Quantum Information: An Ongoing Research Program with Undergraduate Students

David W. Lyons

Lebanon Valley College

MAA MD/DC/VA Section Meeting
27 October 2012

Topics of This Talk

- What are quantum information and quantum computation?
- What is entanglement?
- What is the role of undergraduate students in research?

Information Theory: Abstract Study of Communication

What is communication?

What is communication?

Minimum ingredients

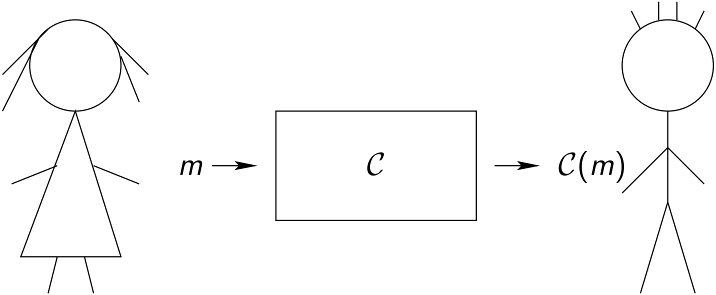
- Two parties: Sender and Receiver
- Message: Information to be sent
- Channel: Medium by which information is sent

Information Theory: Abstract Study of Communication

What is communication?

Minimum ingredients

- Two parties: Sender and Receiver
- Message: Information to be sent
- Channel: Medium by which information is sent



Theory of Computation: Abstract Study of Information Processing

What is computation?

Theory of Computation: Abstract Study of Information Processing

What is computation?

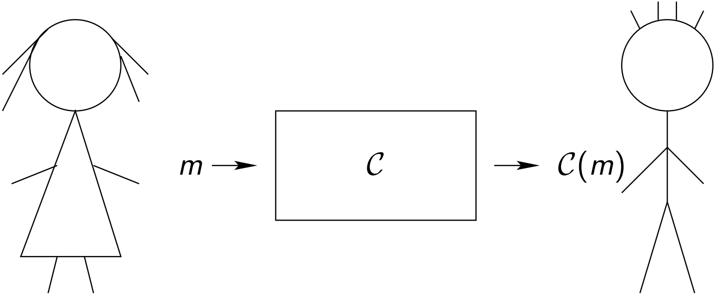
Minimum ingredients

- Input
- Processor or Computer
- Output

Theory of Computation: Abstract Study of Information Processing

What is computation?
Minimum ingredients

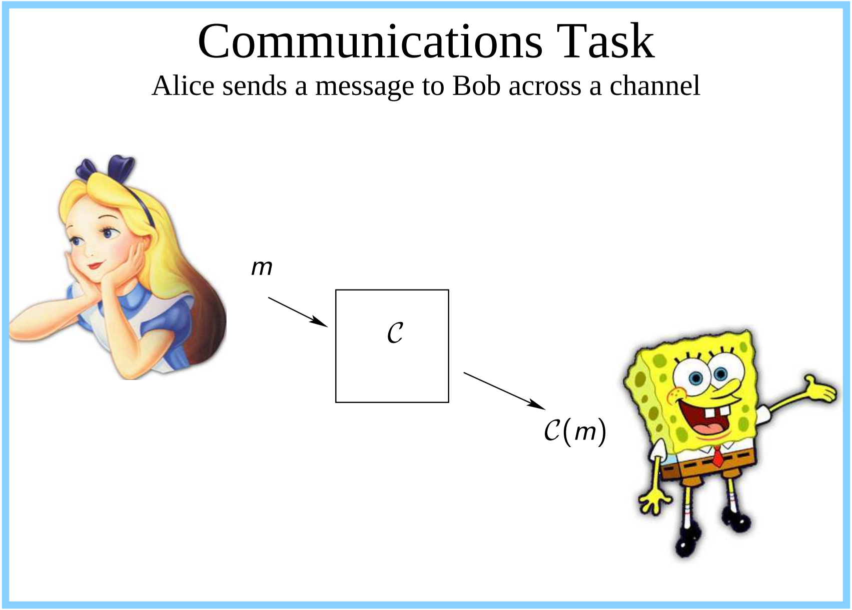
- Input
- Processor or Computer
- Output



Cultural note on sender and receiver

- Sender must be called "Alice"
- Receiver must be called "Bob"
- Slides must be funny

Typical information theory talk slide

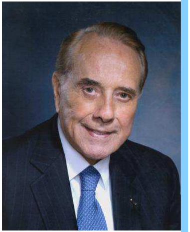


Improved information theory talk slide

Communications Task

Alice sends a message to Bob across a channel

$$m \longrightarrow \boxed{\mathcal{C}} \longrightarrow \mathcal{C}(m)$$



What are the problems of information and computation theory?

Theory of information

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?
- How do we ensure *privacy* between sender and receiver in the presence of (possibly malevolent) eavesdroppers?

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?
- How do we ensure *privacy* between sender and receiver in the presence of (possibly malevolent) eavesdroppers?

Theory of computation

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?
- How do we ensure *privacy* between sender and receiver in the presence of (possibly malevolent) eavesdroppers?

Theory of computation

- Invent algorithms to solve problems

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?
- How do we ensure *privacy* between sender and receiver in the presence of (possibly malevolent) eavesdroppers?

Theory of computation

- Invent algorithms to solve problems
- Classify "hardness", or degree of difficulty

What are the problems of information and computation theory?

Theory of information

- How much information can we pack into a message?
- In the real world, channels are *noisy*, subject to information distortion and loss. How do you keep the message intact in the presence of noise?
- How do we ensure *privacy* between sender and receiver in the presence of (possibly malevolent) eavesdroppers?

Theory of computation

- Invent algorithms to solve problems
- Classify "hardness", or degree of difficulty
- Characterize resources

What is information?

Classical information basic unit: the *bit*

Two bit states 0 and 1

What is information?

Classical information basic unit: the *bit*

Two bit states 0 and 1

Quantum mechanical information basic unit: the *quantum bit* or *qubit*

Quantum bit states are *superpositions*
of *both* classical bit states 0 and 1

What is information?

Classical information basic unit: the *bit*

Two bit states 0 and 1

Quantum mechanical information basic unit: the *quantum bit* or *qubit*

Quantum bit states are *superpositions*
of *both* classical bit states 0 and 1

The state of a quantum bit (or *qubit*) is a vector

$$av_0 + bv_1$$

in a 2-D complex vector space. Here a, b are complex constants and v_0, v_1 are basis states corresponding to the bits 0,1. For convenience we may use

$$v_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, v_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

so that the state vector $av_0 + bv_1$ is the column vector $\begin{bmatrix} a \\ b \end{bmatrix}$.

Dirac notation

"Ket" notation

Basis states are denoted $|0\rangle, |1\rangle$. A general state is denoted

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

(a, b are complex coefficients)

Dirac notation

“Ket” notation

Basis states are denoted $|0\rangle, |1\rangle$. A general state is denoted

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

(a, b are complex coefficients)

The inner product

Why kets? Because they go with “bra”s to make the bracket (bracket $=$ bra $+$ ket), the inner product. Given vectors $|\psi\rangle, |\phi\rangle$, their inner product is

$$\langle\psi|\phi\rangle.$$

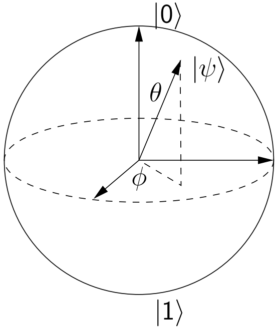
Bloch sphere model of the qubit

A qubit state vector $a\,|0\rangle + b\,|1\rangle$ can be put into standard form

$$\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$$

and there is a one-to-one correspondance between points on the surface of a sphere and qubit states given by spherical coordinates

$$(\theta, \phi) \longleftrightarrow \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$$



Composite Systems

Composite systems of many bits

Registers $A_1, \ldots, A_n$ with bit states $i_1, \ldots, i_n$ are jointly in state $i_1 i_2 \cdots i_n$

Example: Registers A, B, C in states $0, 1, 1$ are jointly in state 011

Composite Systems

Composite systems of many bits

Registers $A_1, \ldots, A_n$ with bit states $i_1, \ldots, i_n$ are jointly in state $i_1 i_2 \cdots i_n$

Example: Registers A, B, C in states $0, 1, 1$ are jointly in state 011

Composite systems of many qubits

Qubits A, B in states $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$ form a composite system AB in state

$$|\psi\rangle\,|\phi\rangle \quad = \quad (a\,|0\rangle + b\,|1\rangle)\,(c\,|0\rangle + d\,|1\rangle)$$

Composite Systems

Composite systems of many bits

Registers $A_1, \ldots, A_n$ with bit states $i_1, \ldots, i_n$ are jointly in state $i_1 i_2 \cdots i_n$

Example: Registers A, B, C in states $0, 1, 1$ are jointly in state 011

Composite systems of many qubits

Qubits A, B in states $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$ form a composite system AB in state

$$\begin{aligned} |\psi\rangle\,|\phi\rangle &= (a\,|0\rangle + b\,|1\rangle)\,(c\,|0\rangle + d\,|1\rangle) \\ &= ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \end{aligned}$$

Composite Systems

Composite systems of many bits

Registers $A_1, \ldots, A_n$ with bit states $i_1, \ldots, i_n$ are jointly in state $i_1 i_2 \cdots i_n$

Example: Registers A, B, C in states $0, 1, 1$ are jointly in state 011

Composite systems of many qubits

Qubits A, B in states $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\phi\rangle = c|0\rangle + d|1\rangle$ form a composite system AB in state

$$\begin{aligned} |\psi\rangle |\phi\rangle &= (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

In general, n-qubit states are linear combinations of vectors of the form $|i_1 i_2 \cdots i_n\rangle$ with complex coefficients. For example, any 3-qubit state has the form

$$a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$$

The power of superposition

Problem: Open a combination lock for which the combination is not known.

???

The power of superposition

Classical solution: Try all possible combinations, one at a time, until you find one that works. Let's say the solution is m_0.

m

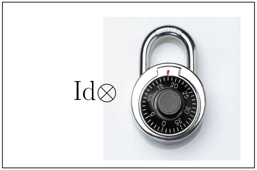
0 if $m \neq m_0$

1 if $m = m_0$

The power of superposition

Quantum solution: Try *all* possible solutions at the same time!

$\sum_m |m\rangle\, |m\rangle$



$$\sum_{m \neq m_0} |m\rangle\, |0\rangle + |m_0\rangle\, |1\rangle$$

The power of superposition

Quantum solution: Try *all* possible solutions at the same time!

$\sum_m |m\rangle\, |m\rangle$

$\mathrm{Id} \otimes$ 

$\sum_{m \neq m_0} |m\rangle\, |0\rangle$
$+ |m_0\rangle\, |1\rangle$

This leads to *quantum speedup*. But…then there's the fine print.

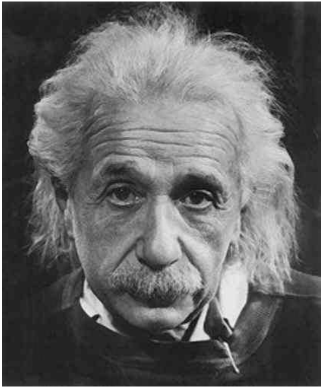
Quantum measurement

The only possible measurement we can perform on a qubit (up to change of basis) yields one of two results: 0 or 1.

Measuring a qubit in state $\alpha|0\rangle + \beta|1\rangle$ yields result 0 with probability $|\alpha|^2$ and yields result 1 with probability $|\beta|^2$.

Post measurement, the qubit is in state $|0\rangle$ or $|1\rangle$, depending on the outcome of the measurement. This is called the *collapse* of the quantum state.

Intellectual dissonance



"God does not play dice with the universe"

Entangled states

A state that is *not* a product

$|00\rangle + |11\rangle$ is not a product $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$ of any two 1-qubit states.

Entangled states

A state that is *not* a product

$|00\rangle + |11\rangle$ is not a product $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$ of any two 1-qubit states.

Proof. If it were, then

$$\begin{aligned} |00\rangle + |11\rangle &= (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

so we have $1 = ac = bd$. Thus a, b, c, d are all nonzero, but the cross terms $ad|01\rangle, bc|10\rangle$ are zero. This is impossible.

Entangled states

A state that is *not* a product

$|00\rangle + |11\rangle$ is not a product $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle)$ of any two 1-qubit states.

Proof. If it were, then

$$\begin{aligned} |00\rangle + |11\rangle &= (a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \end{aligned}$$

so we have $1 = ac = bd$. Thus a, b, c, d are all nonzero, but the cross terms $ad|01\rangle, bc|10\rangle$ are zero. This is impossible.

Definition of *entangled*

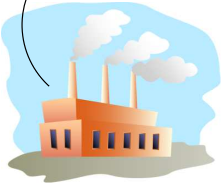
A multi-qubit state is *entangled* if it is not a product of states of proper subsystems. Otherwise a state is called a *product* state.

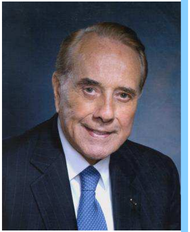
EPR Paradox

EPR Protocol Step 1

Factory prepares state $|00\rangle + |11\rangle$
Sends 1 qubit to Alice, 1 to Bob

$$|\psi\rangle = |00\rangle + |11\rangle$$

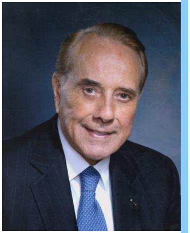




EPR Protocol Step 2

Alice measures his qubit

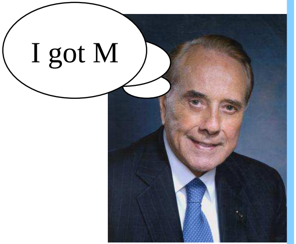
Post measurement state is $|MM\rangle$



EPR Protocol Step 3

Bob measures his qubit

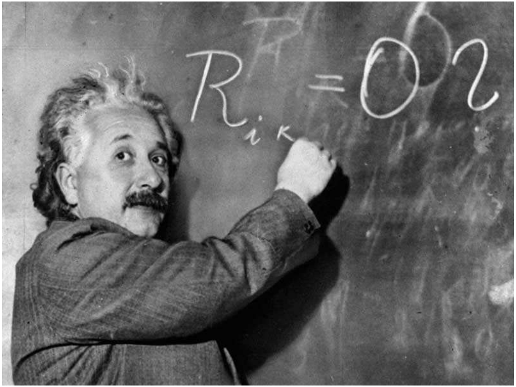
Post measurement state is $|MM\rangle$



EPR Paradox

Alice's measurement determines the result of Bob's. Even if they are separated by great distance.

Intellectual dissonance again!



"...spooky action at a distance"

Secure communication

Current best method: RSA encryption

Secure communication

Current best method: RSA encryption

Weakness: RSA relies on the fact that factoring large composite integers takes a long time. A quantum computer (running Shor's algorithm) will do this fast.

Secure communication

Current best method: RSA encryption

Weakness: RSA relies on the fact that factoring large composite integers takes a long time. A quantum computer (running Shor's algorithm) will do this fast.

Safer method?: Sending a secret message is *easy* if sender and receiver share a *secret key*, that is a long bit string known only to them.

- Alice prepares message M (a string of bits) and sends $M \oplus K$
- Bob decodes by calculating $M \oplus K \oplus K = M$

Secure communication

Current best method: RSA encryption

Weakness: RSA relies on the fact that factoring large composite integers takes a long time. A quantum computer (running Shor's algorithm) will do this fast.

Safer method?: Sending a secret message is *easy* if sender and receiver share a *secret key*, that is a long bit string known only to them.

- Alice prepares message M (a string of bits) and sends $M \oplus K$
- Bob decodes by calculating $M \oplus K \oplus K = M$

Example:

$$\begin{array}{ccc|c|c|c|c|c|c|c} M & = & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ K & = & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline M \oplus K & = & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}$$

Secure communication

New problem: How to share the secret key? This requires secure communication, but secure communication requires a secret key ...

Secure communication

New problem: How to share the secret key? This requires secure communication, but secure communication requires a secret key ...

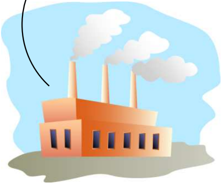
Solution: Quantum Key Distribution **(QKD)**

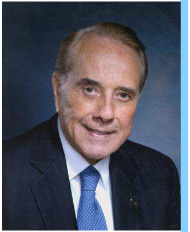
QKD Protocol: Step 1

Factory makes entangled 2−qubit state

Sends 1 qubit to Alice, 1 to Bob

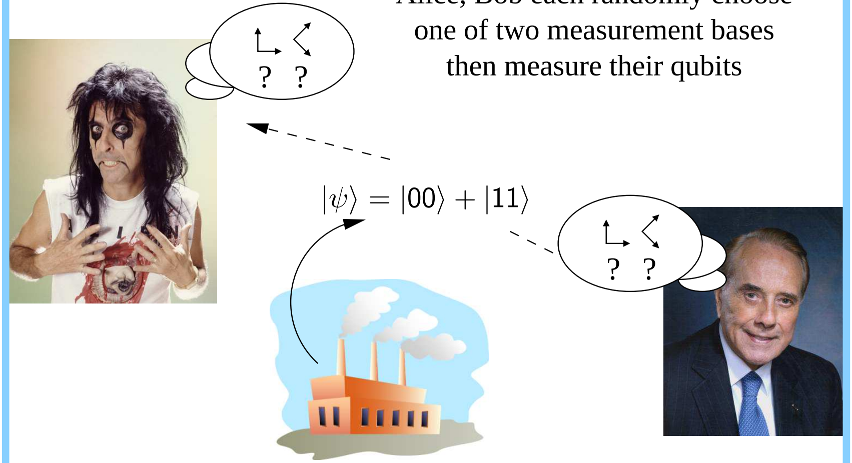
$$|\psi\rangle = |00\rangle + |11\rangle$$





QKD Protocol: Step 2

Alice, Bob each randomly choose
one of two measurement bases
then measure their qubits



Quantum Key Distribution

Repeat steps 1 and 2 many times. Alice and Bob record choices of measurement basis and results of each measurement. Note that whenever they choose the same basis (about half the time) they will get the same measurement result (EPR paradox). When they choose different bases, they agree half the time.

Quantum Key Distribution

Repeat steps 1 and 2 many times. Alice and Bob record choices of measurement basis and results of each measurement. Note that whenever they choose the same basis (about half the time) they will get the same measurement result (EPR paradox). When they choose different bases, they agree half the time.

Step 3: Using a public channel, Alice and Bob compare basis choice lists. They keep measurement bits for basis choices that agree (about half), and discard measurement bits for basis choices that differ. If there has been no eavesdropping, *remaining bit strings agree*.

Quantum Key Distribution

Repeat steps 1 and 2 many times. Alice and Bob record choices of measurement basis and results of each measurement. Note that whenever they choose the same basis (about half the time) they will get the same measurement result (EPR paradox). When they choose different bases, they agree half the time.

Step 3: Using a public channel, Alice and Bob compare basis choice lists. They keep measurement bits for basis choices that agree (about half), and discard measurement bits for basis choices that differ. If there has been no eavesdropping, *remaining bit strings agree*.

Step 4: Again using a public channel, Alice and Bob compare measurement results for a small substring of measurement outcomes. Any eavesdropping produces errors (disagreements). If Alice and Bob discover errors above some threshold, they abort the key and try again. If there are no errors, the remaining bits are their shared secret key K.

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Consequence: As soon as a quantum computer is built, the entire security infrastructure of today's internet is obsolete overnight

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Consequence: As soon as a quantum computer is built, the entire security infrastructure of today's internet is obsolete overnight

Secure quantum communication: fundamentally more secure than today's RSA encryption

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Consequence: As soon as a quantum computer is built, the entire security infrastructure of today's internet is obsolete overnight

Secure quantum communication: fundamentally more secure than today's RSA encryption

Non-additivity of quantum channel capacity: Two zero-capacity quantum channels can transmit a non-zero amount of information

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Consequence: As soon as a quantum computer is built, the entire security infrastructure of today's internet is obsolete overnight

Secure quantum communication: fundamentally more secure than today's RSA encryption

Non-additivity of quantum channel capacity: Two zero-capacity quantum channels can transmit a non-zero amount of information

Metrology: better clocks, rulers, telescopes . . .

Why study entanglement?

The EPR paradox says we should think hard about entanglement: if we believe in quantum mechanics, the world must be a very strange place!

Breakthrough discovery (Peter Shor 1994): Entangled states can be processed in unitary quantum logic gates to quickly factor large integers

Consequence: As soon as a quantum computer is built, the entire security infrastructure of today's internet is obsolete overnight

Secure quantum communication: fundamentally more secure than today's RSA encryption

Non-additivity of quantum channel capacity: Two zero-capacity quantum channels can transmit a non-zero amount of information

Metrology: better clocks, rulers, telescopes ...

GOAL: To measure entanglement and to classify types of entanglement

An approach to entanglement classification

A 2×2 unitary matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acts on a single qubit state $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$:

$$U|\psi\rangle = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{bmatrix} = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$$

An approach to entanglement classification

A 2×2 unitary matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acts on a single qubit state $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$:

$$U|\psi\rangle = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{bmatrix} = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$$

An n-tuple $U = (U_1, U_2, \ldots, U(n))$ of 2×2 unitary matrices acts on an n-qubit product state $|\psi\rangle = |\psi_1\rangle |\psi_2\rangle \cdots |\psi_n\rangle$ by

$$U|\psi\rangle = U_1|\psi_1\rangle \;\; U_2|\psi_2\rangle \cdots U_n|\psi_n\rangle$$

This is the *local unitary* **(LU)** group action.

An approach to entanglement classification

A 2×2 unitary matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acts on a single qubit state $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$:

$$U|\psi\rangle = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{bmatrix} = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$$

An n-tuple $U = (U_1, U_2, \ldots, U(n))$ of 2×2 unitary matrices acts on an n-qubit product state $|\psi\rangle = |\psi_1\rangle |\psi_2\rangle \cdots |\psi_n\rangle$ by

$$U|\psi\rangle = U_1|\psi_1\rangle \;\; U_2|\psi_2\rangle \cdots U_n|\psi_n\rangle$$

This is the *local unitary* **(LU)** group action.

Engtanglement types are *orbits* under this group action.

An approach to entanglement classification

A 2×2 unitary matrix $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ acts on a single qubit state $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$:

$$U|\psi\rangle = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a\alpha + b\beta \\ c\alpha + d\beta \end{bmatrix} = (a\alpha + b\beta)|0\rangle + (c\alpha + d\beta)|1\rangle$$

An n-tuple $U = (U_1, U_2, \ldots, U(n))$ of 2×2 unitary matrices acts on an n-qubit product state $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle \cdots |\psi_n\rangle$ by

$$U|\psi\rangle = U_1|\psi_1\rangle \;\; U_2|\psi_2\rangle \cdots U_n|\psi_n\rangle$$

This is the *local unitary* **(LU)** group action.

Engtanglement types are *orbits* under this group action.

Problem: Classify orbits of the local unitary group action on n-qubit quantum states.

An approach to entanglement classification

General strategy to classify orbits

- Find *invariants* that are constant along orbits.
- Find enough invariants to *distinguish* or *separate* orbits.

An approach to entanglement classification

General strategy to classify orbits

- Find *invariants* that are constant along orbits.
- Find enough invariants to *distinguish* or *separate* orbits.

Invariant theory can be hard

For the local unitary action on quantum states, the number of necessary invariants grows exponenetially in the number of qubits, and calculation is hard.

An approach to entanglement classification

A tractable invariant: the stabilizer

A local unitary element U *stabilizes* a state $|\psi\rangle$ if

$$U|\psi\rangle = |\psi\rangle$$

The set of all U that stabilizes $|\psi\rangle$ forms a subgroup of the local unitary group. The (conjugacy class of the) stabilizer subgroup is a local unitary invariant.

An approach to entanglement classification

A tractable invariant: the stabilizer

A local unitary element U *stabilizes* a state $|\psi\rangle$ if

$$U|\psi\rangle = |\psi\rangle$$

The set of all U that stabilizes $|\psi\rangle$ forms a subgroup of the local unitary group. The (conjugacy class of the) stabilizer subgroup is a local unitary invariant.

Two stage classification program

1. Classify (conjugacy classes of) stabilizer subgroups
2. For each class in that list, classify states that have that stabilizer

An approach to entanglement classification

A tractable invariant: the stabilizer

A local unitary element U *stabilizes* a state $|\psi\rangle$ if

$$U|\psi\rangle = |\psi\rangle$$

The set of all U that stabilizes $|\psi\rangle$ forms a subgroup of the local unitary group. The (conjugacy class of the) stabilizer subgroup is a local unitary invariant.

Two stage classification program

1. Classify (conjugacy classes of) stabilizer subgroups
2. For each class in that list, classify states that have that stabilizer

Stabilizer calculation can be reduced to solving linear systems of equations (using the Lie algebra of the local unitary matrix group).

Example: The GHZ state

The GHZ state

$$|\mathrm{GHZ}\rangle = |00\ldots0\rangle + |11\ldots1\rangle$$

is stabilized by matrices of the form

$$\left(\begin{bmatrix} e^{it_1} & 0 \\ 0 & e^{-it_1} \end{bmatrix}, \ldots, \begin{bmatrix} e^{it_n} & 0 \\ 0 & e^{-it_n} \end{bmatrix} \right)$$

where $\sum t_i = 0$, and is also stabilized by

$$\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)$$

Further, the entanglement type of the GHZ state is completely characterized by this set of stabilizing matrices. This shows how the entanglement type of a known important resource can be characterized by a group theoretic invariant.

LVC Math/Physics Group Summer 2012

Undergraduate students and research

Why do it?

- Real investigation is the most valuable learning experience
- Real investigation in the classroom is very limited
- Posters, talks and papers are great cv items
- It's fun
- Everybody benefits

Undergraduate students and research

Prerequisites

- Linear Algebra
- Supplement with carefully tailored notes and exercises

Student research activities

- Write, run code to calculate examples, run simulations
- Literature search
- Prove conjectures
- Write up results: notes, poster, paper(s)
- Do presentations: posters, talks

Undergraduate students and research

Advice

- Do it!
- Be an activist for support: money, time, credit, etc.
- Think hard and collect problems that undergraduates can work on
- Set goals, plan your calendar
- **Require** a presentation (poster, talk, paper, whatever)

THANK YOU

Visit us at our website
http://quantum.lvc.edu/mathphys