EPISTEMOLOGÍA E HISTORIA DE LA CIENCIA

SELECCIÓN DE TRABAJOS DE LAS XV JORNADAS
VOLUMEN 11 (2005)
TOMO I

Horacio Faas
Aarón Saal
Marisa Velasco
Editores

ÁREA LOGICO-EPISTEMOLÓGICA DE LA ESCUELA DE FILOSOFÍA
CENTRO DE INVESTIGACIONES DE LA FACULTAD DE FILOSOFÍA Y HUMANIDADES
UNIVERSIDAD NACIONAL DE CÓRDOBA

Perspectivas en la axiomatización de la lógica computacional cuántica

Andrea Costa / Graciela Domenecht / Héctor Freytes‡*

Introducción

Desde los comienzos de las matemáticas, sistemas sencillos como los dedos de las manos, palitos y luego el ábaco se vienen utilizando para representar entidades matemáticas y operaciones entre ellas. Y tan pronto como se hizo visible la relación entre operaciones de la aritmética elemental y secuencias de procedimientos implementables físicamente, los diseños pioneros de Pascal y Leibniz los trasladaron a dispositivos mecánicos que por primera vez nos relevaron de tareas tediosas como la de multiplicar dos enteros grandes.

Al igual que la suma o la multiplicación de números, también el cálculo del camino más corto entre dos sitios, del área de una figura o de los esfuerzos sobre los postes de un puente son tareas que tienen la estructura "*entrada* → *cálculo* → *resultado*" y la parte de *cálculo* es siempre realizada por un sistema dinámico que evoluciona en el tiempo. Para hacer un cálculo, es necesario así buscar un sistema físico tal que su evolución temporal se corresponda con ese cálculo y darle los datos de *entrada* como condiciones iniciales de la evolución. Su estado final proveerá el *resultado* buscado.

Hay ejemplos asombrosos de computadoras análogas que fueron diseñadas para resolver un único problema, como la de Lord Kelvin, que utilizaba ruedas y la fricción y presión de fluidos para hallar la solución de una ecuación diferencial. O el procedimiento de Gaudí para encontrar las dimensiones y formas de los arcos de la iglesia de La Sagrada Familia en Barcelona, que consistía en anudar y colgar conjuntos de cuerdas de largos adecuados, dejar que la gravedad "calculara" la forma de todos los arcos y "leer" el resultado mirando la estructura en un espejo. Estos modelos de "máquinas" diseñadas para realizar un único cálculo, cronológicamente con anterioridad a la invención de las computadoras reales, sugirieron el modelo matemático para una computadora universal -la máquina de Turing [T]- y la tesis (de Church-Turing) indemostrable pero ampliamente aceptada de que *cualquier función que se puede calcular de alguna forma, también se puede calcular mediante un procedimiento mecánico por medio de una máquina de Turing*, lo que equivale a decir: por un dispositivo físico razonable. Y aunque hay muchas más funciones que maneras de calcularlas -porque el número de máquinas de Turing es contable mientras que el conjunto de las familias de funciones no lo es- el costo de hacerlo es crucial aun para las que pueden calcularse, costo que se evalúa en términos de los recursos físicos necesarios para la operación. La división usual entre los problemas que se consideran *tratables y los que no* se convierte, desde la aparición de las computadoras digitales, en *calculable eficientemen-*

* Universidad de Buenos Aires. CONICET.

† Universidad de Buenos Aires. CONICET.

‡ Universidad Nacional de Rosario.

Epistemología e Historia de la Ciencia, Volumen 11 (2005)

te o no, y esto se relaciona con el tiempo de cálculo -típicamente el que crece polinómica o exponencialmente con el tamaño de los datos de entrada. Los problemas en el segundo conjunto se consideran intratables.

La teoría de la computación cuántica

Lo que es importante extraer de este resumen es que la pregunta acerca de qué es calculable es asimilable a la pregunta acerca de cuáles sistemas físicos pueden ser realizados y con qué eficiencia evolucionan hacia el resultado. Y la posibilidad de que los dispositivos que evolucionan para llegar al resultado sean cuánticos, o sea: la posibilidad de algoritmos cuánticos, lleva a que sea factible resolver problemas clásicos en tiempo mucho menor -en algunos casos exponencialmente menor- que con algoritmos clásicos. Ejemplo de esta situación es el algoritmo de Simon [S] para el problema del oráculo -en la que se da a la computadora una función como una caja negra y la computadora tiene que calcularla sin conocer el código de la función- que lleva tiempo que aumenta exponencialmente en una computadora clásica (problema intratable) y cuadráticamente en una computadora cuántica, lo que lo convierte en tratable. Pero fueron las claves de encriptamiento [RSA] las que concitaron gran interés por las computadoras cuánticas. Las claves se sostienen en la conjetura de que la multiplicación de enteros es mucho más sencilla que su factorización, y precisamente el problema de la factorización está entre los que clásicamente son intratables pero se convierten en tratables debido a que en un procesamiento cuántico (como el algoritmo de Shor [Sh]) pueden utilizarse evoluciones adecuadas de sistemas físicos en estados tipo "gato de Schrödinger" definiendo nuevos conectivos lógicos.

La teoría de la computación cuántica [NG] sugiere una caracterización semántica para una nueva forma de lógica cuántica diferente de las ortológicas, donde el significado de una sentencia está asociado a un vector en el espacio de estados de un sistema físico y los conectivos lógicos son interpretados como compuertas lógicas. La literatura acerca de la QCL reconoce la inexistencia de una axiomatización para esta lógica. Una técnica canónica para realizar una axiomatización es a partir de una estructura algebraica que se toma como modelo de la lógica de manera de que sus propiedades deductivas se traduzcan en propiedades algebraicas [H]. Dicha estructura algebraica debe tener suficiente riqueza como para espejar todos los procedimientos deductivos. Nuestro abordaje del problema se enmarca en esta perspectiva algebraica. En ella, los conectivos básicos de QCL, al igual que los conectivos booleanos clásicos, pueden entenderse como generalización de operaciones aritmético-lógicas. De las propiedades que satisfacen dichas operaciones se extrae el comportamiento de los correspondientes conectivos.

Como es sabido, los conectivos de la lógica clásica pueden ponerse en correspondencia con sus tablas de verdad asociables a su vez a operaciones aritméticas en base numérica 2 que es el sustrato operacional de la computación clásica. Las unidades de información que la computación clásica procesa son los bits, que toman valores "verdadero" (= 1) o "falso" (= 0). El análogo cuántico a la unidad de información clásica es el qbit, cuya representación se realiza por un vector en un espacio vectorial complejo de dimensión dos con producto interno. Por analogía

con los bits clásicos llamamos {|0⟩, |1⟩} a los elementos de una base ortonormal en este espacio, la base lógica. Luego, un qbit $|\varphi\rangle$ normalizado viene dado por:

$|\varphi\rangle = a|0\rangle + b|1\rangle$ con $|a|^2 + |b|^2 = 1$

Una rutina en computación cuántica puede describirse de la siguiente manera: preparamos un sistema de qbits en un estado inicial (que es equivalente a una valuación de letras proposicionales, esto es: una fila de la matriz de datos de una tabla de verdad en el caso clásico) y lo sometemos a un conjunto de transformaciones representadas por conectivos lógicos en el sentido de la QCL. Durante este proceso la información está codificada en estados cuánticos del tipo "gato de Schrödinger" que carecen de análogo clásico. Precisamente la posibilidad de procesar estados de este tipo, que implica explorar varias posibilidades al mismo tiempo, es la que aumenta enormemente la eficiencia de la computación cuántica respecto de la clásica. Para obtener el resultado de la aplicación de los conectivos al estado inicial (cuya contraparte clásica es hallar el valor de la fórmula respecto de la valuación de variables dada) es necesario convertir la información cuántica en clásica, lo que se realiza en términos de la medición del sistema físico (proyección sobre la base lógica). Este procedimiento ("tabla de verdad cuántica") es un algoritmo probabilístico. Esto es, podemos correr exactamente el mismo programa dos veces ("realizar exactamente los mismos pasos en la construcción de una tabla de verdad cuántica") y obtener diferentes resultados debido a la aleatoriedad del proceso de medición cuántico. Es decir, lo que el algoritmo genera es una distribución de probabilidad de resultados posibles.

Conectivos básicos en QCL

En QCL algunos conectivos son generalizaciones de conectivos clásicos, más precisamente de {¬, ∧, ∨}, y otros son conectivos propios que realizan operaciones sin análogo clásico. Así, por ejemplo, la negación actúa del siguiente modo sobre los elementos de la base lógica de un qbit:

	¬
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

Esta operación es equivalente a la aplicación del operador lineal σ_x de Pauli al qbit inicial, operador que en esta base se representa matricialmente por:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

La conjunción aplicada sobre los mismos elementos de la base realiza el siguiente proceso:

	$\wedge$
$(\|0\rangle, \|0\rangle)$	$\|0\rangle\otimes\|0\rangle\otimes\|0\rangle$
$(\|0\rangle, \|1\rangle)$	$\|0\rangle\otimes\|1\rangle\otimes\|0\rangle$
$(\|1\rangle, \|0\rangle)$	$\|1\rangle\otimes\|0\rangle\otimes\|0\rangle$
$(\|1\rangle, \|1\rangle)$	$\|1\rangle\otimes\|1\rangle\otimes\|1\rangle$

donde $\otimes$ simboliza el producto tensorial. Y la disyunción se define a partir de las leyes de De Morgan.

Uno de los nuevos conectivos es $\sqrt{\neg}$ que transforma los vectores de la base en combinaciones lineales de ellos mismos:

	$\sqrt{\neg}$
$\|0\rangle$	$(\frac{1}{2} - \frac{i}{2})\|0\rangle + (\frac{1}{2} + \frac{i}{2})\|1\rangle$
$\|1\rangle$	$(\frac{1}{2} + \frac{i}{2})\|0\rangle + (\frac{1}{2} - \frac{i}{2})\|1\rangle$

lo que en la base lógica se escribe como

$$\begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} + \frac{i}{2} \\ \frac{1}{2} - \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \end{pmatrix}$$

Lenguaje proposicional en QCL

Definimos un lenguaje proposicional L_{QC} para QCL de la manera habitual a partir del siguiente alfabeto: $\langle P, \neg, \wedge, \vee, \sqrt{\neg}\rangle$ siendo P el conjunto de fórmulas atómicas. Es claro que $\sqrt{\neg}$ es un conectivo unario mientras que el resto preserva la aridad original.

La interpretación natural de L_{QC} se realiza sobre $\bigcup_{n\in N} \otimes^n C^2$, es decir la unión de los productos n-tensoriales de los espacios vectoriales C^2 de cada qbit.

El valor de verdad para una fórmula α de L_{QC} se obtiene a partir de la probabilidad asignada a la interpretación de dicha fórmula en $\bigcup_{n\in N} \otimes^n C^2$, la que se calcula con la prescripción usual de la mecánica cuántica (la regla de Born). Notamos como $p(\alpha)$ a esa probabilidad. Siguiendo esta definición de valuación, se dirá que α es una QCL-tautología si y sólo si $p(\alpha) = 1$. La idea de consecuencia semántica "$\models$" inducida naturalmente por la asignación de probabilidad viene dada por:

$\alpha \models \beta$ sii $p(\alpha) \leq p(\beta)$

Es un problema abierto hallar una teoría de deducción "$\vdash$" compatible con la idea de consecuencia lógica en QCL, es decir que $\alpha \vdash \beta$ sii $\alpha \models \beta$ [CDCGL]. Para resolverlo desde la perspectiva algebraica, debemos encontrar una clase de estructuras en la que sea definible una operación cuyo reflejo sintáctico sea el que

provee un sistema deductivo. Es claro que dicha estructura deberá contener como caso particular a $\bigcup_{n\in N} \otimes^n C^2$, pues este espacio es la interpretación natural de L_{QC}. Un requerimiento inicial operacionalmente adecuado es el de un orden parcial "$\leq$" con elemento máximo "$\top$" y una operación de implicación "$\rightarrow$" tal que $a \leq b$ si y sólo si $a \rightarrow b = \top$ y esto, en el caso de $\bigcup_{n\in N} \otimes^n C^2$, debe ser a su vez equivalente a que $p(a) \leq p(b)$. Desde este punto de vista la dificultad que tiene QCL es que $\bigcup_{n\in N} \otimes^n C^2$ no tiene un orden parcial inducido a partir de las probabilidades y las operaciones $\neg, \wedge, \vee, \sqrt{\neg}$, no lo proveen.

Conclusiones

Proponemos forzar la introducción del conectivo $\rightarrow$ para cubrir la mencionada deficiencia y proveer a $\bigcup_{n\in N} \otimes^n C^2$ de un orden compatible con las asignaciones de probabilidad, expandiendo así como mínimo el lenguaje para L_{QC} a un alfabeto de la forma: $\langle P, \neg, \wedge, \vee, \sqrt{\neg}, \rightarrow, \top \rangle$.

Referencias

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

[H] P. Hájek (2000): *Metamathematics of fuzzy logic*, Kluwer Academic Publishers.

[NG] M. A. Nielsen, I. L. Chuang (2001): *Quantum computation and quantum information*, Cambridge University Press.

[RSA] R. L. Rivest, A. Shamir and L. Adleman (1978): "A method of obtaining digital signatures and public-key cryptosystems", *Comm. Assoc. Comput. Mach.* 21, 120-126.

[S] D. R. Simon (1997): "On the power of quantum computation" *SIAM J. Computing* 26, 1474-1483.

[Sh] P. W. Shor (1997). "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM J Computing* 26, 1484-1509.

[T] A. M. Turing (1936): "On computable numbers, with an application to the Entschneidungsproblem", *Proc Lond. Math. Soc. Ser* 42, 230.