

## LECTURE NOTES ON QUANTUM COMPUTATION

Cornell University, Physics 481-681, CS 483; Spring, 2005

© 2005, N. David Mermin

## VI. Quantum cryptography and some simple uses of entanglement

Most of the examples that follow make use of a very simple entangled state, the 2-Qbit state

$$|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (6.1)$$

It can be produced from two Qbits each in the state  $|0\rangle$  by applying a Hadamard to one of them, and then using it as the control Qbit for a cNOT that targets the other (Figure 6.1(a)):

$$|\psi_{00}\rangle = \mathbf{C}_{10}\mathbf{H}_1|00\rangle. \quad (6.2)$$

We can generalize (6.2) by letting the original pair of unentangled Qbits be in any of the four 2-Qbit computational basis states  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$ , or  $|11\rangle$  (Figure 6.1(b)):

$$|\psi_{xy}\rangle = \mathbf{C}_{10}\mathbf{H}_1|xy\rangle. \quad (6.3)$$

Since the four states  $|xy\rangle$  are an orthonormal set and the Hadamard and cNOT gates are unitary, the four entangled states  $|\psi_{xy}\rangle$  are also an orthonormal set, called the *Bell basis* to honor the memory of the physicist John S. Bell, who discovered, all the way back in 1964 (“Bell’s Theorem”), one of the most extraordinary facts about 2-Qbit entangled states.

Rewrite (6.3) as

$$|\psi_{xy}\rangle = \mathbf{C}_{10}\mathbf{H}_1\mathbf{X}_1^x\mathbf{X}_0^y|00\rangle, \quad (6.4)$$

and recall that  $\mathbf{H}\mathbf{X} = \mathbf{Z}\mathbf{H}$  and that either a  $\mathbf{Z}$  on the control Qbit or an  $\mathbf{X}$  on the target Qbit commute with a cNOT. We then have (see also Figure 6.2)

$$|\psi_{xy}\rangle = \mathbf{Z}_1^x\mathbf{X}_0^y\mathbf{C}_{10}\mathbf{H}_1|00\rangle = \mathbf{Z}_1^x\mathbf{X}_0^y\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (6.5)$$

So the other Bell states are obtained from  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  by either flipping one of the Qbits, changing the  $+$  to a  $-$ . or both. This, of course, can also be derived directly from evaluating (6.3) for the 4 choices of  $x$  and  $y$ , but it is more simply understood from (6.5).

We now examine a few simple protocols in which some or all of the Bell states play an important role.

## A. Quantum cryptography

A decade before Shor's discovery that quantum computation posed a threat to the security of RSA encryption, it was pointed out that Qbits (though the term did not exist at that time) offered a quite different and demonstrably secure basis for the exchange of secret messages.

Of all the various applications and gedanken applications of quantum mechanics to information processing, quantum cryptography arguably holds the most promise for someday becoming a practical technology. There are several reasons for this. First of all, it works Qbit by Qbit. The only relevant gates are a small number of simple 1-Qbit gates. Interactions between pairs of Qbits like those mediated by cNOT gates play no role, at least in the most straightforward versions of the protocol.

Furthermore, in actual physical realizations of quantum cryptography the physical Qbits are extremely simple. Each Qbit is a single photon of light. The state of the Qbit is the linear polarization state of the photon. If the states  $|0\rangle$  and  $|1\rangle$  describe photons with vertical or horizontal polarization, then the states  $\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $\mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$  describe photons diagonally polarized, either at  $45^\circ$  or  $-45^\circ$  to the vertical. Photons in any of these four polarization states can be prepared in any number of ways, most simply (if not most efficiently) by sending a weak beam of light through an appropriately oriented polaroid filter. Once a photon has been prepared in such a polarization state it does not have to be manipulated any further beyond eventually measuring either its horizontal-vertical or its diagonal polarization by, for example, sending it through an appropriately oriented birefringent crystal and seeing which beam it emerges in, or seeing whether it does or does not get through an appropriately oriented polaroid filter. Photons can effectively be shielded from extraneous interactions by sending them through optical fibers, where they can travel in a polarization-preserving manner at the speed of light.

The great utility of easily transportable single Qbits for secret communication comes from one important cryptographic fact: Alice and Bob can have an unbreakable code if they share newly created identical strings of random bits, called *one-time codepads*. Suppose they both have such identical random strings. Alice can then take her message, in the form of a long string of 0's and 1's (obtained by translating her original text using some transparent, generally known binary code such as ASCII coding) and transform it into its bitwise modulo-2 sum (also called the *exclusive or* or XOR) with a random string of 0's and 1's of the same length taken from her one-time codepad. Flipping or not flipping each bit of a coherent message according to whether the corresponding bit of a random string is 0 or 1, converts the message into another random string. If this is not immediately evident, think of the process as flipping or not flipping each bit of the random string, according to whether the corresponding bit of the coherent message is 0 or 1.

There is no way anyone can reconstruct the original string without knowing the random string used to encode it. So only Bob, who does have a copy of that random string,

can decode the message. He can do this quite simply by taking the XOR of the now meaningless string of 0's and 1's he received from Alice with his copy of the same random string she used to do the encoding. The string he gets in this way is  $M \oplus S \oplus S$ , where  $M$  is the message,  $S$  is the random string, and  $M \oplus S$  is the encoded message from Alice. Since  $S \oplus S = 0$ , Bob has recovered the original message.

The problem with one-time codepads is that they can be used only once. If an eavesdropper (Eve) picks up two messages encoded with the same pad, she can take the XOR of the two encoded messages. The random string used to encode the two messages drops out of this process, leaving the XOR of the two unencoded messages. But the XOR of two meaningful messages, combined with the usual code-breaking tricks based on letter frequencies, can be used (with more sophistication than would be required for a single message) to separate and decode both texts. So to be perfectly secure Alice and Bob must continually refresh their one-time codepad with identical new random strings of bits.

The problem of exchanging such random strings in a secure way would appear to be identical to the original problem of exchanging meaningful messages in a secure way. But at this point quantum mechanics comes to the rescue, providing an entirely secure means for exchanging identical sequences of random bits. Pause to savour the strange character of this situation. Nobody has figured out how to exploit quantum mechanics to provide a secure means for directly exchanging meaningful messages. The secure exchange is possible only because the bit sequences are random. On the face of it one would think nothing could be more useless than such a transmission of noise. What is bizarre is that human ingenuity combined with human perversity has succeeded in inventing a context in which the need to hide information from a third party actually provides a purpose for such an otherwise useless exchange of random strings of bits.

The scheme for doing this is known as BB84 after its inventors, Charles Bennett and Gilles Brassard, who published the idea in 1984. Alice sends Bob a long sequence of Qbits in the form of photons, randomly chosen to be in one of four states: polarized horizontally (i.e. in the state  $|0\rangle$ ), polarized vertically (in the state  $|1\rangle$ ), polarized diagonally along  $45^\circ$  (in the state  $\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ), or polarized diagonally along  $-45^\circ$  (in the state  $\mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ). So for each photon Alice randomly chooses a polarization type (horizontal-vertical or diagonal) and within each type randomly chooses a polarization value — one of the two orthogonal states associated with that type of polarization.

For the rest of this discussion we revert from photon polarization language to our more familiar quantum computational language. We divide the four equally likely types of Qbits that Alice sends to Bob into two categories: those with states  $|0\rangle$  or  $|1\rangle$ , which we call type-1 Qbits, and those with state  $\mathbf{H}|0\rangle$  or  $\mathbf{H}|1\rangle$ , which we call type-H Qbits. As each Qbit arrives Bob randomly decides whether to send it directly through a measurement gate, or to apply a Hadamard and only then send it through a measurement gate. We call these two options type-1 and type-H measurements. The Qbits must be individually identifiable in a way that enables Bob and Alice to tell which is which way — for example by

the sequence in which they arrive — so that they can compare certain information about what each of them did to and knows about each individual Qbit.

When Bob has measured all the Qbits in this way, Alice tells him over an insecure channel which Qbits were type-1 and which were type-H. But she does not tell him which of the two states she prepared within each type. For those Qbits (about half of them) for which Bob's random choice of measurement type agreed with Alice's random choice of which type to send, Bob learns from the result of his measurement the actual randomly selected value — 0 or 1 — that Alice sent. For those Qbits (the other half) where Bob's choice of which type to measure disagreed with Alice's choice of which type to send, the result of his measurement reveals nothing about Alice's randomly selected value. This is illustrated in Figure 6.3.

Finally, Bob tells Alice, over an insecure channel, which of the Qbits he subject to a type of measurement that agreed with her choice of which type to prepare — i.e. which Qbits were of the kind that can provide them with identical random bits. They discard the half of their data associated with the useless Qbits for which Bob's type of measurement differed from Alice's type of preparation. They are then able to construct their one-time codepads from the identical strings of random bits they have acquired.

You might wonder why Bob doesn't wait to decide what type of measurement to make on each Qbit until he learns Alice's choice of type for that photon, thereby doubling the number of shared random bits. This would indeed be a sensible strategy if Bob could store the Qbits he received from Alice. However storing individual photons in a polarization-preserving manner is technologically difficult. For currently feasible quantum cryptography Bob must make his decision and measure the polarization of each photon as it arrives.

The reason they have to waste half of their Qbits is security against eavesdroppers. If Alice sent all Qbits of the same type and Bob always made that type of measurement so he always got a bit that agreed with Alice's (or if Alice sent with each Qbit classical information about its type), then an eavesdropper, Eve, could acquire the same information as Bob without being detected.

If, for example, Alice and Bob had agreed that all the Qbits would be type-1 and Eve learned of this, then she could intercept each Qbit before it reached Bob and send it directly through a measurement gate without altering its state, then sending it (or another Qbit she prepared in the state she just learned) on to Bob. In this way she could acquire exactly the same random bit that Alice sent out and that Bob subsequently acquires when he makes his own type-1 measurement. There is nothing to give Bob any hint that Eve was listening in.

By making each Qbit secretly and randomly of type-1 or type-H Alice deprives Eve of this strategy. The best Eve can do, like Bob, is to randomly make type-1 or type-H measurements. But in doing so she necessarily reveals her presence. Bob and Alice can determine that Eve has compromised the security of their bits by using the same protocol as before, but sacrificing some of the identical random bits they extracted from the Qbits

that they both ended up treating in the same way.

They take a sample of these bits and check (over an insecure channel) to see whether they actually do agree, as they will in the absence of eavesdropping. If Eve was intercepting the Qbits, randomly making type-1 or type-H measurements of her own before sending them on to Bob, then for about half of the useful Qbits her choice will differ from the common choice of Alice and Bob. In about half of *those* cases, Eve's intervention will result in the outcome of Bob's measurement disagreeing with what Alice sent him. If, for example, Eve makes a type-1 measurement of a Qbit that Alice has prepared in the state  $\mathbf{H}|0\rangle$ , then she will necessarily change its state to one or the other of the two states  $|0\rangle$  or  $|1\rangle$ . In either case if Bob then applies a Hadamard before measuring he will get the result 0 only half the time.

So if Eve is systematically intercepting Qbits, Bob's result will fail to agree with Alice's preparation for about a quarter of their sample data. This warns them that the transmission was insecure. If all the sample data agrees except for some tiny fraction, then they can set an upper limit to the fraction that Eve might have picked up, enabling them to make an informed judgment of the security with which they can use the remaining ones.

One might wonder whether Eve could do better by a more sophisticated attack, that involved capturing each of Alice's Qbits and processing it in a quantum computer that restored it to its initial state, before sending it on to Bob. This would eliminate the possibility of her eavesdropping being revealed to Bob. But the requirement that Alice's Qbit be returned to its initial state also eliminates the possibility of Eve learning anything useful.

To see this, let  $|\phi_\mu\rangle$ ,  $\mu = 0 \dots 3$ , be the four possible states of Alice's Qbit:  $|0\rangle$ ,  $|1\rangle$ ,  $\mathbf{H}|0\rangle$ , and  $\mathbf{H}|1\rangle$ . Let  $|\Phi\rangle$  be the initial state of the  $n$  Qbits in Eve's computer, and let  $\mathbf{U}$  be the  $(n + 1)$ -Qbit unitary transformation the computer executes on its own Qbits and Alice's. Since Alice's Qbit must emerge in its original state, we have

$$\mathbf{U}\left(|\phi_\mu\rangle \otimes |\Phi\rangle\right) = |\phi_\mu\rangle \otimes |\Psi_\mu\rangle. \quad (6.6)$$

Eve's hope is to devise a  $\mathbf{U}$  that yields four  $|\Psi_\mu\rangle$  whose differences enable her by subsequent processing and measurement to extract useful information about which of the four possible states  $|\phi_\mu\rangle$  was. This, however, is impossible. Because neither  $|\phi_0\rangle$  nor  $|\phi_1\rangle$  are orthogonal to  $|\phi_2\rangle$  or  $|\phi_3\rangle$  one can easily show that all four  $|\Psi_\mu\rangle$  must be identical.

This follows from the unitarity of  $\mathbf{U}$ . Unitary transformations preserve inner products, and therefore the inner product of any two input states to Eve's computation must be the same as the inner product of the two corresponding output states. We therefore have

$$\langle\phi_\nu|\phi_\mu\rangle\langle\Phi|\Phi\rangle = \langle\phi_\nu|\phi_\mu\rangle\langle\Psi_\nu|\Psi_\mu\rangle. \quad (6.7)$$

Because  $\langle\Phi|\Phi\rangle = 1$  and because  $\langle\phi_\nu|\phi_\mu\rangle \neq 0$  for  $\mu\nu = 02, 03, 12, 13$ , it follows that

$$\langle\Psi_\nu|\Psi_\mu\rangle = 1, \quad \mu\nu = 02, 03, 12, 13. \quad (6.8)$$

But the inner product of two normalized states can be 1 only if they are identical, so it follows from (6.8) that

$$|\Psi_0\rangle = |\Psi_1\rangle = |\Psi_2\rangle = |\Psi_3\rangle. \quad (6.9)$$

The price Eve pays for eliminating all traces of her eavesdropping is that she can learn, from the resulting state of her quantum computer, nothing whatever about the four possible states of Alice's Qbit.

There is a less practical (but more elegant) version of this cryptographic protocol that appears, at first sight, to be different, but turns out to be exactly the same. Suppose there were some central source that produced pairs of Qbits in the entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad (6.10)$$

and then sent one member of each pair to Alice and the other to Bob. One easily verifies that

$$(\mathbf{H} \otimes \mathbf{H}) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \quad (6.11)$$

Therefore if Alice and Bob make measurements of the same type, they will get the same results.

This might appear to be even more secure than the first protocol, since the Qbits are in an entangled state until Alice or Bob actually makes a measurement. The correlated bits — the outcomes of the measurement — do not even *exist* until such a moment, and that moment does not happen until both Qbits are safely in their separate possession. But this is only the case if Eve does not intercept a Qbit. If she does measure one before it gets to Bob or Alice, then the correlated bits do come into existence at the moment of her measurement. This is later than in the first protocol (when each bit exists the moment Alice performs her own measurement) but early enough to help Eve in the same way as before.

If Alice and Bob decided to produce their perfectly correlated random bits by always making type-1 measurements then if Eve finds this out she can intercept one member of the pair with type-1 measurements of her own, disentangling the state prematurely, but in a way that enables her to learn what each random bit is, while not altering the the perfect correlations between the values Alice and Bob will subsequently measure. Alice and Bob can guard against this possibility by each randomly (and, necessarily, independently) alternating between type-1 and type-H measurements, and then following a procedure identical to the one they used when Alice sent Bob Qbits in definite states.

This gets us back to the original protocol that made no use of entangled pairs. Indeed, if Alice measures her member of the entangled pair (making either a type-1 or type-H measurement) before Bob measures his, this is completely equivalent to her sending Bob a Qbit with a randomly selected state that she knows. The only difference is that now the random choice of which of the two states to send within each type is not made by

her tossing a coin, but by the basic laws of quantum mechanics that guarantee that the outcome of her own measurement is random.

## B. Bit commitment

One can try to formulate a similar protocol for a procedure called bit commitment. Suppose Alice wishes to assure Bob that she has made a binary decision by a certain date, but does not wish to reveal that decision until some future time. She can do this by writing YES or NO on a card, putting the card in a box, locking the box, and sending the box, but not the key to Bob. Once the box is in Bob's possession he can be sure that Alice has not altered her decision, but while the key is in Alice's possession she can be sure that Bob has not learned what that decision was. When it is time for her to reveal the decision she sends the key to Bob who opens the box and learns what it was.

Of course Alice might worry about Bob breaking into the box by other means. Quantum mechanics offers a more secure procedure (but with a loophole, which we return to momentarily.) Alice prepares a large number  $n$  of labeled Qbits. If her answer is YES, she takes each Qbit to be randomly in the state  $|0\rangle$  or the state  $|1\rangle$ . If her answer is NO she prepares each Qbit randomly in the state  $\mathbf{H}|0\rangle$  or  $\mathbf{H}|1\rangle$ . In either case she notes which Qbits are in which state, and then sends them all off to Bob, who stores them in a way that preserves both their state and their labels.

Now if Bob has a collection of  $N$  Qbits, each of which has been chosen with equal probability to be in one of two orthogonal states  $|\phi\rangle$  or  $|\psi\rangle$ , then there is no way for Bob to get any hint of what  $|\phi\rangle$  and  $|\psi\rangle$  are, for if he measures every pair then the probabilities of getting 0 or 1 are given by

$$p(0) = 1 - p(1) = \frac{1}{2}|\langle 0|\phi\rangle|^2 + \frac{1}{2}|\langle 0|\psi\rangle|^2. \quad (6.12)$$

But

$$|\langle 0|\phi\rangle|^2 + |\langle 0|\psi\rangle|^2 = 1, \quad (6.13)$$

since this is the sum of the squared moduli of the amplitudes of the expansion of  $|0\rangle$  in the basis given by  $|\phi\rangle$  and  $|\psi\rangle$ :

$$|0\rangle = |\phi\rangle\langle\phi|0\rangle + |\psi\rangle\langle\psi|0\rangle. \quad (6.14)$$

Therefore  $p(0) = p(1) = \frac{1}{2}$ , and Bob's measurement outcomes are completely random, independent of what the orthogonal pair of states actually is. The same conclusion holds if he applies a unitary transformation  $\mathbf{U}$  to each Qbit before his measurement — i.e. if he measures in a basis other than the computational basis — since  $\mathbf{U}|\phi\rangle$  and  $\mathbf{U}|\psi\rangle$  are also orthogonal. So the statistics of any measurements Bob can perform on a collection of Qbits, each of which has a 50-50 chance of being in the state  $|0\rangle$  or  $|1\rangle$ , are indistinguishable from the statistics he would get if each had a 50-50 chance of being in the state  $\mathbf{H}|0\rangle$  or  $\mathbf{H}|1\rangle$ . There is no way Bob can learn Alice's choice by measuring the Qbits Alice has sent him.

It is important for this indistinguishability that Alice send Bob a collection of Qbits each of whose two possible states was selected randomly. If, on the contrary, she sent him *exactly*  $\frac{1}{2}N$  Qbits in the state  $|0\rangle$  and  $\frac{1}{2}N$  in the state  $|1\rangle$ , in some random order, then with probability 1 Bob would get an equal number of 0's and 1's if he measured in the computational basis. But if he applied  $\mathbf{H}$  before measuring, the outcome of each measurement would be random, and the probability of getting equal numbers of 0's and 1's for his measurements would be quite small (asymptotically  $\sqrt{2/\pi N}$  for large  $N$ ). Therefore if he found equal numbers he could be rather sure that Alice had sent him photons in the states  $|0\rangle$  and  $|1\rangle$  rather than in the states  $\mathbf{H}|0\rangle$  and  $\mathbf{H}|1\rangle$ .

When the time comes for Alice to reveal her choice for the pair of orthogonal states, she says to Bob something like this: My answer was YES, so each of the Qbits I sent you was either in the state  $|0\rangle$  or  $|1\rangle$ . To prove this I will now tell you that I put Qbits 1, 2, 4, 6, 7, 11, . . . into the state  $|0\rangle$  and I put Qbits 3, 5, 8, 9, 10, 12. . . into the state  $|1\rangle$ . You can confirm that I'm telling the truth by measuring  $\mathbf{Z}$  on each of them. Here Alice uses the language in which a measurement in the computational basis is referred to as "measuring  $\mathbf{Z}$ " while a measurement in the computational basis preceded by an application of  $\mathbf{H}$  is referred to as "measuring  $\mathbf{X}$ ".

Bob makes the measurements and gets every one of Alice's predicted outcomes. If Alice had instead sent him Qbits whose states were randomly  $\mathbf{H}|0\rangle$  or  $\mathbf{H}|1\rangle$  she could do the same trick for  $\mathbf{X}$  measurements. But there is no way she could do the trick for  $\mathbf{X}$  measurements in the first case or for  $\mathbf{Z}$  measurements in the second. The best she could do if she wanted to deceive Bob would be to make random guesses for each outcome, and with  $n$  Qbits she would succeed only with probability  $1/2^n$ . So this works perfectly well, and without the worry of Bob possessing unexpected safe-cracking skills.

But as I warned above, there is a fatal problem. The technological skills required to take advantage of this loophole are spectacularly greater than those required for the naive protocol, so one could imagine a stretch of years or decades when the naive protocol might actually be useful, but ultimately it will be insecure. Suppose Alice cheats and, unknown to Bob, prepares  $n$  labeled entangled pairs in the state (6.11), sending one member to Bob while retaining the other for herself. Then in actual fact the Qbits Bob received would have no states of their own, being entangled with the Qbits Alice kept for herself. Nevertheless, if Bob chose to test some of them with measurements, the statistics he got would be indistinguishable from those he would have got if Alice had been playing the game honestly. No hint of her deception will be revealed by any test Bob can perform.

Now when the time comes for Alice to reveal her choice, if she wants to prove to Bob that it was YES, she measures  $\mathbf{Z}$  on each of the Qbits she has kept and correctly informs Bob what he will get if he measures  $\mathbf{Z}$  on each of the paired Qbits. But if she wants to prove that it was NO, she instead measures  $\mathbf{X}$  on each of her Qbits. In this way she can use entangled pairs of Qbits to cheat at what would otherwise be a perfectly secure bit-commitment protocol.

She can cheat in the same way even if Bob measures  $\mathbf{Z}$  or  $\mathbf{X}$  randomly on his Qbits before she “reveals” her commitment. If she wants to “prove” to Bob she had sent him YES she measures  $\mathbf{Z}$  on each of her Qbits and tells Bob all her results. He notes that they do indeed agree with all the results he found for his  $\mathbf{Z}$  measurements, and is persuaded that she had indeed sent him YES.

Of course the success of Alice’s cheating depends crucially on Bob’s knowing all about one-Qbit states, but never having had the kind of course in quantum mechanics that taught him anything about entangled two-Qbit states. If Bob is as sophisticated a student of the quantum theory as Alice, they will both realize that the protocol is fatally flawed, since it can be defeated by entanglement.

It is in this context that Einstein’s famous complaint about spooky actions at a distance (“*spukhafte Fernwirkungen*”) seems particularly compelling. By finally measuring her members of the entangled pairs, Alice seems to convert the distant Qbits in Bob’s possession into the kind she deceptively said she had sent him long ago, while retaining until the last minute the option of which of the two kinds to pick. But of course Alice’s action is not so much on the Qbits in Bob’s possession as it is on what it is possible for her to *tell him* about those Qbits. It is this peculiar tension between the objective (ontology) and what is known (epistemology) that makes quantum mechanics such a source of delight (or anguish) to the philosophically inclined.

Something like Alice’s discovery of the value of entanglement for cheating actually happened in the historical development of these ideas about quantum information processing. When the bit-commitment protocol described above was first put forth it was realized that entangled pairs could be used to thwart it, but more sophisticated versions were proposed that were believed to be immune to cheating with entanglement. There developed a controversy over whether some form of bit commitment could or could not be devised that would be secure even if entanglement were fully exploitable. The current consensus is that there is no way to use Qbits in a bit-commitment protocol that cannot be defeated by using entangled states. Indeed, it has even been suggested that some clever person might try to prove that the structure of quantum mechanics was uniquely specified by requiring it to lead to the kind of physics that enables the secure exchange of random strings of bits, as in quantum cryptography, but does not enable bit commitment. As far as I know nobody has taken up this challenge. It does seem implausible that God would have taken as a fundamental principle of design that certain kinds of covert activity should be possible while others should be forbidden.

### C. Quantum dense coding

Although an infinite amount of information is required to specify the state  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  of a single Qbit, there is no way for somebody who has acquired possession of the Qbit to learn what that state is, as we have often noted. If Alice prepares a Qbit in the state  $|\psi\rangle$  and sends it to Bob, all he can do is apply a unitary transformation of his

choice and then measure the Qbit, getting the value 0 or 1 — just one bit of information. After that the state of the Qbit is either  $|0\rangle$  or  $|1\rangle$  and no further measurement can teach him anything about its original state  $|\psi\rangle$ . The most Alice can communicate to Bob in this way is a single bit of information.

If, however, Alice has one member of an entangled pair of Qbits in the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \quad (6.15)$$

and Bob has the other, then by suitably preparing her member of the pair and then sending it to Bob, she can convey to him *two* bits of information. She does this by first applying the transformation  $\mathbf{1}$ ,  $\mathbf{X}$ ,  $\mathbf{Z}$ , or  $\mathbf{ZX}$  to her Qbit, depending on whether she wants to send Bob the message 00, 01, 10, or 11. If hers is the Qbit on the left in (6.15) these transform the state of the pair into one of the four mutually orthogonal states, called the Bell basis (after John S. Bell):

$$\begin{aligned} \mathbf{1}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \\ \mathbf{X}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|1\rangle|0\rangle + |0\rangle|1\rangle), \\ \mathbf{Z}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle), \\ \mathbf{Z}_a\mathbf{X}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \end{aligned} \quad (6.16)$$

She then sends her Qbit over to Bob. He applies to the pair the controlled-NOT transform  $\mathbf{cX}_{ab}$  using the Qbit he received from Alice as control, to get

$$\begin{aligned} \mathbf{cX}_{ab}\mathbf{1}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle, \\ \mathbf{cX}_{ab}\mathbf{X}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle, \\ \mathbf{cX}_{ab}\mathbf{Z}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|0\rangle, \\ \mathbf{cX}_{ab}\mathbf{Z}_a\mathbf{X}_a|\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|1\rangle, \end{aligned} \quad (6.17)$$

and then he applies a Hadamard transform to get

$$\begin{aligned} \mathbf{H}_a\mathbf{cX}_{ab}\mathbf{1}_a|\Psi\rangle &= |0\rangle|0\rangle, \\ \mathbf{H}_a\mathbf{cX}_{ab}\mathbf{X}_a|\Psi\rangle &= |0\rangle|1\rangle, \\ \mathbf{H}_a\mathbf{cX}_{ab}\mathbf{Z}_a|\Psi\rangle &= |1\rangle|0\rangle, \\ \mathbf{H}_a\mathbf{cX}_{ab}\mathbf{Z}_a\mathbf{X}_a|\Psi\rangle &= |1\rangle|1\rangle. \end{aligned} \quad (6.18)$$

Measuring the two Qbits then gives him 00, 01, 10, or 11 — precisely the two-bit message Alice wished to send. This process of transforming the Bell basis into the computational basis and then measuring, is called “measuring in the Bell basis.”

One can directly demonstrate that this works with circuit diagrams, without going through any of the analysis in (6.15)-(6.18). Suppose Alice represents the two bits  $x$  and  $y$  she wishes to transmit to Bob as the computational basis state  $|x\rangle|y\rangle$  of two Qbits (top

two wires, Fig. 6.4(a)). If Bob has two Qbits initially in the state  $|0\rangle|0\rangle$  (bottom two wires in Fig. 6.4(a)), then the circuit in Fig. 6.4(a) gets the two bits to Bob in a straightforward classical way, transforming the state  $|x\rangle|y\rangle|0\rangle|0\rangle$  on the right to  $|x\rangle|y\rangle|x\rangle|y\rangle$  on the left by means of direct Qbit-to-Qbit coupling via two cNOT gates. The procedure involves only classical operations on classically meaningful states.

But now one can introduce quantum gates, beginning with the expansion of one of the  $\mathbf{cX}$  into  $\mathbf{HcZH}$  in Fig. 6.4(b). Note next that because the computational basis states are eigenstates of  $\mathbf{Z}$ , when  $\mathbf{Z}$  acts on the control Qbit of a  $\mathbf{cX}$ , the two operators commute. Since  $\mathbf{cX}$  is its own inverse, we can further expand Fig. 6.4(b) to Fig. 6.4(c). We can then bring the  $\mathbf{H}$  and  $\mathbf{cX}$  gates on either side of the  $\mathbf{cZ}$  to the extreme left and right to get Fig. 6.4(d).

We can also expand the two  $\mathbf{cX}$  gates on the right of Fig. 6.4(d) into the three  $\mathbf{cX}$  gates on the right of Fig. 6.4(e), since the action of either set is to flip the target Qbit if and only if the computational basis states of the two control Qbits are different, while leaving the states of the control Qbits unaltered. Because the state  $\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  is invariant under the action of  $\mathbf{X}$ , the  $\mathbf{cX}$  on the extreme right acts as the identity, and Fig. 6.4(e) simplifies to Fig. 6.4(f). The fact that Fig. 6.4(f) has the same action as Fig. 6.4(a) contains all the content of the dense-coding protocol:

The two gates  $\mathbf{cX}_{23}\mathbf{H}_2$  on the right of Fig. 6.4(f) act on the state  $|0\rangle|0\rangle$  to produce the entangled state (6.15). The bottom Qbit of the pair, #3, is given to Bob and the upper one, #2, is given to Alice, who also possesses the upper two, #0 and #1. The two gates  $\mathbf{cZ}_{02}\mathbf{cX}_{12}$  act as  $\mathbf{1}, \mathbf{X}, \mathbf{Z}$ , or  $\mathbf{ZX}$  on Qbit #2 depending on whether the states of Qbits #0 and #1 are  $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle$ , or  $|1\rangle|1\rangle$ . This reproduces the transformation Alice applies to the member of the entangled pair in her possession, depending on the values of the two bits she wishes to transmit to Bob. Alice then sends Qbit #2 to Bob. The final  $\mathbf{H}_2\mathbf{cX}_{23}$  on the left is precisely the transformation (6.18) that Bob performs on the reunited entangled pair before making his measurement, which yields the values  $x, y$  that Alice wished to transmit.

Like dense coding, many tricks of quantum information theory, including the one we examine next, teleportation, rely on two or more people sharing entangled Qbits, prepared some time ago, carefully stored in their remote locations awaiting an occasion for their use. While the preparation of entangled Qbits (in the form of photons) and their transmission to distant places has been achieved, as far as I know there has been no progress in putting them into entanglement-preserving, local, long-term storage.

## D. Teleportation

Suppose Alice has a Qbit in a general state

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle. \quad (6.19)$$

She does not, in general, know the amplitudes  $a_0$  and  $a_1$ . Carol, for example, may have prepared the Qbit for Alice by first applying a unitary transformation to a Qbit initially

in the standard state  $|0\rangle$  and then sending the output Qbit to Alice without telling her what she did to prepare it.

Alice would like to reassign that precise state to another Qbit possessed by Bob. Neither Alice nor Bob (who could be far away from Alice) has any access to the other's Qbit. Alice is, however, allowed to send "classical information" to Bob — e.g. she can talk to him over the telephone. And, most importantly, Alice and Bob again share a pair of Qbits in the entangled state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle). \quad (6.20)$$

The no-cloning theorem prohibits the duplication of the unknown state of Alice's Qbit, either far away from her or nearby. But it turns out to be possible, and does not violate that theorem, for Alice and Bob to cooperate over the telephone to transform the state of Bob's Qbit from  $|0\rangle$  to  $|\psi\rangle$  provided Alice is willing to obliterate all traces of its former state from her own Qbit. The term "teleportation" is apt, because the state that is newly associated with Bob's far away Qbit must necessarily cease to be associated with Alice's.

The initial 3-Qbit state of the Alice's special Qbit and the entangled pair she shares with Bob is

$$(a|0\rangle_a + b|1\rangle_a) \frac{1}{\sqrt{2}} (|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b), \quad (6.21)$$

where I have given the state symbols for the Qbits in Alice's possession a subscript  $a$ , and the state symbols for the Qbit in Bob's possession the subscript  $b$ . To teleport the unknown state of her special Qbit to Bob's member of the entangled pair Alice first applies a **cX** gate using her special Qbit as the control and her member of the entangled pair as the target. This produces the state

$$a|0\rangle_a \frac{1}{\sqrt{2}} (|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) + b|1\rangle_a \frac{1}{\sqrt{2}} (|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b). \quad (6.22)$$

Next she applies a Hadmard transformation **H** to her special Qbit (on the left in (6.22)), which puts all three Qbits into the state

$$\begin{aligned} a \frac{1}{\sqrt{2}} (|0\rangle_a + |1\rangle_a) \frac{1}{\sqrt{2}} (|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b) + b \frac{1}{\sqrt{2}} (|0\rangle_a - |1\rangle_a) \frac{1}{\sqrt{2}} (|1\rangle_a|0\rangle_b + |0\rangle_a|1\rangle_b) = \\ \frac{1}{2} |0\rangle_a |0\rangle_a (a|0\rangle_b + b|1\rangle_b) + \frac{1}{2} |1\rangle_a |0\rangle_a (a|0\rangle_b - b|1\rangle_b) + \\ \frac{1}{2} |0\rangle_a |1\rangle_a (a|1\rangle_b + b|0\rangle_b) + \frac{1}{2} |1\rangle_a |1\rangle_a (a|1\rangle_b - b|0\rangle_b). \end{aligned} \quad (6.23)$$

Alice now measures the two Qbits in her possession. (As noted earlier, such application of **cX** and **H** gates immediately followed by measurement gates is called "measuring in the Bell basis.") If the result is 00, Bob's Qbit (on the right) will indeed be projected into the state (6.19) originally possessed by Alice's Qbit (whose state would then be reduced to  $|0\rangle$ ). But if the result of Alice's measurement is 10, 01, or 11 then the state of Bob's Qbit becomes

$$a|0\rangle_b - b|1\rangle_b, \quad a|1\rangle_b + b|0\rangle_b, \quad \text{or} \quad a|1\rangle_b - b|0\rangle_b. \quad (6.24)$$

Note that in each of these three cases there is a unitary transformation that restores the state of Bob's Qbit to Alice's original (unknown) state (6.19). In the first case we can apply  $\mathbf{Z}$ , (which leaves  $|0\rangle$  alone but changes the sign of  $|1\rangle$ ), in the second case,  $\mathbf{X}$  (which interchanges  $|0\rangle$  and  $|1\rangle$ ), and in the third case,  $\mathbf{ZX}$ .

So all Alice need do to transfer the state of her Qbit to Bob's member of their entangled pair is to telephone Bob and report to him the results of her two measurements. He then knows whether the state has already been transferred (if Alice's result is 00) or what unitary transformation he must apply to his member of the entangled pair in order to complete the transfer (if Alice's result is one of the other three.) This is very similar to the error correction procedures described in Chapter 5. By making a measurement Alice acquires the information necessary to reconstruct a particular quantum state without acquiring any information about what that state actually is.

Note what has been achieved. An unknown state of a Qbit is described by two complex numbers  $a$  and  $b$  taking on a continuum of values, constrained only by the requirement that  $|a|^2 + |b|^2 = 1$ . Yet, with the aid of an entangled pair, Alice is able to provide Bob with a Qbit described by this state, at the price of only two bits of classical information (giving the results of her two measurements) and the loss of the entanglement of their carefully preserved entangled pair.

Of course the teleportation process does not communicate to Bob anything close to all the information that can be encoded in  $a$  and  $b$ . Bob is no more able to learn the values of  $a$  and  $b$  from manipulating his Qbit, now guaranteed to be in the the state  $|\psi\rangle$ , than Alice was able to do when it was her Qbit that was in the same state  $|\psi\rangle$ . On the other hand Alice's state could be produced at a crucial stage of an elaborate quantum computation, and its transference to Bob could enable him to continue with the computation on his own faraway quantum computer, so one can achieve a nontrivial objective by such teleportations.

Like dense coding, teleportation can also be constructed by manipulating an elementary classical circuit diagram, without going through any of the analysis in (6.21)-(6.24). Fig. 6.5(a) shows an elementary classical circuit that obviously works whether  $|\psi\rangle = |0\rangle$  or  $|\psi\rangle = |1\rangle$ . As a quantum circuit it therefore works for arbitrary superpositions,  $|\psi\rangle = a|0\rangle + b|1\rangle$ . Such a circuit can clearly be used to transfer an unknown state  $|\psi\rangle$  from Alice's Qbit (upper wire) to Bob's (lower wire). The entire teleportation protocol can be constructed by appropriately expanding the two gates in Fig. 6.5(a), with the aid of an ancillary Qbit.

In Fig. 6.5(b) the ancillary Qbit Qbit, unacted upon throughout the process, is introduced in the state

$$|\phi\rangle = \mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (6.25)$$

In Fig. 6.5(c) the identities  $\mathbf{X} = \mathbf{HZH}$  and  $\mathbf{1} = \mathbf{HH}$  have been used to rewrite the  $\mathbf{cX}$  gate on the left of Fig. 6.5(b), and an additional  $\mathbf{cX}$  gate has been added on the right, which acts as the identity, since  $\mathbf{X}$  acts as the identity on the state (6.25).

Fig. 6.5(d) follows from Fig. 6.5(c) because the action of  $\mathbf{cZ}$  is independent of which

Qbit is the control and which, the target, and because the two  $\mathbf{cX}$  gates on the right of Fig. 6.5(c) have exactly the same action as the three  $\mathbf{cX}$  gates on the right of Fig. 6.5(d): acting on the computational basis both sets of gates apply  $\mathbf{X}$  on both of the bottom two wires if the state of the top wire is  $|1\rangle$  and act as the identity if the state of the top wire is  $|0\rangle$ .

Fig. 6.5(e) follows from Fig. 6.5(d) by explicitly writing the  $|\phi\rangle$  on the right of Fig. 6.5(d) as  $\mathbf{H}|0\rangle$  and explicitly writing the  $|0\rangle$  on the left of Fig. 6.5(d) as  $\mathbf{H}|\phi\rangle$ . But Fig. 6.5(e) is an automated version of teleportation. To see this introduce measurements (represented by the squares with  $M$  inside them) of the upper two Qbits after the circuit of Fig. 6.5(e) has acted, as in Fig. 6.5(f). Their effect is to collapse the states of each of the two upper wires randomly and independently to  $|0\rangle$  or  $|1\rangle$ . But as noted in Chapter 4, measurement of a control Qbit commutes with any operation controlled by that Qbit, so the measurement gates can be moved to the positions they occupy in Fig. 6.5(g).

Fig. 6.5(g) is precisely the teleportation protocol. The two gates on the right transform the two lower Qbits into the entangled state (6.20). The subsequent applications to the top two Qbits of  $\mathbf{cX}$  followed by  $\mathbf{H}$  are exactly as described above in (6.21)-(6.23). These are followed by measurements of the top two Qbits. Since Alice knows the outcomes of the measurements, she knows whether the subsequent  $\mathbf{cX}$  and  $\mathbf{cZ}$  gates will or will not act, and can replace these physical couplings by a phone call to Bob telling him whether or not directly to apply  $\mathbf{X}$  and/or  $\mathbf{Z}$  to his own Qbit.

Figure 6.6 demonstrates that entanglement can also be teleported. The figure reproduces parts (b), (e), and (g) of Figure 6.5 with two changes. (1) A fourth bundle of  $n$  wires in the  $n$ -Qbit state  $|\Phi\rangle_i$  has been added above each part of the figure. No operations act on these wires. (2) The state to be teleported has been given a subscript  $i$  so it is now  $|\psi_i\rangle$ . The steps from (b) to (e) to (g) in Figure 6.5 clearly are unaffected by these changes.

Because of the linearity of the unitary gates the identity between Fig. 6.5(a) and Fig. 6.5(b) continues to hold if one sums over many values of the index  $i$ , demonstrating that the effect of the circuits in (a) or (b) is to transfer participation in the entangled state  $\sum_i |\Phi_i\rangle |\psi_i\rangle$  from the third wire from the bottom to the bottom wire. Because the final states of the second and third wires from the bottom in (b) are completely disentangled from the state of the other Qbits, the replacement of the two controlled gates on the left by measurement followed by classical communication in Fig. 6.6(c) also continues to be valid.

So even if Alice's Qbit has no state of its own but is entangled with other Qbits, Alice can teleport its role in the entangled state over to Bob's Qbit resulting in Bob's Qbit being entangled in exactly the same way Alice's was, and Alice's Qbit becoming entirely unentangled. If, for example, Alice shares pairs of Qbits in the entangled state (6.20) with both Carol and Bob, then by local operations on the two Qbits in her possession and the communication of two bits of classical information, she can create the entangled state (6.20) between Carol's Qbit and Bob's. After this is done her own Qbit is completely unentangled with either of the other two.

## E. The GHZ state

I conclude with an elementary but striking reminder of just how strange the behavior of Qbits can be. The possibility of such behavior was first pointed out in a rather different context by Daniel Greenberger, Michael Horen, and Anton Zeilinger (“GHZ”) in the late 1980’s. Here is a Qbit version:

Consider the 3-Qbit state

$$|\Psi\rangle = \frac{1}{2}(|000\rangle - |110\rangle - |101\rangle - |011\rangle). \quad (6.26)$$

Note that the form of  $|\Psi\rangle$  is explicitly invariant under any permutation of the three Qbits. Numbering the Qbits from left to right 2, 1, and 0, one easily confirms that  $|\Psi\rangle$  can be written in either of the alternative forms

$$|\Psi\rangle = \mathbf{Z}_1 \mathbf{C}_{21} \mathbf{H}_2 \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \mathbf{Z}_2 \mathbf{C}_{12} \mathbf{H}_1 \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad (6.27)$$

(or any of the four other forms associated with permutations of the subscripts 0,1, and 2.) Since

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \mathbf{C}_{21} \mathbf{C}_{20} \mathbf{H}_2 |000\rangle \quad (6.28),$$

(6.27) and (6.28) provide an explicit way to construct  $|\Psi\rangle$  by operating on  $|0\rangle_3$  with elementary gates.

Note next that

$$\mathbf{H}_2 \mathbf{H}_1 |\Psi\rangle = \mathbf{H}_2 \mathbf{H}_1 \left( \mathbf{Z}_1 \mathbf{C}_{21} \mathbf{H}_2 \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \right) = \mathbf{X}_1 [\mathbf{H}_2 \mathbf{H}_1 \mathbf{C}_{21} \mathbf{H}_2 \mathbf{H}_1] \mathbf{H}_1 \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \quad (6.29)$$

Since the quantity in brackets is just  $\mathbf{C}_{12}$ , a comparison of the forms on the right in (6.29) and (6.27) reveals that

$$\mathbf{H}_2 \mathbf{H}_1 |\Psi\rangle = \mathbf{Z}_2 \mathbf{X}_1 |\Psi\rangle. \quad (6.30)$$

Because of the invariance of  $|\Psi\rangle$  under permutation of the three Qbits we also have

$$\mathbf{H}_2 \mathbf{H}_0 |\Psi\rangle = \mathbf{Z}_2 \mathbf{X}_0 |\Psi\rangle, \quad (6.31)$$

$$\mathbf{H}_1 \mathbf{H}_0 |\Psi\rangle = \mathbf{Z}_1 \mathbf{X}_0 |\Psi\rangle. \quad (6.32)$$

Suppose we prepare three Qbits in the state  $|\Psi\rangle$  using the sequence of gates specified in (6.28) and (6.27) and then allow no further interactions among them. If we now measure each Qbit, it follows from the form (6.26) that because  $|\Psi\rangle$  is a superposition of computational basis states having either 0 or 2 of the Qbits in the state  $|1\rangle$ , the three outcomes are constrained to satisfy

$$x_2 \oplus x_1 \oplus x_0 = 0 \quad (6.33)$$

(where  $\oplus$ , as usual, denotes addition modulo 2.)

Suppose, on the other hand, we apply Hadamards to Qbits #2 and #1 before measuring all three. According to (6.30) this has the effect of flipping the state of Qbit #1 in the superposition (6.26) (and changing the sign of some of the terms). As a result the 3-Qbit state (6.26) is changed into a superposition of computational basis states having either 1 or 3 of the Qbits in the state  $|1\rangle$ . So if the outcomes are  $x_2^H$ ,  $x_1^H$  and  $x_0$ , we must have

$$x_2^H \oplus x_1^H \oplus x_0 = 1. \quad (6.34)$$

Similarly if we apply Hadamards to Qbits #2 and #0 before measuring all three, the outcomes must obey

$$x_2^H \oplus x_1 \oplus x_0^H = 1, \quad (6.35)$$

and if Hadamards are applied to Qbits #1 and #0 and then all three are measured we will have

$$x_2 \oplus x_1^H \oplus x_0^H = 1. \quad (6.36)$$

Consider now the following question: If we are talking about a single trio of Qbits in the state  $|\Psi\rangle$ , must the  $x_0$  appearing in (6.33) be the same as the  $x_0$  appearing in (6.34)? A little reflection reveals that this question makes no sense. After all, (6.33) describes the outcomes of immediately measuring the three Qbits, while (6.34) describes the outcomes of measuring them after Hadamards have been applied to Qbits #2 and #1. Since only one of these two possibilities can actually be carried out, there is no way to compare the result of measuring Qbit #0 in both cases. You can't compare the  $x_0$  you found in the case you actually carried out with the  $x_0$  you might have found in the case you didn't carry out. It's just a stupid question.

Or is it? Suppose Qbits #2 and #1 are measured before Qbit #0. If no Hadamards were applied before those measurements then (6.33) assures us that when #0 is finally measured the result will be

$$x_0 = x_1 \oplus x_2. \quad (6.37)$$

So the outcome of measuring #0 is predetermined by the outcomes of the earlier measurements of #1 and #2. Since all interactions among the Qbits ceased after the state  $|\Psi\rangle$  was prepared, subjecting #1 and #2 to measurement gates can have no effect on #0. If the outcomes of the measurements of #1 and #2 determine (as they do) the outcome of the subsequent measurement of #0, this can only be because they reveal that #0 was already predisposed to give the result (6.37) upon being itself measured. And because the Qbits do not interact, #0 must have had that predisposition even before #1 and #2 were actually measured to reveal what the result of measuring #0 would have to be.

This is a bit disconcerting, since prior to any measurements the Qbits were in the state  $|\Psi\rangle$  in which none of them are individually predisposed to reveal any particular value. Indeed, we seem forced to conclude that the 3-Qbit state  $|\Psi\rangle$  gives an *incomplete* description of the three Qbits. The omitted predisposition of #0 is an additional *element*

of reality that a more complete description than afforded by the quantum theory would take into account.

Suppose all this is true, so that Qbit #0 has a predetermined value even before Qbits #1 and #2 are measured to reveal what that value actually is. Then that predetermined value cannot be altered if Hadamards are applied to Qbits #1 and #2 before they are measured. For the Qbits have ceased to interact, and the predetermined value of #0 is already present before the decision whether or not to apply Hadamards has been made.

So if all this highly plausible reasoning is correct, then the value  $x_0$  appearing in (6.33) must indeed be identical to the value of  $x_0$  appearing in (6.34). The question is not meaningless. The answer is Yes!

Such an argument for elements of reality — predetermined values — was put forth in 1935 (in a different context) by Albert Einstein, Boris Podolsky, and Nathan Rosen (EPR). The controversy and discussion it has given rise to has steadily increased over the past 7 decades. The terms “incomplete” and “element of reality” originated with EPR. Today it is Einstein’s most cited paper.

The wonderful thing about three Qbits in the GHZ state is that they not only provide a beautiful illustration of the EPR argument, but also, when examined further, their behavior reveals that that the argument for predetermined values cannot be correct. To see this note that exactly the same reasoning establishes that the values of  $x_1$  appearing in (6.33) and (6.35) must be the same, as well as the values of  $x_2$  appearing in (6.33) and (6.36). And the same line of thought establishes that the values of  $x_0^H$  in (6.36) and (6.35) must be the same, as well as the values of  $x_1^H$  in (6.36) and (6.34) and the values of  $x_2^H$  in (6.35) and (6.34).

If all this is true, then adding together the left sides of (6.33)-(6.36) we must get 0 modulo 2, since each of  $x_2, x_1, x_0, x_2^H, x_1^H,$  and  $x_0^H$  appears in exactly two of the equations. But the modulo 2 sum of the right sides is  $0 \oplus 1 \oplus 1 \oplus 1 = 1$ .

So the EPR argument doesn’t work. There are no elements of reality — no predetermined values that a more complete theory would take into account. The answer to what is wrong with the simple and persuasive reasoning that led EPR to the existence of elements of reality is still a matter of heated debate after nearly 70 years. How, after all, can Qbit #0 and its measurement gate “know” that if they interact only after Qbits #1 and #2 have gone through their own measurement gates (and no Hadamards were applied) that the result of the measurement of #0 *must* be given by (6.37)? The best explanation anybody has come up with to this day is to insist that no explanation is needed beyond what one can infer from the laws of quantum mechanics.

**Figure 6.1**

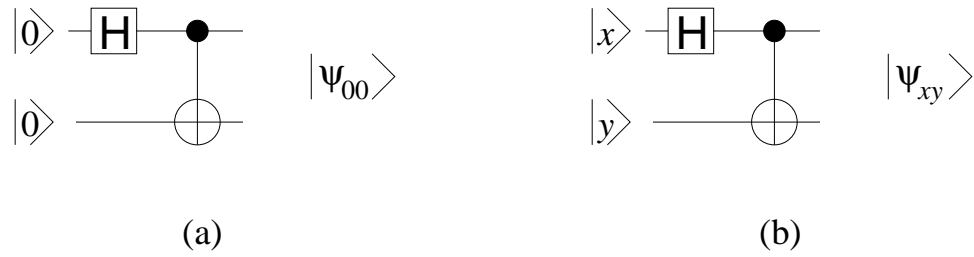


Figure 6.1. (a) Circuit that creates the entangled state  $|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  from the unentangled computational basis state  $|00\rangle$ . (b) Circuit that creates the four orthonormal entangled Bell states  $|\psi_{xy}\rangle$  from the unentangled computational basis state  $|xy\rangle$ .

Figure 6.2

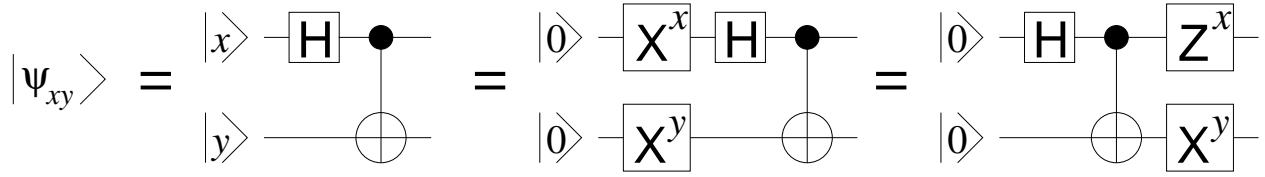


Figure 6.2. Demonstration that the Bell states  $|\psi_{xy}\rangle$  can be constructed from  $|\psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  by either flipping a single Qbit, changing the sign from + to -, or doing both of these.

Figure 6.3

		1	2	3	4	5	6	7	8	9	...
<b>Alice:</b>	Type:	<b>1</b>	<b>H</b>	<b>H</b>	<b>H</b>	<b>1</b>	<b>1</b>	<b>H</b>	<b>1</b>	<b>H</b>	...
	State:	<b>0</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>1</b>	<b>0</b>	<b>0</b>	...
<b>Bob:</b>	Measure- ment type:	<b>H</b>	<b>H</b>	<b>H</b>	<b>1</b>	<b>1</b>	<b>H</b>	<b>1</b>	<b>1</b>	<b>1</b>	...
	Outcome:	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>1</b>	<b>1</b>	<b>0</b>	<b>0</b>	...

Figure 6.3. Quantum cryptography. For each Qbit she sends to Bob, Alice randomly decides which type of state to prepare it in (type **1** means  $|x\rangle$  and type **H** means  $\mathbf{H}|x\rangle$ ) and which state of that type ( $x = 0$  or  $1$ ) to prepare. For each Qbit he receives from Alice, Bob randomly decides whether (**H**) or not (**1**) to apply a Hadamard gate before measuring it. In those cases (about half) where Bob's choice of measurement type is the same as Alice's choice of state, they acquire identical random bits. When their choices differ they acquire no useful information.

Figure 6.4

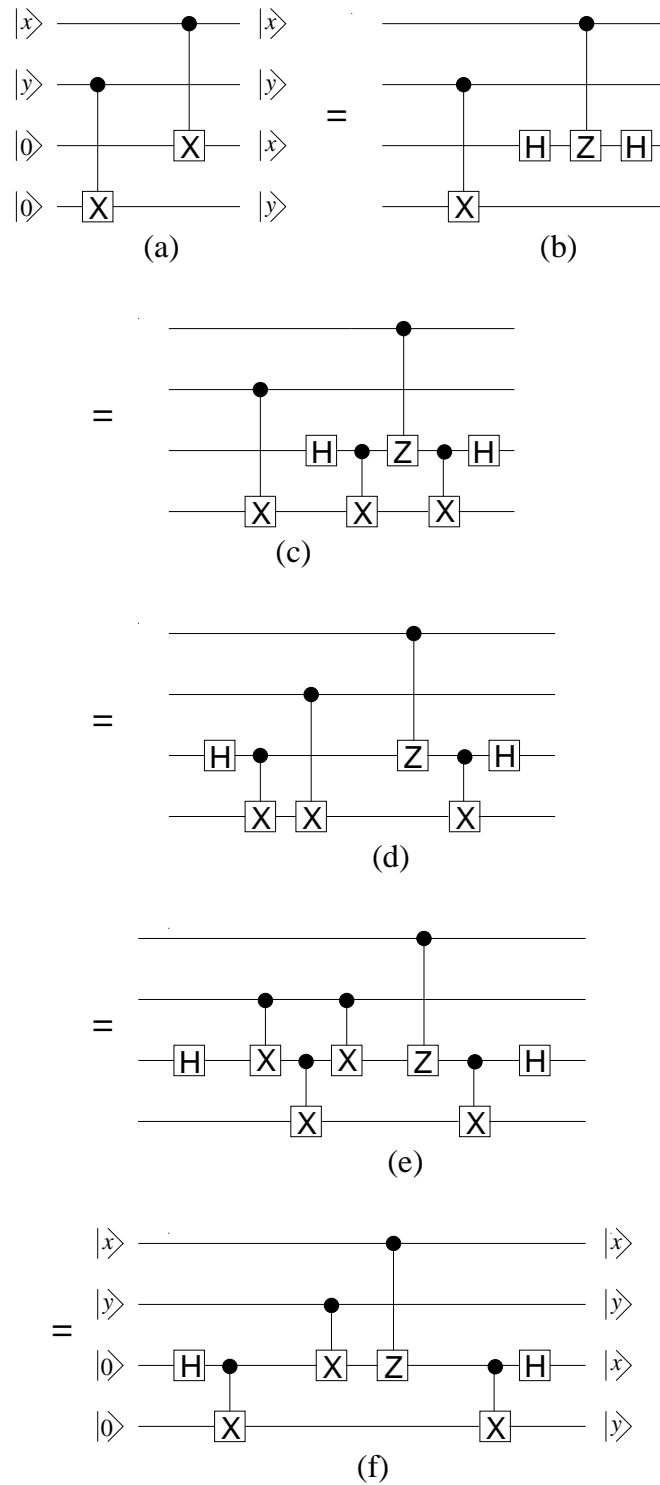


Figure 6.4. A circuit-theoretic derivation of the quantum dense coding protocol.

Figure 6.5

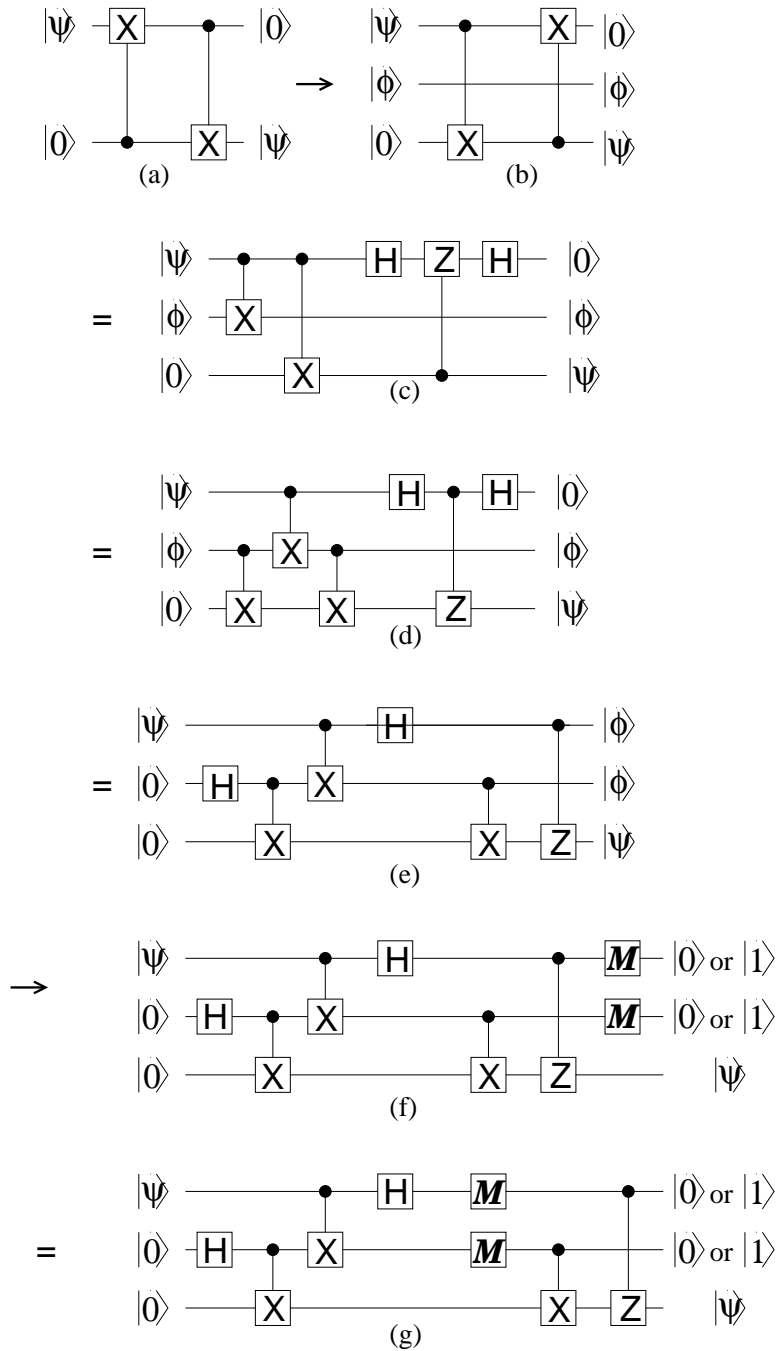


Figure 6.5. A circuit-theoretic derivation of the quantum teleportation protocol.

Figure 6.6

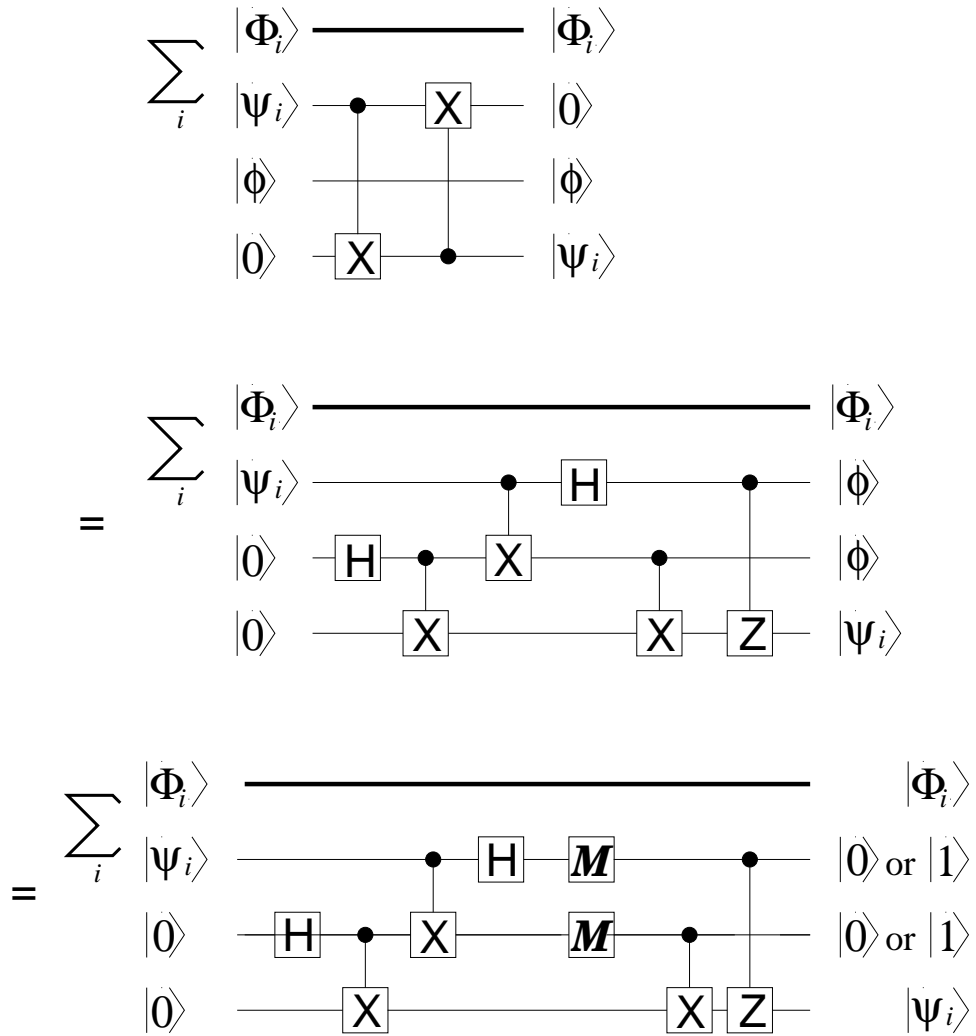


Figure 6.6. A demonstration that entanglement can be teleported.