Indian J Pure Appl Math (2024) 55:893–903
https://doi.org/10.1007/s13226-024-00634-z

ORIGINAL RESEARCH

Copying quantum states

Hans Maassen · Burkhard Kümmerer

Received: 7 January 2024 / Accepted: 23 January 2024 / Published online: 5 July 2024
© The Indian National Science Academy 2024

Abstract The no-broadcasting theorem in quantum information says that a set of states on a quantum system admits a common broadcasting (copying) operation if and only if their density matrices belong to a commuting family. We discuss and prove this theorem, as well as the closely related "no-cloning theorem" in the context of quantum probability theory, i.e. in the category of (finite dimensional) C*-algebras with unital completely positive maps.

Keywords Quantum probability · Quantum information · No-cloning · Matrix algebras

1 Physical introduction

This issue is devoted to the memory of K.R. Parthasarathy. Apart from his important contributions to analysis and probability theory, he was a figurehead in the development of quantum probability theory and quantum stochastic calculus, e.g.: [5,6,13,14].
Quantum probability could be described as the study of C*-algebras and their completely positive maps, to be used as a tool to extend probability theory to quantum mechanics [7,8]. In this paper we apply this tool to discuss a fundamental theme of quantum information theory: the (im)possibility of copying quantum states.
The well-known "no-cloning principle", which states that an unknown (pure) quantum state can not be copied, delineates quantum systems from the systems studied in classical information theory, where unlimited copying is assumed possible.
A 'pure state cloner' or 'quantum amplifier' is an imaginary device that takes as input a quantum system in a state given by the vector ψ in some Hilbert space $\mathcal{H}$, and outputs $n \geq 2$ identical quantum systems in the joint state $\psi^{\otimes n}$. This possibility was suggested by [4], as a means to achieve superluminal communication. It was discussed in the 'Quantum Club' in Amsterdam by Dieks and Hoekzema, and the existence of such a device was soon ruled out. The map $\psi \mapsto \psi^{\otimes n}$ is not a linear map $\mathcal{H} \to \mathcal{H}^{\otimes n}$ [1]. Independently [15] derived the result, using the word "cloning" in this context for the first time.
The principle has been refined in several directions. First it was realized [16] that, in the presence of certain foreknowledge, copying of pure states *is* possible: when the state vector is known to belong to a given orthonormal basis, it can be cloned by measuring in that basis, and then preparing a pair, say, of independent systems which are

Communicated by Apoorva Khare, Rahul Roy.

H. Maassen (✉)
Mathematisch Instituut, Radboud Universiteit, Heyendaalseweg 135, 6525 AJ Nijmegen, Netherlands
E-mail: maassen@math.ru.nl

B. Kümmerer
Fachbereich Mathematik, Technische Universität Darmstadt, Schlossgartenstraße 7, 64289 Darmstadt, Germany
E-mail: kuemmerer@mathematik.tu-darmstadt.de

both in the pure state measured. A second refinement is the "no-broadcasting theorem", extending the principle to mixed states. It says that a mixed quantum state can be "broadcast" (copied) if and only if its density matrix is known to belong to a given commuting family. This extension required ingeneous proofs, one by [3] et al. using fidelities, and later one by [10] based on matrix algebras, which we shall treat here. Later a proof was given, based on convex structure only, by [2] et al.

In the standard textbook treatment, e.g. by [12], the no-cloning principle is presented in the orthonormal-set version mentioned above. Due to a slight oversimplification it is made to look very simple (cf. our remark after Theorem 8). The no-broadcasting version at first sight would seem an easy consequence: if the density matrices are diagonal in an orthonormal basis, then copying is possible; otherwise there is a positive probability for the states to be non-orthogonal, so that no-cloning forbids them to be copied.

To many researchers it therefore comes as a surprise that the proofs of the no-broadcasting theorem mentioned above are quite nontrivial.

In this paper we hope to shed some light on this matter. Briefly, it is the "only if"-direction which is difficult. It must be shown that no quantum operation, say some "quantum amplifier" [16], exists that can double up a state without having to perform any measurement. Moreover the argument using probabilities of pure states cannot be used, since the decomposition of a mixed state into pure ones is far from unique.

We hope to relieve the tension between the simplicity of "no-cloning" and the complexity of "no-broadcasting" proofs, existing in the literature, by giving a fair, more complicated, proof of the first (Theorem 8), and a hopefully somewhat more transparant proof of the second (Theorem 7).

We feel that the no-cloning principle is not just a consequence of the linearity of quantum mechanics, but rather of the non-commuting character of quantum observables, in the context of (completely) positive operations. In fact, classical systems can also be formulated in a (commutative) linear model, and copying them is well possible.

This paper is structured as follows: In Section 2 we define matrix algebras, states, and operations, and formulate basic general results concerning these.

In Section 3 we define the two notions of copying: cloning and broadcasting, showing that one is a pure state version of the other.

In Section 4 we prove "no universal copying" (Theorem 6), "no-broadcasting" (Theorem 7), and good old "no-cloning" (Theorem 8).

2 Mathematical preliminaries

2.1 Matrix algebras and states

By a *matrix algebra* $\mathcal{A}$ we shall mean a subspace of the linear space M_d of all complex $d \times d$-matrices for some $d \in \mathbb{N}$, which is closed under matrix multiplication $(a, b) \mapsto ab$ and the taking of adjoints $a \mapsto a^*$, and which contains a unit element $\mathbb{1}_{\mathcal{A}}$ (often the unit matrix in M_d).

A *state* φ on $\mathcal{A}$ is a linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ which maps positive definite matrices to positive numbers, and satisfies the normalization $\varphi(\mathbb{1}_{\mathcal{A}}) = 1$. The set of all states on $\mathcal{A}$ is denoted by $\mathcal{S}(\mathcal{A})$, its extremal points forming the set $\mathcal{E}(\mathcal{A})$ of *pure states*.

Example 1 (**Pure Quantum Systems**) The matrix algebra M_d has state space

$$\mathcal{S}(M_d) = \{\varphi : a \mapsto \operatorname{tr}(\rho a) |\ \rho \in M_d, \rho \geq 0, \operatorname{tr}(\rho) = 1\ \} .$$

The pure states are given by

$$\mathcal{E}(M_d) = \left\{ \varphi : a \mapsto \langle \psi, a\psi \rangle = \operatorname{tr}\big(|\psi\rangle\langle\psi|a\big) \,\middle|\, \psi \in \mathbb{C}^d, \|\psi\| = 1 \right\} .$$

Example 2 (**Finite Classical Systems**) Let $\mathcal{D}_d \subset M_d$ denote the space of diagonal $d \times d$-matrices. It has state space

$$\mathcal{S}(\mathcal{D}_d) = \left\{ \varphi : a \mapsto \sum_{i=1}^{d} \pi_i a_{ii} \,\middle|\, \pi_1, \pi_2, \ldots, \pi_d \geq 0, \sum_{i=1}^{d} \pi_i = 1 \right\} ,$$

of which the following are pure:

$$\mathcal{E}(\mathcal{D}_d) = \{\delta_1, \delta_2, \ldots, \delta_d\} , \quad \text{where} \quad \delta_i(a) := a_{ii} .$$

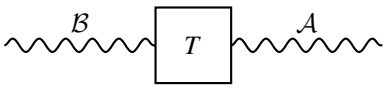
We note that $\mathcal{D}_d$ is isomorphic to the algebra $\mathcal{F} = \mathcal{F}(\Omega_d)$ of complex functions on the finite set $\Omega_d := \{1, \ldots, d\}$, if we let $f \in \mathcal{F}$ correspond to the diagonal matrix

$$\begin{pmatrix} f(1) & 0 & \ldots & 0 \\ 0 & f(2) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & f(d) \end{pmatrix} .$$

States on $\mathcal{F}(\Omega_d)$ are given by probability distributions $\pi : \Omega_d \to [0, 1]$, making Ω_d a probability space. By a slight abuse of notation we shall often identify $\mathcal{D}_d$ with $\mathcal{F}(\Omega_d)$. It is in this sense that the theory of (finite) probability spaces (Ω_d, π) generalizes to that of *quantum probability spaces* $(\mathcal{A}, \varphi)$ [9].

2.2 Completely positive maps

A linear map T from a matrix algebra $\mathcal{A}$ to a matrix algebra $\mathcal{B}$ is called *positive* if it maps positive definite matrices to positive definite matrices. It is called *completely positive* if for all $n \in \mathbb{N}$ the map $T \otimes \mathrm{Id}_{M_n} : \mathcal{A} \otimes M_n \to \mathcal{B} \otimes M_n$ is positive. T is called *unital* if $T(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$.
Matrix algebras with unital completely positive maps form a category, to be called **QP**.
By writing $T : \mathcal{A} \to \mathcal{B}$ we shall always mean that T is a completely positive map from $\mathcal{A}$ to $\mathcal{B}$, mapping $\mathbb{1}_{\mathcal{A}}$ to $\mathbb{1}_{\mathcal{B}}$. Such maps describe *quantum operations*: actions that can be performed on a quantum system. We illustrate the operation by the diagram



to be read from right to left. The map T takes observables in $\mathcal{A}$ to observables in $\mathcal{B}$, and is said to be the operation, seen "in the Heisenberg picture". The dual map $T^* : \mathcal{S}(\mathcal{B}) \to \mathcal{S}(\mathcal{A})$, defined by

$$T^*\varphi(a) := \varphi\big(T(a)\big) ,$$

will be considered as the operation, seen in the "Schrödinger picture", and is denoted by the same diagram, now read from left to right.

2.3 Physical interpretation

A matrix algebra $\mathcal{A} \subset M_d$ may be interpreted as the *observable algebra* of a system, represented on the Hilbert space $\mathcal{H} = \mathbb{C}^d$. Orthogonal projections $p = p^2 = p^* \in \mathcal{A}$ stand for observational statements or "events" concerning the system. If the system is in the state φ, then $\varphi(p) \in [0, 1]$ is interpreted as the *probability* for p to occur in an experiment.
In the classical case of Example 2, when $\mathcal{A}$ is commutative, then projections p are of the form 1_A for some $A \subset \Omega$. Then

$$\varphi(p) = \varphi(1_A) = \sum_{i \in \Omega} \pi_i 1_A(i) = \sum_{i \in A} \pi_i ,$$

i.e. the probability of the classical event A.
A unital completely positive map $T : \mathcal{A} \to \mathcal{B}$, in the Schrödinger picture $T^* : \mathcal{S}(\mathcal{B}) \to \mathcal{S}(\mathcal{A})$, is interpreted as an action that can be performed on a system with algebra $\mathcal{B}$ in a state φ, which yields a system with algebra $\mathcal{A}$ in the state $T^*\varphi$. Note that the time order is that of the Schrödinger picture.
In order to prove "no-go" theorems such as the "no-cloning" and the "no-broadcasting" theorems it is necessary to have universal restrictions on what can be done to a system. In the course of the 1960's and 1970's it was realized that the the category **QP** is a good framework for the handling of open quantum systems.
In the first place, the actions must be linear and positive, and this positivity must be robust against tensor products. Probabilities must add up to 1. These are restrictions on "what can be done" to quantum systems, and they delineate the unital completely positive maps. On the other hand, there seem to be no serious further restrictions: many unital completely positive maps are realized as quantum operations. For instance, the following actions are unital and completely positive.

1 *Free evolution of a closed system during some time*, described by automorphisms of the matrix algebra:

$$a \mapsto u^* a u \ ,$$

where $u^*u = uu^* = \mathbb{1}$.

2 *Embedding* the system into a larger whole. For finite pure quantum systems, i.e. with $\mathcal{A} = M_d$, this must be coupling to an ancilla (auxiliary system), according to Propositions 3.7 and 3.8 in [9]. In the Schödinger picture, this takes the form $\varphi \mapsto \varphi \otimes \vartheta$ for some state ϑ on the ancilla. In the Heisenberg picture it looks like

$$\mathrm{Id} \otimes \vartheta : \quad a \otimes b \mapsto \vartheta(b) a \ .$$

3 *Throwing away* or *ignoring* part of the system. In the Schrödinger picture this is represented by a *partial trace*. If ρ is the density matrix of a state on $M_d \otimes M_n$:

$$\rho \mapsto \mathrm{tr}_2(\rho) : a \mapsto \mathrm{tr}\big(\rho(a \otimes \mathbb{1}_{M_n})\big) \ .$$

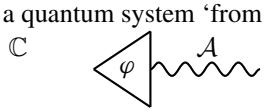
We prefer the simpler Heisenberg picture here:

$$a \mapsto a \otimes \mathbb{1}_{M_n} \ .$$

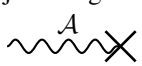
Combinations of these are again quantum operations. By a variation on Stinespring's Theorem (Proposition 1), all unital completely positive maps can be written as a coupling to an ancilla, then a free evolution, followed by a restriction to a subsystem:

$$T(a) = \mathrm{Id} \otimes \vartheta\big(u^*(a \otimes \mathbb{1})u\big) \ .$$

The Trivial *-Algebra. The matrix algebra $\mathbb{C} = M_1$ is interpreted as 'no system' or 'no information'. In diagrams we denote it by no line at all. A state, when viewed as an operation φ from a system $\mathcal{A}$ to 'no system' $\mathbb{C}$, or, in de Schrödinger picture by a *preparation* of a quantum system 'from nothing', will be denoted by the diagram



There exists a single (completely) positive unital map from $\mathbb{C}$ to $\mathcal{A}$, mapping $z \in \mathbb{C}$ to $z \cdot \mathbb{1} \in \mathcal{A}$. We interpret it physically as the operation of 'destroying' or just 'forgetting' the system $\mathcal{A}$. We denote it by the diagram



The mathematical fact that there exist many positive unital maps $\mathcal{A} \to \mathbb{C}$, but only one $\mathbb{C} \to \mathcal{A}$ corresponds neatly to the physical fact that there are many ways to prepare a system, but only one to destroy it.

2.4 Preliminary results

Let us start with a basic fact about completely positive maps, which we shall give without proof. Consult, for example: [12], [7], or [11]

Proposition 1 *(***Stinespring***) Let $T : M_m \to M_n$ be unital and completely positive. Then there exists $k \in \mathbb{N}$ and an isometry $v : \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^k$ such that for all $a \in M_m$:*

$$T(a) = v^*(a \otimes \mathbb{1}_{M_k})v \ .$$

Proposition 2 *(***Kadison-Schwarz***) Let T be a unital completely positive map $\mathcal{A} \to \mathcal{B}$. Then we have, in the positive definite ordering of $\mathcal{B}$:*

$$T(a^*a) \geq T(a)^* T(a) \ .$$

Proof Suppose that $\mathcal{A} \subset M_d$ and $\mathcal{B} \subset M_{d'}$. For $a \in \mathcal{A}$, the matrix $\begin{pmatrix} a^*a & a \\ a^* & \mathbb{1}_{\mathcal{A}} \end{pmatrix} \in M_d \otimes M_2$ is positive definite. It then follows from the complete positivity of T that for all $\psi \in \mathbb{C}^{d'}$

$$\langle \psi, \big(T(a^*a) - T(a)^*T(a)\big)\psi \rangle = \big(\psi, \ -T(a)\psi\big) \begin{pmatrix} T(a^*a) & T(a^*) \\ T(a) & T(\mathbb{1}_{\mathcal{A}}) \end{pmatrix} \begin{pmatrix} \psi \\ -T(a)\psi \end{pmatrix} \geq 0 \ .$$

□

Proposition 3 *(***Multiplicativity***) If $T(a^*a) = T(a)^*T(a)$ for some $a \in \mathcal{A}$, then we have for all $b \in \mathcal{A}$:*

$$T(ba) = T(b)T(a) \ . \tag{1}$$

We say that a is *multiplicative* for T.

Proof For every state φ on $\mathcal{A}$, define the semi-inner product $\langle \cdot, \cdot \rangle_{T,\varphi}$ on $\mathcal{A}$ by

$$\langle a, b \rangle_{T,\varphi} := \varphi\big(T(a^*b) - T(a)^*T(b)\big) \ .$$

By Proposition 2 we then have for all $a \in \mathcal{A}$ that $\langle a, a \rangle_{T,\varphi} \geq 0$. By the Cauchy-Schwarz inequality for $\langle \cdot, \cdot \rangle_{T,\varphi}$ we have

$$|\langle a, b \rangle_{T,\varphi}|^2 \leq |\langle a, a \rangle_{T,\varphi}| \cdot |\langle b, b \rangle_{T,\varphi}| \ .$$

Hence, if $\langle a, a \rangle_{T,\varphi} = \varphi\big((Ta^*a) - T(a)^*T(a)\big) = 0$, then for all $b \in \mathcal{A}$:

$$\varphi\big((T(ba) - T(b)T(a)\big) = \langle b^*, a \rangle_{T,\varphi} = 0 \ .$$

And since this holds for all states φ on $\mathcal{A}$, we may conclude that (1) holds. □

Definition 1 A set S of states on a matrix algebra $\mathcal{A}$ is called *faithful* if for all nonnegative definite $a \in \mathcal{A}$:

$$\Big(\forall_{\varphi \in S} : \varphi(a) = 0\Big) \quad \Longrightarrow \quad a = 0 \ . \tag{2}$$

We say that an observable $a \in \mathcal{A}$ is *invariant* under $T : \mathcal{A} \to \mathcal{A}$ if $T(a) = a$. A state φ on $\mathcal{A}$ is *invariant* under T if $T^*\varphi = \varphi \circ T = \varphi$.

Proposition 4 *(***Fixed Point Algebra***) If $T : \mathcal{A} \to \mathcal{A}$ has a faithful set $S \subset \mathcal{S}(\mathcal{A})$ of invariant states, then the set $\mathcal{I}(T)$ of all invariant observables forms a matrix subalgebra of $\mathcal{A}$.*

Proof If $a \in \mathcal{I}(T)$, then also $a^* \in \mathcal{I}(T)$, since $T(a^*) = T(a)^*$. Moreover for all $\varphi \in S$ we have

$$0 = \varphi \circ T(a^*a) - \varphi(a^*a) = \varphi\big(T(a^*a) - T(a)^*T(a)\big) \ .$$

By Kadison-Schwarz (Proposition 2) $T(a^*a) - a^*a = T(a^*a) - T(a)^*T(a) \geq 0$, hence by faithfulness (2) it follows that $T(a^*a) = a^*a$, i.e., $a^*a \in \mathcal{I}(M)$. Replacing a by $a + b$, where a and b are both in $\mathcal{I}(T)$, and then by $a + ib$, and subtracting (i.e. by "polarization") we obtain that $T(a^*b) = a^*b$: if a and b are invariant, then so is a^*b. □

3 Definitions of copying

A copying operation should map a system with observable algebra $\mathcal{A}$ in a state φ to a pair of systems, described by the algebra $\mathcal{A} \otimes \mathcal{A}$, each in the state φ. Hence in the Schrödinger picture we want our copier to be of the form

$$C^* : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{A}) \otimes \mathcal{S}(\mathcal{A}) \ .$$

For the Heisenberg picture this means

$$C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A} \ .$$

Definition 2 (**Cloning**) We say that $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ *clones* the pure state φ on $\mathcal{A}$ if

$$C^*\varphi = \varphi \otimes \varphi \ .$$

We only consider cloners for *pure* states φ. The reason for this restriction is explained easiest by considering the classical algebra $\mathcal{F}(\Omega)$ for the finite set $\Omega = \{A, B\}$, where A and B may be documents. Suppose we feed A into the device with probability $\frac{1}{3}$ and B with probability $\frac{2}{3}$, and suppose that it, with this probability distribution $(\frac{1}{3}, \frac{2}{3})$ as input, yields as output the product distribution $(\frac{1}{9}, \frac{2}{9}, \frac{2}{9}, \frac{4}{9})$ on $\{(A, A), (A, B), (B, A), (B, B)\}$. Then the copies are *independent*, and not *identical*. This is not what a copying machine is supposed to do: it should map $(\frac{1}{3}, \frac{2}{3})$ to $(\frac{1}{3}, 0, 0, \frac{2}{3})$, producing the pair (A, A) with probability $\frac{1}{3}$ and (B, B) with probability $\frac{2}{3}$.
In this example only for the extremal distributions δ_A and δ_B is this behaviour reasonable:

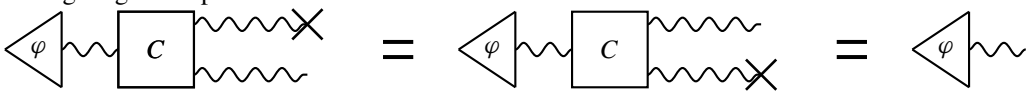
$$\delta_A \mapsto \delta_A \otimes \delta_A \quad \text{and} \quad \delta_B \mapsto \delta_B \otimes \delta_B \ . \tag{3}$$

Instead of Definition 2, for mixed states [3] et al. proposed the following weaker definition, asking the marginals of the output distribution to reflect the input state without requiring independence.

Definition 3 (**Broadcasting**) The map $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ is said to *broadcast* the state φ on $\mathcal{A}$ if for all $a \in \mathcal{A}$:

$$\varphi \circ C(a \otimes \mathbb{1}_{\mathcal{A}}) = \varphi \circ C(\mathbb{1}_{\mathcal{A}} \otimes a) = \varphi(a) \ . \tag{4}$$

The following diagram expresses this situation:



Broadcasting the state φ, and throwing away (or ignoring) one of the copies, leaves us with a system in the state φ.
Henceforth we shall use the word "copying" in the nontechnical sense, and the words "cloning" and "broadcasting" in the sense of definitions 2 and 3 above.
Actually, the term "cloning" is superfluous, as the following lemma shows.

Lemma 5 *Let φ be a pure state on $\mathcal{A}$. Then $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ clones φ if and only if it broadcasts φ.*

Proof Clearly, if $C^*\varphi = \varphi \otimes \varphi$, then both marginals are equal to φ:

$$\varphi \circ C(a \otimes \mathbb{1}) = C^*\varphi(a \otimes \mathbb{1}) = \varphi \otimes \varphi(a \otimes \mathbb{1}) = \varphi(a)\varphi(\mathbb{1}) = \varphi(a) \ ,$$

and the same for $\mathbb{1} \otimes a$.
Conversely, suppose that the right marginal of $C^*\varphi$ is equal to φ itself, as in (4). Let $p \in \mathcal{A}$ be a projection. Then we can write φ as a sum of two positive functionals:

$$\varphi(a) = C^*\varphi(\mathbb{1} \otimes a) = C^*\varphi(p \otimes a) + C^*((\mathbb{1} - p) \otimes a) \ .$$

Since φ is pure, both must be multiples of φ, in particular $C^*\varphi(p \otimes a) = \lambda\varphi(a)$ for some $\lambda \geq 0$. Putting $a = \mathbb{1}$ we find that $\lambda = C^*\varphi(p \otimes \mathbb{1})$, and since the left marginal also equals φ, we have $\lambda = \varphi(p)$. Thus we find

$$C^*\varphi(p \otimes a) = \varphi(p)\varphi(a) \ .$$

As the projections p span the algebra $\mathcal{A}$, we conclude that $C^*\varphi = \varphi \otimes \varphi$. □

4 Results

4.1 Copying all states

Let us first determine under what circumstances a single quantum operation can copy *all states* on a system. The answer is: only if the system is classical:

Theorem 6 *(***No Universal Copier***) For a matrix algebra $\mathcal{A}$ and a unital completely positive map $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ the following are equivalent:*

(a) *C clones all pure states on $\mathcal{A}$;*
(b) *C broadcasts all states on $\mathcal{A}$;*
(c) *$\mathcal{A}$ is commutative and for all $a, b \in \mathcal{A}$ we have $C(a \otimes b) = ab$.*

Proof (a) $\Longrightarrow$ (b): As noted in Lemma 5, the cloner C is also a copier for all pure states: $\varphi \circ C(a \otimes \mathbb{1}) = \varphi \circ C(\mathbb{1} \otimes a) = \varphi(a)$. Since any state is a convex combination of pure states, this equality extends to all states φ on $\mathcal{A}$.
(b) $\Longrightarrow$ (c): As the broadcasting equation (4) holds for all φ on $\mathcal{A}$, we have, for all $a \in \mathcal{A}$:

$$C(a \otimes \mathbb{1}) = C(\mathbb{1} \otimes a) = a \ .$$

It follows that

$$C\big((a \otimes \mathbb{1})^*(a \otimes \mathbb{1})\big) = C(a^*a \otimes \mathbb{1}) = a^*a = C(a \otimes \mathbb{1})^* C(a \otimes \mathbb{1}) \ ;$$

so $a \otimes \mathbb{1}$ is multiplicative for C by Proposition 3. In the same way we see that for all $b \in \mathcal{A}$ the matrix $\mathbb{1} \otimes b$ is multiplicative. Therefore

$$\begin{aligned} ab &= C(a \otimes \mathbb{1})C(\mathbb{1} \otimes b) = C\big((a \otimes \mathbb{1})(\mathbb{1} \otimes b)\big) = C(a \otimes b) \\ &= C\big((\mathbb{1} \otimes b)(a \otimes \mathbb{1})\big) = C(\mathbb{1} \otimes b)C(a \otimes \mathbb{1}) = ba \ . \end{aligned}$$

(c) $\Longrightarrow$ (a): We may identify $\mathcal{A}$ with the algebra $\mathcal{F}(\Omega)$ of all functions on some finite set Ω (cf. Example 2). The pure states on this algebra are the point evaluations $\delta_i : f \mapsto f(i)$, with $i \in \Omega$. These satisfy, for $f, g \in \mathcal{F}(\Omega)$:

$$\begin{aligned} (C^*\delta_i)(f \otimes g) &= \delta_i \circ C(f \otimes g) = \delta_i(f \cdot g) = (f \cdot g)(i) \\ &= f(i)g(i) = \delta_i(f)\delta_i(g) = (\delta_i \otimes \delta_i)(f \otimes g) \ . \end{aligned}$$

I.e.: $C^*\delta_i = \delta_i \otimes \delta_i$ for the pure states δ_i, $i \in \Omega$. □

4.2 Classical copiers

Condition (c) above says that our system is classical, and that C takes the form of the product operation. Although this formulation is mathematically neat, physically it may look puzzling. The following equivalent form may be more transparant. If $\mathcal{A} = \mathcal{F}(\Omega)$, then the map $C : f \otimes g \to f \cdot g$ extends linearly to all $h \in \mathcal{F}(\Omega) \otimes \mathcal{F}(\Omega) = \mathcal{F}(\Omega \times \Omega)$ as

$$C(h)(i) = h(i, i) \ .$$

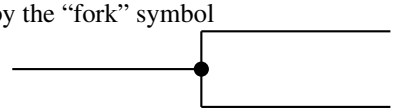
This is the algebraic form of the natural copying operation on Ω:

$$i \mapsto (i, i) \ ,$$

which takes a system in the 'point state' i to two systems, both in that point state. In the Schrödinger picture the classical copier takes the form

$$C^*\pi = \pi \circ C = \sum_{i \in \Omega} \pi_i \cdot \delta_i \otimes \delta_i \ . \tag{5}$$

C^* puts the probability distribution π on Ω onto the diagonal of $\Omega \times \Omega$. A distribution π on the points $i \in \Omega$ is mapped to the same distribution on the pairs (i, i). (See our remarks after Definition 3.) We shall denote the copier of an abelian matrix algebra by the "fork" symbol



Here, all the horizontal straight lines stand for the commutative matrix algebra $\mathcal{F}(\Omega)$.
Theorem 6 makes it clear that classical copiers do exist.
They do their work by measuring the point-state $i \in \Omega$, and producing a pair (i, i) of them. (Cf. (3)). We note that a copying machine does not *measure* the probability distribution in order to copy it. A classical broadcaster does not distinguish between the probability distributions $(\frac{1}{3}, \frac{2}{3})$ and $(\frac{1}{2}, \frac{1}{2})$ on $\Omega := \{A, B\}$ in order to faithfully reproduce the distribution on the copies. The probability distribution takes care of itself.
This phenomenon makes broadcasting very different from mere cloning.

4.3 Copying from a given set of states

Theorem 7 *(***No-Broadcasting Theorem***) Let S be a set of states on a matrix algebra $\mathcal{A} \subset M_d$. Then the following are equivalent.*

(a) *The states in S have a common broadcaster $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$;*
(b) *All states in S are convex combinations of certain states $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$ on $\mathcal{A}$, which have pairwise orthogonal support projections $p_1, p_2, \ldots, p_k \in \mathcal{A}$.*
(c) *The density matrices of the states in S commute pairwise.*

The hard part of the proof is the implication (a)$\Longrightarrow$(b): it basically says that the only way to broadcast a set of states is to perform a von Neumann measurement on the system using certain projections $p_1, p_2, \ldots, p_k$, and on the basis of the outcome to decide which state to output in duplicate.

Proof (b)$\Longrightarrow$(c): Since the states $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$ have orthogonal supports, their density matrices commute, and so do convex combinations of these.

(c)$\Longrightarrow$(b): Let $\mathcal{C} \subset \mathcal{A}$ denote the commutative matrix algebra generated by the density matrices $\{\rho_\varphi |\ \varphi \in S\ \}$. After diagonalization of this algebra we divide the diagonal into (say k) blocks, inside which all the ρ_φ are constant. Thus we obtain a division of $\mathbb{1}_{\mathcal{A}}$ into disjoint projections $p_1, p_2, \ldots, p_k$. By normalization we define states $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$ with supports $p_1, p_2, \ldots, p_k$:

$$\vartheta_i(a) := \frac{\mathrm{tr}(p_i a)}{\mathrm{tr}\, p_i} \ .$$

Note that $\vartheta_i(p_j) = \delta_{ij}$. Every state $\varphi \in S$ is a convex combination of these states: $\varphi = \sum_{i=1}^k \lambda_i^\varphi \vartheta_i$. In particular $\varphi(p_j) = \sum_{i=1}^k \lambda_i^\varphi \vartheta_i(p_j) = \lambda_j^\varphi$, so that

$$\varphi = \sum_{i=1}^k \varphi(p_i)\vartheta_i \ , \tag{6}$$

with $\sum_{i=1}^k \varphi(p_i) = \varphi(\mathbb{1}_{\mathcal{A}}) = 1$.

(b)$\Longrightarrow$(a): We may assume (6). Define C in the Schrödinger picture by

$$C^* : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{A}) \otimes \mathcal{S}(\mathcal{A}) : \quad \varphi \mapsto \sum_{j=1}^k \varphi(p_j)\vartheta_j \otimes \vartheta_j \ .$$

Then C is a broadcaster of S, since for all $\varphi \in S$, by (6),

$$(C^*\varphi)(a \otimes \mathbb{1}) = (C^*\varphi)(\mathbb{1} \otimes a) = \sum_{j=1}^k \varphi(p_j)\vartheta_j(a) = \varphi(a) \ .$$

See Definition 3; note that in the Heisenberg picture

$$C(a \otimes b) = \sum_{i=1}^k \vartheta_i(a)\vartheta_i(b)p_i \ . \tag{7}$$

(a)$\Longrightarrow$(b): Suppose that a broadcaster $C : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ for all the states $\varphi \in S$ is given. We may assume that C is symmetric, otherwise we continue the discussion with the symmetrized broadcaster $a \otimes b \mapsto \frac{1}{2}\big(C(a \otimes b) + C(b \otimes a)\big)$.

Let s be the support of S, i.e., the smallest projection in $\mathcal{A}$ such that $\varphi(s) = 1$ for all $\varphi \in S$. Let $\mathcal{A}_s := s\mathcal{A}s$, a matrix algebra with unit $\mathbb{1}_{\mathcal{A}_s} = s$. By S_s we shall denote the set of restrictions of the states $\varphi \in S$ to $\mathcal{A}_s$.

Define $C_s : \mathcal{A}_s \otimes \mathcal{A}_s \to \mathcal{A}_s$ by:

$$C_s(a \otimes b) := sC(a \otimes b)s \ .$$

Take $\psi \in S_s$, say $\psi(a) = \varphi(a)$ for $a \in \mathcal{A}_s$, and some $\varphi \in S$. Since $\varphi(s) = 1$, the projection s is multiplicative for φ, and since $\varphi \circ C(\mathbb{1} \otimes s) = 1$, the matrix $\mathbb{1} \otimes s$ is multiplicative for $\varphi \circ C$. Therefore, still for all $a \in \mathcal{A}_s$

$$\begin{aligned}\psi \circ C_s(a \otimes \mathbb{1}_{\mathcal{A}_s}) &= \varphi\big(sC(a \otimes s)s\big) = \varphi(s)\varphi\Big(C\big((a \otimes \mathbb{1})(\mathbb{1} \otimes s)\big)\Big)\varphi(s) \\ &= \varphi \circ C(a \otimes \mathbb{1}) \cdot \varphi \circ C(\mathbb{1} \otimes s) = \varphi(a)\varphi(s) = \varphi(a) = \psi(a) \ .\end{aligned}$$

I.e., C_s broadcasts all states in S_s.
Consider the marginal operation $M : \mathcal{A}_s \to \mathcal{A}_s : a \mapsto C_s(a \otimes \mathbb{1}_{\mathcal{A}_s})$. By assumption, $\psi \circ M = \psi$ for all $\psi \in S_s$. As S has support s, this set is faithful for M. By Proposition 4 the invariant set $\mathcal{I}(M)$ is a matrix subalgebra of $\mathcal{A}_s$.
It follows that, for $a \in \mathcal{I}(M)$ we have $a^*a \in \mathcal{I}(M)$, hence

$$C_s\big((a \otimes s)^*(a \otimes s)\big) = C_s(a^*a \otimes s) = M(a^*a) = a^*a = C_s(a \otimes s)^*C_s(a \otimes s) \ ,$$

so $a \otimes s$ is multiplicative for C_s. Therefore, for all $a, b \in \mathcal{I}(M)$,

$$C_s(a \otimes b) = C_s(a \otimes \mathbb{1}_{\mathcal{A}_s}) \cdot C_s(\mathbb{1}_{\mathcal{A}_s} \otimes b) = ab \in \mathcal{I}(M). \tag{8}$$

We conclude that C_s in restriction to $\mathcal{I}(M) \otimes \mathcal{I}(M)$ maps to $\mathcal{I}(M)$ itself. By definition of $\mathcal{I}(M)$ the map C_s broadcasts all states on $\mathcal{I}(M)$. But by Theorem 6 this is only possible if $\mathcal{I}(M)$ is commutative!
Let $p_1, p_2, \ldots, p_k$ be the minimal projections in the commutative matrix algebra $\mathcal{I}(M)$. Consider the ergodic projection $E : \mathcal{A}_s \to \mathcal{I}(M)$:

$$E := \lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} M^j \ .$$

Since every element of $\mathcal{I}(M)$ is a linear combination of the projections $p_1, p_2, \ldots, p_k$, we may write, for $a \in \mathcal{A}_s$,

$$E(a) = \sum_{i=1}^{k} \alpha_i(a) p_i \ . \tag{9}$$

for some functionals $\alpha_1, \alpha_2, \ldots, \alpha_k : \mathcal{A}_s \to \mathbb{C}$. As E is positive, so are the α_i, and as $E(\mathbb{1}_{A_s}) = \mathbb{1}_{A_s}$, we find that $\alpha_i(\mathbb{1}_{\mathcal{A}_s}) = 1$. Define $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$ by $\vartheta_i(a) := \alpha_i(sas)$.
We now have for $j = 1, \ldots, k$:

$$p_j = E(p_j) = \sum_{i=1}^{k} \vartheta_i(p_j) p_i \ ,$$

and therefore $\vartheta_i(p_j) = \delta_{ij}$, i.e., the states have disjoint supports. Moreover, for all $a \in \mathcal{A}$ and $\varphi \in S$ we have by (9):

$$\varphi(a) = \varphi(sas) = \varphi \circ E(sas) = \sum_{i=1}^{k} \alpha_i(sas)\varphi(p_i) = \sum_{i=1}^{k} \varphi(p_i)\vartheta_i(a) \ .$$

Since $\sum_{i=1}^{k} p_i = s$ and $\varphi(s) = 1$, the states $\varphi \in S$ are convex combinations of the states $\vartheta_1, \vartheta_2, \ldots, \vartheta_k$. □

Discussion of the No-Broadcasting Theorem. The von Neumann measurement using the projections $p_1, p_2, \ldots, p_k$ can be seen as a quantum operation from a quantum system to a classical probability space given in the Heisenberg picture by

$$N : \mathcal{F}(\Omega_k) \to \mathcal{A} : \quad f \mapsto \sum_{i=1}^{k} f(i) p_i \ .$$

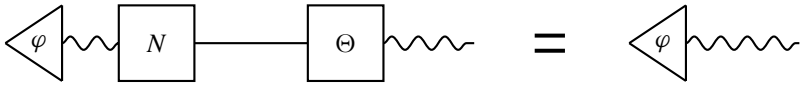
The subsequent preparation of a state ϑ_i is also a quantum operation, Θ say:

$$\Theta : \mathcal{A} \to \mathcal{F}(\Omega_k) : \quad \Theta(a)(i) := \vartheta_i(a) \ .$$

Equation (6) can then be written as

$$\varphi \circ N \circ \Theta = \varphi \ , \tag{10}$$

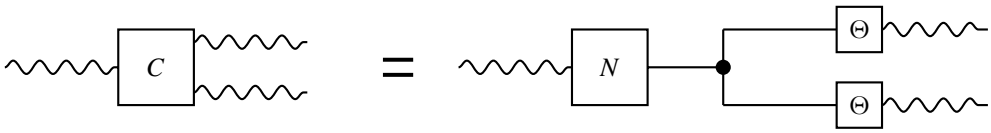
in a picture:



It says that φ can pass through the "entanglement breaking channel" $N \circ \Theta$.
Equation (7) can be written as

$$C = N \circ C_{\mathcal{F}(\Omega_k)} \circ (\Theta \otimes \Theta) \,, \tag{11}$$

in a picture:



where the straight lines stand for the commutative algebra $\mathcal{F}(\Omega_k)$ and the 'fork' denotes its classical broadcaster described in Section 4.2. Theorem 7 says that the states in S can be broadcast by the same quantum operation C if and only if they can all pass through a channel of the form (10) (first picture). If so, then a broadcaster for them is given by equation (11) and the second picture.

4.4 Copying pure states

According to our No-Broadcasting Theorem 7, copying quantum states becomes possible as soon as the state to be reproduced is known to lie in a set S of states whose density matrices commute with each other. For pure states ψ_1 and ψ_2 this means that $|\psi_1\rangle\langle\psi_1| \cdot |\psi_2\rangle\langle\psi_2| = |\psi_2\rangle\langle\psi_2| \cdot |\psi_1\rangle\langle\psi_1|$, i.e. $\psi_1 \parallel \psi_2$ or $\psi_1 \perp \psi_2$. The standard textbook formulation of this fact is called the "No-Cloning Theorem". Since the pure state case figures in all textbooks, and has a much shorter proof [16], we treat it separately below.

Theorem 8 *(***No-Cloning***) Let S be a set of pure states on M_d. Then the states in S possess a common cloner if and only if the associated state vectors are orthogonal.*

Proof Sufficiency: Extend the set of state vectors of states in S to an orthonormal basis $\varepsilon_1, \ldots, \varepsilon_d$ of $\mathcal{H} := \mathbb{C}^d$, and define an isometry $v : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ by $v\varepsilon_i := \varepsilon_i \otimes \varepsilon_i$. Then

$$C : M_d \otimes M_d \to M_d : \quad a \otimes b \mapsto v^*(a \otimes b)v$$

is a common cloner for all states in S, since, for $\varphi = \langle \varepsilon_j, \cdot \varepsilon_j \rangle$,

$$\varphi \circ C(a \otimes b) = \langle \varepsilon_j, v^*(a \otimes b)v\varepsilon_j \rangle = \langle \varepsilon_j \otimes \varepsilon_j, (a \otimes b)\varepsilon_j \otimes \varepsilon_j \rangle = \varphi \otimes \varphi(a \otimes b) \,.$$

To prove necessity, suppose that C is a cloner on M_d for S. By Stinespring's Theorem (Proposition 1) there exist $k \in \mathbb{N}$ and an isometry $v : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H} \otimes \mathbb{C}^k$ such that

$$C(a \otimes b) = v^*(a \otimes b \otimes \mathbb{1}_{M_k})v \,. \tag{12}$$

For $\varphi = \langle \psi, \cdot \psi \rangle \in S$ we have, putting $p := |\psi\rangle\langle\psi|$:

$$\begin{aligned} 1 = \varphi(p)^2 &= \varphi \otimes \varphi(p \otimes p) = \varphi \circ C(p \otimes p) \\ &= \varphi\big(v^*(p \otimes p \otimes \mathbb{1}_{M_k})v\big) = \langle v\psi, (p \otimes p \otimes \mathbb{1}_{M_k})v\psi \rangle \,. \end{aligned}$$

It follows that $v\psi \in \psi \otimes \psi \otimes \mathbb{C}^k$, say $v\psi = \psi \otimes \psi \otimes \alpha$ for some unit vector $\alpha \in \mathbb{C}^k$. Then, if $\langle \vartheta, \cdot \vartheta \rangle$ is another state in S, say with $v\vartheta = \vartheta \otimes \vartheta \otimes \beta$, we have

$$\langle \psi, \vartheta \rangle = \langle v\psi, v\vartheta \rangle = \langle \psi \otimes \psi \otimes \alpha, \vartheta \otimes \vartheta \otimes \beta \rangle = \langle \psi, \vartheta \rangle^2 \cdot \langle \alpha, \beta \rangle \,.$$

So either $\langle \psi, \vartheta \rangle = 0$ or $\langle \psi, \vartheta \rangle \cdot \langle \alpha, \beta \rangle = 1$. As the states $\langle \psi, \cdot \psi \rangle$ and $\langle \vartheta, \cdot \vartheta \rangle$ are different, we have $|\langle \psi, \vartheta \rangle| < 1$. But $|\langle \alpha, \beta \rangle| \leq 1$. Therefore $\psi \perp \vartheta$. □

Remark. The usual proofs of the "no-cloning" principle content themselves with the argument that there is no unitary u with

$$u: \quad \psi \otimes \varepsilon \mapsto \psi \otimes \psi$$

for $\psi \in \{\psi_1, \psi_2\} \subset \mathbb{C}^d$ and a fixed "register" vector $\varepsilon \in \mathbb{C}^d$, unless ψ_1 and ψ_2 are parallel or orthogonal. It leaves one wondering why only operations on such small, d^2-dimensional, closed systems are considered as potential copiers. Even [12] (p. 532) yield to the temptation of simplicity, although they admit that more sophisticated arguments are needed and can be given. The importance of complete positivity as a minimal requirement was first realized by [3], M. Caves, C. Fuchs, R. Jozsa, and B. Shumacher.

Competing interests: The authors declare that they have no conflict of interest.

References

1. D. Dieks. Communication by EPR devices. *Physics Letters*, 92A(6):271–272, 1982.
2. J. Barrett and H. Barnum. Generalized no-broadcasting theorem. *Physical Review Letters*, 99:240501–1–4, 2007.
3. C. Caves and H. Barnum. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818–2821, 1996.
4. N. Herbert. Flash – a superluminal communicator based on a new kind of quantum measurement, 1982. Preprint 81-2003, National Science Foundation, Boulder Creek.
5. R. Hudson and K.R. Parthasarathy. Quantum ito's formula and stochastic evolutions. *Communications in Mathematical Physics*, 93(3):301–323, 1984.
6. M. Krishna and K.R. Parthasarathy. An entropic uncertainty principle for quantum measurements. *The Indian Journal of Statistics*, 64(A3):842–851, 2002.
7. B. Kümmerer and H. Maassen. *Quantum Markov Processes*. Springer, Heidelberg, 2024.
8. B. Kümmerer. Markov dilations on W*-algebras. *Journal of Functional Analysis*, 63(2):139–177, 1985.
9. B. Kümmerer. Quantum markov processes and applications to physics. In O. Barndorff-Nielsen, editor, *Lecture Notes in Mathematics*, volume 1866, pages 259–330, Heidelberg, 2006. Springer.
10. G. Lindblad. A general no-cloning theorem. *Letters in Mathematical Physics*, 47:189–196, 1999.
11. H. Maassen. Quantum probability applied to the damped harmonic oscillator. In J.M. Lindsay and S. Attal, eds., *Quantum Probability Communications*, volume 12, pages 23–58, Singapore, 2003. World Scientific Publishing Company.
12. M. Nielsen and I. Chuang. *Quantum Computing and Quantum Information*. Cambridge University Press, The Edinborough Builing, Cambridge UK, 2000.
13. K.R. Parthasarathy. *An Introduction to Quantum Stochastic Calculus*. Birkhauser, Basel.Boston.Berlin, 1992.
14. K.R. Parthasarathy. Extremal quantum states in coupled systems. *Annales de l'Institut Henri Poincaré B: Probability and Statistics*, 41:257–268, 2005.
15. W.K. Wootters and W.H. Zureck. A single quantum cannot be cloned. *Nature*, 299(28):802–803, 1982.
16. H. Yuen. Amplification of quantum states and noiseless photon amplifiers. *Physics Letters*, 113A(8):404–407, 1986.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.