Malaysia, November 2009.

Quantum Information, Introduction:

one qubit, two qubits, entanglement and applications.

Thomas Durt.

TONA VUB Pleinlaan 2 1050 Brussels.

Quantum Information- An introduction and a survey.

The basic idea of Quantum Information Theory is that Quantum Mechanics allows us to perform tasks that would be impossible or more difficult to realize by using classical systems. It is motivated by the recognition of specifically non-classical features exhibited by quantum systems, such as **“entanglement”** and **“complementarity”**.

The signature of entanglement consists of very special correlations that cannot be simulated thanks to classical (in the sense of **“local realistic”**) systems. Recent experiments show that the ability to simulate such correlations with realistic systems would require the technological ability to send signals at more than **one million times the speed of light**, in clear contradiction with relativistic causality (or locality). (SECTION 1)

Quantum cryptography (SECTION 2) constitutes a first application that makes use of the resource offered by entanglement: due to the fact that, as a consequence of the violation of local realism, the quantum correlations between entangled systems do not exist prior to the measurement process but are created during it, quantum information is to some extent ubiquitous. This information cannot always be located in a single place, and it can also be shown that it cannot be perfectly cloned (APPENDIX 1). This property can be exploited in order to renew a secret cryptographic key. The security of this exchange is guaranteed by Heisenberg uncertainties, which are an aspect of Bohrian complementarity.

The non-local correlations between entangled systems do not vanish with the distance which renders possible the experimental realisation of the so-called **quantum teleportation** or **dense coding** protocols (SECTION 3), a process during which quantum information (the direction of photonic polarisation for instance) gets teleported over macroscopic distances without any kind of material or even spatial support. During a quantum teleportation process, everything happens as if the information instantaneously jumped from one place to the other. These protocols reflect the properties of the generalised Pauli or discrete Heisenberg-Weyl group that possesses numerous applications in Quantum Information (like cloning machines and entanglement swapping that are also presented in the same section).

In SECTION 4 we show how the Galois machinery, in conjunction with properties of the Hesienberg-Weyl group makes it possible to find a solution to the Mean King's problem which ultimately leads to a discrete phase space picture of finite dimensional Hilbert spaces.

It also brings us naturally to conjecture that a deep connection exists between the existence problem of MUB and a combinatorial problem related to the existence of affine structures.

In SECTION 5 we present a totally different application of the (cyclic version of) the generalised Pauli group: SIC POVM's which present promising applications in Quantum Key Distribution and Quantum Tomography as well...

SECTION 1: Basic concepts of Quantum Information.

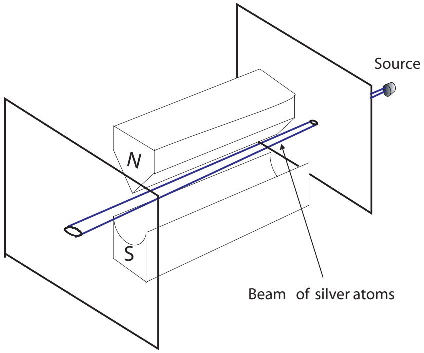
1A. A generic example of discrete Quantum Variable:

the qubit.

Landauer (1961): Information has physical nature.

- Two-level quantum systems (QUBITS) generalize classical binary valued quantities (BITS) thanks to the superposition principle.
- Quantum cats can be ”simultaneously” living and dead,
- quantum bits (qubits) can simultaneously take values 0 and 1
- the possibility to create quantum superpositions offers more flexibility in comparison to classical bits.

Example 1: spin 1/2 particles.



Stern-Gerlach measurement of the spin component along Z.

- Two possible results
- spin up, state $|+\rangle_Z$
- spin down, state $|-\rangle_Z$
- A qubit state is a superposition of the two possible states:
  $|\psi\rangle = \alpha|+\rangle_Z + \beta|-\rangle_Z$
  $(|\alpha|^2 + |\beta|^2 = 1.)$
- The probability to obtain an outcome spin up is $|\alpha|^2$.
- The probability to obtain an outcome spin down is $|\beta|^2$.

Example 2: photonic polarisation states.

- Photonic polarisations also constitute a quantum two-level system; they are massively used in Quantum Information.
- They are described by the same mathematical tools as spin 1/2 systems.
- -for instance we can represent linear horizontal (vertical) polarisation states by the kets $|+_Z\rangle$ ($|-_Z\rangle$)
- -photons with diagonal (45 (135)) polarisation correspond to the states $|+_X\rangle = \frac{1}{\sqrt{2}}(|+_Z\rangle + |-_Z\rangle$ ($|-_X\rangle = \frac{1}{\sqrt{2}}(|+_Z\rangle - |-_Z\rangle)$)
- -left and right circular polarisations correspond to the states $|+_Y\rangle = \frac{1}{\sqrt{2}}(|+_Z\rangle + i|-_Z\rangle$ and $|-_Y\rangle$=$\frac{1}{\sqrt{2}}(|+_Z\rangle - i|-_Z\rangle$.
- Here X Y and Z are orthogonal directions of a 3 dimensional Cartesian frame (Bloch frame, we shall come to it later).

- The equivalent of a Stern-Gerlach measurement, when qubits are polarisations is a “polarisation beam splitter” with two outcome channels and two photo-detectors.

- The measurements of (horizontal/vertical; diagonal45/diagonal135 and circular left circular right) polarisations correspond to the following hermitian operators (observables)
  $\sigma_X = (|+\rangle_X\langle+|_X - |-\rangle_X\langle-|_X)$,
  $\sigma_Y = (|+\rangle_Y\langle+|_Y - |-\rangle_Y\langle-|_Y)$ and
  $\sigma_Z = (|+\rangle_Z\langle+|_Z - |-\rangle_Z\langle-|_Z)$.
  We find by direct computation that
  $\sigma_X = (|+\rangle_Z\langle-|_Z + |-\rangle_Z\langle+|_X)$
  $\sigma_Y = i(|+\rangle_Z\langle-|_Z - |-\rangle_Z\langle+|_Z)$
  $\sigma_Z = (|+\rangle_Z\langle+|_Z - |-\rangle_Z\langle-|_Z)$.

Remark.

In a matricial form these operators are written as:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \text{and } \sigma_{\mathrm{z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

These are the famous σ operators of Pauli...

Wolfgang Pauli.

Remark.

- It is possible to encode BINARY information in a TWO-LEVEL system, then we call this system a qubit and represent the basis-states of the code by the symbols $(|0\rangle, |1\rangle)$
- Example: $|+_Z\rangle \longrightarrow |0\rangle, |-_Z\rangle \longrightarrow |1\rangle$
  $| + (-)_X\rangle \longrightarrow (\frac{1}{\sqrt{2}}(|0\rangle + (-)|1\rangle),$
  $| + (-)_Y\rangle \longrightarrow (\frac{1}{\sqrt{2}}(|0\rangle + (-)i.|1\rangle),$

1.B. Two-qubit systems.

- Let us consider two spin 1/2 particles A and B that are localized in FAR AWAY regions of space.
- Let us measure with Stern-Gerlach devices their spin projection along Z,
- 4 possible outcomes:

  up$_A$-up$_B$,

  up$_A$-down$_B$,

  down$_A$-up$_B$

  and down$_A$-down$_B$.
- corresponding to the states
  $|+\rangle_Z^A \otimes |+\rangle_Z^B$,
  $|+\rangle_Z^A \otimes |-\rangle_Z^B$,
  $|-\rangle_Z^A \otimes |+\rangle_Z^B$
  and $|-\rangle_Z^A \otimes |-\rangle_Z^B$.
- The most general two-qubit state is SUPERPOSITION of those 4 states:
- $|\Psi\rangle = \alpha|+\rangle_Z^A \otimes |+\rangle_Z^B + \beta|+\rangle_Z^A \otimes |-\rangle_Z^B + \gamma|-\rangle_Z^A \otimes |+\rangle_Z^B + \delta|-\rangle_Z^A \otimes |-\rangle_Z^B$.

Factorizable States.

- A state that can be written as follows
- $|\Psi\rangle = (\alpha_A|+\rangle_Z^A + \beta_A|+\rangle_Z^A) \otimes (\alpha_B|+\rangle_Z^B + \beta_B|+\rangle_Z^B)$
  is factorizable
- For such states, the outcomes of local measurements in the A and B region are INDEPENDENT
- WHY?
- Local observables are of the type $O^A \otimes Id.^B$ $(Id.^A \otimes O^B)$ so that
- $\langle i|_Z^A \otimes \langle j|_Z^B O^A \otimes O^B |i\rangle_Z^A \otimes |j\rangle_Z^B = \langle i|_Z^A O^A |i\rangle_Z^A \cdot \langle j|_Z^B O^B |j\rangle_Z^B,$
- which means that outcomes of local measurements are statistically independent...

ENTANGLEMENT-BELL STATES.

Definition: non-factorizable states are said to be entangled.
Examples of maximally entangled states:
the Bell states.

- Bell states are in 1-1 correspondence with Pauli spin operators:

  $\sigma_0 = |+\rangle_Z\langle+|_Z + |-\rangle_Z\langle-|_Z \leftrightarrow |B_0^0\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |+\rangle_Z^B + |-\rangle_Z^A \otimes |-\rangle_Z^B)$

  $\sigma_x = |+\rangle_Z\langle-|_Z + |-\rangle_Z\langle+|_Z \leftrightarrow |B_1^0\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |-\rangle_Z^B + |-\rangle_Z^A \otimes |+\rangle_Z^B)$

  $\sigma_y = i|+\rangle_Z\langle-|_Z - i|-\rangle_Z\langle+|_Z \leftrightarrow |B_0^1\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |-\rangle_Z^B - |-\rangle_Z^A \otimes |+\rangle_Z^B)$

  $\sigma_z = |+\rangle_Z\langle+|_Z - |-\rangle_Z\langle-|_Z \leftrightarrow |B_0^1\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |+\rangle_Z^B - |-\rangle_Z^A \otimes |-\rangle_Z^B)$

- Bell states are not factorizable; for instance if $|B_0^0\rangle$ would factorize then:

  $\alpha^A.\alpha^B$=$\beta^A.\beta^B$=$\sqrt{\frac{1}{2}}$ and $\alpha^A.\beta^B$= $\beta^A.\alpha^B$=0;

  Obviously such a system of equations has no solution (otherwise)

  $\alpha^A.\alpha^B.\beta^A.\beta^B$=$\sqrt{\frac{1}{2}}.\sqrt{\frac{1}{2}}$=$\frac{1}{2}$,

  and $\alpha^A.\beta^B.\beta^A.\alpha^B$=$0.0 = 0$ so

  $1/2 = 0$!?.

- Local observables of entangled states are NOT statistically independent, in general.

- Example, let us measure the spin projection along $\vec{n}_A$ in the region A and the spin projection along $\vec{n}_B$ in the region B (with $n_x^{A/B} = sin\theta^{A/B}$, $n_y^{A/B} = 0$, $n_z^{A/B} = cos\theta$), we can make use of the spinorial transformation law $|+\rangle_{\vec{n}} = \cos\frac{\theta}{2}e^{\frac{-i\phi}{2}}|+\rangle_Z + \sin\frac{\theta}{2}e^{\frac{+i\phi}{2}}|-\rangle_Z$ and $|-\rangle_{\vec{n}} = -\sin\frac{\theta}{2}e^{\frac{-i\phi}{2}}|+\rangle_Z + \cos\frac{\theta}{2}e^{\frac{+i\phi}{2}}|-\rangle_Z$,
  so that the Bell state $|B_0^0\rangle$ transforms as follows:

- $$\begin{aligned}|B_0^0\rangle = \sqrt{\frac{1}{2}}(cos\frac{(\theta_A-\theta_B)}{2}|+\rangle_{\vec{n}}^A \otimes |+\rangle_{\vec{n}}^B \\ -sin\frac{(\theta_A-\theta_B)}{2}|+\rangle_{\vec{n}}^A \otimes |-\rangle_{\vec{n}}^B \\ +sin\frac{(\theta_A-\theta_B)}{2}|-\rangle_{\vec{n}}^A \otimes |+\rangle_{\vec{n}}^B \\ +cos\frac{(\theta_A-\theta_B)}{2}|-\rangle_{\vec{n}}^A \otimes |-\rangle_{\vec{n}}^B).\end{aligned}$$

- Making use of Born's transition rule, the probability that after the preparation of the Bell state $|B_0^0\rangle$ the outcomes of the spin measurements in A and B are found to be UP-UP is equal to $|\langle B_0^0|(|+\rangle_{\vec{n}}^A \otimes |+\rangle_{\vec{n}}^B)|^2$ so to say to $\frac{1}{2}cos^2\frac{(\theta_A - \theta_B)}{2}$.
- Similarly the probability of $(up_A, down_B)$ is $\frac{1}{2}sin^2\frac{(\theta_A - \theta_B)}{2}$,

  the probability of $(down_A, up_B)$ is $\frac{1}{2}sin^2\frac{(\theta_A - \theta_B)}{2}$,

  and the probability of $(down_A, down_B)$ is $\frac{1}{2}cos^2\frac{(\theta_A - \theta_B)}{2}$.
- In particular, when local quantization axes are PARALLEL: ($\theta_A - \theta_B$=0), we get PERFECT CORRELATIONS:

  $P(up_A, up_B) = P(down_A, down_B) = 1/2$

  $P(down_A, up_B) = P(up_A, down_B) = 0$
- Obviously there is no longer statistical independence; otherwise we would get

  $P(up_A, up_B).P(down_A, down_B)$=$1/2.1/2$ =

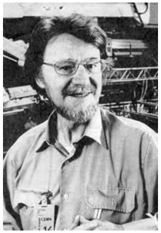
  $P(down_A, up_B).P(up_A, down_B) = 0.0$ so $1/4 = 0$!?

Entanglement and non-locality.

- Along infinitely many directions ($\theta_A - \theta_B$=0) we get perfect correlation
  $P(up_A, up_B) = P(down_A, down_B) = 1/2$
  $P(down_A, up_B) = P(up_A, down_B) = 0;$
- Then we can predict the outcome of a local measurement without measuring it directly; it is sufficient to measure along the same direction the spin of the entangled particle and to exploit the perfect correlations in order to know the result in advance.
- According to Einstein Podolski and Rosen (1935), distant measurements performed in far away regions separated by a SPACELIKE distance are CAUSALLY DISCONNECTED and may thus NOT INFLUENCE each other so that the outcomes must be PREDETERMINED, in violation with the quantum undeterminism...

Bell (1965): Incompatibility between

EPR reasoning (locality or local realism) and quantum predictions.

John Bell 

- If local spin outcomes are predetermined,
- then correlations must obey a constraint (statistical inequality)
- but quantum predictions VIOLATE the inequality
- so Quantum Mechanics is a non-local theory (or a theory incompatible with EPR assumptions-local realism).

Example/Dramatic illustration: Pseudo-telepathy.

- Alice and Bob claim to be telepathically connected to each other;

  this possibility is tested experimentally:

- Alice is on planet Earth, Bob on Jupiter; every minute they undergo a questioning, simultaneously; at each time, a question is chosen at random (independently at each side) among three questions:

  α: Thirsty?

  β: Hungry?

  γ: Tired?

- Alice and Bob make use of entanglement in order to answer:

  they share the Bell state $|B_0^0\rangle$,

  and if they are asked the question α, β, or γ they measure with a Stern-Gerlach device the spin projection along

  $\theta_\alpha = 0, \phi_\alpha = 0$; $\theta_\beta = 2\pi/3, \phi_\beta = 0$; or $\theta_\gamma = 4\pi/3, \phi_\gamma = 0$.

  up=yes; down=no...

- When the QUESTIONS are the SAME, Alice and Bob SIMULATE TELEPATHY because for parallel directions the outcomes are PERFECTLY CORRELATED so they provide the same answers whenever they have to answer to the same questions at the same time.

- According to EPR reasoning, the answers must be predetermined, “written in advance” but then $P(\alpha_A = \beta_B V \beta_A = \gamma_B V \gamma_A = \alpha_B) = 1$,

  because there are TWO ANSWERS and THREE QUESTIONS so that

  TWO QUESTIONS HAVE THE SAME ANSWER...

- Therefore $P(\alpha_A = \beta_B) + P(\beta_A = \gamma_B) + P(\gamma_A = \alpha_B) \geq 1$.

  This is an example of a Bell inequality.

  It ought to be satisfied by any local realistic model for the correlations.

- Making use of quantum correlations, Alice and Bob can violate the inequality:

  $P(\alpha_A = \beta_B) + P(\beta_A = \gamma_B) + P(\gamma_A = \alpha_B)$= $P(\alpha_A = \beta_B = up) + P(\beta_A = \gamma_B = up) + P(\gamma_A = \alpha_B = up)$+ $P(\alpha_A = \beta_B = down) + P(\beta_A = \gamma_B = down)$+$P(\gamma_A = \alpha_B = down)$ =$6.\frac{1}{2}cos^2(\pi/3) = 3/4.$

  Obviously it is not true that $3/4 \geq 1$ and the inequality is violated...

- Conclusion: Alice and Bob (or the entangled particles) have to communicate in some way but between Earth and Jupiter the distance is of the order of 8 light-minutes,

  If they must answer within 1 second, we find that they ought to communicate at a speed equal to

  480 c!!!

- Experimentally, such correlations were tested for instance in Geneva, where Bell inequalities were violated by particles (photons) separated by a SPACELIKE distance equal to 10 km with a temporal duration equal to 5 picosec, we find so

  10 kms/5 picosec=more or less 7.10^6.c !!!

WARNING:

It is worth noting that although the quantum correlations do not admit local realistic explanations, locality (in the sense of relativistic causality) is guaranteed by the fact that the local statistical averages of the correlated outcomes obtained through measurements onto quantum entangled systems cannot be influenced by distant observers (what is sometimes called weak causality or statistical causality).

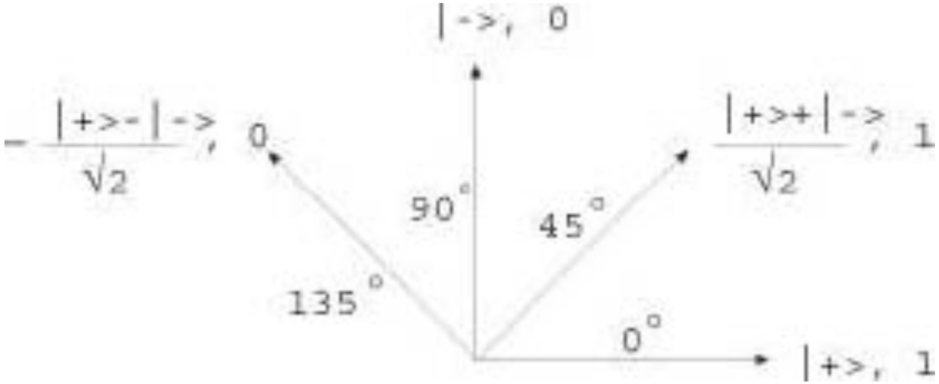
For instance neither classical information nor energy-matter can be transmitted faster than light.

This constitutes a situation of “peaceful coexistence” between quantum mechanics and special relativity.

2A. A generic example of Quantum Key Distribution (QKD) with discrete variables:

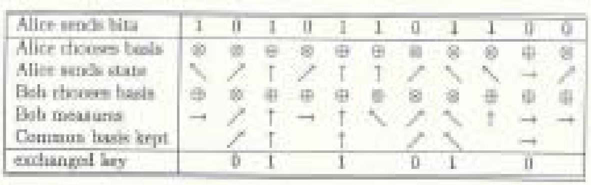
The BB’84 qubit protocol.

- Alice sends a qubit to Bob.
- Alice encodes the qubit EITHER in the X basis OR in the Z basis. To each preparation corresponds a binary value, 0 or 1, and there are 4 possible preparations, 2 in each basis:



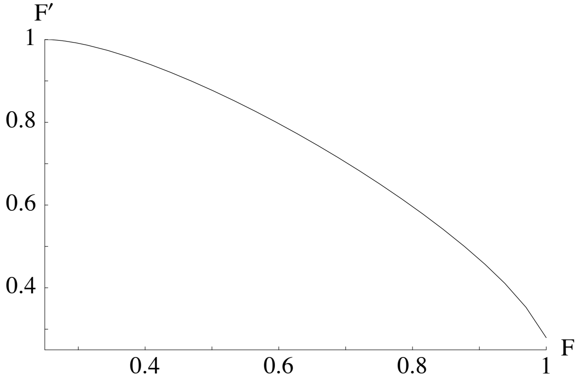
- Bob measures the qubit EITHER in the X basis OR in the Z basis. To each measurement outcome corresponds a binary value, 0 or 1, in agreement with Alice’s conventions.
- Alice and Bob perform the choice of the measurement basis at random and independently of each other.

- After having performed a large number of joint-measurements they communicate on a public channel what were their respective choices of bases.
- They eliminate the outcomes that were not measured in the same basis and are not correlated. What remains constitutes the RAW KEY.



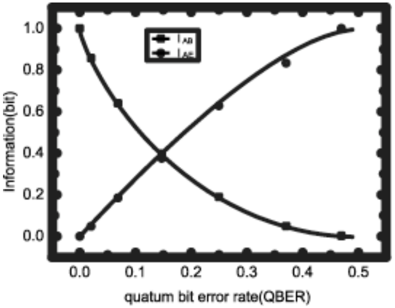
Alice sends bits	1	0	1	0	1	1	0	1	1	0	0
Alice chooses basis	⊗	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗	⊕	⊗
Alice sends state	↖	↗	↑	↗	↑	↑	↗	↖	↖	→	↗
Bob chooses basis	⊕	⊗	⊕	⊕	⊕	⊗	⊗	⊗	⊕	⊕	⊕
Bob measures	→	↗	↑	→	↑	↖	↗	↖	↑	→	→
Common basis kept		↗	↑		↑		↗	↖		→	
exchanged key		0	1		1		0	1		0	

- In the case of perfect (noiseless-error-free) communication their outcomes are perfectly correlated, which means that Alice and Bob share a perfectly identical key.
- In realistic situations, errors are present, but Alice and Bob can locate them and eliminate them, by making use of a public transmission line: this is the so-called RECONCILIATION protocol.
- By doing so they can estimate the error-rate.
- Due to Heisenberg's uncertainty principle, it is impossible for a spy to eavesdrop the communication between Alice and Bob without disturbing the transmission.
- As a consequence there is a trade-off relation between the quality of the transmission and the maximal information of the spy (F and F' on the figure below).

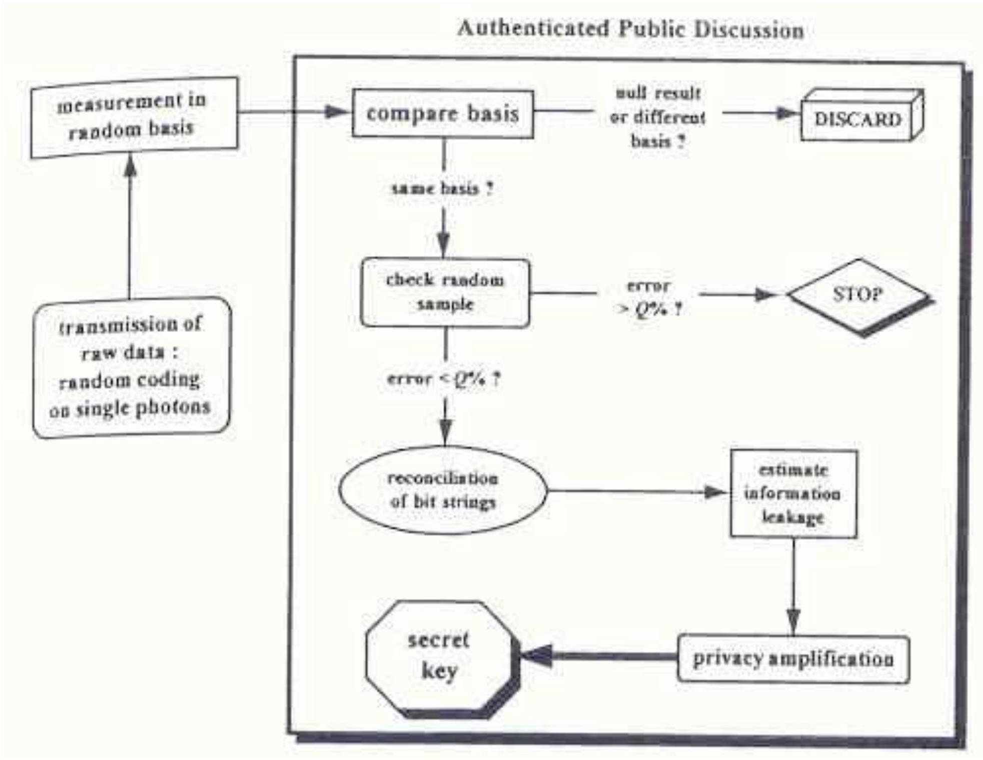


REMARK: THIS IS THE MAIN NOVELTY OF QUANTUM KEY DISTRIBUTION:

THERE EXISTS A TRADE OFF RELATION BETWEEN THE DISTURBANCE CAUSED BY AN EAVESDROPPER ON QUANTUM CORRELATIONS AND THE INFORMATION GAINED BY HIM.



- After completion of the reconciliation protocol, when the error rate is not too low, Alice and Bob know that they possess more mutual information than any other spy in the world.
- Then, they can distillate a secret key with arbitrary level of confidentiality during the PRIVACY AMPLIFICATION protocol.
- As the reconciliation protocol, the privacy amplification protocol is realized on a public transmission line, these are FULLY CLASSICAL protocols.


Authenticated Public Discussion
measurement in random basis
compare basis
null result or different basis ?
DISCARD
same basis ?
check random sample
error > Q% ?
STOP
transmission of raw data : random coding on single photons
error < Q% ?
reconciliation of bit strings
estimate information leakage
secret key
privacy amplification

The full QKD protocol.

2B. The BB’84-Ekert’91 qubit protocol.

- Alice and Bob share the two-qubit Bell state $|B_0^0\rangle$.
- They exchange information thanks to the very strong correlations exhibited by this entangled state.
- To do so they measure their two-level (qubit) component EITHER in the X basis OR in the Z basis.

Remarks:

- As for the BB’84 protocol, Alice and Bob perform the choice of the measurement basis at random and independently of each other.
- After having performed a large number of joint-measurements they communicate on a public channel what were their respective choices of bases.
- They eliminate the outcomes that were not measured in the same basis and are not correlated. What remains constitutes the RAW KEY.

3. Applications of the Pauli Group and Generalised Pauli Group in Quantum Information Theory.

Preliminary remark.

- In practical applications of Quantum Information, it often happens that different states from a same basis play an identical role.
- Example: in the first protocol for Quantum Key Distribution (Bennett and Brassard 1984), two polarisation bases are chosen to encode the signal, and between each of them the two basis states that carry the binary signal (0 ou 1) could be intertwined:

  we could permute the values 0 and 1 without changing the essence of the protocol.
- It is therefore interesting to consider **groups of permutations of a same basis of the Hilbert space**. Those groups constitue a natural symmetry in many applications that were developed in the framework of Quantum Information.

Example d=2, permutations versus displacement operators in the qubit space.

- Most simple case: two-level systems (QUBITS): d=2.
- Two possible permutations: the identity and the negation or NOT gate (exchange of 0 and 1) which permutes the qubit basis state $|0\rangle$ with $|1\rangle$.
- We can express the identity by the identity operator $|0\rangle\langle 0| + |1\rangle\langle 1|$.
- The operator associated to the negation can be written $|1\rangle\langle 0| + |0\rangle\langle 1|$.
- When $|0\rangle$ and $|1\rangle$ correspond to the North and South poles of the Stokes-Poincare-Bloch sphere: (along the Z axis: $|0\rangle$=$|+\rangle_Z$; $|1\rangle$=$|-\rangle_Z$),
- The NOT operator is equal to the Pauli σ_x operator itself!
- This operator is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$.

- We can now repeat the reasoning and consider the two possible permutations of the eigenstates of σ_x.
- We find then the identity operator while the operator that corresponds to the X-negation is equal to $|0\rangle\langle 0| - |1\rangle\langle 1|$.
- When $|0\rangle$ and $|1\rangle$correspond to the North and South poles (along Z), this operator is the Pauli operator σ_z!
- The composition of the operators σ_z et σ_x is equal, up to a global phase, to σ_y.
- σ_y is diagonal in the basis $(\frac{1}{\sqrt{2}}(|0\rangle + i.|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- We find so the 4 Pauli operators:, the identity and the 3 σ operators.

3 A. Three Interesting properties of the

Pauli displacement operators.

1st Property: MUBness.

- Such operators form a group (up to global phases), the Pauli group. This group itself consists of 3 subgroups which consist of the identity and one of the 3 operators $\sigma_{x,y,z}$.
- These 3 subgroups are diagonal in the bases $(|0\rangle, |1\rangle)$, $(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$, and $(\frac{1}{\sqrt{2}}(|0\rangle + i.|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle))$.
- Such bases are said to be ”mutually unbiased” (MUB):

> *Definition: “A collection of orthonormal bases of a d dimensional Hilbert space is said to be mutually unbiased if whenever we choose two states from different bases, the modulus squared of their inproduct is equal to $1/d$. ”*

- The transition probabilities between states from different MUB’s are all equal to $1/d$ (in the qubit case they are 50-50 probabilities as when we toss an UNBIASED COIN).
- To learn more about MUB, please listen to BG Englert and S Weigert’s lectures...

2nd interesting property of the Pauli displacement operators.

The Pauli operators are in one-to-one correspondence with the so-called Bell states:

$\sigma_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \leftrightarrow |B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \leftrightarrow |B\rangle_{10} = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$

$\sigma_y = i(|0\rangle\langle 1| - |1\rangle\langle 0|) \leftrightarrow |B\rangle_{11} = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$

$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \leftrightarrow |B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$

The Bell states possess plenty of applications in Quantum Information (teleportation, cloning). They are maximally ENTANGLED, maximally NON-LOCAL and form an orthonormal basis of the two-qubit Hilbert space ($d = 4$).

3rd property of the

Pauli displacement operators.

- Pauli operators are in 1-1 correspondence with the Bell states
  which form an orthonormal basis of the ($d = 4$) Hilbert space
  therefore the Pauli displacement operators form an orthonormalised basis of the linear operators (relatively to the Trace-norm product).

- As a consequence, any qubit DENSITY MATRIX or density operator is a linear combination of Pauli operators:
  $\rho = \frac{1}{2}(\sigma_0 + k_x\sigma_x + k_y\sigma_y + k_z\sigma_z)$.
  We recognize here Bloch parameters (NMR) or Stokes-Poincaré parameters (polarimetry).

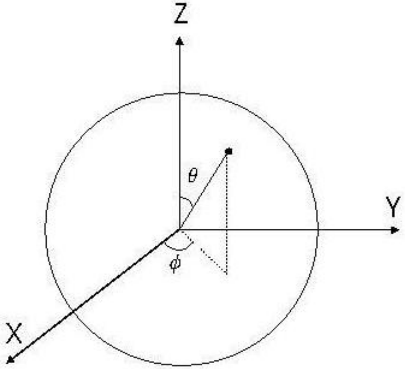
- In order to estimate these parameters it is enough to measure the transition probabilities in the 3 corresponding bases (MUBs).

- By doing so we realize a QUANTUM TOMOGRAPHIC PROCESS so to say we can estimate the qubit quantum state.

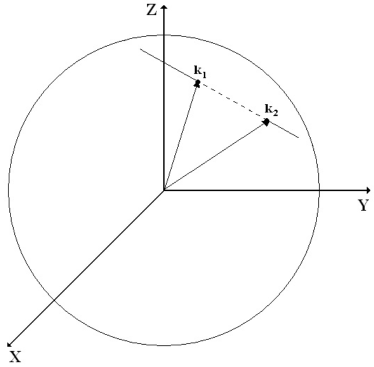
The Bloch vector associated to pure states is situated ON the Bloch sphere. For instance to pure states labelled as follows,

$$|+\rangle_{\vec{n}} = \cos\frac{\theta}{2}e^{\frac{-i\phi}{2}}|+\rangle_Z + \sin\frac{\theta}{2}e^{\frac{+i\phi}{2}}|-\rangle_Z$$

corresponds the Bloch vector $\vec{n}$ (with $n_x = \cos\phi\sin\theta$, $n_y = \sin\phi\sin\theta$, $n_z = \cos\theta$)



The Bloch vector associated to mixed states is situated INSIDE the Bloch sphere. For instance to a weighted sum of two pure states corresponds a convex combination (with the same weights) of their respective Bloch vectors



Remarks.

- The tomographic procedure based on MUB's is OPTIMAL because there is NO REDUNDANCY between data collected in different bases;

  the information is thus never wasted during the data acquisition.

- The MUB's play an important role in quantum cryptography because they maximize the uncertainty relations: whenever a spy measures the signal on a basis that is mutually unbiased with the basis of encryption, his Shannon information about the signal is equal to zero, so that he does not learn anything about the secret key.

  Therefore encryption bases are often MUB's (BB'84 or 6 states qubit protocols for Quantum Key Distribution).

  In the 6 states protocol for instance the authorized users of the cryptographic channel (Alice and Bob) are able to realize a full tomography of the quantum state that they share, which maximizes the constraints to be met by the spy in order to dissimulate the fact that he eavesdrops the signal. The security of the full protocol (for a given signal to noise ratio) is thus maximal.

Generalisations in dimensions higher than 2.

Dimension 4.

- There exist, in dimension 4, 4.3.2=24 permutations between states from a same basis. Two subgroups of this group of 24 elements are particularly interesting:

- The cyclic group with 4 elements generated by the permutation
  $P_1 = |0\rangle \rightarrow |1\rangle;|1\rangle \rightarrow |2\rangle;|2\rangle \rightarrow |3\rangle;|3\rangle \rightarrow |4\rangle.$
  It also contains the identity P_0, and the power 2 and 3 of the generator:
  $P_2 = |0\rangle \rightarrow |2\rangle;|1\rangle \rightarrow |3\rangle;|2\rangle \rightarrow |0\rangle;|3\rangle \rightarrow |1\rangle.$
  $P_3 = |0\rangle \rightarrow |3\rangle;|1\rangle \rightarrow |0\rangle;|2\rangle \rightarrow |1\rangle;|3\rangle \rightarrow |2\rangle.$

- The "Galois" group that contains the identity and the 3 following permutations:
  $P'_2 = |0\rangle \rightarrow |2\rangle;|1\rangle \rightarrow |3\rangle;|2\rangle \rightarrow |0\rangle;|3\rangle \rightarrow |1\rangle.$
  $P'_1 = |0\rangle \rightarrow |1\rangle;|1\rangle \rightarrow |0\rangle;|2\rangle \rightarrow |3\rangle;|3\rangle \rightarrow |2\rangle.$
  $P'_3 = |0\rangle \rightarrow |3\rangle;|1\rangle \rightarrow |2\rangle;|2\rangle \rightarrow |1\rangle;|3\rangle \rightarrow |0\rangle.$

On the basis of the composition law of these (commutative) groups it is easy to define a (commutative) addition law through the relation
$P_i.P_j = P_{i+j}\ (i, j = 0, 1, 2, 3)$.
We find so the following addition tables:

$\oplus_{cycl.}$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	2	3	0
2.	2	3	0	1
3.	3	0	1	2

(1)

$\oplus_G$.	0.	1.	2.	3.
0.	0	1	2	3
1.	1	0	3	2
2.	2	3	0	1
3.	3	2	1	0

(2)

On the basis of these addition tables it is also easy to define a (commutative) multiplication law that is distributive relatively to the addition:,
We find so the following multiplication tables:

$\odot_{cycl.}$.	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	0	2
3.	0	3	2	1

(3)

Remark: The "cyclic" addition (multiplication) are nothing else than the MODULO d (here $d = 4$) addition (multiplication):
$i \oplus_{cyc.} j = i +_{mod.d} j$ and $i \odot_{cyc.} j = i \cdot_{mod.d} j$

$\odot_G$.	0.	1.	2.	3.
0.	0	0	0	0
1.	0	1	2	3
2.	0	2	3	1
3.	0	3	1	2

(4)

Such algebraic structures are called "COMMUTATIVE RINGS"; the Galois multiplication is endowed with a remarkable property:
THERE IS NO DIVIDER OF ZERO, EXCEPTED ZERO ITSELF...
Therefore the Galois ring is also called a FIELD (finite field).
Finite fields were studied by Evariste Galois in the 19th century.
On the basis of such operations we can now define generalised Pauli operators: those operators form a finite displacement group, the generalised Pauli or Heisenberg-Weyl group which constitutes a discrete version of the continuous phase-space displacement operators (largely used in theoretical physics for instance in quantum optics).
Such operators are unitary and can be defined as follows (T. Durt: "A new expression for mutually unbiased bases in prime power dimensions", J. Phys. A: Math. Gen. 38 (2005) 5267-5283):

$$V_i^j = \sum_{k=0}^{d-1} \gamma^{((k \oplus i) \odot j)} |k \oplus i\rangle\langle k|, \tag{5}$$

where $\oplus$ and $\odot$ represent the operations (addition and multiplication) of the finite field/ring while $\gamma$is a well-chosen phase (in the case of Galois operations it is a pth root of unity: $\gamma_G = e^{i.2\pi/p}$ (where the dimension d is a power of p: $d = p^m$), in the case of modulo operations it is a dth root of unity: $\gamma_{cycl.} = e^{i.2\pi/d}$).

Remarks.

- **Whenever the dimension is prime, Galois operations and modulo d (p) operations COINCIDE!!!**
- Many properties are shared by the Galois and cyclic operations. We shall present some of them now (for specific applications of Galois displacement operators and Bell states, like MUB, please listen to BG Englert's lectures...).
- In what follows we shall use the same symbols $\odot$ and $\oplus$ for representing Galois and cyclic (modulo d) operations as well...
- The (Galois as well as cyclic) displacement operators form a **GROUP**:

  Indeed, by a straightforward computation, one can derive the law of composition of these d^2 unitary transformations:

  $$V_i^j . V_l^k = \gamma^{-(i \odot k)} V_{i \oplus l}^{j \oplus k}, \tag{6}$$

  which, up to a global phase, is a group composition law.
- The unitary groups considered here present numerous applications in Quantum Information (tomography, dense coding,teleportation, cloning, error correction and so on).

Remark.

The Galois addition factorizes; for instance, in dimension 4, if we express quartits like tensorial products of 2 qubits: $|0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2$, $|1\rangle_4 = |0\rangle_2 \otimes |1\rangle_2$, $|2\rangle_4 = |1\rangle_2 \otimes |0\rangle_2$, $|3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2$,we can check at the level of the addition table that

if $|i\rangle_4 = |i_1\rangle_2 \otimes |i_2\rangle_2$, et $|j\rangle_4 = |j_1\rangle_2 \otimes |j_2\rangle_2$,

then $|i \oplus_G j\rangle_4 = |i_1 \oplus_{mod2} j_1\rangle_2 \otimes |i_2 \oplus_{mod2} j_2\rangle_2$.

This means that the (quartit here) addition FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. In dimension p^m, the Galois addition always FACTORIZES to the modulo p (=2 here) addition COMPONENTWISE. The Galois multiplication tables are more involved but they are well-known by (some) mathematicians.

Remarks:

One can show that:

$$\sum_{j=0}^{d-1} \gamma_G^{(j \odot_G i)} = d\delta_{i,0} \tag{7}$$

$$\gamma_G^i \cdot \gamma_G^j = \gamma_G^{(i \oplus_G j)} \tag{8}$$

These properties generalize to the (cyclic) MODULO operations:

$$\sum_{j=0}^{d-1} \gamma_{cyc.}^{(j \cdot_{mod.} i)} = d\delta_{i,0} \tag{9}$$

$$\gamma_{cyc.}^i \cdot \gamma_{cyc.}^j = \gamma_{cyc.}^{(i +_{mod.} j)} \tag{10}$$

Galois versus modulo.

IT IS A WELL-KNOWN MATHEMATICAL FACT THAT FINITE FIELDS ONLY EXIST WHEN THEIR NUMBER OF ELEMENTS IS EQUAL TO A PRIME POWER (p^m with p a prime and m a positive integer).

Therefore Galois operations only exist when the dimension is a PRIME POWER

Modulo operations exist for ALL dimensions...

In prime power dimensions, a construction of MUB is known that relies on Galois operations and displacement operators.

In other dimensions, no counterpart of this construction is known (please listen to BG Englert and S Weigert lectures on this problem...).

3B. A new application: Qubit teleportation: (1)theory.

- The ”equation” of teleportation is:

$$(\sum_{i=0}^{1}\phi_i|i\rangle_A)|B_{0,0}\rangle_{B,C}=\sum_{m,n=0}^{1}\frac{1}{2}|B_{m,n}\rangle_{A,B}(\sigma_{m,n}(\sum_{i=0}^{d-1}\phi_i|i\rangle_C)), \qquad (11)$$

where the $\sigma_{m,n}$ represent the conveniently labelled Pauli operators.

Proof:

$$(\phi_0|0\rangle_A+\phi_1|1\rangle_A)(\frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C+|1\rangle_B|1\rangle_C))$$

$$=\frac{1}{2}(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|0\rangle_C+\phi_1|1\rangle_C)$$

$$+\frac{1}{2}(|0\rangle_A|0\rangle_B-|1\rangle_A|1\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|0\rangle_C-\phi_1|1\rangle_C)$$

$$+\frac{1}{2}(|0\rangle_A|1\rangle_B+|1\rangle_A|0\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|1\rangle_C+\phi_1|0\rangle_C)$$

$$+\frac{1}{2}(|0\rangle_A|1\rangle_B-|1\rangle_A|0\rangle_B)\frac{1}{\sqrt{2}}(\phi_0|1\rangle_C-\phi_1|0\rangle_C)$$

3B. Qubit teleportation: (2) in the practice.

- Bob and Charles share the two-qubit Bell state $|B_0^0\rangle$.
- Alice sends a qubit prepared in an arbitrary state $\phi_0|0\rangle_A + \phi_1|1\rangle_A$ to Bob.
- Bob measures the pair in the Bell basis.
- By doing so he projects, whenever he gets the result m, n (m and n vary from 0 to 1) Charles's state onto $\sigma_{m,n}(\phi_0|0\rangle_C + \phi_1|1\rangle_C)$.
- Bob uses a classical communication line to inform Charles about which result he got.
- Charles applies onto his photon the operator $\sigma_{m,n}$; as the square of Pauli operators is equal to unity, he recovers the state $(\phi_0|0\rangle_C + \phi_1|1\rangle_C)$, which is a teleported version of Alice's original state.
- The experiment has been succesfully achieved in Italy, Austria, Switzerland and so on. In Geneva, the teleportation was realized on a distance of 10 km.

Warning: difference between Star Trek teleportation and Quantum Teleportation.

- No matter is teleported during quantum teleportation (Charles's qubit was already present).
- No classical information is teleported: Charles has to wait until he receives Bob's message before he can reproduce Alice's state. Otherwise, his qubit is in a fully noisy state (no "in"formation implies no form!).
- Nevertheless, a continuous variable (the location of a point on the Bloch sphere) gets teleported and this requires only a classical communication of two classical bits (m, n).
- A potential application of Quantum teleportation is that the process could be used as a quantum relay in order to increase the distance of Quantum Key Distribution, we shall come back to it later (in relation with entanglement swapping).

Appendix 1: No cloning ”theorem”.

Quantum information cannot be cloned perfectly well. Otherwise the “peaceful coexistence” between quantum mechanics and special relativity would be broken in accordance with the no-cloning “theorem” (Dieks-Wootters-Zuerk 1982).

Indeed, let us consider the Bell state $|B_{0,0}\rangle_{A,B}$ with A and B in far away regions.

- Alice, in the region A chooses to measure the spin projection along EITHER (1) Z OR (2) X.
- If Bob could perfectly clone the spin state of his local component, he could realize say 1000 PERFECT copies of EITHER (1) $|+\rangle_Z^B$ or $|-\rangle_Z^B$ OR (2) $|+\rangle_X^B$ or $|-\rangle_X^B$.
- By measuring repeatedly the spin component of the copies along Z, Bob would find EITHER (1) no dispersion (up,up,up,up...or d,d,d,d,d...) OR (2) a fifty-fifty distribution of the results (example: up,d,d,up,up,d...).
- By doing so, Bob could know INSTANTANEOUSLY what is the CHOICE of Alice who is separated from him by a SPACELIKE distance: relativistic causality would be violated!

Remark 1:

Because quantum information cannot be cloned perfectly, it is impossible for a spy to eavesdrop a quantum communication without damaging its support, and diminishing the fidelity of the communication between Alice and Bob. This is the basic principle that supports quantum key distribution.

Remark 2:

During a teleportation process, the copy is created at Charles's level while the original qubit that was prepared by Alice gets simultaneously destroyed: teleportation is a ”no cloning process”.

Appendix 2: More on No signalling.

A priori, it is difficult to reconcile quantum non-locality with the well-known impossibility of sending information faster than light. Nevertheless, it is worth noting that it is impossible to make use of non-local correlations in order to send physical information faster than light. This is so because even if Alice carries out measurements and that the outcomes that she observes are correlated to those of Bob, she cannot control which outcomes she will observe due to the stochastic nature of the observation process. Moreover, one can show that the local distribution of outcomes is independent of what happens far away (no signalling condition). Actually, in the situation considered by us (Alice and Bob share an entangled two-qubit state), the local average values for instance in the region B are the same, whatever Alice chooses to do in the region A, even if she measures her qubit or imposes to it any type of unitary evolution, it does not matter. The measurable quantities that make sense in order to carry information are the average values of observables and we simply cannot print a newspaper with randomly chosen characters, it would not contain any information. Thus, transmission of useful information faster than light is not allowed by the laws of quantum mechanics.

This property is known in the literature as the **no signalling** condition. It is a very general property of all quantum entangled systems: local quantum marginals are insensitive to the influences coming from far-away region (here influences due to Alice's actions), whenever those influences occur outside from the past light cone of the region of space-time assigned to local acts of observation (here this region consists of the events associated to Bob's measurements).

It is not too difficult to prove the no signalling property. For convenience we shall limit us to a proof in which pure states only are involved, but the generalisation to non-pure states (mixtures) is straightforward. Let us assume that Alice and Bob's systems are prepared in the pure (but non necessarily factorizable) state $|\Psi\rangle^{AB} = \sum_{i,j=0}^{d-1} \alpha_{ij} |i\rangle^A \otimes |j\rangle^B$ (where $|i\rangle^A$ and $|j\rangle^B$ are states from orthonormalized reference bases) and that Bob measures a local observable in the B region. Such an observable is represented by a local self-adjoint operator of the form $Id.^A \otimes O^B$ so that its average value is equal to

$$\begin{aligned}
& \sum_{i,j,i',j'=0}^{d-1} \alpha^*_{ij}\alpha_{i'j'} \langle i|^A \otimes \langle j|^B Id.^A \otimes O^B |i'\rangle^A \otimes |j'\rangle^B \\
= & \sum_{i,j,i',j'=0}^{d-1} \alpha^*_{ij}\alpha_{i'j'} \delta_{i,i'} \langle j|^B O^B |j'\rangle^B \\
= & \sum_{j,j'=0}^{d-1} \sum_{i=0}^{d-1} \alpha^*_{ij}\alpha_{ij'} \langle j|^B O^B |j'\rangle^B .
\end{aligned}$$

If Alice now imposes a local unitary transformation to her qu$d$it, which sends the state $|i\rangle^A$ onto $|\tilde{i}\rangle^A$, unitarity ensures that $\langle i^A|i'^A\rangle$ = $\langle \tilde{i}^A|\tilde{i}'^A\rangle = \delta_{i,i'}$ so that, after repeating the same (tilded) computation we obtain the same result, showing that the average value of O^B is not affected by the unitary transformation imposed by Alice to the subsystem in her possession. Similarly, if Alice performs a measurement in the $|i\rangle^A$ basis, she will project Bob's state onto a state proportional to the state $\sum_{j=0}^{d-1}\alpha_{ij}|j\rangle^B$ with probability $P_i = \sum_{j=0}^{d-1}|\alpha_{ij}|^2$. The projector on such a state, conveniently renormalized, is equal to $\frac{1}{P_i}\sum_{j,j'=0}^{d-1}\alpha_{ij}|j\rangle^B\alpha^*_{ij'}\langle j'|^B$ so that after averaging over all possible outcomes of Alice (i : $0...d-1$), we get that $\langle O^B\rangle = \sum_{i=0}^{d-1}\frac{P_i}{P_i}\sum_{j,j'=0}^{d-1}\alpha_{ij}\alpha^*_{ij'}\langle j'|^B O^B|j\rangle^B$, equivalent to the average value that we derived in the absence of Alice's measurement.

Actually, when the full state is entangled there does not exist a local pure state that would reproduce the statistical distribution of local measurement outcomes. Instead, this statistics is described by the so-called reduced density matrix.

Reduced density matrices.

It is worth noting that the results of local Bob's measurements are the same as those that he would get if he prepared his system in the state described by the effective or reduced density matrix $\rho^B = \sum_{j,j'=0}^{d-1} \sum_{i=0}^{d-1} \alpha_{ij}^* \alpha_{ij'} |j'\rangle^B \langle j|^B$. Formally, this matrix can be obtained by tracing out external degrees of freedom (in this case Alice's degrees of freedom):

$$\begin{aligned}
Tr_A(|\Psi\rangle^{AB}\langle\Psi|^{AB}) &= Tr_A(\sum_{i,j=0}^{d-1} \alpha_{ij}|i\rangle^A \otimes |j\rangle^B \sum_{i',j'=0}^{d-1} \alpha_{i'j'}^* \langle i'|^A \otimes \langle j'|^B) \\
&= \sum_{k=0}^{d-1} \langle k|^A (\sum_{i,j=0}^{d-1} \alpha_{ij}|i\rangle^A \otimes |j\rangle^B \sum_{i',j'=0}^{d-1} \alpha_{i'j'}^* \langle i'|^A \otimes \langle j'|^B)|k\rangle^A \\
&= \sum_{k=0}^{d-1} (\sum_{i,j=0}^{d-1} \alpha_{ij}\delta_{k,i}|j\rangle^B \sum_{i',j'=0}^{d-1} \alpha_{i'j'}^* \delta_{k,i'} \langle j'|^B \\
&= \sum_{i,j,j'=0}^{d-1} \alpha_{ij}|j\rangle^B \alpha_{ij'}^* \langle j'|^B = \rho^B.
\end{aligned}$$

A density matrix is by definition a convex sum of projectors onto pure states. It contains all the information concerning the state of a system, for instance it could describe situations in which the preparation involves the preparation of different pure states, each of them with a well-defined weight. The average value of an arbitrary observable is then equal to the trace of the product of this observable with the density matrix. The set of density matrices is a set of trace 1, self-adjoint operators with positive spectrum. One can show that the reduced density matrix ρ^B well belongs to this set.

3B. (3) Teleportation in arbitrary dimension d.

Let us define generalized Bell states as follows:

$$|B_{m^*,n}\rangle = d^{-1/2}\sum_{k=0}^{d-1}\gamma^{(k\odot n)}|k^*\rangle|k\oplus m\rangle \tag{12}$$

The amplitudes of $|k^*\rangle$ in the reference (computational) basis are defined to be equal to the complex conjugates of the amplitudes of $|k\rangle$.
In what follows, the reference basis for defining the Bell states wil be the computational basis and $|k^*\rangle$=$|k\rangle$...
Remark: In the qubit case (d=2) our definitions of displacement operators and Bell states agree with the usual definitions (Pauli operators and qubit Bell states).

The (generalised) equation of teleportation is:

$$(\sum_{i=0}^{d-1} \phi_i |i\rangle_A)|B_{0,0}\rangle_{B,C} = \sum_{m,n=0}^{d-1} \frac{1}{d}|B_{m,n}\rangle_{A,B}(V^n_{m,C}(\sum_{i=0}^{d-1} \phi_i |i\rangle_C)) \qquad (13)$$

More concretely: the state $\sum_{i=0}^{d-1} \phi_i |i\rangle_A$ gets teleported to a far away region C, during the local measurement in the Bell basis in the region $A - B$. Depending on the result of the measurement, the teleported state is displaced in the discrete dxd phase space along a distance m, n.

3C. Dense coding in arbitrary dimension d.

(1) Qubit Dense Coding

In the qubit case,

$\sigma_0^A = |+\rangle_Z^A\langle +|_Z^A + |-\rangle_Z^A\langle -|_Z^A$
$\sigma_x^A = |+\rangle_Z^A\langle -|_Z^A + |-\rangle_Z^A\langle +|_Z^A$
$\sigma_y^A = i|+\rangle_Z^A\langle -|_Z^A - i|-\rangle_Z^A\langle +|_Z^A$
$\sigma_z = |+\rangle_Z^A\langle +|_Z^A - |-\rangle_Z^A\langle -|_Z^A,$

while

$|B_{00}^{(AB)}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |+\rangle_Z^B + |-\rangle_Z^A \otimes |-\rangle_Z^B)$
$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |-\rangle_Z^B + |-\rangle_Z^A \otimes |+\rangle_Z^B)$
$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |-\rangle_Z^B - |-\rangle_Z^A \otimes |+\rangle_Z^B)$
$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|+\rangle_Z^A \otimes |+\rangle_Z^B - |-\rangle_Z^A \otimes |-\rangle_Z^B).$

Obviously when Alice displaces the Bell state $|B_{00}^{(AB)}\rangle$ by letting act on it one of the four displacement Σ^A operators she generates the four Bell states.

Dense coding proceeds as follows:

- Alice and Bob share a Bell state $|B_{00}^{(AB)}\rangle$,
- Alice lets act on it one of the four displacement Σ^A operators
- By doing so, she generates one of the four Bell states.
- She sends the qubit to Bob who measures it in the Bell basis.

Conclusion: Alice has sent ONE qudit to Bob; Bob learns TWO dits of information!
This constitutes the interest of quantum DENSE CODING, a task impossible to realize classically, and of which entanglement is an absolutely necessary ingredient.

(2) Qu$d$it Dense Coding

The equation of dense coding in arbitrary dimension is:

$$V_{m,A}^{n} \otimes 1_B |B_{0,0}\rangle_{A,B} = |B_{m,n}\rangle_{A,B}. \tag{14}$$

More concretely: Alice and Bob share a (compound) bipartite qudit system prepared in the (entangled) Bell state $|B_{0,0}\rangle_{A,B}$,
then, Alice displaces her component of a distance m, n in the discrete dxd phase space, and sends it back to Bob.
Bob measures the full state in the Bell basis and gets informed about the distance m, n in the discrete dxd phase space.
Conclusion:
Alice has sent ONE qudit to Bob; Bob learns TWO dits of information!
This constitutes the interest of quantum DENSE CODING, a task impossible to realize classically, and of which entanglement is an absolutely necessary ingredient.

3E Application:

Covariant cloning machines, and error operators.

In quantum cryptography, mutually unbiased bases play an important role because they maximize uncertainty relations which ensures the confidentiality of protocols for quantum key distribution.
As mentioned before, the famous BB84 protocol consists of encrypting the message in a qubit state that is chosen at random between four states that belong to two mutually unbiased bases. The relevance of mutually unbiased bases for quantum cloning has also been recognized, which is not unexpected in view of the close link between cloning and the security of key distribution protocols: as a rule, the most dangerous eavesdropping attacks can be realized with the aid of optimized one-to-two cloners — the so-called phase-covariant cloner, for instance, for attacking the BB84 protocol.

The symmetry properties of the Bell states have important implications in the theory of cloning machines, as we shall sketch briefly now. Under very general conditions, optimal cloning states obey Cerf's ansatz, (Cerf2000):

$$\begin{aligned} |\Psi_{0-3}\rangle &= \sum_{m,n=0}^{N-1} |B_{m,n}, B_{\ominus m,\ominus n}\rangle \gamma^{\ominus m \odot n} a_{m,n} \\ &= \sum_{m,n=0}^{N-1} (\mathbf{1} \otimes V_m^n \otimes \mathbf{1} \otimes V_m^{n\dagger}) |B_{0,0}, B_{0,0}\rangle a_{m,n}\,, \end{aligned} \tag{15}$$

which is a four-particle state that is constructed as a linear superposition of states that have particles 0 and 1 in the m, n Bell state and particles 2 and 3 in the $\ominus m, \ominus n$ Bell state. The coefficients $a_{m,n}$ are arbitrary, their values specify the particular cloning state. Particle 0 will be measured and thus projected on one of a set of chosen states, particles 1 and 3 will be the clones, and particle 2 the anticlone (or "machine").

The expansion of the state (15) in the biorthogonal double-Bell basis, with only N^2 of the N^4 basis states appearing in (15), emphasizes a generic property of such cloning states, namely their covariance when passing from one of the mutually unbiased bases to another. This covariance property is of considerable importance in various contexts, such as cryptography protocols that treat all mutually unbiased bases on the same footing and phase-covariant cloning and also has a bearing on the Mean King's problem.

In the present context, we need yet another symmetry property, namely that the two clones — particles 1 and 3 — play complementary roles. To establish this point, we note that

$$\left|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\right\rangle = \frac{1}{N}\sum_{k,l=0}^{N-1} \left|k^*, k\oplus m, l^*, l\ominus m\right\rangle \gamma^{(k\oplus m)\odot n}\gamma^{\ominus(l\ominus m)\odot n}\,, \qquad (16)$$

where we now employ a notation that indicates which particles are paired in the Bell states: 0 with 1, and 2 with 3, as it is the case in (15). Alternatively, we can pair 0 with 3 and 2 with 1, which gives

$$\left|B^{(03)}_{m,n}, B^{(21)}_{\ominus m,\ominus n}\right\rangle = \frac{1}{N}\sum_{k,l=0}^{N-1} \left|k^*, l\ominus m, l^*, k\oplus m\right\rangle \gamma^{(k\oplus m)\odot n}\gamma^{\ominus(l\ominus m)\odot n}\,. \qquad (17)$$

In fact, the states of (16) span the same N^2-dimensional subspace as the states of (17) in the N^4-dimensional 4-particle Hilbert space.

To justify this remark, we evaluate the transition amplitudes,

$$\begin{aligned}
&\langle B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'} | B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle \\
&\qquad = \frac{1}{N^2}\sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\oplus m)\odot n\ominus(l\ominus m)\odot n\ominus(k'\oplus m')\odot n'\oplus(l'\ominus m')\odot n'} \\
&\qquad\qquad \times \langle k'^{*}, l'\ominus m', l^{*}, k'\oplus m' | k^{*}, k\oplus m, l^{*}, l\ominus m\rangle \\
&\qquad = \frac{1}{N^2}\sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\ominus l\oplus m\oplus m')\odot n}\gamma^{\ominus(k'\ominus l'\oplus m'\oplus m)\odot n'}\gamma^{(m\ominus m')\odot(n\oplus n')} \\
&\qquad\qquad \times \delta_{k',k}\delta_{k'\oplus m',l\ominus m}\delta_{l',l}\delta_{l'\ominus m',k\oplus m}\ ,
\end{aligned} \tag{18}$$

where this product of four Kronecker delta symbols equals $\delta_{k,k'}\delta_{l,l'}\delta_{m\oplus m',l\ominus k}$, a product of only three, with the consequence that

$$\langle B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'} | B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = \frac{1}{N}\gamma^{(m\ominus m')\odot(n\oplus n')}\ . \tag{19}$$

For given $|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle$ these are N^2 transition amplitudes, each of modulus N, and therefore no other $B^{(03)}B^{(21)}$ kets can appear on the right-hand side of

$$|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = \frac{1}{N}\sum_{m',n'=0}^{N-1} |B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'}\rangle \gamma^{(m\ominus m')\odot(n\oplus n')} . \tag{20}$$

It follows that $\langle B^{(03)}_{m',n'}, B^{(21)}_{m'',n''}|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = 0$ unless both $m' \oplus m'' = 0$ and $n' \oplus n'' = 0$, which can be verified directly. In particular, we have

$$|B_{0,0}, B_{0,0}\rangle = |B^{(01)}_{0,0}, B^{(23)}_{0,0}\rangle = \frac{1}{N}\sum_{m,n=0}^{N-1} (\mathbf{1} \otimes V^n_m \otimes \mathbf{1} \otimes V^{n\dagger}_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle , \tag{21}$$

which we use in (15) to arrive at the alternative expansion

$$|\Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} (\mathbf{1} \otimes V^{n\dagger}_m \otimes \mathbf{1} \otimes V^n_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle b_{m,n} , \tag{22}$$

where the coefficients $b_{m,n}$ are the double Galois-Fourier transforms of the $a_{m,n}$s,

$$b_{m,n} = \frac{1}{N}\sum_{m',n'=0}^{N-1} \gamma^{m\odot n'\ominus n\odot m'} a_{m',n'} . \tag{23}$$

The stage is now set for a discussion of cloning. When particle 0 is measured and found in the state described by the bra $\langle\psi^*|$, the resulting state of particles 1–3 is

$$\begin{aligned} |\Psi_{1-3}\rangle &= \sum_{m,n=0}^{N-1} (V_m^n \otimes \mathbf{1} \otimes V_m^{n\dagger})|\psi, B_{0,0}^{(23)}\rangle a_{m,n} \\ &= \sum_{m,n=0}^{N-1} (V_m^{n\dagger} \otimes \mathbf{1} \otimes V_m^n)|B_{0,0}^{(21)}, \psi\rangle b_{m,n} \,. \end{aligned} \tag{24}$$

The resulting statistical operator for particle 1, the first clone, is

$$\rho_1 = Tr.[2\&3]|\Psi_{1-3}\rangle\langle\Psi_{1-3}| = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle\big|a_{m,n}\big|^2\langle\psi_{m,n}| \tag{25}$$

with $|\psi_{m,n}\rangle = V_m^n|\psi\rangle$, and for particle 3, the second clone, we obtain

$$\rho_3 = Tr.[1\&2]|\Psi_{1-3}\rangle\langle\Psi_{1-3}| = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle\big|b_{m,n}\big|^2\langle\psi_{m,n}| \,. \tag{26}$$

The displacement operators V_m^n appear as **error operators** in (25) and (26).

There are two extreme complementary situations: if $a_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $\left|b_{m,n}\right|^2 = 1/N^2$, then $\rho_1 = |\psi\rangle\langle\psi|$ is the projector on the target state $|\psi\rangle$ and $\rho_3 = \mathbf{1}/N$ is the completely mixed state; but if $b_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $\left|a_{m,n}\right|^2 = 1/N^2$, we get $\rho_1 = \mathbf{1}/N$ and $\rho_3 = |\psi\rangle\langle\psi|$. In intermediate situations, both ρ_1 and ρ_3 are imperfect copies of $|\psi\rangle\langle\psi|$.

We see that, as a consequence of the Galois-Fourier relation (23), the two clones are complementary to each other in the sense that if one of them projects on the target state $|\psi\rangle$, then the other is completely mixed. More generally, if one clone is in a pure state (not necessarily the target state), then the other clone is in the completely-mixed state.

This complementarity is important because it helps us to understand the main idea underlying quantum cryptography: if the first clone is received by Bob, to whom it appears as the target state with an admixture of noise, and the second clone is eavesdropper Eve's imperfect copy (she also has access to the anticlone), then the more Eve knows about Alice's or Bob's signals, the less strongly their signals are correlated. In other words, when the entanglement between two of the three parties becomes stronger, the entanglement with the third party weakens, an idea that was already central to the first entanglement-based protocol, the aforementioned 1991 Ekert protocol. For obvious reasons, this property is sometimes referred to as the **"monogamy of quantum entanglement."**

We further note that the generalized Pauli groups are not only related to the error operators that describe the imperfections of the clones, they are also directly related to error correcting codes.

For instance, the Shor code for qubits (see, e.g., the reference book of Nielsen and Chuang about Quantum Information) exploits the fact that the Pauli σ operators are an operator basis in the qubit space. Higher-dimensional generalizations of this code likewise exploit that the generalized Pauli operators, (seen as error operators), constitute an operator basis, especially in the many-qubit case ($N = 2^m$).

3F Application: Entanglement Swapping:

In the extreme complementary situation considered above if $a_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $\left|b_{m,n}\right|^2 = 1/N^2$, we get that

$$\begin{aligned} |\Psi_{0-3}\rangle &= \sum_{m,n=0}^{N-1} |B_{m,n}^{(01)}, B_{\ominus m,\ominus n}^{(23)}\rangle \gamma^{\ominus m \odot n} a_{m,n} = |B_{0,0}^{(01)}, B_{0,0}^{(23)}\rangle \\ &= \sum_{m,n=0}^{N-1} (\mathbf{1} \otimes V_m^{n\dagger} \otimes \mathbf{1} \otimes V_m^n)|B_{0,0}^{(03)}, B_{0,0}^{(21)}\rangle b_{m,n} \\ &= \frac{1}{N} \sum_{m,n=0}^{N-1} |B_{m,n}^{(03)}, B_{\ominus m,\ominus n}^{(21)}\rangle. \end{aligned} \tag{27}$$

Obviously, if now we measure and project the qubit systems labelled by 1 and 2 in the Bell basis we project the qubit systems labelled by 0 and 3 onto Bell states too. What is amazing here is that, although the qubit systems labelled by 0 and 3 are not entangled (they could well be separated by spacelike regions at the time where we measure the qubits 0 and 3 and have never interacted with each other in the past), they become instantaneously entangled when the measurement occurs. In a sense everything happens as if, due to the fact that prior to the measurement the qubit 0 (2) was entangled with the qubit 1(3), this entanglement gets tranferred (swapped) to the qubits 0 and 3 at the time that we measure in the Bell basis the qubits 1 and 2. This process is called entanglement swapping and makes it possible to en- tangle qubits without they ever interact directly. It has potential applications in quantum cryptography where it plays a prior role in the conception of quantum repeaters.

References:

For entanglement swapping: M. Zukowski, A. Zeilinger, M. A. Horne and A.K. Ekert, Phys. Rev. Lett. 71, 4287 (1993). J-W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. 80, 3891 (1998). Matthus Halder, Alexios Beveratos, Nicolas Gisin, Valerio Scarani, Christoph Simon, and Hugo Zbinden, Entangling independent photons by time measure- ment Nature Phys, 3, 692-659 (2007)

For quantum repeaters and entanglement swapping: Briegel, H.-J., Dur, W., Cirac, J. I. and Zoller, P.: Quantum repeaters: The role of imperfect local operations in quantum communication. Phys. Rev. Lett. 81, 59325935 (1998).

Applications of the Generalised Pauli Group

in Quantum Information.

4. Discrete affine structures in Hilbert space.

4A. About discrete Wigner distributions.

Discrete Wigner distribution is supposed to be endowed with properties similar to its continuous counterpart; among others it is supposed that it is a quantum version of classical phase space distributions.

We take for the granted that the displacement operators V_j^i previously introduced are the counterpart of the phase space displacement operators:

-**modulo** d or Galois shifts of the labels of the computational basis (here the eigenstates of Σ_Z) are the counterpart of the **spatial translations** while

-the **shifts in the dual basis (or Fourier-Galois basis)**, here the X basis correspond to translations in the impulsion basis (**Galilean boosts**).

In a d dimensional Hilbert space the Wigner distribution is supposed to consist of the average values of d^2 Wigner operators that obey the following constraints:
(a) Translational invariance: $W_{(i_1,i_2)} = (V_{i_1}^{i_2})^\dagger W_{(0,0)} V_{i_1}^{i_2}$;
(b) Wigner operators are self-adjoint so that Wigner **quasi**-probabilities are REAL (not always POSITIVE!...)
(c) The sum of the d^2 Wigner *quasi*-probabilities $Tr.\rho.W_{(i_1,i_2)}$ is normalized to unity;
(d) Marginals: if we consider STRAIGHT LINES in phase-space defined by the relations $a \odot i_1 = b \odot i_2 \oplus c$, with a b and c elements of the finite modulo ring/Galois field with d elements, the averages of Wigner operators along such lines (marginals) are equal to a projector onto one of the MUB states.
(e) Moreover, according to Wootters approach, it is also assumed that in prime power dimensions, lines are associated to MUB in such a way that marginals along non-intersecting parallel lines correspond to projectors onto orthogonal states of a same MUB while marginals taken along non-parallel directions correspond to projectors onto states from different MUB.

Example: qubit Wigner distribution .

This is the simplest case $d = 2$:

- $W_{0,0} + W_{0,1} + W_{1,0} + W_{1,1} = Id.$ by normalisation;
- In virtue of the marginal's properties:

  $W_{0,0} + W_{0,1}$ and $W_{1,0} + W_{11}$ are projectors onto eigenstates of σ_X, while $W_{0,0} + W_{1,0}$ and $W_{0,1} + W_{1,1}$ are projectors onto eigenstates of σ_Z
- Finally $W_{0,0} + W_{1,1}$ and $W_{1,0} + W_{0,1}$ are projectors onto eigenstates of σ_Y.

We can choose such states to be up (0) or down (1), so that: $(W_{0,0} + W_{0,1}) + (W_{0,0} + W_{1,0}) + (W_{0,0} + W_{1,1}) = \frac{1}{2}(Id.(+/-)_X\sigma_X) + \frac{1}{2}(Id.(+/-)_Y\sigma_Y) + \frac{1}{2}(Id.(+/-)_Z\sigma_Z) = 2.W_{0,0} + Id.$

Once we fix the phases $+/-$ we can derive Wigner operators. Let us for instance choose the + value everywhere, we obtain so the following candidate for the Wigner distribution

$$\left\{\begin{array}{l} P_{00} = \frac{1}{4}\left[1 + p_X + p_Y + p_Z\right] \\ P_{01} = \frac{1}{4}\left[1 - p_X - p_Y + p_Z\right] \\ P_{10} = \frac{1}{4}\left[1 + p_X - p_Y - p_Z\right] \\ P_{11} = \frac{1}{4}\left[1 - p_X + p_Y - p_Z\right] \end{array}\right. \tag{28}$$

(expressed in function of Bloch-Stokes parameters)
These amplitudes have been measured by SIC POVM techniques on a 2 qubit RMN system (Hefei Quantum Information group, China 2006), and on photonic polarisations as well (NUS).

4B. Wigner distributions versus Mean King's problem.

- We have seen before that displacement operators are in 1-1 correspondence with Bell states.
- It can been shown that, following this correspondence, the qubit Wigner distribution derived above is in 1-1 correspondence with the measurement basis associated to the resolution of the Mean King's problem in dimension $d = 2$ (Vaidman-Aharonov 1987):

  Is it possible to ascertain the spin component of a spin 1/2 particle along 3 complementary directions?

> *A Mean King challenges a physicist, Alice, who got stranded on the remote island ruled by the king, to prepare a spin1/2 atom in any state of her choosing and to perform a control measurement of her liking. Between her preparation and her measurement, the king's men determine the value of either σ_X, σ_Y or σ_Z. Only after she completed the control measurement, the physicist is told which spin component has been measured, and she must then state the result of that intermediate measurement correctly. How does she do it?*

A priori, no solution: if Alice has only one qubit at her disposal, the optimal strategy consists of preparing a pure state polarised along one of the 3 directions (for instance Z); thereafter, when the Mean King performs his measure Alice can still measure the spin along a direction in-between X and Y (Breidbart basis), which allows her to infer correctly the spin value along X or Y with a probability equal to $cos^2(22.5) \approx 0,85$. In average Alice infers correctly the spin value with a probability $\approx 0,9 = (1 + 2.0.85)/3$.

Nevertheless, a solution of the problem exists, provided we make use of the resources provided by entanglement (Vaidman et al. 1987). We can express this solution elegantly in function of Bell states as we shall now show .

- Solution: Alice’s strategy is the following.

  She prepares two entangled qubits (one for her one for the King) in the Bell state: ${B^Z}_{00} = \frac{1}{\sqrt{2}}(|0\rangle_A^Z|0\rangle_K^Z + |1\rangle_A^Z|1\rangle_K^Z)$
  During his measurement the King projects thus the initial state prepared by Alice onto one of the 6 product states: $|e_l^0\rangle_{King}\otimes|e_l^0\rangle_{Alice}, l = 0...d-1 = 3$, the job of Alice consists of DISCRIMINATING those 6 product-states.

She can discriminate between those 6 states with CERTAINTY 1 by measuring them in the following basis:

$$\begin{aligned}
|\Psi\rangle_1^Z &= \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K}) \qquad (29)\\
|\Psi\rangle_2^Z &= \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} + |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})\\
|\Psi\rangle_3^Z &= \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} + |B_{1,0}^Z\rangle_{A,K} - i|B_{1,1}^Z\rangle_{A,K})\\
|\Psi\rangle_4^Z &= \frac{1}{4}(|B_{0,0}^Z\rangle_{A,K} - |B_{0,1}^Z\rangle_{A,K} - |B_{1,0}^Z\rangle_{A,K} + i|B_{1,1}^Z\rangle_{A,K})
\end{aligned}$$

Indeed, as $|B\rangle_{00} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ et $|B\rangle_{01} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, whenever one of the two first (last) detectors clicks, and that the King measured in the Z basis, he certainly observed the result 0 (1), because the corresponding projectors are orthogonal to $|1\rangle_K^Z|1\rangle_A^Z$ ($|0\rangle_K^Z|0\rangle_A^Z$).

Remark:

Another crucial ingredient of the proof is that Bell states are “covariant” when they are reexpressed in the two other MUB (along X et Y):

$$\begin{aligned} |B^Z_{0,0}\rangle_{A,K} &= |B^X_{0,0}\rangle_{A,K} = |B^Y_{0^*,0}\rangle_{A,K} \\ |B^Z_{0,1}\rangle_{A,K} &= |B^X_{1,0}\rangle_{A,K} = |B^Y_{1^*,0}\rangle_{A,K} \\ |B^Z_{1,0}\rangle_{A,K} &= |B^X_{0,1}\rangle_{A,K} = i|B^Y_{1^*,1}\rangle_{A,K} \\ |B^Z_{1,1}\rangle_{A,K} &= -|B^X_{1,1}\rangle_{A,K} = (-i)|B^Y_{0^*,1}\rangle_{A,K} \end{aligned} \tag{30}$$

By covariance the result about discrimination generalizes to the 2 other directions (X and Y).

Besides, a Solution of the Generalisation of the Mean King’s problem in dimension p^m has been found thanks to the Galois machinery, in prime power dimensions (T. Durt: “About the Mean King’s problem and discrete Wigner distributions”, International Journal of Modern Physics B, 20, 11-13, 1742-1760 (2006)).

This solution is based on the covariance property of Bell states (which reflects the properties of Clifford group); it can be generalized to higher (prime power) dimensions p^m:

$$|B^0_{m^*,n}\rangle = \gamma_G^{(\ominus_G m \odot_G n)} . (\gamma_G^{((k-1)\odot_G m \odot_G m)})^{\frac{1}{2}} |B^k_{(\ominus_G n \oplus_G (k-1)\odot_G m)^*,m}\rangle,$$

$(k-1) : 0, 1, ..., d-1$

The two-qubit basis used by Alice also generalizes in prime power dimensions:

$$|\Psi\rangle^{0}_{(i_1,i_2)} = \frac{1}{d}(\sum_{m,n=0}^{d-1} \gamma_G^{(i_1,i_2)\odot\odot_G(m,n)}(\gamma_G^{(m\odot_G n)})^{\frac{1}{2}}|B^0_{m,n}\rangle_{K,A})$$

here $\odot\odot_G$ represents the quadratic extension of Galois multiplication, that can be obtained on the basis of the field with d elements by adding a new element (in the same way that complex numbers can be derived from real numbers by adding a new element i, the square root of -1.

Remark: the solution of the problem was found by Vaidman and Aharonov in the qubit case in 1987, and in the prime dimensional case by Aharonov and Englert in 2001, while Aravind found a solution of the prime power dimensional version of the problem in 2003 (essentially it coincides with ours (2004) in those cases, but the role played by Galois-Bell states and their covariance was not emphasised in those solutions as well as the connection with Wigner distributions).

After some tedious calculations we get:

$$W_{i_1,i_2} = \frac{1}{N} \sum_{m,n=0}^{N-1} \gamma^{\ominus i_1 \odot n \oplus i_2 \odot m} \Gamma_{m,n} V_m^n \,. \tag{31}$$

$$\Gamma_{m,n} \; = \left\{ \begin{array}{cl} 1 & \text{for } m = 0\,, \\ \alpha_m^{n \oslash m} & \text{for } m > 0\,, \end{array} \right. \tag{32}$$

where α_m^i is a phase factor that can be found elsewhere... (Durt Englert et al. in preparation).

The operators that we derive in this approach obey several properties (Durt Englert Bengtsson Zijkowsi, MUB in preparation):

(W1) each Wigner operator is hermitian;

(W2) each Wigner operator has unit trace;

(W3) the Wigner operators are pairwise orthogonal; (W4) the set of d^2 Wigner operators is invariant under the unitary tranformations of the d^2 Weyl operators; (W5) the marginals of the operator basis are rank-1 projectors, whereby the d projectors associated with parallel lines are mutually orthogonal and thus compose a basis for the kets and bras, with mutually unbiased bases for different sets of parallel lines.

To these we add a sixth criterion: (W6) in the limit of infinite dimensions (p going to infinity, m fixed) the sequence of discrete bases converges to the standard continuous Wigner basis.

4C. Discrete phase-space ”localisation operators”.

versus discrete phase-space ”affine structure”.

It appears that we obtained a DISCRETE COUNTERPART of continuous WIGNER OPERATORS-the operators associated to the solution of the Mean King’s problem are thus DISCRETE PHASE-SPACE LOCALISATION OPERATORS.

- We can represent the labels of the Wigner operators in a N times N square that would play the role of a discrete phase space.
- Then, in virtue of the marginal property, we have that each vertical line of the square (there are N of them) corresponds to a state of the computational basis, each horizontal line corresponds to a state of the dual basis and more generally each set of parallel straight lines corresponds to a state of one of the MUB.
- This justifies the label *discrete phase space representation*; the horizontal and the vertical axes correspond to a discrete version of the position-impulsion representations.

Affine structures.
A finite (d times d) affine plane or array is such that

- There exist $d + 1$ partitions of the d^2 points into d subsets with d elements each (parallel straight lines).
- Parallel straight lines do not intersect.
- Non-parallel lines intersect in exactly one point.

Conjecture about affine planes.
Finite affine plane with d^2 points do not exist when $N = 6$ and $N = 10$. It is conjectured that such planes exist only when d is a prime power.
This conjecture is fundamental in the study of finite geometries but explicit proofs exist only for $N = 6$ and $N = 10$. This is because the proofs are of combinatorial nature and the lenght of computation increases dramatically with the dimension.

The non-existence of a finite affine plane in the case $N = 6$ was proven at the beginning of the 20th century. It confirmed a conjecture of Euler according to which the problem of the 36 officers does not admit a solution. The problem can be formulated as follows: a group of 36 officers is formed with 6 groups of 6 officers from 6 regiments, and officers of a same regiment have 6 different ranks, chosen among 6 possible ranks (the same for all regiments). Is it possible to let them sleep in 6 different rooms and eat at different tables such that in each room there are 6 officers of different ranks coming from different regiments, while at each table there are 6 officers of different ranks coming from different regiments and different rooms.

Le problème des 36 officiers d’Euler

« Une question fort curieuse, qui a exercé pendant quelque temps la sagacité de bien du monde, m’a engagé à faire les recherches suivantes, qui semblent avoir une nouvelle carrière dans l’analyse, et en particulier dans la doctrine des combinaisons. Cette question rouloit sur une assemblée de 36 officiers de 6 différens grades et tirés de 6 régimens différens qu’il s’agissoit de ranger dans un carré, de manière que sur chaque ligne, tant horizontale que verticale, il se trouvât 6 officiers tant de différens caractères que de régimens différens. Or, après toutes les peines qu’on s’est données pour résoudre ce problème, on a été obligé de reconnoître qu’un tel arrangement est absolument impossible, quoiqu’on ne puisse pas en donner de démonstration rigoureuse.»

14 20 41 05 32 53
30 15 04 51 23 42
21 03 12 40 54 35
02 31 50 13 45 24
43 52 25 34 10 01
55 44 33 22
1
1
0
0

Ce problème est équivalent à trouver 2 carrés latins d’ordre 6 orthogonaux.

En 1900, un douanier algérien, Tarry, a prouvé par épuisement des cas qu’il n’existait pas de tels carrés latins.

Euler conjectured that this problem had no solution although at the time nobody was able to prove it; the conjecture was proven to be true by direct examination of all possible combinations by Tarry in 1900. This implies that no finite affine plane with 36 elements exist; otherwise 4 non parallel directions (associated to the 4 properties regiment rank room and table) would provide a solution to the problem of the 36 officers.

Conjecture about maximal sets of MUB and affine planes.
It has been conjectured that the maximal number of families of parallel sraight lines that satisfy the postulates of affine geometry is equal to the maximal number of MUB, for arbitrary dimension.
The conjecture is confirmed when d is a prime power.
If the conjecture is true then in virtue of the 36 officers problem, the maximal number of MUB in dimension 6 is 3...
The challenge is to bring together two a priori independent problems: MUB and finite affine planes...
Good luck!

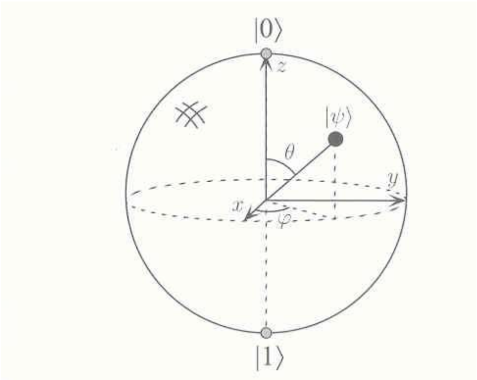
5. Last lecture: SIC POVM’s

or “*SICs*”: Symmetric Informationally Complete

Positive Operator Valued Measure Measurements.

5A. Qubit PVM tomography.

- Quantum tomography is the art of estimating a quantum state.
- Such a state is defined by the DENSITY MATRIX (ρ), a normalised, positive, hermitian operator.
- When a state is a pure state $|\psi\rangle$, ρ is a projector: $\rho = |\psi\rangle\langle\psi|$
- Pauli operators form an orthonormalized basis of the qubit linear operators (relatively to the Trace-norm product).
- As a consequence, any qubit DENSITY MATRIX or density operator is a linear combination of Pauli operators:
  $\rho = \frac{1}{2}(\sigma_0 + k_x\sigma_x + k_y\sigma_y + k_z\sigma_z)$.



- The three parameters k_x, k_y and k_z represent the state of a qubit. They can be represented in a 3-dimensional referential (this is called the Bloch sphere representation).

- In the case of spin 1/2 systems like in Nuclear Magnetic Resonance, the direction of the Bloch vector represents the direction of the spin.

- In the case of polarised photons, these parameters are called Stokes-Jones parameters; they fully determine the state of polarisation of a light beam. Their estimation is a discipline also called POLARIMETRY...it is formally equivalent to a quantum qubit tomographic process.

- In order to estimate these 3 parameters it is enough to measure the transition probabilities in the 3 corresponding bases (X,Y, and Z).

Remark.

- A measurement in the X, Y or Z basis is called a Projective-Valued-Measure (PVM) measurement because the probability of firing of a detector is equal to the average value of a projector:

  $P(+/-)_{X,Y,Z} = Tr.\rho.|+/-\rangle_{X,Y,Z}\langle +/-|_{X,Y,Z}$

- When a state is a pure state $|\psi\rangle$, ρ is a projector: $\rho = |\psi\rangle\langle\psi|$

  and

  $Tr.\rho.|+/-\rangle_{X,Y,Z}\langle +/-|_{X,Y,Z}$=$Tr.|\psi\rangle\langle\psi|.|+/-\rangle_{X,Y,Z}\langle +/-|_{X,Y,Z}$

  =$|\langle\psi|+/-\rangle_{X,Y,Z}|^2$,

  in accordance with the Born transition rule.

PVM versus POVM tomography.

- During PVM qubit tomography, the three parameters k_x, k_y and k_z that characterize the state ρ of the qubit are estimated by performing 3 projective (PVM) measurements (one measures the transition probabilities in 3 bases (X,Y, and Z)).
- In the case of polarised photons, for instance the Stokes-Jones parameters are estimated by successively measuring the degree of polarisation in 3 polarisation bases (horizontal-vertical, diagonal45-diagonal135 and circular left-right).
- The PVM measurements are a sub-class of more general measurement processes called POVM (Positive Operator Valued Measure) measurements.
- In order to realize a POVM measurement it is sufficient to couple the quantum system to another quantum system (called an ancilla), to entangle them, and to realize a PVM measurement onto the full system: original system plus ancilla.

  If we only consider the effect of this process at the level of the original system (that we obtain by tracing out the ancilla), what we get is called a POVM measurement.

- In order to realize POVM tomography of a qubit, we couple it to an ancilla of same dimensionality and let them evolve together in such a way that they become entangled with each other.
- For the initial state of the system $|\psi^S\rangle = \sum_{i=0}^{1} \psi_i |e_i^S\rangle$ and the initial state of the ancilla $|e_0^A\rangle$,

  the most general coherent unitary evolution will map their state onto the state $U^{S-A}|\psi^S\rangle|e_0^A\rangle = \sum_{i=0}^{1} \psi_i U^{S-A}|e_i^S\rangle|e_0^A\rangle = \sum_{i,k,j=0}^{d-1} \psi_i U_{k,j}^i |e_k^S\rangle|e_j^A\rangle$.
- In the latter equality, the coefficients $U_{k,j}^i$ are unambiguously determined by the specific unitary evolution U that is imposed to the system.

- If we now perform a joint-measurement in the product-basis $|e_k^S\rangle|e_j^A\rangle$, the 4 probabilities of firing of the detectors k and j are equal to $|\sum_{i=0}^{1} U_{k,j}^i \psi_i|^2$, where $k, j = 0, 1$.

- Obviously this probability is in turn equal to the modulus square of the inner product of the initial state $|\psi^S\rangle$ with the (not necessarily normalised) state $|U_{k,j}^S\rangle = \sum_{i=0}^{d-1} U_{k,j}^i |e_i^S\rangle$.

- This is the average value of a Positive Operator, not necessarily a projector, from there the name POVM measure.

- POVM is sufficient for tomography whenever the 4 collected probabilities are independent (up to normalization); then we get 3 independent parameters equivalent to Bloch (spin 1/2) or Stokes (polarisation of light) parameters up to reparametrization. Such a POVM is called IC (Informationally Complete) POVM.

- One can show (A. E. Allahverdyan, R. Balian, and Th. M. Nieuwenhuizen, $Phys.Rev.Lett.$, **92**, 120402 (2004), J. Rehacek, B-G Englert, D. Kaszlikowski, $Phys.Rev.A$, **70**, 052321 (2004)) that the optimal POVM tomography corresponds to the situation where the 4 states $|U_{k,j}^S\rangle$ are treated on the same footing and maximally independent.

- In the qubit case this occurs when they form a perfect tetrahedron on the Bloch sphere.

  Such a POVM is called SIC (Symmetric Informationally Complete) POVM.

Example 1: SIC POVM of. spin 1/2 particles in NMR systems.

- We wish to estimate the Bloch parameters p_x, p_y, and p_z necessary in order to describe the unknown state of the qubit a.
- An ancilla is added to this device as qubit b to form a extending system. This device is initially prepared in the state: $\rho_{in} = \rho_a \otimes \left|0\right\rangle \left\langle 0\right|_b$. This state differs according to different input qubits a.

- We let now evolve the entire system under U, a (well-chosen) unitary evolution:

$$U = \frac{1}{2}\begin{pmatrix} e^{i\pi/4}\alpha & \alpha & \beta & -e^{i\pi/4}\beta \\ \alpha & -e^{-i\pi/4}\alpha & -e^{-i\pi/4}b & -\beta \\ \beta & -e^{i\pi/4}\beta & e^{i\pi/4}\alpha & \alpha \\ -e^{-i\pi/4}\beta & -\beta & \alpha & -e^{-i\pi/4}\alpha \end{pmatrix}$$

  where $\alpha = \sqrt{1 + 1/\sqrt{3}}, \beta = \sqrt{1 - 1/\sqrt{3}}$.

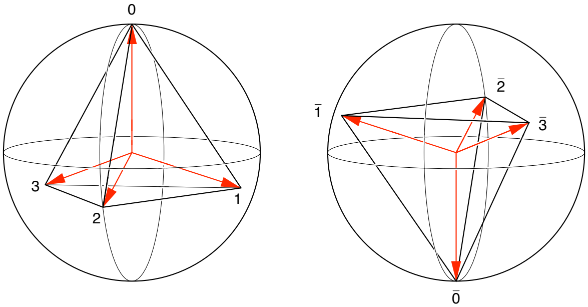
- By measuring the full system in a basis that consists of the product of the a and b qubit computational bases, we obtain four probabilities $P_{00}, P_{01}, P_{10}, P_{11}$.

- Such a POVM measurement is informationally complete due to the fact that the coefficients $P_{00}, P_{01}, P_{10}, P_{11}$ are in one-to-one correspondence with the Bloch parameters p_x, p_y, and p_z as shows the identity

$$\begin{cases} P_{00} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(p_x + p_y + p_z)\right] \\ P_{01} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-p_x - p_y + p_z)\right] \\ P_{10} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(p_x - p_y - p_z)\right] \\ P_{11} = \frac{1}{4}\left[1 + \frac{1}{\sqrt{3}}(-p_x + p_y - p_z)\right] \end{cases}$$

Remark 1.

Actually, P_{00} is the average value of the operator $(\frac{1}{2})(\sigma_{0,0} + (\frac{1}{\sqrt{3}})(\sigma_{1,0} + \sigma_{0,1} + \sigma_{1,1}))$ which is the projector onto the pure state $|\phi\rangle\langle\phi|$ with $|\phi\rangle = \alpha|0\rangle + \beta^*|1\rangle$ and $\alpha = \sqrt{1 + \frac{1}{\sqrt{3}}}$, $\beta^* = e^{\frac{i\pi}{4}}\sqrt{1 - \frac{1}{\sqrt{3}}}$. Under the action of the Pauli group it transforms into a projector onto one of the four pure states $\sigma_{i,j}|\phi\rangle$; $i, j\ :\ 0, 1$: $\sigma_{i,j}|\phi\rangle\langle\phi|\sigma_{i,j} = (\frac{1}{2})((1 - \frac{1}{\sqrt{3}})\sigma_{0,0} + (\frac{1}{\sqrt{3}})(\sum_{k,l=0}^{1}(-)^{i.l-j.k}\sigma_{k,l}))$ The signs $(-)^{i.l-j.k}$ reflect the (anti)commutation properties of the Pauli group. So, the four parameters P_{ij} are the average values of projectors onto four pure states that are "Pauli displaced" of each other. The in-product between them is equal, in modulus, to $1/\sqrt{3} = 1/\sqrt{d+1}$, with $d = 2$. This shows that this POVM is symmetric in the sense that it is in one-to-one correspondence with a tetrahedron on the Bloch sphere; this tetrahedron is obviously invariant under the action of the Pauli group.

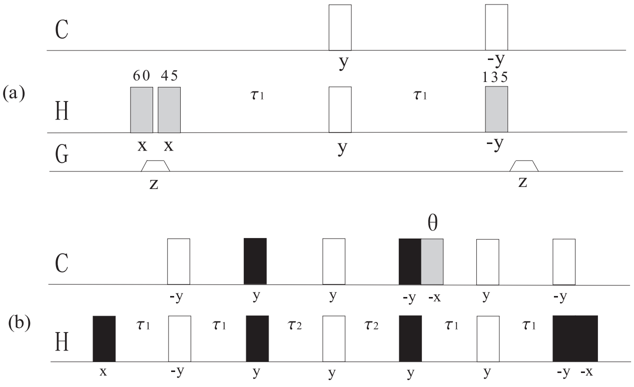


Tetrahedron and its complex conjugate (anti-tetrahedron).

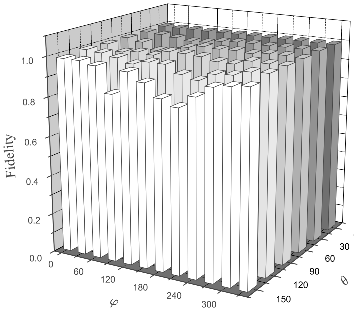
Remark 2.

- SIC POVM tomography of a proton trapped in a chloroform molecule has been realized in China, at the Quantum Information lab. of Hefei University (reference: JF Du, M. Sun, X. Peng and T. Durt, Entanglement Assisted NMR Tomography of a Qubit, Phys. Rev. A, **74**, 042341 (2006)).
- The ancilla was another proton, neighbour to the first one.
- Their unitary evolution was a judicious combination of external Radio-Frequency Pulses (local qubit rotations) and of non-local (entangling) Ising spin-spin (neighbour-neighbour) interaction.

NMR Wigner tomography.



NMR pulses sequence.



Fidelity for 120 different initial qubit states.

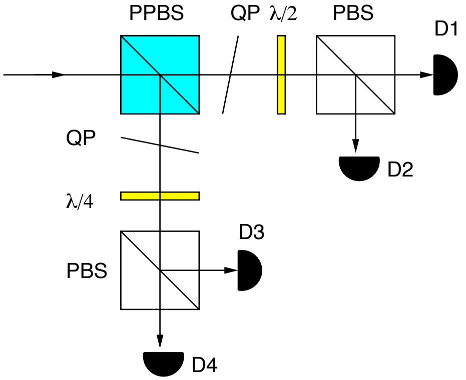
Example 2: Polarimetry by SIC POVM of photonic polarisations.

- Traditionally, in order to estimate the polarisation (Stokes-Jones) parameters, three PVM measurements are necessary, in 3 different polarisation bases.
- To perform SIC POVM polarimetry, one measurement with 4 detectors is enough.
- This has been realized at Singapore University (NUS).
- To do so, the polarisation was coupled (entangled) to spatial localisation by letting pass the pulses through a partially polarising beamsplitter (PPBS) (see picture next page, from the reference A. Ling, S-K Pang, A. Lammas-Linares, and C. Kurtsiefer, $Phys.Rev.A$ **74**, 022309 (2006)).

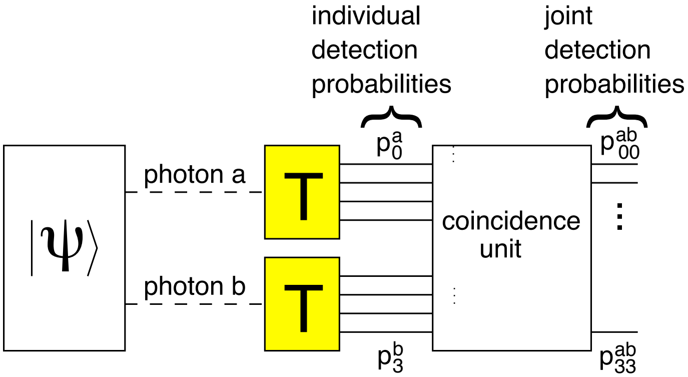
- By adjusting the asymmetry of the PPBS and the angle of the wave plates (half wave and quarter wave plates) in an ad hoc manner, the four b detectors will fire with the same P probabilities as for the spin 1/2 case: $P_{b1} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(p_x+p_y+p_z)\right]$, $P_{b2} = \frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-p_x-p_y+p_z)\right]$, $P_{b3}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(p_x-p_y-p_z)\right]$, $P_{b4}=\frac{1}{4}\left[1+\frac{1}{\sqrt{3}}(-p_x+p_y-p_z)\right]$.

- In the so-called Singapore protocol for QKD, a pair of photons is prepared in a maximally entangled polarisation state (Bell state) in a non-linear crystal.
- Those photons are emitted along opposite directions to the authorized users of the cryptographic line, Alice and Bob, who measure their polarisation by a SIC POVM measurement.
- As we shall discuss soon, Bell states exhibit isotropic anti-correlations when they are measured by local SIC POVM devices.
- These anti-correlations are exploited by Alice and Bob in order to establish a fresh cryptographic key, which is the goal of quantum cryptographic protocols.

2 qubit SIC Full Tomographic Protocol for QKD.



Local set-up



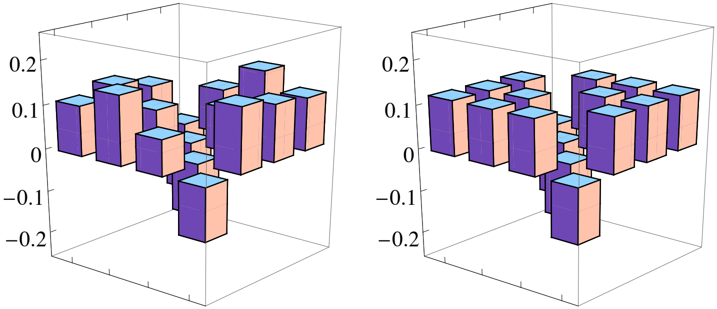
Global set-up

- This is a Full Tomographic Protocol, as we show now:
- Let us denote $P_{k,l}$ (where k and l run from 0 to 3) the joint probability of firing of the kth (lth) SIC detector on Alice's side (on Bob's side), and let us define P_k^a (P_l^b) by $P_k^a = \sum_{l=0}^{3} P_{k,l}^{ab}$ ($P_l^b = \sum_{k=0}^{3} P_{k,l}^{ab}$).
- Then the double Wigner coefficients $W_{k,l}$ can be derived from the statistics of joint detections via the relation $W_{k,l}^{ab} = 3.P_{k,l}^{ab} + \sqrt{3}.(1-\sqrt{3})/4.(P_k^a + P_l^b) + ((1-\sqrt{3})/4)^2$ where the indices k and l run from 0 to 3.
- The density matrix is then reconstructed making use of the relations $(W_{k,l}^{a/b})^{op.} = (1/2)\sum_{i,j=0}^{1}(-)^{i.l-j.k}\sigma_{i,j}^{a/b} =$ $((1/\sqrt{2})\sum_{i=0}^{1}(-)^{i.l})((1/\sqrt{2})\sum_{j=0}^{1}(-)^{-j.k})\sigma_{i,j}^{a/b}$. and $\rho = \sum_{k_0,k_1,l_0,l_1=0}^{1}(1/4)W_{k,l}^{ab}(W_{k_0,k_1}^{a})^{op.}.(W_{l_0,l_1}^{b})^{op.}$ where $k = k_0 + 2.k_1$ and $l = l_0 + 2.l_1$. This establishes that the protocol is a Fully Tomographic Protocol.

- If we impose perfect (and isotropically distributed) anti-correlations then the joint probabilities must obey $P_{k,l} = (1/12) - (1/12)\delta_{k,l}; k, l : 0, 1, 2, 3.$ Then we have $W_{k,l} = (1/8) - (1/4)\delta_{k,l}; k, l : 0, 1, 2, 3$ and ρ=$(1/4)(Id.^{ab} - \sigma^a_X\sigma^b_X - \sigma^a_Y\sigma^b_Y - \sigma^a_Z\sigma^b_Z)$, which is nothing else than the projector $|\Phi_-\rangle\langle\Phi_-|$ onto one of the Bell states, the singlet state $|\Phi_-\rangle = |B_{11}\rangle = \frac{1}{\sqrt{2}}(|1\rangle^a|0\rangle^b - |0\rangle^a|1\rangle^b)$.

- The three other Bell states are equal to $\frac{1}{\sqrt{2}}(|1\rangle^a|0\rangle^b + |0\rangle^a|1\rangle^b)$, $\frac{1}{\sqrt{2}}(|1\rangle^a|1\rangle^b - |0\rangle^a|0\rangle^b)$ and $\frac{1}{\sqrt{2}}(|1\rangle^a|1\rangle^b + |0\rangle^a|0\rangle^b)$. They are obtained by letting act on one of the components of a qubit pair prepared in the singlet state the three sigma operators of Pauli. One can check that the other Bell states will also exhibit isotropic anti-correlations, but for a different pairing of Alice and Bob's detectors.

Wigner Tomography of a Bell state.



Experimental versus theoretical Wigner distribution of a Singlet State.

5B. Higher dimensions.

Optimal PVMs and Weyl Tomography:
Discrete Weyl-type unitary operator basis.
In virtue of the correspondence between two-qudit states and one qudit linear operators, the orthonormalised Bell kets basis $|B_{m,n}\rangle$ corresponds to a basis of linear operators constituted by conveniently normalised displacement operators $N^{-1/2}V_m^n$.
Any linear operator X can thus be expanded in the basis of displacement operators:

$$X = \frac{1}{N}\sum_{m,n=0}^{N-1} V_m^n\, x_m^n \qquad \text{with} \quad x_m^n = \mathrm{tr}\, V_m^{n\dagger}\, X \,. \tag{33}$$

The coefficients x_m^n make up a discrete phase-space function of Weyl-type.
The mapping of the operator X to its Weyl-type phase-space function is one-to-one: there is a unique single–q-nit operator X to the given set of coefficients $\{x_m^n\}_{m,n=0}^{N-1}$, and all x_m^ns are uniquely specified by the given operator X.
In particular, we have

$$x_0^0 = \mathrm{tr}\, X \,. \tag{34}$$

Weyl tomography, on many identically prepared q-nits with statistical operator ϱ, amounts to measuring equal fractions of the q-nits in the $N+1$ MUBs that diagonalize abelian subgroups of the set of displacement operators.
The measurements provide the probabilities $\langle e_k^i|\varrho|e_k^i\rangle$,[a] from which the expansion coefficients

$$\rho_l^i = \operatorname{tr} V_l^{i\dagger}\varrho = c.\sum_{k=0}^{N-1}\gamma^{\ominus k\odot l}\langle e_k^i|\varrho|e_k^i\rangle \tag{35}$$

can then be computed. With $X \to \varrho$, $\operatorname{tr} X \to 1$, $x_l^i \to \rho_l^i$, the statistical operator ϱ is parameterized in terms of the unitary Weyl basis V_l^i and the measured coefficients ρ_l^i.

[a] This is an idealization of the real physical situation. Any actual experiment will give the relative frequencies from which the probabilities can be estimated..

Remarks: 2 Limitations of Weyl tomography.

1. Not efficient in non-prime power dimensions (reasons: the eigenbases of the displacement operators are no longer MUB, moreover they are overnumerous (more than $N+1$)).

2. Intrinsic redundancy in prime power dimensions. There are N measurement outcomes for each of the $N+1$ MUBs, so that one is measuring a total of $N(N+1)$ probabilities (or relative frequencies) in order to determine the N^2-1 parameters of the statistical operator. Clearly, there is some redundancy in the data, namely that $\rho_0^i = 1$ for all $N+1$ values of i. Nevertheless, the measurement of the $N+1$ MUBs realizes state tomography that is optimal in the sense of Wootters: Other choices of $N+1$ von Neumann measurements, not composed of bases that are pairwise mutually unbiased, give estimates for the statistical operator with larger statistical errors when measuring finite samples, as is always the situation in practice.

Yet, when we regard all the $N+1$ measurements of the MUBs, on equal fractions of the q-nits, as jointly defining a POVM with $N(N+1)$ outcomes, then these are more outcomes than really needed to determine N^2-1 parameters. More economic, and thus optimal in a different sense, are POVMs with the minimal number of N^2 outcomes (the one constraint of unit total probability is always there). And among those, a particularly good choice is the so-called “symmetric informationally complete” measurement, or SIC POVM.

SIC POVM tomography for dimensions $d \neq 2$.

(qu$d$it SIC POVM tomography).

- It is possible to find NUMERICALLY qu$d$it Symmetric Informationally Complete POVM that generalize the qubit SIC POVM previously described;
- Concretely this consists of searching families of d^2 pure states that are (generalised) Pauli displaced of each other and have all the same in product in modulus $(1/\sqrt{d+1})$.

  To find them one searches a **seed** or **FIDUCIAL STATE** ANYWHERE in the Hilbert space, and checks wheter the polytope generated by letting act on it the Heisenberg-Weyl group is an equiangular set (so to say ALL the d^2 states generated so have an in-product in modulus equal to $\frac{1}{\sqrt{d+1}}$.
- The search procedure can be carried out on a computer.

MAIN RESULTS.

- Fiducial states have been found **numerical methods** for all dimensions up to 50 (J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, $J.Math.Phys.$, **45**, 2171 (2004)).
- Analytical expressions exist only for low dimensions (2,3,4,6, and 8)
- Otherwise, the problem is still largely an OPEN problem, very intriguing and challenging.

2 REMARKS.

- 1) For qutrits an interesting solution can be found for which SIC POVM tomography is equivalent to Wigner tomography (S. Colin, J. Corbett, T. Durt and D. Gross: “About SIC POVMs and discrete Wigner distribution”, J. Opt. B: Quantum Semiclass. Opt. 7 S778-S785 (2005)).

  For qubits the SIC POVM is also a WIgner POVM.

  This is no longer true in dimensions strictly higher than 3. We don’t really know why...

- 2) There is ONLY one symmetry group that provides SIC POVM’s for ALL dimensions between 2 and 50 (it is the CYCLIC Heisenberg-Weyl group).

  Klappenecker and Rotteler studied all the groups in dimension 2 to 10 that also allows to generate SIC POVM’s (related to so-called nice operator basis approach).

  There is ONLY one symmetry group that provides SIC POVM’s for ALL dimensions between 2 and 10 (it is the CYCLIC Heisenberg-Weyl group).

SICs and Clifford transformations.

An important property of SICs is that if we know one fiducial state of a particular covariant SIC we can generate many other covariant SICs by transforming this fiducial state under the elements of the Clifford group.
The Clifford group is the subset of the unitary operators that map Weyl operators to multiples of Weyl operators under conjugation

$$Vw(q,p)V^\dagger = c(q,p)w(S(q,p)) \tag{36}$$

for maps $c : \mathbb{Z}_d^2 \rightarrow \mathbb{C}$ and $S : \mathbb{Z}_d^2 \rightarrow \mathbb{Z}_d^2$. Among other properties the map S is invertible and $S(0,0) = (0,0)$; the operation associated to its invert S^{-1} is $V^\dagger$. From the definition, it is straightforward to check that the image of the fiducial state of a SIC under a Clifford transformation is still a SIC fiducial state. The proof goes as follows; let us assume that the state $|U_{0,0}\rangle$ is a fiducial state so that $|\operatorname{tr}|U_{0,0}\rangle\langle U_{0,0}|w(m,n)| = |\langle U_{0,0}|w(m,n)|U_{0,0}\rangle| = \sqrt{1/(d+1)}$ whenever $m \neq 0$ or $n \neq 0$; then its image $|U'_{0,0}\rangle$ under a Clifford transformation $V^\dagger$ satisfies
$|\operatorname{tr}|U'_{0,0}\rangle\langle U'_{0,0}|w(m,n)| = |\langle U_{0,0}|Vw(m,n)V^\dagger|U_{0,0}\rangle| = |\operatorname{tr}\langle U_{0,0}|w(S(m,n))|U_{0,0}\rangle|$ $= |\operatorname{tr}\langle U_{0,0}|w(m',n')|U_{0,0}\rangle| = \sqrt{1/(d+1)}$ where we made use of the fact that the map S is invertible and $S(0,0) = (0,0)$ so that if $m \neq 0$ or $n \neq 0$ then $m' \neq 0$ or $n' \neq 0$.

Consequently, if we know a fiducial state of a particular SIC, then we can generate a set of other fiducial states and SICs by letting act on it the Clifford transformations. As these operations form a group, such sets are classes of equivalence of fiducial states (orbits under the Clifford group).

Two remarkable properties characterize these orbits:

-1) The number of orbits is very low (one or two).

Example: in dimension 6 there are 3456 fiducial states: 1728 of them belong to the same orbit, and the 1728 other fiducial states are their images by complex conjugation.

-2) **Zauner's conjecture.** It seems that there always exists a fiducial state that is eigenvector under a certain Clifford operation[a]. This property was conjectured by Zauner and its validity has been checked for all dimensions up to 45 by Appleby, on the basis of the numerical expressions for fiducial states derived by Caves et al. (M. Appleby, J. Math. Phys., **46**, 052107 (2005), quant-ph/0412001, 1-26 (2004)).

[a] Actually this operation generates a subgroup of the Clifford group of order 3; as a consequence the number of fiducial states is equal to the number of Clifford transformations divided by 3 times an integer.

SICs and uncertainties.

One can show that the SIC POVM problem in complex space reduces to a SIC POVM problem in real space, covariant under a reduced (real) subgroup of the generalised Pauli group. Let us denote by R_k the modulus square of a fiducial state expressed in the computational basis.

$$\sum_{k=0}^{d-1} R_k.R_k = d.(\frac{1}{d^2} + \frac{(d-1)}{d^2(d+1)}) = \frac{2}{d+1} \tag{37}$$

and

$$\sum_{k=0}^{d-1} R_k.R_{k+l} = d.(\frac{1}{d^2} - \frac{1}{d^2(d+1)}) = \frac{1}{d+1} \text{ (with} l \neq 0). \tag{38}$$

Besides, normalisation of the fiducial state imposes that

$$\sum_{k=0}^{d-1} R_k = 1. \tag{39}$$

The quadratic Renyi entropy of a probability distribution P_j is equal to $-log_2(\Sigma_j p_j^2)$. The quadratic Renyi entropy of a state $|\psi\rangle$ estimated in a basis $|e_j\rangle$ is thus equal to $-log_2(\Sigma_{j=0}^{d-1}|\langle e_j|\psi\rangle|^2)$.
Besides, as Wootters and Susmann have shown, , when d is a prime power, the minimum of the average quadratic Renyi entropy taken over all MUBs is equal to $-log\frac{2}{d+1}$.
Appleby, Dang and Fuchs have shown (arXiv:0707.2071v1) that one can interpret the constraint 37 as follows: in prime dimensions, each top of a POVM minimizes the average quadratic Renyi entropy averaged over a maximal set of $(d+1)$ Mutually Unbiased Bases. SIC POVMs are thus related to minimal uncertainty states.
When d is prime, the unitary transformations that map the computational basis on a MUB can be shown to be contained in the set of Clifford operations. The sum of the squares of the probabilities of a SIC fiducial state is equal to $\frac{2}{d+1}$ in ANY Clifford image of the computational basis, in particular in the MUBs. Therefore the average Renyi entropy is minimized by ALL fiducial states and is equal to $-log_2\frac{2}{d+1}$.

Open questions:

Ultimately the main questions that remain to be answered about SICs are:

- Do there remain hidden symmetries besides Zauner's conjecture? (minimal entropy principle?)
- Is there a stable limit in the case that d goes to infinity (the continuum)?
- Are there **analytic** expressions for the SIC fiducial states in arbitrary dimension?

  Presently, most results are numerical...but an analytic solution (and a deeper comprehension of Heisenberg-Weyl covariant SIC's) are seemingly *tantanlizingly close.*