International Journal of Theoretical Physics, Vol. 42, No. 3, March 2003 (© 2003)

Foundation for Quantum Computing

S. A. Selesnick[1]

Received February 6, 2003; accepted February 19, 2003

In this paper we introduce a minimal formal intuitionistic propositional Gentzen sequent calculus for handling quantum types, quantum "storage" being introduced syntactically along the lines of Girard's *of course* operator !. The intuitionistic fragment of orthologic is found to be translatable into this calculus by means of a quantum version of the Heyting paradigm. When realized in the category of finite dimensional Hilbert spaces, the familiar *qubit* arises spontaneously as the irreducible storage capable quantum computational unit, and the necessary involvement of quantum entanglement in the "quantum duplication" process is plainly and explicitly visible. Quantum "computation" is modelled by a single extra axiom, and reproduces the standard notion when interpreted in a larger category.

KEY WORDS: quantum computing; quantum logic; mathematical logic.

1. INTRODUCTION

Quantum computers effect computations by exploiting the subtle laws of quantum physics: a profound qualitative shift from classical computational paradigms. Quanta are not objects in the ordinary sense, and their manipulation is not mechanistic in the sense that the movements of beads, pebbles, cog-wheels, chalk, or graphite particles—or even currents within a solid-state device—are. Although ordinary computers use small components whose size begins to encroach upon the domain where quantum effects may have a bearing on their physical behavior, their operations *qua* computational elements—implementing as they do Boolean operations upon arrays of notional bits—are entirely classical.

Indeed, it is perfectly clear that ordinary "classical" computational devices (knotted cords, slide rules, Macintoshes, . . .) require for their use (or programming) *no* knowledge of the physical laws underlying their operations as physical entities existing in the world. Of course, these devices operate according to the laws of physics but these laws are not *themselves* exploited in the course of such an operation or computation: it is not necessary—and would be absurd—to preface

[1] Department of Mathematics and Computer Science, University of Missouri-St. Louis, St. Louis, Missouri 63121; e-mail: selesnick@mindspring.com.

0020-7748/03/0300-0383/0 © 2003 Plenum Publishing Corporation

the definition of a Turing machine, say, with a summary of the laws of classical physics. The same (classical) computation could, in principle, be performed by any sufficiently complex device, regardless of the nature of its physical instantiation. In this sense, the notion of a "classical" computation seems more abstract than the quantum notion since the underlying physics has been abstracted away in the classical case, whereas it seems to be part and parcel of the current quantum computational paradigm.

This circumstance has the appearance of necessity, since, as macroscopic experimenters, we have come upon the quantum domain only recently, and our apprehension of it depends upon delicate and complicated instrumental interfaces. In consequence, the foundations of current quantum computational theory have both an ad hoc and a post hoc appearance, conditioned as they are by classical thinking about computation and additionally encumbered by the interpretative burdens of standard quantum theory. For example, all quantum computational considerations spring from an assumption about the nature of the basic quantum computational unit. This is universally accepted to be what is now referred to as *the qubit:* namely an idealized quantum system having a two-dimensional Hilbert space of states. This is, obviously, the quantized version of the two-state classical computational unit known as the bit, the basic Boolean logical unit. In attempting to provide a *logical* foundation for a theory of quantum computation the argument that the qubit should be taken as the fundamental unit *because* it is the quantization of the classical Boolean bit is clearly Whiggish. If quantal things underlie classical things, then the bit should appear in the macrocosm *because* it is the degenerate macroscopic limit of the more fundamental qubit, and not *vice versa*. Thus, one should seek a *more* fundamental theory of quantum computation that yields up the qubit as the basic quantum computational unit without explicit recourse to specific classical prototypes.

The student of "quantum computing" is indeed faced with a daunting task, as Hirvensalo (2001) notes: an understanding of the fundamentals of the two most notoriously counterintuitive disciplines known to Mankind—namely quantum theory and the theory of computation—must be gained at the outset. Moreover, it is exactly the *most* counter intuitive aspects of quantum theory, which lie at the heart of the current quantum computational ideal.

No such epistemological hurdles obstruct the path to an understanding of theories of classical computation, as we have noted. In this paper and its sequels we attempt to redress this asymmetry; that is to say, we attempt to lay a foundation for an abstract theory of quantum computing from the bottom up, the bottom being a certain variant of standard quantum logic. At the foundational level, the theory is essentially independent of physical considerations, except insofar as these are already present in the axioms of quantum logic.

The layout of the paper is as follows: Section 2 consists of a minimal introduction to those elements of standard nonquantum natural deduction and proof

theory that will be extended to the quantum case in Section 3. The latter section contains a brief overview of those parts of quantum logic that will be relevant in the attempt to construct a minimal calculus for managing quantum "resources." It becomes apparent from these considerations that the classical Heyting paradigm fails in the quantum case.

In Section 3.3 we introduce a purely syntactic minimal intuitionistic Gentzen sequent calculus based upon presumed properties of quantum types, or *resources*, and show (Section 3.4) that a translation of the intuitionistic fragment of orthologic into this calculus may be affected simply by invoking a *quantum* version of the Heyting paradigm. The calculus is then interpreted in the category of finite dimensional Hilbert spaces, with the aid of Grassmannian quantum set theory (Section 3.5).

In Section 4.1 we specify a one-step "quantum computation" purely syntactically in the sequent calculus through the introduction of a single extra axiom. When this axiom is realized in the category of finite dimensional Hilbert spaces, the familiar *qubit* arises spontaneously as the irreducible storage capable quantum computational unit.

The notion of quantum storage, accompanied by the concomitant dual notion of quantum copying or duplication, emerges directly from a consideration of the rule of Contraction as it is realized in our sequent calculus, and the need to invoke quantum entanglement in the course of implementing it is immediately apparent. This is discussed briefly in Section 4.2.

In Section 4.3 we subvert our constructivist quantum principles in an attempt to accommodate classical time as the multiplexed storage capable version of the symbolic time quantum, or step, used in the newly added axiom. Although they are rather formal, these maneuvers reproduce (in a fairly natural manner) the standard picture of a quantum computation as being a one-parameter unitary dynamical group acting in the Schrödinger manner upon a tensor product of qubits.

2. CLASSICAL COMPUTATIONAL PARADIGMS

2.1. Natural Deduction

The irreducible essence of any kind of computation is the act of reducing an expression to another expression according to an agreed upon set of rules. A prescribed set of *atomic* expressions, together with a set of rules for manipulating or rewriting them, comprises the backbone of what is known as a *deductive system*. The study of such systems has come to occupy a significant sector of the modern theory of computation.

A *deduction* (or *derivation*) in such a system is a sequence of rule-based replacements (or rewrites) of expressions starting from a set specified as *axioms*. One may view such a deduction geometrically in various ways: as tree-like, for

example, with axioms as leaves and the concluding expression as the root. Although we have been vague about the nature of the "expressions" involved, it should already be clear that a deduction is very much like a (computer) program, which proceeds in steps to reconfigure patterns of data.

The expressions of interest are, of course, those to be found at the roots of deductions and it is important to remark on the obvious fact that these are produced by entirely *constructive* processes. A derived expression may be specified—in the sense that it may be *constructed*—from the axioms together with the particular deduction tree at whose root it sits. Clearly, this association (of derived expression with deduction tree) is not one-to-one, since a given expression may have many deductions (or, indeed, none). From a constructivist viewpoint it would be better to associate a derived expression with the *set* of deductions leading to it. This kind of association lies at the heart of Heyting's interpretation of intuitionistic logic as that logic which arises from a wholesale adherence to constructivist principles (cf. Section 2.2).

Insofar as we deal with logic per se in this paper we shall deal only with *propositional* logic: that is, we ignore quantification ($\forall$, $\exists$) entirely. However, there is no doubt that a full treatment along the lines to be advocated in this work should include quantification (cf. Finkelstein, 1996).

In this section we informally explore some of the issues associated with deduction by examining a certain system known as *natural deduction*. Specifically, we shall discuss the natural deduction system for minimal implicational intuitionistic (propositional) logic. This treatment combines elements from the early chapters of both Girard *et al*. (1988) and Troelstra and Schwichtenberg (2000).

The basic object of interest in this system is a *deduction* of a *formula* (or *sentence*) A, say, which, after Girard *et al*. (1988), we shall denote by

$$\begin{array}{c} \vdots \\ A \end{array} \tag{2.1}$$

The dots stand for subdeductions, and the whole structure is to be regarded as a finite tree, or at least as being tree-like, since the tree structure will soon be vitiated.

The first rule of deduction, or *inference*, is that a single formula by itself is a deduction (of itself). Strictly speaking, this axiom should be asserted only for a set of *atomic* formulae: the result then follows for all formulae. We will follow custom in this abbreviated overview by omitting the complication of specifying the atoms at this stage.

There are two other rules of inference, which enable new deductions to be constructed from old ones. One rule *introduces* the implication sign $\Rightarrow$ and the other rule *eliminates* it. The expression of these rules requires some notational preliminaries. Suppose A appears in a *single* top node (or *leaf*) of a deduction

whose *conclusion* is B. Then we may unambiguously write

$$\begin{array}{c} A \\ \vdots \\ B \end{array} \tag{2.2}$$

In this case, the rule of introduction posits a new deduction:

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \Rightarrow B} \Rightarrow I \tag{2.3}$$

(Here, the $\Rightarrow I$ labels the rule being used—namely "$\Rightarrow$ introduction"—to extend the tree: it is frequently dropped when ambiguity does not threaten.)

The *occurrence* of A is said to be *open* (or *live*) in (2.2) but considered to be *closed* (or *killed*, or *discharged*) by the application of $\Rightarrow I$ in (2.3). The open occurrences of a formula like A in (2.3) are said to be *hypotheses* for the deduction.

Now, A may appear and be open in other places, for instance in ambient deductions, and in this case we would wish to keep track of which open occurrence of A is being discharged at the $\Rightarrow I$ inference. This can be accomplished by labelling A and then invoking the label at the point of inference. Thus, in place of (2.3) we now write

$$\frac{\begin{array}{c} A^u \\ \vdots \\ B \end{array}}{A \Rightarrow B} u, \Rightarrow I \tag{2.4}$$

As noted, it is possible that open occurrences of A may appear a number of times in the deduction leading to B, and we may choose to discharge a collection of these at the inference. The deductions leading to those occurrences of A in the chosen collection are all then discarded simultaneously at the inference. Members of such a collection may be grouped under a single label, since there is no need to distinguish among these discarded deductions. The notation for such a collection of open occurrences of A is $[A]^u$. Of course, there may be other collections of open occurrences of A that are not chosen for discharge at the inference: these remain open after it.

The complete statement of the $\Rightarrow I$ rule now reads

$$\frac{\begin{array}{c} [A]^u \\ \vdots \\ B \end{array}}{A \Rightarrow B} u, \Rightarrow I \tag{2.5}$$

(Here the degenerate case of $[A]^u$ being empty is allowed. This empty case would still require a label at the inference. Thus,

$$\frac{B}{A \Rightarrow B} v \tag{2.6}$$

is a legal deduction. The v labels the empty class of occurrences, which is discharged at the inference.)

There is some linguistic awkwardness in referring to $[A]$ since it denotes a pattern of *occurrences* of the formula A and is not, strictly speaking, a *set*.

The other rule of inference in this system, which is a rule for eliminating $\Rightarrow$, is just *modus ponens*, and may be rendered as

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A & A \Rightarrow B\end{array}}{B} \Rightarrow E \tag{2.7}$$

Here, two deductions—of A and $A \Rightarrow B$—are combined to produce a new deduction with conclusion B. The hypotheses of the two subdeductions above the inference line, taken together, are the hypotheses of the new deduction (2.7).

(There are natural ways to simplify certain deductions. For instance, a deduction of the form

$$\frac{\begin{array}{cc} & [A]^u \\ \vdots & \vdots \\ A & \frac{B}{A \Rightarrow B} u\end{array}}{B} \tag{2.8}$$

may be replaced by the following simpler direct deduction, considered to be equivalent to it:

$$\begin{array}{c}\vdots \\ [A] \\ \vdots \\ B\end{array} \tag{2.9}$$

The understanding here is that each (discharged) occurrence of A in $[A]^u$ (in (2.8)) has been replaced by a copy of the new deduction of A introduced on the left (in (2.8)).)

2.2. Heyting Paradigm and Curry–Howard Isomorphism

The constructive notion of implication introduced in the preceding text is not the ordinary implication of ordinary propositional calculus (PC), about which we will have more to say in Section 3. Rather, it should be interpreted intuitionistically in light of the so-called *Heyting paradigm* (Heyting, 1956), which gives a semantics

for formal intuitionistic logic (IL) (cf. Troelstra and Schwichtenberg (2000, Section 2.5.1, p.55), where the attribution also includes Brouwer and Kolmogorov). In this interpretation of IL, a formula is intuitionistically *valid* only if a deduction can be explicitly presented or constructed. The interpretation of $A \Rightarrow B$ in (2.4) then becomes—if a deduction of A^u can be constructed then a deduction of B can be constructed, *via* the deduction above the inference line in (2.4). After this encapsulation of the whole process in the formula $A \Rightarrow B$, the open assumption A^u is no longer needed and may be discharged (or closed), the deduction leading to it being, in a sense, discarded.

In the previous section labels were introduced merely to keep track of the flow of closings of collections of open formulae as the $\Rightarrow I$ inference is enacted. (As Girard et al. (1988) observes the link this labelling scheme sets up between formula and inference point effectively destroys the illusion of a tree-like structure.) The significance of this apparently innocent labelling scheme may be realized by another appeal to the Heyting paradigm. Since, in this interpretation of IL a formula is intuitionistically *valid* only if a deduction of it can be produced, a formula may be *identified* with its set of deductions. In more formal terms, a formula determines a *type*, A say, and a label u of A is considered to be a *variable* of type A, for which the standard notation is $u{:}A$. (Formal definitions of types, terms, variables, etc., may be found in the works cited in the preceding text. For our purposes in this note the informal intuitive notion of a type as being a special kind of set, while variables refer to elements of such sets, etc., will suffice.) Returning to the labelling scheme of the last section, we note that the label u in A^u could be regarded as standing in for a generic deduction of A: it is in fact not merely A that is being labelled but a deduction of A. In view of the Heyting interpretation, A^u can be rewritten as $u{:}A$. Similarly, the u in $[A]^u$ stands in for generic deductions of the occurrences of A in the collection $[A]$, which are all "discarded" simultaneously at the inference. Consequently, $[A]^u$ can be rewritten as $[u{:}A]$.

Now that u is being regarded as a variable of type A, this status should be recorded at the point of inference in (2.5). Likewise, the variable of type B corresponding to the deduction of B, which appears above the inference line in (2.5), and which "depends" upon the deduction of A labelled by u, should also be explicitly annotated. Then, (2.5) may be rewritten as

$$\frac{\begin{array}{c}[u{:}A]\\ \vdots \\ [t{:}B]\end{array}}{\lambda u.t{:}A \to B} \tag{2.10}$$

Here, the symbol λ serves to *bind* u within t. The type $A \to B$ is the indicated "function" type, which, in terms of sets, is the set of *functions* from A into B. As noted in the last section, the Heyting paradigm interprets intuitionistic implication

$A \Rightarrow B$ as a function from the set of deductions of the formula A to the set of deductions of the formula B.

The expression $\lambda u.t$ is the name of the function (of type $A \to B$) that produces t upon the "input" of u.

Note also that the binding of u within t *via* the symbol λ in the expression $\lambda u.t$ recapitulates *exactly* the discharging of the associated formula occurrences.

Similarly, the inference rule (2.7), which eliminates $\Rightarrow$, may be rewritten in type theoretic terms as

$$\frac{\begin{array}{cc}\vdots & \vdots \\ s{:}A & t{:}A \to B\end{array}}{ts{:}B} \tag{2.11}$$

where *ts* denotes *application* of the function type t to s.

Using these translations of the inference rules, any deduction may be used to generate a "λ-term," which completely describes, or encapsulates, the deduction. For example, consider the pattern of discharges in the following two deductions of $A \Rightarrow (A \Rightarrow A)$ (from Troelstra & Schwichtenberg, 2000, p. 25):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A^w} \quad \dfrac{\dfrac{}{A^u}}{A \Rightarrow A}\,v}{A}}{A \Rightarrow A}\,u}{A \Rightarrow (A \Rightarrow A)}\,w \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A^w} \quad \dfrac{\dfrac{}{A^u}}{A \Rightarrow A}\,u}{A}}{A \Rightarrow A}\,w}{A \Rightarrow (A \Rightarrow A)}\,v \tag{2.12}$$

(cf. (2.6) for the label v in both cases.) An application of the translation rules given above to the left-most deduction in (2.12) yields

$$\dfrac{\dfrac{\dfrac{\dfrac{}{u{:}A}}{w{:}A \quad \lambda v.u{:}A \to A}}{(\lambda v.u)w{:}A}}{\lambda u.(\lambda v.u)w{:}A \to A}}{\lambda w.(\lambda u.(\lambda v.u)w){:}A \to (A \to A)} \tag{2.13}$$

The reader may check that the the translation of the right-most deduction in (2.12) yields the nonequivalent λ-term:

$$\lambda v.(\lambda w.(\lambda u.u)w){:}A \to (A \to A). \tag{2.14}$$

The calculus of λ-terms (without explicit typing) was posited independently by Church in the 1930s as a means of investigating the computational and logical possibilities of pure functionality. Today the theory goes by the name "simply-typed λ-calculus." The observation, by Curry and Feys (1958), that the translation given above induces a complete structural isomorphism between the minimal natural deduction system outlined in Section 2.1 and simply-typed λ-calculus, apparently came as a surprise to logicians.

Readers familiar with λ-calculus may note that the contraction of deduction (2.8) to deduction (2.9) corresponds to the replacement of an expression of the form $(\lambda u.t)s$ by the expression $t[u/s]$, where the notation means that u is to be replaced by s in t. This is known as β-conversion in the λ-calculus context (modulo many glossed details) and is the basic rule for evaluating functions.

The computational resources of simply-typed λ-calculus and other λ-calculi) have been well studied: see for example Asperti and Longo (1991), Girard *et al*. (1988), Gunter (1992), Mitchell (1996), Stoy (1977), and Troelstra and Schwichtenberg (2000) among many others.

The isomorphism sketched above may be extended to one that obtains between the minimal intuitionistic implicational deductive fragment of Section 2.1 with inference rules for conjunction ($\wedge$) and disjunction ($\vee$) appended, and an appropriately supplemented version of simply-typed λ-calculus.

For example, the inference rules for conjunction are three in number (one Introduction and two Eliminations), namely

$$\frac{A \quad B}{A \wedge B} \wedge I \tag{2.15}$$

$$\frac{A \wedge B}{A} \wedge 1E \qquad \frac{A \wedge B}{B} \wedge 2E \tag{2.16}$$

There are identifications among certain deductions involving $\wedge$. For example,

$$\frac{\begin{array}{cc}\vdots & \vdots \\ A & B\end{array}}{\frac{A \wedge B}{A}} \quad \text{is identified with} \quad \begin{array}{c}\vdots \\ A\end{array} \tag{2.17}$$

and similarly for the other elimination rules.

Disjunction in an intuitionistic system is independent of conjunction (since De Morgan duality does not obtain) and is generally contentious. In our system there are two Introduction rules, namely

$$\frac{A}{A \vee B} \vee 1I \quad \text{and} \quad \frac{B}{A \vee B} \vee 2I \tag{2.18}$$

and one problematical Elimination rule, namely:

$$\frac{\begin{array}{ccc} & [A] & [B] \\ \vdots & \vdots & \vdots \\ A \vee B & C & C\end{array}}{C} \vee E \tag{2.19}$$

The problem here is the extraneous C, which introduces an uncontrollable element into the business of deriving general theorems about deductions (see Girard *et al*., 1988, Ch. 10).

To extend the Curry isomorphism to this supplemented natural deduction system, we again appeal to the Heyting paradigm. For the conjunction $A \wedge B$ to be intuitionistically valid, we must possess a deduction of A *and* a deduction of B, and know which deduction belongs to which formula; that is, we must possess an ordered pair of deductions. If a formula is identified with its set of deductions, then the set of deductions of $A \wedge B$ should be identified with the product of the set of deductions of A and the set of deductions of B.

Thus, the $\wedge$ of formulae should be associated, in the extended correspondence, with the product, $\times$, of the corresponding types.

Similarly, $A \vee B$ is intuitionistically valid only if we have a deduction of A *or* a deduction of B, and an indication of *which* one of these formulae has been deduced. The collection of such pairs constitutes the disjoint union (or direct sum in the category of sets) of the sets of deductions of the constituent formulae.

Thus, the $\vee$ of formulae should be associated, in the extended correspondence, with the sum, $+$, of the corresponding types.

The Curry correspondence thus extended is part of W. A. Howard's contribution to the full isomorphism, which now bears the name Curry–Howard (cf. Troelstra and Schwichtenberg (2000, p. 59). The other part of Howard's contribution to the isomorphism involves quantifiers, which we are ignoring here.)

The importance to computational theory of isomorphisms of the Curry–Howard type is that, since formulae may be regarded as types through their use, *deductions* may be concomitantly regarded as *computations* (or *programs*), which transform types (patterns of data) into types in stepwise fashion. Reversing this perspective, such isomorphisms allow us to regard the apparently static program represented by a λ-term in a dynamical light, since such a term may be unfolded to reveal the underlying deductive structure, with its flow of openings and closings of assumptions. It is this aspect of the Curry–Howard isomorphism that arguably has had the most impact.

2.3. The Gentzen Sequent Calculus

The Gentzen sequent calculus may be regarded initially as a metacalculus for handling deductions in natural deduction systems, though it has been developed in various directions as a style of deductive reasoning in its own right. In its guise as a metacalculus for natural deduction, the sequent calculus delineates certain symmetries and structural aspects of the underlying deductive system which remain hidden, or at least less apparent, if one remains fixed at the natural deduction level. This organizing power of the style has had a major impact on the proof theoretic aspects of deductive logic.

The basic object is the *sequent*

$$\Gamma \vdash \Delta \tag{2.20}$$

in which Γ and Δ stand for (possibly empty) finite sequences of formulae. (Empty sets of formulae are usually denoted by their omission, as in $\Gamma \vdash$, which is Eq. (2.20) with Δ empty.) It is possible—and indeed advisable—to allow more general assemblages of formulae. This becomes apparent when natural deduction is used as the underlying model: then Γ, etc., would stand for collections of formula occurrences. The use of sequences will suffice for our purposes. Upper case Greek characters will have this (standard) connotation in our discussions of sequents.

The informal reading of (2.20) is along the lines of "$\bigwedge\Gamma \Rightarrow \bigvee\Delta$." This reading can be adduced from the natural deduction model, if (2.20) is supposed to describe a deduction with a set Γ of hypotheses and conclusion in Δ: it forces the interpretation of $\vdash \Delta$ as asserting the truth of $\bigvee\Delta$ and $\Gamma \vdash$ as asserting the falsity of $\bigwedge\Gamma$. (In keeping with this model, and noting again the disruptive effects of disjunction in intuitionistic systems, sequents in which Δ consists of at most a single formula are termed "intuitionistic.")

In Gentzen calculi the inference rules are often divided into classes: structural rules, logical rules and an "identity group." A deduction in sequent calculus is usually referred to as a *proof*.

By way of example, we shall briefly describe the rules for a non-intuitionistic minimal propositional sequent calculus. (The horizontal line in a rule represents the inference of the sequent below it from the sequent or sequents appearing immediately above it.)

Structural Rules

These refer to the management of formulae within sequents. (The appropriate label appears to the right of the inference line, as in natural deduction: LE for left exchange, etc.)

Exchange

$$\frac{\Gamma, A, B, \Gamma' \vdash \Delta}{\Gamma, B, A, \Gamma' \vdash \Delta}\ \text{LE} \qquad \frac{\Gamma \vdash \Delta, A, B, \Delta'}{\Gamma \vdash \Delta, B, A, \Delta'}\ \text{RE} \tag{2.21}$$

Weakening

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ \text{LW} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ \text{RW} \tag{2.22}$$

Contraction

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ \text{LC} \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ \text{RC} \tag{2.23}$$

These rules appear quite innocent at first sight: they are what one would expect from the presumed properties of $\wedge$ and $\vee$ in the informal reading of the sequent $\Gamma \vdash \Delta$ as "$\bigwedge\Gamma \Rightarrow \bigvee\Delta$." They appear less innocent in the reading of $\Gamma \vdash \Delta$ as a

description of a deduction in a natural duction system of the type described in the last section. In this reading, Weakening corresponds to the possibility of introducing spurious or null collections of occurrences of a formula A, while Contraction corresponds to the possibility of amalgamating certain collections of occurrences of A. Further innocence is lost, as Girard *et al*. (1988) points out, in an *operational* reading of the sequent calculus. In this reading, formulae, considered as types *à la* Curry–Howard, are regarded as *resources*, and $\Gamma \vdash \Delta$ has the informal interpretation: "Use up Γ to produce Δ." Then LC (2.23), for example, has the connotation that, while two As are required to produce Δ, we can get away with only one use of A to effect the production of Δ. The "resource" A must then be *storable* and can be copied, or cloned, for reuse. One might say that *A admits storage* or is *storage capable*. Clearly, many real resources, like coins, do not have this convenient property: if an item requires two coins for its purchase, then one will not suffice.

The Identity Group

This terminology seems to be due to Girard (Girard *et al*. (1988)).

Axiom

This is the analog of the first rule of inference for natural deduction, namely that a (wellformed) formula is by itself a deduction. The same provisos obtain: the axiom is properly stated only for atomic formula and then can be shown to obtain for general ones. Since we have continued to procrastinate on the issue of atomic formulae, we shall state the axiom in the customary form, to wit:

$$A \vdash A \quad \text{Ax} \tag{2.24}$$

Cut

$$\frac{\Gamma \vdash \Delta, A \quad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'} \quad \text{CUT} \tag{2.25}$$

The CUT rule is an extremely reasonable meta-rule for the handling of natural deductions. Indeed, its natural deduction analog can be deduced from the other rules of natural deduction. The use of A in this rule is akin to the use of a lemma in a mathematical proof, or the use of a subroutine in a computer program. In these forms, the CUT rule would seem to be part and parcel of both of these august disciplines, among others. It is, however, problematical from the point of view of proof theory itself, since the appearance and disappearance of the possibly extraneous and uncontrollable A greatly complicates tree handling techniques. It may therefore come as a surprise to learn that, even in very general Gentzen calculi, cuts can be removed from any proof. That is to say, any proof involving uses of CUT may be recast without using CUT. This is the gist of Gentzen's justly famous "Hauptsatz" (cf. references already cited). This centrally important result is rather counterintuitive at face value since it seems to imply that the usual modes of proof—for instance in mathematics—are somehow redundant. In the programming analogy

the removability of cuts seems more plausible: to "remove" the cuts—i.e, subroutine calls—from a program, compile it into runnable object code. Or, to put it more dynamically, *run* the program. This is, of course, simplistic, but encapsulates the main idea behind the proof.

Logical Rules

These rules *introduce* the logical operators (*via* the right rules) and *eliminate* them (*via* the left rules).

$$\frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_0 \wedge A_1 \vdash \Delta} \mathrm{L}i\wedge, \quad i = 0, 1. \qquad \frac{\Gamma \vdash A, \Delta \quad \Gamma' \vdash B, \Delta'}{\Gamma, \Gamma' \vdash A \wedge B, \Delta, \Delta'} \mathrm{R}\wedge \tag{2.26}$$

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \vee B \vdash \Delta, \Delta'} L\vee \qquad \frac{\Gamma \vdash A_i, \Delta}{\Gamma \vdash A_0 \vee A_1, \Delta} \mathrm{R}i\vee, \quad i = 0, 1. \tag{2.27}$$

$$\frac{\Gamma \vdash A, \Delta \quad \Gamma', B \vdash \Delta'}{\Gamma, \Gamma', A \Rightarrow B \vdash \Delta, \Delta'} \mathrm{L}\Rightarrow \qquad \frac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \Rightarrow B, \Delta} \mathrm{R}\Rightarrow \tag{2.28}$$

For intuitionistic systems, all of these logical rules—with the exception of L$\vee$—are restricted merely by allowing at most one formula to the right of turnstiles. Only in the case of L$\vee$ is the intuitionistic version not just a restriction of this kind, since the Δ, Δ' is disallowed. Instead, the rule is replaced by

$$\frac{\Gamma, A \vdash \Delta \quad \Gamma', B \vdash \Delta}{\Gamma, \Gamma', A \vee B \vdash \Delta} \tag{2.29}$$

where Δ contains at most one formula.

For an *intuitionistic* Gentzen sequent calculus it is generally possible to produce a natural deduction system that might be presumed to underlie it. This is done by judiciously (and recursively) assigning terms to sequents, and then regarding these terms as λ-calculus-like descriptors of underlying deductions. (The correspondence sending a sequent proof to its associated λ-term is generally not one-to-one.)

For instance, for the intuitionistic version of CUT, which reads

$$\frac{\Gamma \vdash A \quad A, \Delta \vdash B}{\Gamma, \Delta \vdash B} \tag{2.30}$$

the term assignment takes the form

$$\frac{\Gamma \vdash t{:}A \quad x{:}A, \Delta \vdash u{:}B}{\Gamma, \Delta \vdash u[x/t]{:}B} \tag{2.31}$$

This is a formalized version of an obvious replacement of deductions in natural deduction: t labels the deduction of A from Γ, and u labels the deduction of B from the deduction x of A and Δ. Thus, from Γ, Δ we may deduce B by using the deduction t in place of x, thereby cutting A out of the lower sequent.

Readers familiar with λ-calculus will recognize that sequent proofs conducted without the use of CUT will produce *normal* λ-terms, i.e. terms that are not reducible. The fact that CUT can be eliminated is essentially equivalent to the fact that simply typed λ-calculus is (strongly) normalizable: every λ-term is reducible to a unique normal form (cf. works already cited).

More to the point for our future purposes is the observation (cf. Abramsky, 1993) that the *computational* aspects of such deductive systems are seen to reside precisely in the process of cut elimination.

The Gentzen sequent formalism reveals structural and behavioral attributes of the underlying, or associated, natural deduction system and the equivalent term calculus. Among its lessons, we emphasize

- the critical importance of the structural rules, and their sensitivity to different semantic readings of the associated natural deduction system;
- the fact, just noted, that all computation resides in the process of cut elimination;
- the value—much appreciated by computer scientists—of the explicit typing of terms and the careful maintenance of such typing through the course of deductions.

In this paper and its sequels we shall attempt to carry these lessons into the quantum domain.

3. QUANTUM COMPUTATIONAL PARADIGMS

3.1. Quantum Logic

The minimal core of quantum logic is known as *orthologic* (OL). This is simply the weakening of classical logic, which results when one does not insist that AND distributes over OR: it is the logic that might have replaced classical logic had classical logicians failed to notice this distributivity in their ambient world of macroscopic objects.

The realization of (first-order) orthologic as a (nonintuitionistic) deductive system seems first to have been achieved by Goldblatt (1974); see also Dalla Chiara *et al*. (2002). The atoms or primitive symbols are

(i) a denumerable collection $\mathbf{\Phi}_0$ of propositional variables $a_1, a_2, \ldots$;
(ii) the connectives $\sim$ ("negation") and $\sqcap$ ("conjunction"); and
(iii) parentheses.

The set $\mathbf{\Phi}$ of (well-formed) *orthoformulae* (or just *formulae*, until this designation becomes ambiguous) is constructed from these in the usual way. Elements of $\mathbf{\Phi}$ will be denoted by lower case Greek characters $\alpha, \beta, \ldots$, taken usually from the beginning of the alphabet. (We shall try to reserve characters at the end of the alphabet for elements of sets of various kinds.)

Since there is no implication sign in $\mathbf{\Phi}$ a formal deductive calculus is based on *sequents* involving at most single formulae and written in the form

$$\alpha \vdash \beta \tag{3.1}$$

for $\alpha, \beta \in \mathbf{\Phi}$, the intended reading of which is that β may be inferred from α. Certain sequents are designated as *axioms*, and there are three *rules of inference*, namely, for any formulae α, β:

Axioms

O1. $\alpha \vdash \alpha$
O2. $\alpha \sqcap \beta \vdash \alpha$
O3. $\alpha \sqcap \beta \vdash \beta$
O4. $\alpha \vdash \sim\sim \alpha$
O5. $\sim\sim \alpha \vdash \alpha$
O6. $\alpha \sqcap \sim \alpha \vdash \beta$

Inference Rules

O7. $$\frac{\alpha \vdash \beta \quad \beta \vdash \gamma}{\alpha \vdash \gamma}$$

O8. $$\frac{\alpha \vdash \beta \quad \alpha \vdash \gamma}{\alpha \vdash \beta \sqcap \gamma}$$

O9. $$\frac{\alpha \vdash \beta}{\sim\beta \vdash \sim\alpha}$$

A conjunctive connective may be introduced according to the definition

$$\alpha \sqcup \beta \equiv \sim((\sim \alpha) \sqcap (\sim \beta)) \tag{3.2}$$

and dual forms of O2, O3, O6 and O8 follow.

A string $s_1; s_2; \ldots; s_n$ of sequents is called a *proof* of its last member s_n if each s_i is either an axiom or follows from some preceding sequent through the use of one of the rules of inference.

If there exists a proof of a sequent $\alpha \vdash \beta$ we write

$$\alpha \vdash_o \beta \tag{3.3}$$

and say that β is *deducible from* α *in orthologic*.

If $\alpha \vdash_o \beta$ for *any* formula α, we say that β is a *theorem of orthologic* or an *orthotheorem*, and we write

$$\vdash_o \beta. \tag{3.4}$$

(Note that this condition is equivalent to $\alpha \sqcup \sim \alpha \vdash_o \beta$.)

We recall that there are completeness theorems for ordinary PC and IL, which assert connections between the analogous forms of deducibility in these logics and the behavior of morphisms, or valuations, of formulae into certain classes of lattices: Boolean algebras in the case of PC and Heyting algebras in the case of IL (cf. Bell & Slomson, 1969). There is an analogous characterization of orthologic, involving a class of lattices called *ortholattices*.

An *ortholattice* is a bounded lattice $\langle L, \sqcup, \sqcap, 0_L, 1_L, ' \rangle$ where $(\ )'$ is a unary operation called *orthocomplementation* satisfying

$$\begin{aligned} \text{complementarity}: &\quad \forall a \in L, a \sqcap a' = 0_L, a \sqcup a' = 1_L \\ \text{unitarity}: &\quad a'' = a \\ \text{antitonicity}: &\quad a \sqsubseteq b \quad \text{iff } b' \sqsubseteq a' \end{aligned}$$

It is easily shown that any ortholattice satisfies De Morgan's laws, e.g.

$$a \sqcup b = (a' \sqcap b')'. \tag{3.5}$$

An ortholattice is said to be *complete* if arbitrary subsets have meets and joins: a complete ortholattice satisfies the complete generalizations of the De Morgan laws. Examples of ortholattices include all Boolean algebras and lattices of closed subspaces of Hilbert spaces, with the usual operations.

Given an ortholattice L, a function $v_L : \Phi_0 \to L$ determines a *valuation* upon Φ *via* the recursive definitions:

$$v_L(\alpha \sqcap \beta) = v_L(\alpha) \sqcap v_L(\beta) \tag{3.6}$$

$$v_L(\sim\alpha) = v_L(\alpha)' \tag{3.7}$$

The algebraic characterization theorem for orthologic may be stated as follows.

Theorem 3.1. (*Goldblatt, 1974*). *$\gamma \vdash_o \alpha$ iff $v_L(\gamma) \sqsubseteq v_L(\alpha)$ for all ortholattices L and all valuations v_L.*

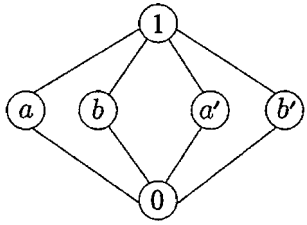
Corollary 3.1. *$\vdash_o \alpha$ iff $v_L(\alpha) = 1_L$ for all ortholattices L and all valuations v_L.*

In classical PC the material implication connective ($\to$) is expressed in terms of other connectives, namely, $p \to q \equiv \neg p \vee q$, a problematic interpretation entailing certain anomalies of great antiquity. In the absence of the distributive law, we might expect further problems for an implication connective cobbled together out of other connectives. This expectation is maximally realized; in fact no viable implication for orthologic can be manufactured out of the other connectives at all.

In ordinary classical PC the interpretation of material implication, $p \to q$, as $\neg p \vee q$ has the consequence that for any Boolean algebra valued valuation v,

$$v(p \to q) = v(p)' \vee v(q) = 1 \quad \text{iff } v(p) \leq v(q). \tag{3.8}$$

However, this situation fails to hold in OL, as the following example shows



(3.9)

In this (nondistributive) ortholattice, known as the *Chinese lantern*, we have $a' \sqcup b = 1$ but $a \not\sqsubseteq b$. Thus (3.8) would fail for certain valuations into this lattice of certain orthoformulae, showing that $\sim\alpha \sqcup \beta$ would not be a viable interpretation of a deduction $\alpha \vdash_o \beta$ in OL, in view of Theorem 3.1.

There is another characterization of classical implication. In any Boolean algebra the element $p \to q$, defined as above, is characterized by the following property:

$$r \leq p \to q \quad \text{iff } r \wedge p \leq q \tag{3.10}$$

from which it follows that $r = p \to q$ is the largest element satisfying $r \wedge p \leq q$. Such elements need not exist in nondistributive lattices, so this avenue of generalization seems to be closed to us: it will reopen later.

The condition (3.10) is an expression of the fact that a Boolean algebra, when considered as a category whose objects are its elements and with morphisms given by $\leq$, is *cartesian closed*, $p \to q$ being the exponential object usually denoted by q^p (cf. Mac Lane & Moerdijk, 1992, p. 48).

What we seek is an orthoformula (or orthopolynomial) in α, β—denote it by $\alpha \xrightarrow[*]{} \beta$—for which $\alpha \vdash_o \beta$ iff $\vdash_o \alpha \xrightarrow[*]{} \beta$. For any orthovaluation v we would then have

$$v(\alpha \xrightarrow[*]{} \beta) = v(\alpha) \xrightarrow[*]{} v(\beta) = 1 \quad \text{iff } v(\alpha) \sqsubseteq v(\beta). \tag{3.11}$$

This is a problem involving only one pair of elements in the target lattice at a time. If these elements themselves lay inside a Boolean subalgebra of the target lattice then the condition $v(\alpha) \sqsubseteq v(\beta)$ would be equivalent to the condition $v(\alpha)' \sqcup v(\beta) = 1$ and the hunt for $\xrightarrow[*]{}$ (with the hope that, at least in this case, we would have $v(\alpha \xrightarrow[*]{} \beta) = v(\alpha)' \sqcup v(\beta)$) might be greatly simplified, albeit at the cost of specializing the logic itself.

Let us then confine our choice of algebraic models to the subclass of ortholattices L satisfying the following condition:

For $a, b \in L$, if $a \sqsubseteq b$ then the subortholattice of L generated by a and b is distributive, hence Boolean.

Ortholattices satisfying this condition are precisely the *orthomodular* ones, examples of which include Boolean algebras, which are just the distributive ones, and the lattice of projections in a W^*-algebra, an example that includes the case of *Hilbert lattices*: namely, the lattices of closed subspaces of Hilbert spaces. The Chinese lantern, depicted above, is also orthomodular (cf. Dalla Chiara *et al*., 2002, Kalmbach, 1983).

There is an important notion of *compatibility* among elements in an ortholattice, an appellation having a physical origin. Namely, an element a is said to be *compatible* with an element b, written aCb, iff

$$a = (a \sqcap b) \sqcup (a \sqcap b') \tag{3.12}$$

It turns out that in an orthomodular lattice:

$$aCb \quad \text{iff} \quad bCa \tag{3.13}$$

and that this condition characterizes orthomodularity.

In a Hilbert lattice this condition is equivalent to the commutativity of the corresponding projections and for this reason the compatibility relation is often called *commutativity*, and written more symmetrically as $a \leftrightarrow b$. This symmetry is justified in an orthomodular lattice in view of (3.13). Note that $a \leftrightarrow b$ iff $a \leftrightarrow b'$ and that if $a \sqsubseteq b$ then $a \leftrightarrow b$. We can also define *orthogonality* ($\perp$) in an ortholattice, namely, $a \perp b$ iff $a \sqsubseteq b'$. Thus, if $a \perp b$ in an orthomodular lattice we also have $a \leftrightarrow b$.

Now we return to the search for an implicative connective in the subclass of orthomodular ortholattices. It can be shown (Dalla Chiara *et al*., 2002, Kalmbach, 1983) that in an orthomodular lattice there are exactly *five* candidates for an implication $\underset{*}{\longrightarrow}$ satisfying condition (3.11). Of these, only one satisfies the following "weak cartesian closure" property (cf. (3.10)), also called the "weak import-export" property:

$$\text{if} \quad a \leftrightarrow b, \quad \text{then } c \sqsubseteq a \underset{*}{\longrightarrow} b \quad \text{iff} \quad c \sqcap a \sqsubseteq b \tag{3.14}$$

and is given by

$$a \underset{q}{\longrightarrow} b \equiv a' \sqcup (a \sqcap b). \tag{3.15}$$

This connective has come to be called the *Sasaki hook*, though the list of names of other pioneering toilers in this field include those of Finch, Mittelstaedt and Hardegree: please see the references already cited, particularly Dalla Chiara *et al*. (2002). By reason of (3.14) the Sasaki hook is often the implicative connective of choice for the logic that is characterized by algebraic models consisting of orthomodular lattices and valuations into them. As Goldblatt has shown (Dalla Chiara *et al*., 2002; Goldblatt, 1974), this logic may be axiomatized by adding a

single axiom (labelled OM) to the list O1–O6, namely

$$\alpha \sqcap (\sim\alpha \sqcup (\alpha \sqcap \beta)) \vdash \beta. \qquad \text{OM}$$

Deducibility in this logic is defined as in OL, and will be denoted by $\vdash_{\text{OM}}$. We will refer to this *orthomodular* logic as OML. (Warning: Dalla Chiara *et al.* (2002) labels it OQL.)

Thus, we have the following theorem:

Theorem 3.2. *$\alpha \vdash_{\text{OM}} \beta$ iff $\vdash_{\text{OM}} \alpha \xrightarrow[q]{} \beta$ iff $v_L(\alpha) \sqsubseteq v_L(\beta)$ for all orthomodular lattice valued valuations v_L.*

Now it happens that the Sasaki hook, optimal though it may be, is, nevertheless, rather anomalous: it can be shown for instance that

$$\alpha \xrightarrow[q]{} (\beta \xrightarrow[q]{} \alpha) \tag{3.16}$$

is not always true. Insofar as $\xrightarrow[q]{}$ reflects deducibility in OML, it would appear from the invalidity of (3.16) that this type of deducibility is far from being constructive in the sense of natural deduction: cf. equation (2.6) for instance. This intractability, unsurprisingly, shows up also in Gentzen calculi for OML. Here, CUT is generally not eliminable (cf. Gibbins, 1987, for example).

Our conclusion is that standard OML is even less suited to the purpose of constructive deduction than is ordinary classical PC, over and above the obviously nonconstructive axioms O5 and O6. In Section 3.2 we will attempt to redress this by extending the intuitionistic "formulae-as-types" paradigm into the quantum domain. This will take some care, and to prepare the way we first briefly examine some of the possible pitfalls by resorting to another class of models for OL, which are of greater semantic interest than the algebraic ones.

3.2. Kripke Orthomodels for OL and the Failure of the Heyting Paradigm

Since the introduction of orthomodularity apparently did nothing to ameliorate the nonconstructive failings of quantum logic, we jettison this condition and return to a very brief consideration of the core logic OL from a proof theoretic perspective as a step along the path—paralleling the route taken in the classical case—to a more expressive resource-sensitive version of quantum logic.

The *Kripke models* for orthologic seem to have appeared first in Goldblatt (1974) and have been extensively elaborated upon by Dalla Chiara and others (cf. Dalla Chiara *et al.*, 2002; Rawling & Selesnick, 2000). To describe them, some terminology is needed.

An *orthogonality space* $F = \langle W, \perp \rangle$ comprises a set W and a binary relation $\perp \subseteq W \times W$ which is an *orthogonality*: namely, it is *irreflexive* (not $x \perp x$) and *symmetric* ($x \perp y$ iff $y \perp x$).

For $x \in W$, $Y \subseteq W$ we write

$$x \perp Y \quad \text{iff } x \perp y \ \ \forall y \in Y \tag{3.17}$$

and define

$$Y^{\perp} \equiv \{x : x \perp Y\} \tag{3.18}$$

In Goldblatt's terminology (Goldblatt, 1973) $Y \subseteq W$ is said to be *regular* if

$$Y^{\perp\perp} = Y. \tag{3.19}$$

Then the class $R(F)$ of $\perp$-regular subsets of W is a complete ortholattice under the partial order given by set inclusion, with the lattice meet given by set intersection and $\perp$ as orthocomplement. It is not hard to show that, for $E, F \subseteq W$

$$E \subseteq E^{\perp\perp} \tag{3.20}$$

and

$$(E \cup F)^{\perp} = E^{\perp} \cap F^{\perp} \tag{3.21}$$

A *proximity space* is a pair $\langle W, \approx\rangle$ in which the relation "$\approx$" is *reflexive* ($w \approx w$) and *symmetric* ($v \approx w$ iff $w \approx v$). Clearly each proximity space $\langle W, \approx\rangle$ determines an orthogonality space $\langle W, \perp\rangle$ where $x \perp y$ iff $x \not\approx y$, and, conversely, each orthogonality space $\langle W, \perp\rangle$ determines a proximity space $\langle W, \approx\rangle$ where $x \approx y$ iff not $x \perp y$.

A *Kripke orthomodel* $\mathcal{M} = \langle W, \approx, \varrho\rangle$ is a proximity space $P = \langle W, \approx\rangle$ and a function (called a *valuation*) $\varrho{:}\mathbf{\Phi} \to R(\langle W, \perp\rangle)$ satisfying

$$\varrho(\sim\alpha) = \varrho(\alpha)^{\perp} \tag{3.22}$$

$$\varrho(\alpha \sqcap \beta) = \varrho(\alpha) \cap \varrho(\beta). \tag{3.23}$$

We will say that a formula α is

true at the "world" $w \in W$, and write $w \models_{\mathcal{M}} \alpha$,
  iff $w \in \varrho(\alpha)$;
true on a set $E \subseteq W$, and write $E \models_{\mathcal{M}} \alpha$,
  iff $w \models_{\mathcal{M}} \alpha$ for all $w \in E$—that is, iff $E \subseteq \varrho(\alpha)$;
true in the Kripke orthomodel $\mathcal{M}$
  iff it is true at every world in $\mathcal{M}$;
Kripke valid, and write $\models \alpha$,
  iff it is true in *all* Kripke orthomodels.

Theorem 3.3. $\vdash_{\mathrm{o}} \alpha$ *iff* $\models \alpha$.

A question that now interposes itself concerns the semantics of disjunction. In a Kripke orthomodel we have, for formulae α and β, and $E \subseteq W$ as above:

$$\begin{aligned} E \models_{\mathcal{M}} \alpha \sqcup \beta \quad \text{iff } E &\subseteq \varrho(\alpha \sqcup \beta) \\ &= \varrho(\sim(\sim\alpha \sqcap \sim\beta)) \\ &= (\varrho(\alpha)^{\perp} \cap \varrho(\beta)^{\perp})^{\perp} \\ &= (\varrho(\alpha) \cup \varrho(\beta))^{\perp\perp} \quad \text{by (3.21)} \\ &\supseteq \varrho(\alpha) \cup \varrho(\beta) \quad \text{by (3.20)} \end{aligned} \tag{3.24}$$

Thus, the interpretations of orthodisjuncts are, in a sense, double negations of ordinary disjuncts of propositions—these are not necessarily themselves ordinary disjuncts: there are generally more "worlds" in $\varrho(\alpha \sqcup \beta)$ than there are in $\varrho(\alpha) \cup \varrho(\beta)$; that is, one could have $w \models_{\mathcal{M}} \alpha \sqcup \beta$ while neither $w \models_{\mathcal{M}} \alpha$ nor $w \models_{\mathcal{M}} \beta$ holds.

When viewed constructively, a proof of an orthotheorem of the form $\alpha \sqcup \beta$ would require a deduction of the truth of an assertion of the form $w \models_{\mathcal{M}} \alpha \sqcup \beta$ at each w in an orthomodel. Thus, w could be used in the labelling of a deduction of $\alpha \sqcup \beta$ while not entering into the labelling of a deduction of either α or β. Deductions of orthodisjuncts are not necessarily determined by deductions of either components. Herein lies one of the highly nonconstructive aspects of quantum logic and one which stands in the way of a direct application of the standard Heyting paradigm to effect a transition to an intuitionistic "quantum" type theory, since, in this case, the classical set of deductions of a "quantum" disjunct cannot be identified with the sum of the classical sets of deductions of the individual components. Rather, some quantum version of the paradigm is called for.

3.3. GQ: A Minimal Intuitionistic Gentzen Calculus for Quantum Resources

Standard quantum logic has been found wanting as a deductive system since deducibility in it is intrinsically nonconstructive, a failing it shares with classical PC. In the classical case the path to a more expressive deductive logic led, through (intuitionistic) proof theoretic systems, to type theories like simply typed λ-calculus and beyond.

In this section we initiate an entirely syntactic attempt to specify a "quantum" type theory in formal imitation of the Curry–Howard correspondence. As we have learnt, the ordinary set theoretic type combinators are inadequate as intuitionistic models here, so new ones must be introduced: this will be done by means of an intuitionistic Gentzen calculus that we shall dub GQ. Upper case Latin characters, $A, B, \ldots$ shall be used to denote formulae (or, synonymously, types) in GQ and we leave the choice of atoms in abeyance.

The multiplicative operation on types that is supposed to correspond intuitionistically to the $\sqcap$ of OL (as $\times$ corresponds to $\wedge$ in the ordinary Curry–Howard correspondence) will, for obvious reasons, be denoted by $\otimes$. Similarly, the operation on types corresponding intuitionistically to the $\sqcup$ of OL will be denoted by $\oplus$, and that corresponding to $\sim(\ )$ by $(\ )^*$. These symbols ($\otimes$, $\oplus$, $(\ )^*$) should not (yet!) be confused with their linear algebra counterparts: their use here is purely syntactic, the purpose being to bring to the fore the *logical* connections between the intuitionistic fragment of OL to be discussed later, and the Gentzen system at hand. Different symbols could (and probably should) be used, but this option seems specious.

Recall that an intuitionistic sequent calculus is one which is supposed to be a metacalculus for some (notional or derivable) underlying natural deduction system, so that only single formulae—or none at all—are allowed on the right hand sides of sequents. We introduce the notation D to represent either a single formula or the absence of a formula (i.e. the null sequence). Otherwise, upper case Greeks will denote (possibly empty) sequences of formulae.

In constructing these rules, we have taken seriously the notion of *discharging* hypotheses in natural deduction. The turnstile $\vdash$ will be read as a kinematical interface through which formulae (quantum resources) may be discharged, this process being registered by the production of the starred version of the formula on the other side of the turnstile. The idea is that a deduction

$$\begin{array}{c} A \\ \vdots \\ B \end{array} \tag{3.25}$$

in the notional underlying natural deduction system results in the discharge of A while B is produced. Put another way, A is discharged *in the presence of* B, resulting in the following inference:

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A^* \otimes B} \tag{3.26}$$

In sequent language, this is expressed as

$$\frac{A \vdash B}{\vdash A^* \otimes B} \tag{3.27}$$

which may be read: if A produces B then it is the case that A is discharged in the presence of B.

If A produces nothing, $A\vdash$, then it may discharge by itself:

$$\frac{A \vdash}{\vdash A^*} \tag{3.28}$$

Similarly, from the presumed behavior of the quantum interface, a sequent of the form $\Gamma, A \vdash B$ has the reading that A in the presence of Γ produces B, and may be discharged through the interface, leaving Γ undischarged. This yields the rule

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A^* \otimes B} \tag{3.29}$$

We presume in addition that this interface is symmetrical to the extent allowed by the structural constraints of an intuitionistic calculus. For instance, if it is the case that A and B are "present," namely $\vdash A \otimes B$, then A may be discharged to leave B no longer in its presence, and this process is also a proof (i.e. a deduction) in the calculus:

$$\frac{\vdash A \otimes B}{A^* \vdash B} \tag{3.30}$$

(Here, B may be absent.)

Similarly, this may be done in the case in which $\Gamma \vdash A \otimes B$. A may be discharged in the presence of Γ to leave B by itself:

$$\frac{\Gamma \vdash A \otimes B}{\Gamma, A^* \vdash B}. \tag{3.31}$$

The rules (3.29) and (3.31) are the rules of *negation* in our calculus. Here, negation is seen as a form of discharge, absorption or annihilation, and should not be confused with negation in OL, just as negation in PC should not be confused with IL-negation. (In fact, negation in IL may also be seen as a form of annihilation: to IL-negate a formula one must deduce falsity from any purported proof of it. That is, identifying the formula A with its set of proofs, and denoting by $\mathbf{f}$ the *falsum*, or logical constant for falsity, the IL-negation of A may be written $A \Rightarrow \mathbf{f}$. Thus A is consigned to the logical vacuum, or annihilated.)

We now consider the structural rules. We shall retain the Exchange rules, insofar as they may be applied under intuitionistic constraints, since there is no implicit logical ordering of the component formulae in OL conjuncts. (Issue could certainly be taken with this point, but we shall adopt this option here, if only for reasons of simplicity.)

The other structural rules are more problematical. We will adopt as our informal guide in these considerations a *quantum* version of the Heyting paradigm. Thus, we will think of the resource (or type) A as behaving *like* a "quantum set" of deductions of some underlying OL formula. Thus, the *terms* of type A will be like deductions of some OL formula, but subject to quantum operations such as superposition. This should not be taken in any literal sense, since our purpose here is merely to arrive at a collection of logical or syntactical rules. (Later, we will indeed take this quantum version of the Heyting paradigm more literally.)

Consider the rule of Contraction (cf. (2.23)), which has only a left form in the intuitionistic calculus, namely

$$\frac{A, A, \Gamma \vdash D}{A, \Gamma \vdash D}. \tag{3.32}$$

In the classical case of a notional underlying natural deduction system this is justified, since the sets of labels for the two collections of deductions of the formula corresponding to the type A can be amalgamated into a single set, while remaining intact, and discharged simultaneously: only a single invocation of A is therefore required. These resources are storage capable. Deductions associated with one occurrence of A can be copied, or duplicated for the benefit of other occurrences of A. In our quantum case certain terms associated with one of the occurrences of the resource A may be annihilated in the course of a deduction while some of those associated with the other occurrence may remain. Thus, amalgamation into single collection may not be possible, owing to the evanescence of quantum processes, and we must jettison Contraction as a general rule. This has the consequence that general quantum resources of this type are *not* storage capable.

The meaning of Weakening (cf.(2.22)), which it will prove convenient to express in the form

$$\frac{\Gamma \vdash D}{\Gamma, A \vdash D}, \tag{3.33}$$

may be interpreted analogously, in the natural deduction model, as the capability of introducing spurious, or null, collections of A occurrences which have no contextual side effects. This seems contrary to the general behavior of actual quantum resources: the introduction of new quantum acts into extant arrangements of acts may interfere with the behavior of those arrangements. (Consider, for example, the interposition of a filter between orthogonal polarizers on an optical bench. Photons previously blocked may now pass through the array.) Unless A is somehow insulated, its introduction might affect the context Γ by mixing or superposition so that $\Gamma, A \vdash D$ is not guaranteed. Thus, we must also relinquish Weakening as a general rule.

If this were all that could be said about the structural rules, our investigation would end here. For, in the absence of storage capable elements, no useful computations could be carried out, even in principle: iterative processes would be blocked and the calculus would be useless. Consequently, inspired by Girard in a similar context (Girard *et al*., 1988), we will institute a search for possible special instances of quantum resources for which the structural rules might be reinstated, or rather, we search for the logical rules which specify such resources. Before embarking on this, we note that, in light of the discussion above, if a storage capable resource could be found for which Contraction holds, then the annihilation or discharge of the terms belonging to separate instances of it in any sequent in which it appears more than once, must, in a sense, be coordinated. Thus quantum duplication

would necessarily be associated with some kind of coordination or correlation of terms distributed over separate instances of the resource. This observation will be confirmed in detail later, a circumstance that has profound consequences.

We continue to adopt as our informal guide in this search a quantum version of the Heyting paradigm, which, curiously, will turn out to work formally as well, revealing better behavior than its non-quantum counterpart. Let us suppose, then, that a quantum type A is in fact the "quantum set" of deductions of some orthoformula α. Then the terms of A denote deductions of α, so certain terms of A may be annihilated or discharged without affecting α itself. Thus, α may be used to *regenerate* A. So, in this case, reuses of the resource—and its concomitant storage capability—could be envisaged. Of course, A cannot generally be regarded as being of this type, but we could try this idea at the next level. Namely, let us assume that the (quantum) set of proofs of A could itself be assembled into a quantum type, denoted $!A$ (pronounced *of course* A—name and notation due to Girard). Then identical considerations apply to A rather than to α, with $!A$ now being storage capable and, presumably, subject to the rule of Contraction.

Moreover, reverting to the case in which A models the quantum set of deductions of some orthoformula α, there is a collection of deductions of α corresponding to instances of axiom O6. Each such deduction corresponds to the inclusion of the proposition Ø into any proposition in any Kripke orthomodel. We could introduce a spurious OL deduction of the form $\varpi \vdash_{\mathrm{o}} \alpha$, where ϖ denotes the *quantum falsum*, which is a logical constant sent to 0 in any algebraic orthomodel. This spurious deduction of α would then give rise to a term of type A denoting in a sense the generic spurious quantum collection associated with A. Recapitulating this at the higher level in which A replaces α and $!A$ replaces A, the existence of such a spurious quantum collection—associated now with $!A$—could presumably be used to implement Weakening for $!A$ in place of A in (3.33).

In addition to Contraction and Weakening—which we now posit for formulae of the from $!A$—we require two more rules pertaining to the operator !. The first,

$$\frac{\Gamma, A \vdash D}{\Gamma, !A \vdash D}, \tag{3.34}$$

reads informally: if Γ in the presence of A can produce the resource D, then Γ in the presence of the type representing all proofs of A can also produce D. This would be reasonable if we were to adopt the axiom $A \vdash A$, which we shall be doing.

The second rule asserts the basic defining property of the operator !: namely, in informal terms, it specifies the explicit circumstances under which a formula A may determine $!A$. To wit

$$\frac{!\Gamma \vdash A}{!\Gamma \vdash !A}. \tag{3.35}$$

(Here $!\Gamma \equiv !A_1, !A_2, \ldots, !A_n$ if $\Gamma \equiv A_1, A_2, \ldots, A_n$.) If A has been produced through the possibly repeated use of the storage capable resources $!\Gamma$, then these resources may also be used to produce the multiplexed or repeatable version of A, namely $!A$. In this rule a formula A must actually be present.

We can now dismantle the preceding verbal scaffolding and formally display the basic sequents of our calculus. Recall that D stands for a single formula or no formula (the empty sequence). When it appears in the form $\otimes D$, the $\otimes$ sign is understood to be absent when D is empty.

GQ

Structural Rules

Exchange

$$\frac{\Gamma, A, B, \Gamma' \vdash D}{\Gamma, B, A, \Gamma' \vdash D} \text{ LE} \qquad \frac{\Gamma \vdash A \otimes B}{\Gamma \vdash B \otimes A} \text{ RE} \tag{3.36}$$

Weakening

$$\frac{\Gamma \vdash D}{\Gamma, !A \vdash D} \text{ LW} \qquad \text{No RW} \tag{3.37}$$

Contraction

$$\frac{!A, !A, \Gamma \vdash D}{!A, \Gamma \vdash D} \text{ LC} \qquad \text{No RC} \tag{3.38}$$

The Identity Group

Axiom

$$A \vdash A \quad \text{Ax} \tag{3.39}$$

Cut

$$\frac{\Gamma \vdash A \quad A, \Gamma' \vdash D}{\Gamma, \Gamma' \vdash D} \text{ CUT} \tag{3.40}$$

Logical Rules

Conjunctive (Multiplicative) Connective

$$\frac{\Gamma, A, B \vdash D}{\Gamma, A \otimes B \vdash D} \text{ L}\otimes \qquad \frac{\Gamma \vdash A \quad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash A \otimes B} \text{ R}\otimes \tag{3.41}$$

Disjunctive (Additive) Connective

$$\frac{\Gamma, A \vdash D \quad \Gamma, B \vdash D}{\Gamma, A \oplus B \vdash D} \; \mathrm{L}\oplus \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \oplus B} \; \mathrm{R}\oplus_1 \tag{3.42a}$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \oplus B} \; \mathrm{R}\oplus_2 \tag{3.42b}$$

Negation

$$\frac{\Gamma \vdash A \otimes D}{\Gamma, A^* \vdash B} \; \mathrm{L}* \qquad \frac{\Gamma, A \vdash D}{\Gamma \vdash A^* \otimes D} \; R* \tag{3.43}$$

!

$$\frac{\Gamma, A \vdash D}{\Gamma, !A \vdash D} \; \mathrm{L}! \qquad \frac{!\Gamma \vdash A}{!\Gamma \vdash !A} \; \mathrm{R}! \tag{3.44}$$

The rule $L\otimes$ is a *formation* rule, while $R\otimes$ is inherited from O8, etc. It is apparent that GQ bears a close resemblance to a fragment of Linear Logic (LL) (cf. Abramsky, 1993; Asperti & Longo, 1991; Blute *et al*., 1993; Girard *et al*., 1988; Seely, 1989; Troelstra & Schwichtenberg, 2000; among many other references to this vast subject.) It is in fact equivalent to a degenerate form of a fragment of this logic, namely, a version of LL in which the operators $\otimes$ and $\oplus$ coincide with their dual forms. (LL often flirts with misconstruals by using the sign $\perp$ for negation.) Various formal connections between versions of LL and versions of quantum logic have already been proposed (cf. the last part of Dalla Chiara *et al*. (2002) for an account of some of these and references to others). None of these seem to be obviously identical to what we have proposed here.

Denoting proof in GQ by $\vdash_{\mathrm{GQ}}$ we have the following.

Lemma 3.1.

1. $A \vdash_{\mathrm{GQ}} A^{**}$ *and* $A^{**} \vdash_{\mathrm{GQ}} A$ *for any* A.
2. $\dfrac{\Gamma, A \vdash_{\mathrm{GQ}} B}{\Gamma, B^* \vdash_{\mathrm{GQ}} A^*}$

Proof:

1. For the first assertion apply Ax, then R$*$ with Γ empty, then L$*$. Similarly for the second.
2. Apply R$*$, then RE, then L$*$. □

A complete type theory would call for a set of term assignments to go with the inference rules given above. Needless to say, this seems not to be straightforward

in the quantum case, and we will postpone a complete treatment until a later paper. (A certain term assignment is discussed in Section 3.5.)

3.4. Intuitionistic Orthologic and its Translation into GQ

If the formal calculus we have posited above is to properly reflect deductions in the underlying deductive system it purports to describe, then we should be able to reproduce this underlying system within the calculus itself. Of course, the best that we could hope for would be to recover an intuitionistic version of this underlying system, namely OL.

We obtain an intuitionistic version of OL by discarding the IL invalid axioms, namely O5 and O6, and adding new ones for the disjunctive connective, since the De Morgan Law does not hold intuitionistically. We denote these connectives by the same symbols as before. The rules for the resulting system—which we shall call IOL—are displayed hereafter.

Axioms

IO1. $\alpha \vdash \alpha$
IO2. $\alpha \sqcap \beta \vdash \alpha$
IO3. $\alpha \sqcap \beta \vdash \beta$
IO4. $\alpha \vdash \alpha \sqcup \beta$
IO5. $\beta \vdash \alpha \sqcup \beta$
IO6. $\alpha \vdash\sim \sim\alpha$

Inference Rules

IO7. $$\frac{\alpha \vdash \beta \quad \beta \vdash \gamma}{\alpha \vdash \gamma}$$

IO8. $$\frac{\alpha \vdash \beta \quad \alpha \vdash \gamma}{\alpha \vdash \beta \sqcap \gamma}$$

IO9. $$\frac{\beta \vdash \alpha \quad \gamma \vdash \alpha}{\beta \sqcup \gamma \vdash \alpha}$$

IO10. $$\frac{\alpha \vdash \beta}{\sim\beta \vdash \sim\alpha}$$

Deduction in IOL will be defined as it is in OL and denoted by $\vdash_{\mathrm{IO}}$.

We now attempt to translate IOL formulae into GQ formulae (assuming some common set of atoms) by reinstating some of the scaffolding used to arrive at the GQ rules. Specifically, we return to the informal reading of $!A$ as the "quantum set of proofs of A." Then we try a translation that is simply the (quantum) Heyting paradigm applied recursively to the logical operators. That is to say, if α^e denotes

the GQ formula that is the translated version of the IOL formula α with

$$\alpha^e \equiv \alpha \quad \text{for } \alpha \text{ atomic,} \tag{3.45}$$

then the Heyting paradigm yields exactly:

$$(\alpha \sqcap \beta)^e = !\alpha^e \otimes !\beta^e, \tag{3.46}$$

$$(\alpha \sqcup \beta)^e = !\alpha^e \oplus !\beta^e, \tag{3.47}$$

$$(\sim\alpha)^e = (!\alpha^e)^*. \tag{3.48}$$

Thus, equation (3.46) in this reading states: the GQ translation of $\alpha \sqcap \beta$ is as (the quantum set of proofs of α^e) $\otimes$ (the quantum set of proofs of β^e). Equation (3.48) in this reading states: the translation of $\sim\alpha$ is as the annihilator of all proofs of α^e. This is the correct intuitionistic interpretation of falsity: every possible proof is refuted.

This translation will be recognized immediately by readers conversant with LL as being almost identical with the Girard embedding of IL into LL. It is worth noting that the Heyting paradigm in its simple pristine non-quantum form is not usually invoked to motivate the Girard embedding. However, as we shall see, it seems to work perfectly and in explicit detail in the quantum case.

Specifically, with the translation rules given above, we have the following:

Theorem 3.4. *If* $\alpha \vdash_{\mathrm{IO}} \beta$ *then* $!\alpha^e \vdash_{\mathrm{GQ}} \beta^e$.

Proof: Before embarking upon the proof, some motivational remarks are in order. We note first that the presence of the GQ formula α^e may be fleeting, whereas the IOL formula α is static and repeatable. Consequently, to have any expectation that the deduction $\alpha \vdash_{\mathrm{IO}} \beta$ may be translatable into a proof in GQ, we should render the "producer" α^e repeatable in GQ. Only then may deductions in IOL, which may require repeated uses of α, be done also in GQ: this explains the presence of $!\alpha^e$ in the translated version of the deduction.

The proof of the theorem is by induction on the length of a deduction: that is, the number n of steps in a deduction $s_1; s_2; \ldots; s_n$ of the sequent s_n, where the axioms and inference rules used are those of IOL.

A deduction with one step must be an axiom, and we first prove the theorem for each axiom in turn.

The proof for (IO1):

$$\text{For any } \alpha, \quad \frac{\alpha^e \vdash_{\mathrm{GQ}} \alpha^e}{!\alpha^e \vdash_{\mathrm{GQ}} \alpha^e} \quad \text{L!}$$

For (IO2):

$$\text{For any } \alpha, \quad \dfrac{\dfrac{\dfrac{!\alpha^e \vdash_{GQ} \alpha^e}{!\alpha^e,\ !\beta^e \vdash_{GQ} \alpha^e}\ \text{above and W!}}{!\alpha^e \otimes !\beta^e \vdash_{GQ} \alpha^e}\ \text{L}\otimes}{!(!\alpha^e \otimes !\beta^e) \vdash_{GQ} \alpha^e}\ \text{L !}$$

$$\text{or} \qquad !(\alpha \sqcap \beta)^e \vdash_{GQ} \alpha^e.$$

For (IO3): Similar to (IO2), but using LE to interchange $!\alpha^e$ and $!\beta^e$ after the second step.

For (IO4):

$$\frac{!\alpha^e \vdash_{GQ} !\alpha^e}{!\alpha^e \vdash_{GQ} !\alpha^e \oplus !\beta^e}\ \text{R}\oplus_1$$

For (IO5): Similar, using $\text{R}\oplus_2$.

For (IO6):

$$\text{For any } \alpha, \quad \dfrac{\dfrac{\dfrac{(!\alpha^e)^* \vdash_{GQ} (!\alpha^e)^*}{!(!\alpha^e)^* \vdash_{GQ} (!\alpha^e)^*}\ \text{L!}}{(!\alpha^e)^{**} \vdash_{GQ} (!(!\alpha^e)^*)^*}\ \text{Lemma 3.1(2)}}{!\alpha^e \vdash_{GQ} (!(!\alpha^e)^*)^*}\ \text{Lemma 3.1(1) and CUT.}$$

But

$$\begin{aligned}(\sim\sim\alpha)^e &= (!(\sim\alpha)^e)^* \\ &= (!(!\alpha^e)^*)^*\end{aligned}$$

which proves the theorem for (IO6).

The inductive hypothesis for n is that the theorem holds for the last sequent in all IOL deductions of length less than n. (The base case has been covered above.)

Consider a deduction $s_1; s_2; \ldots; s_n$ of length n. If s_n is an axiom then we are done, as above. If s_n is not an axiom, then it follows from a rule of inference applied to preceding sequents. Each preceding sequent is itself the result of a shorter deduction, so the theorem holds for each of these, by the induction hypothesis.

We consider each possible rule of inference in turn.

For (IO7): We suppose that s_n is of the form $\alpha \vdash_{IO} \gamma$ and follows, *via* (IO7), from preceding deductions $\alpha \vdash_{IO} \beta$ and $\beta \vdash_{IO} \gamma$. Since, as remarked, these latter deductions are shorter than n, the theorem holds for them, namely $!\alpha^e \vdash_{GQ} \beta^e$ and $!\beta^e \vdash_{GQ} \gamma^e$. It follows from R! that $!\alpha^e \vdash_{GQ} !\beta^e$ and then from CUT that $!\alpha^e \vdash_{LL} \gamma^e$, so the theorem holds for this s_n.

For (IO8): If s_n is of the form $\alpha \vdash_{\mathrm{IO}} \beta \sqcap \gamma$ and follows, *via* (IO8), from prior deductions $\alpha \vdash_{\mathrm{IO}} \beta$ and $\alpha \vdash_{\mathrm{IO}} \gamma$, then, as above, $!\alpha^e \vdash_{\mathrm{GQ}} !\beta^e$ and $!\alpha^e \vdash_{\mathrm{GQ}} !\gamma^e$. So

$$\dfrac{\dfrac{!\alpha^e \vdash_{\mathrm{GQ}} !\beta^e \quad !\alpha^e \vdash_{\mathrm{GQ}} !\gamma^e}{!\alpha^e,\ !\alpha^e \vdash_{\mathrm{GQ}} !\beta^e \otimes !\gamma^e}\ \mathrm{R}\otimes}{!\alpha^e \vdash_{\mathrm{GQ}} !\beta^e \otimes !\gamma^e}\ \mathrm{LC}$$

$$\text{or} \qquad !\alpha^e \vdash_{\mathrm{GQ}} (\beta \sqcap \gamma)^e$$

so the theorem holds for this s_n.

For (IO9): If s_n is of the form $\beta \sqcup \gamma \vdash_{\mathrm{IO}} \alpha$, etc., then we have

$$\dfrac{\dfrac{!\beta^e \vdash_{\mathrm{GQ}} \alpha^e \quad !\gamma^e \vdash_{\mathrm{GQ}} \alpha^e}{!\beta^e \oplus !\gamma^e \vdash_{\mathrm{GQ}} \alpha^e}\ \mathrm{L}\oplus}{!(!\beta^e \oplus !\gamma^e) \vdash_{\mathrm{GQ}} \alpha^e}\ \mathrm{L}!$$

$$\text{or} \qquad !(\beta \sqcup \gamma)^e \vdash_{\mathrm{GQ}} \alpha^e,$$

so the theorem holds for this s_n.

For (IO10): If s_n is of the form $\sim\beta \vdash_{\mathrm{IO}} \sim\alpha$ and follows, *via* (IO10), from the shorter deduction $\alpha \vdash_{\mathrm{IO}} \beta$, then

$$\begin{array}{ll} \dfrac{\dfrac{\dfrac{!\alpha^e \vdash_{\mathrm{GQ}} \beta^e}{!\alpha^e \vdash_{\mathrm{GQ}} !\beta^e}}{(!\beta^e)^* \vdash_{\mathrm{GQ}} (!\alpha^e)^*}}{!(!\beta^e)^* \vdash_{\mathrm{GQ}} (!\alpha^e)^*} & \begin{array}{l}\mathrm{R}! \\ \text{Lemma 3.1(2)} \\ \mathrm{L}!\end{array} \end{array}$$

which is $!(\sim\beta)^e \vdash_{\mathrm{GQ}} (\sim\alpha)^e$ so the theorem holds for this s_n. □

3.5. A Realization of GQ

The pioneering efforts of J. Lambek (see Lambek & Scott, 1986, and references therein)—who demonstrated a perfect correspondence between certain categories (namely the closed cartesian ones) and certain typed λ-calculi (namely the $\lambda\beta\eta$-calculi with surjective pairing)—have led to a general appreciation that certain categories provide good models for certain type theories. In such a model, the types (or formulae) are interpreted as objects in an appropriate category, and deductions are interpreted as morphisms going between the appropriate objects.

In the case of our system GQ the choice of category in which to carry out such an interpretation would be clear on physical and constructive grounds, even if we had used a different notation: namely, the category $\mathcal{H}_F$ of finite dimensional complex Hilbert spaces. To carry out this interpretation, we need to specify, for

each unnamed atomic GQ formula, a corresponding object in $\mathcal{H}_F$. Supposing this to be done, we then obtain for each GQ formula A an object of $\mathcal{H}_F$ merely by interpreting the occurrences of $\otimes$, $\oplus$, $(\ )^*$ in A as carrying their usual meaning in the category $\mathcal{H}_F$, the asterisk denoting the dual space of linear functionals. (We note that in functional analytic contexts a Hilbert space is customarily identified with its dual space *via* a correspondence that does not lie in the category $\mathcal{H}_F$, being conjugate linear. In categorical contexts—and also in some physical ones—it is advisable to maintain this distinction.)

We could now proceed informally by considering GQ formulae to be finite dimensional Hilbert spaces, and, leaving aside for a moment the interpretation of the operator !, we could replace each comma in a nonempty sequence Γ by $\otimes$ and each empty sequence by $\mathbb{C}$. GQ sequents $A \vdash_{\mathrm{GQ}} B$ are then interpreted inductively as elements of $\mathrm{Hom}(A, B)$ according to the interpretations specified for the inference rules. For instance, $A \vdash_{\mathrm{GQ}} A$ (Ax) shall be interpreted as (or by) the identity map $1_A \in \mathrm{Hom}(A, A)$: the other rules hold in the category $\mathcal{H}_F$ and linear maps may be built up which interpret GQ proofs in an obvious way. Thus, for example, in the case of CUT, if we have a proof interpreted as an element of $\mathrm{Hom}(\Gamma, A) \cong \Gamma^* \otimes A$ and a proof interpreted as an element of

$$\mathrm{Hom}(A \otimes \Gamma', D) \cong (A \otimes \Gamma')^* \otimes D \cong A^* \otimes (\Gamma')^* \otimes D,$$

then the tensor product of these two elements lies in

$$\Gamma^* \otimes A \otimes A^* \otimes (\Gamma')^* \otimes D.$$

The $A \otimes A^*$ component may now be contracted (small c!) to yield an element in $(\Gamma \otimes \Gamma')^* \otimes D$. We specify this element as the interpretation in $\mathcal{H}_F$ of the proof $\Gamma, \Gamma' \vdash_{\mathrm{GQ}} D$ given by the CUT rule applied to the original proofs. The other rules not involving ! can be treated similarly, using the properties of the connectives in $\mathcal{H}_F$, an exercise we leave to the interested reader.

Now we turn to the question of how to model $!A$ for a given finite dimensional Hilbert space A. To do this we shall take seriously the earlier wishful interpretation of $!A$ as the "quantum set of proofs of A." Recall that the lattice $L(A)$ constitutes a model of OL and equivalence classes of OL deductions of A in the model $L(A)$ correspond with subspaces of A, by Theorem 3.1. These subspaces can be organized into a "quantum set," namely the exterior algebra $E(A)$—the quantum version of the set of subsets of the "set" A—which is an object in $\mathcal{H}_F$: this is exactly the substance of the extensorial calculus of quantum sets. We shall digress to give a very brief account of this notion, referring to Finkelstein (1996), Selesnick (1998) and their references for fuller accounts.

Suppose we have a linear map $l: W \to C$, where W is a vector space and C is an associative algebra, having the property that for every $w \in W$,

$$l(w)^2 = 0. \tag{3.49}$$

Then there is a universal object satisfying this property. That is to say, for every vector space W, there exists an associative algebra $E(W)$ and a linear map $\iota: W \to E(W)$ satisfying equation (3.49), such that for any other linear map $l: W \to C$ into an algebra satisfying equation (3.49), there exists a unique algebra map $\tilde{l}: E(W) \to C$ such that $l = \tilde{l} \circ \iota$. The algebra $E(W)$ is unique up to appropriately commuting algebra isomorphisms. It is called the *exterior algebra* over W and one instantiation of it is given by the antisymmetric, or fermion, Fock space, namely

$$\begin{aligned} E(W) &= \bigoplus_{k=0}^{\infty} \bigwedge^k W \\ &= \mathbb{C} \oplus W \oplus W \wedge W \oplus \cdots \end{aligned} \tag{3.50}$$

Here $\wedge$ denotes the usual exterior product, $\bigwedge^0 W \equiv \mathbb{C}$ and $\bigwedge^1 W \equiv W$, ι is inclusion of W as the $\bigwedge^1$-summand, and multiplication of homogeneous terms is by $\wedge$-ing them together.

In this case, if W is finite dimensional, of dimension n, say, since

$$\dim \bigwedge^k W = \binom{n}{k}, \tag{3.51}$$

the series in equation (3.50) terminates at $k = n$, and dim $E(W) = 2^n$.

We note a further property of the exterior algebra which will be of significance later, namely, for finite dimensional vector spaces V and W the linear map

$$\bigwedge^m V \otimes \bigwedge^n W \to \bigwedge^{m+n} (V \oplus W) \tag{3.52}$$

given in an obvious notation by

$$(v_1 \wedge \cdots \wedge v_m) \otimes (w_1 \wedge \cdots \wedge w_n) \mapsto v_1 \wedge \cdots \wedge v_m \wedge w_1 \wedge \cdots \wedge w_n \tag{3.53}$$

induces an isomorphism

$$\bigwedge^p (V \oplus W) \cong \bigoplus_{k=0}^{p} \bigwedge^k V \otimes \bigwedge^{p-k} W \tag{3.54}$$

whence an isomorphism of vector spaces (not algebras)

$$E(V \oplus W) \cong E(V) \otimes E(W) \tag{3.55}$$

(cf. Fulton & Harris, 1991, Appendix B; Lang, 1993). If W is a Hilbert space, $E(W)$ may be given a Hilbert structure and is universal in the appropriate category.

Finkelstein seems to have been the first to recognize and address the following problem. Ordinary quantum logic fails to take account of *extensionality*. In the standard interpretation, quantum logical *predicates* (which would determine classes as their *extensions* in naïve classical set theory) correspond to *projections*, or equivalently, *closed subspaces* of a Hilbert space, but *sets* of quanta apparently

do not. Thus there is an asymmetry between quantum *classes* (i.e., quantum predicates, or closed subspaces of a Hilbert space) and quantum *sets* (represented by rays, not in the original space, but in the fermion Fock space (or exterior algebra) based upon it. This asymmetry is absent in (naïve, finitary) classical set theory, where every class is a set. In considering higher order set-theoretic constructs, such as sets of sets, there arises a concomitant problem: standard quantum logic is necessarily only first order, dealing with predicates, but not with predicates whose subjects are predicates, etc. Finkelstein's suggestion to restore extensionality (in the case of finite dimensions) is to replace the relevant Hilbert space with its exterior algebra, and to regard the rays determined by its homogeneous (or simple) elements as representing the *quantum sets* corresponding to the subspace spanned by those elements. This correspondence goes back to Grassmann: specifically, choose a subspace, of W say, spanned by vectors $\{v_1, \ldots, v_k\}$. If another basis $\{w_1, \ldots, w_k\}$ were chosen, then $w_1 \wedge \cdots \wedge w_k = \lambda v_1 \wedge \cdots \wedge v_k$, where λ denotes the determinant of the linear transformation induced by the basis change. Thus, subspaces of W correspond bijectively with rays of homogeneous elements in $E(W)$, and (finite) extensional symmetry is now restored to quantum logic.

Following Finkelstein, our next observation concerns the map $\iota: W \to E(W)$. This map interprets an element $\alpha \in W$ as a (quantum) set $\iota(\alpha)$ in $E(W)$, which is the analog of the classical set $\{\alpha\}$. (This explains the iota, which was Peano's notation for the "unitizing" operation upon sets: $\iota A \equiv \{A\}$.) Since ι is linear, the ray determined by α is sent to the ray determined by $\iota(\alpha)$. (They ray determined by α corresponds to a quantum *predicate* (or *class*), so the ray determined by $\iota(\alpha)$, is a quantum *set*, now interpretable, as in ordinary set theory, as the *extension* of a certain predicate *about* the predicate corresponding to α: namely, the predicate "being α," roughly speaking.) Moreover, we note that the ray $\mathbb{C}$ appearing as the first summand in $E(W)$ represents the empty set $\emptyset$—this follows from our original construction. It is the extension of no quantum predicate. The last nonvanishing component of the exterior product, namely the one-dimensional space $\bigwedge^n W$, where n is the dimension of W, represents the whole "quantum set" W.

Any homogeneous element $\iota(\alpha_1) \wedge \cdots \wedge \iota(\alpha_k)$, say, in $E(W)$ is a quantum analog of the (disjoint) union $\{\alpha_1\} \cup \cdots \cup \{\alpha_k\} = \{\alpha_1, \ldots, \alpha_k\}$, but superpositions are allowed, which of course have no classical counterpart. In fact, $E(W)$ contains a version of classical set theory—a realization which was not lost on Grassmann and some of his followers.

The exterior algebra of a vector (or Hilbert) space has another property of particular interest in the present context, namely, it is a coalgebra, with coproduct $\psi_W: E(W) \to E(W) \otimes E(W)$ given by

$$\psi_W(w) = 1 \otimes w + w \otimes 1 \tag{3.56}$$

and counit given by projection upon the first component in (3.50). (We note that ψ_W is an algebra map if the product on $E(W) \otimes E(W)$ is taken to be the *graded*

product, given by

$$(a \otimes b)(c \otimes d) = (-1)^{\deg(b)\deg(c)}(ac \otimes bd) \tag{3.57}$$

where the degree $\deg(f)$ of an homogeneous element f is the power of the exterior product it belongs to.)

With this coalgebra structure it is not hard to show that the isomorphism (3.55) is in fact an isomorphism of coalgebras.

Now it turns out that this interpretation of the exterior algebra as the quantum set of "proofs" or subspaces of a given space, works perfectly as a model of !; namely,

LW: Consider the counit $c_A{:}E(A) \to \mathbb{C}$, given by projection upon the 0^{th} grade component of $E(A)$. Then an interpretation of a proof $\Gamma \vdash_{\text{GQ}} D$—namely, an element of Hom(Γ, D)—may be composed with the map $\Gamma \otimes E(A) \xrightarrow{1 \otimes c_A} \Gamma \otimes \mathbb{C} \cong \Gamma$ to obtain an element in Hom($\Gamma \otimes E(A)$, D). This element is declared to be the interpretation of the proof obtained *via* LW of the original proof.

LC: A similar argument using the coproduct $E(A) \xrightarrow{\psi_A} E(A) \otimes E(A)$ (equation (3.56)). We shall discuss the interpretation of this rule in a little more detail since it embodies the important notion of quantum copying—or *duplication*—of storage capable quantum resources.

For the purposes of this discussion let us introduce labels (or *terms*) for GQ sequents. Thus, a sequent $\Gamma \vdash D$ may be labelled on the left as in $f{:}\Gamma \vdash D$. (This is equivalent to the notationally more standard expression $\vdash f{:}\Gamma^* \otimes D$.) Rules should now be introduced for the correct formation of terms as GQ proofs are constructed. We shall illustrate only a single short proof, in which these assignments are self-evident: namely

$$\dfrac{\dfrac{f :!A \vdash_{\text{GQ}} B \quad g :!A \vdash_{\text{GQ}} C}{\langle f, g\rangle :!A, !A \vdash_{\text{GQ}} B \otimes C}\ \text{R}\otimes}{\mathbf{dup}_{!A}\langle f, g\rangle :!A \vdash_{\text{GQ}} B \otimes C}\ \text{LC}$$

Read operationally, $\mathbf{dup}_{!A}\langle f, g\rangle$ labels the deduction obtained by "quantum duplicating" the storage capable resource $!A$ in the preceding sequent, and then performing the deduction labelled by $\langle f, g\rangle$. When interpreted in $\mathcal{H}_F$, f and g may be regarded as the appropriate linear maps, and we have

$$\langle f, g\rangle \text{ is interpreted as } f \otimes g$$

and

$$\mathbf{dup}_{!A}\langle f, g\rangle \text{is interpreted as } f \otimes g \circ \psi_A. \tag{3.58}$$

L!: A similar argument using the projection $E(A) \to A$ upon first grade elements.

R!: It suffices to show this for Γ containing at most a single formula, since, if $\Gamma \equiv A_1, A_2, \ldots, A_n$, $!\Gamma$ is interpreted as $!A_1 \otimes !A_2 \otimes \cdots \otimes !A_n$ which is isomorphic as a coalgebra with $!(A_1 \oplus A_2 \oplus \cdots \oplus A_n)$ (equation (3.55)). Then $!\Gamma \to A$ is interpreted as a map $E(\Gamma) \to A$. Dualizing this we obtain a map $A^* \to E(\Gamma)^* \cong E(\Gamma^*)$. From the universal property of $E(\ )$ this map lifts to a map $E(A^*) \to E(\Gamma^*)$, and, dualizing again, we obtain a map $E(\Gamma) \to E(A)$. This is the interpretation of $!\Gamma \vdash !A$ in the conclusion of R!.

All of this could be done much more formally, with little gain in transparency as far as our endeavors in this work are concerned. That the category of finite dimensional vector spaces models full LL, with $!A$ taken to be $E(A^*)^*$, was shown in Blute *et al*. (1993). See also Seely (1989) for a clear discussion of more general categorical interpretations of LL.

We conclude this section with the following remarks:

- We have shown that, by means of the translation Eqs. (3.45)–(3.48) and the interpretation described above, IOL may be realized within the familiar category $\mathcal{H}_F$ *via* a literal use of a quantum version of the Heyting paradigm. Moreover, the logic of $\mathcal{H}_F$, as specified by the rules of GQ, is seen to be an externalization of the intuitionistic fragment of the logic of each of its object's "inner" subspace-lattice models of OL.
- The correct notion of (intuitionistic) "quantum" implication is now seen to be interpretable in terms of morphisms in $\mathcal{H}_F$; that is, in terms of ordinary linear transformations between the underlying vector spaces, all of which are necessarily continuous for any chosen inner products.
- These logical considerations have thrown up a formal specification of the notion of *storage capable quantum resource*. Such resources would be fundamental to any "quantum computational" endeavor, and the exploration of this notion in one form or another will occupy us for the remainder of this note and certain sequels to it.

4. QUANTUM COMPUTATION

4.1. A Model of Quantum Computation and the Emergence of the Qubit

The system GQ is empty of physical content, embodying, rather, minimal rules for making certain deductions about abstract quantum "resources." The task before us is to supply physical input in the form of additional axioms (and, in subsequent papers, additional rules pertaining to the "post-processing" of certain ensuing deductions). A system obtained by adding axioms to an existing system (such as GQ) is called by logicians a *theory* (or a GQ-*theory*). (Often, extra technical constraints are put upon these added axioms to ensure desirable deductive behavior, but we shall not so constrain our (few) axioms here.)

Specifically, in this note, we shall add a single IOL axiom meant to simulate a single "time"-stepped deduction or computation which preserves each type. Here we consider "time"-steps to be resources—necessarily constrained by our formalism to be "quantum" resources—which are produced to accompany, or label, such a transformation. This may be expressed in the static, resource insensitive language of IOL by the axiom

$$\alpha \vdash_{\mathrm{IO}} \mathbf{t} \sqcap \alpha. \tag{4.1}$$

Here α is any IOL formula, and $\mathbf{t}$ is an atom. This is meant to capture the idea that α (re)produces α to the accompaniment (or production) of a single time-step, time-quantum, or clock-tick. It is a crude attempt to force some preconceived notion of "time" upon the logical *tabula rasa*.

The translation of this into GQ then yields the axiom to be added to GQ, namely

$$!\alpha^e \vdash_{\mathrm{GQ}} !\mathbf{t} \otimes !\alpha^e, \tag{4.2}$$

or, equivalently (in view of L$*$, LE, and R$*$):

$$(!\mathbf{t})^* \vdash_{\mathrm{GQ}} (!\alpha^e)^* \otimes !\alpha^e. \tag{4.3}$$

Thus, the axiom amounts to the specification of a deduction from $(!\mathbf{t})^*$ to $(!\alpha^e)^* \otimes !\alpha^e$ for each α.

When realized in the category $\mathcal{H}_F$, the interpretation of $!\mathbf{t}$ is somewhat problematical, but, whatever interpretation is given to it, α^e will be interpreted as a finite dimensional Hilbert space, W say, of dimension n, say, and $(!\alpha^e)^* \otimes !\alpha^e$ will be interpreted as

$$E(W)^* \otimes E(W) \cong \mathrm{End}E(W).$$

In view of equation (3.55) we have

$$\begin{aligned} E(W) &\cong E(\oplus^n \mathbb{C}) \\ &\cong \otimes^n E(\mathbb{C}) \end{aligned} \tag{4.4}$$

where $E(\mathbb{C}) = \mathbb{C} \oplus \mathbb{C}$, the two-dimensional Hilbert space. This space, the *irreducible quantum storage capable unit* in $\mathcal{H}_F$, has come to be called (in the quantum computing literature) the *qubit*. In view of Finkelstein's Grassmannian interpretation of the functor $E(\ )$, the first $\mathbb{C}$ represents the empty quantum set (or the zero subspace of $\mathbb{C}$), while the second $\mathbb{C}$ represents the subspace $\mathbb{C}$ of $\mathbb{C}$, or the whole quantum set. If quantum superpositions were suppressed, we would have discovered the ordinary classical bit. Note that bit-based notions were not explicit in any of the considerations leading up to QG. Thus, the classical bit emerges, quite appropriately, as a classical degeneration of the spontaneously arising qubit: quantum notions should indeed underlie classical ones.

Equation (4.3) thus characterizes a "quantum computation," taking place in some version of "quantum time," as a map from a representer of the dual of the multiplexed quantum time-step resource **t**, namely $(!\mathbf{t})^*$, to a space of the form $\mathrm{End}(\otimes^n \mathfrak{H}^{(2)})$, where $\mathfrak{H}^{(n)}$ denotes a Hilbert space of dimension n ($<\infty$); that is: the annihilators or absorbers of finite quantum sets of time-steps are mapped to endomorphisms of tensor products of qubits.

The problem here is that the formalism seems to have worked too well in that "time" is also necessarily finitely or constructively quantized when forced into the picture, whereas the exigencies of macroscopic existence might require us to adopt a model of time that is infinite and classical. In order to attempt to redress this problem, and arrive at the standard notion of a quantum computation, we will need to step outside the categorical confines of $\mathscr{H}_F$. This will be done in Section 4.3. First, we are required to interpret rather more fully the notion of quantum duplication.

4.2. Quantum Duplication as Entanglement

As we have noted, the general storage capable object in $\mathscr{H}_F$ is of the form $E(\mathfrak{H}^{(n)}) = \otimes^n \mathfrak{H}^{(2)}$: such a tensor product of qubits has come to be called a *quantum register*.

The *quantum duplication operator* that interprets the GQ Contraction rule, namely

$$\frac{!\mathfrak{H}^{(n)}, !\mathfrak{H}^{(n)}, \Gamma \vdash D}{!\mathfrak{H}^{(n)}, \Gamma \vdash D}, \tag{4.5}$$

is the coproduct $E(\mathfrak{H}^{(n)}) \to E(\mathfrak{H}^{(n)}) \otimes E(\mathfrak{H}^{(n)})$. Moreover, in light of the coalgebra isomorphism equation (3.55), which now reads $E(\mathfrak{H}^{(n)}) \cong \otimes^n \mathfrak{H}^{(2)}$, it will be sufficient for our purposes to discuss the quantum duplication operator for the case of a single qubit $\mathfrak{H}^{(2)}$.

At this point there arises an unfortunate clash of notations. When the qubit is realized as the coalgebra $E(\mathbb{C}) = \mathbb{C} \oplus \mathbb{C}$, the first component is generated by the unit of this algebra which is usually denoted by 1, and, since the coproduct $\psi : E(\mathbb{C}) \to E(\mathbb{C}) \otimes E(\mathbb{C})$ preserves units, we have

$$\psi(1) = 1 \otimes 1. \tag{4.6}$$

For an element x of the other $\mathbb{C}$ component we have (cf. equation (3.56))

$$\psi(x) = 1 \otimes x + x \otimes 1. \tag{4.7}$$

In the quantum computational context, a basis $\{1, x\}$ of the qubit would be written, when normalized, as $\{|0\rangle, |1\rangle\}$: as noted, the first element corresponds to the empty quantum set and the second to the whole quantum set. The duplication

operations expressed by the above equations become

$$\psi(|0\rangle) = |0\rangle \otimes |0\rangle \tag{4.8}$$

$$\psi(|1\rangle) = |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle \tag{4.9}$$

relative to the chosen so-called *computational basis* $\{|0\rangle, |1\rangle\}$.

Thus, quantum duplication applied to the "off" computational basis element $|0\rangle$ produces a simple homogeneous pure state of the combined system $\mathfrak{H}^{(2)} \otimes \mathfrak{H}^{(2)}$, whereas duplication applied to the "on" basis element emphatically does not. Indeed, the state corresponding to the right hand side of equation (4.9) is a *maximally entangled* state.

The duplication map ψ applied to any vector in $\mathfrak{H}^{(2)}$ will be a linear combination of the right hand sides of equations (4.8) and (4.9), and one of the upshots of our logical machinations is that quantum duplication, namely, that quantum process which corresponds to the classical possibility of freely copying a resource, *must* in general entail quantum entanglement. This is borne out in the standard theory of quantum computing, where quantum entanglement has been recognized as a fundamental resource and must be used in subtle ways, for instance to implement the transmission of quantum states by "teleportation." Naïve attempts to copy such states would be confounded in view of the so-called "No Cloning" Theorem (see for example, Hirvensalo, 2001; Nielsen & Chuang, 2000).

It seems rather remarkable that "merely" logical considerations have led directly to this subtlety regarding quantum duplication.

4.3. Quantum Computing in Classical Time

We will extend the interpretation of coproducts as quantum duplication-*via*-entanglement to other coalgebras in an attempt to interpret our axiom (4.3) with the multiplexed time-step type $!\mathbf{t}$ now interpreted "classically."

To render classical the type $!\mathbf{t}$ we need to interpret it in classical terms. This can be done by modelling! not by the exterior algebra but by the free commutative algebra generated by the space in question. In our case, this may be viewed as the bosonic Fock space of the one-dimensional Hilbert space, which may be identified with the one-dimensional affine algebraic group $\mathbb{C}[\mathbf{t}]$: this is just the usual complex polynomial algebra in the indeterminate $\mathbf{t}$, equipped with the bialgebra structure described as follows. The coproduct $\psi{:}\mathbb{C}[\mathbf{t}] \to \mathbb{C}[\mathbf{t}] \otimes \mathbb{C}[\mathbf{t}]$ is that algebra map determined by

$$\psi(\mathbf{t}) = 1 \otimes \mathbf{t} + \mathbf{t} \otimes 1 \tag{4.10}$$

and the counit is given by $c(\mathbf{t}) = 0$. Since it is only time that is being treated classically here, we maintain the quantum interpretation of ! in the other parts of axiom (4.3).

Thus, we are required to specify a map

$$\phi : \mathbb{C}[\mathbf{t}]^* \to \mathrm{End}\big(\otimes^n \mathfrak{H}^{(2)}\big). \tag{4.11}$$

We shall make two assumptions concerning this map which together will yield the *Schrödinger option* for describing the classically timed dynamics of a quantum register. The first of these concerns the notion of duplication. The *quantum duplication* of a resource corresponds to the classical operation of copying or repeating the resource. Our first requirement on ϕ is that it should respect this type of repetitive behavior: in other words, ϕ should be required to match the repetitive behavior of the resource "time" to that of the target resource—a sort of synchronization assumption. Thus, ϕ is required to *respect quantum duplication:* for $f, g \in \mathbb{C}[\mathbf{t}]^*$, we should have

$$\phi\big(\mathbf{dup}_{\mathbb{C}[t]}\langle f, g\rangle\big) = \mathbf{dup}_{\mathrm{End}(\otimes^n \mathfrak{H}^{(2)})}\langle \phi(f), \phi(g)\rangle \tag{4.12}$$

or, from equation (3.58),

$$\phi(f \otimes g \circ \psi_A) = \phi(f) \otimes \phi(g) \circ \psi_E, \tag{4.13}$$

where ψ and ψ_E denote the coproducts respectively of $\mathbb{C}[\mathbf{t}]$ and End $(\otimes^n \mathfrak{H}^{(2)})$. The latter coproduct is the dual of the algebra product on the space of endormorhisms *via* its canonical self-duality. (For W finite dimensional we have End$W \cong W^* \otimes W \cong (W \otimes W^*)^* \cong (\mathrm{End}W^*$.)

Equation (4.13) is exactly the requirement that ϕ be an algebra map for the algebra structures dual to the respective coalgebra structures. The dual algebra product on End $(\otimes^n \mathfrak{H}^{(2)})$ is, by design, just the usual one, while the commutative algebra product on $\mathbb{C}[\mathbf{t}]^*$ is easily described.

First, we denote by δ_m the element in $\mathbb{C}[\mathbf{t}]^*$ dual to the basis element $\mathbf{t}^m$ of the vector space $\mathbb{C}[\mathbf{t}]$, $m = 0, 1, \ldots$, so that

$$\delta_m(\mathbf{t}^n) = \delta_{m,n}, \tag{4.14}$$

where $\delta_{m,n}$ denotes the usual Kronecker delta. Then elements of $\mathbb{C}[\mathbf{t}]^*$ may be conveniently written as formal sums of the form $\Sigma c_n \delta_n$.

Proposition 4.1. *The commutative algebra product, denoted* $*$, *induced upon* $\mathbb{C}[\mathbf{t}]^*$ *by the dual of the coproduct* ψ *of the Hopf algebra* $\mathbb{C}[\mathbf{t}]$ *is given by*

$$\begin{aligned} \delta_m * \delta_n &= \binom{m+n}{m} \delta_{m+n} \\ &= \frac{(m+n)!}{m!n!} \delta_{m+n}. \end{aligned} \tag{4.15}$$

Proof: For any m, n, k

$$\begin{aligned}(\delta_m * \delta_n)(\mathbf{t}^k) &= (\delta_m \otimes \delta_n)(\psi(\mathbf{t}^k)) \\ &= (\delta_m \otimes \delta_n)(\psi(\mathbf{t})^k) \\ &= (\delta_m \otimes \delta_n)(1 \otimes \mathbf{t} + \mathbf{t} \otimes 1)^k \\ &= (\delta_m \otimes \delta_n)\left(\sum_{l=0} \binom{k}{l} \mathbf{t}^l \otimes \mathbf{t}^{k-l}\right) \\ &= \sum_{l=0} \binom{k}{l} \delta_{m,l} \delta_{n,k-l}. \end{aligned} \tag{4.16}$$

This sum can be non-zero only if $m + n = k$, and, when this is the case, the single surviving term occurs when $m = l$.

Thus,

$$\begin{aligned}(\delta_m * \delta_n)(\mathbf{t}^k) &= \binom{m+n}{m} \delta_{m+n,k} \\ &= \left(\binom{m+n}{m} \delta_{m+n}\right)(\mathbf{t}^k). \end{aligned} \tag{4.17}$$

□

It follows immediately from equation (4.15) that

$$\delta_{m+n} = \frac{m!n!}{(m+n)!} \delta_m * \delta_n, \tag{4.18}$$

so that, for $n > 0$,

$$\begin{aligned}\delta_n &= \frac{1}{n} \delta_{n-1} * \delta_1 \\ &= \frac{1}{n!} \overbrace{\delta_1 * \cdots * \delta_1}^{n} \\ &= \frac{1}{n!} \delta_1^n. \end{aligned} \tag{4.19}$$

Thus, general elements of $\mathbb{C}[\mathbf{t}]^*$ may be expressed in the form

$$\sum \frac{c_n}{n!} \delta_1^n \tag{4.20}$$

and ϕ, being an algebra map, will be specified once $\phi(\delta_1)$ is assigned.

Now, it is classical that the set of algebra morphisms $\mathrm{Hom}_{\mathrm{Alg}}(\mathbb{C}[\mathbf{t}], \mathbb{C})$, of $\mathbb{C}[\mathbf{t}]$ into $\mathbb{C}$, with product operation inherited from the algebra product on $\mathbb{C}[\mathbf{t}]^*$, may be identified with the additive group of $\mathbb{C}$. This identification is obtained by

noting that every element of $\mathrm{Hom}_{\mathrm{Alg}}(\mathbb{C}[\mathbf{t}], \mathbb{C})$ is given by

$$h_z(\mathbf{t}^n) = z^n, \tag{4.21}$$

for some $z \in \mathbb{C}$. That the association $h_z \mapsto z$ is a group morphism is immediate (cf. Abe, 1977, Ch. 4).

These h_z may be written (for each $z \in \mathbb{C}$) in the form

$$\begin{aligned} h_z &= \delta_0 + z\delta_1 + z^2\delta_2 + z^3\delta_3 + \cdots \\ &= \delta_0 + z\delta_1 + \frac{z^2}{2!}\delta_1^2 + \frac{z^3}{3!}\delta_1^3 + \cdots \end{aligned} \tag{4.22}$$

from equation (4.19). Thus we obtain a map

$$\mathbb{C} \to \mathrm{End}\big(\otimes^n \mathfrak{H}^{(2)}\big) \tag{4.23}$$

given formally by

$$z \mapsto \phi(h_z) = I + z\phi(\delta_1) + \frac{z^2}{2!}\phi(\delta_1)^2 + \cdots, \tag{4.24}$$

since δ_0 is the unit for $*$.

Supposing time to be real, we restrict to the additive subgroup $\mathbb{R}$ of $\mathbb{C}$ to obtain the map

$$\mathbb{R} \to \mathrm{End}\big(\otimes^n \mathfrak{H}^{(2)}\big) \tag{4.25}$$

given by $t \mapsto \exp(t\phi(\delta_1))$. Though defined formally, this series will always converge.

The second Schrödinger-like assumption on ϕ concerns the interpretation of δ_1. The logical atom $\mathbf{t}$ was introduced to represent the notional generic "time-step." Let us now take it more literally to represent the generic infinitesimal time differential dt. Then, its linear dual δ_1 should be interpreted as the dual of dt, which is the tangent $\partial/\partial t$. As an operator, densely defined upon $L^2(\mathbb{R})$, it has the property that

$$\left(\frac{\partial}{\partial t}\right)^\dagger = -\frac{\partial}{\partial t}, \tag{4.26}$$

where the dagger denotes the Hilbert space adjoint.

Our second assumption on ϕ is that it should be chosen to preserve this (virtual) property of δ_1; that is,

$$\phi(\delta_1)^\dagger = -\phi(\delta_1). \tag{4.27}$$

Then we may choose

$$\phi(\delta_1) = -iH \tag{4.28}$$

for some Hermitian matrix H.

Thus, the map realizing the action of time (or, rather, the action of time *intervals*) that constitutes a "quantum computation" may be written in the form $t \mapsto e^{-iHt}$. (The physical interpretation of H is, up to an additive real constant, as the operator Hamiltonian of the system.)

Despite its formality, this model seems to have revealed the major qualitative aspects of those processes called quantum computations. To wit

- the unitarity and time reversibility of the processes;
- the structure of the underlying Hilbert space as a quantum register, or tensor product of qubits;
- the primary rôle of quantum entanglement as a resource in the implementation of quantum duplication.

We note also that the unitarity of the action of the dynamical operator entails the preservation, through the computation, of the associated Kripke orthomodel and subspace lattice structures.

We have arrived at the point at which the current treatments of the embryonic theory of quantum computation start, and interested readers could consult the vast and burgeoning list of works devoted to this fascinating subject. In subsequent work we will return to the problem of term assignments for GQ, and possible applications of the theory.

Questions for further consideration include the following:

1. Are there lattice characterizations of IOL? Such lattices might stand in relation to ortholattices as Heyting algebras do to Boolean algebras.
2. Does the translation theorem (Theorem 3.4) have a converse?
3. Is CUT eliminable from proofs in GQ?
4. Do other categories exist in which GQ is realizable?

ACKNOWLEDGMENTS

My grateful thanks to the following for crucial exchanges: Richard Blute, Prakash Panangaden, Ioannis Raptis, Ivan Selesnick, and Mingsheng Ying.

REFERENCES

Abe, E. (1977). *Hopf Algebras*, Cambridge University Press, Cambridge, UK.

Abramsky, S. (1993). Computational interpretations of linear logic. *Theoretical Computer Science* **111**, 3.

Asperti, A. and Longo, G. (1991). *Categories, Types and Structures. An Introduction to Category Theory for the Working Computer Scientist*, MIT Press, Cambridge, UK.

Bell, J. L. and Slomson, A. B. (1969). Models and Ultraproducts: An Introduction, North Holland, Amsterdam.

Blute, R., Panangaden, P., and Seely, R. A. G. (1993). Holomorphic models of exponential types in linear logic. In *Mathematical Foundations of Programming Semantics*, S. Brookes, M. Main, A. Melton, M. Mislove, and D. Schmidt, eds., Lecture Notes in Computer Science, Springer-Verlag, New York. Vol. 802. (Corrected version available on last author's website.)

Curry, H. B. and Feys, R. (1958). *Combinatory Logic I*, North Holland, Amsterdam. Studies in Logic and the Foundations of Mathematics.

Dalla Chiara, M. L., Giuntini, R., Battilotti, G., and Faggian, C. (2002). Quantum logics. In *Handbook of Philosophical Logic*, 2nd edn., D. M. Gabbay and F. Guenther, eds., Kluwer, Dordrecht, The Netherlands, Vol. 6.

Finkelstein, D. (1996). *Quantum Relativity*, Springer, New York.

Fulton, W. and Harris, J. (1991). *Representation Theory: A First Course*, Springer, New York.

Gibbins, P. (1987). *Particles and Paradoxes—The limits of Quantum Logic*, Cambridge University Press, Cambridge, UK.

Girard, J.-Y., Lafont, Y., and Taylor, P. (1988). *Cambridge Tracts in Theoretical Computer Science Vol. 7: Proofs and Types*, Cambridge University Press, Cambridge, UK.

Goldblatt, R. I. (1973). The Stone space of an ortholattice. *Bulletin of the London Mathematical Society* 7, 45.

Goldblatt, R. I. (1974). Semantic analysis of orthologic. *Journal of Philosophical Logic* **3**, 19.

Gunter, C. A. (1992). *Semantics of Programming Languages*, MIT Press, Cambridge, UK.

Heyting, A. (1956). *Intuitionism: An Introduction*, North Holland, Amsterdam.

Hirvensalo, M. (2001). *Quantum Computing*, Springer, New York.

Kalmbach, G. (1983). *Orthomodular Lattices*, Academic Press, New York.

Lambek, J. and Scott, P. J. (1986). *Cambridge Studies in Advanced Mathematics Vol. 7: Introduction to Higher Order Categorical Logic*, Cambridge University Press, Cambridge, UK.

Lang, S. (1993). *Algebra*, 3rd edn., Addison–Wesley, Reading, MA.

Mac Lane, S. and Moerdijk, I. (1991). *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*, Springer, New York.

Mitchell, J. C. (1996). *Foundations of Programming Languages*, MIT Press, Cambridge, UK.

Nielsen, M. and Chuang, I. (2000). *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK.

Rawling, J. P. and Selesnick, S. A. (2000). Orthologic and quantum logic: Models and computational elements. *Journal of the ACM*, **47**(4), 721.

Seely, R. A. G. (1989). Linear logic, $*$-autonomous categories and cofree coalgebras. In *Categories in Computer Science and Logic*, J. Gray and A. Scedrov, eds., Am. Math. Soc., Providence, RI. Contemporary Mathematics, Vol. 92.

Selesnick, S. A. (1998). *Quanta, Logic and Spacetime: Variations on Finkelstein's Quantum Relativity*, World Scientific Publishing, Singapore.

Stoy, J. E. (1977). *Denotational Semantics: The Scott-Strachey Approach to Programming Language Theory*, MIT Press, Cambridge, UK.

Troelstra, A. S. and Schwichtenberg, H. (2000). *Cambridge Tracts in Theoretical Computer Science Vol. 43: Basic Proof Theory*, 2nd edn., Cambridge University Press, Cambridge, UK.