UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

VIABILIDAD DE LA TELETRANSPORTACIÓN CUÁNTICA

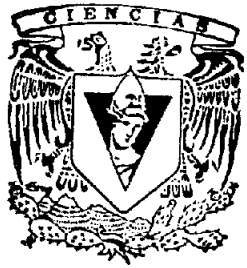
T E S I S

Que para obtener el título de:

F I S I C O

Presenta:

ROMÁN CARLOS BURGOS HIDALGO



FACULTAD DE CIENCIAS
UNAM

Directora de Tesis: Dra. Hilda Noemí Núñez Yépez
Asesor de Tesis: Dr. Rodolfo Patricio Martínez y Romero

2003

m351307

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

VNIVERDAD NACIONAL
AUTÓNOMA DE
MEXICO

ACT. MAURICIO AGUILAR GONZÁLEZ
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
Presente

Comunicamos a usted que hemos revisado el trabajo escrito:

"Viabilidad de la Teletransportación Cuántica"

realizado por Burgos Hidalgo Román Carlos

con número de cuenta 09128045-1 , quien cubrió los créditos de la carrera de:Física

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Director de Tesis Propietario	Dra. Hilda Noemí Núñez Yépez	
Propietario	Dr. Rodolfo Patricio Martínez y Romero	
Propietario	M. en C. Arturo Hugo Nieva Gochicoa	
Suplente	Dr. Roberto José Raúl Gleason Villagrán	
Suplente	Dr. Roberto Allan Sussman Livovsky	

Consejo Departamental de Física

M. EN C. ALICIA ZARZOSA PEREZ

A los Héroes anónimos que
dieron y dan su vida por la Revolución,
los que construyen por la esperanza,
los que no escatiman en esfuerzos,
los que siguen luchando a pesar de todo,
los indispensables.

Resumen

En este trabajo se abordan los prolegómenos de la teoría de la computación clásica, se explican las ideas fundamentales alrededor de la máquina de Turing; se exponen las ideas centrales y experimentos más relevantes sobre la "paradoja" EPR y las desigualdades de Bell. Se tratan las ideas fundamentales sobre la computadora cuántica, así como los problemas prácticos a enfrentarse en su construcción. Finalmente se explica en detalle el fenómeno de la teletransportación cuántica, se discuten los experimentos relacionados y algunos campos de aplicación.

Agradecimientos

Como lo marca la tradición: primero que nada agradezco a mamá Delia y papá Alejandro por inducirme por este largo y sinuoso —pero gratificante— camino de la Ciencia. Gracias a sus atenciones y el tiempo de su vida que decidieron dedicarnos a sus hijos. Espero que no se sientan defraudados.

Gracias a mi asesora Noemí Nuñez por todas las atenciones y facilidades que me brindó para realizar este trabajo. Por su confianza y comprensión. En su pequeño cubículo de la UAM encontré muchas ideas inspiradas en sus valiosos comentarios.

Gracias a Rodolfo Martínez por toda la atención y facilidades brindadas.

Gracias a Georguii Katchatourov y al proyecto 34812-A del CONACYT por el financiamiento brindado. La Física siempre se quedaría en sueños y buenas intenciones de no ser por apoyos de este tipo.

Un sincero agradecimiento a Roberto Gleason; sin su estricto (pero ameno) escrutinio no habría podido entender muchas aparentes sutilezas de primera importancia.

Gracias a mis sinodales Arturo Nieva, y Roberto Sussman.

Gracias a mis hermanitos Inti, Alejandra, Luis y Saraí por su cálida compañía y solidaridad.

Gracias a mi querida Lau "My bridge over troubled waters". Sin su confianza, solidaridad y cariño no hubiera podido seguir.

Gracias a mi sensei Juan Carlos Álvarez por su gran apoyo y tosco —pero muy valioso— aliento, en las buenas y en las malas, por las buenas o por las malas.

Gracias a mi amigo Oscar "El joven" por el estilo que intenté tomarle prestado (sin éxito) y por haber compartido conmigo algunos buenos odios en estos tiempos endemoniados.

Gracias a Cesar "El Garoj", por su claro y sincero consejo, la compañía, la ayuda, la amistad.

Gracias a Elodie Calas por haber sido mi musa y por financiar un fragmento de este trabajo.

Gracias por todo a Vera. ¿Cómo iba a saber que me tardaría tanto?

Gracias a mis amigos Gualberto "El Guajalote", Alejandro, Lalo, Octavio, Bartolo "El Bart", Roberto "El reverendo", Chío, Martha "La Tucita", Marcos "El Ata", Ana, Anita, David, Beto "El Kiko", Leti, Zeus, Gilbran, Estebancito "El Pepito", Tlalli "El Sandi", Mayrita, Gerardo "El pollero", Adair "El Mara", Alejandro, Lourdes, Karel, Arturo "El chiquilín". Amigos de verdad.

Finalmente gracias a la Facultad de Ciencias y a la Universidad Nacional Autónoma de México, por acogerme en su seno (por tantos años). Siempre, y a pesar de todo, por su azul y oro luché sin cesar.

Índice

Introducción

Durante el siglo XVII la humanidad (es decir, el mundo científico occidental, ya que los que sabían leer para entonces eran una minoría y el contacto con el oriente era casi nulo) fue testigo de una de las revoluciones científicas más espectaculares e importantes de su historia. El principal protagonista del suceso fue el neurótico científico inglés Isaac Newton, también conocido por sus huertos de manzanas. Además de su trabajo científico en sí, llevó hasta límites nuevos y asombrosos algo que ya practicaban los científicos griegos, artistas y demás intelectuales: *la abstracción*. En Ciencia, muy en particular, la abstracción permitió resolver problemas complejos, separando sus partes e inventando variables medibles para poder entender los sistemas físicos. Así nacieron los conceptos comunes a todos los sistemas físicos como la Energía, el Potencial, el Momento, la Carga, etc., y también las ecuaciones que los relacionan entre sí y con otras magnitudes. Estas ecuaciones además permiten expresar a cada magnitud de diversas maneras sin pérdidas de información.

Entonces, si se tiene suficiente información sobre un sistema, se pueden hacer predicciones; podemos decir que entendemos el sistema. Pero la información misma puede tomarse como una variable más del sistema y también se puede expresar de diferentes maneras, sin pérdidas significativas; basta elegir un lenguaje, que simplemente es un código predeterminado que se usa para expresarla, y que el receptor cuente con el mismo código; esto resulta un hecho significativo. El almacenamiento y transmisión de información siempre tiene un sustento material, cualquiera que sea el lenguaje utilizado (es decir que se necesitan palabras, caracteres escritos, bits en las superficies de discos compactos o disquets, etc.). La información de hecho es un parámetro importante de los sistemas físicos, a semejanza de la energía o el momento. Hasta inicios del siglo XX, la información en los sistemas físicos sólo estaba implícita en conceptos tales como la entropía.

Desde este punto de vista, la Física fundamental ya no sólo se preguntará por determinar las magnitudes de las variables que se estudian de tal o cual sistema, sino que ahora aparece un nuevo problema fundamental para la Física: descubrir las formas en que la naturaleza permite o impide el expresar o manipular la información.

El que la información se pueda expresar de distintas maneras sin pérdidas significativas, y el que la información tenga un sustento material, tanto para su almacenamiento como para su transmisión la hacen susceptible de ser manipulada por una máquina real, de "carne y hueso". La primera máquina capaz de efectuar algoritmos (aparte de los ábacos, si se les considera como máquinas) de que se tiene noticia es la Pascalina, una máquina con una serie de ruedas contadoras que Blaise Pascal construyó en 1642 para su padre, que era recaudador de impuestos de la corona francesa. Con ella se podían hacer sumas y restas moviendo una manivela que movía sus discos dentados hasta obtener el resultado. Después se construyeron muchos otros artefactos mecánicos que también podían multiplicar y dividir y que más tarde usaron electricidad para mover sus engranes.

Otro precursor importante, que sentaría las bases de la Ciencia Computacional, fue Charles Babbage (1791-1871), un profesor de matemáticas de la Universidad de Cambridge. Él concibió varias máquinas lógicas basadas en engranes, entre las que se encontraba una máquina analítica que contenía los elementos más esenciales de una computadora moderna. La tecnología de su época no permitió construirla, ya que hubiera necesitado un motor de vapor grande, miles de engranes, pequeños y grandes, y hubiera sido del tamaño de un campo de fútbol, sin mencionar lo que habría costado (Penrose 1996). Las contribuciones de Ada Byron también fueron significativas.

Alan Turing (1912-1954) es el que se considera el verdadero padre de la Informática. A mediados de la década de 1930 describió su Máquina Universal. Su principal aportación consistió en determinar qué era lo que exactamente podría realizar una máquina de calcular, y en determinar la importancia de la programación, lo que hoy se conoce como *software*, de la máquina (Clauser y Shimony 1978). El trabajo de Turing a su vez se basó en los trabajos que otro par de matemáticos habían realizado: David Hilbert y Kurt Gödel (Penrose 1996).

Hilbert enfatizó la importancia de hacer las preguntas fundamentales acerca de la naturaleza de las matemáticas, en vez de preguntarse si tal o cual proposición matemática es correcta. En un congreso de matemáticas Hilbert dio a conocer su famoso Décimo problema —el "*Entscheidungsproblem*"— que fue formulado de la siguiente manera: "¿Existe un procedimiento mecánico [automatizable] general que pueda, en principio, establecer

la verdad o falsedad de cualquier proposición matemática bien definida?". Las ideas de Hilbert iban más allá de simples demostraciones matemáticas, tenía un programa que pretendía situar a las matemáticas sobre una base inatacable, es decir, encontrar para cualquier área bien definida de las matemáticas, una lista definitiva de axiomas y reglas de inferencia suficientemente amplia que incorporara *todas* las formas de razonamiento matemático correcto apropiadas para dicha área. Esta lista proveería un criterio definido (y definitivo) para saber si es correcta la demostración matemática de cualquier proposición dentro de dicha área de las matemáticas. Además este sistema de axiomas y reglas sería completo, es decir, nos permitiría en principio, distinguir la verdad o falsedad de cualquier enunciado matemático (sintácticamente correcto) que pueda formularse dentro del sistema. Esto es precisamente con lo que acabó Kurt Gödel, demostrando la existencia de proposiciones sintácticamente correctas dentro de sistemas lógicos formales, que no son demostrables ni refutables (Penrose 1996).

La aportación de Turing fue resolver el Décimo Problema de Hilbert. Para ello ideó un dispositivo teórico mecánico conocido como *la máquina de Turing* (Bell 1965), que era lo suficientemente complicada como para resolver problemas matemáticos bastante sofisticados, pero suficientemente simple como para analizarla a detalle. Turing usó su máquina para mostrar que suponer la existencia de medios mecánicos para establecer si una proposición matemática puede ser probada o no, lleva a una contradicción. Más adelante hablaré más sobre la máquina de Turing.

Las ideas de Turing han servido como fundamento teórico para llevar a cabo todas las computadoras electrónicas realizadas hasta nuestros días. Ha sido un largo recorrido desde las gigantescas computadoras a base de bulbos que ocupaban enormes habitaciones, como la ENIAC, hasta los microprocesadores que sirvieron para realizar esta tesis. La maravillosa evolución de las computadoras, desde principios del siglo XX hasta ahora han dado como resultado mejoras gigantescas en cuanto a poder de cómputo, almacenamiento de información y rapidez (incluso podríamos opinar que las computadoras actuales son más "bonitas"), pero la idea básica de lo que son las computadoras más recientes es la misma que las primeras y ejecutan las mismas operaciones de la misma manera que lo que

lo hacían sus antecesoras, sólo que muchísimo más rápido. Ahora la Ciencia se encuentra ante un posible nuevo umbral al incorporar las ideas y fenómenos de la Mecánica Cuántica a la Informática; nos asomamos a la posible existencia de una máquina que opera de manera fundamentalmente diferente: *La Computadora Cuántica*.

La Mecánica Cuántica es la estructura matemática que involucra, en principio, a toda la Física; en todas las ramas de la Física existen problemas en los que se deben considerar los efectos cuánticos para poder resolverlos. Por ello, la Mecánica Cuántica es la descripción física más cercana a la realidad con que cuenta la humanidad. Pero en este trabajo sólo usaremos una versión simplificada: la Mecánica Cuántica no relativista. De hecho, la característica más significativa de la Mecánica Cuántica para la Computación Cuántica es el hecho de que trabaja con amplitudes cuánticas, o vectores de estado en un espacio de Hilbert, en lugar de variables físicas (para un tratamiento de estados cuánticos como vectores en un espacio de Hilbert ver, por ejemplo, De la Peña 1991). Esto es lo que permite nuevos tipos de información y nuevos algoritmos de cómputo.

El primer trabajo sobre Computación Cuántica fue realizado por Bell en 1964; en él hacía un análisis detallado de un famoso experimento mental propuesto por Einstein, Podolsky y Rosen (EPR 1935) en 1935, con el que argumentaban que la Mecánica Cuántica era —en el mejor de los casos— incompleta como descripción del mundo físico. La conclusión más importante del trabajo de Bell fue el planteamiento de una serie de relaciones que debían cumplirse entre magnitudes involucradas en dicho experimento, las famosas *desigualdades de Bell*, que subrayan la importancia de las correlaciones entre sistemas cuánticos separados que interactuaron (directa o indirectamente) en el pasado pero que aparentemente ya no interactúan entre sí de forma alguna. Fundamentalmente, su argumento muestra que el grado de correlación que puede estar presente en tales sistemas rebasa las predicciones que se pueden hacer sobre la base de cualquier ley física que describa partículas en términos de variables clásicas en vez de estados cuánticos. Los experimentos que se diseñaron a partir de estas ideas entrañaron una dramática lucha, una lucha decisiva que ponía en tela de juicio a la Mecánica Cuántica en su conjunto: si se cumplían las desigualdades de Bell entonces la Mecánica Cuántica resultaba inconsistente con la realidad, o al menos in-

completa. Durante la década de los 70 se llevaron a cabo varios experimentos así como también en los 80 para demostrar o refutar las desigualdades de Bell; la mayoría de ellos mostraron que las desigualdades de Bell se violaban, y por tanto la Mecánica Cuántica resultó —una vez más— consistente con la realidad, y aparentemente completa, por lo menos en el sentido abordado por EPR.

La siguiente aproximación entre la Mecánica Cuántica y la Informática sucedió cuando se encontró que algunas propiedades simples de los sistemas cuánticos, tales como la perturbación inherente a la realización de mediciones, podría tener aplicaciones prácticas en criptografía. Hoy día, los sistemas criptográficos se basan en varias herramientas matemáticas, especialmente la factorización de números enteros muy grandes. La idea fundamental de la criptografía cuántica es la distribución cuántica de información, que consiste en establecer en dos localidades separadas un par de secuencias aleatorias idénticas de dígitos binarios, sin permitir alguna tercera réplica que permitiera conocer la secuencia. Esto resulta muy útil ya que tal secuencia aleatoria podría ser usada como una llave criptográfica que permita la comunicación segura. Los principios de la Mecánica Cuántica garantizarían la seguridad de los datos cuánticos dejando sin trabajo hasta los mejores espías de la transmisión de mensajes. Esta posibilidad podría ser bastante rentable para los grandes capitalistas monopolistas de la industria del software, así como para los gobiernos del mundo, así que el potencial del cifrado cuántico parece ser vasto.

Pero esto todavía está relativamente lejos de la computadora cuántica. Para pensar en una computadora cuántica hay que utilizar la Mecánica Cuántica para visualizar la realidad, ya que esta brinda una explicación fundamental del comportamiento de todos los sistemas físicos (es decir, es la explicación del universo más completa con la que se cuenta, pero no por ello es completa y no por ello es más fácil dar una representación de un sistema en particular); por ello no se puede reproducir simplemente la acción de una máquina de Turing clásica en forma cuántica. Esto representó una gran dificultad para concebir una computadora cuántica. No basta simplemente con identificar un sistema cuántico cuya evolución pueda ser interpretada como un algoritmo de computadora; se debe probar algo mucho más fuerte que esto. A la inversa, sabemos que las computadoras clásicas (las de la vida diaria)

pueden simular con los algoritmos adecuados, la evolución de cualquier sistema cuántico, con la restricción de que ningún proceso clásico permite preparar sistemas separados cuyas correlaciones violen las desigualdades de Bell. Las correlaciones EPR-Bell resultan *absolutamente* cuánticas.

Las primeras ideas que implicaban la conversión de la acción de una máquina de Turing a un proceso reversible equivalente y que incluía un Hamiltoniano de un sistema que evolucionara de tal forma que imitara una máquina de Turing reversible, fueron explicadas en el trabajo de Bennett (Bennett 1973, Lecerf 1963), en el que mostraba también que una máquina universal de Turing clásica se podía hacer reversible sin hacerse demasiado compleja. Otro importante trabajo al respecto fue el de Benioff (1980, 1982) en el que mostró que la evolución cuántica unitaria tiene al menos tanto poder de cómputo como una computadora clásica.

Por su lado, Richard P. Feynman no consideró la posibilidad de computación universal, sino de *simulación universal*, es decir, un sistema cuántico construido específicamente para este propósito, que pudiera simular el comportamiento físico de cualquier otro (Feynman 1982, 1986). Este "sistema simulador" podría ser una computadora universal, ya que cualquier computadora es un sistema físico. Feynman dio argumentos que sugerían que la evolución cuántica de tal sistema podría ser utilizada para procesar ciertos problemas más eficientemente que cualquier computadora clásica. Pero Feynman no especificó suficientemente su dispositivo como para llamarlo una computadora cuántica, especialmente porque él supuso que cualquier interacción entre sistemas de dos estados adyacentes podrían ordenarse, el problema es que no dijo cómo.

En 1985 se dio un importante avance con el trabajo de David Deutsch (1985), que fue considerado por muchos como el primer esbozo serio de una computadora cuántica. Su trabajo es suficientemente específico y simple como para contemplar la posibilidad real de construir tal máquina, que además tuviera la capacidad de ser un simulador universal cuántico. El sistema de Deutsch esencialmente es una línea de sistemas de dos estados. Él probó que si los sistemas de dos estados podían hacerse evolucionar por medio de un pequeño conjunto específico de operaciones simples, entonces cualquier evolución unitaria

podría producirse, y por lo tanto podría hacerse que la evolución general del sistema simulara la evolución de cualquier sistema físico. Con estas ideas se puede hacer que el sistema cuántico se comporte como una máquina de Turing. Las operaciones básicas que propuso Deutsch posteriormente se les llamó "compuertas cuánticas", ya que juegan un papel análogo al de las compuertas lógicas binarias de las computadoras clásicas.

Sin embargo la propuesta de Deutsch no era perfecta. Dos de sus aspectos fundamentales eran cuestionables: eficiencia y viabilidad. La eficiencia es absolutamente fundamental en la Informática y está muy ligada con el concepto de "universalidad"; una computadora universal es aquella que no solamente puede simular la acción de cualquier otra, sino que además puede hacerlo sin ser demasiado lenta. La rapidez de una computadora depende de los pasos requeridos para hacer determinada operación; dicho número no debe crecer exponencialmente con el tamaño de los datos de entrada (en el siguiente capítulo hablaré más de esto).

A principios de los 90, varios científicos buscaron problemas informáticos que podrían ser resueltos por la computadora cuántica mejor que con cualquier computadora clásica y desarrollaron algoritmos cuánticos para resolverlos (ver Deutsch y Jozza 1992, Bernstein y Vazirani 1993). Tales algoritmos cuánticos podrían jugar un papel conceptual similar a la desigualdad de Bell, al definir algo de la naturaleza esencial de la Mecánica Cuántica. Al principio sólo se encontraron algunas diferencias pequeñas en cuanto a desempeño teórico de la computadora cuántica en relación a sus contrapartes clásicos, siempre y cuando el sistema cuántico se encontrara libre de "ruido". Por estas fechas también apareció el trabajo de David Simon (1994) en el que describía un algoritmo cuántico más eficiente para un problema tan abstracto que no podia ser resuelto eficientemente con máquinas clásicas, incluso con métodos probabilísticos. Este trabajo sirvió de inspiración a Peter W. Shor, quien asombró a la comunidad científica inventando un algoritmo que no sólo era eficiente para una computadora cuántica, sino que también resolvía un problema central de la Informática: *la factorización de números enteros grandes* (Shor 1995).

Este problema resulta interesante y de fácil aplicación, debido a que actualmente, los mejores programas clásicos cifran mensajes, generan llaves y códigos secretos en base a la

factorización en números primos de grandes números enteros (más de 256 dígitos). Shor discutió tanto la factorización de dichos números, como los logaritmos discretos (ver Shor 1995), haciendo uso del método de la Transformada de Fourier Cuántica descubierta por Coppersmith y Deutsch.

De la misma forma que en el caso de la Computación Clásica y la Informática, una vez que la Teoría Computacional comenzó a desarrollarse, también se emprendieron esfuerzos para establecer la naturaleza esencial de la información cuántica. Tampoco resultó trivial. La principal dificultad se puede visualizar de la siguiente forma: considérese el sistema cuántico más simple, un sistema con sólo dos estados posibles —un sistema binario—, digamos una partícula con espín un medio en un campo magnético. El estado cuántico de un espín es una cantidad *continua* definida por dos números reales, por lo que en principio podemos almacenar una cantidad infinita de información clásica. Sin embargo, una medición del espín sólo dará como resultado una respuesta con dos posibles opciones (espín arriba o espín abajo); no hay manera de acceder al infinito de información que parece estar ahí, por lo tanto es incorrecto considerar el contenido de información en esos términos. Naturalmente surge la pregunta ¿cuánta información se puede almacenar en un sistema cuántico binario? Este problema fue abordado por Jozza y Schumacher (1994, Schumacher 1995); en sus trabajos encontraron que la respuesta a esta pregunta es que dicha información es la equivalente a la que se puede almacenar en un sistema binario clásico. Parece trivial, pero no lo es. Además demostraron que este sistema binario juega un papel en la Informática Cuántica análogo al que juega un bit en la Informática Clásica. En el caso de la Informática Cuántica, la información contenida en cualquier sistema cuántico puede ser medida significativamente como el número mínimo de sistemas binarios, ahora llamados bits cuánticos o qubits, que serán necesarios para almacenar o transmitir el estado del sistema con gran precisión.

Junto a estas ideas subyace la cuestión de si realmente es posible la Computación Cuántica. La observación elemental, pero fundamentalmente importante, de que los efectos de la interferencia cuántica que provoca que algoritmos como el de Shor sean extremadamente frágiles, subraya el hecho de que la computadora cuántica es megasensible al ruido

experimental y a las imprecisiones. Los primeros científicos que trabajaron en Informática cuántica sabían de esta dificultad, pero su intención sobre todo era establecer si la idea de una computadora cuántica tenía sentido en absoluto. Con el algoritmo de Shor parece que realmente sí tiene sentido hablar de una computadora cuántica; ahora el problema reside en saber si la naturaleza permite la existencia de un dispositivo que trabaje con suficiente precisión como para ejecutar dicho algoritmo para enteros grandes (como del tamaño de un gogol, 10^{100}), o existen límites naturales fundamentales en la precisión de los sistemas reales. Ambas opciones representan percepciones fundamentales de la naturaleza interior de las leyes físicas universales.

Para tratar de resolver esta cuestión se han conjuntado las ideas de la Computación Cuántica y de la Informática Cuántica. Para lograr que una computadora cuántica sea menos sensible al "ruido" se ha desarrollado la llamada corrección de errores cuántica o Teoría de la Información Cuántica de Shanon. En 1996 aparecieron dos importantes artículos, uno de Calderbank y Shor (1996) y otro de Steane (1997), que establecieron un marco general en el que el procesamiento de información cuántica puede ser usado para combatir un amplio intervalo de ruidos en los procesos de cómputo de un sistema cuántico correctamente diseñado. A partir de entonces se han hecho bastantes progresos hacia la generalización de dichas ideas (Knill y Laflamme 1996, Ekert y Macchiavello 1996, Bennett et al 1996b, Gottesman 1998, Calderbank et al 1997). Uno de esos importantes progresos aportado por Shor (1996) y Kitaev (1997), fue la demostración de que la corrección se puede lograr incluso si las operaciones correctivas mismas son imperfectas. Dichos métodos llevan al concepto general de "cómputo tolerante a errores" (Preskill 1997).

En vista de esto último, parece claro que la relación entre la Informática cuántica y las computadoras cuánticas es mucho más estrecha que la relación entre máquinas clásicas y la teoría Informática clásica. La corrección de errores no garantiza por sí misma que las computadoras cuánticas trabajarán con toda precisión, ya que no puede suprimir todos los tipos de errores. La importancia de la corrección de errores estriba en que muestra que es posible que una computadora cuántica trabaje con precisión.

Hasta aquí, no he salido del reino de las ideas. Todo lo que se ha mencionado sobre la computadora cuántica son brillantes ideas. La única manera de realmente resolver la cuestión de la *viabilidad* de la computadora cuántica es construyendo una. Y también en este sentido se ha estado trabajando. Varios autores han propuesto diseños de computadoras cuánticas basadas en las ideas de Deutsch, y sus aportes han consistido en especificar más claramente sus requerimientos físicos y tecnológicos (Teich et al 1988, Lloyd 1993, Berman et al 1994, DiVincenzo 1995).

Hoy en día, el gran reto es construir un sistema lo suficientemente complejo para ser útil, pero cuya evolución sea tanto unitaria como controlable. Cirac y Zoler (1995) propusieron el uso de una trampa lineal de iones, lo que constituyó un avance significativo en cuanto a viabilidad, ya que hoy en día el confinamiento de iones ha alcanzado la precisión y bajas temperaturas necesarias como para obtener sistemas relativamente complejos y estables (Diedrich et. al. 1989). Otra posibilidad se encuentra en las técnicas de la resonancia nuclear magnética, que podrían adaptarse para los fines de la Computación Cuántica (Gershenfeld y Chuang 1997). Hasta la fecha no ha sido construida ninguna computadora cuántica, y parece todavía una remota posibilidad. Sin embargo resultan prometedores los intentos realizados por los equipos de Brune (1994), Monroe (1995), Turchette (1995) y Mattle (1996).

Paralelo al desarrollo de la Computación Cuántica (y en estrecha relación con esta), se desarrolló la *Teletransportación Cuántica* (*Quantum Teleportation*), que es el tema principal de este trabajo. La teletransportación cuántica podría describirse en un solo capítulo, sin embargo, para comprender la relevancia del fenómeno (así como entenderlo cabalmente), me pareció relevante exponer y explicar las bases de la Computación Cuántica, por ello dedico el capítulo tres a dicho tema. La Computación Cuántica a su vez parte de lo aprendido y desarrollado con la Computación Clásica, así que el primer capítulo lo dedico a una somera introducción a la Computación Clásica. El capítulo dos es una especie de paréntesis sobre el entrelazamiento cuántico (*quantum entanglement*) y las desigualdades de Bell, que resultan un tema imprescindible para explicar porqué se necesita un par de partículas con entrelazamiento cuántico (se les llama coloquialmente "un par EPR") para

realizar la teletransportación, y además cómo estas ideas dieron pauta al desarrollo de la Computación Cuántica.

CAPITULO 1
Nuestras computadoras y las máquinas de Turing

Tengo varios amigos matemáticos con los que a veces visito bares y restaurantes, y a la hora de pagar la cuenta y dividirla entre los comensales a menudo les juego una conocida broma: "calcúlalo tú que eres matemático(a)"; invariablemente me contestan con una cariñosa mentada. La realidad es que la mayoría de los matemáticos son bastante ineptos para hacer cuentas, contra lo que podría pensar la gente. No lo hacen a propósito, no fingen ser ineptos para los cálculos aritméticos (en verdad lo son), el problema es que la gente piensa que las matemáticas sólo estudian los números y su utilidad a la hora de pagar cuentas.

Otra creencia popular bastante extendida, y por demás equivocada, es la de que "el objeto de estudio de la Ciencia de la computación son las computadoras". Los computólogos, defendiendo su materia de estudio (y su misma razón de ser) afirman que esto equivale a decir que "el objeto de estudio de la astronomía son los telescopios". Es decir que las computadoras son las máquinas que sirven para computar (¡aunque usted no lo crea!), sólo son las herramientas de los computólogos. El asunto está en la definición de la palabra "computar". Computar es, en un sentido numérico, calcular, hacer cuentas, operaciones con números. En el sentido un poco más general es pasar una colección de datos a través de un proceso que finalmente nos proporciona la solución de un problema. Por ejemplo, ordenar alfabéticamente una lista de personas es un cierto tipo de cómputo.

Si hay que hacer un trabajo tedioso, repetitivo y con tendencia a dejar frustrado a quien lo realiza, toda persona con un poco de sentido común tratará de evitarlo. Este es y siempre ha sido el caso de los cálculos matemáticos. Probablemente por ello las matemáticas son una de las asignaturas más odiadas y temidas entre los estudiantes de todos los niveles (quizá sólo superadas por la Física). Seguro que usted recuerda con algo de tedio el injusto asesinato de sus mañanas o sus tardes infantiles por tener que calcular interminables sumas, restas, multiplicaciones y divisiones; muy probablemente usted también

fue víctima de esos maquiavélicos torturadores de la primaria que osaban llamarse "maestros". No se avergüence, hasta uno de los padres del cálculo diferencial integral, Gottfried Wilhelm Leibniz escribió: "No es admisible que los estudiosos y científicos, en lugar de elaborar y confrontar nuevas técnicas, pierdan su tiempo como esclavos de las fatigas del cálculo, cuando esto podría ser delegado confiablemente a cualquier otro"(Galviz 2004).

Probablemente que Leibniz, lejos de lo que pudiera sospecharse, y pese a que vivió durante el siglo XVII, no estaba pensando en un esclavo humano al que pudiera acomodarle unos latigazos cada que se equivocara en una cuenta; él pensaba en máquinas. Nada menos que en 1671 él hizo una máquina calculadora más poderosa que la que hizo unos años atrás Pascal. Muchos otros grandes científicos han coincidido con Leibniz acerca de calcular, pero definitivamente todos también han coincidido en algo: no se puede dejar de calcular. Calcular es la base de la civilización. Y es que la humanidad debe su capacidad para controlar un buen número de procesos naturales (e inventar muchos otros artificiales) gracias, en buena parte, a su poder de cálculo. Sobre ello se basa nuestra civilización. Esa ha sido el motivo principal para desarrollar las máquinas de computar, las famosas computadoras, y lo es también de la creación y del desarrollo de la computadora cuántica, hoy en día, pero más fundamentalmente es el motor que impulsa a la *Teoría de la Información.* Anteriormente, dicha teoría se consideraba una teoría matemática abstracta de la representación de símbolos provenientes de alguna fuente en términos de un alfabeto fijo (nuestras máquinas modernas utilizan el código binario) cuya representación cumple con varias propiedades. Richard Hamming decía de la teoría de la información: "Claramente, esta es una teoría fundamental para la mayor parte de la manipulación humana de símbolos." (Hamming 1986). Los recientes desarrollos que estudiaré en este trabajo indican que se trata de una teoría física.

El desarrollo de la teoría de la información fue paralelo a la *Teoría de la Codificación*; dicho desarrollo incluyó la aplicación de herramientas matemáticas complejas como la teoría de grupos, teoría de campos finitos (teoría de Galois), geometría proyectiva y programación lineal. A la teoría de la información que se desarrolló sin incorporar las ideas de la Mecánica Cuántica los autores en general coinciden en llamarle *Teoría Clásica de la*

Información. Hay que hacer notar que dicha teoría no se ocupa del *significado* de la información, sólo de la *cantidad* de información proveniente de las fuentes. Como fácilmente podría suponerse, existen una infinidad de fuentes de información (cualquier cosa puede ser una fuente de información); la mayoría de ellas proporcionan la información en forma continua, pero normalmente se hacen "mediciones", "muestreos" o "tomas" en intervalos de tiempo regulares y entonces es posible digitalizar la señal observada; una razón poderosa para hacer esto es que las señales digitales pueden almacenarse, manipularse y transmitirse más confiablemente que las señales análogas. Otra razón para digitalizar las señales es la cultura del silicio: nada conocido y desarrollado hasta hoy procesa información tan rápido y eficazmente como los circuitos digitales integrados (y a un costo tan bajo). Y como todas las máquinas que a lo largo de la historia han manipulado información, las computadoras modernas no "entienden" ni un ápice de los datos que reciben; es decir que *no son inteligentes*, es por ello que la teoría de la información no puede ocuparse del *significado* de la información, sólo de su *procesamiento.*

Cualquier sistema de procesamiento de datos debería reaccionar fielmente a cada señal distinta de la fuente, de la cuál, en general no se puede prever nada, por ello generalmente se considera a cada fuente de información como aleatoria. La fuente puede generar mensajes específicos de un acervo de mensajes (que en general puede ser infinito) y el sistema de transmisión debe estar listo para manipular cualquiera de los mensajes posibles. Por ello la teoría es esencialmente *estadística.*

En este trabajo no abordaré realmente la Teoría Clásica de la Información, por considerar que no es indispensable para comprender las ideas que conducen a la computadora cuántica, además que es un tema basto, que me llevaría aun más tiempo y espacio. Sin embargo sí abordaré la Teoría de la Computación Clásica, que ciertamente tiene mucha relación con la de la Información, pero son cosas diferentes. Para comprender las diferencias fundamentales entre las computadoras clásicas y la proyectada computadora cuántica, conviene saber cuál es la teoría fundamental detrás de las primeras, y contrastarla después con la teoría fundamental detrás de la segunda.

1.1 Teoría de la Computación Clásica

Las cuestiones fundamentales a las que se dirige la teoría de la computación clásica son *saber qué es computable* y *qué se necesita para computarlo.* Lo más básico que se necesita para realizar cómputos son los dispositivos para almacenar y manipular símbolos. En general se considera que un cómputo es ineficiente si la cantidad de recursos requeridos para llevarlo a cabo crecen exponencialmente con el tamaño del problema a resolver. El tamaño del problema está dado por la cantidad de información requerida para especificarlo. Una computadora tiene que ser capaz de poder manipular al menos símbolos binarios, los símbolos unitarios (la notación unitaria usa sólo un símbolo, por ejemplo los números naturales en esta notación usando como símbolo "♣" son: ♣, ♣♣, ♣♣♣,...), no sirven para computar ya que el número de espacios de memoria podría crecer exponencialmente con la cantidad de información a ser manipulada. El desarrollo de las computadoras electrónicas ha demostrado que basta con trabajar con dos símbolos (notación binaria, que normalmente usa como símbolos 0 y 1).

Una puerta lógica binaria es elemento mínimo de procesamiento de cualquier computadora. La puerta lógica más elemental es la que tiene un bit de entrada y un bit de salida; en este caso sólo hay dos posibilidades para la entrada (0 y 1) y dos para la salida (las mismas). Sólo hay dos compuertas lógicas binarias con estas características: la identidad y la negación; usualmente se les denota como : I y NOT. Así

$$\begin{aligned} \mathrm{I}(0) &= 0, \qquad \mathrm{I}(1) = 1 \\ \mathrm{NOT}(0) &= 1, \qquad \mathrm{NOT}(1) = 0 \end{aligned} \tag{1.1}$$

Consideremos ahora una puerta lógica binaria que tome dos bits x, y como entradas y aplica una función $f(x, y)$, que sólo puede dar por resultado los valores 0 ó 1; como hay cuatro posibilidades diferentes para las entradas (00, 01,10 y 11) entonces tenemos 16 posibles funciones f diferentes; a este conjunto de funciones se le llama *conjunto universal*, ya que combinando en series tales compuertas se puede llevar a cabo cualquier transformación

de n bits. Algunas de ellas son:

Función AND =

x	y	$f(x,y)$
1	1	1
1	0	0
0	1	0
0	0	0

(1.2)

Función NAND =

x	y	$f(x,y)$
1	1	0
1	0	1
0	1	1
0	0	1

Función OR =

x	y	$f(x,y)$
1	1	1
1	0	1
0	1	1
0	0	0

Función NOR =

x	y	$f(x,y)$
1	1	0
1	0	0
0	1	0
0	0	1

Además hay compuertas que pueden sustituirse combinando otras, de hecho sólo necesitamos una puerta para representar a todas las demás: la puerta NAND.

Las cadenas o concatenaciones de compuertas lógicas son procedimientos o *algoritmos* que sigue la computadora (cualquiera que ésta sea) para obtener la respuesta f. Roger Penrose habla un poco sobre algoritmos en su fantástico libro *La mente nueva del emperador*: "La palabra 'algoritmo' procede del nombre del matemático persa del siglo IX Abu Ja'far Mohammed ibn Mûsâ *al-Khowârizm*, autor de un interesante texto matemático, escrito alrededor del año 825 d.C., titulado 'Kitab al jabr wa'l-muqabala'" (Penrose 1996). Pero mucho antes de la aparición de este libro ya se conocían varios algoritmos. Uno de los más famosos data de por ahí del año 300 a.C., es el algoritmo de Euclides para encontrar el máximo común divisor de dos números. Sin embargo la formulación precisa del concepto general de algoritmo data del siglo XX; de hecho se han dado varias descripciones alternativas de este concepto, todas datan de los años treinta del siglo pasado.

La más directa y convincente es la llamada *Máquina de Turing,* que ante todo, es un elemento de "matemática abstracta" y no un objeto físico. El concepto fue introducido por el matemático inglés Alan Turing en 1936 (Turing 1937) para tratar un problema muy general conocido como el *Entscheidungsproblem* (El Décimo Problema también conocido como el Problema de Decisión) planteado por el matemático alemán David Hilbert (el de los famosos espacios). La pregunta era: ¿existe algún procedimiento mecánico general que pueda, *en principio,* resolver todos los problemas de las matemáticas, que pertenezcan a alguna clase bien definida? Parte de la dificultad para resolver esta cuestión consistía en decidir lo que se debe entender por "procedimiento mecánico". El concepto iba más allá de las ideas matemáticas comunes de la época. Para poder manejarlo, Turing trató de imaginar cómo podría formalizarse el concepto de "máquina", descomponiendo su modo de operar en términos elementales. Penrose (1996) afirma que Turing también consideraba el cerebro humano como una "máquina" en ese sentido, de tal forma que cualquiera que fuera la actividad que pudiera llevar a cabo un matemático cuando aborda sus problemas, ésta también tendría que entrar en la etiqueta de "procedimientos mecánicos".

Para explicar la máquina de Turing imaginemos una máquina ideal (no tiene problemas de suministro de energía, ni de desgaste, ni necesita condiciones climáticas adecuadas para funcionar, etc.) que tenga un conjunto *discreto* de posibles estados diferentes; dicho conjunto se llamará *estados internos.* Todo lo que nuestra máquina reciba del exterior, los datos, la información que manipulará será la *entrada,* y todo lo que se obtenga de la máquina como resultado de su acción será la *salida.* Aunque nuestra máquina tiene un número finito de estados internos, puede manejar una entrada de cualquier tamaño, en general, ilimitada; además también cuenta con una capacidad de almacenamiento externo ilimitada. Así que no podremos "cargar" todos los datos externos ni todos los resultados de sus propios cálculos; sólo puede examinar las partes de los datos o cálculos previos que está procesando en ese momento, y realizar con ellas todas las operaciones que sea necesario. Turing representaba los datos externos y el espacio de almacenamiento como una cinta sobre la que se hacen marcas, una secuencia lineal de cuadros que se considera infinita en ambas direcciones. Esta cinta sería utilizada por el dispositivo y leída cuando

fuera necesario; el dispositivo podría, como parte de la operación, mover la cinta hacia adelante o hacia atrás. También podría hacer nuevas marcas en los lugares de la cinta donde fuera necesario y podría borrar las viejas, permitiendo actuar a la misma cinta como almacenamiento externo y como entrada. La cinta seguirá pasando por el dispositivo hacia adelante y hacia atrás mientras sea necesario hacer nuevos cálculos. Cuando el cálculo haya terminado, el dispositivo se detendrá y la respuesta aparecerá en la parte de la cinta que queda a un lado del dispositivo. El hecho de que la cinta esté dividida en cuadros implica que puede ser descompuesta y descrita en términos de elementos *discretos* (en vez de continuos); esto implica que en cualquier caso particular la entrada, el cálculo y la salida deben ser siempre *finitos*. Así, aunque la cinta es infinitamente larga, en ella debe haber sólo un número finito de marcas; más allá de cierto punto en cada dirección la cinta debe estar completamente en blanco. Nuestro dispositivo "leerá" la cinta cuadro por cuadro, y después de cada operación se mueve sólo un cuadro a la derecha o a la izquierda. Los espacios en blanco se pueden representar con un 0.

Dada la entrada y su estado inicial nuestro dispositivo actuará en forma completamente determinista: cambia de un estado interno a otro (tal vez el mismo), reemplaza el 0 o el 1 que acaba de leer por el mismo o por un distinto símbolo 0 o 1, se mueve un cuadro a la derecha o a la izquierda, finalmente, decide si continuar el cálculo o si terminarlo y detenerse. Para definir las operaciones de nuestro dispositivo de modo explícito, podemos numerar los diferentes estados internos; así, la operación de nuestro dispositivo —que ahora sí podemos llamar Máquina de Turing— estará totalmente especificada por una lista de sustituciones que especificarán paso a paso qué hará. Si usamos el sistema binario para numerar las instrucciones tendremos un código como el siguiente:

$$\begin{aligned} 00 &\rightarrow 00d \\ 01 &\rightarrow 11d \\ 10 &\rightarrow 01alto \\ 11 &\rightarrow 11d \end{aligned} \tag{1.3}$$

Los caracteres tipo `máquina de escribir` que se encuentran a la izquierda de la flecha representan la entrada de nuestra máquina, y los que están a la derecha de la flecha son la salida que escribirá en la cinta; las letras a la derecha de la flecha indican hacia donde arrastra la cinta nuestra máquina (i=izquierda, d=derecha, sólo se mueve un espacio) y con la instrucción "alto" se detiene. Los dos primeros renglones de la expresión 1.3 significan que si la máquina está en estado interno 0 y la entrada es 0, la maquina se pondrá en estado 0, escribirá un 0 y se desplazará la cinta a la derecha; si la entrada es 1, la maquina se pondrá en estado 1, escribirá un 1 y desplazará la cinta un lugar a la derecha. Los otros dos renglones significan: si el estado interno es 1 y la entrada es 0, poner la máquina en estado 0 escribir un 1 y detenerse; si el estado interno es 1 y la entrada es 1, poner la máquina en estado interno 1, escribir un 1 y desplazarse a la derecha. Este listado de instrucciones describe a una máquina de Turing que simplemente añade un 1 a una cadena de 1s. De manera análoga podemos especificar cualquier máquina de Turing, por ejemplo la que realiza el algoritmo de Euclides para obtener el máximo común divisor de dos números que se menciona en la página 17 (Penrose 1996):

```
00→00d,    01→11i,    10→101d,    11→11i,    100→1010Cd,
                                  101→110d,
110→1000d   111→111d   1000→1000d   1001→1010d   1010→1110i
   1011→1101i   1100→1100i   1101→11i   1110→1110i
1111→10001i   10000→10010i   10001→10001i   10010→100d
      10011→11i   10100→00alto   10101→10101d
```

Pueden especificarse máquinas de Turing para realizar cualquier operación "mecánica". Los matemáticos usan el sustantivo "*algoritmo*" y los adjetivos "*computable*", "*recursivo*" y "*efectivo*" para denotar las operaciones mecánicas que pueden ser realizadas por máquinas teóricas como las de Turing, basta con que sean suficientemente claras y bien definidas. Desde este punto de vista, *los algoritmos son cómputos, procedimientos efectivos u operaciones recursivas que pueden descomponerse en operaciones mecánicas que alguna máquina de Turing puede ejecutar.* A esta afirmación se le conoce como la *Tesis de Church-Turing.* Alonzo Church era un lógico estadounidense que un poco antes que Turing, había desarrollado un esquema —el cálculo *lambda*— dirigido también a resolver el Décimo Problema de Hilbert.

En general, cuando se habla de máquinas de Turing, se habla de la *Máquina Universal* de Turing. Si se codifica la lista de instrucciones para una máquina de Turing arbitraria T en una cadena de ceros y unos que pueda ser representada en una cinta, y esta cinta se utiliza como la parte inicial de la entrada de alguna máquina de Turing particular U, esta máquina actuará sobre el resto de la entrada tal como lo hubiera hecho T; a U se le llama Máquina Universal de Turing, debido a que es un *imitador universal*, es decir, puede actuar exactamente como cualquier otra máquina. Las computadoras modernas de tipo general son —en su forma más esencial— máquinas universales de Turing.

Turing también ideó un método sistemático para numerar sus máquinas, que consiste simplemente en juntar todas las instrucciones que definen a cualquier máquina, con la codificación 0 para 0 ó 0, 10 para 1 ó 1, 110 para d, 1110 para i y 11110 para alto. Así queda un número binario que es el número de la máquina de Turing en cuestión. Por ejemplo, la máquina que simplemente añade un uno a una cadena de unos (expresión 1.3) prescindiendo de las flechas, de los dígitos que los preceden y de las comas tenemos la cadena

$$0000\text{d}0111\text{d}1001\text{alto}1111\text{d} \tag{1.4}$$

que le corresponde el número binario

$$00001100101010110100010111101010101010110 \tag{1.5}$$

que es el número decimal 27206546774, y el número decimal de la máquina que suma uno a un número natural es 451 813 704 461 563 958 982 113 775 643 437 908 (!)(Penrose 1996). Se denota la n-ésima máquina de Turing como T_n. Cabe señalar que no todos los números naturales —de hecho la gran mayoría— representan una máquina de Turing que trabaje en forma alguna. Así, el hecho de que cuando la n-ésima maquina actúa sobre m produce p, se expresa como $T_n(m) = p$. Esto también lo podemos visualizar como una operación particular aplicada al par de números n y m para obtener p. Esta operación particular es un proceso totalmente algorítmico, que por tanto puede ser llevado a cabo por una máquina de Turing U, la máquina universal que se denota como $U(n, m) = T_n(m)$ para cada (n, m) para los que T_n es una máquina de Turing correctamente especificada.

La máquina U, cuando se alimenta inicialmente con el número n, imita exactamente la n-ésima máquina de Turing.

Con todas sus ideas sobre sus máquinas, Turing pudo plantear el problema de Hilbert en términos de decidir si la n-ésima máquina de Turing se detendrá o no cuando actúe sobre el número m. Esto fue llamado el *problema de la detención*. Turing supuso que existía una máquina universal que podría decir si tal o cual máquina se detendrá, pero al encontrar contradicciones manifiestas, demostró que en realidad dicha máquina *no existe*. Al demostrar que no existe ningún algoritmo para decidir la cuestión de la detención de sus máquinas, Turing demostró que *no puede haber un algoritmo general para decidir cuestiones matemáticas*, concluyendo así que el Décimo Problema de Hilbert *no tiene solución*, no hay ningún algoritmo que funcione para *todas* las cuestiones matemáticas, ni para *todas* las máquinas de Turing con todos los números sobre los que podrían actuar. Otra forma de decir esto es que *algunas operaciones matemáticas bien definidas no son computables*.

Todo esto no se refiere a la insolubilidad de problemas particulares, sino a la *insolubilidad algorítmica de familias de problemas*. En cualquier caso particular, la respuesta es o "sí" o "no", de modo que ciertamente habrá un algoritmo para decidir este caso concreto: el algoritmo que simplemente dice "sí" cuando se le plantea el problema, o el que dice "no", según sea el caso. El problema es que no podemos saber cuál de los dos algoritmos usar. En el fondo este es el problema de decidir sobre la verdad matemática de un enunciado, y no el de la decisión sistemática para una familia de enunciados. Hay que notar que los algoritmos no deciden por sí solos sobre la verdad matemática. La validez de un algoritmo debe establecerse siempre por *medios externos*.

Los problemas computables no siempre suelen ser fáciles de resolver en la práctica. Un ejemplo importante es la factorización: dado un número compuesto x, hay que encontrar sus factores primos. Si x es par o múltiplo de un primo pequeño, no hay problema. La cuestión se pone fea cuando los factores primos son grandes. Existen métodos para atacar estos casos; hoy en día se pueden factorizar números de hasta 130 dígitos decimales, empleándose para ello 42 días realizando 10^{12} operaciones por segundo. Si x fuera un poco

mayor el problema se vuelve irresoluble para la tecnología actual: el tiempo de cómputo se incrementa hasta ¡un millón de años!

Sobre estos conceptos fundamentales, que se abordaron en este capítulo, se basa la Ciencia de la Computación. Sobre ellos se basa el funcionamiento de *todas* las máquinas que hoy en día realizan algún tipo de cálculo. Desde al punto de vista de este trabajo, las computadoras cuánticas parten de estos conceptos hacia una forma de operar fundamentalmente diferente, basada en la realidad física de los sistemas cuánticos. En el tercer capítulo hablaré de Computación Cuántica, pero antes era muy importante tener un punto de referencia en la Computación Clásica para poder entender los conceptos y diferencias entre ambas.

CAPITULO 2
Las ideas cuánticas

Desde el renacimiento,[1] con las revolucionarias ideas sobre todo de Newton, y los métodos de Galileo, la Física (de la mano de las Matemáticas) se volvió la Ciencia con más éxito. La capacidad no sólo de dar un modelo del universo coherente y verificable, sino que también de poder predecir, volvió a la Física la Ciencia paradigmática, el modelo a seguir. Su desarrollo, ligado al de la burguesía en ascenso, expresado en el progreso tecnológico, transformó la sociedad universal, aportando la base material sobre la cual se desarrollarían las demás ciencias y las artes. Pero, tanto la Teoría de la Relatividad como la Mecánica Cuántica, naciendo con el nuevo y convulso siglo XX mostraron que aún seguimos en la orilla del mar de misterios que el universo nos representa. Así, después de platicarle las ideas sobre la Computación Clásica, me gustaría platicarle sobre la nueva frontera: el desarrollo de una computación basada en las ideas cuánticas.

Urge revisar primero la vanguardia de la Física, la mejor aproximación que tenemos al mundo real que por su lado también ha servido para explicar satisfactoriamente muchos fenómenos y observaciones en la naturaleza que las teorías clásicas no pudieron: la *Mecánica Cuántica.*

No es mi intención dar una versión ni siquiera abreviada de la Mecánica Cuántica, sólo usaré algunos postulados que en general tomaré como válidos, tanto de representación como de interpretación física. Uno de los conceptos fundamentales de dicha teoría es el concepto de *estado*; dependiendo de la forma en que se aborde la teoría, el estado cuántico de un sistema aislado $\mathcal{Q}$ se representa con una función de onda $\psi(\mathbf{r}, t)$ o un vector $|\psi(\mathbf{r}, t)\rangle$ que pertenece a un espacio de Hilbert; ambas representan lo mismo. Esta última descripción, conocida como la notación de Dirac, es la más generalizada hoy en día, así que es la que usaré. En cualquier caso, la representación está en función de las variables elegi-

[1] Le ofrezco disculpas de antemano, mi querido lector, de usar el tan trillado recurso de remitirse a el nacimiento de la física newtoniana como introducción a un texto científico, pero es que no se me ocurrió nada más. En compensación lo he resumido tanto como pude. Espero que no me abandone solo por eso. Gracias.

das para describir el comportamiento del sistema. Dichas variables tales como la posición y el momento se acostumbran a llamar *observables* y se representan por operadores hermitianos. Por ejemplo los operadores de posición X y de momento P tienen los siguientes elementos de matriz en la eigenbase de X: $\langle x|X|x'\rangle = x\delta(x-x')$ y $\langle x|P|x'\rangle = -i\hbar\delta'(x-x')$. El vector de estado obedece la ecuación de Schrödinger

$$i\hbar\frac{d}{dt}|\psi(\mathbf{r},t)\rangle = \mathcal{H}|\psi(\mathbf{r},t)\rangle \tag{2.6}$$

donde $\mathcal{H}$ es el operador cuántico hamiltoniano. La cuestión de las *mediciones* cobra gran relevancia en la Mecánica Cuántica y provoca debates profundos, ya que en general los sistemas cuánticos son extremadamente sensibles a ellas: una medición perturba de manera fundamental al sistema; por ahora simplemente tomaré como postulado el que ciertas interacciones físicas se pueden distinguir como "mediciones" y su efecto sobre el vector de estado $|\psi\rangle$ es transformarlo en un eigenestado $|k\rangle$ de la variable que se mide, donde el valor k es escogido al azar con probabilidad $P \propto |\langle k|\psi\rangle|^2$ (suponiendo que $|\psi\rangle$ está normalizada). El cambio $|\psi\rangle \rightarrow |k\rangle$ puede ser expresado por el operador de proyección $(|k\rangle\langle k|)/\langle k|\psi\rangle$. Según esto, la evolución de un sistema cuántico aislado siempre es *unitaria*, o en términos vectoriales $|\psi(t)\rangle = U(t)|\psi(0)\rangle$ donde $U(t) = \exp\left[-(i/\hbar)\int \mathcal{H}dt\right]$ es un operador unitario, esto es, que cumple la condición $UU^\dagger = I$. Sin embargo queda el problema de que un sistema verdaderamente aislado es sólo una abstracción, excepto —quizá— para todo el universo. Lo que hay que notar de esto es que al usar la ecuación de Schrödinger para describir los sistemas reales siempre se trata de una *aproximación*, por muy buena que esta sea. -

2.1 La "paradoja" de Einstein, Podolsky y Rosen

Algunas de las ideas de Albert Einstein fueron fundamentales para el desarrollo de la teoría cuántica, sin embargo nunca pudo aceptar que dicha teoría pudiera llegar a ser algo más que una mera descripción provisional del mundo. Es bien conocida su aversión frente al aspecto probabilístico de la teoría resumida en una frase de una carta a Max Born en 1926: "Dios

no juega a los dados". Lejos de lo que se podría pensar, Einstein se situaba del lado de los materialistas; a él le molestaba, más que ese indeterminismo físico, la *falta de objetividad* en la manera empleada para describir la teoría cuántica. Muchos de los partidarios de la Mecánica Cuántica —encabezados por Niels Bohr— se manifestaron abiertamente como *idealistas* (en el sentido filosófico), pretendiendo que la realidad física es un producto de la *mente humana.* Parece que Bohr consideró el estado cuántico de un sistema (sujeto a mediciones) como *carente* de genuina realidad física, como un *"resumen"* de nuestro conocimiento acerca de dicho sistema (Bell 1990); ello implica directamente que la realidad es según la perciba el observador, lo que constituye la piedra de toque del idealismo (si no preguntémosle a Kant, o incluso a Hegel). Pero el mismo Bohr nunca llegó a desechar abiertamente la visión materialista de la realidad, que finalmente para su época llevaba al menos cuatro siglos de éxitos; por ello Bohr tenía que haber considerado que el mundo en el nivel clásico tenía una realidad objetiva, pero que no habría "realidad" en los estados cuánticos que parecen al margen de todo.

Esta imagen era precisamente lo que resultaba inadmisible para Einstein, quien estaba convencido de que también a nivel cuántico debe haber un mundo físico objetivo, independiente de cualquier observador. En muchas discusiones con Bohr intentó demostrar (aunque sin éxito) que había contradicciones inherentes a la imagen cuántica de la realidad, y que debe haber una estructura aún más profunda debajo de la teoría cuántica. En 1935 Albert Einstein, Boris Podolski y Nathan Rosen (EPR) publicaron un artículo cuyo título inquiría "¿Se puede considerar completa la descripción Mecánico Cuántica de la realidad física?". Este artículo ha resultado muy importante para el desarrollo de la Teoría de la Información Cuántica y por mucho tiempo constituyó un desafío importante a la Mecánica Cuántica.

A partir de la discusión iniciada por EPR, se llamó *realistas* a las teorías que apoyaban su punto de vista. El *Realismo* es un punto de vista filosófico según el cual se supone que la realidad externa existe y tiene propiedades definidas independientemente si alguien las observe o no. Muchos científicos durante el siglo XX han buscado que la Mecánica Cuántica sea consistente con dicha realidad. Uno de dichos intentos ha sido reinterpretar

la Mecánica Cuántica en términos de una descripción estadística de una teoría de *variables ocultas*. Los seguidores de Einstein, en particular David Bohm (1957) y De Broglie desarrollaron más este punto de vista según el cual los parámetros que precisa el sistema no nos son directamente accesibles, permanecen como "variables ocultas" y las probabilidades cuánticas surgen porque no se pueden conocer los valores de estos parámetros antes de la medición.

Dentro del marco realista, EPR presentaron un argumento clásico que descansa sobre tres premisas (EPR 1935):

1. Algunas de las predicciones de la Mecánica Cuántica referentes a observaciones sobre un cierto tipo de sistema, que consiste en dos partículas espacialmente separadas, son *correctas*.

2. Proponen un criterio de existencia de "un elemento de realidad física" bastante razonable: "Si podemos —sin que nada perturbe a un sistema en forma alguna— predecir con certeza (i.e. con probabilidad igual a la unidad) el valor de una cantidad física, entonces existe un elemento de realidad física que corresponde a esta cantidad física."

3. No existe la acción a distancia en la naturaleza; es decir, que no existe interacción alguna entre dos sistemas o entre dos partes de un mismo sistema, que sea instantánea. Lo más rápido en todos los marcos de referencia del universo es la velocidad de la luz.

El sistema que ellos consideraron en 1935 consiste de dos partículas preparadas en un estado tal que la suma de sus momentos en una dirección dada $(p_1 + p_2)$ y la diferencia de sus posiciones $(x_1 - x_2)$ están definidas a la vez, independientemente de toda medición. La función de onda $\varphi(x_1 - x_2 - a)$ describe al sistema, y, dado que $(x_1 - x_2) \in \mathbb{C}$ y φ está

normalizada a la unidad:

$$\begin{aligned} & \varphi(x_1 - x_2 - a)(x_1 - x_2)\varphi^*(x_1 - x_2 - a) \\ = \; & (x_1 - x_2)\varphi(x_1 - x_2 - a)\varphi^*(x_1 - x_2 - a) \\ = \; & (x_1 - x_2) = a, \end{aligned} \tag{2.7}$$

$\varphi(x_1 - x_2 - a)$ es una eigenfunción de $(x_1 - x_2)$ con eigenvalor a, que es una "longitud" característica del sistema. De manera análoga se puede mostrar que $\varphi(x_1 - x_2 - a)$ también es eigenfunción del operador $(p_1 + p_2)$ con eigenvalor 0. Midiendo la posición de la partícula 1 se puede predecir con certeza —de acuerdo con la Mecánica Cuántica— qué posición tendrá la partícula 2 si esta se mide inmediatamente. En vista de la premisa iii), dicha predicción se realiza sin perturbar en forma alguna la partícula 2, ya que las dos partículas están espacialmente separadas. Por lo tanto EPR infieren que la posición de la partícula 2 tiene un valor definido predeterminado, que no está incluido en la descripción dada por la función de onda $\varphi(x_1 - x_2 - a)$. Por un argumento análogo EPR también infieren que el momentum de la partícula 2 tiene un valor definido, lo que *contradice* el principio de incertidumbre. De aquí, EPR llegan a la conclusión de que al menos en esta situación particular *la descripción cuántica es incompleta.* John F. Clauser y Abner Shimony (1978) comentaban sobre el artículo de EPR:

> "En nuestra opinión el razonamiento de EPR es impecable, una vez que se remueve una ambigüedad en la frase 'puede predecir', que está en la segunda premisa. En un sentido estrecho, uno puede predecir el valor de una cantidad sólo *cuando un arreglo experimental se elige para determinar el valor de dicha cantidad.* En un sentido amplio, uno puede predecir el valor de una cantidad *si es posible elegir un arreglo experimental para determinarla.* Si el sentido estrecho es aceptado entonces el argumento de EPR claramente no funciona, debido a que los arreglos experimentales para medir la posición y el momentum de una partícula son incompatibles. Desde el punto de vista del realismo físico el sentido amplio de 'puede predecir' es el apropiado, mientras que desde ese punto de vista uno concibe un sistema físico que tenga un conjunto definido de propiedades independientemente de que se las observe, pero que por supuesto pueden ser exploradas a decisión del experimentador. En la situación considerada por EPR se puede predecir, en el sentido amplio, tanto x_2 como p_2.De aquí que si dicho sentido ambiguo de la frase es adoptado, su argumento queda

completo."

Además de desarrollar las teorías de variables ocultas, Bohm también formuló una versión de la "paradoja" EPR en términos de estados discretos. Consideró un par de partículas de espín $\frac{1}{2}$ producidas en un estado singulete. Se pueden medir independientemente varias componentes de espín de cada una de esas partículas al gusto del experimentador. La parte espinorial del vector de estado del sistema está dada por

$$\Psi = \frac{1}{\sqrt{2}}\left[u_{\hat{n}}^{+}(1) \otimes u_{\hat{n}}^{-}(2) - u_{\hat{n}}^{-}(1) \otimes u_{\hat{n}}^{+}(2)\right] \tag{2.8}$$

En esta expresión[2] $\sigma \cdot \hat{n} u_{\hat{n}}^{\pm}(1) = \pm u_{\hat{n}}^{\pm}(1)$, por lo que $u_{\hat{n}}^{\pm}(1)$ describe —en el sentido de la Mecánica Cuántica— un estado en el que la partícula 1 tiene espín arriba o abajo respectivamente a lo largo de la dirección $\hat{n}$; $u_{\hat{n}}^{\pm}(2)$ tiene un significado análogo con respecto a la partícula 2. Como el estado singulete Ψ tiene simetría esférica, $\hat{n}$ puede especificar cualquier dirección. Si por ejemplo se mide el espín de la partícula 1 a lo largo del eje $\hat{x}$, el resultado no está predeterminado por la descripción Ψ, pero de aquí se puede predecir si se encuentra que la partícula 1 tiene su espín paralelo al eje $\hat{x}$, entonces la partícula 2 tendrá su espín antiparalelo a dicho eje si se mide la componente $\hat{x}$ de su espín. Así, el experimentador puede arreglar su aparato de tal forma que pueda predecir el valor de la componente $\hat{x}$ del espín de la partícula 2 sin tener que interactuar con ella (si no existe la acción a distancia). De la misma forma se puede proceder para predecir cualquier componente de la partícula 2. Se puede concluir de este argumento que todas las componentes del espín de cada partícula estarían definidas, lo que por supuesto no es posible en la descripción cuántica, de ahí surge la necesidad de recurrir a los modelos de variables ocultas, de las que Bohm fue ardiente defensor.

El siguiente paso adelante en el entendimiento de los alcances e implicaciones tanto de la Mecánica Cuántica como de la "paradoja" EPR fue aportado por John S. Bell. Él estudió las teorías propuestas por De Broglie en 1928 y por Bohm en 1952; como Bohm, Bell notó que para reproducir las predicciones de la teoría cuántica para un sistema del tipo propuesto por EPR, debería postularse (como lo hicieron EPR) la existencia de *interacciones*

[2] Recuerde que las σ representan las matrices de Pauli, utilizadas para describir cuánticamente el espín de las partículas.

no locales entre partículas espacialmente separadas, entonces se preguntó si la no localidad o extensionalidad exhibida por estos modelos es una *característica genérica* de las teorías de variables ocultas que concuerdan con las predicciones estadísticas de la Mecánica Cuántica. Bell demostró (1965) que la respuesta es *sí*, para toda clase de teorías deterministas de variables ocultas, al menos en términos de aparatos y sistemas ideales; posteriormente Bell mismo y otros, extendieron su demostración a sistemas reales. Dichas versiones establecen básicamente que *todas las teorías realistas locales del fenómeno natural en cuestión, pueden compararse con la Mecánica Cuántica en un solo arreglo experimental, y que cada una de las perspectivas conduce a predicciones diferentes de resultados observables.* Es decir, que se pueden confrontar en un mismo experimento y ambas visiones tendrán predicciones diferentes.

En su artículo de 1965, Bell consideró el mismo experimento imaginario que Bohm describió, en el que el sistema consistía en dos partículas de espín $\frac{1}{2}$ preparadas en el estado singulete Ψ dado por la expresión (2.8). Seguiremos su esquema de razonamiento para explicar sus conclusiones (Bell 1965). Sea $A_{\hat{a}}$ el resultado de una medición del componente de espín de la partícula 1 del par a lo largo de la dirección $\hat{a}$, y sea $B_{\hat{b}}$ el de la partícula 2 a lo largo de la dirección $\hat{b}$. Si normalizamos haciendo $1 = \hbar/2$, tenemos que $A_{\hat{a}}, B_{\hat{b}} = \pm 1$. Note que el producto $A_{\hat{a}} \cdot B_{\hat{b}}$ es un solo observable del sistema de dos partículas (aunque se necesiten dos operaciones distintas para medirlo), y se le representa como un operador autoadjunto del espacio de Hilbert asociado al sistema. Se puede calcular el valor esperado de dicho observable:

$$[E\,(A_{\hat{a}} \cdot B_{\hat{b}})]_{\Psi} = \langle \Psi | \sigma_1 \cdot \hat{a}\sigma_2 \cdot \hat{b} | \Psi \rangle = -\hat{a} \cdot \hat{b}. \tag{2.9}$$

Cuando los analizadores con los que se realizan las mediciones A y B son paralelos tenemos:

$$[E\,(A_{\hat{a}} \cdot B_{\hat{a}})]_{\Psi} = -1 \tag{2.10}$$

para toda dirección $\hat{a}$. Entonces *se puede predecir con certeza* el resultado B, si se obtiene previamente el resultado A. He aquí el determinismo implícito contenido en este sistema idealizado. Como el estado cuántico Ψ no determina el resultado de una medición individual, este hecho —con el argumento de EPR— sugiere que existe una descripción más

completa del estado en el que este determinismo sea manifiesto. Este estado más "completo" se denota como λ, y puede tener muchas dimensiones, partes discretas o continuas, e interacciones diversas con cualquier aparato de medición, etc.

Sea Λ el espacio de los estados λ para un subconjunto de sistemas observados (que pueden ser partículas) comprendidos en un conjunto muy grande de dichos sistemas. No se hacen restricciones sobre qué tipo de espacio es Λ, ni de su dimensionalidad; lo único que se requiere es que exista un subconjunto boreliano de Λ, de tal forma que se puedan definir mediciones probabilísticas sobre él. La función de distribución de λ sobre el espacio Λ está normalizada:

$$\int_{\Lambda} |\lambda(x,t)|^2 \, dx = 1 \tag{2.11}$$

Entonces se puede definir una teoría determinista de variables ocultas como cualquier teoría física que postula la existencia de estados de un sistema para el que los observables de la Mecánica Cuántica siempre tienen valores definidos; en particular, en dicha teoría el observable $A_{\hat{a}} \cdot B_{\hat{b}}$ tiene un valor definido para el estado λ: $(A_{\hat{a}} \cdot B_{\hat{b}})(\lambda)$. Para este tipo de teorías Bell (1965) definió la localidad de la siguiente forma:

Una teoría determinista de variables ocultas es local si para cualquier par de direcciones $\hat{a}$ y $\hat{b}$, y para todo estado del sistema $\lambda_0 \in \Lambda$ tenemos que

$$(A_{\hat{a}} \cdot B_{\hat{b}})(\lambda) = A_{\hat{a}}(\lambda) \cdot B_{\hat{b}}(\lambda). \tag{2.12}$$

Lo que ésta ecuación expresa sencillamente es que, una vez determinado el estado λ, y después de que las partículas se han separado, las mediciones practicadas sobre la partícula 1sólo pueden depender de λ y $\hat{a}$ pero no de $\hat{b}$; algo análogo pasa con las mediciones sobre la partícula 2. Cualquier teoría física realista, determinista y que niega la acción a distancia es local en este sentido.

Se puede generalizar el concepto de localidad. En el argumento aquí presentado $\hat{a}$ y $\hat{b}$ representan las direcciones de orientación de los espines de las partículas, pero en general, a y b representan cualquier parámetro asociado al dispositivo experimental y se encuentran bajo control del experimentador. Considere un par de sistemas correlacionados que tienen un estado conjunto λ; se separan y siguen evolucionando en una forma inherente-

mente estocástica. Dados λ, a y b, se pueden definir probabilidades para cualquier medición en cualquier aparato; estas dos probabilidades pueden depender de cualquiera de los dos parámetros del dispositivo experimental, a o b respectivamente, y por supuesto de λ, pero son independientes una de otra. El resultado (o la probabilidad del resultado) de una medición practicada a una parte del sistema compuesto, es independiente de qué aspectos del otro componente elige medir el experimentador. Esto no significa que se excluye la posibilidad de saber algo del sistema 2 al examinar el sistema 1. El estado λ contiene información común a ambos sistemas, así que una medición en alguno presumiblemente revela algo de dicha información. La definición no impide que una medición en alguna de las componentes la perturbe localmente; lo que no permite es que el valor de una cantidad medida de un sistema no es causalmente afectado por lo que el experimentador elija medir en el otro sistema, ya que los dos sistemas están espacialmente separados cuando se realizan las mediciones.

Continuemos con el argumento de Bell. Para las teorías deterministas locales, el valor esperado de $A_{\hat{a}} \cdot B_{\hat{b}}$ está dado por

$$E\left(A_{\hat{a}} \cdot B_{\hat{b}}\right) = \int_{\Lambda} A_{\hat{a}}\left(\lambda\right) \cdot B_{\hat{b}}(\lambda)\left|\lambda(x,t)\right|^2 da. \tag{2.13}$$

Bell probó (1965) que si se satisfacen la condición de localidad (2.12) y la condición (2.10) en concordancia parcial con la Mecánica Cuántica, entonces los valores esperados para las mediciones satisfacen una simple desigualdad. La ecuación (2.10) se cumple si y sólo si

$$A_{\hat{a}}\left(\lambda\right) = -B_{\hat{a}}(\lambda). \tag{2.14}$$

para toda $\lambda \in \Lambda$; con ayuda de esta expresión podemos calcular una función que involucre tres posibles orientaciones distintas $\hat{a}$, $\hat{b}$ y $\hat{c}$, de tres diferentes analizadores con los cuales

se practican las mediciones $A_{\hat{a}}$, $A_{\hat{b}}$ y $A_{\hat{c}}$:

$$\begin{aligned} E(A_{\hat{a}} \cdot A_{\hat{b}}) - E(A_{\hat{a}} \cdot A_{\hat{c}}) &= -\int_{\Lambda} \left[A_{\hat{a}}(\lambda) A_{\hat{b}}(\lambda) - A_{\hat{a}}(\lambda) A_{\hat{c}}(\lambda)\right] |\lambda(x,t)|^2 \, dx \\ &= -\int_{\Lambda} A_{\hat{a}}(\lambda) \left[A_{\hat{b}}(\lambda) - A_{\hat{c}}(\lambda)\right] |\lambda(x,t)|^2 \, dx \qquad (2.15) \\ &= -\int_{\Lambda} \left[A_{\hat{a}}(\lambda) A_{\hat{b}}(\lambda)\right] \left[A_{\hat{b}}(\lambda) A_{\hat{b}}(\lambda) - \right. \\ \left. A_{\hat{b}}(\lambda) A_{\hat{c}}(\lambda)\right] |\lambda(x,t)|^2 \, dx &= -\int_{\Lambda} A_{\hat{a}}(\lambda) A_{\hat{b}}(\lambda) \left[1 - A_{\hat{b}}(\lambda) A_{\hat{c}}(\lambda)\right] |\lambda(x,t)|^2 \, dx \end{aligned}$$

Como $A_{\hat{n}} = \pm 1$ (condición de normalización), se obtiene

$$|E(A_{\hat{a}} \cdot A_{\hat{b}}) - E(A_{\hat{a}} \cdot A_{\hat{c}})| \leqslant \int_{\Lambda} \left[1 - A_{\hat{b}}(\lambda) A_{\hat{c}}(\lambda)\right] |\lambda(x,t)|^2 \, dx \qquad (2.16)$$

Usando las expresiones (2.13), (2.14) y (2.11) obtenemos

$$|E(A_{\hat{a}} \cdot A_{\hat{b}}) - E(A_{\hat{a}} \cdot A_{\hat{c}})| \leqslant 1 + E(A_{\hat{b}} \cdot A_{\hat{c}}). \qquad (2.17)$$

Esta desigualdad es una de las *desigualdades de Bell*; dichas desigualdades forman toda una familia. Se puede ver fácilmente la incompatibilidad entre las predicciones de la ecuación (2.9) y esta desigualdad tomando $\hat{a}, \hat{b}$ y $\hat{c}$ como vectores coplanares, con $\hat{c}$ haciendo un ángulo de $2\pi/3$ con $\hat{a}$, y $\hat{b}$ haciendo un ángulo de $\pi/3$ con $\hat{a}$ y $\hat{c}$. Entonces tenemos:

$$\hat{a} \cdot \hat{b} = \hat{b} \cdot \hat{c} = \frac{1}{2} \Longrightarrow \hat{a} \cdot \hat{c} = -\frac{1}{2}. \qquad (2.18)$$

Para esas direcciones tenemos según la visión cuántica:

$$|[E(A_{\hat{a}} \cdot A_{\hat{b}})]_{\Psi} - [E(A_{\hat{a}} \cdot A_{\hat{c}})]_{\Psi}| = 1 \qquad (2.19)$$

y por otro lado según la desigualdad de Bell deducida se tiene:

$$1 + [E(A_{\hat{b}}, A_{\hat{c}})]_{\Psi} = \frac{1}{2}. \qquad (2.20)$$

por lo que se muestra que la predicción cuántica y la desigualdad (2.17) son *incompatibles*, al menos para una orientación de los analizadores determinada. Se puede resumir esta versión del teorema de Bell de la siguiente forma: *ninguna teoría determinista de variables ocultas que satisfaga la ecuación* (2.10) *y la condición de localidad* (2.9) *puede estar al mismo tiempo de acuerdo con todas las predicciones de la Mecánica Cuántica con respecto a los espines de un par de partículas con espín* $\frac{1}{2}$ *en el estado singulete.* La cuestión tendría

que trasladarse así a otro plano: la experimentación. Sólo una visión del asunto podría prevalecer y esto sería determinado por los experimentos.

Lo más valioso de este argumento presentado por Bell es que conduce a formulaciones que permiten plantear experimentos para sistemas que se pueden reproducir en el laboratorio. Sin embargo la realidad es más cruel y despiadada. El problema es que esta primera forma de las desigualdades de Bell depende por completo de que la ecuación (2.10) se satisfaga exactamente, y eso no es posible en un experimento real (al menos hasta ahora). Cualquier detector construido por el hombre tiene una eficiencia menor que 100%, y cualquier analizador tiene cierta atenuación y dispersión en su canal ortogonal.

Un equipo de trabajo integrado por J.F. Clauser, M.A. Horne, A. Shimony y R.A. Holt (CHSH 1969) pudo darle la vuelta a este problema. CHSH demostraron el teorema de Bell sin requerir que la ecuación (2.10) se cumpla, derivando una desigualdad diferente que también es incompatible con las predicciones cuánticas para sistemas que nunca logran la perfecta correlación de la ecuación (2.10) pero que logran una cierta correlación mínima. Consideraron un sistema en el cual se usaban cuatro detectores capaces de registrar mediciones de los pares de partículas correlacionados en las direcciones $\hat{a}$, $\hat{b}$, $\hat{a}'$ y $\hat{b}'$, respectivamente. La desigualdad que obtuvieron en este caso es

$$|E(A_{\hat{a}} \cdot A_{\hat{b}}) - E(A_{\hat{a}'} \cdot A_{\hat{b}})| + E(A_{\hat{a}} \cdot A_{\hat{b}'}) + E(A_{\hat{a}'} \cdot A_{\hat{b}'}) \leqslant 2 \qquad (2.21)$$

Si la ecuación (2.10) se cumple, la desigualdad (2.21) implica la desigualdad (2.17) como un caso especial. Esencialmente esta es la desigualdad de Bell. En trabajos posteriores Bell, Clauser y Horne, mostraron que el teorema de Bell es válido tanto para teorías fundamentalmente estocásticas, como para teorías deterministas en las que se incluyan variables ocultas en el dispositivo experimental.

Había, sin embargo, otro problema importante para iniciar la experimentación. Idealmente, cada que se observa una partícula en uno de los detectores, *siempre* se observa la otra partícula en el otro detector. La selección del subconjunto de partículas observadas entre todas las emitidas por la fuente depende sólo del colimador y de la geometría de la fuente y no puede depender de los parámetros a y b. Nótese que la función de distribución fue definida para las partículas observadas e independientemente de a y b.

La realidad de nuevo resultó más compleja: muy a menudo se detectaban partículas cuya pareja no se registraba en absoluto en el otro detector. Por ello el conjunto de partículas considerado en el caso ideal se debe dividir en cuatro subconjuntos disconexos: a) en el que se observan ambas partículas, b) en el que se observa sólo la partícula 1, c) en el que se observa sólo la partícula 2 y c) en que ninguna partícula es observada. Así las cosas, la función de distribución de la unión de estos cuatro conjuntos claramente es independiente de $\hat{a}$ y $\hat{b}$, pero el modo de partirla puede depender de $\hat{a}$ y $\hat{b}$, ya que la detección y varios procesos de atenuación que sufren los fotones les suceden en el camino a los analizadores, por ello no hay motivo para esperar que la composición —y por tanto la distribución— de cada subconjunto sea independiente de $\hat{a}$ y $\hat{b}$. Si se quiere usar la condición de que la densidad de probabilidad está normalizada a la unidad en el espacio Λ, y a la vez esperar que sea independiente de $\hat{a}$ y $\hat{b}$, el conjunto para el que la función de distribución está definido debe incluir también a las partículas que no son observadas, cuyo número en general es desconocido y puede ser muy grande. Esta situación hace que no sea obvio cómo comprobar experimentalmente la predicción de la desigualdad (2.21).

Para atacar este problema se desarrollaron varias propuestas para demostrar el teorema de Bell, de las que destacan las del propio Bell, la del equipo CHSH y la de Clauser y Horne (CH); aquí sólo trataré esta última. Su prueba no requiere hacer hipótesis auxiliares, además define un experimento que se puede llevar a cabo, y que de hecho se llevó a cabo. Este experimento me parece de suma importancia para la plausibilidad de la Mecánica Cuántica, además de que explica la naturaleza de las correlaciones cuánticas, por ello he decidido incluirlo en el presente trabajo.

El dispositivo experimental que usaron CH fue propuesto con anterioridad por CHSH (1969); se muestra esquemáticamente en la figura (2.1)

En este dispositivo, para cada ensamblaje analizador–detector sólo hay dos posibles resultados: detección o no detección. Los resultados se formularon en términos de probabilidades para detecciones individuales y detecciones coincidentes.

Suponga que durante un periodo de tiempo, en el que los parámetros ajustables tengan los valores a y b, la fuente emite N sistemas de interés experimental de dos compo-

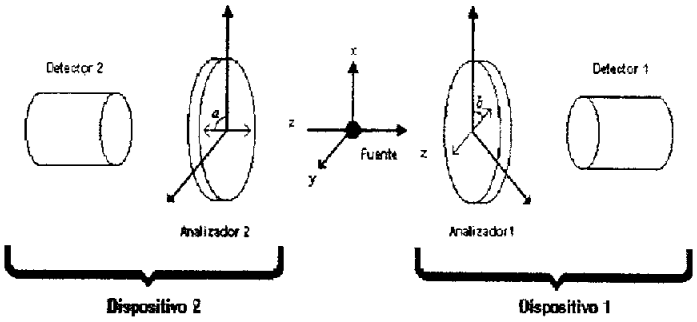


Fig. 2.1. Arreglo experimental utilizado en los experimentos de CHSH y CH. Una fuente generadora de pares EPR se encuentra entre dos dispositivos. Cada dispositivo consiste en un analizador y un detector. Los analizadores tienen los parámetros a y b respectivamente que son ajustados externamente. En esta figura, a y b representan los ángulos entre los ejes del analizador y unos ejes de referencia fijos. (tomada de Clauser y Shimony 1978).

nentes. Denotamos con $N_1(a)$ y $N_2(b)$ el número de detecciones realizadas por los detectores 1 y 2 respectivamente, y con $N_{12}(a,b)$ el número de detecciones simultáneas en los dos detectores (detecciones coincidentes). Cuando N es suficientemente grande las probabilidades de obtener estos resultados para el conjunto completo (permitiendo cierta tolerancia debida a los errores aleatorios) están dadas por:

$$\begin{aligned} p_1(a) &= N_1(a)/N \\ p_2(b) &= N_2(b)/N \\ p_{12}(a,b) &= N_{12}(a,b)/N \end{aligned} \tag{2.22}$$

Dados el estado λ del sistema compuesto y el parámetro a del primer analizador, se supone que la probabilidad de detectar la componente 1, $p_1(\lambda,a)$, estará bien definida; de manera análoga se espera lo mismo para las probabilidades $p_2(\lambda,b)$ y $p_{12}(\lambda,a,b)$; según el punto de vista de las desigualdadesde de Bell, por la condición de localidad, se supone que dichas probabilidades son independientes, así que se puede afirmar que:

$$p_{12}(\lambda,a,b) = p_1(\lambda,a)p_2(\lambda,b). \tag{2.23}$$

De aquí tenemos que los promedios de las probabilidades (2.22) están dadas por:

$$\begin{aligned} \langle p_1(a)\rangle &= \int_\Lambda p_1(\lambda,a)\,|\lambda(x,t)|^2\,dx \\ \langle p_2(b)\rangle &= \int_\Lambda p_2(\lambda,b)\,|\lambda(x,t)|^2\,dx \\ \langle p_{12}(a,b)\rangle &= \int_\Lambda p_1(\lambda,a)p_2(\lambda,b)\,|\lambda(x,t)|^2\,dx. \end{aligned} \tag{2.24}$$

Clauser y Horne introdujeron el siguiente lema, cuya demostración se puede encontrar en su artículo (CH 1974): si x, x', y, y', X, Y son números reales tales que $0 \leqslant x$, $x' \leqslant X$, $0 \leqslant y$ y $y' \leqslant Y$ entonces se cumple la desigualdad

$$-XY \leqslant xy - xy' + x'y + x'y' - Yx' - Xy \leqslant 0 \tag{2.25}$$

Usando esta desigualdad y la ecuación (2.23) tenemos:

$$-1 \leqslant p_{12}(\lambda,a,b) - p_{12}(\lambda,a,b') + p_{12}(\lambda,a',b) + p_{12}(\lambda,a',b') - p_1(\lambda,a') - p_2(\lambda,b) \leqslant 0 \tag{2.26}$$

donde, por la condición de normalización (2.11),

$$X = p_1(\lambda) = p_2(\lambda) = Y = 1 \tag{2.27}$$

que representan simplemente que ambas partículas realmente están ahí. Integrando la desigualdad (2.26)sobre λ con la función de distribución definida por (2.11), y usando las ecuaciones (2.24) se obtiene:

$$-1 \leqslant p_{12}(a,b) - p_{12}(a,b') + p_{12}(a',b) + p_{12}(a',b') - p_1(a') - p_2(b) \leqslant 0 \tag{2.28}$$

El lado derecho de esta desigualdad se puede reescribir como:

$$\frac{p_{12}(a,b) - p_{12}(a,b') + p_{12}(a',b) + p_{12}(a',b')}{p_1(a') + p_2(b)} \leqslant 1 \tag{2.29}$$

Usando las ecuaciones (2.22) y definiendo $R(a,b)$ como el porcentaje de detecciones coincidentes, $r_1(a)$ y $r_2(b)$ como los porcentaje de detecciones de partículas individuales en los detectores 1 y 2 respectivamente, la desigualdad (2.29) puede escribirse directamente en

términos de una razón de porcentajes observados:

$$\frac{R(a,b) - R(a,b') + R(a',b) + R(a',b')}{r_1(a') + r_2(b)} \leqslant 1 \tag{2.30}$$

Esta desigualdad es una *predicción general* para *cualquier* teoría realista del fenómeno observado.

Bell introdujo otra mejora a este esquema para facilitar la experimentación. Primero asignamos valores a los resultados de cualquier medición en alguno de los detectores como sigue:

$$A_a(\lambda) = \left\{ \begin{array}{l} +1, \text{ detección de partícula 1 con espín "arriba"} \\ -1, \text{ detección de partícula 1 con espín "abajo"} \\ 0, \text{ partícula 1 no detectada} \end{array} \right\} \tag{2.31}$$

$$B_b(\lambda) = \left\{ \begin{array}{l} +1, \text{ detección de partícula 2 con espín "arriba"} \\ -1, \text{ detección de partícula 2 con espín "abajo"} \\ 0, \text{ partícula 2 no detectada} \end{array} \right\} \tag{2.32}$$

Para un estado dado λ del sistema emitido se denotan los valores esperados para estas cantidades como $\langle A_a(\lambda)\rangle$ y $\langle B_b(\lambda)\rangle$. Se sigue que $\langle A_a(\lambda)\rangle$, $\langle B_b(\lambda)\rangle \leqslant 1$. En este caso, el valor esperado para el producto de estos valores esperados, está dado por:

$$E(\langle A_a(\lambda)\rangle\langle B_b(\lambda)\rangle) = \int_\Lambda \langle A_a(\lambda)\rangle\langle B_b(\lambda)\rangle \, |\lambda(x,t)|^2 \, dx \tag{2.33}$$

Como en el caso de la expresión (2.21), consideramos un sistema en el cual se usen cuatro detectores capaces de registrar mediciones de los pares de partículas correlacionados en las direcciones $\hat{a}$, $\hat{b}$, $\hat{a}'$ y $\hat{b}'$, respectivamente y consideramos la expresión:

$$E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle) - E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}'}\rangle) = \int_\Lambda [\langle A_a\rangle\langle B_b\rangle - \langle A_a\rangle\langle B_{b'}\rangle] \, |\lambda(x,t)|^2 \, dx \tag{2.34}$$

(se han eliminado las λ entre paréntesis por simplicidad) Esto se puede reescribir como

$$\begin{aligned} E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle) - E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}'}\rangle) = & \int_\Lambda \langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle \, [1 \pm \langle A_{\hat{a}'}\rangle\langle B_{\hat{b}'}\rangle] \, |\lambda(x,t)|^2 \, dx \\ & - \int_\Lambda \langle A_{\hat{a}}\rangle\langle B_{\hat{b}'}\rangle \, [1 \pm \langle A_{\hat{a}'}\rangle\langle B_{\hat{b}}\rangle] \, |\lambda(x,t)|^2 \, dx \end{aligned} \tag{35}$$

Usando el hecho de que $\langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle \leqslant 1$ y $\langle A_{\hat{a}}\rangle\langle B_{\hat{b}'}\rangle \leqslant 1$, tenemos

$$\begin{aligned} E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle) - E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}'}\rangle) \leqslant & \int_\Lambda [1 \pm \langle A_{\hat{a}'}\rangle\langle B_{\hat{b}'}\rangle] \, |\lambda(x,t)|^2 \, dx \\ & + \int_\Lambda [1 \pm \langle A_{\hat{a}'}\rangle\langle B_{\hat{b}}\rangle] \, |\lambda(x,t)|^2 \, dx \end{aligned} \tag{36}$$

a) $p_1(a) \equiv p_1$ y $r_1(a) \equiv r_1$ son independientes de a.

b) $p_2(b) \equiv p_2$ y $r_2(b) \equiv r_2$ son independientes de b.

c) $p_{12}(a,b) \equiv p_{12}(|a-b|)$, $R(a,b) \equiv R(|a-b|)$ y $E(\langle A_{\hat{a}}\rangle\langle B_{\hat{b}}\rangle) \equiv E(|a-b|)$.

Estas relaciones de simetría son susceptibles de verificación experimental. Clauser y Horne (1974) hicieron una demostración del teorema de Bell para las teorías realistas locales, en la que demostraron que la violación de las desigualdades de Bell se hace más evidente si se toman las orientaciones de a, a', b y b' coplanarmente con una diferencia entre ellas de $\phi = \pi/4n$, como se muestra en la figura (2.2):Si se usan estas orientaciones,

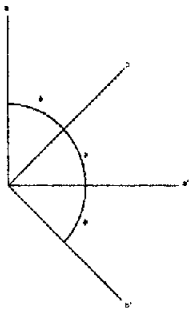


Fig. 2.2. Orientaciones óptimas para a, a', b y b'. La violación más evidente de las desigualdades basadas en las teorías realistas locales sucede cuando $n\phi = \pi/4$ (tomada de Clauser y Horne 1974).

se obtiene la siguiente relación:

$$|a-b| = |a'-b| = |a'-b'| = \frac{1}{3}|a-b'| \equiv \phi \tag{2.39}$$

Si se emplean las relaciones a), b), c), las desigualdades (2.38), y se toma la convención (2.39)se puede obtener:

$$\begin{aligned} |E(|a-b|) - E(|a-b'|) + E(|a'-b|) + E(|a'-b'|)| &\leqslant 2 \\ |E(\phi) - E(3\phi) + E(\phi) + E(\phi)| &\leqslant 2 \\ |3E(\phi) - E(3\phi)| &\leqslant 2 \end{aligned} \tag{40}$$

y de la expresión (2.30), tenemos

$$S(\phi) \equiv \frac{3p_{12}(\phi) - p_{12}(3\phi)}{p_1 + p_2} \leqslant 1 \tag{2.41}$$

o en términos de porcentajes de detección:

$$S(\phi) \equiv \frac{3R(\phi) - R(3\phi)}{r_1 + r_2} \leqslant 1 \tag{2.42}$$

y esta ya es una expresión que se puede verificar directamente en el laboratorio con detectores reales, lo que, es un avance significativo.

2.2 Los experimentos

Durante la segunda mitad de la década de los 60, la de los 70 y los 80, se diseñaron experimentos para poner a prueba explícitamente las predicciones derivadas de las teorías realistas locales usando el teorema de Bell. El primer problema fue encontrar un sistema adecuado cuyas predicciones cuánticas violaran directamente las predicciones del teorema de Bell, pero que al mismo tiempo fuera accesible a la tecnología de la época. Los experimentos que se llevaron a cabo, esencialmente eran los mismos que el que se muestra en la figura (2.1). Además de las predicciones derivadas de los modelos de variables ocultas, los experimentadores contaban con las predicciones cuánticas, que resultaban de la siguiente forma (Clauser 1976):

$$
\begin{aligned}
[p_{12}(\phi)]_{MC} &= \frac{1}{4}\eta_1\eta_2 f_1 g\left[\epsilon_+^1\epsilon_+^2 + \epsilon_-^1\epsilon_-^2 F\cos(n\phi)\right] \\
[p_1]_{MC} &= \frac{1}{2}\eta_1 f_1 \epsilon_+^1 \\
[p_2]_{MC} &= \frac{1}{2}\eta_2 f_2 \epsilon_+^2
\end{aligned}
\tag{2.43}
$$

En estas expresiones η_i representa la eficiencia cuántica efectiva del detector $i = 1, 2$, y

$$
\epsilon_+^i \equiv \epsilon_M^i + \epsilon_m^i \qquad\qquad \epsilon_-^i \equiv \epsilon_M^i - \epsilon_m^i \tag{2.44}
$$

donde ϵ_M^i y ϵ_m^i son los coeficientes de transmisión máxima y mínima (respectivamente) de los analizadores, relativos a las correspondientes bases ortogonales; f_1 y f_2 son funciones que determinan la eficiencia de los colimadores, por lo que también determinan la probabilidad de que una emisión dada de partículas entre a los detectores; normalmente estas son proporcionales a los ángulos sólidos de la "aceptancia" del colimador; g es una función que determina la probabilidad condicional de que, dado que la emisión 1 entra en el detector 1, la emisión 2 entre en el detector 2[5]. La función F es una medida de la pureza del estado inicial y de la correlación cuántica inherente de las dos partículas emitidas. Los valores de n pueden ser 1 o 2, dependiendo de si el experimento se realiza con bosones o fermiones. Si insertamos las condiciones (2.43) en la desigualdad (2.41), tomando por simplicidad $\eta \equiv \eta_1 = \eta_2$, $f = f_1 = f_2$, $\epsilon_+ \equiv \epsilon_+^1 = \epsilon_+^2$ y $\epsilon_- \equiv \epsilon_-^1 = \epsilon_-^2$ (esta suposición resulta plausible ya que todas estas funciones están relacionadas con la operación y construcción

[5] La función g implica a la función f_2, por ello la expresión para la probabilidad de detección conjunta $[p_{12}(\phi)]_{MC}$ no incluye explícitamente a f_2.

del dispositivo experimental; ver CS 1978) tenemos:

$$S(\phi)_{MC} = \frac{\frac{3}{4}\eta^2 fg\left[{\epsilon_+}^2 + {\epsilon_-}^2 F\cos(n\phi)\right] - \frac{1}{4}\eta^2 fg\left[{\epsilon_+}^2 + {\epsilon_-}^2 F\cos(3n\phi)\right]}{\frac{1}{2}\eta f\epsilon_+ + \frac{1}{2}\eta f\epsilon_+} \tag{45}$$

$$= \frac{\frac{3}{4}\eta g\left[{\epsilon_+}^2 + {\epsilon_-}^2 F\cos(n\phi)\right] - \frac{1}{4}\eta g\left[{\epsilon_+}^2 + {\epsilon_-}^2 F\cos(3n\phi)\right]}{\epsilon_+}$$

$$= \eta g\left[\frac{3}{4}\epsilon_+ + \frac{3}{4}\frac{{\epsilon_-}^2}{\epsilon_+}F\cos(n\phi) - \frac{1}{4}\epsilon_+ - \frac{1}{4}\frac{{\epsilon_-}^2}{\epsilon_+}F\cos(3n\phi)\right]$$

$$= \frac{1}{4}\eta g\left[2\epsilon_+ + 3\frac{{\epsilon_-}^2}{\epsilon_+}F\cos(n\phi) - \frac{{\epsilon_-}^2}{\epsilon_+}F\cos(3n\phi)\right]$$

encontramos finalmente que la predicción cuántica para la función $S(\phi)$ estará dada por:

$$S(\phi)_{MC} = \frac{1}{4}\eta g\left\{2\epsilon_+ + \frac{(\epsilon_-)^2}{\epsilon_+}F\left[3\cos(n\phi) - \cos(3n\phi)\right]\right\} \tag{2.46}$$

Usando de nuevo el valor óptimo de $\phi = \pi/4n$ (ver figura 2.2) para sustituirlo en (2.46), se encuentra que la condición de violación de la desigualdad 2.41 y/o 2.42:

$$S(\phi)_{MC} = \frac{1}{4}\eta g\left\{2\epsilon_+ + \frac{(\epsilon_-)^2}{\epsilon_+}F\left[3\cos(\frac{\pi}{4}) - \cos(\frac{3\pi}{4})\right]\right\} \leqslant 1 \tag{2.47}$$

recordando que $\cos(\frac{\pi}{4}) = \frac{1}{\sqrt{2}}$ y que $\cos(\frac{3\pi}{4}) = \frac{-1}{\sqrt{2}}$ tenemos:

$$\frac{1}{4}\eta g\left\{2\epsilon_+ + \frac{(\epsilon_-)^2}{\epsilon_+}F\left[\frac{3}{\sqrt{2}} + \frac{1}{\sqrt{2}}\right]\right\} \leqslant 1 \tag{48}$$

$$\frac{1}{4}\eta g\left\{2\epsilon_+ + \frac{(\epsilon_-)^2}{\epsilon_+}F\left[\frac{4}{\sqrt{2}}\right]\right\} \leqslant 1$$

$$\frac{1}{2}\eta g\epsilon_+\left\{1 + \sqrt{2}F\left(\frac{\epsilon_-}{\epsilon_+}\right)^2\right\} \leqslant 1$$

obteniendo finalmente:

$$\eta g\epsilon_+\left[1 + \sqrt{2}\left(\frac{\epsilon_-}{\epsilon_+}\right)^2 F\right] \leqslant 2 \tag{2.49}$$

Así, en una correlación experimental con valores en el intervalo determinado por esta última desigualdad, es posible distinguir entre la predicción $S(\phi) \leqslant 1$ y la de la teoría cuántica (dada por 2.46).

Los experimentadores se toparon con varios problemas (además del presupuesto) para llevar a cabo los experimentos, tales como requerir de una fuente que pudiera emitir pares de sistemas en estados discretos que pudieran ser detectados con gran eficiencia; que los pares EPR debían ser de una gran pureza cuántica (dado que la Mecánica Cuántica debe

predecir fuertes correlaciones de los observables relevantes de cada par de partículas); que los analizadores fueran capaces de permitir el paso, con gran eficiencia, de partículas en ciertos estados y a la vez rechazar a casi todas las que lleguen en estados ortogonales; y un largo etcétera (Clauser y Shimony 1978).

Los experimentos más exitosos resultaron los de "cascada de fotones". CHSH (1969) sugirieron medir la correlación en una polarización lineal de pares de fotones emitidos en una "cascada atómica" que consiste en lo siguiente: los átomos de una muestra son bombardeados con electrones, y después, al regresar a sus niveles originales, éstos emiten fotones EPR. Los átomos en decaimiento fueron observados por dos sistemas ópticos simétricos que consistían de dos lentes, un filtro de longitud de onda, un polarizador rotatorio y un detector de fotones sencillo. En estos experimentos, típicamente se midió el cociente de coincidencia para dos fotones, $R(\phi)$, como función de ϕ, el ángulo entre los planos de la polarización lineal, definidos por las orientaciones de los polarizadores (con los dos polarizadores montados); R_1 el cociente de coincidencia sin el polarizador 2; R_2 el cociente de coincidencia sin el polarizador 1; y finalmente R_0 el cociente de coincidencia sin polarizadores. En la figura (2.3) se muestra esquemáticamente este dispositivo.

Para estos casos CHSH tuvieron que suponer que dado que un par de fotones emerge de los polarizadores, la probabilidad de su detección conjunta es independiente de las orientaciones de los polarizadores a y b, para todo par emitido. Aunque esta suposición es físicamente plausible, deja abierta una cierta esperanza para los defensores de las teorías de variables ocultas. Partiendo del punto de vista de las variables ocultas, las relaciones que se sometieron a las pruebas experimentales se deducen como sigue. Denotamos con ∞ una configuración del dispositivo sin polarizador. Sea $p_1(\lambda, \infty)$ la probabilidad de que se haga una detección en el detector 1 sin el polarizador 1 y el estado de la emisión de los pares EPR es λ. Una probabilidad similar $p_2(\lambda, \infty)$ puede ser definida para el dispositivo 2; como es más fácil que se registren los fotones incidentes en el detector sin que estén

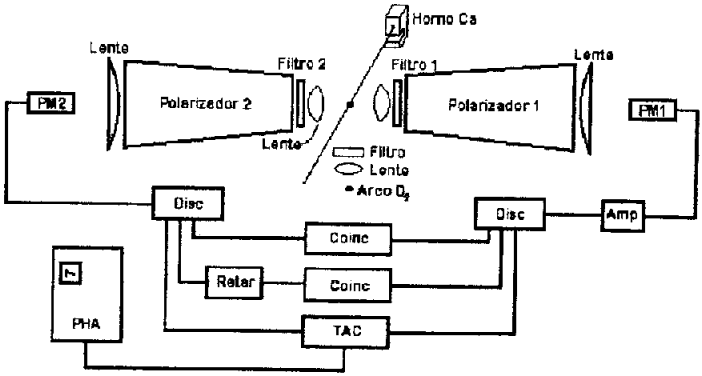


Fig. 2.3. Diagrama esquemático del dispositivo experimental y la electrónica relacionada del experimento de Freedman y Clauser. Los escaladores (que no aparecen en la figura) monitorean las salidas de los discriminadores (Disc) y de los circuitos de coincidencia (Coinc) (Tomada de Clauser 1978).

presentes los polarizadores, se tienen las siguientes desigualdades:

$$\begin{aligned} 0 &\leqslant p_1(\lambda, a) \leqslant p_1(\lambda, \infty) \leqslant 1 \\ 0 &\leqslant p_2(\lambda, b) \leqslant p_2(\lambda, \infty) \leqslant 1 \end{aligned} \tag{2.50}$$

para todo estado λ y cualquier par de orientaciones a y b de los polarizadores. Usando las desigualdades (2.25) y (2.50), junto con argumentos similares a los que se usaron para obtener (2.24) y (2.28) conducen a la desigualdad:

$$-p_{12}(\infty,\infty) \leqslant p_{12}(a,b) - p_{12}(a,b') + p_{12}(a',b) + p_{12}(a',b') - p_{12}(a',\infty) - p_{12}(\infty,b) \leqslant 0 \tag{2.51}$$

De esta expresión se deducen las condiciones requeridas para el experimento:

a) $p_{12}(a,\infty)$ es independiente de $a \Rightarrow R_1(a) \equiv R_1$

b) $p_{12}(\infty,b)$ es independiente de $b \Rightarrow R_2(b) \equiv R_2$

c) $p_{12}(a,b) \equiv p_{12}(\phi) \Rightarrow R(a,b) \equiv R(\phi)$, donde $\phi = |a-b|$.

Aunque estas condiciones no se satisfacen siempre y obviamente no se cumplen cuando cada partícula tiene una polarización lineal definida, se cumplen para todos los experimentos de cascada de fotones al menos para las predicciones cuánticas, y hasta ahora no se han detectado desviaciones experimentales de éstas. En muchos de estos experimentos el cociente de detecciones individuales en el detector 2, r_2 contiene una contribución externa de la excitación al estado intermedio por canales que no involucran el primer nivel del decaimiento. Tal excitación puede provocar la emisión de luz polarizada con la longitud de onda del segundo fotón de la cascada, pero sin presentar coincidencias. En estas condiciones la desigualdad (2.51) —recordando la expresión (2.39)— se transforma en:

$$-p_{12}(\infty,\infty) \leqslant 3p_{12}(\phi) - p_{12}(3\phi) - p_{12}(a',\infty) - p_{12}(\infty,b) \leqslant 0 \qquad (2.52)$$

para cualesquiera orientaciones a' y b. Como los cocientes de emisión en todos los experimentos se mantuvieron constantes y en la mayoría de los casos se monitorearon con ayuda de un dispositivo auxiliar, los cocientes de probabilidad se pueden escribir como cocientes de conteo:

$$\begin{aligned} \frac{p_{12}(\phi)}{p_{12}(\infty,\infty)} &= \frac{R(\phi)}{R_0} \\ \frac{p_{12}(a',\infty)}{p_{12}(\infty,\infty)} &= \frac{R_1}{R_0} \\ \frac{p_{12}(\infty,b)}{p_{12}(\infty,\infty)} &= \frac{R_2}{R_0} \end{aligned} \qquad (2.53)$$

Insertando estas ecuaciones en la desigualdad (2.52) podemos escribir la desigualdad de Bell en términos de los cocientes de coincidencia:

$$-R_0 \leqslant 3R(\phi) - R(3\phi) - R_1 - R_2 \leqslant 0. \qquad (2.54)$$

Freedman (1972) mostró que esta desigualdad se puede hacer aún más simple. Si se toma $\phi = \pi/8$, como el límite superior para el que se violan más claramente las desigualdades de Bell, la desigualdad (2.54) se convierte en

$$-R_0 \leqslant 3R(\pi/8) - R(3\pi/8) - R_1 - R_2 \leqslant 0. \qquad (2.55)$$

Por otro lado, si se toma $\phi = 3\pi/8$ como el límite inferior para el que se violan más claramente las desigualdades de Bell, y en vista de que $9\pi/8 = \pi/8$, tenemos

$$-R_0 \leqslant 3R(3\pi/8) - R(\pi/8) - R_1 - R_2 \leqslant 0 \tag{2.56}$$

Dividiendo ambas desigualdades por R_0, y restando la segunda de la primera obtenemos la más compacta expresión

$$\frac{|R(\pi/8) - R(3\pi/8)|}{R_0} \leqslant \frac{1}{4} \tag{2.57}$$

Esta desigualdad tiene la ventaja de que puede ser verificada midiendo la frecuencia de la detección conjunta de fotones con los polarizadores en sólo dos orientaciones relativas, haciendo innecesario medir los cocientes sin uno de los polarizadores. *Si las teorías realistas locales fueran ciertas los experimentos deberían cumplir esta desigualdad.*

Ahora faltan las predicciones cuánticas para este tipo de experimentos. Consideramos primero un caso ideal con analizadores de polarización y fotodetectores ideales. Aún en este caso, el que la desigualdad (2.57) se respete depende del estado en el que se preparen los pares de fotones. Supongamos que dichos pares de fotones son producidos por la transición $J = 0 \rightarrow 1 \rightarrow 0$, y supongamos también que cada fotón se propaga en direcciones opuestas a su pareja sobre el eje Z, con momento angular total cero y paridad total +1 (este estado aunque es un límite ideal, de hecho puede prepararse en el laboratorio). La parte de la polarización de la función de onda de los dos fotones está dada por:

$$\Psi_0 = \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\\0\end{pmatrix} + \begin{pmatrix}0\\1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\\0\end{pmatrix}\right] \tag{2.58}$$

donde $\begin{pmatrix}1\\0\\0\end{pmatrix}$ representa la polarización a lo largo del eje X, $\begin{pmatrix}0\\1\\0\end{pmatrix}$ representa la polarización a lo largo del eje Y, los vectores a la izquierda de los símbolos $\otimes$ representan al fotón 1 y los otros al fotón 2. Un operador de proyección para la polarización lineal a lo largo de un eje sobre el plano XY, haciendo un ángulo θ con el eje X está dado por:

$$Q(\theta) \equiv \begin{bmatrix}\cos^2\theta & \cos\theta\sin\theta & 0\\ \cos\theta\sin\theta & \sin^2\theta & 0\\ 0 & 0 & 0\end{bmatrix} \tag{2.59}$$

que se puede verificar fácilmente notando que el vector $\begin{bmatrix}\cos\theta\\ \sin\theta\\ 0\end{bmatrix}$, que representa la polarización lineal en dicha dirección es un eigenvector de $Q(\theta)$ con eigenvalor 1. En estas expresiones la polarización a lo largo del eje Z se excluyó por transversalidad; la predicción cuántica para este caso, partiendo de la expresión (2.43), y tomando $\phi = |a-b|$ como antes, obtenemos:

$$\left[\frac{R(\phi)}{R_0}\right]_{\Psi_0} = \langle\Psi_0|Q(a)\otimes Q(b)|\Psi_0\rangle = \frac{1}{4}(1+\cos 2\phi) \tag{2.60}$$

Si metemos en esta expresión los valores de Freedman para ϕ, obtenemos la expresión que se comparó en los experimentos, y que representa la predicción cuántica para ellos:

$$\left[\frac{R(\pi/8)-R(3\pi/8)}{R_0}\right]_{\Psi_0} = \frac{\sqrt{2}}{4} \tag{2.61}$$

que claramente es diferente de la desigualdad (2.57) derivada de las teorías realistas locales.

Acerquémonos un poco más a la realidad. Consideremos ahora la misma transición atómica $J = 0 \rightarrow 1 \rightarrow 0$ con analizadores de polarización ideales, pero que sólo funcionan dentro de un ángulo sólido finito. Supongamos que durante la transición no se intercambia momento angular con el núcleo (cosa bastante factible en este tipo de experimentos). El momento angular total del átomo es cero, y como hay un cambio de paridad en cada transición (y hay dos transiciones), el par de fotones tiene momento angular total cero y paridad par; así podemos expresar exactamente la parte angular de la función de onda del par de fotones:

$$\Psi = \frac{1}{\sqrt{3}}\left[Y^1_{1,1}(\hat{\eta}_1)Y^1_{1,-1}(\hat{\eta}_2) - Y^1_{1,0}(\hat{\eta}_1)Y^1_{1,0}(\hat{\eta}_2) + Y^1_{1,-1}(\hat{\eta}_1)Y^1_{1,1}(\hat{\eta}_2)\right] \tag{2.62}$$

donde $\hat{\eta}_1$ y $\hat{\eta}_2$ son las direcciones variables de propagación de los fotones 1 y 2 respectivamente, y donde $Y^1_{j,m}$ es la función vectorial esférica para el momento angular total j, el número cuántico magnético m y la paridad –1 (los armónicos esféricos). Si los lentes que hacen incidir a los fotones normalmente sobre los analizadores de polarización colectan la luz en conos de luz cuyo ángulo de apertura es 2ξ, entonces la función de onda de un par de fotones que salen del par de lentes se puede representar como $D(\xi)\Psi$, donde $D(\xi)$ es un operador especial definido en un artículo de 1971 por Abner Shimony. En ese mismo artículo se presenta un argumento que señala que ξ es infinitesimal, por lo que $D(\xi)\Psi$ es

igual al vector de polarización ideal Ψ_0 (excepto por alguna constante de normalización) de la ecuación (2.58). Esto resulta razonable ya que no existe momento angular orbital si los dos fotones se propagan sobre una recta. Por tanto, el hecho de que el par de fotones tenga un momento angular total cero implica que cada fotón tiene cero momento angular de espín, como en el estado Ψ_0. Así —partiendo nuevamente de la expresión (2.43)— la predicción de la Mecánica Cuántica para los cocientes de coincidencia en el estado de polarización $D(\xi)\Psi$ resulta:

$$\left[\frac{R(\phi)}{R_0}\right]_{D(\xi)\Psi} = \langle D(\xi)\Psi|Q(a)\otimes Q(b)|D(\xi)\Psi\rangle = \frac{1}{4}+\frac{1}{4}F_1(\xi)\cos(2\phi) \tag{2.63}$$

donde en este caso $F_1(\xi)$ es una función monótonamente decreciente, que toma el valor $F_1 = 1$ cuando $\xi = 0$ y $F_1 = 0.9876$ si $\xi = 30°$. Si de nuevo usamos los valores de Freedman para ϕ, la predicción cuántica de nuevo resulta diferente a la expresión (2.57):

$$\left[\frac{R(\pi/8)-R(3\pi/8)}{R_0}\right]_{D(\xi)\Psi} = F_1(\xi)\frac{\sqrt{2}}{4} \tag{2.64}$$

En los experimentos reales no se pueden lograr analizadores de polarización lineal ideales (como supusimos en el caso anterior), así que la ecuación (2.63) debe ser corregida para tomar en cuenta la eficiencia real de los analizadores. Sean ϵ_M^i la máxima transmitancia del i-ésimo analizador ($i = 1, 2$), y ϵ_m^i la mínima transmitancia, como se definieron para la expresión (2.43). Entonces la ecuación (2.60) debe ser reemplazada por:

$$\begin{aligned}\left[\frac{R(a,b)}{R_0}\right]_{MC} = {} & \epsilon_M^1\epsilon_M^2\langle D(\xi)\Psi|Q(a)\otimes Q(b)|D(\xi)\Psi\rangle \\ & +\epsilon_M^1\epsilon_m^2\langle D(\xi)\Psi|Q(a)\otimes \bar{Q}(b)|D(\xi)\Psi\rangle \\ & +\epsilon_m^1\epsilon_M^2\langle D(\xi)\Psi|\bar{Q}(a)\otimes Q(b)|D(\xi)\Psi\rangle \\ & +\epsilon_m^1\epsilon_m^2\langle D(\xi)\Psi|\bar{Q}(a)\otimes \bar{Q}(b)|D(\xi)\Psi\rangle\end{aligned} \tag{2.65}$$

donde $\bar{Q}(a) = 1 - Q(a)$ y $\bar{Q}(b) = 1 - Q(b)$, y obtenemos por fin (ver Clauser 1969, Shimony 1971):

$$\left[\frac{R(\phi)}{R_0}\right]_{MC} = \frac{1}{4}\left(\epsilon_M^1+\epsilon_m^1\right)\left(\epsilon_M^2+\epsilon_m^2\right)+\frac{1}{4}\left(\epsilon_M^1-\epsilon_m^1\right)\left(\epsilon_M^2-\epsilon_m^2\right)F_1(\xi)\cos 2\phi \tag{2.66}$$

que, una vez más, es muy diferente de la predicción del modelo realista local (2.57), dependiendo de los valores de las transmitancias. Por fin la mesa queda puesta. Ahora el asunto era ver en el laboratorio cuál de estas dos predicciones es la que se apega más a la realidad.

Durante los años 70 se realizaron experimentos tratando de encontrar respuesta al asunto, principalmente utilizando la técnica de transición atómica para producir los pares de fotones correlacionados, pero también se hicieron experimentos usando aniquilación de positrones y dispersión de protones con protones. Sin embargo los más sobresalientes fueron los que utilizaron la primera técnica. Durante aquélla década destacaron cuatro experimentos que a continuación describiré brevemente (por la relevancia que revisten):

1) *Experimento de Freedman y Clauser (1972).* Ellos observaron pares de fotones con longitud de onda 5513 Å y 4227 Å producidos por la transición $4p^2\ {}^1S_0 \rightarrow 4p4s\ {}^1P_1 \rightarrow 4s^2\ {}^1S_0$ en el calcio. Su dispositivo experimental es el que se muestra en la figura (2.3) (de hecho los dispositivos experimentales de estos cuatro experimentos son muy parecidos entre sí). Los átomos de calcio se proyectaron en un haz desde un horno, luego se excitaron en dicho haz por resonancia de absorción al nivel $3d4p\ {}^1P_1$ desde el cual la mayoría de los átomos decayeron al nivel $4p^2\ {}^1S_0$, que se usó como punto de partida para la transición empleada. Se usó calcio porque el 99.855% de sus átomos tienen espín cero, sin preparación alguna. Se usaron polarizadores de placas apiladas con transmitancias $\epsilon_M^1 = 0.97 \pm 0.01$, $\epsilon_m^1 = 0.038 \pm 0.004$, $\epsilon_M^2 = 0.96 \pm 0.01$, $\epsilon_m^2 = 0.037 \pm 0.004$. Cada analizador se podía rotar en incrementos angulares de $\pi/8$. El ángulo ξ subtendido por el lente primario fue 30°. El conteo de coincidencias se llevó a cabo en periodos de 100 s; estos periodos se alternaron, unos con polarizadores y otros sin polarizadores, en cada uno de los cuales se determinaron los cocientes $R(\pi/8)/R_0$ y $R(3\pi/8)/R_0$. Se hicieron correcciones para

coincidencias accidentales, pero incluso sin estas correcciones los resultados *contradijeron significativamente la desigualdad* (2.57). El promedio de los cocientes para cerca de 200 h de experimentación fueron:

$$\left[\frac{R(\pi/8)}{R_0}\right]_{Exper} = 0.400 \pm 0.007 \qquad \left[\frac{R(3\pi/8)}{R_0}\right]_{Exper} = 0.100 \pm 0.003$$

por lo que

$$\left[\frac{R(\pi/8)}{R_0} - \frac{R(3\pi/8)}{R_0}\right]_{Exper} = 0.300 \pm 0.008$$

La predicción cuántica obtenida de la expresión (2.66) (incorporando las incertidumbres introducidas por las mediciones de las transmitancias y el ángulo subtendido), es:

$$\left[\frac{R(\pi/8)}{R_0} - \frac{R(3\pi/8)}{R_0}\right]_{MC} = (0.401 \pm 0.005) - (0.100 \pm 0.005) = 0.301 \pm 0.007$$

La congruencia del experimento con las predicciones cuánticas resulta hasta bella; sencillamente es *excelente*.

2) *Experimento de Holt y Pipkin (1973).* En este experimento se observaron pares de fotones con longitudes de onda de 5676 Å y 4047 Å producidos por la transición $9^1P_1 \rightarrow 7^3S_1 \rightarrow 6^3P_0$ en el isótopo ^{198}Hg, que tiene espín nuclear igual a cero. Los átomos se excitaron bombardeándolos con electrones de 100 eV. Midiendo la polarización de los fotones de 5675 Å, se encontró que la matriz de densidad del nivel 9^1P_1 es aproximadamente $\frac{1}{3}I$, por lo que para hacer las predicciones cuánticas sobre los cocientes de conteo de coincidencias se debe usar la ecuación (2.66) con $-F_2(\xi)$ en vez de $F_1(\xi)$. Se usaron prismas de calcita como analizadores de polarización

cuyas transmitancias medidas fueron:

$$\epsilon_M^1 = 0.910 \pm 0.001 \qquad \epsilon_M^2 = 0.880 \pm 0.001$$

$$\epsilon_m^1 < 10^{-4} \qquad \epsilon_m^2 < 10^{-4}$$

El ángulo ξ se tomó como 13° ($F_2(13^\circ) = 0.9509$). Así, la predicción cuántica para este experimento resultó:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{MC} = 0.333 - 0.067 = 0.266$$

que apenas sí rebasa el límite de $\frac{1}{4}$ fijado por la predicción de variables ocultas (2.57). Los resultados experimentales después de 154.5 h de experimentación fueron:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{Exper} = (0.316 \pm 0.011) - (0.099 \pm 0.009) = 0.216 \pm 0.013$$

que *concuerda con la predicción de variables ocultas y contradice las predicciones cuánticas*. Como este resultado es contrario a lo que Holt y Pipkin esperaban, revisaron con mucho cuidado cualquier posible fuente de errores sistemáticos tales como contaminación de la fuente con isótopos con espín nuclear distinto de cero, perturbación de campos eléctricos o magnéticos externos al sistema, dispersión coherente múltiple de los fotones (radiación atrapada), sensibilidad a la polarización de los fotomultiplicadores, conteos alterados debido a la radioactividad residual y/o a los rayos cósmicos, etcétera. Se encontró un error sistemático causado por los esfuerzos aplicados sobre las paredes del tubo de vidrio usado para contener el cañón de electrones y el vapor de mercurio. *Se estimó* la actividad óptica de estas paredes y se corrigieron los resultados con estas *estimaciones*, pero no cambió nada fundamentalmente (de hecho, los valores que aquí presento fueron los corregidos).

3) *Experimento de Clauser (1976).* Clauser hizo un experimento, con la misma transición y el mismo mecanismo de excitación que se usaron en el experimento de Holt y Pipkin, usando isótopos ^{202}Hg y polarizadores de placas apiladas cuyas transmitancias eran:

$$\epsilon_M^1 = 0.965 \qquad \epsilon_M^2 = 0.972 \qquad \epsilon_m^1 = 0.011 \qquad \epsilon_m^2 = 0.008$$

y $\xi = 18.6°$. La predicción cuántica para este caso es:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{MC} = 0.2841$$

El resultado obtenido en 412 h de experimentación fue:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{Exper} = 0.2885 \pm 0.0093$$

que, como puede apreciar, otra vez *dio la razón a la Mecánica Cuántica, y claramente difiere de la desigualdad* (2.57).

4) *Experimento de Fry y Thompson (1976).* En este experimento se observaron pares de fotones de 4358 Å y 2537 Å emitidos por la transición $7^3S_1 \rightarrow 6^3P_1 \rightarrow 6^1S_0$ en el isótopo ^{200}Hg con espín nuclear cero. Se logró obtener un buen número de datos en poco tiempo (en relación con los otros experimentos), ya que, gracias a la técnica utilizada, sólo se excitó la transición de interés. Los fotones se recolectaron con un ángulo $\xi = 19.9 \pm 0.3°$; se usaron polarizadores de placas apiladas con transmitancias de:

$$\epsilon_M^1 = 0.98 \pm 0.01 \quad \epsilon_M^2 = 0.97 \pm 0.01 \quad \epsilon_m^1 = 0.02 \pm 0.005 \quad \epsilon_m^2 = 0.02 \pm 0.005$$

La matriz de densidad del nivel 7^3S_1 se determinó midiendo la polarización de los fotones de 4358 Å, que resultó ser diagonal aunque los subniveles Zeeman no estaban ocupados equitativamente; así la predicción cuántica resultó:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{MC} = 0.294 \pm 0.007$$

y el resultado experimental de 80 min (mucho menos tiempo que en los experimentos anteriores) fue:

$$\left[\frac{R(3\pi/8)}{R_0} - \frac{R(\pi/8)}{R_0}\right]_{Exper} = 0.296 \pm 0.014$$

de nuevo *en concordancia con la Mecánica Cuántica y violando la desigualdad* (2.57).

De los experimentos que involucraban dispersión de protones y aniquilación de positrones, se realizaron tres, sólo uno de ellos resultó contrario a las predicciones de cuánticas. Así, a finales de los años 70 el marcador estaba: Mecánica Cuántica 5, Realismo Local 2. Ya para estas fechas la gran mayoría de la comunidad científica interesada en estos temas, consideraba muy probable que los dos resultados que contradecían la Mecánica Cuántica fueran producto de errores sistemáticos. Evidentemente, el argumento más fuerte eran los resultados experimentales, que además de violar las desigualdades de Bell, son *cuantitativamente muy cercanos a las predicciones cuánticas.* La complejidad y delicadeza de los experimentos llevan a considerar como "normal" el que haya dos casos anómalos en nueve experimentos.

Pero todavía le quedaba alguna esperanza a las teorías de variables ocultas. En general la Ciencia descarta la *acción a distancia* como algo propio de los cuentos de hadas y princesas (y ogros), dado que no se observa en ninguno de los fenómenos observables a niveles macroscópicos. Esto se formalizó sin ambages con la teoría de la relatividad, que excluye explícitamente la acción a distancia; y la relatividad ganó rápidamente gran prestigio por explicar varios fenómenos observados que no concordaban con las teorías

físicas anteriores. Este hecho es la motivación primordial de los postulados de localidad que antes enuncié. Sin embargo, en todos los experimentos mencionados, la acción a distancia en el sentido relativista, *no queda excluida,* ya que los analizadores siempre se mantienen en orientaciones fijas por periodos de varios segundos; así que hay un amplio intervalo para que la información sobre la orientación de un analizador sea "transmitida", por algún mecanismo desconocido —consistente con la teoría de la relatividad (es decir a velocidad menor o igual a la de la luz)—, al otro analizador (y/o a la otra partícula), influenciando por lo tanto los resultados. Es concebible que tal mecanismo es lo que produce los cocientes de conteo favorables a la Mecánica Cuántica en los experimentos realizados; esto también resulta un argumento de crucial importancia para mantener vivas las teorías de variables ocultas. Para verificar esta posibilidad se requiere un experimento en el que los parámetros a y b se ajusten con gran rapidez mientras las partículas correlacionadas están en "vuelo". Si el evento de ajustar el parámetro a del primer analizador es absolutamente separado espacialmente del evento de la detección de la partícula 2, y viceversa con los eventos de ajuste del analizador 2 y detección de la partícula 1, entonces ninguna señal a velocidad menor que la luz puede comunicar información sobre la orientación de un analizador al otro en el tiempo necesario para afectar la probabilidad de detectar las partículas respectivas. Es decir, si los parámetros a y b son ajustados con suficiente rapidez, *el que no ocurra la acción a distancia implica la localidad.*

Alain Aspect, Jean Dalibard y Gerard Roger (ADR), del *Institut d'Optique Théorique et Appliquée* de la Universidad de París encararon el reto y realizaron un espectacular experimento en el que la elección entre las orientaciones de los analizadores de polarización se producía mediante conmutadores ópticos mientras los fotones se hallaban en vuelo. Su experimento les tomó ocho años y concluyó en 1982 (ADR 1982). En la figura (2.4) se muestra un diagrama del dispositivo experimental que usaron.

En su experimento cada conmutador es un frasquito de agua donde se generan ultrasónicamente y con periodicidad ondas estacionarias. Las ondas sirven de redes de difracción que pueden desviar con un alto rendimiento un fotón incidente. Con las ondas estacionarias, el fotón se desvía hacia un analizador que está orientado de una forma; cuando

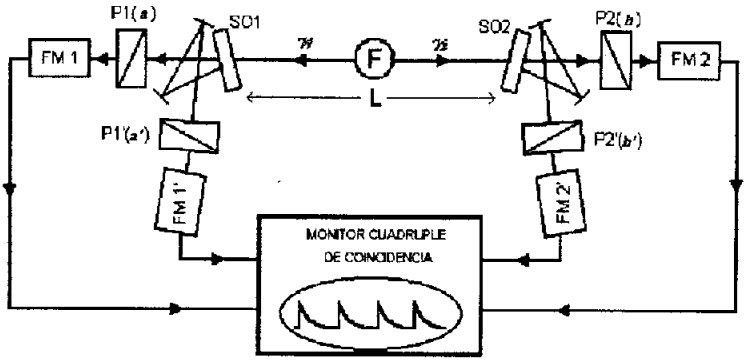


Fig. 2.4. Experimento de registro temporal con interruptores ópticos. Los pares EPR se producen en la fuente F. Los fotones v_1 y v_2 salen en direcciones opuestas, llegando a los conmutadores SO1 y SO2, respectivamente, que se encuentran a la distancia L=14 m. Cada conmutador está precedido de dos polarizadores con dos diferentes orientaciones. Según sea el estado del conmutador los fotones irán a los detectores FM1, FM1', FM2 o FM2', respectivamente. Cada combinación es equivalente a un polarizador que pudiese rotarse *muy rápida* y precisamente, durante el viaje de los fotones al dispositivo. Las detecciones se registran en el monitor cuádruple de coincidencia (Tomado de ADR1982).

no hay ondas, el fotón sigue su trayectoria hacia un analizador que tiene otra orientación. La conmutación entre las orientaciones dura unos 10 ns. Los generadores que abastecen a los dos conmutadores funcionan de modo independiente, aunque la operación es periódica, no aleatoria. Los analizadores se situaron a 13 m uno del otro, por lo que una señal viajando a la velocidad de la luz tardaría 40 ns en recorrer ese intervalo. Esto implica que el segundo analizador de polarización no puede "enterarse" de la orientación del primer analizador "a tiempo", como para poder cambiar la suya; es decir que la elección en la orientación del primer analizador de polarización no debería influir en la transmisión del segundo fotón a través del segundo analizador, y viceversa con la orientación del segundo analizador y la detección del primer fotón, es decir que se respetaría la condición de localidad de Bell y esto implicaría que se violarían las correlaciones cuánticas.

Pero el experimento le dio la razón de nuevo a la Mecánica Cuántica: los datos de las correlaciones concordaron dentro del error experimental con las predicciones cuánticas

calculadas a partir del estado cuántico Ψ_1, y diferían en más de cinco desviaciones estándar de los límites extremos permitidos por *cualquier* modelo local de variables ocultas. Con este resultado quedaron prácticamente eliminados los modelos de variables ocultas.

Posteriormente los argumentos en favor de la Mecánica Cuántica se fortalecieron aún más, cuando Greenberger, Horne y Zeilinger (GHZ 1990) mostraron que si se considera un conjunto de tres fotones en un estado como $(|111\rangle + |000\rangle)/\sqrt{2}$, y se practica una sola medición a lo largo de un eje horizontal para dos partículas y otra a lo largo de un eje vertical para la tercera, se obtendrá un resultado que resulta *exactamente lo contrario* a las predicciones de cualquier sistema de variables ocultas.

2.3 ¿Qué significa todo esto?

Queda una cuestión flotando en el aire: si aceptamos que se ha demostrado la falsedad de las teorías realistas locales (o de variables ocultas) ¿qué premisa fundamentalmente de las mismas es falsa? Al principio de este capítulo (página 28) mencioné cuáles fueron las premisas sobre las que descansaba el argumento de EPR: el realismo, el libre uso de la inducción y la separabilidad de Einstein. De las tres, el *realismo* constituye la premisa fundamental. Una teoría científica debe aportar algo más que una mera descripción de los datos, algo más que una regla empírica para predecir los resultados de futuros experimentos, debe aportar una explicación *lo más objetiva posible* de las regularidades observadas, debe aportar las *causas* de lo que se observa. Esto implica necesariamente que se considera que el mundo exterior a la mente humana *es real* y que existe junto con sus propiedades *independientemente* de lo que se pueda pensar o decir al respecto. Nada menos que el *quid* del *materialismo*.

Los experimentos relatados arriba aparentemente abrieron la puerta —formalmente— a toda una sarta de filósofos neo positivistas que consideran sin sentido cualquier afirmación acerca de la realidad externa que no se refiera de modo directo a las impresiones sensoriales. Pero al conferir a la realidad del mundo una dependencia ligada a la percepción humana, y por tanto suponer que sólo lo que es susceptible de ser "sentido" o "percibido" por el

ser humano existe, los positivistas —de toda calaña— constituyen una vertiente más del *idealismo*, los herederos de Kant.

Desde el punto de vista positivista no tendría sentido atribuir nada que se pareciera a una componente de espín bien definida a una partícula antes de medir dicha componente, y la única realidad verificable es la misma observación, la impresión sensorial (¡claro que si nadie mira los resultados también podría decirse que nunca existió ninguna componente de espín!). Así queda trivializada toda búsqueda de explicaciones (y toda la Ciencia en general) y se lo dejaríamos todo a dios, después de todo, ¡cada cabeza es un mundo! Así que evidentemente resulta muy doloroso y por demás infructuoso renunciar al realismo.

La siguiente premisa que podría cuestionarse es la justificación de postular el libre uso de la inducción. La inducción ha permitido a los científicos hacer extrapolaciones a partir de una serie de correlaciones observadas. En el caso concreto de los experimentos aquí abordados dichas correlaciones son negativas y la conclusión extrapolada es que cualquier par de fotones en el estado singulete tiene valores opuestos de una cualquiera de las componentes del espín, aun cuando no se mida ninguna de las componentes. Dicha extrapolación constituyó un paso esencial en la prueba de la desigualdad de Bell, pero es indefendible si el concepto de propiedades no medidas carece de sentido.

Poco después del artículo de EPR Niels Bohr publicó una réplica en la que defendía la completéz de la descripción cuántica de la naturaleza. Y precisamente basaba su crítica en el uso de la inducción que hacían EPR, que según él no estaba justificado; en base a esto se fundó la famosa *interpretación de Copenhague* de la Mecánica Cuántica. Su razonamiento podría sintetizarse de la siguiente forma: una partícula y un instrumento preparado para tomar una medición específica de la misma, forman ***un solo sistema*** que quedaría alterado de un modo esencial si se cambiara el dispositivo instrumental. Por ello no está permitido hacer inferencias sobre el estado de la partícula sin especificar al mismo tiempo las posiciones de los instrumentos que interaccionarán con la partícula. A mi me parece que esto es sólo una manera más "sofisticada" de renunciar al realismo, ya que su argumento podría reducirse a: la realidad *es* según se la mire (¿un vaso medio lleno o medio vacío?). Al menos Bernard d'Espagnat (1979), junto con otros científicos están de acuerdo

conmigo (o, más humildemente, yo estoy de acuerdo con ellos), al afirmar que "Bohr no era realista, o no lo era al menos de una manera coherente." Cualquier explicación de los experimentos de correlación a distancia que se base en la réplica de Bohr a EPR puede resultar inconsistente incluso con una versión moderada del realismo.

Así que nos quedamos con el realismo y la libre inducción; sólo nos queda cuestionar la *hipótesis de separabilidad* de Einstein. Dicha hipótesis expresaba la idea —intuitivamente razonable— de que las componentes de espín de un fotón no influían en las de otro fotón, si las dos partículas se hallaban suficientemente alejadas. La hipótesis más restrictiva de la separabilidad de Einstein prohibe tal influencia sólo si se propagara con una velocidad mayor que la de la luz. Tras los experimentos resulta que esta hipótesis es *altamente cuestionable*. Fue el experimento de ADR el que decididamente acabó con dicha hipótesis, ya que en él, la decisión de medir cierta componente del espín con un detector se hace hasta que es demasiado tarde para que cualquier influencia de esta decisión pueda alcanzar el otro instrumento o la fuente, incluso a la velocidad de la luz, con tiempo suficiente para alterar el resultado de la segunda medición.

Los pares de fotones correlacionados pueden entenderse como elementos de un sistema físico único que se crea durante la primera interacción y progresivamente se va extendiendo por el espacio hasta que la primera medición lo destruye. Una violación de la separabilidad de Einstein requiere acción a distancia instantánea. ¿Debe abandonarse el principio de propagación con velocidad finita de las señales? Hay que ser cuidadosos al respecto. El principio se introdujo como una premisa derivada de la teoría de la relatividad, y sin él esta teoría pierde su coherencia intrínseca. *Señales* que viajen más rápido que la luz originarían paradojas extrañas de causalidad: los observadores de algunos sistemas de referencia hallarán que un suceso está "causado" por otro que aún no ha ocurrido. Sin embargo, las influencias instantáneas que parece han de operar en los experimentos de correlación a distancia *no exigen* un cambio tan drástico de la separabilidad. Tales influencias no podrían usarse para transmitir *ninguna información* "útil". Ningún suceso que ocasiona otro suceso puede ligarse al segundo mediante este mecanismo; las influencias instantáneas pueden transmitirse *sólo entre sucesos que están relacionados por una causa común.* Por

tanto, el concepto de *señal* tendría que volver a definirse en el sentido de que sólo aquellos medios de comunicación que transmitan información utilizable deberían denominarse señales. Y el principio de propagación a velocidad finita para las señales quedaría a salvo.

Sobre las implicaciones de los experimentos hay toneladas de artículos y libros (para una exposición general y bibliografía ver por ejemplo Popescu 1994). Lo que le expuse no es mas que la punta del iceberg, pero considerar más a profundidad esta discusión me llevaría muy lejos del tema de este trabajo. El punto medular de la teletransportación cuántica es el compartir pares de partículas EPR; entender qué son dichos entes y qué implica su existencia para la Mecánica Cuántica en general, me pareció muy importante para el desarrollo de este trabajo, por ello incluí este capítulo.

CAPITULO 3
Computación Cuántica

Para abordar de lleno la teletransportación cuántica preferí hacer primero una breve y discreta zambullida en las investigaciones que permitieron su descubrimiento, y que representan la más importante fuente de aplicaciones de la misma. Es importante entender la importancia que reviste la Computación Cuántica para entender la valía de las aplicaciones de la teletransportación en este campo.

3.1 El Principio de Church-Turing

Los principios de la Mecánica Cuántica sugieren que la naturaleza se puede visualizar como un procesador de información. El vector de estado $|\psi(\mathbf{r},t)\rangle$ de un sistema cuántico es un concepto que parece extraído de la teoría de la información, ya que es un ente abstracto que contiene exactamente *toda* la información sobre dicho sistema (según uno de los postulados básicos de la Mecánica Cuántica).

Un verdadero pionero —el que realmente formalizó la idea de computadora cuántica— fue D. Deutsch. En su artículo seminal de 1985 inicia con la idea innovadora de proponer que la tesis de Church–Turing (que fue enunciada en la página 20) no se *deriva* de la Mecánica Cuántica sino que la *sustenta*, de la misma forma que un principio tan fundamental como la conservación de la energía. Para ello Deutsch hace una interesante justificación epistemológica y física. La tesis de Church–Turing planteada en este sentido sería que una computadora $\mathcal{M}$ es capaz de simular perfectamente un sistema S, bajo algún método de etiquetado de sus entradas y salidas dado, si existe un programa $\pi(S)$ para $\mathcal{M}$ tal que hace a $\mathcal{M}$ *computacionalmente equivalente* a S bajo dicho método de etiquetado. En otras palabras, $\pi(S)$ convierte $\mathcal{M}$ en una "caja negra" *funcionalmente indistinguible* de S. Precisamente, Deutsch propone el siguiente enunciado del principio de Church–Turing y lo denomina "la versión fuerte" de dicho principio (Deutsch 1985):

Todo sistema físico finito que sea realizable puede ser perfectamente simulado por una máquina universal imitadora operando por medios finitos.

Deutsch señaló que esta versión de dicho teorema es "manifiestamente física y sin ambages. Tiene el mismo estatus epistemológico que otros principios físicos." A mí me parece evidente que es mejor—o más bien dicho, más *general*— que la versión original de Church–Turing porque se refiere exclusivamente a conceptos más objetivos tales como "medición", "preparación" y "sistema físico", que ya se encuentran presentes en la teoría de mediciones. Solo se debe cumplir que el etiquetado referido en este principio debe ser finitamente especificable.

Así enunciado, podemos llamarlo el *principio* de Church–Turing. Nótese que no se refiere a las máquinas de Turing; esto cobra relevancia porque existen diferencias fundamentales entre la naturaleza de éstas y los principios de la Mecánica Cuántica. Las máquinas de Turing están descritas en términos de operaciones con bits clásicos, mientras que los principios cuánticos están en términos de la *evolución de los estados cuánticos*. Es por ello que existe la posibilidad de que la máquina universal de Turing —y las computadoras clásicas en general— sean incapaces de simular eficientemente, al menos parte de los fenómenos naturales. Viceversa, puede ser físicamente posible construir un nuevo tipo de computación esencialmente diferente de la teoría clásica de la computación. Ese es el objetivo central de la teoría llamada *Computación Cuántica*.

3.2 La computadora cuántica

Recordemos, que la Física Clásica no es mas que una *aproximación* a la realidad; también recordemos que las máquinas de Turing basan toda su dinámica en la Física Clásica. Tenemos otro hecho importante que recalcar: la máquina universal de Turing U (especificada en la página 21) no obedece esta versión fuerte del principio de Church–Turing. Estos son los principales motivos para buscar un modelo cuántico que sustituya a U. En 1982 Paul Benioff (1982) construyó un modelo computacional dentro del marco de la Cinemática y la Dinámica Cuánticas. Pero en esencia seguía siendo un modelo clásico en el sentido que

no cumplía con el principio (pero sí con el teorema clásico) de Church–Turing. Fue construido de tal forma que al final de cada paso computacional elemental ninguna propiedad característica de los sistemas cuánticos (como la interferencia, la no separabilidad o el indeterminismo, que ya se abordaron un poco en el capítulo pasado con los pares EPR) puede ser detectada. En consecuencia, todas las operaciones que podía realizar su modelo teórico podían ser simuladas a la perfección por una máquina de Turing. (Benioff 1982, Deutsch 1985).

El carismático Richard Feynman, también en 1982, propuso su simulador universal cuántico que se parecía más a la descripción final de la computadora cuántica. Este consistía en una red de sistemas de espín con interacciones entre vecinos adyacentes libremente especificables. Aunque podía simular cualquier sistema que tuviera un espacio de estados con dimensión finita, no llegó a ser realmente una computadora cuántica en el sentido estricto. "Programar" este simulador consistía en darle órdenes con las leyes dinámicas deseadas y luego poniéndolo en algún estado inicial deseado. Pero el mecanismo que permite seleccionar arbitrariamente las leyes dinámicas no fue modelado. Este era el problema principal que faltaba resolver para especificar realmente una computadora cuántica.

En 1983, David Albert describió un "autómata" que podía realizar mediciones cuánticas y enfatizó que sus propiedades al ser establecidas para medirse a sí mismo no tienen análogos entre los autómatas clásicos (Albert 1983). El autómata de Albert, aunque no era una computadora de propósito general, era realmente la primera computadora cuántica en el sentido moderno. Como antes mencioné, la descripción más formal y general de una computadora cuántica fue establecida formalmente por D. Deutsch en 1984 (Deutsch 1985). Su descripción fue el primer modelo completo de computadora cuántica, capaz de simular perfectamente cualquier sistema físico realizable. Puede simular sistemas idealmente cerrados (a temperatura cero), incluyendo todos los demás ejemplos de computadoras cuánticas y simuladores cuánticos, con exactitud arbitrariamente alta pero no perfecta.

Trataré de resumir la descripción de la computadora cuántica dada por Deustch ya que la considero bastante interesante. Como las máquinas de Turing, el modelo de una computadora cuántica $\mathcal{Q}$ consta fundamentalmente de dos componentes, un procesador

finito y una memoria infinita de la que sólo se usa una porción finita en cualquier caso. El cómputo se realiza en pasos de duración fija T y durante cada paso solamente interactúan el procesador y una parte finita de la memoria, el resto de la memoria permanece estático. El procesador consiste en M observables de dos estados: $\hat{\mathbf{n}} = \{\hat{n}_i\}$ con $i \in \mathbb{Z}_M$, donde $\mathbb{Z}_M$ es el conjunto de enteros desde cero hasta $M-1$. La memoria consiste de una secuencia infinita de observables de dos estados $\hat{\mathbf{m}} = \{\hat{m}_i\}$, que corresponde a la cinta infinita que usaba la máquina de Turing.

Una de las salidas de la máquina de Turing era la posición en que se encontraba la cinta de almacenamiento. Análogo a esta característica hay otro observable $\hat{x}$ relacionado con la memoria $\hat{\mathbf{m}}$, cuyo espectro es todo $\mathbb{Z}$. Se puede decir que $\hat{x}$ es la "localización" o las "coordenadas" exactas de la porción de la cinta que se está leyendo. Todo el asunto de la posición de la cinta es un problema ya resuelto desde la máquina de Turing, así que no es necesario meterlo en esta sopa, sólo lo menciono para que no se le olvide. Así, el estado de $\mathcal{Q}$ es un vector unitario en el espacio $\mathcal{H}$ descrito por los eigenvectores simultáneos:

$$|x; \mathbf{n}; \mathbf{m}\rangle \equiv |x; n_0, n_1 ... n_{M-1}; ... m_{-1}, m_0, m_1 ...\rangle \tag{3.67}$$

donde $x, \mathbf{n}, \mathbf{m}$ son los eigenvalores correspondientes a $\hat{x}, \hat{\mathbf{n}}, \hat{\mathbf{m}}$. A esta expresión se le conoce usualmente como "*estados computacionales base*". También usualmente se toma como espectro de nuestros observables binarios al conjunto

$$\mathbb{Z}_2 \equiv \{0, 1\} \tag{3.68}$$

. Un observable con espectro $\mathbb{Z}_2$ se puede interpretar como el elemento mínimo de memoria; se le llama comúnmente *qubit*[6] (Schumacher 1995) y es también la unidad elemental de información cuántica.

La dinámica de $\mathcal{Q}$ se puede resumir con un *operador unitario* constante U sobre $\mathcal{H}$ que especifica la evolución de cualquier estado $|\psi(t)\rangle \in \mathcal{H}$ (en la representación de Schrödinger al tiempo t) durante un paso computacional elemental:

$$|\psi(kT)\rangle = \mathsf{U}^k |\psi(0)\rangle, \qquad (k \in \mathbb{Z}^+) \tag{3.69}$$

[6] A lo largo de mi exposición, abusaré del idioma y usaré la palabra *qubit* que se deriva de la contracción de las palabras *quantum bit*. Tal vez sería más correcto usar el término *bit cuántico* o *cubit* en español, pero la verdad es que me parece más popular el término en inglés. Cuestión de enfoque.

recordando que T es el tiempo en el que se realiza un paso elemental del cómputo. No será necesario especificar el estado del sistema en cualquier otro momento que no sea algún múltiplo entero de T. El cómputo inicia en $t = 0$; en este momento $\hat{x}$ y $\hat{n}$ están preparados de tal forma que ambos valen cero; el estado de un número finito de las $\hat{\mathbf{m}}$ están preparados como el "programa" y otros como la " entrada" en el sentido del principio de Church–Turing, y el resto se pone en cero. Así:

$$\begin{aligned} |\psi(0)\rangle &= \sum_{m} \lambda_m |0;0;\mathbf{m}\rangle \qquad (3.70) \\ \sum_{m} |\lambda_m|^2 &= 1 \end{aligned}$$

donde sólo un número finito de las λ_m son diferentes de cero y se anulan siempre que haya un número infinito de las $\mathbf{m}$ diferentes de cero.

Para satisfacer el requerimento de que $\mathcal{Q}$ opera por medios finitos, los elementos de matriz de U toman la siguiente forma:

$$\langle x';\mathbf{n}';\mathbf{m}'|\mathsf{U}|x;\mathbf{n};\mathbf{m}\rangle = \left[\delta_{x'}^{x+1}\mathsf{U}^{+}(\mathbf{n}',m'_{x'}|\mathbf{n},m_x) + \delta_{x'}^{x-1}\mathsf{U}^{-}(\mathbf{n}',m'_{x'}|\mathbf{n},m_x)\right]\prod_{y\neq x}\delta_{m_y}^{m'_y} \qquad (3.71)$$

El producto del lado derecho asegura que sólo un bit de memoria, el x-ésimo, participa en un paso computacional elemental. Las deltas de Krónecker $\delta_{x'}^{x\pm1}$ aseguran que durante cada paso la "posición de la cinta" x no cambie por más de una unidad, ya sea hacia adelante, atrás o ambas. Las funciones $\mathsf{U}^{\pm}(\mathbf{n}',m'|\mathbf{n},m)$ que representan un movimiento dinámico que depende sólo de los observables "locales" $\hat{\mathbf{n}}$ y $\hat{m}_x$, son arbitrarios, sólo tienen que cumplir la condición $\mathsf{U}^{\dagger}\mathsf{U}=\mathsf{U}\mathsf{U}^{\dagger} = \mathsf{I}$. Cada elección de $\mathsf{U}^{\pm}$ define una diferente computadora cuántica $\mathcal{Q}\left[\mathsf{U}^{+},\mathsf{U}^{-}\right]$, y de dicha elección dependerá la o las tareas que en particular esa computadora cuántica pueda realizar.

En el capítulo primero se abordó el problema de la *detención* de una máquina de Turing, que resulta otra forma de plantear el problema de la *computabilidad*[7]: si una máquina de Turing se detiene (en algún punto, como parte del programa que ejecuta) realizando una

[7] En computación cuántica se hace aún más patente el hecho de que cualquier cómputo es un proceso físico que involucra la evolución física de las propiedades seleccionadas de un sistema físico. Los problemas de qué es computable y qué es la complejidad de un cómputo deben depender esencialmente de las leyes de la física y no pueden ser caracterizados exclusivamente por las matemáticas.

operación o programa determinado ello implica que dicha operación o programa es *computable* por dicha máquina. Se dice que una máquina de Turing se ha detenido cuando dos estados consecutivos de la máquina son *idénticos*. Como muestra la expresión(3.69), dos estados consecutivos de una computadora cuántica $\mathcal{Q}$ *no pueden ser idénticos* después de un cómputo no trivial (de hecho esto es válido para cualquier computadora *reversible*). Además $\mathcal{Q}$ no debe ser medida antes de que el cómputo haya terminado, ya que ello podría —en general— alterar su estado relativo. Así que el problema de la detención para las computadoras cuánticas tiene otros ángulos antes insospechados para las máquinas de Turing.

La forma en cómo Deutsch (1985) resolvió este problema fue haciendo que las computadoras cuánticas señalaran *activamente* que se han detenido. Para ello, uno de los bits internos del procesador, digamos $\hat{n}_0$, debe reservarse para este propósito. Todo programa computable por $\mathcal{Q}$ debe poner el valor 1 en $\hat{n}_0$ cuando termine, pero no debe interactuar con $\hat{n}_0$ en alguna otra manera. Por ello el observable $\hat{n}_0$ debe ser periódicamente observado externamente sin afectar el funcionamiento de $\mathcal{Q}$. Así el problema de la computabilidad para las computadoras cuánticas se puede expresar de la siguiente manera en forma general:

Un programa P para la computadora cuántica $\mathcal{Q}$ es computable si el valor esperado de su tiempo de cómputo es finito.

Como en el caso de las máquinas de Turing, no podemos idear algún programa que nos diga si tal o cual programa es computables o no; es decir que el problema epistemológico de la computabilidad *no es resuelto por las computadoras cuánticas.*

Sigamos con la descripción de $\mathcal{Q}$. Debido a lo unitario, la dinámica de $\mathcal{Q}$ es *necesariamente reversible*, como cualquier sistema cuántico cerrado. Por otro lado, las máquinas de Turing sufren cambios irreversibles durante sus procesos de cómputo, y de hecho se sostuvo por un buen tiempo que la irreversibilidad era una característica esencial de la computación. Pero desde la década de los 70 Charles Bennett (1973), de la división científica de la IBM, demostró que esto no sucede para un modelo computacional clásico explícitamente reversible equivalente a la máquina universal de Turing U. Se pueden obtener computado-

ras cuánticas $\mathcal{Q}\left[\mathsf{U}^{+},\mathsf{U}^{-}\right]$ equivalentes a cualquier máquina de Turing reversible usando la expresión

$$\mathsf{U}^{\pm}(\mathbf{n}',m'|\mathbf{n},m)=\frac{1}{2}\delta_{\mathbf{n}'}^{A(\mathbf{n},m)}\delta_{m'}^{B(\mathbf{n},m)}[1\pm C(\mathbf{n},m)] \tag{3.72}$$

donde A, B y C son funciones con codominios $(\mathbb{Z}_2)^M$, $\mathbb{Z}_2$ (ver definición en pag. 66)y $\{-1,1\}$, respectivamente (ver expresión 3.68). Así, se puede decir que las máquinas de Turing son aquéllas computadoras cuánticas cuyas dinámicas aseguran que permanecen en un estado computacional base al final de cada paso, dado que inician en uno. Para asegurar la unitariedad es necesario que el mapeo

$$\{(\mathbf{n},m)\}\leftrightarrow\{A(\mathbf{n},m),B(\mathbf{n},m),C(\mathbf{n},m)\} \tag{3.73}$$

sea biyectivo. Deben existir elecciones que hagan a $\mathcal{Q}$ equivalente a una máquina universal de Turing U, de otra forma las funciones constitutivas A, B y C serían arbitrarias.

Para no caer en la construcción explícita de $\mathsf{U}^{\pm}$ —que resulta bastante tediosa (ver Deutsch 1985)— recurrimos a una descripción de $\mathcal{Q}$ más amigable. Para toda función recursiva f existe un programa $\pi(f)$ para U tal que cuando la imagen de $\pi(f)$ está seguida por la imagen de cualquier entero i en la entrada de U, U finalmente se detiene con $\pi(f)$ e i misma es seguida por la imagen de $f(i)$ y todos los bits posteriores se hacen cero. Esto es, para algún entero positivo k

$$\mathsf{U}^{k}|0;\mathbf{0};\pi(f),i,\mathbf{0}\rangle=|0;1,0;\pi(f),i,f(i),\mathbf{0}\rangle \tag{3.74}$$

donde $\mathbf{0}$ denota una secuencia de ceros, y no se muestran explícitamente los eigenvalores cero de $\hat{m}_i(i<0)$. El concepto de U no pierde generalidad si se pide que cada programa organice la memoria como una secuencia infinita de "ranuras" capaces cada una de guardar un entero arbitrario. Para cada función recursiva f y los enteros a y b, existe un programa $\pi(f,a,b)$ que computa la función f sobre el contenido de la ranura a y pone el resultado en la ranura b, dejando la ranura a idéntica. Si el valor inicial de la ranura b no es cero, la reversibilidad implica que no se borre su valor anterior, sino que se combine con el nuevo valor computado de alguna manera que sea reversible; así, resumiendo lo más posible, podemos representar el efecto del programa $\pi(f)$ como

$$|\pi(f,a,b),i,j\rangle\rightarrow|\pi(f,a,b),i,j\oplus f(i)\rangle \tag{3.75}$$

donde $\oplus$ es cualquier operador asociativo y conmutativo que cumpla las propiedades $i \oplus i = 0$ y $i \oplus 0 = i$.

Para completar la descripción de $\mathcal{Q}$ menciono otra propiedad importante: para toda función recursiva biyectiva g existe un programa $\phi(g,a)$ cuyo efecto es solamente remplazar cualquier entero i en la ranura a por $g(i)$. La prueba es inmediata si el valor inicial de la ranura b es cero:

$$\phi(g,a) = \pi(g,a,b) \cdot \pi(g^{-1},b,a) \cdot \pi(I,b,a) \cdot \pi(I,a,b) \tag{3.76}$$

donde I es la función "medición perfecta" (Deutsch 1985) definida por

$$|\pi(I,a,b),i,j\rangle \rightarrow |\pi(I,a,b),i,j \oplus i\rangle \tag{3.77}$$

La computadora cuántica $\mathcal{Q}$ tiene todas las propiedades de la máquina universal de Turing U resumidas en las expresiones (3.74), a la (3.77). Pero además $\mathcal{Q}$ permite otras clases de programas que hacen que los estados computacionales base evolucionen a superposiciones lineales de sí mismos. Todos los programas para $\mathcal{Q}$ se pueden expresar en términos de las operaciones elementales ordinarias para máquinas de Turing (las compuertas lógicas normales, ver expresión 1.2) y otras ocho operaciones (más adelante se muestra que de hecho se pueden expresar como combinaciones lineales de una sola puerta cuántica universal). Se trata de transformaciones unitarias confinadas en un espacio de Hilbert bidimensional $\mathcal{H}$, que es el espacio de todos los estados de un sistema de un solo bit a las que comúnmente se les conoce como *compuertas lógicas cuánticas elementales*. Tales transformaciones o compuertas forman una familia de cuatro parámetros reales, definidos así: sea α cualquier múltiplo irracional de π, entonces las cuatro primeras compuertas lógicas cuánticas serían

$$\begin{aligned} \mathsf{V}_0 &= \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}, & \mathsf{V}_1 &= \begin{bmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{bmatrix} \\ \mathsf{V}_2 &= \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & 1 \end{bmatrix}, & \mathsf{V}_3 &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} \end{aligned} \tag{3.78}$$

que junto con sus respectivas inversas V_4, V_5, V_6 y V_7, generan bajo composición un grupo denso en el grupo de todas las transformaciones unitarias en $\mathcal{H}$[8]. En la literatura también

[8] Un grupo denso G de transformaciones unitarias en el espacio $\mathcal{H}$ es un conjunto de estas que bajo una

se menciona como conveniente (aunque no esencial) añadir otras dos compuertas lógicas cuánticas:

$$\mathsf{V}_8 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \quad \text{y} \quad \mathsf{V}_9 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \tag{3.79}$$

A cada una de estas compuertas (que también se les conoce como generadores) V_i le corresponden elementos de la base computacional, que representan programas $\phi(\mathsf{V}_i, a)$, que ejecutan la operación V_i sobre el bit menos significativo de la a-ésima ranura. Así, si j es cero o uno de dichos elementos de la base computacional, los programas evolucionarán de acuerdo con

$$|\phi(\mathsf{V}_i, a), j\rangle \rightarrow \sum_{k=0}^{1} \langle k|\mathsf{V}_i|j\rangle |\phi(\mathsf{V}_i, a), k\rangle \tag{3.80}$$

La composición de los V_i puede ser afectada por la concatenación de los programas $\phi(\mathsf{V}_i, a)$. Por ello deben existir programas que efectúen sobre el estado de cualquier bit una transformación unitaria arbitrariamente cercana a cualquier otra que se desee.

Conclusiones análogas se aplican al estado conjunto de cualquier número finito L de bits que se especifique. Esta no es una observación trivial ya que tal estado no es necesariamente un producto directo de estados confinados a los espacios de Hilbert de los bits individuales, aunque es en general una superposición lineal de tales productos.

Ahora nótese que las $(2^L)!$ permutaciones posibles de los estados computacionales base de L bits, son funciones recursivas invertibles, y que por tanto pueden ser efectuadas por programas para U y por tanto para Q. Ahora tomemos por hipótesis que las transfor-

---

correspondencia u operación (que en este caso es la composición) que asocia a cada par de elementos $x, y \in G$ un elemento $xy \in G$ que cumple con las siguientes características:

1. i) x(yz)=(xy)z $\forall$ x,y,z$\in$G

   ii) $\exists$ e$\in$G tal que ex=xe=x $\forall$ x$\in$G.

   iii) A cada x$\in$G le corresponde un elemento $x^{-1} \in$G tal que $xx^{-1}=x^{-1}x=e$.

   iv) $[G]=H$ donde $[G]$ denota la cerradura de G.

En resumidas cuentas, todos los estados cuánticos posibles de un sistema de un solo bit, pueden expresarse como combinación lineal de los elementos del conjunto de estas ocho puertas lógicas, que cumplen las propiedades de un grupo.

maciones diagonales de $(L-1)$ bits son precisamente computables por $\mathcal{Q}$. Dichas transformaciones son generadas por ciertas matrices diagonales unitarias de dimensión 2^L cuyos eigenvalores tienen degeneración par. Las permutaciones de los estados base permiten a $\mathcal{Q}$ efectuar precisamente cualquier transformación unitaria diagonal con esta degeneración. La cerradura de este conjunto de transformaciones degeneradas bajo multiplicaciones es un grupo denso de transformaciones diagonales en el grupo de todas las transformaciones diagonales unitarias de dimensión 2^L. También es importante notar que una transformación arbitraria U de dimensión 2^L puede ser efectuada transformando sucesivamente cada eigenvector $|\psi\rangle$ de U en el vector $|0_L\rangle$ de manera precisa (ejecutando el programa $\rho^{-1}(|\psi\rangle)$), y luego llevando a cabo una transformación diagonal unitaria que multiplica $|0_L\rangle$ por el eigenvalor (un factor de fase) correspondiente a $|\psi\rangle$, pero que tenga un efecto arbitrariamente pequeño sobre cualquier otro estado base computacional, y luego ejecutar $\rho(|\psi\rangle)$. Esto establece el sentido en el cual $\mathcal{Q}$ es una computadora cuántica *universal*; es decir que puede simular con precisión arbitraria cualquier otra computadora cuántica $\mathcal{Q}\left[\mathsf{U}^+, \mathsf{U}^-\right]$. Aunque una computadora cuántica tiene un espacio de estados de dimensión infinita, sólo se necesita aplicar una transformación unitaria de dimensión finita en cada paso del cómputo para simular su evolución. He aquí la computadora cuántica, al menos en su idea fundamental.

Se estará haciendo la pregunta ¿y realmente es posible construir este dispositivo? Por supuesto no es un asunto trivial. La mayor parte de las computadoras cuánticas propuestas se han enfocado en el diseño de hamiltonianos construidos especialmente para realizar cómputos, pero que no necesariamente corresponden a algún sistema físico. Las propuestas más prometedoras consisten en arreglos de sistemas cuánticos débilmente acoplados (Lloyd 1993); los cómputos se efectúan sujetando dichos arreglos a secuencias de pulsos electromagnéticos que inducen transiciones entre estados cuánticos localmente definidos. En una dimensión, la computadora cuántica puede consistir en estados electrónicos localizados en un polímero; en dos dimensiones, pueden ser puntos cuánticos en un semiconductor; en tres dimensiones, se pueden usar espines nucleares en una malla cristalina. En estos sistemas los bits pueden estar en superposiciones de 0 y 1, la incertidumbre cuántica se puede usar para generar números aleatorios, y los estados pueden ser creados para exhibir úni-

camente correlaciones cuánticas. La verdad no es mi intención entrar en mucho detalle, porque representa un tema bastante profundo que me llevaría lejos de donde quiero llegar, así que le puedo recomendar por ejemplo el trabajo de Lloyd (1993).

3.3 Información cuántica

Pues a partir de la poderosa idea de la computadora cuántica se desarrolló toda una teoría de la información cuántica que serviría para esta máquina aun hipotética (en realidad desde poco antes). En este apartado sólo voy a mencionar sus generalidades para tener una visión panorámica al respecto.

Una diferencia fundamental entre la Física Clásica y la Cuántica es que en este último caso, el estado de un sistema cuántico es *inmesurable* en principio, es decir, dado un estado cualquiera $|\psi\rangle$ de un qubit no es posible identificarlo completamente. De hecho cualquier medición de $|\psi\rangle$ sólo puede aportar, a lo mucho, un bit de información sobre su identidad, mientras que la descripción completa de $|\psi\rangle$ requiere especificar dos números reales (suponiendo por supuesto que se encuentra en un espacio de Hilbert bidimensional). Toda la información representada por un estado cuántico (que en su vasta mayoría resulta inaccesible) normalmente es referida como *información cuántica*, en contraste con la noción más familiar de la información clásica que puede ser totalmente accesible luego de practicar una medición, y que además no cambia debido a dicha medición.

Todas las compuertas lógicas definidas en (3.78) y (3.79) actúan sobre un qubit y son producto de algún hamiltoniano de la ecuación de Schrödinger, ya que todos son operadores unitarios. Existe una infinidad de compuertas lógicas cuánticas de un solo qubit, en contraste con la teoría de la información clásica, donde sólo hay dos compuertas lógicas para un solo bit: la identidad y la negación. Por ejemplo la puerta lógica cuántica "NOT" realiza la operación de cambiar $|0\rangle$ a $|1\rangle$ y viceversa, por ello es análoga a la puerta clásica NOT (expresión 1.1). A esta puerta lógica cuántica normalmente se le denota como X ya que se trata de la matriz de Pauli σ_x.

En principio, existen compuertas lógicas para un conjunto arbitrario de qubits, pero es interesante fijarnos en un conjunto de operadores unitarios que actúan sobre un par de qubits, y que pueden escribirse como $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \mathrm{V}$, donde I es el operador identidad para un solo qubit y V es alguna otra puerta lógica elemental de un solo qubit. Tal puerta lógica de dos qubits se le llama "V controlada", ya que la acción I o V sobre el segundo qubit depende si el estado del primer qubit es $|0\rangle$ ó $|1\rangle$. Por ejemplo el efecto de NOT controlado (NOC) sería

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned} \tag{3.81}$$

El segundo qubit sufre el efecto de la transformación NOT si y sólo si el primer qubit está en estado $|1\rangle$. El efecto de NOC actuando sobre un estado $|a\rangle|b\rangle$ se puede escribir como $a \rightarrow a, b \rightarrow a \ominus b$, donde $\ominus$ simboliza la puerta lógica de negación exclusiva (XOR).

Se pueden combinar todas estas compuertas lógicas en muchas secuencias diferentes para dar origen a muchas operaciones. Para una revisión exhaustiva ver, por ejemplo, Barenco *et al.* (1995). Para algunas consideraciones de diseño Vlatko Vedral *et al.* (1996) y Beckman *et al.* (1996) presentan discusiones interesantes. Aquí cabe mencionar que existe una puerta *cuántica universal* equivalente a la del caso clásico, que es una puerta que por el uso repetido de combinaciones diferentes de bits puede generar la acción de cualquier otra puerta. Como toda evolución cuántica es unitaria basta con poder generar todas las transformaciones unitarias de n qubits en la computadora. La manera más directa para obtener una puerta universal es considerar dos compuertas: $\mathrm{V}_u(\theta, \phi)$ y NOC, donde

$$\mathrm{V}_u(\theta, \phi) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -ie^{-i\phi}\sin(\frac{\theta}{2}) \\ -ie^{i\phi}\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}. \tag{3.82}$$

Se puede mostrar fácilmente que cualquier matriz unitaria de $n \times n$ puede formarse componiendo compuertas XOR de dos qubits y rotaciones de un qubit (Barenco *et al.* 1995). Resulta notable que simplemente se necesiten compuertas de dos qubits para generar la

puerta universal en el caso cuántico; por ello el concepto de puerta lógica cuántica es bien poderoso e importante.

Ahora nos encontramos con otra característica general de la información cuántica: la no clonación[9]. De hecho esto se ha expresado como un sencillo teorema

Teorema de no clonación.– Un estado cuántico desconocido no puede ser clonado.

Esto se refiere a que es imposible generar copias *idénticas* de un estado cuántico, a menos de que dicho estado sea conocido, es decir que exista la información clásica necesaria para especificarlo. Veamos de dónde sale esta característica de la información cuántica. Para generar una copia de un estado cuántico $|\alpha\rangle$ debemos hacer que un par de sistemas cuánticos sigan la evolución $V(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$, donde V es el operador unitario de evolución. Para que esto funcione para cualquier estado, V no debe depender de α, y por tanto $V(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$ para toda $|\beta\rangle \neq |\alpha\rangle$. Sin embargo, si consideramos el estado $|\gamma\rangle = (|\alpha\rangle + |\beta\rangle)/\sqrt{2}$ tenemos $V(|\gamma\rangle|0\rangle) = (|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle)/\sqrt{2} \neq |\gamma\rangle|\gamma\rangle$ por lo que la clonación, al menos en este caso, no es posible. Esto es válido para cualquier método que quiera emplearse para dicha clonación.

Note que cualquier operación de clonación V dada puede funcionar sólo sobre algunos estados (en el sentido de $|\alpha\rangle$ y $|\beta\rangle$ d el ejemplo anterior), ya que como V preserva la traza, dos diferentes estados clonables deben ser ortogonales: $\langle\alpha|\beta\rangle = 0$. A menos de que ya sepamos que el estado que va a copiarse es uno de esos estados ortogonales, no se puede garantizar que dada V se pueda clonar dicho par de estados. Esto no sucede así en el caso clásico, donde, por ejemplo, se pueden hacer las copias (funcionalmente idénticas) que se deseen de cualquier archivo de computadora, cualquiera que sea la información contenida (siempre y cuando se cuente con el programa clonador adecuado).

El teorema de no clonación junto con la "paradoja" EPR (que estudiamos en el capítulo precedente) muestran de manera bastante ingeniosa que la Mecánica Cuántica no Relativista es una teoría consistente. Si fuera posible clonar cualquier estado cuántico impli-

[9] Aunque en general no resulta conveniente introducir palabras de otro tipo de fenómenos, ya que con ellas pueden colarse ideas de aquéllas que no tienen representación en la física y se pueden prestar a confusiones, en este caso el fenómeno referido como "clonación" resulta bien entendido y conocido de esta forma. Por ello decidí usar dicho término.

caría que las correlaciones EPR podrían ser usadas para enviar información más rápido que la luz, lo que —como antes vimos—es imposible, en concordancia con los principios cuánticos y relativistas (Steane 1997).

Como elementos de información, los qubits se pueden usar para almacenar y transmitir información *clásica*. Antes de continuar conviene introducir a un par de personajes que serán protagónicos en lo sucesivo: Ana y Beto; En la literatura de habla inglesa tradicionalmente los llaman Alice y Bob, y los usan para denotar a una fuente de información A y un receptor B. Para transmitir una cadena clásica de bits —101001, por ejemplo— Ana puede mandar seis qubits preparados en el estado $|101001\rangle$. Beto puede obtener la información midiendo cada qubit en la base $\{|0\rangle, |1\rangle\}$, es decir que estos son los eigenestados del observable medido. La medición arroja como resultado la cadena clásica de bits sin ambigüedades. No se puede transmitir más de un bit clásico por cada qubit enviado.

3.4 Entrelazamiento y superposición

El fenómeno del entrelazamiento, no tiene paralelo en la mecánica clásica, y por tanto resulta radicalmente contrario a la intuición de quien no se ha empapado a fondo de la teoría cuántica. Es a partir de este asunto que las computadoras cuánticas pueden sacar una enorme ventaja y hacer cosas que ninguna máquina clásica podría hacer.

En el cálculo de probabilidades clásico es posible programar una computadora para seleccionar una de varias formas posibles para realizar un cómputo, de acuerdo con las leyes de la probabilidad. En cualquier caso específico de cálculo, sin embargo sólo se usa una de las potenciales formas de realizar el cómputo. Todo aquello que pudo haber pasado pero no pasó no tiene ninguna influencia en el resultado del cómputo. Es lo que el sentido común nos dicta: "el hubiera no existe". Lo que hace a la Computación Cuántica tan poderosa —y contraria a la intuición— es que *todas las formas potenciales de cómputo se usan simultáneamente en una sola unidad del hardware,* de acuerdo con el principio de superposición de la Mecánica Cuántica. Además, todas las formas posibles de realizar el cómputo que podrían dar el mismo resultado *interfieren*; esto ni siquiera tiene sentido en la

computación clásica. Dicha interferencia puede ser constructiva o destructiva. En el caso de interferencia constructiva la probabilidad de que un sistema cualquiera vaya del estado $|a\rangle$ a otro estado $|b\rangle$ por un camino determinado, es más grande que la suma de las probabilidades de que el sistema vaya de $|a\rangle$ a $|b\rangle$ por cada camino diferente. En el caso de interferencia destructiva la cosa es más espectacular. Supongamos que hay una probabilidad diferente de cero de que un sistema vaya del estado $|a\rangle$ al estado $|b\rangle$ a través de un estado intermediario $|c\rangle$; de la misma forma la probabilidad de que el mismo sistema vaya de $|a\rangle$ a $|b\rangle$ a través de otro estado intermediario $|d\rangle$. Según la Mecánica Cuántica, la probabilidad de que el sistema vaya del estado $|a\rangle$ al $|b\rangle$ puede ser cero. Según Richard Feynman (1982) es como si "de una manera u otra alguna de las probabilidades fuera negativa".

Para entender cómo es esto posible necesitamos saber que la Mecánica Cuántica permite que una cantidad arbitraria de estados de la computadora (y en general de cualquier sistema) puedan coexistir simultáneamente en *superposición cuántica*. Supongamos por ejemplo que tenemos una máquina con un bit de memoria. En una computadora clásica este bit podría estar ya sea en el estado $|1\rangle$ ó $|0\rangle$. En una computadora cuántica Q podría estar en una superposición arbitraria de dos estados:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.83}$$

donde β y α son números complejos llamados *amplitudes* de $|1\rangle$ y $|0\rangle$, respectivamente. Estas amplitudes se encuentran sujetas a la restricción $|\alpha|^2 + |\beta|^2 = 1$. Si el estado de la computadora es observado mientras se encuentra en el estado $|\psi\rangle$, habrá una probabilidad de $|\alpha|^2$ de observarlo en el estado $|0\rangle$ y una probabilidad de $|\beta|^2$ de observarlo en el $|1\rangle$. Una consecuencia inevitable de dicha observación es destruir la superposición y proyectar el estado ya sea en $|1\rangle$ ó $|0\rangle$, dependiendo del resultado de la observación (se valen mediciones incompletas que son menos informativas, pero que perturban menos al estado). Mientras el estado no sea perturbado la Mecánica Cuántica permite realizar cómputos que dependen de él en lo que se llama *paralelismo cuántico;* por ejemplo si computamos una función clásica de un solo bit f sobre $\alpha|0\rangle + \beta|1\rangle$ producirá la superposición $\alpha|f(0)\rangle + \beta|f(1)\rangle$; a primera vista esto parece una mera curiosidad, sin embargo es el fundamento físico que permitiría a

una computadora cuántica resolver problemas irresolubles para las computadoras clásicas, por ejemplo el famoso problema de la factorización de números primos muy grandes.

Hagamos otras consideraciones con nuestra misma computadora cuántica de un solo qubit antes de pasar a otro tópico. Sea $|\psi\rangle$ como se definió en (3.83). Considere el siguiente algoritmo conocido como QCF[10](Brassard 1994):

$$\begin{aligned} \text{Si } |\psi\rangle &= |0\rangle \longrightarrow |\psi\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) \\ \text{en otrocaso } |\psi\rangle &= \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \end{aligned} \tag{3.84}$$

Para cualquier valor del estado inicial de $|\psi\rangle$, una medición inmediatamente después de aplicar el algoritmo QCF dará como resultado $|0\rangle$ ó $|1\rangle$ con probabilidad del 50%, ya que $|\sqrt{2}/2|^2 = |-\sqrt{2}/2|^2 = 1/2$. Podemos decir que si comenzamos el cómputo con la máquina en cualquier estado clásico, ejecutamos el algoritmo QCF una vez y observamos el resultado, lo que obtenemos es ¡un volado perfecto entre estados de la máquina!

Veamos qué pasa si repetimos dos veces consecutivas el algoritmo QCF sin observar el resultado entre ellas. Supongamos que el estado inicial es $|\psi\rangle = |1\rangle$. Obtenemos:

$$\begin{aligned} |\psi\rangle &= \frac{\sqrt{2}}{2}\left(\frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) + \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)\right) \\ &= \frac{1}{2}(|0\rangle - |1\rangle + |0\rangle + |1\rangle) \\ &= |0\rangle. \end{aligned} \tag{3.85}$$

Análogamente, si el estado inicial es $|\psi\rangle = |0\rangle$ y procedemos del mismo modo, obtenemos $|\psi\rangle = -|1\rangle$. Observamos que su estado ha cambiado a la negación lógica de su estado original. Por ello, a QCF se le llama comúnmente la raíz cuadrada de la negación.

Ahora considere de nuevo qué pasa si comenzamos con la computadora en estado $|1\rangle$ e iteramos dos veces consecutivas el algoritmo QCF. Pensando clásicamente, existen cuatro posibles caminos para realizar el cómputo de la forma $|a\rangle \rightarrow |b\rangle \rightarrow |c\rangle$:

- $|1\rangle \rightarrow |0\rangle \rightarrow |0\rangle$

[10] Observe que este algoritmo QCF no es otra cosa que la puerta lógica cuántica V_8 definida en (3.79).

- $|1\rangle \rightarrow |0\rangle \rightarrow |1\rangle$
- $|1\rangle \rightarrow |1\rangle \rightarrow |0\rangle$
- $|1\rangle \rightarrow |1\rangle \rightarrow |1\rangle$

La amplitud del segundo camino, por ejemplo, es $\frac{\sqrt{2}}{2} \times \left(-\frac{\sqrt{2}}{2}\right) = -\frac{1}{2}$ ya que la amplitud de ir de $|1\rangle$ a $|0\rangle$ es $\frac{\sqrt{2}}{2}$ y la amplitud de regresar de $|0\rangle$ a $|1\rangle$ es $-\frac{\sqrt{2}}{2}$ (recuerde que la amplitud de cualquier camino es el producto de las amplitudes de las opciones tomadas a lo largo de dicho camino, muy similar a la multiplicación de probabilidades a lo largo de cada camino en los algoritmos probabilísticos). De manera análoga, la amplitud de las tres otras vías es $+\frac{1}{2}$.

Si no hubiera interferencia, la probabilidad de seguir cualquier camino sería el cuadrado de la magnitud de su amplitud $|\pm\frac{1}{2}|^2 = \frac{1}{4}$ para cualquier caso. Cualquier camino seguido tendría la misma probabilidad y el resultado tendría la misma probabilidad de ser $|0\rangle$ ó $|1\rangle$. Pero lo que sucede en realidad es que los dos caminos que terminan en $|0\rangle$ interfieren constructivamente, es decir que sus amplitudes sumadas producen $\frac{1}{2} + \frac{1}{2} = 1$. Por otro lado los dos caminos que terminan en $|1\rangle$ interfieren destructivamente; sus amplitudes sumadas dan $-\frac{1}{2} + \frac{1}{2} = 0$. Lo que obtenemos al final es $|0\rangle$ con certeza, nunca se observa como resultado $|1\rangle$.

Estos simples ejemplos nos dan una idea de los principios básicos detrás del diseño de algoritmos cuánticos. De lo que se trata es de programar a Q de tal forma que las vías que conducen a resultados indeseados interfieran destructivamente, mientras que las que conducen a los resultados que buscamos lo hagan de manera constructiva. Por supuesto que los algoritmos cuánticos no se limitan al caso de trabajar con solo un bit de memoria. Si comenzamos con n bits en estado inicial cero, es decir $|000...0\rangle$, y luego realizamos n aplicaciones sucesivas de un algoritmo similar a QCF, pero aplicado a diferente bit en cada ocasión, dará como resultado la superposición cuántica de todas las diferentes 2^n cadenas de n bits, cada una con amplitud $2^{-n/2}$. De aquí que se pueda realizar una cantidad exponencial de operaciones por el precio de una, pero ello sólo sirve si podemos hacer

que dichos cálculos interfieran de tal forma que se amplifique la probabilidad de observar resultados deseados (más adelante veremos esto más explícitamente). Ello es lo que han estado haciendo los diseñadores de algoritmos cuánticos durante casi dos décadas.

Otra noción fundamental es la distinción entre el uso exponencial y polinomial de recursos en un cómputo. Dicha noción aporta una medida cuantitativa de la distinción esencial entre la Computación Cuántica y la clásica. Consideremos alguna tarea computacional como la siguiente: dado un entero N hay que decir si se trata de un número primo o no. Desearíamos evaluar la cantidad de recursos que se necesitarán para esta tarea como función del tamaño de la entrada, cuya medida se establece con $n = \log_2 N$, que es el número de bits requeridos para almacenar N. Denotamos con $T(n)$ el número de pasos (en una máquina universal de Turing U) que se necesitan para resolver el problema. Lo primero que nos preguntamos es sobre el comportamiento de $T(n)$: desearíamos que pudiera ser acotada por alguna función polinomial en n. Evidentemente, entre menos pasos mejor. En general, consideremos el conjunto de todos los números primos escritos en binario y lo denotamos con $\mathcal{L}$; ahora nuestra tarea computacional consiste en determinar si alguna cadena dada σ de longitud n pertenece a $\mathcal{L}$. Se dice que el conjunto $\mathcal{L}$ es de clase $\mathcal{P}$ (de "tiempo polinomial") si existe un algoritmo que puede realizar dicha tarea, y lo hace en un tiempo $T(n)$ que está acotado por una función polinomial. En otro caso se dice que dicha tarea requiere una cantidad de tiempo exponencial. A los algoritmos que corren en tiempo polinomial se les llama *eficientes*. Los *ineficientes* no nos interesan mucho.

Más en general, es útil considerar algoritmos que incluyen elecciones probabilísticas ("volados") (Ekert y Jozsa 1996). Se dice que el conjunto $\mathcal{L}$ es de clase $\mathcal{PEPA}$ (tiempo polinomial con error probabilístico acotado) si existe un algoritmo que pueda clasificar correctamente la cadena σ en tiempo polinomial con probabilidad al menos de $2/3$. Así, un algoritmo $\mathcal{PEPA}$ puede dar respuestas erróneas, pero iterando el algoritmo y tomando la respuesta más frecuente se puede amplificar la probabilidad de éxito arbitrariamente cerca de 1, mientras todo el proceso se haga en tiempo polinomial. A este tipo de algoritmos se les considera factibles de realizarse en la práctica (Jozsa 1997).

En general el número exacto de pasos de cómputo $T(n)$ dependerá de la elección de la computadora y el modelo computacional adoptado. Sin embargo dentro de los límites de la computación clásica, la distinción entre tiempo exponencial y polinomial parece confiable independientemente de dichas elecciones. En realidad se trata de una distinción *física*. Desde el punto de vista físico resulta natural extender la noción de cómputo eficiente a requerir para dicha categoría el uso eficiente de *todos* los recursos físicos involucrados. Otro importante incentivo (tal vez el más importante) para el desarrollo de la Computación Cuántica es el hecho de que la Mecánica Cuántica parece permitir traspasar los límites que la computación clásica impone a los cómputos de tiempo polinomial y los de tiempo exponencial.

Existen varios algoritmos para computadoras cuánticas que apoyan firmemente la visión de que dichas computadoras podrían realizar algunas tareas exponencialmente más rápido que sus contrapartes clásicas que hoy usamos. El algoritmo más significativo es el algoritmo para factorización de números enteros en tiempo polinomial de Peter Shor (Shor 1994, Ekert y Josza 1996). Su algoritmo es uno de los ejemplos más espectaculares del empleo de la interferencia y superposición de estados cuánticos, de lo que se habló antes.

Podría parecer que esto de la superposición es lo que hace tan atractiva a la Computación Cuántica, pero no. Es más bien el *entrelazamiento cuántico* la característica esencial que hace posible las capacidades sobresalientes de las computadoras cuánticas. El entrelazamiento es una propiedad de sistemas que constan al menos de dos partes A y B, separadas lo suficiente como para impedir cualquier interacción entre ellas, pero que en algún momento anterior interactuaron de alguna forma y por ello mantienen una cierta correlación aunque estén separados. A estos sistemas de dos partes también se les conoce como pares EPR, que estudiamos en el capítulo anterior. Las correlaciones que exhiben dichos sistemas hacen que se violen las desigualdades de Bell cuando se realizan conteos de coincidencia de detecciones de los observables que se elija medir.

El entrelazamiento cuántico es un tipo especial de superposición: superposición en presencia de un producto de estructuras en el espacio de estado, que surge del sistema, que a su vez está compuesto de varios subsistemas. El estado de dicho sistema entrelazado de

al menos dos partes, se encuentra en un espacio de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, es decir, el espacio *producto tensorial* de los respectivos espacios de Hilbert de las partes constitutivas del sistema. Existen estados puros entrelazados y estados mezclados entrelazados, pero por simplicidad sólo me referiré a estados entrelazados puros. Se dice que un estado puro está entrelazado o es no local si y sólo si su vector de estado $|\psi\rangle$ *no puede ser expresado como el producto* $|\psi_A\rangle|\psi_B\rangle$ de los estados puros de sus partes. Los estados entrelazados no pueden prepararse a partir de estados no entrelazados con ninguna secuencia de acciones locales de Ana y Beto, incluso usando comunicación clásica (Bennett *et al.* 1996).

Para ver que la superposición no es en sí misma la característica esencial que permite las proezas de que son capaces las computadoras cuánticas (si existieran) notemos que las ondas clásicas también exhiben dicha característica. Cualquier efecto que dependa sólo de la interferencia cuántica puede ser imitado prácticamente a la perfección por ondas clásicas. Sin embargo, las ondas clásicas y los estados cuánticos son bastante diferentes, lo que hace que no exista ningún análogo clásico del fenómeno de entrelazamiento. Para ver esto, consideremos algunos ejemplos.

Sea $B = \{0, 1\}$ y considere cualquier función no trivial $f : B^n \dashrightarrow B$. Suponga que tenemos una computadora cuántica (marca ACME) lista para realizar el cómputo de f en tiempo polinomial. La entrada de la computadora consta de n qubits, su salida sólo de uno y su operación corresponde a una transformación unitaria $\mathcal{U}_f$ sobre $n+1$ qubits que realiza la evolución:

$$\mathcal{U}_f : |i_1\rangle|i_2\rangle...|i_n\rangle|0\rangle \longrightarrow |i_1\rangle|i_2\rangle...|i_n\rangle|f(i_1,...i_n)\rangle \tag{3.86}$$

donde cada i_k es 1 ó 0. El registro de salida está inicialmente en estado $|0\rangle$ y al final del cómputo contiene el estado base correspondiente al valor de la función. Consideremos de nuevo el algoritmo QCF sobre un qubit, o puerta lógica V_8 que habíamos definido antes en (3.79 y 3.84) y regresemos al caso que antes le mencioné con todos los n qubits de la entrada en estado inicial $|0\rangle$ y luego les aplicamos V_8 a cada uno de forma sucesiva, obtenemos la superposición de los 2^n valores en B^n:

$$\mathsf{V}_8 \otimes ... \otimes \mathsf{V}_8|0\rangle...|0\rangle = \frac{1}{2^{n/2}}\left(|0\rangle + |1\rangle\right)^n = \frac{1}{2^{n/2}}\sum_{i=0}^{2^n-1}|i\rangle \tag{3.87}$$

(donde hemos identificado la cadena $i_1, ..., i_n$ con el número binario $i_1...i_n < 2^n$). Note que este estado está preparado en tiempo polinomial (de hecho en tiempo lineal). Si hacemos trabajar a la computadora con (3.87) como entrada obtenemos el estado final

$$|f\rangle = \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle. \tag{3.88}$$

Gracias al paralelismo cuántico hemos computado una cantidad exponencial de valores de f en superposición, con sólo un esfuerzo polinomial.

Ahora cabe la pregunta y quizás usted ya se la hizo: ¿podría imitarse el resultado anterior con ondas clásicas? Podríamos representar cada qubit con un sistema de ondas clásicas seleccionando dos modos de vibración para representar los estados $|0\rangle$ y $|1\rangle$, que podrían ser por ejemplo los dos modos normales de vibración más bajos en una cuerda tensa con extremos fijos. La superposición correspondiente a $|0\rangle + |1\rangle$ se construye inmediatamente y si lo subdividimos en n segmentos de la cuerda obtenemos el estado representado por (3.87), que es un producto de estados. Sin embargo, a pesar de lo mucho que puedan interactuar los segmentos de cuerda entre sí en su subsecuente evolución vibracional (provocada externamente), su estado conjunto siempre podrá expresarse como un *producto* de n estados vibracionales. El espacio de estado de todo el sistema (clásico) es el *producto cartesiano* de los espacios de estado individuales de cada segmento, mientras que en el caso de la Mecánica Cuántica dicho espacio de estado global es el *producto tensorial* de los espacios de estado de los subsistemas. Esta crucial distinción entre el producto cartesiano y el producto tensorial es precisamente el fenómeno del entrelazamiento cuántico (Brassard 1994). El estado (3.88) generalmente se encuentra entrelazado (si f es no trivial), por lo que la transición entre (3.87) y (3.88) no puede lograrse en un escenario clásico.

Pero todavía nos podemos poner necios en tratar de representar el entrelazamiento usando ondas clásicas. El estado de n qubits es un espacio de 2^n dimensiones y puede ser visto isomórficamente como el espacio de estado de una sola partícula con 2^n niveles; entonces podríamos simplemente interpretar ciertos estados de esta partícula como "entrelazados" usando su correspondencia bajo un algún isomorfismo entre $\otimes^n \mathcal{H}_2$ y $\mathcal{H}_{2^n}$ (donde

$\mathcal{H}_k$ denota un espacio de Hilbert de dimensión k). De esta manera se pueden usar 2^n modos de un sistema clásico oscilatorio para imitar de manera general el entrelazamiento cuántico de n qubits, aparentemente. Sin embargo la implementación física de esta correspondencia involucra siempre un incremento exponencial en algún recurso físico del sistema; por ello el isomorfismo *no es* una correspondencia válida para consideraciones de complejidad. Suponga por ejemplo que los 2^n niveles de un sistema cuántico de una sola partícula son niveles de energía equitativamente espaciados entre sí; un estado general de n qubits requiere una cantidad de energía que crece *linealmente* con n, mientras que un estado general de dicho sistema requiere de 2^n niveles (y por lo tanto el correspondiente sistema clásico de ondas) requiere una cantidad de energía que crece *exponencialmente* con n. Para realizar físicamente dicho sistema y simular el entrelazamiento cuántico de manera clásica, necesitamos una cantidad de recursos exponencial. Eso no pasa en los sistemas cuánticos gracias a la existencia precisamente del entrelazamiento cuántico (Jozsa 1997).

Tal vez recuerde del capítulo la representación unitaria (ver página 16). Nótese que n bits clásicos se pueden acomodar de 2^n maneras diferentes pero que sólo puede estar presente una *sola* manera en cualquier momento, aunque esté probabilísticamente determinada. En contraste, n qubits también pueden acomodarse en 2^n diferentes maneras y todas ellas están presentes en el sistema simultáneamente en forma superpuesta.

Existen sistemas físicos con una cantidad infinita de niveles discretos de energía acumulados por debajo de cierto límite acotado. Podemos usar dichos niveles para representar las superposiciones generales de una cantidad exponencial de modos, siempre al mismo costo de energía y darle la vuelta a las objeciones anteriores. Sin embargo en este caso los niveles se acercarán exponencialmente entre sí y vamos a requerir instrumentos con precisión exponencialmente fina y de nuevo requeriremos esfuerzos exponenciales para ello (Jozsa 1997). No hay vuelta de hoja. La realidad del entrelazamiento cuántico presenta posibilidades inimitables clásicamente.

3.5 Aplicaciones del entrelazamiento

Las aplicaciones del entrelazamiento en el campo de la Computación Cuántica no se terminan en el desarrollo de algoritmos factorizadores de números primos. Lo invito a conocer otras aplicaciones.

Suponga que Ana y Beto comparten un par de qubits entrelazados en el estado $|00\rangle + |11\rangle$ (voy a omitir los factores de normalización). Ana y Beto no están realmente comunicados; entre ellos sólo hay un dispositivo que genera pares entrelazados y envía un qubit a cada uno de ellos; ambos van almacenando sus respectivos qubits. En esta situación Ana puede comunicar *dos* bits clásicos a Beto enviando sólo *un* qubit. Hay dos qubits involucrados, pero Ana sólo usa uno. El método se basa en el hecho de que los cuatro estados mutuamente ortogonales $|00\rangle + |11\rangle$, $|00\rangle - |11\rangle$, $|01\rangle + |10\rangle$ y $|01\rangle - |10\rangle$ se pueden generar entre sí usando operaciones sobre un solo qubit. A este conjunto de estados se le conoce como *base de Bell*, ya que exhibe las correlaciones Bell–EPR más fuertes. Comenzando con $|00\rangle + |11\rangle$, Ana puede generar cualquiera de los estados de la base de Bell actuando sobre su qubit con alguno de los operadores lógicos elementales V. Como hay cuatro posibilidades, la elección de su operador representa dos bits de información clásica. Luego le manda su qubit a Beto que debe deducir en qué estado de la base de Bell está el qubit que le mandan; ahora Beto tiene los dos qubits. Para obtener dicha información aplica la puerta (u operador) XOR a cada qubit, luego mide uno de ellos distinguiendo entre $|00\rangle \pm |11\rangle$ o $|01\rangle \pm |10\rangle$. Para encontrar el signo de la superposición utiliza el operador $H \equiv \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]$ sobre el qubit que le sobró y luego lo mide. Sin ambages, Beto ha obtenido dos bits clásicos de información. A este método de mandar información se le llama "*codificación densa*" y se debe a Stephen Wiesner (Bennett y Wiesner 1992).

La codificación densa es difícil de implementar y no es muy práctica como un método de comunicación estándar. Su atractivo radica en que permite comunicarse *de manera segura*, ya que el qubit enviado por Ana sólo le sirve a quien tenga el otro qubit entrelazado, nadie más puede obtener los dos bits clásicos de información que su qubit lleva. El entre-

lazamiento cuántico es un recurso informático que subraya la relación entre la información clásica, los qubits y el contenido de información de estos.

Otra aplicación interesante del entrelazamiento cuántico es la existencia y construcción de códigos de corrección cuántica, introducidos por Peter Shor (1995) por primera vez. El entrelazamiento permite localizar información cuántica en un sistema compuesto de varios subsistemas. Por ejemplo si $|0\rangle$ y $|1\rangle$ son estados ortogonales entonces los estados entrelazados $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ y $\frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$ son idénticos en términos de información cuántica local (estando cada subsistema en su estado máximamente mezclado en cada caso), mientras que son diferentes en términos de su contenido global de información cuántica. Gracias a una ingeniosa extensión de esta idea (Shor 1995) se puede codificar un estado desconocido de un qubit en un estado entrelazado de varios qubits de tal forma que si cualquier estado desconocido de los subsistemas es contaminado arbitrariamente, el estado original puede reconstruirse perfectamente; esto quiere decir que nada de la información del estado original reside localmente en la codificación. De esta forma un estado puede protegerse de los efectos de las interacciones ambientales espurias, si es que dichas interacciones actúan de manera local (que más o menos siempre es así).

El entrelazamiento cuántico también puede jugar el papel de "canal" de transmisión para información cuántica: un estado cuántico desconocido de un qubit puede ser transferido intacto desde un lugar a otro enviando simplemente dos bits clásicos, si en cada uno de estos lugares hay dos partículas entrelazadas. A este proceso se le llama *Teletransportación Cuántica*, y es el tema del siguiente capítulo.

3.6 Criptografía Cuántica

Antes de pasar de lleno a la teletransportación cuántica abordaré someramente el punto que ha financiado a la Computación Cuántica por todos estos años: la *Criptografía Cuántica*. Todo comenzó con un artículo que Stephen Wiesner escribió por ahí de 1970, que publicó hasta 1983 (Wiesner 1983), que contenía varias ideas que involucraban las propiedades de los sistemas cuánticos para cifrar información. posteriormente hubieron contribuciones

más formales a la fueron realizadas por Bennett *et al.* (1982), Bennett y Brassard (1984). La criptografía tiene la característica de que no se puede demostrar experimentalmente si cierto método es seguro o no; todos los años se invierten muchos recursos en diseñar ataques a los sistemas de cifrado actuales, así como en desarrollar defensas contra ellos y en nuevos métodos de cifrado. La confianza en dichos métodos se basa en demostraciones matemáticas; de hecho la criptografía se considera como una rama de las matemáticas. La mayoría de los trabajos publicados sobre Computación Cuántica precisamente tratan de este tema y resumirlos todos es una tarea titánica, así que no me adentraré mucho en él.

El problema en general se puede dividir en dos: la distribución de llaves cuánticas y la contención de bits. La contención de bits se refiere al escenario en el que Ana tiene que hacer alguna decisión, como una especie de voto secreto, de tal forma que Beto puede estar seguro de que Ana ha emitido su voto en un cierto periodo de tiempo, pero no puede saber cual es hasta que ella quiera. Un método clásico que resulta engorroso para la contención de bits es que Ana escriba su voto y lo ponga en una caja fuerte y se la dé a Beto. Cuando ella quiera que Beto sepa el contenido de información, entonces le da la llave de la caja. El protocolo cuántico típico consiste en que Ana le dé a Beto un qubit preparado en cierta base, lo observe y luego le diga a Beto cuál es esa base. El método de contención de bits, que se pensó por mucho tiempo que era seguro, hace unos años se demostró que no lo era (Mayers 1997, Lo y Chau 1997) debido a que los interlocutores pueden hacer trampa por medio del entrelazamiento cuántico.

Por otro lado está la distribución de llaves cuántica, que es un método en el que los estados cuánticos son utilizados para establecer una llave secreta aleatoria que sirve para cifrar información. Supongamos que Ana y Beto están bien lejos el uno del otro, y por supuesto quieren comunicarse. Ana le manda a Beto $2n$ qubits cada uno preparado en alguno de los estados $|0\rangle$, $|1\rangle$, $|+\rangle$ ó $|-\rangle$ elegidos al azar (hay varios métodos, yo presento este por ser el que me pareció más sencillo, además de ser más o menos general). Beto recibe sus qubits y los observe eligiendo aleatoriamente alguna base de medición que puede ser $\{|+\rangle, |-\rangle\}$ o $\{|0\rangle, |1\rangle\}$. En seguida Ana y Beto se comunican públicamente (es decir que cualquiera puede saber lo que se dicen) qué base usaron para preparar o medir cada

qubit. Así pueden saber en qué ocasiones usaron la misma base, que debe ser la mitad de las veces, y sólo se quedan con dichos resultados. En ausencia de errores o interferencia, ahora comparten la misma cadena aleatoria de n bits clásicos (coinciden por ejemplo en asociar $|0\rangle$ y $|+\rangle$ con 0, y $|1\rangle$ y $|-\rangle$ con 1). A esta cadena clásica de bits frecuentemente se le llama *línea de transmisión cuántica* (LTC).

Hasta aquí no hemos ganado nada usando qubits. Una característica que debe resaltarse —y que es lo relevante del procedimiento descrito— es que es imposible determinar los resultados de las mediciones practicadas por Beto para cualquiera que observe los qubits viajando sin dejar evidencia de su presencia. Lo primero que podría intentar un espía para descubrir la llave sería interceptar los qubits, medirlos y luego pasárselos a Beto. También en promedio el espía coincide la mitad de las veces con la base que usó Ana para preparar los qubits; a dichos qubits las mediciones del espía no los perturba, pero a los demás sí. Así que los valores que el espía adivinó no coinciden con los de Beto, por lo que el espía al final sólo sabe la mitad de los n qubits en que Ana y Beto después deciden confiar, y perturba la otra mitad, por ejemplo cambiando $|+\rangle$ por $|0\rangle$. La mitad de los qubits perturbados se ponen en su estado original enviado por Ana debido a las mediciones practicadas por Beto; en total el espía perturba $n/4$ bits de la LTC.

Ana y Beto pueden detectar la presencia del espía simplemente eligiendo al azar $n/2$ bits de la LTC y comunicándose públicamente los valores que tienen. Si concuerdan todos los contenidos, no hay problema, pueden afirmar que no hay espías interceptando sus mensajes, ya que la probabilidad de que ello ocurra es de $(3/4)^{n/2} \simeq 10^{-125}$ para $n = 1000$ (Steane 1997).

Ya en la práctica el protocolo se vuelve más complejo, ya que los espías pueden usar otras estrategias (por ejemplo podrían no interceptar todos los qubits); además si Ana y Beto usan un canal ruidoso —como normalmente pasaría— se podrían alterar algunos de los qubits sin que sea causa de algún espía. En esta situación más cercana a la realidad, el protocolo de comunicación segura es como sigue: Ana y Beto confiarán en su llave siempre y cuando el porcentaje de los bits que no coinciden esté por debajo del 25%. En seguida procesan su llave en dos fases; primero detectan y eliminan los errores comparando

públicamente la paridad de mediciones practicadas sobre subconjuntos aleatorios de bits elegidos públicamente, descartando los que no concuerden, para evitar dar más información a los espías. El segundo paso es disminuir la información que podrían tener los espías sobre la llave, destilando información para crear una llave más pequeña, compuesta por los valores de la paridad calculados a partir de la llave original. De esta manera se puede obtener una llave de alrededor de $n/4$ bits, de la cual los espías probablemente saben menos de la 10^{-6} parte de un bit (Bennett et al. 1992). Este protocolo que describí no es el único posible. A. Ekert (1991) propuso otro protocolo que involucra pares EPR, que Ana y Beto miden a lo largo de alguno de tres ejes coordenados. Para evitar ser espiados verifican las correlaciones EPR en sus resultados.

Hasta la fecha, la distribución de llaves cuánticas se ha considerado segura. Eli Biham y Tal Mor (1996) mostraron que el sistema de distribución de llaves cuánticas resulta muy confiable ante los ataques más duros que utilizan memorias cuánticas y compuertas cuánticas contra la llave final; para ello calcularon las matrices de densidad reducidas dependientes de la información, estudiaron la geometría del estado cuántico mezclaron y obtuvieron los límites de la información que podría obtener un espía. Sus resultados sugieren que la criptografía cuántica basada en esta técnica es absolutamente segura.

La cuestión importante de la distribución de llaves cuánticas es que *es posible con la tecnología actual.* Los primeros que obtuvieron resultados experimentales al respecto fueron Bennett y Brassard (1989) y de hecho demostraron el principio. Las cosas evolucionaron y para 1997 Zbinden *et. al.* publicaron excelentes resultados de distribución de llaves cuánticas a través de 23 km de fibra de telecomunicaciones común. Parece que el futuro no queda tan lejos ¿no le parece?

CAPITULO 4
La Teletransportación Cuántica

Tal vez el título de este trabajo le pareció casi esotérico; seguramente le recordó la famosísima serie de televisión "Star Trek" (conocida en México como "Viaje a las estrellas") que forjó a varias generaciones, no sólo de estadounidenses, sino también de mexicanos (bueno, al menos los que tenían televisión). Cómo no acordarse del intrépido Capitán Kirk que, justo después de haber resuelto con patadas de karate algún conflicto milenario entre dos o más especies habitantes de un remoto planeta en una remota galaxia, volvía a su legendaria nave, el "Enterprise" —para reflexionar al respecto, dar su moraleja edificante para los jóvenes terrícolas e ir tras la siguiente aventura— solicitando ser *teletransportado* (simplemente tocando su hombro izquierdo con su mano derecha) desde donde estuviera. Tal vez en eso pensaban Charles Bennet, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres y William K. Wooters (Bennett 1993) cuando bautizaron como "*Teleportation*" (*Teletransportación*) al fenómeno que reportaron en 1993.

4.1 Descripción del fenómeno

La idea básica de la teletransportación consiste en que un objeto en el lugar A al tiempo t se "desmaterializa" y luego reaparece en un lugar distante B al tiempo $t+T$. En el caso de la teletransportación cuántica implica que queremos hacer lo mismo con un objeto cuántico. Lo que en realidad sucede es que se teletransporta el *estado cuántico* de dicho objeto de la partícula en A a la partícula en B. Sin embargo, existe un hecho clave que nos permite hablar realmente de teletransportación: las partículas elementales que pueblan el universo son *indistinguibles entre sí* (es decir un electrón en el estado tal en un átomo de hidrógeno es indistinguible —excepto por la posición espacial— de otro electrón en el mismo estado cuántico de otro átomo de hidrógeno, por ejemplo). Lo que define que usted sea usted (y que piense lo que justamente está pensando en este momento) es el estado cuántico de *todas* las partículas elementales de los átomos que lo integran; si pudiéramos transmitir toda

esa información a otro conjunto igual de átomos en algún otro lugar, entonces usted sería efectivamente teletransportado, ya que en el proceso tendríamos que destruir su original para conocer el estado cuántico de las partículas que lo integran (más adelante abordaré de nuevo la "teletransportación humana").

En todas las representaciones de la teletransportación en la Ciencia ficción (además de Star Trek, otra popular representación es The Fly) la cosa sucede así: primero obtenemos *todas* las propiedades del objeto que se desea teletransportar —destruyéndolo en el proceso—, luego se manda la información obtenida en forma de información clásica, al sitio de destino, donde finalmente se recrea otro objeto con *exactamente* las mismas propiedades. Para comenzar, este procedimiento se toparía con el principio de incertidumbre que efectivamente impediría saber realmente *todas* las propiedades del objeto en un momento determinado. Y hay más violaciones a las leyes de la Física, además de los problemas técnicos que implicaría, pero mejor concentrémonos en el asunto de la teletransportación real.

Como antes vimos, la misteriosa (y maravillosa) propiedad de los sistemas cuánticos derivada del principio de superposición, que implica que un sistema cuántico puede estar en una superposición de varios estados al mismo tiempo, permite la existencia de los famosos estados entrelazados, que abordamos en el capítulo anterior. Una medición sobre dicho sistema cuántico lo proyecta hacia uno solo de esos estados; a esto se le conoce como el *postulado de proyección.* También como antes vimos, dichos estados entrelazados permiten la existencia de un canal cuántico que permite llevar a cabo un protocolo para teletransportar sistemas cuánticos, sin necesidad de conocer completamente el estado del mismo.

Para comenzar el protocolo de la teletransportación, primero que nada contamos con nuestros ya legendarios Ana y Beto, que se encuentran bien lejos uno del otro. También necesitamos una fuente emisora de pares de partículas de dos niveles (qubits, que además —para comenzar— siempre serán partículas con espín $\frac{1}{2}$) con entrelazamiento máximo, que podemos tratar como qubits máximamente entrelazados. El estado del sistema integrado

por este par de partículas podría ser por ejemplo

$$|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle\right) \tag{4.89}$$

donde los kets con subíndice A son del qubit de Ana, y los otros del qubit de Beto. Como sabemos, este es un estado entrelazado, por tanto no puede ser expresado como un producto de sus estados individuales, y es diferente de una mezcla estadística —por ejemplo

$$\frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right), \tag{4.90}$$

que es el estado más correlacionado para este sistema, permitido por la Física Clásica—.

Cada quien con su qubit en la mano, ahora resulta que a Ana le cae otro qubit en un estado desconocido para ella, y es el que precisamente ella quiere hacerle llegar a Beto. Denotaré el estado desconocido de este qubit con

$$|\chi\rangle = a|0\rangle + b|1\rangle \tag{4.91}$$

donde a, b son números complejos arbitrarios. Si este estado no fuera desconocido para Ana, la teletransportación sería trivial, ya que si ella conociera $|\chi\rangle$ bastaría con que le llamara por teléfono a Beto y se lo describiera para que él pudiera recrearlo y completar así la teletransportación. Pero como ella no lo conoce, no puede medirlo para obtener toda la información necesaria para especificarlo; acaso puede conocer parte de dicha información, pero no es suficiente para recrearlo en algún lugar remoto. La alternativa que le queda es utilizar las propiedades del estado cuántico del primer qubit que tenía y que se encuentra entrelazado con el que tiene Beto. El estado global de los tres qubits será

$$|\Phi_{AB}\rangle = |\chi\rangle|\Psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(a|0\rangle + b|1\rangle\right)\left(|00\rangle + |11\rangle\right). \tag{4.92}$$

Para fines prácticos, este estado puede escribirse como

$$\begin{aligned} |\Phi_{AB}\rangle &= \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right) \\ &= \frac{1}{2}[|\Phi^+\rangle\left(a|0\rangle + b|1\rangle\right) + |\Phi^-\rangle\left(a|0\rangle - b|1\rangle\right) + \\ &\quad |\Psi^+\rangle\left(a|1\rangle + b|0\rangle\right) + |\Psi^-\rangle\left(a|1\rangle - b|0\rangle\right)] \end{aligned} \tag{4.93}$$

donde

$$
\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)
\end{aligned}
\tag{4.94}
$$

y forman una base ortonormal de los dos qubits de Ana; ya conocíamos desde el capítulo anterior a este conjunto de vectores de estado, que comúnmente se conoce como *base de Bell*. Lo único que pasó aquí es que estamos escribiendo la expresión (4.92) en una base diferente, no hay ningún proceso físico de por medio. La ventaja de esta forma es que muestra más claramente el alto grado de correlación entre los qubits de Ana y los de Beto (que de hecho se encuentran cuánticamente entrelazados), ya que a cada estado de los qubits de Ana le corresponde un estado del qubit de Beto. Ahora sí podemos definir el protocolo de teletransportación (Plenio y Vedral 1998):

"1) Inicialmente, Ana y Beto comparten un par de qubits entrelazados. Cuando Ana recibe el qubit a teletransportar en el estado desconocido $|\chi\rangle$, le practica mediciones proyectivas en la base de Bell sobre sus dos qubits. Esto significa que obtendrá al azar uno de los cuatro estados de Bell, con igual probabilidad.

2) Suponga que Ana obtiene el estado $|\Psi^+\rangle$. Ahora el estado conjunto de los tres qubits (los dos de Ana y uno de Beto) es

$$|\Phi_{AB}\rangle = |\Psi^+\rangle\left(a|1\rangle + b|0\rangle\right) \tag{4.95}$$

Ahora Ana le comunica a Beto el resultado de sus mediciones (por teléfono, por ejemplo). Este mensaje tiene como finalidad informarle a Beto en qué se diferencia el estado de su qubit con el que Ana tenía antes.

3) Ahora Beto sabe exactamente qué hacer para completar la teletransportación. Tiene que aplicarle una transformación unitaria a su qubit, que en este caso debe ser la operación NOT, con lo que el estado de su qubit será $a|0\rangle + b|1\rangle$, que es precisamente el estado $|\chi\rangle$ que Ana quería teletransportar hacia donde él estaba. Esto completa el protocolo. Si $|0\rangle$ y $|1\rangle$ están escritos en su forma vectorial, entonces el operador que Beto tiene que aplicar a su qubit es alguna de las matrices de Pauli."

Es importante notar que todas las operaciones que realizan Ana y Beto son de *naturaleza local*. Esto significa que nunca se realizó —ni se necesita realizar— una transfor-

mación o medición sobre los tres qubits al mismo tiempo, que es lo que precisamente nos permite decir que este protocolo aquí descrito es auténticamente una teletransportación. Note también que las operaciones que Beto realiza son independientes del estado que Ana trata de teletransportarle, y que la comunicación clásica entre ellos en el paso dos es imprescindible (¿como sabría Beto qué hacer con su qubit para obtener $|\chi\rangle$ si ésta no sucediera?). En realidad, la necesidad de dicha comunicación clásica tiene orígenes más serios y profundos: si no fuera necesaria para hacer la teletransportada Ana podría mandar información más rápido que la velocidad de la luz, ya que Beto sabría qué hacerle a su qubit para obtener $|\chi\rangle$ justo después de que Ana le practicó su medición.

¿Y qué pasó con los qubits que Ana tenía antes de iniciar el protocolo? Todavía los tiene, pero su estado inicial ha sido destruido; ahora es un par de qubits en un estado máximamente mezclado de la forma $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. No podría quedarse con el mismo estado que al principio, ya que eso violaría el teorema de No Clonación que enuncié en la página 75. Por supuesto también el estado $|\Psi_{AB}\rangle$ es completamente destruido, lo que implica que ya no hay ninguna correlación entre las partículas de Ana y la de Beto, ya no hay estados entrelazados. Para poder enviar otro estado desconocido a Beto es necesario que de nuevo compartan un par de partículas entrelazadas. Para verlo gráficamente incluí la figura (4.5), que es una esquematización del proceso.

4.2 El papel del entrelazamiento

El entrelazamiento cuántico, es simplemente indispensable para lograr la teletransportación. Por ejemplo, si tomamos dos qubits no entrelazados, cuyo estado sea $|\Psi_{AB}\rangle = |00\rangle$. Como antes se quiere teletransportar el estado $|\chi\rangle$, definido por la expresión (4.91) En este caso el estado global de los tres qubits podría ser

$$|\Upsilon_{AB}\rangle = (a|0\rangle + b|1\rangle)\,|00\rangle \tag{4.96}$$

Ahora aplicamos el protocolo de la teletransportación a este estado: primero Ana practica mediciones proyectivas en la base de Bell sobre sus dos qubits, pero en este caso no obten-

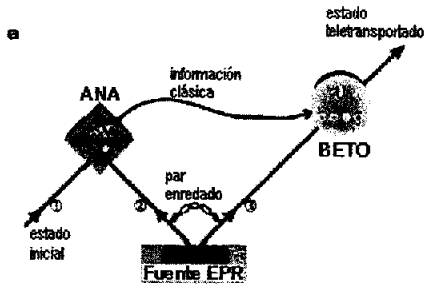


Fig. 4.5. Ana tiene un sistema cuántico, la partícula 1, en un estado inicial que quiere teletransportar a Beto. Ana y Beto también comparten un par de partículas enredadas 2 y 3, emitidas por una fuente EPR. Ana le practica a las partículas que posee (1 y 2) una medición conjunta (BSM), que las proyecta hacia uno de los estados de Bell. Luego le manda la información clásica que obtuvo con su medición a Beto, por medio de un canal convencional, quien ahora sabe qué transformación unitaria (U) debe practicarle a su partícula (3) para obtener exactamente el mismo estado que tenía la partícula original 1 (Tomado de Bouwmeester 1997).

drá ninguno de los estados de Bell. No importa lo que Ana le haga a sus dos qubits, el qubit de Beto siempre se quedará en estado $|0\rangle$, lo que no es más que la expresión de que no existe ninguna correlación entre este y los qubits de Ana, así que el protocolo se trunca en este paso y no puede haber teletransportación. Formalmente hablando, se dice que los qubits A y B son estadísticamente independientes. Esta forma de decirlo podría llevarnos a intentar algo más para lograr la teletransportación sin entrelazamiento de por medio. Considere la mezcla estadística de los estados $|00\rangle$ y $|11\rangle$ que no se encuentran entrelazados:

$$\rho_{AB} = \frac{1}{2}\left(|00\rangle\langle 00| + |11\rangle\langle 11|\right) \tag{4.97}$$

Esto equivale a que Ana y Beto compartan ya sea $|00\rangle$ o $|11\rangle$, pero sin que sepan cada quien cuál tiene. Este estado está claramente correlacionado, ya que podemos saber qué estado tiene cualquiera de los dos si sabemos qué estado tiene uno de ellos. Pero como ambos estados están desentrelazados, no se puede llevar a cabo la teletransportación y por tanto con la mezcla de dichos estados tampoco. Ana le puede practicar las mediciones que quiera a sus qubits y Beto le puede aplicar las transformaciones unitarias que quiera al suyo

pero de todos modos no habrá teletransportación (Popescu 1994). De hecho se sigue que si $\{|\alpha_A^i\rangle\}$ es un conjunto de estados del qubit de Ana, y $\{|\beta_B^i\rangle\}$ es otro conjunto de estados del qubit de Beto, entonces el estado más general desde el cual no se puede llevar a cabo la teletransportación es de la forma

$$\sigma_{AB} = \sum_{ij} p_{ij} |\alpha_A^i\rangle\langle\alpha_A^i| \otimes |\beta_B^i\rangle\langle\beta_B^i| \tag{4.98}$$

donde p_{ij} son un conjunto de probabilidades tales que $\sum_{ij} p_{ij} = 1$. Se trata de la forma general de una mezcla estadística, el estado más general de dos qubits que no están entrelazados. Puede que haya varias correlaciones clásicas entre ellos, pero ninguna cuántica. Tanto las correlaciones clásicas como cuánticas son propiedades globales de dos sistemas cuánticos correlacionados, pero sólo se puede llevar a cabo la teletransportación en presencia de entrelazamiento cuántico.

Este hecho se ha postulado como uno de los teoremas centrales de la Informática Cuántica (Plenio y Vedral 1998):

Teorema de Entrelazamiento. *Ana y Beto no pueden, convertir un estado σ_{AB} no entrelazado en uno entrelazado mediante operaciones locales y comunicación clásica.*

Para probar este teorema tomemos por hipótesis que Ana y Beto pueden construir un estado entrelazado a partir de uno no entrelazado σ_{AB} utilizando únicamente operaciones locales y comunicación clásica; en este caso ellos podrían utilizar este estado para realizar la teletransportación, ello implicaría que estados no entrelazados como el de la expresión (4.96) podrían ser usados para llevar a cabo la teletransportación, lo que como mostré en la página 95, no es posible (Popescu 1994).

4.3 Medida del entrelazamiento

Tal vez no se dio cuenta, pero desde hace rato he hablado de estados "máximamente" entrelazados. Ello implica que deben haber estados "menos entrelazados" ¿no le parece? ¿y cómo sabemos si un estado está más entrelazado que otro? Afortunadamente el entrelaza-

miento cuántico no es como el amor: sí se puede medir. Trataré de explicarle esta cuestión de la medida del entrelazamiento. Considere el estado cuántico total de n pares de partículas entrelazadas, dado por

$$\begin{aligned} |\Psi_{AB}^{\otimes n}\rangle &= (a|00\rangle + b|11\rangle) \otimes (a|00\rangle + b|11\rangle) \otimes ... \otimes (a|00\rangle + b|11\rangle) \\ &= a^n|0000...00\rangle + a^{(n-1)}b\,(|0000...11\rangle + ...|1100...00\rangle) + ... \\ &\quad + b^n|1111...11\rangle. \end{aligned} \tag{4.99}$$

Por convención, en el segundo y tercer renglón de esta expresión los dígitos en posiciones impares en los kets largos (de n lugares), representan los estados que pertenecen a Ana y los demás a Beto. Ana puede llevar a cabo proyecciones sobre sus qubits (a nivel local, por supuesto) hacia subespacios sin estados $|1\rangle$, dos estados $|1\rangle$, diez estados $|1\rangle$, etc., y comunicar sus resultados a Beto. La probabilidad de obtener una proyección exitosa hacia un subespacio particular con $2k$ estados $|1\rangle$ se puede deducir de la expresión (4.99, Bennett 1996) y es

$$p_{2k} = a^{2(n-k)}b^{2k}\binom{n}{k} \tag{4.100}$$

Se puede mostrar que esta probabilidad se puede aproximar a $\ln\binom{n}{k}$ (Bennett 1996). Si suponemos que la unidad de entrelazamiento está dada por el entrelazamiento del estado sencillo (o singulete), se define el entrelazamiento total esperado como

$$E = \sum_{k=0}^{n} a^{2(n-k)}b^{2k}\binom{n}{k}\ln\binom{n}{k}. \tag{4.101}$$

Nos interesa el comportamiento asintótico de esta expresión cuando $n \to \infty$. Se puede ver que tomando el término más significativo obtenemos

$$E \sim (a^2)^{na^2}(b^2)^{nb^2}\binom{n}{nb^2}\ln\binom{n}{nb^2} \tag{4.102}$$

que, usando la aproximación de Stirling, se puede reducir a

$$\begin{aligned} E &\sim \exp\left(-nS_{vN}(\rho_A)\right)\exp\left(n\ln n - a^2 n\ln a^2 n - b^2 n\ln b^2 n\right) \\ &\quad \left(n\ln n - a^2 n\ln a^2 n - b^2\right) \\ &= \exp\left(-nS_{vN}(\rho_A)\right)\exp\left(nS_{vN}(\rho_A)\right)nS_{vN}(\rho_A) \\ &= nS_{vN}(\rho_A) \end{aligned} \tag{4.103}$$

donde S_{vN} es la entropía reducida de von Neumann, que se define como sigue (Vedral 1997):

Dado un estado puro ρ_{AB} de dos subsistemas A y B, se definen los estados $\rho_A \equiv \mathrm{tr}_B\{\rho_{AB}\}$ y $\rho_B \equiv \mathrm{tr}_A\{\rho_{AB}\}$, donde la la traza parcial se ha tomado sobre un subsistema, ya sea A o B. Entonces la entropía reducida o de los operadores de densidad reducidos está dada por:

$$S(\rho_A) := -\mathrm{tr}(\rho_A \ln \rho_A) = -\mathrm{tr}(\rho_B \ln \rho_B) \tag{4.104}$$

La expresión (4.103) es la más usual para la medida del entrelazamiento total de un sistema. Antes de pasar a otras cosas me parece importante mencionar algunas propiedades básicas de la cantidad del entrelazamiento.

Cualquier estado de la forma de la expresión (4.98) —un estado separable— no tiene correlaciones cuánticas, por lo que es un estado no entrelazado; por ello se dice que para cualquier estado separable σ se cumple la relación

$$E(\sigma) = 0. \tag{4.105}$$

Las transformaciones unitarias locales también resultan importantes en el asunto de la teletransportación; estas representan un cambio de la base en la que consideramos algún estado entrelazado. Pero un cambio de base no cambia la cantidad de entrelazamiento accesible a quien practica dichas transformaciones, ya que en cualquier momento simplemente podría revertirse dicho cambio de base. En cualquier caso el entrelazamiento será el mismo, es decir, para cualquier estado σ y cualquier transformación unitaria local de la forma $U_A \otimes U_B$ el entrelazamiento es constante

$$E(\sigma) = E\left(U_A \otimes U_B \sigma U_A^\dagger \otimes U_B^\dagger\right) \tag{4.106}$$

Como antes vimos, Ana y Beto no pueden crear y compartir estados entrelazados con sólo operaciones locales y comunicación clásica. Pero si cuentan con sistemas al menos levemente entrelazados, se puede seleccionar un subconjunto de estados que están más entrelazados, por medio de operaciones locales y comunicación clásica; a este proceso se le llama *purificación de entrelazamiento* y existen varios protocolos para llevarlo a cabo

(Bennett 1996, Plenio y Vedral 1998). Los protocolos más recientes para purificación de entrelazamiento pueden aplicarse en una basta gama de estados puros y mezclados.

Sin embargo lo que no se puede hacer es *incrementar* el nivel de entrelazamiento global del sistema, que está dado por la suma del entrelazamiento individual de cada subsistema, es decir si tenemos un conjunto de sistemas en estado σ y después de varias operaciones locales con comunicación clásica, tenemos varios subconjuntos en estado σ_i con probabilidad p_i para cada sistema de estar en él, se cumple la desigualdad

$$E(\sigma) \geq \sum_i p_i E(\sigma_i) \tag{4.107}$$

Esta condición tiene la importante implicación de que acota la eficiencia de cualquier método de purificación de entrelazamiento. Además se puede fijar un límite inferior que nos diga si tal o cual método de purificación realmente es útil; para ello se define la *fidelidad* $F(\rho)$ del estado ρ como:

$$F(\rho) = máx \quad \langle\psi|\rho|\psi\rangle \tag{4.108}$$

donde la maximización se toma sobre todos los subestados máximamente entrelazados, es decir, sobre todos los estados que uno puede obtener de un estado singulete por medio de operaciones locales unitarias. Este parámetro también resulta la medida fundamental que nos dice si un sistema de teletransportación es exitoso o no.

4.4 Teletransportación clásica

En 1994, Sandu Popescu de la Universidad Libre de Bruselas, hizo notar en un artículo (Popescu 1994) un hecho bastante relevante para el mundo de los teletransportadores. Cuando dos partículas que constituyen el canal cuántico (es decir es un par entrelazado, o par EPR, entre Ana y Beto), el estado desconocido $|\chi\rangle$ puede teletransportarse con fidelidad $F = 1$ (bueno, sin contar el ruido y otros factores inherentes a la realidad que siempre arruinan la perfección humana). Ya en el mismo artículo de Bennett *et al.* (1996) donde se planteó la teletransportación, se hace notar que estados menos entrelazados pueden servir para realizar la teletransportación, aunque con menor fidelidad. Con todo lo que antes le

platiqué, usted pudo haber llegado a la conclusión de que si ambas partículas se encuentran en un estado que se puede expresar como el producto de sus estados individuales (o sea que no están entrelazados) estos no violan ninguna de las desigualdades de Bell y por tanto no pueden emplearse para llevar a cabo la teletransportación. Parece lógico pensar que siempre que dos sistemas espacialmente separados violen alguna de las desigualdades de Bell, estos pueden ser usados para teletransportar y viceversa.

Pero nooo. Popescu mostró que eso no es cierto. Hay situaciones en las que dos sistemas separados espacialmente no violan ninguna de las desigualdades de Bell (ver página 81)pero de todas formas sirven para teletransportar. Es decir que tenemos lo que se ha llamado *teletransportación clásica* (por aquello de que en el mundo clásico no se violan las desigualdades de Bell). La clave son las *mezclas*. Cualquier estado entrelazado puro viola las desigualdades de Bell, pero las mezclas de estados entrelazados no necesariamente. Considere por ejemplo una mezcla del estado singulete $|\Psi^-\rangle$ y del estado triplete $|\Psi^+\rangle$ de la base de Bell de la expresión (4.94). Ambos tienen el mismo peso estadístico, ambos están entrelazados, de hecho máximamente entrelazados, pero esta mezcla es completamente equivalente, desde el punto de vista de las mediciones, a una mezcla de productos directos, $|\psi_1\rangle = |10\rangle$ y $|\psi_2\rangle = |01\rangle$ con iguales pesos. Como $|\psi_1\rangle$ y $|\psi_2\rangle$ son productos directos ninguno de ellos viola las desigualdades de Bell, y por tanto su mezcla tampoco. Esta mezcla no se puede usar para teletransportar, y no viola las desigualdades de Bell.

Pero los productos directos no son los únicos estados puros que no violan las desigualdades de Bell; aunque que se podría pensar que si una mezcla no es equivalente a una mezcla de productos directos debe violar alguna de las desigualdades de Bell. Pero tampoco esto es cierto. Reinhard Werner (1989) mostró que existen mezclas que no son equivalentes a las mezclas de productos directos, y que no violan ninguna desigualdad de Bell. Todas las correlaciones obtenidas con tales mezclas pueden ser obtenidas a partir de un modelo localista de variables ocultas. Analicemos un caso particular de tales mezclas (Popescu 1994). Considere dos partículas con espín $\frac{1}{2}$ descritas por la matriz de densidad

$$W = \frac{1}{8}I + \frac{1}{2}|\Psi^-\rangle\langle\Psi^-| \tag{4.109}$$

donde $|\Psi^-\rangle$ es uno de los estados de la base de Bell (ec. 4.94). Cuando las mediciones de la polarización del espín se realizan por ejemplo en la dirección $\hat{\xi}$ para la primera partícula, y en la dirección $\hat{\eta}$ para la segunda, la probabilidad de obtener el resultado "1,1" es

$$P(S_{\hat{\xi}}^1 = 1, S_{\hat{\eta}}^2 = 1) = \frac{1}{4}\left(1 - \frac{1}{2}\cos\alpha\right) \tag{4.110}$$

donde α es el ángulo entre las direcciones de $\hat{\eta}$ y $\hat{\xi}$. Las mismas probabilidades conjuntas pueden obtenerse del siguiente modelo localista de variables ocultas. Sea la variable local oculta un vector unitario dado por

$$\hat{\lambda} = \sin\theta\cos\phi\hat{\mathbf{i}} + \sin\theta\sin\phi\mathbf{j} + \cos\theta\hat{\mathbf{k}} \tag{4.111}$$

donde $\hat{\mathbf{i}}, \mathbf{j}, \hat{\mathbf{k}}$ forman la base cartesiana rectangular de siempre. Cada par de partículas tiene su propio vector $\hat{\lambda}$, y todos los pares se encuentran distribuidos sobre la esfera unitaria; la función de distribución de la variable oculta $\hat{\lambda}$ está dada por

$$d\rho(\hat{\lambda}) = \frac{1}{4\pi}\sin\theta d\theta d\phi \tag{4.112}$$

Cuando se practican medidas de la polarización sobre cada partícula en un par dado, cada medición da el resultado $|0\rangle$ o $|1\rangle$ de acuerdo con el esquema localista, sin necesidad de que Ana y Beto se comuniquen entre sí. Es decir, la medición sobre la partícula 1 dará como resultado $|1\rangle$ con probabilidad

$$P(S_{\hat{\xi}}^1 = 1, \hat{\lambda}) = \cos^2\left(\frac{\alpha_1}{2}\right) \tag{4.113}$$

donde α_1 es el ángulo entre las direcciones $\hat{\xi}$ y $\hat{\lambda}$. De manera análoga, la probabilidad de que la medición sobre la partícula 2 arroje como resultado $|1\rangle$ es

$$P(S_{\hat{\eta}}^2 = 1, \hat{\lambda}) = \begin{cases} 1 \text{ si } 2\cos^2\left(\frac{\alpha_2}{2}\right) < 1 \\ 0 \text{ si } 2\cos^2\left(\frac{\alpha_2}{2}\right) > 1 \end{cases} \tag{4.114}$$

donde α_2 es el ángulo entre $\hat{\eta}$ y $\hat{\lambda}$. Las probabilidades conjuntas P_c dadas por este modelo clásico son

$$\begin{aligned} P_c\left(S_{\hat{\xi}}^1 = 1, S_{\hat{\eta}}^2 = 1\right) &= \int d\rho(\hat{\lambda}) P(S_{\hat{\xi}}^1 = 1, \hat{\lambda}) P(S_{\hat{\eta}}^2 = 1, \hat{\lambda}) \qquad (4.115) \\ &= \frac{1}{4\pi} \int \cos^2\left(\frac{\alpha_1}{2}\right) (1 \text{ ó } 0) \sin\theta d\theta d\phi \\ &= \frac{1}{4}\left(1 - \frac{1}{2}\cos\alpha\right) \end{aligned}$$

que es exactamente el mismo resultado que obtenemos en el caso cuántico de la expresión (4.110).

Resulta difícil hacerse de un sentido intuitivo de estas mezclas. Por un lado se intuye que no son locales, ya que no pueden obtenerse como mezclas de estados locales (o sea, como productos directos), por otro lado, esta supuesta no localidad no aparece en las correlaciones, es decir que todas las correlaciones generadas por tal mezcla son clásicas. La no separabilidad de estas mezclas se expresa en el hecho de que pueden usarse para la teletransportación.

En efecto, usando partículas en el estado de la expresión (4.109) se puede teletransportar un estado desconocido $|\chi\rangle$, con una fidelidad menor a 100%. Considere la siguiente situación. A Ana le dan una partícula con espín $\frac{1}{2}$ en un estado puro $|\chi\rangle$ desconocido, y a Beto se le pide que prepare otra partícula con espín $\frac{1}{2}$ en un estado puro o mezclado, de tal forma que sea lo más parecido posible a $|\chi\rangle$. En general Beto no podrá reproducir a la perfección el estado $|\chi\rangle$, pero obtendrá algo parecido que denotaré como χ' si se trata de un estado puro o ρ si es mezclado. Definimos la medida del éxito obtenido por Beto como $|\langle\chi|\chi'\rangle|^2$, o equivalentemente como la traza de $\rho|\chi\rangle\langle\chi'|$. Supongamos que este proceso de reproducción de estados se repite muchas veces; cada vez Ana recibe una partícula polarizada en una dirección diferente, con polarización uniformemente distribuida sobre la esfera unitaria. Suponga también que Ana conoce la distribución de direcciones, pero no conoce por supuesto una dirección de polarización en particular. El promedio de los éxitos obtenidos por Beto en los diferentes procesos se puede definir como una medida de la fidelidad de la transmisión (en general la fidelidad se puede definir de varias maneras, según sea el caso).

Si Ana y Beto no se pueden comunicar entre sí, Beto podría tratar de adivinar el estado del qubit de Ana, de acuerdo con algún esquema particular (siempre tiene que preparar una partícula en algún estado); la fidelidad para este caso sería de $\frac{1}{2}$: en este caso Beto está jugando volados. Si existe la posibilidad de que se comuniquen clásicamente y cuánticamente (mediante un par de partículas con espín $\frac{1}{2}$ en estado singulete), se puede llevar a cabo el esquema normal de teletransportación. En este caso la fidelidad es la máxima posible. Si solamente hay entre ellos un canal clásico, la mejor fidelidad que pueden alcanzar es $\frac{2}{3}$ (Popescu 1994). Si Ana y Beto comparten partículas de espín $\frac{1}{2}$en un estado mezclado dado por la expresión (4.109), pueden intentar el protocolo normal de la teletransportación, pero la fidelidad que pueden obtener será de $\frac{3}{4}$, que ya es una mejora sobre el resultado clásico. De hecho la mezcla de la expresión (4.109) se puede visualizar como una mezcla del 50% del estado completamente indeterminado $W = \frac{1}{4}I$, y el 50% del estado puro $|\Psi^-\rangle$. Cuando el estado está completamente indeterminado, el resultado de la teletransportación es completamente aleatorio, por lo que la fidelidad es de $\frac{1}{2}$, como antes vimos, mientras que si el estado es el estado puro la fidelidad es 1, y la teletransportación es perfecta. Por lo tanto el promedio de la fidelidad después de muchos intentos con el par de partículas en estado (4.109) será de $\frac{3}{4}$.

A partir de este modelo de variables ocultas que consideramos podemos concluir que la no localidad revelada por la teletransportación no es equivalente a la no localidad de las correlaciones cuánticas, aunque probablemente son dos aspectos de la misma propiedad física.

4.5 Los primeros experimentos

A finales de la década de los 90, le llegó la hora de la verdad a la teletransportación cuántica, el momento de enfrentarse efectivamente a la realidad: *los experimentos*. El primer experimento que informó la teletransportación cuántica fue realizado en 1997 por un equipo austríaco encabezado por Dik Bouwmeester (Bouwmeester 1997), en la Universidad de Innsbruck, en Austria. Los problemas más difíciles de resolver desde el principio fueron la

producción y medición de estados entrelazados. Para entonces no existían procedimientos experimentales probados para identificar los cuatro estados de Bell para cualquier tipo de sistema cuántico. Aún hoy, sólo existen unas cuantas técnicas experimentales para producir pares entrelazados.

Lo que este equipo usó fue el hecho de que ya se sabía cómo producir pares de fotones entrelazados y cómo proyectarlos hacia al menos dos de los cuatro estados de Bell. La técnica utilizada fue la reconversión paramétrica del tipo II (Kwiat 1995), en la que un fotón, "inyectado" desde el exterior al interior de un cristal no lineal, puede decaer espontáneamente en dos fotones que en este caso de se encuentran en el estado $|\Psi^-\rangle$ de la base de Bell (4.94).

Para lograr la proyección de los dos fotones de Ana hacia uno de los estados de Bell había que hacerlos indistinguibles, por lo que el equipo de Bouwmeester superpuso estos dos fotones en un desdoblador de haz (ver figura 4.6). Así dichos fotones inciden sobre cada lado del desdoblador, siempre que ambos fueran reflejados o transmitidos. En Mecánica Cuántica tenemos que superponer las amplitudes de estas dos posibilidades. Para que las amplitudes estén normalizadas a la unidad, la amplitud para ambos fotones reflejados obtiene un signo menos adicional. Por lo tanto parece que un proceso cancela al otro. Sin embargo, esto es cierto sólo cuando los fotones incidentes están en un estado simétrico. Si están en un estado antisimétrico, las dos posibilidades adquieren otro signo negativo relativo, y por lo tanto interfieren constructivamente (Zeilinger 1994). Por tanto para proyectar los fotones entrelazados al estado antisimétrico $|\Psi^-\rangle$, resulta suficiente poner los detectores en cada una de las salidas del desdoblador de haz y registrar las detecciones simultáneas.

Para asegurarse que los dos fotones de Ana no pueden ser distinguidos por sus tiempos de llegada, se generaron usando un haz de pulso inducido y se hicieron pasar a través de filtros de banda estrecha produciendo un tiempo de coherencia mucho más largo que la duración del pulso inducido. En el experimento, los pulsos inducidos tuvieron una duración de 200 fs y se emitieron con una frecuencia de 76 MHz; con los fotones producto de la reconversión paramétrica, que tenían una longitud de onda de 788 nm y una anchura de banda de 4 nm, se obtuvo un tiempo de coherencia de 520 fs. Es decir, el fotón descono-

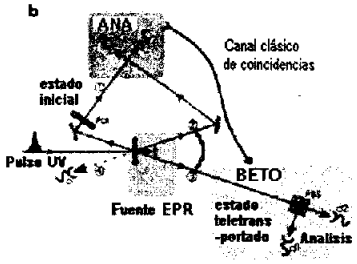


Fig. 4.6. Un pulso de radiación ultravioleta pasa a través de un cristal no lineal, creando el par enredado auxiliar 2 y 3. Después de ser reflejado el mismo pulso UV vuelve a pasar por el cristal creando otro par de fotones, uno de los cuales será preparado en el estado inicial del fotón 1 para ser teletransportado, mientras el otro sirve como indicador de que hay un fotón para teletransportar en camino. Ana entonces busca coincidencias con el desdoblador de haz BS, donde el fotón inicial y uno de los fotones auxiliares se superponen. Después de recibir la información clásica que Ana obtuvo del conteo de coincidencias de los detectores f1 y f2 identificando el estado de Bell $|\Psi^-\rangle_{12}$, Beto sabe que su fotón 3 está en el estado inicial del fotón 1, y corrobora esta información haciendo un análisis de polarización con el desdoblador de haz polarizado PBS y los detectores d1 y d2. El detector p solo indica que el fotón 1 va en camino. (Tomado de Bouwmeester 1997).

cido $|\chi\rangle$ a ser teletransportado, también se produjo como parte de un par entrelazado, y su pareja puede servir para indicar que fue emitido.

Para probar que realmente se llevó a cabo la teletransportación, primero se tiene que mostrar que el proceso de teletransportación usado funciona para una base completa. Una base para los estados de polarización tiene dos componentes, y en principio, podemos elegirla como la base de la polarización horizontal y vertical emitida por la fuente. Pero esto no bastaría para demostrar que la teletransportación funciona para cualquier superposición en general, ya que estas dos direcciones fueron las direcciones típicas de su experimento. Por tanto, en su primera demostración el equipo de Bouwmeester eligió como la base para la teletransportación los dos estados linealmente polarizados a $-45°$ y $+45°$, que son superposiciones de las polarizaciones horizontales y verticales. Después había que mostrar que la teletransportación funciona para las superposiciones de estos estados base. Esto implica —dados los resultados positivos que obtuvieron— que también demostraron que se puede realizar la teletransportación con polarización circular.

El equipo de Bouwmeester realizó dos experimentos. En el primero el fotón desconocido se hallaba polarizado a 45°. La teletransportación se debía llevar a cabo tan pronto como los dos fotones de Ana se detectaran en el estado $|\Psi^-\rangle$, lo que ocurría —como era de esperarse— en el 25% de los casos. Dicho estado $|\Psi^-\rangle$ se identificaba registrando la coincidencia entre los dos detectores f1 y f2 situados a las salidas del desdoblador (ver figura 4.6). Si se detectaba una coincidencia entre los detectores f1 y f2, ello implicaba que el fotón de Beto también debería estar polarizado a 45°. Se analizó la polarización del fotón de Beto haciéndolo pasar a través de un desdoblador de haz polarizado, seleccionando las polarizaciones a $-45°$ y $+45°$. Para demostrar la teletransportación, sólo el detector d2 a la salida de $+45°$ del desdoblador de haz polarizado (Fig. 4.6), debería registrar una detección, una vez que los detectores f1 y f2 también lo hicieran. El solo hecho de registrar detecciones en los detectores d2, f1 y f2, sin registrar detecciones conjuntas en d1, f1 y f2, es la *prueba contundente de que se realizó la teletransportación* (Bouwmeester 1997).

Si no hay teletransportación, los dos fotones de Ana irán a parar ya sea a f1 o a f2 independientemente uno de otro. La probabilidad de coincidencia entre f1 y f2 es por tanto del 50% que es el doble de grande que cuando se realiza la teletransportación. En este caso, como el fotón de Beto está entrelazado —y por tanto no tiene una polarización bien definida, existe la posibilidad del 50% de detectar el fotón de Beto, para cada uno de los detectores d1 y d2. Este sencillo argumento da una probabilidad de 25% tanto para el análisis a $-45°$ como a $+45°$ sin que haya teletransportación. La figura (4.7) resume las predicciones teóricas en función del retardo. La teletransportación exitosa para el estado de polarización a $+45°$ se caracteriza por un decremento a cero en el análisis a $-45°$ (fig. 4.7a) y un valor constante para el análisis a $+45°$ (fig. 4.7)

La predicción teórica de la figura (4.7) se puede entender fácilmente si nota que cuando sucede el retardo igual a cero implica que hay un decrecimiento a la mitad en la razón de coincidencia para los dos detectores f1 y f2, comparado con el caso en que no hay teletransportación. Por tanto, si la polarización del fotón de Beto no tuviera ninguna correlación con los otros fotones, la depresión que aparecería en la gráfica sería de la mitad de profundidad. El hecho de que dicha depresión llega hasta cero en la figura (4.7a), junto

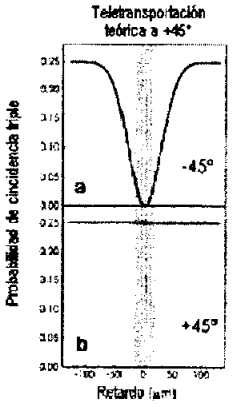


Fig. 4.7. Predicción teórica para la probabilidad de coincidencia de desdoblamientos triples entre los dos detectores de estados de Bell f1 y f2 y uno de los detectores que analizó el estado teletransportado. La prueba de que se teletransportó el estado de polarización a +45° de un fotón, es una disminución hasta cero, justo en el retardo cero en la razón de coincidencia del desdoblamiento triple con el analizador del detector a -45° (d1f1f2)(a) y un valor constante para el analizador del detector a +45° (d2f1f2)(**b**). El área sombreada indica la región de teletransportación. (Tomado de Bouwmeester 1997).

con que se reemplaza con una curva plana en la figura (4.7b), indica que se teletransportó el estado correcto.

Los resultados de la teletransportación experimental con polarización a $+45°$ se muestran en la columna izquierda de la gráfica (4.8).

Compárese las figuras (4.8**a**) y (4.8**b**) con las predicciones teóricas de la figura (4.7). El marcado decrecimiento en el análisis a $-45°$ y la señal mas o menos constante para el análisis a $+45°$, indican que el fotón desconocido de Ana *ha sido teletransportado* (Bouwmeester 1997). Los resultados para dicho fotón polarizado a $-45°$ demuestran que la teletransportación funciona para una base completa de estados de polarización (ver columna derecha de la figura 4.8). Para evitar cualquier explicación clásica de los resultados experimentales, el equipo de Bouwmeester realizó otros experimentos que confirmaran sus resultados, en los que teletransportaron fotones linealmente polarizados a $0°$ y a $90°$, así como fotones circularmente polarizados. La visibilidad de un fotón teletransportado es

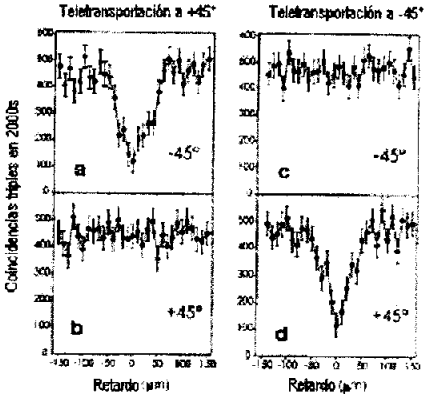


Fig. 4.8. Resultados experimentales. Se trata de las razones de coincidencia d1f1f2 (-45°) y d2f1f2(+45°) en el caso de que el estado del fotón a ser teletransportado esté polarizado a +45° (**a** y **b**) o a -45° (**c** y **d**). Las razones de coincidencia están graficadas en función del intervalo de tiempo entre la llegada del fotón 1 y el 2 al desdoblador de Ana (ver figura 4.6). Las razones de coincidencia de desdoblamientos triples se graficaron luego de eliminar los datos espurios. Estos datos, comparados con la figura 4.7, junto otros datos similares a diferentes polarizaciones (ver tabla 1), confirman la teletransportación para un estado arbitrario. (Tomado de Bouwmeester 1997).

el grado de polarización que tiene en la dirección del estado del fotón original. Los resultados aparecen en la tabla 1, en la que se incluyen las visibilidades de los fotones correspondientes a las depresiones de las curvas para las coincidencias de los desdoblamientos triples, que suceden por análisis ortogonal a la polarización de las entradas.

Visibilidad de la teletransportación experimental	
Polarización	Visibilidad
$+45°$	0.63 ± 0.02
$-45°$	0.64 ± 0.02
$0°$	0.66 ± 0.02
$90°$	0.61 ± 0.02
circular	0.57 ± 0.02

Tabla 1

Los valores de las visibilidades presentados en la tabla 1, se obtuvieron luego de eliminar un cierto desfasamiento o corrimiento debido a coincidencias de desdoblamientos triples espurios. Lo que esta tabla nos quiere decir es una afirmación sencilla pero bien importante: *es posible teletransportar el estado cuántico de un fotón.*

4.6 Teletransportación de átomos

Tanto en los experimentos del equipo de Bouwmeester (aquí descritos) como en otros realizados por el equipo de Boschi (1998), que demuestran que es posible la teletransportación de fotones, no había la posibilidad de realizar una medición completa de los estados de Bell de los dos fotones. Se supo que realmente se había llevado a cabo la teletransportación haciendo una selección de datos *después* de haber terminado el experimento; este proceso de selección consistía en comparar la medición en turno con una operación de reconstrucción preestablecida. Así los resultados eran esencialmente *probabilísticos* y se determinaron a posteriori del experimento.

Más recientemente se logró realizar teletransportación cuántica *determinista de partículas masivas.* El equipo mayoritariamente austriaco de M. Riebe, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T.W. Körber, C. Schmidt-Kaler, D.F.V. James y R. Blatt, reportaron en junio de 2004 (Riebe 2004) teletransportación de partículas masivas, usando sus estados entrelazados. Almacenaron tres iones $^{40}Ca^{+}$ en una trampa lineal de Paul (si quiere consultar una descripción completa de este dispositivo vea Schmidt–Kaler 2003). Los iones fueron arreglados en un cristal lineal con una separación de 5 μm. Un qubit fue codificado en una superposición del estado base $S_{1/2}$ y el estado metaestable $D_{5/2}$ (tiempo de vida $\tau \approx 1.16$ s) del ion $^{40}Ca^{+}$. Cada uno de los qubits que intervinieron en el experimento fueron manipulados independientemente por una serie de pulsos láser en la transición cuadrupolar cercana a 729 nm del estado $|1\rangle \equiv S_{1/2}(m_j = -1/2)$ al $|0\rangle \equiv D_{5/2}(m_j = -1/2)$, empleando radiación láser de banda estrecha enfocada precisamente sobre cada ion de la cadena. Los qubits fueron puestos inicialmente en $|1\rangle$ mediante inyección de fotones. El centro de masa del modo vibracional (con frecuencia angular

$\omega = 2\pi \times 1.2\,\mathrm{MHz}$) de la cadena de iones fue enfriado hasta su estado base para controlar la interacción entre iones (Schmidt–Kaler 2003).

Lo que hicieron fue teletransportar el estado cuántico del ion 1 (el qubit fuente) al ion 3 (el qubit objetivo) usando el circuito cuántico mostrado en la figura (4.9). El protocolo de teletransportación es formalmente equivalente al propuesto por Bennett *et al.* (1993), evidentemente adaptado a las necesidades del dispositivo empleado. Primeramente prepararon el ion 2 (el auxiliar) y el 3 en el estado de Bell $|\Psi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 + |1\rangle_2|0\rangle_3)$, cuyo tiempo de vida sobrepasa los 100 ms, lo que resulta más que suficiente para los fines perseguidos en el experimento, ya que la teletransportación en sí toma menos de 2 ms. El ion 1 fue preparado en un estado inicial arbitrario usando rotaciones locales. El equipo teletransportó un estado $|\chi\rangle$ de entre un conjunto de cuatro estados de prueba no ortogonales: $|\chi^{(1)}\rangle = |1\rangle$, $|\chi^{(2)}\rangle = |0\rangle$, $|\chi^{(3)}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $|\chi^{(4)}\rangle = \frac{1}{\sqrt{2}}(i|0\rangle + |1\rangle)$.

El análisis del estado de Bell lo realizó una puerta de fase controlada (Nielsen 1998) entre el ion 1 y el 2 , seguida por un pulso de $\pi/2$ sobre cada uno de ellos. En seguida se mide el estado cuántico conjunto de los iones 1 y 2, iluminándolos con luz de longitud de onda de 397 nm durante 250 μs. La detección de fluorescencia indicó la proyección del estado cuántico del ion al estado $S_{1/2}$ (estado lógico $|1\rangle$); si no se observaba fluorescencia ello indicaba que se había proyectado al estado $|0\rangle$. Este método para determinar el estado del ion resultó eficiente en aproximadamente 100% de las detecciones. La fluorescencia fue recolectada por un tubo fotomultiplicador y se almacenó el resultado electrónicamente.

Como el proceso de medición debe preservar la coherencia del qubit objetivo, el estado del ion 3 se "ocultó" transfiriéndolo a una superposición de niveles que no fueran afectados por la luz usada para la medición de los otros dos iones. Para ello se movió el estado $S_{1/2}$ a otro nivel Zeeman $|H\rangle \equiv D_{5/2}(m_j = -5/2)$ del Ca^+. Esta misma técnica se usó para la lectura secuencial del ion 1 y del 2, discriminando entre todos los cuatro estados posibles: $\{|0\rangle_1|0\rangle_2, |0\rangle_1|1\rangle_2, |1\rangle_1|0\rangle_2, |1\rangle_1|1\rangle_2\}$. Luego, dependiendo del resultado de la medición, aplicaron la rotación unitaria apropiada: $-i\sigma_y$, $-i\sigma_z$, $i\sigma_x$ ó I para reconstruir el estado $|\chi\rangle$ sobre el estado del ion 3, obteniendo $|\chi^{(\mathrm{exp})}\rangle$. La teletransportación resulta exitosa si el ion 3 se encuentra siempre en estado $|1\rangle$. Este paso condicional determinista,

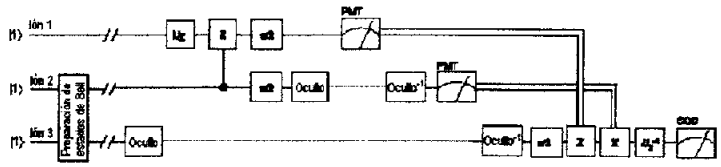


Fig. 4.9. Teletransportación del ion 1 al 3. Primero se preparan los iones 2 y 3 en un estado de Bell. el estado a ser teletransportado se codifica en el ion 1 por medio de la operación U_χ. El analizador de estados de Bell consiste en una puerta Z controlada seguida por rotaciones de $\pi/2$ y detecciones de estado de los iones 1 y 2. Note que esta implementación utiliza una base de Bell rotada $\pi/4$ con respecto a la notación común. Por lo tanto se requiere una rotación de $\pi/2$ sobre el ion 3, antes de reconstruir las operaciones Z y X. Las últimas operaciones se realizan con una rotación de π alrededor de los ejes X y Z, respectivamente. Las líneas grises indican la conducción de qubits protegidos contra la dispersión lumínica. Los iones 1 y 2 se detectan observando su fluorescencia por medio de un tubo fotomultiplicador (PMT). Solo en caso de detectar el estado $|0\rangle$ se aplica la correspondiente operación de reconstrucción al ion 3. La transmisión de información clásica se representa por las líneas dobles. Para el análisis de fidelidad se aplica U_χ^{-1}, y se mide el estado cuántico del ion 3 observando su fluorescencia de resonancia con ayuda de la cámara CCD. (Tomado de Riebe 2004).

en combinación con el análisis completo de los estados de Bell, es uno de los avances más notables de este experimento sobre los anteriores. Otra característica relevante es que después de llevar a cabo la teletransportación el estado $|\chi\rangle$ sigue disponible para posteriores experimentos.

Para obtener directamente la fidelidad de la teletransportación se aplicó al ion 3 el inverso de la transformación unitaria $U_\chi \equiv |\chi\rangle\langle 1| + |\bar{\chi}\rangle\langle 0|$, con $\langle\chi|\bar{\chi}\rangle = 0$, que previamente se había usado para crear el estado inicial del estado $|1\rangle$. Así, la fidelidad quedó definida por la sobreposición $F = \langle 1|U_\chi^{-1}\rho_{\text{exp}}U_\chi|1\rangle$, cuyos cálculos arrojaron un valor de entre 0.73 y 0.76. De hecho se podría llegar a una fidelidad de más de 0.87, mejorando primeramente la estabilidad del campo magnético y reduciendo el ruido de la frecuencia del láser (Riebe 2004).

Otra cosa interesante que se debe notar es que después de la preparación de los estados entrelazados, al ion objetivo sólo se le practican operaciones sencillas locales; por eso, aunque el experimento se llevó a cabo dentro de un potencial de confinamiento común a los

tres iones, se podría —en principio—separar el ion objetivo de los otros dos. Esto podría realizarse utilizando diseños de micro trampas como las que se usaron en este experimento (Kielpinski 2002), que permitirían separar iones individuales de un cristal, logrando así una teletransportación más "remota" (nótese que en este experimento el estado fuente sólo se teletransportó unos cuantos nanómetros).

4.7 La espectacular vanguardia

En agosto del año pasado otro grupo también de austríacos, encabezados por Rupert Ursin y Anton Zeilinger, realizaron un espectacular experimento en el que se teletransportaron con alta fidelidad fotones, a lo lago de 600 m bajo el río Danubio, en Viena (Ursin 2004), con la máxima eficiencia posible en el marco de la óptica lineal. El canal cuántico necesario para la teletransportación fue establecido con un par de fotones con polarización entrelazada, compartido por Ana y Beto. Lograron esto usando una fibra óptica de 800 m de largo, instalada en el sistema de alcantarillado bajo el Danubio, que se encontraba expuesta a fluctuaciones de temperatura y otros factores ambientales. El esquema del dispositivo está en la figura (4.10).

El protocolo de teletransportación que usaron fue el clásico (Bennett 1993), pero también incluía retroalimentación activa por adelantado de los resultados de las mediciones practicadas por Ana, implementada mediante un canal clásico de microondas junto con un modulador electro óptico (EOM) de alta velocidad. Esto permite a Beto implementar la transformación unitaria sobre su fotón entrelazado para obtener una réplica exacta del fotón que Ana le quiere teletransportar. Por ejemplo, si Ana observa el estado $|\Psi^+\rangle$ en su dos fotones (la entrada y el entrelazado), Beto tendrá que implementar un corrimiento de fase de π entre las componentes vertical y horizontal de la polarización de su fotón aplicando un pulso de voltaje de 3.7 kV en el EOM.

Para que la cosa funcionara, pusieron el EOM de Beto correctamente antes de que su fotón llegara; este viajó más lento que la señal clásica debido a que en la fibra óptica viaja a (2/3)c, así que llega como 1.5 μs después de las microondas. Cada sesión experimental

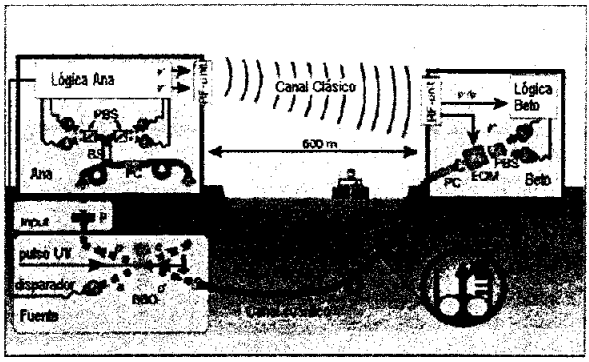


Fig. 4.10. Teletransportación bajo el Danubio. El canal cuántico lo constituye la fibra óptica F instalada en un túnel del alcantarillado bajo el río, y el canal clásico son las micro ondas por encima. Un pulso laser se hace pasar a través de un cristal β de borato de bario (BBO), lo que produce un par de fotones enredados c y d; el par enredado a y b se produce por reconversión paramétrica espontánea. El estado del fotón b después de pasar a través del polarizador P es el input de la teletransportación; a sirve como el disparador. Los fotones b y c son guiados hacia un desdoblador de haz de fibra óptica en modo simple (BS) conectado a los desdobladores polarizados (PBS) para realizar la medición del estado de Bell. La polarización por rotación a causa de las fibras ópticas se corrige con los controladores de polarización (PC) antes de que se hagan las mediciones. La lógica electrónica identifica el estado de Bell detectado, ya sea $|\Psi^-\rangle_{bc}$ o $|\Psi^+\rangle_{bc}$ y comunica el resultado al modulador electro óptico de Beto por medio de la unidad RF, para transformar así el fotón d al estado de input del fotón b. (Tomado de Ursin 2004).

duró 28 h con 0.04 teletransportaciones exitosas por segundo. A pesar de que el dispositivo estuvo expuesto al medio ambiente, se logró la teletransportación de alta fidelidad sin ajustes permanentes.

Con este experimento, el equipo de Ursin y Zeilinger demostraron la teletransportación de tres distintos estados de polarización (a gran distancia y en condiciones atmosféricas): lineal a 45 °, circular izquierdo y horizontal. La fidelidad de la teletransportación que se obtuvo fue de 0.84, 0.86 y 0.90 para el de 45 °, para cada uno de estos estados iniciales respectivos. Estas fidelidades sobrepasan holgadamente el límite clásico de 0.66 (Popescu 1994), lo que prueba que el sistema funciona correctamente. El resultado obtenido constituye un importante paso adelante en la implementación de la repetidora cuántica, que

permitirá compartir entrelazamiento cuántico puro entre partículas distantes en un ambiente público que eventualmente podría ampliarse a escala mundial.

4.8 Las aplicaciones

Parece que todo esto que le he platicado abre la puerta al sueño de teletransportar lo que sea (¡incluyéndolo a usted mismo, por supuesto!) a cualquier lugar en cuestión de segundos (claro, dependiendo de la distancia). Pero como se habrá dado cuenta, apenas estamos en la orilla, falta mucho por hacer. Apenas hemos logrado teletransportar fotones y algunos átomos. Con la tecnología actual no es posible teletransportar objetos macroscópicos. Olvídese de ser teletransportado en un futuro cercano. En una entrevista, reciente (DPA 2005) Anton Zeilinger reveló un curioso cálculo:

> "Solamente la información sobre los estados cuánticos de una persona, que tendrían que transmitirse para la teletransportación, llenarían una pila de CDs de mil años luz de longitud."

Pero la teletransportación tiene otras posibles aplicaciones, especialmente en el mundo de la Informática cuántica. De hecho la teletransportación es un fenómeno colateral descubierto en el desarrollo de la tecnología necesaria para construir una computadora cuántica; por ello dediqué dos capítulos del presente trabajo para hablar de Computación Cuántica. La teletransportación y la Informática cuántica comparten mucho más que sólo qubits.

Anteriormente expliqué lo que sucede cuando el estado entrelazado $|\psi\rangle$ que comparten Ana y Beto es defectuoso, y en general la teletransportación no será posible, o la fidelidad será muy baja. Pero se puede sacar partido de esto. Si reemplazamos $|\psi\rangle$ por $U|\psi\rangle$, donde U es una operación cuántica no trivial, el protocolo de teletransportación produce un resultado que no es el mismo que el de entrada. Si le aplicamos el protocolo de teletransportación al estado $|\chi\rangle$ con este cambio, para cierta U el protocolo puede ser modificado para obtener precisamente $U|\chi\rangle$, una versión modificada de la entrada. La idea

es que *la teletransportación puede servir para implementar compuertas lógicas cuánticas*, indispensables para la construcción de computadoras cuánticas (Gottesman 1999).

Consideremos un ejemplo. En el protocolo normal de teletransportación, Ana mide sus dos qubits (el que se quiere teletransportar $|\chi\rangle$ y uno del par EPR) en la base de Bell; dicha medición proyecta el tercer qubit —que está en poder de Beto— en el estado $R_{xy}|\chi\rangle$, donde R_{xy} está dada por (Gottesman 1999):

$$\begin{aligned} R_{00} &= I \quad \text{la identidad} \\ R_{10} &= X \quad \text{el cambio de bit } |a\rangle \rightarrow |a \oplus 1\rangle \\ R_{01} &= Z \quad \text{el cambio de fase } |a\rangle \rightarrow (-1)^a|a\rangle \\ R_{11} &= Y \quad \text{el cambio de bit y fase } |a\rangle \rightarrow i(-1)^a|a \oplus 1\rangle \end{aligned} \tag{4.116}$$

Las transformaciones X, Y, Z se les conoce como las compuertas lógicas de Pauli, bien conocidas en el mundo de la Computación Cuántica. Otra operación lógica elemental importante es la puerta de Hadamard, definida por

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{4.117}$$

Esta puerta lógica no puede construirse sólo con las compuertas X, Y, Z (Gottesman 1999). Una forma de darle vuelta al problema es usando la teletransportación. En lugar de usar $|\psi\rangle$ para el protocolo de teletransportación, usamos $(I \otimes H)|\psi\rangle$; la operación $I \otimes H$ consiste en aplicar la identidad al primer qubit del par EPR y H al segundo, que es el de Beto. Cuando aplicamos el primer paso de la teletransportación al estado $|\chi\rangle$, el qubit de Beto está en estado $HR_{xy}|\chi\rangle$. Como $HR_{xy} = R_{x'y'}H$; esto es, cuando conmutamos la puerta de Hadamard con uno de los operadores R_{xy}, produce otro operador del conjunto dado por (4.116), que puede ser diferente de HR_{xy}, pero ya que conocemos a priori el mapeo clásico entre xy y $x'y'$, basta con que Beto le aplique a su qubit el operador $R^{\dagger}_{x'y'}$ para obtener el estado $H|\chi\rangle$. He aquí una forma práctica de implementar en la práctica la mentada puerta de Hadamard.

Otra puerta lógica cuántica es nuestra vieja conocida NOC (3.81) que resulta más importante. Se puede teletransportar un estado a través de la puerta NOC usando el circuito

cuántico que se muestra en la figura (4.11). Note que $|\chi\rangle$ (de la figura 4.11) se puede reproducir simplemente aplicando NOC sobre los dos pares EPR (fig. 4.12).

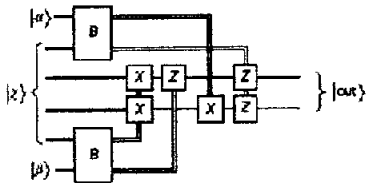


Fig. 4.11. Circuito cuántico para teletransportar dos qubits a través de una puerta NOC. El resultado de esta operación es $|\text{out}\rangle = \text{NOC}|\beta\rangle|\alpha\rangle$, donde los inputs $|\alpha\rangle = a|0\rangle + b|1\rangle$ y $|\beta\rangle = c|0\rangle + d|1\rangle$ son dos qubits arbitrarios. La puerta NOC usa a $|\beta\rangle$ como parámetro de control para actuar sobre $|\alpha\rangle$. El estado especial enredado $|\chi\rangle$ es $[(|00\rangle + |11\rangle)|00\rangle + (|01\rangle + |10\rangle)|11\rangle]/2$. Los qubits múltiples pueden ser teletransportados simplemente repitiendo las veces necesarias el mismo procedimiento que en el caso de un qubit sencillo. Normalmente, para dos qubits, el receptor obtiene el estado $R_{x_1y_1}R_{x_2y_2}|\beta,\alpha\rangle$, pero ya que se ha reemplazado el par EPR normal por el super qubit $|\chi\rangle$, el receptor obtendrá $\text{NOC}R_{x_1y_1}R_{x_2y_2}|\beta,\alpha\rangle$. Como en el caso del operador de Hadamard, NOC cumple con la afortunada propiedad $\text{NOC}R_{x_1y_1}R_{x_2y_2} = R_{x_1'y_1'}R_{x_2'y_2'}\text{NOC}$, lo que significa que el receptor puede aplicar de vuelta un procedimiento de corrección (que aparece en la figura) para obtener $\text{NOC}|\beta,\alpha\rangle$. (Tomado de Gottesman 1999).

Combinando este circuito con (4.11) observamos que se teletransportan dos qubits a través de NOC, y la corrección ahora depende de cuatro bits clásicos en vez de dos. Así podemos construir compuertas NOC entre dos qubits usando sólo operaciones sobre un qubit clásicamente controladas, entrelazamiento cuántico y mediciones en la base de Bell. Como cualquier cómputo cuántico puede realizarse usando sólo operaciones sobre un solo qubit y compuertas NOC (Barenco 1995), esto representa una clara alternativa para realizar en la práctica un conjunto universal de operaciones para cómputos cuánticos, que no requiere operaciones sobre dos qubits excepto por una medición. De hecho, si se generaliza este procedimiento, se puede construir una jerarquía completa de compuertas a través de las cuales se pueden teletransportar estados cuánticos con tolerancia a errores y defectos (Gottesman 1999). No es fortuito que las compuertas H y NOC transformen

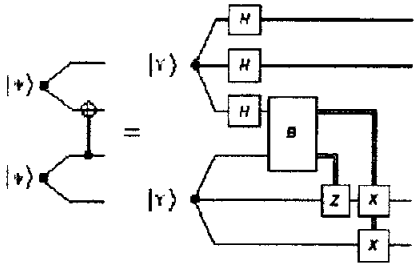


Fig. 4.12. Circuito cuántico para crear el estado $|\chi\rangle$. Utiliza dos pares EPR (izquierda), o dos estados GHZ $|\Upsilon\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ (derecha). H es el operador de Hadamard.

los operadores (4.116) en operadores del mismo conjunto; de hecho, todos los conjuntos de compuertas lógicas que cumplen esta propiedad se les conoce como *grupos de Clifford*, que resultan muy importantes en la teoría de códigos de corrección de errores (Calderbank 1997) y de tolerancia a errores (Gottesman 1998) cuánticos.

Aquí cabe señalar que la meta principal del cómputo cuántico con tolerancia a errores es realizar operaciones lógicas utilizando compuertas cuánticas, restringiendo a la vez la propagación de errores entre los qubits físicos, que podrían comprometer la capacidad de algún código de corrección para corregir errores. El método que usualmente se usa es simplemente incluir operaciones transversales en el código de corrección, es decir, que impliquen la interacción de los qubits de un bloque del código, exclusivamente con los qubits correspondientes en otros bloques del código. Así, aunque los errores puedan propagarse entre bloques, no podrán propagarse dentro de los bloques, y una puerta lógica defectuosa sólo puede causar un error en un solo bloque del código.

Además de los grupos de Pauli (denotados por C_1) y de Clifford (denotados por C_2), existe otro grupo de interés definido como $C_3 \equiv \{U | UC_1U^\dagger \subseteq C_2\}$. En C_3 están contenidos operadores como el de Toffoli (NOCC), el operador $\pi/8$ (una rotación de $\pi/4$ alrededor del eje Z), y el operador de fase ($diag\,(1,1,1,i)$). Los operadores de C_3 normalmente resultan más difíciles de implementar en el laboratorio, y su tolerancia a errores resulta muy reducida (Boykin 1999). La teletransportación permite realizar de manera

práctica y directa cualquier operador de C_3, relajando las restricciones experimentales; a nivel general, esto abre la posibilidad de fabricar computadoras cuánticas a partir de componentes ópticos lineales (Gottesman 1999).Todo esto parece señalar a que las computadoras cuánticas serán esencialmente ópticas, es decir que el electrón, el héroe de la computación del siglo XX, será sustituido por el fotón.

Como antes mencioné, y como usted podrá constatar, la tolerancia a errores resulta de crucial importancia para la construcciones físicas reales de lo que sea, en este mundo tan imperfecto. Por ahora creo que se me acaba el espacio y el tiempo, aunque de ninguna forma el tema: existen muchos campos de estudio, aplicaciones tecnológicas e implementaciones experimentales relacionadas que se me escapan. De hecho mi intención desde el principio no era abarcarlas todas. El horizonte de la Computación Cuántica se vislumbra en verdad muy extenso.

CAPITULO 5
Conclusiones

¿Cual era el objetivo de hacer este trabajo? Ciertamente no se trata de una tesis experimental. Nadie en México hace experimentos sobre teletransportación. El objetivo era explicar el tema y algunas de sus potenciales aplicaciones más relevantes.

El aspecto científico más relevante que toca mi exposición es sin duda el de las correlaciones cuánticas. La acción a distancia, la contraposición de la Mecánica Cuántica con las teorías de variables ocultas, constituyó tal vez el más importante desafío a la Mecánica Cuántica. Para finales de la década de los 60 la teoría cuántica contaba con un buen prestigio, debido a la gran cantidad de fenómenos observados que era capaz de explicar. Y sin embargo quedaba abierta la controversia levantada por Einstein, Podolsky y Rosen en 1935: o la Mecánica Cuántica era incompatible con otra teoría general muy exitosa —la Relatividad, en su aspecto de la localidad—, o simplemente era incompleta. La aportación más significativa de Bell consisistió en expresar dicha contraposición, sencillamente, en la violación o no de sus desigualdades. De manera espectacular, los experimentos durante los años 70 y 80, dieron la razón a la Mecánica Cuántica, convirtiéndose así en la teoría general con más autoridad en nuestros días.

Existen otros aspectos científicos que también se abordan someramente o se intersecan al soslayo, tales como la teoría de la computabilidad, o la posibilidad de la implementación de la inteligencia artificial.

En cuanto aspectos tecnológicos, hay una variada gama relacionada con los temas que abordé, pero sin duda, el más importante es el de la computadora cuántica, más incluso que la misma teletransportación, dadas las dificultades técnicas que todavía hacen impracticable la teletransportación de objetos macroscópicos. Como antes mencioné, el verdadero valor de la teletransportación está en que permite la implementación práctica de compuertas lógicas que serían los ladrillos para la construcción de la computadora cuántica.

Hacia el futuro los pendientes son lograr sistemas cuánticos más estables, acoplar varios sistemas para lograr conjuntos de compuertas lógicas, en fin, ir conformando el

camino hasta el CPU de la computadora cuántica. Tal vez en el camino, o hasta entonces, la teletransportación de objetos macroscópicos se haga viable.

Finalmente, un aspecto colateral que también noté durante mi investigación fue que en México no ha habido una respuesta palpable por parte de la comunidad científica hacia la Computación Cuántica (evidentemente que de parte de la sociedad en general tampoco). Siendo una rama nueva, con tantas posibilidades no tan remotas, y necesitando relativamente un presupuesto relativamente moderado para ingresar en el círculo de la experimentación, podría ser una oportunidad para el desarrollo de tecnología en el país.

La Ciencia en México, como parte de la Ciencia mundial, se halla limitada, o más bien aplastada por el capitalismo. Sin embargo, pienso que muchos de los esfuerzos que hacen los científicos en las direcciones más diversas (por extravagantes que puedan parecer), son de primordial importancia para continuar —a contracorriente— la expansión del conocimiento y defender el importante bastión contra la reacción oscurantista que la Ciencia representa. Yo también tomo mi puesto de combate aquí.

México D.F. a 23 de noviembre de 2005.

Referencias

Albert, David Z. 1983. "On quantum–mechanical autómata." *Physics Letters A.* Vol. **98.** No. 5,6. Pag. 249. Israel.

Aspect, Alain; Dalibard, Jean; Roger, Gérard. 1982. "Experimental Test of Bell's Inequalities Using Time–Varying Analyzers." *Physical Review Letters* Vol **49**, No. 25, pag. 1804. USA.

Barenco A., Bennett C.H., Cleve R., DiVincenzo D.P., Margolus N., Shor P., Sleator T., Smolin J.A. y Weinfurter H. 1995 "Elementary gates for quantum computation." *Physics Review A.* Vol. **52**, pag. 3457. USA.

Beckman D., Chari A., Devabhaktuni S., y Preskill J. 1996. "Efficient networks for quantum factoring." *Physics Review A.* Vol. **54**, pag. 1034.

Bell, John S. 1965. "On the Einstein-Podolsky-Rosen paradox." *Physics* Vol **1**, pag. 195. USA.

Bell, John S. 1990. "Lo decible y lo indecible en Mecánica Cuántica". Alianza Editorial. Madrid. España.

Benioff, Paul. 1980. "The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines." *Journal of Statistical Physics*, Vol **22**, No. 5. USA.

Benioff, Paul. 1982. "Quantum Mechanical Models of Turing Machines That Dissipate No Energy." *Physical Review Letters,* Vol. **48**, No. 23, pag. 1581. USA.

Bennett, C.H. 1973. "Logical Reversibility of Computation." *IBM Journal Research Develop,* Vol. **17.** Pag. 525. USA.

Bennett, C.H. 1982. *International Journal of Theorethical Physics,* Vol. **21.** Pag. 905. USA.

Bennett, Charles H., Brassard, Gilles. 1984, "Quantum cryptography: public key distribution and coin tossing". *Proceedings of the IEEE Conference on Computers, Systems and Signal Precesses,* pag. 175. USA.

Bennett C.H., Charles H. y Wiesner, Stephen J. 1992. "Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states." *Physical Review Letters* **69**, No. 20, pag 2881.

Bennett, Charles H., Brassard, Gilles. 1989, *SIGACT News* **20**, pag. 78. USA.

Bennett C.H., Charles H. y Wiesner, Stephen J. 1992. "Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states." *Physical Review Letters* **69**, No. 20, pag 2881.

Bennett, C.H., Brassard, G., Crépeau, Jozsa R., Peres A. y Wooters, W.K. 1993. "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels." *Physical Review Letters,* Vol. **70**, No. 13, pag. 1895. USA.

Bennett C.H., DiVincenzo D.P., Smolin J.A. y Wootters W.K. 1996. "Mixed-state entanglement and quantum error correction." *Physical Review A,* Vol. **54.** No. 5, pag 3824. USA.

Bennett, C.H., Bernstein, H.J., Popescu, S. y Schumacher, B. 1996b. "Concentrating partial entanglement by local operations." *Physical Review A,* Vol. **53**, No. 4, pag. 2046. USA.

Berman, G.P., Doolen, G.D., Holm D.D. y Tsifrinovich, V.I. 1994. "Quantum computer on a class of one-dimensional Ising systems," *Phisical Letters,* Vol. **193**, pag. 444. UK.

Berstein, E. y Vazirani, U. 1993. "Quantum complexitiy theory". Proceedings of the 25th Annual ACM Symposium on Theory of Computing (ACM, New York) 11-20.

Biham, Eli y Mor, Tal. 1996. "Bounds on Information and the Security of Quantum Cryptography." quant-ph/9605010.

Boschi, D., Branca, S., De Martin, F., Hardy, L. y Popescu, S. 1998. "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolski-Rosen Channels." *Physical Review Letters,* Vol. **80**, pag. 1121. USA.

Bohm, D. Aharonov, Y. 1957. "Discussion of Experimental Proof for the Paradox of Einstein, Rosen and Podolsky." *Physical Review*, Vol. **108**, 4. pag. 1070. Haifa. Israel.

Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H. y Zeilinger, A. 1997. "Experimental quantum teleportation." *Nature* Vol. **390**, pag. 575. Austria.

Boykin, P.G., More, T., Pulver, M., Roychowdhury, V. y Vatan, F. 1999. "On universal and fault–tolerant quntum computing." Preprint quant-ph/9906054, en http://xxx.lanl.gov.

Brassard, Gilles. 1994. "Cryptology Column —Quantum Computing: The end of classical Cryptography?" Sigact News. (preprint)

Brune, M., Nussenzveig, P., Schimidt-Kaler, F., Bermardot, F., Maali, A., Raimond, J.M. y Haroche, S. 1994. "From Lamb shift to light shifts: vacuum and subphoton cavity fields measured by atomic phase sensitive detection". *Physical Review Letters* Vol. **72**, pag. 3339. USA.

Calderbank, A.R. y Shor, P.W. 1996. "Good quantum error-correcting codes exist". *Physical Review A* Vol. **54**, pag. 1098. USA.

Calderbank, A.R. Rains, E.M. Shor, P.W. y Sloane, N.J.A. 1997. "Quantum error correction and orthogonal geometry". *Physical Review Letters* Vol. **78**, pag. 405. USA.

Clauser, J.F., Horne, M.A., Shimony A. y Holt, R.A. 1969. "Proposed experiment to test local hidden–variable theories." *Physical Review Letters* Vol. **23**, pag. 880. USA.

Clauser, J.F., Horne, M.A. 1974. *Physical Review D* Vol. **10**, pag. 526. USA.

Clauser, J.F. 1976. *Physical Review Letters* Vol. **36**, pag. 1223.

Clauser, J.F. y Shimony, A. 1978. "Bell's theorem: experimental tests and implications." *Reports on Progress of Physics*, Vol. **41**, pag. 1881. UK.

Cirac, J.I. y Zoller, P. 1995. "Quantum computations with cold trapped ions". *Physical Review Letters*, Vol. **74**, pag. 4091. USA.

De la Peña, Luis. 1991. "Introducción a la Mecánica Cuántica." FCE/UNAM. México.

d'Espagnat, Bernard. 1979. "Quantum Theory and reality" *Scientific American* **Vol.** 241, Núm. 5. Pag. 158. USA.

Deutsch, David. 1985. "Quantum theory, the Curch–Turing principle and the universal quantum computer." *Procedings of the Royal Society of London A*, **Vol. 400**, pag. 97. Oxford, U.K.

Deutsch, D. y Jozsa, R. 1992. "Rapid solution of problems by quantum computation" *Procedings of the Royal Society of London A*, **Vol. 439**, pag. 553. Oxford, U.K.

Diedrich, F., Bergquist, J.C., Itano, W.M. y Wineland, D.J. 1989. "Laser cooling to the zero-point energy of motion". *Physical Review Letters* Vol. **62**, pag. 403. USA.

Di Vincenzo, D.P. 1995. "Quantum computation." *Science*, Vol. **270**, pag. 255.

DPA. 2005. "Grupo de científicos vieneses logran teletransportar los fotones de Einstein." *La Jornada. Suplemento de Ciencia.* 16/mar/05. México.

Einstein, Albert. B. Podolsky, N. Rosen. 1935. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Physical Review* Vol. **47**, pag 777. Princeton, NJ. USA.

Ekert, Artur. 1991. "Quantum Cryptography Based on Bell's Theorem." *Physical Review Letters* Vol. **67**, No. 6, pag. 661. USA.

Ekert, Artur y Jozsa, Richard. 1996. "Shor's Quantum Algorithm for Factorising Numbers." *Review of Modern Physics* Vol. **68**, pag. 733. UK.

Ekert, A. y Macchiavello, C. 1996. "Quantum error correction for comunication." *Physical Review Letters* Vol. 77, pag. 2585. USA.

Feynman, Richard P. 1982. "Simulating physics with computers." *International Journal of Theoretical Physics,* Vol. **21**. No. 6-7, pag. 467.

Feynman, Richard P. 1986. "Lectures on computation." Addison Wesley. USA.

Freedman, S.J. y Clauser, J.F. 1972. *Physical Review Letters* Vol. **28**, pag. 938. USA.

Fry E.S. y Thompson R.C. 1976. *Physical Review Letters* Vol. **37**, pag. 465. USA.

Galviz, José. 2004. *Elogio de la pereza (la Ciencia de la Computación en una perspectiva histórica).* Prensas de Ciencias. UNAM. México.

Gershenfeld, R.J. y Chuang, I.L. 1997. "Bulk spin-resonance quntum computation". *Science*, Vol. **275**, pag. 350. USA.

Gottesman, Daniel. 1998. "Theory of fault–tolerant quantum computation". *Physical Review A,* Vol. **57**, No. 1, pag. 127. USA.

Gottesman, Daniel y Chuang, Isaac L. "Demostrating the viability of universal quantum computation using teleportation and single–qubit operations." 1999. *Nature* Vol. **402**, pag. 390. USA.

Greenberger, Daniel M.; Horne, Michael A.; Shimony, Abner; Zeilinger, Anton. 1990. "Bell's theorem without inequalities". *American Journal of Physics,* Vol. **58**, No. 12. USA.

Hamming, Richard W. 1986. "Coding and Information Theory." Prentice-Hall. Englewood Cliffs, NJ, USA.

Holt, R.A. y Pipkin, F.M. 1973. Preprint. Harvard University.

Jozsa, R. y Schumacher, B. 1994. "Anew proof of the quantum noiseless coding theorem" *Journal of Modern Optics,* Vol **41**, pag. 2343. UK.

Jozsa, Richard. 1997. "Entanglement and Quantum Computation." *Geometric Issues in the Foundations of Science.* Editores S. Huggett, L. Mason, K.P. Tod, S.T. Tsou y N.M.J. Woodhouse. Oxford University Press. UK.

Kielpinski, D., Monroe, C. y Wineland, D.J. 2002. "Architecture for large–scale ion–trap quantum computer". *Nature*, Vol. **417**, pag. 709. USA.

Kitaev, A. Yu. 1997. "Fault–tolerant quantum computation by anyons". Preprint quant-ph/9707021, en http://xxx.lanl.gov.

Knill, E. y Laflamme, R. 1996. "Concatenated quantum codes". Preprint quant-ph/9608012, en http://xxx.lanl.gov.

Kwiat, P.G. *et al.* 1995. "New high intensity source of polarization–entangled photon pairs." *Physical Review Letters* Vol. **75**, pag. 4337.USA.

Lecerf, Y. 1963. "Machines de Turing réversibles." *C.R. Acad. Fracaise Sci.* Vol. **257**, pag. 2597. France

Lloyd, Seth. 1993. "A potentially Realizable Quantum Computer". *Science* Vol. **261**, pag 1569.

Lo, Hoi-Kwong y Chau, H.F. 1997. "Is Quantum Bit Commitment Really Possible?" *Physical Review Letters* Vol. **78**, pag. 3410. USA.

Mattle, K., Weinfurter, H., Kwiat, P.G. y Zeilinger, A. 1996. "Dense coding in experimental quantum communication". *Physical Review Letters* Vol. **76**, pag. 4656.USA.

Mayers, Dominic. 1997. "Unconditionally secure quantum bit commitment is imposible". *Physical Review Letters* Vol. **78**, pag. 3414.USA.

Monroe, C., Meekhof, D.M., King, B.E., Itano, W.M. y Wineland, D.J. 1995. "Demonstration of a universal quantum logic gate." *Physical Review Letters* Vol. **75**, pag. 4714.USA.

Nielsen, M.A., Knill, E. y Laflamme, R. 1998. "Complete quantum teleportation using nuclear magnetic resonance". *Nature* Vol. **396**, pag. 52. USA.

Plenio, Martin B. y Vedral, Vlatko. 1998. "Teleportation, entanglement and thermodynamics in the quntum world." *Contemporary Physics* Vol. 39, No. 6, pag 431. UK.

Penrose, Roger, 1996. "La mente nueva del emperador". Fondo de Cultura Económica. México.

Popescu, Sandu. 1994. "Bell's Inequalities versus Teleportation:What is Nonlocality?" *Physical Review Letters* Vol. **72**, No. 6, pag. 797. USA.

Preskill, J. 1997. "Reliable quantum computers". Preprint quant-ph/9705031, en http://xxx.lanl.gov.

Riebe M., Häffner H., Roos C.F., Hänsel W., Benhelm J., Lancaster G.P.T., Körber T.W., Becher C., Schmidt-Kaler F., James D.F.V. y Blatt R. 2004. "Deterministic quantum teleportation with atoms". *Nature* Vol. 429, pag. 734. USA.

Schmidt-Kaler, F. *et al.* 2003. "How to realize a universal quantum gate with trapped ions." *Applied Physics B* Vol 77, pag. 789. USA.

Schumacher, B. 1995. "Quantum coding." *Physical Review A*, Vol. 51, pag. 2738. USA.

Shimony, Abner. 1971. "Foundations of Quantum Mechanics." pp. 182-194, 470-480. Compilado por B. D'Espagnat. Academic Press. New York. USA.

Shor, Peter W. 1995. "Algorithms for Quantum Computation: Discrete Log and factoring." *Physics Review A,* Vol. **52.** R2493. USA.

Shor, Peter W. 1996. "Fault tolerant quantum computation". LANL quant-ph/9605011, en http://xxx.lanl.gov. Oxford. UK.

Simon, D. 1994. "On the power of quantum computation", *Proc. 35th Annual Symposium of Foundations of Computer Science,* pag. 124. IEEE Press, Los Alamitos. USA.

Steane, Andrew. 1997. "Quantum computing". LANL quant-ph/9708022, en http: //xxx.lanl.gov. Oxford. UK.

Teich, W., Obermayer, K. y Mahler, G. 1988. "Structural basis of multistationary quantum systems." *Physical Review B*, Vol. **37**, pag. 8111. USA.

Turchette, Q.A., Hood, C.J., Lange, W., Mabushi, H. y Kimble, H.J. 1995. "Measurement of conditional phase shifts for quantum logic". *Physical Review Letters* Vol. **75**, pag. 4710.USA.

Turing, Alan M. 1937. "On computable numbers, with an aplication to the Entscheidungsproblem". *Proceedings of the London Mathematical Society*, (ser. 2), 42, pag. 230-265; corrección en 43, pag. 544-546. London, UK.

Ursin, R., Jennewein, T., Aspelmeyer, M., Kaltenbaek, R., Lindenthal, M., Walther, P. y Zeilinger, A. 2004. "Quantum teleportation across the Danube". *Nature* Vol. **430**, pag. 849.

Vedral V., Barenco A. y Ekert A. 1996. "Quantum networks for elementary arithmetic operations". *Physics Review A*. Vol. **54**, pag. 147. USA.

Vedral V., Plenio M.B., Rippin M.A. y Knight P.L. 1997. "Quantifying Entanglement". *Physical Review Letters*, Vol. **78**, No. 12, pag. 2275. USA.

Werner, Reinhard F. 1989. "Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden–variable model". *Physical Review A*, Vol. **40**, No. 8, pag. 4277. USA.

Wiesner, Stephen J. 1983. "Conjugate Coding." *SIGACT News* Vol. **15**, No. 1, pag. 78. USA.

Zbinden, H., Gautier, J.D., Gisin, N., Huttner, B., Muller, A. y Tttle, W. 1997. "Interferometry with Faraday mirrors for quntum cryptography". *Electrical Letters* Vol **33**, pag. 586. USA.

Zeilinger, A., Bernstein, H.J. y Horne, M.A. (1994). "Information transfer with two–state two–particle quntum systems." *Journal of Modern Optics* Vol. **41**, pag. 2375.