Is entanglement monogamous?

B. M. Terhal

In this paper I discuss some of the early history of quantum information theory. By considering the question of whether entanglement is "monogamous," I illustrate Charles Bennett's influence on modern quantum information theory. Finally, I review our recent answers to this entanglement question and its relation to Bell inequalities.

Introduction

It was a pleasure to contribute to the May 2003 scientific festivities at the IBM Thomas J. Watson Research Center commemorating Charles Bennett's sixtieth birthday. I believe that I was there representing the younger generation of quantum information theorists. Like John Smolin and Ashish Thapliyal, who also did their Ph.D. research at IBM, I can say that Charlie Bennett is my "scientific father." Not being at a university, Charlie has never assembled a large group of doctoral students. Nonetheless, I think that he has inspired many of us, students, postdocs, and also senior researchers, many of whom were present at the event. In some sense I would say that we are all Charlie's students. **Figures 1–6** show the growing number of participants at the Quantum Information Processing (QIP) conferences. The QIP conferences were established to provide a venue for computer science and algorithmic aspects of quantum information processing. The first conference, called "Algorithms in Quantum Information Processing," was held in 1998 in Århus, Denmark. (Photographs courtesy of C. H. Bennett, I. L. Chuang, and G. S. Frandsen.)

Charlie's influence in quantum information theory does not limit itself to the direct effects of his scientific work—quantum teleportation, quantum key distribution, and the framework of entanglement manipulations, to name a few. There seems to be a deeper thread running through quantum information theory to which Charlie has contributed considerably.

The fact is that quantum information is not a subject that evolved yesterday, or after 1994, when Shor discovered that large numbers could be factored efficiently on a quantum computer [1]. It is quite a bit older than that. For example, a few years ago I found a paper on the subject written in 1976 by the Polish mathematical physicist Roman Ingarden [2]. The title of the paper is "Quantum Information Theory," and the first few sentences of the abstract go like this:

> "A conceptual analysis of the classical information theory of Shannon (1948) shows that this theory cannot be directly generalized to the usual quantum case. The reason is that in the usual quantum mechanics of closed systems there is no general concept of joint and conditional probability. Using, however, . . . , it is possible to construct a quantum information theory being then a straightforward generalization of Shannon's theory."

This paper was published in the Polish journal *Reports on Mathematical Physics*, which I found in the library at the Thomas J. Watson Research Center a few years ago. (Actually, when I recently wanted to have a look at this paper again, it turned out that the library did not have the journal anymore; unfortunately, it was discarded after a recent cleanup!)

Ingarden was one of a group of physicists, many of them in Eastern Europe and the former Soviet Union, who were thinking about the intersection of information theory, probability, and quantum physics in the 1960s and 1970s. The most notable member of this group may be Alexander Holevo from the Steklov Mathematical Institute in Russia, who is still very active in modern quantum information theory. His 1973 result that n quantum bits, or qubits for short, cannot carry more than n bits of information [3] is frequently invoked in modern quantum information theory.

Ingarden's paper is one of the first attempts at building a theory of quantum information analogous to Shannon's classical theory of information. He considers the problem of transmitting classical information through a quantum channel whose output is measured by *fixed* single-letter projective measurements. Since input and output are then

©**Copyright** 2004 by International Business Machines Corporation. Copying in printed form for private use is permitted without payment of royalty provided that (1) each reproduction is done without alteration and (2) the *Journal* reference and IBM copyright notice are included on the first page. The title and abstract, but no other portions, of this paper may be copied or distributed royalty free without further permission by computer-based and other information-service systems. Permission to *republish* any other portion of this paper must be obtained from the Editor.

0018-8646/04/$5.00 © 2004 IBM

Figure 1

Participants at AQIP ’98 in Århus.

Figure 2

Participants in the hotel lobby at AQIP ’99 in Chicago.

Figure 3

Participants in Montréal at QIP 2000.

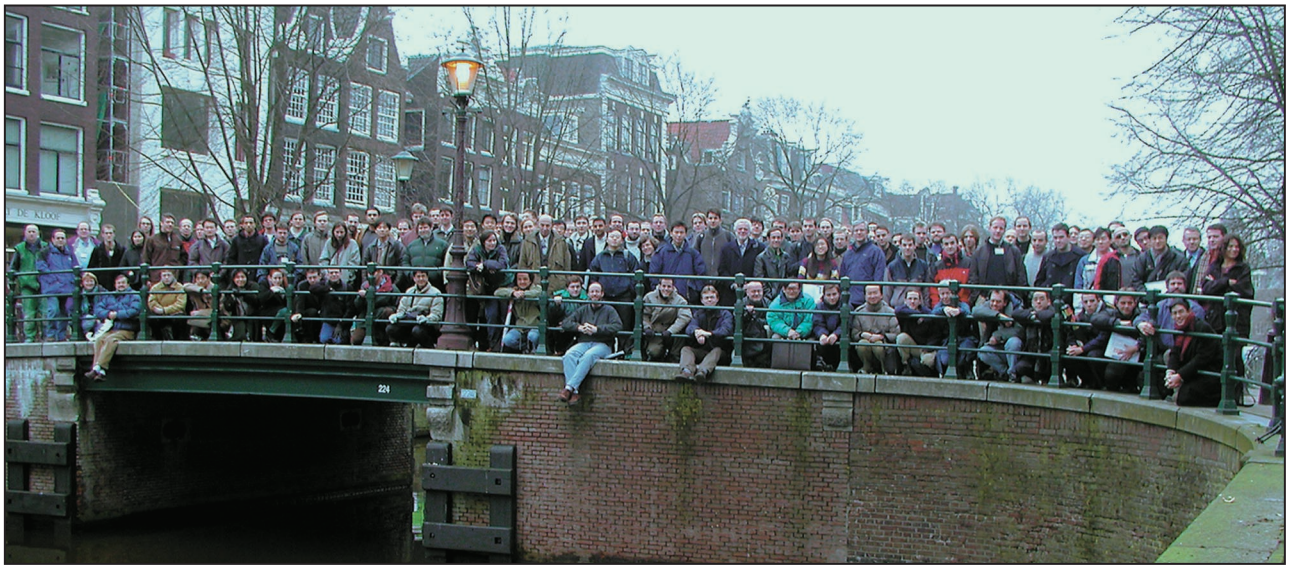

Figure 4

Participants on the canal in Amsterdam at QIP 2001.

classical, Shannon's expression of the classical capacity can be applied directly.

So now it is an interesting question to consider in what way modern quantum information theory is different from the earlier work, and here, I believe, is where Charlie comes in.

First, there is of course the difference in volume. A search at the quantum physics archive at the *arxiv.org* Web

Figure 5

Participants in front of the IBM Thomas J. Watson Research Center at QIP 2002.

Figure 6

Participants in the Mathematical Sciences Research Institute (MSRI), Berkeley, at QIP 2003.

site reveals that over the past years there have appeared about 883 papers with the word *information* in the abstract and about 597 papers with *entanglement* in the abstract, and this probably understates the current output.

The second difference, however, is more fundamental. In the modern theory of quantum information, we speak of quantum systems in the hands of Alice and Bob and Eve—these names first made their appearance in cryptography in the 1970s. We say things such as "Alice sends Bob a qubit and forgets what she did," "Bob does a measurement and tells Alice," and "Eve does a random unitary transformation on her half of the Einstein–Podolsky–Rosen (EPR) pair." Even though this seems very casual, it is, at least to the reader familiar with quantum information jargon, crystal clear what is meant in these situations.

In the earlier work, we are more likely to see descriptions such this one from a paper by G. Lindblad in 1973 [4]:

> "The map $T_A: W \to W$ extended to $B(H)$ is a special case of an expectation in the operator algebra $B(H)$, i.e., a linear map from $B(H)$ into a von Neumann subalgebra satisfying $T \circ I = I$ where I is the identity operator."

This example illustrates the fact that the earlier work on the subject was first of all grounded in mathematical physics and less well connected to a world in which we may actually send quantum systems around, do measurements, and transform states. What has changed since the 1960s and 1970s is not that we have actually seen Eve do a random unitary transformation on her half of an EPR pair, but somehow we have started to dream and imagine that it would happen some day. Somehow, people at IBM Research and elsewhere started to think about irreversibility, physics, and information. And those people, most particularly Charlie Bennett, preferred to think about quantum information in a more conceptual, intuitive way. The goal was to ask simple questions which could have profound nonintuitive answers, e.g., in quantum teleportation, and in this way we started to understand how quantum information is different from classical information.

The new language in which the questions were posed was one of action and operation. A prime example is Charlie's question, "What happens when we throw in an EPR pair?" in the discussion that led to the discovery of quantum teleportation. This operational point of view, i.e., asking how quantum information and entanglement can be used and manipulated for quantum information processing, has been extremely fruitful, and I believe that Charlie Bennett has played a key role in its success.

Is entanglement monogamous?

Turning to the title of this paper, I consulted our modern-day oracle, the search engine Google**. When I googled "entanglement monogamous," I got 215 hits in 0.02 seconds, and as you may expect, a fair number of them were unrelated to science. Here are the first three:

- ". . . You can't become entangled simply by talking on the telephone. Entanglement is monogamous—the more entangled Bob is with Alice, the less entangled he can be . . ." at *qpip-server.tcs.tifr.res.in/~qpip/HTML/Courses/Bennett/TIFR2.pdf*.
- ". . . this idea doesn't fit with the traditional view of monogamous societies, Siva . . . The technique has the added bonus of improving the entanglement of pairs that pass . . . " at *www.dhushara.com/book/upd3/2002a/28apr01/nsapr.htm*.
- ". . . My monogamous wonderful forever relationship has fallen apart . . . are trying a polyamorous relationship but it will be long distance and with minimal entanglement. . . . " at *www.cavegirl.org/polyhell.html*.

The first quote is taken from a set of lectures that Charlie gave at the Tata Research Institute in India. These few phrases suggest exactly what I mean with the question "Is entanglement monogamous?". Is entanglement indeed a property that one can have with only one person or quantum system, or can one share it with many? I would like to consider an example taken from political life. There are two opinions that were considered relevant early in 2003. A person was either for the U.S. invasion in Iraq or against it. It is clear that it did not take much for the President to convince most people in the United States to be pro-war. And if President Bush had been against the war, quite likely most of the American people would have been against it. In this sense, a classical bit of correlation—to be or not be against the war in Iraq—can *at least in principle* be shared by an unlimited number of people.

But now consider a scenario in which President Bush and Secretary of Defense Rumsfeld start out in an entangled state containing both opinions:

$$\frac{1}{\sqrt{2}}\left(|\text{PRO WAR}\rangle_{\text{Bush}} \otimes |\text{PRO WAR}\rangle_{\text{Rumsfeld}} + |\text{AGAINST WAR}\rangle_{\text{Bush}} \otimes |\text{AGAINST WAR}\rangle_{\text{Rumsfeld}}\right); \quad (1)$$

i.e., as a superposition of two states: One is a state in which Bush and Rumsfeld are both pro-war and the other is a state in which both, unlikely though it may seem, are against the war. In this example, the amplitudes for both states are equal, but we may adjust them; say we assign an arbitrarily small amplitude of $\sqrt{\epsilon}$ to the no-war state in order to make it resemble the real situation more closely. When both opinions are measured, we find that the two always agree, and the purely classical correlation that is found can again be shared freely.

The Bush–Rumsfeld state is a pure entangled state. (I am taking the liberty of following current trends of renaming well-established concepts for political reasons; thus, I do *not* call this an EPR pair.) This implies that there is no quantum state shared by three parties, Bush, Rumsfeld, and someone else (say, Joe Smith) such that when we remove Joe we get the Bush–Rumsfeld state *and*, at the same time, the total three-party state would not change if Joe and Rumsfeld were interchanged. The reason is

simple. Let us represent pro-war by a 0 and anti-war by a 1. The first requirement implies that since the Bush–Rumsfeld state is pure, the state for three parties must be a state for Joe alone in tensor product with the Bush–Rumsfeld state:

$$|\text{Joe's state}\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle_{\text{Bush}} \otimes |0\rangle_{\text{Rumsfeld}} + |1\rangle_{\text{Bush}} \otimes |1\rangle_{\text{Rumsfeld}}). \quad (2)$$

But then it is clear that there is no symmetry between Joe and Rumsfeld; Joe is unentangled with Bush, whereas Rumsfeld is maximally entangled. This simple observation is the basis for Charlie's phrase "Entanglement is monogamous"; unlike partners or opinions, entanglement cannot be freely shared.

So now here is a question a modern quantum information theorist typically would ask him/herself. First, what is this observation good for, and second, is it true for all entangled states?

It turns out that this property of entanglement is essential in quantum cryptography. In 1984 Bennett and Brassard proposed a protocol for quantum key distribution, a way of letting two people, Alice and Bob, share a set of random perfectly correlated bits about which no one else has any information [5]. In other words, Alice and Bob want to establish a "monogamous correlation."

Now, given the arguments above, it is clear that if Alice and Bob were to share an entangled state, like the Bush–Rumsfeld state, they would be finished. They would measure and get the same random bit, and no one would know what they got.

Following this line of reasoning, Lo and Chau showed in 1999 [6] how Alice and Bob can proceed in order to obtain (something close to) a set of entangled states, and in this way they proved the security of an entanglement-based quantum key distribution scheme. The work by Lo and Chau was the stepping stone on which Shor and Preskill [7] in 2000 built their security proof of Bennett and Brassard's 1984 scheme.

The relation between the establishment of secrecy or a "monogamous" correlation between parties and the transmission of quantum information or entanglement has recently been investigated by Igor Devetak at IBM and A. Winter in Bristol. The basic idea is that coherent versions of schemes to establish secret random bits lead to optimal protocols that achieve the quantum capacity of a quantum channel [8] or lead to optimal one-way entanglement distillation protocols [9].

Shareability for general states

Let us now turn to the question of whether all entangled states are monogamous; more precisely, are mixed entangled states necessarily monogamous? A first example of a mixed entangled state that is is not monogamous but *shareable* (the term is from Ben Schumacher) can be found in the 1996 paper by Bennett et al., "Mixed State Entanglement and Quantum Error Correction" [10]. A noisy quantum channel is constructed in the following way: With probability 1/2, the input to a qubit channel is transmitted unchanged to Bob. In that case, the eavesdropper Eve has a completely random qubit. And with probability 1/2, Eve gets the qubit that Alice sends and Bob gets a completely random qubit. If Alice sends half of a maximally entangled state to Bob, then one can show that the state for Alice and Bob by itself is still entangled. At the same time, the total state that includes Eve's part is always symmetric with respect to Eve and Bob, and so Eve is equally entangled with Alice. This is an example of shareable noisy entanglement. The shareability directly implies that the one-way distillable entanglement of the state is zero, and similarly the secret key that can be distilled by one-way communication is zero.

It is not hard to find other examples of such states; in a recent paper [11], we have done so. One considers the following optimization problem.

Problem 1

Given ρ *on* $\mathcal{H}_A \otimes \mathcal{H}_{B_1}$, *is there a symmetric extension of* ρ' *to* $\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$ *such that*

$$\text{Tr}_{B_2}\rho' = \rho, \qquad \text{Tr}_{B_1}\rho' = \rho? \quad (3)$$

Under some reformulation, this optimization problem can be written as a semi-definite program which either returns a symmetric extension ρ' or returns the answer that there are no feasible solutions for the program, implying that there is no symmetric extension. One can generalize the problem to multiple parties; one requires that ρ be symmetrically extendible to systems $B_2, \cdots, B_n$ in the sense that the extension ρ' be invariant under any permutation of the parties $B_1, \cdots, B_n$. A weaker symmetry requirement on ρ' is one that states that the original density matrix ρ should equal the reduced density matrix ρ_{AB_i} derived from ρ' for all i. All features discussed in the next section hold for both notions of symmetric extension.

The last but perhaps most interesting property of shareable mixed entanglement lies in its relation to violations of Bell's inequalities; at least, this is how I started to think about this notion.

Bell inequalities

In the 1960s John Bell formulated an inequality that must be obeyed by any theory that is classical and local [12]. As it turns out, local measurements on entangled quantum states may violate his inequality. In particular, we know

that for every pure entangled state there exists a Bell inequality that is violated.

However, as with the notion of shareability, one may also ask whether mixed entangled states violate Bell inequalities. This question has some history, starting with work by Reinhard Werner showing that there exist states, now called Werner states, which are entangled but do not violate Bell inequalities for any number of local measurement settings [13]. Despite the large body of work on Bell inequalities, no clear-cut criteria have been developed to decide whether a state does or does not violate some Bell inequality.

The problem is first that in order to find a violation, a possibly infinite number of settings and measurement choices should be considered, which is not feasible. Second, it is a hard computational problem to enumerate all Bell inequalities for a given setting; this corresponds to enumerating the facets of some highly symmetric polytope.

Conversely, there have been no constructive methods for formulating local hidden variable models for states, if they exist. Such a thing would be quite desirable. As it turns out, there is a very nice relation between the shareability of entanglement and the existence of a local hidden variable model. The correspondence is the following.

Theorem 2 [11]

Let ρ be a density matrix on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{B_1}$. If ρ has a symmetric extension ρ' on $\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_m}$, then there exists a local hidden variable description of ρ when Alice has an arbitrary number and Bob has m possible measurements.

The intuitive picture behind this theorem is simple. The proof of the theorem rests on three observations. First, if ρ has a symmetric extension ρ', then Bob may do his measurements $\mathcal{M}_{B_1}, \cdots, \mathcal{M}_{B_m}$ on ρ'; that is, he does measurement $\mathcal{M}_{B_i}$ on the space $\mathcal{H}_{B_i}$. Since ρ' is a symmetric extension of ρ, the joint probabilities of outcome for some $\mathcal{M}_{A_j}$ and $\mathcal{M}_{B_i}$ are the same as for ρ. Second, Bob's m measurements on ρ' can be viewed as one large measurement $\mathcal{M}_{B_1} \times \mathcal{M}_{B_2} \times \cdots \times \mathcal{M}_{B_m}$. Third, it is known that there always exists a local hidden variable description of measurements on a quantum state when one of the two parties has only one measurement. Therefore, the measurements on ρ' have a local hidden variable description from which we can deduce the local hidden variable description of the original measurements on ρ.

Before I finish, I would like to return to the title of this paper and say that Charlie was right, as usual, that all entanglement *is* monogamous *in an asymptotic sense*. An entangled mixed state may have extensions to some number of parties, but are there entangled mixed states that can be extended to a infinite number of parties? The answer is *no*. There is a theorem that states that only unentangled states have infinite symmetric extensions.

Theorem 3 (Fannes–Lewis–Raggio–Schumacher–Verbeure–Werner) [14, 15]

A quantum state ρ on $\mathcal{H}_A \otimes \mathcal{H}_{B_1}$ is unentangled or separable if and only if ρ has symmetric extensions ρ' on $\mathcal{H}_A \otimes \mathcal{H}_{B_1} \otimes \cdots \otimes \mathcal{H}_{B_n}$ for all $n = 2, 3, \cdots$.

Concluding remark

In conclusion, let me say that I hope to have conveyed some of the flavor of the questions and answers in quantum information theory and Charles Bennett's role in this exciting area of research.

**Trademark or registered trademark of the Google Corporation.

References

1. P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM J. Computing* **26,** No. 5, 1484–1509 (1997); see *http://arxiv.org/abs/quant-ph/9508027/*. An earlier version of this paper was published in the *Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, Santa Fe, 1994.
2. R. S. Ingarden, "Quantum Information Theory," *Rep. Math. Phys.* **10,** 43–72 (1976).
3. A. S. Holevo, "Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel," *Problemy Peredachi Informatsii* **9,** No. 3, 3–11 (1973). English translation in *Problems of Information Transmission* **9,** 177–183 (1973).
4. G. Lindblad, "Quantum Entropy, Information and Quantum Measurements," *Commun. Math. Phys.* **33,** 305–322 (1973).
5. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179.
6. H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science* **283 (5410),** 2050–2056 (1999); see *http://arxiv.org/abs/quant-ph/9803006/*.
7. P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.* **85,** 441–444 (2000); see *http://arxiv.org/abs/quant-ph/0003004/*.
8. I. Devetak, "The Private Classical Information Capacity and Quantum Information Capacity of a Quantum Channel"; see *http://arxiv.org/abs/quant-ph/0304127/* (2003).
9. I. Devetak and A. Winter, "Distillation of Secret Key and Entanglement from Quantum States," see *http://arxiv.org/abs/quant-ph/0306078/* (2003).
10. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed State Entanglement and Quantum Error Correction," *Phys. Rev. A* **54,** 3824–3851 (1996); see *http://arxiv.org/abs/quant-ph/9604024/*.
11. B. M. Terhal, A. C. Doherty, and D. Schwab, "Local Hidden Variable Theories for Quantum States," *Phys. Rev. Lett.* **90,** 157903 (2003).
12. J. S. Bell, "On the Einstein–Podolsky–Rosen Paradox," *Physics* **1,** 195–200 (1964).

13. R. F. Werner, "Quantum States with Einstein–Podolsky–Rosen Correlations Admitting a Hidden Variable Model," *Phys. Rev. A* **40,** 4277–4281 (1989).
14. M. Fannes, J. T. Lewis, and A. Verbeure, "Symmetric States of Composite Systems," *Lett. Math. Phys.* **15,** 255–260 (1988).
15. G. A. Raggio and R. F. Werner, "Quantum Statistical Mechanics of General Mean Field Systems," *Helv. Phys. Acta* **62,** 980–1003 (1989).

Received June 16, 2003; accepted for publication July 17, 2003

Barbara M. Terhal *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (terhal@watson.ibm.com).* Dr. Terhal is a Research Staff Member in the Physical Sciences Department at the Thomas J. Watson Research Center. She received an M.S. degree in theoretical physics from the University of Amsterdam in 1995, and a Ph.D. (cum laude) in physics from the University of Amsterdam in 1999. She was a visiting scientist at the Thomas J. Watson Research Center from 1999 to 2001 and a postdoctoral fellow at the California Institute of Technology in 2002. In 2002 she joined IBM to continue her theoretical research on quantum information theory and quantum computation. Dr. Terhal is an author or coauthor of 27 technical papers on various aspects of quantum information theory.