

---

ACADEMIA DE CIENCIAS DE LA REGIÓN DE  
MURCIA

---

**NUEVAS TECNOLOGÍAS CUÁNTICAS PARA EL  
PROCESADO Y TRANSMISIÓN DE INFORMACIÓN:  
UN PASEO POR LA FÍSICA DEL SIGLO XXI**

Discurso de ingreso leído por el Académico electo

**Ilmo. Sr. D. Ignacio Cirac Sasturain**

en el acto de su solemne toma de posesión  
como Académico de Honor,  
celebrado el 15 de noviembre de 2007

y

Discurso de contestación del Académico de Número

**Ilmo. Sr. D. Pablo Artal Soriano**



**Murcia, 2007**

**Todos los derechos reservados.**

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y ss. del Código Penal).

© Academia de Ciencias de la Región de Murcia, 2007

I.S.B.N.: 978-84-611-6576-6

Depósito Legal: MU-810-2007

Imprime: Compobell S.L., Murcia

**NUEVAS TECNOLOGÍAS CUÁNTICAS PARA EL  
PROCESADO Y TRANSMISIÓN DE INFORMACIÓN:  
UN PASEO POR LA FÍSICA DEL SIGLO XXI**

Discurso de ingreso leído por el Académico electo

**Ilmo. Sr. D. Ignacio Cirac Sasturain**



Excmo Sr. Presidente,  
Ilmos Sras y Sres Académicos  
Señoras y señores

Es para mi un auténtico honor el haber sido nombrado Académico de Honor de la Academia de Ciencias de la Región de Murcia. Me produce una gran satisfacción el poder unirme de esta manera tan especial a una institución joven y moderna, integrada por científicos eminentes, cuyo objetivo fundamental es el de cultivar, fomentar y difundir la ciencia y sus aplicaciones. Por ello me gustaría agradecer sinceramente a la Academia y, en particular, a su Presidente y los académicos numerarios Drs. Artal y Ortuño, por haberme concedido tan alto honor. Deseo también mostrar mi plena disposición a colaborar con la Academia en lo que considere oportuno para conseguir sus objetivos. Quiero también aprovechar estas primeras líneas de mi discurso para agradecer al Dr. Pablo Artal su disponibilidad para pronunciar su discurso de contestación.

En este discurso deseo hablar sobre la situación de la Física actual, y de su papel en la Ciencia y la Sociedad del siglo XXI. Mi intención es dar un « paseo » por alguno de los problemas más fundamentales a los que se enfrenta esta disciplina en este siglo que comienza ahora. El objetivo es mostrar que,

aunque parezca que las bases fundamentales de la Física ya han sido establecidas y que sólo nos queda aplicarlas a otros campos, las teorías de las que disponemos hoy en día no explican muchos de los fenómenos que observamos. Es, por tanto, posible que en este siglo asistamos a una o más revoluciones en este campo que cambien nuestra forma de entender la naturaleza y den lugar a nuevas e inimaginables aplicaciones.

### **RETOS PARA EL SIGLO XXI**

Si hubiésemos preguntado a principios del siglo XX qué rama de la Ciencia podría revolucionar nuestras vidas, poca gente hubiese apostado por la Física. Por aquel entonces se pensaba que se conocían las ecuaciones básicas que rigen la Naturaleza y, por tanto, los verdaderos retos eran resolverlas (para lo cual las matemáticas eran esenciales) o usarlas para encontrar aplicaciones prácticas (algo que los ingenieros harían). Sin embargo, los avances tecnológicos logrados a finales del siglo anterior permitieron hacer nuevas medidas, mucho más precisas que las que existían hasta entonces. Estas mediciones dieron lugar a resultados que no eran compatibles con las teorías y ecuaciones existentes. Gracias a esto, dos nuevas teorías emergieron a principios del siglo pasado, la Relatividad y la Cuántica, que, de hecho, han revolucionado nuestra sociedad. Por un lado, han cambiado completamente nuestras ideas sobre la Naturaleza y, por otro, han dado lugar a la mayoría de las aplicaciones que tenemos hoy en día; por ejemplo, todas las basadas en la electrónica o los láseres.

En los últimos años, la tecnología ha experimentado unos avances espectaculares. Hoy en día podemos hacer medidas increíblemente precisas. Por ejemplo, podemos construir relojes atómicos que se retrasarían menos de un segundo en toda la edad del universo. También podemos experimentar en situaciones límite: a muy altas energías, a muy bajas temperaturas, a pequeñas o grandes distancias. Esto nos va a permitir dentro de poco tiempo someter a nuevos tests las teorías existentes y, muy probablemente, encontrar contradicciones entre sus predicciones y los resultados experimentales. Al igual que hace 100 años, esto nos llevará a introducir nuevas teorías, que pueden llegar a revolucionar nuestro conocimiento y nuestra sociedad. Más aún, la Relatividad General y la Física Cuántica parecen no ser compatibles. Esto nos llevaría a la necesidad de encontrar una nueva teoría que, de alguna forma, las supere.

Además de todo esto, estamos consiguiendo domesticar el mundo microscópico. Dentro de poco será posible construir máquinas o circuitos con unos pocos átomos y acceder a las propiedades de sus componentes. Podremos realizar reacciones químicas en unas condiciones impensables hasta hace poco y manipularlas con láseres, además de entender las estructuras espaciales de los compuestos químicos (e.g., de las proteínas). Los avances en la Física llevarán, sin ninguna duda, a nuevas posibilidades para los químicos, biólogos, médicos e ingenieros en los próximos años.

A continuación, discutiré brevemente algunos de los problemas y cuestiones abiertas en el campo de la Física y que, tal vez, puedan ser resueltas en los próximos años.

### **1. El origen y el fin del universo.**

Utilizando las leyes de la Relatividad General es posible entender cuál es el pasado de nuestro universo. En particular, pensamos que éste se ha desarrollado a partir de una explosión inicial, el llamado *Big Bang*. Sin embargo, sólo podemos entender que pasó desde poco después de este estallido. Durante éste y hasta poco después (mucho menos de un segundo) el universo estaba tan concentrado que es necesario utilizar las leyes de la Mecánica Cuántica (pues se trataba de un objeto pequeño) y de la Relatividad (pues era un objeto con mucha masa) para describirlo. No siendo compatibles estas dos teorías, no podemos, pues, caracterizar esos instantes iniciales. Por otro lado, sabemos que el Universo se está expandiendo actualmente, pero no podemos asegurar si lo hará para siempre, o en algún momento se volverá a concentrar en un solo punto debido a la fuerza gravitatoria existente entre los planetas y estrellas.

### **2. Los constituyentes esenciales de la materia.**

Ya desde Aristóteles se creía que los objetos están constituidos por objetos más pequeños, y éstos por otros más pequeños, y así hasta los elementos fundamentales, a los que se les llamaba átomos. En el siglo pasado se estableció un modelo llamado Standard que nos dice que todo está formado a partir de unos objetos esenciales, los Quarks y los Leptones. Este modelo ha predicho varios fenómenos que han sido observados experimentalmente en aceleradores de partículas. Sin embargo,

todavía existen predicciones fundamentales que no han podido ser verificadas. Así, ¿están los Quarks y Leptones formados por objetos más fundamentales? ¿Acaba en algún momento este proceso de buscar los objetos fundamentales, o tal y como decía Leonardo da Vinci, los mundos están consitutidos por otros mundos y este proceso no termina nunca? Además de estas preguntas, el Modelo Standard no es completamente satisfactorio pues no predice cuáles son las propiedades fundamentales (masas, cargas, espines, etc) de todos los objetos. Más aún, medidas astronómicas recientes indican que los planetas se mueven como si existiesen unas masas que no podemos ver. El origen de esta masa oscura es desconocido y hace pensar que existe materia de distinto origen del que conocemos (o del que predice el Modelo Standard).

**3. Nuevas fuerzas en la Naturaleza.** Hasta el momento sabemos que existen cuatro fuerzas fundamentales: la gravitatoria, responsable de que los planetas se atraigan; la electromagnética, responsable de la electricidad y el magnetismo; la débil, responsable de las desintegraciones nucleares; la fuerte, responsable de mantener los protones y neutrones juntos en los núcleos. Según el Modelo Standard, las tres últimas corresponden (a bajas energías) a distintos aspectos de una misma interacción y así pueden ser consideradas como una sola. La gravitatoria no se puede « unificar » con esta interacción, dada la mencionada incompatibilidad entre la Relatividad y la Mecánica Cuántica. En los últimos años se han obtenido unas observaciones astronómicas muy sorprendentes, que pueden llevar a la conclusión de que existe otra fuerza fundamental (o la existencia de la

llamada constante cosmológica): las galaxias del universo cada vez se alejan más rápido unas de otras. Las fuerzas existentes no son capaces de aclarar el por qué de esta expansión: la gravitatoria debería tender a desacelerar la expansión, mientras que las demás fuerzas son demasiado débiles a distancias astronómicas. A la energía responsable de este fenómeno se le llama oscura y no se sabe cuál es su origen.

**4. La existencia de un mundo objetivo.** La Mecánica Cuántica, además de permitirnos describir y utilizar el mundo microscópico, tiene consecuencias filosóficas muy importantes. En particular, nos dice que algunas propiedades de los objetos no están definidas mientras no los observamos. Sólo cuando lo hacemos, quedan definidas algunas propiedades y otras pierden la definición. Esto es lo que afirma, por ejemplo, el principio de incertidumbre de Heisenberg. Si medimos la posición de un objeto (observamos la propiedad posición), automáticamente queda su velocidad indefinida (es decir, si la midiésemos, podría dar cualquier valor). Esta incertidumbre no es debido a que no tengamos conocimiento suficiente sobre las leyes del movimiento, sino que es intrínseca. La Naturaleza es así. Esta predicción bizarra de la Mecánica Cuántica ha sido comprobada experimentalmente y, de hecho, es la base de nuevas aplicaciones en el mundo de la informática y la comunicación. También puede hacer pensar que no existe un mundo objetivo más allá de nosotros mismos, si no que según vamos viviendo (y observando) lo vamos definiendo. La pregunta es si nos tenemos que resignar con esta interpretación, o existen otras interpretaciones menos revolucionarias. En particular podemos preguntarnos si estos aspectos de la Mecánica Cuántica sólo afectan

al mundo microscópico. Pero en este caso, ¿dónde está la frontera? ¿Es este cambio abrupto o continuo? ¿Se puede decir que existen infinitos universos paralelos y que en cada uno de ellos están pasando cosas diferentes, según vayamos observando?

**5. Gravedad Cuántica.** Una de los aspectos más sorprendentes de la teoría de la Relatividad es la llamada dilatación del tiempo (y el espacio). El tiempo pasa de una manera distinta dependiendo de cómo nos movamos. Esto da lugar al ejemplo de los gemelos: si uno de ellos se mueve muy deprisa, al cabo de un tiempo, un hermano será todavía joven, mientras que el otro se habrá hecho viejo. Así, el hermano joven habrá viajado al futuro (pues no sólo su hermano, sino también todo lo que le rodea habrá envejecido). La cuestión es si es posible viajar al pasado. Argumentos básicos de reducción al absurdo demuestran que esto no es posible. Si fuese así, alguien podría viajar a los tiempos en los que su abuelo era joven y matarlo, de tal forma que él no hubiera nacido, lo que llevaría a una contradicción. Sin embargo si, como he mencionado anteriormente, la Mecánica Cuántica nos llevase a concluir la existencia de infinitos universos paralelos, tal vez sería posible viajar al pasado de otro universo de tal forma que se pudiesen evitar las contradicciones lógicas. Antes de predecir si esto es posible habrá que hacer, una vez más, compatible la teoría de la Relatividad General y la Mecánica Cuántica (en lo que daría lugar a una teoría de la Gravedad Cuántica). En estos momentos existen muchos esfuerzos para conseguir una teoría unificada (uno de ellos es a través de la llamada Teoría de Cuerdas), pero, por ahora, estamos muy lejos de conseguirlo.

**6. Nuevos estados de la materia:** Desde pequeños aprendemos que existen tres estados de la materia: sólido, líquido y gaseoso. Sin embargo, en condiciones muy especiales, la materia puede adoptar otras formas con unas propiedades físicas completamente distintas. Así, en presencia de campos eléctricos y magnéticos fuertes o temperaturas muy altas, los electrones se pueden separar de los núcleos atómicos para formar un plasma. A temperaturas muy bajas algunos gases de átomos, en lugar de formar líquido o sólidos se transforman en un nuevo estado de la materia llamado condensado de Bose-Einstein. En este estado, todos los átomos tienden a acumularse en un mismo estado cuántico y se empiezan a comportar de una manera muy extraña, como si todos quisieran hacer lo mismo a la vez. De hecho, este fenómeno es el que explica las propiedades extrañas de algunos materiales, como la superconductividad o la superfluidez. Pues bien, a bajas temperaturas es posible que aparezcan nuevos estados de la materia desconocidos hasta el momento. Estos pueden dar lugar a nuevas propiedades en materiales, que nos permitan tener nuevas aplicaciones.

**7. La emergencia de la complejidad.** Ya he hablado anteriormente de los constituyentes esenciales de la materia. Una vez los conozcamos y sepamos las leyes fundamentales que rigen su movimiento y sus interacciones, ¿será la Física sólo una cuestión de las Matemáticas y la Ingeniería? Pues parece que no. Aunque tengamos las ecuaciones que describen el movimiento de las partículas, es imposible resolverlas. La mayoría de los objetos que vemos y utilizamos son complejos, formados por muchísimas partículas elementales (diez elevado a veinticuatro). Además, existen comportamientos

que no se pueden explicar en términos de las propiedades de las partículas fundamentales. Así se dice que emerge la complejidad y para entender los objetos grandes no basta con estudiar los pequeños. El aspecto más extraordinario de la complejidad es la Vida. ¿Cómo podemos entenderla a partir de elementos inertes? Más aún, en la mayoría de seres vivos, aparte de mecanismos automáticos que pueden ser descritos por ecuaciones, puede existir la libre elección. Esto es, nuestras decisiones no parecen ser predictibles. O, dicho de otra forma, si conociésemos las posiciones iniciales de todas las partículas del Universo y sus leyes ¿podríamos predecir exactamente si voy a querer ir al cine el próximo fin de semana? Nuevos experimentos, así como la comprensión de la Mecánica Cuántica, pueden llevarnos a poder contestar esta importante pregunta.

### **INFORMACIÓN CUÁNTICA**

He dejado para el final el campo en el que mi grupo de investigación concentra sus esfuerzos.

Se trata de un nuevo campo de investigación que combina los principios de la Física Cuántica con las aplicaciones en el procesamiento y transmisión de comunicación. La teoría cuántica, aparte de ser responsable de muchos de los avances tecnológicos ocurridos en el siglo pasado, tiene una vertiente más fundamental. De hecho, afirma que las propiedades de los objetos microscópicos no están definidas, en general, y que sólo adquieren sus valores cuando observamos los objetos. El celebrado principio de incertidumbre de Heisenberg es sólo una manifestación de este hecho. La posición y la velocidad de una partícula no están bien

definidas. Más aún, si medimos la posición de ésta, entonces quedará definida. Pero su velocidad estará entonces totalmente indefinida. No es que no sepamos cuanto vale, si no que simplemente no tiene un valor determinado. Esta afirmación, que parece más bien sacada de un tratado de filosofía que de uno de física, tiene consecuencias apasionantes en el mundo microscópico. De hecho, puede ser utilizada para construir sistemas de comunicación seguros y eficientes, o para procesar la información y hacer cálculos numéricos con una rapidez inimaginable. El campo de la información cuántica está todavía en su infancia, pero promete aplicaciones que pueden dar lugar a una revolución tecnológica en el siglo XXI.

### **Ordenadores cuánticos**

De manera general, al realizar un cálculo con un ordenador tenemos que introducir un "input" (un número o una palabra) que, tras un proceso físico, se convierte en un "output", el resultado deseado. En los ordenadores que tenemos a nuestra disposición, este proceso físico está relacionado con el movimiento de electrones dentro de algunos materiales. Estos fenómenos, aunque tienen su explicación dentro del marco de la Mecánica Cuántica, no utilizan explícitamente el principio de superposición cuántico. Por eso, a estos ordenadores se le suele llamar ordenadores clásicos. Un ordenador cuántico sería aquél en el que el proceso físico está basado en el principio de superposición. Básicamente, esto significa que, además de poder introducir y obtener ciertos números como "inputs" y "outputs", también podemos utilizar superposiciones de números. Esta posibilidad hace que un ordenador cuántico

sea mucho más potente que los que tenemos hoy en día.

Los ordenadores (clásicos) son cada vez más potentes y hoy podemos hacer con ellos cosas que resultaban inimaginables hace veinte años. Continuamente se están produciendo descubrimientos que permiten hacer circuitos electrónicos más pequeños, a la vez que más rápidos. La potencia de un ordenador cuántico, sin embargo, no tiene nada que ver con estos descubrimientos, sino con que la Mecánica Cuántica proporciona "nuevas reglas de juego" (superposiciones) para poder realizar cálculos. Para entender lo que quiero decir, utilizaré una analogía. Hace un par de siglos, la comunicación se realizaba por medios mecánicos. Las cartas se hacían llegar a sus destinatarios utilizando distintos medios de transporte. Por supuesto, la evolución tecnológica de estos medios de transporte dio lugar a una mejora considerable en la comunicación. De hecho, hoy en día es posible utilizar aviones para mandar información. Sin embargo, hace tiempo se produjo un descubrimiento que dio lugar a una verdadera revolución: las ondas electromagnéticas. Con ellas, podíamos utilizar otras reglas de juego (leyes de la física) para comunicarnos. Por mucho que mejorase la tecnología del transporte, jamás será posible comunicarnos de la forma que lo hacemos hoy en día por medio de las ondas electromagnéticas. Así, estos descubrimientos nos permiten conseguir el mismo objetivo (comunicarnos) pero de una manera mucho más eficaz (por teléfono, por ejemplo). En la información cuántica ocurre lo mismo. Con ella podemos hacer cálculos o comunicarnos de una manera totalmente distinta que como lo hacemos habitualmente.

El input en un ordenador se codifica normalmente en bits; esto es, en ceros y unos. En un ordenador cuántico también codificamos la información en bits cuánticos (llamados también qubits). Por ejemplo, el 0 puede representar un átomo con un electrón en la primera órbita y 1 en la segunda. Si utilizamos el principio de superposición también es posible tener el electrón en una superposición cuántica del 0 y el 1. Si evaluamos cualquier función  $f$  sobre estos inputs, los resultados serán  $f(0)$ ,  $f(1)$  o una superposición de estos dos resultados, respectivamente. En este último caso tenemos que con una sola ejecución el output contiene información sobre el resultado de la función evaluada en 0 y 1. Es como si tuviésemos varios procesos corriendo a la vez en el mismo ordenador. Si tenemos 100 qubits, podemos tener pues muchísimos procesos corriendo en paralelo... en un solo ordenador. Esto muestra que un ordenador cuántico puede hacer lo mismo que uno clásico, y más. De hecho, utilizando esta propiedad de la Mecánica Cuántica se han podido encontrar algoritmos con los cuales se podrían resolver problemas de una manera mucho más eficiente que sin utilizarla. Un ejemplo es el problema de la factorización, en donde el objetivo es, dado un número, encontrar otros dos tal que si los multiplicamos obtengamos dicho número. Con los ordenadores actuales (clásicos) es fácil factorizar un número de un par de cifras, pero es imposible construir un ordenador tan rápido que pueda factorizar un número de mil cifras. La razón es que los algoritmos que funcionan en nuestros ordenadores tienen un tiempo de ejecución que escala prácticamente exponencialmente con el número de cifras del número que queremos factorizar. En un ordenador cuántico el esfuerzo en factorizar un número con mil cifras

sería comparable con el de factorizar uno de pocas, ya que en el año 1994 Peter Shor descubrió un algoritmo cuántico en el que el tiempo de ejecución escala polinómicamente con el número de cifras. Es interesante apuntar que el hecho de que los ordenadores actuales no sean capaces de factorizar números grandes se utiliza para enviar información secreta (entre bancos, por internet, etc) con la seguridad de que nadie la podrá descifrar (pues para ello tendría que factorizar un número grande). Así que con un ordenador cuántico todos estos métodos de comunicación dejarían de ser seguros. Por otro lado, Lov Grover en 1996 introdujo un algoritmo cuántico que permite buscar en bases de datos de una manera mucho más eficiente que con los algoritmos clásicos.

Los componentes básicos de un ordenador cuántico son los llamados bits cuánticos o qubits. Estos son sistemas físicos de dos niveles que pueden encontrarse en el estado  $0,1$ , o en cualquier superposición de estos dos. Los inputs y outputs se pueden almacenar en qubits; por ejemplo, si tenemos 4 qubits y queremos introducir el número 11 sólo tenemos que preparar a los qubits en los estados  $|1\rangle|0\rangle|1\rangle|1\rangle$ , ya que 11 en binario es igual a 1011. También es posible preparar un estado superposición, como por ejemplo el  $|1\rangle|0\rangle|1\rangle|1\rangle + |0\rangle|1\rangle|1\rangle|0\rangle$ . Estos estados de superposición de varios qubits se llaman entrelazados y juegan un papel esencial en el algoritmo de factorización de Shor. Una computación cuántica es una operación que transforma el estado de los qubits. Al igual que en el caso clásico, existe un conjunto de puertas lógicas cuánticas universales, de tal forma que toda computación se puede obtener concatenando estas puertas en los distintos qubits.

Si los ordenadores cuánticos son tan interesantes, ¿por qué no se ha construido ninguno todavía? El problema está en que las superposiciones cuánticas son extremadamente frágiles ya que cualquier agente externo actúa como un observador, y hace que sus propiedades queden determinadas (dejan de ser superposiciones). Así que para poder generarlas es necesario tener un objeto completamente aislado de todo lo demás. Tecnológicamente, es imposible aislar completamente objetos grandes pues siempre hay aire, luz, etc. que interaccionan con ellas. Esta es la razón por la cual no se pueden construir superposiciones con objetos macroscópicos. Sin embargo, algunos objetos microscópicos, como los átomos, si se pueden aislar (y de hecho con ellos se pueden crear superposiciones). Por el momento, conocemos muy pocos sistemas físicos que cumplan todos los requisitos necesarios para poder construir con ellos un ordenador cuántico. El impedimento más importante está relacionado con la necesidad de encontrar un sistema cuántico que esté lo suficientemente aislado, pero en el cual existan las interacciones adecuadas; en particular, las necesarias para llevar a cabo las puertas lógicas. Existen tres tipos de sistemas físicos que cumplen, al menos, la mayoría de los requerimientos:

*Optico-Cuánticos:* los qubits se almacenan en los estados internos de varios átomos y las puertas lógicas se obtienen manipulándolos mediante luz láser. Son sistemas muy limpios, en el sentido en que en ellos es posible observar fenómenos cuánticos muy claramente. De hecho, con ellos se han creado estados con analogías a los de la paradoja del gato de Schrödinger, se ha medido el efecto Zeno

cuántico, se han llegado a condensar mediante enfriamiento láser, etc. Además, estos sistemas son los utilizados para crear relojes atómicos, y con ellos se realizan las medidas de mayor precisión que conocemos. Actualmente, en varios laboratorios de Europa (en un Instituto Max Plank de investigación alemán y en las universidades de Innsbruck y Oxford) y de Estados Unidos (en los centros de investigación de Los Alamos y NIST) se han conseguido construir ordenadores cuánticos con unos pocos átomos que se atrapan en trampas electromagnéticas y se enfrían con la ayuda de láseres para que se queden parados. Es de esperar que en los próximos años se puedan llegar a manipular unas cuantas decenas de qubits.

*Sólidos:* Existen varias propuestas para construir ordenadores cuánticos con superconductores, puntos cuánticos o sistemas magnéticos. En ellos los qubits se almacenan, por ejemplo, en pares de electrones (pares de Cooper) en un lado u otro de una unión Josephson, o bien, en electrones en distintos estados de los puntos cuánticos. Por ahora se han podido aislar un par de qubits y realizar puertas lógicas en varios laboratorios de todo el mundo. La mayor dificultad en estos casos es el aislamiento, dado que en un sólido es difícil evitar a las interacciones con otros átomos, impurezas, fonones, etc. Sin embargo, estos sistemas tienen la gran ventaja de que si algún día funcionan, será más sencillo construirlos a escalas mayores.

*Moléculas:* En este caso los qubits están almacenados en los átomos de una molécula y las manipulaciones se producen con la técnica de Resonancia Magnética Nuclear. En un principio

se pensó que esta tecnología era muy apropiada para implementar ordenadores cuánticos, ya que no es necesario enfriar las moléculas (lo que presentaría una gran dificultad en la práctica). De hecho, se han hecho varios experimentos por todo el mundo con hasta siete qubits. Sin embargo, recientemente se ha puesto en duda que estos sistemas en realidad tengan algo que ver con la computación cuántica, pues la señal que se obtiene en la medida decrece exponencialmente con el número de qubits.

### **Criptografía Cuántica.**

Es también posible utilizar las superposiciones cuánticas para encriptar mensajes. En particular, estas superposiciones pueden ser usadas para distribuir claves secretas con las que más tarde se pueden codificar y decodificar mensajes secretos mediante la técnica del OTP («one-time pad»). Los primeros en darse cuenta de este hecho fueron C. Bennet y G. Brassard en 1984 cuando propusieron un protocolo para distribuir claves secretas en el que el remitente envía aleatoriamente uno de los cuatro estados  $|0\rangle, |1\rangle, |0\rangle+|1\rangle$  o  $|0\rangle-|1\rangle$  y el que los recibe realiza una medida de dos posibles. Si alguien intenta interceptar la comunicación, destruirá la superposición, y por tanto será detectado. Un segundo protocolo fue introducido por A. Ekert en 1991 y está basado en la utilización de estados entrelazados que también se destruyen si alguien intenta detectarlos.

Los experimentos en este campo están mucho más avanzados que en el de los ordenadores cuánticos, y ya es posible enviar mensajes secretos entre lugares próximos. El primer experimento de criptografía cuántica se realizó

en IBM en una distancia de 30 cm. Actualmente, grupos experimentales en Ginebra (Suiza), Los Alamos (EEUU), Viena (Austria), Malvern (Gran Bretaña), Munich (Alemania), etc. han conseguido llegar a distancias del orden de 70 km. Es de esperar que en el futuro próximo se llegue a 100 o 200 km. En todos estos experimentos, los estados cuánticos se almacenan en fotones que se envían a través de fibras ópticas. El principal obstáculo para poder llegar a distancias mayores es la absorción de los fotones en la fibra óptica. Para solucionar este problema se están desarrollando sistemas de comunicación con satélites y repetidores cuánticos, que amplificarían los estados entrelazados. Existen hoy en día varias empresas que comercializan este método de comunicación secreta. La importancia de la criptografía cuántica sería mucho mayor en el caso en que existieran ordenadores cuánticos, pues entonces los métodos tradicionales (clásicos) de criptografía no serían seguros y sólo la criptografía cuántica sería capaz de ofrecer una solución completamente satisfactoria.

En definitiva, la Mecánica Cuántica, además de darnos una nueva visión sobre la Naturaleza, permite obtener efectos que pueden ser aprovechados en el campo de la comunicación y de la computación. Estos efectos están directamente relacionados con el principio de superposición. En particular, el hecho de que un computador pueda aceptar "inputs", producir "outputs" y manejar superposiciones de estados puede ser utilizado para resolver problemas de una manera más eficiente. La puesta en práctica de estas ideas es, sin embargo, muy complicada. Los primeros experimentos sobre computación

cuántica están teniendo lugar. Sin embargo, todavía es muy pronto para saber cuándo tendremos ordenadores cuánticos. Lo que sí está claro es que si somos capaces de construirlos, podremos realizar tareas que nunca podríamos realizar con ordenadores clásicos. En criptografía, por el contrario, los experimentos están ya muy avanzados y es posible incluso comprar un sistema criptográfico cuántico. Más aún, es fácil predecir que muchas de las aplicaciones del futuro en el campo de la comunicación y de la computación estarán basadas en el principio de superposición cuántico y en la existencia de los estados entrelazados.

Con esto, me gustaría concluir no sin antes comentar que esta lista de temas que he mencionado no es ni exhaustiva ni, tal vez, contenga algunas de los retos más importantes de la Física. Así, he dejado fuera temas como la Nanotecnología, la Óptica, la Fusión Nuclear, la existencia de vida en otros planetas, o la predicción del clima. Es muy probable que en los próximos años haya descubrimientos revolucionarios que cambien nuestra Sociedad. Además, estoy seguro de que la mayor revolución ocurrirá en algún tema que no he mencionado en este discurso, ni en el que hayamos pensado hasta ahora pues, la Ciencia Básica es así: los mayores descubrimientos son los inesperados.

**Bibliografía :**

A. Galindo, *Quanta e información*, Revista Espanola de Física, **14**, 30 (2000).

J.I. Cirac, *Quanta y computación*, Revista Espanola de Física, **14**, 48 (2000).

C.W. Bennett y D. DiVincenzo, *Quantum Information and Computation*, Nature, **404**, 247 (2000).

J. I. Cirac and P. Zoller , *New frontiers in Quantum Information with atoms and ions*, Phys. Today **57**, 38 (2004).

J. I. Cirac and P. Zoller, *How to manipulate cold atoms*, Science **301**, 176 (2003).



# **DISCURSO DE CONTESTACIÓN**

**por el**

**Ilmo. Sr. D. Pablo Artal Soriano**



Excmo. Sr. Presidente.  
Ilustrísimos señora y señores Académicos.  
Señoras y señores.

Es para mí un honor, y una gran alegría, dar la bienvenida a la Academia de Ciencias de la Región de Murcia, como Académico de Honor, al Profesor D. Ignacio Cirac. Para una institución joven como nuestra academia, incorporar a Ignacio Cirac tiene un significado extraordinario, tanto por su personalidad, como por sus impresionantes logros científicos.

El Profesor Cirac, Ignacio, nació en Manresa en 1965; sí, ¡acaba de cumplir sólo 42 años! Su juventud contrasta con los datos casi increíbles del currículum que describiré brevemente en lo que sigue. Cursó los estudios de Física en la Universidad Complutense de Madrid, y posteriormente realizó su doctorado en el Departamento de Óptica de esa Universidad, leyendo su Tesis Doctoral en 1991. Desde esos inicios, Ignacio ha estado vinculado a la Óptica. Lo maravilloso de la Óptica, esa parte "humana" de la Física, es que ha contribuido al avance más profundo del conocimiento científico, pero también ha aportado soluciones prácticas en miles de aplicaciones que han mejorado la calidad de vida de los ciudadanos. Ignacio se encuentra justo en el medio de estas dos situaciones. Sus actividades en Óptica Cuántica tienen la voluntad de entender el mundo, pero es muy posible que cambien nuestra forma de vida. Los gigantes de la ciencia son aquellos que simultáneamente consiguen avances en nuestra comprensión del mundo y abren nuevas

vías para el desarrollo de la tecnología. Es emocionante compartir este acto con alguien que está llamado a formar parte de esa reducida élite de "gigantes" de la ciencia.

Tras terminar su Tesis, Ignacio consiguió un puesto de profesor titular en la entonces recién creada Universidad de Castilla-La Mancha. Afortunadamente, la tradición de la universidad española, donde muchos entienden la obtención de un puesto de funcionario como una "culminación" de expectativas, que en muchos casos representa el fin de una carrera antes de empezar, no le afectó en absoluto. Durante sus años en Ciudad Real, realizó varias estancias en el JILA de la Universidad de Colorado, un laboratorio clave en un momento clave de la Física Atómica. En 1996, decide dejar España y se traslada al grupo del Prof. Zoller en la Universidad de Innsbruck, otro laboratorio líder. Desde 2001 está en Garching, cerca de Munich, en el Instituto Max Planck de Óptica Cuántica, del que ha sido director de su división de teoría. Ignacio durante su carrera ha realizado numerosas estancias de investigación, entre ellas en las universidades de Harvard, MIT, CALTECH, Colorado, Berkeley, Santa Barbara, Ecole Normal Supérieure, Cambridge, Oxford, etc.; sin duda todo un catálogo de lugares excelentes.

La repercusión y el impacto del trabajo de Ignacio ha sido, y sigue siendo, simplemente impresionante. Ha publicado unos 250 artículos, entre ellos 7 en Nature, 4 en Science y unos 80 en Physical Review Letters. Pero en realidad, estos números, aunque ya de por sí extraordinarios (¿de donde saca el tiempo este hombre?), no son lo más destacable. Lo

realmente fuera de toda comparación con la inmensa mayoría de científicos, son las citas que sus trabajos han obtenido. Existe un consenso cada vez mayor que nuestro trabajo como científicos, si ha de medirse, no deberá ser al "peso", es decir simplemente por el número de publicaciones de un autor. Un parámetro mucho más adecuado para evaluar nuestra calidad científica es contar el número de citas que han recibido nuestras publicaciones. Esta vara de medir es mucho más exigente y coloca a partir de ciertos números a quien los posee en un nivel claro de excelencia. El cálculo de citas y diversas aritméticas con ellas se han puesto muy de moda últimamente, y casi todos los científicos sabemos cual es (y el que nos gustaría que fuera) nuestro índice h. Este parámetro, propuesto por Jorge Hirsch hace unos pocos años es el número de artículos con al menos un cierto número de citas. Como un ejemplo, alguien tiene un índice h de 30, si 30 de sus publicaciones han recibido 30 o más citas. Parece demostrado que la mayoría de los científicos que han sido muy influyentes (y recompensados con premios importantes, como el Nobel) han tenido carreras largas con muchos trabajos influyentes y altos índices h. Estos son algunos números de Ignacio: sus publicaciones han recibido más de 12.000 citas.

Tiene una publicación con más de 1.000 citas (lo que es considerado como un clásico), dos con más de 500, 30 con más de 100, y 58 con 58 o más citas (es decir un índice h igual a 58). Para poner estos números en perspectiva, un buen científico profesional con un alto nivel internacional puede tener unas 1000 citas y un índice h de alrededor de 20. Toda una institución española media, como nuestra

Universidad de Murcia, con unos 8500 artículos publicados tiene un índice h, sólo ligeramente superior de 75. ¿Y en cuanto al número total de citas? Ignacio es el segundo científico más citado en los campos de la Física Atómica y la Computación Cuántica en los últimos 10 años, con 8456 citas, sólo por detrás de W. Ketterle (Premio Nobel de Física 2001, 8690 citas), y por delante de P. Zoller (Premio Niels Bohr de la UNESCO, 7682 citas), T. Hänsch (Premio Nobel de Física 2005, 7237 citas), C. Wieman y E. Cornell (Premios Nobel de Física 2001, 5275 y 5156 citas).

Por supuesto, con esta trayectoria, el número de premios y honores que Ignacio ha recibido es muy grande. Recuerdo que al felicitarle por alguno de los últimos, bromeé con él diciéndole que de seguir así, tendría ocupado todo su tiempo en la "dura" tarea de recibir premios y dar discursos de recepción. Afortunadamente, no me hizo mucho caso y también aceptó convertirse en Académico de Honor de nuestra academia y venir hoy a Murcia. Entre los premios recibidos, quizás mencionar dos: el Príncipe de Asturias de Investigación recibido en 2006 y el premio nacional de investigación de este año 2007.

¿Y el premio con el que de vez en cuando soñamos todos los científicos, aunque no lo reconozcamos? Dicen que es mejor no hablar de ciertas cosas para evitar la mala suerte..., pero con el bagaje de Ignacio, con sus contribuciones, con su edad, es uno de los pocos elegidos que pueden pensar en despertarse un día de su sueño con una llamada de teléfono desde Estocolmo.

Si algo sorprende de la personalidad de Ignacio es su sencillez. No exhibe ese endiosado distanciamiento de algunos de nuestros colegas que se sienten importantes, superiores o elegidos. Es un científico que tiene la capacidad de divulgar conceptos difíciles y que hace sentirse cerca de él a sus audiencias.

¿Y sus contribuciones? ¿Por qué son tan importantes? ¿Por qué despiertan tanto interés? Sería pretencioso por mi parte, que me he instalado en la parte de la Óptica más aplicada, mas cerca de la ingeniería y de las ciencias de la visión y me he ido alejando de los conceptos abstractos de la Física Cuántica, intentar resumirlas o explicarlas aquí de nuevo. Y en especial después de oír su discurso donde nos ha deleitado con sus hallazgos en un paseo por la Física del siglo XXI, una Física a la que él habrá contribuido de forma decisiva.

En nombre del Presidente y de los Ilustrísimos señora y señores Académicos, doy la bienvenida, una vez más, a Ignacio Cirac como nuevo Académico de Honor.