The Power of Entanglement

Anthony Sudbery
Department of Mathematics, University of York
Heslington, York, U.K. YO10 5DD
email: as2@york.ac.uk

4 January, 2006

Plenary lecture at the Fourth International Symposium on Quantum Theory and Symmetries, Varna, Bulgaria, 16 August 2005.

Published in *Quantum Theory and Symmetries*, ed. V.K.Dobrev (Heron Press, Sofia 2006) pp.10–21.

Introduction

The notion of entanglement was introduced in discussions of the foundations of quantum mechanics, but in recent years it has been realised that it can have great practical power. The first part of this talk is a review of the concept of entanglement and some of its potential practical applications. In the second part I will describe recent joint work (with Lieven Clarisse, Simone Severini and Sibasish Ghosh) [7] on the power of quantum operations to generate entanglement.

Part I: Powerful Entanglement

Entanglement is Schrödinger's term for the physical consequences of the mathematical fact that the the tensor product $V_A \otimes V_B$ of two vector spaces V_A and V_B is larger than their Cartesian product $V_A \times V_B$, and the same is true of the corresponding projective spaces. Not every element of the tensor product can be factorised as $\mathbf{v}_A \otimes \mathbf{v}_B$ with $\mathbf{v}_X \in V_X$. The physical interest lies in taking V_A and V_B to be the state spaces of quantum objects A and B. A pure state $|\Psi\rangle \in V_A \otimes V_B$ of the combined system is *separable* if it can be factorised as $|\Psi\rangle = |\psi_A\rangle|\psi_B\rangle$. By the principle of superposition there are also

states of the form $a|\phi_A\rangle|\phi_B\rangle + b|\psi_A\rangle|\psi_B\rangle$, which in general are not separable. When the combined system is in such a state the individual objects cannot be assigned independent pure states, and are said to be *entangled* with each other.

A familiar example of an entangled state is the singlet state

$$|\Psi\rangle = \tfrac{1}{\sqrt{2}}\big(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\big)$$

of two (distinguishable) spin-$\frac{1}{2}$ particles. In a singlet each individual particle has no definite direction of spin; the state of the particle A is the mixed state

$$\rho_A = \mathrm{tr}_B\,|\Psi\rangle\langle\Psi| = \tfrac{1}{2}(|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow|) \tag{1}$$

representing total ignorance of the spin state.

Entanglement and locality

Einstein argued that spatially separated objects must have separate descriptions; the quantum-mechanical description of objects in an entangled state must therefore be incomplete. This is the content of the famous paper by Einstein, Podolsky and Rosen [8], which brought out the fundamental nature of entanglement (indeed, Schrödinger introduced the term in the course of a commentary on the EPR paper [17]). The EPR argument is that in the state (1), a measurement of s_z for one of the particles reveals the value of s_z for the other particle; if the particles are separated, this, by a principle of *locality* which was axiomatic for Einstein, implies that the value of s_z for the second particle must already exist. Such a value is not contained in the quantum-mechanical state, which must therefore be completed by some "hidden variables". Thus

$$\text{entanglement} \;+\; \text{locality} \quad\Longrightarrow\quad \text{hidden variables.} \tag{2}$$

On the other hand, John Bell, looking more thoroughly at the measurements that can be made on two particles in an entangled state, showed that the predictions of quantum mechanics were incompatible with the existence of such hidden variables [1]. He considered the possible results of spin measurements in two different directions for each particle. Let $P_{ij}(a,b)$ be the probability that if the spin of A is measured in direction i and the spin of B is measured in direction j, then the results are a and b respectively. If the particles have independent states, as required by the EPR argument, then, even if the underlying theory is indeterministic, the probabilities must factorise as

$$P_{ij}(a,b) = Q_i(a)R_j(b).$$

Even if we don't know what the individual states are, there will be a distribution over various possibilities and the joint probabilities will be of the form

$$P_{ij}(a_i, b_j) = \sum_\lambda p(\lambda) Q_i^{(\lambda)}(a_i) R_j^{(\lambda)}(b_j). \tag{3}$$

Bell showed that in the singlet state there are measurements for which the probabilities predicted by quantum mechanics cannot be written in this form. Later, Gisin showed that this is true in any entangled state [12]. Thus

$$\text{Entanglement} \quad \Longrightarrow \quad \text{nonlocality.}$$

There is a useful geometrical representation of Bell's proof [15, 16]. The sixteen probabilities $P_{ij}(a, b)$ can be taken as coordinates of a vector in $\mathbb{R}^{16}$. *Bell's inequalities* are the conditions for this vector to lie in the convex hull of the vectors of the form $P_{ij}(a, b) = Q_i(a) R_j(b)$, which is a polytope whose vertices are obtained by taking the functions Q_i and R_j to be $(0, 1)$ functions. Points inside this polytope satisfy inequalities which become equations on the faces of the polytope; the Bell inequalities are therefore linear in $P_{ij}(a, b)$. This condition on the probabilities is equivalent [11] to the statement that the four two-variable probability distributions P_{ij} are marginals of a four-variable distribution $P(a_1, a_2, b_1, b_2)$ (for example,

$$P_{12}(a, b) = \sum_{a_2, b_1} P(a, a_2, b_1, b)).$$

This is an example of a problem in probability theory; given probability distributions on subsets of a set of binary variables, what are the conditions for them to be the marginals of distribution on the full set of variables? The general case appears to be open. Other particular cases, and some examples of the corresponding problem for quantum states of a set of qubits, are studied in [6].

Entanglement killed the cat

The concept of entanglement can be used to solve a notorious problem in the interpretation of quantum mechanics which was graphically illustrated in the same paper by Schrödinger [17]. This is the problem of Schrödinger's cat, often stated as follows: "Quantum mechanics predicts that, since a cat can be alive and it can be dead, it can also be in a superposition state $a|\text{alive}\rangle + b|\text{dead}\rangle$. Why, then, do we never see such superposition states?" The answer [10, 20] is that if we are to determine what the theory predicts about what we see, then we must put ourselves into the theory. We know

that the laws of physics will evolve a state of a live cat and an inquisitive observer into a state of a live cat and a happy observer seeing a live cat; similarly, they will evolve a state of a dead cat and an inquisitive observer into a state of a dead cat and an unhappy observer seeing a dead cat. A state of a cat in the superposition $a|\text{alive}\rangle + b|\text{dead}\rangle$, together with an inquisitive observer, will therefore evolve to

$$a|\text{alive}\rangle_{\text{cat}}|\text{“I see a live cat”}\rangle_{\text{observer}} + b|\text{dead}\rangle_{\text{cat}}|\text{“I see a dead cat”}\rangle_{\text{observer}}.$$

The cat becomes *entangled* with the observer. Nowhere in this entangled state is there a state of an observer seeing a superposition state of the cat; the theory tells us that the only states that the observer can experience are those of seeing a live cat and seeing a dead cat.

Quantum Cryptography

The context in which entanglement was first introduced and explored was purely theoretical, not to say philosophical. It is only in the last fifteen years that it has been realised that the ideas described above have practical applications. I will now describe three examples of the practical power of entanglement.

The first is a novel solution to the cryptographic problem of key distribution [9]. It is well known [18] that the only perfectly secure method of encoding a message is to use a key as long as the message, and to use a different key for each message. A *message* can always be written in an alphabet of two symbols (say 0 and 1), when it becomes a string of binary digits, i.e. a vector $\mathbf{m}$ in $\mathbb{Z}_2^N$ for some N. A *key* is another vector $\mathbf{k} \in \mathbb{Z}_2^N$. The coded message is the vector (or bitwise) sum $\mathbf{c} = \mathbf{m} + \mathbf{k}$ (mod 2); knowing $\mathbf{k}$, one can recover $\mathbf{m}$ from $\mathbf{c}$. But one wants to be sure that nobody else can read the message, so one is faced with the problem of distributing the key so that nobody can intercept it, or keeping it so that nobody can steal it. The solution offered by entanglement is often called “quantum key distribution”, but it is in fact a process of quantum key *generation*. The key is safe from burglary because it does not exist until the moment of use.

The sender Alice and the receiver Bob obtain the digits of their key from an ordered collection of pairs of *qubits*. Each qubit is a quantum object with a two-dimensional state space (e.g. a spin-$\frac{1}{2}$ particle), so that it has an orthonormal “computational” basis which can be labelled $|0\rangle$ and $|1\rangle$. Measuring an observable which has these states as eigenstates is called “measuring in the computational basis”. Each pair of qubits, one held by Alice and one by Bob, is in the entangled state $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. When they want to generate their key, Alice and Bob both measure their qubits in the

computational basis. The result (0 or 1) is unpredictable, but the entanglement of each pair guarantees that Alice and Bob will get the same result for corresponding qubits. These results are the digits of their key.

Quantum codebreaking

In practice we already have secure cryptography; commercial communication generally uses encryption based on the RSA system which can in principle be broken, but only by solving the problem of finding the prime factors of a large integer. In theory this can be done, and there is no proof that it cannot be done quickly; but in practice it appears to be impossible. The key for the RSA code consists of a pair of large primes p, q (having, say, N binary digits each). Encoding a message uses the integer pq, which can be found by performing about N^2 multiplications and additions. Decoding, however, requires finding p and q given the $2N$-digit number pq, which requires dividing by all candidate factors up to $\sqrt{pq}$, therefore doing about 2^N divisions. There are faster methods, but they are still exponential in $N^{1/3}$, and it is easy to make N large enough that the time required on the fastest computer is comparable to the age of the universe.

So the description of quantum key generation by Ekert in 1991 was a solution to a non-existent problem.[1] But it became a potentially real problem in 1994, when Peter Shor showed that the basis of RSA coding could be undermined by a quantum computer. He discovered an algorithm which could factorise a $2N$-digit number using less than N^3 quantum operations, running on a quantum computer — which makes essential use of entanglement.

Quantum computing

In essence, a quantum computer harnesses the power of superposition (of which entanglement is just one example). A highly stylised picture of a quantum computer can be obtained by thinking of a classical computer in a superposition of a number Q of orthogonal states, in each of which it is performing a different calculation. One could then say that in the time needed for a classical computer to do one calculation, the quantum computer is performing Q calculations. But this speed-up is only apparent, since we only have access to the result of one of these calculations — in fact the quantum computer performs worse, since we have no control over which

[1] The history of quantum cryptography is actually a little more complicated than this. The entanglement-based quantum key described here was first devised by Wiesner in the 1960s, *before* the RSA system, but it was not accepted for publication. A different quantum scheme, not using entanglement, was published by Bennett and Brassard in 1984.

calculation we learn the answer to. The power of quantum computation results from the possibility of asking different questions. For example, by making a different measurement we could obtain the answer to the question "Are the results of the calculations all the same?" To answer this question on a classical computer, we would have to run all Q calculations, taking Q units of time. On a quantum computer we could obtain the answer in one unit.

Shor's factorisation algorithm uses quantum superposition to find the period of a function by evaluating the function just once, but applying this evaluation to a superposition of all input states. This results in a state in which the input system (or "register") is entangled with the output register. It has been shown that this entanglement is essential for the exponential speed-up over classical algorithms.

Superdense coding

Entanglement makes it possible to transmit two bits of information by sending one qubit. Thus it doubles the classical capacity of a channel: a bit (in the sense of an object which can be in just one of two states) can carry only one bit of information (in the sense of an answer to a yes/no question, e.g. 0 or 1?) But suppose Alice and Bob share a pair of qubits in the entangled state $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$. Alice encodes two bits of information by specifying one of the four operators

$$U_\pm = |0\rangle\langle 0| \pm |1\rangle\langle 1|, \qquad V_\pm = |0\rangle\langle 1| \pm |1\rangle\langle 0|. \tag{4}$$

When one of these operators is applied to Alice's qubit, the two-qubit state becomes

$$(U_\pm \otimes \mathbf{1})|\Psi_+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle \pm |1\rangle|1\rangle) = |\Psi_\pm\rangle \tag{5}$$

$$\text{or} \quad (V_\pm \otimes \mathbf{1})|\Psi_+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle) = |\Phi_\pm\rangle. \tag{6}$$

She transmits the message by sending her single qubit to Bob, who now holds one of the four states $|\Psi_\pm\rangle, |\Phi_\pm\rangle$. A single measurement then tells him which message Alice sent.

Quantum teleportation

The idea of teleportation is to transmit a material object by transmitting the information needed to assemble the object. In a favourite science fiction comic strip of my boyhood [13], Dan Dare is transported from the northern

to the southern hemisphere of Venus by stepping into a box where the constitution of his body is precisely measured. The measurements are sent by radio to his destination, where there is a supply of body parts which are reassembled according to the information in the radio transmission. Although the idea arose in science fiction, there is nothing remarkable about this process for classical objects. In fact we already have teleportation devices — we call them fax machines. But for quantum objects the process is blocked at the measurement stage: it is impossible to obtain the full information about the quantum state of an object by measuring it. The discovery of quantum teleportation in 1993 [4] was therefore a great surprise.

In quantum teleportation the channel for the transmission of information is not radio but entanglement. In order for Alice to transmit Dan Dare to Bob, both Alice and Bob must have stores of body parts, with the two stores in an entangled state. Alice makes a joint measurement of Dan Dare and her store; this has an immediate effect on Bob's supply of body parts, assembling them into something related to Dan Dare. But in order to convert this preliminary version into a precise copy of Dan Dare, Bob needs more information which Alice can only transmit to him by radio or some other method of classical communication.

To show exactly how this works, let us replace Dan Dare by a qubit. Alice and Bob share a pair of qubits in the standard entangled state $|\Psi_+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$; Alice also holds the message qubit (Dan Dare) in the state

$$|\mathrm{DD}\rangle = a|0\rangle + b|1\rangle$$

which is to be transmitted. Thus the initial state of the three qubits is

$$\begin{aligned}
|\phi\rangle_A|\Psi\rangle_{AB} &= \frac{1}{\sqrt{2}}\big(a|0\rangle_A + b|1\rangle_A\big)\big(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\big) \\
&= \tfrac{1}{2}|\Psi_+\rangle_A\big(a|0\rangle + b|1\rangle\big)_B + \tfrac{1}{2}|\Psi_-\rangle_A\big(a|0\rangle - b|1\rangle\big)_B \\
&\quad + \tfrac{1}{2}|\Phi_+\rangle_A\big(a|1\rangle + b|0\rangle\big)_B + \tfrac{1}{2}|\Phi_-\rangle_B\big(a|1\rangle - b|0\rangle\big)_B \\
&= \tfrac{1}{2}\big(|\Psi_+\rangle U_+|\mathrm{DD}\rangle + |\Psi_-\rangle U_-|\mathrm{DD}\rangle + |\Phi_+\rangle V_+|\mathrm{DD}\rangle + |\Phi_-\rangle V_-|\mathrm{DD}\rangle
\end{aligned}$$

where the states $|\Phi_\pm\rangle$ and $|\Psi_\pm\rangle$ and the operators $U_\pm$ and $V_\pm$ are as defined in (4) and (5). Alice measures her two qubits in the basis $\{|\Psi_\pm\rangle, |\Phi_\pm\rangle\}$. This projects Bob's qubit into one of the four states $U_\pm|\mathrm{DD}\rangle, V_\pm|\mathrm{DD}\rangle$. In order to recover the state $|\mathrm{DD}\rangle$, he must apply one of the "Bell rotations" $U_\pm^{-1}$ or $V_\pm^{-1}$, depending on the projection caused by Alice's measurement; he will only know what this was when Alice tells him the result of the measurement.

It is amusing to note that the authors of the Dan Dare story already, in 1950, realised the part played by the final Bell rotation in the teleportation procedure: by a technical hitch, the Bell rotation is omitted in the teleportation of Dan Dare's companion Digby, who arrives at the destination upside-down.

Part II: The Power to Entangle

Quantifying Entanglement

If entanglement is so useful, we want to know how to create it, and as much of it as possible. In this part of the talk we will examine the question "What operations on two quantum objects are best at entangling them?" In order to answer this, we need to quantify the entanglement in a state of the two objects.

The mark of an entangled state of two objects A and B is that each individual object does not have a definite (pure) state, but is in a mixed state. Consider a pure state $|\Psi\rangle_{AB}$ of two qubits. By the Schmidt decomposition we can always find orthonormal bases $|0\rangle_{A,B}, |1\rangle_{A,B}$ such that

$$|\Psi\rangle_{AB} = a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B.$$

The entanglement of this state can be equated with the lack of knowledge of Alice's state, or the lack of purity in her density matrix

$$\rho_A = |a|^2|0\rangle\langle 0| + |b|^2|1\rangle\langle 1|.$$

Such lack of knowledge (the information needed to specify the state $|0\rangle$ or $|1\rangle$ when they occur with probabilities $|a|^2$ and $|b|^2$) is measured by the von Neumann entropy of ρ_A, which is equal to the von Neumann entropy of ρ_B and also called the *entanglement entropy* of $|\Psi\rangle_{AB}$,

$$E(|\Psi\rangle_{AB}) = S_{\text{vN}}(\rho_A) = -\operatorname{tr}(\rho_A \log_2 \rho_A) = -\operatorname{tr}(\rho_B \log_2 \rho_B)$$

$$= -|a|^2 \log_2 |a|^2 - |b|^2 \log_2 |b|^2.$$

This has its maximum value when $|a|^2 = |b|^2 = \frac{1}{2}$, e.g. for the state $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, often called a "singlet" because

$$\tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) = \big(\mathbf{1} \otimes i\sigma_y\big)\tfrac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$$

i.e. it differs from the usual singlet only by an operation on Bob's qubit. The entanglement of the state, being a joint property, is unaffected by such *local operations* $U \otimes V$.

A more financial approach to quantifying the amount of entanglement in a state is to regard this maximally entangled state as a gold standard and to ask how much the state $|\Psi\rangle_{AB}$ is worth in gold units. If Alice and Bob have N copies of $|\Psi\rangle$, how many singlets can they make using local operations and classical communication? The answer [3] is at most M, where

$$\frac{M}{N} \to E(|\Psi\rangle) \text{ as } N \to \infty.$$

It can also be shown that this is the *cost* of $|\Psi\rangle$, in the sense that at least M singlets are needed to make N copies of $|\Psi\rangle$. However, this equality holds only for pure states.

Thus the entanglement entropy, based on the von Neumann entropy, is a natural measure of entanglement. But the log functions make it difficult to work with, and for qualitative purposes (such as finding the maximum) we can equivalently work with any monotonic function of it. A convenient alternative is the "linear entropy"

$$S_{\mathrm{L}}(|\Psi\rangle) = 2\,\mathrm{tr}\left(\rho_A - \rho_A^2\right) = 4|a|^2|b|^2$$

which clearly measures the departure of ρ_A from purity (when $\rho_A^2 = \rho_A$). Generalising to the case where A and B are not qubits but have state spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of equal dimension d, we define

$$S_{\mathrm{L}}(|\Psi\rangle) = \frac{d}{d-1}\left(1 - \mathrm{tr}\,\rho_A^2\right). \tag{7}$$

This is normalised to lie in $[0, 1]$.

Entangling power

We can now quantify the entangling power of a joint operation on A and B, in the form of a unitary operator $U : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$, by asking "How much entanglement does U create when acting on an unentangled pure state (on average)?" Measuring the entanglement of a pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ by the linear entropy (7), this gives the entangling power of U as

$$\mathcal{E}(U) = \int_{S(\mathcal{H}_A)\times S(\mathcal{H}_B)} S_{\mathrm{L}}\big[U(|\phi\rangle|\psi\rangle\big]\,\mathrm{d}|\phi\rangle\mathrm{d}|\psi\rangle \tag{8}$$

where $S(\mathcal{H})$ is the unit sphere of normalised vectors in the Hilbert space $\mathcal{H}$, and $d|\psi\rangle$ is the unitary-invariant measure on $S(\mathcal{H})$, normalised so that the measure of the whole sphere is 1.

Calculation of entangling power

The integral in (8) has been calculated by Zanardi [19], using a correspondence between operators $X : \mathcal{H} \to \mathcal{H}$ and pure bipartite states $|X\rangle \in \mathcal{H} \otimes \mathcal{H}$, defined relative to an orthonormal basis $|i\rangle$ for any Hilbert space $\mathcal{H}$:

$$X|j\rangle = \sum_j x_{ij}|i\rangle \quad \longleftrightarrow \quad |X\rangle = \sum_{ij} x_{ij}|i\rangle|j\rangle \tag{9}$$

We are interested in operators $U : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B$, for which we define a slightly different correspondence: such an operator can be expanded as $U = \sum_m X_m \otimes Y_m$ where the X_m and Y_m are operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, and we define the corresponding (non-normalised) state to be

$$|U\rangle = \sum_m |X_m\rangle|Y_m\rangle \in (\mathcal{H}_A \otimes \mathcal{H}_A) \otimes (\mathcal{H}_B \otimes \mathcal{H}_B)$$

where the states $|X_m\rangle$ and $|Y_m\rangle$ are given by (9). Then, for example, the identity operator $I = \sum_{ij} |ij\rangle\langle ij|$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ corresponds to

$$|I\rangle = |\Psi_+\rangle_A|\Psi_+\rangle_B \qquad \text{where} \quad |\Psi_+\rangle_A = \sum_i |i\rangle|i\rangle.$$

If $\mathcal{H}_A = \mathcal{H}_B$, we also have the *swap* operator $S = \sum_{ij} |ij\rangle\langle ji|$, which corresponds to

$$|S\rangle = |\Psi_+\rangle_{AB} = \sum_{ij} |ij\rangle|ij\rangle.$$

Zanardi [19] gives the entangling power of a bipartite operator U in terms of the entanglement entropies of the corresponding state, as follows:

$$\mathcal{E}(U) = \frac{d}{d+1}\big[S_{\mathrm{L}}(|U\rangle) + S_{\mathrm{L}}(|US\rangle) - S_{\mathrm{L}}(|S\rangle)\big] \tag{10}$$

where S is the swap operator, as above.

The most entangling

It follows fairly immediately from Zanardi's formula (10) that

$$\mathcal{E}(U) \leq \frac{d}{d+1} \tag{11}$$

and

$$\begin{aligned} \mathcal{E}(U) = \frac{d}{d+1} \quad &\iff \quad |U\rangle \text{ and } |US\rangle \text{ are both maximally entangled} \\ &\iff \quad \mathrm{tr}_A\, |U\rangle\langle U| = \mathrm{tr}_A\, |US\rangle\langle US| = \mathbf{1}. \end{aligned}$$

Here

$$|U\rangle = \sum_{ijkl} u_{ij,kl}|ij\rangle|jl\rangle$$

and

$$|US\rangle = \sum_{ijkl} u_{ij,kl}|il\rangle|jk\rangle$$

where

$$U = \sum_{ijkl} u_{ij,kl}|ij\rangle\langle kl|.$$

Is the bound (11) attained? The above shows that this is equivalent to the existence of a four-party state which is maximally entangled as a state of two pairs, for each of the splits $12|34, 13|24, 14|23$. This can be expressed as a matrix problem: given a $d^2 \times d^2$ matrix U whose matrix elements form a 4-index tensor $u_{ij,kl}$, define the $d^2 \times d^2$ matrices V and W by

$$v_{ij,kl} = u_{ik,jl}, \qquad w_{ij,kl} = u_{il,jk}.$$

Can the three matrices U, V, W all be unitary? It is known [14] that for $d = 2$ the answer is *No*. However, we will show that for all other d except possibly $d = 6$, the answer is Yes.

Permutations

A convenient class of unitary operators in which to search for maximal entanglers is the class of permutation operators relative to a given orthonormal basis, which permute elements of the basis:

$$U_\sigma|i\rangle = |\sigma(i)\rangle \qquad (\sigma \in S_n,\ n = \dim \mathcal{H})$$

where S_n is the set of permutations of $N = \{1, \ldots, n\}$. We are interested in the case $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$, so $n = d^2$; then N is the set of pairs (i, j) with $1 \leq i, j \leq d$, a permutation $\sigma \in S_{d^2}$ is given by $\sigma(i, j) = (k_{ij}, l_{ij}$, and the corresponding operator $P = \mathrm{U}_\sigma$ acts as

$$P|i\rangle|j\rangle = |k_{ij}\rangle|l_{ij}\rangle \tag{12}$$

with $k_{ij}, l_{ij} \in \{1, \ldots, d\}$. It is known that such an operator is *non-entangling* if and only if it is of one of the forms $U \otimes V$ or $(U \otimes V)S$ where U and V are permutation operators on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. It follows that for large d, most permutations create entanglement: the probability that a randomly chosen permutation is non-entangling is

$$\frac{2(d!)^2}{(d^2)!} \to 0 \quad \text{as } d \to \infty.$$

Entangling power of permutations

Zanardi's formula gives the entangling formula of a permutation P as

$$\mathcal{E}(P) = \frac{d^2(d^2+1) - Q_P - Q_{PS}}{d(d-1)(d+1)^2}$$

where

$$Q_P = \sum_{ijmn} a_{ijm} a_{ijn} b_{imn} b_{jmn},$$

$$\begin{aligned} a_{ijm} &= \langle l_{im} | l_{jn} \rangle \\ &= 1 \text{ only if } P \text{ takes the vertical pair } (|im\rangle, |jm\rangle) \\ &\quad \text{to another vertical pair,} \end{aligned}$$

$$\begin{aligned} b_{imn} &= \langle k_{im} | k_{in} \rangle \\ &= 1 \text{ only if } P \text{ takes the horizontal pair } (|im\rangle, |in\rangle) \\ &\quad \text{to another horizontal pair.} \end{aligned}$$

(Here the terms "horizontal" and "vertical" refer to position in the $d \times d$ square of basis elements $|ij\rangle$.) Hence the summand $r_{ijmn} = a_{ijm} a_{ijn} b_{imn} b_{jmn}$ in Q_P satisfies

$$\begin{aligned} r_{ijmn} &= 1 \text{ only if } P \text{ takes the rectangle } (|im\rangle, |in\rangle, |jm\rangle, |jn\rangle) \\ &\quad \text{to another rectangle in the same orientation.} \end{aligned}$$

Similarly,

$$Q_{PS} = \sum_{ijmn} r'_{ijmn}$$

where

$$\begin{aligned} r_{ijmn} &= 1 \text{ only if } P \text{ takes the rectangle } (|im\rangle, |in\rangle, |jm\rangle, |jn\rangle) \\ &\quad \text{to a rectangle in the opposite orientation.} \end{aligned}$$

Maximally entangling permutations

To maximise the entangling power $\mathcal{E}(P)$, we have to minimise Q_P and Q_{PS}. Now the summands r_{ijmn} and r'_{ijmn}, each 0 or 1, are certainly equal to 1 when $i = j$ and $m = n$; minimum values of Q_P and Q_{PS} will be attained if P is such that $r_{ijmn} = r'_{ijmn} = 0$ for all other values of i, j, m, n. If this is the case, $Q_P = Q_{PS} = d^2$ and so $\mathcal{E}(P)$ takes its maximum value $d/(d+1)$.

Thus P should not take any rectangle to a rectangle, i.e. it should not take any pair of elements in the same row or column to elements in the same row or column. This implies that the matrix of row numbers k_{ij} is a *latin square*, as is the matrix of column numbers l_{ij}. Finally, the map $(i,j) \mapsto (k_{ij}, l_{ij})$ must be a permutation; this means that the k_{ij} and l_{ij} are *orthogonal* latin squares.

Orthogonal latin squares were first considered by Euler, who gave constructions for $d \times d$ squares when $d \equiv 0, 1$ or $3 \pmod 4$ but, being unable to do so for $d \equiv 2 \pmod 4$, conjectured that orthogonal latin squares of these sizes did not exist. However, he was wrong; in 1960 it was proved [5] that orthogonal $d \times d$ latin squares exist for all d except $d = 2$ and $d = 6$. It follows that there exist permutation operators attaining Zanardi's bound for the entangling power of bipartite unitary operators, in all dimensions except these two. For $d = 2$ we have already seen that the bound is not attained; in fact the maximum entangling power of a two-qubit unitary operator is not $d/(d+1) = 2/3$ but $4/9$, which is attained by the permutation CNOT. For $d = 6$ the greatest entangling power of a permutation is $\frac{628}{735}$ [7]. We do not know whether Zanardi's bound of $\frac{6}{7}$ is attained by some non-permutation operator.

References

[1] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964. Reprinted in [2].

[2] J. S. Bell. *Speakable and unspeakable in quantum mechanics*. Cambridge University Press, 1987.

[3] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046, 1996. `9511030`.

[4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting a quantum state via dual classical and epr channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[5] R. C. Bose, S. S. Shrikhande, and E. T. Parker. Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Canad. J. Math.*, 12:189, 1960.

[6] P. Butterley, A. Sudbery, and J. Szulc. Compatibility of subsystem states. *Found. Phys.*, 2006. to be published. `quant-ph/0407227`.

[7] L. Clarisse, S. Ghosh, S. Severini, and A. Sudbery. Entangling power of permutations. *Phys. Rev. A*, 72:012314, 2005. `quant-ph/0502040`.

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[9] A. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[10] E. Joos et al. *Decoherence and the appearance of a classical world in quantum theory.* Springer, Berlin, 2nd edition, 2003.

[11] A. Fine. Hidden variables, joint probability, and the Bell inequalities. *Phys. Rev. Lett.*, 48:291, 1982.

[12] N. Gisin. Bell's inequality holds for all non-product states. *Phys. Lett. A*, 154:201, 1991.

[13] F. Hampson and H. Johns. Dan Dare: Pilot of the Future. *Eagle*, 1, 1950.

[14] A. Higuchi and A. Sudbery. How entangled can two couples get? *Phys. Lett. A*, 273:213, 2000. `quant-ph/0005013`.

[15] A. Peres. All the Bell inequalities. *Found. Phys.*, 29:589, 1999. `quant-ph/9807017`.

[16] I. Pitowsky. Correlation polytopes: their geometry and complexity. *Math. Programming*, 50:395, 1991.

[17] E. Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23:807, 1935.

[18] S. Singh. *The Code Book.* Fourth Estate, London, 2000.

[19] P. Zanardi. Entanglement of quantum evolutions. *Phys. Rev. A*, 62:030301, 2000.

[20] H. D. Zeh. Roots and fruits of decoherence. `quant-ph/0512078`.