Quantum verification with limited resources

Aleksandra Gočanin[1]

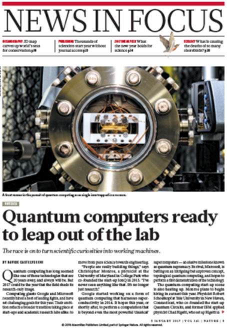
[1] Faculty of Physics, University of Belgrade

09.09.2021.

Outline

Milestone

- Construction of the (commercial) quantum computer.
- The use of quantum resources for solving various problems.
- Simulations of physical systems.
- Era of NISQD (noisy-intermediate scale quantum devices).



NEWS IN FOCUS

Quantum computers ready to leap out of the lab

The race is on to turn scientific curiosities into working machines.

Current use of Quantum devices

- Quantum processors up to 100 qubits - scientific development, simulations of biological systems, optimization problems, machine learning...
- 32 qubit simulator available online for experiments and studies.
- IBM Q Experience (https ://qiskit.org/textbook/preface.html).

FIGURE – https ://www.research.ibm.com/ibm-q/

Basics of Quantum Information

- $\mathcal{H} = \mathbb{C}^d$: The most relevant case is $d = 2$.
- Pure state of a qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

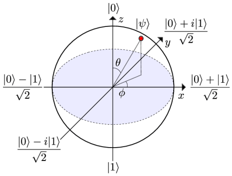


FIGURE – Representation of qubit states on Bloch sphere

- Pure state of N qubits

$$|\psi_N\rangle = \sum_{i_1 \dots i_N = 0,1} \alpha_{i_1 \dots i_N} |i_1 \dots i_N\rangle \qquad \sum_{i_1 \dots i_N = 0,1} |\alpha_{i_1 \dots i_N}|^2 = 1.$$

- Preparation of the mixed state : $\{p_i, |\psi_i\rangle\}$. The density operator *mixed state for such a system is*

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad \sum_i p_i = 1.$$

Basics of Quantum Information

- **Transformation**
  - Time-evolution of a **isolated** quantum system $\rho' = U\rho U^\dagger$
  - **Non-isolated** system : *Kraus operators* $\sum_a M_a^\dagger M_a = \mathbb{1}$.
    Quantum channel : $\epsilon(\rho) = \sum_a M_a \rho M_a^\dagger$.
- **Measurement**
  - **Projective measurement** $M = \sum_m m P_m$, $p(m) = \mathrm{Tr}(P_m \rho)$ and $\rho_{after} = \frac{P_m \rho P_m}{\mathrm{Tr}(P_m \rho)}$.
  - **General quantum measurement** : $\sum_m M_m^\dagger M_m = \mathbb{1}$ $p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho)$.
    POVM elements $E_m = M_m^\dagger M_m$, $\sum_m E_m = \mathbb{1}$ and $p(m) = \mathrm{Tr} E_m \rho$.
- **Operational approach to Quantum Mechanics**

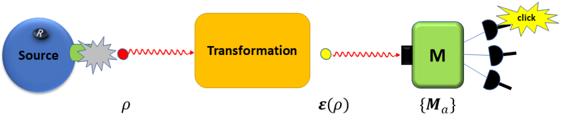


FIGURE – The basic elements of quantum information processing : preparation, transformation and measurement of a quantum system.

Quantum entanglement

- 2 subsystems A and B : $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is *separable if and only if :*

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle.$$

$$\rho_{AB} = \sum_i p_i |\psi_A^{(i)}\rangle\langle\psi_A^{(i)}| \otimes |\psi_B^{(i)}\rangle\langle\psi_B^{(i)}|, \;\; \textit{such that} \;\; p_i \in [0,1] \;\; \textit{and} \;\; \sum_i p_i = 1.$$

- *N subsystems (e.g. qubits)*

  Pure state $|\psi_N\rangle \in \otimes_{k=1}^{N} H^{(k)}$ *is fully separable* $|\psi_N\rangle = \otimes_{i=1}^{N} |\phi_i\rangle$.

  Mixed state ρ_N *is fully separable if*
  $\rho = \sum_k \omega_k |\phi_1^{(k)}\rangle\langle\phi_1^{(k)}| \otimes |\phi_2^{(k)}\rangle\langle\phi_2^{(k)}| ... \otimes |\phi_N^{(k)}\rangle\langle\phi_N^{(k)}|$, *where* $\sum_k \omega_k = 1$.

- *If the quantum state is not fully separable then it contains some* ***entanglement****.*

> ***Quantum entanglement*** *:*
> *Resource for quantum computation and quantum communication.*

The task of quantum verification

Given a limited number of interactions with a large system, how much classical information can we learn with a high degree of certainty?

Motivation

Verification of quantum entanglement

- Reliable verification of quantum entanglement is a considerable challenge when dealing with large-scale quantum systems.
- Two main issues : Resources (time, experimental stability, number of different measurements, number of copies) and complex data post-processing.

The witness operator

(O. Gühne, & G. Tóth, *Phys. Rep.* **474**, 1 (2009).)

- $\mathrm{Tr}(W\rho_s) \geq 0$ for all separable states ρ_s.
- Local decomposition of witness operator.
- Large number of identically prepared copies in order to extract the corresponding mean value with high accuracy.

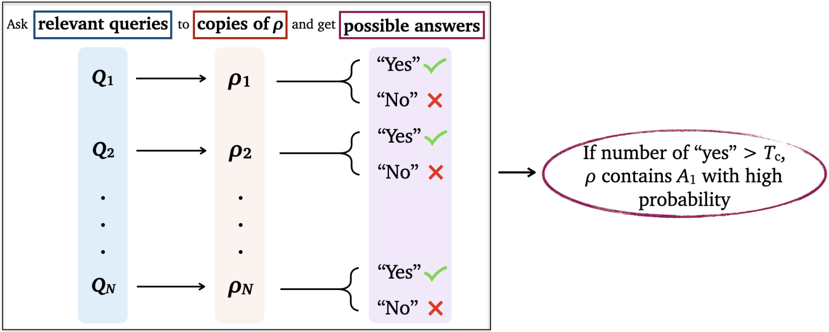
Quantum state tomography

- Unfeasible for large systems due to the exponential growth of the number of measurements with the size of the system.

New approach !

Probabilistic approach to the property verification

Does ρ contain the property A_1?



Probabilistic entanglement detection

The goal

- Given a **large quantum system** (tens of qubits), verify whether entanglement is present in it by minimizing time and resources.

- Focus on a single experimental run.

- Central quantity for entanglement detection is **the probability of success** of the quantum state to perform certain binary tasks.

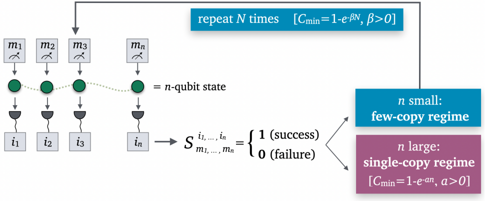
Advantages :

a) It promises a dramatic reduction of the resources needed for reliable verification in large quantum systems.

b) It provides a simple tool for reliable statistical analysis of errors and confidence intervals.

A. D. & B. Dakić. *NPJ Quantum Information* **4(1),** 11 (2018).

Probabilistic framework for entanglement detection



1. A sequence of measurement settings $\{m_1, m_2, \ldots, m_n\}$ is randomly generated from the probability distribution of settings $\Pi(m_1, \ldots, m_M)$.
2. The measurements are locally executed on each subsystem and the set of outcomes $\{i_1, \ldots, i_n\}$ is obtained.
3. A certain binary (1/0) cost function of settings and outcomes $S_{[n]} = F^{i_1 \ldots i_n}_{m_1 \ldots m_n}$ is computed.
4. If $S_{[n]} = 1/0$ we associate "success/failure" to the experimental run.

- Repeating this procedure N times, the probability of detecting entanglement goes to unity exponentially fast in N for target state preparations, i.e. the (lower bound on) detection confidence grows as $C_{\min} = 1 - \exp[-\alpha(n)N]$

Example of k-producible entangled states

- **k-producible state** : $|\phi_1\rangle|\phi_2\rangle\dots|\phi_n\rangle$, where the products $|\phi_s\rangle$ involve at most k parties.
- For simplicity - **quantum singlet** : $|\psi_0\rangle = \left|\psi^-\right\rangle^{\otimes n}$, where $\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
- Set of $\{X, Y, Z\}$ measurement settings for each qubit with binary outcomes $i = 0, 1$.
- The quantum singlet : $X \otimes X = Y \otimes Y = Z \otimes Z = -1 \implies$ perfect anticorrelations.

Choice of measurement settings :

$$m_1 = \frac{\mathbb{1} - X \otimes X}{2}, \quad m_2 = \frac{\mathbb{1} - Y \otimes Y}{2}, \quad m_3 = \frac{\mathbb{1} - Z \otimes Z}{2}.$$

- Entanglement detection : there is no separable state for which the measurement reveals $m_1 = m_2 = m_3 = 1$.

$$P_{\rho sep} = \langle \frac{1}{3}(m_1 + m_2 + m_3) \rangle \leq \frac{2}{3}$$

Quantum singlet example

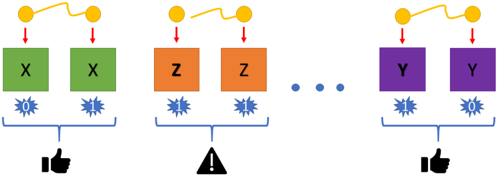


FIGURE – Protocol for $2n$ qubit state, ideally consisting of quantum singlets.

- Perform our protocol and calculate : $R_{[n]} = \sum_{p=1}^{n} S_p$, where S_p is the outcome of the correlation measurement on individual pair.

$$S_p = \frac{1}{2}\left(1 - (-1)^{i_p + j_p}\right), i_p, j_p = 0, 1$$

- The cost function is defined as

$$S_{[n]} = \begin{cases} 1, & R_{[n]} \geq (\frac{2}{3} + \delta)n \\ 0, & R_{[n]} < (\frac{2}{3} + \delta)n \end{cases}$$

Quantum singlet example

- The overall **probability of success** reads :

$$P_\rho[S_{[n]} = 1] = P_\rho\left[S_1 + \cdots + S_n \geq \left(\frac{2}{3} + \delta\right) n\right]$$

- Chernoff bound !

$$\boxed{P_{\rho_{sep}}[S_{[n]} = 1] \leq e^{-D(\frac{2}{3}+\delta||\frac{2}{3})n},}$$

where $D(x||y) = x \log \frac{x}{y} + (1-x) \log \frac{1-x}{1-y} \geq 0$ is the Kullback–Leibler divergence ;

- $\delta = \frac{s}{N} - \frac{2}{3}$, where s is number of successful outcomes in experiment.
- $\delta > 0 \implies$ probability of success for entanglement detection : $1 - e^{-D(\frac{2}{3}+\delta||\frac{2}{3})N}$.
- $\delta \leq 0 \implies$ experimental run is inconclusive.

Other examples

- **Linear cluster state (LCS)**
  - The n-qubit LCS is uniquely defined by the set of 2^n stabilizers, i.e.

    $$G_{q_1\dots q_n}|LCS\rangle = G_1^{q_1}\dots G_n^{q_n}|LCS\rangle = +1|LCS\rangle,$$

    where $G_k = Z_{k-1}X_kZ_{k+1}$ and $q_k = 0, 1$.
  - Combinatorics : Dividing LCS into partitions of L qubits.
  - Applying suitably chosen measurements related to stabilizers to the partitions - using incompatibility of local measurements.
  - Chernoff bound :

    $$P_{\rho sep}[S_{[n]} = 1] \leq e^{-D(\frac{2}{3}+\delta||\frac{2}{3})L}$$

    One copy of 24-qubit LCS suffices to verify entanglement with confidence $> 95\%$!

- **Ground states of local Hamiltonians**
  - L-local Hamiltonian on some graph of n particles $H = \sum_{k=1}^n H^{(k)}$, where $H^{(k)}$ acts on at most L subsystems (L is fixed and independent of n).
  - Entanglement gap $g_E = \epsilon_s - \epsilon_0 > 0 \rightarrow P_{\rho sep}[S_{[n]} = 1] \leq \exp[-n\kappa^2\delta^2], \quad \kappa > 0.$

Building the general framework

What if we work with smaller quantum systems ? Or we want to work in Device-Independent regime ?

Expectations ?

Provide generic framework to translate any entanglement witness to a reliable and resource-efficient decision procedure which :

a) detects quantum entanglement with confidence that grows exponentially fast to certainty with the number of copies of the quantum state,
b) is implemented via local measurements only
c) does not require an assumption of *independent and identically distributed* (**i.i.d.**) experimental runs and
d) provides reliable detection even if the number of available copies is less than the total number of measurement settings needed to extract the mean value of the witness operator.

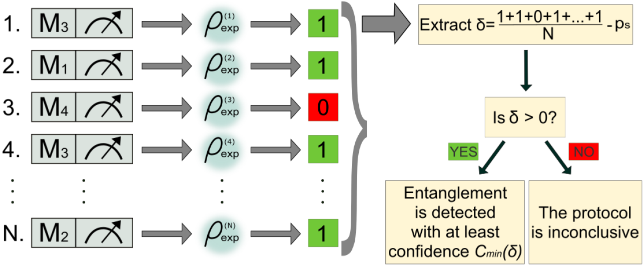
V. Saggio, A. D., C. Greganti, L. A. Rozema, P. Walther, and B. Dakić, *Nature Physics*, **15**, 935-940 (2019).

Translation of entanglement witnesses

How to choose appropriate measurement settings M_k ?

- Equivalence transformation $W \rightarrow W' = aW + b\mathbb{1}$.
- Probability of success : $\langle W' \rangle = \mathrm{Tr}(W' \rho_{exp})$.
- $\langle W \rangle = \mathrm{Tr}(W \rho_s) \geq 0$ for any separable state ρ_s.
- $\langle W' \rangle$ upper bounded by p_s for any separable state and achieves $p_e > p_s$ for a certain entangled state.
- Find the local decomposition of W'.

Building the realistic framework



$$C_{\min}(\delta) = 1 - e^{-D(p_s+\delta||p_s)N}$$

Entanglement verification procedure

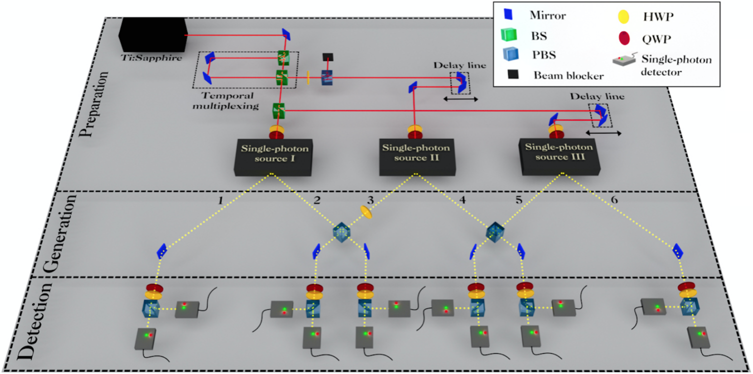
1. Randomly draw the measurements M_k's (each with probability Π_k) from the set $\mathcal{M}$ N times;
2. Apply each drawn M_k to ρ_{exp} to get the corresponding binary outcome $m_k = 1, 0$;
3. Count the number of successful outcomes S and calculate the difference $\delta = \frac{S}{N} - p_S$;
4. If $\delta > 0$, entanglement is certified with at least confidence $C_{\min}(\delta)$. Otherwise, the test is inconclusive.

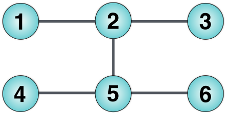
Illustrative example

Example of n-qubit cluster state

1. Start with standard witness $W = \frac{1}{2}\mathbb{1} - |G\rangle\langle G|$.
2. After equivalence transformation : $W' = \frac{1}{2}\mathbb{1} + \frac{1}{2}|G\rangle\langle G| \implies \langle W' \rangle \leq 3/4 = p_s$.
3. Decomposition via stabilizers : $|G\rangle\langle G| = \frac{1}{2^n}\sum_{k=1}^{2^n} S_k$.
4. $W' = \frac{1}{2^n}\sum_{k=1}^{2^n} M_k$, where $M_k = (\mathbb{1} + S_k)/2$ with uniform sampling

Experimental implementation





H-shaped six-qubit cluster state

$$|Cl_6\rangle = \frac{1}{2}(|H_1 H_2 H_3 H_4 H_5 H_6\rangle + |H_1 H_2 H_3 V_4 V_5 V_6\rangle + |V_1 V_2 V_3 H_4 H_5 H_6\rangle - |V_1 V_2 V_3 V_4 V_5 V_6\rangle)$$

Adaption of the protocol to our state

It means...

...finding the M_k operators and the separable bound p_s for our target state.

- We start from two witness operators (detecting *genuine six-qubit entanglement*) and translate them into our probabilistic protocol :

$W_1 = 3\mathbb{1} - 2\left(\prod_{k=1,3,5} \frac{\mathbb{1}+G_k}{2} + \prod_{k=2,4,6} \frac{\mathbb{1}+G_k}{2}\right)$	$W_2 = \frac{1}{2}\mathbb{1} - \lvert Cl_6\rangle\langle Cl_6\rvert$
$\{M_1 = \prod_{k=1,3,5} \frac{\mathbb{1}+G_k}{2},$ $M_2 = \prod_{k=2,4,6} \frac{\mathbb{1}+G_k}{2}\}$	$M_k = \frac{\mathbb{1}+S_k}{2}$ where $k = 1, ..., 2^6$
$p_{s1} = \frac{3}{4}$	$p_{s2} = \frac{3}{4}$

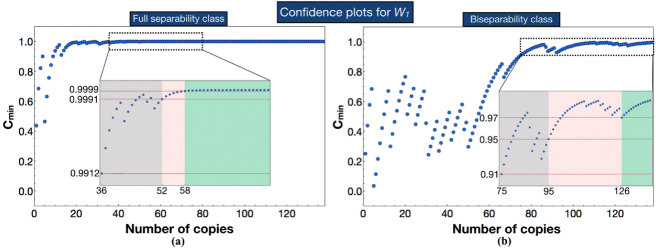
- Additionally, we can numerically find a bound to detect *only some entanglement* :

$p_{fs1} = \frac{9}{16}$	$p_{fs2} = \frac{5}{8}$

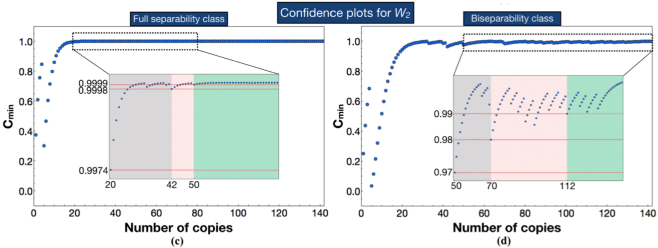
G. Tóth & O. Gühne, *Phys. Rev. Lett.* **94(6),** 060501 (2005).

Results

- 2 measurement settings sampled $N = 150$ times.

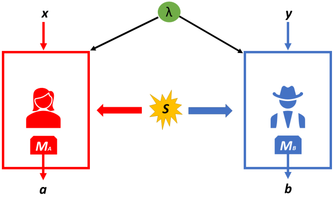


- 64 measurement settings sampled $N = 160$ times.



Nonlocality

- Typical Bell experiment

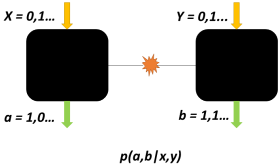


- Locality condition in the context of Bell experiments is as follows :

$$p(a, b|x, y) = \int_{\Lambda} \mathrm{d}\lambda q(\lambda) p(a|x, \lambda) p(b|y, \lambda).$$

Bell Theorem : *No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics.*

Self-testing



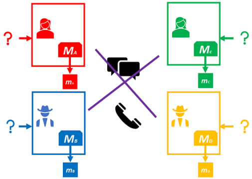
- Self-testing is a method to deduce the underlying physics of a quantum experiment in a black box scenario.
- Device-independent scenario.
- Self-test of a target quantum state : maximal violation of corresponding Bell's inequality.
- For source producing separable states one gets

$$\mathcal{F}(\{p(a,b|x,y)\}) \leq \mathcal{B}.$$

- Example of **3-qubit GHZ state** : $\psi_{GHZ} = (|000\rangle + |111\rangle)/\sqrt{2}$.
- Its self-test : the maximal violation of the Mermin inequality :

$$\langle A_0 B_0 C_1 \rangle + \langle A_0 B_1 C_0 \rangle + \langle A_1 B_0 C_1 \rangle - \langle A_1 B_1 C_1 \rangle \leq 2$$

Nonlocality detection



- Example of 4-qubit cluster state : $|LCS_4\rangle = \frac{1}{2}(|+\rangle|0\rangle|+\rangle|0\rangle + |+\rangle|0\rangle|-\rangle|1\rangle + |-\rangle|1\rangle|-\rangle|0\rangle + |-\rangle|1\rangle|+\rangle|1\rangle)$.
- Inequality : $A_1C_1D_2 + 2A_2B_1C_2D_2 + A_1C_2D_1 - 2A_2B_1C_1D_1 + B_2C_1D_2 + B_2C_2D_1 \leq 4$
- The algebraic maximum of 8 with a cluster state.
- (A_i, B_j, C_k, D_l) are Z and X up to local rotations.

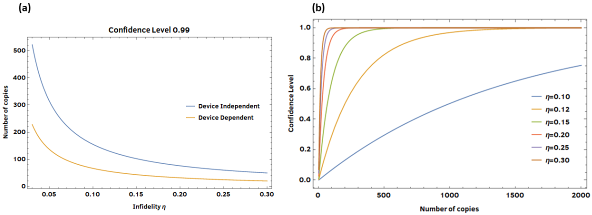
$$P_s = \frac{1}{8}(Q_1 + 2Q_2 + Q_3 + 2Q_4 + Q_5 + Q_6),$$

where $Q_1 = \frac{\mathbb{1}+A_1C_1D_2}{2}$, $Q_2 = \frac{\mathbb{1}+A_2B_1C_2D_2}{2}$, $Q_3 = \frac{\mathbb{1}+A_1C_2D_1}{2}$, $Q_4 = \frac{\mathbb{1}-A_2B_1C_1D_1}{2}$, $Q_5 = \frac{\mathbb{1}+B_2C_1D_2}{2}$ and $Q_6 = \frac{\mathbb{1}+B_2C_2D_1}{2}$.

- Local wining strategy $p_{local} = 3/4$.
- Confidence level $C(\delta_0) = 1 - P(\delta_0) \geq 1 - e^{-D(p_{local}+\delta_0||p_{local})N} = C_{\min}(\delta_0)$.

Device Independent Quantum State Verification

- Fix the lower bound on average extractability (i.e. fidelity $\frac{1}{N}\sum_{i=1}^{N}\langle\psi|\rho|\psi\rangle$) that we want to certify $1-\eta$ which implies the lower bound on the average success probability of the whole sample.
- Fix the allowed tolerance from the optimal success rate and the corresponding verification confidence $1-\delta$.
- Run the protocol : measure all the available copies (N of them) according to a procedure corresponding to a self-test for the corresponding target state.
- If the success rate is greater than minimal allowed, the protocol is successful and average extractability of the measured sequence of states is $\Xi \geq 1-\eta$ with confidence level $1-\delta$. Otherwise, the protocol is inconclusive.



Dimić, A., Šupić, I., Dakić, B. (2021). Sample-efficient device-independent quantum state verification and certification. arXiv preprint arXiv :2105.05832.

Conclusions

- We provide a method to detect entanglement/verify quantum state with high confidence with a reduced number of copies.
- The protocol is based on a probabilistic procedure and a translation of witness operators/Bell's inequality into it.
- *Any* witness operator/ Bell's inequality/ tight self-test can be translated into the protocol.
- Rather than measuring mean values of witness operators or collecting the whole statistics while testing Bell's inequality, we focus on single-copy measurements only.

For the real end !

Take the right fingerprint of the target quantum state !

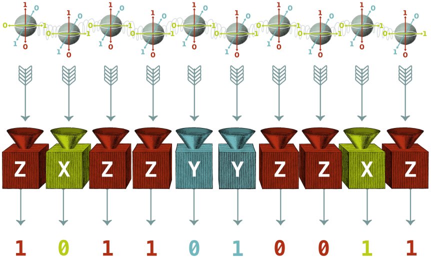


Photo credit : Juan Palomino