COMPUTACIÓN CUÁNTICA + LÓGICAS PARACONSISTENTES = TEORÍAS PARACONSISTENTES DE LA COMPUTACIÓN

Andrés Sicard

Grupo Lógica y Computación
Departamento de Ciencias Básicas
Escuela de Ciencias y Humanidades
Universidad EAFIT, Medellín, Colombia

“Quizás no sea una exageración afirmar que las máquinas del futuro serán, básicamente paraconsistentes.”

Newton C. Da Costa y Renato A. Lewin [5, p. 200]

Computación cuántica (discreta)

N-qubit($|\,x\rangle \in \mathbb{C}^{2^n}$):

$$\begin{aligned} |\,x\rangle &= |\,x_1, \ldots, x_n\rangle \\ &= |\,x_1\rangle \otimes \cdots \otimes |\,x_n\rangle\,. \end{aligned}$$

Qubit($|\,x_i\rangle \in \mathbb{C}^2$):

$$|\,x_i\rangle = a_i\,|\,0\rangle + b_i\,|\,1\rangle\,,$$

donde $|a_i|^2 + |b_i|^2 = 1$.

Evolución: La evolución de un n-qubit $|\,x\rangle$ es determinada por un operador unitario U, el cual actúa sobre el espacio $\mathbb{C}^{2^n}$:

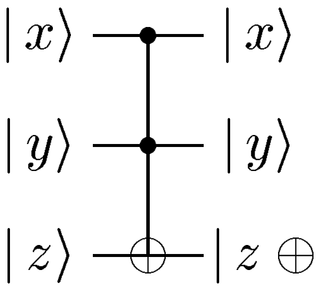
$$U^\dagger U = Id.$$

El operador de evolución actúa sobre los qubits, generando nuevos qubits:

$$|\,x(t)\rangle = U^t\,|\,x(0)\rangle\,, t \in \mathbb{Z}^+.$$

Modelos de computación cuántica (discreta)

1. Máquinas de Turing cuánticas.
2. Circuitos cuánticos (compuerta universal de Toffoli):



$$|\, z \oplus min(x,y)\rangle = \begin{cases} |\, x \wedge y\rangle & \text{si } |\, z\rangle = |\, 0\rangle, \\ |\, \neg z\rangle & \text{si } |\, x\rangle = |\, y\rangle = |\, 1\rangle, \\ |\, x\rangle & \text{si } |\, z\rangle = |\, 0\rangle, |\, y\rangle = |\, 1\rangle. \end{cases}$$

Computabilidad y complejidad algorítmica

Computabilidad:

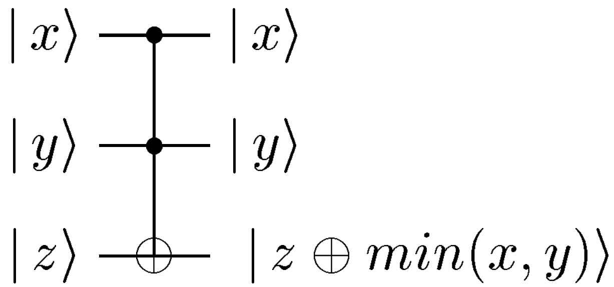
$$\begin{tikzcd}
\boxed{\text{MT clásica}} \arrow[r, dash, "\equiv"] \arrow[d, dash, "\equiv"'] & \boxed{\text{MT probabilista}} \arrow[d, dash, "\equiv"] \\
\boxed{\text{MT reversible}} \arrow[r, dash, "\equiv"] & \boxed{\text{MT cuántica}}
\end{tikzcd}$$

Complejidad algorítmica:
Peter Shor (1994): Algoritmo para factorizar un número en sus factores primos de complejidad polinomial.

Número de dígitos	**Clásico**	**Cuántico**
129	1,85 años	45,9 minutos
250	$2{,}1 \times 10^6$ años	3,4 horas
1000	$4{,}5 \times 10^{25}$ años	3,07 días

Compuertas cuánticas

$\texttt{TOFFOLI}(|x\rangle, |y\rangle, |z\rangle)$:



$\texttt{AND}(|x\rangle, |y\rangle) = \texttt{TOFFOLI}(|x\rangle, |y\rangle, |0\rangle)$

$\texttt{NOT}(|x\rangle):$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$\sqrt{\texttt{NOT}}(|x\rangle:$ $\begin{pmatrix} \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\ \frac{1}{2}-\frac{i}{2} & \frac{1}{2}+\frac{i}{2} \end{pmatrix}$

Quantum Computational Logic (QCL)

Propuesta por Gianpero Cattaneo, Maria Luisa Dalla Chiara, Roberto Giuntini y Roberto Leporini, en enero del 2002 [3].

Conectivos lógicos:
Negación ($\neg$), conjunción ($\curlywedge$), raíz cuadrada de la negación ($\sqrt{\neg}$) y disyunción ($\curlyvee$).

Conjunto de fórmulas $\mathfrak{F}$: De la manera usual.

Realización cuántica computacional:
Qub: $\mathfrak{F} \to \bigcup_n \mathbb{C}^{2^n}$, donde n es una función de la longitud de la fórmula.

Probabilidad de un vector

Sea $|\psi\rangle = \sum_{j=0}^{2^n-1} a_j\,|j\rangle$ un vector de $\mathbb{C}^{2^n}$. La probabilidad de $|\psi\rangle$ es:

$$Prob(|\psi\rangle) := \sum_{a_j \in C^+|\psi\rangle} |a_j|^2,$$

donde C^+ son las amplitudes asociadas a los vectores bases de $\mathbb{C}^{2^n}$ que finalizan en 1.

Ejemplo:
Sea $|\psi\rangle = \frac{\sqrt{3}}{2}\,|0\rangle + \frac{1}{2}\,|1\rangle)$, entonces $Prob(|\psi\rangle) = \left|\frac{1}{2}\right|^2 = \frac{1}{4}$.

Sea $|\psi\rangle = \frac{1}{2}(|0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle)$, entonces $Prob(|\psi\rangle) = \left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 = \frac{1}{2}$.

Semántica para QCL

Sean α y β fórmulas y sea Qub una realización cuántica computacional tal que $Qub(\alpha) = |\,\alpha\rangle$ y $Qub(\beta) = |\,\beta\rangle$, entonces:

$$
\begin{aligned}
|\,\alpha\rangle &\in \mathbb{C}^2 \text{ si } \alpha \text{ es una fórmula atómica,}\\
|\,\neg\alpha\rangle &= \mathtt{NOT}(|\,\alpha\rangle),\\
|\,\alpha \curlywedge \beta\rangle &= \mathtt{AND}(|\,\alpha\rangle\,, |\,\beta\rangle),\\
\left|\,\sqrt{\neg}\alpha\right\rangle &= \sqrt{\mathtt{NOT}}(|\,\alpha\rangle),\\
|\,\alpha \curlyvee \beta\rangle &= |\,\neg(\neg\alpha \curlywedge \neg\beta)\rangle = \mathtt{NOT}(\mathtt{AND}(\mathtt{NOT}(|\,\alpha\rangle\,, \mathtt{NOT}(|\,\beta\rangle)))).
\end{aligned}
$$

La probabilidad de α es:

$$Prob(\alpha) = Prob(|\,\alpha\rangle) := \sum_{a_j \in C^+|\,\alpha\rangle} |a_j|^2,$$

Verdad (lógica), consecuencia (lógica)

- α es verdadera en la realización cuántica computacional Qub ($\models_{Qub} \alpha$), si y sólo si, $Prob(\alpha) = 1$.
- α es una verdad lógica ($\models \alpha$), si y sólo si, para cualquier realización cuántica computacional Qub se tiene que $\models_{Qub} \alpha$.
- β es una consecuencia de la teoría $\Gamma = \{\alpha_1, \ldots, \alpha_n\}$ en la realización cuántica computacional Qub ($\Gamma \models_{Qub} \beta$), si y sólo si, $\mathrm{Prob}(\Gamma) = \mathrm{Prob}(\{\alpha_1, \ldots, \alpha_n\}) \equiv_{def} \mathrm{Prob}(\alpha_1 \curlywedge \cdots \curlywedge \alpha_n) \leq \mathrm{Prob}(\beta)$.
- β es una consecuencia lógica de la teoría $\Gamma = \{\alpha_1, \ldots, \alpha_n\}$ ($\Gamma \models \beta$), si y sólo si, para cualquier realización cuántica computacional Qub se tiene que $\Gamma \models_{Qub} \beta$.

Algunos (no) teoremas en QCL

Teoremas:

1. $\alpha \models \neg\neg\alpha, \quad \neg\neg\alpha \models \alpha;$
   (doble negación)

2. $\sqrt{\neg}\sqrt{\neg}\alpha \models \neg\alpha,$
   $\neg\alpha \models \sqrt{\neg}\sqrt{\neg}\alpha;$

3. $\alpha \curlywedge \beta \models \beta \curlywedge \alpha, \quad \alpha \curlyvee \beta \models \beta \curlyvee \alpha;$
   (conmutatividad)

4. $\alpha \curlywedge \alpha \models \alpha.$
   (semi-idempotencia 1)

No teoremas:

1. $\alpha \not\models \alpha \curlywedge \alpha;$
   (semi-idempotencia 2)

2. $\not\models \alpha \curlyvee \neg\alpha$
   (tercio excluido)

3. $\not\models \neg(\alpha \curlywedge \neg\alpha);$
   (no contradicción)

4. $(\alpha \curlywedge \beta) \vee (\alpha \curlywedge \gamma) \not\models \alpha \curlywedge (\beta \curlyvee \gamma).$
   (distributiva)

Lógica paraconsistente (1)

Lógica:
Una lógica $\mathcal{L}$ es una estructura $< \mathcal{L}, \vdash >$, donde $\mathcal{L}$ es cualquier conjunto de objetos llamados fórmulas, denotados por $\alpha, \beta, \gamma, \ldots$; los conjuntos de fórmulas son llamados teorías, denotados por $\Gamma, \Delta, \ldots$, y $\vdash$ es una relación entre teorías y fórmulas llamada relación de consecuencia [1, p. 96].

Dominio de una lógica, conectivos: El dominio de una lógica sentencial es (usualmente) una álgebra libre generada con funciones, llamadas conectivos lógicos, a partir de un conjunto de fórmulas llamadas fórmulas atómicas [1, p. 96].

Lógica paraconsistente (2)

Negación:
Una negación es al menos una función unaria sobre el dominio de una lógica, denotada por $\neg$. Dada la fórmula α, la fórmula $\neg\alpha$ es llamada la negación de α [1, p. 96].

Principio EC (informal): Desde una contradicción es posible derivar cada cosa (*ex-contradictio sequitur quod libet*).

El principio EC en términos formales puede ser escrito como:

Principio EC (formal): Sean α y β dos fórmulas cualesquiera y sea Γ una teoría cualquiera, entonces $\Gamma, \alpha, \neg\alpha \vdash \beta$.

Lógica paraconsistente (3)

Lógica paraconsistente (rechazo al principio EC): Sea $\mathcal{L}$ una lógica con una negación $\neg$. Esta negación es paraconsistente, si y sólo si, existe una teoría Γ y existen fórmulas α y β tales que $\Gamma, \alpha, \neg\alpha \nvdash \beta$. Una lógica es paraconsistente, si y sólo si, ella contiene una negación paraconsistente [1, p. 98].

Teoría trivial: Una teoría Γ es trivial si $\Gamma \vdash \alpha$ para toda fórmula α [1, p. 97].

Teoría inconsistente: Sea $\mathcal{L}$ una lógica con una negación $\neg$. Una teoría Γ es inconsistente si existe una fórmula α tal que $\Gamma \vdash \alpha$ y $\Gamma \vdash \neg\alpha$ [1, p. 98].

Teoría paraconsistente: Sea $\mathcal{L}$ una lógica con una negación $\neg$. Una teoría Γ es paraconsistente si Γ es una teoría inconsistente y Γ es una teoría no trivial [1, p. 98].

Paraconsistencia de QCL

Teorema 0.1. *El conectivo negación* ($\neg$) *es un conectivo paraconsistente.*

Teorema 0.2. *El conectivo raíz cuadrada de la negación* ($\sqrt{\neg}$) *es un conectivo paraconsistente.*

Teorema 0.3. *La lógica* $\boldsymbol{QCL}$ *es una lógica paraconsistente.*

Teorías paraconsistentes de la computación

Teorema 0.4. *Sean* Γ *una teoría y* α *una fórmula de la* $\boldsymbol{QCL}$. *Si* $\alpha \in \Gamma$ *y* $\neg\alpha \in \Gamma$, *entonces la teoría* Γ *es una teoría paraconsistente.*

Teorema 0.5. *Sean* Γ *una teoría y* α *una fórmula de la* $\boldsymbol{QCL}$. *Si* $\alpha \in \Gamma$ *y* $\sqrt{\neg}\alpha \in \Gamma$, *entonces la teoría* Γ *es una teoría paraconsistente.*

Conclusiones

- De acuerdo a los teoremas 0.1, 0.2 y 0.3, la *Quantum Computational Logic* (***QCL***) es una lógica paraconsistente, es más, podría decirse que es una lógica "bi-paraconsistente", puesto que contiene dos operadores de negación paraconsistentes[a].
- Quizás el resultado más importante, lo constituya la demostración de la existencia de teorías paraconsistentes en el contexto de la computación (cuántica) (teoremas 0.4 y 0.5).

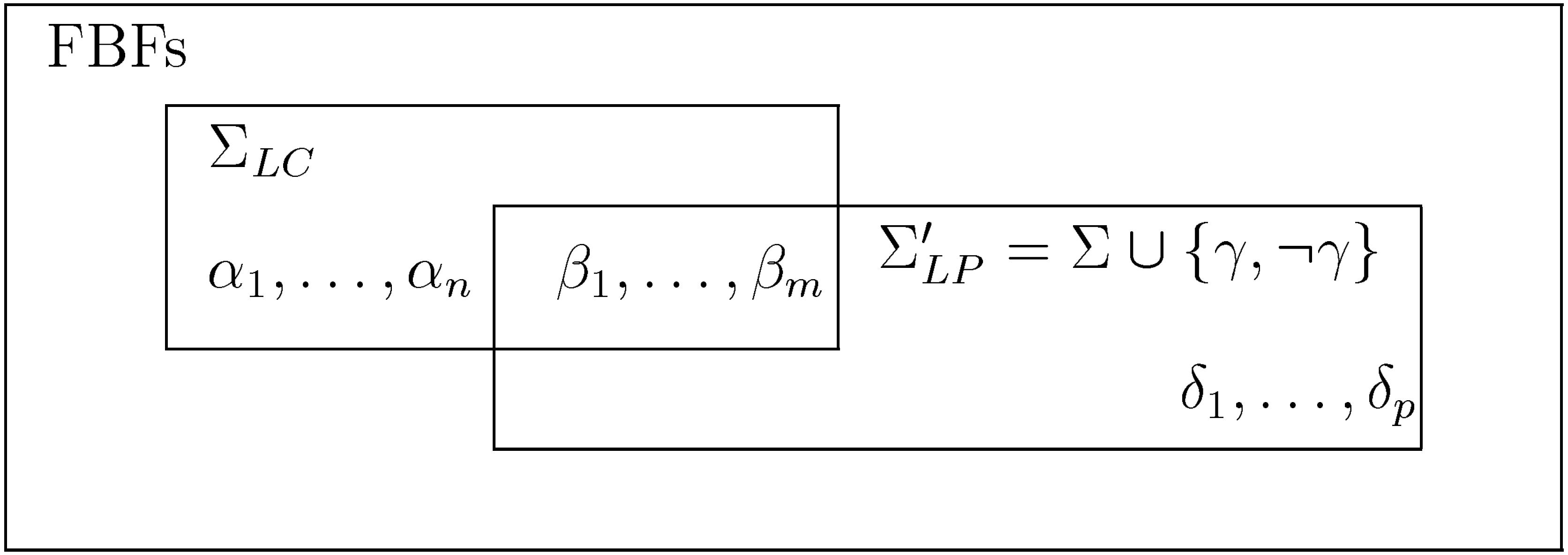
---

[a]La **QCL** además de ser una lógica paraconsistente, es una lógica multivaluada, en particular ∞-valuada, puesto que el valor de verdad asociado a una sentencia α está dado por:

$$\mathrm{Prob}(\alpha) = \mathrm{Prob}(Qub(\alpha)) = \mathrm{Prob}(|\,\alpha\rangle) = \sum_{a_j \in C^+|\,\alpha\rangle} |a_j|^2.$$

Problemas abiertos (1)

- Paraconsistencia - Hipercomputación - Computación cuántica
  Paraconsistencia:



Problemas abiertos (2)

Hipercomputación:
"A hypercomputer is any information-processing device able to carry out tasks that cannot be carried out by a standard universal Turing machine" [4].

Propuestas de hipercomputación cuánticas:
Sustentadas en la posibilidad de que los modelos de computación cuántica "operen" sobre espacios (de Hilbert) infinito dimensionales [2, 6].

Problema:
Generalización la **QCL** para la adecuada manipulación de espacios de Hilbert infinito dimensionales (para ello es necesario, o bien modificar la definición de realización computacional cuántica, o bien permitir que las fórmulas de la **QCL** sean de longitud infinita).

Problemas abiertos (3)

- Analizar la paraconsistencia o no de la **QCL**, bajo definiciones más restrictivas de "lógica paraconsistente" y/o "negación paraconsistente"
- Debido a la equivalencia entre el modelo de circuitos cuánticos y el modelo de máquinas de Turing cuánticas, surge el problema de adecuar la **QCL**, la cual es establecida en el contexto de los circuitos cuánticos, al contexto de las máquinas de Turing cuánticas.
- Aunque la **QCL** es establecida en el nivel sentencial (*zero order level*), esta sólo es construida en su fragmento de nivel cero (*zero degree fragment*), puesto que sólo estan definidos los conectivos de, negación ($\neg$), conjunción ($\curlywedge$), raíz cuadrada de la negación ($\sqrt{\neg}$) y disyunción ($\curlyvee$). Un problema es la ampliación de la **QCL** a fragmentos de mayor grado, es decir, es necesario definir un conectivo de implicación para la **QCL**.

[1] Jean-Yves Béziau. "Frontiers of paraconsisten logic (ed. Diderik Batens et al.)", capítulo What is paraconsisten logic? Hertfordshire, England: Research Studies Press LTD. (2000).

[2] Cristian S. Calude y Boris Pavlov. Coins, quantum measurements, and Turing's barrier. Eprint: `arXiv.org/abs/quant-ph/0112087` (2001).

[3] Gianpero Cattaneo, Maria L. Dalla, Roberto Giuntini y Roberto Leporini. An unsharp logic from quantum computation. Eprint: `arXiv.org/abs/quant-ph/0201013` (2002).

[4] Jack Copeland y Gordon Aston. Hypercomputation. Eprint: `www.alanturing.net/pages/Reference\%\,20Articles/hypercomputation/` [20-Jun-2000] (2001).

[5] Newton C. A. da Costa y Renato A. Lewin. Lógica paraconsistente. En "Encliclopedia IberoAmericana de Filosofía", tomo 7: Lógica, páginas 185–204. Madrid: Editorial Trotta, S.A. (1995).

[6] Tien D. Kieu. Computing the noncomputable. Eprint: `arXiv.org/abs/quant-ph/0203034` (2002).

Agradecimientos y contacto

Agradecimientos:
Este trabajo fue financiado por la Universidad EAFIT, bajo el proyecto de investigación No. 817430.

Contacto:
Andrés Sicard
Universidad EAFIT
email: `asicard@eafit.edu.co`
página *web*: `sigma.eafit.edu.co/~asicard/personal`