Otros algoritmos: Sistema Inmunológico Artificial, Computación Cuántica, Computación Molecular

Jose Aguilar

Sistema Inmune Artificial

Sistema Inmunológico (SI)

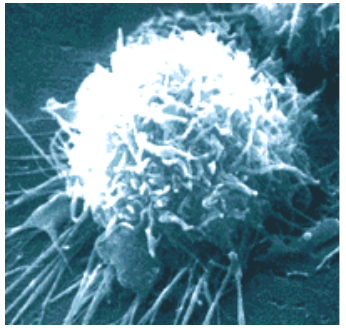
El sistema inmunológico humano — que es un sistema complejo formado por linfocitos (glóbulos blancos), anticuerpos y muchos otros componentes — ha evolucionado con el tiempo para ofrecer una protección poderosa contra toxinas y otros agentes patógenos.

Sistema Inmunológico (SI)

Sistema de defensa más importante que tiene el organismo frente a las agresiones de virus, bacterias y otras sustancias extrañas.

Reconocer las células en el cuerpo y categorizarlas como propias (self) y no propias (non-self)

GENERALIDADES DEL SISTEMA INMUNE



Agresiones del ambiente o injuria producidas por agentes patogenos

ALTERACIONES DE LA HOMEOSTASIS

SISTEMA NERVIOSO ↔ **SISTEMA INMUNE** ↔ SISTEMA ENDOCRINO

INMUNIDAD NATURAL O INESPECÍFICA

Mecanismo del organismo para protegerse antes de la infeccion (sin memoria)

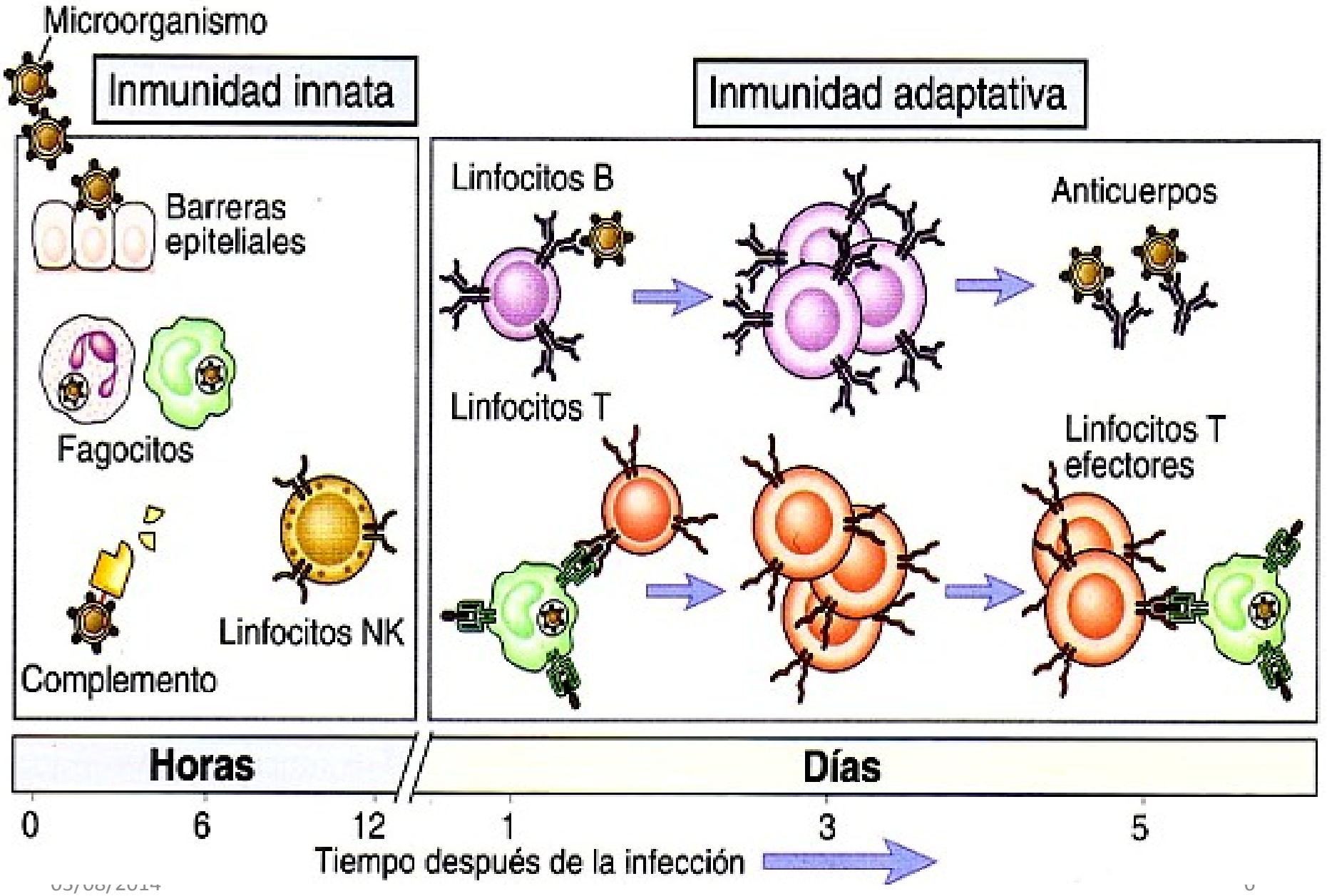
- BARRERA FÍSICA
- BARRERA QUÍMICA
- CÉLULAS FAGOCITARIAS
- PROTEÍNAS PLASMATICAS

INMUNIDAD ADAPTATIVA O ESPECIFICA

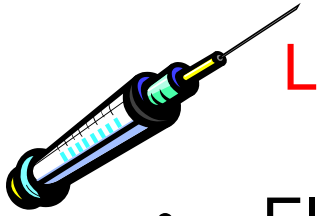
Mecanismo producidos por el cuerpo al infectarse (con memoria)

- INMUNIDAD HUMORAL ANTICUERPOS
- INMUNIDAD CELULAR LINFOCITOS

TIPOS DE INMUNIDAD



Sistema Inmunológico (SI)

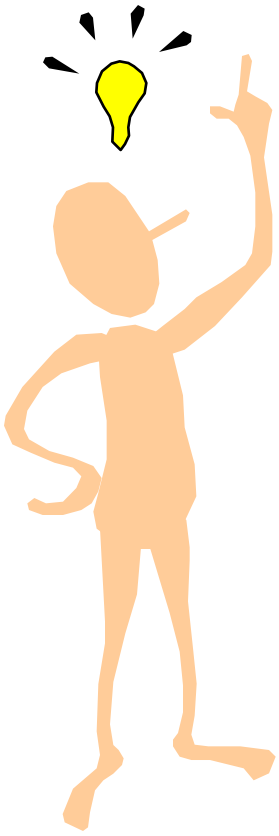


Los elementos clave de un sistema inmune muy simplificado son.

- Elementos peligrosos: proteínas llamadas antígenos.
- antígenos inocuos llamadas antígenos de uno mismo, o self-items.

- Antígenos son detectados por los linfocitos.
- Cada linfocito tiene varios anticuerpos, que pueden considerarse como detectores. Cada anticuerpo es específico para un antígeno en particular.
- Normalmente, porque la coincidencia de antígeno-anticuerpo es sólo aproximada, linfocitos no desencadenará una reacción cuando un anticuerpo solo detecta un antígeno único. Sólo después que varios anticuerpos detectan sus antígenos correspondientes los linfocitos se estimulan y desencaden algún tipo de reacción defensiva.
- No hay linfocitos con anticuerpos que detectan un self-item.
- Los anticuerpos son generados por el sistema inmune en el timo,
- Los anticuerpos que detectan self-items son destruidos antes de ser liberado (proceso llamado apoptosis).

Sistema Inmune Artificial

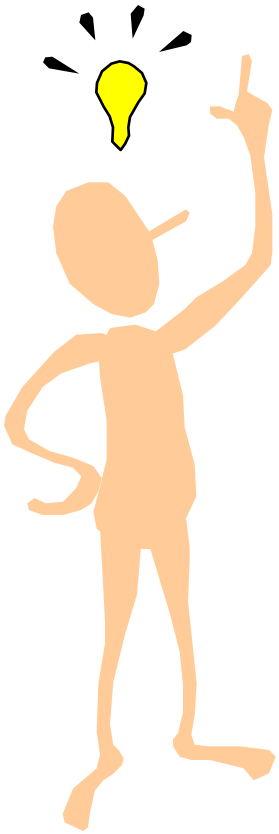


Es una abstracción de la estructura y función del sistema inmune en los sistemas computacionales,

Sistemas adaptables, inspirados en inmunología teórica

Las técnicas más comunes son inspirados por las teorías inmunológicas que explican la función y el comportamiento del sistema inmune adaptativo de los mamíferos

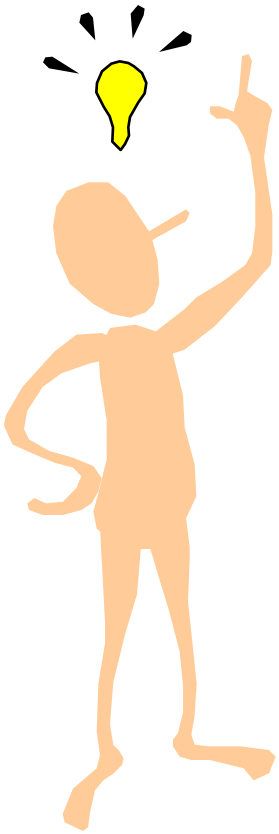
Técnicas Sistema Inmune Artificial



Algoritmo de Selección Clonal: inspirados en la teoría de la selección clonal de la inmunidad adquirida que explica cómo los linfocitos B y T mejoran su respuesta a los antígenos a través del tiempo. Estos algoritmos se aplican comúnmente en reconocimiento de patrón, y optimización

Algoritmo de selección negativa: Inspirado en los procesos de selección positivos y negativos que se producen durante la maduración de las células T en el timo llamado tolerancia de células T. La selección negativa se refiere a la identificación y eliminación de las células T en ataques. Estos algoritmos se utilizan normalmente en clasificación y reconocimiento de patrones donde se modela los conocimientos disponibles (detección de anomalías el algoritmo prepara un conjunto de detectores de patrones)

Técnicas Sistema Inmune Artificial

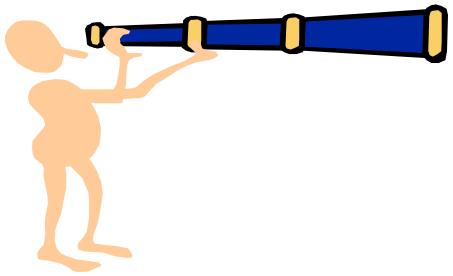


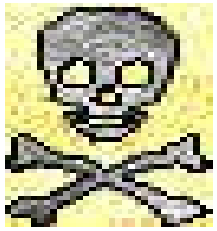
Algoritmos de redes Inmunes: Algoritmos inspirados en la teoría de la red idiotípica propuesto por Niels Kaj Jerne que describe la regulación del sistema inmune por anticuerpos anti-idiotipo (anticuerpos que seleccionan otros anticuerpos). Esta clase de algoritmos se basa en un grafo donde los anticuerpos representan los nodos y el algoritmo de entrenamiento consiste en cultivar y podar, bordes entre los nodos basados en afinidad (similitud en el espacio del problema). Se han utilizado en la agrupación, la visualización de datos, control y optimización

Algoritmos celulares Dendríticas: se basa en un modelo abstracto de las células dendríticas (DCs) (modelar diversos aspectos de las DCs), se granula en diferentes capas, logrado un procesamiento multi-escala.

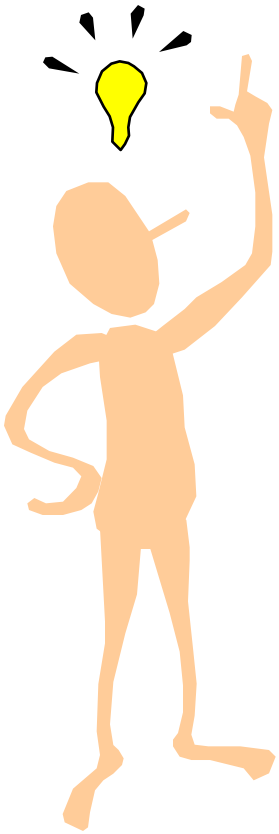
Algoritmo de selección negativa

- El Sistema Inmune usa el conjunto de lo propio (patrones de condición normal en pozos LAG) para producir detectores capaces de discriminar lo propio de lo no propio (patrones de condición anormal).





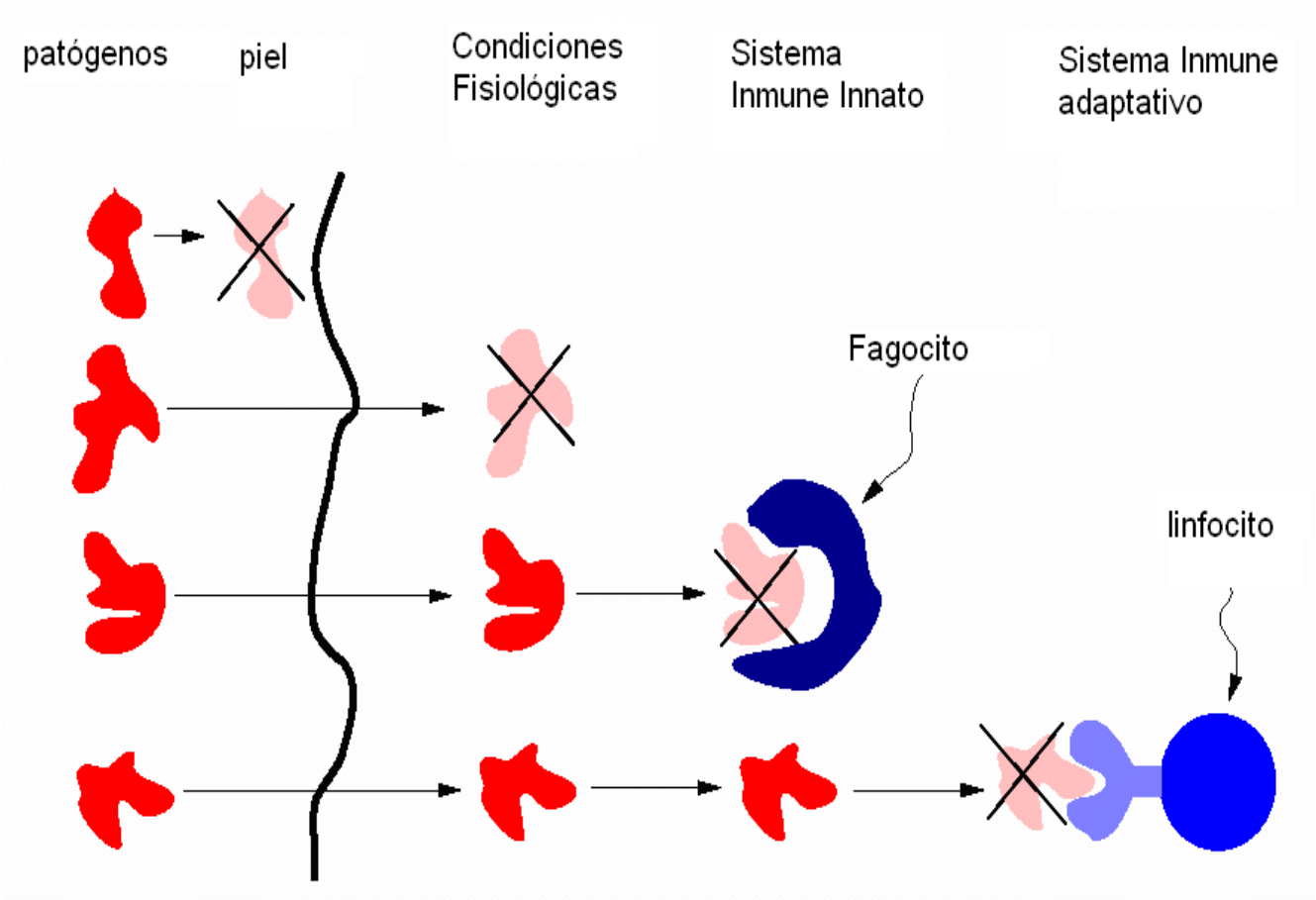
Algoritmo de selección negativa



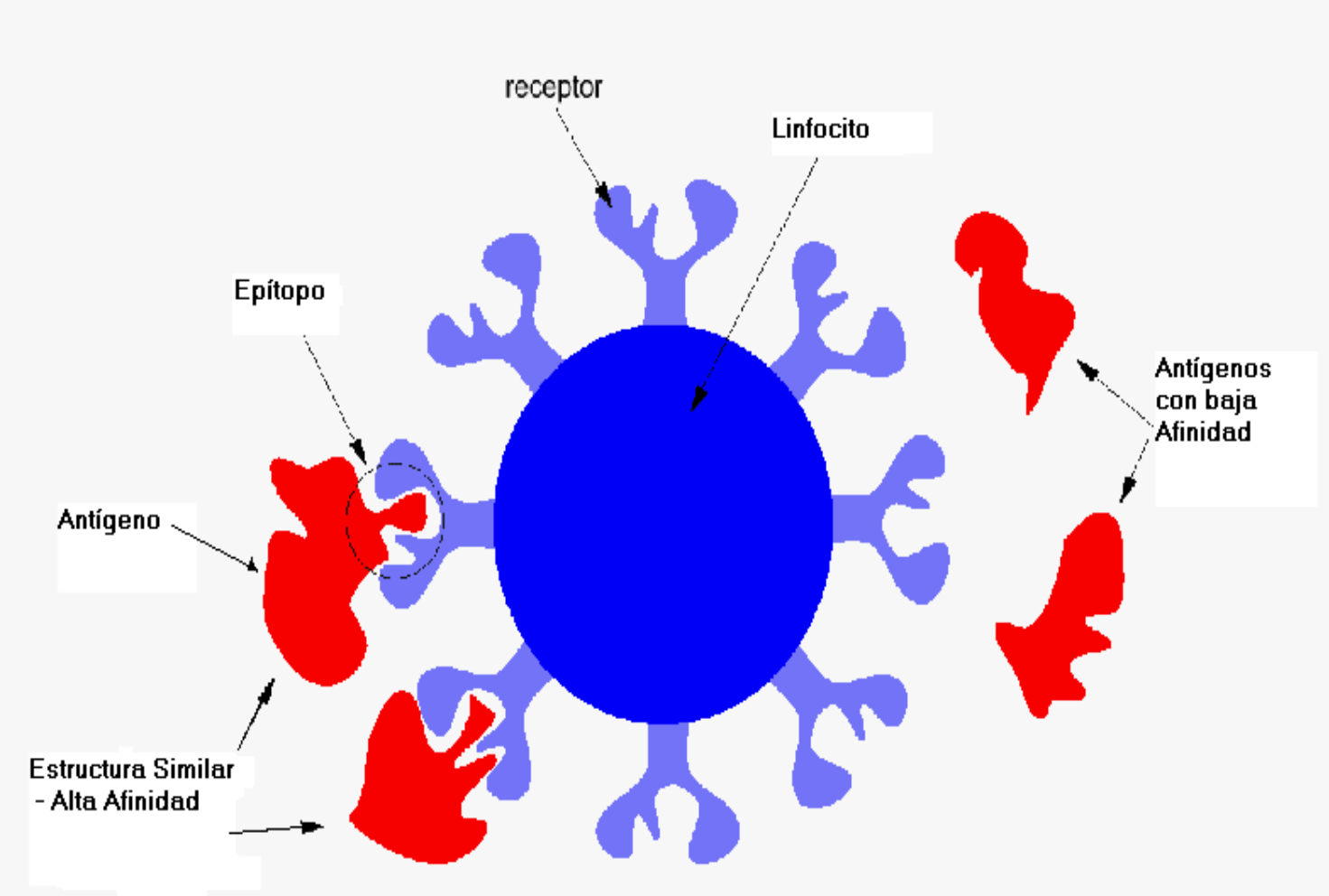
Es un modelo artificial y sencillo de la respuesta inmune que involucra los procesos llevados a cabo por el Sistema Inmune Biológico

- Mecanismo de selección negativa
- Proceso de reclutamiento de células

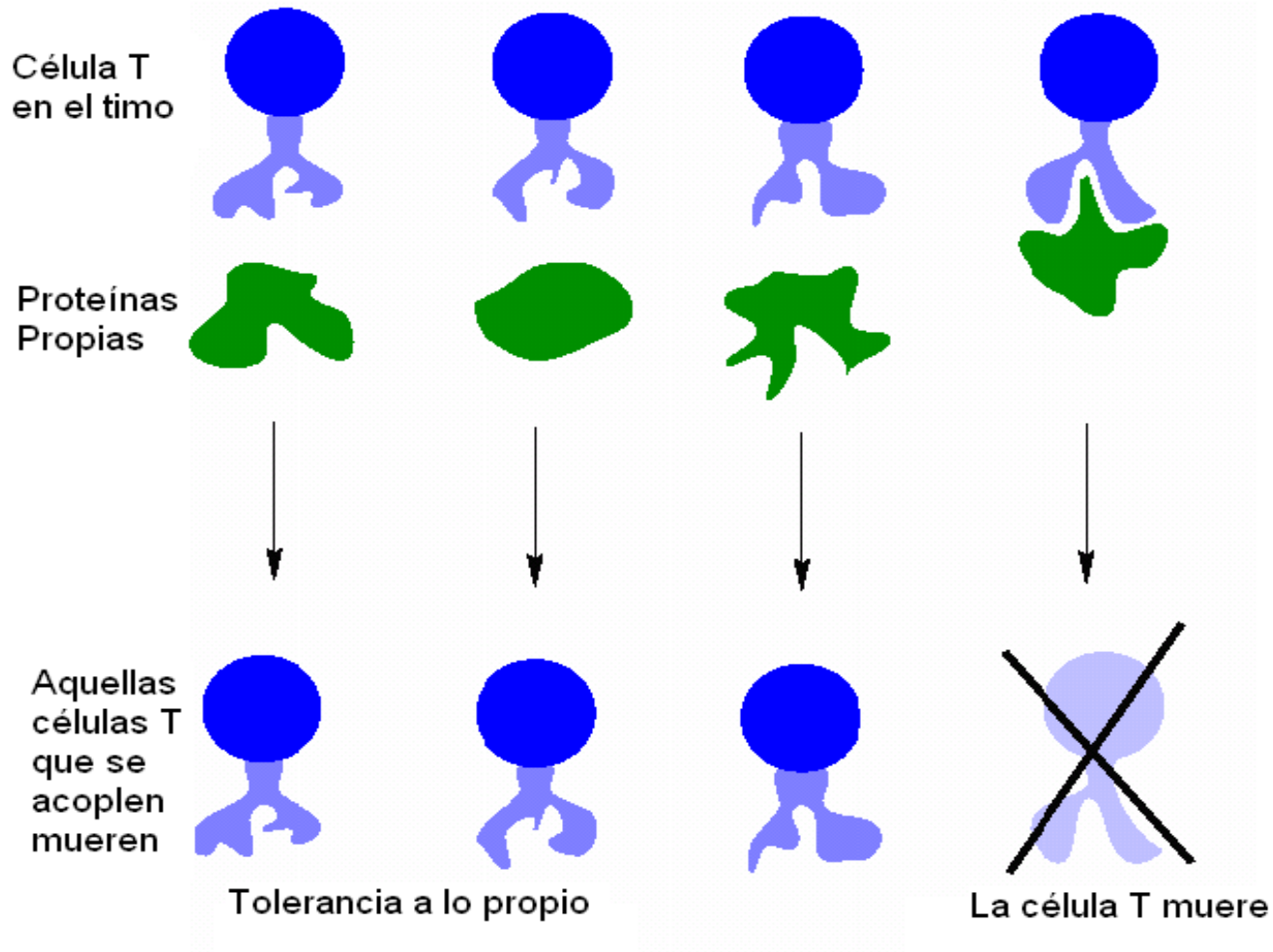
¿Cómo resuelve el SI el problema de detección?

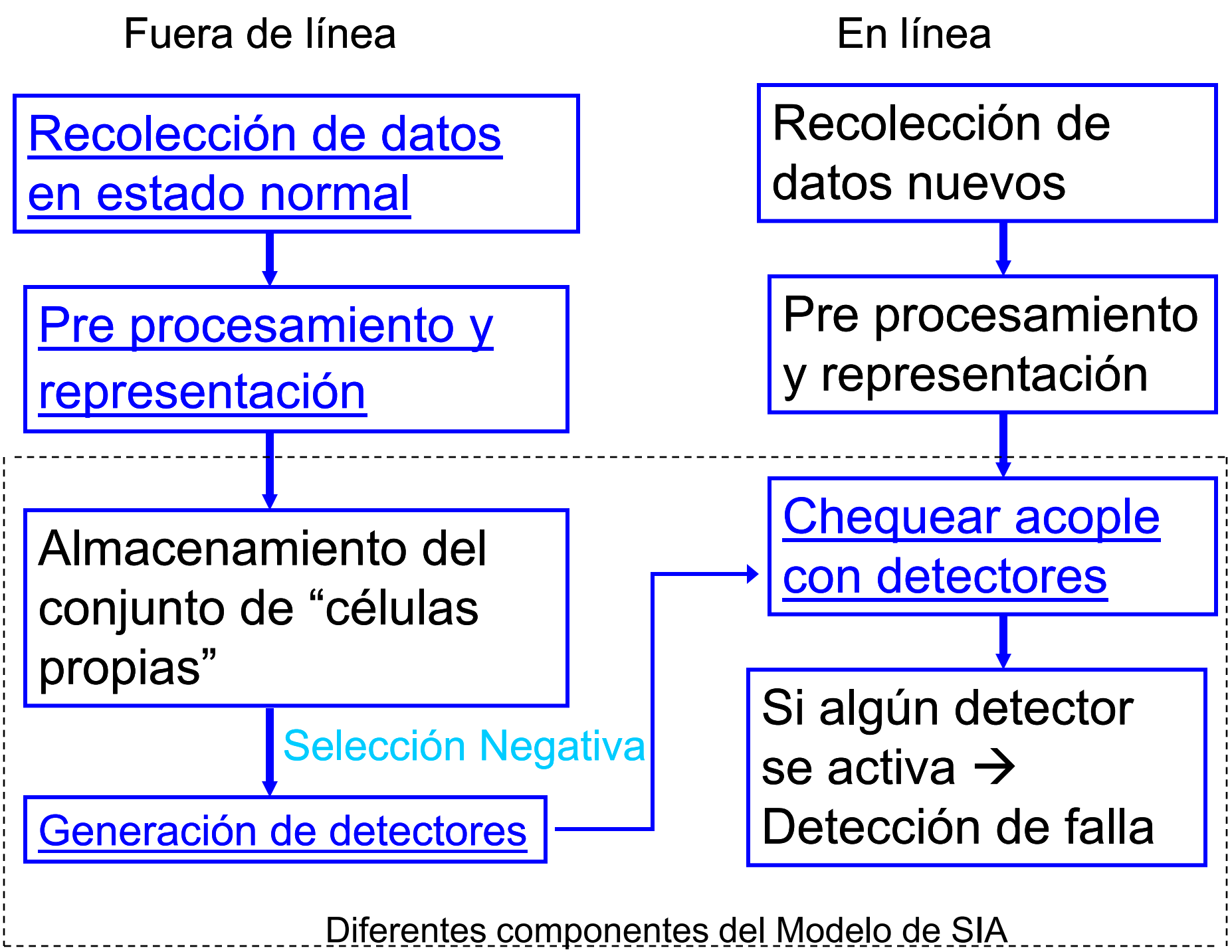


¿ Cómo detectan los linfocitos los antígenos?



Selección Negativa

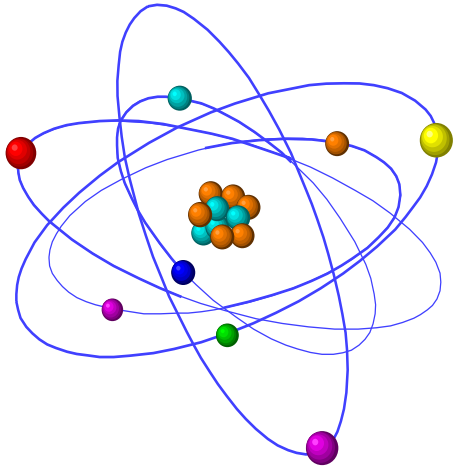



Fuera de línea
En línea
Recolección de datos en estado normal
Pre procesamiento y representación
Almacenamiento del conjunto de “células propias”
Selección Negativa
Generación de detectores
Recolección de datos nuevos
Pre procesamiento y representación
Chequear acople con detectores
Si algún detector se activa → Detección de falla
Diferentes componentes del Modelo de SIA

Conclusiones

- Aplicable a procesos de alto riesgo, donde lo importante es detectar las condiciones anormales de operación a tiempo real y sin necesidad de conocer todos los tipos de falla.
- Se generaron detectores que probabilisticamente distinguen cualquier desviación en el proceso de producción.
- Además de la cantidad, es importante la calidad de los detectores, esto es, que cubran el espacio cuasi-uniformemente.
- Mejorando la manera de generar detectores y el método de reconocimiento podrían obtenerse resultados mejores

Computación Cuántica



Basado en el curso dictado en EVI 2013 por el Dr. B. Barán

Computación Cuántica en Internet

Unos 68.500.000 accesos encontrados por Google usando las palabras claves «*Quantum Computer*»

Teleportation: Behind the Science of Quantum Computing

http://news.nationalgeographic.com/news/2013/08/130814-physics-quantum-computing-teleportation-star-trek-qubit-science/

Google's Quantum Computer Proven To Be Real Thing

http://www.wired.com/wiredenterprise/2013/06/d-wave-quantum-computer-usc/

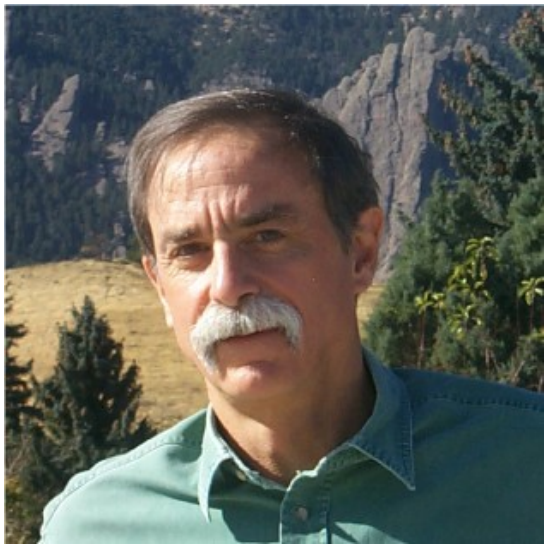
Quantum chip connected to Internet is yours to command

http://www.newscientist.com/article/dn24159-quantum-chip-connected-to-internet-is-yours-to-command.html

NASA Google Quantum Computer:
The World's Most Expensive Computer Thinks Like a Human

http://www.policymic.com/articles/46159/nasa-google-quantum-computer-the-world-s-most-expensive-computer-thinks-like-a-human

Serge Haroche y **David Wineland**
Premio Nobel de Física 2012

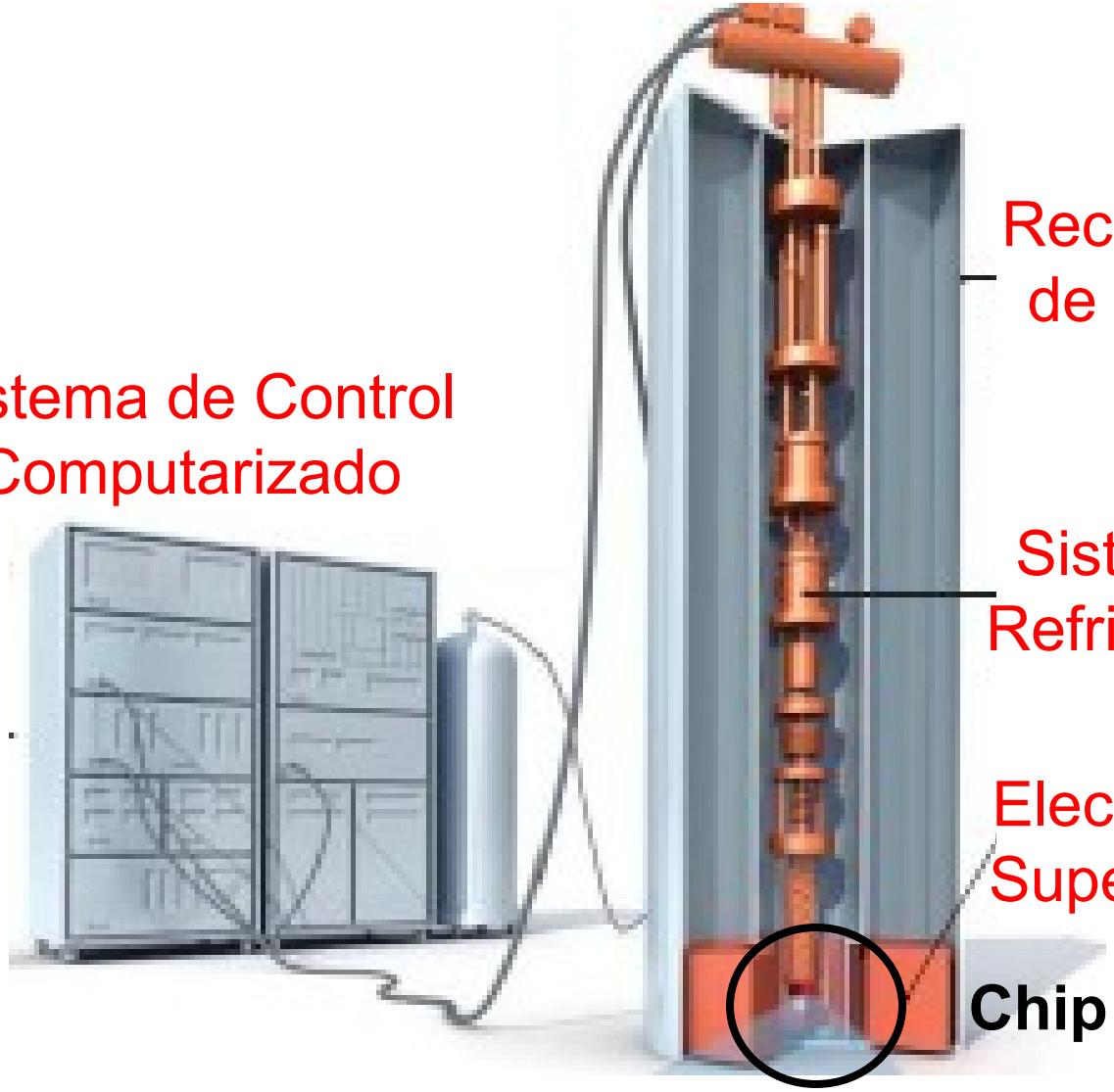


http://spectrum.ieee.org/tech-talk/computing/hardware/quantum-physicists-snatch-nobel-prize/?utm_source=techalert&utm_medium=email&utm_campaign=101112

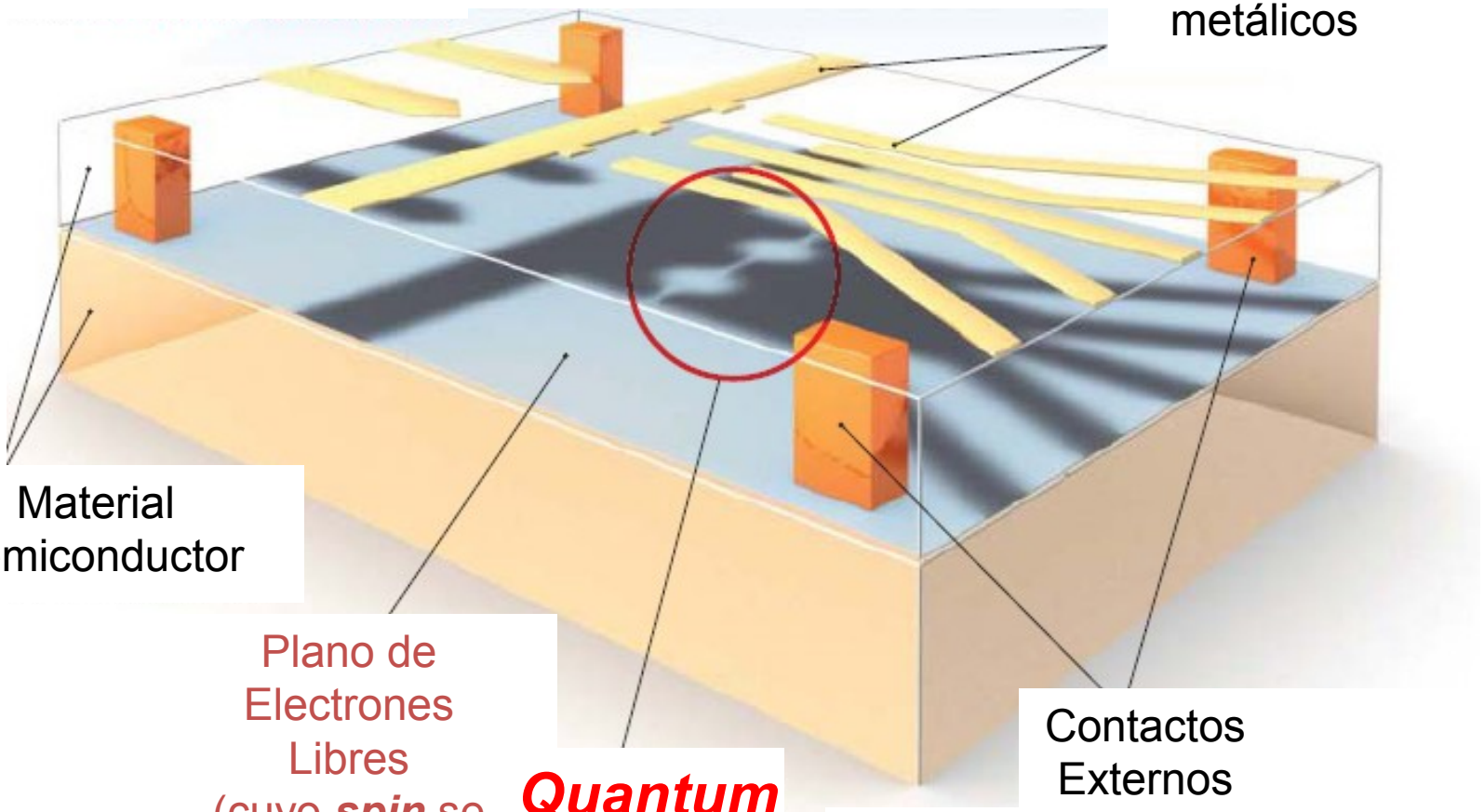
Estocolmo, (PL).- La Real Academia de Ciencia de Suecia otorgó el Premio Nobel de Física 2012 a los investigadores *Serge Haroche* de Francia y *David J. Wineland* de Estados Unidos por sus trabajos experimentales que permiten la manipulación individual de sistemas cuánticos, un paso trascendente para la ***computación cuántica*.**

Computador Cuántico

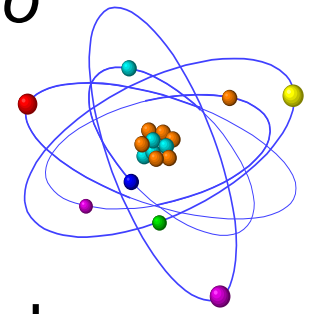
IEEE Spectrum | Septiembre 2007 | pg. 34-39



Chip Cuántico



Reseña de la Mecánica Cuántica



1900 Max Planck "*Radiación de un cuerpo negro*"

1905 Albert Einstein "*Efecto Fotoeléctrico*"

1913 Niels Bohr propone su "*modelo atómico*"

1916 R.A. Millikan mide **h**, la constante de Planck

1923 Efecto Compton (choque inelástico de fotón y electrón

1924 Louis de Broglie propone *comportamiento ondulatorio*

1927 C.J. Davisson y L.H. Germer de Bell Telephone experimentan difracción de electrones

1925 Erwin Schrödinger propone una "*Ecuación de ondas*"

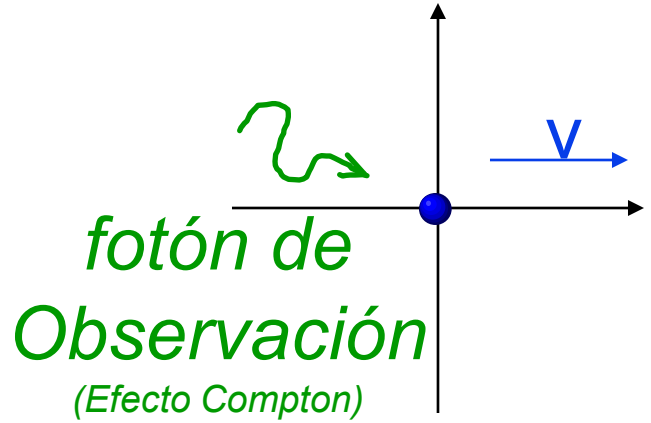
1927 Werner Heisenberg: *"Principio de la Incertidumbre"*

Principio de Incertidumbre de Heisenberg

"Al medir una partícula se modifica su estado, por lo que existe un límite hasta donde se pueden conocer simultáneamente ciertas magnitudes físicas observables."

$$\Delta p.\Delta x \gtrsim \hbar$$

$$\Delta E.\Delta t \gtrsim \hbar$$



Ecuación de Schrödinger

$$\frac{-\hbar^2}{2m}\left(\frac{\partial^2\Psi}{\partial x^2}+\frac{\partial^2\Psi}{\partial y^2}+\frac{\partial^2\Psi}{\partial z^2}\right)+V(x,y,z).\psi(x,y,z,t) = i.\hbar\frac{\partial\Psi}{\partial t}$$

$\hbar = h / 2\pi$ $\qquad$ $i = (-1)^{1/2}$

$\Psi(x,y,z,t)$ ... función (compleja) de onda

$V(x,y,z)$ ... función de energía potencial

$|\Psi(x,y,z,t)|^2$ ··· puede entenderse como la probabilidad de encontrar la partícula en estudio en las coordenadas x,y,z,t.

Principio de Superposición

"La combinación lineal de 2 soluciones, es también solución"

Estado base: $\Psi_1(x,t) = A\, e^{-i\,Et/\hbar}\, \mathrm{sen}(\pi/L)$

1° estado excitado: $\Psi_2(x,t) = A\, e^{-i\,4Et/\hbar}\, \mathrm{sen}(2\pi/L)$

Luego, también será solución la superposición de estos 2 estados:

$$\Psi(x,t) = \alpha\, \Psi_1(x,t) + \beta\, \Psi_2(x,t) \; ; \quad \text{con} \quad |\alpha|^2 + |\beta|^2 = 1$$

posible **QUBIT** en computación cuántica

Superposición Generalizada

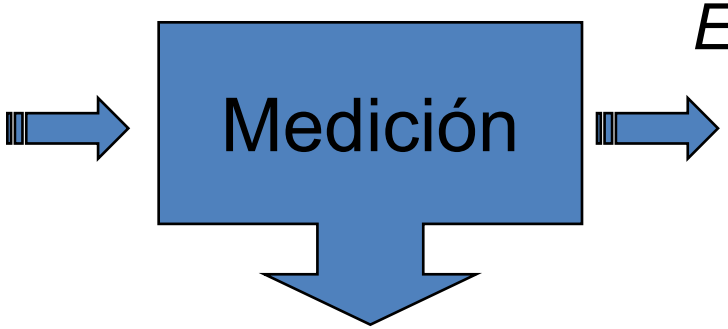
"La combinación lineal de *n* soluciones, es también solución"

$$\Psi(x,t) = \sum_n c_n \Psi_n(x,t) \qquad \sum_n |c_n|^2 = 1$$

Notación vectorial: vector de estado normalizado $|\Psi\rangle$

[FÍSICA. Seis ideas fundamentales, T.A. Moore. Mc Graw Hill 2005. ISBN 970-10-4895-4]

$$|\Psi\rangle = \begin{pmatrix} \Psi_1 \\ \vdots \\ \Psi_n \end{pmatrix}$$



Eigenvector k

$|\Psi_k\rangle$

Observable *k*

Eigenvalue k

Quantum Bit - **QUBIT**

$\Psi(x,t) = \alpha\,\Psi_0(x,t) + \beta\,\Psi_1(x,t)$ con $|\alpha|^2 + |\beta|^2 = 1$

Notación KET
(Notación de Dirac)

$$|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \Rightarrow \boxed{\text{Medición}} \Rightarrow |1\rangle$$

Eigenvector k

Se observa $|1\rangle$ con probabilidad $|\beta|^2$

No Cloning Theorem ⟼ Stephen Wiesner propone e
Dinero Cuántico en los 70's

Reseña de la computación cuántica

1936 Alan Turing propone la *Máquina de Turing*.

1948 Claude Shannon desarrolla la *Teoría de la Información.*

1982 Richard Feynman propone el *Computar Cuántico.*

1984 Charles Bennett y Gilles Brassard proponen un sistema de Distribución de Claves (BB84) basado en la Cuántica.

1985 David Deutsch conceptualiza el *Computador Cuántico*.

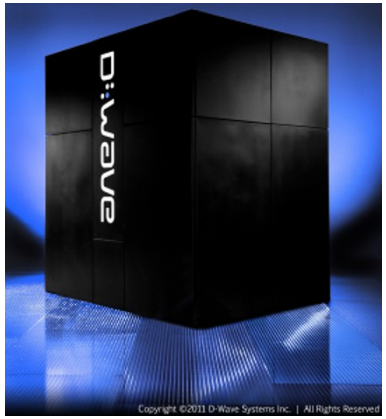
1992 Charles Bennett y Stephan Wiesner, *Código Superdenso.*

1994 Peter Shor demuestra como encontrar factores primos y calcular logaritmos discretos *(se rompería la seguridad del RSA).*

1995 Ben Schumacher define el QUBIT, iniciándose el interés en la *Teoría de la Información Cuántica.*

1995 Lov Grover propone un algoritmo rápido para búsqueda en bases no estructuradas de datos.

Reseña de los computadores cuánticos



1998 **D. Loss (Bassel Univ. - Suiza) & D. DiVincenzo (IBM) proponen los Puntos Cuánticos (*Quantum Dots)* usando *spin* de electrones.**

2001 **L. Vandersypen et al. factoriza número 15. Proyecto de Standfor University e IBM.**

2004 **L. Vandersypen et al. proponen métodos indirectos para medir *spin* de electrones individuales.**

2005 **C. Marcus de Harvard University, logra controlar experimentalmente *spin swap* cuánticos.**

2006 **L. Vandersypen et al., logran controlar el *spin*.**

2011 **La empresa D-Wave anuncia el "*D-wave One*," primer computador cuántico comercial.**

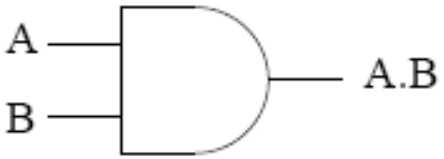
2013 ***Google* compra computador cuántico de empresa *D-wave*.**

Ejemplo de Circuitos

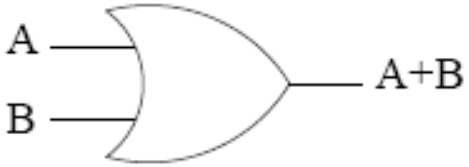
Clásicos

NOT

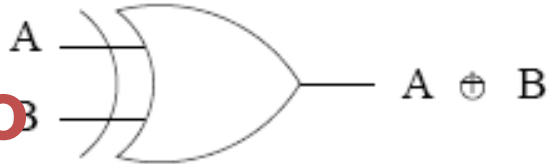
AND



OR

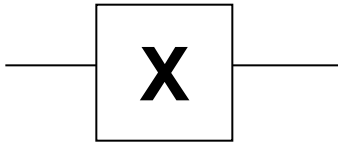


OR exclusivo

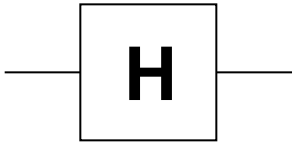


Cuánticos

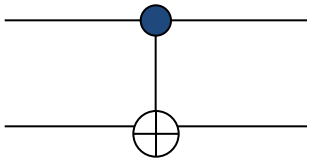
Pauli X



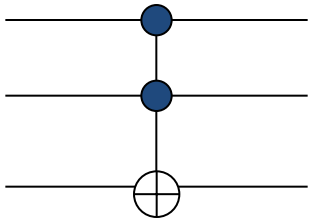
Hadamard



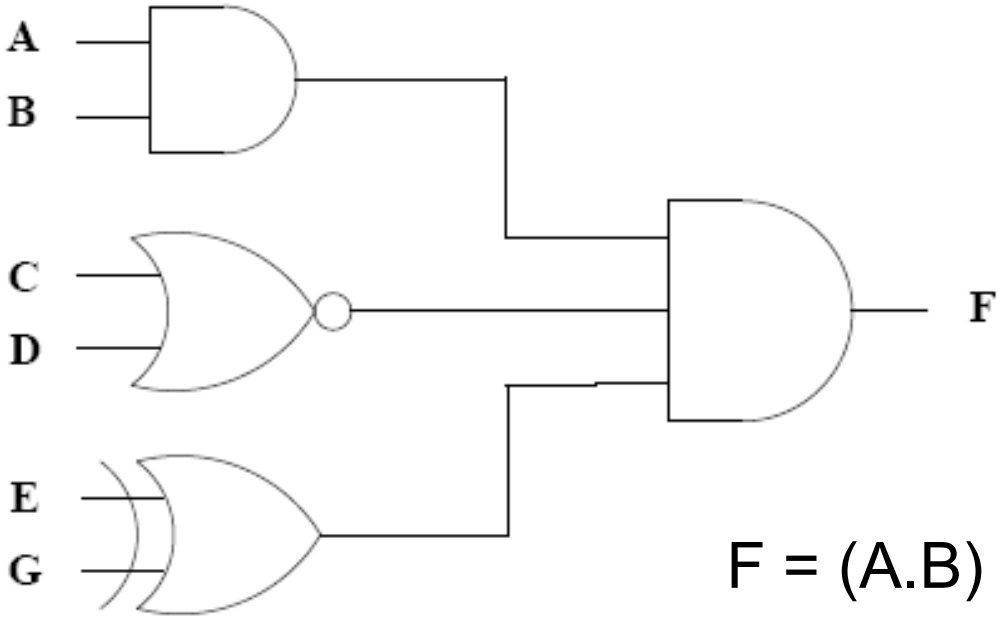
Controlled NOT



Toffoli



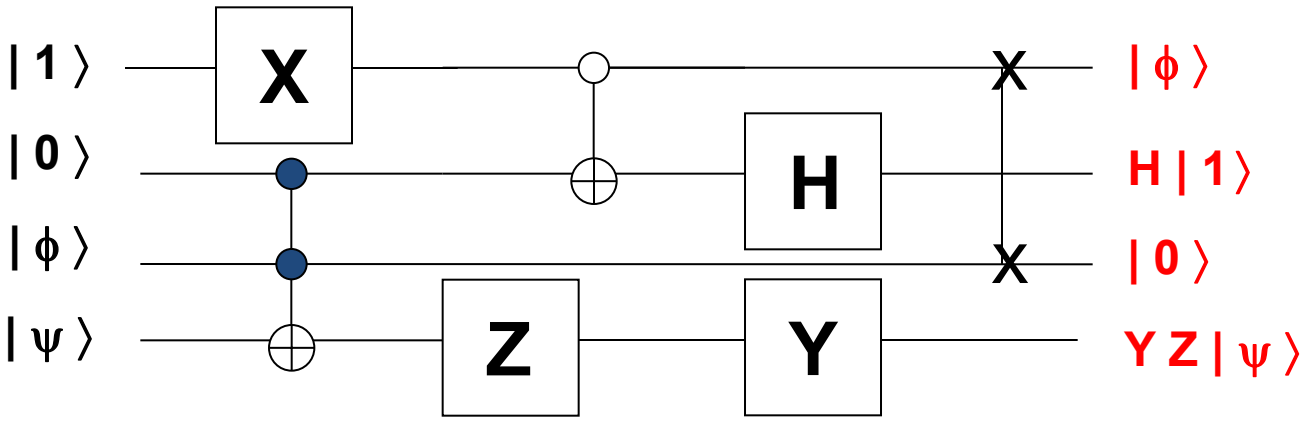
Ejemplo de un Circuito Clásico



$$F = (A.B) . \overline{(C + D)} . (E \oplus G)$$

Circuitos clásicos son estudiados con el **Álgebra de Boole**

Ejemplo de un Circuito Cuántico



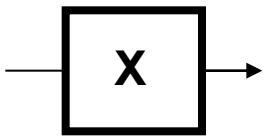
Circuitos cuánticos son estudiados con el

Álgebra Tensorial en un espacio de Hilbert

Los circuitos cuánticos se diseñan REVERSIBLES

Circuitos Cuánticos como Operadores Lineales

Pauli **X**



(circuito negador)

$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Ejemplos

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \xrightarrow{\mathbf{X}} X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \xrightarrow{\mathbf{X}} X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

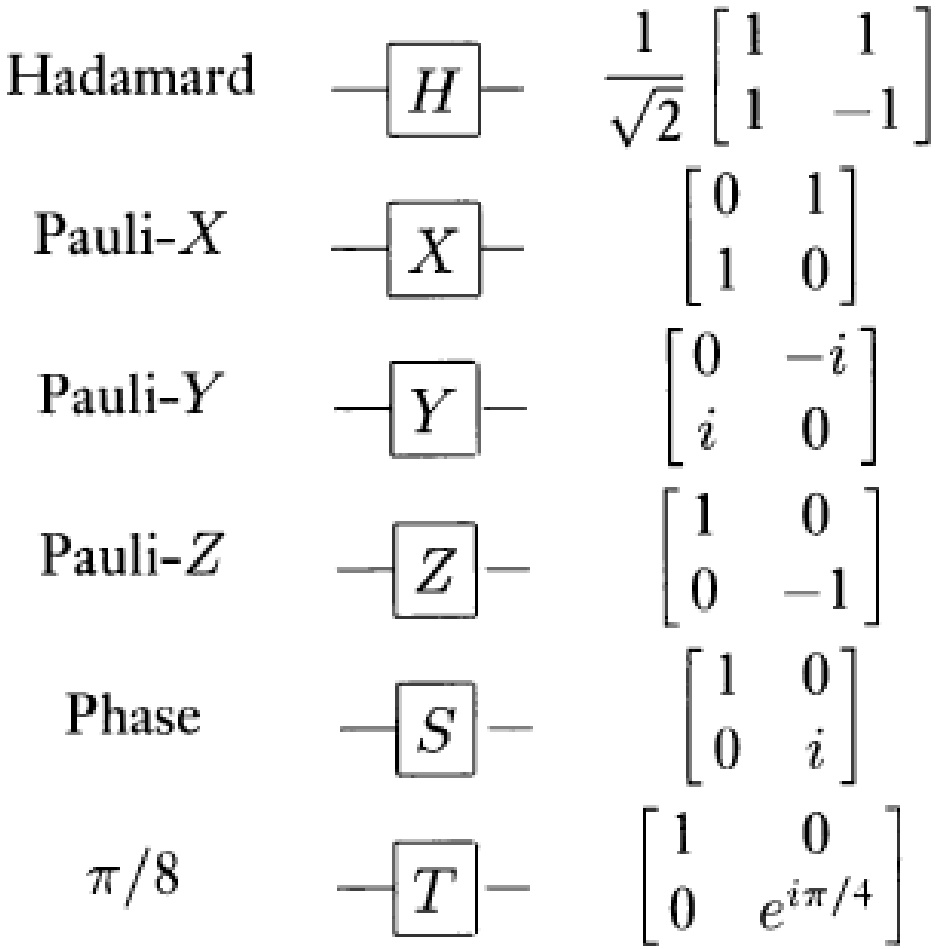
Producto Tensorial

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

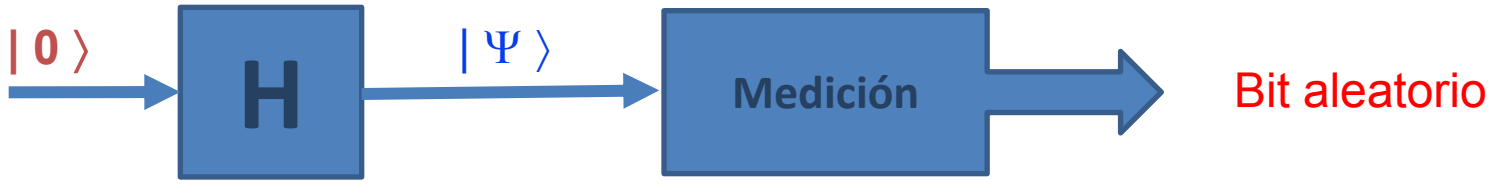
$$|010\rangle = |0\rangle \otimes |10\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

n QUBITS se representan con un vector de dimensión 2^n

Representación Matricial de Circuitos operando sobre un único QUBIT



Generador de Números Aleatorios usando compuerta Hadamard



$$| \Psi \rangle = H | 0 \rangle = (1 / \sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

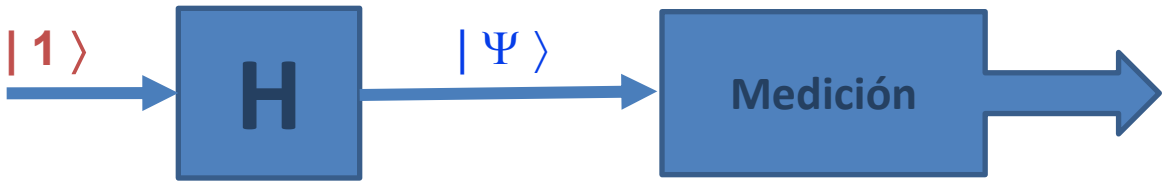
$$| \Psi \rangle = (1 / \sqrt{2}) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = (1 / \sqrt{2}) \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (1 / \sqrt{2}) \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$| \Psi \rangle = (| 0 \rangle + | 1 \rangle) / \sqrt{2}$$

Quantum Card

PCI Express

Compuerta Hadamark



Bit aleatorio

$$| \Psi \rangle = H | 1 \rangle = (1 / \sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$H | 1 \rangle = (1 / \sqrt{2}) \begin{pmatrix} 1 \\ -1 \end{pmatrix} = (1 / \sqrt{2}) \begin{pmatrix} 1 \\ 0 \end{pmatrix} - (1 / \sqrt{2}) \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$H | 1 \rangle = (| 0 \rangle - | 1 \rangle) / \sqrt{2}$$

mientras que

$$H | 0 \rangle = (| 0 \rangle + | 1 \rangle) / \sqrt{2}$$

Circuitos operando sobre 2 QUBITs

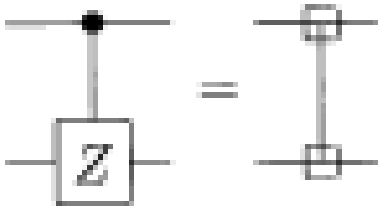
controlled-NOT

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

swap

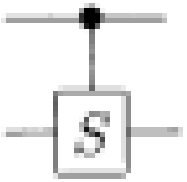
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

controlled-Z



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

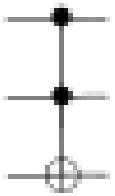
controlled-phase



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

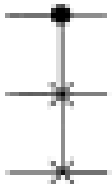
Circuitos operando sobre 3 QUBITs

Toffoli



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

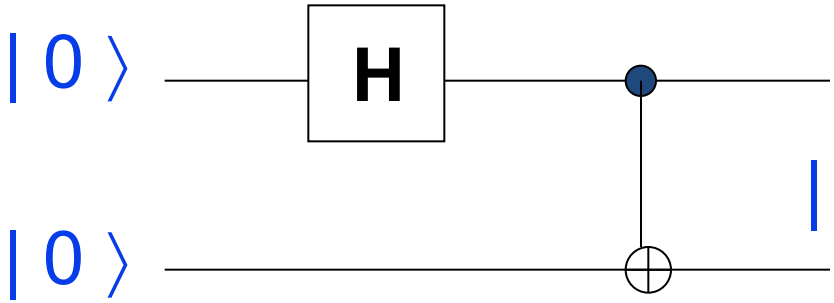
Fredkin (controlled-swap)



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

Bell-state

Paradoja EPR (Einstein, Podolsky, Rosen - 1935)

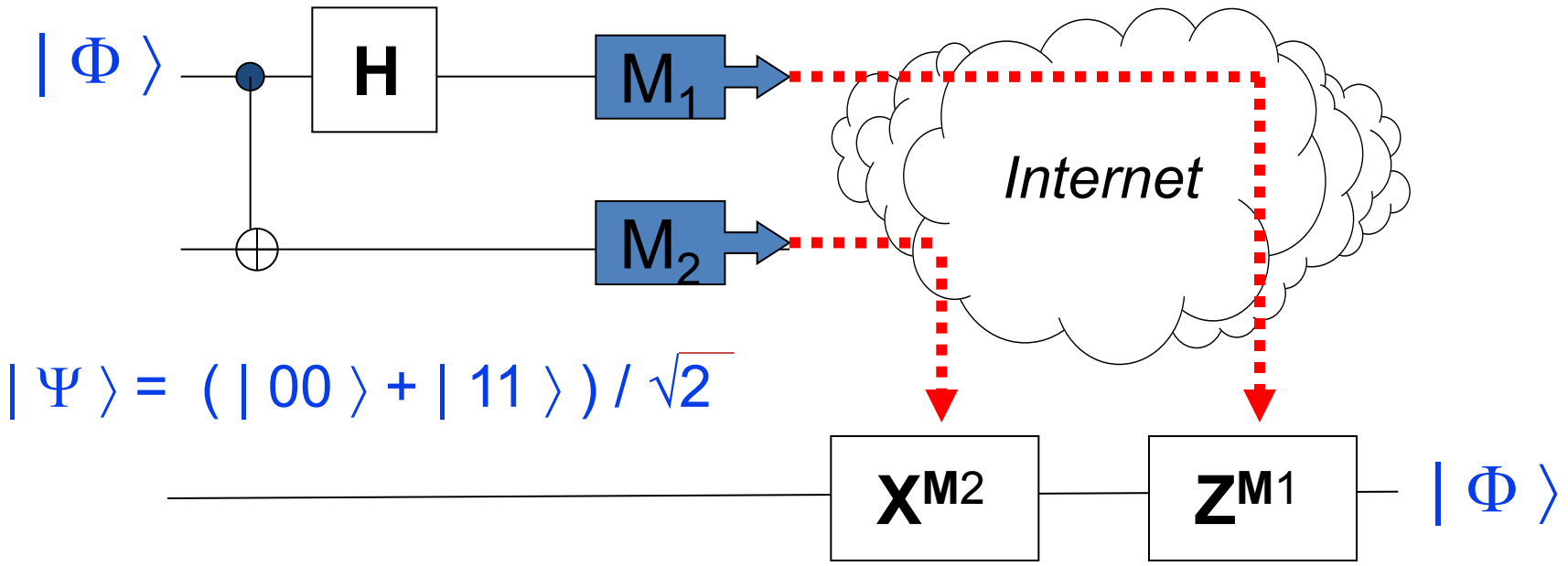


$$| \Psi \rangle = (| 00 \rangle + | 11 \rangle) / \sqrt{2}$$

El estado de un Qubit depende del otro Qubit y ninguno tiene un estado individual propio. Cada Qubit da una probabilidad de ½ de medir un |0⟩ o un |1⟩, pero realizada una medición, el otro Qubit "*se entera*" y mide el mismo valor.

Los 2 Qubits quedan enmarañados (*entangled Qubits*) y se los conoce como en la literatura como par EPR.

Tele-transportación Cuántica



- Se crea un par EPR. El transmisor se queda con un *entangled Qubit* y el receptor lleva el otro *entangled Qubit* (por ejemplo, a otra galaxia).
- Un Qubit desconocido $|\Phi\rangle$ puede ser tele-transportado, aplicando compuertas c-NOT y H, seguidos de mediciones (ver figura).
- Si el resultado de las mediciones es transmitido al receptor (por ejemplo por Internet), este puede reconstruir $|\Phi\rangle$ usando el *entangled Qubit* que él posee.

Tele-transportación Cuántica

Demostración

Qubit a tele-transportar: $|\Phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

Entrada: $|\Psi_0\rangle = [\ \alpha|0\rangle\ (|00\rangle + |11\rangle) + \beta|1\rangle\ (|00\rangle + |11\rangle)\ ] / \sqrt{2}$

c-NOT: $$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

Hadamard (H): $$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle\ (\alpha|0\rangle + \beta|1\rangle) + |01\rangle\ (\alpha|1\rangle + \beta|0\rangle) + |10\rangle\ (\alpha|0\rangle - \beta|1\rangle) + |11\rangle\ (\alpha|1\rangle - \beta|0\rangle)\right]$$

Mediciones M_1 y M_2:

$$00 \longmapsto |\psi_3(00)\rangle \equiv \left[\alpha|0\rangle + \beta|1\rangle\right] = |\Phi\rangle$$

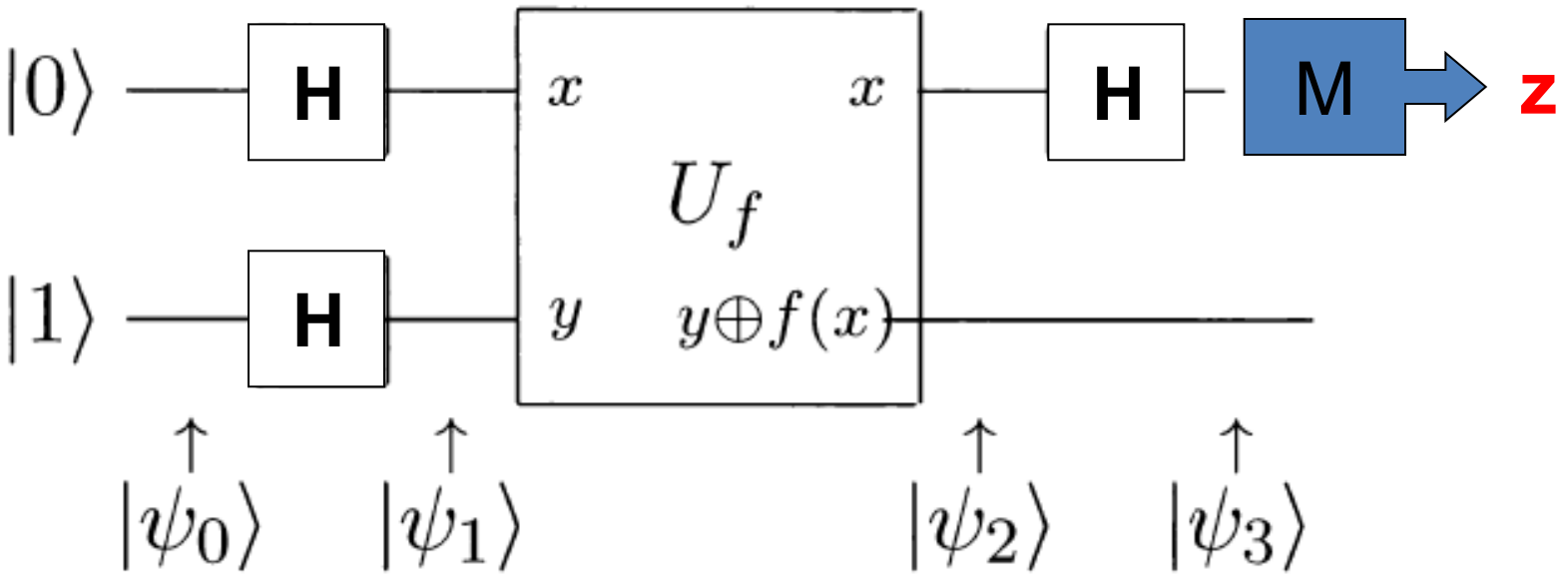
$$01 \longmapsto |\psi_3(01)\rangle \equiv \left[\alpha|1\rangle + \beta|0\rangle\right] \xrightarrow{X} = |\Phi\rangle$$

$$10 \longmapsto |\psi_3(10)\rangle \equiv \left[\alpha|0\rangle - \beta|1\rangle\right] \xrightarrow{Z} = |\Phi\rangle$$

$$11 \longmapsto |\psi_3(11)\rangle \equiv \left[\alpha|1\rangle - \beta|0\rangle\right] \xrightarrow{XZ} = |\Phi\rangle$$

Deutsch's Algorithm

Dada una función binaria f(x) que puede calcularse con un circuito cuántico U_f, el algoritmo calcula en una única evaluación **z** = f(0) ⊕ f(1)



Paralelismo cuántico – Interferencia.

Deutsch's Algorithm

Demostración

$$|\psi_0\rangle = |01\rangle$$

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) = f(1) \\ \pm|1\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] & \text{if } f(0) \neq f(1). \end{cases}$$

… y al medir el primer Qubit, se obtiene el resultado esperado.

El problema de Bernstein-Vazirani

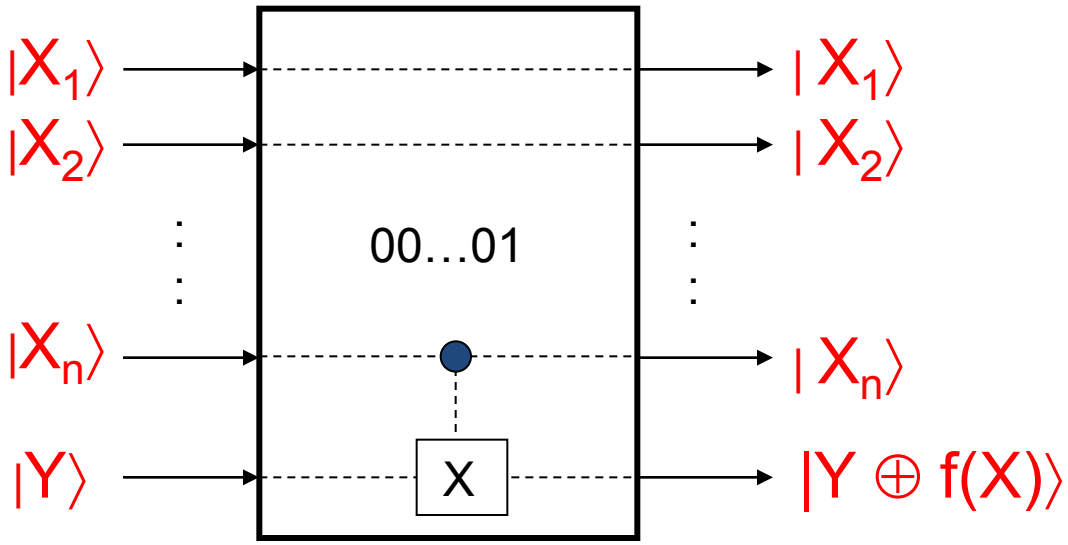
Conocidos n bits de entrada $X = [X_1, X_2, \ldots X_n]$, $X_i \in \{0,1\}$

y un vector incógnita $A = [A_1, A_2, \ldots A_n]$, $A_i \in \{0,1\}$

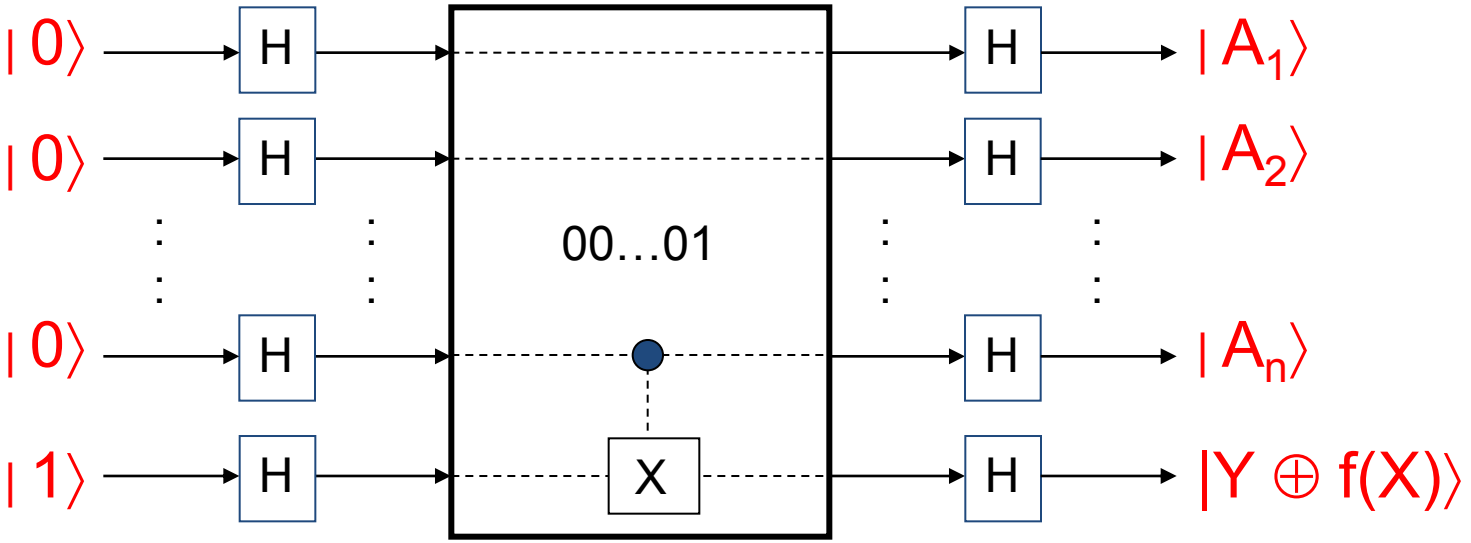
Dada una función $f(X) = \sum_{\oplus} A_i X_i = A_1X_1 \oplus A_2X_2 \oplus \ldots \oplus A_nX_n$

¿En cuantas consultas a f(X) se puede conocer A?

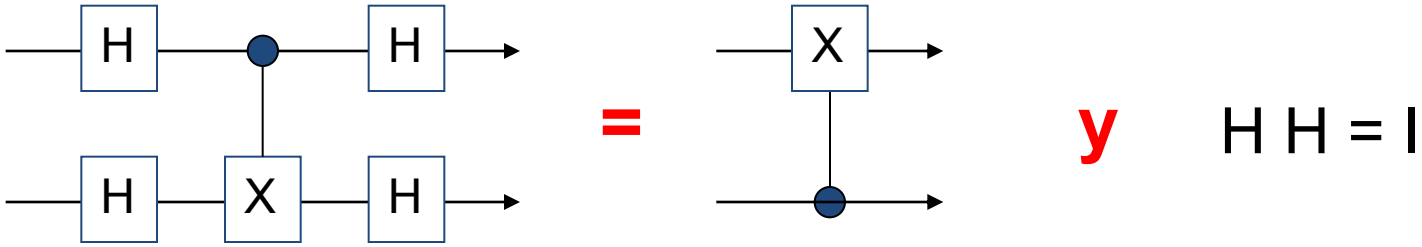
Con un computador clásico, se requieren *n* consultas



Con un computador cuántico, es suficiente con una *sola* consulta !!!



Para este simple ejemplo, esto se demuestra con la identidad:



y H H = I

Transformada Discreta de Fourier

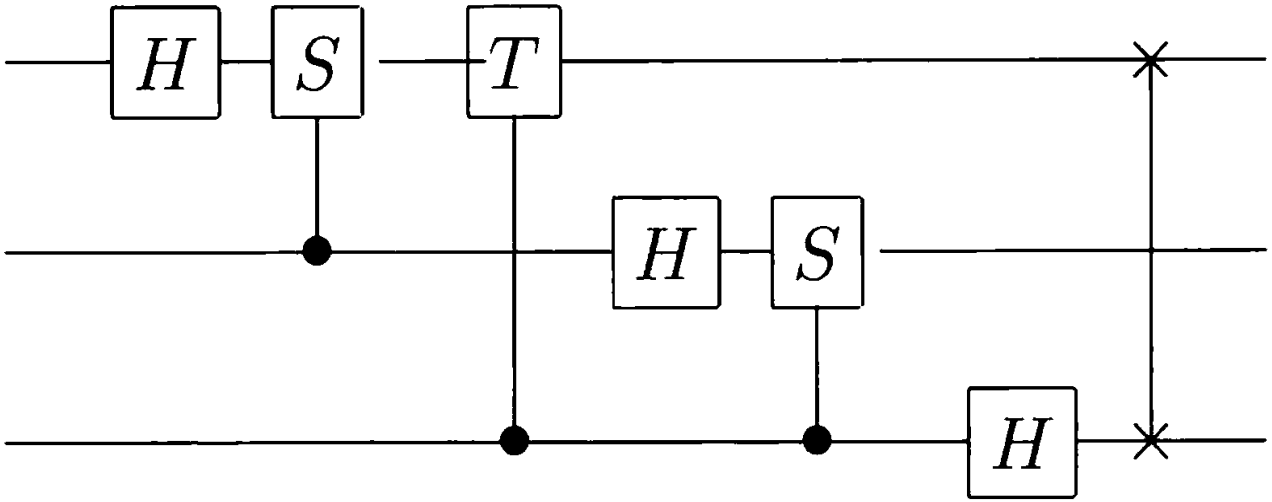
Definición clásica: $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} x_j$; generalmente, N = 2^n

Equivalente cuántico: $|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle$

... y por superposición: $\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i j k/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle$

Calcular una transformada rápida de Fourier en un computador clásico tiene una complejidad de **O**($n2^n$), mientras un computador cuántico lo tiene con complejidad **O**(n^2). **Ahorro exponencial!**

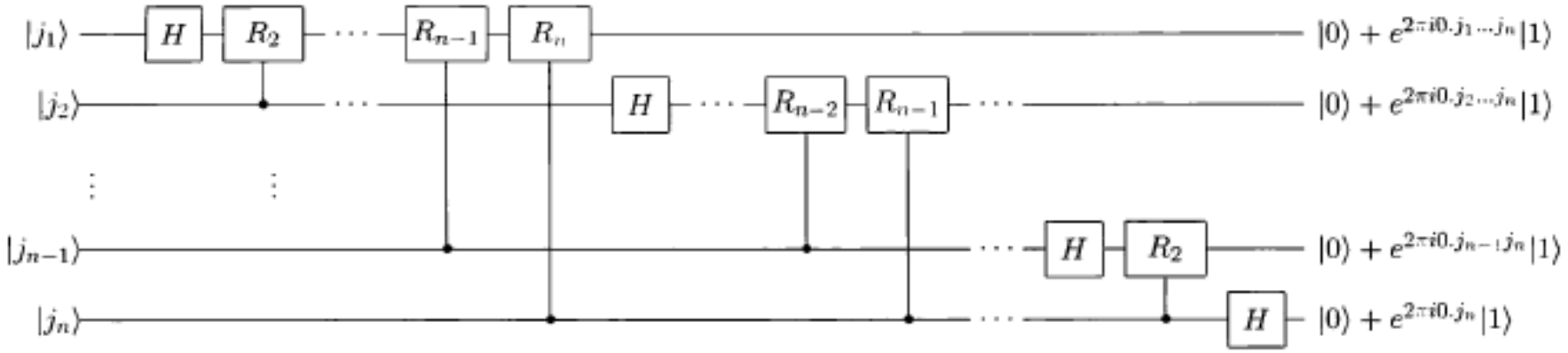
Transformada Cuántica de Fourier para 3 qubits



$$\omega = e^{2\pi i/8} = \sqrt{i},$$

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

Transformada Cuántica de Fourier



con $R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$

Complejidad

La complejidad C está dada por el número de circuitos cuánticos. En este caso, por la serie aritmética:

C = n + (n - 1) + ….. + 2 + 1 = n (n – 1) / 2 ~ **O**(n^2)

(2) Algorithm: Quantum order-finding

Inputs: (1) A black box $U_{x,N}$ which performs the transformation $|j\rangle|k\rangle \rightarrow |j\rangle|x^j k \bmod N\rangle$, for x co-prime to the L-bit number N, (2) $t = 2L + 1 + \lceil \log\left(2 + \frac{1}{2\epsilon}\right) \rceil$ qubits initialized to $|0\rangle$, and (3) L qubits initialized to the state $|1\rangle$.

Outputs: The least integer $r > 0$ such that $x^r = 1 \pmod N$.

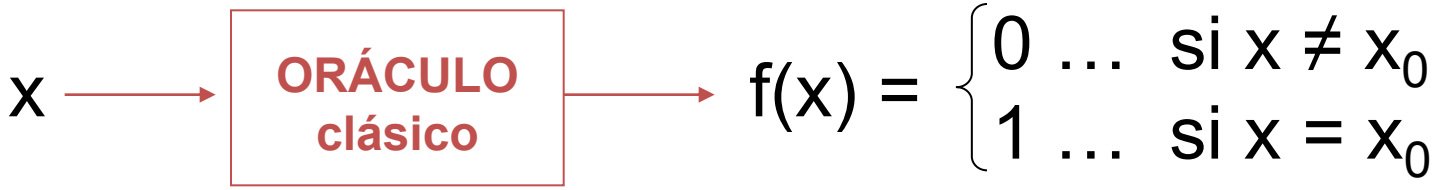
Runtime: $O(L^3)$ operations. Succeeds with probability $O(1)$.

Procedure:

1.	$\|0\rangle\|1\rangle$	initial state
2.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|1\rangle$	create superposition
3.	$\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \|j\rangle\|x^j \bmod N\rangle$	apply $U_{x,N}$
	$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} \|j\rangle\|u_s\rangle$	
4.	$\rightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \|\widetilde{s/r}\rangle\|u_s\rangle$	apply inverse Fourier transform to first register
5.	$\rightarrow \widetilde{s/r}$	measure first register
6.	$\rightarrow r$	apply continued fractions algorithm

Algoritmo de Búsqueda

(Ejemplo: números de una Guía Telefónica ordenada por apellidos)



¿Cuántas consultas a un Oráculo se necesita para encontrar X_0?

Se necesitan probar al menos N/2 entradas para tener prob. = ½ de encontrar x_0.

Complejidad de la búsqueda: O(N)

Ejemplo para N = 4

Algoritmo de Grover para Búsqueda Cuántica

Encuentra la solución en O($\sqrt{N}$) consultas al oráculo !

Algorithm: Quantum search

Inputs: (1) a black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$, where $f(x) = 0$ for all $0 \leq x < 2^n$ except x_0, for which $f(x_0) = 1$; (2) $n + 1$ qubits in the state $|0\rangle$.

Outputs: x_0.

Runtime: $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$.

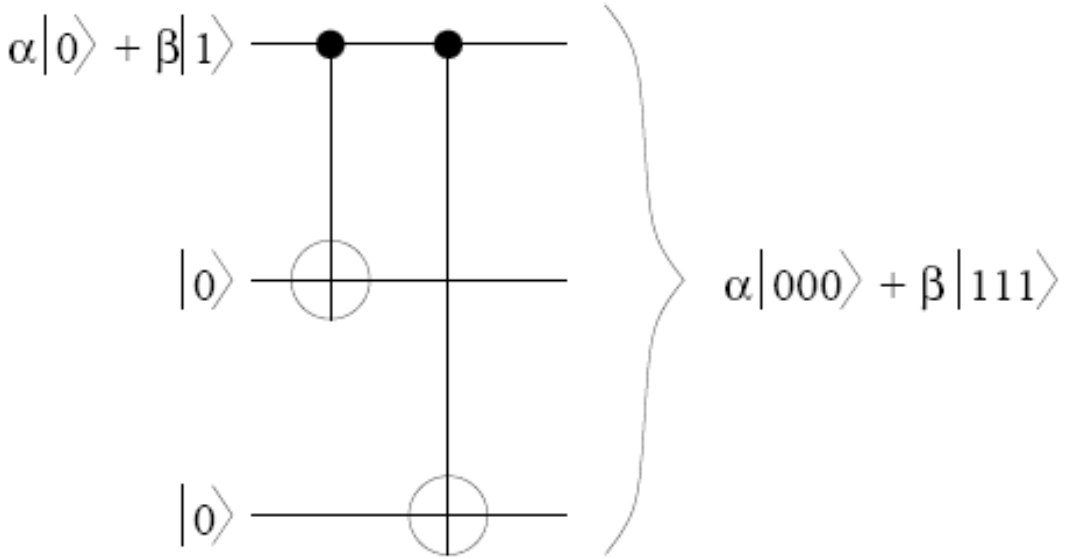
Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$ — initial state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — apply $H^{\otimes n}$ to the first n qubits, and HX to the last qubit
3. $\rightarrow \left[Q|\psi\rangle\langle\psi| - I)O\right]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$ — apply the Grover iteration $R \approx \lfloor \pi\sqrt{2^n}/4 \rfloor$ times.

   $\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$
4. $\rightarrow x_0$ — measure the first n qubits

Códigos Correctores de Errores

Un codificador sencillo para corregir un error

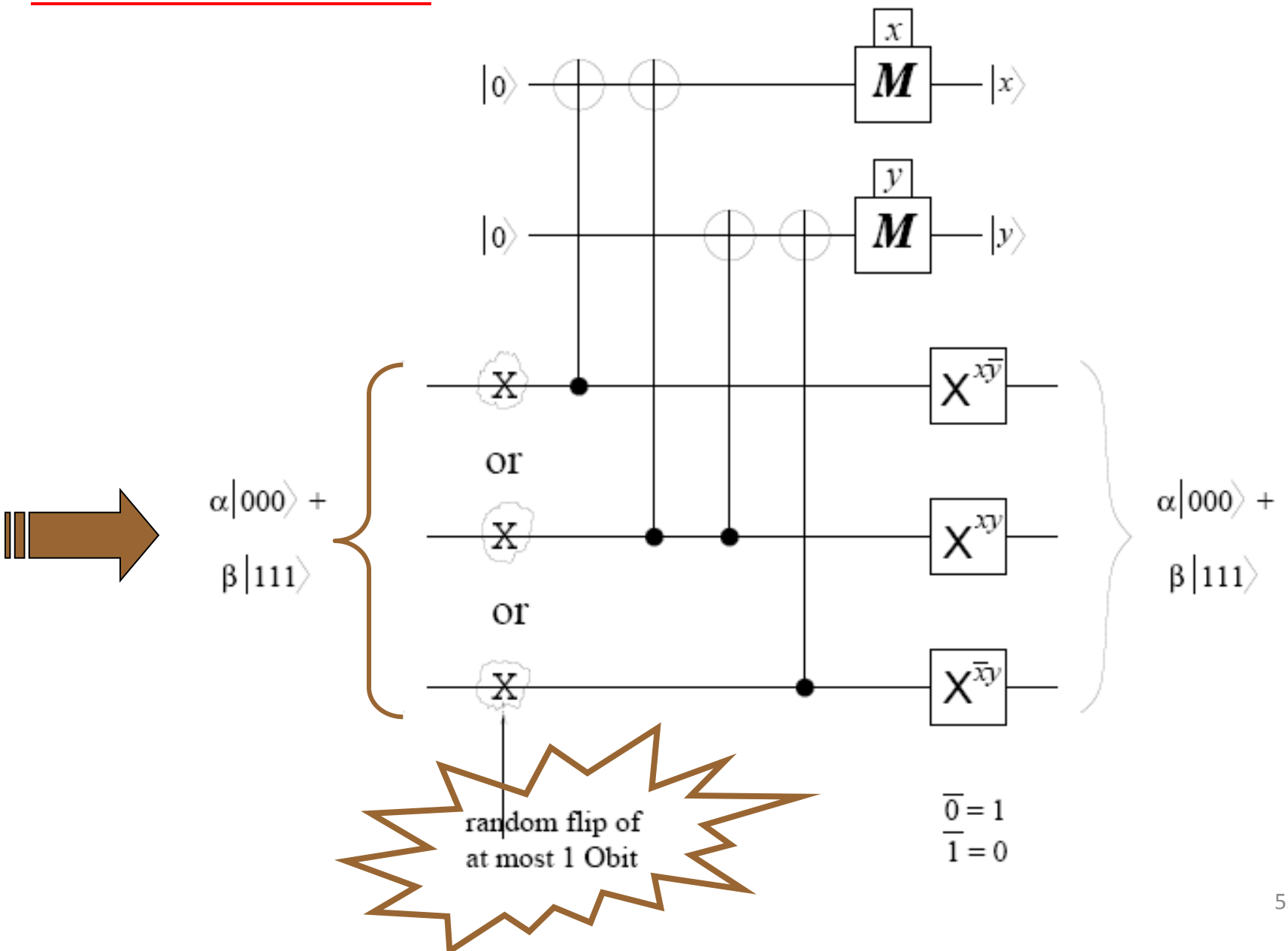


$$|\Psi\rangle = \alpha|000\rangle + \beta|111\rangle$$

Canal con 1 error

$$|\Psi_0\rangle = \mathbf{X}_0|\Psi\rangle = \alpha|001\rangle + \beta|110\rangle,$$
$$|\Psi_1\rangle = \mathbf{X}_1|\Psi\rangle = \alpha|010\rangle + \beta|101\rangle,$$
$$|\Psi_2\rangle = \mathbf{X}_2|\Psi\rangle = \alpha|100\rangle + \beta|011\rangle,$$

Un decodificador sencillo



Códigos Superdensos

Alice

Bob

$|\Phi\rangle$

¿Un Qubit solo lleva 1 bit de información?

Si Alice y Bob tienen cada uno, un Qubit de un par EPR (*entangled Qubits)*

(1) Dependiendo lo que Alice quiere transmitir, aplica una transformación I, X, Z o ZX a su *entangled* qubit, obteniendo:

00 → $\mathbf{1}_a|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big),$

01 → $\mathbf{X}_a|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|1\rangle|0\rangle + |0\rangle|1\rangle\big),$

10 → $\mathbf{Z}_a|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle - |1\rangle|1\rangle\big),$

11 → $\mathbf{Z}_a\mathbf{X}_a|\Psi\rangle = q\frac{1}{\sqrt{2}}\big(|0\rangle|1\rangle - |1\rangle|0\rangle\big).$

… y lo envía a Bob.

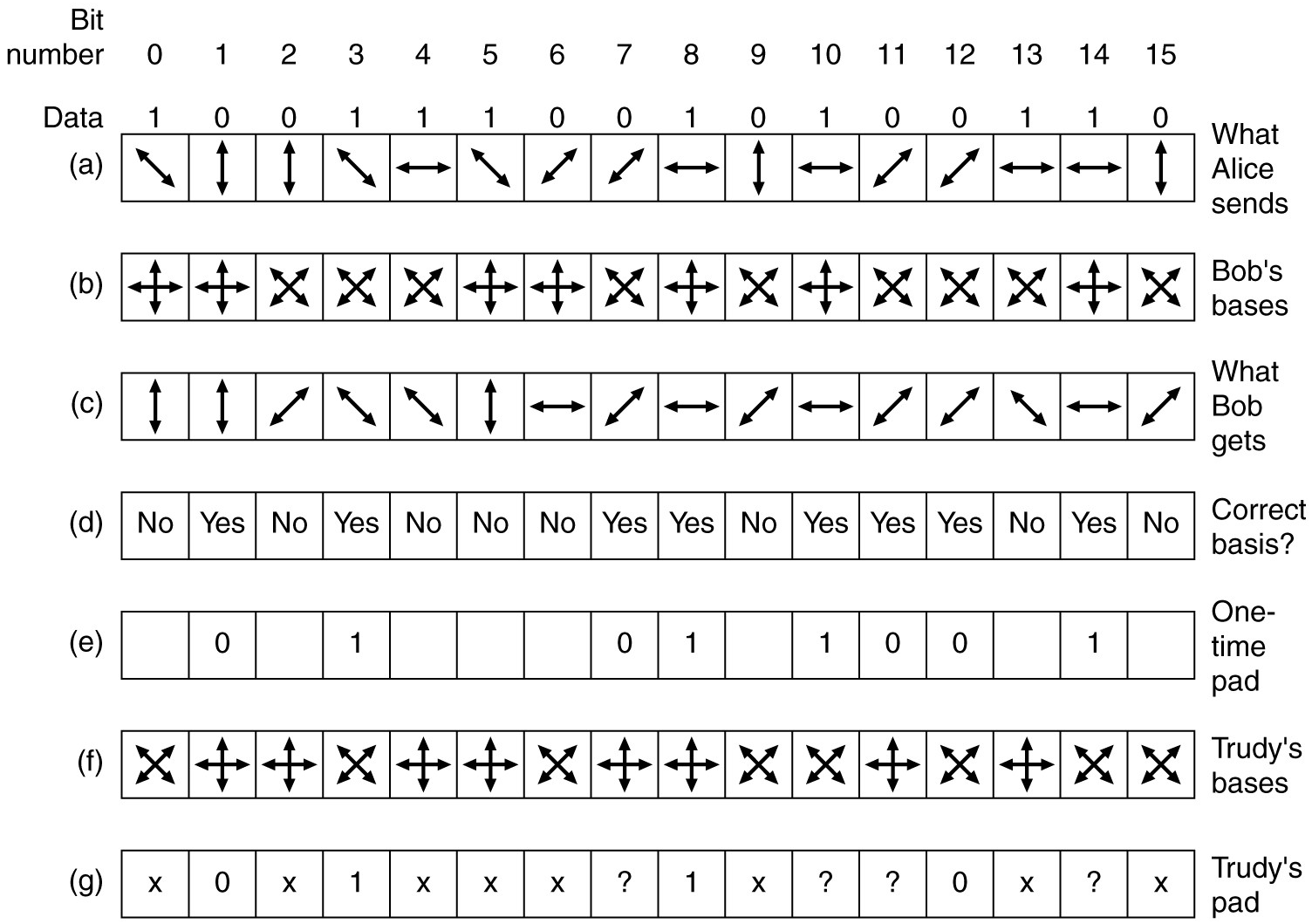
(2) Bob usa el Qubit recibido para controlar con c-NOT a su Qubit, y a este resultado le aplica una transformación Hadamard (H) obteniendo:

$$\mathbf{H}_a\mathbf{cX}_{ab}\mathbf{1}_a|\Psi\rangle = |0\rangle|0\rangle,$$
$$\mathbf{H}_a\mathbf{cX}_{ab}\mathbf{X}_a|\Psi\rangle = |0\rangle|1\rangle,$$
$$\mathbf{H}_a\mathbf{cX}_{ab}\mathbf{Z}_a|\Psi\rangle = |1\rangle|0\rangle,$$
$$\mathbf{H}_a\mathbf{cX}_{ab}\mathbf{Z}_a\mathbf{X}_a|\Psi\rangle = |1\rangle|1\rangle.$$

M → **Bob obtiene 2 bits!**

Criptografía Cuántica BB84

[Distribución de Claves. *Bennet & Brassard, 1984*]



Algunas Empresas ofreciendo Productos Cuánticos

- ID Quantique
  http://www.idquantique.com/

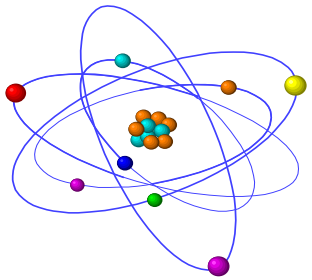
- NEC *Empowering Innovation*
  http://www.nec.com/

- Toshiba
  www.toshiba.com/

- D Wave
  http://www.dwavesys.com/

Posibles Realizaciones Físicas de un Computador Cuántico

System	τ_Q	τ_{op}	$n_{op} = \lambda^{-1}$
Nuclear spin	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^{4}
Ion trap (In^{+})	10^{-1}	10^{-14}	10^{13}
Electron – Au	10^{-8}	10^{-14}	10^{6}
Electron – GaAs	10^{-10}	10^{-13}	10^{3}
Quantum dot	10^{-6}	10^{-9}	10^{3}
Optical cavity	10^{-5}	10^{-14}	10^{9}
Microwave cavity	10^{0}	10^{-4}	10^{4}



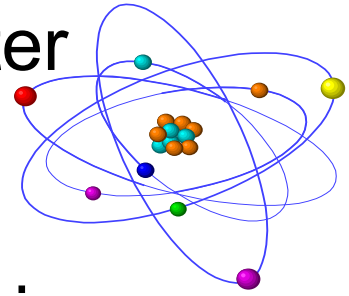
τ_Q … tiempo hasta la decoherencia

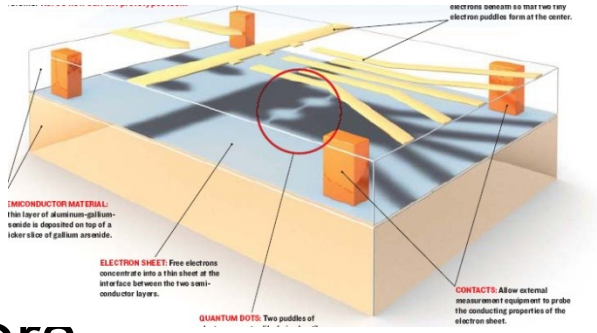
τ_{op} … tiempo que lleva una operación

n_{op} … número de operaciones potencialmente posibles ($n_{op} = \tau_Q / \tau_{op}$)

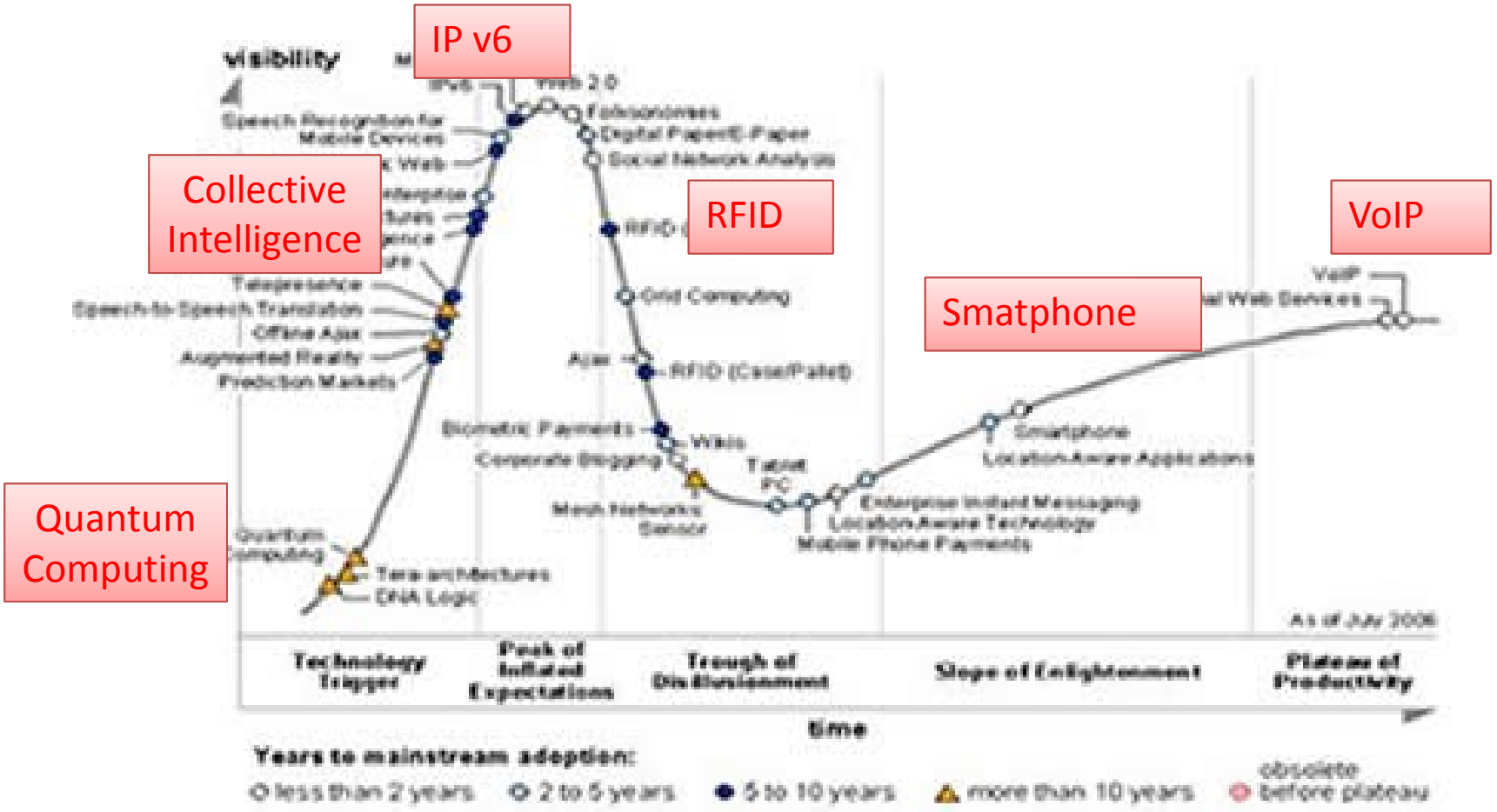
Posibles Tecnologías para implementar un Computador Cuántico

- Harmonic oscillator quantum computer
- Optical photon quantum computer
- Optical cavity quantum electrodynamics
- Ion traps
- Nuclear magnetic resonance – NMR
- Quantum dots
- Superconductor Technology
- Nuclear spin in semiconductors

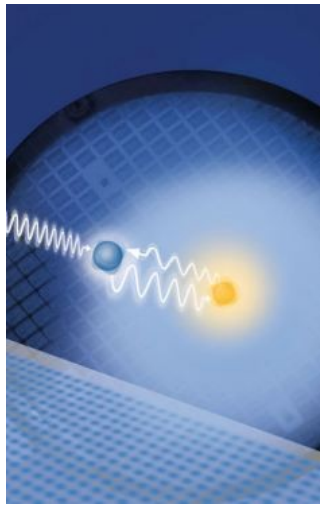




Madurez Tecnológica a inicios del siglo XXI

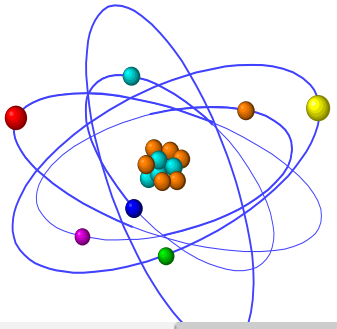


¿Qué podemos esperar de los computares cuánticos?

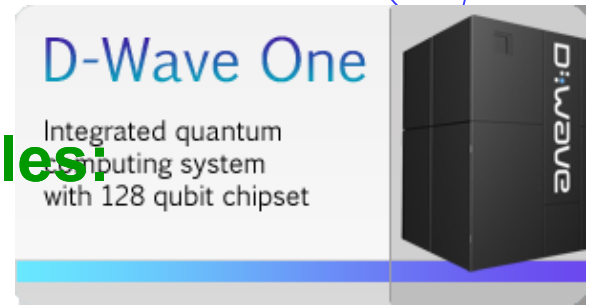


- Aumentar el tiempo de coherencia de las actuales 10^{-8} s a por lo menos microsendos (10^{-6} s).
- Integración práctica de compuertas cuánticas ya desarrolladas, en un único.
- Extender el número de qubits a docenas, centenas o tal vez millares.

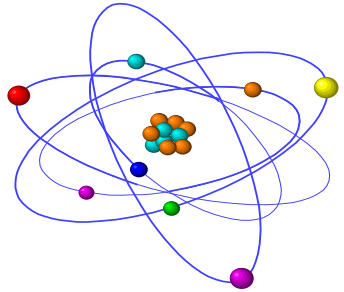
El computador cuántico solo podrá ser comercial en algunas décadas más.



Aunque ya existan ofertas comerciales.



Cursos Disponibles en Internet

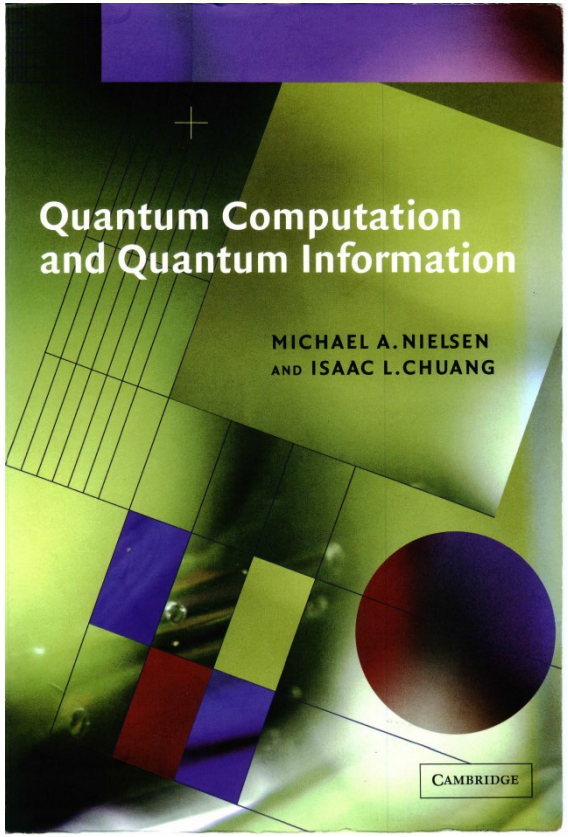


Prof. John Preskill:
http://www.theory.caltech.edu/people/preskill/ph229/index.html

Prof. Umesh Vazerani:
http://www.cs.berkeley.edu/~vazirani/quantum.html

Prof. David Mermin:
http://people.ccmr.cornell.edu/~mermin/homepage/ndm.html

Principal Libro Recomendado



Quantum Computation and Quantum Information

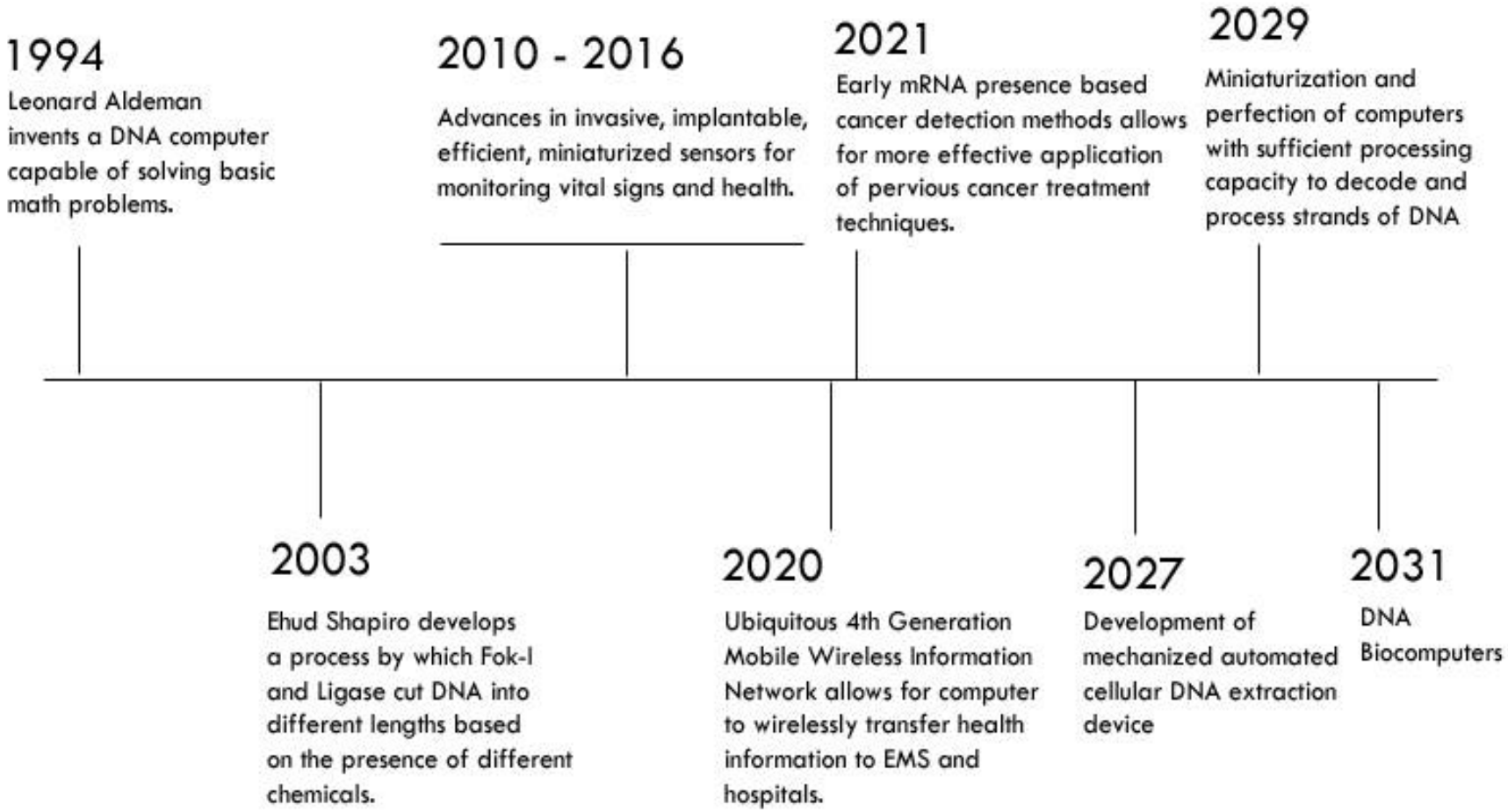
Michael A. Nielsen & Isaac L. Chuang

Computación Molecular

Historia

- 1994 – Leonard Aldeman inventa un computador ADN capaz de resolver problemas matemáticos básicos.
- 2003 – Ehud Shapiro desarrolla un proceso por el cual las enzimas Fork-I y Ligasa cortan ADN en diferentes longitudes basado en la presencia de diferentes sustancias químicas.
- 2007 – Yaakov Benenson y su equipo de trabajo desarrollan un sistema para construir evaluadores lógicos basados en RNAi universales que operan en células de mamíferos.

Historia – Previsiones Futuras

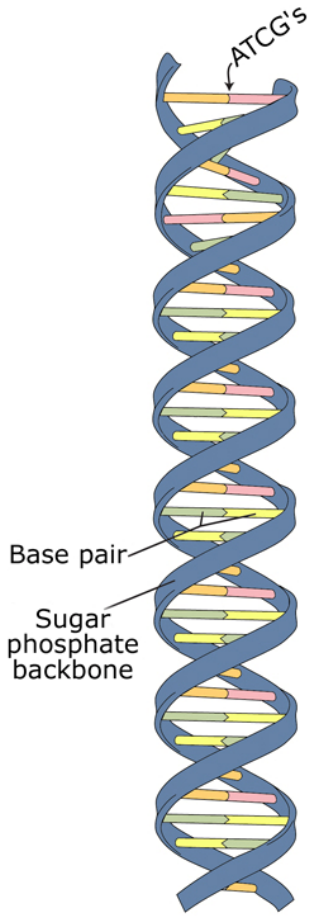


Computación Celular

Fundamentalmente, la computación con ADN pone de manifiesto que las células humanas y los computadores tienen la capacidad de almacenar y procesar la información de manera similar.

- Los computadores almacenan la información en series de unos y ceros, y
- el ADN lo hace en función de la colocación de sus bases (adenina, guanina, timina y citosina).

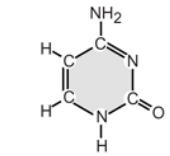
Computación celular



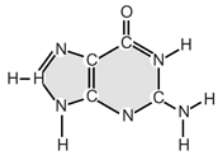
DNA

Deoxyribonucleic acid

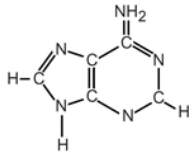
C Cytosine



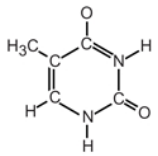
G Guanine



A Adenine



T Thymine



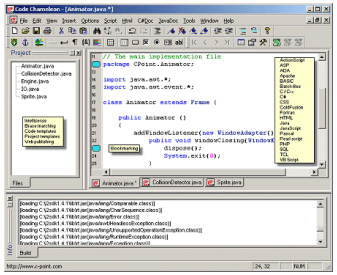
Nitrogenous Bases

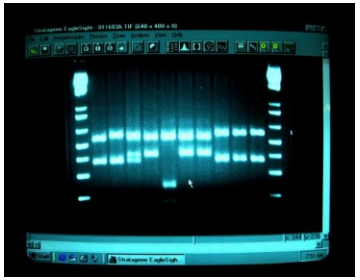
```
0100100101101110011
0110011011110111001
0110110101100001011
0100011010010110111
0110111000100000011
0011011101000110111
0111001001100101011
0100001000000110000
0111001100100000011
0010011010010110111
0110000101110010011
100100101110
```

```
ACTGAGCTGATCGATCGATCGAT
CGTATGCAGCTATCGATGCTAGC
ACGTAGCTAGCTACTGACTCATA
ATCAGTACGTAGCTAGCTACTGC
TACTGACTGCATGCATGCATGCA
TGACTGCATGCATGACTGCACAT
CATGCGTTGCTGACTGACGTACG
AGTGTCTGCAGTCATGACGTCTG
ACGTCATGCATGCAGTATAGCTA
ATATATATCGCGCGCGACTACGT
ACACTGTACTACGTACGACTACG
```

In DNA computing the four bases of DNA, AGCT, replace the 1s and 0s of binary computing.

Computadoras vs Computación ADN





1010101011

GATCGACTAC

Computación celular

Razones para su uso:

- El ADN puede replicarse extremadamente rápido y eficientemente
- Capacidad inmensa de memoria, aproximadamente 100 veces mayor que los computadores de hace dos décadas.
- Estos enormes almacenes de información se contienen en un volumen muy pequeño (15 mil trillones de computadoras en una cucharada).
- Magnifica habilidad para procesar varios cálculos paralelamente (casi 109 cálculos por mL de ADN por segundo.

Memoria ADN

Cadena de ADN puede ser visto como un memoria para guardar información:

- 4 tipos of unidades (A,C,G,T) ▷ números en base 4
- Unidades Complementarias: A-T,C-G
- Cuerdas de doble cadena:

```
ATGGATCAGCTGA
TACCTAGTCGACT
```

Computación Molecular

- El ADN es una doble cadena entrelazada, de cuatro diferentes nucleótidos : Adenina (A), Citocina (C), Guanina (G), y Timina (T). Una cadena es el complemento de la otra asi :

  Adenina-Timina (A-T) y Guanina-Citocina (G-C).

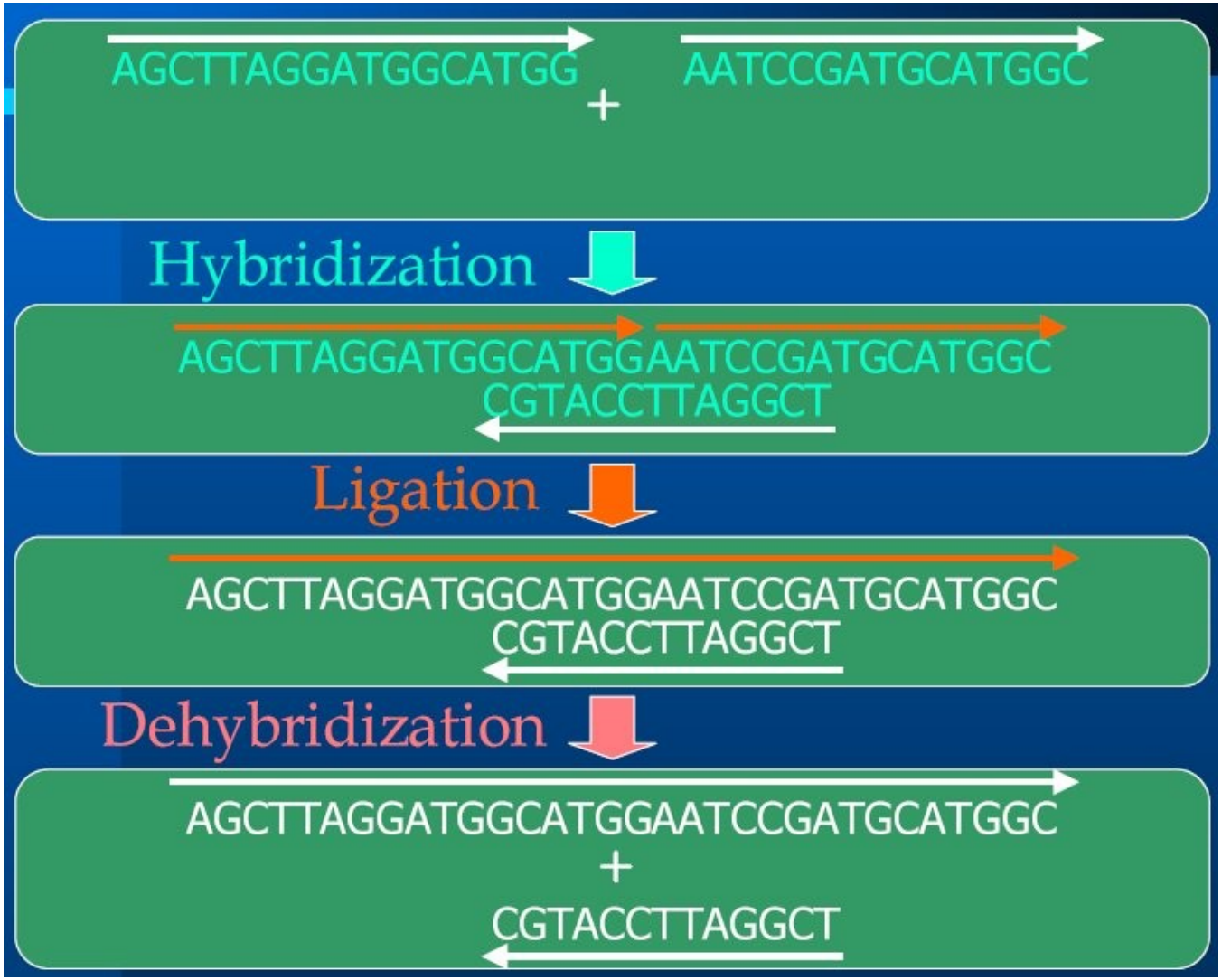
AACCTTGGACTG
TTGGAACCTGAC

- El proceso que permite el encadenamiento de nucleótidos sencillos para formar cadenas de ADN es llamado Polimerización.

Operadores ADN:

- Hibridación
- Ligadura
- Reacción en Cadena de la Polimerasa (PCR)
- Electroforesis en gel
- separación por afinidad
- Las enzimas de restricción

Hibridación y Ligadura



Computación Molecular

- El ADN se puede replicar mediante un proceso conocido como PCR (Polymerase Chain Reaction)
- El ADN se puede reparar por medio de ligasa

CTTC + CAAGGAA = CTTCCAAGGAA

GAAGGTT CCTT GAAGGTTAATT

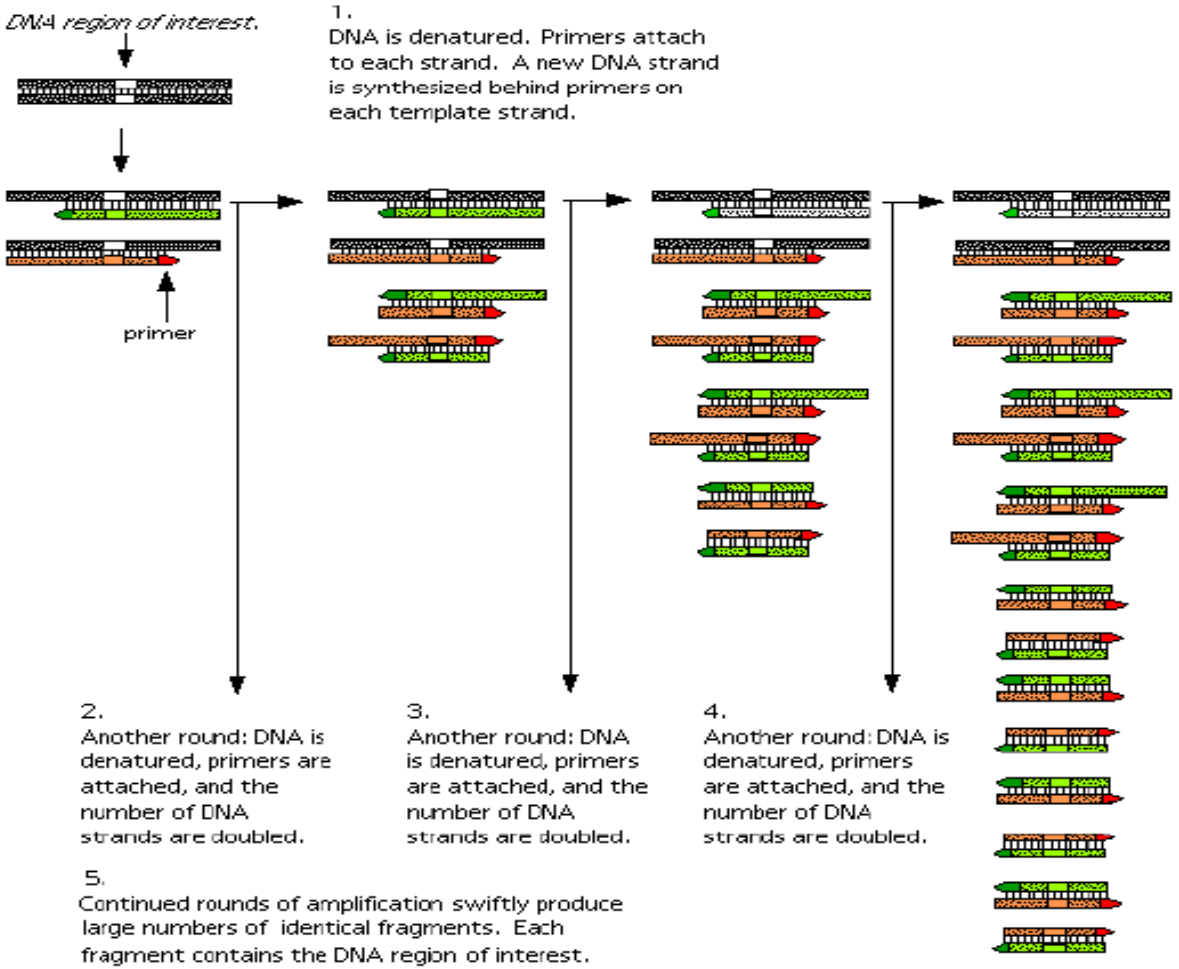
- El ADN se puede cortar por medio de nucleasas o enzimas de restricción

CTTCCAAGGAA = CTTC + CAAGGAA

GAAGGTTAATT GAAGGTT CCTT

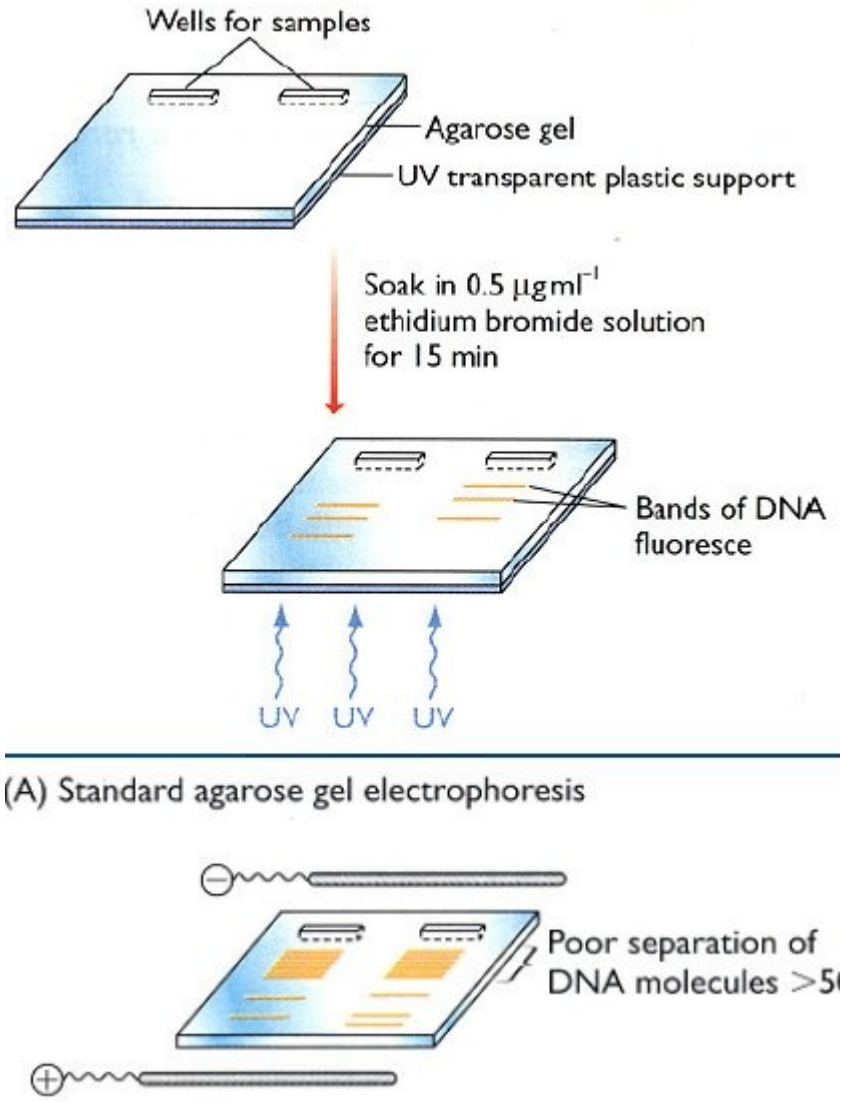
PCR

Amplificar (copias idénticas) cadenas de moléculas de ADN

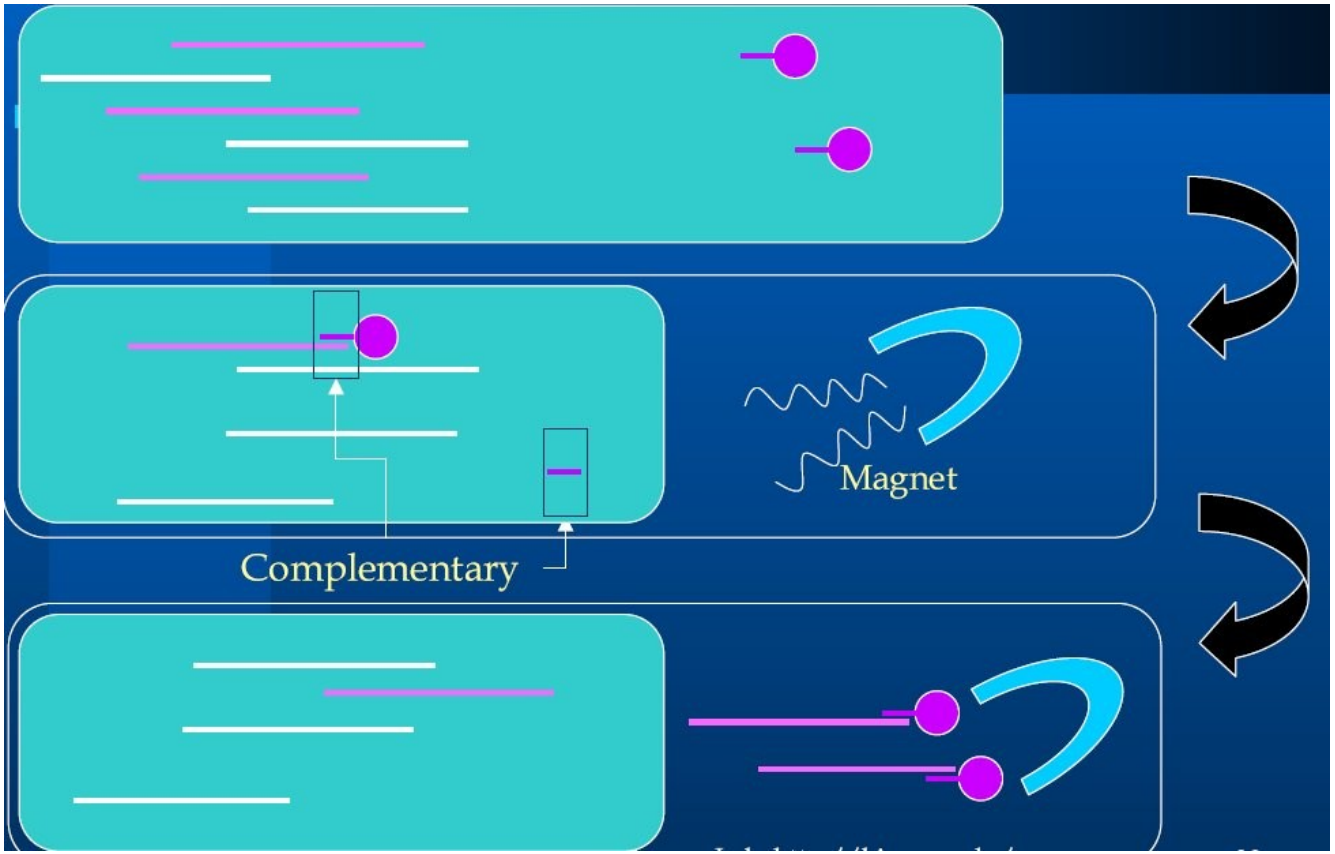


Gel electrophoresis

detección de específicos ADNs



Separación por afinidad



Un campo magnético se la utiliza para sacar todos los fragmentos de ADN que contienen una secuencia

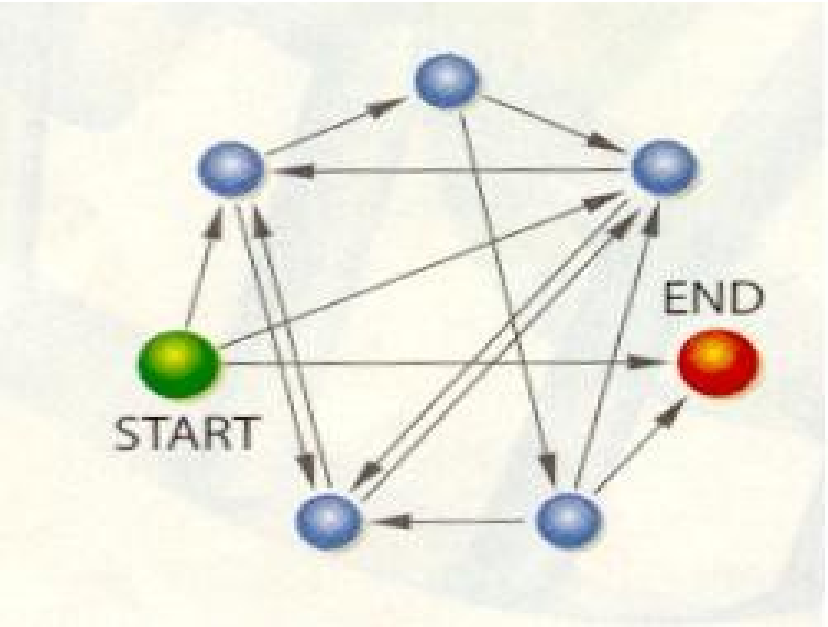
Enzimas de restricción

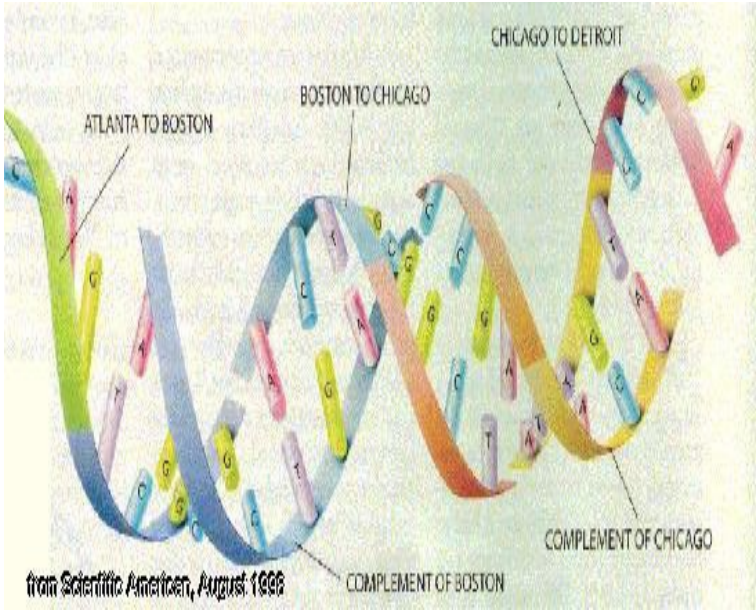
Corta el ADN en un sitio de secuencia específica

1994

Adelman propuso un algoritmo usando ADN para resolver el camino hamiltoniano con 7 nodos

(revista science. Dic.1994)

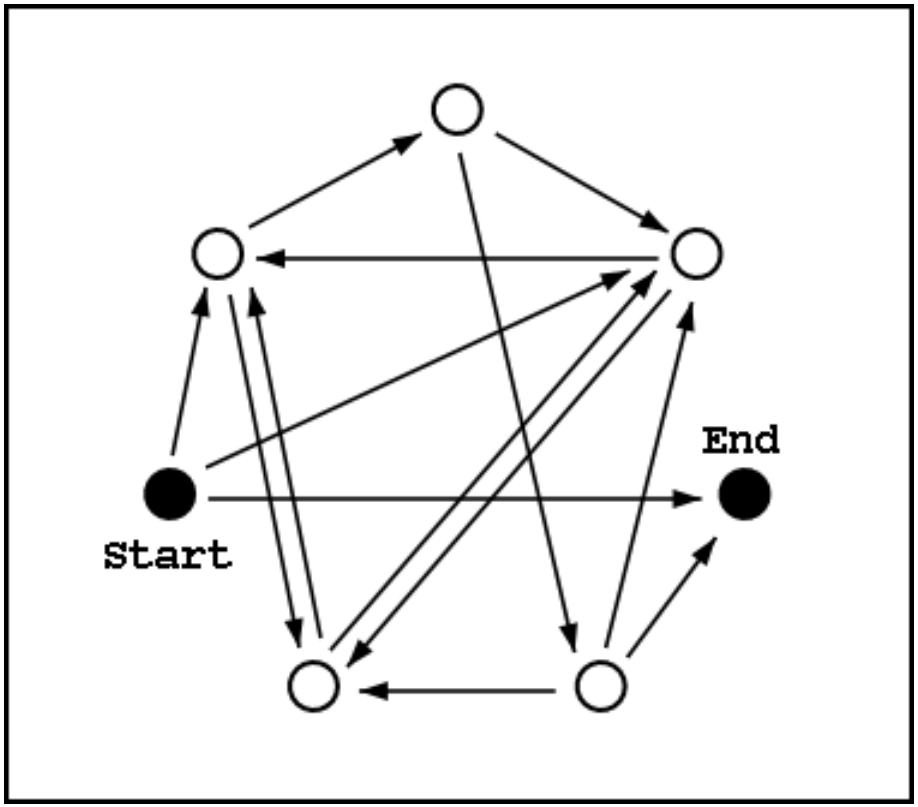




El proceso consiste de:

1. Construir moléculas de ADN que codifican caminos aleatorios a través del grafo.
2. Amplificar mediante la reacción en cadena polimerasa (PCR), para dejar solo los caminos que empiezan en el inicio y terminan en el final.
3. Separar, mediante electroforesis de geles, las cadenas de ADN de acuerdo al tamaño para quedarse solo con la que contienen solo 7 nodos.
4. Aplicar un proceso de purificación por afinidad para dejar las que pasan por cada ciudad solo una vez.
5. Determinar si alguna de las secuencias es la solución buscada. (secuenciación)

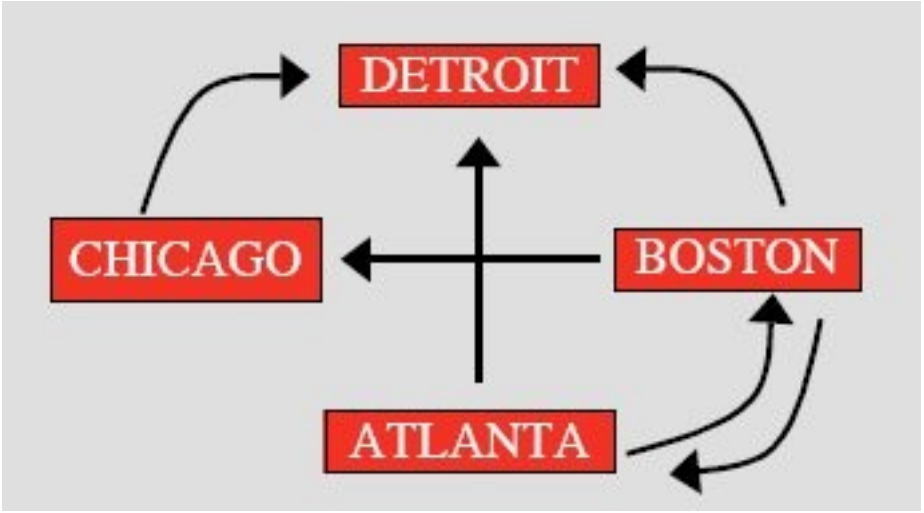
Viajero de comercio



Viajero de comercio

- VC: Un vendedor debe ir de la ciudad A a la Z, visitar otras ciudades en el ínterin. Algunas de las ciudades están unidas por avión. Hay una trayectoria de A a Z visitando cada ciudad una vez?

  A = ATLANTA y Z = DETROIT, SI
  A = BOSTON y Z = DETROIT, NO



Viajero de comercio

1. Codificar cada ciudad (nodo) como una cadena de ADN de 8 unidades
2. Codificar cada enlace permitido con cadenas de ADN de 8 unidades
3. Generar trayectorias aleatorias entre N ciudades (exponencial)
4. Identificar las rutas de acceso que parten de A y terminan en Z
5. Mantener sólo las rutas correctas (el tamaño, hamiltonianos)

Viajero de comercio (codificación de caminos)

CITY	DNA NAME	COMPLEMENT
ATLANTA	ACTTGCAG	TGAACGTC
BOSTON	TCGGACTG	AGCCTGAC
CHICAGO	GGCTATGT	CCGATACA
DETROIT	CCGAGCAA	GGCTCGTT

FLIGHT	DNA FLIGHT NUMBER
ATLANTA - BOSTON	GCAGTCGG
ATLANTA - DETROIT	GCAGCCGA
BOSTON - CHICAGO	ACTGGGCT
BOSTON - DETROIT	ACTGCCGA
BOSTON - ATLANTA	ACTGACTT
CHICAGO - DETROIT	ATGTCCGA

Atlanta – Boston:

```
ACTTGCAGTCGGACTG
     ||||||||
     CGTCAGCC
R:  (GCAGTCGG)
```

(A+B)+Chicago:

```
ACTTGCAGTCGGACTGGGCTATGT
               ||||||||
               TGACCCGA
R:            (ACTGGGCT)
```

Solución A+B+C+D:

ACTTGCAGTCGGACTGGGCTATGTCCGAGCAA

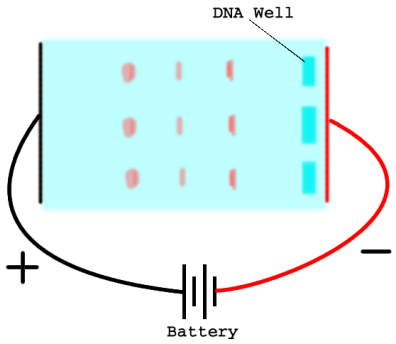
hibridación y ligadura entre las moléculas de la ciudad y las moléculas de enlace interurbano

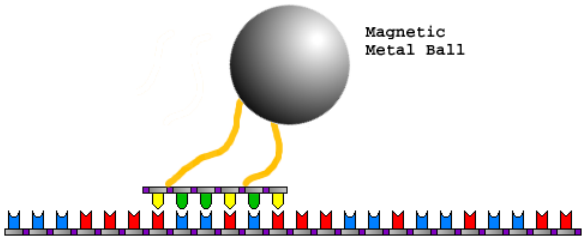
Filtrar las soluciones correctas

1.Identificar los caminos a partir de A y terminando en Z
   PCR para la identificación de secuencias a partir de los últimos nucleótidos de A y terminando en los primeros nucleótidos de Z

2. Mantener sólo las rutas con ciudades N (N = número de ciudades)
   La electroforesis en gel

3. Mantener sólo las rutas con todas las ciudades (una vez)
   Anticuerpos separación del grano con cada vértice (ciudad)





Las secuencias que pasan todos los pasos son las soluciones

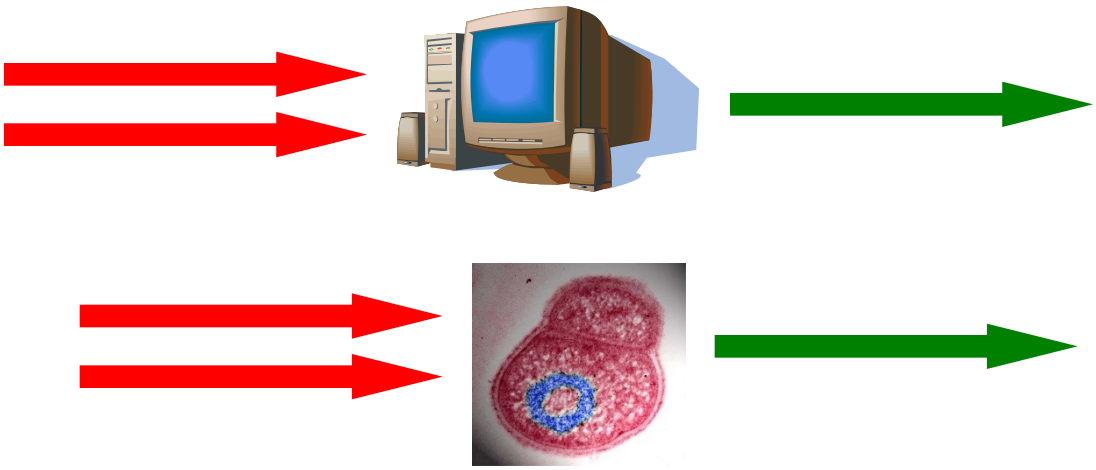
Desarrollo de computadores a nanoescala

- ***Tipos de manipulaciones moleculares básicas para computación ADN:***

  - *Hibridación simple:* Es la forma básica de la actividad del ADN. Fusión de dos células de distinta estirpe para dar lugar a otra de características mixtas.
  - *Tratamiento enzimático:* Es la manera de operar con diferentes formas de ADN.

Evaluador lógico universal

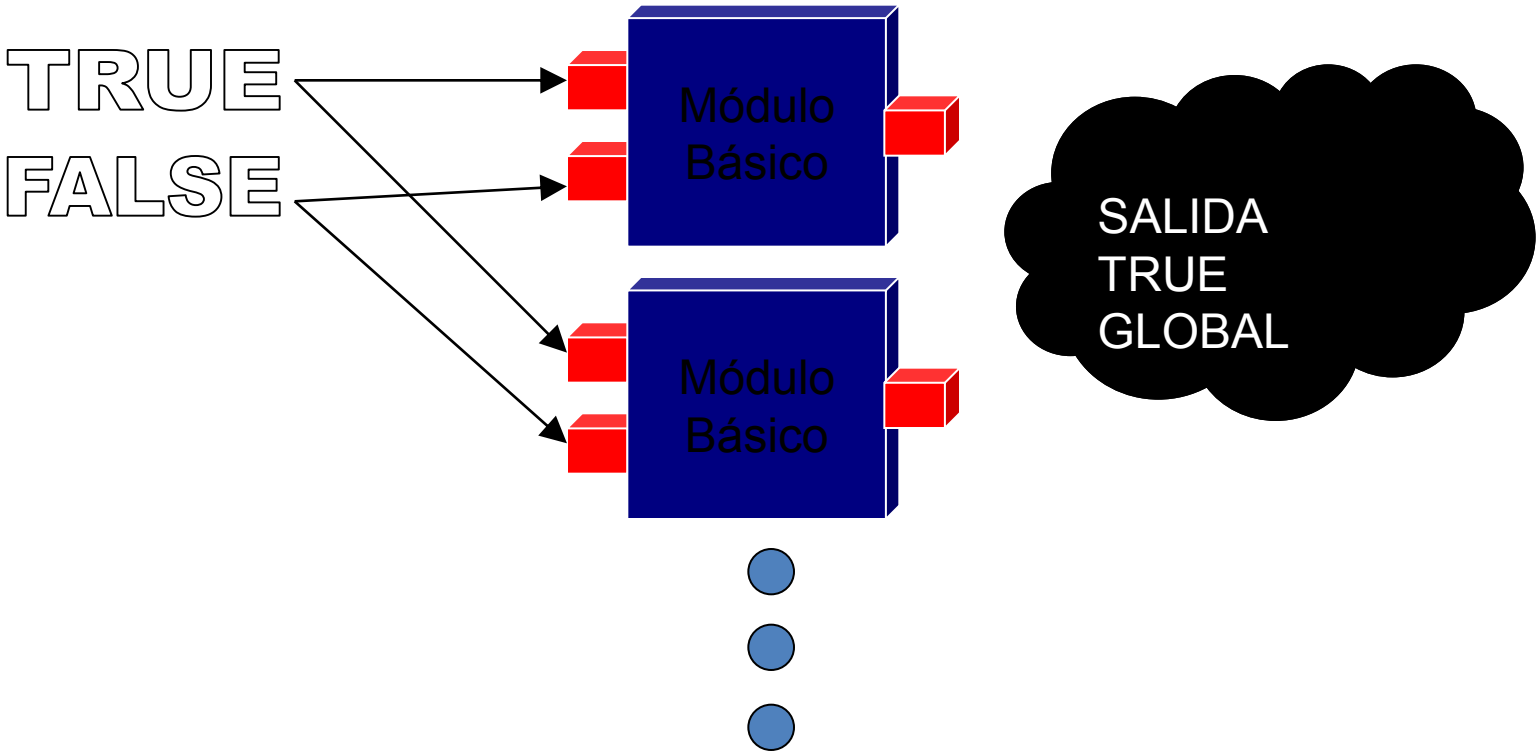
Un autómata molecular es un sistema molecular manipulado unido a un entorno (bio) molecular por “el flujo de mensajes de entrada y las acciones de los mensajes de salida”, donde los mensajes de entrada son procesados por un “conjunto de elementos intermedio”, esto es, un computador.



Evaluador lógico universal

- Primera aproximación:

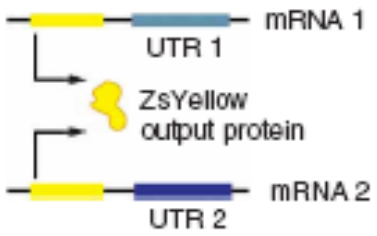
Consistente en ser muy estricto con los módulos básicos, e interconectándolos de manera menos estricta.



Evaluador lógico universal

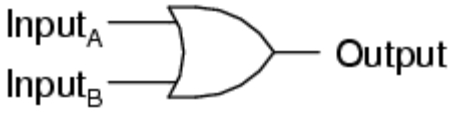
- Construcción de una puerta OR:

a



mRNA 1↑	mRNA 2↑	Output	mRNA 1↑ OR mRNA 2↑
False	False	–	False
True	False	+	True
False	True	+	True
True	True	+	True

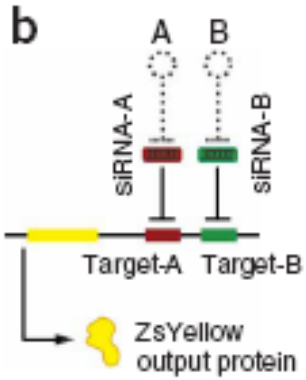
2-input OR gate



A	B	Output
0	0	0
0	1	1
1	0	1
1	1	1

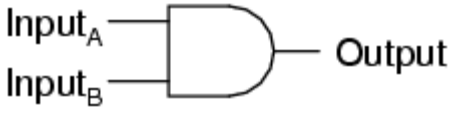
Evaluador lógico universal

- Construcción de una puerta AND:



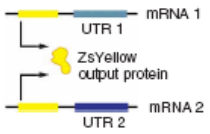
A↑	B↑	Output	A↑ AND B↑
False	False	–	False
True	False	–	False
False	True	–	False
True	True	+	True

2-input AND gate



A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

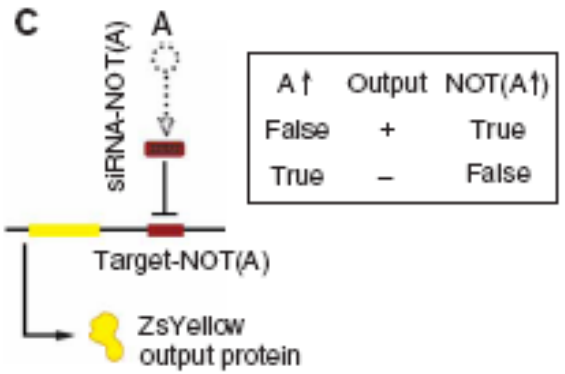
a



mRNA 1↑	mRNA 2↑	Output	mRNA 1↑ OR mRNA 2↑
False	False	–	False
True	False	+	True
False	True	+	True
True	True	+	True

Evaluador lógico universal

- Construcción de una puerta NOT:

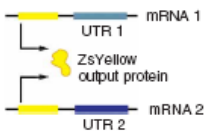


A↑	Output	NOT(A↑)
False	+	True
True	–	False

NOT gate truth table

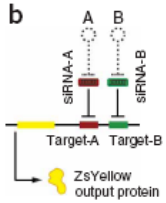
Input	Output
0	1
1	0

a



mRNA 1↑	mRNA 2↑	Output	mRNA 1↑ OR mRNA 2↑
False	False	–	False
True	False	+	True
False	True	+	True
True	True	+	True

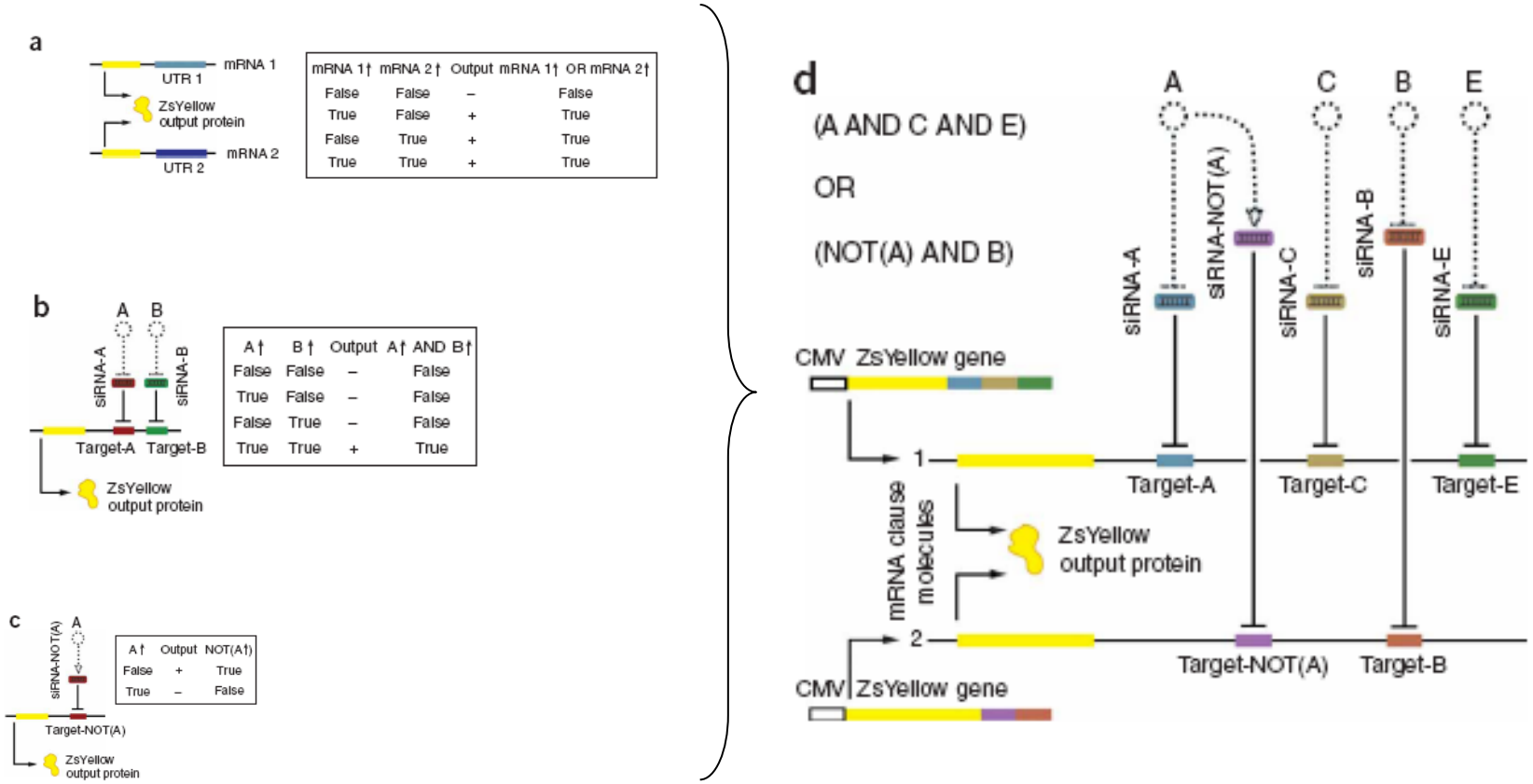
b



A↑	B↑	Output	A↑ AND B↑
False	False	–	False
True	False	–	False
False	True	–	False
True	True	+	True

Evaluador lógico universal

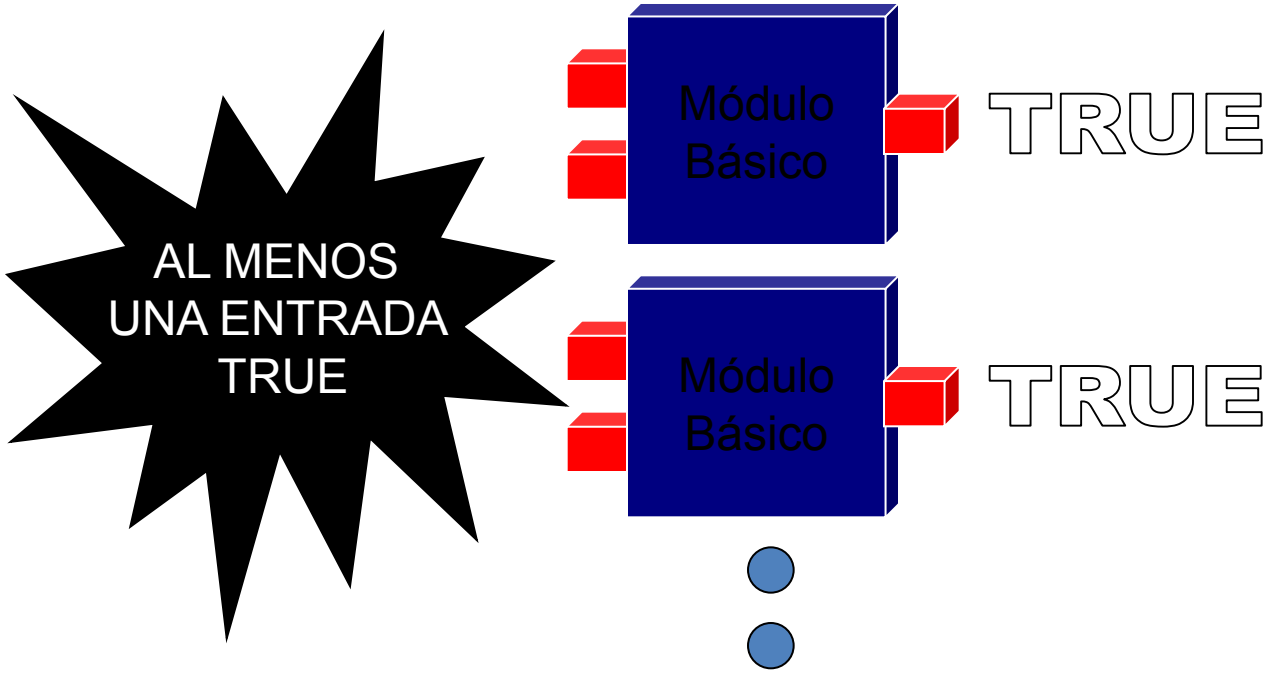
- Construcción de una expresión lógica simple:



Evaluador lógico universal

- Segunda aproximación

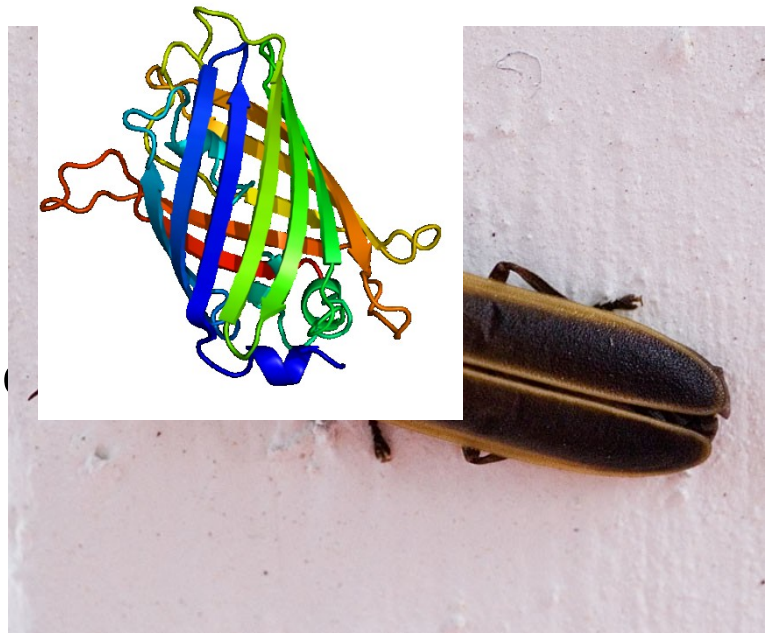
  Consiste en ser menos estricto en los módulos básicos, pero poner exigencias estrictas en la combinación de módulos

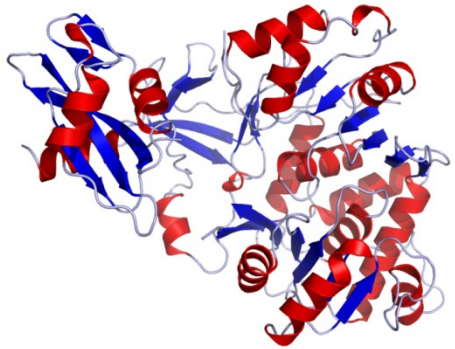


LA SEGUNDA APROXIMACION SE AJUSTA A CNF Y LA OTRA A DNF

Evaluador lógico universal

- Para esta experimentación se eligieron derivativos de conocidos siRNAs, y se construyeron cinco parejas de cadenas siRNA en secuencias publicadas de genes no pertenecientes a mamíferos para representar hasta cinco entradas:
- T1 de Renilla reniformis
- FF3 de Firefly luciferases
- SI 4 de Enhanced green fluoresc

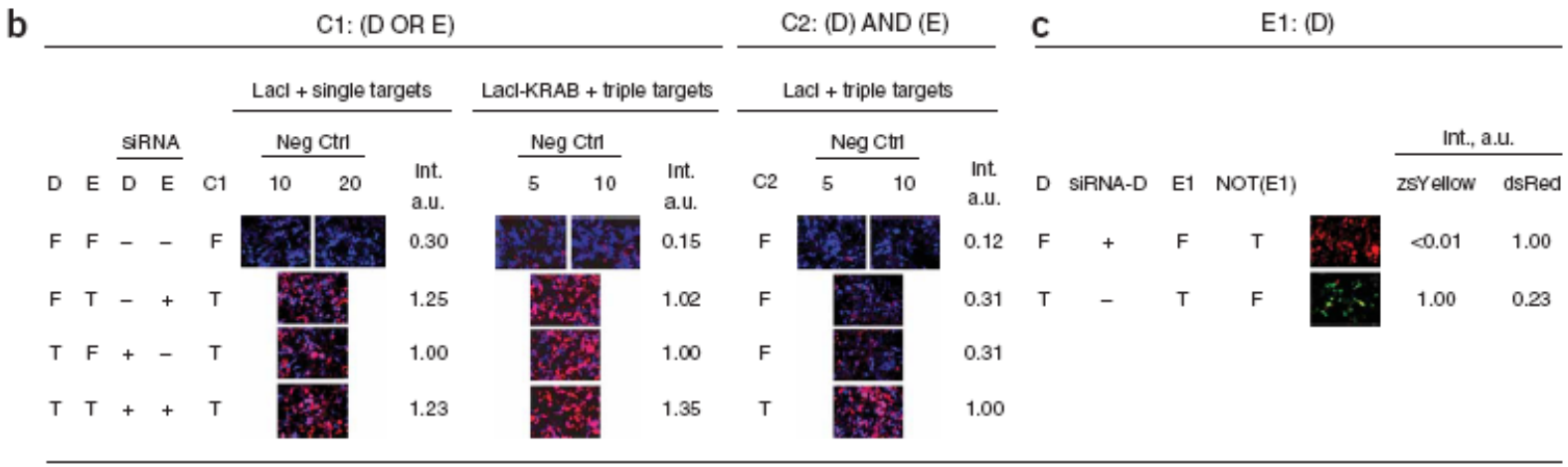




Evaluador lógico universal

D = siRNA → Firefly luciferases.

E = siRNA → Renilla reniformis.



Graficamente: eGFP

Ventajas de la computadora de ADN

- **Paralelismo**. Velocidad (cantidad de procesos simultáneos y cantidad de operaciones por u. de tiempo)

10^{14} operaciones/segundo

100x más rápido que actuales supercomputadores

- **Capacidad de memoria**. Un millón de Gbits por pulgada cuadrada. Los mejores CD veinte Gbits por pulgada cuadrada.

1 bit/nanometro cubico

10^{12} veces más que un videotape

- **Bajo consumo energético**

2×10^{19} operaciones/joule.

Computadores del Silicon usan 10^{9} veces más energia

Mas limpias y menos afectaciones al medio ambiente

Ejemplo

Supongamos que encriptamos un mensaje, con un algoritmo de encriptación de 64 bits, eso significaría que si hiciéramos un ataque de fuerza bruta, necesitaríamos comprobar en el peor de los casos las 18446744073709551616 combinaciones posibles.

Vamos a suponer que codificando ese algoritmo en ensamblador nos salen unas 30 instrucciones máquina y la CPU tendría que ejecutar unas 5534023222112865484480 y suponiendo un ciclo por instrucción y un AMD overcloqueado a 4 GigaHerzios, necesitamos 263.224 años para descifrar el mensaje, aunque es posible, si tenemos mucha suerte, que lo consigamos en solo 100 años.

Para poder leer un mensaje secreto, necesitamos o bien un sistema extremadamente rápido o bien un sistema extremadamente paralelo.

El sistema extremadamente rápido, es el ordenador quántico, y todavía hace falta muchos años, para tener un sistema que pueda ser usado en criptoanálisis.

Los sistemas extremadamente paralelos, hay varias formas, usar un gusano de red que robe tiempo de CPU de las máquinas que infecte, montar un sistema parecido al del proyecto SETI o la más reciente:

La computación DNA

Futuro

- DNA Computer resuelve problemas NP completos mas rápido que las computadoras tradicionales.
- Es una mala idea hacer competir DNA computer con computadoras tradicionales para resolver problemas del mismo dominio.
- La biotecnología resulta un campo principal de aplicaciones futuras, porque opera precisamente con moléculas biológicas.
- La gran perspectiva se orienta a las aplicaciones medicas.

Bibliografía

- Nature Biotechnology. Mayo 2007. Letter: A universal RNAi-based logic evaluator that operates in mammalian cells.
- ChemMatters: Cellular Silicon, a medical revolution.
- Current Nanoscience, 2005. Development of Nano-Scale DNA Computing Devices.
- Nature Biotechnology. Volume 24, number 09 September 2006. Biotechnology in Spain: Special repport.
- Medical Dictionary: Medterms dictionary: http://www.medterms.com/script/main/hp.asp
- Medical Dictionary: Merrian Webster medical dictionary: http://www.intelihealth.com/IH/ihtIH/WSIHW000/9276/9276.html
- Wikipedia, entrada Biotecnologia. (Definición).
- Technology review. October 2004. www.technologyreview.com
- Wikipedia, entrada FPGA
- http://www.eecg.toronto.edu/~vaughn/challenge/fpga_arch.html