International Journal of Theoretical Physics, Vol. 43, No. 6, June 2004 (© 2004)

Computational Logic on Fock Space

S. Gudder[1]

Received

Fock space may provide an important mathematical model for quantum computation. For this reason, it may be useful to generalize previous work on computational logic to the Fock space framework. The basic construction of this computational logic is the set $\mathcal{D}(H)$ of density operators on a Fock space H. We first define n-sector $p_n(\rho)$ and total probabilities $p(\rho)$ of elements $\rho \in \mathcal{D}(H)$. We next discuss NOT, AND, and OR operations on $\mathcal{D}(H)$. Natural equivalence classes and Scotian elements are described. We also discuss minimal and maximal elements and quantum numbers for the equivalence classes. We finally treat the operation $\sqrt{\text{NOT}}$ and the stronger equivalence classes associated with this operation.

KEY WORDS: computational logic; Fock space; quantum gates; quantum computation.

1. INTRODUCTION

There are two main mathematical models for quantum computation, the quantum gate model and the quantum Turing machine model. In the quantum gate model one takes a Hilbert space $\mathcal{H}$ of sufficiently large finite dimension for a desired accuracy and represents quantum gates by unitary operators on $\mathcal{H}$. In this framework the basic computational structure is a two-level quantum system called a *qubit* (Nielsen and Chuang, 2000; Pittenger, 2001). The pure states of a qubit are represented by unit vectors in the two-dimensional Hilbert space $\mathbb{C}^2$. The Hilbert space $\mathcal{H}$ usually has the form $\mathcal{H} = \mathbb{C}^{2^n}$ which is the state space for an n-qubit system. In this case we have n qubits and the Hilbert space is the n-fold tensor product

$$\mathcal{H} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \otimes^n \mathbb{C}^2$$

We now briefly comment on the quantum Turing machine model (Nielsen and Chuang (2000). The simplest machine language for any computer consists of words constructed from a binary alphabet $A = \{0, 1\}$. We identify the letters of A

[1] Department of Mathematics, University of Denver, Denver, Colorado 80208; e-mail: sgudder@math.du.edu.

0020-7748/04/0600-1409/0 © 2004 Springer Science+Business Media, Inc.

with an orthonormal basis $|0\rangle$, $|1\rangle$ for $\mathbb{C}^2$. Let

$$\mathcal{K} = \mathbb{C} \oplus \mathbb{C}^2 \oplus \otimes^2\mathbb{C}^2 \oplus \otimes^3\mathbb{C}^2 \oplus \cdots \oplus \otimes^n\mathbb{C}^2 \oplus \cdots$$

be the tensor algebra over $\mathbb{C}^2$. Of course, $\mathcal{K}$ corresponds to a full Fock space in quantum field theory. There is a bijection between the set of words over A and an orthonormal basis of $\mathcal{K}$. Indeed we identify $1 \in \mathbb{C}$ with the empty word and if $w = x_1x_2\cdots x_n$ is a word over A of length n, we identify w with the basis element

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle, \quad x_i \in A,\ i = 1, \ldots, n$$

Of course, there is a lot more to a quantum Turing machine than this set of words. However, it is not our purpose to give a full discussion of quantum Turing machines here. We merely want to point out the importance of the computational space $\mathcal{K}$ as a motivation for our studies.

Previous studies (Cattaneo *et al.*, 2002; Cattaneo *et al.*, preprint; Dalla Chiara, 2002; Gudder, 2003) of quantum computational logic have taken place in the Hilbert space $\mathcal{H} = \otimes^n\mathbb{C}^2$. More precisely, the dimension of $\mathcal{H}$ has been left unspecified so technically the relevant space is $\cup_{n=1}^{\infty} \otimes^n \mathbb{C}^2$ which is not a Hilbert space. Our present work discusses a quantum computational logic over the space

$$H = \mathbb{C}^2 \oplus \otimes^2\mathbb{C}^2 \oplus \otimes^3\mathbb{C}^2 \oplus \cdots \oplus \otimes^n\mathbb{C}^2 \oplus \cdots$$

which is the full Fock space except for the vacuum for which we do not seem to have a use. There are several advantages to working on H. As we mentioned earlier except for the empty word, H is a Hilbert space that is important for the description of quantum machines. Moreover, if relativistic effects become important in the operation of quantum computers then quantum field theory will be an essential ingredient for their description. In this case, a Fock space framework will be necessary. For our present discussions the full Fock space is employed so we are assuming that individual qubits are distinguishable. Until now almost all investigations in quantum computation and quantum information have assumed distinguishability. This is because the qubits are far enough apart so that their wave functions have essentially nonoverlapping support or the qubits have definite locations so they can be distinguished. However, it is likely as more sophisticated quantum computers are constructed and studied that this assumption will no longer be valid. Thus, later studies may involve symmetric or antisymmetric Fock spaces. In fact, research on Fermionic and Bosonic quantum computation has already begun (Bravyi and Kitaev, 2002; Eckert *et al.*, 2002).

Another advantage of our present approach is that the states appear in the same Hilbert space so they can be combined naturally whereas in previous work the states could be in different Hilbert spaces. For example, we can have mixtures of states or superpositions of pure states involving different numbers of qubits. Finally, from a mathematical point of view, the resulting computational logic has a more complex and interesting structure. We refer the reader to the abstract for a summary of the contents of this paper.

2. PROBABILITIES OF STATES

In the theory of quantum computation, a *qubit* is a two-dimensional quantum system. A pure qubit state is represented by a unit vector $|\psi\rangle$ in the Hilbert space $\mathbb{C}^2$. Denoting the standard orthonormal basis for $\mathbb{C}^2$ by $|0\rangle = (1, 0)$, $|1\rangle = (0, 1)$, we call $\{|0\rangle, |1\rangle\}$ the *computational basis* for the qubit. We can then write $|\psi\rangle = a|0\rangle + b|1\rangle$ where $a, b \in \mathbb{C}$ with $|a|^2 + |b|^2 = 1$. For a positive integer n, an n-qubit is a quantum system consisting of n distinguishable qubits. In this case, the pure states are represented by unit vectors in $\otimes^n\mathbb{C}^2 = \mathbb{C}^{2^n}$. The 2^n unit vectors of the form $|i_1\rangle \otimes \cdots \otimes |i_n\rangle$, $i_j \in \{0, 1\}$, $j = 1, \ldots, n$ give the computational basis for an n-qubit. It is standard practice to use the notation

$$|i_1 i_2 \cdots i_n\rangle = |i_1\rangle|i_2\rangle \cdots |i_n\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$$

An arbitrary pure n-qubit state $|\psi\rangle \in \mathbb{C}^{2^n}$, $\|\psi\| = 1$ has the form

$$|\psi\rangle = \sum a_{i_1 \cdots i_n} |i_1 \cdots i_n\rangle \tag{2.1}$$

where $a_{i_1 \cdots i_n} \in \mathbb{C}$ with $\sum |a_{i_1 \cdots i_n}|^2 = 1$, $i_j \in \{0, 1\}$, $j = 1, \ldots, n$.

Employing (2.1) we can write

$$\begin{aligned} |\psi\rangle &= \sum a_{i_1 \cdots i_{n-1} 0} |i_1 \cdots i_{n-1} 0\rangle + \sum a_{i_1 \cdots i_{n-1} 1} |i_1 \cdots i_{n-1} 1\rangle \\ &= |\psi_0\rangle + |\psi_1\rangle = \left|\widetilde{\psi}_0\right\rangle|0\rangle + \left|\widetilde{\psi}_1\right\rangle|1\rangle \end{aligned}$$

where $|\psi_1\rangle \perp |\psi_1\rangle$ and $\|\psi_1\|^2 + \|\psi_1\|^2 = 1$, and $\|\widetilde{\psi}_0\| = \|\psi_0\|$, $\|\widetilde{\psi}_1\| = \|\psi_1\|$. We call $|\psi_0\rangle$ a 0-vector and $|\psi_1\rangle$ a 1-vector. Thus any pure n-qubit state has a unique representation as the sum of a 0-vector and a 1-vector in the computational basis. We think of a 0-vector as having truth value "false" and a 1-vector as having truth value "true."

We now form the full Fock space (except for the vacuum)

$$\begin{aligned} H &= \mathbb{C}^2 \oplus \otimes^2\mathbb{C}^2 \oplus \otimes^3\mathbb{C}^2 \oplus \cdots \oplus \otimes^n\mathbb{C}^2 \oplus \cdots \\ &= \mathbb{C}^2 \oplus \mathbb{C}^{2^2} \oplus \mathbb{C}^{2^3} \oplus \cdots \oplus \mathbb{C}^{2^n} \oplus \cdots \end{aligned}$$

We call $\otimes^n\mathbb{C}^2$ the n-sector in the Hilbert space H. The n-sector projection is the orthogonal projection $P^{(n)} \colon H \to \otimes^n\mathbb{C}^2$ $n = 1, 2, \ldots$. Letting $P_0^{(n)}$ be the orthogonal projection onto the span of the 0-vectors in $\otimes^n\mathbb{C}^2$ and $P_1^{(n)}$ the orthogonal projection onto the span of the 1-vectors in $\otimes^n\mathbb{C}^2$, we have that

$$P_0^{(n)} + P_1^{(n)} = P^{(n)} \quad n = 1, 2, \ldots$$

Letting P_1 be the orthogonal projections onto the span of the i-vectors, $i = 0, 1$, we have that $P_0 = \sum P_0^{(n)}$ and $P_1 = \sum P_1^{(n)}$.

Let $\mathcal{D}(H)$ be the set of all density operators on H. Then $\mathcal{D}(H)$ is a σ-convex set in the sense that if $\rho_i \in \mathcal{D}(H)$ and $\lambda_i \geq 0$ with $\sum \lambda_i = 1$, then $\sum \lambda_i \rho_i \in \mathcal{D}(H)$. The extreme points of $\mathcal{D}(H)$ are the one-dimensional projections $P_\psi = |\psi\rangle\langle\psi|$ onto the span of a unit vector $|\psi\rangle$ which we identify with a pure state $|\psi\rangle$. For $\rho \in \mathcal{D}(H)$ define $\rho_n = P^{(n)}\rho P^{(n)}$. Then ρ_n is a positive trace class operator and

$$\sum \mathrm{tr}(\rho_n) = \sum \mathrm{tr}\big(P^{(n)}\rho\big) = \mathrm{tr}\left(\sum P^{(n)}\rho\right) = \mathrm{tr}(\rho) = 1 \qquad (2.2)$$

For $\rho \in \mathcal{D}(H)$ we define the probability of the n-sector in the state ρ to be $p_\rho(n) = \mathrm{tr}(\rho_n)$, $n = 1, 2, \ldots$. Applying (2.2) we have that $\sum p_\rho(n) = 1$. We define the n-sector probability of ρ to be

$$p_n(\rho) = \mathrm{tr}\big(P_1^{(n)}\rho_n\big) = \mathrm{tr}\big(P_1^{(n)}\rho\big) \quad n = 1, 2, \ldots$$

and the probability of ρ to be

$$p(\rho) = \sum p_n(\rho) = \mathrm{tr}(P_1\rho)$$

Of course, $p_n(\rho) \leq p_\rho(n)$ and $0 \leq p(\rho) \leq 1$. Notice that $p_n(\rho) = p_\rho(n)$ is equivalent to $P_1^{(n)}\rho P_1^{(n)} = \rho_n$ which is equivalent to $P_0^{(n)}\rho P_0^{(n)} = 0$. We define the n-sector conditional probability of ρ to be

$$p(\rho \mid n) = \begin{cases} p_n(\rho)p_\rho(n) & \text{if } p_\rho(n) \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

We then have that $p_n(\rho) = p_\rho(n)p(\rho \mid n)$ and

$$p(\rho) = \sum_n p_\rho(n)p(\rho \mid n)$$

If $\rho^{(i)} \in \mathcal{D}(H)$ and $\lambda_i \geq 0$ with $\sum \lambda_i = 1$, then

$$p\left(\sum \lambda_i \rho^{(i)}\right) = \mathrm{tr}\left(P_1 \sum \lambda_i \rho^{(i)}\right) = \sum \lambda_i \mathrm{tr}\big(P_1\rho^{(i)}\big) = \sum \lambda_i p\big(\rho^{(i)}\big)$$

Hence, p preserves convex combinations. In a similar way, p_n preserves convex combinations, $n = 1, 2, \ldots$. Moreover, letting $\rho = \sum \lambda_i \rho^{(i)}$ we have that

$$\begin{aligned} p_\rho(n) &= \mathrm{tr}\big(P^{(n)}\rho\big) = \mathrm{tr}\left(P^{(n)} \sum \lambda_i \rho^{(i)}\right) = \sum \lambda_i \mathrm{tr}\big(P^{(n)}\rho^{(i)}\big) \\ &= \sum \lambda_i p_{\rho^{(i)}}(n) \end{aligned}$$

We denote the identity matrix on $\otimes^n \mathbb{C}^2$ by I_n. Let X be the Pauli matrix

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

and define the unitary matrix N_n on $\otimes^n \mathbb{C}^2$ by $N_n = I_{n-1} \otimes X, n = 1, 2, \ldots$. Define the unitary operator N on H by

$$N = P^{(1)} N_1 P^{(1)} + P^{(2)} N_2 P^{(2)} + \cdots = N_1 \oplus N_2 \oplus \cdots$$

and for $\rho \in \mathcal{D}(H)$ define $\mathrm{NOT}\rho \in \mathcal{D}(H)$ by $\mathrm{NOT}\rho = N\rho N$. Since $N^2 = I$ we have that $\mathrm{NOT}(\mathrm{NOT}\rho) = \rho$. Since

$$N P_1^{(n)} N = N_n P_1^{(n)} N_n = P_0^{(n)}$$

we have that

$$\begin{aligned} p_n(\mathrm{NOT}\rho) &= \mathrm{tr}\big(P_1^{(n)} \mathrm{NOT}\rho\big) = \mathrm{tr}\big(P_1^{(n)} N\rho N\big) = \mathrm{tr}\big(P_0^{(n)} \rho\big) \\ &= \mathrm{tr}\left(P^{(n)} \rho\right) - \mathrm{tr}\big(P_1^{(n)} \rho\big) = p_\rho(n) - p_n(\rho) \end{aligned} \tag{2.3}$$

Applying (2.3) gives

$$p(\mathrm{NOT}\rho) = \sum p_n(\mathrm{NOT}\rho) = \sum p_\rho(n) - \sum p_n(\rho) = 1 - p(\rho)$$

which is what we would expect. Moreover, if $p_\rho(n) \neq 0$ then (2.3) gives

$$p(\mathrm{NOT}\rho \mid n) = \frac{p_n(\mathrm{NOT}\rho)}{p_\rho(n)} = 1 - \frac{p_n(\rho)}{p_\rho(n)} = 1 - p(\rho \mid n)$$

Notice that $\mathrm{NOT}\rho$ and ρ give the same n-sector probabilities. This is because $P^{(n)} N = N P^{(n)}$ implies that

$$\begin{aligned} p_{\mathrm{NOT}\rho}(n) &= \mathrm{tr}\big(P^{(n)} \mathrm{NOT}\rho\big) = \mathrm{tr}\big(P^{(n)} N\rho N\big) = \mathrm{tr}\big(P^{(n)} N^2 \rho\big) \\ &= \mathrm{tr}(P^n \rho) = p_\rho(n) \end{aligned}$$

Finally, it is clear that NOT preserves convex combinations.

The quantum Toffoli gate $T^{(m,n,1)} : \mathbb{C}^{2^{m+n+1}} \to \mathbb{C}^{2^{m+n+1}}$ is the unitary operator given by Cattaneo *et al.* (2002, preprint)

$$T^{m,n,1} : |i_1 \cdots i_m j_1 \cdots j_n k\rangle = |i_1 \cdots i_m j_1 \cdots j_n\rangle |i_m \cdot j_n + k \pmod 2\rangle$$

For $\rho, \sigma \in \mathcal{D}(H)$ define the positive linear operator $\mathrm{AND}(\rho, \sigma)_n : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ by

$$\mathrm{AND}(\rho, \sigma)_n = \sum_{\substack{i,j \\ i+j+1=n}} T^{(i,j,1)} \rho_i \otimes \sigma_j \otimes |0\rangle\langle 0| T^{(i,j,1)}$$

Defining

$$\mathrm{AND}(\rho, \sigma) = \mathrm{AND}(\rho, \sigma)_3 \oplus \mathrm{AND}(\rho, \sigma)_4 \oplus \cdots$$

we have

$$\mathrm{tr}\,(\mathrm{AND}(\rho, \sigma)) = \sum_n \sum_{\substack{i,j \\ i+j+1=n}} \mathrm{tr}(\rho_i) \mathrm{tr}(\sigma_j) = \sum_{i,j} \mathrm{tr}(\rho_i)\, \mathrm{tr}(\sigma_j) = 1$$

so that AND$(\rho, \sigma) \in \mathcal{D}(H)$. It is easy to check that AND preserves joint convex combinations in both arguments. It follows from Gudder (2003) that

$$p_n\left(\text{AND}(\rho,\sigma)\right) = \text{tr}\left(P_1^{(n)}\text{AND}(\rho,\sigma)\right) = \sum_{\substack{i,j \\ i+j+1=n}} \text{tr}\left(P_1^{(i)}\rho\right)\text{tr}\left(P_1^{(j)}\sigma\right)$$

$$= \sum_{\substack{i,j \\ i+j+1=n}} p_i(\rho)p_j(\sigma) \tag{2.4}$$

Applying (2.4) we have that

$$p\left(\text{AND}(\rho,\sigma)\right) = \sum_n \sum_{\substack{i,j \\ i+j+1=n}} p_i(\rho)p_j(\sigma) = \sum_i p_i(\rho)\sum_j p_j(\sigma) = p(\rho)p(\sigma)$$

Defining OR(ρ, σ) = NOT (AND(NOTρ, NOTσ)) we have that

$$p\left(\text{OR}(\rho,\sigma)\right) = p(\rho) + p(\sigma) - p(\rho)p(\sigma)$$

Analogous to (2.4) it follows directly that for $\delta = \text{AND}(\rho, \sigma)$ we have

$$p_\delta(n) = \sum_{\substack{i,j \\ i+j+1=n}} p_\rho(i)p_\sigma(j)$$

3. EQUIVALENCE CLASSES OF STATES

For $\rho, \sigma \in \mathcal{D}(H)$ write $\rho \models \sigma$ if $p(\rho) \leq p(\sigma)$. Then $\models$ is a reflexive, transitive relation. We write $\rho \simeq \sigma$ if $p(\rho) = p(\sigma)$. Then $\simeq$ is an equivalence relation with equivalence classes denoted by $[\rho]_0$. Defining $[\rho]_0 \models [\sigma]_0$ if $\rho \models \sigma$, $\models$ becomes a partial order relation on the set of equivalence classes

$$L_0 = \{[\rho]_0 : \rho \in \mathcal{D}(H)\} = \mathcal{D}(H)/\simeq$$

However, $\models$ is a very weak order and it is not very interesting because it is a total order. In fact, L_0 is isomorphic to $[0, 1] \subseteq \mathbb{R}$ in a natural way Gudder (2003). We now define a more interesting order.

For $\rho, \sigma \in \mathcal{D}(H)$ define $\rho \leq \sigma$ if for $n = 1, 2, \ldots$ we have that

$$\text{tr}\left(P_1^{(n)}\rho\right) \leq \text{tr}\left(P_1^{(n)}\sigma\right) \tag{3.1}$$

$$\text{tr}\left(P_0^{(n)}\rho\right) \geq \text{tr}\left(P_0^{(n)}\sigma\right) \tag{3.2}$$

We can write (3.1) and (3.2) as $p_n(\rho) \leq p_n(\sigma)$ and

$$p_\rho(n) - p_n(\rho) \geq p_\sigma(n) - p_n(\sigma)$$

Notice that the second inequality is equivalent to $p_n(\text{NOT}\rho) \geq p_n(\text{NOT}\sigma)$. Again $\leq$ is reflexive and transitive and we write $\rho \sim \sigma$ if $\rho \leq \sigma$ and $\sigma \leq \rho$. Notice that

$\rho \sim \sigma$ if and only if $p_\rho(n) = p_\sigma(n)$ and $p_n(\rho) = p_n(\sigma)$ for $n = 1, 2, \ldots$. Then $\sim$ is an equivalence relation and we denote equivalence classes by $[\rho]_1$. Defining $[\rho]_1 \le [\sigma]_1$ if $\rho \le \sigma$, $\le$ becomes a partial order relation on the set of equivalence classes

$$L_1 = \{[\rho]_1 : \rho \in \mathcal{D}(h)\} = \mathcal{D}(H)/\sim$$

Theorem 3.1. (i) *If* $\rho \le \sigma$ *then* $\mathrm{NOT}\rho \le \mathrm{NOT}\sigma$. (ii) *If* $\rho \sim \sigma$ *then* $\mathrm{NOT}\rho \sim \mathrm{NOT}\sigma$. (iii) *If* $\rho \sim \rho'$ *and* $\sigma \sim \sigma'$ *then* $\mathrm{AND}\,(\rho, \sigma) \sim \mathrm{AND}\,(\rho', \sigma')$

Proof: (i) Assume that $\rho \le \sigma$. Applying (2.3) and (3.1) gives

$$\begin{aligned} p_{\mathrm{NOT}\sigma}(n) - p_n(\mathrm{NOT}\sigma) &= p_\sigma(n) - p_\sigma(n) + p_n(\sigma) = p_n(\sigma) \ge p_n(\rho) \\ &= p_{\mathrm{NOT}}(\rho) - p_n(\mathrm{NOT}\rho) \end{aligned}$$

Hence, $\mathrm{NOT}\sigma \le \mathrm{NOT}\rho$. (ii) This follows from (i). (iii) Assuming $\rho \sim \rho'$ and $\sigma \sim \sigma'$ we have by (2.4) that

$$\begin{aligned} p_n(\mathrm{AND}(\rho, \sigma)) &= \sum_{\substack{i,j \\ i+j+1=n}} p_i(\rho) p_j(\sigma) = \sum_{\substack{i,j \\ i+j+1=n}} p_i(\rho') p_j(\sigma') \\ &= p_n(\mathrm{AND}(\rho', \sigma')) \end{aligned}$$

Moreover, letting $\delta = \mathrm{AND}(\rho, \sigma)$ and $\delta' = \mathrm{AND}(\rho', \sigma')$ we have that

$$\begin{aligned} p_\delta(n) &= \mathrm{tr}\left(P^{(n)} \mathrm{AND}(\rho, \sigma)\right) = \sum_{\substack{i,j \\ i+j+1=n}} \mathrm{tr}(\rho_i)\mathrm{tr}(\sigma_j) = \sum_{\substack{i,j \\ i+j+1=n}} p_\rho(i) p_\sigma(j) \\ &= \sum_{\substack{i,j \\ i+j+1=n}} p_{\rho'}(i) p_{\sigma'}(j) = p_{\delta'}(n) \end{aligned}$$

It follows that $\mathrm{AND}(\rho, \sigma) \sim \mathrm{AND}(\rho', \sigma')$. □

Applying Theorem 3.1 (ii), $\mathrm{NOT}[\rho]_1 = [\mathrm{NOT}\rho]_1$ is well defined. Moreover, $\mathrm{NOT}\,(\mathrm{NOT}[\rho]_1) = [\rho]_1$ and $[\rho]_1 \le [\sigma]_1$ implies $\mathrm{NOT}[\sigma]_1 \le \mathrm{NOT}[\rho]_1$. Applying Theorem 3.1 (iii), $\mathrm{AND}\,([\rho]_1, [\sigma]_1) = [\mathrm{AND}(\rho, \sigma)]_1$ is well defined and so is $\mathrm{OR}\,([\rho]_1, [\sigma]_1) = [\mathrm{OR}(\rho, \sigma)]_1$. Let $p^{(n)}$, $n = 1, 2, \ldots$, be defined by $\rho^{(n)} = P_1^{(n)}/2^{n-1}$. Then $p_n(\rho^{(n)}) = 1$ and $p_j(\rho^{(n)}) = 0$, $j \ne n$. Since $[p^{(n)}]_1, n = 1, 2, \ldots$, are maximal unrelated elements of L_1, there is no largest element of L_1. In a similar way there is no smallest element of L_1. Hence, L_1 is an unbounded involution poset.

For $0 \le \lambda \le 1$ define

$$\rho_n(\lambda) = \frac{1-\lambda}{2^{n-1}} P_0^{(n)} + \frac{\lambda}{2^{n-1}} P_1^{(n)} \in \mathcal{D}(H), \quad n = 1, 2, \ldots$$

For $\alpha_i \geq 0$ with $\sum \alpha_i = 1$ and $0 \leq \lambda_i \leq 1$ with $\lambda_i = 0$ whenever $\alpha_i = 0$, $i = 1, 2, \ldots$, define $\rho(\{\alpha_i\}, \{\lambda_i\})$ by

$$\rho(\{\alpha_i\}, \{\lambda_i\}) = \alpha_1\rho_1(\lambda_1) \oplus \alpha_2\rho_2(\lambda_2) \oplus \cdots$$

Then $\rho(\{\alpha_i\}, \{\lambda_i\})_n = \alpha_n\rho_n(\lambda_n)$, $n = 1, 2, \ldots$, and we have that

$$p_{\rho(\{\alpha_i\},\{\lambda_i\})}(n) = \alpha_n \tag{3.3}$$

$$p_n(\rho(\{\alpha_i\}, \{\lambda_i\})) = \lambda_n\alpha_n \tag{3.4}$$

For an arbitrary $\rho \in \mathcal{D}(H)$ choose $\alpha_n = p_\rho(n)$ and $\lambda_n\alpha_n = p_n(\rho)$, $n = 1, 2, \ldots$. It follows from (3.3) and (3.4) that $\rho \sim \rho(\{\alpha_i\}, \{\lambda_i\})$. Moreover, the corresponding $[\rho]_1 \mapsto \rho(\{\alpha_i\}, \{\lambda_i\})$ is bijective and preserves the logical operations. In this way, each $\rho(\{\alpha_i\}, \{\lambda_i\})$ gives a unique representation of its equivalence class. We call $(\{\alpha_i\}, \{\lambda_i\})$ the quantum numbers for the corresponding equivalence class. For example, the quantum numbers for $[\rho^{(n)}]_1$ are $\alpha_n = \lambda_n = 1, \alpha_i = \lambda_i = 0$ for $i \neq n$. We now characterize minimal and maximal elements of L_1. Not that $[\rho]_1$ is minimal if and only if NOT$[\rho]_1$ is maximal.

Theorem 3.2. (i) $[\rho]_1$ *is minimal in* L_1 *if and only if*

$$\rho \sim \sum \frac{\alpha_i}{2^{i-1}} P_0^{(i)}, \quad \alpha \geq 0, \quad \sum \alpha_i = 1$$

(ii) $[\rho]_1$ *is maximal in* L_1 *if and only if*

$$\rho \sim \sum \frac{\alpha_i}{2^{i-1}} P_1^{(i)}, \quad \alpha_i \geq 0, \quad \sum \alpha_i = 1$$

Proof: (i) Assume that $\rho = \sum(\alpha_i/2^{i-1})P_0^{(i)}$. If $\rho_1 \leq \rho$ then

$$\operatorname{tr}\left(P_1^{(n)}\rho_1\right) \leq \operatorname{tr}\left(P_1^{(n)}\rho\right) = 0$$

so that $p_n(\rho_1) = p_n(\rho)$ for all n. Also,

$$\operatorname{tr}\left(P_0^{(n)}\rho_1\right) \geq \operatorname{tr}\left(P_0^{(n)}\rho\right) = \alpha_n, \quad n = 1, 2, \ldots$$

Hence,

$$1 = \sum \alpha_n \leq \sum \operatorname{tr}\left(P_0^{(n)}\rho_1\right) = \operatorname{tr}(P_0\rho_1) \leq 1$$

It follows that

$$\operatorname{tr}\left(P_0^{(n)}\rho_1\right) = \alpha_n = \operatorname{tr}\left(P_0^{(n)}\rho\right)$$

Therefore, $\rho_1 \sim \rho$ and $[\rho]_1$ is minimal in L_1. Conversely, assume that $[\rho]_1$ is minimal and let $\rho \sim \rho(\{\alpha_i\}, \{\lambda_i\})$. Suppose that $\alpha_m\lambda_m \neq 0$ and let $\rho_1 = \rho(\{\alpha_i\}, \{\lambda_i/2\})$. Then

$$p_n(\rho_1) = \frac{\lambda_n}{2}\alpha_n \leq \lambda_n\alpha_n = p_n(\rho), \quad n = 1, 2, \ldots$$

Moreover,

$$p_{\rho_1}(n) - p_n(\rho_1) = \alpha_n - \frac{\lambda_n}{2}\alpha_n \geq \alpha_n - \lambda_n\alpha_n = p_\rho(n) - p_n(\rho), \quad n = 1, 2, \ldots$$

and $p_m(\rho_1) < p_m(\rho)$. Hence, $\rho_1 \leq \rho$ and $\rho_1 \not\sim \rho$ which is a contradiction. Therefore, $\alpha_m\lambda_m = 0$ for every $m = 1, 2, \ldots$. Without loss of generality, we can assume that $\lambda_n = 0, n = 1, 2, \ldots$. Thus, ρ has the form $\rho = \sum(\alpha_i/2^{i-1})P_0^{(i)}$ where $\alpha \geq 0$, $\sum \alpha_i = 1$. (ii) This follows from (i) because $[\rho]_1$ is maximal if and only if NOT$[\rho]_1$ is minimal. □

Applying Theorem 3.2 we see that $[\rho]_1$ is minimal if and only if its quantum numbers satisfy $\lambda_i = 0$ for all i and $[\rho]_1$ is maximal if and only if its quantum numbers satisfy $\lambda_i = 1$ whenever $\alpha_i \neq 0$.

We say that $\rho \in \mathcal{D}(H)$ is sector down Scotian if $P_0^{(n)}/2^{n-1} \leq \rho$ for some n, ρ is sector up Scotian if $\rho \leq P_1^{(n)}/2^{n-1}$ for some n and ρ is sector Scotian if for some n

$$\frac{P_0^{(n)}}{2^{n-1}} \leq \rho \leq \frac{P_1^{(n)}}{2^{n-1}}$$

Theorem 3.3. (i) *ρ is sector up Scotian if and only if $p(\rho) = p_n(\rho)$ for some n.* (ii) *ρ is sector down Scotian if and only if $p(\rho) = 1 - p_\rho(n) + p_n(\rho)$ for some n or equivalently $p(\text{NOT}\rho) = p_n(\text{NOT}\rho)$ for some n.* (iii) *ρ is sector Scotian if and only if $p_\rho(n) = 1$ for some n.*

Proof: (i) The condition $\rho \leq P_1^{(n)}/2^{n-1}$ is equivalent to

$$\text{tr}\big(P_1^{(m)}\rho\big) \leq \text{tr}\left(P_1^{(m)}\frac{P_1^{(n)}}{2^{n-1}}\right), \quad m = 1, 2, \ldots \tag{3.5}$$

Now (3.5) is equivalent to $p_m(\rho) = 0$ for $m \neq n$ which is equivalent to $p(\rho) = p_n(\rho)$. (ii) Notice that ρ is sector down Scotian if and only if NOTρ is sector up Scotian. By Part (i) and (2.3) this is equivalent to

$$1 - p(\rho) = p_\rho(n) - p_n(\rho)$$

which gives the desired condition. (iii) If ρ is Scotian then by Parts (i) and (ii) we have that $p_\rho(n) = 1$. Conversely, if $p_\rho(n) = 1$ then $\rho = P^{(n)}\rho P^{(n)}$ so that $p(\rho) = p_n(\rho)$. Applying Parts (i) and (ii) shows that ρ is Scotian. □

If $[\rho]_1$ has quantum numbers $(\{\alpha_i\}, \{\lambda_i\})$ we see that NOT$[\rho]_1$ has quantum numbers $(\{\alpha_i\}, \{\alpha_i(1 - \lambda_i)\})$. Applying Theorem 3.1 (i) we see that ρ is sector up Scotian if and only if there is an n such that the corresponding quantum numbers $\lambda_m = 0$ for $m \neq n$. It follows that ρ is sector down Scotian if and only if there is an n such that the corresponding quantum numbers $\lambda_m = 1$ whenever $\alpha_m \neq 0$ for $m \neq n$. Finally, ρ is sector Scotian if and only if $\alpha_n = 1$ for some n.

We have considered the concept of Scotian relative to a very specific type of minimal or maximal element. We now give a more general definition. We say that ρ is down Scotian relative to the minimal element σ if $\sigma \leq \rho$, ρ is up Scotian relative to the maximal element σ if $\rho \leq \sigma$, ρ is Scotian relative to the minimal element σ if $\sigma \leq \rho \leq \text{NOT}\sigma$.

Theorem 3.4. (i) *ρ is up Scotian relative to σ if and only if $p_n(\rho) \leq p_\sigma(n)$ for all n.* (ii) *ρ is down Scotian relative to σ if and only if for all n we have that*

$$p_n(\text{NOT}\rho) = p_\rho(n) - p_n(\rho) \leq p_\sigma(n)$$

(iii) *ρ is Scotian relative to σ if and only if for n we have that*

$$p_\rho(n) - p_\sigma(n) \leq p_n(\rho) \leq p_\sigma(n)$$

Proof: (i) If $\rho \leq \sigma$ then for all n we have that

$$p_n(\rho) \leq p_n(\sigma) \leq p_\sigma(n)$$

Conversely, suppose that $p_n(\rho) \leq p_\sigma(n)$ for all n. Since σ is maximal we have that $p_\sigma(n) = p_n(\sigma)$ for all n. Hence, $p_n(\rho) \leq p_n(\sigma)$ and

$$p_\rho(n) - p_n(\rho) \leq p_\sigma(n) - p_n(\sigma)$$

for all n. Thus, $\rho \leq \sigma$. (ii) This follows from (i) and the fact that $\sigma \leq \rho$ if and only if $\text{NOT}\rho \leq \text{NOT}\sigma$. (iii) This follows from (i) and (ii). □

4. SQUARE ROOT OF NOT

Letting M be the unitary matrix given by

$$M = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$

we have that $M = \sqrt{X}$. Let $(\sqrt{N})_n$ be the unitary matrix on $\otimes^n\mathbb{C}^2$ given by $(\sqrt{N})_n = I_{n-1} \otimes M$, $n = 1, 2, \ldots$, and define the unitary operator $\sqrt{N}$ on H by

$$\begin{aligned} \sqrt{N} &= P^{(1)}(\sqrt{N})_1 P^{(1)} + P^{(2)}(\sqrt{N})_2 P^{(2)} + \cdots \\ &= (\sqrt{N})_1 \oplus (\sqrt{N})_2 \oplus \cdots \end{aligned}$$

For $\rho \in \mathcal{D}(H)$ define $\sqrt{\text{NOT}}\,\rho \in \mathcal{D}(H)$ by $\sqrt{\text{NOT}}\,\rho = \sqrt{N}^*\rho\sqrt{N}$. Then

$$\sqrt{\text{NOT}}\,(\sqrt{\text{NOT}}\,\rho) = \text{NOT}\rho$$

so we can think of $\sqrt{\text{NOT}}$ as the square root of NOT. The operator $\sqrt{\text{NOT}}$ is a quantum gate that has no classical analogue (Cattaneo *et al.*, preprint). We shall incorporate $\sqrt{\text{NOT}}$ to obtain a quantum computational logic with no classical analogue. Since $P^{(n)}\sqrt{N} = \sqrt{N}\, P^{(n)}$ we have that $p_{\sqrt{\text{NOT}}}(n) = p_\rho(n)$ for all n. Let Y be the Pauli matrix

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

and define the unitary matrix R_n on $\otimes^n \mathbb{C}^n$ given by $R_n = I_{n-1} \otimes Y, n = 1, 2, \ldots$. It is shown in Gudder (2003) that

$$p_n(\sqrt{\text{NOT}}\,\rho) = \frac{1}{2} p_\rho(n) + \frac{1}{2}\text{tr}(R_n \rho_n) \tag{4.1}$$

For $\rho, \sigma \in \mathcal{D}(H)$ define strong preorder $\rho \preceq \sigma$ by (i) $\rho \leq \sigma$ and (ii) $\sqrt{\text{NOT}}\,\sigma \leq \sqrt{\text{NOT}}\,\rho$. It is clear that $\rho \preceq \sigma$ implies that $\rho \leq \sigma$. However, simple examples show that the converse does not hold. As before $\preceq$ is reflexive and transitive and we define the strong equivalence relation $\rho \approx \sigma$ if $\rho \preceq \sigma$ and $\sigma \preceq \rho$. Of course, $\rho \approx \sigma$ if and only if $\rho \sim \sigma$ and $\sqrt{\text{NOT}}\,\rho \sim \sqrt{\text{NOT}}\,\sigma$. Hence $\rho \approx \sigma$ if and only if for all n we have that

(1) $p_\rho(n) = p_\sigma(n)$
(2) $p_n(\rho) = p_n(\sigma)$
(3) $p_n(\sqrt{\text{NOT}}\,\rho) = p_n(\sqrt{\text{NOT}}\,\sigma)$

Applying (4.1) we see that point (3) is equivalent to $\text{tr}(R_n\rho_n) = \text{tr}(R_n\sigma_n)$ for all n. Denote the $\approx$ equivalence classes by $[\rho]_2$ and let

$$L_2 = \{[\rho]_2 \colon \rho \in \mathcal{D}(H)\} = \mathcal{D}(H)/\approx$$

Defining $[\rho]_2 \leq [\sigma]_2$ if $\rho \preceq \sigma$, $\leq$ becomes a partial order relation on L_2.

Since R_n is self-adjoint and unitary we have that $-1 \leq \text{tr}(R_n\rho_n) \leq 1$ Letting $\beta_n = \text{tr}(R_n\rho_n)$ we conclude that $-1 \leq \beta_n \leq 1$ and by (4.1) we have

$$\beta_n = 2p_n(\sqrt{\text{NOT}}\,\rho) - p_\rho(n)$$

Summing over n gives $-1 \leq \sum \beta_n \leq 1$. Then each $[\rho]_2$ is determined by the quantum numbers

$$[\rho]_2 \to (\{\alpha_i\}, \{\lambda_i\}, \{\beta_i\})$$

where $\{\alpha_i\}$, $\{\lambda_i\}$ are as before and $-1 \leq \beta_i \leq 1, -1 \leq \sum \beta_i \leq 1$. We do not know whether the converse holds. That is, given such a set of quantum numbers, does there exist a $\rho \in \mathcal{D}(H)$ satisfying: $p_\rho(n) = \alpha_n$, $p_n(\rho) = \lambda_n\alpha_n$, $p_n(\sqrt{\text{NOT}}\,\rho) = \frac{1}{2}\alpha_n + \frac{1}{2}\beta_n$? Also, can we find representatives of $[\rho]_2$ analogous to $[\rho]_1 \to \rho(\{\alpha_i\}, \{\lambda_i\})$?

Theorem 4.1. (i) *If* $\rho \preceq \sigma$ *then* $\text{NOT}\sigma \preceq \text{NOT}\rho$. (ii) *If* $\rho \approx \sigma$, *then* $\text{NOT}\rho \approx \text{NOT}\sigma$ *and* $\sqrt{\text{NOT}}\,\rho \approx \sqrt{\text{NOT}}\,\sigma$. (iii) *If* $\rho \approx \rho'$ *and* $\sigma \approx \sigma'$ *then* $\text{AND}(\rho, \sigma) \approx \text{AND}(\rho', \sigma')$.

Proof: (i) Suppose that $\rho \preceq \sigma$. We then have that $\rho \leq \sigma$ so by Theorem 3.1 (i), $\text{NOT}\sigma \leq \text{NOT}\rho$. By definition $\sqrt{\text{NOT}}\,\sigma \leq \sqrt{\text{NOT}}\,\sigma$ so again by Theorem 3.1 (i)

$$\sqrt{\text{NOT}}\,\text{NOT}\rho = \text{NOT}\sqrt{\text{NOT}}\,\rho \leq \text{NOT}\sqrt{\text{NOT}}\,\sigma = \sqrt{\text{NOT}}\,\text{NOT}\sigma$$

Hence, $\text{NOT}\sigma \preceq \text{NOT}\rho$. (ii) If $\rho \approx \sigma$ then $\text{NOT}\rho \approx \text{NOT}\sigma$ follows from (i). We also have that $\sqrt{\text{NOT}}\,\rho \sim \sqrt{\text{NOT}}\,\sigma$ and

$$\sqrt{\text{NOT}}\,\sqrt{\text{NOT}}\,\rho = \text{NOT}\rho \sim \text{NOT}\sigma = \sqrt{\text{NOT}}\,\sqrt{\text{NOT}}\,\sigma$$

so that $\sqrt{\text{NOT}}\,\rho \approx \sqrt{\text{NOT}}\,\sigma$. (iii) Suppose that $\rho \approx \rho'$ and $\sigma \approx \sigma'$. By Theorem 3.1 (iii), $\text{AND}(\rho, \sigma) \sim \text{AND}(\rho', \sigma')$. We must show that

$$p_n(\sqrt{\text{NOT}}\,\text{AND}(\rho, \sigma)) = p_n(\sqrt{\text{NOT}}\,\text{AND}(\rho', \sigma')) \tag{4.2}$$

for all n. But (4.2) is a consequence of the following result [6]

$$p_n(\sqrt{\text{NOT}}\,\text{AND}(\rho, \sigma)) = \frac{1}{2} \sum_{\substack{i,j \\ i+j+1=n}} p_\rho(i)p_\sigma(j) \tag{4.3}$$

Hence, $\text{AND}(\rho, \sigma) \approx \text{AND}(\rho', \sigma')$. □

From (4.3) we obtain the interesting fact that

$$p(\sqrt{\text{NOT}}\,\text{AND}(\rho, \sigma)) = \frac{1}{2} \sum_n \sum_{\substack{i,j \\ i+j+1=n}} p_\rho(i)p_\sigma(j)$$
$$= \frac{1}{2} \sum p_\rho(i) \sum p_\sigma(j) = \frac{1}{2}$$

Applying Theorem 4.1 the following relations and operations are well defined: $[\rho]_2 \leq [\sigma]_2$ if $\rho \preceq \sigma$, $\text{NOT}[\rho]_2 = [\text{NOT}\rho]_2$, $\sqrt{\text{NOT}}\,[\rho]_2 = [\sqrt{\text{NOT}}\,\rho]_2$, AND $([\rho]_2, [\sigma]_2) = [\text{AND}(\rho, \sigma)]_2$,

$$\text{OR}\,([\rho]_2, [\sigma]_2) = [\text{NOT AND}(\text{NOT}\rho, \text{NOT}\sigma)]_2$$

We then have that $\text{NOT NOT}[\rho]_2 = [\rho]_2$, $[\rho]_2 \leq [\sigma]_2$ implies that $\text{NOT}[\sigma]_2 \leq \text{NOT}[\rho]_2$ and $\sqrt{\text{NOT}}\sqrt{\text{NOT}}\,[\rho]_2 = \text{NOT}[\rho]_2$.

We say that ρ is strongly sector down Scotian if $P^{(n)}/2^{n-1} \preceq \rho$ for some n, ρ is strongly sector up Scotian if $\rho \preceq P_1^{(n)}/2^{n-1}$ for some n and ρ is strongly sector Scotian if for some n

$$\frac{P_0^{(n)}}{2^{n-1}} \preceq \rho \preceq \frac{P_1^{(n)}}{2^{n-1}}$$

Theorem 4.2. (i) *ρ is strongly sector up Scotian if and only if there exists an n such that $p(\rho) = p_n(\rho)$ and $p_n(\sqrt{\mathrm{NOT}}\,\rho) \geq 1/2$.* (ii) *$\rho$ is strongly sector down Scotian if and only if there exists an n such that $p(\rho) = 1 - p_\rho(n) + p_n(\rho)$ and $p_\rho(n) \geq p_n(\sqrt{\mathrm{NOT}}\,\rho) + \frac{1}{2}$ (and hence, $p_n(\sqrt{\mathrm{NOT}}\,\rho) \leq 1/2$.)* (iii) *$\rho$ is strongly sector Scotian if and only if there exists an n such that $p_\rho(n) = 1$ and*

$$p(\sqrt{\mathrm{NOT}}\,\rho) = p_n(\sqrt{\mathrm{NOT}}\,\rho) = \frac{1}{2}$$

Proof: (i) By definition ρ is strongly up Scotian if and only if $\rho \leq P_1^{(n)}/2^{n-1}$ and $\sqrt{\mathrm{NOT}}\,P_1^{(n)}/2^{n-1} \leq \sqrt{\mathrm{NOT}}\,\rho$ for some n. By Theorem 3.2 (i) the first inequality is equivalent to $p(\rho) = p_n$. By (3.1) and (3.2) the second inequality is equivalent to

$$p_m\left(\sqrt{\mathrm{NOT}}\,\frac{P_1^{(n)}}{2^{n-1}}\right) \leq p_m(\sqrt{\mathrm{NOT}}\,\rho), \quad m = 1, 2, \ldots \tag{4.4}$$

$$\mathrm{tr}\left(P_0^{(m)}\sqrt{\mathrm{NOT}}\,\frac{P_1^{(n)}}{2^{n-1}}\right) \geq \mathrm{tr}\big(P_0^{(m)}\sqrt{\mathrm{NOT}}\,\rho\big), \quad m = 1, 2, \ldots \tag{4.5}$$

Now (4.4) is equivalent to $p_n(\sqrt{\mathrm{NOT}}\,\rho) \geq 1/2$ and (4.5) holds automatically. (ii) This follows from (i) and the fact that ρ is strongly sector down Scotian if and only if NOTρ is strongly sector up Scotian. (iii) This follows from (i) and (ii). □

We do not know what the minimal and maximal elements of L_2 are or even whether they exist. We say ρ is strongly down Scotian relative to the L_1 minimal element ρ if $\sigma \preceq \rho$, ρ is strongly up Scotian relative to the L_1 maximal element σ if $\rho \preceq \sigma$, ρ is strongly Scotian relative to the L_1 minimal element σ if $\sigma \preceq \rho \preceq$ NOTσ.

Theorem 4.3. (i) *ρ is strongly up Scotian relative to σ if and only if $p_n(\rho) \leq p_\sigma(n)$ and $p_n(\sqrt{\mathrm{NOT}}\,\rho) \geq p_\sigma(n)/2$ for every n.* (ii) *ρ is strongly down Scotian relative to σ if and only if*

$$p_n(\mathrm{NOT}\rho) = p_\rho(n) - p_n(\rho) \leq p_\sigma(n)$$

and $p_n(\sqrt{\mathrm{NOT}}\,\rho) \leq p_\sigma(n)/2$ for every n. (iii) ρ is strongly Scotian relative to σ if and only if

$$p_\rho(n) - p_\sigma(n) \leq p_n(\rho) \leq p_\sigma(n)$$

and $p_n(\sqrt{\mathrm{NOT}}\,\rho) = p_\sigma(n)/2$ for every n.

Proof: (i) By Theorem 3.4 (i) we have that $\rho \preceq \sigma$ if and only if $p_n(\rho) \leq p_\sigma(n)$ and $\sqrt{\text{NOT}}\,\sigma \leq \sqrt{\text{NOT}}\,\rho$. The second inequality is equivalent to

$$\frac{p_\sigma(n)}{2} = p_n(\sqrt{\text{NOT}}\,\sigma) \leq p_n(\sqrt{\text{NOT}}\,\rho).$$

(ii) This follows from (i). (iii) This follows from (i) and (ii). □

REFERENCES

Bravyi, S. and Kitaev, A. (2002). Fermionic quantum computation. *Annals of Physics* **298**, 210–226.

Cattaneo, G., Dalla Chiara, M., Giuntini, R., and Leporini, R. (2002). An unsharp logic from quantum computation, e-print: quant-phys/0201013.

Cattaneo, G., Dalla Chiara, M., Giuntini, R., and Leporini, R. (preprint). Quantum computational structures.

Dalla Chiara, M., Giuntini, R., Leporati, A., and Leporini, R. (2002). Quantum semantics and quantum trees, e-print: quant-phys/0211190.

Eckert, K., Schliemann, J., Bruss, D., and Lewenstein, M. (2002). Quantum correlations in systems of indistinguishable particles. *Annals of Physics* **299**, 88–127.

Gudder, S. (2003). Quantum computational logic. *International Journal of Theoretical Physics* **42**, 39–47.

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

Pittenger, A. (2001). *An Introduction to Quantum Computing Algorithms*, Birkhäusen, Boston.