# The Role of Unitary and Anti–Unitary Operators for No–Go Theorems in Quantum Computing

Graziana Conte
Department of Philosophy
University of Milan,
Italy

## ABSTRACT

No–go theorems for quantum computing give a mathematical proof that quantum dynamic should be linear as well unitary. In this paper we analyze in a detailed way the role of linearity and unitarity for no–cloning theorem; also we introduce a no–go theorem for the square root of Not gate $\sqrt{\texttt{Not}}$ which can never would work in the complete complex Hilbert space.

### General Terms:

Quantum Computation, Symmetry operations

### Keywords:

No–go theorems, Wigner's theorem, Quantum Computing, Square Root of Not gate

## 1. INTRODUCTION

Classical information is encoded in bits which can interact through various discrete operations, the classical logical gates. From a physical point of view a bit behaves like a macroscopic classical object stable in either of two physical states mathematically represented by the values 0 and 1. In the Quantum Computation and Information theory information is encoded by qubits whose mathematical description is based on the two-dimensional complex Hilbert space $\mathbf{C}^2$: in this framework the Boolean states 0 and 1 are represented by a fixed pair of normalized and mutually orthogonal quantum states, usually $|0\rangle$ and $|1\rangle$, that form the standard computational basis $\mathcal{B} = \{|0\rangle, |1\rangle\}$ of this space. Unlike a bit, a qubit can be in a state other than $|0\rangle$ or $|1\rangle$, precisely a qubit can be in a superposition represented as complex linear combination of the basis states

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1}$$

where $\alpha, \beta \in \mathbf{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. Classical and quantum information differ in many ways. In particular, there are no theoretical limitations on manipulation of classical information, conversely there are fundamental limitations on the basic operations that one can perform on information encoded in quantum states. In a sense, *genuine* quantum information seems to have something to do with the information needed to specify a particular state vector from an ensemble of non-orthogonal states, to be more more precise: given two non-orthogonal states $|\psi_1\rangle$ and $|\psi_2\rangle$ of a quantum system, it is possible to decompose $|\psi_2\rangle$ as a superposition of components parallel and perpendicular to $|\psi_1\rangle$

$$|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,\left|\psi_1^{\perp}\right\rangle \tag{2}$$

where $\langle\psi_1^{\perp}|\psi_1\rangle = 0$, $|\alpha|^2 + |\beta|^2 = 1$ and $|\beta| \leq 1$. Since fully quantum dynamic is unitary, the states $\left|\psi_1^{\perp}\right\rangle$ and $|\psi_1\rangle$ will evolve as thought independent, remaining orthogonal in a such a way that the decomposition in (2) is preserved. Now, although $|\psi_1\rangle$ and $|\psi_2\rangle$ are two mathematically distinct states, there is no physical process that can distinguish them with certainty. From the perspective of quantum information theory, two non–orthogonal vectors form the smallest set of states for which no–go theorems are already active: information encoded in two non–orthogonal quantum states cannot be leaked out or shared while keeping the original information content intact (the no–cloning theorem of Wootters and Zurek [10]), it cannot be deleted (the Pati and Baurnstein no–deleting theorem [3]), it is an inseparable entity (no–splitting theorem [7]), it cannot be partially erased ([2]).

Differently, no–go theorems involving quantum logical gates have a strong dissimilarity with these *general* no–go theorem: the impossibility to manipulate arbitrary qubits by global operations which correspond to quantum logic gates does not depend on the orthogonality of quantum states. Both for no–flipping theorem ([9]) and no–universal Hadamard gate ([1]) the linearity of quantum theory and the superposition principle forbid global operations on unknown quantum states.

In this paper we present a deeper understanding of the role of linearity and unitarity of quantum dynamic for the no–cloning theorem and we introduce a no–go theorem for the quantum square of root not gate $\sqrt{\texttt{Not}}$.

## 2. THE ROLE OF UNITARY AND ANTI–UNITARY OPERATORS IN QUANTUM COMPUTING

A linear operator on a Hilbert space $\mathcal{H}$ is a map $L : \mathcal{H} \mapsto \mathcal{H}$ such that for all $\alpha, \beta \in \mathbf{C}$ and $|\psi\rangle, |\phi\rangle \in \mathcal{H}$

$$L(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha L\,|0\rangle + \beta L\,|1\rangle \tag{3}$$

The operator is anti–linear if $L(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha^* L\,|0\rangle + \beta^* L\,|1\rangle$. Unitarity of quantum evolution imposes stricter conditions than just linearity; an operator on a Hilbert space $U : \mathcal{H} \mapsto \mathcal{H}$ is an unitary operator if:

(1) it is a bijection;

(2) it preserves the inner product: $\langle U\phi|U\psi\rangle = \langle\phi|\psi\rangle$, $\forall\,|\psi\rangle\,,|\phi\rangle \in \mathcal{H}$.

An *anti–unitary* operator $K$ is defined to be a map from an Hilbert space $\mathcal{H}$ to itself $K : \mathcal{H} \mapsto \mathcal{H}$ such that:

(1) it is anti–linear;
(2) it preserves the complex conjugate of the inner product: $\langle K\psi|K\phi\rangle = \langle\psi|\phi\rangle^*$.

Unitary operators appear naturally in quantum mechanics whenever there is a symmetry of a physical system. Let us now recall the well known Wigner's theorem about symmetry operations [8] (in the version proposed by Bargmann [5]), which for the scope of the present paper is restricted to the case of symmetries *internal* to a fixed Hilbert space. A *symmetry operation* $\mathbf{T}$ (called also *invariance principle*, or simply *symmetry*) *internal* to a Hilbert space $\mathcal{H}$ is an onto correspondence which yields for each pure state $\mathbf{\Phi} = [\phi]$ of the Hilbert space $\mathcal{H}$, another pure state $\mathbf{\Phi}' = [\phi']$ of the same Hilbert space, such that all the transition probabilities are preserved. In terms of rays, $\mathbf{T}$ defines a mapping $\mathbf{\Phi} \mapsto \mathbf{\Phi}' = \mathbf{T}(\mathbf{\Phi})$ of rays *onto* rays such that

$$\mathbf{\Phi}_1' \cdot \mathbf{\Phi}_2' = \mathbf{\Phi}_1 \cdot \mathbf{\Phi}_2 \qquad if \quad \mathbf{\Phi}_i' = \mathbf{T}(\mathbf{\Phi}_i) \tag{4}$$

(Note that this condition of preservation of transition probabilities implies that the mapping $\mathbf{T}$ is one-to-one).In terms of representatives of states this condition can be expressed as follows:

$$|\langle\phi_1'|\phi_2'\rangle|^2 = |\langle\phi_1|\phi_2\rangle|^2 \qquad if \quad \phi_i \in \mathbf{\Phi}_i \ and \ \phi_i' \in \mathbf{\Phi}_i' \tag{5}$$

The Wigner's theorem says that every such ray mapping $\mathbf{T}$ can be replaced by a vector mapping $T$ of $\mathcal{H}$ which is either unitary or anti–unitary. Precisely, there exists a mapping $T : \mathcal{H} \mapsto \mathcal{H}$, either unitary or anti–unitary, such that $\phi \in \mathbf{\Phi}$ implies $T(\phi) \in \mathbf{T}(\mathbf{\Phi})$. Trivially, this implies that

$$|\langle T(\phi_1)|T(\phi_2)\rangle|^2 = |\langle\phi_1|\phi_2\rangle|^2 \tag{6}$$

Adopting Bargmann's terminology, the operator $T$ is said to be *compatible* with $\mathbf{T}$, and $\mathbf{T}$ is said to be *generated* by (or an *extension* of) the mapping $T$. It is clear that any unitary or anti–unitary operator $T$ induces a symmetry $\mathbf{T}$ associating to any ray $[\phi]$ the corresponding ray $\mathbf{T}[\phi] := [T(\phi)]$. Wigner's theorem asserts that any symmetry is generated only by operators of this kind.

It is known that in ordinary quantum mechanics symmetry transformations and unitary transformations are virtually synonymous, only some discrete symmetries, such as time reversal, are implemented by anti–unitary operators. In mathematical model of quantum information processes, a quantum device acting on the states of a small numbers of qubits is any unitary operator on the associated Hilbert space. The reason is that the anti–unitarily implemented symmetries are non completely positive, i.e. they cannot be applied to a small system living the rest of the world alone and a quantum device is exactly a device which acts on a selected numbers of qubits: as consequence, all quantum processes and computational tasks which can be possibly executed must be represented by unitary operators.

It is interesting to note that in this context (with the exception of no–cloning principle) the non–unitary implementability of symmetries allows to identify no–go theorems which establish that it is impossible to design some important *universal* one–qubit gates as unitary operators. Let us explain this fact.

Let $u = (u_x; u_y; u_z)$ be a fixed vector on the unit surface $S_1(R^3)$ (radius one surface of Euclidean space $R^3$, centered in the zero vector) with polar representation $u = (\sin\vartheta\cos\phi, \sin\vartheta\sin\phi, \cos\vartheta) \equiv (\vartheta, \phi)$ whose antipodal on $S_1(R^3)$ is the unit vector $u^\perp = (\vartheta + \pi, \phi)$. Suppose we are given a qubit pointed in a fixed direction $u$; the usual conceptual approach to the realizations of the basic manipulations of quantum states corresponding to the logical quantum gates is based on finding a suitable unitary operator which, generally, depends from the polar angles $\vartheta; \phi$. In other words, this procedure responds to the following condition:

—for any fixed direction $(\forall u)$, there exists an operator, in general depending from $u$, $(\exists Tu)$ such that (...)

A very different question is the following: is it possible to find a *unique* operator that realizes a certain quantum logical gate for any *arbitrary* direction $w \neq u$ of the unit sphere $S1(R^3)$? Formally, we ask

—there exist a operator $(\exists T)$, such that for every direction $(\forall w)$ (...).

In this case the requirement is very strong and it expresses an *universality* condition (with respect to all the possible directions $w$) which has to be satisfied in order to ensure that all input states are transformed with the same quantum efficiency. In the framework of unitary operators, there are cases in which the latter question has a negative answer. Conversely, these processes can be mathematically described in their exact forms by universal anti–unitary transformations. Because the universal operators are realized by anti-unitary operators, as consequence these universal transformations are examples of *impossible* operations: Werner's no–universal Not gate theorem ([9]), and Pati's no–universal Hadamard gate theorem ([1]) are the most important examples.

## 3. NO–CLONING THEOREM

Classical information can be copied by standard fan-out gate FO:$\{0, 1\} \mapsto \{0, 1\}^2$ expressed by the mapping $x \to (x, x)$ for $x \in \{0, 1\}$.

A well known limitation suffered by quantum information in comparison to classical information is that quantum mechanics does not allow *all* quantum states to be copied exactly and imposes strict restrictions on the possibility to make approximate copies.

The quantum *universal* process of replicating a $\mathbf{C}^2$ state can be formalized in its essential version by some operator $W_{QC} : \mathbf{C}^2 \otimes \mathbf{C}^2 \mapsto \mathbf{C}^2 \otimes \mathbf{C}^2$ on the Hilbert space of the original qubit and the copy which should perform the transformation:

$$|\psi\rangle\,|b\rangle \to\ W_{QC}\ |\psi\rangle\,|\psi\rangle \tag{7}$$

where $|b\rangle$ is the blank state of the copy. If the input original qubit is in an unknown quantum state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ we should obtain the following result:

$$|\psi\rangle\,|b\rangle \to |\psi\rangle\,|\psi\rangle = \alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \beta\alpha\,|10\rangle + \beta^2\,|11\rangle \tag{8}$$

It is not difficult to show that such a machine cannot exist.

Let us now analyze in a detailed way the role of linearity and unitarity conditions for the no–cloning principle: let us consider what result actually corresponds to the transition (7) when the original input is an arbitrary quantum state; firstly, we take into account the role of *linearity*. If the linearity condition is required to hold then the operator $W_{QC}$ must satisfy the correspondence:

$$((|\psi\rangle\,|b\rangle) \to\ W_{QC}\ \alpha W_{QC}\,|0b\rangle + \beta W_{QC}\,|1b\rangle \tag{9}$$

which leads to the transition:

$$(|\psi\rangle\,|b\rangle) \rightarrow\ W_{QC}\ \ |\psi\rangle\,|\psi\rangle = \alpha^2\,|00\rangle + \beta^2\,|11\rangle \qquad (10)$$

that corresponds to what we actually obtain by linearity; it is evident it is incompatible with the ideal result of cloning machine in (9).

Let us now consider the consequences of a minimal requirement of *partial* unitary behavior of the operator $W_{QC}$ (without any requirement of linearity).

This minimal requirement of unitary can be formalized by the rule which must hold for an *arbitrary* pair of vectors $|\psi\rangle\,, |\phi\rangle$:

$$\langle W_{QC}(\psi \otimes b)|W_{QC}(\phi \otimes b)\rangle = \langle \psi \otimes b|\phi \otimes b\rangle \qquad (11)$$

This condition leads to

$$\langle W_{QC}(\psi \otimes b)|W_{QC}(\phi \otimes b)\rangle = \langle \psi|\phi\rangle \cdot \|b\|^2 \qquad (12)$$

On the other hand the application of the operator $W_{QC}$ defined in (7) to this inner product leads to

$$\langle W_{QC}(\psi \otimes b)|W_{QC}(\phi \otimes b)\rangle = \langle \psi \otimes \psi|\varphi \otimes \phi\rangle = \langle \psi|\phi\rangle^2 \quad (13)$$

Putting together these two identities, under condition $\|b\| = 1$, we obtain

$$\langle \psi|\phi\rangle = \langle \psi|\phi\rangle^2 \qquad (14)$$

i.e., $\langle\psi|\phi\rangle(1 - \langle\psi|\phi\rangle) = 0$, which leads to the two alternatives: either $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$. In this second case the further conditions $\|\phi\| = \|\psi\| = 1$ imply that $\langle\psi|\phi\rangle = \|\psi\| \cdot \|\phi\|$ and it is well known that the Schwarz equality holds iff $\psi = e^{i\theta}\phi$, i.e., the two unit vectors are representative of the same state.

More generally, given a nonzero vector $\psi$ any vector $|\phi\rangle = \frac{|\psi\rangle}{\||\psi\rangle\|^2}$ satisfies the condition $\langle\psi|\phi\rangle = 1$ which assures the (partial) unitary behavior of operator $W_{QC}$. In the particular case of $|\psi\rangle = |\phi\rangle$ the now stated alternative reduces the the single case $\|\psi\| = 1$ in which the vector cloning is allowed, whereas this cloning is forbidden for any vector for which $\||\psi\rangle\| \neq 1$.Therefore, the cloner process is not possible under quantum mechanical evolution when $|\psi\rangle$ and $|\phi\rangle$ are non-orthogonal, i.e., $\langle\psi|\phi\rangle \neq 0$. However known quantum states or orthogonal quantum states can always be perfectly copied. Let us stress that there is no universal anti–unitary cloning process.

## 4. NO–UNIVERSAL SQUARE ROOT OF NOT GATE

No–go theorems involving quantum logic gates have a strong dissimilarity with respect to the no–cloning theorem: not only they don't depend on the orthogonality of quantum states, but it is possible to define universal anti–unitary operators that perfectly realize quantum gates. Also, these theorems admit some *exceptions*: unitary quantum gates work perfectly when their action is restricted to *special* sets of quantum input states. For example, the non–existence of an universal Hadamard gate was demonstrated by Pati in [1] and subsequently Maitra and Pashar [4] defined the most general set of qubits for which an universal Hadamard gate exists. In this section we extend the lack of universality to the quantum square root of not gate $\sqrt{\texttt{Not}}$.

Quantum Hadamard $H$ and quantum square root of not $\sqrt{\texttt{Not}}$ gates have no classical counterpart: both these gates implement nontrivial superpositions of basis states, so they play a very important role for the realization of quantum algorithms. At the same time they are two distinct gates: from a physical point of view, they represent two different ways to implement quantum interference, in fact that square root of not and Hadamard quantum gates correspond respectively to a spatially symmetric and a spatially asymmetric beam splitter; also they realize two different *logical* operations. Let us remember that the Hadamard quantum gate is defined to be the unitary operator $H : \mathbf{C}^2 \mapsto \mathbf{C}^2$ whose action on qubits basis states is

$$H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (15)$$

$$H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The Hadamard quantum gate squares the identity: when it is followed by another identical gate, the output is always the identity of the input, i.e. for any vector $|\psi\rangle \in \mathbf{C}^2$, $H(H)\,|\psi\rangle) = I$.

The square root of not is the single qubit gate mathematically represented by the unitary operator $\sqrt{\texttt{Not}} : \mathbf{C}^2 \mapsto \mathbf{C}^2$ whose action on the qubit states is defined by:

$$\sqrt{\texttt{Not}}\,|0\rangle = \frac{1}{2}(1+i)\,|0\rangle + \frac{1}{2}(1-i)\,|1\rangle \qquad (16)$$

$$\sqrt{\texttt{Not}}\,|1\rangle = \frac{1}{2}(1-i)\,|0\rangle + \frac{1}{2}(1+i)\,|1\rangle$$

The square root of not squares the quantum Not gate, when twice applied it gives the Not gate: for any input vector $|\psi\rangle \in \mathbf{C}^2$ the output $\sqrt{\texttt{Not}}(\sqrt{\texttt{Not}}\,|\psi\rangle)$ =Not$|\psi\rangle)$ is always the negation of the input. The physical models of this gate have suggested [6] the logical interpretation of $\sqrt{\texttt{Not}}$ in terms of a *tentative negation*: by applying twice the *attempt* to negate, a full negation is obtained.

Let us now introduce our analysis of the $\sqrt{\texttt{Not}}$ gate starting from the following question: given an unknown qubit $|\psi\rangle \in \mathbf{C}^2$ is it possible to design a quantum logic gate which perfectly transforms the input qubit according to the following rules?:

$$|\psi\rangle \mapsto \frac{1}{2}\Big((i+1)\,|\psi\rangle + (1-i)\,\left|\psi^{\perp}\right\rangle\Big) \qquad (17)$$

$$\left|\psi^{\perp}\right\rangle \mapsto \frac{1}{2}\Big((i-1)\,|\psi\rangle + (1+i)\,\left|\psi^{\perp}\right\rangle\Big)$$

This transformation should realize an equal superposition of the input qubit $|\psi\rangle$ and its orthogonal complement $\left|\psi^{\perp}\right\rangle$ and, generally, corresponds to the action of the square root of not gate $\sqrt{\texttt{Not}}$.

THEOREM 1. *(No–universal square root of not gate). There is no unitary square root of not gate $\sqrt{\texttt{Not}}$ which acts on an unknown quantum state creating an equal superposition of the original state $|\psi\rangle$ and its orthogonal complement $\left|\psi^{\perp}\right\rangle$.*

PROOF. The proof of the theorem is based on the unitarity of quantum dynamic. We proceed by contradiction; let us suppose that a universal square root of not gate exists, so for any two distinct qubits $\{|\psi_1\rangle\,, |\psi_2\rangle\}$ and their complement states $\{\left|\psi_1^{\perp}\right\rangle, \left|\psi_2^{\perp}\right\rangle\}$ such that $|\psi_i\rangle = \alpha_i\,|0\rangle + \beta_i\,|1\rangle$ and $\left|\psi_i^{\perp}\right\rangle = \alpha_i^*\,|1\rangle - \beta_i^*\,|0\rangle$ with $i = 1, 2$, we should obtain

$$\{|\psi_1\rangle \mapsto \frac{1}{2}[(1+i)\,|\psi_1\rangle + (1-i)\,\left|\psi_1^{\perp}\right\rangle)] \qquad (18)$$

$$\left|\psi_1^{\perp}\right\rangle \mapsto \frac{1}{2}[(1-i)\,|\psi_1\rangle + (1+i)\,\left|\psi_1^{\perp}\right\rangle)]$$

and

$$\{|\psi_2\rangle \mapsto \frac{1}{2}[(1+i)\,|\psi_2\rangle + (1-i)\,\left|\psi_2^{\perp}\right\rangle)] \qquad (19)$$

$$\left|\psi_2^\perp\right\rangle \mapsto \frac{1}{2}[(1-i)\left|\psi_2\right\rangle + (1+i)\left|\psi_2^\perp\right\rangle)]$$

The inner product is:

$$\begin{aligned}\langle\psi_1|\psi_2\rangle \mapsto\ & \frac{1}{4}(\langle\psi_1|\psi_2\rangle(1+i)^2 + \langle\psi_1|\psi_2^\perp\rangle(1+i)(1-i) + \\ & +\langle\psi_1^\perp|\psi_2\rangle(1-i)(1+i) + \langle\psi_1^\perp|\psi_2^\perp\rangle(1-i)^2 \quad (20)\end{aligned}$$

and

$$\begin{aligned}\langle\psi_1^\perp|\psi_2^\perp\rangle \mapsto\ & \frac{1}{4}(\langle\psi_1|\psi_2\rangle(1-i)^2 + \langle\psi_1|\psi_2^\perp\rangle(1-i)(1+i) + \\ & +\langle\psi_1^\perp|\psi_2\rangle(1+i)(1-i) + \langle\psi_1^\perp|\psi_2^\perp\rangle(1+i)^2) \quad (21)\end{aligned}$$

For two arbitrary qubits the following conjugations rules are always satisfied:

$$\langle\psi_i|\psi_j^\perp\rangle = -\langle\psi_i^\perp|\psi_i\rangle^* = \langle\psi_i^\perp|\psi_i\rangle \quad (22)$$

and

$$\langle\psi_i|\psi_j\rangle = \langle\psi_i^\perp|\psi_j^\perp\rangle^* \quad (23)$$

When we replace these conditions in the above inner product relations it is straightforward to check that the inner product is not preserved. Hence, a universal unitary $\sqrt{\texttt{Not}}$ doesn't exist. □

On the other hand, there exists an *universal* square root of not gate define by the *anti–unitary* operator $\texttt{U-}\sqrt{\texttt{Not}} : \mathbf{C}^2 \mapsto \mathbf{C}^2$ such that for any qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of $\mathbf{C}^2$ produces the transition

$$\begin{aligned}( \quad & \texttt{U} - \sqrt{\texttt{Not}}(|\psi\rangle) = \frac{1}{2}((1+i)|\psi\rangle) + (1-i)\left|\psi^\perp\right\rangle \\ &= \frac{1}{2}(1+i)(\alpha|0\rangle + \beta|1\rangle) + (1-i)(\beta^*|0\rangle - \alpha^*|1\rangle) \\ &= \frac{1}{2}[(1+i)\alpha|0\rangle + (1+i)\beta|1\rangle + (1-i)\beta^*|0\rangle - (1-i)\alpha^*|1\rangle] \\ &= \frac{1}{2}[(1+i)\alpha + (1-i)\beta^*]|0\rangle - [(1-i)\alpha^* - (1+i)\beta]|1\rangle \quad (24)\end{aligned}$$

The universal anti-unitary operator $\texttt{U-}\sqrt{\texttt{Not}}$ takes a completely unknown quantum state $|\psi\rangle$ and generates the equal superposition with its orthogonal complement according to (17). Let us now consider a completely unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and calculate the *linear* extension of square root gate $\sqrt{\texttt{Not}}$ to this vector:

$$\begin{aligned}&\sqrt{\texttt{Not}}(|\psi\rangle) = \sqrt{\texttt{Not}}(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha\sqrt{\texttt{Not}}|0\rangle + \beta\sqrt{\texttt{Not}}|1\rangle \\ &= \alpha\frac{(1+i)|0\rangle + (1-i)|1\rangle]}{2} + \beta\frac{[(1-i)|0\rangle + (1+i)|1\rangle]}{2} \\ &= \frac{(1+i)\alpha + (1-i)\beta}{2}|0\rangle + \frac{(1-i)\alpha + (1+i)\beta}{2}|1\rangle \quad (25)\end{aligned}$$

The actual output state is very different with respect to the ideal output obtained via the action of $\texttt{U-}\sqrt{\texttt{Not}}$.

Let us now approach the following problem: we want to find the most general class of qubits for which it is possible realize the transformation (17) by the action of the *standard* unitary square root of not $\sqrt{\texttt{Not}}$. By a comparison between the ideal output of $\texttt{U} - \sqrt{\texttt{Not}}$ and the actual output obtain by $\sqrt{\texttt{Not}}$ it is possible to state that the two expressions:

$$(1+i)\alpha + (1-i)\beta^* = (1+i)\alpha + (1-i)\beta \quad (26)$$

$$-[(1i)\alpha^* - (1+i)\beta = (1-i)\alpha + (1+i)\beta$$

should be equal, i.e. $\beta^* = \beta$, so $\beta$ is real and $\alpha^* + \alpha = 0$, as consequence $\alpha$ is imaginary. If we set $\alpha = ia$ and $\beta = b$ the form of the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is restricted to

$$|\psi\rangle = ia|0\rangle + b|1\rangle \quad (27)$$

Following the same procedure it is possible to determine the form of orthogonal complement $\left|\psi^\perp\right\rangle$ that is restricted to the vector

$$\left|\psi^\perp\right\rangle = b|0\rangle + ia|1\rangle \quad (28)$$

THEOREM 2. *The most general qubit states for which it is possible to design an universal square root of not gate that satisfies the conditions in (17) are given by* $\{|\psi\rangle, \left|\psi^\perp\right\rangle : |\psi\rangle = ia|0\rangle + +b|1\rangle; \left|\psi^\perp\right\rangle = b|0\rangle + ia|1\rangle\}$ *where a and b are real numbers such that* $a^2 + b^2 = 1$, $(-1 \leq a \leq 1)$.

PROOF.

$$\begin{aligned}\sqrt{\texttt{Not}}(|\psi\rangle) &= \frac{1}{2}\begin{pmatrix}1+i & 1-i \\ 1-i & 1+i\end{pmatrix}\begin{pmatrix}ia \\ b\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}(1+i)ia & (1-i)b \\ (1-i)ia & (1+i)b\end{pmatrix} \\ &= \frac{1}{2}[(1+i)|\psi\rangle + (1-i)\left|\psi^\perp\right\rangle \quad (29)\end{aligned}$$

If we take the vector $\left|\psi^\perp\right\rangle$:

$$\begin{aligned}\sqrt{\texttt{Not}}(\left|\psi^\perp\right\rangle) &= \frac{1}{2}\begin{pmatrix}1+i & 1-i \\ 1-i & 1+i\end{pmatrix}\begin{pmatrix}b \\ ia\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}(1+i)ia & (1-i)b \\ (1-i)ia & (1+i)b\end{pmatrix} \\ &= \frac{1}{2}[(1+i)|\psi\rangle + (1-i)\left|\psi^\perp\right\rangle \quad (30)\end{aligned}$$

□

Let us now try the largest set of qubits which can be realized as a perfect superposition by the action of a unitary operator, i.e. we relax the universality requirement and consider state dependent $\sqrt{\texttt{Not}}$ quantum gates. Let us start by considering qubits from the polar great circle; ideally we should obtain the following transformations:

$$\begin{aligned}&|\psi(\theta)\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle \mapsto \\ &\mapsto \frac{1}{2}[(1+i)(\cos\frac{\theta}{2}|0\rangle + (1+i)\sin\frac{\theta}{2}|1\rangle] + \\ &+[(1-i)\cos\frac{\theta}{2}|1\rangle - (1-i)\sin\frac{\theta}{2}|0\rangle] \\ &= \frac{1}{2}[(1+i)(\cos\frac{\theta}{2} - (1-i)\sin\frac{\theta}{2}]|0\rangle + \\ &+[(1-i)\cos\frac{\theta}{2} + (1+i)\sin\frac{\theta}{2}]|1\rangle \quad (31)\end{aligned}$$

In this context there is no-state dependent square root of not: we can prove it by considering the most general unitary matrix in the form:

$$\begin{pmatrix}\cos\beta & \sin\beta \\ -\sin\beta & \cos\beta\end{pmatrix}\begin{pmatrix}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}\end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{2}(1+i)\cos\frac{\theta}{2} - \frac{1}{2}(1-i)\sin\frac{\theta}{2} \\ \frac{1}{2}(1-i)\cos\frac{\theta}{2} + \frac{1}{2}(1+i)\sin\frac{\theta}{2} \end{pmatrix} \tag{32}$$

When we develop this equation we obtain:

$$\begin{cases} \cos\beta\cos\frac{\theta}{2} + \sin\beta\sin\frac{\theta}{2} = \frac{1}{2}(1+i)\cos\frac{\theta}{2} - \frac{1}{2}(1-i)\sin\frac{\theta}{2} \\ -\sin\beta\cos\frac{\theta}{2} + \cos\beta\sin\frac{\theta}{2} = \frac{1}{2}(1-i)\cos\frac{\theta}{2} + \frac{1}{2}(1+i)\sin\frac{\theta}{2} \end{cases}$$

and finally we obtain the two following results:

$$\begin{aligned} &\tfrac{1}{2}\cos\tfrac{\theta}{2} - \tfrac{1}{2}\sin\tfrac{\theta}{2} = \\ &= \cos\beta\cos\tfrac{\theta}{2} + \sin\beta\sin\tfrac{\theta}{2} + \tfrac{1}{2}\cos\tfrac{\theta}{2} + \tfrac{1}{2}\sin\tfrac{\theta}{2} = 0 \end{aligned} \tag{33}$$

and

$$\begin{aligned} &\tfrac{1}{2}\cos\tfrac{\theta}{2} + \tfrac{1}{2}\sin\tfrac{\theta}{2} = \\ &= -\sin\beta\cos\tfrac{\theta}{2} + \cos\beta\sin\tfrac{\theta}{2} - \tfrac{1}{2}\cos\tfrac{\theta}{2} + \tfrac{1}{2}\sin\tfrac{\theta}{2} = 0 \end{aligned} \tag{34}$$

and this is a contradiction.
On the contrary we can find a state-dependent square root of not for great equatorial circle quantum states: let us consider the general unitary matrix:

$$\begin{aligned} &\begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2}e^{i\phi} \end{pmatrix} = \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}}\cos\beta + \frac{1}{\sqrt{2}}\sin\beta e^{i\phi} \\ -\frac{1}{\sqrt{2}}\sin\beta + \frac{1}{\sqrt{2}}\cos\beta e^{i\phi} \end{pmatrix} \\ &= \begin{pmatrix} \frac{1}{\sqrt{2}}(\cos\beta + \cos\phi\sin\beta + i\sin\phi\sin\beta) \\ \frac{1}{\sqrt{2}}(-\sin\beta + \cos\beta\cos\phi + i\cos\beta\sin\phi) \end{pmatrix} \end{aligned} \tag{35}$$

The final state is

$$\frac{1}{2}(1+i)\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i\phi}|1\rangle\Big) + \frac{1}{2}(1-i)\Big(\frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}e^{i\phi}|0\rangle\Big) \tag{36}$$

which can be expressed in a more compact form as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where

$$\alpha = \frac{1}{2\sqrt{2}}(1 - \cos\phi + \sin\phi) + i\frac{1}{2\sqrt{2}}(1 + \sin\phi + \cos\phi) \tag{37}$$

and

$$\beta = \frac{1}{2\sqrt{2}}(1 + \cos\phi - \sin\phi) + i\frac{1}{2\sqrt{2}}(-1 + \sin\phi + \cos\phi) \tag{38}$$

With the adequate calculi we find the following system of equations:

$$\begin{cases} \sin\phi = -\frac{1\pm i}{2} \\ \cos\phi = \frac{1\mp i}{2} \end{cases}$$

When we resolve this system we find two possible unitary matrices that realizes two possible states dependent squares root of not:

$$\sqrt{\mathtt{Not}}_E = \frac{1}{2}\begin{pmatrix} 1+i & -(1+i) \\ 1+i & 1+i \end{pmatrix} \tag{39}$$

$\Big($whose transpose is $\sqrt{\mathtt{Not}}_E^{\dagger} = \frac{1}{2}\begin{pmatrix} 1-i & (1-i) \\ -(1-i) & 1-i \end{pmatrix}\Big)$

and

$$\sqrt{\mathtt{Not}}_E \frac{1}{2}\begin{pmatrix} 1-i & -(1-i) \\ (1-i) & 1-i \end{pmatrix} \tag{40}$$

$\Big($whose transpose is $\sqrt{\mathtt{Not}}_E^{\dagger} = \frac{1}{2}\begin{pmatrix} 1+i & (1+i) \\ -(1+i) & 1+i \end{pmatrix}\Big)$.

In order to state that these state dependent squares root of not gate for equatorial great circle are exactly the operators we were looking for it is sufficient to take in account the conjugations rules for the following states, i.e.

$$\langle\psi(\phi_1)|\psi(\phi_2)^{\perp}\rangle = \langle\psi(\theta_1)^{\perp}|\psi(\phi_2)\rangle \tag{41}$$

$$\langle\psi(\phi_1)|\psi(\phi_2)\rangle = \langle\psi(\phi_1)^{\perp}|\psi(\phi_2)^{\perp}\rangle \tag{42}$$

PROOF. Easy. □

## 5. CONCLUSIONS

From a general point of view, no–go theorems are results undoubted very relevant that give a profound insight about the role of universality in quantum computing. In this paper we concentrate on the role of unitary and anti–unitary operators in the context of no–go theorems: with the exception of no–cloning principle, anti–unitary realizations of quantum gates have the remarkable property to be universal gates, in other words they give a positive answer to the full information process. Also we have demonstrated that when information is encoded in a pure unknown quantum state the process to obtain an equal superposition of the original state and its complement is generally impossible by a unique unitary operator. Although an anti–unitary universal realization of quantum square root of not exists, the different states dependent versions of this gate we introduce have the positive aspect to be unitary, but with the drawback of performing only a partial, also if sufficiently great, number of superpositions.

## 6. REFERENCES

[1] A.K.Pati. General impossible operations in quantum information. *Physical Review A*, 63:014301–014307, 2002.

[2] A.K.Pati and B.C.Sanders. No-partial erasure of quantum information. *Physics Letters A*, 359:31–36, 2005.

[3] A.K.Pati and S.L.Braunstein. No-deleting principle. *Nature*, 404(164), 2000.

[4] A.Maitra and P.Pashar. Hadamard type operations for qubits. 2005.

[5] V. Bargmann. Note on wigner's theorem on symmetry operations. *Journal of Mathematical Physics*, 5:862–868, 1964.

[6] E.Ekert D.Deutsch and R.Lupacchini. Machines, logic and quantum physics. *Bullettin of Symbolic Logic*, 3:265–283, 2000.

[7] B.Zeng D.L.Zhou and L.You. Quantum information cannot be split into complementary parts. *Physics Letters A*, 352:41–44, 2006.

[8] E.P.Wigner. Group theory. 1959.

[9] M.Hillery V.Buzek and R.F.Werner. Optimal manipulations with qubits. *Physical Review A*, 60:2626–2629, 1999.

[10] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.