ISSN (EN LINEA): 1850 - 1158

LÓGICAS DIFUSAS ASOCIADAS A LAS COMPUERTAS CUÁNTICAS

FUZZY LOGIC ASSOCIATED TO QUANTUM GATES

G. Domenech[a] y H. Freytes[b]

a. Instituto de Astronomía y Física del Espacio (IAFE)
CC 67 – suc 28 – 1428 Buenos Aires – Argentina
domenech@iafe.uba.ar
b. Departamento de Matemática – Faculatad de Cienicas Exactas y Naturales
Universidad de Buenos Aires
hfreytes@dm.uba.ar

Palabras claves: compuertas cuánticas, PMV–álgebras, lógica difusa
Key words: quantum gates, PMV-algebras, fuzzy logic

En este trabajo utilizamos estructuras residuadas asociadas a la lógica difusa para desarrollar ciertos aspectos del procesamiento de la información cuántica. Con este propósito, introducimos un sistema axiomático cuya interpretación natural es la estructura irreversible de Poincaré.

In this paper we use residuated structures associated to fuzzy logic in order to develope certain features of the processing of quantum information. With this purpose, we introduce an axiomatic system whose natural interpretation is the Poincaré irreversible structure.

I. INTRODUCCIÓN

El significado de una sentencia elemental en la lógica asociada a la computación cuántica[1] está representado por la cantidad de información cuántica codificada en una colección de qbits, el equivalente cuántico de los bits clásicos (0, 1 ó F, V), o de qmixes. La conjunción y la disyunción de la información contenida en los q-registros tienen características diferentes de sus homónimas no sólo en la lógica clásica sino también en la lógica cuántica estándar. La articulación de esas sentencias admite además otros conectivos, como el unario no funcional $\sqrt{\neg}$, que reflejan un comportamiento cuántico genuino asociado al procesamiento de la información en una computadora cuántica –en particular la aparición de estados tipo *gato de Schrödinger* de los qbits- que no admiten un paralelo ni en la lógica clásica ni en la cuántica ordinaria.

Nuestro planteo para la axiomatización de esta lógica está basado en el *razonamiento aproximado* en el sentido de la lógica difusa, siguiendo la sugerencia de Dalla Chiara *et al.* de que la lógica de la computación cuántica es "un nuevo ejemplo de lógica difusa"[2]. Así establecemos una axiomatización que permite obtener un teorema de completitud tipo Pavelka[3] en un cálculo infinito-valuado de Łukaciewicz[4] enriquecido. Dicho cálculo refleja el conjunto mínimo de propiedades básicas asociadas a los esquemas computacionales cuánticos. Más concretamente, los modelos naturales resultan ser las PMV-estructuras[5].

II. EL LENGUAJE

La semántica natural para el cálculo de la lógica asociada a la computación cuántica está basada en una asignación de probabilidad sobre el intervalo real [0, 1] con las operaciones de suma truncada, negación de Łukaciewicz y el producto habitual. La idea de consecuencia lógica $\phi \models \varphi$ está dada a partir de una desigualdad de probabilidades $p(\phi) \leq p(\varphi)$, siendo p la probabilidad asignada a una proposición acerca del sistema vía la regla de Born de la mecánica cuántica. Desde el punto de vista sintáctico, dicha consecuencia es tomada como que la fórmula $\phi\rightarrow\varphi$ es una tautología en [0, 1], siendo $\rightarrow$ la implicación de Łukaciewicz en dicho intervalo.

El lenguaje proposicional $\mathcal{L}$ asociado a la computación cuántica- vale decir, la noción de fórmula- se construye de la manera usual a partir del siguiente alfabeto:

$$\langle P, \copyright, \mid, \bullet, \rightarrow, \vee, \wedge, \neg, \sqrt{\neg}, S, (,) \rangle$$

donde P es el conjunto de letras proposicionales, ©, $\mid$, $\bullet$, $\rightarrow$, $\vee$, $\wedge$, $\neg$ son los conectivos del cálculo infinito valuado de Łukaciewicz enriquecido con el producto, $\sqrt{\neg}$ es el conectivo mencionado y S es un conjunto de conectivos constantes dado por el álgebra densa generada por ½ en el intervalo real [0, 1]. Esta álgebra densa dará los *axiomas de contabilidad* en las extensiones de Pavelka. Se considera además un conectivo de equivalencia "≡", dado como abreviación, de la siguiente manera:

$$\varphi \equiv \phi \quad \text{si y sólo si} \quad (\varphi \rightarrow \phi) \mid (\phi \rightarrow \varphi)$$

III. LA PROPUESTA

Para poder considerar el aspecto semántico de esta lógica, introducimos la noción de *modelo* como la aplicación e del lenguaje $\mathcal{L}$ al conjunto $D(C^2)$ de los operadores densidad ρ que cumple:

1. Si * es un conectivo binario, entonces $e(\varphi * \phi) = e(\varphi) * e(\phi)$
2. $e(\sqrt{\varphi}) = \sqrt{e(\varphi)}$
3. $e(\neg\varphi) = \neg\, e(\varphi)$
4. $e(\bar{s}) = \rho_s$ para cada $\bar{s} \in \dddot{S}$
5. $e(\perp) = P_o$
6. $e(\int) = P_1$

donde P_o es el proyector asociado al qbit $|0\rangle$ y P_1 al $|1\rangle$. Esto posibilita que el cálculo proposicional se relacione con las propiedades de la asignación de probabilidad: el valor de probabilidad $e_p(\varphi)$ de una sentencia φ es $e_p(\varphi) = p(e(\varphi))$ y ϕ es consecuencia de φ si y sólo si $e_p(\phi) \le e_p(\varphi)$. Con estos elementos nos ha sido posible construir una axiomática para la lógica computacional cuántica. La construcción detallada de los axiomas puede encontrarse en la ref. [(6)].

IV. SISTEMA AXIOMÁTICO

Obtenemos cinco conjuntos de axiomas:

<u>Axiomas de Łukaciewicz</u>

W1 $\alpha \to (\beta \to \alpha)$

W2 $(\alpha \to \beta) \to ((\beta \to \gamma) \to (\alpha \to \gamma))$

W3 $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$

W4 $((\alpha \to \beta) \to \beta) \to ((\beta \to \alpha) \to \alpha)$

<u>Axiomas de equivalencia</u>

E1 $\alpha \mid \beta \equiv \neg(\neg\alpha \copyright \neg\beta)$

E2 $\alpha \to \beta \equiv \neg(\alpha \mid \neg\beta)$

E3 $\neg\alpha \equiv \alpha \to \perp$ ($\perp$ representa el 0 en S)

E4 $\alpha \wedge \beta \equiv \alpha \mid (\alpha \to \beta)$

E5 $\alpha \vee \beta \equiv (\alpha \to \beta) \to \beta$

E6 $\neg\perp \equiv \int$ ($\int$ representa el 1 en S)

<u>Axiomas de producto</u>

P1 $\alpha \bullet \beta \to \beta \bullet \alpha$

P2 $\int \bullet\, \alpha \equiv \alpha$

P3 $(\alpha \bullet \beta) \to \beta$

P4 $(\alpha \bullet \beta) \bullet \gamma \equiv \alpha \bullet (\beta \bullet \gamma)$

P5 $\alpha \bullet (\beta \mid \neg\gamma) \equiv (\alpha \bullet \beta) \mid \neg(\alpha \bullet \gamma)$

<u>Axiomas para S</u> (*de contabilidad*)

para cada $\bar{r}, \bar{s} \in S$

S1 $\bar{r} \mid \bar{s} \equiv \overline{r \,\square\, s}$

S2 $\bar{r} \to \bar{s} \equiv \overline{r \to s}$

S3 $\bar{r} \bullet \bar{s} \equiv \overline{r \bullet s}$

<u>Axiomas de $\sqrt{\neg}$</u>

Q1 $\sqrt{\neg}\sqrt{\neg}\,\alpha \equiv \neg\alpha$

Q2 $\sqrt{\neg}(\neg\alpha) \equiv \neg\sqrt{\neg}\,\alpha$

Q3 si $*$ es un conectivo binario, $\sqrt{\neg}\,(\alpha * \beta) \equiv ½$

Q4 $\sqrt{\neg}\,\bar{s} \equiv ½$

Q5 $\{((¼ \bullet \alpha) \copyright (¼ \bullet \sqrt{\neg}\,\alpha)) \to \bar{s} \ge (1+\sqrt{2})/4\sqrt{2}$

y se toma el *modus ponens* como única regla de inferencia. Las nociones asociadas al concepto de teoría y a la deducción son las habituales de la lógica difusa.

IV. COMPONENTE SEMÁNTICA

El modelo natural del cálculo asociado a $\mathcal{L}$ está dado a partir de valuaciones en el intervalo [0, 1]. Pero no es posible considerar el conjunto completo de todas las posibles valuaciones de $\mathcal{L}$ al [0, 1]. Las valuaciones admisibles se construyen de la siguiente forma: sea el círculo unitario $C = \{(r_1, r_2) : r_1^2 + r_2^2 \le 1\}$. Se define una noción de modelo como una función

$$e : \mathcal{L} \to \mathcal{C}$$

tal que a cada fórmula α le asigna un par

$$e(\alpha) = (r_1, r_2) \in \mathcal{C}$$

y la valuación al [0, 1] se define como

$$e_p(\alpha) = (1 - r_2)/2\,, \quad e_p(\sqrt{\neg}\,\alpha) = (1 - r_1)/2$$

Una fórmula α es una tautología si y sólo si para todo modelo e, $e_p(\alpha) = 1$. Esto se notará como $\models \alpha$. Por otro lado, decimos que α es consecuencia de la teoría $\mathcal{T}$ (y lo indicamos como $\mathcal{T} \models \alpha$) si y sólo si para todo modelo e y para toda fórmula $\beta \in \mathcal{T}$ resulta que si $e_p(\beta) = 1$ entonces $e_p(\alpha) = 1$.

V. COMPLETITUD EN EL SENTIDO DE PAVELKA

En el estudio de las lógicas tipo Pavelka, se introducen constantes de verdad en el lenguaje con el objeto de definir un *grado de prueba* o demostrabilidad de una fórmula α respecto de una teoría $\mathcal{T}$. En nuestro caso, el grado de prueba se da a partir de un supremo. Por otro lado, también se define un *grado semántico* de una teoría $\mathcal{T}$ respecto de una fórmula α, lo que representa la relevancia de la teoría respecto de la fórmula. Esto es el ínfimo de las valuaciones que α puede tomar cuando esas valuaciones asignan el valor 1 a las fórmulas de $\mathcal{T}$. Un teorema de completitud de Pavelka se obtiene cuando los grados de prueba y semántico coinciden. En el caso de la lógica asociada a la computación cuántica, la axiomatización al igual que la completitud de Pavelka eran problemas abiertos, que hemos resuelto.

Referencias

1- Nielsen, M. A. and Chaung, I. L.: "Quantum computation and quantum information", Cambridge University Press, Cambridge (2000).

2- Cattaneo, G., Dalla Chiara, M. L., Giuntini, R. And Leporini, R.: *An unsharp logic from quantum computation*, Int. J. Theor. Phys. **43**, 1803-1817 (2004).

3- Pavelka, J.: *On fuzzy logic I, II, III,* Zeitschr. F. Logik und Grundl. Del Math. **25**, 45-52, 119-134, 447-464 (1979).

4- Cignoli, R., D'Ottaviano, M. and Mundici, D.: *Algebraic foundations of many valued reasoning*, Kluwer, Dordrecht (2000).

5- Montagna, F.: *An algebraic approach to propositional fuzzy logic*, J. of Logic, Language and Informat. **9**, 91-124 (2000).

6- Domenech, G. and Freytes, H., *Fuzzy propositional logic associated with quantum computational gates*, submitted to the Int. J. Theor. Phys. (2005).