

**CALCULATION OF QUANTUM ENTANGLEMENT USING A GENETIC
ALGORITHM**

A Thesis by

Joseph Lesniak

Bachelor of Science, University of Wisconsin – Eau Claire, 1984

Submitted to the Department of Physics
And the faculty of the Graduate School of
Wichita State University
In partial fulfillment of
The requirements for the degree of
Master of Science

May 2007

© Copyright 2007 by Joseph Lesniak

All Rights Reserved

CALCULATION OF QUANTUM ENTANGLEMENT USING GENETIC ALGORITHM

I have examined the final copy of this thesis for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Master of Science with a major in Physics.

Elizabeth C. Behrman, Committee Chair

We have read this thesis
And recommend its acceptance

Jason W. Ferguson, Committee Member

James E. Steck, Committee Member

Shades of grey wherever I go
The more I find out the less that I know
Black and white is how it should be
But shades of grey are the colors I see
Billy Joel

ACKNOWLEDGMENTS

I would like thank Dr. Elizabeth C. Behrman for her many, many, years patience and understanding. I also want to thank the members of my committee for their patience, Dr. James E. Steck and Dr. Jason W. Ferguson. And Toboe, for him being his silly self.

ABSTRACT

Quantum entanglement is a multifaceted property that has attracted much attention, since it is used as the basis for such applications as quantum cryptography, quantum teleportation, and quantum computing. The calculation of quantum entanglement therefore has gained importance. As systems that use entanglement have evolved, the calculation of entanglement has become much more complex. A general method was developed for the calculation of entanglement for n-qubit or n-qudit system, based on the relative entropy of entanglement, and using a genetic algorithm technique. The method was tested on a two qubit system, for which there are some known points, and compared to exact calculations using the entanglement of formation and to another approximate method based on a quantum neural network. Advantages and disadvantages of the method and future work are discussed.

TABLE OF CONTENTS

| Chapter | Page |
|---|------|
| I. Introduction | 1 |
| II. Postulates for Entanglement Measures | 5 |
| III. Entanglement Measures | 10 |
| IV. Genetic Algorithm | 17 |
| V. Minimal Entanglement of a Two Qubit System | 21 |
| VI. Results | 27 |
| VII. Discussion and Future Work | 35 |
| List of References | 41 |
| Appendix | 46 |

Chapter 1

Introduction

Quantum entanglement has been known since 1935 when Einstein, Podolsky and Rosen, (EPR) [1], and Schrödinger [2] investigated the counterintuitive properties of quantum systems. The question of expected locality of the entangled quantum systems raised by EPR allowed Bell to develop his famous inequalities serving as a test of strange properties of the simplest entangled wave function represented by a singlet state. Still science had to wait a long time for the first experimental demonstration of the violations of Bell's inequalities [3, 4, 5] and for proposals of practical applications of quantum entanglement [6]. Nowadays such proposals constitute two main branches of nonclassical information theory: quantum communication and quantum computing. The first comprises quantum cryptography [7], quantum dense coding [8], and quantum teleportation [9], which developed into the quantum channels theory. The second is based on quantum algorithms [10, 11], which have been shown to work better than their classical counterparts, in two ways: first, that there are things quantum computers can calculate much faster than classical computers; and second, that there are things quantum computers calculate which it is impossible for classical computers to calculate. The main obstacle to the physical realization of all those highly nonclassical and nontrivial phenomena is their sensitivity to quantum noise. This leads to the development of quantum error correction [12, 13] and fault tolerant computing [11] on the quantum computing theory [14].

We begin with a few definitions that will be important in the discussion. **Entangled and separable states:** A state of a compound system is called entangled if it cannot be written as a single tensor product of subsystem states. This state which can be written in product form $\Psi = \Psi^A \times \Psi^B$ is called unentangled or separable [15].

CHSH (Bell's) Inequality: Let S_1, S_2, T_1, T_2 , be random variables that have ± 1 as the only possible values. Then the probabilities $\text{prob}(S_j=T_k)$ satisfy the inequality

$$\text{prob}(S_1=T_2) \leq \text{prob}(S_1=T_1) + \text{prob}(S_2=T_1) + \text{prob}(S_2=T_2) \quad (1.1)$$

Bell was the first to derive inequalities for the joint probabilities that can discriminate between quantum mechanics and local realistic theories. This is a variant of Bell's inequality and is due to Clauser, Horne, Shimony, and Holt [3]. Local realism refers to any theory that satisfies the assumptions of realism and independence, which implies, in particular, an assumption of locality [15].

Local general measurements, LGM: These are performed by the two parties, A and B, separately and are described by two sets of operators satisfying the completeness relations $\sum_i A_i^\dagger A_i = 1$ and $\sum_i B_i^\dagger B_i = 1$. The joint action of the two is described by $\sum_{ij} A_i \otimes B_j = \sum_i A_i \otimes \sum_j B_j$, which is again a complete general measurement, and obviously local.

Classical communication, CC: This means that the actions of A and B can be correlated. This can be described by a complete measurement on the whole space $A + B$ and is not necessarily decomposable into a sum of direct products of individual operators as in LGM. If ρ_{AB} describes the initial state shared by A and B then the transformation involving "LGM+CC" would look like

$$\Phi(\rho_{AB}) = \sum_i A_i \otimes B_i \rho_{AB} A_i^\dagger B_i^\dagger \quad (1.2)$$

where $\sum_i A_i^\dagger A_i B_i^\dagger B_i = 1$ meaning the actions of A and B are "correlated." [16]

Any study of entanglement measures must begin with a discussion of what entanglement is, and how we actually use it. Entanglement can loosely be described as the quantum

correlations that can occur in many party quantum states. How do we define quantum correlations, and what differentiates them from classical correlations? In the context of quantum information a precise way to define classical correlations is by LOCC, Local Operations and Classical Communication, operations. Classical correlations can be defined as those that can be generated by LOCC operations. If we observe a quantum system and find correlations that cannot be simulated classically, then we attribute them to quantum effects, and label them quantum correlations. Suppose that we have a noisy quantum state, and we process it using LOCC operations. If in this process we obtain a state that can be used for some task that cannot be simulated by classical correlations, such as violating a Bell inequality [15], then we must not attribute these effects to the LOCC processing that we have performed, but to quantum correlations that were already present in the initial state, even if the initial state was quite noisy. This is an extremely important point that is at the heart of the study of entanglement. It is the constraint to LOCC operations that elevates entanglement to the status of a resource.

The usefulness of entanglement emerges because it allows us to overcome a particular constraint that is called the LOCC constraint. This restriction has both technological and fundamental motivation, and arises naturally in many explicit physical settings involving quantum communication across a distance.

In any quantum communication experiment we would like to be able to distribute quantum particles across distantly separated laboratories. Perfect quantum communication is essentially equivalent to perfect entanglement distribution. If we can transport a quantum system without any decoherence, then any entanglement shared by that quantum system will also be distributed perfectly. Conversely, if we can distribute entangled states perfectly then with a small amount of classical communication we may use teleportation to transmit quantum states

perfectly [14]. However, in any foreseeable experiment involving these processes, the effects of noise will inevitably impair our ability to send quantum states over long distances.

One way of trying to overcome this problem is to distribute quantum states by using the noisy quantum channels that are available, but then to try to combat the effects of this noise using higher quality local quantum processes in the distantly separated labs. Such local quantum operations, ‘LO’, will be much closer to ideal, as they can be performed in well controlled environments without the decoherence induced by communication over long distances. However, there is no reason to make the operations of separated labs totally independent. Classical communication, ‘CC’, can essentially be performed perfectly using standard telecom technologies, and so we may also use such communication to coordinate the quantum actions of the different labs.

The complete usefulness of entanglement is not presently known, just as it is not yet known what the power of quantum computing will enable us to do. Unfortunately, despite a great deal of work by a large number of well-funded and very bright people, entanglement and the calculation of entanglement are not yet fully understood. In Chapter 2 a few postulates for what "entanglement" is are presented and discussed. Entanglement measures are introduced, and discussed, in Chapter 3. Most if not all of these are a) difficult to calculate and/or b) not generalizeable. A possible approach to this difficulty is the use of genetic algorithm, which is presented in Chapter 4. Chapter 5 discusses how entanglement measures and genetic algorithm can be used together to find minimum entanglement. The results of the genetic algorithm calculations of the entanglement are compared to other methods in Chapter 6. Chapter 7 is the discussion and future work section.

Chapter 2

Postulates for Entanglement Measures

How can entanglement be measured? Various quantities have been proposed for entanglement measures: entanglement distillation [17, 18, 19]; the entanglement cost [17, 20, 21, 22, 23]; the relative entropy of entanglement [16, 24, 25]; and the squashed entanglement [26]. Each of these will be discussed in detail in Chapter 3. In this chapter we will present some background and basic properties that any entanglement measure should have. In general, we would want a measure which is generally applicable to a system of any size, since any really useful application of entanglement will demand a large quantum system.

First the quantum system must be defined. Usually, quantum computing is based on the idea of “qubits”, which are quantum versions of the binary “bit” familiar in classical computing. A qubit has two states, usually designated as $|0\rangle$ and $|1\rangle$, and preserves their superposition. It is a unit of computation. A network of quantum computer consists of a bundle of qubits. Quantum computation is a sequence of quantum gates, unitary transformations, on the qubits. A large quantum system would then have a large number of these qubits. As with classical computing, the power of the quantum computer would increase with size; though, because of the possibility of quantum superposition [15], each qubit contains within itself an effectively large number of equivalent bits, and the power increases exponentially with the number of qubits.

Another way of increasing the size and therefore the power of the computer would be with the use of “qudits”, quantum versions of d-ary digits such as binary or trinary [27]. Multiple-valued quantum logic is in such relation to binary quantum logic as multiple-valued reversible logic to binary reversible logic. Although building quantum computers based on multiple-valued logic has many advantages over binary quantum computers and is already

technically possible on experimental scale, very little research in qudits has been performed so far, either related to practical realization or to design theory of multiple valued quantum computers. Qubit-based quantum computation is adequate for considering fundamental issues such as complexity classes or computability, but, from a practical perspective, encoding as qudits may be more natural, or constitute a more efficient use of resources. For example, coupled harmonic oscillators can admit various qudit encodings that exploit the full Hilbert space and can serve as a control state with any qudit as the target state, or vice versa [27, 28]. Qubits are often only ideals: many systems involve multiple levels for each degree of freedom, and the qubit is encoded into the two lower of these levels. For example, an atom has an infinite number of energy levels. There is no need to restrict to only two of them. The theory for hybrid qudit systems can be useful for different interacting physical systems, with a d_1 -dimensional qudit natural for one system and a d_2 -dimensional qudit natural for another. The major difference between quantum logic and binary logic is the concept of the information itself. While the classical, binary or multi-valued, representations of information are precise and deterministic, in Multi Valued (MV) Quantum Computing the concept of bit is replaced by the qudit. Unlike classical bits that are realized as electrical voltages or currents present on a wire, MV quantum logic operations manipulate qudits, which are microscopic entities such as a photon or atomic spin. Analogous to the $|0\rangle$ and $|1\rangle$ states for the qubit, in a d -level system, the d states can be labelled as

$$|k\rangle (k = 0, 1, 2, \dots, d-1). \quad (2.1)$$

When we express states and operators in matrix form we identify it with d -dimensional vector

$$|k\rangle = \begin{pmatrix} 0, 0, \dots, 0, \underset{\substack{k \\ v}}{1}, 0, \dots, 0 \end{pmatrix}, \quad (2.2)$$

where t means transpose. Allowing d to be arbitrary enables a tradeoff between the number of qudits making up the quantum computer and the number of levels in each qudit. Quantum computation with qudits is a sequence of unitary transformations on a bundle of qudits, just with the qubit case.

When a network is constructed in an actual physical system, decoherence arises. This is caused by interaction with the environment. Thus it is better that number of steps and overall time of computation is small. Use of a multi-valued unit may decrease the number of steps. This is favorable for the decoherence problem. Additionally, the waste of high excited states in physical systems may fall off with large d [27].

Whether with a large number of qubits, or a (perhaps smaller) number of qudits, we need a general method for measuring the entanglement. What properties should a good entanglement measure possess? Most authors agree that a good entanglement measure should obey the following :

1. A bipartite entanglement measure $E(\rho)$ is a mapping from density matrices into positive real numbers:

$$\rho \rightarrow E(\rho) \in \mathbb{R}^+ \quad (2.3)$$

defined for states of arbitrary bipartite systems. A normalization factor is also usually included such that the maximally entangled state

$$|\Psi_d^+\rangle = \frac{|0,0\rangle + |1,1\rangle + \dots + |d-1,d-1\rangle}{\sqrt{d}} \quad (2.4)$$

of two qudits, d -dimensional quantum particles, has $E(|\Psi_d^+\rangle) = \log d$.

2. $E(\rho) = 0$ if the ρ is separable.
3. E does not increase on average under LOCC

$$E(\rho) \geq \sum_i p_i E\left(\frac{A_i \rho A_i^\dagger}{\text{tr} A_i \rho A_i^\dagger}\right) \quad (2.5)$$

where the A_i are the Kraus operators describing some LOCC protocol and the probability of obtaining i is given by $p_i = \text{tr} A_i \rho A_i^\dagger$. The definition of a Kraus operator is the following. Let H and G be Hilbert spaces of dimension n and m respectively, and Φ be a quantum operation taking the density matrices acting on H to those acting on G . Then there are matrices

$$\{B_i\}_{1 \leq i \leq nm} \quad (2.6)$$

acting on G such that

$$\Phi(S) = \sum_i B_i^* S B_i. \quad (2.7)$$

Conversely, any map Φ of this form is a quantum operation provided

$$\sum_i B_i B_i^* \leq 1. \quad (2.8)$$

The matrices B_i are called Kraus operators. [29]

4. For a pure state $|\Psi\rangle\langle\Psi|$ the measure reduces to the entropy of entanglement

$$E(|\Psi\rangle\langle\Psi|) = (S \circ \text{tr}_B)(|\Psi\rangle\langle\Psi|). \quad (2.9)$$

where S denotes the von Neumann entropy $S(\rho) = -\text{tr}[\rho \log_2 \rho]$ and tr_B denotes the partial trace over subsystem B .

We will call any function E satisfying the four conditions an entanglement monotone [30]. The term entanglement measure will be used for any quantity that satisfies axioms (1), (2) and (4), and also does not increase under deterministic LOCC transformations. Conditions (1) - (4) may be replaced by an equivalent set of slightly more abstract conditions. Also, some authors [30, 31] impose additional requirements for entanglement measures:

Convexity – The concept of convexity which means that we require

$$E\left(\sum_i p_i p_i\right) \leq \sum_i p_i E(p_i). \quad (2.10)$$

Requiring this mathematically very convenient property is sometimes justified as capturing the notion of the loss of information.

Additivity – Given an entanglement measure and a state σ one may ask for the condition $E(\sigma^{\otimes n}) = nE(\sigma)$ to be satisfied for all integer n . A measure satisfying this property is said to be additive. Significant entanglement measures do not satisfy this condition and for this reason additivity is not a basic postulate.

Continuity – $S(\rho_A)$ represents the reversible rate of conversion between pure states in asymptotic regime which strongly suggests that it is appropriate measure of entanglement for pure states. It turns out that any entanglement monotone that is (a) additive on pure states, and (b) sufficiently continuous must equal $S(\rho_A)$ on all pure states.

Extremal Entanglement Measures – Entanglement measures ranges need to be bounded. Suppose that we have a quantity $L(p)$ satisfying condition (1) – (3) above, that is also asymptotically continuous on mixed states, and also has a regularization

$$\lim_{x \rightarrow \infty} \frac{L(\rho^{\otimes n})}{n}. \quad (2.11)$$

Then it can be shown that

$$E_C(\rho) \geq \lim_{x \rightarrow \infty} \frac{L(\rho^{\otimes n})}{n} \geq E_D(\rho). \quad (2.12)$$

Chapter 3

Entanglement Measures

How can entanglement be measured? Various quantities have been proposed for entanglement measures: entanglement distillation; the entanglement cost; the entanglement of formation, the relative entropy of entanglement; and the squashed entanglement. Each of these will now be discussed in detail.

The distillable entanglement – The distillable entanglement [17, 18, 19, 30, 31], $E_D(\rho)$, provides us with the rate at which noisy mixed states ρ may be converted into the “gold standard” singlet state by LOCC alone.

$$E_D(\rho) := \sup \{r : \lim_{n \rightarrow \infty} [\inf_{\Psi} \text{tr} |\Psi(\rho^{\otimes n}) - \Phi(2^n)|] = 0\}. \quad (3.1)$$

Despite the importance, for practical applications, of the distillable entanglement as an entanglement, very little progress has been made in terms of its computation. It is known for pure states where it equals the entropy of entanglement and for some simple but very special states [16, 38] such as the Bell diagonal states of rank 2. The computation requires the explicit construction of complex purification procedures in the asymptotic limit to find the lower bound.

The entanglement cost – For a given state ρ the entanglement cost [17, 20, 21, 22, 23, 30, 31] quantifies the maximal possible rate r at which one can convert blocks of 2-qubit maximally entangled states into output states that approximate many copies of ρ , such that the approximations approach zero in the limit of large block sizes. If we denote a general trace preserving LOCC operation by Ψ , and write $\Phi(K)$ for the density operator corresponding to the maximally entangled state vector in K dimensions, $\Phi(K) = |\psi_K^+\rangle\langle\psi_K^+|$, then the entanglement cost is defined as

$$E_C(\rho) := \inf\{r : \lim_{n \rightarrow \infty} [\inf_{\Psi} \text{tr} |\rho^{\otimes n} - \Psi(\Phi(2^m))|] = 0\} \quad (3.2)$$

This quantity is very difficult to compute. It is known to equal the entropy of entanglement for pure bipartite states (i.e., for a two-qubit system). It can also be computed for trivial mixed states $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ where $|\psi_i\rangle$ may be discriminated locally perfectly without destroying that states. A simple example is $|\psi_1\rangle = |00\rangle$ and $|\psi_2\rangle = (|11\rangle + |22\rangle)/\sqrt{2}$. A closely related measure of entanglement, entanglement of formation, may actually equal the entanglement of cost.

The entanglement of formation – For a general state ρ it is defined as [30]

$$E_F(\rho) := \inf\left\{\sum_i p_i E(|\psi_i\rangle\langle\psi_i|)\right\}. \quad (3.3)$$

$$\text{where } \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad (3.4)$$

This measure represents the minimal possible average entanglement over all pure state decompositions of ρ_i where $E(|\psi\rangle\langle\psi|) = S(\text{tr}_B\{|\psi\rangle\langle\psi|\})$ is taken as the measure of entanglement for pure states, and S is the von Neumann entropy [21]. It can be expected to be closely related to the entanglement cost of ρ . In general E_F is extremely difficult to solve and one must resort to numerical techniques for general states [32], restrict attention to cases with high symmetry [33, 34, 35], or consider only cases of low dimensionality. A closed form solution is known for bi-partite qubit states [22, 23, 32]. This exact formula is based on the often used two-qubit concurrence which is defined as

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \quad (3.5)$$

where the λ_i are in decreasing order, the square roots of the eigenvalues of the matrix $\rho\sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$ where ρ^* is the complex conjugate of ρ . For general bi-partite qubit states it has been shown that [23]

$$E_F(\rho) = s\left(\frac{1 + \sqrt{1 - C^2(\rho)}}{2}\right) \quad (3.6)$$

with

$$s(x) = -x \log_2 x - (1-x) \log_2 (1-x). \quad (3.7)$$

The two-qubit $E_F(\rho)$ and the two-qubit concurrence are monotonically related. It should be noted that the entanglement of formation is an entanglement measure, and the concurrence obtains its meaning via its relation to entanglement of formation and not vice versa. For higher dimensional systems this connection breaks down, in fact there is not even a unique definition of the concurrence.

Entanglement measures from convex roof constructions – The entanglement of formation E_F is an important example of the general concept of a convex roof construction. The convex roof \hat{f} of a function f is defined as the largest convex function that is for all arguments bounded from above by the function f . The importance of the convex roof method is based on the fact that it can be to construct entanglement monotones from any unitarily invariant and concave function of density matrices [36].

The relative entropy of entanglement – The regularized version of the relative entropy of entanglement is a measure that lies between entanglement cost and entanglement of distillation [16, 24, 25]. The quantum mutual information is [6]

$$I(\rho_{AB}) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}). \quad (3.8)$$

Employing the quantum relative entropy

$$S(\rho \parallel \sigma) := \text{tr}\{\rho \log \rho - \rho \log \sigma\} \quad (3.9)$$

which is a measure of distinguishability between quantum states, one may then write the quantum mutual information as

$$I(\rho_{AB}) = S(\rho_{AB} \parallel \rho_A \otimes \rho_B). \quad (3.10)$$

The total correlations are quantified by a comparison of the state ρ_{AB} with the closest separable state, a classically correlated state devoid of quantum correlations. The general definition of the relative entropy of entanglement [16, 24, 37, 38] with respect to a set X as

$$E_R^X(\rho) := \inf_{\sigma \in X} S(\rho \parallel \sigma). \quad (3.11)$$

This definition leads to a class of entanglement measures known as the relative entropies of entanglement [39]. In the bipartite setting the set X can be taken as the set of separable states, states with positive partial transpose, or non-distillable states. In the multiparty setting there are even more possibilities [37, 40] but for each such choice a valid entanglement measure is obtained as long as the set X is mapped onto itself under LOCC.

See Figure 1, which shows the relative entropy of entanglement is defined as the smallest relative entropy distance from the state ρ to state σ taken from the set X . The set X may be defined as the set of separable states, non-distillable states or any other set that is mapped onto itself by LOCC [30].

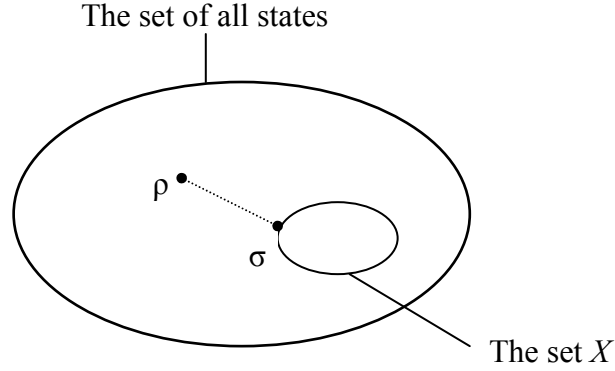


Figure 1. The relative entropy of entanglement is defined as the smallest relative entropy distance from the state ρ to state σ taken from the set X . The set X may be defined as the set of separable states, non-distillable states or any other set that is mapped onto itself by LOCC.

Employing the properties of the quantum relative entropy it is then possible to prove that it is a convex entanglement measure satisfying all the conditions (1) – (4) [16].

The squashed entanglement – Squashed entanglement is defined as

$$E_{sq} := \inf \left[\frac{1}{2} I(\rho_{ABE}) : tr_E \{ \rho_{ABE} \} - \rho_{AB} \right] \quad (3.12)$$

where :

$$I(\rho_{ABE}) := S(\rho_{AE}) + S(\rho_{BE}) - S(\rho_{ABE}) - S(\rho_E) \quad (3.13)$$

$I(\rho_{ABE})$ is the quantum conditional mutual information. E_{sq} comes from related quantities in classical cryptography that determine correlations between two communicating parties and an eavesdropper. The squashed entanglement is a convex entanglement monotone that is a lower bound to $E_F(\rho)$ and an upper bound to $E_D(\rho)$, and equal to $S(\rho_A)$ on pure states.

Entanglement Witness monotonies – Entanglement Witnesses are tools used to determine whether a state is separable. A Hermitian operator W is defined as an Entanglement Witness if:

$$tr \{ W \rho \} < 0 \quad (3.14)$$

for non separable ρ . W acts as a linear hyperplane separating some entangled states from the convex set of separable ones. See Figure 2, (Note that the use of the particular scale cited here is arbitrary. In a previous paper [41], we use a different scale.)

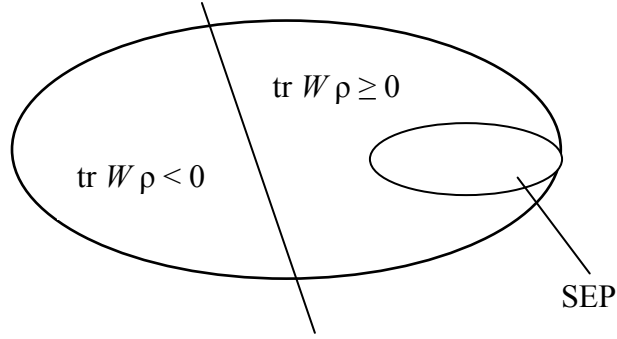


Figure 2. An entanglement witness is a Hermitean operator defining a hyperplane in the space of positive operators such that for all separable states we have $\text{tr } W \rho \geq 0$ and there is a ρ for which $\text{tr } W \rho < 0$.

An example of an entanglement witness is that of Tóth and Gühne [42].

$$W_{TG-B} = I - \sigma_{xA} \sigma_{xB} - \sigma_{zA} \sigma_{zB} \quad (3.15)$$

where $\sigma_{xA} = \sigma_x \otimes I$, $\sigma_{zA} = \sigma_z \otimes I$, $\sigma_{xB} = I \otimes \sigma_x$, $\sigma_{zB} = I \otimes \sigma_z$. It is optimized for states close to $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$.

As is noted above, all the measures are very difficult to calculate in general. The only one for which there exists a closed form solution is the entanglement of formation and even then the solution is only for the two-qubit case. But, as noted in Chapter 1, we are going to need at the very least large numbers of qubits for any realistic application, and, probably, large numbers of qudits. Thus we will need a general method for determining the entanglement of an n-qubit system or n-qudit system.

Entanglement witnesses have been designed that can easily be calculated, measured, and applied, even to multiple qubit systems. However, these are only approximate, they do not tell

us how much entanglement there is and, frequently, they are inaccurate as well [41]. Clearly, we need a convenient and accurate method for general entanglement calculation. In this thesis, we develop a general method for calculating the entanglement, based on a genetic algorithm technique applied to the entropy of entanglement. We test and apply it to the relatively simple two-qubit system, in order that we will be able to determine whether it is working; however, its advantage is that it is easily extendible to multiple qubit systems and to qudit systems.

Chapter 4

Genetic Algorithm

Genetic algorithm can be used to solve many different types of problems for which exact algorithms are not known. It will be used in this thesis to find the minimum entanglement (Chapter 5). This chapter explains how genetic algorithm works and how different options may affect the minimization process.

Genetic algorithm [43, 44] is a method for solving both constrained and unconstrained optimization problems that is based on natural selection, the process that drives biological evolution. A genetic algorithm repeatedly modifies a population of individual solutions. At each step, the genetic algorithm selects individuals at random from the current population to be parents and uses them to produce the children for the next generation. Over successive generations, the population evolves toward an optimal solution. You can apply the genetic algorithm to solve a variety of optimization problems that are not well suited for standard optimization algorithms, including problems in which the objective function is discontinuous, nondifferentiable, stochastic, or highly nonlinear. The genetic algorithm uses three main types of rules at each step to create the next generation from the current population:

- Selection rules select the individuals, called parents, that contribute to the population at the next generation.
- Crossover rules combine two parents to form children for the next generation.
- Mutation rules apply random changes to individual parents to form children.

The genetic algorithm differs from a classical, derivative-based, optimization algorithm in two main ways. A classical algorithm generates a single point at each iteration, and then the

sequence of points approaches an optimal solution. The selection of the next point in the sequence is by a deterministic computation. A genetic algorithm generates a population of points at each iteration and then the best point in the population approaches an optimal solution. The selection of the next population is by computation which uses random number generators.

A genetic algorithm is a computational technique based on the evolution of the species. A possible solution to the problem is coded in a binary string, called a chromosome. An initial population of chromosomes is created at random and processed by natural selection. During reproduction: crossover, the exchange of parts of the binary string between chromosomes; mutation, the inversion of the bits of the binary string; and inversion, all take place at random position in the binary string. An evaluation of the fitness, how good the solution is, takes place for all individuals in the population. With these rules, the features of one solution can be transmitted to next generation of chromosomes and better solutions can be found. Natural selection and reproduction are probabilistic stages and, hence, a genetic algorithm is a random process. The best solution cannot be predicted, but a number of generations must run to find the best solution.

There seven basic steps to using a genetic algorithm.

1. Start with a random population of individuals.
2. Calculate the value or fitness of each these individuals from the fitness function.
3. Choose two individual based on fitness and call them parents. Remove them from the population.
4. The parents are now allowed to have children. They are allowed to share their bits.
5. The children's bits are now mutated.
6. Two children are called the new generation.

- Return to Step 2 until the new generation contains n individuals. Then replace the old population with the new generation. Return to Step 1.

Figure 3 shows a flow chart of the algorithm.

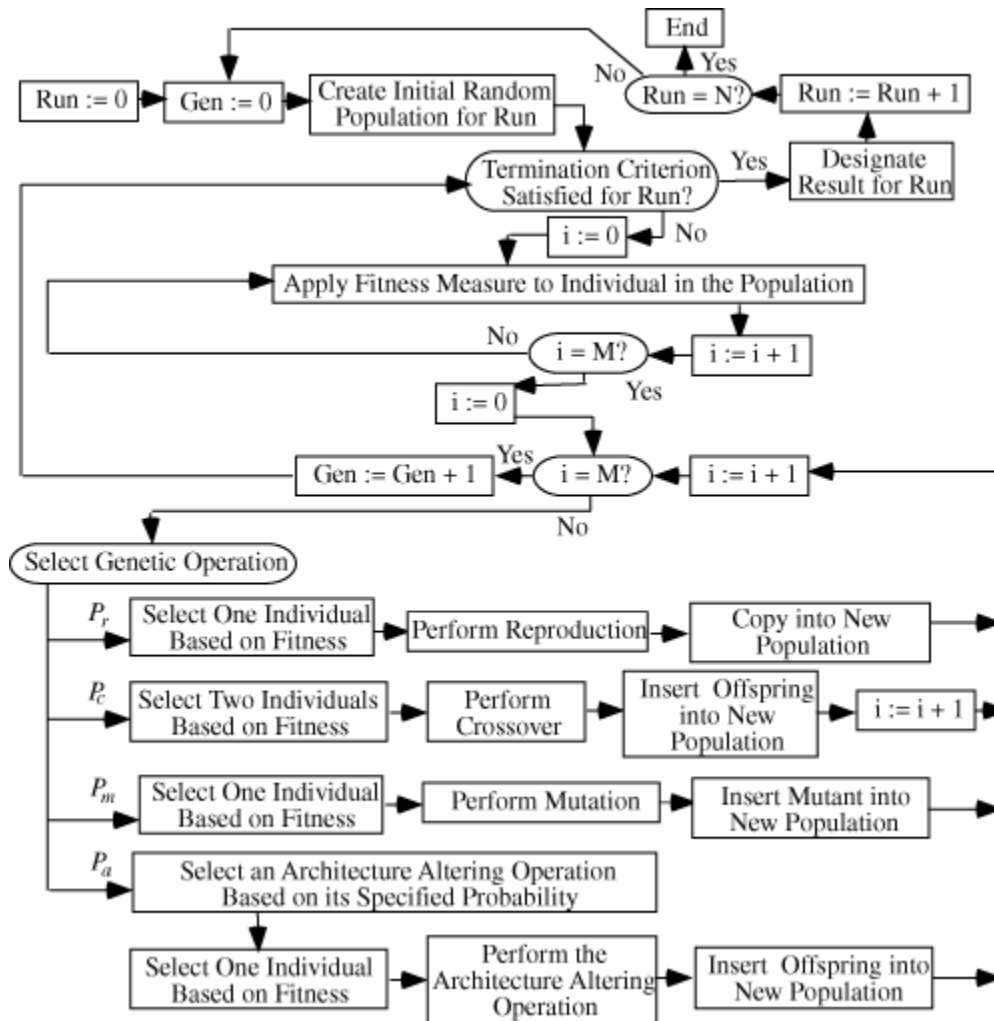


Figure 3 The figure is a flowchart showing the execution steps of a run of genetic programming. The flowchart shows the genetic operations of crossover, reproduction, and mutation as well as the architecture-altering operations. This flowchart shows a two-offspring version of the crossover operation.

There are numerous applications of genetic programming. Black Art Problems, such as the automated synthesis of analog electrical circuits, controllers, antennas, networks of chemical reactions, optical systems, and other areas of design. Programming The Unprogrammable, PTU,

which involves the automatic creation of computer programs for unconventional computing. This includes devices such as cellular automata, multi-agent systems, parallel programming systems, field-programmable gate arrays, field-programmable analog arrays, ant colonies, swarm intelligence, distributed systems, and the like. Commercially Useful New Inventions (CUNI) involving the use of genetic programming as an automated "invention machine" for creating commercially usable new inventions.

Chapter 5

Minimal Entanglement of a Two Qubit System

In this chapter, a genetic algorithm is applied to the calculation of the entanglement of a two qubit system. We do this by using the relative entropy of entanglement (see Chapter 3), which is defined as a minimum distance to the set of separable states. The Bures distance is used for the distance measure. This chapter describes how it is implemented, and tested on a set of states for which the answer is known (completely entangled and completely separable states). The test results are also shown.

Consider a general quantum system consisting of two parts labeled A and B. Any pure state $|\Phi\rangle$ of the system can always be written in the form

$$|\Phi\rangle = \sum_{i=1}^n c_i |\phi_i^A\rangle \otimes |\phi_i^B\rangle \quad (5.1)$$

where $\{|\phi_1^A\rangle, \dots, |\phi_n^A\rangle\}$ and $\{|\phi_1^B\rangle, \dots, |\phi_n^B\rangle\}$ are sets of orthonormal states for subsystems A and B, respectively, and the c_i 's are a set of positive coefficients. The possibility of entanglement is simply the possibility that there may be more than one term in the above sum. The values c_i are precisely the features of the state $|\Phi\rangle$ that do not change when the parts of the system are subjected to separate unitary transformations. Therefore any reasonable definition of the entanglement of $|\Phi\rangle$ should depend only on those values.

A pure state is defined as one for which a ket exists. The density matrix for a pure state can then be written as

$$\rho_{pure} = |\chi\rangle\langle\chi| \quad (5.2)$$

where $|\chi\rangle$ is the ket and $\langle\chi|$ is the bra, the Hermitian conjugate of the ket. A mixed state is one that cannot be written as a ket. For example, the state

$$\rho_{mixed} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \quad (5.3)$$

is mixed. A mixed state can in general be written in an infinite number of pure state decompositions of the form of equation (3.4).

The entanglement of formation is (see Chapter 3)

$$E_f(\rho) = \inf \sum_j p_j E(\Phi_j), \quad (5.4)$$

where the infimum is taken over all pure-state decompositions of ρ . By definition, the entanglement of formation of ρ is zero if and only if ρ is separable, that is, if and only if ρ can be written as a mixture of product states. Entanglement of formation is additive if

$$E_f(\rho \otimes \sigma) = E_f(\rho) + E_f(\sigma), \quad (5.5)$$

where ρ and σ are any two bipartite states. [19]

The definition of entanglement of formation requires finding the minimum average entanglement over all possible pure-state decompositions of the given mixed state ρ . Even for a simple system such as a pair of qubits, the number of parameters required to specify all possible decompositions can be large. A mixed state can be written as a sum of pure states in a large number of different ways. But due to a theorem by Uhlmann [45], it is sufficient to consider decompositions with no more than r^2 terms, where r is the rank of ρ , in order to find the minimum average entanglement. Thus for a pair of qubits, one needs only consider mixtures of 16 or fewer pure states. In fact it turns out that for a pair of qubits one never needs more than four terms [22, 46]. However, for mixed states of larger systems, the number of terms needed in an optimal decomposition often greatly exceeds the rank of the density matrix [47, 48].

The Bures distance [49, 50]

$$D_B(\rho_1, \rho_2)^2 = 2 - 2\text{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} = 2 - 2\sqrt{F(\rho_1, \rho_2)} \quad (5.6)$$

is a function of fidelity [51]

$$F(\rho_1, \rho_2) := \left[\text{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}} \right]^2. \quad (5.7)$$

This quantity is sometimes called Uhlmann transition probability [50], since for a pair of pure states it reduces to the squared overlap, $F = \text{Tr}\rho_1\rho_2 = |\langle\psi_1|\psi_2\rangle|^2$.

$F(\rho_1, \rho_2)$ satisfies the following natural axioms [50]:

1. $F(\rho_1, \rho_2) \leq 1$ and $F(\rho_1, \rho_2) = 1$ if and only if $\rho_1 = \rho_2$.
2. $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$.
3. If ρ_1 is a pure state $\rho_1 = |\psi_1\rangle\langle\psi_1|$ then $F(\rho_1, \rho_2) = \langle\psi_1|\rho_2|\psi_1\rangle$
4. $F(\rho_1, \rho_2)$ is invariant under unitary transformations on the state space.

Many years ago this thesis started out trying to find the minimal entanglement using the Bures distance. Various approaches were tried. The first approached, for a two-qubit pure system, involved solving a system of fifteen equations for fifteen unknowns. For mixed states the number of variables would be four times as large. This was too much for MAPLE to handle, so a different method needed to be tried. Genetic algorithm seemed a good avenue to explore, since the number of variables was so large. To implement this using FORTRAN would have required creating and testing a software library for finding the square root of a matrix, the logarithm of a matrix, and genetic algorithm. MATLAB had the software for finding the square root of a matrix, the logarithm of a matrix, and genetic algorithm in its function set, so MATLAB was used. Appendix A and B has the MATLAB code for the project. A lot of time was used

learning how the genetic algorithm software worked. It has numerous parameters to set, and if they are not set correctly, the results for the calculation will not be correct.

The first the minimal entanglement of a two qubit system was for the Bures distance. In order to do this, we needed a general formulation for the set X (see Figure 1). The general density matrix for a separable two qubit system is

$$\rho_{pure} = \frac{1}{|a|^2 + |b|^2} \frac{1}{|c|^2 + |d|^2} \begin{pmatrix} aa^* & ab^* \\ ba^* & bb^* \end{pmatrix} \otimes \begin{pmatrix} cc^* & cd^* \\ cd^* & dd^* \end{pmatrix}. \quad (5.8)$$

There are eight variables in equation 5.8, plus one for probability; then for a general mixed state, a total of four equations 5.8 were added together, for a total of 36 variables. The genetic algorithm finds sets of 36 variables, and evolves towards the set which maximizes the desired fitness criterion, in this case, closeness to the set of separable states. The 36 variables are for software flexibility. The sum of the probability still must add to one and the density matrix is also normalized. For mixed states, this must be done for n pure states. The Bures distance is not minimized directly; rather the fidelity minimized, then Bures distance is computed. (The reason is that it cuts down on the number of calculations and it found better results.) Some standard density matrices were chosen, with known entanglements, to make sure the software was working correctly. The results are in Table 1. The increment for the theta was an eighth pi. Note that we have chosen to normalize maximum entanglement to one. (The scale is arbitrary; some researchers prefer $\log(2)$ for historical reasons.)

The rows and columns labels for the density matrices used throughout this thesis are

$$\begin{array}{c}
 |11\rangle \quad |10\rangle \quad |01\rangle \quad |00\rangle \\
 \langle 11| \begin{pmatrix} x & x & x & x \\ \langle 10| \begin{pmatrix} x & x & x & x \\ \langle 01| \begin{pmatrix} x & x & x & x \\ \langle 00| \begin{pmatrix} x & x & x & x \end{pmatrix}
 \end{array} \tag{5.9}$$

Table 1

| Density Matrix | Known Entanglement | Calculated Entanglement |
|---|-----------------------|-------------------------|
| $\frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & e^{i\theta} & 0 \\ 0 & e^{-i\theta} & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ <p>EPR</p> | 1 (for all θ) | 1.00 |
| $\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & e^{i\theta} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ e^{-i\theta} & 0 & 0 & 1 \end{pmatrix}$ <p>Bell</p> | 1 (for all θ) | 1.00 |
| $\frac{1}{2} \begin{pmatrix} 1 & e^{i\theta} & 0 & 0 \\ e^{-i\theta} & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ | 0 (for all θ) | 0.00 |
| $\frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ | 0 | 0.00 |

Table 1 (continue)

| Density Matrix | Known Entanglement | Calculated Entanglement |
|---|--------------------|-------------------------|
| $\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ <p>Mixed state</p> | 0 | 0.00 |
| $\frac{1}{4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ <p>Mixed stat</p> | 0 | 0.00 |
| $\frac{1}{3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ <p>Mixed state</p> | 0 | 0.00 |

Chapter 6

Results

In this chapter, the genetic algorithm is used to calculate the entropy of entanglement for large classes of states, using three different distance measures: the Bures distance, the Hilbert – Schmidt distance, and the von Neumann distance. These results are compared to those of two reference methods (not using genetic algorithm). The first of these is the entanglement of formation, which is calculated according to the exact formula for two-qubit systems, equation (3.6). This method is not generalizable to multiple qubits or to qudits. The second is Quantum Neural Network (QNN). This is not an exact calculation of any of the entanglements discussed in Chapter 3; however, it is another method at least potentially generalizable to multiple qubits or to qudits, and (a bonus) doesn't require experimental knowledge of the density matrix.

The genetic algorithm results can be thought of as a ceiling for the entanglement, since these will be the minimum distance found to the set X (See figure 1). It is always possible that there is another matrix in the set X which we did not find, which is closer still to the system's density matrix, and, thus, that the correct value for the entanglement is smaller. So the consistencies of the results are important. The genetic algorithm results should show similar behavior to tested and calculated values. What to look for in the graphed results are:

1. Are the starting and ending points similar?
2. Do results of the known and the genetic algorithm of similar slopes?
3. Do they have zero entanglement about at the same point?

In graphed results, there are five different entanglement calculations shown.

1. Quantum Neural Network (QNN) [41] calculated using different software.

2. Entanglement of formation as calculated according to the exact formula, equation 3.6, of Wootters [22], calculated using different software.
3. The entropy of entanglement, using the Bures distance (equation (5.6)) to the set of separable states, calculated using the genetic algorithm
4. The entropy of entanglement, using the Hilbert – Schmidt distance to the set of separable states, calculated using the genetic algorithm. The Hilbert – Schmidt distance is defined as [52]

$$Hilbert - Schmidt(\rho_1, \rho_2) = \sqrt{Tr \left[(\rho_1 - \rho_2)^2 \right]} \quad (6.1)$$

where ρ_1 and ρ_2 are density matrices.

5. The entropy of entanglement using the von Neumann distance to the set of separable states is calculated using the genetic algorithm. The von Neumann distance is defined as

$$VonNeumann(\rho, \sigma) = \rho \log \frac{\rho}{\sigma} \quad (6.2)$$

where ρ and σ are density matrices [52].

Numbers 3 through 5 are the results of this study. The QNN and Wootters, numbers 1 and 2, are reference values to check how the genetic algorithm program results compare. The Bures, Hilbert-Schmidt, and Von Neumann results use different distance measures in the genetic algorithm program. For mixed states the program allows the necessary four pure states [22, 46] in the summation to define the mixed state. The rest of the genetic algorithm parameters are in appendix A.

Figures 7 – 9 show results for states with white noise. States with white noise are important applications of the method, since as was explained in Chapter 1, any realistic implementation of quantum entanglement applications must deal with the problems of noise.

Figure 4 shows results for of $|00\rangle + |11\rangle + \gamma|01\rangle$. This is a pure state, the Bell triplet, with a varying amount γ of contamination that maintains coherence. The normalized density matrix is

$$\left(\frac{1}{2+\gamma^2} \right) \begin{pmatrix} 1 & 0 & \gamma & 1 \\ 0 & 0 & 0 & 0 \\ \gamma & 0 & \gamma^2 & \gamma \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad (6.3)$$

Figure 4

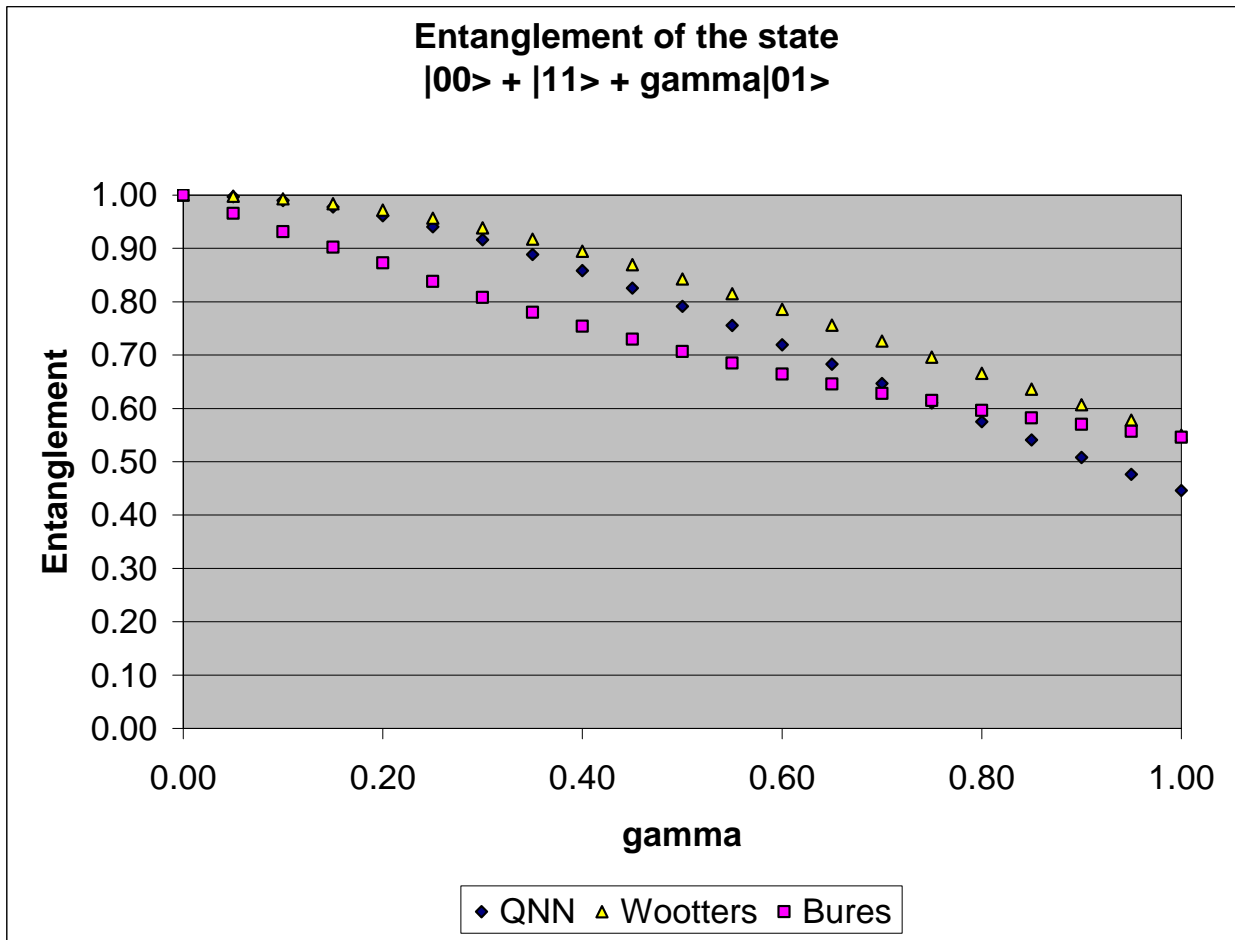


Figure 4 is missing the Von Neumann results because the density matrices turn out to be singular and logarithm calculation did not converge. The Hilbert – Schmidt distance was found to be one for all values of gamma for this state and was therefore left off the graph.

Figure 5 shows results for $M'(\gamma)$, which is a fully entangled state (EPR, triplet $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$) with a varying amount of mixture contamination, that is, a density matrix given by

$$\left(\frac{1}{2+\gamma}\right) \begin{pmatrix} \gamma & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (6.4)$$

Figure 5

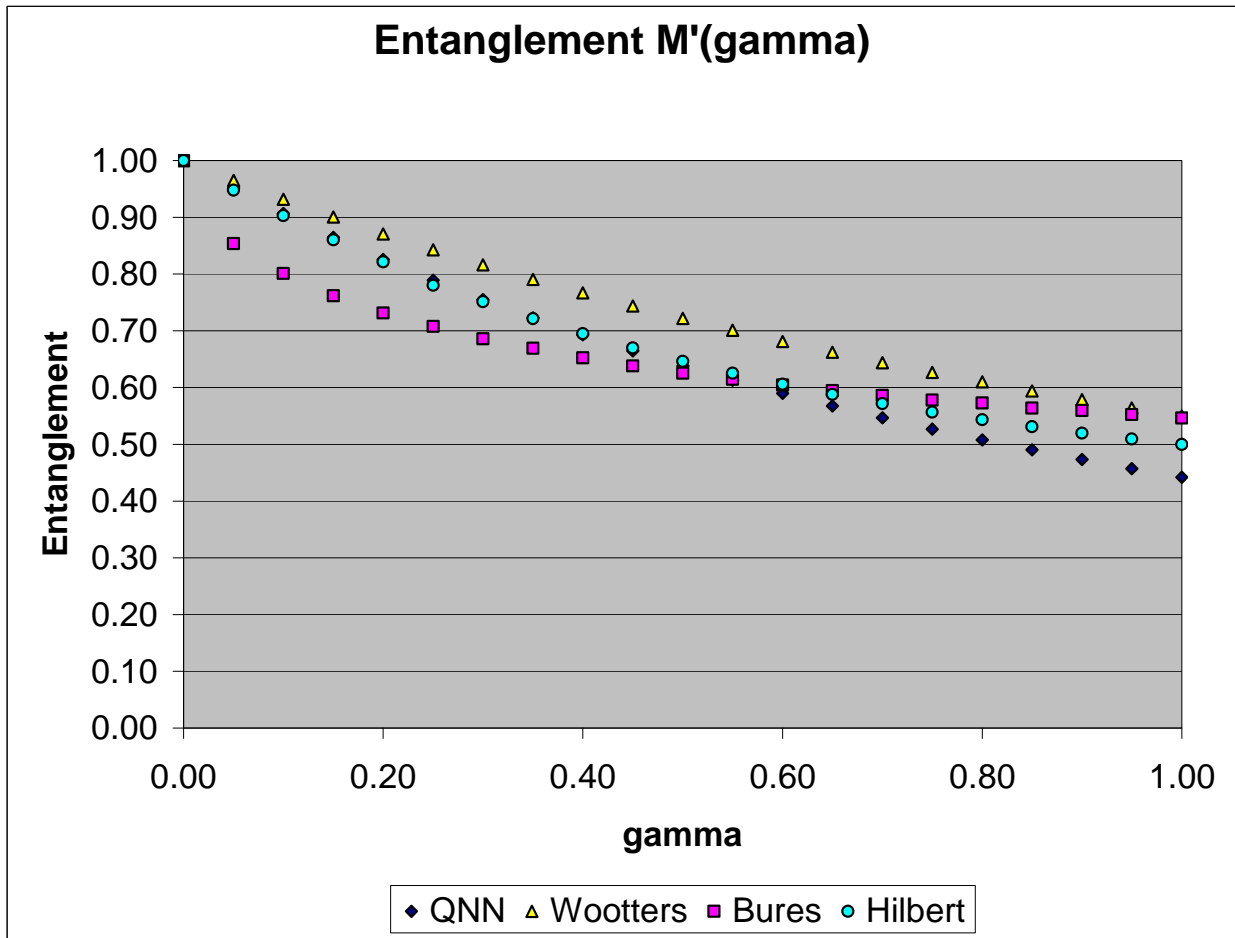


Figure 5 is again missing the Von Neumann results because the density matrices turn out to be singular and logarithm calculation did not converge.

Figure 6 is a calculation of entanglement for the Werner states, which are EPR triplet states with noise. The Werner states are defined as

$$Werner(F) = F|\psi^-\rangle\langle\psi^-| + \left(\frac{1-F}{3}\right)(|\psi^+\rangle\langle\psi^+| + |\varphi^+\rangle\langle\varphi^+| + |\varphi^-\rangle\langle\varphi^-|) \quad (6.5)$$

Where

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle) \quad (6.6)$$

$$|\varphi^\pm\rangle = \frac{1}{\sqrt{2}}(|11\rangle \pm |00\rangle) \quad (6.7)$$

$$|\psi^\pm\rangle\langle\psi^\pm| = \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle)(\langle 10| \pm \langle 01|) \quad (6.8)$$

$$= \frac{1}{2}(|10\rangle\langle 10| + |01\rangle\langle 01| \pm |10\rangle\langle 01| \pm |01\rangle\langle 10|) \quad (6.9)$$

$$= \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (6.10)$$

$$|\varphi^\pm\rangle\langle\varphi^\pm| = \frac{1}{2}(|11\rangle \pm |00\rangle)(\langle 11| \pm \langle 00|) \quad (6.11)$$

$$= \frac{1}{2}(|11\rangle\langle 11| + |00\rangle\langle 00| \pm |11\rangle\langle 00| \pm |00\rangle\langle 11|) \quad (6.12)$$

$$= \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & \pm 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \pm 1 & 0 & 0 & 1 \end{pmatrix} \quad (6.13)$$

$$Werner(F) = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & F & -F & 0 \\ 0 & -F & F & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \frac{1}{2} \left(\frac{1-F}{3} \right) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6.14)$$

$$Werner(F) = F \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0.5 & -0.5 & 0 \\ 0 & -0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \left(\frac{1-F}{3} \right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6.15)$$

Figure 6

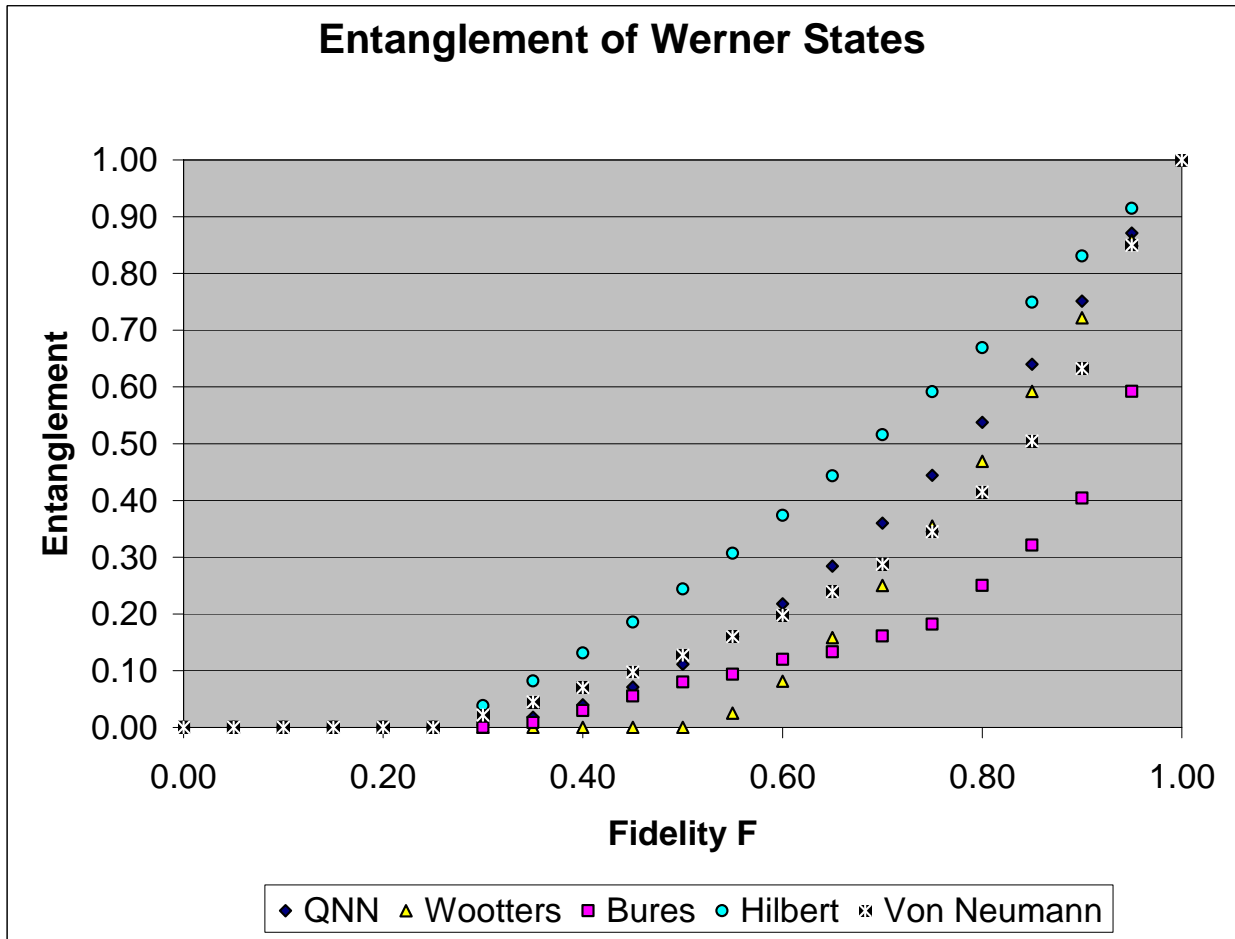


Figure 7 shows the Bell triplet plus white noise.

$$Bell(p) = \frac{p}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} + \frac{(1-p)}{4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6.16)$$

Figure 7

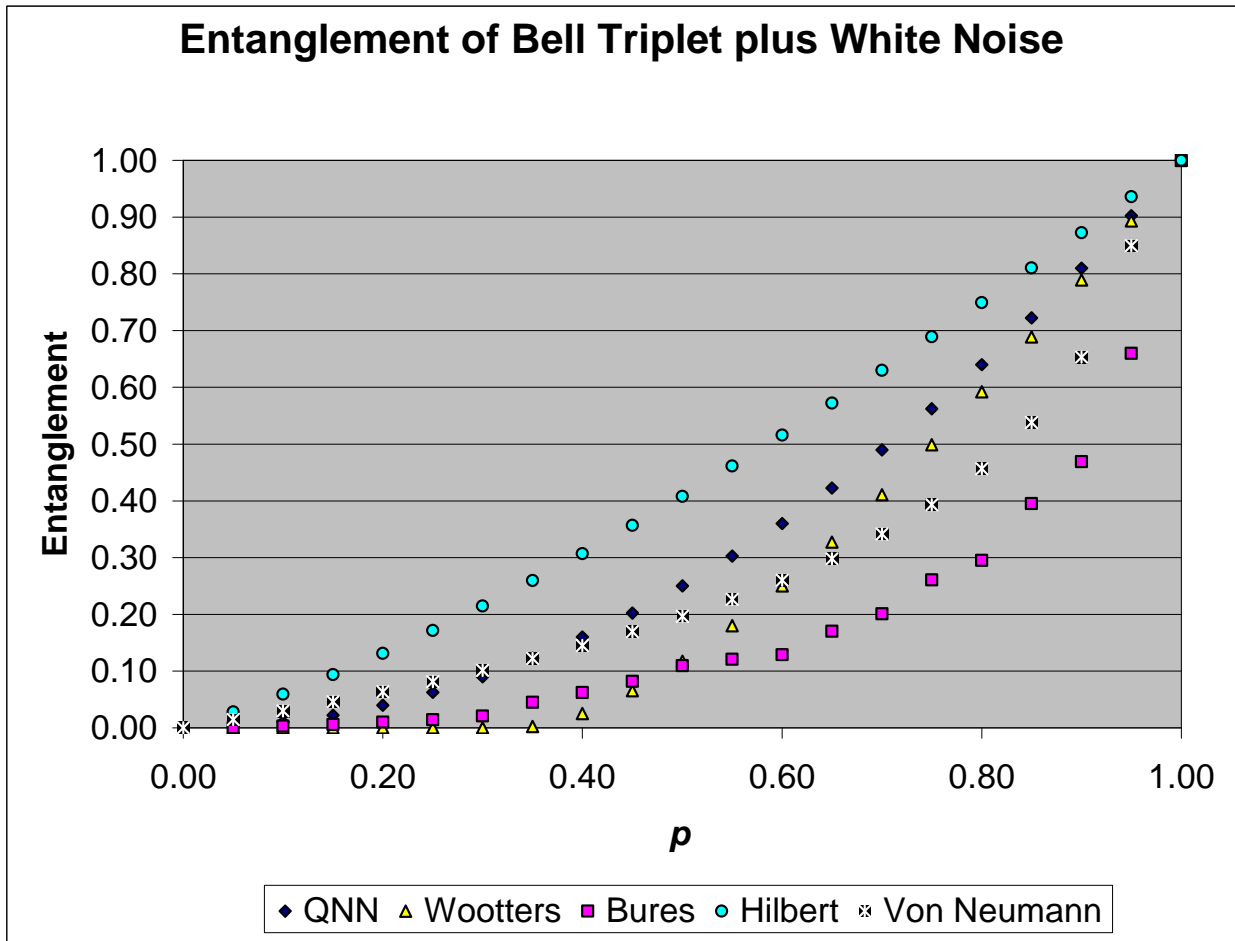


Figure 8 shows results for the EPR triplet state with white noise.

$$EPR(p) = \frac{p}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \frac{(1-p)}{4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (6.17)$$

Figure 8

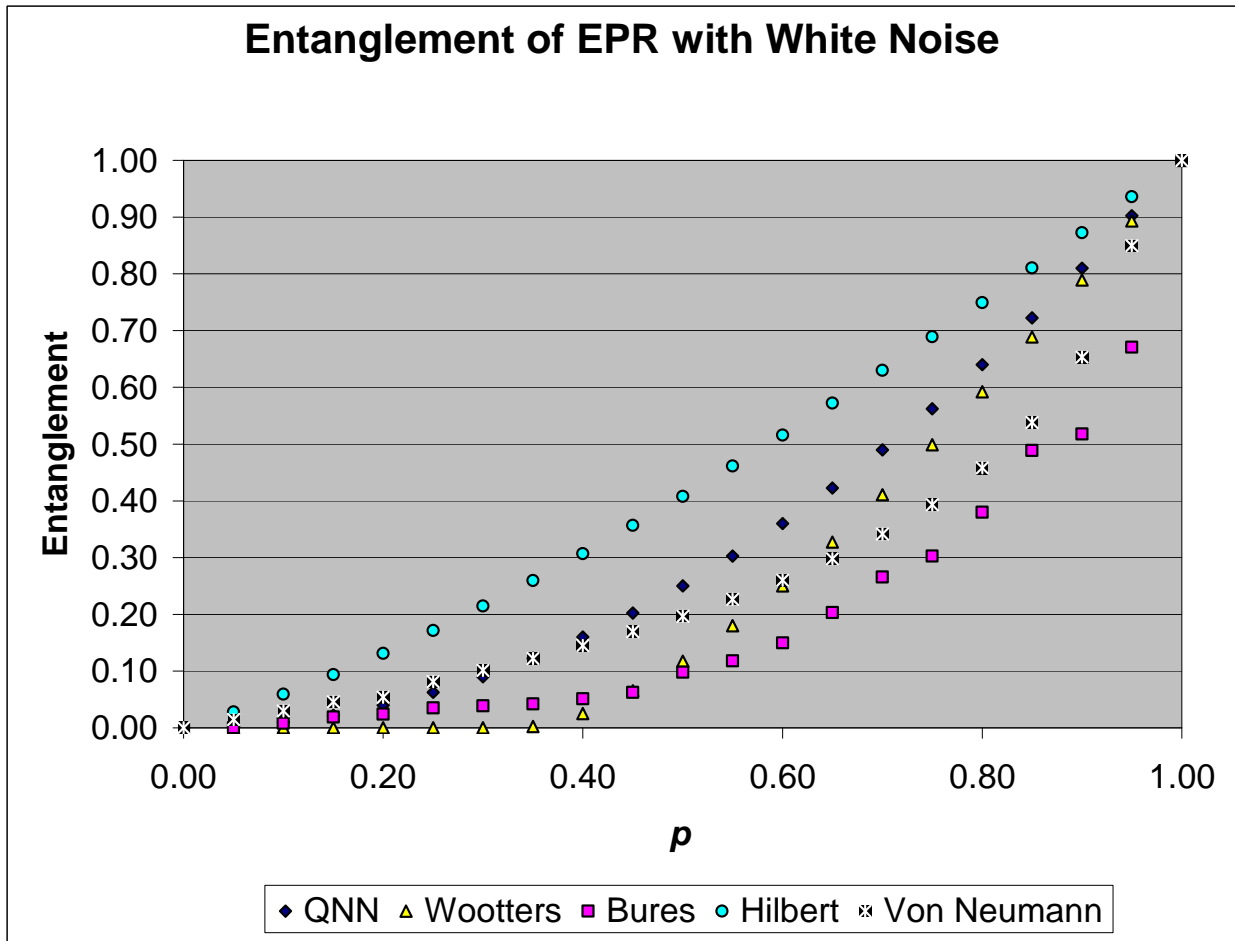
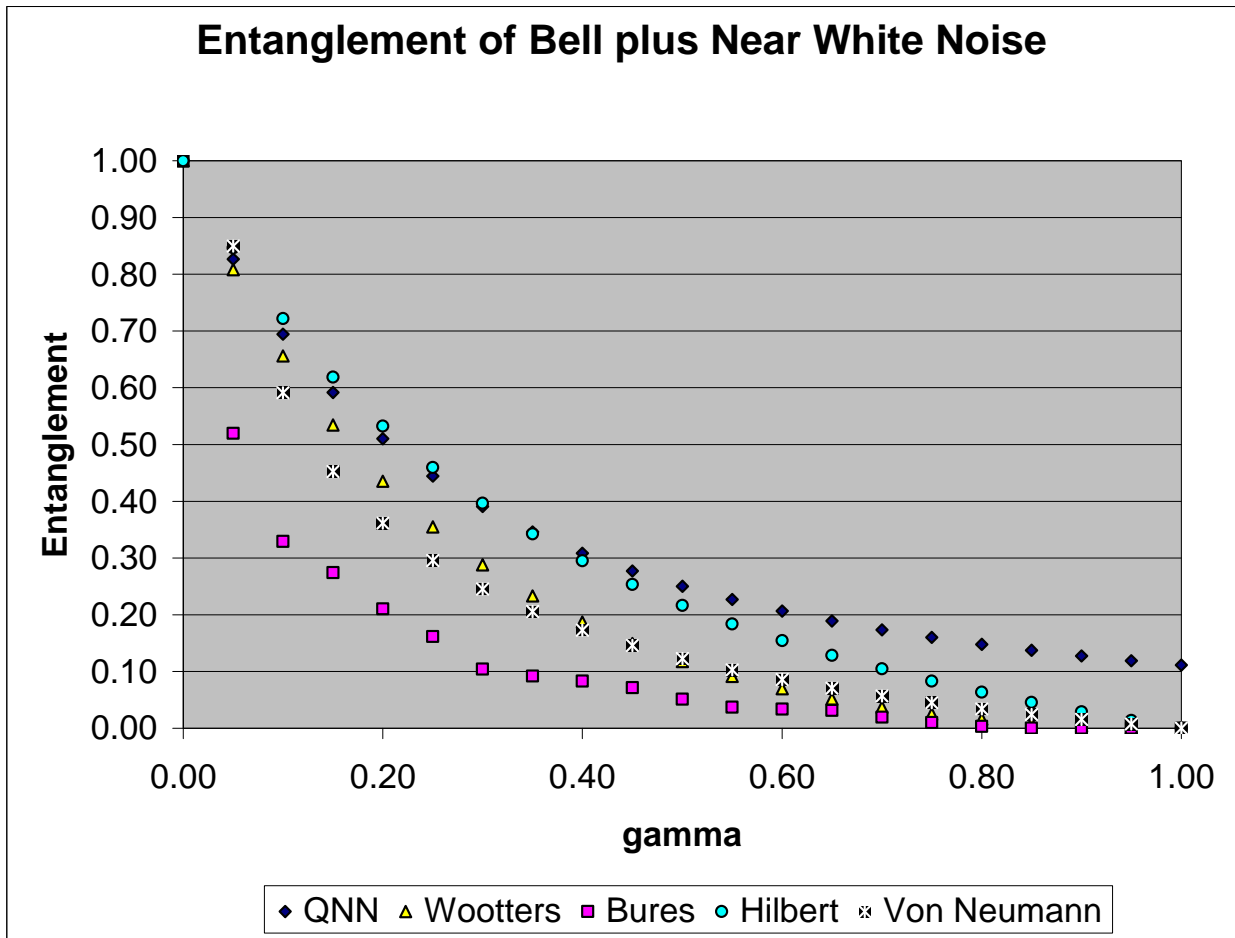


Figure 9 shows the Bell Triplet plus near white noise.

$$Bell(\gamma) = \frac{1}{2+(4\gamma)} \begin{pmatrix} 1+\gamma & 0 & 0 & 1 \\ 0 & \gamma & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 1 & 0 & 0 & 1+\gamma \end{pmatrix} \quad (6.18)$$

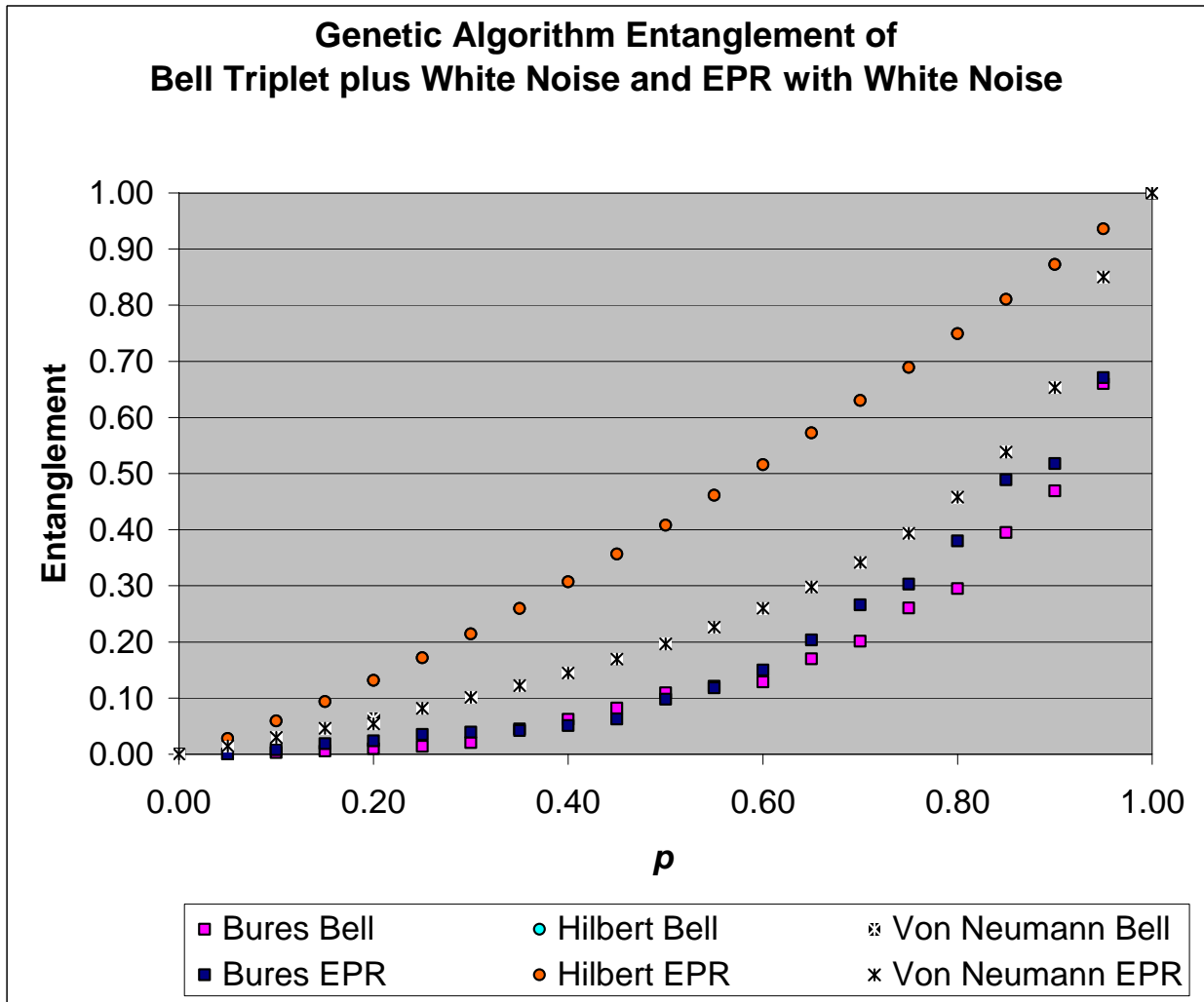
Figure 9



When looking at figures 4 – 9, the general consistencies of the results are achieved. The beginning and ending points are similar. The general slopes of the graphs are consistent with the reference values. The zero entanglement point of figure 6 of the genetic algorithm is the same as the QNN method.

Figure 10 shows the entanglement of the, Bell triplet, $|\phi^+\rangle$, plus white noise and EPR triplet state, $|\psi^+\rangle$, with white noise using the genetic algorithm method. The difference between the Bell triplet and EPR is the definition of the density matrix is rows and columns, that is, by symmetry the expected results would be the same. For the Hilbert – Schmidt and Von Neumann the values are the same. The Bures distance graphs demonstrates the noise problem with that method. It is the least straightforward to calculate of the three, and having different start matrix may affect how the square root results. The size of the discrepancy indicates the size of the expected error.

Figure 10



The results were calculated using MATLAB R2006b Version 7.3.0.267 with Genetic Algorithm and Direct Search Toolbox 2.1 in Microsoft Windows XP Professional Version 2002 Service Pack 2 on Intel Core2 CPU 6600 @2.4GHz with 2.00 GB of RAM. Typical runs take about two hours to produce each line on the graph.

Chapter 7

Discussion and Future Work

When looking at Figures 4 – 9 of the genetic algorithm results, we can see that the Bures distance is always the lowest, Von Neumann in the middle, and the Hilbert-Schmidt the highest. The genetic algorithm results can be thought of as a ceiling for the entanglement, since these will be the minimum distance found to the set X . It is always possible that there is another matrix in the set X which we did not find, which is closer still to the system's density matrix, and, thus, that the correct value for the entanglement is smaller. However, the fact that the Bures numbers are always the lowest, then the von Neumann, then the Hilbert – Schmidt, gives us some confidence that the method is getting good minimization, since if we were not, the rankings would be arbitrary and probably not consistent. As it is, the rankings can be ascribed to the differences among the distance measures. It is also good to see that for each of the Figures 4 – 9, the curves generally have the same shape. The Bures distance has a bit more noise, but there are multiple square roots of matrices involved, so one would expect more problems with these calculations.

The Wootters numbers (equation 3.6) are an exact calculation of the entanglement of formation. Of course, this formula will only work for a two-qubit system. For a multiple qubit system, calculating the entanglement of formation is very difficult. Note that this is not the same function that we are calculating, which is the entropy of entanglement (see Chapter 3.) The entropy of entanglement, which we calculate with the genetic algorithm, is at least straightforward to generalize to any number of qubit (or qudits.)

In the QNN [41] method, developed by our group over the past five years, the system learns to compute its own degree of entanglement by comparing its output with the desired results for a given training set of known input – output pairs, then adjusting its parameters

systematically till its output matches the desired ones. The numbers given in Figures 4 – 9 are results of a system trained on a set of four (the Bell triplet, two pure product states, and the state $|00\rangle + |11\rangle + |01\rangle$.) (Note: As figures 4-9 show, the QNN does a pretty good job of reproducing the entanglement of formation for large classes of two – qubit states.) Like the genetic algorithm method developed in this thesis, the QNN is straightforwardly generalizeable to multiple qubits or qudits, or, at least, so it might appear. However, so far we have not been successful in extending it even to a three – qubit system.

The major advantage of using our method, a genetic algorithm to find the minimum entanglement, is that it is very easy to change what you are minimizing. The genetic algorithm does not care about the complexity of the system; if it can calculate the results it will find a minimum. The theorem [46] for the minimum number of pure states necessary to represent a mixed state was also tested. A series of runs of between one and four pure states was done, and after four, runs of increments of two. The program was set up to run using 16 pure states, or 144 total variables. It took awhile, but it worked fine. There was no difference between the four and the 16 pure states results.

The major disadvantage of using a genetic algorithm method is that, since it is a random process, it does take a long time processing. Sometimes with a complicated equation, the genetic algorithm method can get stuck in a local minimum, instead of the global minimum desired. Multiple attempts may have to be tried until the global minimum is found.

There are a number of items that could be done next. So far, entropy of entanglement has been tried, but other entanglement calculation described in Chapter 3 could also be tested. Most of these require an extremum calculation for which could be use our genetic algorithm procedure. Also, three or greater qubit systems could be tried. The same procedure can easily be

used with minor modifications. Extension to qudit systems is also easy to see how to do. A graphic user interface could be added to software. This would make it be easier for the user to operator the software and this way it could compiled and run much faster.

REFERENCES

List of References

- [1] Einstein, A., Podolsky, B. and Rosen, N., “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” *Physical Review*, Vol. 47, May 1935, pp 777-780.
- [2] E. Schrodinger, E., “Discussion Of Probability Relations Between Separated Systems,” *Proceedings of the Cambridge Philosophical Society*, Vol. 31, 1935, pp 555-563
- [3] Clauser, J.F, Horne, J.F., Shimony, A., and Holt, R.A., “Proposed Experiment To Test Local Hidden-Variable Theories,” *Physical Review Letters*, Vol. 23, No. 15 October 1969 pp 880-884.
- [4] Clauser, J.F. and Horne, M.A. “Experimental Consequences Of Objective Local Theories,” *Physical Review D*, Vol. 10, No. 2, July 1974 pp526-535.
- [5] Freedman, S.J. and Clauser, J.F., “Experimental Test Of Local Hidden-Variable Theories,” *Physical Review Letters*, Vol. 28, No. 14, April 1972, pp 938-941.
- [6] Nielsen, M., and Chuang, I., “*Quantum Computation and Quantum Information*,” Cambridge University Press, New York, NY, 2000
- [7] Ekert, A., “Quantum Cryptography Based On Bell’s Theorem,” *Physical Review Letters*, Vol. 67 No.6, August 1991, pp 661-663
- [8] Bennett, C.H and Wiesner, S.J., “Communication Via One- And Two-Particle Operators On Einstein-Podolsky-Rosen States,” *Physical Review Letters*, Vol. 69, No. 20, November 1992, pp 2881-2884.
- [9] Bennett, C., Brassard, C., Crepeau, C., Jozsa, R., Peres, A. and Wootters, W.K., “Teleporting An Unknown Quantum State Via Dual Classical And Einstein-Podolsky-Rosen Channels,” *Physical Review Letters*, Vol. 70, No. 13, March 1993, pp 1895-1899.
- [10] Shor P., “Algorithms For Quantum Computation: Discrete Logarithms And Factoring,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, IEEE Computer Society Press, 1994, pp.124-134.
- [11] Steane, A., “Quantum Computing,” *Reports on Progress in Physics*, Vol. 61, No. 2, February 1998, pp 117-173.
- [12] Shor, P., “Dipole Polarizabilities And Hyperpolarizabilities Of Excited Valence States Of Be,” *Physical Review A*, Vol. 52, No. 3, September 1995, pp 2439-2441.

- [13] Steane, A., "Error Correcting Codes in Quantum Theory," *Physical Review Letters*, Vol. 77, No. 5, July 1996 pp 793 - 797.
- [14] Horodecki, P., and Horodecki, R., "Distillation And Bound Entanglement," *Quantum Information and Computation*, Vol. 1, No. 1 June 5, 2001 pp 45-75.
- [15] Thaller, B., *Advanced Visual Quantum Mechanics*, Springer, New York, NY, 2005
- [16] Vedral, V, and Plenio, M.B., "Entanglement Measures And Purification Procedures," *Physical Review A*, Vol 57, No. 3, March 1998, pp. 1619 – 1633.
- [17] Bennett, C.H., Bernstein, H., Popescu S., and Schumacher, B., "Concentrating Partial Entanglement By Local Operations," *Physical Review A*, Vol. 53, No. 4 April 1996, pp. 2046-2052
- [18] Rains, E. M. "Rigorous Treatment Of Distillable Entanglement," *Physical Review A*, Vol. 60, No. 1, July 1999, pp. 173 – 178
- [19] Rains, E. M. "Bound On Distillable Entanglement," *Physical Review A*, Vol. 60, No. 1, July 1999, pp. 179 – 184
- [20] Hayden, P. M., Horodecki, M., and Terhal, B. M., "The Asymptotic Entanglement Cost Of Preparing A Quantum State," *Journal of Physics A*, Vol. 34, No. 35 September 2001, pp. 6891 - 6898
- [21] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K., "Mixed-State Entanglement And Quantum Error Correction," *Physical Review A*, Vol. 54 No. 5, November 1996, pp 3824 – 3851
- [22] Wootters, W.K. "Entanglement of Formation of an Arbitrary State of Two Qubits," *Physical Review Letters*, Vol. 80 No. 10, March 1998, pp 2245 – 2248
- [23] Wootters W.K., "Entanglement of Formation and Concurrence", *Quantum Information and Computation*, Vol. 1, No. 1, 2001, pp 27-44
- [24] Vedral, V., Plenio, M. B., Rippl, M. A., and Knight, P. L., "Quantifying Entanglement," *Physical Review Letters*, Vol. 78, No. 12, March 1997, pp 2275 - 2279
- [25] Vedral, V., Plenio, M. B., Jacobs, K., and Knight, P. L., "Statistical Inference, Distinguishability of Quantum States, and Quantum Entanglement," *Physical Review A*, Vol. 53 No. 6, December 1997, pp 4452 – 4455
- [26] Christandl, M. and Winter, A., "'Squashed Entanglement': An additive entanglement measure," *Journal of Mathematical Physics*, Vol .45, No. 3, March 2004, pp. 829-840

- [27] Al-Rabadi, A., Casperson, L., and Perkowski, M., "Multiple-Valued Quantum Logic," *Quantum Computers and Computing*, Moscow State University and Russian Academy of Sciences, Institute of Computer Science, Russia, Vol. 3, No. 1, 2002, pp. 63-91.
- [28] Muthukrishnan, A. and Stroud, Jr., C.R., "Multivalued Logic Gates For Quantum Computation," *Physical Review A*, Vol. 62, No. 5, October 2000, 052309, 8 pages.
- [29] [URL] http://en.wikipedia.org/wiki/Quantum_operation [cited 14 April 2007]
- [30] Plenio, M.B. and Virmani, S., "An Introduction To Entanglement Measures" *Quantum Information and Computation*, Vol. 7, No. 1, 2007, pp 001 – 051
- [31] Horodecki, M., and Horodecki, R., "Entanglement Measures," *Quantum Information and Computation*, Vol. 1, No. 1 June 5, 2001 pp 3 – 26.
- [32] Audenaert, K., Verstraete, F., and De Moor, B., "Variational Characterizations Of Separability And Entanglement Of Formation," *Physical Review A*, Vol. 64 No. 5, October 2001, 052304 13 pages.
- [33] Vollbrecht, K. G. H. and Werner, R. F. "Entanglement Measures Under Symmetry," *Physical Review A*, Vol. 64 No. 6, November 2001, 062307, 15 pages
- [34] Eisert, J., Felbinger, T., Papadopoulos, P. Plenio, M. B., and Wilkens, M., "Classical Information and Distillable Entanglement," *Physical Review Letters*, Vol. 84, No. 4, February 2000, pp 1611 – 1614
- [35] Terhal, B. M. and Vollbrecht, K. G. H., "Entanglement of Formation for Isotropic States," *Physical Review Letters*, Vol. 85, No. 12, September 2000, pp 2625 – 2628
- [36] Vidal, G., "Entanglement Monotones," *Journal of Modern Optics*, Vol. 47, No. 2 & 3, February 2000, pp 355 – 376
- [37] Vedral, V., Plenio, M. B., Jacobs, K., and Knight, P. L., "Statistical Inference, Distinguishability Of Quantum States, And Quantum Entanglement," *Physical Review A*, Vol. 56 No. 6, December 1997, pp 4452 – 4455
- [38] Plenio, M. B., Virmani, S. and Papadopoulos, P., "Operator Monotones, The Reduction Criterion And The Relative Entropy," *Journal of Physics A: Mathematical and General*, Vol. 33, No. 22, June 9, 2000, pp L193 – L197
- [39] Horodecki, M., Horodecki, P., Horodecki, R., Oppenheim, J., Sen(De), A., Sen, U., and Synak-Radtke, B., "Local Versus Nonlocal Information In Quantum-Information Theory: Formalism And Phenomena," *Physical Review A*, Vol. 71, June 9, 2005, 062307, 25 pages

- [40] Plenio, M.B., and Vedral, V., “Bounds On Relative Entropy Of Entanglement For Multi-Party Systems,” *Journal of Physics A: Mathematical and General*, Vol. 34 No. 35, September 7, 2001, pp 6997 – 7002
- [41] Behrman, E.C., Steck, J.E., Gagnebin, K.A., Walsh, K.A, and Skinner, S.R., “Quantum Algorithm Design Using Dynamic Learning”, *Quantum Information and Computation*, to appear 2007.
- [42] Tóth, G., and Gühne, O. “Detecting Genuine Multipartite Entanglement with Two Local Measurements,” *Physical Review Letters*, Vol. 94, No. 6 February 17, 2005, 060501
- [43] *MATLAB Genetic Algorithm and Direct Search Toolbox 2 User’s Guide*, The MathWorks, Inc., Natick, MA, 2007
- [44] [URL] <http://www.genetic-programming.com/> [cited 14 April 2007]
- [45] Uhlmann, A., “Entropy And Optimal Decompositions Of States Relative To A Maximal Commutative Subalgebra,” arXiv:quant-ph/9704017v2
- [46] Sanpera1, A., Tarrach, R., and Vidal, G., “Local Description Of Quantum Inseparability,” *Physical Review A*, Vol. 58, No. 2, August 1998, pp 826 – 830
- [47] DiVincenzo, D. P. Terhal, B. M., and Thapliyal, A. V., “Optimal Decompositions of Barely Separable States,” arXiv:quant-ph/9904005
- [48] Lockhart, R.B., “Optimal Ensemble Length of Mixed Separable States,” arXiv:quant-ph/9908050
- [49] Bures, D. “An Extension of Kakutani's Theorem on Infinite Product Measures to the Tensor Product of Semifinite $w *$ -Algebras ,” *Transactions of the American Mathematical Society*, Vol. 135, January 1969, pp 199 – 212
- [50] Uhlmann, A., “The “Transition Probability” In The State Space Of A $*$ -Algebra,” *Reports on Mathematical Physics*, Vol. 9, No 2, April 1976, pp 273 – 279
- [51] Jozsa, R., “Fidelity for Mixed Quantum States”, *Journal of Modern Optics*, Vol. 41, No. 12, December 1994 , pp 2315 – 2323
- [52] Sommers, H., and Zyczkowsk, K., “Bures Volume Of The Set Of Mixed Quantum States”, *Physical Review A*, Vol. 36, No. 39, October 2003, 10083–10100

APPENDICES

APPENDIX A

Program Listing for genflex.m a MATLAB program

```
%genflex.m
%
filename = 'hbn4413.wk1';
states = 4;
tvars = states*9;
% for loog vars
start = 1.00;
inc = -0.05;
finish = 0.00;
nogaloops = 3;
%
%method = 'fidelity';
method = 'hilbert';
%method = 'neumann';
%
%fitcurve = 'test2';
%fitcurve = 'werner';
%fitcurve = 'bell triplet noise';
fitcurve = 'bell with near noise';
%fitcurve = 'EPR with white noise';
%fitcurve = 'ident';
%
warning off all
%
options = gaoptimset;
options = gaoptimset(options,'PopulationType', 'doubleVector');
options = gaoptimset(options,'PopInitRange', [0;0]);
options = gaoptimset(options,'PopulationSize',50);
options = gaoptimset(options,'EliteCount', 4);
options = gaoptimset(options,'CrossoverFraction', 0.5000);
options = gaoptimset(options,'MigrationDirection', 'both');
options = gaoptimset(options,'MigrationInterval', 50);
options = gaoptimset(options,'MigrationFraction', 0.5000);
options = gaoptimset(options,'Generations', 5000);
options = gaoptimset(options,'TimeLimit', Inf);
options = gaoptimset(options,'FitnessLimit', -Inf);
options = gaoptimset(options,'StallGenLimit', 1000);
options = gaoptimset(options,'StallTimeLimit', 5000);
options = gaoptimset(options,'TolFun', 1.0000e-008);
options = gaoptimset(options,'TolCon', 1.0000e-008);
options = gaoptimset(options,'InitialPopulation', []);
```

```

options = gaoptimset(options,'InitialScores', []);
options = gaoptimset(options,'InitialPenalty', 50);
options = gaoptimset(options,'PenaltyFactor', 100);
options = gaoptimset(options,'PlotInterval', 1);
options = gaoptimset(options,'CreationFcn', @gacreationuniform);
options = gaoptimset(options,'FitnessScalingFcn', @fitscalingrank);
options = gaoptimset(options,'SelectionFcn', @selectionstochunif);
%cf = [@crossoverheuristic; 2]
options = gaoptimset(options,'CrossoverFcn', @crossoverheuristic);
options = gaoptimset(options,'MutationFcn', @mutationadaptfeasible);
% options = gaoptimset(options,'HybridFcn', @patternsearch );
options = gaoptimset(options,'HybridFcn', [] );
options = gaoptimset(options,'Display', 'off');
options = gaoptimset(options,'PlotFcns', []);
% options = gaoptimset(options,'PlotFcns', [@gaplotbestf]);
options = gaoptimset(options,'OutputFcns', []);
options = gaoptimset(options,'Vectorized', 'off');
%
LB = zeros( 1 , tvars );
UB = zeros( 1 , tvars );
for i = 1 : 1: states
    LB( ( (i-1)*9 )+ 1) = 0;
    UB( ( (i-1)*9 )+ 1) = 1;
    for ii = 2:1:9
        LB( ( (i-1)*9 )+ ii ) = -1;
        UB( ( (i-1)*9 )+ ii ) = 1;
    end;
end;
%
record= [];
xrec=[];
%
%
%
%for index1 = 0.05:0.050:0.95;
%for index = 1.00:-0.05:0.00;
for index = start:inc:finish
    %
    fvalmax = 10.0;
    xkeep = zeros( 1, tvars);
%
    for index2=1:1:nogaloops;
        gafun = @(x) gafunfit(x, states, index, method, fitcurve);
        [x fval reason output population scores]=ga(gafun, tvars,[],[],[],[],LB,UB,[],options);
        %
        if ( fval < fvalmax )

```

```

        fvalmax = fval;
        xkeep = x;
    end
%
% disp( [index2 index index1 fval])
disp( [index2 index fval])
%
end
if ( fval < fvalmax )
    fvalmax = fval;
    xkeep = x;
end
%
record = [record; index fvalmax];
xrec = [xrec; index xkeep];
%
% record = [record; index1 index fvalmax];
% disp( [index fvalmax xkeep])
end
%end
wk1write(filename,record);
%
```


APPENDIX B

Program Listing for ganfunfit.m a MATLAB program

```

function z = gafunfit( x, states, inpar, method, fitcurve )
%
p = zeros( 1 , states );
a = zeros( 1 , states );
b = zeros( 1 , states );
c = zeros( 1 , states );
d = zeros( 1 , states );
%
RHOT = zeros( 4 , 4 );
%
fail = 0;
for i = 1 : 1: states
    p(i) = x( ( i-1)*9 )+ 1);
    a(i) = complex( x( ( i-1)*9 )+ 2), x( ( i-1)*9 )+ 3 );
    b(i) = complex( x( ( i-1)*9 )+ 4), x( ( i-1)*9 )+ 5 );
    c(i) = complex( x( ( i-1)*9 )+ 6), x( ( i-1)*9 )+ 7 );
    d(i) = complex( x( ( i-1)*9 )+ 8), x( ( i-1)*9 )+ 9 );
    if ( ( ( abs(a(i))^2 + abs(b(i))^2 ) * ( abs(c(i))^2 + abs(d(i))^2 ) ) == 0 )
        fail = 1;
    end
end;
%
pt = 0.0;
for i = 1 : 1: states
    pt = pt + p(i);
end;
%
if ( ( pt ~= 0.0 ) && ( fail == 0 ) )
    for i = 1 : 1: states
        %
        A = [a(i)*conj(a(i)) a(i)*conj(b(i)); b(i)*conj(a(i)) b(i)*conj(b(i))];
        B = [c(i)*conj(c(i)) c(i)*conj(d(i)); d(i)*conj(c(i)) d(i)*conj(d(i))];
        %
        R = kron(A,B);
        %
        %if ( ( a(i) ~= 0 && b(i) ~= 0 ) || ( c(i) ~= 0 && d(i) ~= 0 ) )
        RH = R / ( ( abs(a(i))^2 + abs(b(i))^2 ) * ( abs(c(i))^2 + abs(d(i))^2 ) );
        %else
        % RH = R * 0.0;
        %end
        %
        np = p(i)/pt;
    end
end

```

```

%
RHOT = RHOT + np*RH ;
end;
%
RT = trace (RHOT);
RHO = RHOT / RT;
%
switch fitcurve
case 'werner'
    F=inpar;
    K1 = [ 0.0 0.0 0.0 0.0; 0.0 0.5 -0.5 0.0; 0.0 -0.5 0.5 0.0 ; 0.0 0.0 0.0 0.0 ];
    K2 = [ 1.0 0.0 0.0 0.0; 0.0 0.5 0.5 0.0; 0.0 0.5 0.5 0.0 ; 0.0 0.0 0.0 1.0 ];
    K = (F*K1) + ((1.0-F)/3.0)*K2;
case 'bell triplet noise'
    pp = inpar;
    K1 = [ 1.0 0.0 0.0 1.0; 0.0 0.0 0.0 0.0; 0.0 0.0 0.0 0.0 ; 1.0 0.0 0.0 1.0 ];
    K2 = [ 1.0 0.0 0.0 0.0; 0.0 1.0 0.0 0.0; 0.0 0.0 1.0 0.0 ; 0.0 0.0 0.0 1.0 ];
    K = pp*0.5*K1 + ( 1.0-pp)*0.25*K2;
case 'bell with near noise'
    G = inpar;
    K2 = [ 1.0+G 0.0 0.0 1.0; 0.0 G 0.0 0.0; 0.0 0.0 G 0.0 ; 1.0 0.0 0.0 1.0+G ];
    K = ( 1.0/(2.0+4.0*G))*K2;
case 'EPR with white noise'
    pp = inpar;
    K1 = [ 0.0 0.0 0.0 0.0; 0.0 1.0 1.0 0.0; 0.0 1.0 1.0 0.0 ; 0.0 0.0 0.0 0.0 ];
    K2 = [ 1.0 0.0 0.0 0.0; 0.0 1.0 0.0 0.0; 0.0 0.0 1.0 0.0 ; 0.0 0.0 0.0 1.0 ];
    K = pp*0.5*K1 + ( 1.0-pp)*0.25*K2;
case 'test1'
    F=inpar;
    K1 = [ 0.0 0.0 0.0 0.0; 0.0 0.5 -0.5 0.0; 0.0 -0.5 0.5 0.0 ; 0.0 0.0 0.0 0.0 ];
    K = (F*K1);
case 'test2'
    F=inpar;
    K2 = [ 1.0 0.0 0.0 0.0; 0.0 0.5 0.5 0.0; 0.0 0.5 0.5 0.0 ; 0.0 0.0 0.0 1.0 ];
    K = ((1.0-F)/3.0)*K2;
case 'ident'
    K = [ 1.0 0.0 0.0 0.0; 0.0 1.0 0.0 0.0; 0.0 0.0 1.0 0.0 ; 0.0 0.0 0.0 1.0 ];
otherwise
    K = [ 1.0 0.0 0.0 0.0; 0.0 1.0 0.0 0.0; 0.0 0.0 1.0 0.0 ; 0.0 0.0 0.0 1.0 ];
end
% end switch fitcurve
%
T = trace (K);
S = K / T;
%
%
```

```

switch method
case 'fidelity'
    try
        SQR = sqrtm(RHO);
    %
        x = SQR * S * SQR;
        SRQx = sqrtm(x);
        tr = trace ( SRQx );
        z = -real (tr);
    catch
        %disp ( 'matrix error' );
        z = 14;
    end;
%
case 'hilbert'
    diff = RHO - S;
    diff2 = diff*diff;
    tr = trace ( diff2 );
    z = -real (sqrt(tr));
%
case 'neumann'
    y = RHO/S;
    try
        ly = logm(y);
        yr = RHOT * ly;
        tr = trace( yr );
        z = -real (tr);
    catch
        z = 14;
        %disp('no logm');
    end;
%
otherwise
    z = 16;
end
% end switch method
else
    z = 15;
end

```