

**IPN**  
**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA**  
**UNIDAD CULHUACAN**

**TESIS**

Que como prueba escrita de su Examen Profesional para obtener el Título de **INGENIERO EN COMPUTACIÓN** deberán desarrollar el C.:

**JAVIER DURAN VEGA**

**"COMPUTACIÓN CUÁNTICA Y NANOESTRUCTURAS"**

En este trabajo se presentan los principios básicos de la nanociencia y las nanoestructuras esenciales para el desarrollo de la tecnología actual. Por otro lado, se discuten los avances tecnológicos que han impactado en la computación, muchos de ellos contemplados cualitativamente en lo que conocemos como la ley de Moore; particularmente, se discute el impacto sobre la capacidad de cómputo. Debido a limitantes para la extensión del documento, se ha optado por discutir únicamente el cómputo cuántico y hacer una breve introducción a las compuertas lógicas cuánticas, los algoritmos cuánticos y la manera general en que está construida una computadora cuántica. Finalmente se presenta lo que se considera son los puntos clave para el desarrollo, en conjunto, de la nanociencia y la computación cuántica, pues la nanociencia será la que haga que dichos dispositivos sean más accesibles para la humanidad.

Capitulado:

	INTRODUCCIÓN.
CAPÍTULO I.-	CÓMPUTO CONVENCIONAL Y CÓMPUTO CUÁNTICO.
CAPÍTULO II.-	SISTEMAS NANÓMETRICOS.
CAPÍTULO III.-	FENÓMENOS FÍDICOS Y NANOESTRUCTURAS.
CAPÍTULO IV.-	LÓGICA EN NLA COMPUTADORA CUÁNTICA.
CAPÍTULO V.-	DISPOSITIVOS NANOESTRUCTURADOS.
	CONCLUSIONES.

Ciudad de México, a 27 de febrero de 2019.

  
\_\_\_\_\_  
**DR. ELIEL CARVAJAL QUIROZ**  
PRIMER ASESOR

  
\_\_\_\_\_  
**M. EN C. JORGE PILO GONZÁLEZ**  
SEGUNDO ASESOR

  
\_\_\_\_\_  
**M. EN C. JOSÉ ANTONIO LOAIZA BRITO**  
JEFE DE LA CARRERA DE I.C.

  
\_\_\_\_\_  
**DR. EUSEBIO RICARDEZ VÁZQUEZ**  
SUBDIRECTOR ACADÉMICO INTERINO






### CARTA DE AUTORIZACIÓN DE USO DE OBRA

En la Ciudad de México, a 27 de febrero del año 2019, el que suscribe **JAVIER DURAN VEGA** alumno de la carrera de **Ingeniería en Computación**, con número de registro **R-010/19**, egresado de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán, manifiesto que soy el autor intelectual del presente trabajo de Tesis, bajo la asesoría del **DR. ELIEL CARVAJAL QUIROZ** y **EL M. EN C. JORGE PILO GONZÁLEZ**, y autorizo el uso del trabajo titulado **"COMPUTACIÓN CUÁNTICA Y NANOESTRUCTURAS"**, al **Instituto Politécnico Nacional**, para su difusión con fines académicos y de investigación.

Los usuarios de la información no deberán reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o asesor del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección de correo: **duranj93@gmail.com** Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

  
Javier Duran Vega  
Nombre y firma del alumno



INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y

ELÉCTRICA UNIDAD CULHUACAN

COMPUTACIÓN CUÁNTICA  
Y NANOESTRUCTURAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

PRESENTA:

JAVIER DÚRAN VEGA

JURADO EXAMINADOR

PRESIDENTE: M. EN C. JOSÉ ANTONIO LOAIZA BRITO

SECRETARIA: M. EN C. MARBELLA CALVINO GALLARDO

1ER VOCAL: DR. ELIEL CARVAJAL QUIROZ

2DO VOCAL: M. EN C. JORGE PILO GONZALEZ

3ER VOCAL: ING. FRANCISCO DE SANTIAGO VARELA



MÉXICO, CD. DE MÉXICO

JULIO, 2019



# Contenido

Agradecimientos . . . . .	IX
Resumen . . . . .	XI
Abstract . . . . .	XIII
Motivación . . . . .	XV
Objetivos . . . . .	XVII
Introducción . . . . .	XIX
<b>1 Cómputo convencional y cómputo cuántico . . . . .</b>	<b>1</b>
<b>2 Sistemas nanométricos . . . . .</b>	<b>13</b>
<b>3 Fenómenos físicos y nanoestructuras . . . . .</b>	<b>21</b>
<b>4 Lógica en la computación cuántica . . . . .</b>	<b>31</b>
<b>5 Dispositivos nanoestructurados . . . . .</b>	<b>41</b>
Conclusiones . . . . .	47



# Agradecimientos

Al Instituto Politécnico Nacional por el apoyo otorgado, durante el desarrollo de este trabajo de tesis, a través del Proyecto Multidisciplinario 20181937.

Quiero agradecer con especial afecto al Dr. Eliel Carvajal Quiroz, persona que dirigió esta tesis y también gran parte de mi carrera profesional como profesor. Gracias por ser un maestro tan apasionado por la ciencia y la investigación, por personas impactantes como usted se generan semillas que germinan en investigadores dispuestos a contribuir al camino tan demandante de la ciencia. Sin duda alguna es usted un gran ser humano.

Para poder dar una forma inicial a este proyecto fue necesaria la ayuda del Dr. Jorge Pilo Gonzalez. De antemano muchas gracias por guiar este proyecto. También me gustaría destacar la grandiosa persona que eres, ya que con el ejemplo has inspirado en mi las ganas de perseguir mis sueños sin importar lo inalcanzables que pueden ser, todo con esfuerzo y perseverancia.

Guadalupe Vega Chávez, sin duda alguna usted ha sido la persona más impactante de mi vida, no me alcanzarán nunca las palabras para demostrar lo agradecido que estoy con la vida, por saber que usted esta ahí apoyándome, para impulsarme a perseguir mis sueños y no rendirme nunca

A mi padre por brindarme siempre los consejos, que necesite y sobre todas las cosas por enseñarme que todo lo que se hace con corazón persevera.

A mi hermana Jocelyn por darme las palabras de aliento siempre que las necesite, por procurar mi persona y ser la personita que me impulsa a levantarme todos los días, pues si una sonrisa puede motivarme, es la tuya sin duda. Estoy completamente orgulloso del ser humano en que te estas convirtiendo.

A Arthur Jafed Zizumbo por enseñarme que siempre puedes ser la mejor opción de alguien. Por ser la antorcha que ilumina mi camino y mi corazón. Gracias por tanto socio, antorcha, hermano.

A Wendy González Vega por retarme día a día a superar mis propias expectativas, por enseñarme que las cosas siempre pasan para algo y no por algo. Por confiar, tomar mi mano y seguir a mi lado sin importar lo que venga. Gracias porque juntos somos dinamita.

A Irazú García Reynoso por enseñarme que ser más humano me llevaría a crear una mejor versión de mí mismo. Por ser viento bajo mis alas y demostrarme que el vuelo se disfruta más si es con tus seres queridos, y que no se trata solo de llegar al objetivo. Por enseñarme que siempre tuve una segunda oportunidad de vivir, amiga, por eso y más estaré en deuda contigo siempre.

A mi familia siempre estaré agradecido por todo lo que me han dado, desde un buen consejo hasta el impulso para continuar luchando. Por enseñarme que siempre tengo que mantener la humildad, ante todo.

A mi estimada sociedad 55 Summa Ukulele, sin duda fueron aliento y sustento cuando decidí llevar mi vida a un otro nivel. Gracias por ser esa segunda familia que la vida se encargó de entregarme y de lo cual estoy muy contento.



# Resumen

En este trabajo se presentan los principios básicos de la nanociencia y las nanoestructuras esenciales para el desarrollo de la tecnología actual. Por otro lado, se discuten los avances tecnológicos que han impactado en la computación, muchos de ellos contemplados cualitativamente en lo que conocemos como la ley de Moore; particularmente, se discute el impacto sobre la capacidad de cómputo. Debido a limitantes para la extensión del documento, se ha optado por discutir únicamente el cómputo cuántico y hacer una breve introducción a las compuertas lógicas cuánticas, los algoritmos cuánticos y la manera general en que está construida una computadora cuántica.

Finalmente se presenta lo que se considera son los puntos clave para el desarrollo, en conjunto, de la nanociencia y la computación cuántica, pues la nanociencia será la que haga que dichos dispositivos sean más accesibles para la humanidad.



# Abstract

The basic principles for the Nanoscience are discussed at this work; besides, those nanostructures which must be essential for the today technology development were presented. Also, technological advances which have been relevant to computation are discussed, even if most of them are qualitatively included in that known as Moore's Law; particularly, impact on computing capacity is discussed. Because it is not intended to be exhaustive, just quantum computing was discussed with a brief introduction to quantum logic gates, quantum algorithms and the general way a quantum computer is built.

Finally, it was presented which is considered the key points for the development of quantum computing and nanoscience, because nanoscience could be the tool to make reachable quantum computers.



# Motivación

La principal motivación del presente trabajo es dar a conocer los avances de lo que muchos científicos llaman “el futuro de la computación”, destacando que la implementación de esta tecnología está a cargo principalmente de los nanomateriales y los fenómenos cuánticos que estos pueden presentar. Se pretende demostrar el poder que tiene la teoría de la información cuántica. Es necesario comentar que las computadoras cuánticas se encuentran en una etapa de desarrollo de prototipos, aún así, existen algunas empresas comercializando estas computadoras, siendo estas las más influyentes, actualmente, en el ramo de la tecnología. Independientemente del debate que existe en torno a si las computadoras cuánticas lograrán cierta supremacía con respecto al cómputo actual, se pretende explicar la teoría de información cuántica, la cual lleva bastante tiempo desarrollándose y gracias a dichos estudios es como se ha dado pauta al desarrollo de diferentes algoritmos, que son los que convierten a esta tecnología en algo revolucionario. Finalmente, hacer una comparación crítica entre la computación actual y el cómputo cuántico, y de esta forma tener un panorama más amplio respecto a dónde nos dirigimos en las áreas correspondientes a la computación. Al igual que sucedió en su momento con la teoría de cómputo y la creación del “mundo tecnológico”, justo como lo conocemos ahora, se busca demostrar que no será una tecnología que desplace a lo anteriormente implementado; por el contrario, ayudaría a un crecimiento acelerado en las técnicas actuales, como el blockchain, big data, cifrado y redes neuronales, lo cual a su vez sería clave para la implementación en diferentes áreas como la

medicina, simulaciones o seguridad de datos, entre otras.

# Objetivos

## Objetivo general

Evidenciar la relevancia de los sistemas nanoestructurados en el avance de la computación cuántica.

## Objetivos particulares

Contrastar la computación convencional y la computación cuántica para mostrar que, tratándose de paradigmas diferentes, se complementan y no sustituye una a la otra. Hacer una revisión de las propuestas que se han hecho para utilizar materiales nanoestructurados y los fenómenos físicos asociados que impulsarían el desarrollo de las computadoras cuánticas. Explicar los principios básicos de la computación cuántica, así como de los algoritmos y soluciones que se han conseguido gracias a la implementación de dicha tecnología.





# Introducción

La evolución de la computación ha generado una tendencia a miniaturizar los dispositivos y a aumentar su velocidad de cómputo para poder realizar las tareas de una manera fluida y casi inmediata para el usuario.

El cambio de discos duros por dispositivos de estado sólido, así como la implementación de nuevos protocolos, han provocado que los cuellos de botella en el tráfico de información sean casi nulos; incluso las memorias, que anteriormente representaban un problema para los productores de computadoras, cuentan con diferentes opciones para realizar un intercambio de información rápido.

Con la aparición de la computadora personal (PC, por sus siglas en inglés) se han podido resolver problemas de diferente índole: desde procesamiento de audio, reproducción de videojuegos, operaciones bancarias, desarrollo de la inteligencia artificial, entre muchos otros, para los cuales una computadora no fue diseñada originalmente. Sin embargo, la eficiencia de la unidad de procesamiento central (CPU, por sus siglas en inglés) convencional puede reducirse notablemente frente a tareas específicas, asumiendo que el algoritmo está diseñado para explotar los recursos de manera óptima.

Una de las áreas en las que es útil la computación es en el desarrollo de la inteligencia artificial. En ésta se desarrollan redes neuronales artificiales, que no son otra cosa que una simulación de las neuronas que se encuentran en nuestro cerebro, para entrenarlas

y hacer que asocien patrones. Si bien con un CPU se es capaz de entrenar a la red desarrollada, el tiempo de ejecución en ese CPU es demasiado para estas tareas; así que, buscando disminuir el tiempo requerido para esas operaciones, se ha creado una arquitectura que se denomina unidad de procesamiento neuronal (NPU, por sus siglas en inglés). La diferencia fundamental entre un CPU y los NPU es que los últimos están basados en la forma en la que están estructuradas las neuronas del cerebro humano [1].

Por otro lado, una unidad de procesamiento de gráficos (GPU, por sus siglas en inglés) cuenta con una arquitectura que permite ejecutar muchísimos más núcleos que en un CPU y cuenta con una cantidad de memoria suficiente para hacer un intercambio de información fluido y veloz. Las tareas de procesamiento de imágenes pueden ser ejecutadas con una gran eficiencia y con velocidad superiores a las logradas en un CPU; debido a que se procesa una gran cantidad de datos [2], ha sido ocupada para realizar minería de datos, aunque este no era el objetivo inicial.

Es aquí donde destaca uno de los puntos para los que las computadoras están siendo diseñadas: el cifrado. Actualmente, existe una infinidad de algoritmos de cifrado que nos ofrecen diferentes niveles de seguridad en el mundo virtual. Por otro lado, existen métodos que permiten vulnerar estos algoritmos, ya sea por interceptación de mensajes, fuerza bruta o, una muy interesante, que es el uso de una computadora cuántica. Vulnerar un algoritmo RSA (acrónimo derivado de los nombres de los inventores: Rivest, Shamir y Adleman) por el método de factorización conlleva una gran cantidad de cálculos que tardarían años o meses, en el mejor de los casos, con una computadora de alto rendimiento y para un RSA-1024 bits [3]. Esto se debe a que la base radica en establecer dos números primos y, al multiplicar dichos números primos, se obtendrá una clave, la cual podrá ser compartida de manera pública; en caso de que se busque factorizar la clave pública, para obtener números generadores, se deberán realizar una serie de cálculos que, entre mayor sea la cifra del número primo, mayores serán las po-

sibilidades de obtener dos números que satisfagan dicha factorización, pero sin el éxito garantizado pues podría no ser la clave posible. Una computadora cuántica se basa en la manipulación de las propiedades cuánticas de una partícula individual, a diferencia de una computadora convencional que hace uso de efectos cuánticos al comportamiento promedio de los portadores de carga dentro de sus componentes. Gracias a la manipulación de dichos efectos es posible ejecutar algoritmos como el de Shor, que ayuda a encontrar los números primos generadores de una clave pública [4] y esto permitiría romper fácilmente el algoritmo RSA. Así que se podría afirmar que la computación cuántica será la causante de generar vulnerabilidades en la seguridad cibernética. Pero simultáneamente será la causante de crear un nivel seguridad completamente nuevo; propiedades cuánticas como el entrelazamiento permitirían detectar si se ha realizado una intrusión. También da la pauta para diseñar diferentes algoritmos de cifrado, que sólo contarán con limitantes relacionadas con la mecánica cuántica [5]



# Capítulo 1

## Cómputo convencional y cómputo cuántico

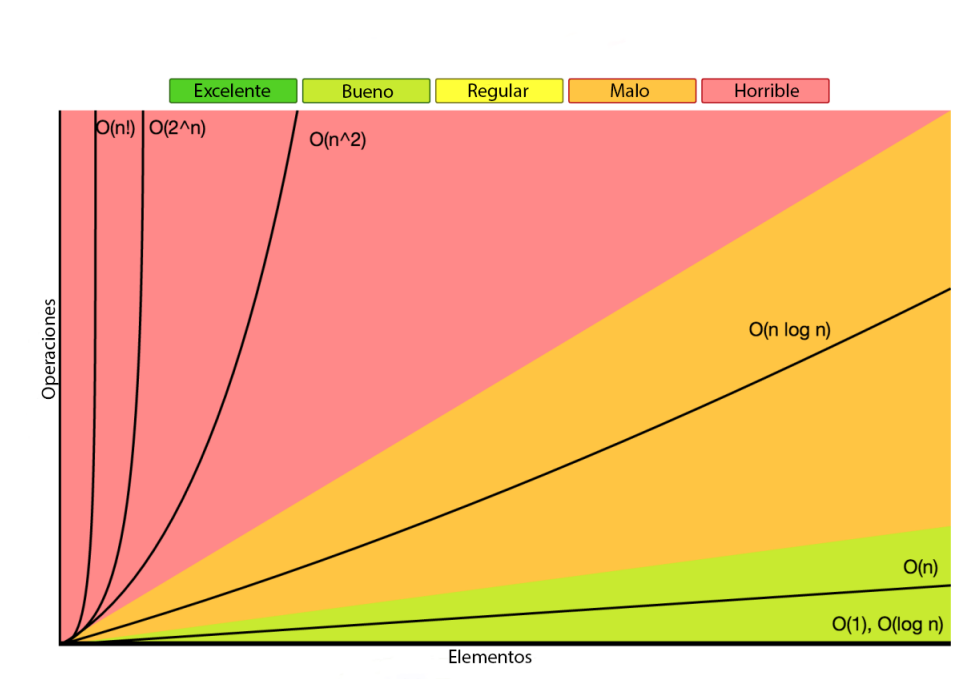


## Generalidades de la computación convencional

Se iniciará el análisis de la computación a partir de un algoritmo, que cuenta con múltiples definiciones según el autor. Para fines prácticos, se definirá a un algoritmo de manera informal como: una serie de instrucciones que, tomando un valor de entrada, es capaz de producir un valor de salida. Así, es posible considerar la tesis de Church-Turing, la cual enuncia que: “Toda tarea ejecutable de manera efectiva es computable”. Con esto surge un término que es muy común, hoy en día, para la sociedad: la “computabilidad”. Esto lleva a introducir la computadora como aquella máquina que tendría la capacidad de ejecutar algoritmos. La primera computadora es la llamada máquina de Turing, la cual está compuesta por una cinta, una unidad de control y un cabezal de lectura y escritura; además, está gobernada por el conjunto de instrucciones llamado programa. Conjuntando todos los términos antes mencionados, se puede afirmar que una máquina de Turing es capaz de computar cualquier algoritmo que tenga solución, o bien, que una máquina de Turing puede dar solución a un problema que se pueda ejecutar de manera efectiva. Partiendo del análisis de algoritmos es posible esperar un consumo de recursos, tanto espaciales (memoria) como temporales, de ejecución (procesador) [6].

En torno a la forma en que se ejecutan los algoritmos surge un término al que llamaremos complejidad; esta, como se mencionó, hará que se administren diferentes recursos, puesto que los problemas que pudiesen ser resueltos por una computadora son diferentes unos de otros. No se tiene un esquema, o regla, a seguir para el diseño de algoritmos. Aunado a eso, también es posible introducir en el juego las diferentes arquitecturas que han sido diseñadas (desde la primera máquina de Turing) y la forma en que algunas son más eficientes que otras para la optimización de los recursos. Todo lo anterior generará diferencias en el uso de los recursos; aunque diferentes algoritmos permiten resolver un problema, hay que considerar que en algunos casos se requerirá

ejecutar más operaciones o almacenar múltiples elementos en memoria (Fig. 1.1) [6].



**Figura 1.1:** Diferencias entre algoritmos generales; se contrasta el número de operaciones con la memoria consumida por los elementos almacenados. Con los colores es posible catalogar el desempeño de dichos algoritmos. Se puede observar la complejidad como la función  $O$ , con los diferentes argumentos que podría tomar según el algoritmo. (Imagen tomada de [7]).

Considerando una computadora convencional, resulta que la unidad de procesamiento más básica es el transistor. De él se derivan las compuertas lógicas, capaces de realizar acciones múltiples para la unidad básica de información (el bit) y esto provee la capacidad de realizar operaciones aritméticas básicas como sumas y multiplicaciones; a su vez, lo último da pauta al escalamiento, al grado de crear sistemas inteligentes que pueden comunicarse con un ser humano, como ocurre en el caso de los chatbots.

Por otro lado, el componente computacional más conocido debe ser el procesador, que está conformado por un conjunto de transistores. Para poder conjuntar al grupo de transistores y crear un procesador se sigue un proceso fotolitográfico que, a grandes rasgos, consiste en imprimir un circuito mediante rayos ultra violeta. Dicha impresión se realiza sobre una oblea de un material semiconductor y, posteriormente, se baña la oblea



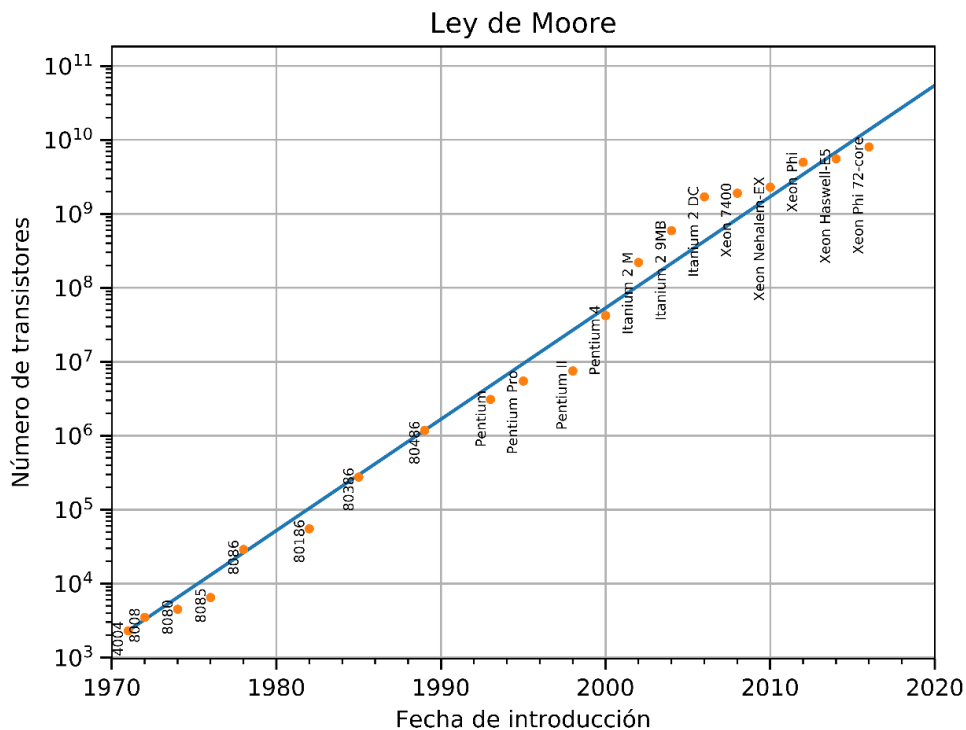
con otro material semiconductor para crear conjuntos PNP ó NPN; es decir, se crean secuencias de semiconductores extrínsecos en los que abundan los portadores positivos (P) o negativos (N). Con el paso del tiempo se han logrado desarrollar técnicas que permiten crear estructuras tridimensionales, reducir la sección transversal del haz del rayo con el que se imprimen los transistores e incrementar la densidad de transistores en dichas obleas [8].

En 1965 Gordon E. Moore notó una tendencia y afirmó que el número de transistores, por unidad de superficie en circuitos integrados, se duplicaría cada año; desde entonces, a esa afirmación se le conoce como la ley de Moore. Aunque la afirmación se corrigió en 1975, porque el número de transistores se ha duplicado cada dos años, y pese a algunas excepciones, esta ley se ha cumplido (Fig. 1.2) cual si hubiera sido un reto para los fabricantes de microprocesadores [9]. Sin embargo, se estima que para el año 2020 se contará con procesadores con transistores de siete nanómetros, llegando al límite posible en el diseño de microprocesadores basados en transistores de silicio[10].

El procesador es la parte principal de una computadora, pero se encuentra lejos de ser el único componente indispensable; se requieren al menos tres elementos mínimos para que una computadora pueda realizar cálculos:

- una unidad de procesamiento,
- un sistema de memoria, y
- dispositivos de entrada y salida.

Usualmente, al conjunto de conexiones, componentes e interfaces se le refiere como organización de computadora y, hoy en día, no se cuenta con una organización de computadora específica, ya que los fabricantes de procesadores están en constante implementación de nuevas tecnologías. Por lo anterior, es necesario crear protocolos, o

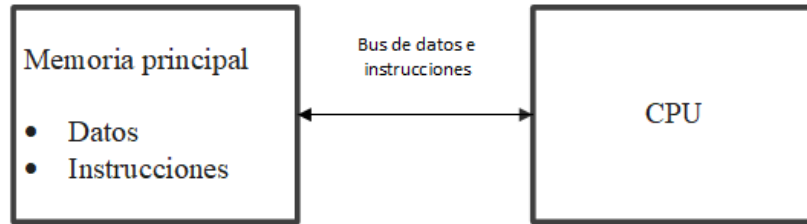


**Figura 1.2:** Relación entre el número de transistores contenidos en un procesador y el año de su introducción al mercado, que evidencia la afirmación establecida en lo que se conoce como la Ley de Moore. Datos obtenidos de [11].

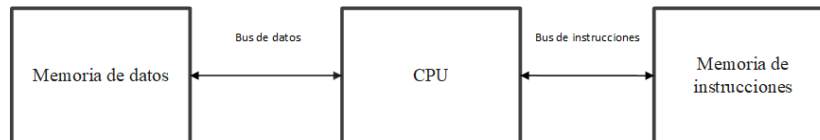
conexiones, que permitan la ejecución correcta. Aun así, la arquitectura que presentan los CPUs está basada en las arquitecturas Harvard y von Neumann, pero esto únicamente tendrá que ver con el camino en que los datos son transferidos entre los diferentes componentes.

La arquitectura von Neumann (Fig. 1.3) se basa en compartir los buses de instrucciones con los de datos. Sin embargo, para hacer más eficiente la forma en que se comparten los datos, es posible recurrir a una arquitectura Harvard (Fig. 1.4), en la que se cuenta con dos buses: uno para las instrucciones y otro para los datos.

Pero independientemente de la arquitectura, para que una instrucción pueda ser ejecutada en un procesador debe llevarse a cabo un ciclo de instrucción(Fig. 1.5) que involucra la búsqueda y decodificación de la instrucción, la generación y búsqueda de los



**Figura 1.3:** Arquitectura von Neumann. En donde solo se tiene un bus de datos para compartir información entre la memoria principal y el CPU.

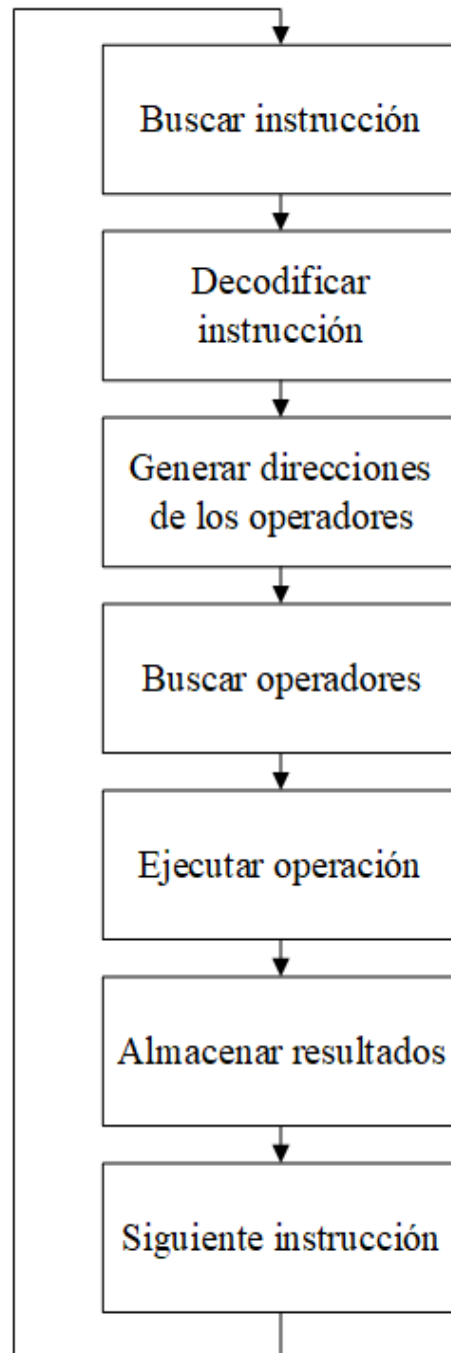


**Figura 1.4:** Arquitectura Harvard. En donde se presentan un bus para acceder a la memoria de instrucciones y uno para la memoria de datos, de manera que, se puede acceder a ambos recursos de manera simultánea, agregando una línea extra de comunicación.

operadores, la ejecución de la operación y el almacenamiento de los resultados. Además, para que las instrucciones de una computadora puedan ser ejecutadas rápidamente, se requiere del paralelismo; este se refiere a la ejecución de las instrucciones de manera secuencial, de tal forma que parezca que las instrucciones son ejecutadas al mismo tiempo.

Una técnica para generar ese paralelismo es el pipelining, que consiste en mantener todas las etapas de ejecución del procesador ocupadas (Tabla 1.1). El paralelismo podría confundirse con multiprocesamiento, pero a diferencia del primero, el multiprocesamiento hará uso de múltiples CPUs para poder ejecutar las instrucciones y reducir el tiempo general de ejecución.

Cuando se ejecutan las instrucciones empleando un CPU es necesario contar con una memoria, para poder intercambiar información antes y después de ser procesada; además, existe una jerarquía para la forma en que se comparte la información. Es posible observar que cuanto mayor sea la velocidad del intercambio de datos, menor será la capacidad de intercambio.



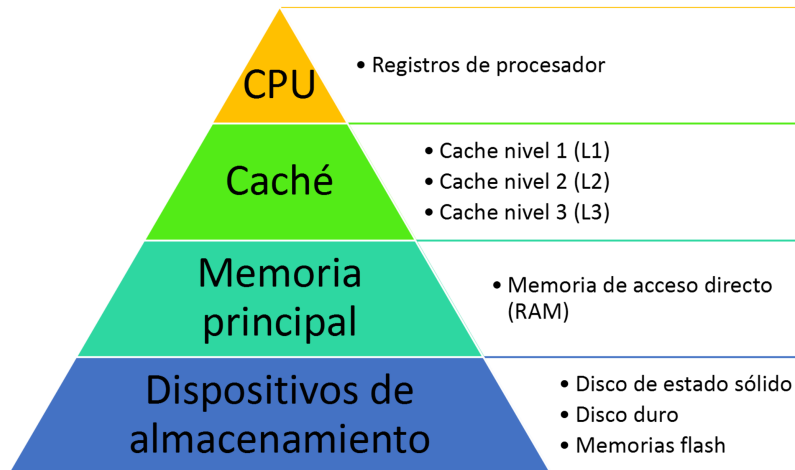
**Figura 1.5:** Ciclo de ejecución de instrucciones en un procesador.

	1	2	3	4	5	6	7	8	9
Instrucción 1	BI	DI	GO	BO	EO	AR			
Instrucción 2		BI	DI	GO	BO	EO	AR		
Instrucción 3			BI	DI	GO	BO	EO	AR	
Instrucción 4				BI	DI	GO	BO	EO	AR
Instrucción 5					BI	DI	GO	BO	EO
Instrucción 6						BI	DI	GO	BO
Instrucción 7							BI	DI	GO

**Tabla 1.1:** Ejecución de instrucciones en Pipeline: buscar instrucción (BI), decodificar instrucción (DI), generar direcciones de operadores (GO), buscar operadores (BO), ejecutar operación (EO), almacenar resultados (AR).

Debido a las limitantes tecnológicas, actualmente nos encontramos con la necesidad de administrar el intercambio de información entre el procesador y la memoria, de una manera jerárquica, poniendo como punto principal al procesador, que será el encargado de ejecutar todas las tareas que se le presenten (Fig. 1.6).

Se cuenta con la memoria caché, que es una memoria con capacidad promedio de 16 MB, capaz de comunicarse con el procesador en cuestión de nanosegundos. Aunque este tipo de memorias resultan insuficientes en capacidades mayores, esto se debe a la forma en la que están construidas, independientemente del número de celdas que se pudiesen generar en un área determinada. Esto genera una limitante de velocidad: cuando se intenta buscar información en una memoria con mayor cantidad de registros, mayor será el tiempo de demora para entregar los datos requeridos. Incluso, entre memorias de acceso aleatorio (RAM, por sus siglas en inglés) existen tecnologías que son eficientes para diferentes tareas. Por ejemplo, en una VRAM se puede leer datos mientras otros son escritos, de manera simultánea; técnicamente es muy similar a una DRAM, pero la diferencia radica en el hecho de que en la DRAM sólo se pueden escribir ó leer los datos, únicamente se ejecuta una instrucción a la vez. La DRAM es usada como una memoria de intercambio, más cercana al CPU, gracias a la cantidad de instrucciones que puede almacenar; pero una VRAM no le serviría a un CPU, más bien sería ocupada para una arquitectura de GPU, en la que se hacen más cálculo, al mismo tiempo, y se requiere



**Figura 1.6:** Jerarquía para el acceso a las memorias. En tanto más cercana a la cúspide, mayor será la jerarquía del elemento.

escribir y leer información de manera simultánea.

Si bien las tareas de los CPUs se centran en la ejecución de instrucciones secuenciales, para disminuir el tiempo de ejecución entre una instrucción y otra, en el caso de los GPUs la arquitectura se basa en la necesidad de procesamiento de información de manera simultánea. Esto último se logra teniendo más de un núcleo, siendo que cada núcleo no es más que un procesador que puede actuar de manera independiente sin entorpecer el desempeño de los otros; de esa manera se realizan todos los cálculos requeridos, de manera distribuida, y los resultados se obtienen con mayor rapidez.

Como se puede observar, el hilo conductor para las propuestas tecnológicas ha sido lograr reducir el tiempo en el que se procesan los datos y se ejecutan los algoritmos; pero también hay que notar que actualmente existe una propuesta tecnológica particular, que puede romper todos los esquemas antes mencionados: la computadora cuántica, que fue descrita por Paul Benioff en 1981 [12].

Quizá lo más importante es entender cuál es la unidad de información básica en la que se basa una computadora cuántica; siendo un bit la unidad básica de información para una computadora tradicional, un qubit juega ese papel para una computadora

cuántica. La gran diferencia entre ellos radica en que un bit puede tener asociado un valor 0 ó 1, pero un qubit puede tener asociados los valores 0 y 1 simultáneamente. Considerando un conjunto de cuatro bits se pueden obtener 16 combinaciones diferentes, una a la vez; pero con un conjunto de cuatro qubits es posible obtener esas mismas 16 combinaciones al mismo tiempo. Es por eso que el desempeño, en cuestión del número de cálculos efectuados, es mayor que en una computadora convencional.

Aunque una computadora cuántica debería operar regida bajo un principio de “caja cerrada” (es decir, que debería de estar aislada del resto del universo), en el momento en que se introducen y leen datos en ella, también se genera ruido en el sistema. Es por esto que para una computadora de ese tipo se requiere corregir el error que se genera al introducir y leer los datos. Para reducir la corrección del error cuántico (QEC, por sus siglas en inglés) existen múltiples técnicas: una de ellas requiere el uso de los puntos cuánticos, estos a su vez son sistemas nanométricos, de los cuales se hablará en profundidad más adelante.





# Capítulo 2

## Sistemas nanométricos



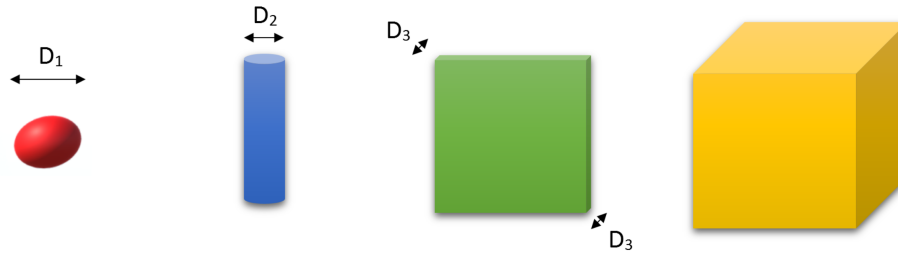
En 2016 fue creado un transistor de un nanómetro de longitud, pero, siendo un tamaño menor a los siete nanómetros, las manifestaciones cuánticas se hacen presentes; entre ellas destaca el efecto túnel, aunque el conjunto de esas cualidades impide que se use como un transistor convencional [13]. Sin embargo, el comportamiento no es exclusivo del transistor mencionado, los fenómenos cuánticos se presentan en toda la materia y destacan cuando las dimensiones se encuentran en la escala nanométrica, especialmente entre 1nm y 100nm. Más aún, usualmente las propiedades físicas, químicas, mecánicas, catalíticas, etc., difieren radicalmente de aquellas esperadas en el mismo tipo de materia cuando sus dimensiones son macroscópicas.

Debido a lo anteriormente planteado, se ha abierto un área del conocimiento que se conoce como nanociencia; en esta se concentra el estudio de los fenómenos y la manipulación de los materiales a nivel atómico, molecular y macromolecular, en el intervalo de dimensiones ya mencionado. Sin embargo, dicho intervalo de longitudes no es lo único que determina las propiedades novedosas; también resulta relevante cuántas de las dimensiones del segmento de materia son confinadas en ese intervalo. Así que las nanoestructuras pueden ser clasificadas según su confinamiento, que no es más que la región del espacio en la que se mueven los electrones: puede ser en tres, dos, una o cero dimensiones (Tabla 2.1, Fig. 2.1).

Estructura	Confinamiento cuántico	Dimensiones restringidas
Punto cuántico	0-D	3
Nanoalambre	1-D	2
Pozo cuántico	2-D	1
Material volumétrico	3-D	0

**Tabla 2.1:** Estructuras, confinamiento y dimensiones de las diferentes nanoestructuras.

Las propiedades físicas o químicas de la materia utilizada para construir estructuras nanométricas puede ser diversa, considerando las propiedades que exhiben cuando las dimensiones son macroscópicas. Partiendo de lo anterior, la manera en que se pueden

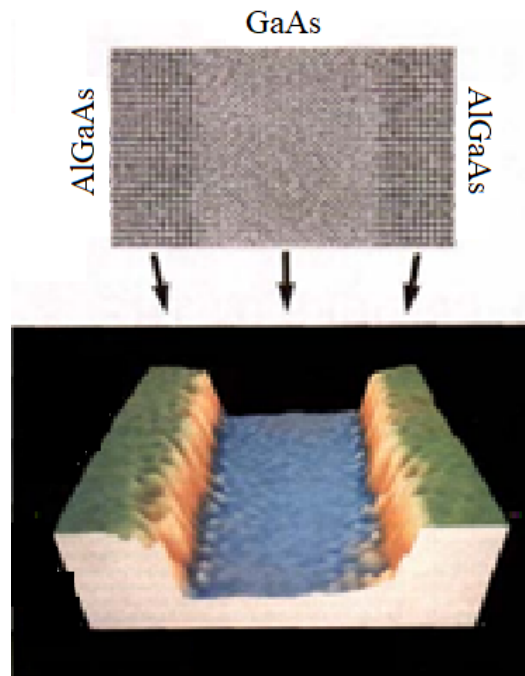


**Figura 2.1:** Modelos básicos de los tipos de confinamiento. Los puntos cuánticos son representados en color rojo. Los nanoalambres con color azul, nanocapas en color verde y por ultimo un material volumétrico con el color amarillo. Para el primer caso, el diámetro ( $D_1$ ) es de magnitud menor a los 100 nm; algo similar debe ocurrir con el diámetro ( $D_2$ ) del alambre, cuya longitud es típicamente mucho mayor a esas dimensiones; finalmente, el grosor de las capas ( $D_3$ ) también es menor a los 100 nm.

construir los pozos cuánticos también es diversa. Se trata de tener una estructura en la que los electrones sólo pueden moverse en un número restringido de dimensiones. Esto se puede lograr tomando dos materiales con diferente comportamiento eléctrico (Fig. 2.2); uno deberá ser un aislante o semiconductor, con una brecha mayor a la del otro material, para que esto impida el paso de los electrones entre los materiales, creando así la especie de “pozo” o cauce en donde podrían moverse los portadores de carga [14]. Así que los pozos pueden tenerse en diferentes dimensiones.

La generación de nanocapas de materia requiere una capa muy fina, o una película, para la que el área resulta infinita si se le compara con el espesor; este último va desde uno hasta 100nm. Además, estas capas son la pauta para poder crear nanotubos, que son una suerte de estructuras cuasi-bidimensionales.

Los nanotubos, como cualquiera de las nanoestructuras, pueden elaborarse partiendo de diferentes compuestos o elementos químicos. Quizá los que detonaron el interés, por este tipo de estructuras, sean los nanotubos de carbón. Estos últimos, como cualesquiera otros, existen en diferentes tipos: pueden ser monocapa, surgir de hojas con bordes en zigzag o brazo de silla, o bien ser quirales, entre otros (Figs. 2.3, 2.4). Según sea el caso, pueden presentar propiedades electrónicas diferentes, pueden comportarse como aislantes, semiconductores o conductores; dependiendo del diámetro y la helicidad de



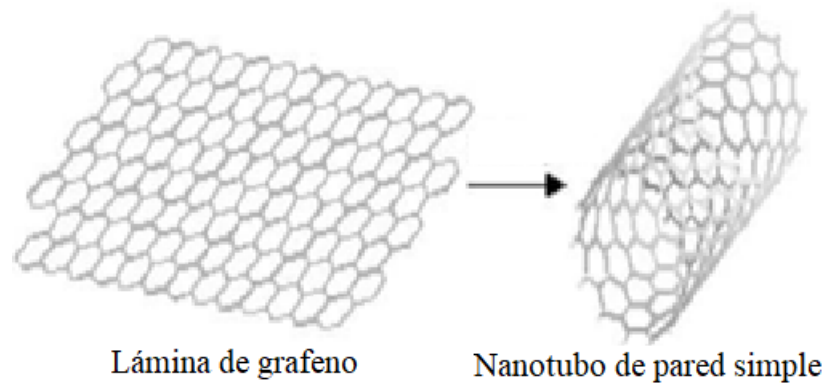
**Figura 2.2:** Modelo de un pozo cuántico de GaAs, delimitado por AlGaAs, tomado de [14].

la estructura. Aunque también es posible que exhiban propiedades magnéticas, ópticas o mecánicas diferentes. Un punto muy importante, asociado a estos nanotubos, es la elevada resistencia mecánica que presentan, pues hay estructuras que suelen ser más resistentes que el titanio [16].

Las técnicas de preparación de las nanoestructuras son tan diversas como las propiedades que tienen asociadas. En particular, los nanotubos pueden ser producidos por medio de diferentes técnicas, como el depósito químico en fase de vapor, la electrólisis o la descarga de arco, entre otras técnicas.

En cuanto a las aplicaciones de mayor interés, quizá las mejor posicionadas sean aquellas asociadas a la creación de memorias RAM no volátiles, a los sensores electrónicos y a la producción de fibras textiles para la fabricación de ropa libre de arrugas o prácticamente imposible de ser manchada [17].

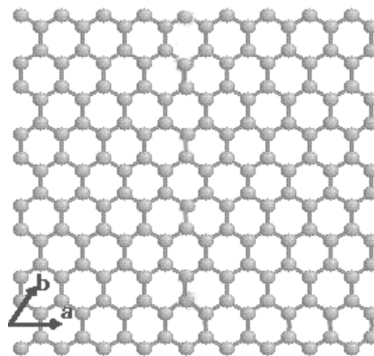
Los puntos cuánticos usualmente son cristales coloidales; es decir, aunque están



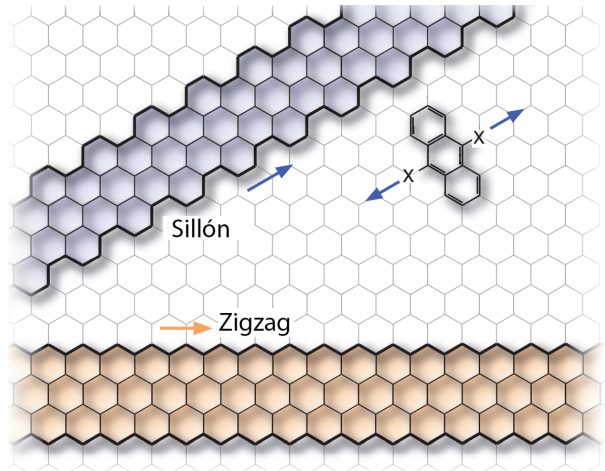
**Figura 2.3:** Nanotubo generado a partir del enrollamiento de una lámina de grafeno. Propuesta de modelo tomada de [15]

constituidos por varios átomos, son lo suficientemente pequeños como para presentar un movimiento browniano. Estos puntos cuánticos o cúmulos están contruidos por átomos ordenados en una estructura cristalina; y, aunque podría pensarse que forman esferas, la geometría de cada cúmulo depende del número de átomos agregados y de la naturaleza de los enlaces entre ellos, entre otras cosas. Los átomos estarán confinados a mantenerse dentro de esas estructuras, que también son denominadas como “átomos artificiales”, pues tienen asociado un conjunto de estados discretos.

Los puntos cuánticos pueden ser sintetizados recurriendo a diferentes métodos; pero



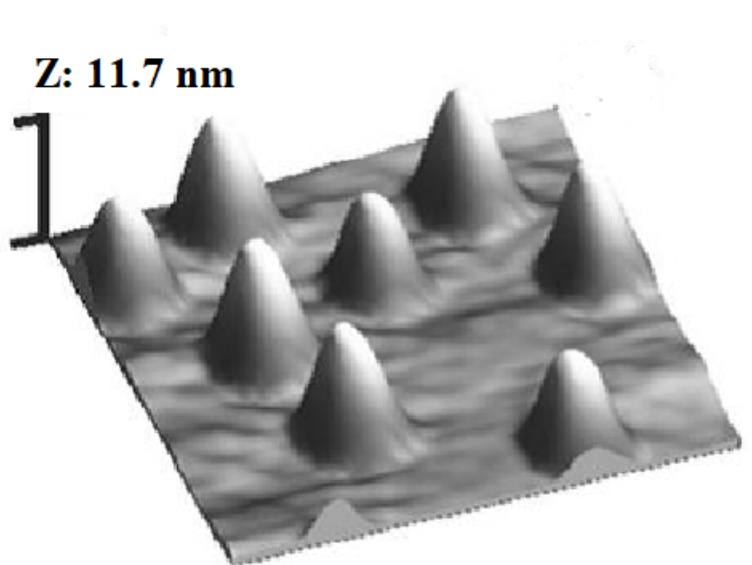
**Figura 2.4:** Lámina de grafeno, mostrando la pareja de vectores en función de los que pueden construirse sistemas chirales [15].



**Figura 2.5:** Nanocintas de grafeno con los bordes con estructura en zigzag y sillón (brazos de silla). Aunque parezca irrelevante, la forma de la frontera modifica el comportamiento eléctrico [18].

uno común es conocido como síntesis coloidal. En este método se requiere disolver una sal, del precursor metálico o del óxido a preparar, recurriendo a un reductor y un estabilizante en una fase dispersante [18].

Los puntos cuánticos son ocupados en áreas múltiples, que van desde la biomedicina hasta la genética molecular; principalmente, se recurre a ellos en el análisis de células. Entre otras ventajas, los puntos cuánticos tienen propiedades ópticas, magnéticas o catalíticas que los hacen atractivos en diversas áreas. Un avance muy significativo es la creación de un dispositivo denominado “lab-on-a-chip” que, a grandes rasgos, consiste en una serie de módulos que pueden llevar a cabo múltiples reacciones químicas simultáneas y con esto disparar indicadores positivos o negativos de las reacciones [19].



**Figura 2.6:** Imagen obtenida al realizar microscopía de fuerza atómica de puntos cuánticos de una celda solar de InAs/GaAs; tomada de [20].



# Capítulo 3

## Fenómenos físicos y nanoestructuras

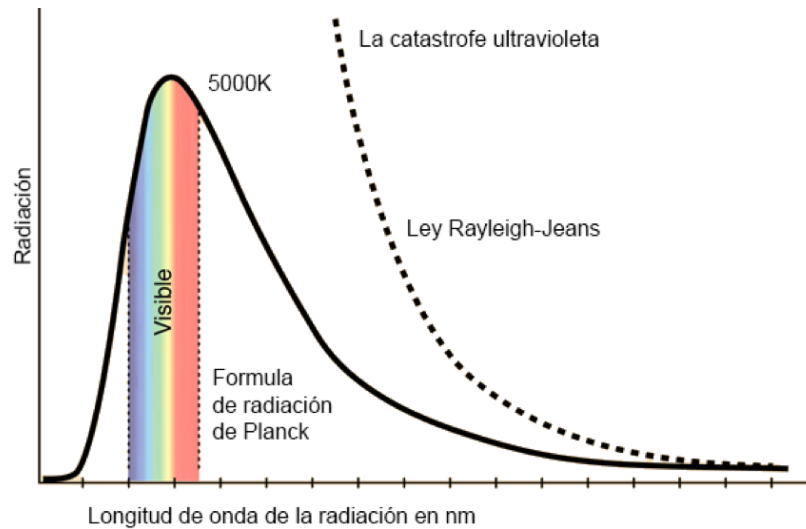


La escala y el confinamiento no son los únicos puntos de interés asociados a las nanoestructuras. Como se ha mencionado, se presentan diferentes fenómenos físicos entorno a los nanomateriales, específicamente debido a que la escala permite que sean notorios los efectos cuánticos. Entre esos fenómenos hay algunos que son esenciales para el entendimiento de la nanociencia, pues están vinculados a los orígenes de la mecánica cuántica. En esta última se busca explicar, de manera más precisa y desde una perspectiva que difiere radicalmente de la correspondiente a la mecánica clásica, el comportamiento observado en ciertos fenómenos, muchos de los cuales se originan por la interacción entre la radiación y la materia. En general, lo anterior da la pauta para generar algoritmos que hagan uso de la teoría e incidan en la computación. Sin embargo, para facilitar el entendimiento de esa teoría fundamental es útil abordar los experimentos cuyos resultados dieron origen a lo que ahora conocemos como la mecánica cuántica.

De manera específica, históricamente resulta importante el problema de la radiación de cuerpo negro; éste último es un objeto capaz de almacenar energía, llegar al equilibrio y emitir la radiación necesaria para mantener el equilibrio térmico con su entorno. A finales del siglo XIX se llegó a una situación que ahora se conoce como la catástrofe ultravioleta. Se creía que el comportamiento del llamado cuerpo negro podía ser descrito mediante las leyes de la física clásica. En concreto, la Ley de Rayleigh-Jeans funcionaba para describir lo que ocurría para frecuencias cuya longitud de onda era grande; pero había una incongruencia, al llegar a las frecuencias de la región ultravioleta, los datos que se obtenían eran completamente absurdos. Fue así que Max Planck propuso uno de los principios de la mecánica cuántica: la energía constituida por paquetes, también denominados cuantos de energía. Esto quiere decir que, aunque la energía viaja de manera continua, puede hablarse de entidades discretas.

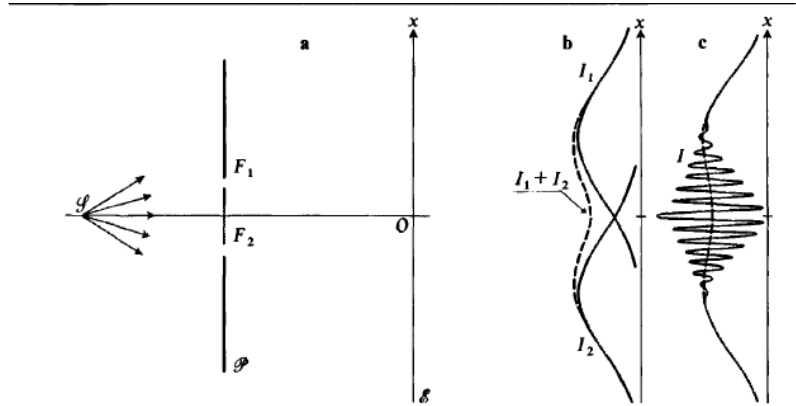
Otro fenómeno que ha resultado de suma importancia para el avance científico y tecnológico actual es el efecto fotoeléctrico; fue estudiado y teorizado por Albert Einstein

y, gracias a él, le fue otorgado el premio novel de física en el año 1921. Dicho efecto se puede observar cuando un fotón impacta una placa de metal y se genera cierta diferencia de potencial eléctrico; esto ocurre porque la energía del fotón, que tiene asociada cierta frecuencia, es absorbida por la placa. Lo curioso de dicha teoría es que está basada en la propuesta cuántica de Planck. [21]



**Figura 3.1:** Distribución de la radiación emitida por un cuerpo negro, como función de la longitud de onda. En la gráfica se comparan curvas que surgen del postulado de Planck y de la Ley de Rayleigh-Jeans (curva punteada).

A partir de la construcción de nuevos conceptos (como la mencionada cuantización de la energía) es como se da pauta a la concepción de la mecánica cuántica, y a su vez a la generación de nuevas teorías que permitan explicar fenómenos que con la física clásica se es incapaz de aclarar. Tratar de entender cómo se comportan los electrones, por ejemplo, puede resultar más simple desde la perspectiva cuántica; puede renunciarse a visualizarlos como partículas y concebirlos como ondas. Tienen un comportamiento un tanto peculiar: desde la visión de la física clásica, los electrones deberían comportarse de forma ondulatoria o de manera corpuscular; sin embargo, cuando un electrón es observado, éste se comportara como una partícula, pero actuará como onda cuando no



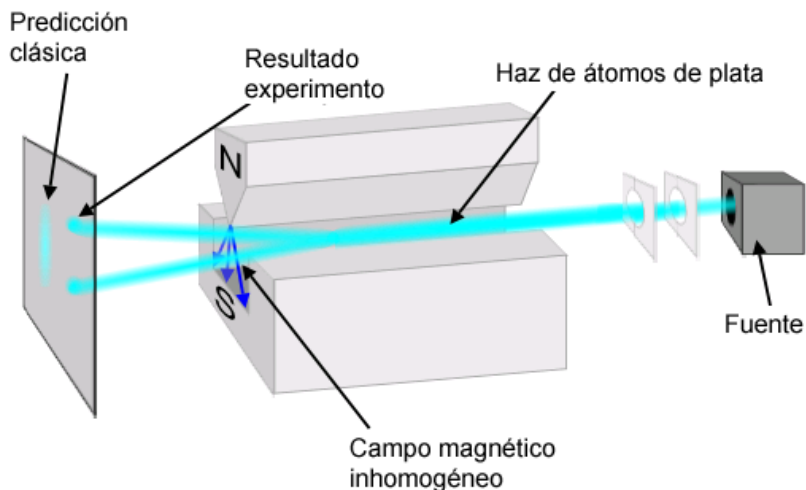
**Figura 3.2:** Experimento de Young. Se puede observar que al emitir la fuente sobre las rendijas  $f_1$  y  $f_2$ , se forma un patrón de difracción en la pantalla b, dicho patrón estaría dado por las intensidades de  $I_1$  e  $I_2$ , cuando están abiertas una a la vez. En la pantalla c podemos observar que, al estar abiertas ambas rendijas, las intensidades  $I_1$  e  $I_2$  no se suman, forman un patrón de interferencia, aunque lo que se esperaría es la suma de ambas intensidades y no el patrón de interferencia.

se encuentre bajo observación alguna. Es decir, que se encuentre en movimiento [22]. En algún momento, Louis de Broglie describió este comportamiento como la dualidad onda-partícula. En un principio se observó dicho comportamiento gracias al experimento de Young, o mejor conocido como experimento de la rendija doble: consiste en dejar pasar un haz de electrones por una primera rendija (para colimarlo), después de esa rendija se encontrará otra rendija (doble, que ocasionará interferencia) y, finalmente, habrá una placa o pantalla donde se impactaran los electrones (Fig. 3.2 a). En síntesis, lo que se debería observar es un patrón construido por ondas (fig. 3.2 c) o por partículas (fig. 3.2 b) que han interferido. Lo que se observe dependerá de las condiciones en que se tome la medición correspondiente, a lo que se hace referencia como el colapso de la función de onda. Será posible tener dos patrones: si el tiempo es corto, parecerá que las marcas en la pantalla se encuentran de manera aleatoria pero, para tiempos suficientemente largos, se observará un patrón de franjas oscuras y brillantes alternadas. Esto último está relacionado con la interferencia constructiva o destructiva de las ondas; así que a los cuerpos puede asociárseles una longitud de onda y pueden ser descritos mediante la función de onda propuesta por Erwin Schrödinger, que puede indicar:

- momento,
- momento angular,
- posición, o
- energía.

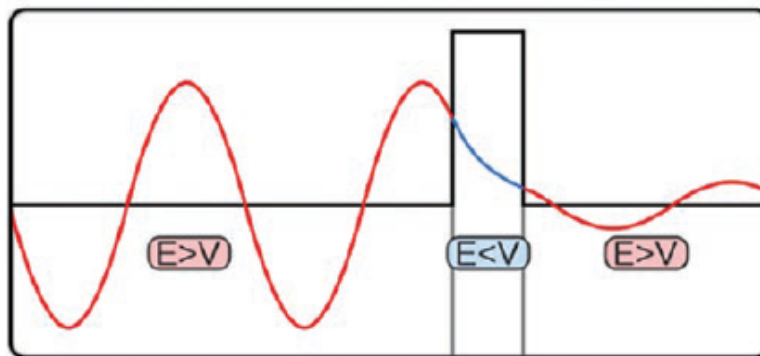
Por otro lado, en 1922, Otto Stern y Walther Gerlach realizaron un experimento con el fin de medir el momento magnético de los átomos. Este experimento consistió en hacer pasar átomos de plata a través de un campo magnético inhomogéneo (Fig. 3.3). Para dicho experimento se genera un haz de átomos de plata y se le hace pasar por una zona en la que se ha producido un campos magnéticos inhomogéneos, con una gradiente a lo largo de un eje específico (Z). Con este experimento se esperaba obtener el momento magnético en función del momento angular orbital; lo que se obtuvo es que el haz sólo se dividió en dos direcciones. Posteriormente, en 1927, se realizaron diferentes modificaciones a dicho experimento, como pasar un haz de átomos de hidrógeno que se esperaba no sufriera ninguna deflexión, pero se dividía en dos. Lo anterior y las hipótesis de George Uhlenbeck y Samuel Goudsmith se introdujo el número cuántico del spin, el cual tiene un valor de  $s = \pm \frac{\hbar}{2}$ .

Aún en el marco definido por ese grupo de conceptos, que permitieron desarrollar una visión novedosa de la naturaleza y de los átomos en particular, el desarrollo de una computadora cuántica suena como algo fuera de lugar; parece que sería mejor seguir desarrollando la tecnología basada en el silicio y los transistores y buscar formas de mejorar la computación clásica. Sin embargo, se puede identificar una limitante: el efecto túnel (Fig. 3.4). Parte de la espectacularidad de dicho efecto radica en el hecho de que, en el mundo de la física clásica, es posible observar la propiedad de impermeabilidad sobre cualquier objeto sólido; es decir, resulta sencillo crear barreras que impidan el paso o salida de diferentes objetos, con lo cual se logra el confinamiento. En el mundo



**Figura 3.3:** Experimento de Stern-Gerlach. Un haz de átomos de plata se hace pasar por un campo magnético inhomogéneo; contrario a lo esperado, el haz se divide en dos y no se mantiene viajando en una dirección única, como se esperaría clásicamente [23]

cuántico, en cambio, el hecho de que un electrón tenga asociada una probabilidad de estar en un espacio determinado, ocasiona que al encontrarse una barrera éste tenga probabilidad de ubicarse después de dicha barrera, aunque la probabilidad sea reducida. Es decir, el electrón tiene asociada una probabilidad de “tunear” entre su posición y la barrera. Así que, para menores barreras la probabilidad de que los electrones se encuentren de un lado u otro de la barrera son mayores.



**Figura 3.4:** Representación del tunelaje cuántico. Una partícula con energía  $E$ , tratando de pasar una barrera con un potencial de energía  $V$  tiene una probabilidad de éxito distinta de cero [24]

Como se comentó anteriormente, es posible que las cargas pasen de un lado de la barrera al otro, con lo cual parece que el principio de un transistor quedaría descartado; sin embargo, al igual que se tienen ciertos inconvenientes al trabajar en estas escalas, también se pueden ocupar múltiples herramientas para obtener los resultados provechosos. En este caso, uno de los elementos de los que se puede hacer uso es el spin del electrón; y esto da lugar a lo que ya se conoce como la espintrónica.

Los fenómenos anteriormente mencionados pueden hacerse presentes en los materiales de dimensiones nanométricas, debido a que cuentan con propiedades únicas que dependen de la estructura geométrica, del número de átomos que contienen y de cómo se acomodan espacialmente los componentes. Con esto podrán adquirir propiedades estructurales, electrónicas, magnéticas y ópticas que difieran radicalmente de las correspondientes a la estructura macroscópica original [23].

Las propiedades estructurales no son más que la forma geométrica que adopta la estructura nanométrica. La forma que tome dependerá del tipo de elementos químicos (y sus enlaces), de la temperatura y su gradiente y del número de átomos con los que cuente el sistema. Pero esa forma geométrica puede incidir notoriamente en las propiedades mecánicas del sistema nanoestructurado y eso se hace evidente en los cúmulos.

Un grupo de estructuras que resultan de especial interés es el conjunto de las que se pueden generar a partir del carbono, pues este elemento tiene una gran capacidad para ligarse químicamente con otros átomos. Esa característica hace que muchos de sus compuestos moleculares adopten una forma de cadena o de anillos. El carbono genera una infinidad de compuestos; si bien se habla mucho del grafito y del diamante por ser dos formas alotrópicas del carbono, se podrían considerar muchas más gracias al descubrimiento de los fullerenos, los cuales son estructuras huecas de carbono.

El arreglo geométrico de las nanoestructuras hará que estas presenten diferentes propiedades electrónicas, magnéticas, térmicas u ópticas. La estructura de la cual se



ha oído mucho en los últimos años es el grafeno, la cual es un derivado del carbono: se trata de una capa similar a la que conforma al grafito. La diferencia es que el grafeno es una lámina bidimensional con un grosor monoatómico.

Un nanotubo es un cilindro hueco y se puede crear enrollando una lámina de grafeno y uniendo sus bordes sobre sí misma. Si bien el grafito como tal no es una estructura muy rígida ni resistente, un nanotubo o el grafeno tienen resistencia y rigidez que pueden superar a las del acero. Los nanotubos se pueden ocupar como conductores eléctricos y térmicos, todo dependerá del diámetro, longitud, quiralidad y cierre de la lámina. Esto último les dará la capacidad de ser conductores, semiconductores o aislantes; así que las aplicaciones para los nanotubos son demasiadas, pero las de interés (para este trabajo) son aquellas que pueden incidir en el cómputo convencional o cuántico.

Los experimentos que evidenciaron la dualidad onda-partícula, el espín electrónico y la cuantización de los estados energéticos, entre otros fundamentos de la mecánica cuántica, junto con el desarrollo de los nanomateriales y la nanociencia en sí, son los que han hecho posible que, en la actualidad, se considere utilizar los efectos cuánticos como los mecanismos que permitan el diseño de dispositivos novedosos en diferentes áreas de interés. De ahí que los pilares de la computación cuántica es el uso del teorema de superposición y el entrelazamiento cuántico.



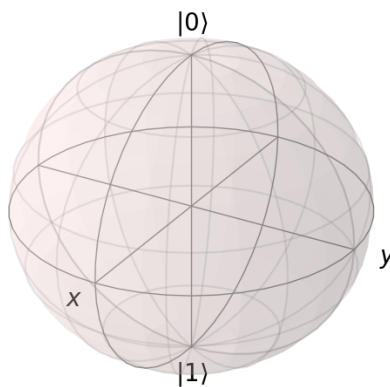
## Capítulo 4

# Lógica en la computación cuántica



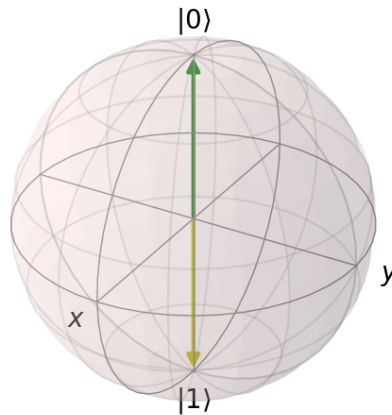
Tratándose de un paradigma nuevo, las computadoras cuánticas deberán ser útiles para ejecutar algoritmos cuánticos; así que no será posible ejecutar un videojuego como Overwatch o instalar Windows en este tipo de computadoras, debido a que su lógica difiere radicalmente de la utilizada en el cómputo convencional. Se requiere rediseñar algunos algoritmos para que sea posible obtener resultados similares a los obtenidos con una computadora convencional [25].

Para entender cómo funciona la información cuántica es necesario hacer uso de una herramienta conocida como la esfera de Bloch, la cual ayuda a interpretar todas las operaciones realizadas con la unidad básica de información cuántica: el qubit. Dicha esfera se puede observar en la Fig. 4.1 y muestra el vector correspondiente al qubit, que puede estar representado por dos estados básicos:  $|0\rangle$  y  $|1\rangle$  (Fig. 4.2). Estos dos signos característicos, llamados ket ( $|a\rangle$ ) y que corresponden a la llamada notación de Dirac, describen el estado físico de un sistema y representan el estado del vector. Para cada vector también existe el vector conjugado; ese está representado por un bra ( $\langle a|$ ) y al producto interno del primero por el segundo se le conoce como un braket, que es un escalar generado mediante una operación vectorial.



**Figura 4.1:** La esfera de Bloch es el espacio donde se puede representar la información de un estado cuántico.

Al igual que en el cómputo convencional, en el cómputo cuántico se cuenta con bits;



**Figura 4.2:** Esfera de Bloch en la que se representan los estados básicos del qubit: los estados  $|0\rangle$  y  $|1\rangle$  con colores verde y amarillo, respectivamente.

estos son operados mediante compuertas y conforman una serie de instrucciones para el procesador. En una computadora cuántica también se cuenta con compuertas y las operaciones actuarán sobre los estados de los qubits, o bien sobre los estados de los vectores asociados a dichos qubit. [26]

Si únicamente se toman en cuenta a los estados fundamentales antes mencionados, no se podrá diferenciar a la computación cuántica de la computación tradicional. Pero existe una diferencia radical: mientras que un bit sólo puede tomar uno de los valores 0 o 1, un qubit puede encontrarse en un estado que sea una combinación lineal de estos dos estados. Es decir, el estado del qubit puede ser una superposición y puede ser representada en una esfera de Bloch (Fig. 4.3). Esto, a su vez, es una compuerta cuántica y es llamada compuerta Hadamard, cuyo papel es aplicar una matriz 4.1.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4.1)$$

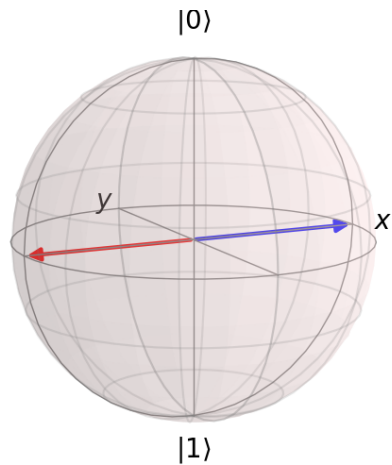
En esos términos, una de las operaciones más sencillas que es posible realizar es la aplicación de las matrices de Pauli; estas harán que un vector gire  $\phi$  sobre el eje  $X$ ,  $Y$

o  $Z$ . Dependiendo del eje en torno al que se desee rotar, el operador recibirá el nombre: compuerta de Pauli- $X$  (4.2) , Pauli- $Y$  (4.3) o Pauli- $Z$  (4.4), según sea el caso.

$$X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (4.2)$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (4.3)$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (4.4)$$



**Figura 4.3:** Esfera de Bloch en donde se representa una superposición cuántica; el  $|+\rangle$  con color azul y el  $|-\rangle$  con color rojo.

Cabe destacar que en el eje  $Z$  de la esfera tendrán los estados deseados; en el eje  $X$  los estados superpuestos y en el eje  $Y$  la combinación de dichas superposiciones. El uso de la esfera es muy conveniente ya que todo vector tendrá que estar acotado a dicha región y no podrá extenderse más allá de la misma; dicho de otro modo: los módulos de los componentes de los vectores que representarán los estados deberán de sumar 1, debido a que la información en los qubits es información probabilística.

Una compuerta “shift” puede modificar la fase  $\phi$  del estado cuántico y dicho cambio se realiza operando la matriz 4.5

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \quad (4.5)$$

Para dos qubits se podrán tener cuatro estados:  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  y  $|11\rangle$ . Además se pueden aplicar las compuertas antes mencionadas, por lo cual al tener una operación significaría que tenemos 50 % de probabilidad de medir 0 ó 1 en ambos qubits. Operar los qubits de esta forma sería lo equivalente a operarlos unitariamente; sin embargo, se cuenta con operaciones que pueden ser ejecutadas considerando el estado de un qubit, al cual se llama qubit de control. Un qubit de control, junto con una operación extra, determinarán el estado de un qubit objetivo. Tomando lo anterior como base se generan nuevas compuertas cuánticas, como la CNOT, a las cuales es posible aplicar una matriz 4.6; para el caso específico de la CNOT se generaría una tabla de estados 4.1, para los que cabe destacar que el qubit de control será el primero, de izquierda a derecha, dentro del ket.

Estado Inicial	Estado Final
$ 00\rangle$	$ 00\rangle$
$ 10\rangle$	$ 10\rangle$
$ 01\rangle$	$ 11\rangle$
$ 11\rangle$	$ 01\rangle$

**Tabla 4.1:** Estados iniciales y finales, al aplicar una compuerta CNOT, donde el qbit de control es el que se encuentra a la derecha de cada ket y el qbit de destino es el de lado izquierdo del ket.

$$CNOT = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \quad (4.6)$$



Se han comparado los procesos de cifrado y descifrado de datos, así como la velocidad con la que se realizan dichos procesos, para respaldar las ventajas que ofrece el nuevo paradigma de la computación. Pues bien, para que una computadora convencional evalúe una cadena de cuatro bits, por ejemplo, se necesitaría que esta sea evaluada, en el peor de los casos, 16 veces; se podría decir que en una computadora cuántica es lo mismo, podríamos evaluar uno a la vez y, probablemente, dicho cálculo demore más tiempo. Sin embargo, la diferencia radica en el tipo de algoritmos que es posible ejecutar; en una computadora convencional es imposible usar la mecánica cuántica a favor del usuario, así que no es posible ejecutar un algoritmo cuántico, pero obviamente en una computadora cuántica si es posible. Así que, en vez de realizar 16 evaluaciones, únicamente se realizaría una, pero esto haría que el resultado se encuentre entre 16 resultados posibles y se regresa al mismo punto de partida. Para encontrar una solución se cuenta con el algoritmo de Grover, que permitirá descartar los 15 resultados menos probables, dejándonos con uno solo. Por ende, es posible deducir que atacar los problemas desde la computación cuántica requerirá rediseñar algoritmos y pensar diferente. Es equivalente a escoger un algoritmo para acomodar datos y evaluar cuál es la mejor opción según sea el caso [25].

Una computadora cuántica tiene la capacidad de realizar las operaciones antes mencionadas; sin embargo, no será capaz de ejecutar un programa convencional, puesto que la información se manipula de manera diferente. Es posible emular ciertas operaciones clásicas con una computadora cuántica, igual que se emulan operaciones cuánticas con una computadora clásica; sin embargo, no es el proceso óptimo. El hecho de poder aplicar compuertas cuánticas a los qubits nos da la libertad para diseñar algoritmos cuya complejidad sea menor a la complejidad que tendría un algoritmo clásico. Esto se verá reflejado directamente en la cantidad de cálculos que deberá realizar la máquina e, indirectamente, se tendrá un tiempo de ejecución menor. Debido a que este tipo de

tecnologías se encuentran en desarrollo, no se tiene la estabilidad deseada, por lo tanto, no es posible hablar de que se tenga una velocidad mayor a la de los procesadores de última generación. Aquí es donde aparece el concepto de supremacía: una computadora cuántica deberá de tener un gran número de qubits para poder rebasar, en tiempo de ejecución, a una computadora convencional.

El primer aporte en la rama de la computación cuántica fue realizado por el premio nobel Richard Feynman. En 1982 propuso que una computadora podría ser capaz de usar las propiedades de la mecánica cuántica; pero fue hasta 1995 cuando el primer algoritmo cuántico fue propuesto por Peter Shor (el algoritmo Shor), con el cual propuso calcular las raíces de un número primo, haciendo uso de las propiedades cuánticas.

Uno de los algoritmos más sencillos es el de Deutsch-Jozsa [27]: nos permite evaluar una función  $f(x)$ , tomando como entrada una cadena de  $n$ -bits en  $x$ , lo cual entrega 0 o 1 como datos de salida. El problema consiste en determinar si la función es constante o balanceada haciendo el menor número de evaluaciones posibles. Esto, en computación clásica, tomaría  $2^{n-1}$  evaluaciones, en el peor de los casos. Con el algoritmo de Deutsch-Jozsa el problema sería resuelto haciendo sólo una evaluación.

Aparentemente no resulta tan atractivo el algoritmo Deutsch-Jozsa como para pensar en construir una computadora cuántica; sin embargo, este conduce a un algoritmo que le da sentido al desarrollo de dicha tecnología: el algoritmo de Grover. Este algoritmo permite resolver el problema de búsqueda no estructurada, que se genera al buscar un dato característico  $w$  en una lista de  $N$  elementos. Recurriendo a la computación convencional tendríamos que realizar  $N$  comparaciones, en el peor de los casos, para encontrar el dato característico; en cambio, recurriendo a la computación cuántica, bastaría con realizar  $\sqrt{N}$  evaluaciones [28].

En cuanto a la seguridad informática, el algoritmo de Shor resulta ser un punto clave. Como se mencionó antes, gran parte de la criptografía moderna (como el algoritmo

RSA y sus derivados) se basa en el uso de números primos muy grandes. Factorizar dichos números, de manera “clásica”, es posible realizando un número de operaciones del orden de  $O(\exp(\frac{64}{9}n^{\frac{1}{3}}(\log(n))^{\frac{2}{3}}))$ , siendo  $n$  el número de bits usados para representar el número buscado. En cambio, recurriendo al algoritmo publicado por Peter Shor (1994), es posible realizar esa tarea realizando un número de operaciones del orden de  $O(\log(n))$ , en una computadora clásica [29].

Tomando estos algoritmos como pilares, y al igual que sucedió con la computación y la informática cuando se tenían algoritmos muy sencillos, es posible prever que la computación cuántica será capaz de traer soluciones a múltiples campos del conocimiento, como ocurre con las redes neuronales, para las que se están diseñando algoritmos que provean la capacidad de incluir una mayor cantidad de píxeles (incluso los colores) dentro de las matrices que sirven para entrenar a las redes [30]. Por otro lado, en el área de la química se están logrando avances al simular moléculas de la naturaleza (p. ej. el caso de la cafeína) que, a pesar de ser moléculas simples, requieren mucho poder de procesamiento y memoria para poder simularse[31].

La plataforma IBM Q Experience ofrece la posibilidad de practicar con un simulador de una computadora cuántica, pero también con una computadora cuántica mediante un servicio en la nube. Esta oferta permite preparar a los futuros desarrolladores “cuánticos” y, paralelamente, generar cada vez más algoritmos. La plataforma mencionada cuenta con dos herramientas muy importantes: un editor visual, con el que es posible aplicar las compuertas cuánticas construyendo circuitos, y un *kit de desarrollo de software* (SDK, por sus siglas en Inglés) para el lenguaje de programación Python, que permite integrar de una manera muy sencilla ambas tecnologías sin hacer uso de nuevos lenguajes. Particularmente, esto último resulta ser la herramienta más llamativa para los desarrolladores de software.



# Capítulo 5

## Dispositivos nanoestructurados



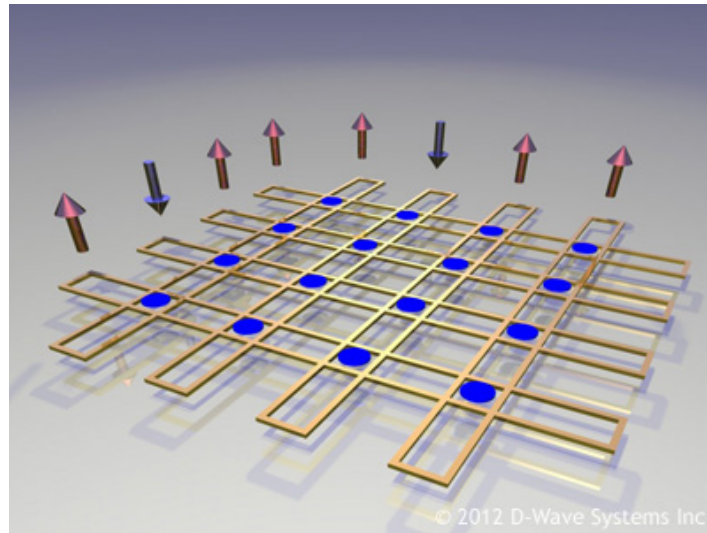
Es importante destacar que el desarrollo de las nanociencias ha generado diferentes soluciones para la implementación de dispositivos que puedan manipular principios cuánticos. Podría citarse, por ejemplo, el caso de los generadores de energía solar (aunque los dispositivos tradicionales no requieren de elementos nanométricos), en los cuales se hace uso del efecto fotoeléctrico para generar un potencial. Sin embargo, la discusión se centrará en los dispositivos nanoestructurados que se han generado con la finalidad de realizar la manipulación de información cuántica, como los molbytes, moléculas orgánicas que pueden almacenar información y funcionan como dispositivos de lectura y escritura [32].

Cabe mencionar que los prototipos de computadoras cuánticas, e incluso las computadoras “comerciales” actuales, hacen uso de diferentes efectos cuánticos para implementar las múltiples técnicas en torno a la información. Sin embargo, este trabajo estará enfocado en aquellas computadoras para las que resulta relevante el entrelazamiento y la superposición cuántica.

Como se mencionó en el capítulo anterior, la superposición se mueve entorno a compuertas cuánticas, o lo que es igual, operaciones para manipular los vectores que representan a un qubit. El tener compuertas que generen dichas operaciones es sin duda algo muy ambicioso debido a que no se cuenta con compuertas universales, esto es principalmente por las técnicas para manipular los estados de los qubits, razón por la cual los prototipos varían con respecto al tipo de compuertas “avanzadas”. Por consiguiente, se analizaron los intentos por realizar entrelazamiento cuántico y superposición, sin tomar en cuenta el tipo de operaciones que se puedan realizar con los qubits.

Un prototipo que sin duda es llamativo es el que implementa la empresa D-WAVE. Este prototipo genera una conexión de qubits por medio de un dispositivo superconductor de interferencia cuántica (SQUID, por sus siglas en inglés), el cual consiste en generar un bucle de superconductividad, mismo que está compuesto por una unión Jo-

sephson y una inductancia. Es necesario que todas las uniones sean idénticas, por lo cual estas uniones son reguladas mediante un campo magnético. Cada qubit cuenta con tres etapas: una de ellas es un regulador de inductancia, para la unión Josephson; posteriormente pasa por una compensación de corriente persistente que mantiene el flujo de corriente constante a medida que se realiza el recorrido del circuito (Fig. 5.1)



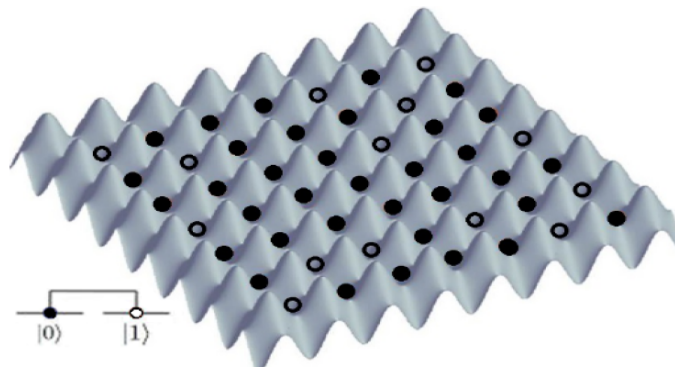
**Figura 5.1:** Bucle de qubits con SQUIDs; se muestra la distribución de los qubits, que se encuentran representados con color azul.

Una computadora cuántica debe ser capaz de realizar una corrección de error cuántico; es decir, deben de ser capaz de corregir el ruido que entra a ella y por ende es necesario estabilizarla para que sea capaz de mantener su estado cuántico. A esto se le llama inicialización y, dependiendo del prototipo, suele tener algunas deficiencias en el tipo de perturbaciones que entran al sistema. Por ejemplo, para una computadora basada en un SQUID se genera demasiado calor, por lo cual requerirá ser enfriada a una temperatura de 15 mK (180 veces más frío que el espacio interestelar). En principio suena complicado, pero si se analizan los beneficios que proporcionan los superconductores y los nanomateriales, se convierte en una posibilidad [33].

Si bien se ha hablado de modelos con diferentes limitaciones, las computadoras cuánticas de trampas de iones son las que han logrado mejor rendimiento, y es por



ello que la discusión se centrará en ellas. La técnica consiste, básicamente, en tomar átomos ionizados y “atraparlos” con la ayuda de campos electromagnéticos. Esto es muy factible, ya que permite considerar que, por cada trampa, se tendrá un qubit y éste puede ser acomodado como se presenta en la Fig. 5.2. Gracias a que las partículas se encuentran atrapadas, es posible manipular su carga por medio de un laser (la hará girar) y esa carga será la que se utilizará como vector de información para el qubit.

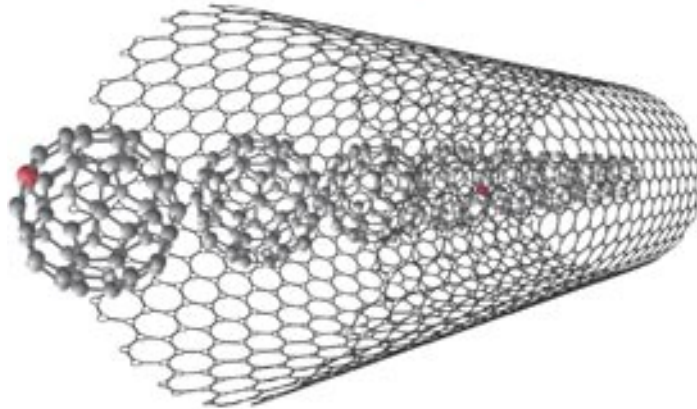


**Figura 5.2:** Arreglo de trampas de iones, en el que se pueden observar los estados fundamentales de los qubits.

Uno de los fenómenos cuánticos que se pretende manipular es el entrelazamiento cuántico, pues esto tendrá un gran impacto en las comunicaciones y en la seguridad de la información. Se ha logrado entrelazar partículas, por medio de una técnica conocida como espacios de diamantes. En esa técnica se aprovecha la falta de un átomo de C (en la superficie del diamante) y se llena dicho espacio con un átomo de N. De esta forma es posible manipular el espín del átomo de N. Esta técnica permite conservar la superposición y, de igual forma, entrelazar las partículas de manera efectiva.

Hay un modelo muy interesante que depende de una Memoria de Acceso Aleatorio Cuántica (QRAM, por sus siglas en inglés) y de una Unidad Lógica y Aritmética Cuántica (QALU, por sus siglas en inglés). La razón por la que dicho modelo resulta atractivo es que se pretende sea controlado directamente con señales clásicas, lo cual permitiría tener una computadora cuántica “híbrida”.

Las computadoras cuánticas basadas en el uso de la Resonancia del Espín del Electrón (ESR, por sus siglas en inglés) pretenden usar el espín de las moléculas dentro de los fullerenos (Fig. 5.3).



**Figura 5.3:** Peapod. En la imagen se puede observar un nanotubo, a modo de “vaina”, con “guisantes” en su interior.

Se puede notar que se está teniendo un desarrollo notable en la implementación de computadoras cuánticas funcionales, pero se está lejos de lograr lo que se pretende sea una supremacía cuántica. El rendimiento que pudiese tener una “computadora de alto rendimiento” sin duda opacaría, en una simulación, a una computadora cuántica; sin embargo, los efectos que se presentan (y se explotan) en las computadoras cuánticas, nos dejan con la tarea de seguir investigando e implementando nuevos nanomateriales para sumar esfuerzos y poder ver un progreso para cuando la ley de Moore se vea cumplida.

# Conclusiones



Se observa que el diseño y construcción de una computadora cuántica a simple vista es algo muy complicado y que una vertiente es seguir desarrollando algoritmos que exploten los recursos de una computadora de una mejor manera, sin embargo, al igual que sucede con la diferencia de procesamiento que entrega un CPU contra un GPU, podemos afirmar que al ocupar prototipos de computadoras cuánticas y buscar que algoritmos cuánticos resuelvan problemas ya existentes se logrará que hagamos de la computación algo más robusto. Se puede observar que las PC, celulares inteligentes e incluso relojes, cuentan no solo con un CPU, si no también con un GPU y en algunas ocasiones con un NPU, mismos que facilitan tareas específicas, pero que dejan al CPU libre de carga en muchas ocasiones, con lo cual podríamos ejecutar programación paralela, justo lo que ocurre con los programas CUDA de NVIDIA, mismos que buscan resolver problemas de arquitectura, imagen en medicina o ciencia ambiental [34]. También contamos con aplicaciones para biométricos, las cuales tienen una unidad NPU que hace todo el trabajo de cómputo, con lo cual aseguran que una vez sea autenticado el usuario pueda continuar con sus tareas sin tener retrasos en el uso del CPU [1].

Al igual que las unidades de estado sólido dieron un avance significativo para el rendimiento de la PC en la actualidad y de como servicios WEB como los de Google o Facebook facilitan el desarrollo de aplicaciones. Es sencillo observar que el desarrollo de prototipos de computadoras cuánticas operadas por servicios WEB facilitarán las tareas de seguridad para los programadores y también para el desarrollo científico y tecnológico.

Computadoras para aprendizaje profundo de alto rendimiento como NVIDIA SATTURNV, o los prototipos de Google Stadia para videojuegos, prueban que las tendencias apuntan hacia realizar cómputo en la nube, esto sumado a la plataforma que ofrece IBM para cómputo cuántico y las implementaciones de D-WAVE por medio de servicios web, dan pauta a pensar que todo lo relacionado a futuros prototipos se generará por servicios WEB, por lo cual se entiende que no podrán ser usadas como una computadora

personal. Sin embargo las soluciones que pretende resolver los problemas presentados en este trabajo, ayudarán al desarrollo de redes neuronales, simulaciones y como se mencionó antes de la seguridad informática.

Es un hecho que con esta tecnología se prevee un rediseño en la seguridad cibernética actual, sin embargo las posibles soluciones estarían a cargo de la computación cuántica, en principio el entrelazamiento cuántico es una propiedad muy atractiva para implementar codificación y seguridad, ya que si un qubit se encuentra superpuesto y este a su vez es interceptado para verificar la información que contiene; este sería determinado en un estado fundamental y se sabría el momento en que este fue vulnerado. Por lo cual estarémos en posición de responder a los ataques de manera inmediata.

Es importante destacar que el desarrollo de la nanociencia ha generado diferentes soluciones para la implementación de dispositivos que puedan manipular principios cuánticos, es bajo esta premisa que aseguramos que el desarrollo de la computación cuántica estará relacionada a la síntesis de nuevos nanomateriales, mismos que optimicen la temperatura, decoherencia y velocidad de los procesos para aplicar las acciones cuánticas de los qubits.

Hay que tener conciencia de que esta rama es un área en pleno crecimiento y el desarrollo de la misma depende de los prototipos que se generan luego de haber estudiado los principios cuánticos y de poder elaborar tecnología que nos permita manipular dichos efectos, lo cual va de la mano con encontrar y sintetisar materiales optimos.

# Bibliografía

- [1] Introducing qualcomm zeroth processors: Brain-inspired computing.
- [2] Asano, S., Maruyama ,T., Yamaguchi ,Y. Performance comparison of fpga, gpu and cpu in image processing. *2009 International Conference on Field Programmable Logic and Applications.*, page 126, 2016.
- [3] Douglas, R., Maura, B. *Cryptography Theory and Practice*. CRC Press, 4a edition, 2019.
- [4] I. B. M. Research. IBM q experience.
- [5] UPM. Seminario de introducción a la computación y criptografía cuántica 1.
- [6] Sipser M. *Introduction to the Theory of Computation*. CENGAGE Learning, 3rd edition, 2013.
- [7] Wikipedia contributors. Abdur rafey masood, 2017.
- [8] Intel. Transistors to transformations. 2012.
- [9] J. C Cheang. Revista digital universitaria. *Revista Digital Universitaria*, (6):6:2–6:9, 2005.
- [10] Kumar S. Fundamental limits to moore’s law. *Journal of Experimental Algorithmics*, 2006.

- [11] Wikipedia contributors. Transistor count, 2019.
- [12] Paul A. B. Int. j. theor. phys. pages 177–201, 1982.
- [13] Desai, S., Madhvapathy, S., Sachid, A., Llinas, J., Wang, Q., Ahn, G. Mos2 transistors with 1-nanometer gate lengths. *Science*, page 99, 2016.
- [14] Cuevas J. *Propiedades electrónicas de alambres cuánticos de carburo de silicio tipo B*. Instituto Politécnico Nacional.
- [15] Maubert M., Soto L., León A., Flores J. Nanotubos de carbono - la era de la nanotecnología.
- [16] Isadora B. *Síntesis y caracterización de nanomateriales 0D, 1D y 2D*. Universidad Autónoma de Madrid, 2013.
- [17] Felipe D. *Introducción a los nanomateriales*. Universidad Nacional Autónoma de México, 2012.
- [18] Ruffieux P., Wang S., Yang B., Sánchez C., Liu J., Dienel T. On-surface synthesis of graphene nanoribbons with zigzag edge topology. *Nature*, 1(531):531:489, 2016.
- [19] Pombo B., Goyanbes V. Revista complutense de ciencias veterinarias. 1(5):69–102, 2011.
- [20] Gélvez A., Gutierrez W., Rodriguez F. Efecto aharonov-bohm en puntos cuánticos no uniformes. *Innovaciencia*, 1(3):9–17, 2015.
- [21] Einstein A. *On a Heuristic Point of View about the Creation and Conversion of Light*. 1905.
- [22] Robert E., Robert R. *Física cuántica. Átomos, moléculas, sólidos, núcleos y partículas*. Limusa, 2018.



- 
- [23] Morán J., Rodríguez J. *Los materiales nanoestructurados Sus propiedades y aplicaciones en la revolución científica y tecnológica del siglo XXI*. Fondo de Cultura Economica, 1a edition, 2013.
- [24] Silva V. *Practical quantum computing for developers*. FApress, 1a edition, 2019.
- [25] Thomas E., Catherine D., Rober M., Federico S., Jeremy L., Gangotree C. A study of complex deep learning networks on high performance, neuromorphic, and quantum computers. *2nd Workshop on Machine Learning in HPC Environments IEEE*, 2016.
- [26] Ladd T., Jelezko F., Laflamme R., Nakamura Y., Monroe C., O'Brien L. Quantum computers. *Nature*, 464:45–53, 2010.
- [27] IBM Q Team. Deutsch-jozsa algorithm, 2018.
- [28] IBM Q Team. Grover's algorithm, 2018.
- [29] Hayward M. Quantum computing and shor's algorithm, 2019.
- [30] Temme K., Gambetta J. Researchers put machine learning on path to quantum advantage, 2019.
- [31] IBM Q Team. Quantum chemistry, 2019.
- [32] Syllaymanov Y. Storing information in molbytes. *Science*, page 1147, 2019.
- [33] D-Wave Systems Inc. The d-wave 2x, 2015.
- [34] Sander, J., Kandrot, E. *CUDA by example*. Addison Wesley, 2011.