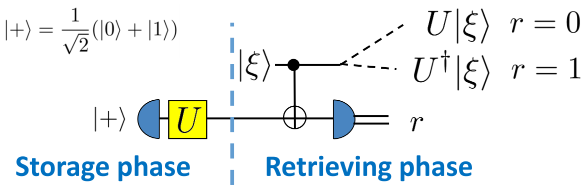

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|\xi\rangle$
$U|\xi\rangle$ $r=0$
$U^\dagger|\xi\rangle$ $r=1$
$|+\rangle$
U
r
Storage phase
Retrieving phase

Figure 1: Optimal 1 → 1 PSR of phase gates.

Let us write two inequalities that are given by Eq. (28) for any $J = 0,\dots,N$

$$\mu_J \leq p_J \tag{30}$$
$$\mu_{J-1} \leq p_J \tag{31}$$

We define coefficient $f_J \in [0,1]$ for $J = 0,\dots,N$ via the formula $f_J = (N-J)/N$. Since $f_0 = 1$ and $f_N = 0$ we can multiply Eq. (30) by f_J and Eq. (31) by $1 - f_J$ sum them up for all J. We obtain

$$\sum_{J=0}^{N} f_J\ \mu_J\ + (1-f_J)\ \ \mu_{J-1}\ \leq \sum_{J=0}^{N} p_J = 1 \tag{32}$$

The above inequality can be rewritten as $\sum_{J=0}^{N-1} \frac{N+1}{N} \mu_J \leq 1$, which proves that $\lambda \leq N/(N+1)$. Let us mention that the coefficient f_j was intentionally chosen so that the coefficient multiplying μ_J is constant and we get an upper bound on λ in Eq. (29).

Finally, we finish the proof of Theorem 1 by showing that the obtained upper bound can be saturated. One can simply choose $p_j = \frac{1}{N+1}$ $j = 0,\dots,N$ $\mu_J = \frac{1}{N+1}$ $J = 0,\dots,N-1$ and check that conditions in Eq. (29) are satisfied and $\lambda = N/(N+1)$. 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.

3 1 → 1 PSR of phase gate

From the general derivation in the previous section it follows that the maximum probability with which we can store and retrieve a phase gate if we apply it only once during the storage is $1/(1+1) = 1/2$. Such success probability can be easily obtained (see Fig. (2)) if we apply the gate on a state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and feed the resulting state as a program state into stochastic programmable gate for U(1) operations proposed by Vidal, Masanes, and Cirac [9]. Action of the gate U_φ on state $|+\rangle$ results in a state $|\psi_\varphi\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$. Suppose for simplicity of the explanation that the state on which the retrieved gate should act is a pure state $|\xi\rangle = \alpha|0\rangle + \beta|1\rangle$, but thanks to linearity of quantum mechanics all works for mixed states as well. The CNOT gate $C_\oplus$ whose control qubit is in a state $|\xi\rangle$ and target qubit is in the state $|\psi_\varphi\rangle$ acts as

$$\begin{aligned} C_\oplus(|\xi\rangle \otimes |\psi_\varphi\rangle) &\mapsto \frac{1}{\sqrt{2}}(\alpha|00\rangle + \alpha e^{i\varphi}|01\rangle + \beta|11\rangle + \beta e^{i\varphi}|10\rangle \\ &= U_\varphi|\xi\rangle \otimes \frac{1}{\sqrt{2}}|0\rangle + U_{-\varphi}|\xi\rangle \otimes \frac{1}{\sqrt{2}}|1\rangle \end{aligned} \tag{33}$$

We see that measurement of the second (target) qubit in the computational basis will with probability $1/2$ yield zero and with $1/2$ outcome one. In case of outcome zero, the first qubit is collapsed into the desired state $U_\varphi|\xi\rangle$. Otherwise, the resulting state is rotated in the Z axis in the opposite direction by an unknown angle, which we cannot correct without further resources.

4 $N \to 1$ PSR of phase gate: qudit realization

The aim of this section is to generalize the construction presented in the previous section for general N. Thanks to $U(1)$ irreps being one-dimensional it is sufficient not to use ancillary system when the unknown gate U_φ is acting on the input state $|\psi\rangle$. Thus, instead of taking $|\psi\rangle$ as in Eq. (9) we can take $|\psi\rangle = \sum_{j=0}^{N} \frac{1}{\sqrt{N+1}}|v_j\rangle \in \mathscr{H}_A$, where $|v_j\rangle$ is any normalized vector defining an irrep $e^{ij\varphi}$ of $U(1)$ in $\mathscr{H}_A$, i.e. any computational basis state with j ones. The reason is that a fixed unitary can interlink those two $N+1$-dimensional subspaces and the value of the amplitudes $\sqrt{p_j} = 1/\sqrt{N+1}$ follows from proof of Theorem 1.

Let us denote the above $N+1$-dimensional subspace $V_D = span\{|v_j\rangle\}_{j=0}^{N}$ as a virtual qudit, whose dimension is $D = N+1$ and we denote its basis states as $\{|t\rangle \equiv |v_t\rangle\}_{t=0}^{N}$. We denote $P_D = \sum_{t=0}^{N}|t\rangle\langle t|$ the projector onto V_D, and by $P_D^\perp = I - P_D$ the projector onto its orthocomplement. During the storage state $|\psi\rangle \in V_D \subset \mathscr{H}_A$ evolves into $|\psi_\varphi\rangle = \frac{1}{\sqrt{N+1}}\sum_{j=0}^{N} e^{ij\varphi}|v_j\rangle \in V_D$. We can now define a channel $\mathscr{E}$, which maps from $\mathscr{H}_A$ to V_D and on V_D acts as identity. This is achieved by

$$\mathscr{E}(\rho) = P_D\, \rho\, P_D + Tr(\rho P_D^\perp)|t_0\rangle\langle t_0|, \tag{34}$$

where $\rho \in \mathscr{L}(\mathscr{H}_A)$ and $|t_0\rangle$ is some state in V_D. In particular, $Tr(|\psi_\varphi\rangle\langle\psi_\varphi|P_D^\perp) = 0$, thus $\mathscr{E}(|\psi_\varphi\rangle\langle\psi_\varphi|) = |\psi_\varphi\rangle\langle\psi_\varphi|$, since $|\psi_\varphi\rangle \in V_D$. Next, we define *a control shift-down gate* $C_\ominus$ as a bipartite gate with control qubit and a target qudit via the formula

$$C_\ominus|c\rangle \otimes |t\rangle \mapsto |c\rangle \otimes |t \ominus c\rangle. \tag{35}$$

Suppose that the state on which the retrieved gate should act is again a pure state $|\xi\rangle = \alpha|0\rangle + \beta|1\rangle$. The control shift-down gate $C_\ominus$ whose control qubit is in a state ξ and target qubit is in the state $|\psi_\varphi\rangle$ acts as

$$\begin{aligned} C_\ominus(|\xi\rangle \otimes |\psi_\varphi\rangle) \mapsto & \alpha|0\rangle \otimes \frac{1}{\sqrt{N+1}}\sum_{t=0}^{N} e^{it\varphi}|t\rangle + \beta|1\rangle \otimes \frac{1}{\sqrt{N+1}}\left(\sum_{t=1}^{N} e^{it\varphi}|t-1\rangle + |N\rangle\right) \\ &= U_\varphi|\xi\rangle \otimes \frac{1}{\sqrt{N+1}}\sum_{t=0}^{N-1} e^{it\varphi}|t\rangle + U_{-N\varphi}|\xi\rangle \otimes \frac{e^{iN\varphi}}{\sqrt{N+1}}|N\rangle \end{aligned} \tag{36}$$

Last step of the implementation is a measurement of the qudit in its computational basis $\{|t\rangle\}_{t=0}^{N}$. The probability of observing outcome t is $1/(N+1)$ and it is calculated as $Tr\left(C_\ominus(|\xi\rangle\langle\xi| \otimes \mathscr{E}(|\psi_\varphi\rangle\langle\psi_\varphi|))C_\ominus^\dagger\; I \otimes |t\rangle\langle t|\right)$. The post-measurement state of a qubit is in case of outcome $t = 0,\dots,N-1$ the same and reads

$$U_\varphi|\xi\rangle\langle\xi|U_\varphi^\dagger = Tr_2\left(C_\ominus(|\xi\rangle\langle\xi| \otimes \mathscr{E}(|\psi_\varphi\rangle\langle\psi_\varphi|))C_\ominus^\dagger\; I \otimes |t\rangle\langle t|\right). \tag{37}$$

while for outcome $t = N$ the qubit collapses into a state $U_{-N\varphi}|\xi\rangle\langle\xi|U_{-N\varphi}^\dagger$. At this point it is easy to see that the presented implementation of the storage and retrieval of the phase gate would work also for mixed input states ξ due to linearity of quantum mechanics. We conclude that the presented realization succeeds with optimal probability $N/(N+1)$, since this is the total probability of obtaining result other than $t = N$.

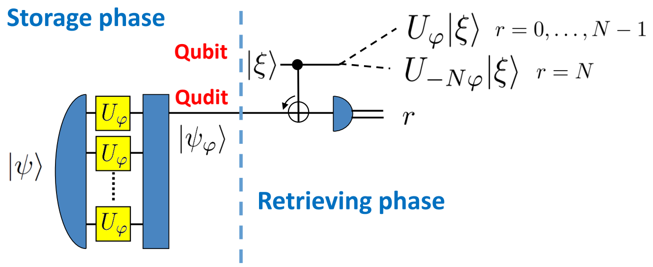


Figure 2: Optimal $N \to 1$ PSR of phase gates - principal scheme.

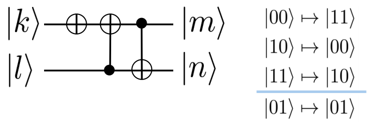

$|k\rangle$
$|l\rangle$
$|m\rangle$
$|n\rangle$
$|00\rangle \mapsto |11\rangle$
$|10\rangle \mapsto |00\rangle$
$|11\rangle \mapsto |10\rangle$
$|01\rangle \mapsto |01\rangle$

Figure 3: Small quantum circuit performing shift down operation in the subspace $V_3 = span\{|00\rangle, |10\rangle, |11\rangle)\}$ of two qubits.

5 $2 \to 1$ PSR of phase gates

This section specializes on the case, where the gate U_φ can be accessed twice in the storage phase. We present a design of the optimal circuit, which follows the ideas from the previous section, but our aim here is to decompose all the operations into elementary quantum gates [10]. The first part of the circuit (see figure 4) formed by a CNOT gate, $R_y(\pi/4) = \exp[i\frac{\pi}{8}\sigma_y]$, $R_y(-\pi/4)$ and one qubit gate

$$M = \begin{pmatrix} \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \\ \sqrt{\frac{2}{3}} & \frac{-1}{\sqrt{3}} \end{pmatrix} \tag{38}$$

transforms the second and third qubit from state $|00\rangle$ into state

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle). \tag{39}$$

$$\tag{40}$$

The action of phase gate U_φ on the second and third qubit leads to a state $|\psi_\varphi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + e^{i\varphi}|10\rangle + e^{i2\varphi}|11\rangle)$. We chose subspace $V_3 = span\{|00\rangle, |10\rangle, |11\rangle)\}$ as our virtual qutrit. Using σ_x and two CNOT gates one can construct shift down operation in the V_3 subspace as we illustrate in figure 3. In the retrieving part we can perform the controlled shift down gate (see Eq. (35)) by simply adding a control qubit to those three gates (see figure 4). The resulting quantum circuit for $2 \to 1$ PSR of phase gates contains 2 Toffoli gates, 2 CNOT gates, and 3 fixed one qubit gates. The success or failure of the retrieval is determined by the outcomes of the measurement of second and third qubit in the computational basis. Outcome 01 never appears, 11 corresponds to failure and 00, 10 signalize successful retrieval of the phase gate. One can verify by a direct calculation that the success probability is $2/3$ and the related post-measurement state is $U_\varphi|\xi\rangle$.

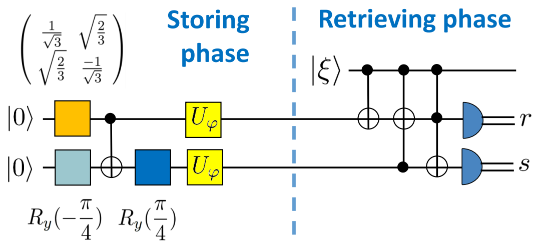


Figure 4: Optimal 2 → 1 PSR of phase gates using 2 CNOT gates, 2 Toffoli gates and 3 fixed one qubit gates.

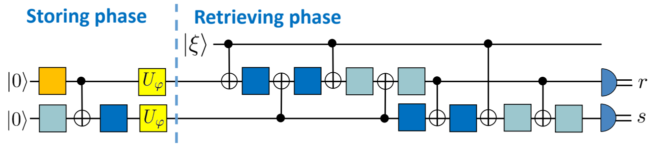


Figure 5: Optimal 2 → 1 PSR of phase gates using 8 CNOT gates and 11 fixed one-qubit gates. The color coding of one-qubit gates is the same as in figure 4.

Finally, the two Toffoli gates can be decomposed into elementary gates. Exact implementation of each Toffoli gate requires 6 CNOT gates [11]. However, we can be more efficient, because we have two Toffoli gates next to each other. We can employ a 3-CNOT circuit (see [10] page 16) that differs from Toffoli gate only by a phase of one state ($|100\rangle \mapsto -|100\rangle$). Luckily, this unwanted additional phase can be in our case cancelled (by suitable choice of the first and the second control qubit when using [10] page 16) as we had two Toffoli gates next to each other. In this way 6 CNOT gates can be saved. The resulting quantum circuit is depicted on figure 5. One can verify by a direct calculation that the unitary transformation performed by the two Toffoli gates (from figure 4) is exactly reproduced by the last 6 CNOT gates surrounded by 8 one qubit gates in figure 5. We conclude that we designed a quantum circuit containing 8 CNOT gates and 11 fixed one-qubit gates, which performs optimal 2 → 1 PSR of phase gates.

6 $(2^k - 1) \to 1$ PSR of phase gates

Designing a quantum circuit build from elementary gates and achieving optimal $N \to 1$ PSR of phase gates for arbitrary N seems to be a challenging task. Already for $2 \to 1$ PSR of phase gates as we saw in the previous section it is not easy to find circuit containing low number of CNOT gates. For this reason it seems rather surprising if we manage to find the whole family of circuits with lowest possible complexity optimally realizing the task.

In section 3 we used programmable phase gate by Vidal, Masanes and Cirac [9] to construct 1 → 1 PSR of phase gates. The main result of Vidal, Masanes and Cirac in their paper [9] was actually to show that with suitable program states they can construct probabilistic phase gate, whose failure probability is exponentially small with respect to the number of qubits used as a program state. They proposed an iterative procedure, where the first step is a CNOT gate between the gate's input $|\xi\rangle$ and a program state $|\varphi\rangle \equiv |\psi_\varphi\rangle = (|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$ (see Eq.(33)). As we saw in section 3 if measurement of the target qubit

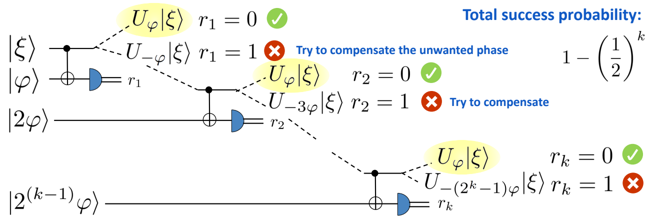

$|\xi\rangle$
$|\varphi\rangle$
$|2\varphi\rangle$
$|2^{(k-1)}\varphi\rangle$
$U_\varphi|\xi\rangle$ $r_1 = 0$ ✓
$U_{-\varphi}|\xi\rangle$ $r_1 = 1$ ✗
Try to compensate the unwanted phase
r_1
$U_\varphi|\xi\rangle$ $r_2 = 0$ ✓
$U_{-3\varphi}|\xi\rangle$ $r_2 = 1$ ✗
Try to compensate
r_2
$U_\varphi|\xi\rangle$ $r_k = 0$ ✓
$U_{-(2^k-1)\varphi}|\xi\rangle$ $r_k = 1$ ✗
r_k
Total success probability:
$1 - \left(\frac{1}{2}\right)^k$

Figure 6: VMC result

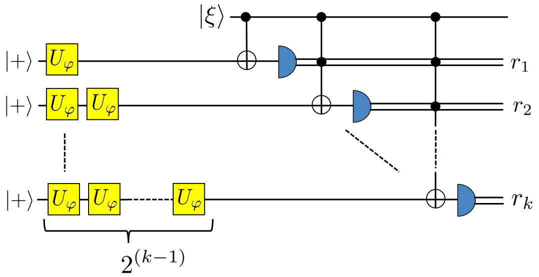


Figure 7: Optimal $(2^k-1) \to 1$ PSR of phase gates using k CNOT gates and k one-qubit measurements.

yielded bit 0 (signalizing the success) then the gate's output was $U_\varphi|\xi\rangle$, otherwise they proposed to feed the output state $U_{-\varphi}|\xi\rangle$ again to their gate, but this time using the program state $|2\varphi\rangle$ (see figure 6). The gate would again succeed or fail with probability $1/2$, thus, after k repetitions the success probability is $P_S = 1 - 1/2^k$.

Let us now calculate the number of uses of the gate U_φ we would need to prepare the program states for the Vidal, Masanes and Cirac scheme. To prepare states $|\varphi\rangle, |2\varphi\rangle, \ldots, |2^{k-1}\varphi\rangle$ one clearly needs

$$1 + 2 + \ldots + 2^{k-1} = \sum_{m=0}^{k-1} 2^m = 2^k - 1 \tag{41}$$

uses of the gate U_φ. Our theorem 1 implies that any procedure using the U_φ gate $N = 2^k - 1$ times to probabilistically store and retrieve one use of U_φ can succeed with probability at most $N/(N+1) = 1 - 1/2^k$. This means that preparation of k qubits in the state $|+\rangle$, production of states $|\varphi\rangle, |2\varphi\rangle, \ldots, |2^{k-1}\varphi\rangle$ by $2^k - 1$ fold application of U_φ gate and iterative application of programmable phase gate by Vidal, Masanes and Cirac [9] constitutes (see figure 7) a realization scheme for an optimal $(2^k-1) \to 1$ PSR of phase gates. The clear advantage of the realization scheme described above is that it requires only k CNOT gates and k one-qubit measurements, while having exponentially small failure probability $1/2^k$ in the number of qubits k, which are used for the storage.

A Proof of Eq. (24)

For any J the we define operator $R_s^{(J)} := I_J \otimes I_J \otimes s^{(J)}$. We will perform direct calculation to evaluate $\langle\psi|R_s^{(J)}|\psi\rangle$. Let us remind that $U(1)$ has one-dimensional irreps

$$|v_j\rangle_A \otimes |0\rangle_C = |w_j\rangle \otimes |j\rangle \qquad |v_{j+1}\rangle_A \otimes |1\rangle_C = |w_j\rangle \otimes |j+1\rangle,$$

where $|v_j\rangle \in \mathscr{H}_j$, $|w_J\rangle \in \mathscr{H}_J$, $|j\rangle \in \mathscr{H}_{m_j^{(j)}}$, $|j+1\rangle \in \mathscr{H}_{m_j^{(j+1)}}$. Similarly we have,

$$|v_j\rangle_{A'} \otimes |0\rangle_D = |w_j\rangle \otimes |j\rangle \qquad |v_{j+1}\rangle_{A'} \otimes |1\rangle_D = |w_j\rangle \otimes |j+1\rangle,$$

where $|v_j\rangle \in \mathscr{H}_j$, $|w_K\rangle \in \mathscr{H}_K$, $|j\rangle \in \mathscr{H}_{m_j^{(j)}}$, $|j+1\rangle \in \mathscr{H}_{m_j^{(j+1)}}$. In the above notation we have $|\psi\rangle_{AA'} = \bigoplus_{j=0}^{N} \sqrt{p_j} |v_j\rangle_A \otimes |v_j\rangle_{A'}$ For $J = K = -1$ and $J = K = N$ the multiplicity spaces $\mathscr{H}_{m_{-1,-1}}$, $\mathscr{H}_{m_{N,N}}$ are one-dimensional, $s^{(-1)}$ and $s^{(N)}$ are just numbers. Direct calculation gives

$$\langle\psi|R_s^{(-1)}|\psi\rangle = p_0 s^{(-1)} |1\rangle\langle 1|_C \otimes |1\rangle\langle 1|_D \qquad \langle\psi|R_s^{(N)}|\psi\rangle = p_N s^{(N)} |0\rangle\langle 0|_C \otimes |0\rangle\langle 0|_D \,,$$

which are operators not proportional to $|I\rangle\rangle\langle\langle I|_{CD} = (|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)$. Thus, we conclude that perfect storing and retrieving condition (see Eq. (20)) requires $s^{(-1)} = s^{(N)} = 0$.

For $J = K = 0, \ldots, N-1$ $s^{(J)}$ is an operator in 4 dimensional multiplicity space. Due to Eq. (23) $s^{(J)}$ has only four nonzero elements, which we mark in the following way

$$s^{(J)} = \sum_{a,b \in \{J, J+1\}} s_{a,b}^{(J)} |a\rangle|a\rangle\langle b|\langle b|, \tag{42}$$

where $|a\rangle|a\rangle, |b\rangle|b\rangle, \in \mathscr{H}_{m_{JJ}}$ (see Eq.(17)) and we remind that $|I_{m_J^{(J)}}\rangle\rangle = |J\rangle|J\rangle$, $|I_{m_J^{(J+1)}}\rangle\rangle = |J+1\rangle|J+1\rangle$. Direct calculation for $J = 0, \ldots, N-1$ then gives

$$\langle\psi|R_s^{(J)}|\psi\rangle = p_J s_{J,J}^{(J)} |00\rangle\langle 00| + p_{J+1} s_{J+1,J+1}^{(J)} |11\rangle\langle 11| + \sqrt{p_J p_{J+1}} \left(s_{J,J+1}^{(J)} |00\rangle\langle 11| + s_{J+1,J}^{(J)} |11\rangle\langle 00| \right),$$

which is proportional to $|I\rangle\rangle\langle\langle I|_{CD}$ if and only if $s_{j,j'}^{(J)} = \mu_J / \sqrt{p_j p_{j'}}$. Here μ_J is some number, which must be non-negativity due to positive-semidefinitness of R_S.

References

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

[2] M. A. Nielsen and Isaac L. Chuang, Phys. Rev. Lett. 79, 321 (1997)

[3] A. M. Kubicki, C. Palazuelos, D. Perez-Garcia, Phys. Rev. Lett. 122, 080505 (2019)

[4] M. Sedlák, A. Bisio, M. Ziman, Phys. Rev. Lett. 122, 170502 (2019)

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

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

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

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

[9] G. Vidal, L. Masanes, J.I. Cirac, Phys. Rev. Lett. 88, 047905 (2002)

[10] A. Barenco, et.al., "Elementary gates for quantum computation", Physical Review A **52** 3457-3467 (1995)

[11] Vivek V. Shende, Igor L. Markov, Quant.Inf.Comp. 9(5-6):461-486 (2009)