Efficient Preparation of Cyclic Quantum States

Fereshte Mozafari[1] Yuxiang Yang[2,3] Giovanni De Micheli[1]

[1] *Integrated Systems Laboratory, EPFL, Lausanne, Switzerland*
[2] *Quantum Information and Computation Initiative, The University of Hong Kong, Pokfulam Road, Hong Kong*
[3] *Institute for Theoretical Physics, ETH, Zurich, Switzerland*

Abstract— Universal quantum algorithms that prepare arbitrary n-qubit quantum states require $O(2^n)$ gate complexity. The complexity can be reduced by considering specific families of quantum states depending on the task at hand. In particular, multipartite quantum states that are invariant under permutations, e.g. Dicke states, have intriguing properties. In this paper, we consider states invariant under cyclic permutations, which we call cyclic states. We present a quantum algorithm that deterministically prepares cyclic states with gate complexity $O(n)$ without requiring any ancillary qubit. Through both analytical and numerical analyses, we show that our algorithm is more efficient than existing ones.

I. Introduction

Preparing quantum states is among the most important tasks in quantum computing. Multiple algorithms [1–6] have been proposed for preparing *arbitrary quantum states*, which require an exponential number of quantum gates with respect to the number of qubits. To reduce this complexity, researchers either use free-qubits or prepare quantum states approximately [7–9]. Both ways add overheads. To remove these overheads, another way is to consider, instead of arbitrary quantum state, specific families of quantum states such as uniform quantum states [10, 11] and *Dicke states* [12].

There are interesting metrological properties associated with multipartite quantum states that are invariant under certain permutations [13–17]. The most studied family is the Dicke states [18] of n-qubit system with Hamming weight k, which are invariant under any permutation in a symmetric group $S(n)$. Inspired by Dicke states, in this paper we introduce another important family of n-qubit states with Hamming weight k, which are invariant under cyclic permutations. We call these states as *cyclic states*. The family of cyclic states has widespread attention for tasks in quantum internet [19] and quantum metrology [20], which is explained in more detail in Section III. To prepare cyclic state, the methods presented for preparing arbitrary quantum states or uniform quantum states are used. But these methods generate an exponential number of quantum gates, in the worst case.

In this paper, we propose an efficient algorithm for preparing cyclic states with arbitrary value of k. We further present its circuit construction. The idea is based on creating cyclic permutations step-by-step. We design our algorithm such that creating each permutation requires only a constant number of 2-qubit and 3-qubit gates regardless of the total number of qubits n. Notably, the number of qubits required for creating each permutation is independent of n, since 2-qubit and 3-qubit gates require only constant numbers of elementary quantum gates. As a result, our algorithm requires only $O(n)$ elementary quantum gates.

As cyclic states are a special subset of uniform quantum states, we can use the methods presented in [10, 11]. Authors in [10] utilize symbolic representations to reduce runtime and elementary quantum gates. In [11], they try to find dependencies between qubits to reduce the number of elementary quantum gates. Their experiments show that they can reduce the number of gates but they cannot provide a linear complexity for preparing cyclic states. Authors in [12] present an efficient algorithm for preparing Dicke states, which uses $O(kn)$ quantum gates. However, their method works only for cyclic states with $k = 1$ or $k = n - 1$, not any value of k. Hence, their method is not useful for preparing cyclic states. In [21], the authors show a method to prepare quantum states associated with graphs. The method prepares some specific subsets of Dicke states including cyclic states with only $k = 2$. In contrast, we propose an algorithm for preparing cyclic states with arbitrary values of k ranging from 1 to n. Note that, in [21], it is claimed that the method can be extended to cyclic states with other values of k, but the extension is highly nontrivial as far as we can see. In addition, the complexity of preparing generic cyclic states using the method in [21] is unclear.

We compare our results with previous methods. These methods, however, either do not cover arbitrary values of k or are too computationally expensive to implement. Comparison over [11] shows that we reduce elementary quantum gates from exponential to linear complexity. While, our evaluation against [12, 21] shows that our circuit construction works for any value of k as well as gains a significant reduction of elementary quantum gates.

This paper is organized as follows. In Section II, we explain some preliminaries on quantum circuits. In Section III, we introduce cyclic states, their properties, and our motivation for preparing them. In Section IV, we propose our algorithm and its circuit construction. Next, in Sections V, we evaluate our algorithm and compare our results against state-of-the-art methods. Finally, Section VI concludes our work.

II. Preliminaries

In this section, we introduce necessary background on quantum circuit and computation.

A *quantum bit* (qubit) is the elementary unit of information in quantum computation. A *quantum state* $|\phi\rangle$ over n qubits is characterized by

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle, \tag{1}$$

978-1-6654-2135-5/22/$31.00 ©2022 IEEE

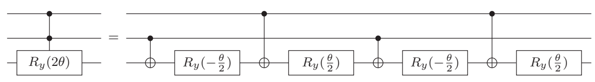

Fig. 1. Decomposing a 2-controlled $R_y(2\theta)$ gate into elementary quantum gates.

a column vector of 2^n *amplitudes* $\alpha_i \in \mathbb{C}$ with $|\alpha_0|^2 + \cdots + |\alpha_{2^n-1}|^2 = 1$. Each squared amplitude $|\alpha_i|^2$ indicates the probability that after measurement the n qubits are in the classical state i.

A *quantum circuit* is a structural description of a quantum program in terms of quantum gates connected with quantum wires which show passing of time. A *quantum gate* is an operation applied to one or more qubits to change their quantum state. Quantum gates that act on n qubits can be specified by $2^n \times 2^n$ unitary matrices U [22, 23]. A matrix U is *unitary* if

$$U^\dagger U = UU^\dagger = I, \tag{2}$$

where $U^\dagger$ is the complex conjugate transposed of U. The *matrix product* $A \cdot B$, the *direct sum* $A \oplus B$, and the *direct product* (also called *Kronecker product*) $A \otimes B$ of two matrices A and B, respectively, are defined as usual [23].

In this paper, we consider the following elementary quantum gates: The *1-qubit gates*

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \quad R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},$$
$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}, \tag{3}$$

with parameter $\theta \in \mathbb{R}$, and the *NOT gate* (NOT)

$$U_{\mathrm{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4}$$

The *2-qubit gate* called *controlled NOT gate* (CNOT)

$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5}$$

We also use 1-controlled R_y gates and 2-controlled R_y gates. A 1-controlled $R_y(2\theta)$ is easily seen to be created by 2 $R_y(\pm\theta)$ and 2 CNOTs. It is also easy to see that a 2-controlled $R_y(2\theta)$ is created by 4 $R_y(\pm\frac{\theta}{2})$ and 4 CNOTs that is depicted in Fig. 1.

III. Cyclic states and their properties

Dicke states are an important family of n-partite (for $n \in \mathbb{N}^*$) pure quantum states [18]. For example, their robustness against photon-loss noise makes them a desirable resource in building noise-resilient quantum sensors [14, 24]. Due to the importance of Dicke states, their preparation has been demonstrated experimentally in various settings [25–27], and quantum algorithms have been proposed to prepare them efficiently [12, 27–29].

Dicke states are fully symmetric, i.e., they are invariant under any permutation in the symmetric group $S(n)$ of n parties. Many realistic problems, nevertheless, only have partial symmetry rather than the full symmetry. Consider, for instance, a quantum network consisting of n nodes associated with a graph. A common type of tasks is to prepare a global (i.e. n-partite) quantum state such that each node is only entangled to a certain subset of nodes. Such tasks are growing more crucial as the quantum internet is being established [19, 30]. Dicke states obviously fail to achieve this goal unless in the special case where the network graph is complete.

In this paper, we focus on cyclic states: A new family of partially symmetric multipartite pure states that are more versatile than Dicke states in network applications. Cyclic states are generated by performing the group of cyclic permutations $C(n)$ in coherent superpositions on a computational basis state $|1\rangle^{\otimes k}|0\rangle^{\otimes m}$ $(m := n - k)$:

$$|C_k^n\rangle := \frac{1}{\sqrt{n}} \sum_{\pi \in C(n)} \pi\left(|1\rangle^{\otimes k}|0\rangle^{\otimes m}\right). \tag{6}$$

In other words, they are the uniform superpositions of computation basis states whose Hamming weights are equal and whose ones are adjacent.

Note that $|C_1^n\rangle$ coincides with the W state [31]. One also gets back the original definition of Dicke states by replacing $C(n)$ with the full symmetry group $S(n)$ in the above definition.

Cyclic states, as promised, have intriguing entanglement and coherence properties, which promise their applications in quantum internet [19] and quantum metrology [20]. Their arbitrary bipartite marginal state can be evaluated. Assuming w.o.l.g. $k \geq m$, straightforward calculation shows that the bipartite marginal state $\rho_{ij} := \mathrm{tr}_{\overline{ij}}\, |C_k^n\rangle\langle C_k^n|$ is given by

$$\rho_{ij} = \begin{cases} \frac{k-1}{n}|11\rangle\langle 11| + \frac{m-1}{n}|00\rangle\langle 00| + \frac{1}{n}|01\rangle\langle 01| + \frac{1}{n}|10\rangle\langle 10| \quad , \\ \qquad\qquad\qquad \text{if } |i-j| \neq m, |i-j| \neq k \\ \frac{2}{n}|\Psi^+\rangle\langle\Psi^+| + \frac{m-1}{n}(|01\rangle\langle 01| + |10\rangle\langle 10|) + \frac{k-m}{n}|11\rangle\langle 11| \quad , \\ \qquad\qquad\qquad \text{if } |i-j| = m \text{ or } k \end{cases} \tag{7}$$

where $|\Psi^+\rangle := (|01\rangle + |10\rangle)/\sqrt{2}$. One can immediately see that any two nodes are entangled if and only if they are separated by $m-1$ nodes (as the entanglement of formation [32] is non-zero). This is in contrast to Dicke states, for which there is the same amount of entanglement between any two subsystems. In more details, by the Hashing inequality [33, 34], one can lower bound the distillable entanglement E_D of the marginal state. For the case when $|i-j| = m = k$, the distillable entanglement [35, 36] satisfies

$$E_D \geq \left(\tfrac{m+1}{2m}\right)\log_2\left(\tfrac{m+1}{m}\right) - \left(\tfrac{m-1}{2m}\right)\log_2\left(\tfrac{m}{m-1}\right) > 0. \tag{8}$$

The above implies that if n nodes in a quantum network share multiple copies of a cyclic state, the relevant nodes (those whose distance is either m or k) can distill pure Bell states via local operation and classical communication. This means that each node in the network can establish secure quantum communication with one certain node in the network, while sharing only classical correlation with others. Such a property can be used in quantum communication tasks such as network routing [37, 38].

The above property of cyclic states also has useful applications in quantum metrology [20] or, more precisely, multipartite phase estimation problems. Imagine that a cyclic state $|C_k^n\rangle$ is, again, shared by n individual nodes in a quantum network. The j-th node passes its qubit through a phase gate $P_j := e^{i\phi_j}|0\rangle\langle 0| + e^{-i\phi_j}|1\rangle\langle 1|$ with an unknown phase ϕ_j, resulting in the global state $|C_k^n(\vec{\phi})\rangle := \left(\otimes_{j=1}^n P_j\right)|C_k^n\rangle$. The goal

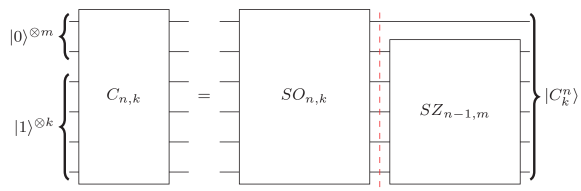

Fig. 2. The general structure of the cyclic state preparation algorithm.

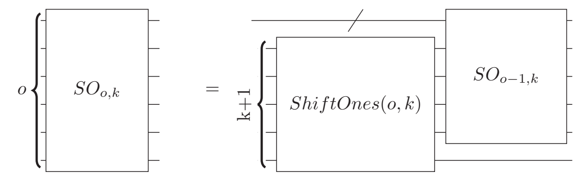

Fig. 3. The construction of SO block iteratively.

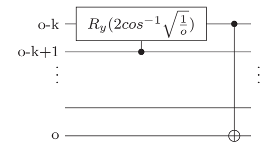

Fig. 4. The circuit implementation of $ShiftOnes(o,k)$.

is for arbitrary two nodes to jointly measure their phase difference $\delta_{ij} := \phi_i - \phi_j$. Then, two nodes can jointly estimate δ_{ij} if and only if either $|i-j|$ equals m or k. Otherwise, they cannot extract any useful information since the marginal state is independent of δ_{ij}.

Given the above desired features, it is therefore meaningful to consider how to *prepare cyclic states efficiently*. In the remaining part of the paper, we address this problem by proposing a quantum algorithm that prepares any cyclic state with circuit complexity linear in n.

IV. Proposed Method

As mentioned before, a *cyclic state* is defined as Eq. 6.

Example 1 *The cyclic state $|C_3^5\rangle$ is represented by*

$$|C_3^5\rangle = \frac{1}{\sqrt{5}}(|11100\rangle + |01110\rangle + |00111\rangle + |10011\rangle + |11001\rangle). \tag{9}$$

In this section, we propose an algorithm to prepare cyclic states deterministically. Next, we propose a quantum circuit construction and a pseudo-code for our algorithm. We also present a proof of correctness.

A. Cyclic State Preparation Algorithm

To prepare cyclic states, we design a unitary operator $C_{n,k}$, which takes as input the classical state $|1\rangle^{\otimes k}|0\rangle^{\otimes m}$ corresponding to $|q_n\rangle|q_{n-1}\rangle\dots|q_1\rangle$, and generates the cyclic state $|C_k^n\rangle$

$$C_{n,k}(|1\rangle^{\otimes k}|0\rangle^{\otimes m}) = |C_k^n\rangle. \tag{10}$$

From definition of cyclic states in Eq. 6, and by considering the Example 1, it is obvious that cyclic states are the superposition of two types of basis states. For the first type, all the ones are together in the binary string of the basis states. In the second, ones are split in the beginning and the end of the string. Hence, we divide our preparation into two parts. First, we apply a block to *Shift Ones* (SO). This block generates all basis states of the first type and results $|0\rangle^{\otimes m}|1\rangle^{\otimes k}$ in the end that goes to the second block as input. Second, we create the basis states of the second type. They are generated by circular shifting of $|0\rangle^{\otimes m}|1\rangle^{\otimes k}$ that corresponds to *Shift Zeros* (SZ). To keep ones in the beginning and in the end of the string, and to avoid creating repetitious basis states, we shift zeros one less time. Hence, we apply the SZ block on the last $n-1$ qubits. The general construction of our algorithm is depicted in Fig. 2.

B. Cyclic State Circuit Construction

In this section, we propose the detailed structure of SO and SZ blocks in creating all desired basis states. We further present a pseudo-code of our algorithm.

B.1 Explicit Construction of $SO_{o,k}$

In the following, we describe a construction of shifting ones unitary $SO_{o,k}$. In this notation o shows the total number of qubits entering the subroutine. The Fig. 3 shows its structure. First, we apply a block on the last $k+1$ qubits to shift k ones, one position to the right called $ShiftOnes(o,k)$. Next, we apply same procedure iteratively on the first $o-1$ qubits that is showed by $SO_{o-1,k}$.

***ShiftOnes*(*o, k*) Building Block.** We need to transform $|1\rangle^{\otimes k}|0\rangle$ to $|0\rangle|1\rangle^{\otimes k}$. In this regard, we design a quantum circuit that maps:

$$|1\rangle^{\otimes k}|0\rangle \to \sqrt{\frac{1}{o}}|1\rangle^{\otimes k}|0\rangle + \sqrt{\frac{o-1}{o}}|0\rangle|1\rangle^{\otimes k}. \tag{11}$$

This transformation is constructed by a 1-controlled $R_y(2cos^{-1}\sqrt{\frac{1}{o}})$ which maps $|0\rangle \to \sqrt{\frac{1}{o}}|0\rangle + \sqrt{\frac{o-1}{o}}|1\rangle$, and a CNOT, that is shown in Fig. 4. On one hand, as we have k successive ones, we only need to check one of them. On the other hand, we know q_{o-k+1} is modified in the previous step to create the previous permutation. Hence, we select q_{o-k+1} as the control-qubit for the 1-controlled R_y gate to create the current permutation. Then, we apply a CNOT to convert the last qubit to $|0\rangle$ state.

B.2 Explicit Construction of $SZ_{z,m}$

Here, a construction of shifting zeros unitary $SZ_{z,m}$ is described. Its structure is shown in the Fig. 5. Here, z shows the number of input to the block. First, $ShiftZeros$ block is applied on the last $m+1$ qubits to shift m zeros one position to the right. Next, we iteratively apply SZ block on the first $z-1$ qubits that is shown by $SZ_{z-1,m}$.

***ShiftZeros*(*z, m*) Building Block.** This time, we need to transform $|0\rangle^{\otimes m}|1\rangle$ to $|1\rangle|0\rangle^{\otimes m}$. Hence, we design a quantum circuit to transform

$$|0\rangle^{\otimes m}|1\rangle \to \sqrt{\frac{1}{z-m+1}}|0\rangle^{\otimes m}|1\rangle + \sqrt{\frac{z-m}{z-m+1}}|1\rangle|0\rangle^{\otimes m}. \tag{12}$$

Note that the first part (SO) consists of m $ShiftOnes$ blocks. We consider its effect in adjusting amplitudes in Eq. 12. This transformation is constructed by two CNOTs and a 2-controlled $R_y(-2cos^{-1}\sqrt{\frac{1}{z-m+1}})$, in between, with negative controls that

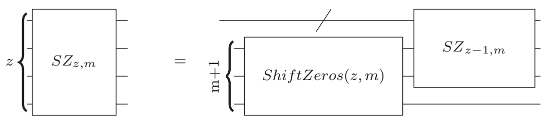

Fig. 5. The construction of SZ block iteratively.

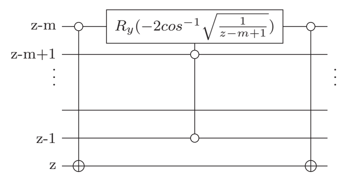

Fig. 6. The circuit implementation of $ShiftZeros(z, m)$.

is shown in Fig. 6. The R_y gate maps $|1\rangle \rightarrow \sqrt{\frac{1}{z-m+1}}|1\rangle + \sqrt{\frac{z-m}{z-m+1}}|0\rangle$. Here, to transform q_{z-m} into $|0\rangle$, all previous m qubits should be $|0\rangle$, but in practice it is not essential to check all the m qubits. In fact, we find that it is enough to check q_{z-1} and q_{z-m+1} to guarantee proper functionality. Furthermore, we add one more CNOT in the beginning, as the SO block may have changed something.

Algorithm 1 shows the pseudo-code of our deterministic algorithm for preparing the cyclic states that we have already explained in detail.

Algorithm 1: Deterministic Preparation of Cyclic States.

Input: The number of qubits n, The number of ones k
Output: The quantum circuit qc
Proc $C(n,\ k)$**:**
  qc = CreateAndInitializeQC(n, k)
  ApplySO(qc, 1, n, k)
  ApplySZ(qc, 2, n, $n-k$)
  return qc

Proc *CreateAndInitializeQC*$(n,\ k)$**:**
  qc = CreateNewQC()
  for $i = 1, \ldots, n$ **do**
    qc.CreateQubit(i)
    if $i > n - k$ **then**
      qc.ApplyNOT(i)
  return qc

Proc *ApplySO*$(qc,\ q_{start},\ q_{end},\ k)$**:**
  $o = q_{end}$ - $q_{start} + 1$
  if $o \leq k$ **then**
    return
  qc.ApplyShiftOnes(o, k)
  return ApplySO(qc, q_{start}, $q_{end} - 1$, k)

Proc *ApplySZ*$(qc,\ q_{start},\ q_{end},\ m)$**:**
  $z = q_{end}$ - $q_{start} + 1$
  if $z \leq m$ **then**
    return
  qc.ApplyShiftZeros(z, m)
  return ApplySZ(qc, q_{start}, $q_{end} - 1$, m)

C. Proof of correctness

Here we show that the circuit indeed prepares the cyclic state as desired. To this purpose, we first define two families of intermediate states:

$$|\psi_l\rangle := \sqrt{\frac{1}{n}}\sum_{i=0}^{l-1}|0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i} + \sqrt{\frac{n-l}{n}}|0\rangle^{\otimes l}|1\rangle^{\otimes k}|0\rangle^{\otimes m-l} \tag{13}$$

and

$$|\phi_l\rangle := \sqrt{\frac{1}{n}}\sum_{i=0}^{m-1}|0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i} + \sqrt{\frac{1}{n}}\sum_{j=0}^{l-1}|1\rangle^{\otimes j}|0\rangle^{\otimes m}|1\rangle^{\otimes k-j} + \sqrt{\frac{n-m-l}{n}}|1\rangle^{\otimes l}|0\rangle^{\otimes m}|1\rangle^{\otimes k-l}. \tag{14}$$

By definition, the initial state is $|\psi_0\rangle = |1\rangle^{\otimes k}|0\rangle^{\otimes m}$. First, we analyse the action of $SO(n,k)$ on the input state. In the process of preparing cyclic states, any input to the shift one operation is in a superposition of qubit strings of the form $|0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i}$. Notice that, according to Fig. 4, $ShiftOnes(n-l,k)$ acts non-trivially only if the $(n-l-k+1)$-th qubit is $|1\rangle$, and we have

$$ShiftOnes(n-l,k)|0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i} = |0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i} \qquad i < l, \tag{15}$$

and

$$ShiftOnes(n-l,k)|0\rangle^{\otimes l}|1\rangle^{\otimes k}|0\rangle^{\otimes m-l} = \sqrt{\frac{n-l-1}{n-l}}|0\rangle^{\otimes l}|1\rangle^{\otimes k}|0\rangle^{\otimes m-l} + \sqrt{\frac{1}{n-l}}|0\rangle^{\otimes l+1}|1\rangle^{\otimes k}|0\rangle^{\otimes m-l-1}.$$

Substituting into Eq. 13, we have

$$ShiftOnes(n-l,k)|\psi_l\rangle = |\psi_{l+1}\rangle \tag{16}$$

and thus

$$SO(n,k)|\psi_0\rangle = |\psi_m\rangle. \tag{17}$$

It remains to be shown that $SZ(n,m)|\psi_m\rangle = |C_k^n\rangle$. By Eqs. 13 and 14, we have $|\psi_m\rangle = |\phi_0\rangle$. Next, notice that

$$ShiftZeros(n-l,m)|1\rangle^{\otimes l}|0\rangle^{\otimes m}|1\rangle^{\otimes k-l} = \sqrt{\frac{n-l-m}{n-l-m+1}}|1\rangle^{\otimes l}|0\rangle^{\otimes m}|1\rangle^{\otimes k-l} + \sqrt{\frac{1}{n-l-m+1}}|1\rangle^{\otimes l+1}|0\rangle^{\otimes m}|1\rangle^{\otimes k-l-1} \tag{18}$$

and

$$ShiftZeros(n-l,m)|1\rangle^{\otimes j}|0\rangle^{\otimes m}|1\rangle^{\otimes k-j} = |1\rangle^{\otimes j}|0\rangle^{\otimes m}|1\rangle^{\otimes k-j} \qquad j < l. \tag{19}$$

In addition, since we assumed $m \leq k$, we also have

$$ShiftZeros(n-l,m)|0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i} = |0\rangle^{\otimes i}|1\rangle^{\otimes k}|0\rangle^{\otimes m-i}. \tag{20}$$

Therefore, substituting both into Eq. 14 we have

$$ShiftZeros(n-l,m)|\phi_{l-1}\rangle = |\phi_l\rangle \tag{21}$$

$$SZ(n-1,m)|\phi_0\rangle = |\phi_{k-1}\rangle. \tag{22}$$

The proof is concluded since by definition in Eq. 14

$$|\phi_{k-1}\rangle = |C_k^n\rangle. \tag{23}$$

V. Results & Evaluation

We compute the number of elementary quantum gates $\{CNOT, R_y, NOT\}$ of our circuit construction. We assume $k \geq m$, otherwise, we only need to add n extra NOTs at the beginning to ensure $k > m$. To bring back the circuit into the correct state, we must also add n more extra NOTs at the end.

Shifting ones consists of m $ShiftOnes$ blocks. Considering the quantum circuit depicted in Fig. 4, m 1-controlled R_y and m CNOT gates are required.

Shifting zeros consists of $k-1$ $ShiftZeros$ blocks. As shown in Fig. 6, this part requires $k-1$ 2-controlled R_y gates except when $m=1$ or $m=2$ which it requires $k-1$ 1-controlled R_y gates, instead. It also needs $2(k-1)$ CNOT gates. Moreover, this part requires NOT gates to apply negative controls. Each $ShiftZeros$ block consists of 8 NOTs which at least one of them can be canceled by the next block. Hence, in-between blocks require 6 NOTs and the total number of NOTs is upper bounded by $6(k-1)+2$. Note that when $m=1$ or $m=2$, as $ShiftZeros$ blocks are constructed by 1-controlled R_y gates, $6(k-1)$ NOTs are required.

To create elementary quantum gates, we decompose 1-controlled R_y and 2-controlled R_y gates into {2 CNOTs, 2 R_y gates}, and {4 CNOTs, 4 R_y gates}, respectively, as explained in Section II. As a result, the cost function regarding the number of CNOT gates (c), R_y gates (r), and NOT gates (n) are formulated as follows:

$$Cost_c(n,k) = \begin{cases} 7 & \text{if } k=2, n=3 \\ 4n-5 & \text{if } k=n-1, n>3 \\ 4n-6 & \text{if } k=n-2 \\ 3n+3k-6 & \text{otherwise} \end{cases}, \tag{24}$$

$$Cost_r(n,k) = \begin{cases} 4 & \text{if } k=2, n=3 \\ 2n-2 & \text{if } k=n-1, n>3 \\ 2n-2 & \text{if } k=n-2 \\ 2n+2k-4 & \text{otherwise} \end{cases}, \tag{25}$$

and

$$Cost_n(n,k) = \begin{cases} 6 & \text{if } k=2, n=3 \\ 6n-12 & \text{if } k=n-1, n>3 \\ 6n-18 & \text{if } k=n-2 \\ 6k-4 & \text{otherwise} \end{cases}. \tag{26}$$

We compare our approach with state-of-the-art methods [12, 21] in terms of the number of CNOTs that are more expensive than 1-qubit gates in NISQ architectures. We also show the number of R_y gates. The results are shown in Table I. To compare with [21], k should be only 2. As we assume $k \geq m$, it corresponds to $k=n-2$ with $2n$ extra NOTs. Considering Eqs. 24, 25, and 26, our method generates $4n-6$ CNOTs, $2n-2$ R_y, and $6n-18$ NOT gates. The result of [21] is a little bit better, but it only covers $k=2$. To compare with Dicke state preparation method introduced in [12], we can only consider some specific Dicke states $|D^n_k\rangle$ that are equal to a cyclic state $|C^n_k\rangle$. From their definitions, they are equal when either $k=1$ or $k=n-1$. As shown in the table, our method reduces both CNOT and R_y gates significantly. Hence, our circuit construction is more general (no constraints on k) and effective as compared to methods in [12, 21].

TABLE I
Proposed method comparison over methods in [12, 21].

	#CNOT	#Ry
[21] $k=2$	$\frac{7}{2}n+3$	$4n+2$
Proposed Method	$4n-6$	$2n-2$
[12] $k=1$	$>5n$	$>4n$
Proposed Method	$4n-5$	$2n-2$
[12] $k=n-1$	$>5n$	$>4n$
Proposed Method	$4n-5$	$2n-2$

As previous methods are limited to special values of k, we compare our method with the uniform quantum state preparation method in [10] that is more general. This method not only covers arbitrary values of k but also is more efficient over arbitrary state preparation methods. The results regarding the number of CNOTs are presented in Table II, for different number (random) of n and k. The results show that our method reduces the number of CNOTs by a factor of 2. When the number of qubits (n) is small, for some cases (here for $n=10$ and $k=5$), our results are worse. This is due to the fact that, for these cases, there exist good dependencies between qubits which are utilized by [10] to reduce CNOTs. In the case that the number of qubits (n) is large, we reduce CNOTs with linear complexity, for all values of k . Conversely, [10] increases the number of CNOTs exponentially.

VI. Conclusions

Efficient quantum state preparation is a crucial step to design quantum computing systems. In this work, we propose a construction method as well as quantum circuits that deterministically generate cyclic states. Our circuit construction method uses $6n-15$ CNOT gates in the worst case when $k=n-3$, which is significantly better than the state-of-the-art methods that generate exponential number of CNOTs. We further provide experimental results that confirm this analysis.

Acknowledgements

This research was supported by the Swiss National Science Foundation (200021-169084 MAJesty) and by the Google PhD Fellowship.

References

[1] M. Mottonen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, "Transformation of quantum states using uniformly controlled rotations," *Quantum Information and Computation*, vol. 5, no. 6, pp. 467–473, 2005.

[2] V. V. Shende, S. S. Bullock, and I. L. Markov, "Synthesis of quantum-logic circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 6, pp. 1000–1010, 2006.

[3] P. Kaye and M. Mosca, "Quantum networks for generating arbitrary quantum states," in *International Conference on Quantum Information*. Optical Society of America, 2001, p. PB28.

[4] P. Niemann, R. Datta, and R. Wille, "Logic synthesis for quantum state generation," in 46^{th} *International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 2016, pp. 247–252.

TABLE II
Comparing the number of CNOTs for the proposed method and the preparation method in [10].

n	10				12				15				17				19			
k	1	2	5	7	1	4	7	10	1	2	5	7	1	2	5	8	1	2	7	9
[10]	519	107	35	72	2057	262	86	300	16396	1089	1034	282	65550	2161	570	542	262160	8304	1058	1058
Proposed Method	35	34	39	45	43	42	51	42	55	54	54	60	63	62	60	69	71	70	72	78
Improvement (%)	93.3	68.2	-11.4	37.5	97.9	84.1	40.7	86.0	99.7	95.0	94.8	78.7	99.9	97.1	89.4	87.3	99.9	99.1	93.2	92.6

[5] R. Iten, R. Colbeck, I. Kukuljan, J. Home, and M. Christandl, "Quantum circuits for isometries," *Physical Review A*, vol. 93, no. 3, p. 032318, 2016.

[6] M. Plesch and Č. Brukner, "Quantum state preparation with universal gate decompositions," *Physical Review A*, vol. 83, no. 3, p. 032302, 2011.

[7] A. Zulehner, S. Hillmich, I. L. Markov, and R. Wille, "Approximation of quantum states using decision diagrams," in 25^{th} *Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2020, pp. 121–126.

[8] C. Zoufal, A. Lucchi, and S. Woerner, "Quantum generative adversarial networks for learning and loading random distributions," *npj Quantum Information*, vol. 5, no. 1, pp. 1–9, 2019.

[9] I. F. Araujo, D. K. Park, F. Petruccione, and A. J. da Silva, "A divide-and-conquer algorithm for quantum state preparation," *Scientific Reports*, vol. 11, no. 1, pp. 1–12, 2021.

[10] F. Mozafari, H. Riener, M. Soeken, and G. De Micheli, "Efficient boolean methods for preparing uniform quantum states," in *IEEE Transactions on Quantum Engineering (TQE), in press.*

[11] F. Mozafari, M. Soeken, H. Riener, and G. De Micheli, "Automatic uniform quantum state preparation using decision diagrams," in 50^{th} *International Symposium on Multiple-Valued Logic (ISMVL)*. IEEE, 2020, pp. 170–175.

[12] A. Bärtschi and S. Eidenbenz, "Deterministic preparation of dicke states," in *International Symposium on Fundamentals of Computation Theory*. Springer, 2019, pp. 126–139.

[13] G. Tóth, "Multipartite entanglement and high-precision metrology," *Physical Review A*, vol. 85, no. 2, p. 022322, 2012.

[14] Z. Zhang and L. Duan, "Quantum metrology with dicke squeezed states," *New Journal of Physics*, vol. 16, no. 10, p. 103037, 2014.

[15] L. Pezze, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, "Quantum metrology with nonclassical states of atomic ensembles," *Reviews of Modern Physics*, vol. 90, no. 3, p. 035005, 2018.

[16] Y. Ouyang, N. Shettell, and D. Markham, "Robust quantum metrology with explicit symmetric states," *arXiv preprint arXiv:1908.02378*, 2019.

[17] H. Hakoshima and Y. Matsuzaki, "Efficient detection of inhomogeneous magnetic fields from a single spin with dicke states," *Physical Review A*, vol. 102, no. 4, p. 042610, 2020.

[18] R. H. Dicke, "Coherence in spontaneous radiation processes," *Physical review*, vol. 93, no. 1, p. 99, 1954.

[19] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[20] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum metrology," *Physical Review Letters*, vol. 96, no. 1, p. 010401, 2006.

[21] A. Burchardt, J. Czartowski, and K. Życzkowski, "Entanglement in highly symmetric multipartite quantum states," *arXiv preprint arXiv:2105.12721*, 2021.

[22] R. P. Feynman, "Quantum mechanical computers," *Foundations of physics*, vol. 16, no. 6, pp. 507–531, 1986.

[23] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. American Association of Physics Teachers, 2002.

[24] G. Tóth and I. Apellaniz, "Quantum metrology from a quantum information science perspective," *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 42, p. 424006, 2014.

[25] N. Kiesel, C. Schmid, G. Tóth, E. Solano, and H. Weinfurter, "Experimental observation of four-photon entangled dicke state with high fidelity," *Physical review letters*, vol. 98, no. 6, p. 063604, 2007.

[26] W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurter, "Experimental entanglement of a six-photon symmetric dicke state," *Physical review letters*, vol. 103, no. 2, p. 020504, 2009.

[27] D. Hume, C.-W. Chou, T. Rosenband, and D. J. Wineland, "Preparation of dicke states in an ion chain," *Physical Review A*, vol. 80, no. 5, p. 052302, 2009.

[28] C. S. Mukherjee, S. Maitra, V. Gaurav, and D. Roy, "Preparing dicke states on a quantum computer," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–17, 2020.

[29] J. K. Stockton, R. Van Handel, and H. Mabuchi, "Deterministic dicke-state preparation with continuous measurement and control," *Physical Review A*, vol. 70, no. 2, p. 022106, 2004.

[30] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[31] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A*, vol. 62, no. 6, p. 062314, 2000.

[32] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Physical Review Letters*, vol. 80, no. 10, p. 2245, 1998.

[33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824, 1996.

[34] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[35] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating partial entanglement by local operations," *Physical Review A*, vol. 53, no. 4, p. 2046, 1996.

[36] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, no. 5, p. 722, 1996.

[37] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," *npj Quantum Information*, vol. 5, no. 1, pp. 1–7, 2019.

[38] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, "Routing entanglement in the quantum internet," *npj Quantum Information*, vol. 5, no. 1, pp. 1–9, 2019.