Entanglement Extraction: A Computational Perspective (Term paper)

Ke Yang <yangke@cs.cmu.edu>

May 10, 2001

Abstract

In this paper, we survey the issue of extracting quantum entanglement. Suppose Alice and Bob plan to perform some teleportation operation, but the qubit pairs they share are not exactly in Bell states. Can they, after performing some local operations and classical communications, manage to produce some EPR pairs or ones that are close to EPR pairs? The general question is some times called "entanglement concentration", and it hasn't been fully understood, but there are positive answer to some special cases. This term paper plans to survey this topic and view the results in a computational perspective, that is, in addition to the possibility, we are also concerned about the *feasibility* of the results and procedures. We also present some original results in our study.

1 Introduction

Consider the following story: Alice and Bob own a company called "Teleportation Inc."[1], and they perform qubit teleportation between Pittsburgh and Boston. They charge 0.99 dollars per qubit teleported, and they, like any honest business people, have an guarantee that the fidelity of their service is at least 99.9%, "or your money back"[2]. To perform teleportation, they must prepare a lot of EPR pairs and distribute them between Pittsburgh and Boston. Alice and Bob decide to buy those EPR pairs from C-KNOT Ltd., located in Philadelphia, instead of manufacturing these pairs by themselves, since C-KNOT Ltd. has the best CNOT gates in the world, which can be used to produce EPR pairs.

One day Alice received a call from Cindi, the CEO of C-KNOT Ltd.. "I am terribly sorry", said Cindi, "but our CNOT gates were sort-of broken — instead of producing pairs that look like $\Phi = \frac{1}{\sqrt{2}}(|\,00\rangle + |\,11\rangle)$, it produces something like $\Phi' = (\cos\theta|\,00\rangle + \sin\theta|\,11\rangle)$. We are running experiments trying to determine this θ, but I think it is something like $\pi/3$. I believe the 2,048 qubit-pairs you ordered last week are all like this... To bad we just found it out, and I guess it takes at least 1 week to fix our machines." Alice almost dropped her phone, since one very important customer, CMUnited, plans to teleport 1,000 qubits to their RoboSoccer term competing CMU vs. MIT annual tournament, and the 1,000 qubits would be the secret weapon they would use to defeat MIT. The tournament will take place tomorrow, and Teleportation Inc. can't afford to

[1] Forgive me for copying Prof. Griffith's imaginary company's name from the class. My creativity in names is rather weaker.

[2] They also plan to introduce a premium service of fidelity 99.999% and they plan to charge 4.99 dollars per qubit — any guess how they do that?

lose such a customer as CMUnited. The only other EPR producer is in Pasadena, CA, which is too far away, and you know, the qubits are very delicate things that don't withstand such a long travel. The only reserve Alice and Bob have are the 2,048 qubit pairs from C-KNOT, and they don't even have a quantum channel between Pittsburgh and Boston. What should they do? "... Fortunately, Alice, we found out that our CNOT gates are very stable, and you can have my words that all the pairs you got are identical", said Cindi. Is there any hope Alice and Bob could do to produce 1,000 EPR pairs out of the 2,048 imperfect pairs they share? Can they do it efficiently?

We will investigate this problem in our paper. We will show that Alice and Bob can produce 1,000 EPR pairs with reasonable high probability. We also discuss some different scenarios:

1. Mixed-State pairs: suppose each pair is in a mixed state, rather than in a pure state. We show if each pair is sufficiently entangled, there is still possibility of extracting EPR pairs.
2. Faulty Pairs: suppose now Alice and Bob share 1,000 EPR pairs and now some pairs are measured. Alice and Bob don't know which measured pairs are. (It could happen that the delivery service, UQPS (Unitied Quantum Particle Service) inadvertently shook several boxes that contains the the qubits, causing a light beam passing through them and measured them). We discuss the possibility that Alice and Bob recover some the EPR pairs.

2 Preliminaries and Notations

All the logarithms are base-2, unless stated otherwise. We often write a state $|\Psi\rangle$ as $|\Psi\rangle = \sum_j \alpha_j |j_A\rangle |j_B\rangle$, where $|j_A\rangle$ means the state $|j\rangle$ in Alice's lab, and $|j_B\rangle$ means the state $|j\rangle$ in Bob's lab. We identify a binary string with a number this string represents. So $|5\rangle$ really means $|101\rangle$.

By an *EPR pair*, we mean a pair of qubits in state

$$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

this state, along with the other 3 states:

$$\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

forms a *Bell basis*. All these 4 states are maximally entangled.

For pure system shared between Alice and Bob, we can write it in the Schmidt form

$$\Psi = \sum_j \alpha_j |A_j\rangle |B_j\rangle$$

where $\{|A_j\rangle\}$ forms an orthonormal basis in Alice's lab and $\{|B_j\rangle\}$ forms an orthonormal basis in Bob's lab. Then the *entanglement* shared between Alice and Bob is defined to be

$$E(\Psi) = -\sum_j |\alpha_j|^2 \log_2(|\alpha_j|^2)$$

As pointed out in literatures [BDS+96, NC00], entanglement of mixed states is yet to be studied and we refrain from giving a definition here.

As in most physics papers, this paper will be "hand-wavy" in a lot of mathematical details.

3 Extracting entanglement from identical qubit pairs in pure state

We first look at the simplest case: suppose all the pairs shared between Alice and Bob are in the same pure state:

$$\Phi' = (\cos\theta|\,00\rangle + \sin\theta|\,11\rangle)$$

We present the result of [BBP+96] here:

In this case, it is easy to compute the entanglement of each pair:

$$E(\Phi') = -(\cos^2\theta\log(\cos^2\theta) + \sin^2\theta\log(\sin^2\theta))$$

we denote this by E_0. Suppose Alice and Bob share N such pairs, and then the total entanglement they share is $N \cdot E_0$. The entanglement extraction for this case is particularly easy: since the complete state can be described as

$$\Psi_N = \bigotimes_{j=1}^{N}(\cos\theta|\,0_A0_B\rangle + \sin\theta|\,1_A1_B\rangle)$$

and we can expand it using the binomial coefficients:

$$\begin{aligned}\Psi_N &= \bigotimes_{j=1}^{N}(\cos\theta|\,0_A0_B\rangle + \sin\theta|\,1_A1_B\rangle) \\ &= \sum_{j=0}^{N}(\cos^j\theta\sin^{N-j}\theta)\sum_{|X|=j}|\,X_A\rangle|\,X_B\rangle\end{aligned}$$

where $|X|$ means the number of '1's in X. So if we define

$$|\,\psi_j\rangle = \sum_{|X|=j}|\,X_A\rangle|\,X_B\rangle$$

for $j = 0, 1, ..., N$, then it is easy to see that $\{|\,\psi_j\rangle\}$ forms an orthogonal basis. Therefore Alice can measure these N qubits use the $\{|\,\psi_j\rangle\}$ basis. With probability $p_j = \binom{n}{j}\cos^{2j}\theta\sin^{2(N-j)}\theta$, the outcome will be $|\,\psi_j\rangle$. Notice one nice feature about the the states $|\,\psi_j\rangle$ is that they are all *maximally entangled* — all the "atomic" states have the same coefficients. Therefore, with probability p_j, Alice and Bob get a system with full entanglement of $E_J = E(|\,\psi_j\rangle) = \log\binom{n}{j}$. A word on the efficiency: we claim that this measurement can be done efficiently: Alice uses $k = \lceil\log N\rceil$ ancillary qubits to "count" the number of ones in the N qubits she shares with Bob — it is not hard to construct a quantum circuit to perform counting, and the counting only takes N rounds. After counting, Alice measures the k ancillary bits, and that is equivalent to measuring the N bits using the $|\,\psi_j\rangle$ basis. The complexity for this measurement is $O(N)$.

Notice either Alice can call Bob about the result of the measurement, or Bob can measure the state himself — because of the entanglement between Alice and Bob, the result of Bob's measurement would be the same as Alice's.

Next we show how Alice and Bob can perform local operations to transform their shared state into the product of EPR pairs: if the state is $|\psi_j\rangle$, then the entanglement is $E_j = \log\binom{N}{j}$, and Alice and Bob should be able to produce about $\lfloor\log\binom{N}{j}\rfloor$ EPR pairs — we use T_j to denote $\lfloor\log\binom{N}{j}\rfloor$. A unitary transform is needed to translate the states $|X\rangle$ where $|X| = j$, to the "more compact" states $|00..0\rangle$, $|00..1\rangle$, ... $|11...1\rangle$. Perhaps the most natural thought is: since there are $\binom{n}{j}$ X's such that $|X| = j$, there is a natural ordering for them: there exists an bijection

$$g_j : \{X \in \{0,1\}^n \,:\, |X| = j\} \longmapsto \left\{0, 1, ..., \binom{n}{j}\right\}$$

Furthermore, both g and its inverse are efficiently computable. Therefore both Alice and Bob can apply the mapping g_j to their states $|\psi_j\rangle$ and arrive at a new shared state $|\psi'_j\rangle$ (we use M_j to denote $\binom{n}{j}$):

$$|\psi'_j\rangle = \frac{1}{\sqrt{M_j}} \sum_{k=0}^{M_j-1} |k_A\rangle|k_B\rangle$$

If M_j is a power of 2, then great, $|\psi'_j\rangle$ is already a product of $T_j = \log\binom{N}{j}$ EPR pairs and Alice and Bob are ready to use them: notice each k_A is a binary string of length T_j, and since M_j is a power of two, different bits of the binary string are disentangled.

However, when M_j is not a power of 2, Alice and Bob still cannot use $|\psi'_j\rangle$ directly: for example, take $M_j = 3$, and the state between Alice and Bob is

$$\frac{1}{\sqrt{3}}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|2\rangle)$$

or

$$\frac{1}{\sqrt{3}}(|00\rangle|00\rangle + |01\rangle|01\rangle + |10\rangle|10\rangle)$$

if written in binary form. Obviously the two qubits Alice has are entangled. There are many ways to solve this problem, and we will present several solutions.

3.1 Method 1: Recursive Measurement

This solution is discovered by the author, and we are not sure if it is original.

We know Something more has to be done: notice since we have $2^{T_j} \le M_j < 2^{T_J+1}$, Alice and Bob can perform a measurement on the Most Significant Bit (MSB) of the qubits they have (the T_j-th bit). There are two possibilities:

1. With probability $\frac{2^{T_j}}{M}$, a result of 0 is obtained, and the states shared by Alice and Bob collapses into

$$\frac{1}{2^{T_j/2}} \sum_{k=0}^{2^{T_j}-1} |k_A\rangle|k_B\rangle$$

   and Alice and Bob get T_j EPR pairs: they can use the 0-th, 1-st, ..., $(T_j - 1)$-th bits, which are disentangled.

2. With probability $\frac{M-2^{T_j}}{M}$, a result of 1 is obtained and the states between Alice and Bob collapses into

$$\frac{1}{M-2^{T_j}} \sum_{k=2^{T_j}}^{M_j} |k_A\rangle |k_B\rangle$$

In this case, Alice and Bob are left with a shared state of entanglement $\log(M-2^{T_j})$. In this case Alice and Bob can throw away the T_j-th bit, which is already 1, and measure the (T_j-1)-th bit, and do this recursively.

We examine the efficiency of the above procedure: if we write M_j in binary:

$$M_j = 2^{b_0} + 2^{b_1} + \cdots + 2^{b_s}$$

where $b_0 < b_1 < \cdots < b_s = T_j$, then:

- with probability $\frac{2^{b_s}}{M_j}$, Alice and Bob can extract b_s EPR Pairs.
- with probability $\frac{2^{b_{s-1}}}{M_j}$, Alice and Bob can extract b_{s-1} EPR Pairs.

  ...
- with probability $\frac{2^{b_0}}{M_j}$, Alice and Bob can extract b_0 EPR pairs.

In particular, if M_j is an odd number, then with tiny probability $1/M_j$, Alice and Bob might miserably fail and don't extract any EPR pairs — but that is a very rare situation.

When we look at the *expected* number of EPR pairs Alice and Bob can obtain, it is

$$E = \frac{1}{M_j} \sum_{l=0}^{s} 2^{b_l} \cdot b_l$$

We shall prove that $E \geq \log M_j - 3$: We first do a lemma:

Lemma 1 *For $x > y > 0$,*

$$x\log(x) + y\log(y) - 3y \geq (x+y)\log(x+y) - 3(x+y)$$

Proof: Direct computation:

$$\begin{aligned}
& (x+y)\log(x+y) - 3\log(x+y) - (x\log(x) + y\log(y) - 3y) \\
= \; & x\log(1+\frac{y}{x}) + y\log(1+\frac{x}{y}) - 3x \\
\leq \; & x \cdot \frac{y}{x} \cdot \log_2 e + y \cdot \frac{x}{y} \cdot \log_2 e - 3x \\
< \; & 1.44y + 1.44x - 3x \\
< \; & 0
\end{aligned}$$

■

Next we prove that $E \geq \log M_j - 3$ by induction: write $M_j = 2^{b_s} + T$, where $T < 2^{b_s}$. Therefore we have

$$\begin{aligned}
E &= \frac{1}{M_j} \sum_{l=0}^{s} 2^{b_l} \cdot b_l \\
&= \frac{1}{M_j} \left[2^{b_s} \cdot b_s + \sum_{l=0}^{s-1} 2^{b_l} \cdot b_l \right] \\
&\geq \frac{1}{M_j} \left[2^{b_s} \cdot b_s + T \cdot (\log T - 3) \right] \quad \text{(inductive hypothesis)} \\
&\geq \frac{1}{M_j} (2^{b_s} + T) \left[\log(2^{b_s} + T) - 3 \right] \quad \text{(lemma)} \\
&= \log M_j - 3
\end{aligned}$$

So up to a additive constant, Alice and Bob extracts the entanglement almost optimally. Another nice feature is Alice and Bob succeeds with reasonably high probability: the probability that Alice and Bob extracts less than k bits is bounded by $2^k / M_j \leq 1/2^{T_j - k}$, which decreases exponentially with k. Therefore, the probability Alice and Bob extracts less than half of the entanglement is less than $1/2^{T_j/2} \doteq 1/\sqrt{M_j}$, which is generally very small since $M_j = \binom{N}{j}$ is generally very large.

The running time for the extraction is proportional to T_j, the amount of entanglement in the state $|\psi_j\rangle$.

3.2 Method 2: Repeated Sampling

This method is presented in [BBP+96], where it is called the "Schmidt Projection" method.

The idea is roughly as follows: suppose Alice and Bob are at state $|\psi_j\rangle$, where there are $\binom{N}{j}$ "atomic" states. If $\binom{N}{j}$ is a power of 2 or is slightly higher than a power of 2, then Alice and Bob can measure the MSB (as in the Recursive Measurement method), and with very high probability, the state will collapse into a subspace of dimension 2^{T_j}. So the bad case is that $\binom{N}{j}$ is far from a power of 2. In this case, One can take another block of N qubit pairs and does a measurement —- suppose this time a state $|\psi_{j_2}\rangle$ is obtained. Then we check the new dimension of the combined state, which is $\binom{N}{j_1}\binom{N}{j_2}$ (we use j_1 to denote j). If this number is slightly larger than a power of 2, we are happy. Otherwise we take another block of N and measure...

In general, Alice and Bob take m batches, each of N qubit pairs, and measure each batch. Then Alice and Bob will get a space of total dimension

$$L = \binom{N}{j_1} \binom{N}{j_2} \cdots \binom{N}{j_m}$$

Alice and Bob stop until L is close to a power of 2, or more precisely, when $2^l \leq L < 2^l(1+\epsilon)$ for some l and a pre-determined ϵ. So this space can be split into 2 orthogonal subspaces, on of dimension 2^l and another of dimension $L - 2^l$. Now, as in method 1, Alice and Bob can first "compress" the states and then measure the MSB. With probability at least $(1-\epsilon)$, they will end up with the large space and obtain l EPR pairs.

In [BBP+96], the Bennett et. al. argue that as m increases, with probability 1, Alice and Bob will obtain an L such that $2^l \leq L < 2^l(1+\epsilon)$. However, it is unclear from their paper that how large an m is needed to ensure that such an L exists. Therefore, although theoretically simple and elegant, we find this Repeated Sampling method not appealing in practice — unless some finer analysis is done regarding the number of blocks m needed, to ensure that Alice and Bob have a high probability to extract EPR pairs. We tried some analysis, and the result we get is $m = \Omega(\epsilon)$. Therefore, in order for Alice and Bob to have an overwhelmingly high probability (over $1/\mathsf{poly}(n)$) to succeed (meaning getting at least 1 EPR pair), super-polynomially many blocks are needed. On the contrary, the recursive measurement method has a logarithmic relation with the failing probability ϵ: the probability of getting less than $1/2$ of the expected EPR pairs is already exponentially small.

3.3 Method 3: Procrustean

One problem with the first 2 methods is that they both rely on many pairs of identical qubit pairs. Suppose Alice and Bob share just one pair of qubits, the previous 2 method will not be able to extract anything at all. However, the Procrustean method, also introduced in [BBP+96], solves this problem. It works for individual qubit pairs: for each pair of qubits Alice and Bob share, this method will product an EPR pair with certain probability, though not as efficient as the previous methods. This method can be understood as follows: suppose the state of each qubit pair shared between Alice and Bob is $\Phi' = (\cos\theta|\,00\rangle + \sin\theta|\,11\rangle)$, and suppose $0 \leq \theta \leq \pi/4$, and thus $\cos\theta \geq \sin\theta$. The Alice performs a probabilistic "cut" on her qubit by passing it through a device called "polarization-dependent absorber". The effect of it would be: with probability $2\cos^2\theta$, the qubit will be kept, and with probability $(1 - 2\cos^2\theta)$, the qubit will be absorbed. If the qubit is absorbed Alice claims the experiment fails and asks Bob to discard his part of the qubit. If the qubit is kept, Alice informs Bob so, and now the qubit pairs between them becomes an EPR pair. Notice the polarization-dependent absorber is a physical device that is available now, and thus it is very easy to perform this Procrustean method.

A disadvantage for the Procrustean method is that it requires Alice and Bob to know the *exact* state of the qubit pairs they share, since they need the information to build a "customized" polarization-dependent absorber. While the first 2 methods don't require this. Also this method isn't very efficient.

3.4 Summary and Comparison

We have 3 methods now for Alice and Bob to extract entanglement between the identical qubit pairs they share. All three methods will produce perfect EPR pairs, though they might fail from time to time.

The Recursive Measurement method achieves nearly optimal yield in the number of EPR pairs it produces, and it is very stable: the probability that it produces less number of pairs decreases exponentially with the discrepancy. The implementation is reasonably easy: the unitary transformation for "compressing" states $|\,X\rangle$ to states $|\,k\rangle$ could be problematic, but one doesn't have to keep many qubit around. In this method, one doesn't need to know the exact state between Alice and Bob — so long as all the pairs are identical and in a pure state, this method would work.

The Repeated Sampling method also achieves nearly optimal yield, as the author in [BBP+96] claims. However, the error probability (the probability Alice and Bob don't produce any EPR pair) is high: if Alice and Bob share totally N pairs, the error probability could be $\Omega(1/N)$ [3]. Also there might be problems implementing this method, since Alice and Bob has to keep all the blocks they measure so far, until a proper L is reach. Storing many qubits could be a problem. Like the Recursive Measurement method, the Repeated Sampling method doesn't require that Alice and Bob know the exact states they share.

[3] The author in [BBP+96] doesn't give an quantitative analysis, and thus our claim might be overly pessimistic.

The Procrustean method isn't optimal in terms of efficiency, but it works for single qubits. This is particularly desirable when Alice and Bob only need a few EPR pairs. Also this method is especially simple and very easy to implement — the current technology should be able to achieve that. One drawback is that Alice and Bob need to know the exact state shared by Alice and Bob, otherwise they can only produce approximately correct EPR pairs.

We summarize the 3 methods in the table below, where N is the number of EPR pairs Alice and Bob produces.

Method	Needs to know exact state	efficiency	failure probability	implementation
Recursive Measurement	No	near optimal	$O(2^{-N})$	Easy
Repeated Sampling	No	near optimal	$O(1/N)$	Hard
Procrustean	Yes	sub-optimal	$O(1)$	Very easy

Considering the case of the story, since Alice and Bob don't know the exact state of the qubit pairs they share, they should use the recursive measurement method to produce EPR pairs. A simple computation verifies that each qubit pair $\cos\theta|00\rangle + \sin\theta|11\rangle$ contains about 0.81 ebits of entanglement when $\theta = \pi/3$, and thus Alice and Bob, having 2,048 qubit pairs in hand, will be able to produce 1,000 EPR pairs with high probability.

4 Extracting entanglement from identical qubit pairs in mixed state

Now we consider the slightly more complicated case: still all pairs shared between Alice and Bob are identical, but they are in a mixed state. We show several definitions of the "entanglement" here, since people still don't fully understand the entanglement in the mixed state. We also show some procedures to extract (approximate) EPR pairs. The results are from [BDS+96].

Unfortunately, researchers in quantum information theory have yet fully understood the entanglement in mixed states. They are multiple (candidate) definitions for the entanglement and different justifications for each. In this term paper, we survey part of them and present them "as is".

4.1 Candidate definitions of entanglement in mixed states

We first study definition of entanglement in mixed states. Let's recall the definition of entanglement for a bipartite pure state: We use $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ to denote the state space shared between Alice and Bob. For a state $\Psi \in \mathcal{H}$, we can perform Schmidt Decomposition and write Ψ as

$$\Psi = \sum_j \alpha_j | A_j\rangle | B_j\rangle$$

where $\{| A_j\rangle\}$ and $\{| B_j\rangle\}$ form orthonormal basses in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Then the entanglement is defined as

$$E(\Psi) = -\sum_j |\alpha_j|^2 \log(|\alpha_j|^2)$$

which is also the von Neumann entropy for the partial density matrix of Alice and the the von Neumann entropy for Bob. Namely,

$$E(\Psi) = S(\rho_A) = S(\rho_B)$$

where $\rho_A = \mathrm{Tr}_B(\rho) = \mathrm{Tr}_B|\Psi\rangle\langle\Psi|$ and $\rho_B = \mathrm{Tr}_A(\rho) = \mathrm{Tr}_A|\Psi\rangle\langle\Psi|$.

Intuitively[4], this makes sense: von Neumann entropy measures how much "uncertainty" a quantum system has, as Shannon entropy measure how much uncertainty a classical system has. If Alice and Bob share a pure state, then the "total uncertainty" is completely in the quantum side (as compared to a mixed state, where the total uncertainty is distributed between the quantum uncertainty and classical uncertainty). Also since Alice can *completely* determine Bob's state if she measures her partial state alone, all the uncertainty exists in the "entangled" form. Therefore the entanglement should be equal to the total uncertainty of the state, which is the total uncertainty of the von Neumann entropy of Alice.

Furthermore, there are several natural (and intuitively justified) criteria for a measurement of entanglement, some of which are axiomatic and some of which are derivable from th rest:

1. **Zero:** If the state of Alice and the state of Bob are un-entangled, then their entanglement is zero.
2. **Unit:** An EPR pair shared between Alice and Bob has one unit of entanglement. We use *ebit* to denote this unit. This requirement is more or less arbitrary, but proved convenient.
3. **Additivity:** Entanglement should be additive for independent systems. For example, suppose Alice and Bob shares n identical states Ψ (i.e., the complete state between Alice and Bob is $\Psi^{\otimes n}$), then the total entanglement between Alice and Bob should be n times the entanglement of Ψ. Notice both Shannon and von Neumann entropy satisfies additivity.
4. **Monotonicity:** The entanglement between Alice and Bob shouldn't be increased by local operations performed by Alice and Bob, even with classical communications. Essentially, this is because we want the entanglement to be a pure measurement of a *global quantum* quantity, and thus local operations and classical communications shouldn't increase entanglement. However entanglement can be decreased by local operations: for example, Alice and Bob measure all their qubits, and the resultant state has ZERO entanglement.
5. **Upper bound for single qubit pairs:** The maximum entanglement for a single qubit pair is 1 ebit, which is achieved when this pair is in one of the Bell states. Notice Alice and Bob can perform teleportation by using one EPR pair and 2 bits of classical communication. They use up one EPR pair and can possibly create a new pair of entangled qubits. By the monotonicity requirement, we know that entanglement of the new pair cannot be higher than the entanglement of the EPR pair, which is 1 ebit.
6. **Conservation of local unitary operation:** Local unitary operations are reversible. Therefore if there is one local unitary operation U that decreases entanglement, then $U^\dagger$ will increase entanglement, contradicting the monotonicity requirement. Therefore local unitary operations shouldn't change the entanglement.
7. **Feasibility** A system of entanglement m should be able to (asymptotically) transformed to m EPR pairs and/or be obtained from m EPR pairs, but only using local operations and classical communications.

[4] Although quantum mechanics is notorious for its anti-intuitiveness, the author still attempts to appeal to intuition for understanding the concepts.

This is the most unclear requirement, and it not obviously justified. This requirement says there should be a way to relate a system of certain entropy with a "standard" system of m EPR pairs: these two system should be able to be transformed back and forth. An argument for this is: unless the definition of entanglement satisfies the feasibility requirement, the definition isn't really useful, since nobody can "extract" the right amount of entanglement out of it.

It is easy to check that the definition for pure state entanglement satisfies all these requirement, and this is the only definition that does so[5]

However, the situation becomes more complicated in mixed states, and precisely, the reason is from the feasibility requirement. As discussed in [BDS+96], people don't know if every entangled system that takes m EPR pairs to build will product about m EPR pairs by local operation and classical communication. In other words, there might be an asymmetry between a general mixed state and the "standard" state of m EPR pairs: it could take more EPR pair to obtain a mixed state than to extract from that state.

We introduce 3 (candidate) definitions of the entanglement for a mixed state:

1. **Entanglement of formation**

   In this definition, the entanglement of a mixed state M is the minimal expected entanglement of any ensemble of pure states realizing M, and denoted by $E(M)$. In [BDS+96], it is proven to be a proper definition. However, it is general not known how to find the most "economical" way to generate a particular mixed state M from a pure state, where "economical" meaning that minimal amount of expected pure-state entanglement is used. Therefore, no general procedure is known to compute $E(M)$ given the density matrix of M.

   Nevertheless, some lower bounds are known for very special cases of M: if M is a mixed state of a single pair of qubits shared between Alice and Bob, a lower bound for $E(M)$ is known, and the lower bound is tight if M is either a pure state or a Bell-diagonal mixture (meaning the density matrix of M, written over the Bell-state basis, is a diagonal matrix).

2. **Entanglement of purification with 1-way/2-way communication**

   This definition (along with the next) is on the opposite direction to the "entanglement of formation" definition: while "entanglement of formation" is concerned is how much pure-state entanglement is required to *build* a mixed state M, this purification definition is all about how much entanglement can be *extracted* (or "purified", as in [BDS+96]). A little more formally, the purification entanglement of a system M, denoted by $D_1(M)$ or $D_2(M)$ (referring to 1-way or 2-way communication), is

   $$D_P(M) = \lim_{n\to\infty} \frac{m_P}{n}, \quad P = 1, 2^6,$$

   where m_P is the maximum number of EPR pairs that can be produced from n identical, independent copies of M by local operations and P-way classical communication. So $D_1(M)$ is the max rate of EPR pairs can be produced by local operation and 1-way classical communication (Alice talks to Bob, and Bob doesn't say anything), and $D_2(M)$ is the rate for local operation and 2-way classical communication (Alice and Bob both can talk).

[5] Again, we make this statement without proof.

[6] Pedantically, we might use sup instead of lim, unless one proves such a limit exsits. However since this is supposed to be a *physics* paper, we don't care.

It is not hard to see that

$$D_1(M) \leq D_2(M) \leq E(M)$$

since 2-way communication should be at least as powerful as 1-way communication, and by the monotonicity of entanglement, the number of EPR pairs that can be extracted from a state M cannot exceed the number of EPR pairs used to build M. Also notice the definition of purification entanglement is the "aggregation" definition, where a collection of identical copies of M are needed. We need this since it is easy to measure entanglement in terms of EPR pairs, and we have to deal with the "rounding error".

If M is a pure state, then we have $D_1(M) = D_2(M) = E(M)$, and the definition is clean (see [BBP+96, NC00] for "entanglement distillation and dilution"). However for mixed states, these 3 quantities might not be equal, and that is the source of a lot of confusions. The readers are referred to [BDS+96] for details, and we don't elaborate in this paper, since we are mainly interested in extracting entanglement.

4.2 Entanglement extraction

We discuss various techniques for extracting entanglement from mixed states. Due to the nature of the mixed states, the analysis here would be even more "hand-wavy" than the analysis for pure states. Furthermore, the notion of "optimality" is also fuzzy since no single clear definition for entanglement of mixed states is known (and not even known to exist).

4.2.1 Preliminary: Werner states and local operations

Werner states, defined as

$$W_F = F \cdot |\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}\left(|\Psi^+\rangle\langle\Psi^+| + |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-|\right),$$

plays an important role in entanglement purification for mixed states. It can be shown that a general two-particle mixed state M can be converted to a Werner state (possibly irreversibly). There are several ways to do it, and the simplest one is a *random bilateral rotation*. We don't want to go into the details of this method. What's important here is: converting a general state into a Werner state is normally the first step people do in entanglement purification.

The particular nice feature about Werner states is that they are diagonal matrices over the basis of Bell states. In other words, the state can be regarded as a mixture of different Bell states. Entanglement purification for Werner states are much easier. Notice in converting any state into a Werner state, some entanglement might be lost since the transformation can be irreversible. Therefore this Werner-state preprocessing approach doesn't guarantee optimal yield. However, first transforming to a Werner state is still a common practice..

Now we discuss some local operations Alice and Bob can perform. There are single-bit operations, and there are 2-bit operations. What's especially interesting is the *bilateral XOR* operations, or BXOR. For this operation, Both Alice and Bob perform a CNOT operation with the first bit as CONTROL and second bit as TARGET. An important feature is this BXOR transform maps Bell states back into Bell states.

Let's look at a particular example: suppose the state shared between Alice and Bob is $\Phi^+ \otimes \Psi^-$, or

$$\begin{aligned}
\Phi^+ \otimes \Psi^- &= \frac{1}{2}(|\,0_A0_B\rangle + |\,1_A1_B\rangle)(|\,0_A1_B\rangle - |\,1_A0_B\rangle) \\
&= \frac{1}{2}\left[|\,00_A\rangle|\,01_B\rangle - |\,01_A\rangle|\,00_B\rangle + |\,10_A\rangle|\,11_B\rangle - |\,11_A\rangle|\,10_B\rangle\right]
\end{aligned}$$

and BXOR will transform that to

$$\begin{aligned} & \frac{1}{2}[|\,00_A\rangle|\,01_B\rangle - |\,01_A\rangle|\,00_B\rangle + |\,11_A\rangle|\,10_B\rangle - |\,10_A\rangle|\,11_B\rangle] \\ = \ & \frac{1}{2}(|\,0_A0_B\rangle - |\,1_A1_B\rangle)(|\,0_A1_B\rangle - |\,1_A\rangle 0_B) \\ = \ & \Phi^- \otimes \Psi^- \end{aligned}$$

In general, one can work out the complete transformation and the readers are referred to [BDS+96] for a nice table describing the complete operation.

Next we describe several methods for entanglement purification in the mixed states.

4.2.2 Recurrence method

The recurrence method first appeared in [BBP+96b], and was discussed in [BDS+96] later. The The protocol isn't very complicated:

1. Alice and Bob start from 2 qubit pairs they share. These two qubit pairs are identical and independent, and both are in a Werner state that is "mostly" Ψ^-.
2. Alice performs a σ_y rotation on each qubit she posesses — this will convert a Ψ^- state to a Φ^+ state, and therefore will convert a "mostly" Ψ^- state to a "mostly" Φ^+ state.
3. Alice and Bob perform a BXOR operation: both apply the CNOT operation to the qubits they posess, and both measure the target qubit along the z-axis. This measurement will reliably distinguish $\Phi^\pm$ from $\Psi^\pm$, since Alice and Bob will get the same result for $\Phi^\pm$, and different results for $\Phi^\pm$. Alice and Bob discard these two pairs of qubits if they get different results. Otherwise they discard the target bit and keep the control bit.
4. Alice performs another σ_y rotation on the remaining qubit, thus transforming the system back to a "mostly Ψ^- state.

The idea behind this protocol is also simple: One may regard the BXOR operation as a kind of "polarization" — if two states are "mostly" Φ^+, then after the BXOR, with reasonably high probability this pair will "pass" the measurement (meaning that Alice and Bob obtain the same results), and if they pass, the remaining qubit pair is closer to Φ^+ then before. Keep doing this polarization procedure, one get qubit pairs that are "purer" than the original ones.

This recurrence method isn't very efficient: each time 2 pairs of qubits are used, while expected less than 1 pair remains. In order to get a qubit pair that is very close to an EPR pair, a lot of such purification processes have to be done and the overall yield goes to zero. Macchiavello (in a private conversation with the author of [BDS+96]) describes a better method that has high yield. But this yield still approaches zero with the requited fidelity approaching 1. We don't give a detailed analysis here.

4.2.3 Direct purification

In this section we describe a method that directly purifies a mixed state, without first transforming it into a Werner state. Here we just give a particular example: suppose the state shared between Alice and Bob is

$$M = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|\Psi^+\rangle\langle\Psi^+|$$

So with probability $1/2$, M is a fully entangle qubit pair. This state cannot be directly purified using the recurrence method described above. However, Alice and Bob can do the following: they apply the BXOR operation (each applies the CNOT operation to their qubits) and then each measures the target qubit in the $0-1$ basis. It can be shown (left as an exercise to the reader) that with probability $1/8$, the result from the measurement is $|0_A\rangle|0_B\rangle$, i.e., both measures "0". Furthermore, in this case, the qubits left un-measured as in state Ψ^+, a perfect EPR pair. This method works for state $M = (1-p)|00\rangle\langle 00| + p|\Psi^+\rangle\langle\Psi^+|$, where the yield is $p^2/4$.

However, this particular method cannot be generalized to work with *any* qubit pairs with non-zero entanglement. Horodecki et. al. [H96] presented a general strategy of purification: they apply a filtering operation that enhances the fraction of EPR pairs of the surviving qubits, and then use the recurrence method discussed above. In this way, they manage to show that for any two-qubit systems of non-zero entanglement, some "pure" entanglement can be extracted. Their result implies that for these systems, $E(M) > 0$ implies that $D_2(M) > 0$.

4.2.4 One-way hashing method

We describe yet another way of extracting entanglement from mixed states. This method is similar the "privacy enhancement" technique in classical cryptography.

This hash method assumes the state is a mixture of Bell states — one can pre-process a state into a Werner state to satisfy this. Also it is required that the density matrix of the state M, is known — call it W. Suppose the von Neumann entropy for W is $s = S(W)$, then this hash method will extract EPR pairs with a rate asymptotically $(1 - S(W))$. The algorithm only needs to know the actual value of $S(W)$ since it is one of the parameters in the algorithm. This algorithm also has a controllable "confidence" δ — the smaller δ is, the less the probability this algorithm fails. The actual quantitative analysis isn't given here.

Let's first motivate this algorithm before actually going into the details: since M is a mixture of Bell states, we can write

$$W = \sum_{j=1}^{4} p_j B_i$$

where B_i's are density matrices of the Bell basis states. Now if we look at the total state of n identical copies of M: the density matrix would be

$$W^{\otimes n} = \left(\sum_{j=1}^{4} p_j B_i\right)^{\otimes n}$$

Now, as we do in compressing information (classical and quantum) using the Law of Large Numbers, we use this law again: we know that the most probabilistic weight is on the "typical sequences". So we know with very high probability, Alice and Bob can assume the qubits they share is also one of the typical sequences.

Now if Alice and Bob know exactly which typical sequence the state is, their density matrix will look like

$$W_0 = B_{j_1} \otimes B_{j_2} \otimes \cdots \otimes B_{j_m}$$

which is a product of k Bell states. After getting W_0, we can apply proper unitary transformations to get m EPR pairs.

There are about $2^{n \cdot S(W)}$ typical sequences, and thus about $n \cdot S(W)$ measurements are needed, each eliminating half of the sequences. Another way to look at this is: W is a large probabilistic ensemble of entropy $n \cdot S(W)$, and we need to determine which element we are in. Therefore we need to bring the entropy down by $n \cdot S(W)$ bits. Each measurement eliminate at most 1 bit of information, and thus $n \cdot S(W)$ measurements are needed.

The tricky part is to make sure that each measurement does give about one bit of information, or close to 1 bit. Since the structure of the typical sequences is rather complicated, and it is infeasible to keep track of all of them, one uses a "random" measurement — a random measurement can ensure that the (remaining) typical sequences will be divided almost evenly with very high probability. It is a common trick used in computer science and discrete mathematics: suppose there are N typical sequences, a random measurement means that each sequence will be measured "plus" with probability exactly $1/2$. So the remaining number of sequences has expected value $N/2$, and the probability it deviates from $N/2$ by any constant fraction is exponentially small — this is again the Law of Large Numbers.

However, it is still infeasible to perform a completely random measurement — simpler describing that measurement will take exponentially number of bits. This is the place the second trick comes into play: "use universal hash functions in the place of random functions" — it is a motto in theoretical computer science. In this case, a random parity function is good enough: notice the crucial difference: a random parity function takes n bits to describe and a random function takes 2^n bits to describe. Also the parity functions are efficiently computable.

Now this the intuition for the hashing method, and we describe the actual action, which is also very simple:

1. Alice and Bob start by transforming the qubit pairs they share into the "diagonal Bell states" — meaning that the density matrix for each qubit pair is a diagonal matrix when written in Bell state basis. Suppose Alice and Bob share n such pairs, which is $2n$ qubits.
2. Alice and Bob compute the entropy of the density matrix of each qubit pair, $S(W)$. Let $k = n(S(W)+2\delta)$. Alice and Bob will repeat the following measurement for k rounds:
3. In round l, Alice generate a random parity function on $2(n-l+1)$ bits — this is equivalent to generating $2(n-l+1)$ random bits — and send to Bob.
4. Both Alice and Bob measure their collection of qubits: $2(l-1)$ of them have already been measured, and there are $2(n-l+1)$ unmeasured qubits. Alice and Bob apply the parity function to these $2(n-l+1)$ bits and measure the results. After the measurement Alice and Bob through away one qubit pair they share.
5. After k rounds, Alice and Bob share $n - k = n(1 - S(W) - \delta)$ pairs of qubits, and with very high probability that these pairs are in a pure state that is a product of Bell-states.

Here the δ is used as an error parameter that can be made smaller than any constant (the example given in [BDS+96] is $\delta = O(n^{1/4})$. In this way, the error probability will approach 0 when n increases, and the yield will approach $n(1 - S(M))$.

This hashing method is technically very interesting, however it is not very efficient — starting from a Werner state will waste some entanglement, and by keeping measuring using parity functions, a lot of information is "thrown out". Since there isn't a single definition for entanglement in this case, it is particularly hard to measure the "efficiency" of an extracting algorithm. One nice feature of this hashing method is that it only involves 1-way classical communication: only Alice sends random bits to Bob and Bob doesn't have to say anything.

4.2.5 Summary

We summarize the several methods we discussed in this section: the recurrent method, the direct purification, and the hashing method.

The Recurrence method repeats the uni-lateral rotation – BXOR — measure — uni-lateral rotation cycle. If the state starts from a Werner state that is close to Ψ^-, then each cycle will make the surviving state "closer" to Ψ^-, and thus does the "polarization". For this to work, Alice and Bob don't have to know the exact state they start with. But the yield approaches zero when the fidelity increases towards 1, and no exact EPR pairs are produced. 2-way communication is needed since Alice and Bob need to know which qubits to keep and which to discard.

There are actually 2 direct purifications: the first one works only for some particular state – a direct rotation followed by BXOR and measurement. This produces exact EPR pairs, and 2-way communications are needed. The second direct purification is proposed by Horodecki et. al., which uses a "filter" to enhance the fraction of Bell-states in the surviving states, and then switched to recurrence method. So again 2-way communication is needed and the result are not perfect EPR pairs. Exact states are also needed for the filtering. The second direct method has the contribution that it proves that for 2-qubit states M, $E(M) > 0$ implies $D_2(M) > 0$.

The hashing method works with Werner states, and Alice and Bob only need to know the entropy of the mixed state they share, not the exact matrix. Hashing method will produce exact EPR pairs and only used 1-way communication.

We summarize our discussing in the following table:

Method	**Exact state**	**Werner state**	**Perfect EPR pairs**	**yield rate**	**1-way / 2-way**
Recurrence	No	Yes	No	0	2-way
Direct Purification(1)	Yes	No	Yes	$p^2/4$	2-way
Direct Purification(2)	Yes	No	No	non-zero	2-way
Hashing	No	Yes	Yes	$1 - S(W)$	1-way

So, even if the qubit pairs Alice and Bob share are in mixed state, Alice and Bob still have chances to extract perfect or almost-perfect EPR pairs. However, the yield could be low, and our friends in Teleportation Inc. might have a problem with teleporting the 1,000 qubits for CMUnit. Let's wish them good luck.

5 Extracting entanglement from faulty qubit pairs

Next we discuss a even worse case: suppose that the C-KNOT company works perfectly, but they use UQPS (United Quantum Particle Service) to deliver the qubits from Philadelphia to Pittsburgh and Boston. During the delivery, one of the boxes containing the qubits was opened, and one qubit was measured: the EPR pair collapse into $|00\rangle$ or $|11\rangle$ with probability 1/2 each. To make things worse, Alice and Bob have no idea which pair was measured. Now, is there a way Alice and Bob can extract at least one EPR pair?

More formally, suppose Alice and Bob share n EPR pairs: $\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and one of the pair is measured. Can Alice and Bob, by performing local operations and classical communications, extract 1 perfect EPR pair?

We are still studying this problem, but we think the answer is yes. We present some partial results here:

This lemma is due to Andris Ambainis [A01].

Lemma 2 *If Alice and Bob share 2 EPR pairs and one of them is measured. Alice and Bob can perform local operations and classical communications to obtain a Bell state that is either* $\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *or* $\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

Proof: We show the actual protocol:

1. Both Alice and Bob does the following unitary transformation U to the 2 qubits they posess:

$$\begin{aligned} U|00\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ U|01\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ U|10\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\ U|11\rangle &\longrightarrow \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \end{aligned}$$

2. Both Alice and Bob measure their first bit, and Alice sends the result to Bob.
3. Bob compares the two results. If the two results are equal he does nothing, and if the two results are not equal, he flips his second bit.

Now let's analyze what happens:

First the state *prior* to the measurement by UQPS is

$$\Psi = \frac{1}{2}(|00\rangle + |11\rangle)(|00\rangle + |11\rangle) = \frac{1}{2}\left[|00_A\rangle|00_B\rangle + |01_A\rangle|01_B\rangle + |10_A\rangle|10_B\rangle + |11_A\rangle|11_B\rangle\right]$$

- If the first pair is measured, and the result is 0, then the state becomes

$$\Psi_0 = \frac{1}{\sqrt{2}}(|00_A\rangle|00_B\rangle + |01_A\rangle|01_B\rangle)$$

  After both Alice and Bob apply U, the state becomes

$$\begin{aligned} \Psi_0' &= \frac{1}{2}\left[|00_A\rangle + |11_A\rangle)(|00_B\rangle + |11_B\rangle) + |01_A\rangle + |10_A\rangle)(|01_B\rangle + |10_B\rangle)\right] \\ &= \frac{1}{2}\left[|00_A\rangle|00_B\rangle + |00_A\rangle|11_B\rangle + |01_A\rangle|01_B\rangle + |01_A\rangle|10_B\rangle + \right. \\ &\quad \left. |10_A\rangle|01_B\rangle + |10_A\rangle|10_B\rangle + |11_A\rangle|00_B\rangle + |11_A\rangle|11_B\rangle\right] \end{aligned}$$

  Now we look at different possibilities of the measurement by Alice and Bob.

– Both Alice and Bob measure 0:
The resultant state is

$$\frac{1}{\sqrt{2}}(|\,00_A\rangle|\,00_B\rangle + |\,01_A\rangle|\,01_B\rangle) = (|\,0_A\rangle|\,0_B\rangle) \otimes \Phi^+$$

Bob does nothing and the second qubits are in Φ^+.

– Alice measures 0, and Bob measures 1:
The resultant state is

$$\frac{1}{\sqrt{2}}(|\,00_A\rangle|\,11_B\rangle + |\,01_A\rangle|\,10_B\rangle) = (|\,0_A\rangle|\,1_B\rangle) \otimes \Psi^+$$

After Bob does his flip, the second qubits will become Φ^+.

– Alice measures 1, and Bob measures 0:
The resultant state is

$$\frac{1}{\sqrt{2}}(|\,10_A\rangle|\,01_B\rangle + |\,11_A\rangle|\,00_B\rangle) = (|\,1_A\rangle|\,0_B\rangle) \otimes \Psi^+$$

After Bob does his flip, the second qubits will become Φ^+.

– Both Alice and Bob measure 1:
The resultant state is

$$\frac{1}{\sqrt{2}}(|\,10_A\rangle|\,10_B\rangle + |\,11_A\rangle|\,11_B\rangle) = (|\,1_A\rangle|\,1_B\rangle) \otimes \Phi^+$$

Bob does nothing and the second qubits are in Φ^+.

- If the first pair is measured and the result is 1, then the state becomes

$$\Psi_1 = \frac{1}{\sqrt{2}}(|\,10_A\rangle|\,10_B\rangle + |\,11_A\rangle|\,11_B\rangle)$$

  One can similar work out the transformation and different results after the measurements.

- If the second pair is measured, we also can work out the details. The only tricky part is when Alice and Bob get different results, then after Bob flips his qubit, the final state is in $\Phi^- = \frac{1}{\sqrt{2}}(|\,00\rangle - |\,11\rangle)$, instead of Φ^+.

So to summarize: the protocol will produce a fully entangled pair, which is Φ^+, except when the second qubit pair is measured and Alice and Bob obtains different results, in which case Φ^- is obtained.

■

We call this protocol the "Ambainis Protocol".

So this lemma can "sort of" purify 1 EPR pair, except the pair isn't always known. This result isn't good enough for teleportation, but if Alice and Bob just want fully-entanglement states, this is good enough.

However, now we can use the Hashing method in [BDS+96]: suppose Alice and Bob share $2n$ qubit pairs to start with, and these $2n$ qubit pairs are put into n pairs. Alice and Bob apply the Ambainis protocol to each of the n pairs. Then Alice and Bob share n pairs of fully entangled pairs, and at most of them is Φ^- while all the rests are Φ^+.

There are $(n+1)$ possibilities, and Alice and Bob can perform $\log(n+1)$ additional measurements to determine which is the case.

Notice the case here is actually simpler than in [BDS+96], since we have far fewer number of "typical sequences", namely, $(n+1)$ of them, and we know them explicitly. Also we are not dealing with the full Bell basis – just Φ^+ and Φ^-. Notice if we denote Φ^+ and Φ^- by 1 and 0, and look at their behavior under BXOR operation (see the middle of table 1 in [BDS+96]):

$$\begin{aligned} 00 &\longrightarrow 00 \\ 01 &\longrightarrow 11 \\ 10 &\longrightarrow 10 \\ 11 &\longrightarrow 01 \end{aligned}$$

So the total effect is like a CNOT gate with the second bit as control while the first bit as target — we call it a "macro CNOT", since this CNOT is actually working over 2 pairs of qubits, and only works for specific pairs. Notice the control/target direction is the opposite to the direction in the control/target direction in the BXOR operation.

The cleanest way to show how Alice and Bob can use $m = \lceil \log(n+1) \rceil$ measures to determine which pair is Φ^- is to assume Alice and Bob have m extra EPR pairs, all in state Φ^+ — they might have a small reserve of EPR pair "for emergency use".

Alice and Bob use binary search to locate the "bad" pair, which is a Φ^-. At first, Alice and Bob take the BXOR of the first $1/2$ of the pairs, putting the result in an extra EPR pair. Then Alice and Bob performs a measurement on the extra EPR pair — they can reliably distinguish a Φ^+ from a Φ^- state. Then they will know which half of the pairs contains the Φ^-. Notice this measurement is non-destructive: all the qubits, except the extra EPR pair, are preserved. So Alice and Bob can engage this binary-search for m times, consuming m extra EPR pairs, and determine where the Φ^- is. Then Alice and Bob perform a local operation to change Φ^- to Φ^+ (a simple σ_Z by Alice does this). Then Alice and Bob get n perfect EPR pairs back.

The yield of the procedure above is $n/(2n + \log n) \doteq 1/2$, and we are currently investigating possible procedures with yield close to 1.

Again Alice and Bob can be saved, if UQPS screws up one qubit.

6 Conclusion

We discussed the problem of extracting perfectly (or almost perfectly) entangled qubit pairs, or EPR pairs from partially entanglement bi-partite systems by using only local operations and classical communications. This problem is useful for teleportation, where perfect EPR pairs are needed for high fidelity.

We discussed this problem in different settings: identical copies of qubit pairs in pure state; identical copies of qubit pairs in mixed state; qubit pairs with unknown member measured. We demonstrated different techniques that are used for entanglement extraction, and compared their performance and quality. In the first 2 cases, the assumption that one has identical copies of pair is a great advantage, since the Law of Large Numbers can be utilized. In the 3rd case, a binary search is used to find the "faulty" place.

Some ideas in this paper are original (or at least found independently by the author): they include the recursive measurement method in section 3.1, and the idea for extracting entanglement from faulty qubit pairs (joint work with Andris Ambainis in UC Berkeley).

7 Epilogue

So finally Alice and Bob managed to produce 1,000 EPR pairs and teleported the qubits for CMUnited. With these secret 1,000 qubits, CMUnite defeated MIT 26:0 in the 2nd CMU vs. MIT annual RoboSoccer tournament. So everyone was happy :-)

References

[A01] Andris Ambainis, *Private communication.*

[BBP+96] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, *Concentrating partial entanglement by local operations*, In *Physical Review A*, vol. 53, No. 4, April 1996.

[BBP+96b] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters, *urification of Noisy Entanglement and Faithful Teleportation via Noisy Channels*, In *Physics Review Letters*, vol. 76, page 722, 1996.

[BDS+96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, *Mixed-state entanglement and quantum error correction.* In *Physical Review A*, vol. 54, No. 5, November 1996.

[H96] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki, *Distillability of Inseparable Quantum Systems.* In `quant-ph/9607009`.

[NC00] Michael Nielsen, Isaac Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.