L&PS – Logic and Philosophy of Science
Vol. X, No. 1, 2012

L&PS – Logic and Philosophy of Science
http://www2.units.it/~episteme
ISSN: 1826-1043

L&PS – Logic & Philosophy of Science
Vol. X, No. 1, 2012, pp. 3-14

T×W Epistemic Modality

Andrea Iacona
Department of Metaphysics and Theory of Knowledge
University of Valencia
andrea.iacona@uv.es

ABSTRACT. So far, T×W frames have been employed to provide a semantics for a language of tense logic that includes a modal operator that expresses historical necessity. The operator is defined in terms of quantification over possible courses of events that satisfy a certain constraint, namely, that of being alike up to a given point. However, a modal operator can as well be defined without placing that constraint. This paper outlines a T×W logic where an operator of the latter kind is used to express the epistemic property of definiteness. Section 1 provides the theoretical background. Sections 2 and 3 set out the semantics. Sections 4 and 5 show, drawing on established results, that there is a sound and complete axiomatization of the logic outlined.

KEYWORDS: time, worlds, epistemic modality.

1. Introduction

This paper originates from some reflections on future contingents. Among those who have attempted to provide a rigorous account of future contingents, there is a widespread tendency to think that the most appropriate formal semantics for

Published by L&PS – Logic and Philosophy of Science
http://www2.units.it/~episteme/ – ISSN: 1826-1043

a tensed language involves branching time structures, that is, structures formed by a set of times and a tree-like partial order defined on the set. This inclination is fostered by two assumptions. One is that indeterminism entails *branching*, that is, the conception according to which there is a plurality of possible courses of events that overlap up to a certain point, the present. The other is that an adequate account of the semantic properties of future contingents hinges on the notion of *determinacy*, understood as truth in all possible courses of events. In a branching time structure, overlapping possible courses of events are represented as maximal linearly ordered subsets of times, and determinacy is expressed in terms of truth at a time relative to all possible courses of events that include that time[1].

However, both assumptions might be rejected. Against the first it may be argued that, at least on a plausible understanding of indeterminism, indeterminism does not entail branching. If determinism is understood as the claim that for any time, the state of the universe at that time is entailed by the state of the universe at previous times together with the laws of nature, and indeterminism is understood as the negation of that claim, then indeterminism is consistent with a conception according to which possible courses of events do not overlap. Possible futures may be conceived as parts of possible worlds that are wholly distinct, rather than branches that depart from a common trunk[2].

The second assumption may be questioned in at least two ways. In the first place, it may be argued that any account of future contingents centred on the notion of determinacy neglects a crucial distinction, namely, that between truth and determinate truth. Suppose that the following sentence is uttered now

(1) It will rain

It is at least consistent to claim that (1) may be true even though it is not determinately true, if it is true in the actual course of events but false in some other possible course of events. Secondly, it may be argued that some of the facts that the notion of determinacy is intended to capture in reality are epistemic facts,

[1] The notion of branching time structure goes back to Kripke, see [9], pp. 27-29.

[2] Hoefer considers a definition of indeterminism along these lines, see [5]. Lewis argues against branching in [8], pp. 206-209. In [7] I discuss the claim that indeterminism entail branching.

hence that an account of them in terms of a formal representation of a state of knowledge is preferable to one that depends on unnecessary metaphysical assumptions. Consider the apparent difference between (1) and the following sentence

(2) Either it will rain or it will not rain.

This difference can be explained epistemically as follows: now we are not able to tell whether (1) is true because as far as we know (1) is true in some but not in all possible courses of events. By contrast, we can confidently assert (2), as (2) seems to be true in all possible courses of events[3].

If the two assumptions are rejected, no strong motivation remains for regarding branching time structures as a privileged formal tool to deal with the issue of future contingents. In particular, if the second assumption is rejected on the basis of considerations about the epistemic nature of facts such as that considered, there seems to be no reason to restrict attention to metaphysical interpretations of formal semantics. This paper explores one of the alternative routes. The model of time that will be outlined, *the grid model*, belongs to the family of T×W semantics, and the interpretation of it that will be considered is epistemic rather than metaphysical[4].

2. The grid model

Let Φ be the set of propositional variables. Our language will be the smallest set including Φ that is closed under composition by means of the propositional connectives and the operators G, H and D. Its semantics is based on the following definition.

DEFINITION 1. *Let T and W be sets. A $\mathscr{G}$-frame is a pair $\langle \{T_w, <_w\}_{w\in W}, \approx\rangle$ that satisfies the following conditions.*

1. *For any $w \in W$, $T_w \subseteq T$. For any $w, w' \in W$ such that $w \neq w'$, $T_w \cap T_{w'} = \emptyset$.*

[3] In [7] I argue for the distinction between truth and determinate truth.

[4] The original formulation of T×W semantics is given by Thomason in [10]. The epistemic interpretation that will be considered develops a suggestion that I advanced in [6].

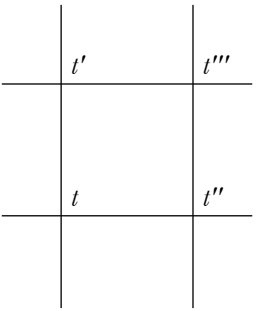

FIG. 1: *The grid of worlds and instants*

2. *For any $w \in W$, $<_w$ is a linear order on T_w. A relation $<$ on T is defined accordingly: for any $t,t' \in T$, $t < t'$ iff there is a w such that $t,t' \in T_w$ and $t <_w t'$.*

3. *$\approx$ is an equivalence relation on T such that (a) for any $t \in T$ and $w \in W$, there is a unique t' such that $t' \in T_w$ and $t \approx t'$, (b) if $t,t' \in T_w, t'',t''' \in T_{w'}, t \approx t'', t' \approx t'''$ and $t <_w t'$, then $t'' <_{w'} t'''$.*

From now on, Dn will abbreviate 'definition n', and D$n.m$ will abbreviate 'clause m of definition n'. The members of T are called times. The members of W are called worlds. So from D1.1 and D1.2 it turns out that worlds are linearly ordered disjoint sets of times. This means that times are world-relative temporal units, in that each time belongs at most to one world. The relation $\approx$ specified in D1.3, by contrast, expresses the trans-world relation of "being at the same time", so induces a partition of times that is orthogonal to their chaining into worlds. To make this clear, the equivalence classes of times determined by $\approx$ may be called "instants", following the terminology adopted by Belnap, Perloff and Xu in [1]. In figure 1, worlds are represented as straight vertical lines that run parallel, whereas instants are represented as straight horizontal lines that cut across them: for example, t and t' belong to the same world, while t and t'' belong to the same instant.

DEFINITION 2. *A $\mathscr{G}$-structure is a triple $\langle \{T_w, <_w\}_{w \in W}, \approx, V\rangle$, where $\langle \{T_w, <_w\}_{w \in W}, \approx\rangle$ is a $\mathscr{G}$-frame and V is a function that assigns a truth-value to each*

formula α *for any time* t *in the following way:*

1. $V_t(\alpha) \in \{1,0\}$ *for* $\alpha \in \Phi$.
2. $V_t(\sim \alpha) = 1$ *iff* $V_t(\alpha) = 0$.
3. $V_t(\alpha \supset \beta) = 1$ *iff* $V_t(\alpha) = 0$ *or* $V_t(\beta) = 1$.
4. $V_t(G\alpha) = 1$ *iff for every* t' *such that* $t < t'$, $V_{t'}(\alpha) = 1$.
5. $V_t(H\alpha) = 1$ *iff for every* t' *such that* $t' < t$, $V_{t'}(\alpha) = 1$.
6. $V_t(D\alpha) = 1$ *iff for every* t' *such that* $t \approx t'$, $V_{t'}(\alpha) = 1$.

D2.1-D2.3 are standard. D2.4 and D2.5 specify the meaning of G and H, read as 'henceforth' and 'hitherto'. D2.6 characterizes D, read as 'definitely'. D differs from G and H in a way that is easy to grasp visually. G and H ask you to move along the vertical axis and go up or down on the same world, while D asks you to move along the horizontal axis and go left and right on the same instant[5].

Other symbols may be added to the language on the basis of D2. $\wedge$ and $\vee$ depend on $\sim$ and $\supset$ in the usual way. Two operators F and P may be defined in terms of G and H as follows: $F\alpha \equiv \sim G \sim \alpha$ and $P\alpha \equiv \sim H \sim \alpha$. Similarly, an operator C may be defined in terms of D as follows: $C\alpha \equiv \sim D \sim \alpha$. Truth in a structure and validity are defined in the standard way:

DEFINITION 3. α *is true in a* $\mathscr{G}$*-structure iff for any* t, $V_t(\alpha) = 1$.

DEFINITION 4. α *is valid, that is,* $\models \alpha$, *iff* α *is true in all* $\mathscr{G}$*-structures.*

The semantics outlined is a kind of T×W semantics. In particular, the version of T×W semantics that best suits the present purposes is that provided by Kutschera in [11]. Kutschera defines a STW frame as a triple $\langle \{T_w, <_w\}_{w \in W}, \approx, \sim \rangle$, where the first two terms satisfy the conditions specified in D1 and $\sim$ is an equivalence relation that differs from $\approx$ in that it is designed to express historical necessity. So $\mathscr{G}$-frames are nothing but STW frames without that relation[6].

[5] A modal operator defined in terms of unrestricted quantification over worlds, like D, was first considered by Di Maio and Zanardo in [2].

[6] The letter S in STW stands for 'separated', to distinguish STW frames from standard T×W frames as defined by Thomason in [10]. In [11], Kutschera shows that for every T×W structure there is an equivalent STW structure, and vice versa, see p. 243.

3. The epistemic interpretation

On the interpretation of the grid model that will be considered, times designate epistemically possible global states of affairs, and worlds are understood as epistemically possible courses of events. The underlying thought is that, for every sentence 'p' such that we are not in a position to know that p, there are at least two worlds: one in which p and one in which it is not the case that p. For example, today we are not in a position to know whether it will rain tomorrow. So there are at least two worlds: one in which it rains tomorrow and one in which it doesn't.

The use of the expression 'in a position to know' presupposes that a meaningful distinction can be drawn between knowing that p and being in a position to know that p. Being in a position to know that p, like knowing that p, is factive: if one is in a position to know that p, then it is true that p. But the two states are not exactly the same. While knowing that p entails being in a position to know that p, being in a position to know that p does not entail knowing that p: one may be in a position to know that p without knowing that p, just like one may fail to see something that is in front of one's eyes[7].

Note that the differences between epistemically possible courses of events are not limited to the future. For example, we are not in a position to know whether the number of cats that slept inside the Colosseum on September 4th 1971 is even or odd. So there are at least two worlds: one in which that number is even, the other in which that number is odd. The same goes for the present. For example, we don't know the exact location of a certain whale that is now swimming in the ocean, so we are not able to discriminate between times that differ as to the location of that whale. The absence of a unique present time is a key feature of the grid model. In figure 1 there is no point that indicates where you are. The reason is that you don't know exactly where you are, in that you don't know which of the two worlds is your world. What allows you to locate yourself on the diagram is a line rather than a point, that is, an instant.

On the epistemic interpretation, D expresses truth in all epistemically possi-

[7] Williamson provides a characterization of the distinction along these lines, see [12], p. 95. In any case, nothing substantial will depend on this distinction. The underlying thought of the epistemic interpretation could equally be rephrased as follows: for every sentence 'p' such that we don't know that p, there are at least two worlds: one in which p and one in which it is not the case that p.

ble courses of events. To say that it is definitely the case that p is to say that one is in a position to know that p. For example, the apparent difference between (1) and (2) may be explained in terms of definiteness. Consider figure 1. If p is true at t' but false at t''', then DFp is false at t, while $D(Fp \vee \sim Fp)$ is true at t.

The operator C is construed accordingly. To say that one is in a position to know that p is to say that every epistemically possible course of events is such that p. Therefore, if one is not in a position to know that it is not the case that p, then one is not in a position to exclude that p, that is, some epistemically possible course of events is such that p.

4. Axiomatization

T×W logic has been shown to be complete under two axiomatizations. One is the finite axiomatization adopted by Kutschera in [11], which includes the irreflexivity rule introduced by Gabbay in [4]. The other is the infinite axiomatization adopted by Di Maio and Zanardo in [3], which is free from that rule. The system outlined here follows Kutschera, for the completeness proof is simpler with the irreflexivity rule. But a similar system could be constructed in terms of the other axiomatization.

Let S be a system whose axioms include the standard propositional axioms and the following:

A1 $G(\alpha \supset \beta) \supset (G\alpha \supset G\beta)$

A2 $H(\alpha \supset \beta) \supset (H\alpha \supset H\beta)$

A3 $\alpha \supset HF\alpha$

A4 $\alpha \supset GP\alpha$

A5 $G\alpha \supset GG\alpha$

A6 $F\alpha \supset G(F\alpha \vee \alpha \vee P\alpha)$

A7 $P\alpha \supset H(F\alpha \vee \alpha \vee P\alpha)$

A8 $D\alpha \supset \alpha$

A9 $D(\alpha \supset \beta) \supset (D\alpha \supset D\beta)$

A10 $C\alpha \supset DC\alpha$

A11 $DG\alpha \supset GD\alpha$

A12 $DH\alpha \supset HD\alpha$

A13 $FD\alpha \supset DF\alpha$

A14 $PD\alpha \supset DP\alpha$

A1-A7 are standard axioms of linear tense logic. A1-A2 state that distribution holds for G and H. A3-A4 ensure that G and H depend on accessibility relations that are converse to each other. A5 expresses the transitivity of $<$. A6 rules out branching to the future, while A7 rules out branching to the past.

A8-A10 characterize D as a modal operator. A8 expresses a platitude, as it amounts to saying that being in a position to know is factive. A9 is easily justified. If one is in a position to know that if p then q and one is in a position to know that p, then one must be in a position to know that q. For all that is needed to get to the conclusion that q is to apply a valid rule of inference. A10 entails that if for all one knows it could be the case that p, then one is in a position to know that for all one knows it could be the case that p. This is quite plausible. Suppose that one is not in a position to know that it is not the case that p. Then, presumably, the negation of p does not hold in all possible courses of events in virtue of some logical principle, and one is in a position to know that.

A11-A14 state a connection between G, H, F and P on the one hand, and D on the other. According to A11, if it is knowable that from now on it will be the case that p, then from now on it will be knowable that p. This is acceptable if one thinks that the antecedent of the conditional is satisfied only for those truths that hold at any time. For example, it is true at any time in every epistemically possible course of events that if it rains then it rains. Thus, it is knowable that from now on if it rains then it rains. But if so then the consequent is satisfied, that is, from now on it will be knowable that if it rains then it rains. The motivation for A12-A14 is similar.

Let $\vdash$ stand for derivability in S. The rules of inference of S are the following:

R1 If $\vdash \alpha \supset \beta$ and $\vdash \alpha$, then $\vdash \beta$

R2 If $\vdash \alpha$, then $\vdash G\alpha$ and $\vdash H\alpha$

R3 If $\vdash \alpha$, then $\vdash D\alpha$

R4 If $\vdash D(\sim p \wedge Gp) \supset \alpha$, then $\vdash \alpha$, where p is a propositional variable that does not occur in α

R1 is *modus ponens*, R2 is temporal generalization, while R3 amounts to the rule of necessitation. R4 is the version of Gabbay's irreflexivity rule used by Kutschera.

5. Soundness and Completeness

S is sound. It is straightforward to verify that A1-A14 are valid and R1-R4 preserve validity. The completeness of S can be proved through the method used by Kutschera for a system called TW. Kutschera defines STW systems as sets of maximal consistent sets of formulas endowed with a relational structure, and shows that STW systems induce STW structures. Thus, in order to prove that TW is complete it suffices to show that for every formula that is not a theorem of TW there is a STW system that includes its negation, for that in turn entails the existence of a STW structure in which the formula is not true at some time. Here a proof will be provided to the effect that STW systems induce $\mathscr{G}$-structures. So the completeness of S will be obtained in the same way, using von Kutschera's result about the existence of a STW system.

Let us grant Kutschera's definition of STW systems. To abbreviate, 'mcs' will stand for 'maximal consistent set of formulas'. The relation R_G is defined as follows: if S and S' are mcss, SR_GS' iff $G(S) \subseteq S'$, where $G(S) = \{\alpha : G\alpha \in S\}$. The relations R_H and R_D are defined in similar way. If S and S' are mcss, SR_HS' iff $H(S) \subseteq S'$, where $H(S) = \{\alpha : H\alpha \in S\}$. If S and S' are mcss, SR_DS' iff $D(S) \subseteq S'$, where $D(S) = \{\alpha : D\alpha \in S\}$. R_G and R_H are transitive, while R_D is an equivalence relation.

DEFINITION 5. *A STW system is a pair* $\langle \{S_t\}_{t\in T}, \{T_w\}_{w\in W} \rangle$ *defined as follows.*

1. *W is set of indices.*

2. *The sets T_w are disjoint, and T is the union of them.*

3. *For every $t \in T$, S_t is a mcs. Each $t \in T$ has its own mcs, so if $t \neq t'$ then $S_t \neq S_{t'}$.*

4. *For every $w \in W$ and $t \in T_w$, if $F\alpha \in S_t$ then there is a $t' \in T_w$ such that $S_t R_G S_{t'}$ and $\alpha \in S_{t'}$. The same goes for P and R_H. The case of C and R_D is similar, but without the condition that $t' \in T_w$.*

5. *For every $t, t' \in T_w$, either $S_t = S_{t'}$ or $S_t R_G S_{t'}$ or $S_{t'} R_G S_t$.*

6. *For every $t \in T$ and for some propositional variable p, $D(\sim p \wedge Gp) \in S_t$.*

7. *For every $w, w' \in W$ and every $t \in T_w$, there is a $t' \in T_{w'}$ such that $S_t R_D S_{t'}$.*

Let it be granted that $t <_w t'$ iff $t, t' \in T_w$ and $S_t R_G S_{t'}$, and that $t \approx t'$ iff $S_t R_D S_{t'}$. Now it will be shown that for every STW system there is a correspondent $\mathscr{G}$-structure.

THEOREM 1. *If $\langle \{S_t\}_{t \in T}, \{T_w\}_{w \in W} \rangle$ is a STW system, then $\langle \{T_w, <_w\}_{w \in W}, \approx \rangle$ is a $\mathscr{G}$-frame.*

PROOF. D1.1 follows from D5.2. D1.2 follows from D5.5. To see that D1.3 is satisfied, consider condition (a) first. The existence of t' is entailed by D5.7. The uniqueness of t' is shown as follows. Suppose that $t, t' \in T_w$ and $t \approx t'$. From D5.5 we get that either $S_t = S_{t'}$ or $S_t R_G S_{t'}$ or $S_{t'} R_G S_t$. But the second disjunct cannot hold, because from D5.6 we get that $Gp \in S_t$, hence that $p \in S_{t'}$. Since we also have that $D \sim p \in S_t$, hence that $\sim p \in S_{t'}$ because $t \approx t'$, we get that both $p \in S_{t'}$ and $\sim p \in S_{t'}$, which contradicts D5.3. A similar reasoning shows that the third disjunct cannot hold. Therefore, $S_t = S_{t'}$.

Now consider condition (b). Suppose that $t, t' \in T_w$, $t'', t''' \in T_{w'}$, $S_t R_D S_{t''}$, $S_{t'} R_D S_{t'''}$ and $S_t R_G S_{t'}$. From D5.5 we get that either $S_{t''} = S_{t'''}$ or $S_{t''} R_G S_{t'''}$ or $S_{t'''} R_G S_{t''}$. But the first disjunct cannot hold. D5.6 entails that $D(\sim p \wedge Gp) \in S_t$, hence that $\sim p \in S_{t''}$. Since we also have that $DGp \in S_t$, A11 entails that $GDp \in S_t$, hence that $Dp \in S_{t'}$ and consequently that $p \in S_{t'''}$. Therefore, the first disjunct contradicts D5.3. The third disjunct leads to a similar conclusion. For D5.6 entails that $D(\sim p \wedge Gp) \in S_t$, hence that $\sim p \in S_{t''}$. Since D5.6, in combination with A5, also entails that $DGGp \in S_t$, by A11 we get that $GDGp \in S_t$, and consequently that $DGp \in S_{t'}$. Since $S_{t'} R_D S_{t'''}$, it follows that $Gp \in S_{t'''}$. So if it were the case that $S_{t'''} R_G S_{t''}$, we would get that $p \in S_{t''}$. Therefore, $S_{t''} R_G S_{t'''}$. □

THEOREM 2. *For each STW system* $\langle \{S_t\}_{t\in T}, \{T_w\}_{w\in W}\rangle$ *there is a* $\mathscr{G}$*-structure* $\langle \{T_w, <_w\}_{w\in W}, \approx, V\rangle$ *such that, for every* α, $V_t(\alpha) = 1$ *iff* $\alpha \in S_t$.

PROOF. Let $\langle \{S_t\}_{t\in T}, \{T_w\}_{w\in W}\rangle$ be a STW system. Theorem 1 entails that $\langle \{T_w, <_w\}_{w\in W}, \approx\rangle$ is a $\mathscr{G}$-frame. A function V can be defined on the frame in accordance with D2, assuming that, for each α in Φ, $V_t(\alpha) = 1$ iff $\alpha \in S_t$. This way it can be shown by induction on the complexity of α that for every α, $V_t(\alpha) = 1$ iff $\alpha \in S_t$. The case of $\sim\alpha$ and $\alpha \supset \beta$ is trivial. Consider the case of $G\alpha$. Let us assume that $V_t(\alpha) = 1$ iff $\alpha \in S_t$, and suppose that $V_t(G\alpha) = 1$. From D2.4 we get that for t' such that $t < t'$, $V_{t'}(\alpha) = 1$. Since $t < t'$ iff $S_t R_G S_{t'}$, $G\alpha \in S_t$ if $\alpha \in S_{t'}$. So $G\alpha \in S_t$. Now suppose that $G\alpha \in S_t$. Since $t < t'$ iff $S_t R_G S_{t'}$, for every t' such that $t < t'$ we get that $\alpha \in S_{t'}$, hence that $V_{t'}(\alpha) = 1$. So D2.4 entails that $V_t(G\alpha) = 1$. The case of $H\alpha$ and $D\alpha$ is similar. Therefore, $\langle \{T_w, <_w\}_{w\in W}, \approx, V\rangle$ is a $\mathscr{G}$-structure such that, for every α, $V_t(\alpha) = 1$ iff $\alpha \in S_t$. □

Kutschera proves that if a formula is not a theorem of TW, there is a STW system $\langle \{S_t\}_{t\in T}, \{T_w\}_{w\in W}\rangle$ such that for some $t \in T$, the negation of the formula belongs to S_t. A similar result holds for S, that is,

THEOREM 3. *If it is not the case that* $\vdash \alpha$, *then there exists a STW system* $\langle \{S_t\}_{t\in T}, \{T_w\}_{w\in W}\rangle$ *such that for some* $t \in T$, $\sim\alpha \in S_t$.

PROOF. In [11], pp. 246-247, Kutschera shows how theorem 3 can be proved in two steps. First, Gabbay's irreflexivity lemma can be used to show that if it is not the case that $\vdash \alpha$, then there is a set $\{S_t\}_{t\in T}$ that satisfies certain conditions and a t_0 such that $\sim\alpha \in S_{t_0}$ (theorem 4.1). S is like TW in this respect, as it includes the rule R4, which is required by the proof. Second, a STW system can be constructed from $\{S_t\}_{t\in T}$ by defining a set of $\{T_w\}_{w\in W}$ (theorem 4.2). Again, S is like TW in this respect, as it includes the axioms used in the proof. □

THEOREM 4. *If* $\models \alpha$ *then* $\vdash \alpha$.

PROOF. From theorems 2 and 3 it follows that if is not the case that $\vdash \alpha$, then there is a $\mathscr{G}$-structure such that $V_t(\alpha) = 0$ at some t. □

REFERENCES

[1] N. Belnap, M. Perloff, and M. Xu. *Facing the Future*. Oxford University Press, 2001.

[2] C. Di Maio and A. Zanardo. Synchronized histories in prior-thomason representation of branching time. In D. Gabbay and H. Ohlbach, editors, *Proceedings of the first international conference on temporal logic*, pages 265–282. Springer, 1994.

[3] C. Di Maio and A. Zanardo. A Gabbay-rule free axiomatization of T×W validity. *Journal of Philosophical Logic*, 27:435–487, 1998.

[4] D. Gabbay. An irreflexivity lemma with applications to axiomatization of conditions on tense frames. In U. Mönnich, editor, *Aspects of philosophical logic*. Reidel, 1981.

[5] C. Hoefer. Causal determinism. In E. Zalta, editor, *The Stanford Encyclopedia of Philosophy (Spring 2010 Edition)*. URL http://plato.stanford.edu/archives/spr2010/entries/determinism-causal/.

[6] A. Iacona. Commentary on R. Thomason,'Combinations of tense and modality'. *Humana.Mente*, 8:185–190, 2009.

[7] A. Iacona. Timeless truth. In F. Correia and A. Iacona, editors, *Around the Tree: Semantic and Metaphysical Issues concerning Branching and the Open Future*. Springer, 2013. Forthcoming.

[8] D. Lewis. *On the Plurality of Worlds*. Blackwell, 1986.

[9] A. N. Prior. *Past, Present and Future*. Clarendon Press, 1967.

[10] R. H. Thomason. Combinations of tense and modality. In D. Gabbay and G. Guenthner, editors, *Handbook of Philosophical Logic*, volume 2, pages 135–165. Reidel, 1984.

[11] F. von Kutschera. T×W Completeness. *Journal of Philosophical Logic*, 26:241–250, 1997.

[12] T. Williamson. *Knowledge and its limits*. Oxford University Press, 2000.

L&PS – Logic & Philosophy of Science
Vol. X, No. 1, 2012, pp. 15-30

A Self-contained Proof of the Standard Completeness in HW-algebras

Martinvaldo Konig
University of Cagliari, via Is Mirrionis 1, I-09123 Cagliari
martinvk@iol.it

ABSTRACT. This paper has a survey-character and studies many-valued logic endowed with two different kinds of implication: Łukasiewicz's implication and Gödel's implication. We focus on the class of algebras containing the algebraic counterpart of this new logic: the class of Heyting Wajsberg algebras. We introduce a new direct Chang-style proof of subdirect representation and standard algebraic completeness theorem.

KEYWORDS: Bounded distributive lattice, MV-algebra, HW-algebra, filter, subdirect product, standard algebraic completeness, l-group first order theory.

1. Introduction

The contribution of this paper is mainly taxonomic and aims to complete the study of Gödel Łukasiewicz Logic in [13]. There is an important connection between any logical calculus S and the class of adequate models for it – i.e. the class of algebraic structures which verify exactly the provable formulae of S. For instance Boolean algebras are the algebraic counterpart of classical propositional logic and Heyting algebras correspond to intuitionistic propositional logic (see pp. 380-3 in [10]).

Published by L&PS – Logic and Philosophy of Science
http://www2.units.it/~episteme/ – ISSN: 1826-1043

Heyting Wajsberg algebras were introduced by Giampiero Cattaneo and Davide Ciucci in [2] and have two different implications as primitive operators: Łukasiewicz's implication and Gödel's implication [11]. By the composition of the two primitive operators with the **0**-element it is possible to define two different negations and the modal operators of necessity and possibility. Moreover the equational theory of the variety of Heyting Wajsberg algebras is capable to contain both the equational theory of Heyting algebras and the one of Wajsberg algebras [13]. Wajsberg algebras are proven to be termwise equivalent to MV-algebras (section 4.2 in [9]). Then the logical calculus whose algebraic counterpart is the class of Heyting Wajsberg algebras (i.e. Gödel Łukasiewicz Logic [13]) results to be an extension of both intuitionistic logic and of Łukasiewicz many-valued logic (i.e. the logical systems arising from Heyting and MV-algebras). Furthermore, in [13] Gödel Łukasiewicz Logic is shown to be decidable, to have the deduction-detachment theorem and to be strongly complete.

All these results hold with the necessary support of the standard completeness theorem. Up to now, the standard completeness of Heyting Wajsberg algebras has been obtained indirectly by the equivalence proven in [4] between Heyting Wajsberg algebras and other algebraic structures, for instance MVΔ-algebras (Theorem 3.2.13 in [12]). The main contribution of this paper is to give a direct proof of the standard completeness theorem for Heyting Wajsberg algebras in a traditional Chang-like style.

In section 2 the basic notions and properties of this algebraic structure are introduced. In section 3 I introduce a suitable extension of the definition of implicative filter and show that any Heyting Wajsberg algebra is isomorphic to a subdirect product of linear Heyting Wajsberg algebras. Finally, in section 4 I prove the whole variety of Heyting Wajsberg algebras to be generated by the real unit interval model. It is worth reminding that from the logical point of view this result entails that in Gödel Łukasiewicz Logic any tautology is provable.

2. Basic notions

Definition 2.1. Let $\mathscr{A} = \langle A, \to_L, \to_G, \mathbf{0}\rangle$ be an algebraic structure of type $\langle 2,2,0\rangle$. $\mathscr{A}$ is a *Heyting Wajsberg algebra* (briefly HW-algebra) if for any $x, y, z \in A$, once defined

$$\begin{gathered}\neg x := x \to_L 0\\ \sim x := x \to_G 0\\ x \wedge y := \neg((\neg x \to_L \neg y) \to_L \neg y)\\ x \vee y := (x \to_L y) \to_L y\\ \mathbf{1} := \neg \mathbf{0}\end{gathered}$$

the following identities are satisfied:

(HW1) $x \to_G x = \mathbf{1}$

(HW2) $x \to_G (y \wedge z) = (x \to_G z) \wedge (x \to_G y)$

(HW3) $x \wedge (x \to_G y) = x \wedge y$

(HW4) $(x \vee y) \to_G z = (x \to_G z) \wedge (y \to_G z)$

(HW5) $\mathbf{1} \to_L x = x$

(HW6) $x \to_L (y \to_L z) = \neg(x \to_L z) \to_L \neg y$

(HW7) $\neg \sim x \to_L \sim\sim x = \mathbf{1}$

(HW8) $(x \to_G y) \to_L (x \to_L y) = \mathbf{1}$

It is useful to define also the following operators:

$$\begin{gathered}x \oplus y := \neg x \to_L y\\ x \odot y := \neg(\neg x \oplus \neg y)\\ \flat x := \neg \sim \neg x\\ x \oslash y := x \oplus \neg y\end{gathered}$$

We assume familiarity with the basic notions of MV-algebra and its main properties. Any of them can be found by the readers in [9]. Moreover any HW-algebra $\mathscr{A} = \langle A, \to_L, \to_G, \mathbf{0}\rangle$ has the MV-algebra $\mathscr{A}^\star = \langle A, \oplus, \neg, \mathbf{0}\rangle$ as term reduct and any HW-algebra $\mathscr{A} = \langle A, \to_L, \to_G, \mathbf{0}\rangle$ has the bounded distributive lattice $\mathscr{A}^{\star\star} = \langle A, \wedge, \vee, \mathbf{0}, \mathbf{1}\rangle$ as term reduct ([4],[3]).

It is also shown in [4] (proposition 1.1) that the natural partial order $\leq$ defined by $\wedge$ or $\vee$ (*i.e.* $x \leq y := x \wedge y = x$ or $x \leq y := x \vee y = y$) has the following property:

$$x \leq y \Leftrightarrow x \to_L y = \mathbf{1} \Leftrightarrow x \to_G y = \mathbf{1}$$

Remark 1. Any linear MV-algebra can be enriched in a natural way with a new unary operator in order to have a HW-algebra term reduct.

Proof. By [4] any HW-algebra is termwise equivalent to a Stonean MV-algebra. An MV-algebra is Stonean when there can be defined a Stonean negation (see also [5]). Any linear MV-algebra is trivially Stonean once defined the Stonean negation $\sim$:

$$\sim x = \begin{cases} \mathbf{0} & \text{if } x \neq \mathbf{0} \\ \mathbf{1} & \text{if } x = \mathbf{0} \end{cases}$$

Then any linear MV-algebra enriched in such a way has a HW-algebra term reduct. □

In the sequel we'll adopt the following notation. Given a HW-algebra $\mathscr{A}$, $\forall x \in A$ and $\forall n \in N$:

$$nx = \begin{cases} \mathbf{0} & \text{if } n = 0 \\ x & \text{if } n = 1 \\ \underbrace{x \oplus \ldots \oplus x}_{n-times}, & \text{if } 2 \leq n \in N \end{cases}$$

and

$$x^n = \begin{cases} \mathbf{1} & \text{if } n = 0 \\ x & \text{if } n = 1 \\ \underbrace{x \odot \ldots \odot x}_{n-times}, & \text{if } 2 \leq n \in N \end{cases}$$

A HW-algebra $\mathscr{A}$ is *linear (or totally ordered)* iff for any pair of elements $x, y \in A$, either $x \leq y$ or $y \leq x$.

Now we introduce the most important example of HW-algebra, the model we will prove at the end of this article to generate the whole variety of HW-algebras.

Example 1 (Standard HW-algebra)**.** $\mathscr{A}_{[0,1]} = \langle [0,1], \to_L, \to_G, 0 \rangle$ where:

$$[0,1] \subset R,$$

$$x \to_L y := \begin{cases} 1 & \text{if } x \leq y \\ 1 - x + y & \text{otherwise} \end{cases},$$

and

$$x \to_G y := \begin{cases} 1 & \text{if } x \leq y \\ y & \text{otherwise} \end{cases}.$$

We recall some important basic results that will be useful in the sequel below.

Lemma 2.1. Let $\mathscr{A}$ be a HW-algebra and $x \in A$. Then
(i) $\sim\sim x = \neg \sim x$
(ii) $x \wedge \sim x = \mathbf{0}$ $\quad x \vee \flat x = \mathbf{1}$
(iii) $x \leq \sim\sim x$ $\quad \flat\flat x \leq x$
(iv) $x \leq y \quad \Rightarrow \quad \sim y \leq \sim x, \flat y \leq \flat x$

Proof. (i) is the interconnection rule ((in)p. 336 in [3]) and can be derived from (HW7) and (HW8) (see Proposition 4.6 in [3]). In (ii) we find B3 (p. 336) and its dual AB4 (p.337) of [3]. (iii) is SBL$_\neg$2 (p. 347, [3]) and AB1 (p. 337, [3]). (iv) is (B2b) p. 335 in [3] and its dual.

□

Lemma 2.2. Let $\mathscr{A}$ be a HW-algebra and $x, y \in A$. Then
(i) $\sim (x \wedge y) = \sim x \vee \sim y$ $\quad \flat(x \vee y) = \flat x \wedge \flat y$
(ii) $\sim (x \vee y) = \sim x \wedge \sim y$ $\quad \flat(x \wedge y) = \flat x \vee \flat y$

Proof. (i) is reported B2a (p. 335) and its dual AB3 (p. 337) in [3]. (ii) is B2 (p. 335) and its dual AB2 (p. 337) in [3].

□

Lemma 2.3. Let $\mathscr{A}$ be a HW-algebra and $x, y \in A$. Then
(i) $\sim (x \oplus y) = \sim x \odot \sim y$ $\quad \flat(x \odot y) = \flat x \oplus \flat y$
(ii) $x \wedge \sim y = x \odot \sim y$ $\quad x \vee \flat y = x \oplus \flat y$
(iii) $x \vee \sim y = x \oplus \sim y$ $\quad x \wedge \flat y = x \odot \flat y$
(iv) $\sim x \oplus \sim x = \sim x \odot \sim x = \sim x$

Proof. (i), (ii) and (ii) are (v) and (iii) with duals in Lemma 1.1, p. 361 in [4]. (iv) follows directly from (iii).

□

Corollary 2.1. Let $\mathscr{A}$ be a HW-algebra and $x, y \in A$. Then
(i) $\sim\sim (x \oplus y) = \sim (\sim x \odot \sim y) = \sim\sim x \oplus \sim\sim y$
(ii) $\flat\flat(x \odot y) = \flat(\flat x \oplus \flat y) = \flat\flat x \odot \flat\flat y$

Proof. (ii) By Lemma 2.3 (i) $\flat\flat(x \odot y) = \flat(\flat x \oplus \flat y)$. By Lemma 2.3 $(ii), (iii)$ and Lemma 2.2 (i), $\flat(\flat x \oplus \flat y) = \flat(\flat x \vee \flat y) = \flat\flat x \wedge \flat\flat y = \flat\flat x \odot \flat\flat y$. (i) is dual.

□

3. Subdirect representation

Definition 3.1. A *filter* F of a HW-algebra $\mathscr{A}$ is a subset of A which satisfies the following conditions:

(F1) $\mathbf{1} \in F$

(F2) if $x \in F$ and $x \leq y$, then $y \in F$

(F3) if $x \in F$ and $y \in F$, then $x \odot y \in F$

(F4) if $x \in F$ then $\flat\flat x \in F$

Notice that the filter defined above is an implicative MV-filter (Definition 4.2.6, p. 86 [9]) plus the additional condition F4. Then any MV-filter F can be extended naturally in a filter $F^\star$ in the following trivial way:

$$F^\star := \{x \in A \mid \exists y \in F : x \geq \flat\flat y\}$$

It has to be also noticed that $F^\star$ is trivially the smallest HW-filter containing F.

Definition 3.2. A filter F of a HW-algebra $\mathscr{A}$ is *proper* iff $\mathbf{0} \notin F$.

Definition 3.3. Let $\mathscr{A}=\langle A, \to_L, \to_G, \mathbf{0}\rangle$ be a HW-algebra, let F be a filter of $\mathscr{A}$ and $x \in F$. We introduce the definition of *filter generated by* $F \cup \{x\}$, denoted $Fi(F \cup \{x\}) := \{y \in A \mid y \leq i \odot x^n$, for some $i \in F$ and some $n \in N\}$. Further the *filter generated by* x, denoted $Fi(x) :=$ the filter generated by $\{\mathbf{1}\} \cup \{x\}$.

Definition 3.4. A filter J of a HW-algebra $\mathscr{A}$ is *maximal* iff it is proper and for any filter F of $\mathscr{A}$ s.t. $J \subseteq F$, either $F = J$ or $F = A$.

Definition 3.5. A filter J of a HW-algebra $\mathscr{A}$ is *prime* iff it is proper and if for any pair of elements $x, y \in A$, either $x \oslash y \in J$ or $y \oslash x \in J$.

It can be noticed that in general $\{\mathbf{1}\}$ is a non-prime filter.

Definition 3.6 (Distance function on a HW-algebra $\mathscr{A}$)**.** Let $x, y \in A$, $q(x,y) := (x \oslash y) \odot (y \oslash x)$.

Definition 3.7. Let F be a filter of a HW-algebra $\mathscr{A}$, $\forall x, y \in A$:

$x \equiv_F y \Leftrightarrow q(x,y) \in F$.

In order to prove $\equiv_F$ to be a congruence relation we need to prove the following lemma.

Lemma 3.1. Let F be a filter of a HW-algebra $\mathscr{A}$ and let $x,y \in A$, if $x \oplus y \in F$ then $\flat\flat x \oplus \flat\neg y \in F$.

Proof. By Lemma 2.1 (i) and (iii) $y \leq \sim\sim y = \neg \sim y = \flat\neg y$ and thus, by monotonicity, $x \oplus y \leq x \oplus \flat\neg y \in F$. By Lemma 2.3 (ii) $x \oplus \flat\neg y = x \vee \flat\neg y \in F$. By F4 $\flat\flat(x \vee \flat\neg y) \in F$. Hence, by Lemma 2.2 (i) and (ii), $\flat\flat x \vee \flat\flat\flat\neg y = \flat\flat x \vee \flat\neg y \in F$. Since in any MV-algebra and then in any HW-algebra $x \vee y \leq x \oplus y$ we obtain $\flat\flat x \oplus \flat\neg y \in F$.

□

Theorem 3.1. Let F be a filter of a HW-algebra $\mathscr{A}$, $\forall x,y \in A$: $x \equiv_F y$ is a congruence relation on $\mathscr{A}$.

Proof. First we prove that $\equiv_F$ is an equivalence relation. $\equiv_F$ is trivially symmetric and since any HW-algebra defines an MV-algebra $\mathscr{A}^\star = \langle A, \oplus, \neg, \mathbf{0}\rangle$ and in any MV-algebra $x \oplus \neg x = \mathbf{1} = \mathbf{1} \odot \mathbf{1} \in F$ we have $\equiv_F$ is reflexive. To prove transitivity we have just to prove $q(x,z) \geq q(x,y) \odot q(y,z)$. We assume familiarity with MV-algebra and lattice properties. $\mathbf{0} = y \odot \neg y \geq (y \wedge z) \odot (\neg y \wedge \neg x) = z \odot (\neg z \oplus y) \odot \neg x \odot (x \oplus \neg y)$. Thus $\neg(x \oslash z) \odot (x \oslash y) \odot (y \oslash z) = \mathbf{0}$. By Lemma 1.1.2 in [9] (p. 9) in any MV-algebra and then in any HW-algebra $\neg y \odot x = \mathbf{0} \Leftrightarrow y \geq x$. It follows $(x \oslash z) \geq (x \oslash y) \odot (y \oslash z)$. Analogously we obtain $(z \oslash x) \geq (y \oslash x) \odot (z \oslash y)$. Then by monotonicity we have $(x \oslash z) \odot (z \oslash x) \geq (x \oslash y) \odot (y \oslash z) \odot (y \oslash x) \odot (z \oslash y)$ that is $q(x,z) \geq q(x,y) \odot q(y,z)$. Since in [4] (Theorem 2.5 and 2.6) it is proven $x \to_G y = \sim (x \odot \neg y) \oplus y$, $x \to_L y = \neg x \oplus y = \neg(x \odot \neg y)$ and since $\sim x = \neg\flat\neg x$, in order to prove $\equiv_F$ preserves $\to_G$ and $\to_L$ we have just to show that $\equiv_F$ preserves $\neg$, $\flat$ and $\odot$. By $\neg\neg x = x$ we have trivially that $q(x,y) = q(\neg x, \neg y)$ and $\equiv_F$ preserves $\neg$. About $\odot$ to prove $x \equiv_F y$ and $s \equiv_F t$ implies $x \odot s \equiv_F y \odot t$, by F2 and F3 we have just to show that $q(x \odot s, y \odot t) \geq q(x,y) \odot q(s,t)$. $\mathbf{0} = x \odot s \odot \neg(x \odot s) \geq \neg(x \odot s) \odot x \odot (\neg x \oplus y) \odot s \odot (\neg s \oplus t) = \neg(x \odot s) \odot (x \wedge y) \odot (s \wedge t) = \neg(x \odot s) \odot y \odot (\neg y \oplus x) \odot t \odot (\neg t \oplus s) = \neg(x \odot s) \odot y \odot t \odot (x \oslash y) \odot (s \oslash t) = \neg((x \odot s) \oslash (y \odot t)) \odot (x \oslash y) \odot (s \oslash t) = \mathbf{0}$. By Lemma 1.1.2 in [9] (p.9) in any MV-algebra and then in any HW-algebra $\neg y \odot x = \mathbf{0} \Leftrightarrow y \geq x$. This means $(x \odot s) \oslash (y \odot t) \geq (x \oslash y) \odot (s \oslash t)$. Analogously we obtain $(y \odot t) \oslash (x \odot s) \geq (y \oslash x) \odot (t \oslash s)$. By monotonicity we have $q(x \odot s, y \odot t) \geq q(x,y) \odot q(s,t)$. Now we show how $\equiv_F$ preserves $\flat$: $q(x,y) \in F \Rightarrow q(\flat x, \flat y) \in F$. If $(x \oslash y) \odot (y \oslash x) \in F$ then $(x \oplus \neg y) \in F$ and $(y \oplus \neg x) \in F$. By Lemma 3.1 we have $(\flat\flat x \oplus \flat\neg\neg y) \in F$ and $(\flat\flat y \oplus \flat\neg\neg x) \in F$.

By F4 and Lemma 2.1 (i), it follows $(\neg\flat x \oplus \flat y) \odot (\neg\flat y \oplus \flat x) \in F$. Thus $\equiv_F$ is a congruence relation and it induces a quotient HW-algebra $\mathscr{A}/F$ homomorphic to the original $\mathscr{A}$ (for general concepts of universal algebra see [1]).

□

Moreover, by duality on Chen Chung Chang's result on MV-algebras [6] with ideals, if F is a prime MV-filter, then the quotient MV-algebra $\mathscr{A}/F$ is linear. It follows that if F is prime, then the quotient HW-algebras $\mathscr{A}/F$ is linear. Let us now define the last main concepts necessary to present the subdirect representation Theorem.

Definition 3.8. A *direct product* of a given family of HW-algebras $\{\mathscr{A}_i \mid i \in I\}$ is a HW-algebra $\Pi_{i\in I}\mathscr{A}_i = \langle \Pi_{i\in I}A_i, \rightarrow_L, \rightarrow_G, \mathbf{0}\rangle$ where $\Pi_{i\in I}A_i :=$ the cartesian product of $\{A_i \mid i \in I\}$ and the operators are defined componentwise as the operators of each original MV-algebra $\mathscr{A}_i$. The $\mathbf{0}$-element is obviously the sequence of all the $\mathbf{0}$-elements of $\{A_i \mid i \in I\}$.

Every element x of a direct product $\Pi_{i\in I}\mathscr{A}_i$ of HW-algebras $\{\mathscr{A}_i \mid i \in I\}$ is expressed in the following way: $x = \langle x_1, ..., x_n, ..\rangle$ where each x_i belongs to each HW-algebra $\mathscr{A}_i$ of $\Pi_{i\in I}\mathscr{A}_i$.

Definition 3.9. Let a HW-algebra $\Pi_{i\in I}\mathscr{A}_i$ be a direct product of a family of HW-algebras $\{\mathscr{A}_i \mid i \in I\}$ and $j \in I$. Let $\pi_j : \Pi_{i\in I}A_i \mapsto A_j$ be the *j-th projection function* s.t. $\forall x = \langle x_1, ..., x_n, ..\rangle \in \Pi_{i\in I}A_i$, $\pi_j(x) := x_j$. A HW-algebra $\mathscr{A}$ is a *subdirect product* of a given family of HW-algebras $\{\mathscr{A}_i \mid i \in I\}$ iff there exists a one-one homomorphism $h : \mathscr{A} \mapsto \Pi_{i\in I}\mathscr{A}_i$ such that for any $j \in I$, the compose map $\pi_j \circ h$ is a homomorphism onto $\mathscr{A}_j$.

Obviously every subdirect product of a family of HW-algebras $\{\mathscr{A}_i \mid i \in I\}$ is a subalgebra of the direct product of the same family of HW-algebras.

Theorem 3.2. A HW-algebra $\mathscr{A}$ is isomorphic to a subdirect product of a family of linear HW-algebras if there is a family of prime filters $\{F_i \mid i \in I\}$ of $\mathscr{A}$ such that $\bigcap F_i = \{\mathbf{1}\}$.

Proof. By duality to Theorem 1.3.2 in [9].

□

Remark 2. Given a HW-algebra $\mathscr{A} = \langle A, \rightarrow_L, \rightarrow_G, \mathbf{0}\rangle$, $\{\mathbf{1}\}$ is trivially a HW-filter of $\mathscr{A}$.

To prove the next theorem we need the following three lemmas.

Lemma 3.2. In any HW-algebra $\mathscr{A}$, $\forall a,x,y,z \in A$, $a \geq x \odot y, a \geq x \odot z \Rightarrow a \geq x \odot (y \vee z)$.

Proof. By duality to Theorem 1.5 in [6] and axiom 11 of [7] we have $a = a \vee a \geq (x \odot y) \vee (x \odot z) = x \odot (y \vee z)$.

□

Lemma 3.3. In any HW-algebra $\mathscr{A}$, $\forall x,y \in A$, $\forall m \in N$, $(x \oslash y)^m \vee (y \oslash y)^m = \mathbf{1}$.

Proof. This lemma is Theorem 3.7 in [6].

□

Lemma 3.4. In any HW-algebra $\mathscr{A}$, $\forall x,y, \in A$, $x \vee y = \mathbf{1} \Rightarrow \flat\flat x \vee \flat\flat y = \mathbf{1}$.

Proof. By Lemma 2.1 (i) and (iii), $\mathbf{0} \geq \flat\flat\mathbf{0} = \neg \sim \mathbf{0} = \sim \mathbf{1}$. Thus if $x \vee y = \mathbf{1}$ then $\flat\flat(x \vee y) = \sim \neg(x \vee y) = \mathbf{1}$. By Lemma 2.2 (i) we have $\flat(\flat x \wedge \flat y) = \mathbf{1}$. Then, by Lemma 2.2 (ii), $\flat\flat x \vee \flat\flat y = \mathbf{1}$.

□

Theorem 3.3. Let $\mathscr{A}$ be a HW-algebra. For any $z \in A, z \neq \mathbf{1}$, there is a prime HW-filter $F \subseteq A$ such that $z \notin F$.

Proof. $\{\mathbf{1}\}$ is trivially a HW-filter of $\mathscr{A}$ and a MV-filter of its MV-algebra term reduct $\mathscr{A}^\star$. Suppose $z \neq \mathbf{1}$. By the duality between filters and ideals with a routine application of Zorn's lemma $\{\mathbf{1}\}$ can be extended into a HW-filter F which is maximal with respect to the property "$z \notin F$". We show that F is prime: suppose, by ctr., $\exists x,y \in A$ s.t. $x \oslash y \notin F$ and $y \oslash y \notin F$. We define for any $x,y \in A$, $F^\star_{x \oslash y} := (Fi(F \cup \{x \oslash y\}))^\star$. $F^\star_{x \oslash y}$ and $F^\star_{y \oslash x}$ are HW-filters containing $Fi(F \cup \{x \oslash y\})$ and $Fi(F \cup \{y \oslash x\})$. By maximality of F with respect to "$z \notin F$", $z \in F^\star_{x \oslash y}$ and $z \in F^\star_{y \oslash x}$. Thus, $\exists r \in Fi(F \cup \{x \oslash y\})$ and $\exists s \in Fi(F \cup \{y \oslash x\})$ s.t. $z \geq \flat\flat r$ and $z \geq \flat\flat s$. Now $r = i \odot (x \oslash y)^n$ for some $i \in F$ and $n \in N$, $s = j \odot (x \oslash x)^m$ for some $j \in F$ and $m \in N$. Then, by Corollary 2.1, we have that $z \geq \flat\flat(i \odot (x \oslash y)^n) = \flat\flat i \odot \flat\flat((x \oslash y)^n)$ and $z \geq \flat\flat(j \odot (y \oslash x)^m) = \flat\flat j \odot \flat\flat((y \oslash x)^m)$. It is important to remind that by two application of Lemma 2.1 (iv), if $x \leq y$ then $\flat\flat x \leq \flat\flat y$. Hence, let $k = max\{n,m\}$, by monotonicity $z \geq (\flat\flat i \odot \flat\flat j) \odot \flat\flat((x \oslash y)^k)$ and $z \geq (\flat\flat i \odot \flat\flat j) \odot \flat\flat((x \oslash y)^k)$. By Lemma 3.2 we have $z \geq (\flat\flat i \odot \flat\flat j) \odot (\flat\flat((x \oslash y)^k) \vee \flat\flat((y \oslash x)^k))$. By Lemma 3.3 $(x \oslash y)^k \vee (y \oslash x)^k = \mathbf{1}$. By Lemma 3.4

$\flat\flat((x \oslash y)^k) \vee \flat\flat((y \oslash x)^k) = \mathbf{1}$. Hence $z \geq \flat\flat i \odot \flat\flat j$. Since F is a HW-filter and $i, j \in F$, by F4 $\flat\flat i \in F$ and $\flat\flat j \in F$. Thus $\flat\flat i \odot \flat\flat j \in F$. By F2 we have $z \in F$, against our ab absurdo hypothesis. Then F is a prime HW-filter.

□

Now we can state the subdirect representation theorem.

Theorem 3.4. Any HW-algebra $\mathscr{A}$ is isomorphic to a subdirect product of a family of linear HW-algebras.

Proof. We have already all the ingredients. Since for any $z \in A$, $\{\mathbf{1}\}$ can be extended in a prime HW-filter F such that $z \notin F$, we have that $\{\mathbf{1}\} = \bigcap\{F_i \mid F_i$ is a maximal prime filter of $\mathscr{A}\}$. By Theorem 3.2 and Theorem 3.3 we have the thesis.

□

4. Standard algebraic completeness

We will prove that an equation defined on the language of the HW-algebras holds in any HW-algebra if it holds in the standard HW-algebra. We will follow the track of Chang's standard completeness theorem for MV-algebras [7]. Then we assume familiarity with this proof and with all the results utilized to pursue it (see also [8]). Chang's proof exploits the completeness of the first order theory of divisible totally ordered Abelian groups (Chang's references are [14] and [15] but, as reported in footnote at page 79 [7], Tarski's proof has never appeared explicitly, then for a clear presentation of this result we advise the readers to consult appendix at page 91 of [8]). As a fundamental step of his proof, Chang had build a totally ordered abelian group made of infinite copies of an MV-algebra. Since any HW-algebra has an MV-algebra term reduct we can exploit the same argument. We introduce this expedient:

Definition 4.1. Let $\mathscr{A}$ be a linear HW-algebra. The algebraic structure $\mathscr{G}_A$ is defined in the following way, $G_A := \{(n,x) \mid n \in Z, x \in \mathrm{A} - \{\mathbf{1}\}\}$. Its operators are defined as:

$$(m,x) + (n,y) := \begin{cases} (n+m, x \oplus y) & \text{if } x \oplus y \neq \mathbf{1} \\ (n+m+1, x \odot y) & \text{if } x \oplus y = \mathbf{1} \end{cases}$$

$$-(n,x) := \begin{cases} (-n,\mathbf{0}) & \text{if } x = \mathbf{0} \\ (-(n+1),\neg x) & \text{if } \mathbf{0} \neq x \neq \mathbf{1} \end{cases}$$

and its related order relation is

$$(n,x) \sqsubseteq (m,y) \quad := \quad n < m \text{ or, } n = m \text{ and } x \leq y$$

Chang in [9] proved that $\mathscr{G}_{\mathscr{A}} = \langle G_A, +, -, \sqsubseteq, (0,\mathbf{0})\rangle$ is a totally ordered abelian group. Moreover if we define:

Definition 4.2. Let $\mathscr{G}=\langle G, +, -, 0, \sqsubseteq\rangle$ be a totally ordered abelian group and $u \in G$:

$$\Gamma(\mathrm{G},u) := \{x \in G \mid 0 \sqsubseteq x \sqsubseteq u\}$$
$$\neg x := u - x$$
$$x \oplus y := min\{u, x+y\}$$

we can immediately verify that $\Gamma(\mathscr{G},u) = \langle \Gamma(\mathrm{G},u), \oplus, \neg, 0\rangle$ is a linear MV-algebra. By Remark 1, once defined

$$\sim x := \begin{cases} \mathbf{0} & \text{if } x \neq \mathbf{0} \\ \mathbf{1} & \text{if } x = \mathbf{0} \end{cases}$$

the arising structure $\Gamma(\mathscr{G},u)^\star = \langle \Gamma(\mathrm{G},u), \to_L, \to_G, 0\rangle$, where for any $x, y \in \Gamma(\mathrm{G},u)$,

$$x \to_L y := \neg x \oplus y \text{ and}$$
$$x \to_G y := \sim \neg(\neg x \oplus y) \oplus y$$

is a linear HW-algebra.

Remark 3. The above definition of Gödel implication introduced in [4] (see Theorem 2.5 and 2.6) is given in terms of $\sim$, $\neg$ and $\oplus$. It is worth to be observed that by linearity since in any linear MV-algebra and then in any linear HW-algebra $\neg(\neg x \oplus y) = x \odot \neg y = \mathbf{0}$ if and only if $x \leq y$, we obtain that in any linear HW-algebra

$$x \to_G y = \begin{cases} \mathbf{1} & \text{if } x \leq y \\ y & \text{otherwise} \end{cases}$$

We recall that $u \in G$ is a *strong unit* iff for any $x \in G$ there exists an $n \in N$ s.t. $x \sqsubseteq nu$. $\mathscr{G}_{\mathscr{A}}$ is composed of infinite copies of $\mathscr{A}$; $\Gamma(\mathrm{G}_A, (1,\mathbf{0}))^\star$ belongs to them, then we have:

Theorem 4.1. If $\mathscr{A}$ is a linear HW-algebra, $\Gamma(\mathrm{G}_A, (1,\mathbf{0}))^\star$ is isomorphic to $\mathscr{A}$.

This result can be generalized to:

Theorem 4.2. If u is the strong unit of a totally ordered abelian group $\mathscr{G}$, there exists an isomorphism f from $\mathscr{G}$ onto $\mathscr{H} = \mathscr{G}_{\Gamma,(\mathrm{G},u)^\star}$:

i) $f(u) = (1,\mathbf{0})$

ii) $x \sqsubseteq y$ in $\mathscr{G} \Leftrightarrow f(x) \sqsubseteq f(y)$ in $\mathscr{H}$

Proof. It follows either Theorem 2.4.10 in [8] or [7]. □

The first order language of totally ordered abelian groups theory L' is composed by the usual logic symbols and 0,+,-,$\sqcap$,$\sqcup$ with their traditional meaning. We have to fix their corresponding definitions:

Definition 4.3. A language L of a HW-algebra $\mathscr{A}$ is composed by:

$\mathbf{0}$: costant

$x_1, ..., x_n, ..$: variables

$\rightarrow_L$: binary functor

$\rightarrow_G$: binary functor.

We define inductively a *HW-term*:

1) $\mathbf{0}, x_1, ..., x_n, ..$ are HW-terms.
2) If x_i and x_j are HW-terms, then $x_i \rightarrow_G x_j$ is a HW-term.
3) If x_i and x_j are HW-terms, then $x_i \rightarrow_L x_j$ is a HW-term.

Let p be a HW-term containing the variables $x_1, ..., x_t$ and assume $a_1, ..., a_t$ are elements of $\mathscr{A}$. Substituting an element $a_i \in A$ for all occurrences of the variable x_i in p, for $i = 1, ..., t$, by the above rules 1)-3) and interpreting the symbols $\mathbf{0}$,$\rightarrow_L$ and $\rightarrow_G$ as the corresponding operations in $\mathscr{A}$, we obtain an element of A, denoted $p^{\mathscr{A}}(a_1, ..., a_t)$. In more detail, proceeding by induction on the number of operation symbols occurring in p, we define $p^{\mathscr{A}}(a_1, ..., a_t)$ as follows:

i) $x_i^{\mathscr{A}} = a_i$, for each $i = 1, ..., t$;

ii) $(p \rightarrow_L q)^{\mathscr{A}} = (p^{\mathscr{A}} \rightarrow_L q^{\mathscr{A}})$;

iii) $(p \rightarrow_G q)^{\mathscr{A}} = (p^{\mathscr{A}} \rightarrow_G q^{\mathscr{A}})$;

By the above definition, given any HW-algebra $\mathscr{A}$ we can associate each HW-term in the variables $x_1,...,x_n$ with a function $p^{\mathscr{A}} : A^n \mapsto A$. These functions are called *term functions on A*.

A *HW-equation on variables* $x_1,...,x_t$ is an expression $p = q$, where p and q are HW-term containing at most the variables $x_1,...,x_t$. We say that a HW-algebra $\mathscr{A}$ *satisfies* a HW-equation $p = q$ (we write $\mathscr{A} \models p = q$) if and only if for any sequence of elements $(a_1,...,a_t) \in A$, $p^{\mathscr{A}}(a_1,...,a_t) = q^{\mathscr{A}}(a_1,...,a_t)$.

Theorem 4.3. If a HW-algebra $\mathscr{A}$ is a subdirect product of a family of linear HW-algebras $\{\mathscr{A}_i \mid i \in \mathrm{I}\}$, then $\mathscr{A} \models p = q \Leftrightarrow$ for any i $\mathscr{A}_i \models p = q$.

Proof. In the subdirect representation theorem (Theorem 3.4) there is a homomorphism from $\mathscr{A}$ onto any linear HW-algebra of its subdirect product: the Łukasiewicz implication operator $\to_L$ and the Gödel implication operator $\to_G$ are preserved into these structures; then every HW-equation continues to hold in any $\mathscr{A}_i$. Vice versa if a HW-equation holds in any $\mathscr{A}_i$, it holds in their direct product $\Pi_{i\in I}\mathscr{A}_i$. Since $\mathscr{A}$ is isomorphic to a subalgebra of $\Pi_{i\in I}\mathscr{A}_i$, it holds in $\mathscr{A}$.

□

Corollary 4.1. A HW-equation is satisfied in any HW-algebras if and only if it is satisfied in any linear HW-algebra.

We will report in the following steps Chang's standard completeness proof, as it has been presented in [8], to check its validity with respect to the Heyting Wajsberg algebras case. Every totally ordered abelian group can be embedded into a divisible totally ordered abelian group. From the completeness of the first order theory of these last structures it follows that every universal sentence of the first order theory of totally ordered abelian groups is satisfied in the additive group Q of rational numbers if and only if it is satisfied in any totally ordered abelian group [7]. Then any HW-equation has to be associated to an universal sentence of the first order language of totally ordered abelian groups theory L' to exploit its completeness. We will do it by induction on the degree of complexity of a HW-term.

Definition 4.4. The *degree of complexity* of a HW-term p: $d(p)$:= the number of times that symbols $\to_L$ and $\to_G$ appear in p.
We associate to any HW-term p a term $p' \in L'$ by induction on the degree of complexity of p:

If $d(p)$=0 (p=0 or $p = x_i$) then $p' = p$.
We suppose to have associated HW-terms until degree of complexity n; then if $d(p)$=$n+1$, we can have either:
1) $p = q \to_L r$ with $d(q) \leq n$ and $d(r) \leq n$ or
2) $p = q \to_G r$ with $d(q) \leq n$ and $d(r) \leq n$.
Let z be a free variable that belongs to L', we define, fir case 1 and 2 respectively:
1) $p' = z \sqcap (z - q' + r')$;
2) $p' = \begin{cases} z & \text{if } q' \sqsubseteq r' \\ \\ r' & \text{otherwise} \end{cases}$
Then we define $\alpha_{pq} := \forall x_1, ..., x_n (0 \sqsubseteq x_i \sqsubseteq z \bigwedge, ..., \bigwedge 0 \sqsubseteq x_n \sqsubseteq z) \to p' = q'$.

As a routine it can be checked, by the way $\mathscr{G}_A$ has been built, that the following sentence holds:

Proposition 4.1. Let $\mathscr{A}$ be a linear HW-algebra, let $p = q$ be a HW-equation; $\mathscr{A} \models p = q \Leftrightarrow \alpha_{pq}(z)$ is true in $\mathscr{G}_A$ when we attribute to z the value $(1, \mathbf{0})$.

At last we can introduce:

Theorem 4.4 (Standard Completeness Theorem)**.** A HW-equation is satisfied in any HW-algebra if and only if it is satisfied in the standard HW-algebra $\mathscr{A}_{[0,1]}$.

Proof. $\Leftarrow$ (not trivial) : By contradiction we suppose there is a HW-algebra $\mathscr{A}$ such that $\mathscr{A} \not\models p = q$. From Corollary 4.1 we infer that there is a linear HW-algebra $\mathscr{B}$ s.t. $\mathscr{B} \not\models p = q$. By Proposition 4.1 above there is an universal sentence β of the 1^o order theory of the totally ordered Abelian groups, $\beta = \forall z > 0\ \alpha_{pq}(z)$ s.t. β is false in $\mathscr{G}_B$, and hence, by the completeness of totally ordered abelian groups, β is false in Q (group of rational numbers with usual operations). It means that there is a $c > 0, c \in Q$ s.t. c does not verify β in Q. Let's consider f: $Q \mapsto Q$ defined by $f(x) := c^{-1}x$. $f(c) = 1$. f is an isomorphism from Q onto itself (antiautomorphism), then f preserves falsity of sentences and therefore β is false in Q when we attribute to z the value $1 \in Q$. By Theorem 4.2 Q is isomorphic to $\mathscr{G}_{\Gamma(Q,1)^\star}$. Thus β is false in $\mathscr{G}_{\Gamma(Q,1)^\star}$ with $z = 1$ and, by Proposition 4.1, $\Gamma(Q,1)^\star = \mathscr{A}_{[0,1]} \not\models p = q$. □

REFERENCES

[1] BURRIS, S., SANKAPPANAVAR, H.P. (1981), *A Course in Universal Algebra*. Springer-Verlag, New York.

[2] CATTANEO, G. and CIUCCI, D. (2002), "Heyting Wajsberg algebras as an abstract environment linking fuzzy and rough sets", *Lecture Notes in Artificial Intelligence*, 2475, pp. 77–84.

[3] CATTANEO, G., CIUCCI, D., GIUNTINI, R. and KONIG, M. (2004), "Algebraic Structures Related to Many Valued Logical Systems Part I: Heyting Wajsberg Algebras", *Fundamenta Informaticae*, 63, pp. 331–355.

[4] CATTANEO, G., CIUCCI, D., GIUNTINI, R. and KONIG, M. (2004), "Algebraic Structures Related to Many Valued Logical Systems Part II: Equivalence Among Widespread Structures", *Fundamenta Informaticae*, 63, pp. 357–373.

[5] CATTANEO, G., GIUNTINI, R. and PILLA, R. (1998), "BZMV^{dM} algebras and Stonean MV-algebras (Applications to fuzzy sets and rough approximations)", *Fuzzy Sets and Systems*, 108, pp. 201–222.

[6] CHANG, C.C. (1958), "An Algebraic Analysis of many valued logics", *Transactions of the American Mathematical Society*, 88, pp. 476–490.

[7] CHANG, C.C. (1959) "A new proof of the completeness of Łukasiewicz axioms", *Transactions of the American Mathematical Society*, 93, pp. 74–80.

[8] CIGNOLI, R., D'OTTAVIANO, I. and MUNDICI, D. (1994), *Álgebras das Lógicas de Łukasieweicz*. Colecao CLE 12, Campinas (Brazil).

[9] CIGNOLI, R., D'OTTAVIANO, I. and MUNDICI, D. (2000), *Algebraic Foundation of Many-valued Reasoning*. Kluwer Academic Publishers, Boston/Dodrecht/London.

[10] DUNN, J.M. and HARDEGREE, G.M. (2001), *Algebraic Methods in Philosophical Logic*. Clarendon Press, Oxford.

[11] GÖDEL, K. (1933), "Zum intuitionistischen Aussagenkalkül", *Anzeiger der Akademie der Wissenschaften Wien, Mathematisch-Naturwissenschaftliche Klasse*, 69, pp. 65–69.

[12] HÀJEK, P. (1998), *Metamathematics of Fuzzy Logic*. Kluwer Academic Publishers, Boston/Dodrecht/London.

[13] KONIG, M. (2010), "Gödel Łukasiewicz Logic", *L&PS Logic and Philosophy of Science: an Electronic Journal*, 8, 1, pp. 119–142.

[14] TARSKI, A. (1931), "Sur les ensembles définissable de nombre réels" I, *Fundamenta Mathematicae*, 17, pp. 210–239.

[15] TARSKI, A. (1956), *Logics, Semantics, Metamathematics*. Oxford: Clarendon Press.

L&PS – Logic & Philosophy of Science
Vol. X, No. 1, 2012, pp. 31-51

La logica computazionale quantistica dei sistemi aperti

Giuseppe Sergioli
Dipartimento di Filosofia e Teoria delle Scienze Umane,
Università di Cagliari, Via Is Mirrionis 1, I-09123 Cagliari
giuseppe.sergioli@gmail.com

SOMMARIO. Esistono fenomeni fisici come la decoerenza, il rumore, la misura effettuata nel mezzo del processo computazionale, che difficilmente possono essere interpretati attraverso il paradigma quantistico standard. In un processo computazionale, una qualsiasi interazione del sistema con l'ambiente causa un'inevitabile perdita di informazione che rende il processo stesso irreversibile. Per tener conto di situazioni di questo tipo, la computazione quantistica ha recentemente adottato un nuovo approccio che si spinge oltre a quello standard. Lo scopo di questo articolo è quello di riassumere in maniera descrittiva (evitando di entrare in dettagli tecnici) i caratteri principali di questo nuovo approccio e analizzarne qualche possibile applicazione.

ABSTRACT. There are physical phenomena that can be hardly interpreted by standard quantum paradigm: decoherence, noise, measurements in the middle of a computation – basically, any computational process that involves an interaction with the environment – call into play an unavoidable loss of information that renders the process itself irreversible. To conveniently describe such situations, alongside with the kind of processes that

Published by L&PS – Logic and Philosophy of Science
http://www2.units.it/~episteme/ – ISSN: 1826-1043

are dealt with by the standard approach, a new, more comprehensive perspective has been recently developed in quantum computation. The aim of this paper is to survey and to describe (without come into technical details) some original applications of this new approach.

KEYWORDS: Computazione quantistica, reversibilità, universalità, logica computazionale quantistica.

1. Introduzione

La teoria della *computazione quantistica* [3, 5, 22] si pone l'obiettivo di offrire un modello formale di calcolatore in cui l'evoluzione da uno stato al successivo sia determinata dalla teoria quantistica. Come verrà mostrato in dettaglio nel paragrafo 2, la teoria della computazione quantistica fu inizialmente pensata in termini esclusivamente reversibili: vennero considerate solo situazioni in cui uno stato iniziale evolvesse verso uno stato finale in modo tale che fosse sempre possibile considerare l'evoluzione inversa, quella cioè che conduceva dallo stato finale a quello iniziale. Vedremo in seguito come questo tipo di situazioni siano in realtà piuttosto "ideali" e rappresentino solo il caso in cui un sistema fisico sia completamente isolato dall'ambiente esterno. In realtà, per quanto accurate possano essere le precauzioni prese dallo sperimentatore per schermare il sistema che sta osservando, è ben noto come l'idea di ottenere un sistema perfettamente chiuso (cioè completamente isolato) sia in realtà di difficilissima realizzazione (ancor di più in ambito microscopico). Per questo motivo può risultare utile generalizzare la teoria della computazione quantistica ad un generico sistema aperto, in modo da tenere in considerazione anche le interazioni sistema-ambiente. Ogni interazione del sistema con l'ambiente – tra cui ad esempio la misura di una qualsivoglia osservabile fisica – consiste in un'operazione che, in ambito microscopico, modifica in maniera irreversibile lo stato del sistema. In questo articolo verrà presentata una panoramica molto generale relativa a un nuovo approccio alla computazione quantistica, in cui l'evoluzione dello stato del sistema possa essere sia reversibile che irreversibile. Verrà introdotto anche il tema dell'universalità in computazione quantistica e, in conclusione, verranno indicati possibili nuovi sviluppi di ricerca in cui l'approccio di

natura irreversibile suggerisce nuove soluzioni relativamente all'individuazione di nuovi insiemi di operazioni universali in computazione quantistica.

L'articolo è organizzato nel seguente modo: nel paragrafo 2, dopo una breve introduzione storica, verranno descritte le principali caratteristiche dell'approccio standard alla computazione quantistica, che vede operatori unitari (che rappresentano trasformazioni reversibili) agire su vettori unitari; nel paragrafo 3 verrà invece trattato il passaggio dall'approccio unitario a quello più generale, in cui operazioni quantistiche (che rappresentano trasformazioni sia reversibili che irreversibili) agiscono su operatori di densità; verranno quindi analizzate nel dettaglio le caratteristiche del nuovo approccio e le implicazioni che ne conseguono. In particolare verranno discusse le sue conseguenze sulla nuova logica che sostiene questo nuovo approccio formale alla computazione quantistica. Nel paragrafo 4 verranno introdotte la definizione di universalità approssimata e di insieme di operazioni approssimativamente universale. Infine, nel paragrafo 5, verrà presentato un nuovo strumento formale per trattare alcune particolari trasformazioni fisiche irreversibili nel contesto quantistico computazionale.

2. L'approccio unitario alla computazione quantistica

All'inizio del ventesimo secolo la meccanica quantistica e la teoria della computazione erano due teorie studiate in maniera del tutto separata [21, 8, 1, 27, 26].

Già precedentemente all'avvento dei computer, la comunità scientifica era solita interrogarsi su questioni del tipo: "che cosa intendiamo per problema?", "Quali problemi sappiamo risolvere?", "Con quante e quali macchine?", "Se non fosse possibile risolvere un certo problema con una certa macchina, potrebbe essere possibile risolverlo con un'altra?" e molte altre ancora. Questo tipo di interrogativi diede vita, nella prima metà del secolo scorso, a quella che venne denominata *teoria della calcolabilità* (o della *computabilità*).

La teoria della calcolabilità intendeva quindi comprendere quali fossero le funzioni che potevano essere calcolate tramite un determinato procedimento automatico (*algoritmo*) a prescindere dalla quantità di risorse richieste. Per offrire una risposta a tali esigenze teoriche, lo sforzo iniziale fu quello di offrire una definizione formale e rigorosa all'idea intuitiva di funzione calcolabile, in modo da distinguere la categoria dei problemi teoricamente risolvibili da quella dei

problemi non risolvibili. Passo successivo fu quello di definire rigorosamente il concetto di algoritmo, in modo che i programmi potessero essere concretamente pensati in termini di funzioni che, a partire da un certo input, restituissero un determinato risultato.

Non è difficile identificare in Alan Turing il pioniere della teoria della calcolabilità. Fu lui a introdurre una macchina ideale – chiamata appunto, *macchina di Turing* – che, eseguendo delle semplici istruzioni (algoritmo) inizialmente impostate (da un programma) fosse in grado di calcolare in maniera deterministica qualsiasi funzione intuitivamente computabile (tesi di Church-Turing). La macchina di Turing, però, pur offrendo lo spunto per nuovi straordinari contributi scientifici dal punto di vista teorico, rimaneva comunque una macchina ideale che non offriva allo stesso modo grandi prospettive in termini di efficienza e concreta utilizzabilità. Inoltre, la nascita dei primi computers, la rapidissima miniaturizzazione delle componenti hardware degli stessi e la continua ricerca di dispositivi sempre più efficienti, condussero a una nuova idea di computazione in cui vennero considerati per la prima volta anche fenomeni di natura microscopica (quindi regolati dalla teoria quantistica) e in cui l'efficienza implementativa assunse un ruolo di primaria importanza.

Il primo studioso a immaginare un'applicazione del paradigma quantistico alla teoria della calcolabilità fu Richard Feynman. L'idea di base era quella secondo cui, mentre la macchina di Turing è rigorosamente deterministica e sequenziale, al contrario la meccanica quantistica presenta in maniera essenziale la nozione di *stato sovrapposto* che – come verrà meglio mostrato in seguito – si basa sui concetti di probabilità e parallelismo. Inoltre, mentre l'alfabeto utilizzato dalla macchina di Turing si limita a un numero di simboli estremamente ristretto, questa limitazione non viene mantenuta nella teoria quantistica. In sostanza, mentre l'informazione espressa da un bit classico era limitata a soli due valori (lo *zero* e l'*uno*), il bit quantistico risulta infinitamente più informativo e questo fece pensare a come un possibile calcolatore quantistico potesse essere assai più efficiente di qualsiasi macchina di Turing. Nel 1982 Feynman dimostrò [13] che nessuna macchina di Turing è in grado di simulare certi fenomeni fisici senza subire un rallentamento esponenziale delle prestazioni. Di contro, un calcolatore quantistico sarebbe in grado di effettuare tali simulazioni con un' efficienza enormemente superiore. Nel 1985 David Deutsch formalizzò il primo modello teorico di macchina di Turing quantistica universale [10] e da lì ebbe inizio una nuova disciplina che ha avuto notevoli sviluppi negli ultimi anni e che

prende il nome di *computazione quantistica*, di cui adesso verranno presentate le caratteristiche essenziali che la differenziano in maniera evidente dal modello classico.

In meccanica quantistica a ogni stato di un arbitrario sistema fisico è associato un vettore unitario (cioè di lunghezza 1) in uno spazio di Hilbert di dimensione adeguata. Allo stesso modo, in computazione quantistica l'unità di informazione è rappresentata da un vettore unitario in uno spazio di Hilbert basato sui numeri complessi. Tale vettore unitario è il corrispettivo quantistico del bit classico e per questo prende il nome di *quantum-bit* o, più sinteticamente, *qubit*. Dal punto di vista logico, mentre i valori di verità che assume un bit classico possono essere solo il "vero" o il "falso", il bit quantistico rappresenta un'informazione più ricca che è formalmente espressa da una *sovrapposizione* tra lo stato vero e lo stato falso: in sostanza un bit quantistico può rappresentare un'informazione vera, falsa o qualsiasi possibile "via di mezzo" tra il vero e il falso. L'espressione "via di mezzo" va però intesa in termini probabilistici: vi è quindi una certa probabilità di *rilevare* – dopo un processo di misura – il sistema (o l'informazione) che si sta descrivendo nello stato "vero" oppure nello stato "falso" e tale probabilità è espressa formalmente dalla nota regola di Born. Ogni stato sovrapposto corrisponde quindi a uno stato "incerto" .

Il qubit è un vettore unitario: dal punto di vista formale l'unitarietà del vettore corrisponde alla *massimalità* dell'informazione che questo rappresenta: la quantità d'informazione si definisce massimale se non può essere ulteriormente incrementata – in modo non contraddittorio – attraverso successive osservazioni. È, in sostanza, l'informazione più completa possibile sullo stato del sistema fisico che si sta descrivendo, che in questo caso si dirà essere uno *stato puro*. La lunghezza del vettore corrisponde quindi alla quantità di informazione che il vettore stesso porta con sé: l'informazione massimale sarà per questo rappresentata da un vettore di lunghezza unitaria. Può essere utile notare come uno stato sovrapposto, quindi *incerto*, possa rappresentare comunque una quantità di informazione massimale e sia quindi ancora uno stato *puro*. Risulta conveniente offrire una rappresentazione geometrica del qubit tramite la sfera di Bloch-Poincaré: è una sfera di raggio unitario, sicché vi è una naturale biiezione tra ciascun punto sulla superficie della sfera e ciascun vettore di lunghezza unitaria (Fig. 1).

Quanto appena detto riguarda esclusivamente la descrizione formale di un singolo sistema fisico. È facile immaginare come in realtà sia necessario offrire

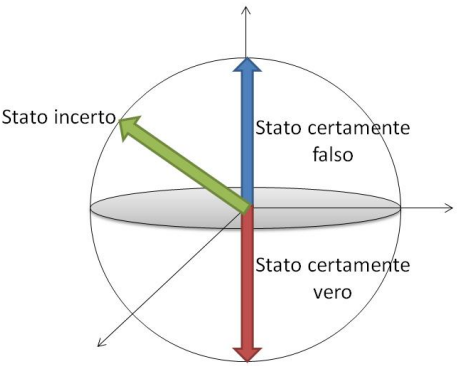

FIGURA 1: *Sfera di Bloch-Poincaré*

una rappresentazione formale anche di più sistemi fisici che interagiscono tra loro. Lo strumento formale che permette tale rappresentazione è il prodotto tensoriale. Due (o più) sistemi fisici che interagiscono sono quindi formalmente rappresentati dal prodotto tensoriale tra i due (o più) vettori unitari nello spazio di Hilbert dei numeri complessi, ciascuno dei quali è la rappresentazione formale del sistema fisico a cui ci si riferisce. Tale prodotto tensoriale di più vettori unitari sarà ancora un vettore unitario che viene chiamato *registro quantistico* o *quregister* e la sua dimensione dipende direttamente dal numero di sistemi fisici interagenti che il registro rappresenta. Chiaramente un registro quantistico di dimensione arbitraria non può essere rappresentato tramite la sfera di Bloch-Poincaré, ma quanto precedentemente detto circa la corrispondenza tra unitarietà del vettore e massimalità dell'informazione resta valido.

Fino ad ora si è offerta una descrizione dello stato del sistema, ma non della sua evoluzione. Così come in ambito classico le porte logiche sono quelle che determinano l'evoluzione del bit classico, lo stesso avviene nell'ambito computazionale quantistico: l'evoluzione dei qubits è regolata dalle porte logico-quantistiche (quantum gates) che formalmente sono rappresentate da operatori unitari. Quando si è definita l'unità di informazione quantistica, si è mostrato come l'espressione "unitarietà del vettore" fosse sinonimo di "massimalità dell'informazione". Adesso invece unitarietà è sinonimo di reversibilità. Per definizione, infatti, affinché un operatore sia unitario deve esistere il suo operatore inverso: applicando un operatore unitario su un sistema fisico, questo passa

da uno stato iniziale a uno stato finale; l'operatore inverso è quell'operatore che, applicato allo stato finale, lo riporta nuovamente allo stato iniziale. È proprio in questo senso che unitarietà dell'operatore e reversibilità della trasformazione sono due concetti così strettamente correlati.

Le porte logico-quantistiche riproducono il comportamento delle porte classiche ma inoltre lo generalizzano ad un contesto molto più ampio. Si consideri per esempio la negazione: dal punto di vista classico, la negazione del falso (cioè di un'informazione falsa) offrirà il vero come output (cioè un'informazione vera) e viceversa. In ambito quantistico questo comportamento viene perfettamente riprodotto, ma, a differenza del caso classico, una porta logico-quantistica potrà essere applicata anche a sovrapposizioni di vero e falso, mantenendo il proprio connotato di reversibilità. Come già accennato in precedenza, una sovrapposizione di vero e falso corrisponde a un terzo stato (differente sia dal "vero" che dal "falso") su cui è possibile soltanto dire che, dopo un eventuale processo di misura, si avrà una certa probabilità che il sistema *collassi* nello stato "vero" e un'altra probabilità che collassi nello stato "falso". L'azione della negazione quantistica su di un siffatto stato agirà invertendo tali probabilità. Applicando però nuovamente l'operatore negazione al vettore appena ottenuto, questo invertirà nuovamente le probabilità del vero e del falso, restituendo alla fine lo stesso vettore che si aveva all'inizio. L'esempio appena analizzato costituisce un caso particolare. La negazione è infatti un operatore quantistico che corrisponde al suo inverso: l'operazione che consiste nell' applicare due volte la negazione può quindi essere interpretata come la sequenza che consiste nell'applicare la negazione e successivamente l'operazione inversa, giungendo quindi allo stesso stato di partenza (in altre parole anche in computazione quantistica vale il principio secondo cui due negazioni affermano). L'esempio poc'anzi citato può essere visto come un caso particolarmente semplice di reversibilità dell'operatore quantistico.

È interessante notare come la negazione quantistica sia un esempio di porta che viene detta *semiclassica*, poiché, se si rimanesse confinati esclusivamente agli stati "vero" e "falso" (cioè ai vettori che costituiscono la base computazionale), riprodurrebbe esattamente il comportamento di una porta classica; però, a differenza di queste ultime, la negazione quantistica è applicabile anche a stati sovrapposti ed è in questo senso che le porte logico-quantistiche sono utilizzabili in un contesto molto più ampio rispetto a quelle classiche. Inoltre, mentre le porte logico-quantistiche conservano sempre il loro connotato di reversibilità,

la logica classica è invece naturalmente irreversibile. Basti pensare alla congiunzione: se il risultato del valore di verità di una congiunzione è "falso", non c'è modo di sapere con certezza il valore di verità dei due congiunti o, in altri termini, non è possibile applicare un'operazione inversa alla congiunzione per tornare univocamente dallo stato finale a quello iniziale. La congiunzione quantistica (che è un altro esempio di porta semiclassica) invece lo consente, anche se a costo di un aumento della dimensione dello spazio vettoriale su cui agisce.

Esistono però porte logico-quantistiche che non riproducono neanche in parte il comportamento di alcuna porta classica e che per questo vengono dette *genuinamente quantistiche*. Si tratta di porte che, applicate al "vero" o al "falso", danno in uscita uno stato sovrapposto, comportamento che non è assimilabile in nessun modo ad alcun fenomeno classico. Un esempio è la porta "radice della negazione", così chiamata poiché, se applicata una volta allo stato (ad esempio) "vero", darà in uscita una sovrapposizione tra vero e falso, ma se a tale sovrapposizione si applica nuovamente lo stesso operatore allora in uscita si otterrà lo stato "falso". La radice della negazione si comporta quindi come una sorta di *semi-negazione*. Questa semi-negazione non è solamente un'astrazione matematica ma è la rappresentazione di numerosi fenomeni fisici: uno specchio semi-riflettente che si fa attraversare da metà dei fotoni incidenti ma riflette tutti gli altri costituirebbe un perfetta rappresentazione fisica della radice della negazione. L'intero comportamento dell'interferometro di Mach-Zehnder può essere spiegato mediante il coinvolgimento della radice della negazione [23].

Ritornando quindi alla rappresentazione geometrica offerta in precedenza, così come ogni bit quantistico corrisponde a un vettore di lunghezza unitaria all'interno di una sfera di raggio pari a 1, analogamente l'azione di una porta logico-quantistica corrisponde semplicemente a una rotazione che, essendo un'isometria, preserva l'unitarietà del vettore finale e corrisponde sempre a un'operazione reversibile. Lo stesso discorso può facilmente essere generalizzato a una dimensione arbitrariamente grande: l'operatore, per essere applicato a un vettore, dove naturalmente avere la sua stessa dimensione.

3. Dall'universo reversibile a quello irreversibile

Nel paragrafo precedente si è detto come l'unità di informazione sia espressa da un vettore unitario che rappresenta un'informazione massimale. Non è però

difficile convincersi di come sia piuttosto implausibile che un osservatore riesca ad avere un'informazione massimale sul sistema fisico osservato: se infatti le dimensioni di un sistema fisico non sono estremamente ridotte e se il sistema fisico non è perfettamente schermato dall'esterno, allora avere un'informazione massimale sulle possibili interazioni tra tutte le varie componenti del sistema e sulle molteplici interazioni tra sistema e ambiente è un compito davvero molto arduo [6]. Nasce quindi l'esigenza di un modello formale più generale, in cui sia possibile considerare dei sistemi su cui l'osservatore abbia solo un certo "grado di conoscenza".

L'oggetto matematico capace di descrivere l'unità di informazione in termini di conoscenza non esclusivamente massimale è l'operatore di densità. Dal punto di vista strettamente matematico, un operatore di densità è un operatore autoaggiunto, non negativo con traccia 1. Dal punto di vista computazionale l'operatore di densità viene chiamato *qumix*, cioè stato quantistico misto, proprio in contrapposizione con la definizione di stato puro offerta nel paragrafo precedente. Rimanendo confinati, per semplicità, alla descrizione di un solo sistema, è possibile mostrare come ogni operatore di densità sia rappresentabile nello spazio vettoriale degli operatori che agiscono su spazi di Hilbert, tramite combinazione lineare delle matrici di Pauli e della matrice identità; proprio i coefficienti di tale combinazione lineare rappresentano il "grado di conoscenza" dell'informazione che l'operatore di densità porta con sé e esattamente: la somma dei quadrati dei coefficienti della combinazione lineare prima citata è un numero compreso tra 0 e 1. Si può vedere che tale valore gioca per gli operatori di densità ruolo analogo a quello della lunghezza nel contesto dei vettori, ragion per cui può essere interpretato come "grado di conoscenza".

In particolare, nel caso in cui questa lunghezza sia pari a 1 allora si è nuovamente in presenza di un'informazione massimale: in questo caso l'informazione potrà essere espressa tanto da un vettore unitario quanto da un operatore di densità che, in questo caso particolare, sarebbe un operatore di proiezione che proietta proprio su quel vettore unitario. Insomma, in questo caso limite l'operatore di densità e il vettore unitario corrisponderebbero perfettamente e avrebbero lo stesso significato fisico. In tutti gli altri casi, però, l'operatore di densità esprime un grado di conoscenza sempre minore e viene graficamente rappresentato da un vettore di lunghezza minore di 1, fino al caso degenere in cui finisce per rappresentare la totale ignoranza sul sistema. Per riepilogare, un operatore di densità può essere visto:

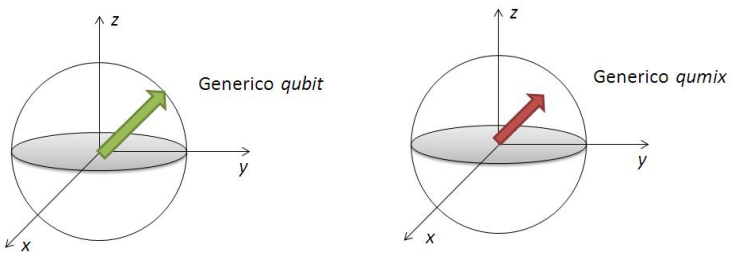

FIGURA 2: *Qubit and qumix*

- dal punto di vista geometrico come un punto (interno o sulla superficie) della sfera di Bloch-Poincaré (Fig. 2);
- dal punto di vista algebrico come un vettore di lunghezza minore o uguale all'unità;
- dal punto di vista epistemico come un'informazione generalmente non massimale.

Da questa prima descrizione dovrebbe quindi apparire già evidente come gli operatori di densità *generalizzino* effettivamente i qubit, nel senso che ogni qubit può essere espresso tramite un operatore di densità (in particolare come un operatore di proiezione), mentre tutti quegli operatori di densità che rappresentano informazioni non massimali non possono in nessun modo essere espressi come qubit.

Così come gli operatori unitari agiscono sui vettori unitari descrivendone l'evoluzione, analogamente è possibile introdurre una nuova entità matematica che sia capace di determinare l'evoluzione di un qualsiasi operatore di densità e che nello stesso tempo possa generalizzare il comportamento di un qualsiasi operatore unitario. Tale entità matematica è rappresentata dalle *operazioni quantistiche*: un'operazione quantistica è una mappa da operatori di densità a operatori di densità che gode di particolari proprietà (è una mappa lineare, completamente positiva che preserva la traccia [18]). Ma una caratteristica fondamentale è quella secondo la quale il comportamento di ogni operatore unitario può essere replicato da un'opportuna operazione quantistica: in sostanza, è possibile applicare una operazione quantistica che rappresenti l'evoluzione di un operatore unitario ad una quantità di informazione che non sia unitaria.

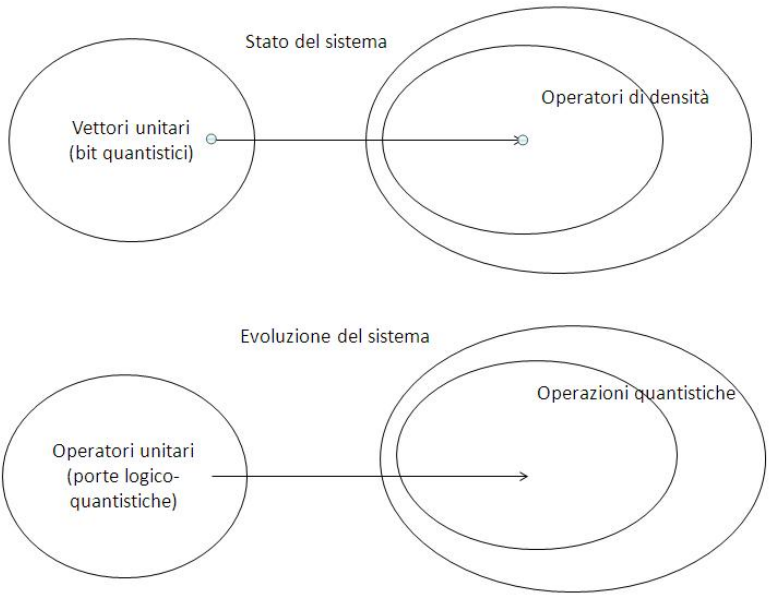

FIGURA 3: *Stato ed evoluzione del sistema*

Rimane il fatto che, se il comportamento di ogni operatore unitario è replicabile da un'operazione quantistica (in questo caso si parlerà di *operazioni quantistiche unitarie*), di contro esistono operazioni quantistiche che non possono essere rappresentate da alcun operatore unitario (in questo caso si parlerà di *operazioni quantistiche non unitarie*). Se un'operazione quantistica corrisponde ad un operatore unitario vuol dire che il significato fisico di entrambi è, ancora una volta, quello di una trasformazione reversibile, ma nel caso in cui l'operazione quantistica non corrisponda ad alcun operatore unitario allora vuol dire che tale operazione quantistica corrisponde fisicamente ad una trasformazione irreversibile.

Si è quindi passati da un contesto in cui si valutava l'evoluzione esclusivamente reversibile di quantità di informazione esclusivamente massimali ad un contesto molto più generale in cui si valuta l'evoluzione sia reversibile che irreversibile di quantità di informazione sia massimali sia non massimali. Nella figura 4 a seguire viene riassunto graficamente quanto detto nel presente paragrafo.

Informazione quantistica

	QUBIT	QUMIX
Geometricamente	Punto sulla superficie della sfera	Punto sulla superficie o interno alla sfera
Algebricamente	Vettore unitario	Operatore di densità
Epistemicamente	Informazione massimale	Informazione generalmente non massimale
Evoluzione	Reversibile	Generalmente irreversibile

FIGURA 4: *Schema riassuntivo sull'informazione quantistica*

4. L'universalità in computazione quantistica: due approcci differenti

È ben noto come in logica classica le leggi di interdefinibilità dei connettivi consentano di esprimere alcuni connettivi tramite l'esclusivo utilizzo di altri. Ad esempio, all'interno del contesto classico, la negazione e la congiunzione consentono di rappresentare, tramite opportuni principi di equivalenza, il comportamento degli altri connettivi classici. In questo caso si dirà che la negazione e la congiunzione costituiscono un insieme di connettivi *funzionalmente* universale. In ambito computazionale, la tematica dell'universalità ha sempre rappresentato un problema fondamentale [11, 10, 25, 2].

Trovare un insieme di porte logiche universale di cardinalità più ridotta possibile, permetterebbe di contare sull'esclusivo utilizzo di porte appartenenti a tale insieme per "replicare" il comportamento di ciascuna altra porta logica. Insomma, con l'esclusivo impiego di un numero ridotto di porte logiche sarebbe possibile "costruire" un circuito qualsiasi. Dal punto di vista classico, ad esempio, è noto come la porta di Toffoli sia capace, da sola, di riprodurre il comportamento di ciascuna altra porta di un circuito classico. Quindi la sola porta di Toffoli è funzionalmente universale in ambito computazionale classico.

In computazione quantistica, in virtù di quanto ampiamente discusso nei paragrafi precedenti, gli operatori sono delle isometrie che, dal punto di vista geometrico, corrispondono a rotazioni. Per questo l'insieme degli operatori quantistici (e quindi anche delle operazioni quantistiche) è più che numerabile (poichè

l'isieme delle possibili rotazioni è più che numerabile) e non è quindi possibile in computazione quantistica – sia nel suo approccio unitario sia in quello non unitario – trovare un insieme finito di operatori (o operazioni quantistiche) che possa risultare funzionalmente universale. In virtù del fatto, sottolineato nel paragrafo 3, che l'approccio non unitario generalizza quello unitario, d'ora in avanti il tema dell'universalità verrà affrontato rimanendo confinati all'approccio più generale che prevede operazioni quantistiche che agiscono su operatori di densità.

Shi e Aharonov hanno mostrato [2, 25] come esistano due operazioni quantistiche unitarie capaci di replicare in maniera "approssimata" il comportamento di qualsiasi altra operazione quantistica. In questo caso si parlerà di *universalità approssimata*: un insieme di operazioni quantistiche viene detto approssimativamente universale se, scelta una qualsiasi altra operazione quantistica, è sempre possibile "costruire" un circuito (in cui siano presenti solo le operazioni quantistiche dell'insieme approssimativamente universale) che replichi in maniera arbitrariamente approssimata (cioè a meno di una costante arbitraria) l'azione dell'operazione scelta su un arbitrario operatore di densità. L'insieme di operazioni quantistiche approssimativamente universale introdotte da Shi e Aharonov è costituito dalle operazioni quantistiche di *Toffoli* e di *Hadamard*[1]. L'operatore di Toffoli è ternario e si comporta mantenendo inalterati i primi due qubits e cambiando il terzo solo quando i primi due siano entrambi *veri*. La funzione corrispondente all'operatore di Toffoli risulta già universale in computazione classica ed è particolarmente importante in computazione quantistica in quanto offre la possibilità di ottenere una congiunzione quantistica reversibile (la congiunzione si ottiene grazie all'operatore di Toffoli, dove i primi due qubits corrispondono ai due congiunti e il terzo è un qubit-*ancilla* fissato, in input, sempre nello stato *falso*). L'operatore di Hadamard è genuinamente quantistico e viene anche chiamato "*radice dell'identità* ", per un motivo simile a quello descritto precedentemente per la radice della negazione. Applicando infatti la radice dell'identità a un vettore della base computazionale si ottiene in uscita un vettore sovrapposto, ma applicando a tale vettore sovrapposto nuovamente la radice dell'identità, si otterrà nuovamente il vettore di partenza. La radice dell'identità si comporta quindi come una *semi-identità*.

[1] Per operazione quantistica di Toffoli – o Hadamard – si intende l'*operazione quantistica* che corrisponde all'*operatore quantistico* di Toffoli – o Hadamard – rispettivamente.

Dal punto di vista intuitivo, il fatto che l'insieme di operazioni quantistiche approssimativamente universali sia costituito proprio da Toffoli e Hadamard, potrebbe risultare fortemente emblematico e niente affatto "casuale" : l'operatore di Toffoli infatti contiene tutti i fondamentali ingredienti di "classicità", essendo già da solo classicamente universale; di contro l'operatore di Hadamard, essendo genuinamente quantistico, racchiude uno stretto connotato quantistico. Ecco che l'insieme costituito da queste due porte può apparire come la sintesi più completa e essenziale tra universo computazionale classico e quantistico, rendendo così molto intuitiva l'idea che proprio queste due porte costituiscano un insieme approssimativamente universale in computazione quantistica.

Un volta individuati in Toffoli e Hadamard due operatori particolarmente significativi in computazione quantistica, passaggio naturale è risultato quello di cercare di ottenere una struttura logico-algebrica basata appunto su questi due operatori [15, 9], una struttura algebrica quindi in cui le operazioni consentite riproducano proprio il comportamento degli operatori Toffoli ed Hadamard.

Essendo costruita *ad hoc* sui due operatori, tale struttura è stata nominata "*algebra computazionale quantistica di Shi-Aharonov*". Si tratta di una struttura il cui universo è costituito dall'insieme di tutti gli operatori di densità (di arbitraria dimensione) e le cui uniche operazioni sono le operazioni quantistiche di Hadamard e Toffoli, oltre a tre elementi privilegiati: gli operatori di densità che rappresentano rispettivamente il *vero*, il *falso* e il *perfettamente indeterminato* (che corrisponde a uno stato la cui probabilità del "vero" corrisponde esattamente alla probabilità del "falso"). In tale struttura è definibile una relazione basata esclusivamente sulla probabilità degli operatori di densità del dominio e degli operatori di densità evoluti in seguito all'applicazione dell'operazione quantistica di Hadamard. Si dimostra come tale relazione sia un preordine il quale induce in modo canonico una relazione d'equivalenza che risulta essere una congruenza sull'algebra. Quozientando il dominio della struttura algebrica precedentemente introdotta rispetto a tale relazione[2], si ottiene [15, 9] un'algebra isomorfa alla più semplice *algebra quantistica computazionale*, il cui universo è dato dalle coppie di numeri reali che designano i punti all'interno di un

[2] Dato che la struttura algebrica è basata fondamentalmente sulla probabilità degli operatori di densità del dominio e degli operatori di densità evoluti in seguito all'applicazione dell'operazione quantistica di Hadamard, il quoziente permette di considerare come equivalenti tutti gli operatori di densità *equiprobabili* nei due sensi appena indicati.

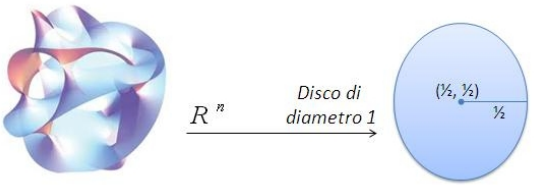

FIGURA 5: *Da* $\mathbb{R}^n$ *al disco*

disco di diametro unitario e centrato sul punto $(\frac{1}{2}, \frac{1}{2})$ e le cui operazioni sono le operazioni quantistiche di Toffoli e Hadamard, il cui dominio d'azione si riduce ai punti del disco sopra indicato (Fig. 5). I punti di questo disco sono ricavabili da considerazioni di carattere matematico riferite ad alcune proprietà della probabilità di un arbitrario operatore di densità.

Il significato intuitivo di tale risultato consiste in una notevolmente semplificazione dell'attività di ricerca delle proprietà logico-algebriche dell'insieme approssimativamente universale di Toffoli e Hadamard: il risultato descritto consente infatti di confinare la ricerca di tali proprietà a una struttura molto più semplice (che ha come universo il disco unitario) e di estendere successivamente ciascun risultato al ben piú ampio dominio degli operatori di densità di dimensione arbitraria.

Si noti infine come tale risultato si sia ottenuto non utilizzando il contesto unitario, bensì il più generale contesto delle operazioni quantistiche (che costituiscono le operazioni della struttura algebrica considerata) applicate a operatori di densità (che costituiscono il dominio della stessa struttura algebrica).

Le due operazioni che formano l'insieme approssimativamente universale che è stato introdotto sopra, derivano comunque da operatori unitari. Ma, in base alle considerazioni del paragrafo precedente, è possibile includere anche operazioni quantistiche che non derivino unicamente da operatori unitari e che magari corrispondano a funzioni di natura irreversibile.

5. Un nuovo strumento per trattare l'irreversibilità

Nel § 3 si è visto come da ogni operatore unitario sia possibile ottenere la corrispettiva operazione quantistica unitaria, che rappresenta ancora una volta una

evoluzione reversibile dell'operatore di densità a cui è applicata. Si è però notato come questo sia solo un caso particolare: esistono operazioni quantistiche che non risultano provenire da alcun operatore unitario e che quindi rappresentano un'evoluzione irreversibile. In questo paragrafo introdurremo una classe speciale di operazioni quantistiche, chiamate *operazioni quantistiche polinomiali*, che sono in grado di rappresentare, propriamente o approssimativamente, il comportamento di alcune particolari trasformazioni irreversibili di largo uso sia puramente teorico sia più applicativo [4, 3, 19, 9].

Una operazione quantistica polinomiale è definita in termini esclusivamente probabilistici: si dirà che un'operazione quantistica è polinomiale se e solo se esiste un polinomio a coefficienti reali e ad n variabili tale che per ogni n-pla di operatori di densità si ha che la probabilità dell'operazione quantistica applicata al prodotto tensoriale tra tutti gli n operatori di densità è uguale al valore che il polinomio assume quando a ciascuna delle n variabili è assegnata come interpretazione il valore di probabilità di ciascuno degli n operatori di densità. Dal punto di vista intuitivo, una operazione quantistica polinomiale può essere immaginata come quell'operazione che rappresenterebbe una evoluzione di tipo polinomiale di un determinato sistema quantistico. L'importanza di considerare evoluzioni polinomiali è dovuta al fatto che, se il polinomio non è una funzione iniettiva, questo rappresenta un'evoluzione di tipo irreversibile, in quanto partendo da stati iniziali differenti si può giungere allo stesso stato finale. L'introduzione delle operazioni quantistiche polinomiali risulta essenziale per quel teorema [24] in cui si mostra come esista sempre una operazione quantistica polinomiale in grado di rappresentare probabilisticamente una qualunque funzione polinomiale che rispetti le seguenti condizioni:

- i coefficienti del polinomio sono compresi tra i valori 0 e 1;
- la restrizione della funzione per valori compresi tra 0 e 1 assume a sua volta valori compresi tra 0 e 1.

Successivamente, in una versione ulteriormente affinata del teorema [12] si mostra come esista sempre un'operazione quantistica polinomiale in grado di rappresentare in maniera approssimata, cioè *a meno di una costante*, il comportamento di una qualsiasi funzione continua (e quindi non necessariamente polinomiale) che rispetti le due stesse condizioni elencate sopra. A corredo di questo risultato vi è un ulteriore teorema di convergenza che mostra come il valore della costante che sancisce l'accuratezza dell'approssimazione possa essere arbitrariamente piccolo. Il prezzo che però bisognerà pagare sarà il sempre più elevato

grado di complessità dell'operazione quantistica approssimante. Dal punto di vista strettamente intuitivo, il teorema appena introdotto consente di affermare che: se un sistema fisico evolve secondo una funzione polinomiale (reversibile o irreversibile) che soddisfa determinati requisiti, allora è sempre possibile costruire un circuito quantistico che rappresenti (a limite in maniera approssimata) l'evoluzione di tale sistema.

L'attenzione verso la rappresentazione operazionale in chiave quantistica di determinate funzioni irreversibili, è suggerita dall'esigenza di offrire una rappresentazione fisica di alcune particolari funzioni note come *norme triangolari* o, più brevemente, *t*-norme. Le *t*-norme sono funzioni in due variabili nell'intervallo reale $[0,1]$ che soddisfano i requisiti di commutatività, associatività, monotonia; inoltre 1 deve fungere da elemento neutro e 0 da annichilatore. Queste funzioni hanno trovato presto largo uso in ambiti di ricerca anche molto vari: dalla fisica delle particelle alla statistica, dalla teoria dei giochi fino alla teoria del pensiero critico [7, 14, 16, 20]. Le *t*-norme sono utilizzate per interpretare il connettivo di congiunzione nell'ambito delle logiche fuzzy [17, 28], i cui valori di verità non sono soltanto il *vero* (indicato, in maniera usuale, col numero 1) o il *falso* (indicato con lo 0), ma tutti i possibili valori "intermedi" tra essi compresi. La logica fuzzy ha trovato numerose applicazioni in ambito elettronico: i *sistemi di controllo fuzzy* costituiscono infatti una alternativa ai sistemi digitali ed hanno consentito la realizzazione di strumenti di uso quotidiano (quali lavatrici, macchine fotografiche, condizionatori) contando su un'elettronica in cui il segnale è rappresentato da un numero appartenente all'intervallo continuo compreso tra il valore 0 ed il valore 1. Tale idea, in realtà, richiama immediatamente il significato di bit quantistico introdotto all'inizio di questo lavoro.

Tre *t*-norme di particolare importanza sono le seguenti:

- la *t*-norma Prodotto (che corrisponde proprio al prodotto algebrico);
- la *t*-norma di Łukasiewicz;
- la *t*-norma di Gödel (che corrisponde al *minimo*).

L'importanza è legata al fatto che, tramite l'utilizzo esclusivo di queste tre *t*-norme è possibile esprimere, in un senso appropriato, qualsiasi altra *t*-norma continua. Inoltre, è importante notare come la rispettiva definizione in termini funzionali di ciascuna di queste tre, corrisponda a una evoluzione di tipo strettamente irrervesibile. Ecco che esprimere queste tre *t*-norme in termini di operazioni quantistiche sancisce la stesura di un forte legame tra gli studi in ambito quantistico computazionale e il vasto ambito relativo alle logiche polivalenti.

La prima versione del teorema che è stato sopra descritto permette in maniera quasi immediata di rappresentare la *t*-norma prodotto come operazione quantistica polinomiale. Essendo infatti il prodotto algebrico già di per sé un polinomio (che rispetta i vincoli preposti), è direttamente possibile ottenere l'operazione quantistica che ne rappresenti il comportamento. Per far questo è dunque sufficiente ricorrere alla prima versione del teorema che permette di ottenere una rappresentazione *esatta* (e non approssimata) della *t*-norma Prodotto come operazione quantistica polinomiale.

Discorso differente va fatto per le altre due *t*-norme che, pur essendo funzioni continue, non corrispondono ad alcuna espressione polinomiale. Ecco che, per rientrare nelle condizioni richieste dalla seconda versione del teorema, è risultato necessario ricorrere a un passo preliminare: tramite strumenti analitici è stato possibile approssimare tali *t*-norme ad altre funzioni che però rispettassero le condizioni richieste dal teorema. Si sono così ottenute due operazioni quantistiche in grado di riprodurre in maniera approssimata, ma arbitrariamente accurata, il comportamento sia della *t*-norma di Łukasiewicz che della *t*-norma di Gödel.

6. Conclusione

L'obiettivo di questo lavoro è stato quello di presentare in maniera generale ma dettagliata, volutamente senza il coinvolgimento di dettagli formali, le caratteristiche peculiari di una struttura che permette innanzitutto di rappresentare sistemi fisici aperti (consentendo così di tener conto delle svariate interazioni tra sistema fisico e ambiente circostante) e anche la loro evoluzione, eventualmente di natura irreversibile. Questi risultati possono rappresentare un punto di incontro tra sistemi fisici reali e teoria computazionale quantistica la quale, seppur altamente predittiva, appariva praticamente descrittiva solo di sistemi fisici estremamente schermati da qualsiasi tipo di interazione esterna e le cui evoluzioni fossero strettamente di natura reversibile. Cioè, in sostanza, sistemi fisici ideali.

I risultati descritti nell'ultimo paragrafo, infine, aprono a nuove interessanti prospettive di ricerca nell'individuazione di insiemi di operazioni quantistiche approssimativamente universali: sarebbe infatti interessante individuare un insieme approssimativamente universale costituito (totalmente o in parte) da ope-

razioni quantistiche non unitarie. Tale possibilità, oltre a rappresentare una sostanziale novità dal punto di vista teorico, offrirebbe l'opportunità di disporre di un modello teorico pensato appositamente in risposta all'esigenza di tener conto delle inevitabili interazioni del sistema con l'ambiente e, per questo, risulterebbe più adeguato dal punto di vista dell'implementazione ed offrirebbe nuovi stimolanti prospettive dal punto di vista applicativo.

RINGRAZIAMENTI. Il presente lavoro di ricerca è stato finanziato dalla Regione Autonoma della Sardegna, POR Sardegna FSE-M.S. 2007-2013 L.R. 7/2007. Desidero ringraziare Roberto Giuntini e Francesco Paoli per i numerosi e preziosi suggerimenti, utili sia per il conseguimento dei risultati riassunti nel presente articolo sia per la stesura dello stesso.

Riferimenti bibliografici

[1] P. Adrien, M. Dirac. *The principles of Quantum Mechanics*. Oxford University Press, 1981.

[2] D. Aharonov. "A simple proof that Toffoli and Hadamard are quantum universal". [arXiv:quant-ph/0301040v1], 2003.

[3] E. Beltrametti, G. Cassinelli. *The logic of quantum mechanics*. Encyclopedia of Mathematics and its Applications, Vol. 15. Addison-Wesley, Reading, Massachusetts, 1981.

[4] J. Berchtold, A. Bowyer. "Robust arithmetic for multivariate Bernstein-form polynomials". *Computer Aided Design*, 32, pp. 681–689, 2000.

[5] S. L. Braunstein. *Quantum computing: where do we want to go tomorrow?*. Wiley-VCH, 1999.

[6] H. P. Breuer, F. Petruccione. *The Theory of Open Quantum Systems*. Oxford University Press, 2002.

[7] D. Butnariu, E. P. Klement. "Triangular Norm-Based Measures and Games with Fuzzy Coalitions". Kluwer Academic Publishers, Dordrecht, 1993.

[8] C. Cohen-Tannoudji, B. Diu, F. Laloe. *Quantum Mechanics*. Wiley-Interscience, 2006.

[9] M. L. Dalla Chiara, R. Giuntini, H. Freytes, A. Ledda, G. Sergioli. "The algebraic structure of an approximately universal system of quantum computational gates". *Foundations of Physics*, 39, 6, 2009.

[10] D. Deutsch. "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 400 (1818), pp. 97–117, 1985.

[11] D. Deutsch, A. Barenco, A. Ekert. *Universality in Quantum Computation. Proc. Royal Society London A*, 449, pp. 669–677, 1980.

[12] H. Freytes, G. Sergioli, A. Aricò. "Representing continuous t-norms in quantum computation with mixed states". *Journal of Physics A: mathematical and theoretical* 43, 465–306, 2010.

[13] R. Feynman. "Simulating physics with computers". *International Journal of Theoretical Physics*, 21(6), pp. 467–488, 1982.

[14] J. Fodor, M. Roubens. "Fuzzy Preference Modeling and Multicriteria Decision Support". Kluwer Academic Publishers, Dordrecht, 1994.

[15] R. Giuntini, F. Paoli, A. Ledda, G. Sergioli. "Some generalizations of fuzzy structures in quantum computational logic". *International Journal of General Systems*, 40, 1, pp. 61–83, 2009.

[16] M. Grabisch, H. T. Nguyen, E.A. Walker. *Fundamentals of Uncertainty Calculi with Applications to Fuzzy Inference*. Dordrecht, Kluwer, 1995.

[17] P. Hájek. *Metamathematics of Fuzzy Logic*. Kluwer, Dordrecht,, 1998.

[18] A. Y. Kitaev, A. H. Shen, M. N. Vylayi. *Classical and Quantum Computation*. AMS Bookstore, 2002.

[19] A. Ledda, G. Sergioli. "Towards quantum computational logics". *International Journal of Theoretical Physics*, 49 (12), pp. 3158–3165, 2010.

[20] K. Menger. “Statistical metrics”. *Proceedings of the National Academy of Sciences*, 37, pp. 57-60, 1942.

[21] A. Messiah. *Quantum Mechanics*. Courier Dover Publications, 1999.

[22] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[23] J. G. Rarity, P. R. Tapster, E. Jakeman, T. Larchuk, R. A. Campos, M. C. Teich, B. E. A. Saleh. “Two-photon interference in a Mach-Zehnder interferometer”. *Physical Review Letters*, 65, pp. 1348–1351, 1990.

[24] G. Sergioli, A. Ledda, H. Freytes. “Continuous functions as quantum operations: a probabilistic approximation”. *Logic & Philosophy of Science*, 3, 4, pp. 1–17, 2010.

[25] Y. Shi. “Both Toffoli and controlled-not need little help to do universal quantum computation”. [arXiv:quant-ph/0205115v2], 2002.

[26] T. Toffoli. “Reversible computing”. In *Automata, Languages and Programming* a cura di J. W. de Bakker e J. van Leeuwen, Springer, pp. 632-644, 1980.

[27] A. M. Turing. “Computability and λ-definability”. *The Journal of Symbolic Logic*, 2, 4, pp. 153–163, 1937.

[28] L. Zadeh “Fuzzy sets”. *Information and Control*, 8, pp. 338–353, 1965.

L&PS – Logic & Philosophy of Science
Information on the Journal

Aims and contents

L&PS – Logic and Philosophy of Science is an on-line philosophical journal sponsored by the Department of Humanistic Studies of the University of Trieste (Italy). The journal promotes both theoretical and historical research in the philosophy of science and logic, without excluding any particular cultural perspective.

Topics welcomed by the journal include:

– the theory of scientific knowledge and the analysis of the general methodological problems of science (such as scientific discovery, causation, scientific inference, induction and probability, the structure of scientific theories and their relations with empirical data);
– the methodological and foundational problems of the different sciences, from the natural, to the biomedical, to the social sciences;
– the problems related to the historical development of logic, in all its branches, and to the role of logical methods both in the general methodology of science and in the foundations of empirical and mathematical sciences;
– the philosophical problems raised by the development of the cognitive sciences and the philosophy of mind, with particular attention to those results that are relevant for the analysis of scientific practice;
– the epistemological problems related to Artificial Intelligence, robotics, virtual reality, and artificial life;
– the problems in the sociology and the history of science that are relevant to the philosophical investigation of science;
– the problems related to the ethics of science;
– the questions related to the historical and conceptual development of the philosophy of science and logic;
– the problems of the philosophy of language, with particular attention to those results that are relevant for logic and philosophy of science.

Information for the authors

Papers submitted to the journal must be written either in Italian or in English, and must be accompanied by a short summary in English (and also in Italian for the articles written in Italian). All papers will be evaluated by anonymous referees.

In order to promote critical discussion and exchange among scholars, the journal is willing to publish reports on work in progress, to be submitted and evaluated according to the criteria already mentioned above.

The copyright is left to the authors, provided that any reprint of the paper explicitly mentions the version previously published in L&PS.