No-cloning theorem and related issues (Lecture of the Quantum Information class of the Master in Quantum Science and Technology)

Géza Tóth

Theoretical Physics, University of the Basque Country (UPV/EHU), Bilbao, Spain
Donostia International Physics Center (DIPC), San Sebastián, Spain
IKERBASQUE, Basque Foundation for Science, Bilbao, Spain
Wigner Research Centre for Physics, Budapest, Hungary

UPV/EHU, Leioa
11, 16 February 2021

Outline

No-cloning theorem

Received 15 June; accepted 1 September 1982.

1. Kagi, J. H. R. & Nordberg, M. (eds) *Metallothionein* (Birkhauser, Basle, 1979).
2. Karin, M. & Herschman, H. R. *Science* **204,** 176–177 (1979).
3. Pulido, P., Kagi, J. H. R. & Vallee, B. L. *Biochemistry* **5,** 1768–1777 (1966).
4. Rudd, C. J. & Herschmann, H. R. *Tox. appl. Pharmac.* **47,** 273–278 (1979).
5. Karin, M. & Herschman, H. R. *Eur. J. Biochem.* **107,** 395–401 (1980).
6. Kissling, M. M. and Kagi, J. H. R. *FEBS Lett.* **82,** 247–250 (1977).
7. Karin, M. *et al. Nature* **286,** 295–297 (1980).
8. Karin, M., Slater, E. P. & Herschman, H. R. *J. cell. Physiol.* **106,** 63–74 (1981).
9. Durnam, D. M. & Palmiter, R. D. *J. biol. Chem.* **256,** 5712–2716 (1981).
10. Hager, L. J. & Palmiter, R. D. *Nature* **291,** 340–342 (1981).
11. Karin, M. & Richards, R. *Nucleic Acids Res.* **10,** 3165–3173 (1982).
12. Lawn, R. M. *et al. Cell* **15,** 1157–1174 (1978).
13. Southern, E. M. *J. molec. Biol.* **98,** 503–517 (1975).
14. Benton, W. D. & Davis, R. W. *Science* **196,** 180–182 (1977).
15. Glanville, N., Durnam, D. M. & Palmiter, R. D. *Nature* **292,** 267–269 (1981).
16. Breathnach, R. *et al. Proc. natn. Acad. Sci. U.S.A.* **75,** 4853–4857 (1978).
17. Weaver, R. F. & Weissman, C. *Nucleic Acids Res.* **5,** 1175–1193 (1979).
18. Kayb, K. E., Warren, R. & Palmiter, R. D. *Cell* **29,** 99–108 (1982).
19. Brinster, R. L. *et al. Nature* **296,** 39–42 (1982).
20. Kingsbury, R. & McKnight, S. L. *Science* **217,** 316–324 (1982).
21. Larsen, A. & Weintraub, H. *Cell* **29,** 609–672 (1982).
22. Proudfoot, N. J. & Brownlee, G. G. *Nature* **263,** 211–214 (1976).
23. Calos, M. P. & Miller, J. H. *Cell* **20,** 579–595 (1980).
24. Hollis, F. G. *et al. Nature* **296,** 321–325 (1982).
25. Leuders, K., Leder, A., Leder, P. & Kuff, E. *Nature* **295,** 426–428 (1982).
26. Van Arsdell, S. W. *et al. Cell* **26,** 11–17 (1981).
27. Jagadeeswaran, P., Forget, B. G. & Weissman, S. M. *Cell* **26,** 141–142 (1982).
28. Nishioka, Y., Leder, A. & Leder, P. *Proc. natn. Acad. Sci. U.S.A.* **77,** 2806–2809 (1980).
29. Wilde, C. D. *et al. Nature* **297,** 83–84 (1982).
30. Shaul, Y., Kaminichik, J. & Aviv, H. *Eur. J. Biochem.* **116,** 461–466 (1981).
31. Perry, R. P. *et al. Proc. natn. Acad. Sci. U.S.A.* **77,** 1937–1941 (1980).
32. Hofer, E. & Darnel, J. E. *Cell* **23,** 585–593 (1981).
33. Bell, G., Karam, J. H. & Rutter, W. J. *Proc. natn. Acad. Sci. U.S.A.* **78,** 5759–5763 (1981).
34. Rigby, P. W. J. *et al. J. molec. Biol.* **113,** 237–251 (1977).
35. Wahl, G. M., Stern, M. & Stark, G. R. *Proc. natn. Acad. Sci. U.S.A.* **76,** 3683–3687 (1979).
36. Maxam, A. & Gilbert, W. *Meth. Enzym.* **65,** 499–559 (1980).
37. Sanger, F., Nicklen, S. & Coulson, A. R. *Proc. natn. Acad. Sci. U.S.A.* **74,** 5463–5468 (1979).
38. Goodman, H. M. *Meth. Enzym.* **65,** 63–64 (1980).
39. Heidecker, G., Messing, J. & Gronenborn, B. *Gene* **10,** 69–73 (1980).
40. O'Farrel, P. *Focus* **3,** 1–3 (1981).

LETTERS TO NATURE

A single quantum cannot be cloned

W. K. Wootters*

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130–33, California Institute of Technology, Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom

on an incoming photon with polarization state $|s\rangle$:

$$|A_0\rangle|s\rangle \rightarrow |A_s\rangle|ss\rangle \quad (1)$$

Here $|A_0\rangle$ is the 'ready' state of the apparatus, and $|A_s\rangle$ is its final state, which may or may not depend on the polarization of the original photon. The symbol $|ss\rangle$ refers to the state of the radiation field in which there are two photons each having the polarization $|s\rangle$. Let us suppose that such an amplification can in fact be accomplished for the vertical polarization $|\updownarrow\rangle$ and for the horizontal polarization $|\leftrightarrow\rangle$. That is,

$$|A_0\rangle|\updownarrow\rangle \rightarrow |A_{vert}\rangle|\updownarrow\updownarrow\rangle \quad (2)$$

and

$$|A_0\rangle|\leftrightarrow\rangle \rightarrow |A_{hor}\rangle|\leftrightarrow\leftrightarrow\rangle \quad (3)$$

No-cloning theorem II

We are looking for a mechanism that clones quantum states

$$U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle,$$

where U is a unitary dynamics.
Let us see why this is not possible. For the two basis states we have

$$U|0\rangle \otimes |0\rangle = |0\rangle \otimes |0\rangle,$$

$$U|1\rangle \otimes |0\rangle = |1\rangle \otimes |1\rangle.$$

Then, due to the linearity of quantum mechanics

$$U(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle).$$

However, we wanted

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Thus, a quantum state cannot be cloned.

Outline

Measurement problem

- Von Neumann postulated two types of quntum dynamics: unitary dynamics for closed systems and the dynamics under measurement, if the system is connected to a measuement device.

- We would expect that the dynamical description for closed systems can be used even for the case of a quantum measuement, if the measured particle and the measuring device are in one closed system.

- However, this is not the case. A unitary dynamics cannot describe the dynamics of the measured particle, the device (D) and the envoronment (E).

Measurement problem II

- We have the spin, the measurement device and the environment. The measurement dynamics should be

$$U|s = +\frac{1}{2}\rangle \otimes |D_0\rangle \otimes |E_0\rangle = |s = +\frac{1}{2}\rangle \otimes |D_{+1/2}\rangle \otimes |E'\rangle,$$

and

$$U|s = -\frac{1}{2}\rangle \otimes |D_0\rangle \otimes |E_0\rangle = |s = -\frac{1}{2}\rangle \otimes |D_{-1/2}\rangle \otimes |E''\rangle.$$

Measurement problem III

- If the spin is in a superposition of $s = +1/2$ and $s = -1/2$, then we get

$$U\frac{1}{\sqrt{2}}\left(|s=+\frac{1}{2}\rangle + |s=+-\frac{1}{2}\rangle\right)\otimes|D_0\rangle\otimes|E_0\rangle$$
$$= \frac{1}{\sqrt{2}}\left(|s=+\frac{1}{2}\rangle\otimes|D_{+1/2}\rangle\otimes|E'\rangle + |s=-\frac{1}{2}\rangle\otimes|D_{-1/2}\rangle\otimes|E''\rangle\right)$$

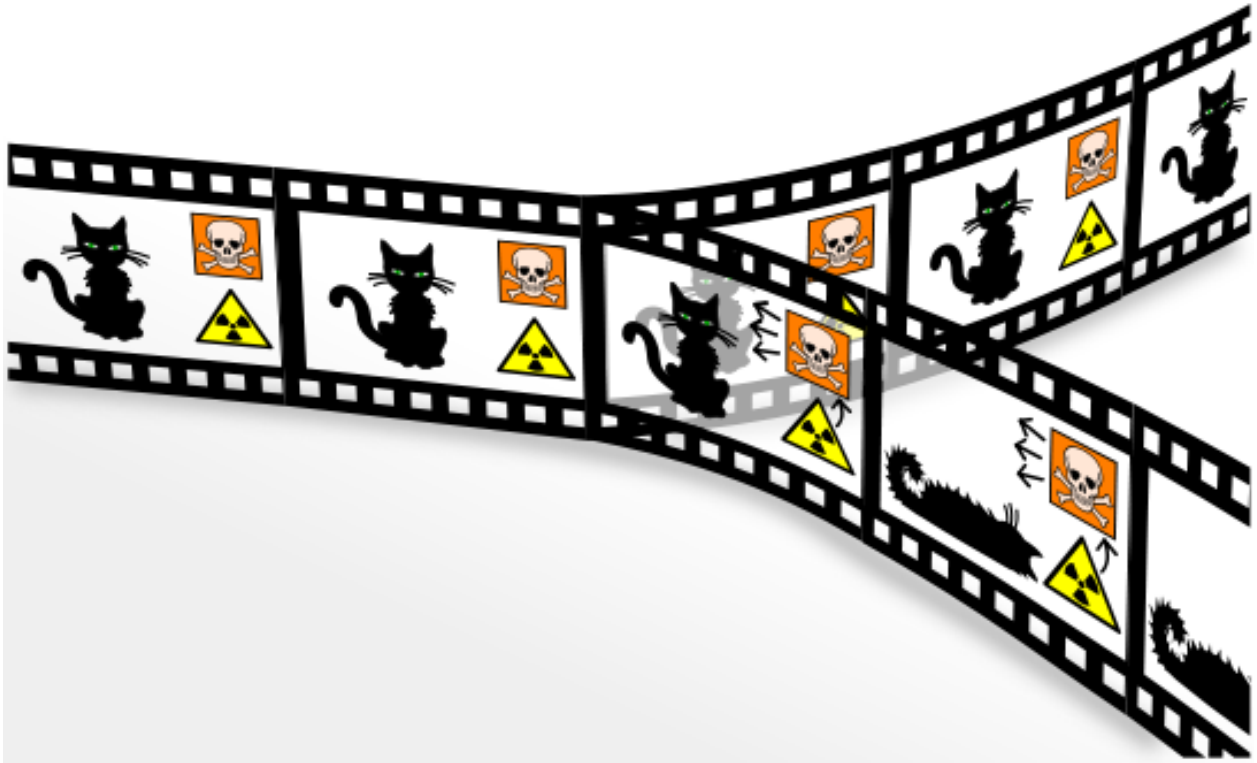
- We get a superposition of two states, rather than one or the other.

- This is a fundamental problem in quantum mechanics. A possible solution is the many-world interpretation.

Measurement problem IV

- A possible solution is the many-world interpretation.

- The idea of MWI originated in the Ph. D. thesis of Everett at Princeton in 1957, with the title "The Theory of the Universal Wavefunction", developed under his thesis advisor John Archibald Wheeler.



Measurement problem V

$$U\frac{1}{\sqrt{2}}\left(|s=+\frac{1}{2}\rangle+|s=+-\frac{1}{2}\rangle\right)\otimes|D_0\rangle\otimes|E_0\rangle\otimes|\mathrm{MIND}_0\rangle.$$

$$=\frac{1}{\sqrt{2}}\Big(|s=+\frac{1}{2}\rangle\otimes|D_{+1/2}\rangle\otimes|E'\rangle\otimes|\mathrm{MIND}_{+1/2}\rangle$$

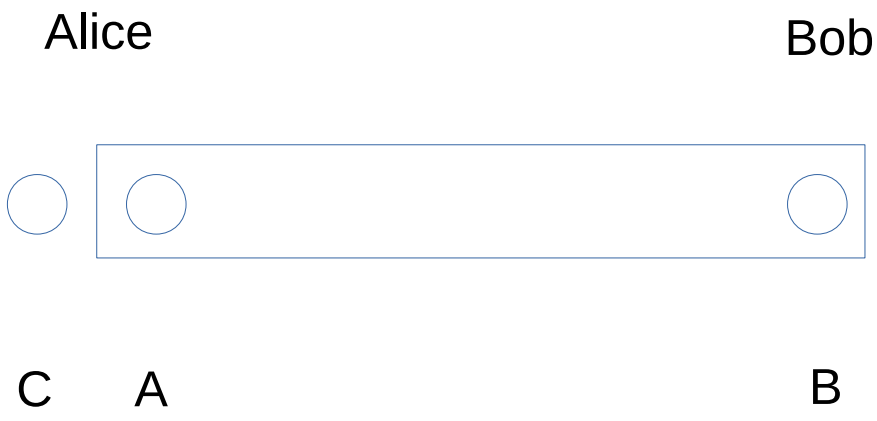
$$+|s=-\frac{1}{2}\rangle\otimes|D_{-1/2}\rangle\otimes|E''\rangle\otimes|\mathrm{MIND}_{-1/2}\rangle\Big)$$

Outline

Quantum teleportation

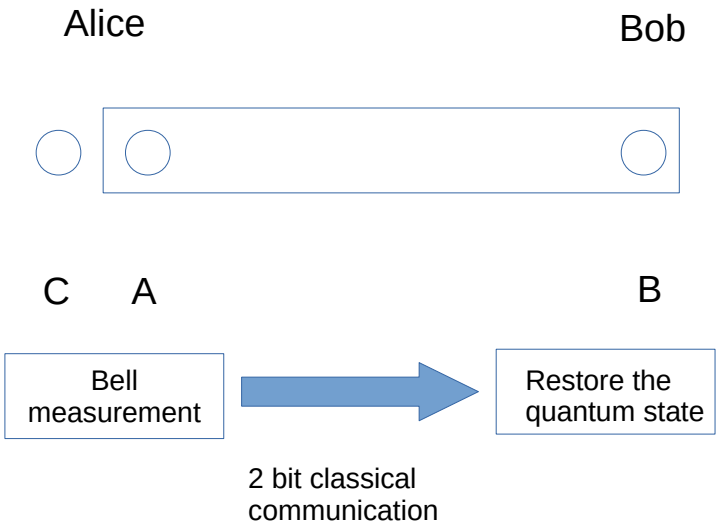
- A quantum state cannot be copied/cloned.
- But, it can be transferred from one particle to another one such that the state of the original particle is destroyed.

Quantum teleportation II



- A,B,C are spin-1/2 particles ≡ qubits.
- Alice wants to send the state of particle C to Bob.
- AB is in a singlet state $(|00\rangle + |11\rangle)/\sqrt{2}$.

Quantum teleportation II



- 1. Measurement of AC in the Bell basis
- 2. Alice sends the two-bit result to Bob
- 3. Depending on the result, Bob carries out $\varrho \rightarrow \sigma_l \varrho \sigma_l$, where $l \in \{0, x, y, z\}$.
- 4. The state of B is the same as the state of C was at the beginning.

Quantum teleportation III

- Initial state:

$$|\Psi\rangle_{AB} \otimes |\Psi\rangle_C = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \otimes (\alpha|0\rangle_C + \beta|1\rangle_C).$$

Alice and Bob want to teleport. Alice has two particles: A and C. She wants to teleport the C particle to the B particle of Bob. Particle A is helping the teleportation.

- Alice makes a measurement on particles A and C in the Bell basis. The Bell basis consists of the states:

$$|\Phi^{\pm}\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC} \pm |11\rangle_{AC})$$

and

$$|\Psi^{\pm}\rangle_{AC} = \frac{1}{\sqrt{2}}(|01\rangle_{AC} \pm |10\rangle_{AC}).$$

Quantum teleportation IV

- To see how this works, one can rewrite

$$
\begin{aligned}
&|\Psi\rangle_{AB} \otimes |\Psi\rangle_C \\
&\quad = \tfrac{1}{2}[|\Phi^+\rangle_{AC} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + |\Phi^-\rangle_{AC} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\
&\quad +|\Psi^+\rangle_{AC} \otimes (\beta|0\rangle_B + \alpha|1\rangle_B) + |\Psi^-\rangle_{AC} \otimes (\beta|0\rangle_B - \alpha|1\rangle_B)].
\end{aligned}
$$

- Hence, measurement of AC in the Bell basis results in one of the four possibilities above for particle B. Knowing the result of the measurement, we can obtain

$$(\alpha|0\rangle_B + \beta|1\rangle_B).$$

  Thus, we successfully teleported the state of particle C to particle B.

- Note that this does not make possible faster than light communication, since the result of the Bell measurement has to be sent classically.

Quantum teleportation V

- Experiment: Experimental quantum teleportation Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger, Nature 390, 575-579 (11 December 1997).

Quantum teleportation VI

- 143 km, employing an optical free-space link between the two Canary Islands of La Palma and Tenerife, Zeilinger's group, 2012.

(figure from www.iqoqi-vienna.at)

Outline

Imperfect cloning

- While perfect clonig is not possible, we can create imperfect clones.
- $1 \to N$ cloning means that from a single state we create N imperfect copies
- The larger the N, the worse is the quality of the copies.
- For instance, $1 \to \infty$ cloning means that we can make infinite number of copies. The procedure is simple.
  - We measure in the $\{|0\rangle, |1\rangle\}$ basis.
  - If the result is $|0\rangle$, then the output is $|0\rangle^{\otimes N}$.
  - If the result is $|1\rangle$, then the output is $|1\rangle^{\otimes N}$.

  Here, N can be arbitrarily large. Of course, the clones are not perfect. It works well for states close to $|0\rangle$ and $|1\rangle$, but works very bad for the state $(|0\rangle + |1\rangle)/\sqrt{2}$.

Outline

Classical cryptography

- One-time Pad: The safest cryptography. However, one needs to send the code book to the other person.

  Problem: What if someone else finds the codebook?

- Private key, public key: Encryption with the private key, decryption with the public key.

  Public key is known to everybody, private key is not known to everybody.

  Problem: what if the private key becomes known to outsiders?

Quantum cryptography: Coding in the $|0\rangle/|1\rangle$ or on the $(|0\rangle + |1\rangle)/(|0\rangle - |1\rangle)$ basis

- Let us code a classical bit $b \in 0, 1$ in a qubit. We can use the $0/1$ basis as before:

$$|q\rangle = (1 - b)|0\rangle + b|1\rangle.$$

- We can also use another basis, the $0 + 1/0 - 1$ basis:

$$|q'\rangle = (1 - b)\frac{|0\rangle + |1\rangle}{\sqrt{2}} + b\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

- If we do not know the basis, we cannot recover the bit b.

Quantum cryptography: Coding in the $|0\rangle/|1\rangle$ or on the $(|0\rangle + |1\rangle)/(|0\rangle - |1\rangle)$ basis II

- Let us assume we used the $0/1$ to code the bit

$$|q\rangle = (1 - b)|0\rangle + b|1\rangle.$$

- Then, a *single* measurement of

$$M = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|$$

will give the bit exactly.

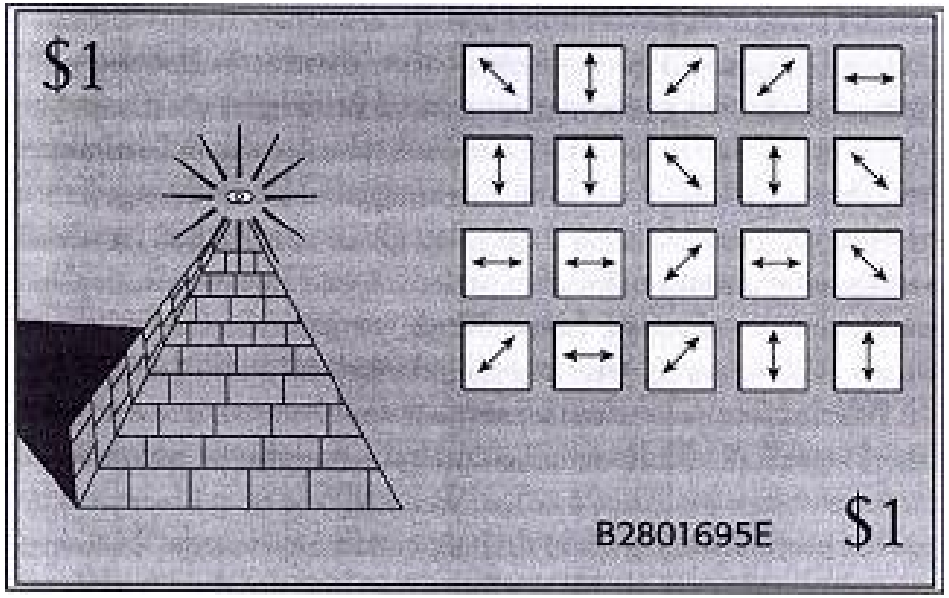
- If the bit was encoded in the $0 + 1/0 - 1$ basis, then we get with 50% probability 0, 50% probability 1, independently from b.

Quantum cryptography: Coding in the $|0\rangle/|1\rangle$ or on the $(|0\rangle + |1\rangle)/(|0\rangle - |1\rangle)$ basis III

- Note: if the quantum state could be copied, we could just copy the state many times. From many copies, we could guess, which basis was used.
- Thus, it is very important that the quantum states cannot be copied.

Quantum money

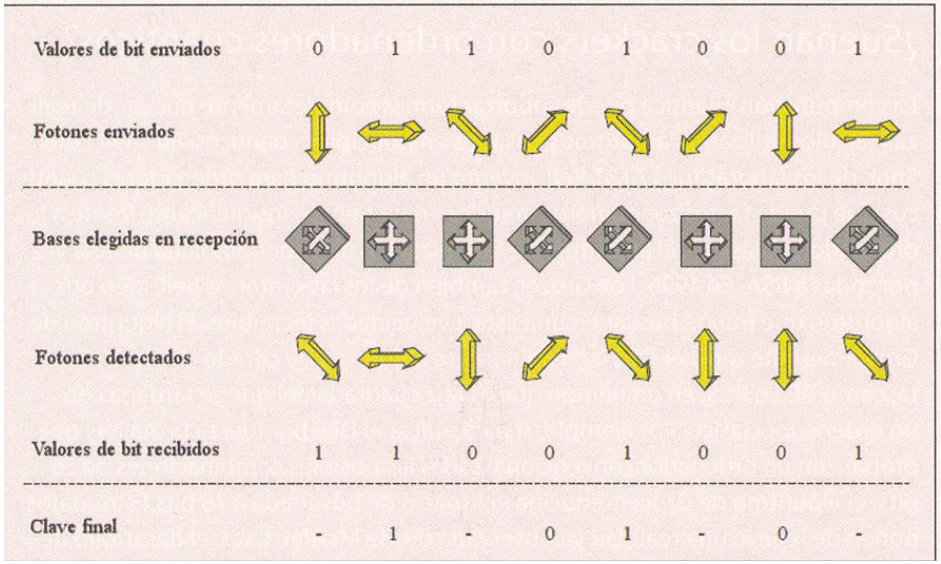
- S. Wiesner 1970, a graduate student at Columbia University, published in 1983.



- Every banknote has a code, a series of bits.
- The bits are encoded either in the 0/1 basis or in the 0+1/0-1 basis.
- The bank has the list of bases.
- The banknote cannot be copied.
- Its validity can be verified by the bank.

Quantum cryptography (BB84)

- Alice sends the secret message in qubits, randomly choosing the bases: 0/1 or (0+1)/(0-1).
- Bob receives the qubits and measures them in randomly chosen bases.
- Alice and Bob decides, using a public classical channel, for which qubits they used the same bases.



(figure from Wikipedia)

Quantum cryptography (BB84) II

Why is it safe?

- Without knowing in which basis the bit was encrypted, it is not possible to know the bit.
- The evesdropping (Eve) causes discrepancies between the qubits announced over the public channel. Errors of the channel also cause such discrepacies.

New notions

- Information reconciliation: Removing the errors by parity checks.
- Privacy amplification: Using the keys of Alice and Bob, creates a new shorter key about which Eve has very few information.

Ekert protocol (E91)

- Protocol based on entangled particles: Two-particle singlets

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

  are distributed between Alice and Bob.

- Remember that $\langle \sigma_l \otimes \sigma_l \rangle = -1$ for $l = x, y, z$.

- Both Alice and Bob measure in some basis, then they announce what they measured.

- Note: It can be proven that If the particles violate a Bell inequality, then there was really a singlet, not just shared random numbers.

Experiments

- In 2004, the world's first bank transfer using QKD was carried in Vienna, Austria. (Zeilinger group, Vienna)
- Quantum encryption technology provided by the Swiss company ID Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capital in the national election occurring on 21 October 2007. (Gisin group, Geneva)
- In 2013, Battelle Memorial Institute installed a QKD system built by ID Quantique between their main campus in Columbus, Ohio and their manufacturing facility in nearby Dublin.

Outline

Quantum error correction

- Classical error correction: we store 1 bit with odd number of bits (e.g., 3).
- If they are not the same, then majority vote matters. (This is the reason for the odd number. Even number of voters cannot always decide.)
- Quantum error correction: we store 1 qubit on several qubits.
- However, we must be careful. We cannot jut read out and correct. Reading out would destroy the quantum state.

Bit-flip code

- The bit flip code can correct a bit flip, as the name suggests. Thus, it helps to fight the error of the type

$$\epsilon(\varrho) = (1 - p)\varrho + p\sigma_x\varrho\sigma_x.$$

- It is based on using using redundancy:

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle.$$

  Thus, one qubit is now stored on three qubits.

Bit-flip code II

- The bit flip code can handle the case of 0 or 1 bit flip. Let us see in detail.
- First we need to detect which bit is flipped. This can be done by measuring $\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle$ and $\langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle$.

$$
\begin{aligned}
&\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle = +1, \quad \langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle = +1 \rightarrow \text{No error,} \\
&\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle = -1, \quad \langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle = +1 \rightarrow \text{Error on qubit 1,} \\
&\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle = +1, \quad \langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle = -1 \rightarrow \text{Error on qubit 3,} \\
&\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle = -1, \quad \langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle = -1 \rightarrow \text{Error on qubit 2.}
\end{aligned}
$$

- After detecting the error, we can correct it. We can just flip the qubit on which we found an error.
- We keep repeating these two steps to protect the qubit stored on three qubits.

Bit-flip code III

- Concrete example: let us assume a bit-flip error on the first qubit. Then, our state is

$$\alpha|100\rangle + \beta|011\rangle.$$

- For this state, we have

$$\langle \sigma_z^{(1)} \sigma_z^{(2)} \rangle = -1, \quad \langle \sigma_z^{(2)} \sigma_z^{(3)} \rangle = +1.$$

- We can correct it by flipping the first qubit, i.e.,

$$\varrho \to \sigma_x^{(1)} \varrho \sigma_x^{(1)}.$$

- Then, at the end we will have

$$\alpha|000\rangle + \beta|111\rangle.$$

Phase-flip code

- The phase flip code can correct a phase flip, as the name suggests. Thus, it helps to fight the error of the type

$$\epsilon(\varrho) = (1 - p)\varrho + p\sigma_z\varrho\sigma_z.$$

- The ideas are similar, no we have σ_z rather than σ_x.

Shore code

- It needs 9 qubits to store 1 qubit. It uses the econding

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle_S + \beta|1\rangle_S,$$

where

$$|0\rangle_S = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle),$$
$$|1\rangle_S = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle).$$

- The Shore code can correct any 1 bit error: 1 bit flip error, 1 phase flip error or both.

- Saying it differently: it can correct any unitary transformation happening on a single qubit.
  P. W. Shor, Phys. Rev. A 52, R2493(R) (1995).