International Journal of Theoretical Physics, Vol. 46, No. 4, April 2007 (© 2006)
DOI: 10.1007/s10773-006-9254-5

Foundation for Quantum Computing II

S. A. Selesnick[1]

Received May 28, 2006; accepted August 7, 2006
Published Online: December 14 2006

In this continuation of an earlier paper we develop further the theme of quantum logical specification and derive from it some apparently physically viable instantiations of potential quantum computing devices. Specifically, in the case of a one-parameter set of terms (or labels)—read as instants of time—we find, emerging quite naturally from the algebraic setup, the paradigm for a single qubit epitomized by the case of a two-state fermion interacting with an external single mode boson. This covers the cases: cavity QED, trapped ions, and, when the qubits are multiplexed appropriately, NMR based systems. (This case degenerates to one in which only bosons are relevant as in the case of pure bosonic harmonic oscillator models in the "dual rail" representation. Such models fly in the face of the logic itself, thus clearly revealing even at this level their well-known shortcomings as practical quantum computing devices. Here as elsewhere logical constraints apparently dominate physical ones.)

In a final section we indicate briefly how this process exactly generalizes, in the case of a manifold of terms more general than the one-parameter case, to yield the notion of holonomic quantum computation.

In the course of this investigation we find an interpretation of path integrals as limits of sequences of logical CUTS, thus establishing a link—though still tenuous—between ensembles of acts of quantum computation and Lagrangians.

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

1. REVIEW

In this section we briefly review the results and notations of Selesnick (2003a). We argued there that, like ordinary classical logic, full quantum logic is inadequate for the constructive exigencies of computational applications. One problem with classical logic lies in the anomaloulsy non-constructive nature of material implication—a problem compounded in quantum logic even for the best behaved choice of implicative connective, namely the Sasaki hook, whose behavior depends crucially upon the presence of orthomodularity. Consequently, we jettisoned orthomodularity and returned to the core quantum logic known as orthologic, or

[1] Physics and Astronomy, University of Missouri St. Louis, St. Louis, Missouri 63121; e-mail: selesnick@mindspring.com

rather that sublogic of it, intuitionistic orthologic, obtained by deleting the non-constructive axioms.

Given rules of inference, the process of making deductions from a set of formulae deemed to be axioms may be codified into a system known as *natural deduction*. A simple such system reproduces, for example, the deductions of intuitionistic logic, and epitomizes the so-called Heyting interpretation of this logic: a formula is identified with its set of deductions and the rules of intuitionistic logic are thereby modelled by adhering grimly to this constructive paradigm. Thus A is intuitionistically valid if and only if its proof set is non-empty, etc. In particular, B is deducible from A if and only if there exists a map from the set of proofs of A to the set of proofs of B. Cartesian products of such proof sets are associated with logical conjunctions of the corresponding formulae, and disjoint unions with logical disjunctions of them. If labels are now used to systematically keep track of the ebb and flow of deductions through their trees, a constructive model of computation soon emerges, describable by means of λ-calculus. Thus, a formula determines a *type* and a label for one of its deductions may be considered to be a variable (or *term*) of that type. Deductions then correspond to *programs*, which transform types. When formalized, this correspondence between deductions in a natural deduction system and programs (i.e. sequences of λ-terms) is known as the *Curry-Howard* correspondence. (For this section please see Selesnick (2003a) and its references.)

In order to formulate a theory applicable wholesale to the universe of such proofs (or programs) it is necessary to move up to a level at which such proofs are themselves the basic entities. This step was achieved by Gentzen with his so-called *sequent calculus*. In this calculus the basic object is the sequent

$$\Gamma \vdash \Delta \tag{1}$$

in which Γ and Δ stand for (possibly empty) finite sequences of formulae, and the informal reading of Eq. (1) is along the lines of: "$\bigwedge \Gamma \Rightarrow \bigvee \Delta$". One may start from the formal specification of a sequent calculus, without assumptions concerning the presence or otherwise of an underlying natural deduction system, and proceed formally *in abstracto* to develop a theory of proofs with wide ramifications. Quite often it is possible—by a judicious choice of term assignments—to reproduce an underlying deduction system for which this sequent calculus then represents a metacalculus. As metacalculi for natural deduction systems these sequent caculi delineate certain symmetries and structural aspects of the underlying deductive system which are hidden if one remains at the lower level of the underlying system. The organizing power of the style has had a major impact on the proof theoretic aspects of deductive logic.

The sequent calculus idea lends itself to other interpretations. A revolution occurred when Girard realized that it could be used to effect an extremely refined computational theory of resource management: here, a sequent of the form (1) is read, roughly speaking, as the depiction of a process in which the resource Γ is consumed to produce the resource Δ. The concomitant logical rules and connectives then acquire entirely new and more general interpretations and obey new laws. The computational and logical ramifications of the resulting logic, called linear, have been deep and wide. This system contains standard intuitionistic logic, with a concomitant deep analysis of its implicative connective, and much else besides.

In Selesnick (2003a) we posited a minimal sequent calculus, **GQ**, for quantum resources, which in fact coincides with a fragment of a version of linear logic. We found that formulae in the deductive version of intuitionistic orthologic translate into formulae of **GQ** *via* a recipe derived by applying a quantum version of the Heyting paradigm. This recipe is identical to one used to translate (non-quantum) intuitionistic logic into linear logic, which thereby acquires an interesting quantum interpretation.

We shall be concerned in this paper only with the multiplicative fragment of **GQ**, whose rules are reproduced below.

GQ

StructuralRules

EXCHANGE

$$\frac{\Gamma, A, B, \Gamma' \vdash D}{\Gamma, B, A, \Gamma' \vdash D}\text{LE} \qquad \frac{\Gamma \vdash A \otimes B}{\Gamma \vdash B \otimes A}\text{RE} \tag{2}$$

WEAKENING

$$\frac{\Gamma \vdash D}{\Gamma, !A \vdash D}\text{LW} \qquad \text{No RW} \tag{3}$$

CONTRACTION

$$\frac{!A, !A, \Gamma \vdash D}{!A, \Gamma \vdash D}\text{LC} \qquad \text{No RC} \tag{4}$$

The Identity Group

AXIOM

$$A \vdash A \quad \text{Ax} \tag{5}$$

CUT

$$\frac{\Gamma \vdash A \quad A, \Gamma' \vdash D}{\Gamma, \Gamma' \vdash D}\text{CUT} \tag{6}$$

Multiplicative Logical Rules

CONJUNCTIVE (MULTIPLICATIVE) CONNECTIVE

$$\frac{\Gamma, A, B \vdash D}{\Gamma, A \otimes B \vdash D}\text{L}\otimes \qquad \frac{\Gamma \vdash A \quad \Gamma' \vdash B}{\Gamma, \Gamma' \vdash A \otimes B}R\otimes \tag{7}$$

NEGATION

$$\frac{\Gamma \vdash A \otimes D}{\Gamma, A^* \vdash D}L* \qquad \frac{\Gamma, A \vdash D}{\Gamma \vdash A^* \otimes D}R* \tag{8}$$

!

$$\frac{\Gamma, A \vdash D}{\Gamma, !A \vdash D}\text{L}! \qquad \frac{!\Gamma \vdash A}{!\Gamma \vdash !A}\text{R}! \tag{9}$$

(Recall that here D stands for either a single formula or no formula, i.e. the empty sequence, and when it appears in the form $\otimes D$, the $\otimes$ symbol is presumed to be absent when D is empty.)

To introduce a dynamical element into the *tabula rasa* represented by **GQ** we append a single axiom, which in this paper we shall name, as follows.

AXIOM D

$$!A \vdash !\mathbf{t} \otimes !A \qquad \text{Ax D} \tag{10}$$

Here $\mathbf{t}$ denotes a logical atom and A is any formula. The idea is that $\mathbf{t}$ represents a resource (a "time step") which may be used to accompany, or "time," each repeatable resource $!A$ via a deduction (10) which preserves each type. When expressed as a deduction in the static, resource insensitive language of intuitionistic orthologic this condition translates into Ax D. It is a simple exercise to show that an equivalent form for it is:

$$(!\mathbf{t})^* \vdash (!A)^* \otimes (!A) \tag{11}$$

If the formula D can be deduced from Γ in **GQ**, with Ax D appended, we shall in this paper write $\Gamma \vdash D$, leaving the turnstile unadorned. Such sequents are called *proofs*. The *of course* operator !—following Girard in his parlance and notation—is provided for the purposes of supplying the storage capable version of a quantum resource, which in general does not admit such an operation of copying into storage.

As discussed in Selesnick (2003a) **GQ** may be realized or interpreted within the category $\mathcal{H}_F$ of finite dimensional complex Hilbert spaces, a natural choice from the point of view of quantum physics. In this realization each atomic formula in **GQ** is associated with an object in $\mathcal{H}_F$. Then **GQ** formulae are built up by interpreting $\otimes$ and $(\ )^*$ to have their usual meanings in $\mathcal{H}_F$, and by assigning interpretations in $\mathcal{H}_F$ to the basic sequents of **GQ**. (As in Selesnick (2003a) we shall not in this paper distinguish notationally between formulae used abstractly in **GQ** and their interpretations in $\mathcal{H}_F$.)

Of particular interest is the interpretation of $!A$ as the exterior algebra $E(A)$ (or Fermi–Dirac Fock space based on A) with its full structure as a graded Hopf algebra with coproduct $\psi : E(A) \to E(A) \otimes E(A)$, determined on first grade elements x by

$$\psi(x) = 1 \otimes x + x \otimes 1, \tag{12}$$

effecting the quantum duplication operation in the rule LC (of (4)), an operation clearly producing entangled states. (As of this writing, no other candidate for $!A$ realized in $\mathcal{H}_F$ seems to be known.) It is interesting also since if A is taken to represent a "quantum set," then $E(A)$ represents the quantum set of quantum subsets of this quantum set A, in Finkelstein's formulation: this enables a direct logical interpretation to be given to the basic storage capable unit, namely $E(\mathfrak{H}^{(1)}) \cong \mathbb{C} \oplus \mathfrak{H}^{(1)}$, where $\mathfrak{H}^{(n)}$ represents the complex Hilbert space of dimension n. $E(\mathfrak{H}^{(1)})$ is of course also known as the *qubit*.

Returning to Ax D in the form in given in Eq. (11) we note that whatever interpretation is given to $\mathbf{t}$ in $\mathcal{H}_F$ the right-hand side will yield:

$$E(A)^* \otimes E(A) \cong \operatorname{End} E(A) \tag{13}$$

and with a choice of basis in A inducing a decomposition

$$A \cong \bigoplus_{k=1}^{n} \mathbb{C}, \tag{14}$$

where $n = \dim A$, we obtain

$$\begin{aligned} E(A) &\cong E\left(\bigoplus_{k=1}^{n} \mathbb{C}\right) \\ &\cong \bigotimes_{k=1}^{n} E(\mathbb{C}) \\ &\cong \mathfrak{H}^{(2n)}. \end{aligned} \tag{15}$$

Thus, as noted, for $n = 1$, the qubit $E(\mathbb{C})$ emerges as the irreducible storage capable unit in $\mathcal{H}_F$, and the general case is a tensor product of these.

To interpret the multiplexed time step *classically* requires a different choice for the interpretation of the ! operator, which takes us out of the category $\mathcal{H}_F$. This could be allowed for by expanding somewhat both the rules of **GQ** and the target category in which we interpret them, a project we leave for a later paper. To avoid any possible toxicity arising from such mixing of categories—which would affect only the rules of negation—we shall in this paper adopt Ax D in the form given by Eq. (11), taking care to avoid inappropriate uses of the rules of negation.

In Selesnick (2003a) we chose to interpret $!\mathbf{t}$ as $\mathbb{C}[\mathbf{t}]$, the (commutative) polynomial algebra in one variable (which coincides both with the bosonic Fock space and the tensor algebra on the one-dimensional space) with its (cocommutative) coalgebra coproduct given as in Eq. (12). Then $\mathbb{C}[\mathbf{t}]^*$, expressible also as the space $\mathbb{C}[[\mathbf{t}]]$ of formal power series in $\mathbf{t}$, becomes a commutative algebra with product $*$ given by the dual of the coproduct. With

$$\delta_m(\mathbf{t}^n) = \delta_{m,n}, \tag{16}$$

where $\delta_{m,n}$ denotes the usual Kronecker delta, we found that

$$\delta_m * \delta_n = \frac{(m+n)!}{m!\,n!}\,\delta_{m+n} \tag{17}$$

so that

$$\delta_n = \frac{1}{n!}\,\delta_1^n \tag{18}$$

where powers are taken in the product $*$.

Taking $\mathbf{t}$ literally to represent the infinitesimal time step dt we may interpret its dual δ_1 (in End $E(A)$) as the tangent $\frac{\partial}{\partial t}$, an antihermitian operator in its usual incarnation. If we assume also that Ax D (in the form (11)) respects the repetitive behavior of the resource "time," we arrive at the specification of the map which interprets (11) as an algebra homomorphism in which δ_1 is assigned an operator upon End $E(A)$ of the form $-iH$, where H is Hermitian. On noting that the additive group $\mathbb{C}$ is isomorphic with the group $\mathrm{Hom}_{\mathrm{Alg}}(\mathbb{C}[\mathbf{t}], \mathbb{C})$ (with the group structure inherited from the Hopf algebra structure, which coincides with $*$ when the later set is regarded as a subset of $\mathbb{C}[\mathbf{t}]^*$) *via* the map

$$z \mapsto h_z \tag{19}$$

where

$$h_z = \delta_0 + z\,\delta_1 + z^2\,\delta_2 + \cdots \tag{20}$$

we obtain a map

$$\mathbb{R} \hookrightarrow \mathbb{C} \to \mathrm{End}\,\mathfrak{H}^{(2n)} \tag{21}$$

given by

$$t \mapsto e^{-iHt}. \tag{22}$$

Thus is derived the basic notion of a quantum computation in classical time.

2. CUTS AND LAGRANGIANS

Starting from an unadorned (intuitionistic) Gentzen sequent calculus one may generally derive a corresponding natural deduction system by the judicious assignment of terms to sequents and by then regarding these terms as λ-calculus like descriptions of underlying deductions. In this way a Gentzen sequent calculus yields its computational capacity and/or acquires a functional interpretation. Significant such interpretations have been given to linear logic, for instance, in Abramsky (1993).

Since in this paper we shall be dealing exclusively with an interpretation in a category of vector spaces of the sequent calculus **GQ**, with Ax D appended, we shall postpone the ticklish exercise of rigorous term assignment to this calculus itself. Instead, we shall use the logical structure of **GQ** as a guide to the manipulation of the familiar terms of the theory of these spaces. Thus, for a sequent of the form $A \vdash B$, term assignments would entail the possibility of naming (or labelling) different terms of type $\mathrm{Hom}(A, B)$ or, in the category $\mathcal{H}_F$, of naming different maps.

The sequent calculus conventions usually place the term to the right of the turnstile as in: $A \vdash \phi : B$.

Consider a sequent of the form (cf. (11)):

$$A, B \vdash A. \tag{23}$$

Two instances of this sequent, namely

$$A, B \vdash \phi_1 : A \qquad A, B \vdash \phi_2 : A \tag{24}$$

may be CUT to produce the sequent (cf. (6))

$$A, B, B \vdash \phi_2 ? \phi_1 : A \tag{25}$$

where the term $\phi_2 ? \phi_1$ to the right of the turnstile will be interpreted as follows: the two interpreted sequents

$$\phi_1 : A \otimes B \to A \qquad \phi_2 : A \otimes B \to A \tag{26}$$

are CUT to produce

$$\phi_2(\phi_1 \otimes 1_B) : A \otimes B \otimes B \to A. \tag{27}$$

Now $\phi_k : A \otimes B \to A$ uniquely determines a map $f_k : B \to \operatorname{End} A$ $(k = 1, 2)$ given in an obvious notation by

$$f_k(b)\, a = \phi_k(a \otimes b) \tag{28}$$

(cf. Mac Lane (1963), p. 145) so that

$$\begin{aligned} \phi_2(\phi_1 \otimes 1_B)(a \otimes b_1 \otimes b_2) &= \phi_2(\phi_1(a \otimes b_1) \otimes b_2) \\ &= \phi_2(f_1(b_1)\, a \otimes b_2) \\ &= f_2(b_2) f_1(b_1)\, a \end{aligned} \tag{29}$$

Thus, cutting the two sequents together yields the map $B \otimes B \to \operatorname{End} A$ given by

$$b_1 \otimes b_2 \mapsto f_2(b_2) f_1(b_1), \tag{30}$$

and, similarly, applying CUT to n such sequents yields a map $\bigotimes_{k=1}^{n} B \to \operatorname{End} A$ given by

$$b_1 \otimes \cdots \otimes b_n \mapsto f_n(b_n) \cdots f_1(b_1). \tag{31}$$

Note that the f_k s are applied in the order in which the cuts are executed, with the earlier ones appearing to the right.

Now we apply this to n instances of Ax D, with $B = \mathbb{C}\,[\mathbf{t}]^* \, (= \mathbb{C}\,[[\mathbf{t}]])$ in the form $A, \mathbb{C}\,[\mathbf{t}]^* \vdash A$ non-toxically derived from (11), A being finite dimensional, with a fixed Hilbert space $A (= \mathfrak{H}^{(2n)}) \equiv \mathfrak{H}$, but with possibly different choices H_k of Hamiltonians. We obtain the map

$$\bigotimes^{n} \mathbb{C}\,[[\mathbf{t}]] \to \operatorname{End} \mathfrak{H} \tag{32}$$

given by the analogue of (31), and, as in Section 1, we obtain the map of additive groups

$$\bigotimes\nolimits_{\mathbb{Z}}^{n} \mathbb{R} \to \bigotimes\nolimits_{\mathbb{Z}}^{n} \mathbb{C}\,[[\mathbf{t}]] \tag{33}$$

given by

$$t_1 \otimes \cdots \otimes t_n \mapsto h_{t_1} \otimes \cdots \otimes h_{t_n} \tag{34}$$

(with the commutative algebra structure $*$ of $\mathbb{C}\,[[\mathbf{t}]]$ being used on the right: recall that $h_{t_1+t_2} = h_{t_1} * h_{t_2}$ in the notation of Section 1.) Composing the last two maps, we obtain, for any sequence $(\Delta t_1, \Delta t_2, \ldots, \Delta t_n)$ of real numbers, the map

$$\prod^{n} \mathbb{R} \to \operatorname{End} \mathfrak{H} \tag{35}$$

given by

$$(\Delta t_1, \Delta t_2, \ldots, \Delta t_n) \mapsto e^{-i H_n \Delta t_n} e^{-i H_{n-1} \Delta t_{n-1}} \ldots e^{-i H_1 \Delta t_1}. \tag{36}$$

In summary, for choices H_k and any sequence $(\Delta t_1, \Delta t_2, \ldots, \Delta t_n)$ of real numbers, by executing the indicated CUTS we obtain in discrete form the corresponding time-ordered integral, denoted in the physics literature as

$$\mathrm{T}e^{-i\int_T H(t)\,dt}, \tag{37}$$

where T is a *path* in $\mathbb{R}$ (since the Δt_k may differ in sign) whose subdivision yields the Δt_k.

Thus we have realized the execution of cuts—the primary locus of "computation" itself in the proof theoretical view of computation—in terms of the basic quantum mechanical dynamical operator (37). (In the Schrödinger picture of quantum mechanics a state ψ at time t, $|\psi(t)\rangle$, is given a general prescription of the form

$$|\psi(t)\rangle = \mathrm{T}e^{-i\int_0^t H(t)dt}\,|\psi(0)\rangle\,.) \tag{38}$$

Now the quantities of physical interest are not the observable operators themselves but rather their associated amplitudes, and it is when we consider these amplitudes that the Lagrangian appears. The general formula for such a transition amplitude between sufficiently characteristic states $|\psi(t_2)\rangle$ and $|\psi(t_1)\rangle$, as discovered by Feynman, is given by

$$\langle\psi(t_2)|\psi(t_1)\rangle = \int e^{i\int_{t_1}^{t_2} L(t)dt}\,\mathcal{D}\psi \tag{39}$$

where L denotes the associated Lagrangian; the inner integral is over a *path* connecting $\psi(t_1)$ to $\psi(t_2)$ and the outer integral is over *all* such paths, $\mathcal{D}\psi$ denoting a rather optimistically conceived measure over the space of such paths.

The inner integral is a limit of discretizations of the relevant path in $\mathbb{R}$ and we have, over an element of such a discretization:

$$\langle\psi(t+\Delta t)|\psi(t)\rangle \propto e^{iL(t)\Delta t}. \tag{40}$$

The inner path integral itself may be realized as the limit of products proportional to the right hand side of (40). Such products may now be thought to result from the execution of cuts of instances of Ax D, with the L_k replacing the H_k.

Thus $e^{i\int L dt}$ is the limit of the amplitudes which result from all the possible cuts, or quantum computations, required to compute that path's contribution toward the transition amplitude. So, in a sense, the operator $\int L dt$ contains all the information concerning the effect of sequences of those cuts required to accomplish the computation, along the path in question, of that path's contribution to the transition amplitude between the initial and final states. Thus it is indeed a good representer of "computational capacity" relative to the path in question, as surmised by Toffoli (Toffoli (1999); see also Frank (2005)).

We digress briefly to interpret a simple such path integral from this point of view: namely, the case of the vacuum-to-vacuum amplitude for a charged fermion of mass m and charge e interacting with an external electromagnetic field. Here the interaction Lagrangian density is of the form

$$\mathcal{L}_I = \bar{\eta}\,(i\not{D} - m)\,\eta \tag{41}$$

where $\not{D} = \not{\partial} + ie\not{A}$, and η denotes the fermion field operator regarded here as a Grassmannian variable. (Note that since the Dirac matrices are essentially operator versions of the differentials dx_μ, $\not{\partial}$ is essentially an operator version of the act of infinitesimal transport along a principle generator of the light-cone. So the term $\bar{\eta}\,\not{\partial}\,\eta$ may be parsed loosely as follows:

η *destroys a particle;*

$\not{\partial}$ *infinitesimally transports the resulting hole through spacetime;*

$\bar{\eta}$ *then creates a particle at the site of the relocated hole.*

Consequently, this term, when integrated, computes the transport of the particle along a path. Similarly, the term $\bar{\eta}\not{A}\eta$ represents in-place interaction of the fermion with the external field.)

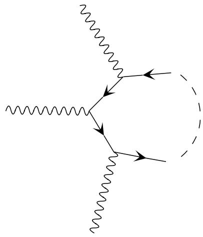
The vacuum-to-vacuum transition amplitude is given by the Grassmannian path integral

$$\begin{aligned}\int e^{i\int\bar{\eta}(i\not{D}-m)\eta}\,\mathcal{D}\bar{\eta}\,\mathcal{D}\eta &= \det(i\not{D} - m)\\ &= \det(i\not{\partial} - m - e\not{A})\\ &= \det(i\not{\partial} - m)\det\left(1 - \frac{i}{i\not{\partial} - m}(-ie\not{A})\right).\end{aligned} \tag{42}$$

Ignoring the first factor (an infinite constant) and recalling that $\det M = \exp(\operatorname{tr}\ln M)$ we may expand the interaction factor as:

$$\begin{aligned}\det\left(1 - \frac{i}{i\not{\partial} - m}(-ie\not{A})\right) &= \exp\sum_{n=1}^{\infty}\left(-\frac{1}{n}\right)\operatorname{tr}\left[\left(\frac{i}{i\not{\partial} - m}(-ie\not{A})\right)^{n}\right]\\ &= \exp\sum_{n=1}^{\infty}\left(-\frac{1}{n}\right)\int \operatorname{tr}[(-ie\not{A}(x_1))S_F(x_2 - x_1)\cdots\\ &\qquad\cdots(-ie\not{A}(x_n))S_F(x_1 - x_n)]\,dx_1\ldots dx_n,\end{aligned} \tag{43}$$

where S_F is the appropriate propagator. Now each term in the summation represents a possible "computation" of the relevant contribution to the vacuum-to-vacuum amplitude in which the particle propagates between interactions with the bosons of the external field. Each such term corresponds to the Feynman vacuum-to-vacuum diagram with n legs shown below:



Thus, in this naïve example, the path integral does indeed contain explicit information concerning the entire repertoire of quantum "computations" open to the system (fermion, field) undergoing a vacuum-to-vacuum transition, each of which is depicted by a Feynman diagram of the above type.

3. MODELS AND REPRESENTATIONS

In this section we consider the structure of possible Hamiltonians, as constrained by the algebraic dictates of our logical model. First we briefly mention a consequence of the qubit register structure which will be taken up in more detail elsewhere. Namely, as already noted, for an object $\mathfrak{H}^{(n)}$ in $\mathcal{H}_F$ a choice $\{\xi_k\}_{k=1}^n$ of basis induces an isomorphism

$$\begin{aligned}\mathfrak{H}^{(n)} &\cong \bigoplus_{k=1}^{n} \mathbb{C}\\ &\equiv \mathbb{C}\,\xi_1 \oplus \cdots \oplus \mathbb{C}\,\xi_n,\end{aligned} \tag{44}$$

where we use the last expression in order to distinguish the summands. Such a decomposition then induces an isomorphism, or *encoding*, of the exterior algebra into the n-fold quantum register. Namely,

$$\begin{aligned}E\left(\mathfrak{H}^{(n)}\right) &\cong E\,(\mathbb{C}\,\xi_1 \oplus \cdots \oplus \mathbb{C}\,\xi_n)\\ &\cong E\,(\mathbb{C}\,\xi_1) \otimes \cdots \otimes E(\mathbb{C}\,\xi_n).\end{aligned} \tag{45}$$

For example, with $n = 2$, we have a two qubit register decomposing as

$$E\,(\mathbb{C}\,\xi_1) \otimes E\,(\mathbb{C}\,\xi_2) \cong E\,(\mathbb{C}\,\xi_1 \oplus \mathbb{C}\,\xi_2) \tag{46}$$

or

$$(\mathbb{C} \oplus \mathbb{C}\,\xi_1) \otimes (\mathbb{C} \oplus \mathbb{C}\,\xi_2) \cong \mathbb{C} \oplus (\mathbb{C}\,\xi_1 \oplus \mathbb{C}\,\xi_2) \oplus \bigwedge^2 (\mathbb{C}\,\xi_1 \oplus \mathbb{C}\,\xi_2)\,. \tag{47}$$

The unadorned $\mathbb{C}$ one both sides represents the corresponding "vacuum" or quantum "off" states (which function also as the units for the respective algebras). The middle term on the right is itself a qubit and corresponds (*via*) canonical isomorphisms) to a component of the left hand side as follows:

$$\mathbb{C}\,\xi_1 \oplus \mathbb{C}\,\xi_2 \cong (\mathbb{C}\,\xi_1 \otimes \mathbb{C}) \oplus (\mathbb{C} \otimes \mathbb{C}\,\xi_2) \tag{48}$$

in which $\xi_1 \mapsto \xi_1 \otimes 1$ and $\xi_2 \mapsto 1 \otimes \xi_2$.

In the usual notation the 1s correspond to the "off" computational states, which we shall write $|0\rangle_1$ and $|0\rangle_2$, and the ξ_k to the "on" states $|1\rangle_k$, $k = 1, 2$. Thus our encoding yields a representation of a qubit in a combined system in which a basis of computational states may be written $|1\rangle_1\,|0\rangle_2$ and $|0\rangle_1\,|1\rangle_2$ or just $|10\rangle$ and $|01\rangle$. This is the "dual-rail" representation: cf. Nielsen and Chuang (2000). (More elaborate encodings are possible with bigger qubit registers and there are concomitant physical interpretations in terms of many body systems. These matters will be taken up elsewhere.)

Now we turn to the issue of Hamiltonian structure. As is well-known, and easily checked, the most general single qubit Hamiltonian acting on some $\mathfrak{H}^{(2)}$ may be written in the form:

$$H = \Omega_0 I + \Omega_1\sigma_1 + \Omega_2\sigma_2 + \Omega_3\sigma_3 \tag{49}$$

where the Ωs are, for the time being, real constants and the σs are the usual Pauli matrices: $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Here $\mathcal{H}^{(2)}$ is assumed fixed. (We have absorbed, or ignored, various constants which are irrelevant to our discussion here.)

Introducing a term structure into **GQ** entails the possibility of multiplexing instantiations of $\mathfrak{H}^{(2)}$ itself over some set of terms. Such a set of terms may be identified with a set of experimenters, each using a different instantiation of $\mathcal{H}^{(2)}$, or with a set of labels for such a set of experimenters. Then the ubiquitous overall ignorable complex phase which would accompany each state in $\mathfrak{H}^{(2)}$ in a particular instantiation—that is, at a particular label—would in general vary from label to label. That is to say, the space $\mathfrak{H}_1^{(2)} \cong \mathbb{C} \otimes_{\mathbb{C}} \mathfrak{H}^{(2)}$ at time t_1 will in general be related to the space $\mathfrak{H}_2^{(2)} \cong \mathbb{C} \otimes_{\mathbb{C}} \mathfrak{H}^{(2)}$ at time t_2 by a unitary Berry-like phase factor $g_{12} \equiv e^{i\theta_{12}}, \theta_{12} \in \mathbb{R}$, acting on the first factor $\mathbb{C}$. (These factors are, of course, ignorable in the case of a fixed choice of $\mathfrak{H}^{(2)}$ for all terms (times)). Assuming consistency among the various phase factors for different t, the collection of $\mathbb{C}$s form a (complex) *line bundle* $\mathbf{L}$ over the set of terms, or space of parameters $\mathbb{R}$.

Now the multiplexing of a Hilbert space of states over a space of parameters marks the transition to a (quantum) field theory and requires the introduction of machinery—second quantization—appropriate to that subject. Observables must now act globally upon the bundles involved and in this context line bundles are associated with the statistics of *bosons*, essentially because any tensor product $\otimes^n \mathbf{L}$

of line bundles is necessarily symmetric. (See Selesnick (1983), or Mallios (2006) for an exhaustive treatment.) In our case a simplification is achieved because **L** may always be trivialized ($\mathbb{R}$ being contractible) and so we can consider it to be the trivial bundle over $\mathbb{R}$ with fibre $\mathbb{C}$. The L^2 cross-sections of such a bundle, which constitute the Hilbert space of states for the boson field that emerges, is then just $L^2(\mathbb{R})$ realized as the bosonic Fock space over $\mathbb{C}$ defining a field of bosons of a single species or mode, with annihilation (creation) operators written $a(a^\dagger)$.

Proceeding entirely formally, we revert to the general Hamiltonian (Eq. (49)) and note that it may be second quantized to accommodate the boson field by the usual method of replacing the real amplitudes Ω_k by Hermitian operators upon $L^2(\mathbb{R})$, all of which may be expressed ultimately in terms of the operators $a,\ a^\dagger$. Thus H is promoted as follows:

$$H = \Omega_0 \otimes I + \Omega_1 \otimes \sigma_1 + \Omega_2 \otimes \sigma_2 + \Omega_3 \otimes \sigma_3. \tag{50}$$

In this way, a general mechanism for executing quantum computations upon a single qubit seems to be generated by:

- coupling a fermionic two-state quantum to a field of single mode bosons; and
- inducing transitions by joint annihilation/creation of the paired fields.

We can now make some simple choices for the Ω operators. For instance, let us try first the following prescription:

$$\Omega_0 = c_0 a^\dagger a, \quad \Omega_k = 0, \quad k = 1, 2, 3$$

where c_0 is a real constant. This is exactly the pure bosonic quantum harmonic oscillator, in which the fermionic storage capable element is entirely irrelevant. This can be encoded according to the "dual-rail" prescription described earlier and turns out to be unsatisfactory for various reasons (Nielsen and Chuang, 2000). From our point of view, the problem resides in the fact—already mentioned—that this representation is not *storage capable* in the technical sense of our logic. The problem with it is usually attributed to its not being "digital."

More interesting is the following minimal choice, for real constants c_k:

$$\Omega_0 = c_0 a^\dagger a, \tag{51}$$

$$\Omega_1 = c_1(a + a^\dagger), \tag{52}$$

$$\Omega_2 = c_2 i(a - a^\dagger), \tag{53}$$

$$\Omega_3 = c_3. \tag{54}$$

With $c_1 = c_2 = g$ this yields

$$H = c_0 a^\dagger a \otimes I + g(a^\dagger \otimes \sigma_- + a \otimes \sigma_+) + c_3\sigma_3 \tag{55}$$

where $\sigma_\pm = \frac{1}{2}(\sigma_1 \pm \sigma_2)$.

With an appropriate choice of constants, this is exactly the *Jaynes–Cummings* Hamiltonian (in the "rotating wave" representation). The first term represents a harmonically oscillating boson source and the middle term corresponds to the interaction between the boson field and the fermion qubit: a boson annihilation(a)/creation($a^\dagger$) is accompanied by a fermion raising(σ_+)/lowering(σ_-) as a boson is absorbed/emitted. The third term represents the Hamiltonian for the two-state fermion itself, c_3 being interpreted as the energy difference between its two levels.

This Hamiltonian covers the quantum computational paradigms described by the terms: cavity QED (the bosons being photons) and trapped ions (in which the boson are phonons in the ambient medium). When suitably multiplexed to many qubits, it also covers the case of the NMR paradigm. (Cf. Mawhinney and Schreckenbach (2004) and Nielsen and Chuang (2000).)

4. HOLONOMIC QUANTUM COMPUTATIONS

In this brief final section we shall indicate how the setup described above—which generates quantum computations—maybe generalized, in a completely natural fashion, to more general spaces of parameters to yield the notion of holonomic quantum computation.

Let us return to Ax D in the form given in Eq. (11):

$$\mathbb{C}\,[\mathbf{t}]^* \vdash \mathrm{End}\,\mathfrak{H}. \tag{56}$$

We have identified $\mathbf{t}$ with the 1-form dt on $\mathbb{R}$ which generates the space $\Omega^1(\mathbb{R})$ of (complex) cotangents on $\mathbb{R}$ (which is the space dual to the tangent space). Moreover, the algebra structure on $\mathbb{C}[\mathbf{t}]^*$ is given by the dual of the coalgebra coproduct on $\mathbb{C}\,[\mathbf{t}]$ (Eq. (12)).

This generalizes to the case when the manifold $\mathbb{R}$ of presumed parameters (instants of time) is replaced by a more general manifold of parameters $\mathcal{M}$, which could be spacetime itself or sub-manifolds thereof, or something more general. Then, $\mathbb{C}\,[\mathbf{t}]$ $(\cong T\big(\Omega^1(\mathbb{R})\big))$ is replaced by $T(\Omega^1(\mathsf{M}))$ where $T(\ )$ as usual denotes the tensor algebra functor, and the map interpreted by the analogue of Eq. (56) is presumed to also preserve the algebra structures. Then Ax D generalizes directly to yield

$$T(\Omega^1(\mathsf{M}))^* \vdash \mathrm{End}\,\mathfrak{H}, \tag{57}$$

an algebra morphism with the algebra product on the left being that given by the dual of the algebra product on the tensor algebra. This (commutative) product, also denoted by $*$, is given explicitly on generators by adding all shuffles of their indices, a shuffle of two sets being a permutation of their union preserving the original order of each constituent set (cf. Selesnick (2003b), p. 227). Thus, for example

$$a_{k_1k_2} * a_{k_3} = a_{k_1k_2k_3} + a_{k_1k_3k_2} + a_{k_3k_1k_2}. \tag{58}$$

(Note that this of course reduces to the product $*$ on $\mathbb{C}\,[\mathbf{t}]^*$.) The generalization of Eq. (22), namely the assignment

$$\mathbf{t}^* = \delta_1 = (dt)^* = \frac{\partial}{\partial t} \mapsto -iH,$$

for Hermitian H, now generalizes to

$$\frac{\partial}{\partial x_\mu} = X^\mu \mapsto -iA^\mu \tag{59}$$

where the X^μ constitute a tangent field on $\mathcal{M}$, $\mu = 1, \ldots, \dim \mathcal{M}$, with A^μ Hermitian. The $-iA^\mu$ constitute a field of elements in the Lie algebra $\mathfrak{u}(N)$, $N = \dim \mathcal{H}$, of the unitary group $U(N)$. Now, writing $T(\Omega^1(\mathbb{M}))^*$ as the space of formal series $T[[X^\mu]]$, we note that the tensor algebra $T(X^\mu)$ on the symbols X^μ inherits the shuffle product structure from $T[[X^\mu]]$ when realized as the subspace of finite series (or finitely supported) elements thereof. Moreover, $T\,(X^\mu)$ acquires also a non-cocommutative *coproduct* structure, coming essentially from the original product structure of the tensor algebra $T(X^\mu)$. It is given explicitly by

$$\begin{aligned}\psi_C\,(X^{\mu_1}X^{\mu_2}\cdots X^{\mu_n}) = X^{\mu_1}\cdots X^{\mu_n} \otimes 1 + X^{\mu_1}\cdots X^{\mu_{n-1}} \otimes X^{\mu_n} \\ + \cdots + 1 \otimes X^{\mu_1}\cdots X^{\mu_n}.\end{aligned} \tag{60}$$

(Note that in the case of a single generator this reduces to the one dimensional affine algebraic structure Eq. (12) described in Section 1). This coproduct is in fact a morphism for the shuffle product so that with the shuffle product and the coproduct given above $T\,(X^\mu)$ has the structure of a bialgebra. Consequently, $\mathrm{Hom}_{\mathrm{Alg}}(T\,(X^\mu)\,, \mathbb{C})$ has the structure of a (non-commutative) semigroup given as usual by $\phi_1 * \phi_2 = \phi_1 \otimes \phi_2 \circ \psi_C$.

Now the assignment (59) naïvely encapsulates the notion of a ($\mathfrak{u}(N)$) *connection* on what is now a bundle of $\mathfrak{H}$s which vary over the space of terms or parameters: for each tangent at a point of $\mathcal{M}$, an infinitesimal transformation is assigned to the corresponding Hilbert space fibre. Conversely, given such an assignment, it is possible to globalize it in a way which generalizes the steps from (11) to (22). In the course of so doing holonomic computations arise quite naturally. We shall summarizes the steps in this quite technical argument: more detail is supplied in Selesnick (2003b), Chapter 12.

Suppose then that we have a set X^μ, $\mu = 1, \ldots, n$, of indeterminates, and assignments

$$X^\mu \mapsto B^\mu, \tag{61}$$

where the B^μ are elements of the Lie algebra $\mathfrak{g}$ of a compact Lie group G. The Lie algebra $\mathfrak{g}$ may be embedded into its universal enveloping algebra $U(\mathfrak{g})$ *via* the canonical map

$$\iota : \mathfrak{g} \to U(\mathfrak{g}). \tag{62}$$

Since $U(\mathfrak{g})$ is an associative algebra, composition of this with the assignments (61) lifts to a map of algebras

$$\phi_B : T\,(X^\mu) \to U(\mathfrak{g}) \tag{63}$$

by the universal property of the tensor algebra. This map is given by

$$\phi_B\,(X^{\mu_1}\cdots X^{\mu_k}) = \iota\,(B^{\mu_1})\cdots\iota\,(B^{\mu_k})\,. \tag{64}$$

It is quickly verified that this is a map also of coalgebras. Consequently, the dual

$$\phi_B^* : U(\mathfrak{g})^* \to \; T\,(X^\mu)^* \tag{65}$$

is a map of the dual algebras. Let $R(G)$ denote the (Hopf) algebra of representative functions on G. This is the algebra generated (finitely in the Lie case) by the coefficients of irreducible unitary representations. There is a commutative algebra morphism

$$\theta : R(G) \to U(\mathfrak{g})^* \tag{66}$$

given on generators as follows. For an irreducible unitary representation $\sigma : G \to GL(V^{(\sigma)})$, where $GL(\,)$ denotes the general linear group of the vector space argument, let

$$u_{ij}^{(\sigma)}(g) = \langle \xi_i\,|\sigma(g)|\,\xi_j\rangle \tag{67}$$

where $g \in G$ and $\{\xi_k\}$ is an orthonormal basis in $V^{(\sigma)}$. Then $d\sigma : \mathfrak{g} \to \mathfrak{gl}(V^{(\sigma)})$, where $\mathfrak{gl}(V^{(\sigma)})$ is the Lie algebra of $GL(V^{(\sigma)})$, is a map of Lie algebras. By the universal property of $U(\,)$, $d\sigma$ lifts uniquely to a map of algebras

$$L_\sigma : U(\mathfrak{g}) \to \mathrm{End}\,V^{(\sigma)}. \tag{68}$$

Then θ is given, for $w \in U(\mathfrak{g})$, by

$$\theta\big(u_{ij}^{(\sigma)}\big)(w) = \langle \xi_i\,|L_\sigma(w)|\,\xi_j\rangle. \tag{69}$$

Thus we obtain a map of commutative algebras

$$\phi_B^* \circ \theta : R(G) \to T(X^\mu)^* \tag{70}$$

where the shuffle product is understood on the right.

Now suppose that we are given a sufficiently well-behaved curve C in $\mathcal{M}$. Then, as observed by Ree (1958), a homomorphism, also denoted by C,

$$C : T(X^\mu)^* \to \mathbb{C}, \tag{71}$$

is determined by

$$C(X^{\mu_1}\cdots X^{\mu_n}) = \int_C dx_{\mu_1}\dots dx_{\mu_n} \tag{72}$$

where the right hand side denotes the corresponding Chen iterated integral defined inductively as follows. We suppose the curve C to be defined by specifying a continuous function $f:[a,b]\to\mathcal{M}$ of bounded variation. For each integer $m\ge 0$ and $t\in[a,b]$ we define an *iterated integral* (over the curve C) recursively by

$$\int_a^t 1 = 1, \tag{73}$$

$$\int_a^t dx_{\mu_1}\dots dx_{\mu_n} = \int_a^t \left(\int_a^s dx_{\mu_1}\dots dx_{\mu_{n-1}}\right)\dot{x}_{\mu_n}(f(s))\,ds \tag{74}$$

Then the iterated integral over C—the right hand side of Eq. (72)—is defined to be $\int_a^b dx_{\mu_1}\dots dx_{\mu_n}$ (cf. Tavares (1994)).

Now, owing to the fact the for each σ there exists a conjugate representation $\bar{\sigma}$ such that

$$u_{ij}^{(\bar{\sigma})} = \overline{u}_{ij}^{(\sigma)}$$

for some choice of basis, it is easy to see that the composition

$$h_C^B \equiv C\circ\phi_B^*\circ\theta : R(G)\to\mathbb{C} \tag{75}$$

satisfies

$$h_C^B(\bar{f}) = \overline{h_C^B(f)}. \tag{76}$$

Consequently, by the Tannaka–Krein duality theorem, there exists an element $g\in G$ such that, for all $f\in R(G)$:

$$f(g) = h_C^B(f). \tag{77}$$

For $f = u_{ij}^{(\sigma)}$ and unfolding the various maps we obtain

$$\begin{aligned}\left\langle \xi_i\,|\sigma(g)|\,\xi_j\right\rangle &= \sum_{p=0}^{\infty}\sum\int_C \left\langle \xi_i\,|\,L_\sigma(\iota(B^{\mu_1})\cdots\iota(B^{\mu_p}))|\,\xi_j\right\rangle dx_{\mu_1}\dots\, dx_{\mu_p}\\ &= \langle \xi_i\,|\,\sum_{p=0}^{\infty}\sum\int_C L_\sigma(\iota(B^{\mu_1})\cdots\iota(B^{\mu_p}))\,dx_{\mu_1}\dots dx_{\mu_p}\,|\,\xi_j\rangle.\end{aligned} \tag{78}$$

Since σ and $\{\xi_k\}$ are arbitrary we conclude that

$$\sum_{p=0}^{\infty}\sum\int_C B^{\mu_1}\cdots B^{\mu_p}\,dx_{\mu_1}\dots\, dx_{\mu_p}\in G. \tag{79}$$

This is exactly the formula for computing the *holonomy* along C: namely, that element in the structure group of the bundle that effects the parallel transport of fibres along the path. (Note that when pulled back appropriately, or when $\mathcal{M}$ is Euclidean space, the iterated integral amounts to an ordinary integration over a simplex of the form $\{(x_{k_1}, \ldots, x_{k_p}) : a \leq x_{k_1} \leq \ldots \leq x_{k_p} \leq b\}$).

By remarkable results of Chen (cf. Tavares (1994)) it is the case that a sufficiently nice curve C is uniquely determined by the family of iterated integrals over it up to a reasonable notion of equivalence of curves. Moreover, when curves are regarded in this way as elements of $\mathrm{Hom}_{\mathrm{Alg}}(T(X_\mu), \mathbb{C})$ (with the shuffle product on $T(X_\mu)$) the operation of composition of curves corresponds exactly to the semigroup product on $\mathrm{Hom}_{\mathrm{Alg}}(T(X_\mu), \mathbb{C})$ described earlier.

Thus, denoting by $\mathbf{P}\mathcal{M}$ the set of paths in $\mathcal{M}$, the embedding

$$\mathbf{P}\mathcal{M} \to T(X^\mu)^*$$

given above preserves the respective semigroup structures: this is a direct generalization of the procedure described in Section 1 (and Selesnick (2003a)) for the case of a one-parameter set of terms.

As before, executing sequences of cuts yields compositions of holonomies which preserve the order of execution. In particular, let us consider the case in which a short line segment C is given by

$$f(s) = (f_{\mu_1}(s), \ldots, f_{\mu_n}(s)), \text{ where } f_{\mu_k}(s) = s\Delta x_{\mu_k}, \ s \in [0, 1]. \tag{80}$$

Then

$$\int_C B^{\mu_1} \cdots B^{\mu_p}\, dx_{\mu_1} \ldots dx_{\mu_p} = \frac{1}{p!} B^{\mu_1} \cdots B^{\mu_p} \Delta x_{\mu_1} \ldots \Delta x_{\mu_p} \tag{81}$$

so that

$$\sum_{p=0}^{\infty} \sum \int_C B^{\mu_1} \cdots B^{\mu_p}\, dx_{\mu_1} \ldots dx_{\mu_p} = \exp\left(B^\mu \Delta x_\mu\right), \tag{82}$$

invoking the Einstein summation convention on the right. By approximating any curve by similar short line segments, and setting $B^\mu \equiv -iA^\mu$, we obtain sequences of holonomic computations arising from cuts exactly as before: the induced ordering is now called *path*-ordering.

In this way, holonomic quantum computations induced by driving a system along paths in some manifold of parameters may be effected. It is indeed remarkable that this paradigm seems actually to be physically implementable, though the details, both physical and mathematical, are exceedingly subtle. (Cf. for instance Wu *et al.* (2005).)

We will return to this topic in a sequel.

ACKNOWLEDGMENTS

Grateful thanks are owed to Nadine Castro, Michael Frank and Ivan Selesnick for invaluable help in the preparation of this paper.

REFERENCES

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

Frank, M. P. (2005). On the interpretation of energy as the rate of quantum computation. *Quantum Information Processing* **4**(4), 283.

Mac Lane, S. (1963). *Homology*, Springer–Verlag, Berlin, Heidelberg, New York.

Mallios, A. (2006). *Modern Differential Geometry in Gauge Theories*, Vol. 1, Birkhäuser, Boston, Basel, Berlin.

Mawhinney, R. C. and Schreckenbach, G. (2004). NMR quantum computing: applying theoretical methods to designing enhanced systems. *Magnetic Resonance in Chemistry* **42**, S88.

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

Ree, R. (1958). Lie elements and an algebra associated with shuffles. *Annals of Mathematics* **68**(2), 210.

Selesnick, S. A. (1983). Second quantization, projective modules and local gauge invariance, *International Journal of Theoretical Physics* **22**(1), 29.

Selesnick, S. A. (2003a). Foundation for Quantum Computing, *International Journal of Theoretical Physics* **42**(3), 383.

Selesnick, S. A. (2003b). *Quanta, Logic and Spacetime*, Second Edn., World Scientific Publishing, Singapore, London and Hong Kong.

Tavares, J. N. (1994). Chen integrals, generalized loops and loop calculus, *International Journal of Modern Physics A* **9**(26), 4511.

Toffoli, T. (1999). Action, or the fungibility of computation. In Hey, A. J. G. (Ed.), *Feynman and Computation*, Perseus Books Publishing, Cambridge.

Wu, L.-A., Zanardi P., and Lidar D. (2005). Holonomic computation in decoherence-free subspaces, *Physical Review Letters* **95**, 130501.