In a course like this there is only a limited time, and only a limited number of topics can be covered. Some additional topics will be covered in the class projects. In this lecture, I will go (briefly) through several more, enough to give the flavor of some past and present areas of research.
Entanglement and LOCC

Entangled states are useful as a resource for a number of QIP protocols: for instance, teleportation and certain kinds of quantum cryptography. In these cases, Alice and/or Bob measure their local subsystems, transmit the results of the measurement, and then do a further unitary transformation on their local systems.

We can generalize this idea to include a very broad class of procedures: \textit{local operations and classical communication}, or \textit{LOCC} (sometimes written LQCC). The basic idea is that Alice and Bob are allowed to do anything they like to their local subsystems: any kind of generalized measurement, unitary transformation or completely positive map. They can also communicate with each other classically: that is, they can exchange classical bits, but not quantum bits.
Suppose Alice and Bob share a system in an entangled state $|\Psi_{AB}\rangle$. Using LOCC, can they transform $|\Psi_{AB}\rangle$ to a different state $|\Phi_{AB}\rangle$ reliably? If not, can they transform it with some probability $p > 0$? What is the maximum $p$?

We can measure the entanglement of $|\Psi_{AB}\rangle$ using the entropy of entanglement

$$S_E(|\Psi_{AB}\rangle) = -\text{Tr}\{\rho_A \log_2 \rho_A\}.$$  

It is impossible to increase $S_E$ on average using only LOCC. (It may be possible to raise $S_E$ with some probability, but only if the average over all outcomes is not higher.) $S_E$ is an entanglement monotone.

If $|\Psi_{AB}\rangle$ is unentangled, it is impossible to produce an entangled state using LOCC.
One very simple but profound result concerns asymptotic transformations. Suppose Alice and Bob have $N$ copies of $|\Psi_{AB}\rangle$ where $N \to \infty$, and want to produce $M$ copies of $|\Phi_{AB}\rangle$. This is only possible in general if

$$\frac{M}{N} \leq \frac{S_E(|\Psi_{AB}\rangle)}{S_E(|\Phi_{AB}\rangle)}.$$ 

In the limit of large $M, N$, this is reversible. So the entropy of entanglement really does seem to measure the total amount of entanglement in a state.

For single copies of a state, the rule is more complicated.
Single copy transformations

- It is not always possible to reliably transform one state to another, even if the second has lower entanglement. However, it is always possible to do so with some probability (unless the first state is unentangled), and the optimal procedures are known.

- Whether a state $|\Psi_{AB}\rangle$ can be transformed to $|\Phi_{AB}\rangle$ depends on the Schmidt coefficients of the two states.

$$|\Psi_{AB}\rangle = \sum \sqrt{p_j}|j\rangle_A|j\rangle_B, \quad |\Phi_{AB}\rangle = \sum \sqrt{q_j}|j\rangle_A|j\rangle_B.$$

We can transform $|\Psi_{AB}\rangle$ to $|\Phi_{AB}\rangle$ with $p = 1$ if the coefficients $\{q_j\}$ majorize the coefficients $\{q_j\}$. This is Nielsen's theorem. If not, the transformation has $p < 1$.

- There is thus a complete theory of bipartite pure state entanglement.
Mixed State Entanglement

While we understand bipartite pure state entanglement, there are many unanswered questions about mixed state entanglement. For example, with pure states, all of the entanglement used to prepare a state can be extracted again (in the limit of many copies of the system). With mixed states it cannot: generally, one can extract ("distill") strictly less entanglement than it takes to prepare a state. Indeed, there are some entangled mixed states from which no entanglement can be extracted. These are called bound entangled states.

Because of complications like this, there is no single obvious measure of entanglement for mixed states; and those measures which are known are not fully understood. Even determining whether a given mixed state is entangled or separable is difficult.
Classically, communication complexity problems have the following form: Alice and Bob are separated, and each of them has an $n$-bit number, respectively $x$ and $y$. They wish to calculate a function $f(x, y)$ such that one of them (say Alice) knows the result at the end. How many bits must be communicated to calculate this function? This generalizes to $M$ parties in an obvious way.

Obviously, Bob could just send his entire number $y$ to Alice, using $n$ bits of communication; so the maximum complexity is $n$. However, this is sometimes not necessary. Some functions require only a single bit of communication. For instance suppose $f(x, y)$ is the parity of the concatenated string $xy$. Bob need only send Alice the parity of his string $y$. Others require $n$ bits of communication; e.g., $f(x, y) = x \cdot y$. 
There are two ways to generalize this using quantum resources. First, the parties can communicate classically, but share some prior entanglement. Second, they can exchange quantum bits rather than classical bits. (Or both, of course.)

It turns out that in both these approaches there are some functions $f$ which have lower communication complexity using quantum resources than they do classically. For known instances, this advantage is only polynomial; but unlike most computational advantages, these quantum protocols are provably better than the best classical protocol.
In addition to allowing secret communication, cryptographic protocols are used for a variety of other purposes as well. These mostly have to do with either authentications (e.g., proving that a particular document was produced by a particular person) or interactions between parties which do not trust each other (e.g., remote gambling).

There are quantum versions of a number of these protocols, which we will examine briefly.
Secret sharing

In classical secret sharing, one encrypts some classical information (a string of bits) and divides up the encrypted bits among $n$ people so that any $m$ of them together can decrypt the information, but fewer than $m$ cannot. For example, we might encrypt the formula for Classic Coke and distribute it among the board of directors, so that (for example) any five of them can reconstruct the formula, but four or fewer cannot.

In the quantum version, suppose one has a particular quantum state $|\psi\rangle$; for simplicity, let it be the state of a single q-bit. We wish to share this state among $n$ parties, in such a way that any $m$ or more of them together can reconstruct the state, $(m < n)$, but fewer than $m$ can learn nothing about the state. This can be done using quantum error correction codes.
Use a code which encodes the state of one q-bit in \( n \), and can correct up to \( n - m \) errors. Each of the \( n \) parties receives one of these bits.

Suppose that \( m \) of the parties get together to try to reconstruct the state. They have \( m \) of the bits, but \( n - m \) bits are missing. These can be replaced by q-bits in the state \(|0\rangle\). It is now as if an erasure error has occurred to each of those \( n - m \) bits; by performing error correction and then decoding, the state \(|\psi\rangle\) can be recovered.

It is slightly less obvious that fewer than \( m \) parties can learn nothing about the state, but for a good code this must be true; otherwise, it is guaranteed by the no-cloning theorem that if the decoded state is completely undisturbed, no information can have been learned about it.
Bit commitment

Classical bit commitment would be a protocol of the following form: Alice chooses a random bit, and encrypts it in some way before sending it to Bob. This encryption would have the following two properties:

1. Bob cannot read the bit until he receives a key from Alice.
2. Alice cannot change the bit once she has sent it to Bob.

Bit commitment would be very useful for certain kinds of remote dealing between untrusting parties. For instance, in gambling over the internet, it would be nice to know that the casino can’t choose the outcome of the roulette spin depending on how one bets.
A physical scheme would have Alice write the bit on a piece of paper and then lock it in a safe, which she sends to Bob. Obviously, this is not absolutely secure: Bob can hire an expert safecracker. A better solution would be some type of cryptographic scheme.

Unfortunately, *no such scheme exists*. Every classical scheme lets either Alice or Bob cheat: either Bob can in principle decrypt the bit, or Alice can send two possible keys and choose the bit value after sending it.

There was a great deal of optimism, based on the success of quantum cryptography, that bit commitment would be possible using *quantum* resources. Schemes were put forward that seemed to work. But in fact, quantum bit commitment is *also* impossible, and for a very curious reason.
It turns out that Alice can almost always cheat by sending Bob half of an entangled pair. In a sense, she simultaneously commits to both 0 and 1. Before sending the key to Bob, she measures her half of the pair in a particular basis, and then based on the outcome sends one of two keys, depending on which result she wants him to find. A theorem showing this for a large class of protocols was proven by Lo and Chau.

In spite of numerous attempts to get around this loophole, no unconditionally secure scheme for quantum bit commitment has been demonstrated.

However, a somewhat weaker scheme is possible.
Remote Coin Flipping

One thing that bit commitment would allow is *remote coin flipping*: Alice and Bob are physically separated, and bet on the flip of a coin. If either of them flips the coin, they can cheat by lying to the other about the result.

Unlike bit commitment, here Alice and Bob only want to cheat in one direction: Alice wants the coin to be heads, and Bob wants it to be tails.

Surprisingly, this makes the problem solvable. Alice prepares and sends a state to Bob, and Bob measures it; this can be done in such a way that Alice’s probability of winning is no more that $1/2 + \varepsilon$, where $\varepsilon > 0$ can be made arbitrarily small.
Quantum computational complexity

The class of problems for which there is a uniform family of quantum circuits with polynomial size is called \textbf{BQP}, and is the quantum analogue to the class of polynomial classical problems \textbf{P} (or, more correctly, \textbf{BPP}).

What, then, is the quantum generalization of \textbf{NP}? Proposals have been made for classes \textbf{BQNP} or \textbf{QMA} which correspond to problems which are checkable in polynomial time by a quantum computer.

Many issues in classical complexity have quantum analogues that have been studied.
There are quantum analogues to NP-complete problems as well. Here is a canonical example:

The Local Hamiltonian Problem. Given a $k$-local Hamiltonian $\hat{H}$ on $n$ q-bits, where $k = O(1)$, and two numbers $0 \leq a < b$ with $b - a = \Omega(n^{-\alpha})$, $\alpha > 0$, does $\hat{H}$ have an eigenvalue not exceeding $a$, or are all eigenvalues of $\hat{H}$ greater than $b$?

By a $k$-local Hamiltonian, we mean a Hamiltonian which is a sum of terms, each of which affects no more than $k$ of the q-bits.

It is possible to prove that the Local Hamiltonian Problem is BQNP-complete.

There are many open questions about how quantum computers fit into the (generally believed) hierarchy of classical complexity classes.
The class of decision problems that can be solved efficiently on a quantum computer is called BQP. This class is known to include some problems in the class NP (in particular, factoring), but not NP-complete problems.

It has recently been conjectured that BQP not only includes problems in NP, but some problems that are outside of NP altogether. In fact, it is conjectured that BQP may include some problems that are outside the entire Polynomial Hierarchy (PH).

This would imply that the quantum complexity classes do not fit neatly into the usual classical complexity classes.
Quantum Coding Theory

A very active area of research is the theory of quantum error-correcting codes (QECCs). Much progress has been made in constructing new kinds of codes for both communication and computation, and proving results about fault-tolerance in quantum computing.

Quantum analogues have been found of many types of classical codes. One area of current interest is in quantum versions of modern codes, like Turbo codes, LDPC codes, and convolutional codes.

A new type of code are operator QECCs, which “correct” certain errors passively. These are hybrids between QECCs and decoherence-free subsystems. Another recent discovery are entanglement-assisted QECCs, which boost transmission rates using pre-shared entanglement.
New models of quantum computing

Beyond the circuit model that we have studied, several other models of quantum computing have been developed. Here are a few:

- **Cluster-state QC.** A collection of bits is prepared (by local interactions) in a massively entangled state. Computation can is done by a sequence of single-q-bit measurements.

- **Adiabatic QC.** The computer is prepared in the ground state of a known Hamiltonian, and this Hamiltonian is slowly changed; the ground state of the final Hamiltonian encodes the solution to a difficult problem. The superconducting D-Wave chip is designed to be a 128-q-bit adiabatic computer (though not for general-purpose calculations).
Quantum walks. These are unitary analogues of classical random walks, and may make new algorithms possible. It has been shown that some types of quantum walk are also universal for quantum computation.

Topological QC. Here the q-bits are states of quasiparticles called anyons in a two-dimensional quantum field. This type of computer would be intrinsically fault-tolerant. Such systems may exist in what is called the fractional quantum Hall effect, but this has not been experimentally demonstrated.

Linear Optical QC. Q-bits are made from photons in this scheme; a non-universal set of gates is constructed using linear-optical elements like beam splitters, mirrors, and polarization rotators. To get a universal set of gates one uses measurements.
Quantum Shannon Theory

Claude Shannon invented what we now call information theory. He studied the trade-offs between communication resources, such as noisy and noiseless channels, shared randomness, and side information. The asymptotic rates of these trade-offs include channel capacities and compressibility.

With quantum information there is a far richer set of resources: classical and quantum channels (with and without noise), shared entanglement, quantum states.

Studying the asymptotic rates of trade-offs among these resource is the subject of Quantum Shannon Theory, and has become a very active field of its own.
This is only a taste of the kind of problems that are being worked on in quantum information theory. Many facets of classical information theory and computer science have quantum extensions; and there are inherently quantum problems, as well, which have no simple classical analogue.

There has also been slow but steady improvement on the experimental side. Recent years have seen great improvements in ion traps, superconducting q-bits, quantum dots, and optical QC.

There has been tremendous progress in the last eighteen years. Quantum information processing has become a rich and beautiful theory. But in spite of all we have learned, there are very many areas yet to be explored.