POSIBILIDAD DE HIPERCOMPUTACIÓN DESDE LA COMPUTACIÓN CUÁNTICA

Andrés Sicard

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

Hipercomputación

Definición 1:

"Un hipercomputador es un dispositivo que computa todo lo que computa una máquina de Turing, y más. La hipercomputación es la disciplina que estudia los hipercomputadores" [6, p. 4].

Definición 2:

"A hypercomputer is any information-processing device able to carry out tasks that cannot be carried out by a standard universal Turing machine" [2].

Posibilidad y modelos de hipercomputación

Posibilidad:

Thesis Church-Turing: *"Any procedure than can be carried out by an idealised human clerk working mechanically with paper and pencil can also be carried out by a Turing machine"* [1].

Thesis M: *Whatever can be calculated by a machine (working on finite data in accordance with a finite program of instructions) is Turing machine computable"* [1].

Modelos:

1. Máquinas de Turing con oráculos.
2. Máquinas de Turing aceleradas.
3. Familia de circuitos booleanos no uniforme.
4. Redes neuronales recurrentes análogas.

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 $\mathbb{C}^{2^n}$:

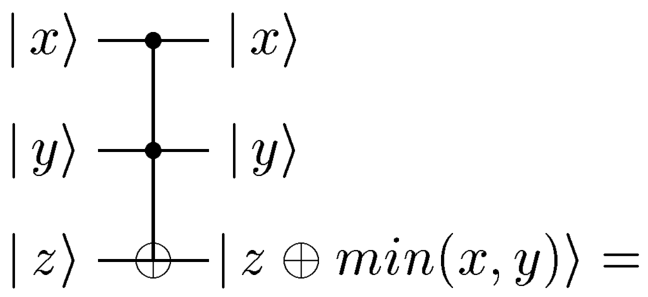
$$U^\dagger U = Id.$$

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):



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

Computabilidad y complejidad algorítmica

Computabilidad:

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

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	2.1×10^{6} años	3.4 horas
1000	4.5×10^{25} años	3.07 días

Computación cuántica adiabática (CCA)

Sea $\tilde{H}(\tau)$, $0 \leq \tau \leq 1$, una familia de hamiltonianos, tal que el hamiltoniano $H(t)$ está definido por $H(t) = \tilde{H}(\tau) = \tilde{H}(\frac{t}{T})$, donde $t = T\tau$.

$\Longrightarrow T$ controla la forma como $H(t)$ evoluciona: $\begin{cases} T \to 0 : \text{repentina}, \\ T \to \infty : \text{adiabática}. \end{cases}$

Uso del teorema adiabático (caso del estado fundamental):
Sea $H(0)\,|\,\psi(0)\rangle = E_0(0)\,|\,\psi(0)\rangle$, entonces, $H(\tau)\,|\,\psi(\tau)\rangle \approx E_0(\tau)\,|\,\psi(\tau)\rangle$, donde $\psi(\tau) = U_T(\tau)\,|\,\psi(0)\rangle$, para T suficientemente grande [3, 4].

Experimentalmente, $T \gg \frac{cte}{g^2_{min}}$ donde, $g^2_{min} = \min\limits_{0 \leq \tau \leq 1}(E_1(\tau) - E_0(\tau))$ [3, p. 3].

Computación cuántica continua (CCC)

Sea $H = (P^2 + X^2)/2$ el hamiltoniano del oscilador armónico y sean $a^\dagger = \frac{\sqrt{2}}{2}(Q - iP)$ y $a = \frac{\sqrt{2}}{2}(Q + iP)$, los operadores de creación y aniquilación respectivamente[a], donde $[Q, P] = i$ e $[a, a^\dagger] = 1$ [7].

$\Longrightarrow H = \frac{1}{2}(aa^\dagger + a^\dagger a) = N + \frac{1}{2}$, donde N el es operador número, con autovalores y autovectores dados por $N\,|\,n\rangle = n\,|\,n\rangle\,; \quad n = 0, 1, 2, \dots,$

y representación "matricial" $N = \begin{pmatrix} 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 2 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$.

[a] Óptica cuántica: $a^\dagger\,|\,n\rangle = \sqrt{n+1}\,|\,n+1\rangle$ y $a\,|\,n\rangle = \sqrt{n}\,|\,n-1\rangle$.

CCCA y problemas no Turing-computables (1)

El problema de determinar si una ecuación diofántica tiene soluciones enteras es no Turing-computable.

Tien D. Kieu ha propuesto una estrategía (29 marzo del 2002) para solucionar el anterior problema desde la CCCA [5]:

1. Asociar a la equación diofántica $D(x_1, \ldots, x_K) = 0$, el hamiltoniano $H_P = \left(D(a_1^\dagger a_1, \ldots, a_K^\dagger a_K)\right)^2$ (computación cuántica continua).

2. Determinar el estado fundamental de H_P, dado por $H_P \,|\, g\rangle = E_g \,|\, g\rangle$. Entonces, la ecuación $D(x_1, \ldots, x_K) = 0$ tiene al menos una solución entera sii $E_g = 0$.

CCCA y problemas no Turing-computables (2)

Problema: hallar el estado fundamental de H_P

Solución (computación cuántica adiabática):
$\tilde{H}\left(\frac{t}{T}\right) = \left(1 - \frac{t}{T}\right) H_I + \frac{t}{T} H_P$, donde H_I sea un hamiltoniano inicial para el cual sea fácil determinar su estado fundamental.

Sea $H_\alpha = (a^\dagger - \alpha^*)(a - \alpha)$, donde $a \,|\, \alpha\rangle = \alpha \,|\, \alpha\rangle$ y
$|\, \alpha\rangle$ (estados coherentes) $= e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \,|\, n\rangle$, entonces
$H_I = \sum_{i=1}^{K} (a_i^\dagger - \alpha_i^*)(a_i - \alpha_i)$, donde
$|\, g_I\rangle = |\, \alpha_1 \cdots \alpha_K\rangle$ es el estado fundamental de H_I.

Conclusiones

1. La estrategia de replantear un problema de computación, en un problema de hallar el estado de fundamental de algún hamiltoniano, es aplicable a una gran variedad de problemas (de decidibilidad).

2. Mientras la CC sobre espacios N-dimensionales es equipotente a la Turing-computabilidad; la CC sobre espacios ∞-dimensionales "presenta en principio" la característica de hipercomputación.

3. De los diferentes modelos de hipercomputación conocidos, el modelo sustentado sobre la CCCA, es quizás el modelo más cercano a una posible implementación.

4. En general, la CC ha abierto la puerta a una nueva y fructífera relación entra las teorías físicas contempóranes y los límites de lo computable.

[1] JACK COPELAND. The Church-Turing thesis. Stanford Encyclopedia of Philosophy. Eprint: `plato.stanford.edu/entries/church-turing/` [07-Sep-2001] (1996).

[2] JACK COPELAND Y GORDON ASTON. Hypercomputation. Eprint: `www.alanturing.net/pages/Reference\%\,20Articles/hypercomputation/` [20-Jun-2000] (2001).

[3] EDWARD FARHI ET AL. Quantum computation by adiabatic evolution. Eprint: `arXiv.org/abs/quant-ph/0001106` (2000).

[4] A. GALINDO Y P. PASCUAL. "Mecánica cuántica". Madrid: Editorial Alhambra, S.A. (1978).

[5] TIEN D. KIEU. Computing the noncomputable. Eprint: `arXiv.org/abs/quant-ph/0203034` (2002).

[6] GERT-JAN C. LOKHORST. Hypercomputation (slides). Eprint: `www.eur.nl/fw/staff/lokhorst/hypercomputation.helsinki.html` [02-Sept-2001].

[7] A. MESSIAH. "Mecánica cuántica", tomo I. Madrid: Editoral Tecnos (1973).

Agradecimientos y contacto

Agradecimientos:
A Mario Elkin Vélez y a la Universidad EAFIT.

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