Int. Journ. of Unconventional Computing, Vol. 7, pp. 389–407
Reprints available directly from the publisher
Photocopying permitted by license only

Through the Looking Glass: What Computation Found There

ROSSELLA LUPACCHINI

Department of Philosophy, University of Bologna, Italy
E-mail: rossella.lupacchini@unibo.it

Received: February 23, 2011. Accepted: February 26, 2011.

Commenting about the fact that *two* matrices **1** and $-\mathbf{1}$ in the two-dimensional *complex* space correspond to the *identity* matrix **1** in the three-dimensional real space, Goldstein (1957) remarks that "such a paradoxical situation plays no havoc with our common sense" as the complex space is entirely a mathematical construction. Focusing on the notion of 'observability', this paper aims to entrust the complex space with physical and computational meaning. In the light of quaternions, the efficiency of the Grover search algorithm finds its source in that "paradoxical situation".

Keywords: Observability, measurability, computability, imaginary units, quaternions, mirrors.

1 OBSERVABILITY IN COMPUTATION AND PHYSICS

The following quotation from Hermann Weyl's 1949 book reveals both the intimate link between foundational issues in physics and mathematics as well as their common root in Hilbert's work.

> The 'physical process' undisturbed by observation is represented by a mathematical formalism without intuitive [*anschauliche*] interpretation; only the concrete experiment, the measurement by means of a grating, can be described in intuitive terms. This contrast of physical process and measurement has its analogue in the contrast of formalism and meaningful thinking in Hilbert's system of mathematics. ([23], p. 261.)

But Hilbert's finitary programme failed. Gödel's incompleteness theorems and Turing's negative solution of the *Entscheidungsproblem* took Hilbert's proof theory to its limits as they showed that mathematical procedures cannot be completely included in one ‘formal system’. Those limits, set by a *Turing machine*, overlap with classical physics.

By stretching the ideal of formalism and finitism - *i.e.*, “to atomize mathematical reasoning into such tiny steps that nothing is left to the imagination, nothing is left out!” [5] - a Turing machine, on one hand, guarantees to mathematics its ‘existence’ *via* undecidability;[1] on the other, it demands for indeterminism to be capable of “meaningful thinking”. Computability limits set by Turing are motivated as boundedness conditions on the configurations of symbols which are operated on by a (human) ‘computer’. All such configurations must be “immediately recognisable” *by* the computer; hence, they cannot exhibit an infinity of symbols. In accordance with experience, “if we were to allow an infinity of symbols, then there would be symbols differing to an arbitrarily small extent.” ([20], p. 75.)

In arguing for the adequacy of his notion, Turing focused on the essential capacity involved in computing, namely *distinguishing* symbols.[2] By connecting the *effectiveness* of computability to the ‘resolution power’ of the *computer* involved, Turing’s conceptual analysis of computability shows that, beside any ‘concrete’ physical process, any ‘effective’ process of computation rests on observation and measurement. No adequate understanding of effective procedures can dispense with the medium of the agent - be it a computer, an observer or a measurer - working out the operations involved. Computational and physical processes are bound to observability constraints. Yet quantum theory demands more, it demands to refine the very notion of ‘observability’.

2 QUANTUM OBSERVABILITY

Any physical theory is about observables, namely physical quantities which can be measured on a system, but the classical presupposition that the measured values correspond to actual properties of the system is not tenable in quantum theory because its observables can be *incompatible*. According to the Heisenberg principle, the uncertainty in the value of one observable has to be rigorously distinct from, but is *not independent* of, the uncertainty in the values of the others incompatible observables. Thus ‘incompatible’ does not mean “unable to live together”, quite the contrary. Incompatible observables

[1] “The very day on which the undecidability does not obtain any more, mathematics as we now understand it would cease to exist; it would be replaced by an absolutely mechanical prescription, by means of which anyone could decide the provability or unprovability of any given sentence.” ([21], p. 11.)

[2] Refining Turing’s conceptual argument, Gandy replaces ‘sensory’ limitations of a *computor* with ‘physical’ limitations of a *mechanical device*: a lower bound on the size of atomic components and an upper bound on the speed of signal propagation (a locality condition set by relativity theory). [9] This point has been elaborated particularly in [18]. See also [19].

live *within one and the same* representation space and are represented by operators which are *mutually transformable* and *do not commute*.

Quantum observables without classical analogues are the intrinsic spins of quantum particles. Consider a triad S_x S_y, S_z representing the spin components of an electron. Each of these observables is assumed to have two values, '+' and '-'. Any 'pure' state of the electron assigns probability 1 to exactly one value of one observable, say $(S_z, +)$, and probability 0 to the opposite value $(S_z, -)$, and the same probability 0.5 to the values of the incompatible observables $(S_x, +)$ and $(S_x, -)$, $\left(S_y, +\right)$ and $\left(S_y, -\right)$. Accordingly, any pure state of one observable is equidistant from the pure states of the other observables.

A unit sphere is a convenient way to visualize the *symmetry and continuity* constraints on probabilities associated with such incompatible observables, keeping in mind that the angular separation between 'orthogonal' pure states of the same observable *doubles* $\frac{\pi}{2}$. If a pure state $|\psi\rangle$ of one observable is represented by the point $\sigma = (\phi, \theta)$ on the sphere,[3] the second pure state of the same observable, orthogonal to the first, is represented by the antipode $\sigma^* = (\pi \pm \phi, \theta)$. As an 'observer-subject', the state $|\psi\rangle$ assigns probabilities to each *experimental question* concerning the value of each observable S_σ over the sphere, *i.e.*, concerning the "object" $\sigma^+ \equiv (S_\sigma, +)$. The probability is a symmetrical and continuous function f of the angular separation δ between any pair of states corresponding to the points σ and ϑ on the sphere: $p_\sigma(\vartheta) = f(\delta_{\sigma,\vartheta}) = p_\vartheta(\sigma)$. Thus $|\psi\rangle$ assigns probability 1 to exactly one point, that coincides with its own 'point of view', namely when $\delta = 0$, and the same probability $p_\psi\ (\sigma)$ to all points on the same 'latitude' as σ.

The point at issue is that no pure state of one observable can coincide with a pure state of another observable, for all pure states must be *distinguishable*. Here is the reason to require, beside orthogonality between pure states of one and the same observable, that the operators representing incompatible observables do not commute. Notice that, by *rotating* the sphere, the diagram of S_σ–results can be transformed into the diagram of S_ϑ-results as the operators are mutually transformable. Thus pure states of the same observable are *invariantly* mutually orthogonal, while pure states of incompatible observables are mutually 'oblique'. That is how probabilities are assigned to quantum states over a unit sphere according to the uncertainty principle.

Now we must distinguish between the three dimensional Euclidean space, which contains the 'tactile' unit sphere,[4] and the *representation* space from which the usual algorithm generates probability assignments. (See [14], p. 124.) Since any quantum state of the electron spin results from a linear combination of two 'basis' states, the corresponding basis vectors span a

[3] The azimuthal angle ϕ can vary as $-\pi < \phi \leq \pi$ and the longitude θ as $-\frac{\pi}{2} < \theta \leq \frac{\pi}{2}$.

[4] "Euclidean geometry is tactile because its assertions agree with our sense of touch but not always with our sense of sight. [...] We never *see* parallel lines." ([15], p. 170.)

two-dimensional representation space.[5] How to render in two dimensions the network of probability relations amongst the values of the three spin components of the electron? The symmetry group of the unit sphere, which is the set of all its rotations about its centre, has no representation in the two-dimensional 'real' space. A subtle invention is needed.

3 ALBERTI'S VEIL *VS* EINSTEIN'S

In classical physics, a complete description of how things are now is given by a point in the phase space and the Hamiltonian function determines how things change with time. However, to make classical physics deterministic, an additional assumption is needed, namely that the physical system is *closed*. In quantum physics, a deterministic description of how the state of a system evolves with time is given by the Schrödinger wave equation. Nevertheless quantum theory is inherently probabilistic. A quantum state is a kind of precarious 'intermediate' state, shaped as a 'superposition' of basis states by the wave function. Consider, for instance, the quantum state of the electron's spin S_σ written in the form:

$$|\psi\rangle_\sigma = \alpha\,|+\rangle + \beta\,|-\rangle\,. \tag{1}$$

Here α and β are the '*complex* probability *amplitudes*' of observing the values $(S_\sigma, +)$ and $(S_\sigma, -)$ respectively.[6] Once a measurement is performed, we get either the state $|+\rangle$, with probability $|\alpha|^2$, or the state $|-\rangle$, with probability $|\beta|^2$; the superposition state is lost. The 'probability wave' vanishes. The nature of the wave function has been viewed as a crucial issue in most discussions about the interpretation of quantum theory. What does it tell us about physical phenomena? Does matter possess a wave character? If it does, how can we detect such a character? In his doctorate dissertation, Luis de Broglie conjectured that the wave character of photons should be extended "to all material particles and notably to electrons". De Broglie's work appealed to Einstein who wrote that de Broglie had "lifted a corner of the great veil" which hides the true face of Nature. (Cf. [25].) Despite Einstein's efforts to lift the whole veil, the wave function seems entitled to describe nothing but a sort of *pre*-probability or, as it is called, a 'probability amplitude'. But then the wave character of photons emanates from the very notion of 'probability'.

A quantum state does not describe how things are but how their probabilities are weaved. Quantum physics differs from classical physics as to

[5] The elements of this representation space are called 'spinors'.

[6] Since a probability is the squared modulus of a probability amplitude, α and β must be such that $|\alpha|^2 + |\beta|^2 = 1$.

the impossibility of performing certain measurements simultaneously with accuracy: a measurement is not a passive record, it is an *inter-action* between the system-to-be-observed and the observer-system; hence, it establishes a connection between the two parts. As far as measurement is viewed as a subject-object interaction, with the twin requirement of freedom in choosing the observable to be questioned and capability of distinguishing 'incompatible' outcomes, quantum theory demands to sharpen the probability relations associated with its possible states and, consequently, to refine their mathematical representation on a *complex* space.

As mentioned above, the probability distribution over the unit sphere is a uniform map of points whose angular separation is *twice* the angular separation between the corresponding quantum states. This doubling of angles recalls Hamilton's mistake in his attempt to give a meaning to *imaginary units* through rotations. The fascinating story of the invention of 'quaternions' is masterfully told by Altmann (1992). Here it is worth recalling that Hamilton's 'original sin' lies in interpreting a *pure normalized* quaternion, such as $Q = \left[\cos\frac{\pi}{2}, \sin\frac{\pi}{2}\mathbf{r}\right] = [0, \mathbf{r}]$, as a vector $\mathbf{r}$ rather than as a 'binary rotation'. In two dimensions, such a rotation requires a *reflection* operator.

Almost four centuries before the invention of quaternions, we can recognize a reflection operator in the 'Alberti's veil', the most eloquent icon of the invention of *perspectiva pingendi*. It is well known that carrying over concepts and methods of the medieval optics, or '*natural* perspective', into a flat surface, the Renaissance artists worked out a system of '*artificial* perspective'. But the new *inventio* asks the light to get rid of any material character and its rays to challenge the rules of Euclidean geometry.[7] In his *Della Pittura*, Leon Battista Alberti described how to attain a 'focused' view of a scene by observing it through a '*velo*' loosely woven of fine thread (see Figure 1). The mathematical rules of perspective must enable the painter to transfer points of the scene, seen and captured through the veil's weave, to points on the canvas. The result is a painted or drawn scene, which is supposed to be indistinguishable from the one transmitted by a glass or reflected by a mirror. It is achieved by projecting the three-dimensional scene on a plane, letting the flight lines converge in a *vanishing* point specularly symmetrical to the unmoving eye of the painter-observer. In this representation space, any picture-object is anchored to its author-subject through Alberti's veil acting as a 'beam-splitter'.

A superb illustration of the epistemological value of artificial perspective is provided by the subject-object specular symmetry emerging from the Arnolfini portrait by van Eyck. In this painting, approximately at the point where, according to the correct rules of perspective, the flight lines would converge,

[7] Traveling in parallel they meet in one point, and give rise to a non-Euclidean '*visual* space'.

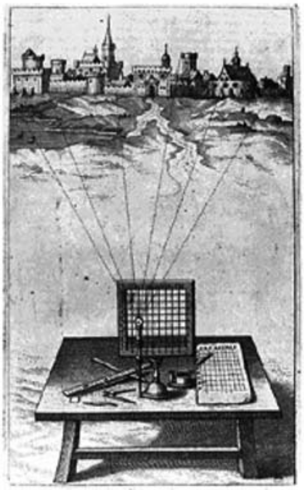

FIGURE 1
Alberti's veil. The painter imagines that his canvas is a window, through which he looks at the scene, *as well as* a mirror, which reflects his eye in the 'vanishing point'.

FIGURE 2
Self-portrait of the painter-observer in the 'vanishing point' (J. van Eyck, *The Arnolfini Portrait*, 1434).

we can see the outline of van Eyck reflected in a mirror (Figure 2). The self-portrait of the painter makes evident what the rules of perspective would set up as a 'formal system': the displaying of the 'pictorial' space through an *imaginary* dimension traced to the painter's eye. To allow the scene to take shape a third dimension must be added: then the Arnolfinis' room is unfolded to the rear, while the painter is projected to the front by its mirror image.

Thus the painter-observer can benefit from two 'complementary' points of view: one 'real', *i.e.*, that of the person who watches the painting and sees the frontal scene; the other 'virtual', *i.e.*, that of the self-portrait within the reality constructed by art, beyond the plane of the representation. The *perspectival* representation space enables the painter to be inside and outside the representation, alternatively observer-subject and observed-object, because the two conditions - observing and being observed - are symmetrical, mutually transformable, thanks to the overturning through the painting.

Coming back to Hamilton's concern about imaginary units, the first step is to understand the meaning of the multiplication rule

$$\mathbf{i}^2 = -1, \tag{2}$$

at the origins of complex algebra. On the Argand plane, one can easily see a complex number $z = (x + iy)$ as a 'vector' $\mathbf{z} = (x, y)$, and the action of the imaginary unit on $\mathbf{z}$[8] as a rotation by $\frac{\pi}{2}$, which gives $\mathbf{z}_\perp = (-y, x)$. By repeating this operation, $\mathbf{z}$ is rotated by π and changes sign.[9] Accordingly, $\mathbf{i}^2 = -1$ is understood as a *binary rotation*. So far, in the '*flatland*' of Argand, so good.

Quaternions arise by continuing the 'doubling' process that gives us complex numbers from real numbers. They require three imaginary units $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, with the multiplication rules:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1, \qquad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}. \tag{3}$$

A quaternion $A = (a + A_x i + A_y j + A_z k)$ can be written as a couple $A = [a, \mathbf{A}]$ made up of a scalar a and a vector $\mathbf{A} = (A_x, A_y, A_z)$. It follows that A will be *normalized* when

$$|A|^2 = a^2 + |\mathbf{A}|^2 = 1. \tag{4}$$

Notice that all quaternions of the form $[\cos\alpha, \sin\alpha\mathbf{n}]$, with $|\mathbf{n}|^2 = 1$, are normalized. Moreover, when $\alpha = \frac{\pi}{2}$, these quaternions are also *pure*, namely of the form $[0, \mathbf{n}]$. So, for Hamilton, a pure normalized quaternion is a unit vector. It follows that, since quaternions must perform rotations, a normalized quaternion acting on a unit vector must simply rotate the vector. The result is again a pure normalized quaternion. For instance, the product of two quaternions such as $\rho = [0, \mathbf{r}]$ with $|\mathbf{r}| = 1$ and $A = [\cos\alpha, \sin\alpha\mathbf{n}]$ gives:

$$A\rho = [\cos\alpha, \sin\alpha\mathbf{n}]\,[0, \mathbf{r}] = [0 - \sin\alpha\mathbf{n}\cdot\mathbf{r}, \cos\alpha\mathbf{r} + \sin\alpha\,(\mathbf{n}\times\mathbf{r})]\,. \tag{5}$$

[8] $z = x + iy \Rightarrow iz = -y + ix = z_\perp$
[9] $\mathbf{i}^2\mathbf{z} = \mathbf{i}\mathbf{z}_\perp \Rightarrow iz_\perp = -(x + iy) = -z \Rightarrow -\mathbf{z} = (-x, -y)$

If **n** and **r** are orthogonal, the scalar product $\mathbf{n}\cdot\mathbf{r}$ will be null, and the outcome will be a pure normalized quaternion:

$$A\rho = [0, \cos\alpha\,\mathbf{r} + \sin\alpha\,(\mathbf{n}\times\mathbf{r})] = \left[0, \mathbf{r}'\right] = \rho'. \tag{6}$$

Hamilton associates the quaternion A with the rotation $R(\alpha\mathbf{n})$, by the angle α about the axis **n**,

$$A = [\cos\alpha, \sin\alpha\,\mathbf{n}] \Rightarrow R(\alpha\mathbf{n}). \tag{7}$$

Therefore, he reads equation (6) as a rotation of the vector **r** by α, as shown in Figure 3A. But, in fact, his reading is wrong.

The rotation to be associated with the quaternion is by double the angle of the quaternion (see next section); **r** is not an ordinary vector but a rotation axis; a pure normalized quaternion is not a unit vector but a binary rotation. The correct interpretation of (6) is illustrated in Figure 3B. Here we see that a binary rotation about **r** followed by a rotation by 2α about the axis **n**, perpendicular to **r**, equals a binary rotation about $\mathbf{r}'$, with $\mathbf{r}'\perp\mathbf{n}$, at an angle α from **r**.[10] But all this means that the quaternion A describes the rotation $R(2\alpha\mathbf{n})$:

$$A = [\cos\alpha, \sin\alpha\,\mathbf{n}] \Rightarrow R(2\alpha\mathbf{n}) \tag{8}$$

Like any other quaternion, a pure normalized quaternion acts as a rotation, indeed as a binary rotation:

$$\rho = [0, \mathbf{r}] = \left[\cos\frac{\pi}{2}, \sin\frac{\pi}{2}\mathbf{r}\right] \Rightarrow R(\pi\mathbf{r}). \tag{9}$$

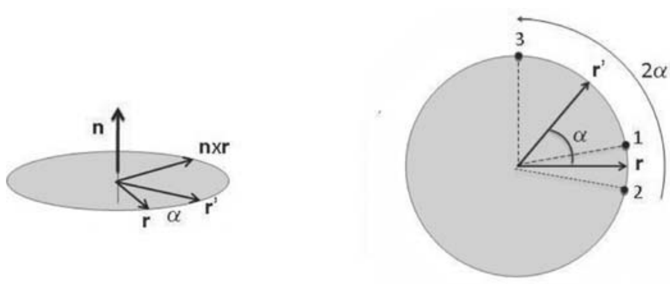

FIGURE 3
A: Hamilton's rotation. B: $[0, \mathbf{r}]$ rotating by 2α becomes $[0, \mathbf{r}']$.

[10] For a detailed analysis of strength and weakness of Hamilton's work, see [3], chap. 2.

Now, if an imaginary unit, as a pure normalized quaternion, is a rotation by π,

$$\mathbf{i} = [0, \mathbf{i}] \Rightarrow R\,(\pi\,\mathbf{i}) \tag{10}$$

its square must be a rotation by 2π:

$$\mathbf{i}^2 = [\,\cos\pi, \sin\pi\,\mathbf{i}] = -1 \qquad \Rightarrow \qquad R\,(2\pi\,\mathbf{i})\,. \tag{11}$$

However strange it may appear, the rotation by 2π is not the identity!

4 ROTATIONS AND MIRRORS

On the unit sphere, a rotation by β about the axis $\mathbf{m}$, $R(\beta\mathbf{m})$, followed by a rotation $R(\alpha\mathbf{l})$ must equal some rotation $R(\gamma\mathbf{n})$:

$$R(\alpha\mathbf{l})R(\beta\mathbf{m}) = R(\gamma\mathbf{n}). \tag{12}$$

This result was proved by Euler (1775). The geometrical relation, *i.e.*, the spherical triangle drawn by the three rotations, was found by Rodrigues (1840). In modern vector notation, the angle and axis of the resultant rotation, in terms of those of the given rotations, are provided by the following equations:

$$\cos\frac{\gamma}{2} = \cos\frac{\alpha}{2}\cos\frac{\beta}{2} - \sin\frac{\alpha}{2}\sin\frac{\beta}{2}\mathbf{l}\cdot\mathbf{m} \tag{13}$$

$$\sin\frac{\gamma}{2}\mathbf{n} = \sin\frac{\alpha}{2}\cos\frac{\beta}{2}\mathbf{l} + \cos\frac{\alpha}{2}\sin\frac{\beta}{2}\mathbf{m} + \sin\frac{\alpha}{2}\sin\frac{\beta}{2}(\mathbf{l}\times\mathbf{m}). \tag{14}$$

These equations verify Hamilton's quaternion multiplication rule:

$$[\,\cos\frac{\alpha}{2}, \sin\frac{\alpha}{2}\mathbf{l}][\,\cos\frac{\beta}{2}, \sin\frac{\beta}{2}\mathbf{m}] = [\,\cos\frac{\gamma}{2}, \sin\frac{\gamma}{2}\mathbf{n}]. \tag{15}$$

Once more quaternions elicit 'rotations', but those which appear in the quaternions are half-angles of rotation. As to the imaginary units $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, they can be viewed as binary rotations around three mutually perpendicular axes. Yet quaternions do not dwell in a three-dimesional *real* space, they have been brought about in two dimensions.

It is time to retrieve our quantum observables and to pursue our search for a proper representation of their probability relations in two dimensions. The problem at issue is as to how three-dimensional rotations can be 'projected' on a plane. The rotations of the Euclidean space are represented by 3×3 real orthogonal matrices. Among these, those with determinant $+1$ represent the *proper* rotations and form the so-called *Special Orthogonal group* $SO(3)$. The Cayley-Klein parameters a, b, provide the keys to transfer a rotation $R(\theta\mathbf{n})$ from the real space $\mathbf{R}^3$ into the two-dimensional complex space $\mathbf{C}^2$:

$$a = \cos\frac{\theta}{2} - in_z \sin\frac{\theta}{2}, \qquad b = (n_y + in_x)\sin\frac{\theta}{2} \tag{16}$$

$$\mathbf{U} = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \tag{17}$$

To any rotation which leaves invariant the angular separation between points of the unit sphere, there corresponds *two* unitary tranformatios $\mathbf{U}$ and $-\mathbf{U}$ on the set of rays of $\mathbf{C}^2$, which leave invariant the angular separation between rays. When the unitary matrix $\mathbf{U}$ corresponds to an orthogonal real matrix, so does $-\mathbf{U}$. These unitary matrices form the *group* $SU(2)$.

One peculiar feature of matrices involving Cayley-Klein parameters is the presence of half-angles. The presence of half-angles in the 2×2 unitary matrices corresponding to 3×3 rotation matrices reveals a distinct character of the complex representation space. Whereas, in the Euclidean space, a rotation by $\theta = 2\pi$ about z results in the identity transformation $\mathbf{R}_{2\pi} = \mathbf{1}$, the corresponding matrix, in $\mathbf{C}^2$, is $\mathbf{U}_{2\pi} = -\mathbf{1}$!

$$\mathbf{R}_{\theta\mathbf{z}} = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \Leftrightarrow \mathbf{U}_\theta = \begin{pmatrix} e^{\frac{i\theta}{2}} & 0 \\ 0 & e^{-\frac{i\theta}{2}} \end{pmatrix} \tag{18}$$

Two 2×2 complex matrices, $\mathbf{1}$ and $-\mathbf{1}$, correspond to the same 3×3 real matrix $\mathbf{1}$. Does any physical meaning attach to the structure of such a space?

Let us take a closer look at the quaternion multiplication rule. In the product of two quaternions $A = [a, \mathbf{A}]$ and $B = [b, \mathbf{B}]$, that is

$$AB = [ab - \mathbf{A} \cdot \mathbf{B}, a\mathbf{B} + b\mathbf{A} + \mathbf{A} \times \mathbf{B}], \tag{19}$$

we can recognize an *axial* vector, which results from the *cross product* of two *polar* vectors $\mathbf{A}$ and $\mathbf{B}$:

$$\mathbf{A} \times \mathbf{B} = (A_yB_z - A_zB_y, A_xB_z - A_zB_x, A_xB_y - A_yB_x). \tag{20}$$

Axial and polar vectors disclose their nature through a mirror. How they behave under reflection and 'inversion', *i.e.*, a transformation which carries any point into its antipode, is shown in Figure 4 (mind the grey arrows). In contrast to polar vectors, axial vectors change sign under reflection (Figure 4A). As to polar vectors, they can also be generated by objects of a different

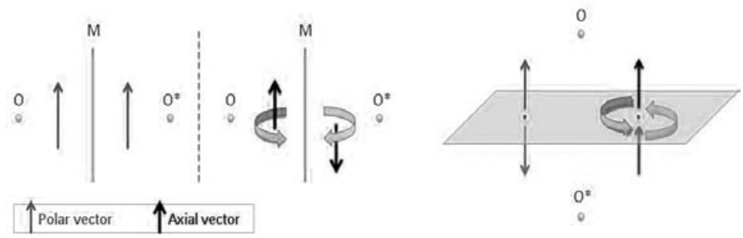

FIGURE 4
A: Reflection. B: Inversion.

'nature'. The *tensor product* of two objects like $\lambda = (\lambda_1, \lambda_2)$, $\mu = (\mu_1, \mu_2)$, gives:

$$\lambda_1\mu_1, \lambda_1\mu_2, \lambda_2\mu_1, \lambda_2\mu_2. \tag{21}$$

From this product we can take out two 'new' objects, one with three symmetric components,

$$(\lambda_1\mu_1, \lambda_1\mu_2 + \lambda_2\mu_1, \lambda_2\mu_2), \tag{22}$$

another with one antisymmetric component,

$$\lambda_1\mu_2 - \lambda_2\mu_1. \tag{23}$$

Under rotation and reflection, the object (22) performs like a polar vector; hence we are entitled to call it as such. Notice that, even though λ and μ change sign, (22) does *not* change sign. Therefore, it maintains its identity of vector under rotation by 2π. Objects such as λ and μ were invented by Cartan in 1913. In the 1920s, Pauli drew the same objects from the wave equation of the electron 'spin'. Here is the reason to call *spinors* the bases of the representation space of two-valued quantum observables, *i.e.*, the Hilbert space $\mathbf{C}^2$.

Quantum incompatible observables such as the electron spin are knitted together in a way precisely captured by a complex representation space. Their mutual interdependence has an essentially probabilistic character, but not of the kind found in classical physics. The 'bilateral' symmetries between any quantum state and its alternatives bring about an 'imaginary' dimension, hence *complex* probability *amplitudes*. The way in which symmetry and continuity constraints mould the probability relations between quantum observables can be visualized on the Euclidean sphere. The way in which quantum theory depicts those relations in the complex space is reminiscent of the way in which theoretical constructions are determined by perspective in art: projecting geometrically from three to two dimensions and doing the opposite, generating

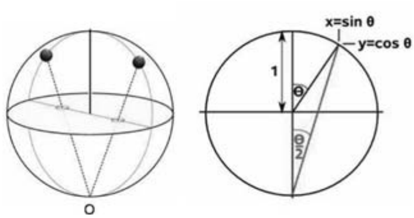

FIGURE 5
Stereographic projection.

three dimensions from two. In fact, a *stereographic projection*, in which each point of the sphere is projected onto the 'equator' plane (as shown in Figure 5), illustrates how to map every rotation of $SO(3)$ to a 'rotation', namely a unitary transformation, of $SU(2)$.[11]

Any rotation around one point on the plane is the product of two reflections about two *lines* intersecting at that point, separated by half-angle of rotation (as shown in Figure 3B). Although this rotation is presented as a strict operation in two dimensions, it can be readily regarded as a rotation around an axis perpendicular to the plane of the two 'mirror lines'. The fact that in this way we generate three dimensions starting from a strict two-dimensional operation is paralleled by the fact that the bases of $SU(2)$ in a two-dimensional space, the spinors, generate by their tensor product the vectors and scalars in $SO(3)$. Finally reflections are the fundamental operations that generate all spaces of higher dimension.

We have seen the quaternion units as binary rotations in three dimensions. Now we can see them in two dimensions through 'Pauli spin matrices'. The general form of the matrix representing a two-value observable S_σ,

$$\mathbf{S}_\sigma = \begin{pmatrix} z & x - iy \\ x + iy & -z \end{pmatrix}, \tag{24}$$

can be written as $\mathbf{S}_\sigma = x\sigma_x + y\sigma_y + z\sigma_z$, where σ_x, σ_y, σ_z are the *Pauli spin matrices*:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{25}$$

They are orthogonal *mirrors* perpendicular to **x**, **y**, **z**, respectively. A complex space provides quantum theory with a looking glass. Through the looking glass, quantum observables become intelligible in their multiplicity and mutability. May complex numbers also throw light on computational processes?

[11] To light this topic, see [2], chapp. 7-9, as well as [13], chap. 3.

5 SEARCH ALGORITHM THROUGH THE LOOKING GLASS

As mentioned above, a requirement for 'observability' is also crucial in Turing's computability, for distinguishing symbols is the essential capacity required of the computing 'agent'. Now, if the computing agent is a *quantum physical system*, how does its 'complex' observability affect computation?

In Wittgenstein's words, "Turing machines are humans who calculate". Indeed Turing's constraints on computability rest on the 'sensory' limitations of a *human* computer. If a computation is performed by reading and writing symbols on paper, the number of symbols must be finite, to ensure that all symbols (which take part in a computational step) can be observed at one glance. In so far as a computation is conceived as a discrete, mechanical procedure, Turing's computability echoes Hilbert's finitary tenets:

> The fundamental idea of my proof theory is none other than to describe the activity of our understanding, to make a protocol of the rules according to which our thinking actually proceeds. Thinking, it so happens, parallels speaking and writing: we form statements and place them one behind another. ([12], p. 475.)

Nevertheless once it was clear that there can be no Turing machine for the *Entscheidungsproblem*, Hilbert's proof theory was confronted with its limits. Hilbert's ingenious attempt to secure the *continuum* by projecting it into the *discrete* was defeated by applying the diagonal process. No Turing machine can decide whether an *alleged* computable function $f(x)$ on positive integers is indeed such a function. Can a '*quantum* Turing machine' do anything better?

The description of a *quantum Turing machine* is derived from a Turing machine, but using quantum theory to define the operations carried out by the computer. Since the computer is now a quantum physical system, any computational step is a unitary operation. A two-state quantum system, like the electron spin, provides a model for a single computational unit, called *qubit*. Consider a spin component S_σ. Its basis states $|+\rangle_\sigma$, $|-\rangle_\sigma$ can be associated with the computational basis states $|0\rangle$, $|1\rangle$ of the qubit. Then the basis states of an 'incompatible' observable, such as the spin component S_ϑ, will correspond to a different computational basis:

$$|+\rangle_\vartheta = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle_\vartheta = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{26}$$

When a qubit is in one of the states (26), the probability for measuring either the bit $|0\rangle$ or the bit $|1\rangle$ is $1/2$. Not surprisingly, the Euclidean unit sphere - the so called 'Bloch sphere' - provides a convenient representation of a qubit. If the 'North pole' $\sigma = (0, 0)_{\phi,\theta}$ represents the state $|0\rangle$ and the 'South pole' $\sigma^* = (\pi, 0)_{\phi,\theta}$ represents the state $|1\rangle$, then each of the infinite points on the sphere maps a qubit state:

$$|\psi\rangle = \cos\frac{\phi}{2}\,|0\rangle + e^{i\theta}\sin\frac{\phi}{2}\,|1\rangle\,. \tag{27}$$

A qubit consists of all the linear combinations of the classical bits with complex amplitudes constrained only by the normalization condition. A quantum algorithm is constructed of unitary operators acting on qubits. If the initial state contains n qubits, the algorithm will spread out on a 2^n-dimensional complex space. Notice that: (*i*) while the state of one bit conveys a single bit of information, the state of a single qubit holds infinitely many bits of information; (*ii*) whereas unitary operations are reversible, the only classically meaningful reversible operations on n bits are the $(2^n)!$ different permutations of 2^n binary sequences. It would seem that "instead of being limited to shuffling a finite collection of bit states through permutation, one can act on qubits with a continuous collection of unitary transformations." ([16], p. 27.) But it is not so.

Although, at first, this appearance of continuity might question Turing's computability, in fact there is no way to extract information from the qubits, other than to *measure* them. To read the final state of a quantum computation means to perform a measurement; hence, to reduce qubits to classical bits. Quantum computability does not break away from Turing's constraints. Rather than unleash Turing's constrains, quantum theory of computation "provides dramatic proof that the abstract analysis of computation cannot be divorced from the physical means available for its execution".[12] Before performing the measurement, however, quantum observability can play its role.

Grover's search algorithm constitutes a remarkable result for quantum computing. It is a procedure for searching N possibilities in $O(\sqrt{N})$ steps. In his 2001 paper, Grover calls for an incisive explanation:[13]

> *What is the reason that one would expect that a quantum mechanical scheme could accomplish the search in $O(\sqrt{N})$ steps*? It would be insightful to have a simple two line argument for this without having to describe the details of the search algorithm. ([11], p. 15.)

The algorithm may be summarized as follows (see [17], pp. 248 ff.) It begins with the computer in the state $|0\rangle$ composed of n qubits.[14] The

[12] Although this passage is intended to highlight a characteristic feature of quantum theory of computation. See [16], p. 23.

[13] I am grateful to Giuseppe Castagnoli for drawing my attention to this point. His answer (2010) is that any quantum algorithm takes the time of a classical algorithm knowing in advance 50% of the information that specifies the solution of the problem. This is due to 'quantum correlation' between selecting the problem and reading out the solution.

[14] More precisely, this state should be written as $|0\rangle^{\otimes n}$.

'Hadamard transform' $H^{\otimes n}$ takes it to the equal superposition state,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle \tag{28}$$

Then, the same unitary transformation, the so called 'Grover iterate' G, is applied $O(\sqrt{N})$ times. It can be broken into four steps:

(1) action of a 'quantum oracle' O;
(2) Hadamard transformation;
(3) conditional phase shift of -1 on every basis state except $|0\rangle$,

$$|x\rangle \rightarrow (-1)^{\delta_{x0}} |x\rangle \, ; \tag{29}$$

(4) Hadamard transformation.

Step (1). Consider a function $f(x)$ on positive integers in the range 0 to $N-1$. Suppose $f(x) = 1$ if x is a solution to the search problem, and $f(x) = 0$ if x is not a solution to the search problem. The *quantum oracle O* can *see* solutions to the search problem and signal them on a single qubit $|q\rangle$. Let x be a particular instance of the search problem. The action of the oracle on the computational basis is the unitary operation

$$|x\rangle\,|q\rangle \rightarrow |x\rangle\,|q \oplus f(x)\rangle \, , \tag{30}$$

where $\oplus$ denotes addition modulo 2. The *oracle qubit* $|q\rangle$ is flipped if $f(x) = 1$, while it is unchanged if $f(x) = 0$. To check whether or not x is a solution of the search problem, one can apply the oracle to the initial state $|x\rangle\,|q\rangle$ and read the final state of the oracle qubit. Now, if the initial state of the oracle qubit is $(|0\rangle - |1\rangle)/\sqrt{2}$, then, when x is a solution of the search problem, the action of the oracle interchanges $|0\rangle$ and $|1\rangle$ and gives the final state $-|x\rangle\,|q\rangle$.[15] Therefore, the action of the oracle can be written as:

$$|x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow (-1)^{f(x)} |x\rangle \, \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{31}$$

Since the state of the oracle qubit does not change, it can be omitted and the action of the oracle results in:

$$|x\rangle \rightarrow (-1)^{f(x)} |x\rangle \, . \tag{32}$$

This lights the oracle *marking* the solution to the search problem, by shifting the phase of the solution. It turns out that it suffices to apply the quantum

[15] When x is not a solution to the search problem, the oracle does nothing.

oracle $O(\sqrt{N})$ times in order to obtain a solution. It seems as though the oracle already 'knows' the answer to the problem. But, in fact, it does not. The oracle acts just like a mirror oriented in direct line with solutions. It reflects what it 'sees', without necessarily knowing what it is.

Steps (2)-(4). After applying the quantum oracle O, the action of the next three steps gives:

$$H^{\otimes n}(2\,|0\rangle\,\langle 0| - I)H^{\otimes n} = 2\,|\psi\rangle\,\langle\psi| - I, \tag{33}$$

where $|\psi\rangle$ is the state (28). Thus the whole *Grover iterate* can be written $G = (2\,|\psi\rangle\,\langle\psi| - I)O$. From a geometrical point of view, it appears as a rotation of $|\psi\rangle$ by an angle θ, which depends on N and the number of solutions, towards the solution to the search problem.

Take $|k\rangle$ to denote the weighted sum over all x which are *not* solutions to the search problem, and $|k_\perp\rangle$ to denote the weighted sum over all x which are solutions. As shown in Figure 6, in the representation space spanned by $|k\rangle$ and $|k_\perp\rangle$, the initial state $|\psi\rangle$ can be written as:

$$|\psi\rangle = \cos\frac{\theta}{2}\,|k\rangle + \sin\frac{\theta}{2}\,|k_\perp\rangle\,.^{16} \tag{34}$$

The action of the oracle O can be visualized as a *reflection* about the vector $|k\rangle$,

$$O\,|\psi\rangle = \cos\frac{\theta}{2}\,|k\rangle - \sin\frac{\theta}{2}\,|k_\perp\rangle\,, \tag{35}$$

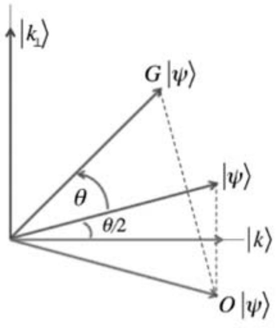

FIGURE 6
Geometrical interpretation of the Grover iterate.

[16] If the search pursues one solution, $\cos\frac{\theta}{2} = \sqrt{\frac{N-1}{N}}$ and $\sin\frac{\theta}{2} = \sqrt{\frac{1}{N}}$. Hence, for large N, we find that $\theta = 2/\sqrt{N}$.

and the operation $(2\,|\psi\rangle\,\langle\psi| - I)$ as a *reflection* about the vector $|\psi\rangle$,

$$G\,|\psi\rangle = \cos\frac{3\theta}{2}\,|k\rangle + \sin\frac{3\theta}{2}\,|k_\perp\rangle\,. \tag{36}$$

Thus the Grover iteration can be broken in *two reflections* about two lines whose angular separation is $\theta/2$. The search is accomplished once $|\psi\rangle$ is taken to $|k_\perp\rangle$.

As we might have expected, the product of two reflections equals a rotation. This double reflection, which can well be regarded as a double projection, seems to act as a sort of 'counter-diagonalization' reducing the number of steps from N to $\sqrt{N}$. The language of quaternions may help to throw light on this point.

In terms of quaternions, the oracle O acts as an imaginary unit, namely as a binary rotation about $|k\rangle$,

$$O = [\,\cos\frac{\pi}{2}, \sin\frac{\pi}{2}\,|k\rangle\,]; \tag{37}$$

the operator $(2\,|\psi\rangle\,\langle\psi| - I)$, in guise of a quaternion, brings about a rotation by 2θ about the axis $\mathbf{n}$, perpendicular to $|k\rangle$,

$$[\,\cos\theta, \sin\theta\,\mathbf{n}] \qquad \Rightarrow \qquad R\,(2\theta\mathbf{n})\,. \tag{38}$$

Therefore, the Grover iterate G acts as a *binary rotation* about $|\psi\rangle$:

$$G = [\,\cos\frac{\pi}{2}, \sin\frac{\pi}{2}\,|\psi\rangle\,], \tag{39}$$

which 'unveils' the vision of the oracle. But, then, the rotation involved in the Grover iterate is by 2θ, not by θ.[17] And the Grover iterate applied n times equals $2n$ rotations by θ.

As to the issue raised by Grover, the reason for accomplishing the search in $O(\sqrt{N})$ steps is that the rotation to be associated with the Grover iterate *doubles* the rotation of the initial state $|\psi\rangle$. Notice that the $|\psi\rangle$ performs both as a polar vector, under the action of the oracle, and as an axial vector, under the Grover iteration. Indeed the *binary* rotation about $|\psi\rangle$ triggered by the Grover iterate equals the binary rotation about $|k\rangle$ triggered by the oracle, followed by a rotation by 2θ towards the solution state $|k_\perp\rangle$. Both the oracle *O and* the Grover iterate G act like mirrors.

To summarize. Quantum theory has been driven to complex space by a search for 'more effective' observability. By focusing on probability relations between incompatible observables, one discovers complex probability

[17] $G = [0, 0\,|\psi\rangle\,] = [\,\cos\theta, \sin\theta\mathbf{n}][0, 0\,|k\rangle\,] \qquad \Rightarrow \qquad R(\pi\,|\psi\rangle\,) = R\,(2\theta\mathbf{n})\,R(\pi\,|k\rangle\,).$

amplitudes. By squaring their modulus, one restores ‘real’ probabilities. Yet the complex character of quantum amplitudes cannot be locked by a strict arithmetic operation. As it demands complex numbers, *i.e.*, numbers involving *binary rotations*, it releases computational paths in a ‘perspectival’ space. Here, the reversible relation between observables, once disclosed through the Alberti’s veil, is preserved in the unitary operators which enable a quantum computer to *see* - not to *measure*! - a solution to a problem faster than a Turing machine. If “Turing machines are humans who calculate”, *quantum* Turing machines are computing agents equipped with looking glasses.

ACKNOWLEDGMENTS

I am indebted to Simon Altmann for delighting and instructing me with his books as well as in conversations, for his comments on the manuscript and his kindness in allowing me to reproduce two illustrations from his book (1992) as Figure 3 in this paper. I am also grateful to Stefano Mancini for urging a more detailed description of the Grover algorithm, and to Annalisa Marzuoli for suggesting a significant change.

REFERENCES

[1] Leon Battista Alberti (1435). *De Pictura*. Basilea 1540. Critical edition by L. Mallé. Florence 1950.

[2] Simon L. Altmann (1986). *Rotations, Quaternions, and Double Groups*. Oxford University Press, Oxford.

[3] Simon L. Altmann (1992). *Icons and Symmetries*. Clarendon, Oxford.

[4] Giuseppe Castagnoli (2010). Quantum Correlation Between the Selection of the Problem and that of the Solution Shades Light on the Mechanism of the Quantum Speed-up. In: *Physical Review A*. **82**.

[5] Gregory Chaitin (2002). *Conversations with a Mathematician. Math, Art, Science and the Limits of Reason*. Springer, Berlin.

[6] Jack B. Copeland (2004). *The Essential Turing*. Clarendon, Oxford.

[7] Martin Davis (1958). *Computability and Unsolvability*. McGraw-Hill, New York.

[8] Solomon Feferman (1998). Deciding the Undecidable: Wrestling with Hilbert’s Problems. In: *In the Light of Logic*. Oxford Univ. Press, Oxford.

[9] Robin Gandy (1980). Church’s Thesis and the Principles for Mechanism. In: John Barwise, Jerome H. Keisler, Kenneth Kunen (eds). *The Kleene Symposium*. North-Holland, Amsterdam.

[10] Herbert Goldstein (1957). *Classical Mechanics*. Addison-Wesley, Reading Mass.

[11] Lov K. Grover (2001). From Schrödinger’s Equation to the Quantum Search Algorithm. In: *Quant-ph/0109116*.

[12] David Hilbert (1927). Die Grundlagen der Mathematik. English trans.: The Foundations of Mathematics. In: Jean van Heijenoort (ed.), *From Frege to Gödel, a Source Book in Mathematical Logic, 1879-1931*. Harvard Univ. Press, Cambridge.

[13] David Hilbert and Stephan Cohn-Vossen (1932). *Anschauliche Geometrie*. English trans.: *Geometry and the Imagination*. Chelsea Publ. Co., New York 1952.

[14] R. I. G. Hughes (1989). *The Structure and Interpretation of Quantum Mechanics*. Harvard Univ. Press, Cambridge Mass.

[15] Morris Kline (1953). *Mathematics in Western Culture*. Oxford Univ. Press, Oxford.

[16] David Mermin (2003). From Cbits to Qubits: Teaching Computer Scientists Quantum Mechanics. In: *American Journal of Physics*, **71**.

[17] Michael A. Nielsen and Isaac L. Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge Univ. Press, Cambridge.

[18] Wilfried Sieg (2002). Calculations by Man and Machine: Mathematical Presentation. In: Peter Gärdenfors, Jan Wolenski, Katarzyna Kijania-Placek (eds). *In the Scope of Logic, Methodology and Philosophy of Science*. Kluwer, Dordrecht.

[19] Wilfried Sieg (2009). On Computability. In: Andrew D. Irvine (ed.). *Handbook of the Philosophy of Mathematics*. Elsevier.

[20] Alan M. Turing (1937). On Computable Numbers with an Application to the *Entscheidungsproblem*. In: *Proceedings of the London Mathematical Society*, Serie 2, **43**. Reprinted in Copeland 2004.

[21] John von Neumann (1927). Zum Hilbertschen Beweistheorie. In: *Mathematische Zeitschrift*, **26**. Reprinted in: *Collected Works*, vol. I. Pergamon Press, Oxford 1961.

[22] Hermann Weyl (1931). *Gruppentheorie und Quantenmechanik*. Methuen and Company, Ltd. English trans.: *The Theory of Groups and Quantum Mechanics*. Dover, New York 1950.

[23] Hermann Weyl (1949). *Philosophy of Mathematics and Natural Sciences*. Princeton Univ. Press, Princeton.

[24] Hermann Weyl (1952). *Symmetry*. Princeton Univ. Press, Princeton.

[25] Anton Zeilinger (2003). *Einstein Schleier. Die neue Welt der Quantenphysick*. Verlag, München.