WORKSHOP ON QUANTUM COMPUTATION USING IBM Q, PART III

William de la Cruz de los Santos

Universidad Autónoma del Estado de México
Ingeniería en Computación

WeWork Montes Urales, June 18 to 22, 2018

UAEM | Universidad Autónoma del Estado de México

Tecnológico de Monterrey

IBM

HISTORY OF QUANTUM MECHANICS

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.* It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one

A paradox first enunciated by Einstein et al. (1935), who proposed a thought experiment that appeared to demonstrate quantum mechanics to be an incomplete theory.

THE EPR PARADOXON

1. *Completeness*: Each element of realism should have its correspondence in a theory.
2. *Realism*: If a property can be assigned to a physical system with certainty then there exists an element of realism that corresponds to this property.
3. *Locality*: Measurements of different elements of realism in spatially separated systems can not influence each other.

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
(Received March 25, 1935)

OCTOBER 15, 1935 PHYSICAL REVIEW VOLUME 48

Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*
(Received July 13, 1935)

PHYSICAL REVIEW VOLUME 108, NUMBER 4 NOVEMBER 15, 1957

Discussion of Experimental Proof for the Paradox of Einstein, Rosen, and Podolsky

D. BOHM AND Y. AHARONOV
Technion, Haifa, Israel
(Received May 10, 1957)

QUBITS

From classical to quantum computation the following map is considered:

$$0 \longrightarrow |0\rangle$$
$$1 \longrightarrow |1\rangle$$

QUBITS

A qubit is a superposition of two basic states $|0\rangle$ and $|1\rangle$

$$\psi = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

The tensor product of $x = (x_0, \ldots, x_{n-1})$ e $y = (y_0, \ldots, y_{m-1})$:

$$x \otimes y = (x_0 y_0, \ldots, x_0 y_{m-1}, \ldots, x_{n-1} y_0, \ldots, x_{n-1} y_{m-1}).$$

1-quregister: a qubit
k-quregister: the tensor product of a $(k-1)$-quregister with a qubit.
Each k-quregister is a complex vector of dimension 2^k.

For instance:

$$\begin{aligned}
|00\rangle &= e_{00} = e_0 \otimes e_0 = (1, 0, 0, 0) \\
|01\rangle &= e_{01} = e_0 \otimes e_1 = (0, 1, 0, 0) \\
|10\rangle &= e_{10} = e_1 \otimes e_0 = (0, 0, 1, 0) \\
|11\rangle &= e_{11} = e_1 \otimes e_1 = (0, 0, 0, 1)
\end{aligned}$$

BASIC PRINCIPLES

For $k \geq 2$ and $\boldsymbol{\varepsilon} = \varepsilon_{k-1} \dots \varepsilon_1 \varepsilon_0 \in (0+1)^k$,

$$|\boldsymbol{\varepsilon}\rangle = e_{\boldsymbol{\varepsilon}} = \bigotimes_{j=0}^{k-1} e_{\varepsilon_j} \text{ is a } k\text{-quregister.}$$

$\mathbb{H}_k$: linear complex space of dimension 2^k.

MEASUREMENTS

ONE QUBIT: If $\psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, each of $|0\rangle$ or $|1\rangle$ is got with equal probability, since $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$.

TWO QUBITS: For $\phi^+ = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, by measuring the first qubit, it is reduced to the one qubit case. E.g.

$$\begin{aligned} \psi_1 = |0\rangle \quad &\Longrightarrow \quad \phi^+ = |00\rangle \ \& \ \psi_2 = |0\rangle \\ \psi_1 = |1\rangle \quad &\Longrightarrow \quad \phi^+ = |11\rangle \ \& \ \psi_2 = |1\rangle \end{aligned}$$

ENTANGLED STATES

The following states are the Bell states:

$$\begin{aligned} \mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00}+\mathbf{e}_{11}) & \mathbf{b}_{10} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{00}-\mathbf{e}_{11}) \\ \mathbf{b}_{01} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{10}+\mathbf{e}_{01}) & \mathbf{b}_{11} &= \frac{1}{\sqrt{2}}(\mathbf{e}_{10}-\mathbf{e}_{01}) \end{aligned}$$

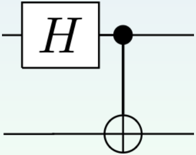
The Bell states form an orthonormal system, known as the Bell basis $\mathcal{B}_{Bell}$.

ENTANGLED STATES

Exercise: generate the Bell states in $\mathbb{H}_2$.

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} = \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} = \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} = \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} = \|\beta_{11}\rangle$

Quantum circuit



Mnemonic notation

$$|\beta_{xy}\rangle = \frac{|0, y\rangle + (-1)^x |1, \overline{y}\rangle}{\sqrt{2}}$$

Pure and mixed states

Pure states: If $\mathbf{x}_j = \sum_i a_{ij}|i\rangle$, where $\sum_i |a_{ij}|^2 = 1$, then it is a pure state.

Mixed states: If there exists a probability density $P \sim [p_0, \ldots, p_{k-1}]$, s. t. $\mathbf{x} = \sum_j p_i \mathbf{x}_j = \sum_{i,j} p_j a_{i,j}|i\rangle$, i.e. $M = [p_i a_{i,j}]_{i,j}$, then it is a mixed state.
E.g., the system can be found in any pure state $|i\rangle$ with probability p_i.

We consider only pure states.

THE SEPARABILITY PROBLEM IN PURE STATES

- Given $\mathbf{z} \in \mathbb{H}_k$, decide whether there exist $\mathbf{x} \in \mathbb{H}_{k_1}$ and $\mathbf{y} \in \mathbb{H}_{k_2}$, with $k = k_1 + k_2$ and $1 \leq k_1, k_2 \leq k$, s. t. $\mathbf{z} = \mathbf{x} \otimes \mathbf{y}$, with $\mathbf{x} \in \mathbb{H}_{k_1}$ (length k_1, dimension 2^{k_1}), and $\mathbf{y} \in \mathbb{H}_{k_2}$ (length k_2, dimension 2^{k_2}).

$$\text{I.e.: Find } \mathbf{x} = \sum_{j=0}^{2^{k_1}-1} x_j |(j)_{2,k_1}\rangle, \quad \mathbf{y} = \sum_{j=0}^{2^{k_2}-1} y_j |(j)_{2,k_2}\rangle \tag{1}$$

s. t.

$$z = x \otimes y = \sum_{i=0}^{2^{k_1}-1} \sum_{j=0}^{2^{k_2}-1} x_i y_j |(i \cdot j)_{2,k_1+k_2}\rangle. \tag{2}$$

THE PAULI MATRICES

The following are the Pauli matrices:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If we rename the Pauli matrices:

$$\sigma_{00} = \sigma_0 \quad , \quad \sigma_{01} = \sigma_x \quad , \quad \sigma_{10} = \sigma_y \quad , \quad \sigma_{11} = \sigma_z .$$

PRODUCT OPERATIONS OF PAULI MATRICES

	σ_{00}	σ_{01}	σ_{10}	σ_{11}
σ_{00}	σ_{00}	σ_{01}	σ_{10}	σ_{11}
σ_{01}	σ_{01}	σ_{00}	$-i\,\sigma_{11}$	$i\,\sigma_{10}$
σ_{10}	σ_{10}	$i\,\sigma_{11}$	σ_{00}	$-i\,\sigma_{01}$
σ_{11}	σ_{11}	$-i\,\sigma_{10}$	$i\,\sigma_{01}$	σ_{00}

DENSE CODING PROTOCOL

Let $\mathbf{b}_{00} = \frac{1}{\sqrt{2}}(\mathbf{e}_{00} + \mathbf{e}_{11})$, then let us consider the following:

$$
\begin{aligned}
(\mathbb{I} \otimes \sigma_{00})\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \sim \mathbf{b}_{00} \\
(\mathbb{I} \otimes \sigma_{01})\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \sim \mathbf{b}_{01} \\
(\mathbb{I} \otimes \sigma_{10})\mathbf{b}_{00} &= \frac{i}{\sqrt{2}}(|01\rangle - |10\rangle) \sim \mathbf{b}_{11} \\
(\mathbb{I} \otimes \sigma_{11})\mathbf{b}_{00} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \sim \mathbf{b}_{10}
\end{aligned}
$$

where the equivalence relation "$\sim$" is s.t. given the vectors $e^{i\theta}\psi$ and ψ, if $e^{i\theta}\psi \sim \psi$ then the vectors are equal w.r.t. measurements.

Pauli matrices operations

Let $\tau_{ij} = \mathbf{1} \otimes \sigma_{ij}$, with $ij = 00, 01, 10, 11$.
τ_{ij}: the first qubit of a 2-quregister remains the same whilst the second is changed by σ_{ij}.

APPLY OF τ_{ij}

$\mathbf{b}_\varepsilon \setminus \mathbf{b}_\delta$	$\mathbf{b}_{00}$	$\mathbf{b}_{01}$	$\mathbf{b}_{10}$	$\mathbf{b}_{11}$
$\mathbf{b}_{00}$	τ_{00}	τ_{01}	τ_{10}	$-i\,\tau_{11}$
$\mathbf{b}_{01}$	τ_{01}	τ_{00}	$-i\,\tau_{11}$	τ_{10}
$\mathbf{b}_{10}$	τ_{10}	$-i\,\tau_{11}$	τ_{00}	τ_{01}
$\mathbf{b}_{11}$	$-i\,\tau_{11}$	τ_{10}	τ_{01}	τ_{00}

Each entry $T_{\varepsilon\delta}$ is such that $\mathbf{b}_\varepsilon = T_{\varepsilon\delta}\mathbf{b}_\delta$

Superdense coding in two dimensions

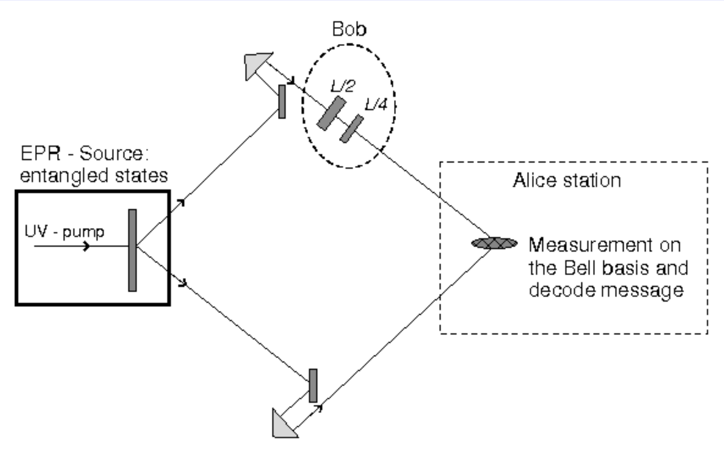
ASSUMPTIONS: Two parties, Alicia and Beto.

- Beto wants to convey two classical bits to Alicia: $\varepsilon_0\varepsilon_1$
- Both, Alicia and Beto share an entangled state $\boldsymbol{b}_{\delta_0\delta_1}$.

PROTOCOL: the precedure is as follows

- Beto apply $\sigma_{\varepsilon_0\varepsilon_1}$ to his qubit, wich means that $\tau_{\varepsilon_0\varepsilon_1}$ is applied to $\boldsymbol{b}_{\delta_0\delta_1}$ and by the table $\mathbf{y} = \boldsymbol{b}_{\eta_0\eta_1}$.
- Then Beto transmit his qubit to Alicia, who now knows $\mathbf{y}$.
- Making a measurement to $\mathbf{y}$ with respect to the Bell basis, then Alicia recognizes $\boldsymbol{b}_{\eta_0\eta_1}$.
- From the table Alicia is able to recover $\varepsilon_0\varepsilon_1$.

Optical implementation of the Dense Coding protocol



SUPERDENSE CODING

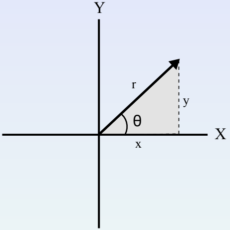
Sharing an entangled state is possible to transmit two classical bits using a single qubit.

Anthony Lawlor: *The Einstein-Rosen-Podolsky Bridge*

A *complex number* is denoted as $z = x + iy$ where x, y are real numbers and $i = \sqrt{-1}$ is called the imaginary unit. The set of all complex numbers is denoted as $\mathbb{C}$.

The complex conjugate of a complex number $x + iy$ is $x - iy$, and commonly is represented by $\overline{z}$.

The *modulus* of a complex number $x + iy$ is defined as $|x + iy| = \sqrt{x^2 + y^2}$.
There exists a one-to-one correspondence between the set $\mathbb{R}^2$ and $\mathbb{C}$ such that $(x, y) \in \mathbb{R}^2 : (x, y) \mapsto x + iy$.



Any complex number z can be written as (polar form)

$$z = x + iy = r(\cos\theta + i\sin\theta).$$

Let $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ and $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$ be complex numbers in polar form, it can be shown that:

$$z_1 z_2 = r_1 r_2\{\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\}$$

and

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\{\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2)\}.$$

In general, given $z_1, \ldots, z_n$ complex numbers,

$$z_1 \cdots z_n = r_1 \cdots r_n\{\cos(\theta_1+\cdots+\theta_n) + i\sin(\theta_1+\cdots+\theta_n)\}$$

and if $z_1 = \cdots = z_n$ we have that

$$\begin{aligned} z^n &= \{r(\cos\theta + i\sin\theta)\}^n \\ &= r^n(\cos n\theta + i\sin n\theta). \end{aligned}$$

If $n \in \mathbb{Z}^+$, the n-th root w of a complex number $z \in \mathbb{C}$ is expressed as

$$\begin{aligned} w &= z^{1/n} \\ &= \{r(\cos\theta + i\sin\theta)\}^{1/n} \\ &= r^{1/n}\left\{\cos\left(\frac{\theta+2k\pi}{n}\right) + i\sin\left(\frac{\theta+2k\pi}{n}\right)\right\} \end{aligned}$$

for $k = 0, 1, 2, \ldots, n-1$.

The *Euler formula* is $e^{i\theta} = \cos\theta + i\sin\theta$.

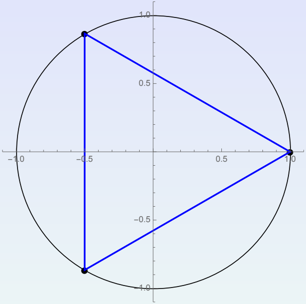
In general, for any
$z \in \mathbb{C}: e^{z} = e^{x+iy} = e^{x}e^{iy} = e^{x}(\cos y + i\sin y)$.

The solutions of the polynomial equation $z^n = 1$, with $n \in \mathbb{Z}^+$, are called the n-th roots of unity and are given by

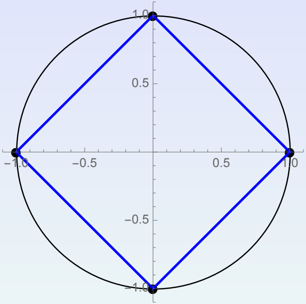
$$z = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{2k\pi i/n}$$

for $k = 0, 1, 2, \dots, n-1$.

Example: roots of unity

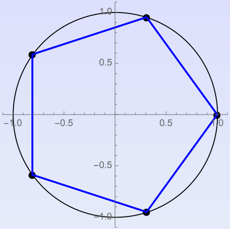


$k = 3$

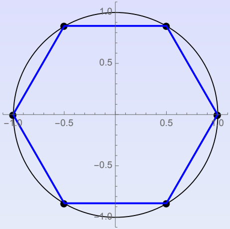


$k = 4$

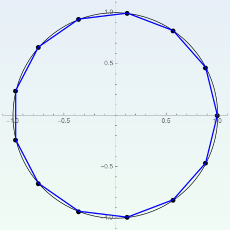
Preliminaries



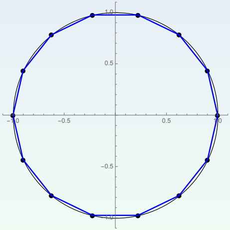
$k = 5$



$k = 6$



$k = 13$



$k = 14$

SUPERDENSE CODING

Let $k \geq 2$.
$\rho_k = e^{i\frac{2\pi}{k}}$: the primitive k-th root of unity.
$\mathbb{H}_1^{(k)} = \mathbb{C}^k$: the k-dimensional complex vector space and $\mathbf{e}_0, \ldots, \mathbf{e}_{k-1}$: the vectors in its canonical basis.
For any $m, n \in [\![0, k-1]\!]$ let

$$\mathbf{b}_{mn} = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{jm} \mathbf{e}_j \otimes \mathbf{e}_{(j+n) \bmod k}.$$

Then $B_{k2} = (\mathbf{b}_{mn})_{m,n \in [\![0,k-1]\!]}$ is an orthonormal basis of $\mathbb{H}_2^{(k)} = \mathbb{H}_1^{(k)} \otimes \mathbb{H}_1^{(k)}$, called Bell basis.

For any $m, n \in [\![0, k-1]\!]$ let $U_{mn} = [u_{mn\mu\nu}]_{\mu,\nu \in [\![0,k-1]\!]}$,

$$u_{mn\mu\nu} = \rho_k^{m\nu} \delta_{\mu,(\nu+n) \bmod k},$$

where, as usual δ_{ij} is the Kronecker's delta. Then

$$U_{mn}\mathbf{e}_j = \sum_{\mu=0}^{k-1} \rho_k^{mj} \delta_{\mu,(j+n) \bmod k} \mathbf{e}_\mu = \rho_k^{mj} \mathbf{e}_{(j+n) \bmod k}$$

$$\begin{aligned}
(\mathbf{1}_k \otimes U_{mn})\,\mathbf{b}_{00} &= (\mathbf{1}_k \otimes U_{mn}) \left(\frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \mathbf{e}_j \otimes \mathbf{e}_j \right) \\
&= \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} (\mathbf{1}_k \otimes U_{mn}) \left(\mathbf{e}_j \otimes \mathbf{e}_j \right) = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \mathbf{e}_j \otimes U_{mn}\mathbf{e}_j \\
&= \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{mj} \mathbf{e}_j \otimes \mathbf{e}_{(j+n) \bmod k} = \mathbf{b}_{mn}
\end{aligned}$$

Let $C_k = \left[\delta_{\mu,(\nu+1)\bmod k}\right]_{\mu,\nu\in[\![0,k-1]\!]}$ be the "rotation" $\mathbf{e}_\nu \mapsto \mathbf{e}_{(\nu+1)\bmod k}$. Then,

$$\begin{aligned}\forall m,n: \quad U_{mn} &= C_k^n U_{m0} = C_k^n U_{10}^m \\ &= C_k^n \left(\operatorname{diag}\left[\rho_k^\nu\right]_{\nu\in[\![0,k-1]\!]}\right)^m.\end{aligned}$$

Besides

$$U_{10} C_k = \rho_k C_k U_{10}.$$

Consequently, $U_{10} C_k^p = \rho_k^p C_k^p U_{10}$ y $U_{10}^q C_k^p = \rho_k^q C_k^p U_{10}^q$, which implies

$$\forall m,n,p,q: \quad U_{mn} U_{pq} = \rho_k^{nq} U_{(m+p)\bmod k,(n+q)\bmod k}.$$

Thus,

$$\begin{aligned}
(\mathbf{1}_k \otimes U_{mn})\,\mathbf{b}_{pq} &= (\mathbf{1}_k \otimes U_{mn}) \circ (\mathbf{1}_k \otimes U_{pq})\,\mathbf{b}_{00} \\
&= (\mathbf{1}_k \otimes (U_{mn}U_{pq}))\,\mathbf{b}_{00} \\
&= \rho_k^{nq}\left(\mathbf{1}_k \otimes U_{(m+p)\bmod k,(n+q)\bmod k}\right)\mathbf{b}_{00} \\
&= \rho_k^{nq}\,\mathbf{b}_{(m+p)\bmod k,(n+q)\bmod k},
\end{aligned}$$

and $\forall m, n, p, q$

$$\forall m, n, p, q : \left[\rho_k^{-(m-p)(n-q)\bmod k}\left(\mathbf{1}_k \otimes U_{(m-p)\bmod k,(n-q)\bmod k}\right)\right]\mathbf{b}_{pq} = \mathbf{b}_{mn}.$$

A TWO PARTY PROTOCOL

The equations (3) and (3) allow a superdense coding protocol:

1. Alice and Bob agree in a maximally entangled state $\mathbf{b}_{pq}$.
2. Bob applies to his qubit a transformation U_{uv} in order to produce a phase displacement of $\mathbf{b}_{mn}$, according to eq. (3), and sends his qubit to Alice.
3. Knowing both qubits, Alice is in possession of a phase displacement of $\mathbf{b}_{mn}$. She perform a measurement with respect to Bell basis B_{k2}, she recognizes $\mathbf{b}_{mn}$ and using eq. (3) she is able to recognize the transformation U_{uv} applied by Bob.

Thus through the transmission of one qubit, Bob may communicate $\log_2 k^2$ classical bits to Alice.

Let $k \geq 2$.
$\mathbb{H}_k^{(k)} = \left(\mathbb{H}_1^{(k)}\right)^{\otimes k}$: the k-fold tensorial power of $\mathbb{H}_1^{(k)} = \mathbb{C}^k$.
For any $n_0, n_1, \ldots, n_{k-1} \in [\![0, k-1]\!]$

$$\mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}} = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \rho_k^{j n_0} \mathbf{e}_j \otimes \bigotimes_{\ell=1}^{k-1} \mathbf{e}_{(j+n_\ell) \bmod k} \cdot$$

Then $B_{kk} = \left(\mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}}\right)_{n_0, n_1, \ldots, n_{k-1} \in [\![0, k-1]\!]}$ is an orthonormal basis of $\mathbb{H}_k^{(k)}$. As in eq. (3),

$$\left(\mathbf{1}_k \otimes \bigotimes_{\ell=1}^{k-1} U_{p_\ell q_\ell}\right) \mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}} =$$
$$\rho_k^{\sum_{\ell=1}^{k-1} q_\ell n_\ell} \, \mathbf{b}^{(k)}_{(n_0 + \sum_{\ell=1}^{k-1} p_\ell) \bmod k, (q_1+n_1) \bmod k, \cdots, (q_{k-1}+n_{k-1}) \bmod k}$$

However, at present case there are $\left(k^2\right)^{k-1} = k^{2k-2}$ maps of the form $\left(\mathbf{1}_k \otimes \bigotimes_{\ell=1}^{k-1} U_{p_\ell q_\ell}\right)$ and there are k^k registers in Bell basis. One can see that for any two $\mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}}$, $\mathbf{b}^{(k)}_{m_0 m_1 \cdots m_{k-1}}$ there are exactly

$$\frac{k^{2k-2}}{k^k} = k^{k-2}$$

maps transforming the first register into the second one. Thus there is no univocity in superdense coding.

Let $U^r_{m_0 m_1 \cdots m_{k-1}} \subset \left(\mathbf{1}_k \otimes \bigotimes_{\ell=1}^{k-1} U_{p_\ell q_\ell}\right)$ for $r \in [\![0, k^{k-2} - 1]\!]$, s.t. satisfies:

$$U^r_{m_0 m_1 \cdots m_{k-1}} \mathbf{b}^{(k)}_{n_0 n_1 \cdots n_{k-1}} = \mathbf{b}^{(k)}_{m_0 m_1 \cdots m_{k-1}},$$

- We have that $\mathrm{card}(U^r_{m_0 m_1 \cdots m_{k-1}}) = k^k$, for any subset r, then we can transmit $\log_2 k^k$ classical bits.
- In general for any vector $\mathbf{b}^{(k)}_{n_0 n_1, \cdots n_{k-1}}$ each subset r is s.t. its indexes $p_\ell q_\ell$ are as follow: for $p = \sum_{\ell=1}^{k-1} p_\ell$ fixed, with $p \in [\![0, k-1]\!]$, the values $q_\ell = q_1 q_2 \cdots q_{k-1}$ maintain a lexicographical order.

THE STEINER PROTOCOL

Given the observable

$$M_x = \begin{pmatrix} \cos x & \operatorname{sen} x \\ \operatorname{sen} x & -\cos x \end{pmatrix}, \quad x \in [0, 2\pi] \tag{3}$$

with eigenvalues $\lambda_0 = -1, \lambda_1 = +1$ and eigenvectors

$$\mathbf{u}_{x0} = \operatorname{sen}\frac{x}{2}\mathbf{e}_0 - \cos\frac{x}{2}\mathbf{e}_1 \tag{4}$$

$$\mathbf{u}_{x1} = \cos\frac{x}{2}\mathbf{e}_0 + \operatorname{sen}\frac{x}{2}\mathbf{e}_1. \tag{5}$$

For any $\mathbf{y} \in \mathbb{H}$, the observable M_x outputs the eigenvalue λ_i with probability $\langle \mathbf{y} | \mathbf{u}_{xi} \rangle$. If $\mu_x(\mathbf{y})$ is the result of applies M_x on $\mathbf{y}$, then μ_x is a measurement,

$$\Pr(\mu_x(\mathbf{e}_i) = \lambda_j) = \langle \mathbf{e}_i | \mathbf{u}_{xj} \rangle^2 = \left(\operatorname{sen}^2\frac{x}{2}\right)\delta_{ij} + \left(\cos^2\frac{x}{2}\right)(1 - \delta_{ij}) \tag{6}$$

VON NEUMANN MEASUREMENTS $(M_x)_{x\in[0,2\pi]}$

If Alice and Bob are applying measurements M_{x_0} and M_{x_1} over the first and the second qubit of a Bell vector $\mathbf{b}_{i_0 i_1}$ respectively, then the corresponding outputs are $\mu_{x_k}(\mathbf{e}_{i_k})$, $k = 0, 1$. According to relation (6), for any $j_0, j_1 \in \{0, 1\}$, we have

$$\begin{aligned}
&\Pr((\mu_{x_0}(\mathbf{e}_{i_0}), \mu_{x_1}(\mathbf{e}_{i_1})) = (\lambda_{j_0}, \lambda_{j_1})) \qquad (7)\\
&= \frac{1}{2}\begin{cases} \left(\cos^2 \frac{x_0-(-1)^{i_0}x_1}{2}\right)\delta_{j_0 j_1} + \left(\mathrm{sen}^2 \frac{x_0-(-1)^{i_0}x_1}{2}\right)(1-\delta_{j_0 j_1}) & \text{if } i_0 = i_1 \\ \left(\mathrm{sen}^2 \frac{x_0-(-1)^{i_0}x_1}{2}\right)\delta_{j_0 j_1} + \left(\cos^2 \frac{x_0-(-1)^{i_0}x_1}{2}\right)(1-\delta_{j_0 j_1}) & \text{if } i_0 \neq i_1 \end{cases}
\end{aligned}$$

Simulation using local hidden variables

$(t_n)_n$ is a sequence of unif. dist. random number in $[0,1]$	
Bob	**Alice**
$y_0 \in [0,1]$ $(s_n)_n$ is a sequence of unif. dist. random numbers in $[0,1]$. $k_0 = \min(k \mid s_k \leq \lvert\cos(2\pi(t_k - y_0))\rvert)$ Output $a_0 = \mathrm{Sgn}(\cos(2\pi(t_{k_0} - y_0)))$	$y_1 \in [0,1]$ Receive k_0 Output $a_1 = \mathrm{Sgn}(\cos(2\pi(t_{k_0} - y_1)))$

We have that $\Pr(a_0 = a_1) = \cos^2(2\pi(t_{k_0} - y_1))$. Thus, whenever $y_0 = y_1$, Alice and Bob would output the same values. This protocol allows measurements on the Bell state $\mathbf{b}_{00}$.

The Brassard protocol

Let $x, y \in [0, 2\pi]$ be the measurement parameters over the first and second qubit of Ψ_{AB} and let $a, b \in \{0, 1\}$ their respective outcomes.

	$\Pr[b = 0]$	$\Pr[b = 1]$
$\Pr[a = 0]$	$\frac{1}{2}\cos^2(\frac{x-y}{2})$	$\frac{1}{2}\sin^2(\frac{x-y}{2})$
$\Pr[a = 1]$	$\frac{1}{2}\sin^2(\frac{x-y}{2})$	$\frac{1}{2}\cos^2(\frac{x-y}{2})$

There exists a local hidden variable scheme that reproduces this probability distribution.

The collection $V_{10} = \left(e^{i\frac{\pi}{5}j}\right)_{j\in[\![0,9]\!]}$ is the regular decagon in the unit circle in $\mathbb{C}$. For each $j \in [\![0,9]\!]$, let $A_j = \{e^{2i\pi x} \in \mathbb{C} |\ \frac{j}{10} \leq x < \frac{j+1}{10}\}$ be the arc joining the j-th and $(j+1)$-th vertexes in the regular decagon. Similarly, let for $t \in [0, \frac{3}{10}[$ and for $j \in [\![0,2]\!]$,

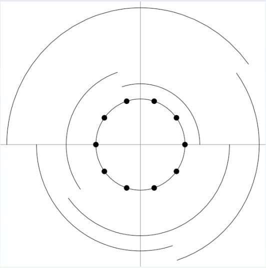
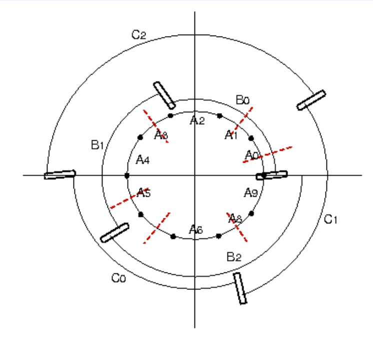


FIGURE: Sets B_{tj} and C_{tj}, for $t = 0$.

$$
\begin{aligned}
\beta_{tj} &= \frac{3}{10}j + t, \\
B_{tj} &= \left\{e^{2i\pi x} \in \mathbb{C} |\ \beta_{tj} \leq x < \beta_{t,(j+1)\bmod 3}\right\} \\
\gamma_{tj} &= \beta_{tj} + 1/2, \\
C_{tj} &= \left\{e^{2i\pi x} \in \mathbb{C} |\ \gamma_{tj} \leq x < \gamma_{t,(j+1)\bmod 3}\right\}.
\end{aligned}
$$

Let $\mathcal{P}_t = \left(A_{j_a} \cap B_{tj_b} \cap C_{tj_c}\right)_{(j_a,j_b,j_c)\in[\![0,9]\!]\times[\![0,2]\!]^2}$ be the induced partition over the unit circle.

- If t is a multiple of $\frac{1}{10}$ then $\mathcal{P}_t$ consists of 10 arcs A_j.
- Otherwise it consists of 16 arcs.



Given a point $e^{2i\pi x}$ in the unit circle, there is an unique triple $(j_a, j_b, j_c)(x, t) \in [\![0, 9]\!] \times [\![0, 2]\!]^2$ s.t. $e^{2i\pi x} \in A_{j_a(x,t)} \cap B_{tj_b(x,t)} \cap C_{tj_c(x,t)}$. Four bits are sufficient to determine $(j_a, j_b, j_c)(x, t)$, says $\varepsilon(x, t) \in \{0, 1\}^4$.

Simulation using local hidden variables

Alice and Bob share a hidden variable $c \in \{0, 1\}$, they agree in a parameter $t \in [0, \frac{3}{10}[$. Alice possesses $x \in [0, 1]$ and Bob $y \in [0, 1]$.

1. Alice calculates $\delta = \varepsilon(x, t)$ and sends it to Bob. She outputs bit $a = c$.
2. Bob calculates the triple (i_a, i_b, i_c) corresponding to δ and his own triple $(j_a, j_b, j_c) = (j_a, j_b, j_c)(y, t)$.
   2.1. If $|i_a - j_a| > 2$ then $y = y + \frac{1}{2}$ and $c = 1 - c$;
   2.2. for each $j \in [\![0, 2]\!]$ let $\alpha_j = \beta_{tj}$;
   2.3. if $j_a \in \{7, 8, 9, 0, 1\}$ then for each $j \in [\![0, 2]\!]$ let $\alpha_j = \gamma_{tj}$;
   2.4. if $\exists j \in [\![0, 2]\!]$: $\alpha_j \leq x, y \leq \alpha_{j+1}$ then output $b = c$
   else there exists $j \in [\![0, 2]\!]$ such that α_j lies between x and y; output $b = c$ with probability $1 - \frac{3\pi}{5} \sin(2\pi|y - \alpha_j|)$.

ENTANGLEMENT SIMULATION

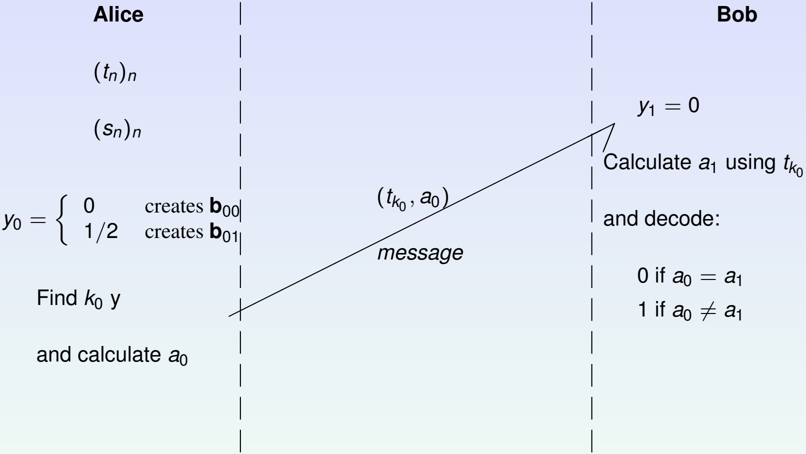


FIGURE: Simulation scheme using the Steiner protocol. The transversal line represent classical information transfer.

ENTANGLEMENT SIMULATION

Alice

$$x = \begin{cases} 0 & \text{creates } \mathbf{b}_{00} \\ \pi & \text{creates } \mathbf{b}_{01} \end{cases}$$

Calculate $\delta = \varepsilon(x, t)$

and outputs

the bit a

$(\delta \in \{0,1\}^4, a)$

message

Bob

$y = 0$

Calculate b using δ

y decode:

0 if $a = b$

1 if $a \neq b$

FIGURE: Simulation scheme using the Brassard protocol. The transversal line represent classical information transfer.

Thanks for your attention !!