Notes on Classical & Quantum Error-Correcting Codes

April 18, 2018

P. Ramond

Lecture 6: Quantum Cryptography?

Transmitting information without fear of it being intercepted is obviously important. There are many schemes based on classical methods, which are used to this day. Does quantum mechanics offer new ways of shielding information from Eavesdroppers (generically called Eve)? It does in a very fundamental way. Interception means measurement, and measurement of a quantum signal necessarily disrupts it because of Heisenberg's uncertainty principle. All that is needed is then to invent algorithms where senders and recipients can quickly check the disruption and act accordingly. Quantum Mechanics offers additional advantages by providing faster algorithms to crack "impregnable" classical of the trap-door variety.

Wiesner

A graduate student at Columbia University, Stephen Wiesner, wrote in 1970 a paper entitled "Conjugate Coding" where he introduced a way of transmitting information using the principles of quantum mechanics. The paper was rejected, but was reprinted in 1983 when its importance was realized!

He was motivated by the uncertainty principle: knowing the momentum of a particle assures that nothing is known about its position, and vice-versa. He invents communication channels which have no analog in classical physics.

Wiesner presents two examples:

- "A means of transmitting two messages either but not both of which may be received": sender transmits two messages A and B to one recipient in such a way that he/it/she can decide which message to read (A or B). Reading A destroys the other message B irreversibly, and vice-versa.

- "Money that it is impossible to counterfeit".

Wiesner transmits information using polarized light going through light fibers. Measuring photon polarizations uses devices which single out two classes of polarizers, linear and circular polarizations. In quantum mechanics each uses a convenient basis in the two-dimensional Hilbert space of each photon.

Wiesner singles out three "mutually conjugate bases"

– rectilinear basis $(0^\circ,\ 90^\circ):\quad |\leftrightarrow\rangle,\ \ |\updownarrow\rangle,$

– diagonal basis $(45^\circ,\ 135^\circ):\quad \frac{1}{\sqrt{2}}\big(|\leftrightarrow\rangle+|\updownarrow\rangle\big),\quad \frac{1}{\sqrt{2}}\big(|\leftrightarrow\rangle-|\updownarrow\rangle\big),$

– circular basis: $\quad |\circlearrowright\rangle=\frac{1}{\sqrt{2}}\big(|\leftrightarrow\rangle+i|\updownarrow\rangle\big),\quad |\circlearrowleft\rangle=\frac{1}{\sqrt{2}}\big(|\leftrightarrow\rangle-i|\updownarrow\rangle\big)$

Measuring a photon state in any of these basis introduces maximum uncertainty ($50-50$ or "kif-kif") in the conjugate basis.

The characteristic of conjugate bases is that the projection of the basis state on those of conjugate basis have the same magnitude, as can easily be checked. In general, two orthonormal bases $|\,a_i\,\rangle$ and $|\,b_i\,\rangle$, $i=1,2\ldots N$ are mutually conjugate if

$$|\langle a_i|\,b_j\,\rangle|^2=\frac{1}{N}.$$

It follows that

$$\langle\psi|\,a_i\,\rangle=\sum_j\langle\psi|\,b_j\,\rangle\langle b_j|\,a_i\,\rangle=\frac{1}{\sqrt{N}}\sum_j\langle\psi|\,b_j\,\rangle.$$

All probabilities are equal, resulting in maximum uncertainty $1/\sqrt{N}$.

Consider an unpolarized (white) light beam impinging on a calcite crystal (analyzer) which splits it into two beams with different polarizations, each detected by different (upper and lower) photomultipliers.

Their polarizations depend on the analyzer . Wiesner consider two types, R and C: R splits to ($\leftrightarrow$, $\updownarrow$), and C splits to ($\circlearrowright$, $\circlearrowleft$).

Assume that the incoming beam, polarized along $\leftrightarrow$,:

- hits analyzer R: one beam emerges, polarized along $\leftrightarrow$

- hits analyzer C: two beams emerge, one polarized as $\circlearrowright$, the other as $\circlearrowleft$

What happens when the incoming beam is replaced by well-separated one-photon bursts? Quantum Mechanics must be invoked: suppose the incoming one photon states are polarized in the rectilinear basis, $\mid \leftrightarrow \rangle$ or $\mid \updownarrow \rangle$, as the sender chooses.

- If the incoming photon $\mid \leftrightarrow \rangle\rangle$ hits analyzer R, only the upper light detector will be hit; if the incoming photon is in the $\mid \leftrightarrow \rangle$ state, only the lower detector will light up. The outcome is totally deterministic.

- If the incoming photon $\mid \leftrightarrow \rangle\rangle$ hits analyzer C, it will either be detected by the upper or by the lower photomultiplier. This is not deterministic as there is no way to know which of the two detectors will be activated for any given event. However, if the experiment is repeated many times, the lower and upper detectors will record the same number of hits, because the incoming photon and the analyzer are set in conjugate bases.

Wiesner applies these considerations to communications, and assigns a 0 or 1 for an incoming photon in $\mid \leftrightarrow \rangle\rangle$ or in $\mid \updownarrow \rangle$.

- With the R analyzer, the outcome is deterministic: 0 (1) means the upper (lower) detector is hit, and the information is transmitted.

- With the C analyzer, the outcome is a hit on either the upper or lower detector, each with equal probability, so that there is maximum uncertainty in the transmission. Information about the incoming signal is irretrievably lost!

With each one-photon burst, the recipient of the signal finds that only one detector gets hit, and so he/she/it does not know how to interpret it, unless the recipient has information from the sender.

In his paper Wiesner uses this mechanism to send two messages, each a string of zeroes and ones. For the first message, the incoming photons are rectilinearly polarized and for the second message they are circularly polarized. For each one-photon emission he/she/it decides by flipping a coin which message to send.

The recipient can use either analyzer R or C, and can randomize which analyzer to use for each burst.

It follows that if the one photon state is prepared in a given basis, for instance rectilinear, then when it is measured by an analyzer set up in a conjugate basis, the measurement puts it in the measured basis, resulting in maximum uncertainty.

This process was called quantum multiplexing, by which Brassard means that the sender sends two messages to a recipient who decides which message to read, at the cost of destroying the other message. Others called it "Oblivious transfer.

Quantum Money

Wiesner now applies this principle to produce "quantum money", made of bills that contain N two-dimensional Hilbert spaces.

At the mint each bill is given not only a serial number as is normally done, but also a quantum signature. Start with a number of isolated systems. Place each in four possible states determined as follows: generate two binary random sequences $M = \{m_i\}$ and $N = \{n_i\}$ with $i = 1, 2, \ldots, N$. For a given i, there are four possible states attached to (m_i, n_i):

$$(0,0) \quad \Rightarrow \quad |\leftrightarrow\rangle; \qquad (0,1) \quad \Rightarrow \quad |\updownarrow\rangle$$

$$(1,0) \quad \Rightarrow \quad |\circlearrowright\rangle; \qquad (1,1) \quad \Rightarrow \quad |\circlearrowleft\rangle$$

When the money is returned to the bank, the initial setting is checked to verify that the bill has not been modified.

Suppose a counterfeiter wants to duplicate the bill. Although he/it/she knows that there are N quantum states on the bill, what measurement to make? The forger goes ahead anyway and make a measurement, but a measurement that distinguishes $|\leftrightarrow\rangle$ from $\updownarrow$ destroys all information about the circular states. For each i there is a 25% chance of being wrong, so that the probability of being right, $(.75)^N$, is very small for large N.

Cryptography

This year celebrates the 100th anniversary of the Vernam cypher, named after Gilbert Vernam, an AT&T engineer. The sender and recipient are called Alice and Bob in crypto jargon.

To encode and decode N messages, Alice and Bob share N different strings of numbers. Each string is called a one-time pad because it is used for one message only ; it is Encoding of the message proceeds in two steps: Alice maps the letters into numbers using a letter-number dictionary; the numbers are added to the one-time pad without carry-over.

Alice sends the encoded string to Bob who proceeds in the inverse order to read the message: subtract the one-time pad and use the dictionary between numbers and letters. After encoding and decoding, Alice and Bob destroy the one-time pad used for that message.

In the Vernam cypher, the letter-number dictionary is the "Public Key", and the one-time pad is the "Private Key". It uses the same one-time pad to encode and decode the message. It is a symmetric cypher where Alice and Bob share the same "private key". This cypher has been used widely by spies and diplomats the world over. It is fool-proof but pretty ackward as the length of the private key is the same size as the message.

BB84

'Public Key Cryptography" (PKC) describes a class of cyphers: Alice has two "keys", one public, the other private; the private key is Alice's own and acts as the inverse of the public key; it is designed to decode a message encrypted by the public key.

When Bob receives the public key, he uses the public key to encode a message and sends it to Alice. Alice uses her private key to decode the message. Et voilà!

In 1984, Bennett and Brassard adapt the Wiesner ideas to PKC. Their actual "BB84" proposal for the private key is as follows:

Alice sends to Bob a sequence of single photons either rectilinearly (R) or circularly (C) polarized. She keeps track of the sequence of R&Ds.

Bob does the same thing, setting randomly his analyzer to R or C before every burst. He also keeps track of his sequence.

Alice and Bob compare their sequences using open classical channels. When they agree, that is R&R or C&C for say the *ith* photon, they know that the information sent by Alice is correctly transmitted; at no point do they specify if it was a one or a zero. When they disagree as in R&D or D&R, Bob knows that, even though the photon always hits one of the detectors, the information is garbage. Information has been safely transmitted.

Suppose ever snooping eavesdropper "Eve" intercepts the quantum message; it is necessarily corrupted by her measurement. When Bob and Alice compare their lists of safely transmitted zeros and ones, they may notice that for example the list fails a crude parity check.

Threshold Schemes

I want to send to my trusted interlocutor a message. I do not trust the channels or couriers at my disposal, so I split the full message into n shares, cleverly devised so that it takes at least k shares to recover the information. These protocols are called $((k, n))$ threshold schemes, with $k \leq n$.

Cleve, Gottesman and Lo invented in 1999 a $((k, n))$ quantum threshold scheme.

They introduce a 27-dimensional Hilbert space spanned by three qutrits $|\, i\, j\, k\,\rangle = |\, i\,\rangle_1 \otimes |\, j\,\rangle_2 \otimes |\, k\,\rangle_3$, where $i, j, k = 0, 1, 2$ belong to $GF(3)$ with (mod 3) composition.

The (secret) message lives in the first qutrit,

$$|\,\psi\,\rangle = \alpha|\,0\,\rangle_1 + \beta|\,1\,\rangle_1 + \gamma|\,2\,\rangle_1.$$

Define a nine-dimensional subspace spanned by the orthonormal $|\,\bar{i}\,\rangle_{123}$ on all three qutrits,

$$\begin{aligned}
|\,\bar{0}\,\rangle &= \frac{1}{\sqrt{3}}(|\,000\,\rangle + |\,111\,\rangle + |\,222\,\rangle), \\
|\,\bar{1}\,\rangle &= \frac{1}{\sqrt{3}}(|\,012\,\rangle + |\,120\,\rangle + |\,201\,\rangle), \\
|\,\bar{2}\,\rangle &= \frac{1}{\sqrt{3}}(|\,021\,\rangle + |\,102\,\rangle + |\,210\,\rangle),
\end{aligned}$$

and introduce the unitary operator $\mathcal{U}_{12}$ acting on the first and second qutrits according to,

$$\mathcal{U}_{12}: \quad |\, i\,\rangle \otimes |\, j\,\rangle \quad \longrightarrow \quad |\, 2i+j\,\rangle \otimes |\, i+j\,\rangle,$$

$$\mathcal{U}_{12}^{\dagger}: \quad |\, i\,\rangle \otimes |\, j\,\rangle \quad \longrightarrow \quad |\, i-j\,\rangle \otimes |\, 2i-j\,\rangle,$$

with all (mod 3) operations. For example $|\, 10\,\rangle \to |\, 21\,\rangle$.

The "raison d'être" of $\mathcal{U}_{12}$ is to change the barred basis kets into basis kets of the first qutrit,

$$\mathcal{U}_{12}|\,\bar{i}\,\rangle = |\, i\,\rangle_1 \otimes \frac{1}{\sqrt{3}}(|\, 00\,\rangle_{23} + |\, 21\,\rangle_{23} + |\, 12\,\rangle_{23}).$$

Then on a three-qutrit state,

$$|\,\bar{\psi}\,\rangle = \alpha|\,\bar{0}\,\rangle + \beta|\,\bar{1}\,\rangle + \gamma|\,\bar{2}\,\rangle$$

the action of $\mathcal{U}_{12}$ is,

$$|\,\psi'\,\rangle = \mathcal{U}_{12}|\,\bar{\psi}\,\rangle = (\alpha|\,0\,\rangle_1 + \beta|\,1\,\rangle_1 + \gamma|\,2\,\rangle_1) \otimes (|\, 00\,\rangle_{23} + |\, 21\,\rangle_{23} + |\, 12\,\rangle_{23}),$$

where the last two entries of the ket always appear in the same linear combination, and the message has been transferred to the first qutrit.

One can define unitary operators $\mathcal{U}_{13}$ and $\mathcal{U}_{23}$ which act on the first and third qutrits and second and third qutrits, respectively, with similar results.

The quantum sharing procedure encodes an arbitrary state in a three-dimensional Hilbert space into another three-dimensional Hilbert space spanned by the barred basis,

$$|\,\psi\,\rangle = \alpha|\,0\,\rangle_1 + \beta|\,1\,\rangle_1 + \gamma|\,2\,\rangle_1 \quad \to \quad |\,\bar{\psi}\,\rangle_{123} = \alpha|\,\bar{0}\,\rangle_{123} + \beta|\,\bar{1}\,\rangle_{123} + \gamma|\,\bar{2}\,\rangle_{123}.$$

In the CGL scheme, $|\,\bar{\psi}\,\rangle_{123}$ is broken up into three shares each pertaining to a different qutrit.

Since the coding and decoding is done by unitary operators which acts on two different qutrits, a courier with knowledge of one qutrit alone will not be able to reconstruct the message. Two couriers can get together and enact the unitary operators $\mathcal{U}_{ab}$ to read the message.

There is a close connection with error-correcting codes which allow information with errors to be reconstructed; in this case knowledge of the third qutrit is not necessary to decode, just like a code with one error reconstruction.

Quantum Teleportation

Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wooters, *Phys. Rev. Lett.* **70**, 1895 (1993), proposed a method to transport a quantum state from one place to another without destroying it. They use a very special ancilla, two spins, correlated into an EPR pair.

The scheme requires three spin one-half particles, living in different two-dimensional Hilbert spaces, each is spanned by orthogonal $|\uparrow\rangle_a$, $|\downarrow\rangle_a$, $a = 1, 2, 3$.

Alice wants to send to Bob the quantum state of the first spin one-half particle, which lives in the first Hilbert space with ket,

$$|\phi\rangle_1 = a|\uparrow\rangle_1 + b|\downarrow\rangle_1.$$

The second and third Hilbert spaces sustain an entangled EPR pair of two other spin one-half particles,

$$|\psi^{\rm EPR}\rangle_{23} = \frac{1}{\sqrt{2}}\big[|\uparrow\rangle_2|\downarrow\rangle_3 - |\downarrow\rangle_2|\uparrow\rangle_3\big],$$

the two spin one-half state with zero total angular momentum. There are three more two-spinor states with total angular momentum equal to one, but they do not appear in the ancilla.

Alice begins with the state vector of the three particles in the EPR ancilla,

$$|\Psi\rangle_{123} = |\phi\rangle_1 \otimes |\psi^{\rm EPR}\rangle_{23}.$$

Alice can perform measurements on this state, but she has access only to the first two spinors. She decides to organize them in terms of their total angular momentum,

$$|\psi^{\rm EPR}\rangle_{12} = \frac{1}{\sqrt{2}}\big[|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2\big],$$

together with three state vectors of total angular momentum one,

$$\begin{aligned} |\Phi^{(0)}\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_2|\uparrow\rangle_1\big), \\ |\Phi^{(\pm)}\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\uparrow\rangle_1|\uparrow\rangle_2 \pm |\downarrow\rangle_1|\downarrow\rangle_2\big). \end{aligned}$$

These four states form an orthonormal basis. Alice's expansion in this basis is,

$$
\begin{aligned}
|\,\Psi\,\rangle_{123} &= |\,\psi^{\rm EPR}\,\rangle_{12}\otimes\big(-a|\uparrow\rangle_3-b|\downarrow\rangle_3\big)+|\,\Phi^{(0)}\,\rangle_{12}\otimes\big(-a|\uparrow\rangle_3+b|\downarrow\rangle_3\big)\\
&\quad +|\,\Phi^{(+)}\,\rangle_{12}\otimes\big(-b|\uparrow\rangle_3+a|\downarrow\rangle_3\big)+|\,\Phi^{(-)}\,\rangle_{12}\otimes\big(b|\uparrow\rangle_3+a|\downarrow\rangle_3\big),\\
&\equiv \sum_{i=1}^{4}|\,i\,\rangle_{12}|\,\phi^i\,\rangle_3.
\end{aligned}
$$

Alice decides to perform a von Neumann experiment, that is by "collapsing" the state vector in four equally probable fashion. For each, Bob receives four states for the third particle

$$
\begin{aligned}
|\,\phi^1\,\rangle_3 &= -|\,\phi\,\rangle_3, \qquad\qquad |\,\phi^2\,\rangle_3=\begin{pmatrix}-1&0\\0&1\end{pmatrix}|\,\phi\,\rangle_3,\\
|\,\phi^3\,\rangle_3 &= \begin{pmatrix}0&1\\1&0\end{pmatrix}|\,\phi\,\rangle_3, \quad |\,\phi^4\,\rangle_3=\begin{pmatrix}0&-1\\1&0\end{pmatrix}|\,\phi\,\rangle_3.
\end{aligned}
$$

In the first case where Alice measures with the EPR pair, the third particle is, up to an overall minus sign in the same state as the first particle was, but now Bob has it. Alice destroyed it by her measurement but it reappears unscather in Bob's hand.

Bob does not know a priori which of these four states Alice has collapsed, but Alice informs by snail mail which experiment she has performed, and also provides the (2×2) matrix appropriate for each case.

By a combination of quantum magic, and classical snail mail, Alice has teleported the state of the first particle into the exact same state of the third particle which Bob can read. The quantum state has not been destroyed, just transmitted unscather to Bob.

RSA Encryption

Encoding and decoding schemes of secret messages had traditionally been symmetric between senders and receivers. In 1970, James Ellis, at the Government Communications Headquarters (GCHQ), UK's equivalent of US's NSA, suggested that non-secret encryption and decryption could be asymmetric.

The next step belonged to Clifford Cocks who invented in 1973 the concept of a trap door, using prime number factorization. However his invention was kept secret by GCHQ.

In 1977, unaware of Ellis and Cocks' previous work that was classified, Ronald Rivest, Adi Shamir, and Leonard Adleman (re-)invented the trap-door scheme.

Let G_p denote the positive integers up to $p-1$, where p is a prime. Fermat's little theorem states that if $a \in G_p$, then

$$a^{(p-1)} = 1, \pmod{p}.$$

To see this, use recursion. Suppose that $b^p = b \pmod{p}$. Let $a = (1+b)$ and expand: $a^p = (1+b)^p = 1 + \cdots + b^p = (1+b) = a, \pmod{p}$, because the dots are terms proportional to p. It extends to two primes, p and q,

$$\left[a^{(p-1)}\right]^{(q-1)} = \left[a^{(q-1)}\right]^{(p-1)} = 1 \pmod{pq}.$$

Raise this equation to an integer power k and multiply it by a to get

$$a^{1+k(p-1)(q-1)} = a \pmod{pq}.$$

Let c be an integer in $G_{(p-1)(q-1)}$ with no factor in common with $(p-1)(q-1)$. Its inverse d must also be in $G_{(p-1)(q-1)}$. Setting $cd = 1 + k(p-1)(q-1)$, yields

$$a^{cd} = 1 \pmod{pq}.$$

It follows that

$$b \equiv a^c \pmod{pq}, \quad \longrightarrow \quad b^d \equiv a \pmod{pq}.$$

This is the basis of the RSA scheme, where a is the message, $N = pq$ and c are the public keys, and d is the private key.

A later version of the RSA scheme uses Euler's totient function defined as

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

with the product taken over prime numbers that divide n. It counts the positive integers up to a given integer n that are relatively prime to n. For any two integers m and n, the totient function is multiplicative,

$$\varphi(mn) = \varphi(m)\varphi(n),$$

and for prime p,

$$\varphi(p) = (p-1); \quad \varphi(p^k) = p^{k-1}(p-1).$$

Euler's theorem states that if a and n are relative primes then

$$a^{\varphi(n)} = 1 \pmod{n}.$$

It reduces to Fermat's little theorem when n is prime,

Encryption Procedure

Bernard picks two primes, p and q, and an integer c which has no common factors with $(p-1)(q-1)$. He computes its inverse d, with $cd = 1, (\text{mod } n = pq)$.

Bernad sends $n = pq$ and c to Alice, but **not** the individual primes. n and c are the public key of the RSA scheme.

Alice wants to send a message m. She forms the integer $b = m^c, \pmod{n}$, and sends it to Bernard.

After receiving b, Bernard who knows d, easily finds m by taking the dth power of b since

$$b^d = m^{cd} = m \pmod{n}.$$

The only pieces of data made public were the N and c by Bernard, and b by Alice.

All three could have been intercepted by Eve(sdropperskova). However, knowing only n and c, she does not know how to get

$$d = \frac{1 + k(p-1)(q-1)}{c} = \frac{1 + k\varphi(n)}{c},$$

because it requires knowing $\varphi(n)$. For very large n this could take as much time as the age of the universe!

Peter Shor (again!) comes to the rescue, and proposes an algorithm where the factoring could be done much faster than the exponential time of classical search protocols. Big money came to the field of quantum computing!