Investigating the Werner Basis Conjecture

Justin Cammarota

Lebanon Valley College, 17003 Annville, United States

(Dated: January 25, 2019)

Abstract

Multiparticle states called Werner states are defined by their invariance under the same unitary evolution operator acting on each particle. Already demonstrating nonlocal quantum properties, these states also have potential application in quantum computation and cryptography. This project is an attempt to prove a conjecture which hopes to ensure the set of Werner states constructed from non-crossing polygon diagrams can uniquely represent all Werner states.

I. INTRODUCTION

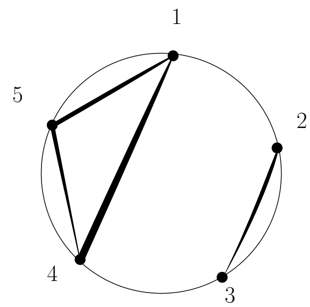
The discipline of quantum information science gained importance in the 1990s as researchers realized quantum states could be used for currently impossible computations. Many useful classes of states have been found, each with their individual uses, but the focus of this project is the class of Werner states. Werner states are defined by their invariance under the same unitary operation on every qubit position. This is important because many noise descriptions are based on unitary operators, so Werner states are useful in carrying information in noisy quantum channels [1], as it is possible to recover information lost to noise with known error-correcting operators.

II. BACKGROUND

Quantum information is stored in qubits, the quantum analog to classical bits. A n-qubit quantum state lies in a complex vector space and is formed by taking linear combinations (or superpositions) of n-bit strings. For example, a 3-qubit state vector could be $\frac{1}{10}(|000\rangle - 5i\,|010\rangle + 8\,|101\rangle + \sqrt{10}\,|111\rangle)$. Dirac's ket notation ($|\psi\rangle$) is used to represent vectors (complex conjugate-transposed vectors are represented by bras ($\langle\psi|$)). Quantum states are conventionally normalized, which means $\langle\psi|\psi\rangle$ must $= 1$. In a 1-qubit system, the basis vectors are $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, combined to produce higher dimensional qubit spaces using a tensor product ($\otimes$), which denotes the Kronecker product of the two matrices, done by multiplying each entry in the first matrix by the second matrix, and forming a matrix of those values. For example, a basis vector for the 2-qubit space is $|0\rangle \otimes |1\rangle$, which is normally written as $|01\rangle$.

III. FORMING WERNER STATES

A diagram method has been developed to represent Werner States in n-qubits [1]. To construct these states, a non-crossing polygon diagram with a total of n points along the circle, not all of which must be connected to another, is created. For example, in 5 qubits, a possible state can be represented by this diagram:



For each polygon in the diagram, the cyclic permutations of the bit strings of the size of the polygon are summed, with a normalization factor (so magnitude is 1) and roots of unity coefficients. Then, this string is turned into a density matrix. All the density matrices for each size bit string are summed, then normalizing the result. The final Werner state is formed by tensoring the density matrices in the positions specified by the points on the diagram.

$C_{[1,4,5]}(001) = \frac{1}{\sqrt{3}}(|001\rangle + e^{\frac{2\pi i}{3}} |010\rangle + e^{\frac{4\pi i}{3}} |100\rangle)$

$C_{[2,3]}(01) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

$C_3 = \frac{1}{2}(C_{[1,4,5]}(001)C_{[1,4,5]}(001)^\dagger + C_{[1,4,5]}(011)C_{[1,4,5]}(011)^\dagger)$

$C_2 = C_{[2,3]}(01)C_{[2,3]}(01)^\dagger$

$\rho_{\mathcal{D}} = (C_3)_{[1,4,5]} \otimes (C_2)_{[2,3]}$

Theorem 1 (Werner Basis Conjecture) *The states $\rho_{\mathcal{D}}$ (as $\mathcal{D}$ varies over all non-crossing polygon diagrams) form a basis for the space of Werner states (in the larger space of real linear combinations of Pauli tensors). [1]*

It has been shown that the size of this set matches the dimension of the Werner space, and the subject of our work was to prove this set is linearly independent.

IV. MATRICES AND INDEPENDENCE

Most of the work was done with the assistance of the GAP system, a free and open software package. All code examples are written for this program. The standard test for independence, which begins supposing $\sum_{\mathcal{D}} c_{\mathcal{D}}\rho_{\mathcal{D}} = 0$, is only practical for 2 qubits, as the higher dimensions become computationally infeasible.

For example, in 2 qubits, there are two possible Werner States:

$$\begin{bmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

which are independent by observation.

V. TRACE TESTS

One method tried was centered on applying a summation function (basically the trace extended to superdiagonals) to the set of Werner Diagrams at each superdiagonal. Using the scalar nature of the summation function, the coefficients could be pulled out and each successive superdiagonal summed. Each superdiagonal reduced the set of matrices to an equation. Once the summation function was applied to every superdiagonal, the set of equations is simpler than solving one equation for every position, but still fairly complicated, for example, in 4 qubits, 9 equations is obtained in 14 unknowns.

In 3 qubits (there are 5 non-crossing polygon diagrams) the equations are:

Level 0 (main diagonal): $c_1 + c_2 + c_3 + c_4 + c_5 = 0$

Level 1: $-\frac{1}{2}c_2 - \frac{1}{6}c_5 = 0$

Level 2: $-\frac{1}{2}c_3 - \frac{1}{6}c_5 = 0$

Level 3: $-\frac{1}{2}c_4 - \frac{1}{6}c_5 = 0$

VI. HILBERT-SCHMIDT INNER PRODUCT

After working with the summation function, a matrix of the Hilbert-Schmidt Inner Product (HIP) between each pair of diagrams was created, which would be square, and it can be shown that if the matrix is invertible, it would prove independence (therefore proving the Werner Basis Conjecture). In 3 and 4 qubits, the inner products were mostly real fractions. However, in higher dimensions, GAP began to give results as combinations of roots of unity, which made calculating the determinant and eigenvalues difficult, even for GAP. For 6 and fewer qubits, GAP was capable of returning values, which led to a conjecture on the determinant of these HIP matrices:

Theorem 2 (HIP Determinant Conjecture) $\det(A_n) = -\sum_{\ell=1}^{n-1} c_\ell \cdot (e^{\frac{2\pi i}{n}})^\ell$, *such that* $c_\ell = c_{n-\ell}$ *and* $c_\ell \neq 0$ *and the sum* $\neq 0$

Below is an example of the code used to create HIP matrices:

```
HIP := function(integer)
n:=integer;
c:=Catalan(n);
A:=IdentityMat(c);
B:=WD(n);
for i in [1..c] do;
for j in [1..c] do;
t:=TraceMat(B[i]*B[j]);
A[i][j]:=t; od; od; return A; end;
```

After running the code for 4 qubits (14 non-crossing polygon diagrams), the determinant of the HIP matrix was found to be $\frac{10935}{1125899906842624}$, showing the already difficult nature of the calculations, which only became more complex at higher dimensions.

A. Trends

Some trends were observed among entries in the HIP matrices. For example, when the same shape diagrams are multiplied together, the inner product returns the same value. The inner product also appeared to depend on the number of paired qubits or chord structure shared between the diagram states. However, it is not understand how this affects the inner products. Because the HIP matrices are symmetric, all values occur more than once, but it was also observed when roots of unity appeared, there were the same number of each root in the diagram. However, all the HIP matrices were Hermitian with real, rational traces, but this could not be leveraged into a general proof.

VII. GRAHAM-SCHMIDT PROCESS

As constructed, the Werner diagram basis is not orthonormal, so next GAP was used to orthonormalize each set. The goal was to find a new non-zero value in some place in each successive matrix; however, the n-gon's matrix always only included values in places from all the preceding matrices' values. The first several, usually all the single chord diagrams, are clearly independent after this process, however it is not so clear afterwards. Except for the all dots case, which has trace 1 (as a multiple of the identity), the trace of these orthonormalized diagrams is zero. For these diagrams, the roots and their conjugates appear in the same positions across the diagonal.

VIII. PERMUTATION MATRICES

Another form of matrix can be constructed from non-crossing polygon diagrams, a special kind of permutation matrix (denoted by V). These are formed by creating a permutation matrix for each polygon, and tensoring these together to form the matrix for the diagram. As it is known the permutation matrices form a basis over the space of the diagram states [2], the next idea was to use the permutation matrices and their relation to the Werner Diagrams to prove independence. By definition of a basis, any Werner diagram can be written as a linear combination of permutation matrices, and it can easily be shown the top Werner Diagram can be written in the form

$$\rho_{n\text{-gon}} \propto \sum_{k=0}^{n-1} (e^{\frac{2\pi i}{n}})^k V_{n\text{-gon}}^k \tag{1}$$

Exploring the expansion of Werner Diagrams and the powers of the top permutation matrices in the permutation basis, it was hoped to be able to express the powers of the top permutation matrix as a non-zero coefficient with the top matrix and some combination of lower diagrams, which could then form the foundation for a induction proof to show the top permutation matrix was also a combination of Werner Diagrams. These combinations could then be used in (1) to show independence of the Werner diagrams.

Theorem 3 (Method based on Permutation Matrices) *The set of Werner Diagrams is linearly independent if, when $\rho_{n\text{-}gon}$ is expanded in the permutation basis, the coefficient of $V_{n\text{-}gon}$ is nonzero.*

This code is an example of expanding a given matrix over a provided basis (`list`)

```
BasisCoef:=function(list,matrix)
A:=list; D:=[];
for i in [1..Length(A)] do;
Add(D,flatten(A[i])); od;
B:=matrix; C:=SolutionMat(D,flatten(B)); return C; end;
```

After running this code for the $V_{4\text{-gon}}$, the expansion of powers is shown below.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} V_{4\text{-gon}}^1$$

$$\begin{bmatrix} 1 & -1 & -1 & 0 & -1 & 0 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -2 \end{bmatrix} V_{4\text{-gon}}^2$$

$$\begin{bmatrix} -2 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & -1 & -1 & -1 & -1 & 1 \end{bmatrix} V_{4\text{-gon}}^3$$

A. N-gon coefficients

When expanding the powers of the top permutation matrices in the permutation basis, an interesting pattern developed. It began similar to an alternating Pascal's triangle, but by the fourth row ($n = 6$) the values began to differ. By the sixth row ($n = 8$), the sequence did not match any in the OEIS. Based on the symmetry and properties of the roots of unity, it can be shown the sum across any even row will always be real and across any odd row the sum will always be imaginary, however, it was unable to be shown the sum will not be zero.

Triangle of Coefficients of $V_{n\text{-gon}}$ to powers from 1 to $n-1$

$n=2$	1						
$n=3$	1	-1					
$n=4$	1	-2	1				
$n=5$	1	-3	3	-1			
$n=6$	1	-4	8	-4	1		
$n=7$	1	-5	17	-17	5	-1	
$n=8$	1	-6	33	-56	33	-6	1

Based on the observations, it is conjectured the expansion of the top permutation matrix squared is

$$V_{n\text{-gon}}^2 = (2-n) \cdot V_{n\text{-gon}} + \text{ others},$$

which then could be use for induction on higher powers of $V_{n\text{-gon}}$ to show the coefficient is nonzero. It was also observed the coefficients of the identity matrix in these expansions are the values from the triangle, but backwards across the rows.

B. Inverse Matrices

While trying to discover where these coefficients come from, the expansion of the inverse of the top permutation matrices was experimented with. The inverse of the k power of the $V_{n\text{-gon}}$ is the $n-k$ power, so it was hoped understanding the power and its inverse's relationship would help to understand where the coefficients come from, as the power and the inverse have the same top matrix coefficient, sometimes with the opposite sign, when expanded in the permutation basis. These observations led to this proven conjecture on the form of the inverse.

Theorem 4 *Expansion of* $V_{n\text{-}gon}^{-1}$

$V_{n\text{-}gon}^{-1} = \mathrm{Id} + \sum_{k=0}^{n} (-1)^k \sum_{|p|=k} V_{p\cup\mathrm{dots}}$

IX. RESULTS AND FURTHER WORK

While the Werner Basis Conjecture was unable to be proven, it was possible to investigate several avenues for proof, and the last idea on the expansion of Werner Diagrams in the permutation basis has the best chance of success. The proof hinges on the understanding of the triangle of coefficients, as if it can be understood where they come from and a formula can be obtained, it could be shown the coefficient for the top permutation matrix will never be zero, and the proof follows from there.

X. ACKNOWLEDGEMENTS

This work was supported by a Lebanon Valley College Arnold faculty-student research grant in 2016. Thank you to my faculty mentor, Dr. David Lyons. Lebanon Valley College

Mathematical Physics Research Group

`http://quantum.lvc.edu/mathphys`

---

[1] David W. Lyons, Abigail M. Skelton, and Scott N. Walck. Werner state structure and entanglement classification. *Advances in Mathematical Physics*, 2012:463610, 2012. arXiv:1109.6063v2 [quant-ph].

[2] Markus Grassl, Martin Rötteler, and Thomas Beth. Computing local invariants of quantum-bit systems. *Phys. Rev. A*, 58:1833–1839, Sep 1998. arXiv:quant-ph/9712040.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.