POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID

Grupo de Computación Cuántica

Grupo de Computación Natural

Computación no convencional.
La computación del futuro

Fernando Arroyo – ncg

Jesús García - gcc

eui UPM

UNIVERSIDAD POLITÉCNICA DE MADRID

Resumen

1. Computación no convencional
   - CONCEPTOS
2. Computación Cuántica
   - LEY DE MOORE
   - PROPIEDADES ESPECIALES
   - REALIDADES
   - RETOS FUTUROS
3. Computación Natural
   - DEFINICIÓN?
   - REALIDADES
   - RETOS FUTUROS
   - EJEMPLOS

eui UPM

2

© 2007 Dpto. Organización y Estructura de la información

UNIVERSIDAD POLITÉCNICA DE MADRID

1. Computación no Convencional

- Conceptos: [Wikipedia]
  - Computación desarrollada a través de métodos inusuales. Conocida también como computación alternativa
  - Las técnicas más utilizados en computación no convencional son:
    - Computación óptica
    - Computación cuántica
    - Computación química
    - Computación natural
    - Computación bio-inspirada
    - Etc.

3

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

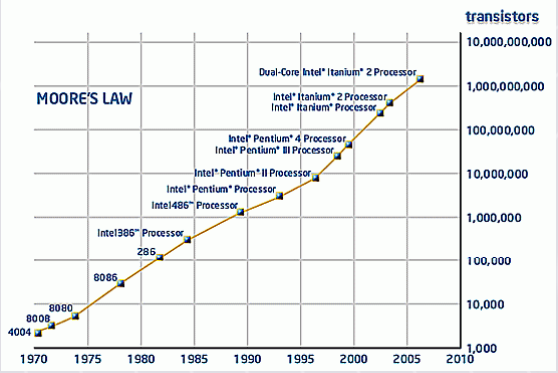
- LEY DE MOORE
  - ❑ Límites de la tecnología actual
  - ❑ Futuro de la tecnología de computadores
  - ❑ Unidad de información cuántica (qubit)
  - ❑ Más ley de Moore…

4

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Límites de la tecnología actual



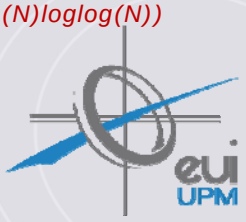
¡No se puede mantener indefinidamente el crecimiento de la potencia de los ordenadores!

5

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Futuro de la tecnología de computadores
  - ***Tecnología cuántica***: una tecnología del futuro
  - ***Algoritmos cuánticos***. Ya están aquí y tienen propiedades sorprendentes:
    - ***Shor (1994)***: *Factorizar un número natural N Y calcular el logaritmo discreto de A módulo N* $O(\log^4(N)\log\log(N))$
    - ***Grover (1995)***: *Encontrar un elemento en un conjunto desordenado de tamaño N* $O(\sqrt{N})$
  - ***Criptografía cuántica***. Más sorprendente todavía:
    - ***Protocolo BB84 (1984)***: *Permite la distribución segura de claves privadas (QKD).*

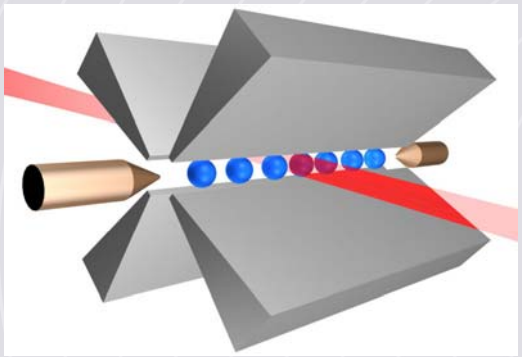


6

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Unidad de información cuántica (qubit)



Soporte:

- **Un fotón de luz**
- **El espín de un electrón**
- **Un átomo**
- **Un ión**

7

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Unidad de información cuántica (qubit)

Estado 1:  $|0\rangle$

Estado 1:  $|1\rangle$

Estado mezcla:  $|0\rangle + |1\rangle$

Principio de superposición

8

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Unidad de información cuántica (qubit)

$$\frac{|0\rangle + \sqrt{3}|1\rangle}{2} \qquad \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$$

9

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- Más ley de Moore…

N qubits → **2^N estados clásicos superpuestos**

Puerta cuántica: actúa sobre los 2^N estados a la vez

Tamaño N → **Tamaño memoria: $O(2^N)$**

Operaciones/puerta: $O(2^N)$

10

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- PROPIEDADES ESPECIALES
  - Medidas cuánticas
  - Qubits entrelazados (EPR)
  - Imposibilidad de copiar qubits
  - Teletransporte de qubits

11

UNIVERSIDAD POLITÉCNICA DE MADRID

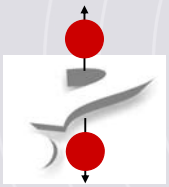
2 Computación Cuántica

- Medidas cuánticas

Leer (medir):

$\sqrt{2}$

Resultado:



con prob. 1 / 2

con prob. 1 / 2

12

2 Computación Cuántica

- Qubits entrelazados (EPR)

Par EPR:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Medida de los dos qubits:

Posibilidades

- **Los dos valen 0** → $|00\rangle$
- **Los dos valen 1** → $|11\rangle$

2 Computación Cuántica

- Imposibilidad de copiar qubits

Si un algoritmo C copia bien el estado $|0\rangle$ ***y el estado*** $|1\rangle$***:***

$$C\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle$$

$$C\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle$$

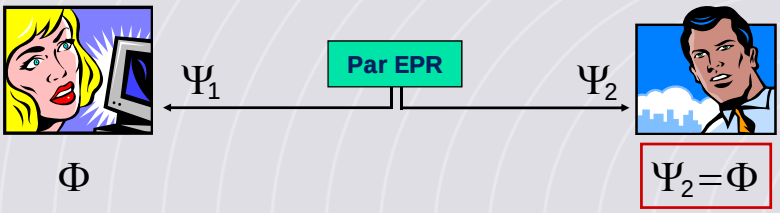
Entonces no copia bien el estado $|0\rangle + |1\rangle$***:***

$$C\,(|0\rangle + |1\rangle)\,|0\rangle \neq (|0\rangle + |1\rangle)\,(|0\rangle + |1\rangle)$$

© 2007 Dpto. Organización y Estructura de la información

2 Computación Cuántica

- Teletransporte de qubits



- **Alice opera con los estados Φ y Ψ_1**
- **Da instrucciones por teléfono a Bob**
- **Bob opera con Ψ_2 siguiendo instrucciones**

2 Computación Cuántica

- REALIDADES

Líneas de investigación del grupo:

Vicente Martín Ayuso, Director del Centro de Supercomputación y Visualización de Madrid (CESVIMA):
- Línea 1: Criptografía cuántica

Jesús García López de Lacalle:
- Línea 2: Algoritmos cuánticos
- Línea 3: Computación cuántica discreta
- Línea 4: Entrelazamiento cuántico
- Línea 5: Modelos de error continuo

Pedro Salas Peralta:
- Línea 6: Computación tolerante a fallos

Resultados de investigación del grupo:

Resultado 1
- Software registrado y patentes sobre QKD

Resultado 2
- Modelos continuos de error
- Modelo discreto de computación
- Relación complejidad-entrelazamiento

Resultado 3
- Simulación de un ordenador cuántico

Resultado 4
- Computación tolerante a fallos

© 2007 Dpto. Organización y Estructura de la información

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- REALIDADES

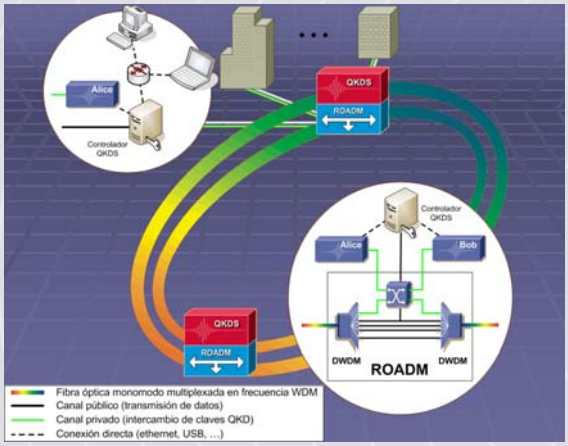
Título	Financiación	Duración
Estudios en Información y Computación Cuántica	MEC	2003 a 2005
Línea experimental de criptografía cuántica	CAM	2006
Red experimental de criptografía cuántica	CAM	2007
Criptografía Cuántica (OPI Proyecto CENIT: ``SEGUR@ Seguridad y Confianza en la Sociedad de la Información")	MEC Telefónica I+D	2007 a 2009
Nuevos Protocolos de Seguridad y Algoritmos Criptográficos para la Protección de Servicios Telemáticos	MEC	2008
Preparación Proyecto AQUA: Advanced Quantum Cryptography Architecture	MEC	2008
Transmisión segura de información cuántica		....
Quantum Information Technologies in Madrid (QUITEMAD)	CAM	2010 a 2013

17

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- REALIDADES



Proyecto más destacado

18

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- REALIDADES

Número de investigadores del grupo	14
Proyectos de investigación financiación pública/privada	8/1
Personal contratado/becado	3
Publicaciones internacionales (revistas/congresos)	14
Publicaciones nacionales (revistas/congresos)	21
Patentes/Registro software	5
Informes técnicos	9
Conferencias, cursos y seminarios	33
Tesis doctorales en desarrollo	7
Inversiones en equipamiento	120.000
Subvenciones	395.460

19

UNIVERSIDAD POLITÉCNICA DE MADRID

2 Computación Cuántica

- RETOS FUTUROS

Ignacio Cirac (EUI, 2006)

- Criptografía cuántica
- Computación cuántica discreta
- Modelos de error continuo
- Complejidad de estados cuánticos

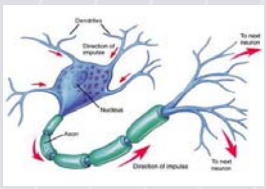
- Bibliografía para los trabajos (6-12 páginas)
- Seminario online de Computación y Criptografía Cuántica

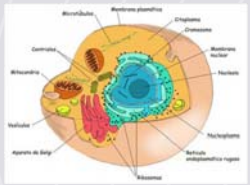
20

UNIVERSIDAD POLITÉCNICA DE MADRID

3 Computación Natural

- DEFINICIÓN
  - Desarrollo de Modelos de Computación inspirados en procesos biológicos.





21

UNIVERSIDAD POLITÉCNICA DE MADRID

3 Computación Natural

- REALIDADES:
  1. Algoritmos Genéticos
  2. Redes de Neuronas Artificiales
  3. Computación con ADN
  4. Computación con Membranas
  5. Redes de Procesadores Evolutivos
  6. Biología Sintética

MODELOS TEÓRICOS

22

UNIVERSIDAD POLITÉCNICA DE MADRID

3 Computación Natural

- Futuro
  - Metas:
    - Solución de problemas difíciles
    - Búsqueda de nuevos límites para la computación
    - Búsqueda de nuevos modelos formales de representación de problemas complejos

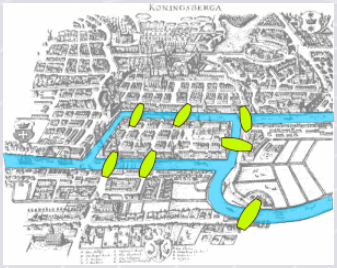
23

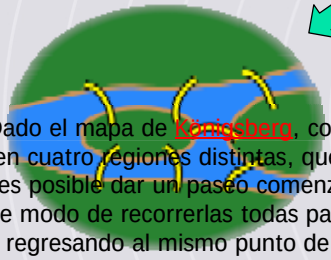
UNIVERSIDAD POLITÉCNICA DE MADRID

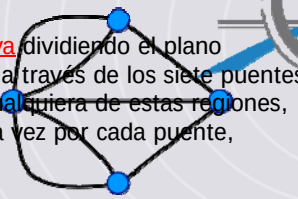
Computación con ADN:

- Los puentes de Königsberg

Comienzo de la
Teoría de Grafos







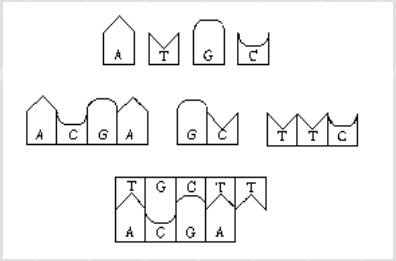
Dado el mapa de Königsberg, con el río Pregolya dividiendo el plano en cuatro regiones distintas, que están unidas a través de los siete puentes, ¿es posible dar un paseo comenzando desde cualquiera de estas regiones, de modo de recorrerlas todas pasando sólo una vez por cada puente, y regresando al mismo punto de origen?

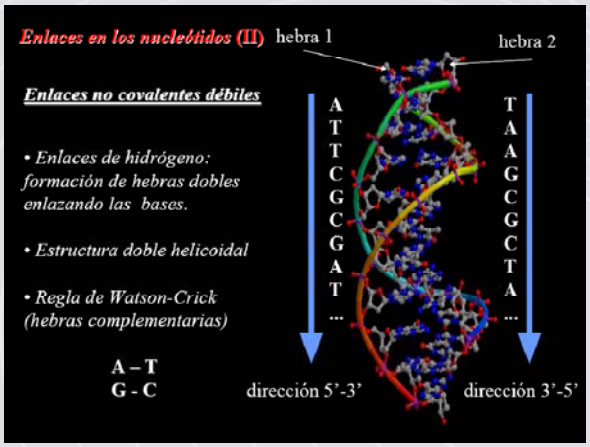
24

UNIVERSIDAD POLITÉCNICA DE MADRID

Computación con ADN:

- ¿Qué es el ADN?





25

UNIVERSIDAD POLITÉCNICA DE MADRID

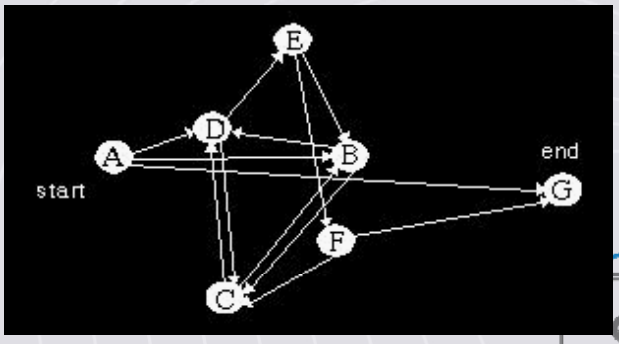
Computación con ADN:

26

UNIVERSIDAD POLITÉCNICA DE MADRID

Computación con ADN:

- El Experimento



Problema del camino hamiltoniano

27

UNIVERSIDAD POLITÉCNICA DE MADRID

Computación con ADN:

- La codificación

28

UNIVERSIDAD POLITÉCNICA DE MADRID

Computación con ADN:

- El algoritmo
  - Se precisan las cadenas que comienzan en la ciudad A y terminan en la ciudad G.
  - Se eliminan aquellos que no pasan exactamente por 7 ciudades
  - Se mantienen aquellas cadenas que contienen una única vez cada una de las ciudades.

29

UNIVERSIDAD POLITÉCNICA DE MADRID

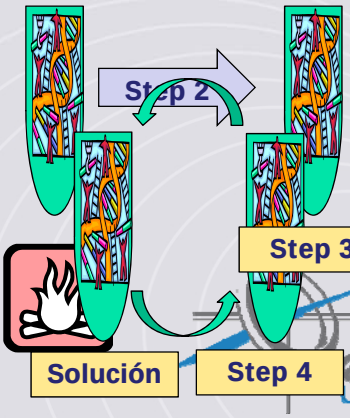
Computación con ADN:

- La implantación

Input: Las ciudades de entrada y salida son marcadas como Vin(0) y Vout(0) respectivamente

  - Step 1: generar de forma aleatoria las cadenas de ADN.
  - Step 2: eliminar las que no empiezan por Vin y no finalizan en Vout.
  - Step 3: eliminar las que no tienen exactamente 7 ciudades.
  - Step 4: para cada una de las ciudades, eliminar las cadenas que no la contengan.

Output: Si no hay cadenas en el tubo de ensayo, no hay solución del problema; en otro caso, el problema tiene solución y en el tubo se encuentran todas las posibles soluciones diferentes de él.



30


UNIVERSIDAD POLITÉCNICA DE MADRID
Muchas Gracias
por su atención
eui
UPM
31