Elizalde E.[1]

QUANTUM DELETION IS POSSIBLE VIA PARTIAL RANDOMIZATION PROCEDURE

IInstituto de Ciencias del Espacio (CSIC)

Institut d'Estudis Espacials de Catalunya (IEEC/CSIC), Edifici Nexus, Gran Capità 2-4, 08034 Barcelona, Spain

and

Departament ECM i IFAE, Facultat de Física, Universitat de Barcelona, Diagonal 647, 08028 Barcelona, Spain

The possibility of constructing a consistent quantum information theory and, what is more, of making practical use of its impressive potentialities (e.g., quantum cryptography [2], quantum teleportation [3,4], quantum computing [5], etc.) has attracted considerable attention in the Physics community during the last twenty years [5]. Almost as old is, however, the quantum "no-cloning theorem", due to Wooters and Zurek [6], and Dieks [7], which prevents the replication of unknown quantum states. In spite of this result - which does not allow, in particular, quantum information to be amplified accurately - and as it usually happens with no-go theorems, different alternatives to circumvent this strict prohibition have appeared in the literature [8]-[13]. They reestablish, in several different ways, a sort of consistency between the quantum theory and its possible real application as an information theory, which will obviously have the processes of copying, storing, and retrieving of information as some of its most basic tasks.

However, such consistency has been regained, at the very best, only at the level of arbitrarily good approximations in specific circumstances, while the no-cloning theorem still remains as a cornerstone in this field.

Not long ago Pati and Braunstein formulated what looks a complement to this theorem, namely a proposition that can be termed as a quantum "no-deleting theorem" [1]. In the same way as the no-cloning theorem told us that, contrary to what happens in classical information issues, the cloning of quantum information cannot be taken for granted, it also would now happen that deleting quantum information is in no way a trivial operation. One might argue, at first sight, that this result sounds quite old and well known (see Szilard [14] and Landauer [15]). In fact, replacing a sequence of 0's and 1's by a perfectly ordered state of 0's is thermodynamically costly, at the classical level. But the concept of deletion used in [1] has a more subtle formulation, which prevents the result from being trivial, and makes it much resemble the inverse of the usual cloning operation in [6,7], in the sense that it consists in the deletion of just one copy of a bit that is kept in several (at least two) copies. In other words, this sort of deletion can only start when one has two arbitrary, unknown but identical, bits (which can be termed "original" and "copy").

To be precise, and for the benefit of the reader, let us here recall the controlled not (or C-not) operation of classical information theory, which allows the deletion and copying of an arbitrary sequence of classical bits (see, for instance, Zurek [16]). Confronted with a pair of states, $|s_1\rangle|s_2\rangle$, C-not yields:

$$\begin{aligned} &|0\rangle|0\rangle \to |0\rangle|0\rangle, \quad |0\rangle|1\rangle \to |0\rangle|1\rangle, \\ &|1\rangle|0\rangle \to |1\rangle|1\rangle, \quad |1\rangle|1\rangle \to |1\rangle|0\rangle, \end{aligned} \tag{1}$$

that is, it replaces the second bit by its opposite whenever the first bit is $|1\rangle$, and leaves it untouched, when the first is $|0\rangle$. It is immediate that, classically, this operation clones the first component of a sequence of pairs of states (by imprinting it in the second component), when acting on a sequence of pairs where the second components are all 0's (blank sequence). Thus, for instance,

[1] Presently on leave at Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Ave, Cambridge, MA 02139. E-mail: elizalde@math.mit.edu elizalde@ieec.fcr.es

$$|0\rangle|0\rangle,|0\rangle|0\rangle,|1\rangle|0\rangle,|0\rangle|0\rangle,|1\rangle|0\rangle,|1\rangle|0\rangle,...$$
$$\rightarrow|0\rangle|0\rangle,|0\rangle|0\rangle,|1\rangle|1\rangle,|0\rangle|0\rangle,|1\rangle|1\rangle,|1\rangle|1\rangle,... \quad (2)$$

Moreover, this operation is reversible: when confronted with a sequence of identical pairs of states (such as for instance the second one in (2)), the C-not operation will turn out a sequence where the first components remain unchanged, while the second ones are all 0's. It is rather immediate (see e.g. [16]) that this simple operation fails altogether as a copying or deleting tool when applied to pairs of *quantum* bits (qubits). In terms of the states $|0\rangle$ and $|1\rangle$ a qubit will have the general form $|s\rangle=\alpha|0\rangle+\beta|1\rangle$ (α and β being complex numbers such that $|\alpha|^2+|\beta|^2=1$) and, the C-not operation acting, for instance, on the pair $|s\rangle|0\rangle$ yields an entangled state:

$$(\alpha|0\rangle+\beta|1\rangle)|0\rangle\rightarrow\alpha|0\rangle|0\rangle+\beta|1\rangle|1\rangle \quad (3)$$

(the C-not operation is linear). Put it in this way, it looks like there is no way out of the conclusion in the paper by Pati and Braunstein [1] - to which the reader is addressed for conventions, notation and additional references - that it is impossible to delete a copy of a quantum state, that comes in at least two copies, $|s\rangle|s\rangle$. Our main idea here will be to use a *different* form of the C-not operation together with an alternative notion of deletion, which depart from and extend in a way the definitions above.

We shall now fix our strategy. We give the term *deletion* a similar sense as in Ref. [1], as has been just described and which, in the words of Zurek [16], may be termed a narrow concept, but one that is being indeed most widely employed. This means, in what follows we shall just (as above) delete a single copy of some classical or quantum information piece that is kept in some device in at least two copies, so that at least one copy of the information remains in the end. But, as already advanced, our logical deleting/cloning operations will be *different* from the C-not operation. They will be called, respectively, *random deletion* and *cloning from random*, the first being a genuine R-choice. As it happens with the C-not operation, they also can operate both on classical and quantum systems. Being more specific, classical R-deletion will be defined as:

$$\begin{cases} |0\rangle\rightarrow R|0\rangle=\begin{cases}|0\rangle, \text{with } p=1/2,\\ |1\rangle, \text{with } q=1-p=1/2,\end{cases} \\ |1\rangle\rightarrow R|1\rangle=\begin{cases}|0\rangle, \text{with } p=1/2,\\ |1\rangle, \text{with } q=1-p=1/2,\end{cases}\end{cases} \quad (4)$$

where p and q denote probabilities and we have obviated the extra copies. That is, any state of the classical system is replaced by a reference state, which is not determined to be the $|0,0,0,...,0\rangle$ state, but rather one chosen each time at random, from a given set of pure states. Plainly, we would, for instance, delete the information contained in a Shakespearian play not by replacing all the characters with say *a*'s, but by replacing it with say[1] an equally long play written by a monkey sitting in front of a typewriter (that is, an arbitrary state in a thermal bath, rather than a chosen, standard, zero-state [17,18]). Of course, it will not always be the same play and the obvious question could be asked: how can we know *a priori*, on looking to a track or a whole disk, that it has undergone a deletion process, e.g., that it is empty and does not contain any information, if spins are not all aligned as in the usual $|0,0,0,...,0\rangle$ state? One of the possible answers: we know that the device is “empty” because it is labeled as such. For this we will just need an additional bit. To give a further visual picture of this last issue, let us mention that it freely corresponds to what we do at home when we decide that a video-tape or a CD are ready for re-use, after we have seen the movie (or are just fed up with the music) that we had previously recorded on them. In short, the new bit just mentioned should mimic this practice.

It should be noted that there is presently a great deal of confusion about the definition of “deletion” in the case of quantum information [19]. Classically, the convention seems to be that deletion is the reversible implementation of the erasure map: $|\psi\rangle\langle\psi|\otimes|\psi\rangle\langle\psi|\rightarrow|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|$ - where $|0\rangle$ is a standard initial pure state - with $|\psi\rangle$ restricted to the classical symbols from some alphabet (usually {0,1}). Whether the map is reversible or not is determined by its action on states with different symbols on the two systems. Quantumly, it is obvious that this is not possible [19]. A related (albeit different) definition of a (complete) randomization process, that has features in common with the one we have implemented in R-deletion, was introduced in [20], and has been used very recently in different situations [21,22,19] (although never in the context of the no-deletion principle). Ideally one would wish to delete without generating heat, but the amount produced in the present case is strictly bounded. In particular, it has been proven in [21] that the generation of n bits of entropy is sufficient and necessary in order to randomize arbitrary tensor products of n real amplitude qubits. Observe that this is just an upper bound, in our case, since the randomization here amounts only to a unit fraction of the total for the tensor product state. While this might be a technical problem at some point, it does not prevent the definition and use of our R-deletion operator as a working, alternative erasure method and a substitute for ordinary deletion. (Often the physical

[1] I apologize for the example

implementation of related procedures is not without difficulties).

One may observe that the purpose of deletion or erasure is to prepare the system for reuse, what requires a standard pure state, and that R-deletion (classically or quantumly) will defer this process to when the system is actually used again. And then, in the quantum case, the net effect of losing a copy of the state to the environment or the apparatus by the time the system is reused could still occur. Neither of these are true. In fact, the use of a set of pure states for the family of standard states and the introduction of a new operator, that we shall call R-cloning – and is classically an extension of the ordinary logical operation `inverse' to C-not – will take care of the first issue. As for the second, it turns out that the copy that is lost to the environment, by the time the system is reused, is going to be always an informationless, randomized remnant of the initial copy and *no* information will go to the reusing apparatus either. The new pure state to be prepared for reuse is got from the newly randomized state, which has lost any information on the initial one. Quantumly this corresponds to a diagonalization of the randomized density matrix, obtained in the first step of the procedure.

R-cloning has no essential difference with respect to the ordinary logical operation "inverse" to C-not in Eq. (1) [6,7] (see also the very clear description by Zurek [16]). By presenting pairwise the state to be cloned together with the random state (whatever it may be), R-cloning will replace the last with the first. There is nothing essentially distinct with the procedure in this case but, rigorously, it is a *different* operator, as we shall later explain.

In complete analogy with (4), quantum R-deletion starts by considering first a family of quantum states, labeled by a random parameter, σ. The parameter range can be finite or infinite, discrete or continuous. Actually, a family with only two members (as the states of a pair of horizontally and vertically polarized photons) would suffice to get an information loss in the way we are going to see. (For an example of a continuous, infinite family one may think, for instance, in the set of wave functions φ_σ given by Gaussian distributions $N(0,\sigma)$), with σ a positive real number that labels here the family of quantum states φ_σ). The quantum states in the family will be chosen to be pure states. Using the same notation of Pati and Braunstein [1], let us consider a couple of identical qubits (as two photons of arbitrary polarization) in some quantum state $|\psi\rangle$ together with an ancilla in a state $|A\rangle$, corresponding to the "ready" state of the deleting device [1]. The aim of the deleting device in the spirit of Ref. [1] was to replace one of the two copies of $|\psi\rangle$ with some standard, fixed state of a qubit $|\Sigma\rangle$. However, in the spirit of our approach to deletion (as described above, in the classical case), the R-deletion operator yields, in the quantum situation:

$$|\psi\rangle|\psi\rangle|A\rangle \to |\psi\rangle|\Sigma_{\sigma_1}\rangle|A_\psi\rangle, \qquad (5)$$

where now the standard state of a qubit ($|\Sigma\rangle$ in [1]) is replaced with one of the family of pure states, chosen at random, $|\Sigma_{\sigma_1}\rangle$.

When we now consider the action of R-deletion on a pair of horizontally and vertically polarized photons, respectively, we obtain

$$|H\rangle|H\rangle|A\rangle \to |H\rangle|\Sigma_{\sigma_2}\rangle|A_H\rangle, \qquad (6)$$

$$|V\rangle|V\rangle|A\rangle \to |V\rangle|\Sigma_{\sigma_3}\rangle|A_V\rangle, \qquad (7)$$

and odds are against having the same standard state for the deleted copy, namely $|\Sigma_\sigma\rangle$ (therefore the three different labels). By applying now R-deletion to an arbitrary input qubit $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ (with $|H\rangle$ and $|V\rangle$ forming a basis, and α and β being complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$), we obtain

$$|\psi\rangle|\psi\rangle|A\rangle \to \alpha^2|H\rangle|\Sigma_{\sigma_2}\rangle|A_H\rangle + \\ +\beta^2|V\rangle|\Sigma_{\sigma_3}\rangle|A_V\rangle + \sqrt{2}\alpha\beta|\Phi\rangle, \qquad (8)$$

where $|\Phi\rangle$ is the state obtained by R-deletion of the entangled state $(1/\sqrt{2})(|H\rangle|V\rangle + |V\rangle|H\rangle)|A\rangle$. But, whatever this state be in our actual realization of R-deletion, we do *not* recover now, from the linearity of Quantum Mechanics, the result in [1] that $|A_\psi\rangle = \alpha|A_H\rangle + \beta|A_V\rangle$. In fact, the strong implications that the linearity of QM has for the ordinary deletion process are *lost* when using the R-deletion transformation (the most obvious reason being the lack of a unique, standard $|\Sigma\rangle$ state to play with). Note that, in order to completely define the operation, we must still assign values to the rest of the basis of the tensor space, namely: $|H\rangle|V\rangle|A\rangle$ and $|V\rangle|H\rangle|A\rangle$ - what can be done freely – to close then the definition by extending *linearly* the operator to the whole of the tensor space of our quantum system [23]. This is in common with the ordinary definition of deletion, the only difference being thus the multiple choice of pure states to be assigned to the last component of the symmetrical elements of the basis for the tensor product. The generalization of this example to higher dimensional Hilbert spaces is straightforward.

In few words, the definition of R-deletion, although linear in essence, induces a weird behaviour when combined with the linear transformations of QM. As it involves randomly several "standard" states, it prevents the linearity of the relation $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ from being simply transfered to the ancilla state $|A_\psi\rangle$, what would eventually lead to a preservation of the whole information content and prevent its deletion [1]. In fact, R-deletion acting on $|\psi\rangle|\psi\rangle|A\rangle$ yields (5) which, on the other hand, if $|A_\psi\rangle$ were to be given by $|A_\psi\rangle = \alpha|A_H\rangle + \beta|A_V\rangle$, by taking into account (6) and (7), would yield the identity:

$$\begin{aligned}&\alpha^2|H\rangle|\Sigma_{\sigma_2}\rangle|A_H\rangle + \beta^2|V\rangle|\Sigma_{\sigma_3}\rangle|A_V\rangle \\ &+\sqrt{2}\alpha\beta|\Phi\rangle \\ &= \alpha^2|H\rangle|\Sigma_{\sigma_2}\rangle|A_H\rangle + \beta^2|V\rangle|\Sigma_{\sigma_3}\rangle|A_V\rangle \\ &+\alpha\beta(|H\rangle|\Sigma_{\sigma_1}\rangle|A_V\rangle + |V\rangle|\Sigma_{\sigma_1}\rangle|A_H\rangle),\end{aligned} \quad (9)$$

which is impossible to fulfill given the nature of R-deletion (in particular, the randomness of the σ_i, $i = 1,2,3$). Given that the states $|\Sigma_{\sigma_i}\rangle$, $i = 1,2,3$, are unrelated, it is now impossible to recover information about the state $|\psi\rangle$ from that of the ancilla remnant $|A_\psi\rangle$. In conclusion, we have actually managed to delete one copy of the information, in the end.

R-deletion does not seem to have much new to say on results about cloning. Notwithstanding that, if one considers cloning as (in some sense) an inverse procedure to deleting, we are here in the presence of two sensibly different deleting operations to which, in the classical case, the same cloning operation appears to be a common inverse. This is in fact not completely true. Strictly speaking, the cloning operation which is the inverse of R-deletion strictly *contains* the cloning operation that is the inverse of C-not. This is so, since the last cloning will always act on the standard blank state $|0,0,0,\ldots,0\rangle$ or $|\Sigma\rangle$ state only (as the second state, to be cloned). Only provided its definition were extended, allowing it to act on *any* state as second in the pair, would it coincide with the cloning which is the (classical) inverse of R-deletion.

To summarize, the new logical operation, R-deletion, that has been here introduced, is able to avoid the linear transference of the information kept in any arbitrary quantum state to the ancilla, as it inevitably happened with the ordinary deletion procedure [1], what prevented even the least amount of deletion of quantum information in that case. Our result provides support to a recent suggestion [19] that the non-deletion principle should preferably be called the erasure-only principle.

Acknowledgments

This investigation has been supported by DGICYT (Spain), by CIRIT (Generalitat de Catalunya), and by a USA-Spain Cooperation Agreement.

References

1. Pati A.K., Braunstein S.L. Impossibility of deleting an unknown quantum state // Nature. 2000. V. 404, P. 164-165.
2. Bennett C.H., Brassard G. The dawn of a new era for quantum cryptography: the experimental prototype is working! // SIGACT News. 1989. V. 20. P. 78-82.
3. Bennett C.H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels // Phys. Rev. Lett., 1993. V. 70. P. 1895-1899.
4. Bouwmeester D. et al. Experimental quantum teleportation // Nature. 1997. V. 390. P. 575-579.
5. Zeilinger A. Fundamentals of quantum information // Phys. World. 1998. (March). P. 35-40.
6. Wooters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. 1982. V. 299. P. 802-803.
7. Dieks D. Communication by EPR devices // Phys. Lett. 1982. V. A92. P. 271-272.
8. Bužek V., Hillery M.H. Quantum copying: beyond the no-cloning theorem // Phys. Rev. 1996. V. A 54. P. 1844-1852.
9. Bužek V., Braunstein S.L., Hillery M.H., Bruß D. Quantum copying: a network // Phys. Rev. 1997. V. A 56 P. 3446-3452.
10. Gisin N., Massar S. Optimal quantum cloning machines // Phys. Rev. Lett. 1997. V. 79, P. 2153-2156.
11. Duan L.M., Guo G.C. Probabilistic cloning and identification of linearly independent states // Phys. Rev. Lett. 1998. V. 80. P. 4999-5002.
12. Yuen H.P. Amplification of quantum states and noiseless photon amplifiers // Phys. Lett. 1986. V. A 113. P. 405-407.
13. Pati A.K. Quantum superposition of multiple clones and the novel cloning machine // Phys. Rev. Lett. 1999. V. 83. P. 2849-2852.
14. Szilard L. // Z. Phys.1929. V. 53, P. 840-856.
15. Landauer R. // IBM J. Res. Dev. 1961. V. 3. P. 183-191.
16. Zurek W.H. Schrödinger's sheep // Nature. 2000. V. 404. P. 130-131.
17. Elizalde E. Ten physical applications of spectral zeta functions. Springer, Berlin, 1995.
18. ElizaldeE., Odintsov S.D., Romeo A., Bytsenko A.A., Zerbini S. Zeta regularization techniques with applications. World Sci., Singapore, 1994.
19. Thanks are given to an anonimous referee for this crucial observation.
20. Braunstein S., Lo H.-K., Spiller T. Forgetting qubits is hot to do. 1999, unpublished.
21. Mosca M., Tapp A., de Wolf R. Private quantum channels and the cost of randomizing quantum information // quant-ph/0003101.
22. Boykin P.O., Roychowdhury V. Optimal encryption of quantum bits // quant-ph/0003059.
23. Kato T. Perturbation theory for linear operators. Springer, Berlin, 1980.