Quantum Random State Generation with Predefined Entanglement Constraint
Anmer Daskin, Ananth Grama, and Sabre Kais

Abstract
Entanglement plays an important role in quantum communication, algorithms, and error correction. Schmidt coefficients are correlated to the eigenvalues of the reduced density matrix. These eigenvalues are used in Von Neumann entropy to quantify the amount of the bipartite entanglement. In this paper, we map the Schmidt basis and the associated coefficients to quantum circuits to generate random quantum states. We also show that it is possible to adjust the entanglement between subsystems by changing the quantum gates corresponding to the Schmidt coefficients. In this manner, random quantum states with predefined bipartite entanglement amounts can be generated using random Schmidt basis. This provides a technique for generating equivalent quantum states for given weighted graph states, which are very useful in the study of entanglement, quantum computing, and quantum error correction.

Index Terms
Entanglement, Quantum circuits, Von Neumann Entropy.

I. INTRODUCTION:
In quantum information, a quantum state encodes information and is used in the design of algorithms. Random numbers and random matrix theory [1] play important roles in various applications, ranging from wireless communications [2] to determining physical properties of a quantum system [3]. Consequently, generating random quantum states is important in quantum communication and information. For instance, unique random states can be used to design quantum bills (money) [4]. Statistical properties of random quantum states show that random quantum states generated within some restricted set of states can still be effectively random [5].

A quantum state, defined as a vector in Hilbert space, contains all the accessible-measurable information about the system [6]. Entanglement is one of the quantum mechanical accessible phenomena used to build efficient quantum algorithms. For a given multi-qubit state, a graph state can be used to specify the graph-based representation of the entanglement between qubits. A graph state is comprised of vertices and edges, where the vertices correspond to qubits and edges represent entanglement between qubits. Non-local properties [7], [8] and entanglement characterizations [9] of graph states have been studied, and their use has been demonstrated for different applications in quantum error correction [10], quantum communication, and one-way quantum computation [11], among others (Hein et al. [12] present an excellent review of the applications of graph states). Realization of graph states has been experimentally demonstrated for six photons [13]. As a generalization of graph states, weighted graph states include weights on each edge, quantifying the amount of the entanglement. Weighted graph states are shown to be useful in the study of bipartite entanglement in spin chains [14] and many-body quantum states [15]. Based on a weighted graph state representation of certain classes of multi-particle entangled states, a variational method [16], [17] is proposed for arbitrary spin and infinite-dimensional systems. These representations are also used in error correction schemes in one-way quantum computing [18], and in many other applications (please refer to Hein at al. [12]).

In this paper, we map the Schmidt basis and the associated coefficients to quantum circuits to generate random quantum states. We show that for state generation, by using quantum gates corresponding to Schmidt coefficients, the amount of the bipartite entanglement between subsystems can be controlled. Therefore, we show that if quantum gates corresponding to the Schmidt basis are chosen randomly, one can generate random states with bipartite entanglement amounts predefined by the gates implementing the coefficients. This provides a way to tune the entanglement between subsystems in a generated state, which can be used to generate certain type of weighted graph states on quantum computers. This can be used in the utilization and characterization of entanglement [19] in quantum communication, cryptography, and cluster state computation [20]. In addition, our method can be used to simulate entanglement distribution of particular quantum systems in quantum computing. An example of this is in the simulation of the entanglement distribution in light-harvesting complexes [21], [22] to investigate energy transfer and efficiency.

A. Daskin and A. Grama are with Department of Computer Science, Purdue University, West Lafayette, IN, 47907 USA.
S. Kais is with Department of Chemistry, Department of Physics and Birck Nanotechnology Center, Purdue University, West Lafayette, IN 47907 USA and Qatar Environment and Energy Research Institute, Doha, Qatar.
II. Preliminaries

a) Schmidt Decomposition: Given Hilbert spaces $H_A$ and $H_B$ of dimension $d_A$ and $d_B$, and a quantum state $|\psi\rangle \in H_{AB} = H_A \otimes H_B$, the Schmidt decomposition is defined as:

$$|\psi\rangle = \sum_{i}^{\min(d_A, d_B)} s_i |u_i\rangle |v_i\rangle,$$

where $s_i$s are the Schmidt coefficients, $|u_i\rangle \in H_A$, and $|v_i\rangle \in H_B$. The reduced density matrix for system $A$ or $B$ can be found from the Schmidt decomposition as follows:

$$\rho_A = \sum_{i} s_i^2 |u_i\rangle \langle u_i|.$$

The above expression shows that the coefficients of the Schmidt decomposition are related to the eigenvalues of the reduced density matrix.

b) Von Neumann Entropy: For a given density matrix $\rho$, Von Neumann Entropy is defined as:

$$S(\rho) = -Tr(\rho \ln \rho)$$

If the density matrix $\rho$ has the eigenvalue decomposition $\rho = \sum_j \lambda_j |j\rangle \langle j|$, then the entropy is defined as:

$$S(\rho) = -\sum_j \lambda_j \ln \lambda_j$$

For pure states, we can use the Schmidt coefficients in the Von Neumann Entropy to quantify the bipartite entanglement between systems $A$ and $B$ as:

$$S(\rho_A) = S(\rho_B) = -\sum_{j}^{\min(d_A, d_B)} s_j^2 \ln s_j^2$$

III. Random State Generation With Predetermined Entanglement

Since the Schmidt coefficients are important in determining entanglement, by suitably mapping the Schmidt decomposition to a circuit design, we can control entanglement. Please note that in this paper, we will only consider the real space for the circuit designs.

A. 2-qubit Case

![Quantum Circuit Diagram](image)

Fig. 1: Quantum circuit which is found by following the Schmidt decomposition and can generate any quantum state of dimension 4. In the circuit $U$ and $V$ are the Schmidt basis and $R$ is the rotation gate defined with the Schmidt coefficients.

The Schmidt decomposition for $H = H_1 \otimes H_2$, and $H_1$ and $H_2 \in \mathcal{R}^{\otimes 3}$ is as follows:

$$|\psi\rangle = \sum_{i=1}^{2} s_i |u_i\rangle |v_i\rangle.$$  

The circuit in Fig.1 can be used generate any general $|\psi\rangle$ state for two qubits, where the entanglement defined by the quantum gate $R$ whose elements are determined from the Schmidt coefficients. We can determine the entanglement as:

$$R = \begin{pmatrix} s_1 & -s_2 \\ s_2 & s_2 \end{pmatrix}.$$  

Choosing the elements for this gate and random Schmidt basis $U$ and $V$, one can also create a two-qubit random state with predetermined entanglement.
B. Generalization to \( n \) qubits

We can generalize the idea to an \( n \)-qubit system: The Kronecker tensor product of the Schmidt bases \( U \) and \( V \) can be written as:

\[
U \otimes V = [u_{e_1} \otimes v_{e_1} \ldots u_{e_1} \otimes v_{e_k} \ u_{e_2} \otimes v_{e_1} \ldots u_{e_2} \otimes v_{e_k} \ldots u_{e_k} \otimes v_{e_1} \ldots u_{e_k} \otimes v_{e_k}]
\]  

(8)

In the Schmidt decomposition of a vector \( |\psi\rangle \):

\[
|\psi\rangle = \sum_{i=1}^{k} s_i u_{e_i} \otimes v_{e_i},
\]  

(9)

the Schmidt coefficients \( s_1 \ldots s_k \) are related to the columns: \( 1, (k + 2), (2k + 3), \ldots, (k^2) \), respectively. Therefore, if we have an input \( |\varphi\rangle \) to \( (U \otimes V) \) in the following form:

\[
|\varphi\rangle = \begin{bmatrix}
    s_1 \\
    \vdots \\
    s_2 \\
    0 \\
    0 \\
    \vdots \\
    s_3 \\
    0 \\
    \vdots \\
    0 \\
    \vdots \\
    0 \\
    0
\end{bmatrix},
\]  

(10)

then \( (U \otimes V) |\varphi\rangle = |\psi\rangle = \sum_{i=1}^{k} s_i u_{e_i} \otimes v_{e_i} \). If we assume the initial input to the circuit as \( |0\rangle \), then the first column of the matrix representation of the circuit defines the output. Therefore, to generate \( |\psi\rangle \), first we construct the Schmidt coefficients in the first column of the matrix \( S \) of dimension \( \text{min}(d_A, d_B) \). If \( S \) is on the first subsystem, then the global unitary operator is \( (S \otimes I) \) with the first column:

\[
\begin{bmatrix}
    s_1 \\
    \vdots \\
    0 \\
    \vdots \\
    0 \\
    \vdots \\
    0 \\
    \vdots \\
    0 \\
    \vdots \\
    0
\end{bmatrix},
\]  

(11)

To get the Schmidt coefficients to the rows \( 1, (k + 2), (2k + 3), \ldots, (k^2) \) as in Eq.(10), we apply a permutation matrix \( P \) to switch the rows and columns: \( P(S \otimes I)P \). Therefore, the final circuit can be represented by the matrix vector product as:

\[
|\psi\rangle = (U \otimes V)P(S \otimes I)P|0\rangle.
\]  

(12)

In the corresponding circuit design, \( U \) and \( V \) are defined as the operators on the first and the second subsystems, respectively. \( S \), whose first column is the Schmidt coefficients, is considered on the first subsystem. Since the operator \( P \) is a permutation matrix, it is implemented by a combination of controlled \( \text{NOT} \) gates.

C. 4-qubit Case

As an example, consider a 4-qubit system, where the subsystems \( H_{12} \) and \( H_{34} \) are composed of two qubits. Thus, in the Schmidt decomposition, there are four coefficients: \( s_1, s_2, s_3, \) and \( s_4 \). The circuit in Fig.2 generates any quantum state that has the Schmidt coefficients implemented by \( S \) and Schmidt bases implemented by \( U \) and \( V \). For the implementation of \( S \) given in Fig.3, we follow the idea first presented in ref. [23]: The coefficients are divided into two unit vectors as \( 1/k_1 \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \) and \( 1/k_2 \begin{bmatrix} s_3 \\ s_4 \end{bmatrix} \), with normalization constants \( 1/k_1 \) and \( 1/k_2 \). Then, the rotation gates in Fig.3 are defined as:

\[
R_1 = \frac{1}{k_1} \begin{bmatrix} s_1 & -s_2 \\ s_2 & s_1 \end{bmatrix}, \quad R_2 = \frac{1}{k_2} \begin{bmatrix} s_3 & -s_4 \\ s_4 & s_3 \end{bmatrix},
\]  

(13)

and

\[
R_3 = \begin{bmatrix} k_1 & -k_2 \\ k_2 & k_1 \end{bmatrix}.
\]  

(14)
entanglement between state of dimension 16. In the circuit Fig. 2: Quantum circuit for 4 qubits which is found by following the Schmidt decomposition and can generate any quantum state of dimension 16. In the circuit $U$ and $V$ are the Schmidt basis and $S$ implements the Schmidt coefficients controlling the entanglement between $H_{12}$ and $H_{34}$.

$$S \equiv \begin{pmatrix} R_1 & I \\ I & R_2 \end{pmatrix} (R_3 \otimes I)$$

The first column of $S$ consists of the Schmidt coefficients, which is shown in Fig. 3.

**IV. BIPARTITE ENTANGLEMENT CONTROL FOR N QUBITS**

We now show that we can sequentially combine the Schmidt decomposition circuits for two qubits to control the entanglement between various parts of the system with the rest of the system in the random state: e.g., for a 5 qubit system, controlling entanglement between $H_1$ and $H_{2345}$ and $H_{12}$ and $H_{345}$.

**A. Connecting three qubits linearly**

We start with the initial state $|\psi_0\rangle = |000\rangle$. If we assume the first two qubits are entangled by the circuit in Fig. 1, where the Schmidt basis is chosen to be identity: $V_1 = U_1 = I$, then we get the following:

$$|\psi_1\rangle = s_1 |0\rangle |0\rangle |0\rangle + s_2 |1\rangle |1\rangle |0\rangle ,$$

where $s_1$ and $s_2$ are Schmidt coefficients. To also entangle the 2nd and 3rd qubits, we apply the same Schmidt circuit to these qubits: First, the $CNOT$ gate is applied:

$$|\psi_2\rangle = s_1 |0\rangle CNOT(|0\rangle |0\rangle ) + s_2 |1\rangle CNOT(|1\rangle |0\rangle )$$

$$= s_1 |0\rangle |0\rangle |0\rangle + s_2 |1\rangle |1\rangle |0\rangle .$$

Then, we apply the rotation gate $R$, which has the Schmidt coefficients, $k_1$ and $k_2$, as elements:

$$R_2 = \begin{pmatrix} k_1 \\ -k_2 \\ k_1 \end{pmatrix}$$

This generates the following state:

$$|\psi_3\rangle = s_1 |0\rangle R_2 |0\rangle |0\rangle + s_2 |1\rangle R_2 |1\rangle |1\rangle$$

$$= s_1 |0\rangle (k_1 |0\rangle + k_2 |1\rangle) |0\rangle + s_2 |1\rangle (-k_2 |0\rangle + k_1 |1\rangle) |1\rangle$$

$$= s_1 k_1 |000\rangle + s_1 k_2 |010\rangle - s_2 k_2 |101\rangle + s_2 k_1 |111\rangle$$

After the second $CNOT$, the final state becomes:

$$|\psi_4\rangle = s_1 k_1 |000\rangle + s_1 k_2 |011\rangle - s_2 k_2 |101\rangle + s_2 k_1 |110\rangle$$

Since $U_2$ and $V_2$ are the local operators, they do not change the entanglement. Therefore, the entanglement between $H_{12}$ and $H_{3}$, and the entanglement between $H_1$ and $H_{23}$ can be found from $|\psi_4\rangle$. 

---

Fig. 2: Quantum circuit for 4 qubits which is found by following the Schmidt decomposition and can generate any quantum state of dimension 16. In the circuit $U$ and $V$ are the Schmidt basis and $S$ implements the Schmidt coefficients controlling the entanglement between $H_{12}$ and $H_{34}$.

Fig. 3: Quantum circuit that has the matrix representation whose first column is the Schmidt coefficients.
circuit designs can be generated for different graphs in the same manner.

Graph states, where vertices represent qubits (a vertex can also be a subsystem), and an edge between vertices determines the bipartite entanglement between subsystems. They are used in determining the capacity of quantum channels and quantum error correction. We use weighted circuit designs to achieve desired entanglement between two disentangled subsystems.

Finally, we find:

\[ S(\rho_3) = (k_1)^2 \ln (k_1)^2 + (k_2)^2 \ln (k_2)^2, \]

which is determined solely from the Schmidt coefficients, the entanglement is controlled as expected.

The entanglement between \( H_{12} \) and \( H_3 \) is also defined as \( S(\rho_1) = S(\rho_{23}) \). Here, the reduced density matrix \( \rho_1 \) can be obtained as follows:

\[ \rho_1 = \text{Tr}_{H_{12}} (|\psi_4\rangle \langle \psi_4|) = (s_1 k_1)^2 |0\rangle \langle 0| + (s_1 k_2)^2 |1\rangle \langle 1| + (s_2 k_2)^2 |1\rangle \langle 1| \]

\[ = (s_1^2 k_1^2 + (s_1 k_2)^2) |0\rangle \langle 0| + ((s_1 k_2)^2 + (s_2 k_2)^2) |1\rangle \langle 1| \]  

(22)

Finally, we find \( S(\rho_1) = (s_1)^2 \ln (s_1)^2 + (s_2)^2 \ln (s_2)^2 \). Eq.(21) and Eq.(22) prove that we can use the Schmidt circuit sequentially to achieve desired entanglement between two disentangled subsystems.

**B. Definition of a Graph State**

For a given multi-qubit state, a graph state is an instance of the graph-based representation of the entanglement between qubits [12]. They are used in determining the capacity of quantum channels and quantum error correction. We use weighted graph states, where vertices represent qubits (a vertex can also be a subsystem), and an edge between vertices \( v_i \) and \( v_j \) determines the bipartite entanglement between subsystems \( i \) and \( j \).

If a graph state is acyclic, i.e. there is only one edge connecting two subsystems, successively using the Schmidt circuit in Fig.1 and controlling the Schmidt coefficients, as done for three qubits above, the desired entanglement between each subsystems can be derived. Example circuits are given in Fig.4 and Fig.5 for linear and star graphs with five qubits. Similar circuit designs can be generated for different graphs in the same manner.

---

**Fig. 4:** Quantum circuit that can generate random state for 5 qubits with the entanglement amount between qubits defined on the linear graph.

**Fig. 5:** Quantum circuit that can generate random state for 5 qubits with the entanglement amount between qubits defined on the star graph.

The Von Neumann entropy \( S(\rho_3) = S(\rho_{12}) \) defines the entanglement between the systems \( H_{12} \) and \( H_3 \). For the entropy, the reduced density matrix \( \rho_3 \) can be found as follows:

\[ \rho_3 = \text{Tr}_{H_{12}} (|\psi_4\rangle \langle \psi_4|) = (s_1 k_1)^2 |0\rangle \langle 0| + (s_1 k_2)^2 |1\rangle \langle 1| + (s_2 k_2)^2 |1\rangle \langle 1| \]

\[ + (s_2 k_1)^2 |0\rangle \langle 0| \]

\[ = ((s_1 k_1)^2 + (s_2 k_1)^2) |0\rangle \langle 0| + ((s_1 k_2)^2 + (s_2 k_2)^2) |1\rangle \langle 1| \]

\[ = (s_1 k_1)^2 |0\rangle \langle 0| + (s_2 k_2)^2 |1\rangle \langle 1| \]  

(21)

The entanglement between \( H_{12} \) and \( H_3 \) is also defined as \( S(\rho_1) = S(\rho_{23}) \). Here, the reduced density matrix \( \rho_1 \) can be obtained as follows:

\[ \rho_1 = \text{Tr}_{H_{23}} (|\psi_4\rangle \langle \psi_4|) = ((s_1 k_1)^2 + (s_2 k_1)^2) |0\rangle \langle 0| + ((s_1 k_2)^2 + (s_2 k_2)^2) |1\rangle \langle 1| \]

\[ = (s_1^2 k_1^2 + (s_1 k_2)^2) |0\rangle \langle 0| + ((s_1 k_2)^2 + (s_2 k_2)^2) |1\rangle \langle 1| \]

(22)

Finally, we find \( S(\rho_1) = (s_1)^2 \ln (s_1)^2 + (s_2)^2 \ln (s_2)^2 \). Eq.(21) and Eq.(22) prove that we can use the Schmidt circuit sequentially to achieve desired entanglement between two disentangled subsystems.
V. NUMERICAL RESULTS

We now show the degree of the randomness of the output states when the entanglement is controlled through a given probability distribution of the generated states. Let $G(m,n)$ be an $m \times n$ matrix of independent and identically distributed standard normal real random variables. The distribution of the matrices is defined as [24]:

$$\frac{1}{2\pi^{mn/2}} e^{-\frac{1}{2} \left\| G \right\|^2}$$  \hspace{1cm} (23)

In MATLAB, we use the function $G = \text{randn}(m,n)$ to generate matrices with the above Gaussian distribution. Starting with a normally distributed matrix and taking QR or singular value decomposition of the matrix generates random orthogonal matrices distributed according to Haar measure. One can also generate standard random orthogonal matrices with the same distribution by using successive plane rotations with random angle values generated according to Gaussian distribution [25]. Therefore, for quantum states generated using the Schmidt decomposition by choosing random Schmidt coefficients and basis (or the corresponding quantum gates), the distribution of the overlaps or the angle values between these states is expected to be Gaussian. This is also numerically shown in Fig.6 for 100 random quantum states generated using random Schmidt basis and coefficients for an eight-qubit star graph state.

![Histogram of the angles between the generated quantum states](image1)

Fig. 6: Angles between the generated quantum states for an eight-qubit star graph: Both the Schmidt coefficients and basis are chosen randomly for each state.

In Fig.7 and Fig.8, the bipartite entanglements, and the Schmidt coefficients, are chosen to be the same for the states. If we compare the histograms in Fig.6 with Fig.8 and Fig.7, we see that fixing Schmidt coefficients and the alignment of the qubits does not have much impact on the distribution of the generated random states. However, for the two qubit system shown in Fig.9, the Schmidt coefficients, or the amount of entanglement play important roles, since the size of the system is small. If the entanglement amount is high between two qubits, the overlap of the generated quantum states becomes almost a uniform distribution, an indication that the generated states are more alike. However, when it is low, since the Schmidt basis becomes dominant in the randomness of the state, we see a Gaussian distribution. In addition, in larger systems, having the same Schmidt coefficients in the generated states does not affect the distribution of the overlaps: e.g., Fig.10 compares the distributions for 4-qubit system when the entanglement is low and high.

VI. CONCLUSION

In this paper, we map the Schmidt decomposition for a general quantum state into quantum circuits, which can be used to generate random quantum states. We show that in random state generation, the entanglement amount between subsystems can

![Histogram of the angles between the generated quantum states](image2)

Fig. 7: Histogram of the overlaps of the generated random quantum states for eight qubits where the Schmidt coefficients are fixed and the corresponding bipartite entanglements are given as weights of the edges on the graph.
be controlled by using quantum gates implementing the desired Schmidt coefficients. We also show that one can combine the Schmidt circuits sequentially to generate an equivalent quantum state for an acyclic weighted graph state in which vertices and edges correspond to subsystems and the bipartite entanglement between subsystems, respectively, and also the amount of entanglement is given by the weights of the edges.

Our method can be used in different applications and protocols relying on entanglement. In the simulation of quantum systems, one can use the method to create an instance of the desired system. In addition, decoherence effects the quality of the entanglement and generally cause errors in computations. A similar idea can be used in quantum error correction to correct an imperfect bipartite entanglement, and so a quantum channel.

**REFERENCES**

[1] A. Edelman and N. R. Rao, “Random matrix theory,” *Acta Numerica*, vol. 14, pp. 233–297, 5 2005.
[2] A. M. Tulino and S. Verdú, *Random matrix theory and wireless communications*. Now Publishers Inc, 2004, vol. 1.
[3] W. K. Wootters, “Random quantum states,” Foundations of Physics, vol. 20, no. 11, pp. 1365–1378, 1990.
[4] S. Wiesner, “Conjugate coding,” SIGACT News, vol. 15, no. 1, pp. 78–88, 1983.
[5] C. W. J. Beenakker, “Random-matrix theory of quantum transport,” Rev. Mod. Phys., vol. 69, pp. 731–808, Jul 1997.
[6] I. M. Tigner, A. Acin, E. Schenck, and M. Aspelmeyer, “Nonlocality of cluster states of qubits,” Phys. Rev. A, vol. 71, p. 042325, Apr 2005.
[7] M. Hein, J. Eisert, and H. J. Briegel, “Multiparty entanglement in graph states,” Phys. Rev. A, vol. 69, p. 062311, Jun 2004.
[8] D. Schlingemann and R. F. Werner, “Quantum error-correcting codes associated with graphs,” Phys. Rev. A, vol. 65, p. 012308, Dec 2001.
[9] M. Hein, W. Dr., J. Eisert, and H. J. Briegel, “A one-way quantum computer,” Phys. Rev. Lett., vol. 86, pp. 5188–5191, May 2001.
[10] M. Hein, W. Dr., J. Eisert, R. Raussendorf, Van den Nest, and H.-J. Briegel, “Entanglement in graph states and its applications,” in *the Proceedings of the International School of Physics “Enrico Fermi” on “Quantum Computers, Algorithms and Chaos”*, Varenna, Italy, July, vol. 162, pp. 115–218, 2006.
[11] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, and J.-W. Pan, “Experimental entanglement of six photons in imperfect bipartite entanglement, and so a quantum channel.

**Fig. 8:** Histogram of the overlaps of the generated random quantum states for eight qubits where the Schmidt coefficients are fixed and the corresponding bipartite entanglements are given as weights of the edges on the graph.
Fig. 9: Angles between the generated quantum states for two qubits, where the Schmidt coefficients are fixed to a certain value and the amount of the entanglement is high in (a) and low in (b).

Fig. 10: Angles between the generated quantum states for four qubits, where the Schmidt coefficients are fixed to a certain value and the amount of the entanglement is high in (a) and low in (b).