2. Xie, Q., Suarez-Lopez, P. and Gutierrez, C., *EMBO J.*, 1995, **14**, 4073–4082.
3. Ach, R. A., Durfee, T., Miller, A. B., Taranto, P., Hanley-Bowdoin, L., Zambryski, P. C. and Gruissem, W., *Mol. Cell. Biol.*, 1997, **17**, 5077–5086.
4. Weinberg, R. A., *Cell*, 1995, **81**, 323–330.
5. Sunter, G. and Bisaro, D. M., *Plant Cell*, 1992, **4**, 1321–1331.
6. Devereaux, J., *Nucleic Acids Res.*, 1984, **12**, 387–395.
7. Thomson, J. D., Higgins, D. G. and Gibson, T. J., *Nucleic Acids Res.*, 1994, **22**, 4673–4680.
8. Schuler, G. D., Altschul, S. F. and Lipman, D. J., *Protein Struct. Funct. Genet.*, 1991, **9**, 180–190.
9. Karlin, S. and Altschul, S. F., *Proc. Natl. Acad. Sci. USA*, 1990, **87**, 2264–2268.
10. Liu, L., Saunders, K., Thomas, C. L., Davies, J. W. and Stanley, J., *Virology*, 1999, **256**, 270–279.
11. Stanley, J. (pers. commun.)

ACKNOWLEDGEMENTS. We acknowledge the computational facilities of the Bioinformatics Centre at the School of Biotechnology and Prof. S. Krishnaswamy for helpful discussions. We thank the anonymous referee for suggesting that gaps could be avoided near the motif.

Received 19 August 2000; revised accepted 3 October 2000

S. SUJATHA[†,#]
R. USHA[‡,*]

[†]*Bioinformatics Centre and*
[‡]*Centre for Plant Molecular Biology,*
School of Biotechnology,
Madurai Kamaraj University,
Madurai 625 021, India
[#]*Present address:*
Molecular Biophysics Unit,
Indian Institute of Science,
Bangalore 560 012, India
**For correspondence.*
e-mail: usha@mrna.tn.nic.in

Is there really a 'quantum-no-deleting principle'?

A recent issue of *Nature*[1] contains a letter entitled 'Impossibility of deleting an unknown quantum state' by Pati and Braunstein (PB). The main contention of PB is that it is impossible to delete an 'unknown' quantum state. Further, they claim intrinsic security to files in a quantum computer as a corollary. What they have actually considered is uncopying, which means deleting against a copy. To claim intrinsic security, irreversible deleting must also be considered. We find that their claim is not true even for the (restricted) act of uncopying. To uncopy a state, it is necessary to have at least an additional copy. An uncopying device accepts two identical inputs – the original and a copy – and switches the copy to a standard state while keeping the original intact. This is strictly, called conditional uncopying.

Yuen[2] has defined copying of a quantum state $|\psi\rangle$ (of two-state system or a q-bit) using the transformation $\mathbf{T}_c$:

$$\mathbf{T}_c|\psi\rangle\,|\quad\rangle\,|A\rangle = |\psi\rangle\,|\psi\rangle\,|A_\psi\rangle,$$

where $|Ó\rangle$ is the standard state onto which the copy is made, and $|A\rangle$ and $|A_\psi\rangle$ are, respectively, the initial and final states of the copying device (or ancilla). PB define an uncopying transformation, $\mathbf{T}$, that is analogous to $\mathbf{T}_c$. The unitary operator $\mathbf{T}$, which represents a Schrödinger evolution, transforms a composite state $|\psi\rangle\,|\psi\rangle\,|A\rangle$ as

$$\mathbf{T}\,|\psi\rangle\,|\psi\rangle\,|A\rangle = |\psi\rangle\,|Ó\rangle\,|A_\psi\rangle. \qquad (1)$$

PB attempt to show that if $\mathbf{T}$ exists for the orthogonal basis states, then, linearity of quantum mechanics will prevent it from working for any superposed state. We show that PB's arguments are untenable, and hence, there is nothing like a 'quantum no-deleting principle'.

The operational part of PB's 'derivation' is very simple: They assume that the operator $\mathbf{T}$ exists for two orthogonal states $|H\rangle$ and $|V\rangle$. Thus

$$\mathbf{T}\,|H\rangle\,|H\rangle\,|A\rangle = |H\rangle\,|Ó\rangle\,|A_H\rangle, \qquad (2)$$

$$\mathbf{T}\,|V\rangle\,|V\rangle\,|A\rangle = |V\rangle\,|Ó\rangle\,|A_V\rangle, \qquad (3)$$

where $\mathbf{T}\,|A_H\rangle$ and $|A_V\rangle$ are the final states of the device. Now, the question is whether the same $\mathbf{T}$ can uncopy a state obtained as an arbitrary linear superposition, $|\psi\rangle = \alpha|H\rangle + \beta\,|V\rangle$, with $|\alpha^2| + |\beta^2| = 1$. (It may be noted that eqs (2) and (3) by themselves do not define $\mathbf{T}$ for the complete Hilbert space.) After a few simple steps, one finds that this is indeed possible with an appropriate $|A_\psi\rangle = (\alpha|A_H\rangle + \beta|A_V\rangle)$. Also the entangled state, $(|H\rangle\,|V\rangle + |V\rangle\,|H\rangle)\,|A\rangle$, transforms to $(|H\rangle\,|\Sigma\,\rangle\,|A_V\rangle + |V\rangle\,|\Sigma\rangle\,|A_H\rangle)$. Thus, the conclusion should have been that the sought after transformation is indeed possible – though it has not been constructed explicitly. However, at this point PB take a different view. They observe that $|A_H\rangle$ and $|A_V\rangle$ are orthogonal and $|A_\psi\rangle$ is a linear superposition of them, and then claim, '*The transformation is therefore not uncopying at all, but merely swapping onto a two-dimensional sub-space of the ancilla. It appears that there is no option but to move the information around without deleting it*' (emphasis is ours).

We state a consequence directly following from the definition, eq. (1). The orthogonality of $|A_H\rangle$ and $|A_V\rangle$ follows from unitary property of operator $\mathbf{T}$. For instance let $|A_{ø_1}\rangle$ and $|A_{ø_2}\rangle$ be the ancilla states corresponding to two states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively, in eq. (1). Then one may argue using unitarity of $\mathbf{T}$ and continuity of scalar product $\langle\psi_1\psi_2\rangle$ that orthogonality of $|\psi_1\rangle$ and $|\psi_2\rangle$ implies that of $|A_{ø_1}\rangle$ and $|A_{ø_2}\rangle$. (Since this is true for every unitary operator $\mathbf{T}$, the mere orthogonality of $|A_H\rangle$ and $|A_V\rangle$ cannot be the deciding factor as to whether $\mathbf{T}$ represents uncopying or swapping.)

Also, one might wonder why there is a sudden concern about swapping. (A swapping operator on the state $|\psi_1\rangle\,|\psi_2\rangle$ of two q-bits, transforms it to $|\psi_2\rangle\,|\psi_1\rangle$.) PB had advanced the following argument for not considering swapping as uncopying. According to them, 'The standard erasure of $|\psi\rangle$ does not use the original (i.e. first $|\psi\rangle$, and so is the case, if $\mathbf{T}$ swaps the copy (i.e. second) $|\psi\rangle$ and $|A\rangle$'. They thereby imply the equivalence of swapping and erasure. But, erasure is not reversible, while swapping of two states is a unitary operation which can be considered as legitimate uncopying (*albeit* unconditional).

Finally, while it is indeed true that $|A_H\rangle$ and $|A_V\rangle$ are orthogonal for swapping transformation; the converse is not true. For, consider a trivial case where the device is a single q-bit, and **T** be defined as

$$\mathbf{T}\,|H\rangle\,|H\rangle\,|\acute{O}\rangle = |H\rangle\,|\acute{O}\rangle\,|V\rangle, \tag{4}$$

$$\mathbf{T}\,|V\rangle\,|V\rangle\,|\acute{O}\rangle = |V\rangle\,|\acute{O}\rangle\,|H\rangle, \tag{5}$$

Here, $|A_H\rangle = |V\rangle$ and $|A_V\rangle = |H\rangle$ are orthogonal, but **T** *does not swap* the second and third states. We thus find that PB's argument (which uses the converse) to infer the 'quantum-no-deleting principle' is not correct. Explicit construction, of *conditional* quantum deleting machines, using a cascade of quantum logic gates is also possible[3]. In any case, finding $|A_\psi\rangle = \alpha|A_H\rangle + \beta|A_V\rangle$ should not be of any concern once the primary objective of uncopying $|\psi\rangle$, as defined in eq. (1), has been realized. (Rather one would worry about resetting the device in its final state $|A_\psi\rangle$ back to $|A\rangle$ for the next uncopying operation!)

PB remark that the quantum-no-deleting principle has been 'proved' for reversible as well as irreversible operations, in spite of their restricting to uncopying through Schrödinger evolution! They even forget that their concern was limited to only uncopying; nevertheless, PB proceed to make several claims: 'We emphasize that copying and deleting of information in a classical computer are inevitable operations, whereas similar operations cannot be realized perfectly in quantum computers. This may have potential applications in information processing because it provides intrinsic security to quantum files in a quantum computer. No one can obliterate a copy of an unknown file from a collection of several copies in a quantum computer,.... Nevertheless, nature seems to put another limitation on quantum information imposed by the linearity of quantum mechanics.' These high-sounding claims lie well outside the premise of the matter of their discussion.

In summary, reversible uncopying as well as irreversible deleting of a known or unknown quantum state should always be possible. More importantly, there is no case for a quantum no-deleting principle.

For an interested reader, a more detailed account of our analysis, which also touches upon quantum controlled-NOT operator[4] for copying and uncopying, is available in a preprint[5].

1. Pati, A. K. and Braunstein, S., *Nature*, 2000, **404**, 164.
2. Yuen, H. P., *Phys. Lett.*, 1986, **113A**, 405.
3. Bhagwat, K. V. *et al.*, *Phys. Rev. Lett.* (submitted).
4. Zurek, W. H., *Nature*, 2000, **404**, 130.
5. Bhagwat, K. V. *et al.*, A critique on 'quantum no-deleting principle', http://xxx.lanl.gov/abs/quant-ph/0005006.

Received 9 August 2000; accepted 6 October 2000

K. V. BHAGWAT*
D. C. KHANDEKAR
S. V. G. MENON
R. R. PURI
D. C. SAHNI

Technical Physics and Prototype Engineering Division,
Bhabha Atomic Research Centre,
Trombay,
Mumbai 400 085, India
**For correspondence.*
e-mail: kvb@apsara.barc.ernet.in