REAL ACADEMIA DE CIENCIAS
EXACTAS, FÍSICAS Y NATURALES

LOS JUEGOS NO LOCALES: UN NEXO ENTRE LAS MATEMÁTICAS, LA FÍSICA Y LAS CIENCIAS DE LA COMPUTACIÓN

DISCURSO LEÍDO EN EL ACTO DE SU RECEPCIÓN
COMO ACADÉMICO DE NÚMERO POR EL

EXCMO. SR. D. DAVID PÉREZ GARCÍA

Y CONTESTACIÓN DEL

EXCMO. SR. D. FERNANDO BOMBAL GORDÓN

EL DÍA 8 DE MARZO DE 2023

MADRID
Domicilio de la Academia
Valverde, 22

Dedicado a la memoria de mi padre

Índice

Parte I

DISCURSO DEL EXMO. SR. D. DAVID PÉREZ GARCÍA

1. INTRODUCCIÓN

Excelentísimo Señor Presidente,
Excelentísimos Señores Académicos,
Señoras, Señores,

Es difícil expresar con palabras, y más aún para alguien no especialmente hábil con ellas, mi profundo agradecimiento a los miembros de la Real Academia de Ciencias por confiar en mí para ocupar la medalla número 51, dentro de la Sección de Ciencias Matemáticas. Pondré todo mi empeño en estar a la altura del honor que me han concedido y en contribuir, en la medida de mis posibilidades, a la misión y tareas de esta Academia.

Desde 2018 he tenido el orgullo de ser Académico Correspondiente. Pero, ya desde mucho antes, la influencia de esta Real Academia en mi vida, y no solo científica, ha sido más que notable; en primer lugar, y por encima de todo, porque mis dos grandes maestros, Don Fernando Bombal Gordón y Don Ignacio Cirac Sasturain, son Académicos Numerarios de esta institución.

Tuve el placer de conocer a Fernando Bombal durante mis años de Licenciatura en la Universidad Complutense de Madrid, en los que cursé con él Teoría de la Medida, Variable Compleja y Análisis Funcional. Ya desde entonces, su conocimiento enciclopédico, histórico y profundo del análisis matemático me encandiló. Algo que no hizo más que aumentar durante mis años de tesis doctoral, codirigida entre él y Don Ignacio Villanueva Díez. Durante esos maravillosos años, Fernando se convirtió también en un segundo padre para mí, del que aprendí, y sigo aprendiendo, mucho más que matemáticas. Escucharle hablar de cualquier tema (política, cultura, economía, ...) es siempre iluminador. Es lo que tienen los sabios.

A Ignacio Cirac le conocí en un curso de verano que él impartía sobre Información y Computación Cuántica en la Universidad Menéndez Pelayo allá por 2004. Asistí al curso por sugerencia de mi buena amiga María Isabel González Vasco, con la que tuve la suerte de compartir departamento durante mis breves años en la Universidad Rey Juan Carlos. Desde el primer momento, todavía no tengo muy claro por qué, Ignacio creyó en

mí, tanto como para ofrecerme una posición postdoctoral en su grupo a pesar de mi total desconocimiento hasta de los conceptos más básicos de la física. El año que pasé con él en Garching es, seguramente, uno de los más interesantes, e intensos, de mi vida. La generosidad con la que me trató, y me sigue tratando, la cantidad (enorme) de tiempo que invirtió (y sigue invirtiendo) en mí, en enseñarme básicamente todo lo que sé de física cuántica, es algo que nunca podré agradecerle lo suficiente.

De Fernando he aprendido, entre otras muchas cosas, a apreciar el poder del enfoque abstracto de los problemas. A veces, para resolver un problema muy concreto, es mejor verlo como una instancia de un problema más general, que permita aislar la estructura matemática adecuada que marque el camino de su solución.

De Ignacio he aprendido, entre otras muchas cosas, a apreciar el poder del enfoque concreto de los problemas. A veces, para resolver un problema general, es necesario ganar intuición a partir de ejemplos concretos especialmente relevantes que marquen el camino de su solución.

De ambos he aprendido que la ciencia, y en particular las matemáticas, requieren de proyectos a largo plazo, del desarrollo pausado y profundo de nuevas teorías, de ser arriesgado y apostar por caminos no convencionales. Estoy convencido de que no estaría hoy aquí de no ser por ellos.

Pero no solo los profesores Bombal y Cirac han sido los únicos Académicos que han marcado mi vida personal y profesional. Por ejemplo, Don José María Montesinos Amilibia me enseñó, en sus clases irrepetibles de Geometría Riemanniana, la belleza y la potencia de interconectar distintas áreas de las matemáticas. No creo que ninguna clase me haya impactado e influenciado tanto como aquel curso del año 2000.

Con otros muchos Académicos, tanto Numerarios como Correspondientes, he tenido el placer de compartir proyectos comunes: Don Ildefonso Díaz Díaz, Don Alberto Galindo Tixaire, Don Francisco Luis Hernández Rodríguez, Don Miguel Ángel Herrero García, Don Manuel de León Rodríguez, Don Miguel Ángel Martín-Delgado Alcántara y Don David Ríos Insúa. Todos ellos han sido siempre referentes para mí. Jamás llegué a soñar que algún día pasarían a ser mis compañeros en esta Real Academia de Ciencias.

Y, por supuesto, no puedo dejar de mencionar a Don Manuel Maestre Vera, Académico Correspondiente, y al Profesor Richard Martin Aron, Académico Extranjero, que me han acompañado desde mis primeros pasos como investigador, con un cariño del que no soy merecedor. He intentado siempre seguir sus consejos, tanto en la vida como en la ciencia.

Sobre la presentación

He de empezar confesando que ha sido difícil para mí elegir el tema de este discurso, así como preparar su contenido. Quería elegir un tema de actualidad, en el que yo hubiera hecho contribuciones relevantes y que, a la vez, pudiera ser presentado a una audiencia tan variada como esta; con expertos de primera línea en las distintas ciencias, pero también con familiares y amigos, de manera que todos pudieran disfrutar de la presentación.

Creo que el tema elegido, los juegos no locales, cumple todos esos requisitos. Espero que mi discurso haga justicia a la belleza y profundidad del tema.

En la presentación no seguiré un enfoque histórico o cronológico, sino más bien pedagógico, dejando que sea el hilo del argumento el que decida en qué orden irán apareciendo las principales ideas y resultados.

Por esas casualidades del destino, cuando estaba ultimando los detalles de este discurso, se ha hecho público el Premio Nobel de Física 2022, otorgado a los Profesores Alain Aspect, John F. Clauser y Anton Zeilinger precisamente por sus contribuciones en este tema; más concretamente por sus experimentos asociados a la vertiente de los juegos no locales conectada con la teoría de la información cuántica. Algo de lo que hablaré en breve.

Empecemos.

2. LOS JUEGOS NO LOCALES

Imaginemos un programa de televisión en el que dos participantes, Alice y Bob [1], juegan de forma cooperativa para intentar ganar. Al llegar al plató, se les explican las reglas del juego:

- **Regla 1:** Antes de empezar el juego, se les aislará en habitaciones separadas y no podrán comunicarse

- **Regla 2:** El presentador elegirá al azar de entre un conjunto de preguntas conocidas por los concursantes y enviará una parte de la pregunta a Alice y otra a Bob.

  Por ejemplo, las preguntas podrían ser "Países europeos", y la forma de dividir la pregunta podría ser enviar a Alice ternas de países como "(España, Francia, Italia)" y a Bob la posición dentro de esa terna del país elegido como pregunta, por ejemplo "posición 2". Esto identificaría unívocamente a "Francia" como pregunta, aunque en este caso ni Alice ni Bob lo sabrían con certeza porque están aislados por la Regla 1.

- **Regla 3:** Alice y Bob tienen que responder de entre un conjunto de respuestas conocidas; en el ejemplo anterior podría ser la capital del país en cuestión.

- **Regla 4:** Para todas las combinaciones de preguntas y respuestas posibles, qué combinaciones son correctas y cuáles no, es conocido también de antemano por los concursantes. En el ejemplo mostrado podría ser considerado correcto que al menos uno de los concursantes responda la capital de forma correcta.

El objetivo es intentar ganar el juego con la mayor probabilidad posible. Por ejemplo, si Alice elige al azar uno de los tres países y responde su capital, y Bob no responde nada, la probabilidad de ganar el juego sería del 33 %, es decir $\frac{1}{3}$.

[1] Aunque sean en inglés, mantendré llamar a los participantes Alice y Bob por ser los nombres que siempre se utilizan en este contexto.

Es el objetivo de este discurso mostrar cómo este sencillo juego y sus variantes describen una cantidad enorme de problemas, tanto en matemáticas como en física y en ciencias de la computación y, precisamente por ello, estos *juegos no locales*, como suelen llamarse, han constituido un puente de unión enormememente rico entre esas tres disciplinas.

Para lograr estudiar de forma rigurosa los juegos no locales, tenemos también que definir las reglas de manera rigurosa. La abstracción matemática de las reglas anteriores serían las siguientes reglas:

- **Regla 1:** Antes de empezar el juego, se aislará a los participantes Alice y Bob en habitaciones separadas y no podrán comunicarse.

- **Regla 2:** El presentador elegirá el par de preguntas (x, y), con probabilidad $\pi(x, y)$ de entre un conjunto finito de ellas Q, y le pasará la pregunta x a Alice y la pregunta y a Bob.

  Definir el conjunto de preguntas como pares (x, y) es lo que formaliza la división de una pregunta en dos partes, cada una enviada a cada uno de los participantes.

- **Regla 3:** Alice, respectivamente Bob, tiene que responder eligiendo una respuesta a, respectivamente b, de entre un conjunto finito de respuestas A.

- **Regla 4:** Para todas las combinaciones de preguntas y respuestas posibles, hay una función $V(a, b, x, y)$ con valores en $\{0, 1\}$ que determina si esa combinación gana el juego (resultado 1) o lo pierde (resultado 0).

Por supuesto, se les facilita a los concursantes tanto los conjuntos A, Q, como la distribución π y la función $V(a, b, x, y)$, y se les permite juntarse en una habitación con antelación para decidir qué estrategia van a seguir una vez empiece el juego.

La pregunta es la misma de antes: ¿cuál es la probabilidad óptima de ganar y cuál es la estrategia que lo consigue?

Conviene detenerse un momento a pensar en cómo formalizar la noción de *estrategia*. Básicamente, consiste en decidir con qué probabilidad responder el par (a, b) si se recibe como pregunta el par (x, y); pro-

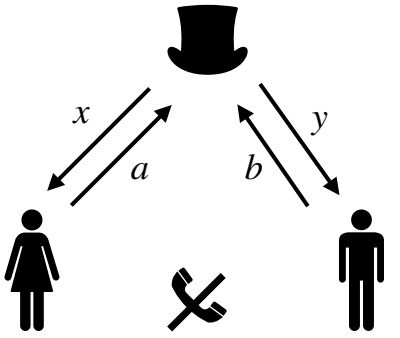

Figura 2.1: Los juegos no locales son el objeto central en este discurso. Los participantes, Alice y Bob, deben dar respuestas a, b adecuadas para cada par de preguntas x, y, sin poder comunicarse entre ellos.

babilidad que se denotará por $p(ab|xy)$. Al ser $p(ab|xy)$, para cada par (x, y), una distribución de probabilidad, se tiene que $p(ab|xy) \geq 0$ y $\sum_{ab} p(ab|xy) = 1$ para todo x, y.

Ahora bien, las reglas del juego restringen las distribuciones de probabilidad $p(ab|xy)$ posibles. La estrategia más general posible para Alice y Bob consiste en utilizar el tiempo que están juntos en una habitación antes del juego para muestrear de una distribución de probabilidad $q(\lambda)$, lo que de forma efectiva corresponde a asumir que, cuando el juego empieza, tienen acceso a una fuente común de aleatoriedad compartida. De esta manera, la estrategia más general posible que pueden utilizar es de la forma

$$p(ab|xy) = \sum_{\lambda} q(\lambda) p_A(a|x\lambda) p_B(b|y\lambda)$$

para distribuciones de probabilidad $p_A(a|x\lambda)$, $p_B(b|y\lambda)$ que recogen la forma en la que Alice (resp. Bob) responde a la pregunta x (resp. y).

Como la probabilidad de ganar el juego utilizando una estrategia dada no es más que

$$\sum_{a,b,x,y} p(ab|xy)\pi(x, y)V(a, b, x, y),$$

es claro que siempre existe una estrategia óptima que es de *tipo producto*, es decir de la forma $p(ab|xy) = p_A(a|x)p_B(b|y)$.

Antes de continuar, puede ser interesante plantear un primer ejemplo concreto de juego, conocido como juego CHSH, del que más adelante comentaré sobre su origen e interés.

En el juego CHSH hay dos preguntas posibles para Alice y Bob $\{0,1\}$ y dos respuestas posibles $\{0,1\}$. Las cuatro combinaciones de preguntas $00, 01, 10, 11$ se preguntan con la misma probabilidad $\frac{1}{4}$ y la función de verificación es

$$V(a,b,x,y) = 1 \text{ si y solo si } xy = a \oplus b,$$

donde $\oplus$ es la suma módulo 2, también llamada XOR. Es decir, el valor de $V(a,b,x,y)$ viene dado por los valores de la siguiente tabla:

(a,b) \ (x,y)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	1	1	1	0
$(0,1)$	0	0	0	1
$(1,0)$	0	0	0	1
$(1,1)$	1	1	1	0

Es fácil encontrar una estrategia que gana el juego con probabilidad $\frac{3}{4}$; por ejemplo, si Alice y Bob siempre responden 0. En la notación anterior, esta estrategia se corresponde con la elección

$$p_A(0|0) = p_A(0|1) = 1,\ p_A(1|0) = p_A(1|1) = 0,$$

$$p_B(0|0) = p_B(0|1) = 1,\ p_B(1|0) = p_B(1|1) = 0.$$

Como la respuesta $(a,b) = (0,0)$ es correcta salvo para el par de preguntas $(x,y) = (1,1)$, esta estrategia gana el juego con probabilidad $\frac{3}{4}$. No es difícil ver que no existe una estrategia mejor.

3. NO ES TAN SENCILLO COMO PARECE

Dado un juego G, que viene descrito por los conjuntos A, Q y las funciones $\pi(x, y)$ y $V(a, b, x, y)$, se llama *valor* del juego, y se denota $\omega(G)$, a la probabilidad óptima de ganar el juego.

A pesar de su apariencia sencilla, computar $\omega(G)$, incluso dar una aproximación razonable de su valor, es difícil; de hecho, enormemente difícil. ¿Podemos cuantificarlo? ¿Cómo se puede cuantificar lo difícil que es un problema?

Uno podría pensar que esa dificultad es algo puramente subjetivo y radica simplemente en la inteligencia del que lo quiere resolver: problemas que son complicados de resolver para algunas personas pueden ser muy sencillos para otras. Por ejemplo, yo jamás he sido capaz de resolver el cubo de Rubik pero he visto a niños resolverlo en menos de un minuto y con los ojos cerrados.

Sin embargo esto no es así. La teoría matemática de la complejidad computacional permite, precisamente, clasificar de forma rigurosa los problemas en *fáciles* y *difíciles*, al menos desde cierto punto de vista. Veamos cómo.

Complejidad computacional: P vs NP

Empecemos con el problema de multiplicar dos números naturales; pongamos 32×21. ¿Cuántas operaciones *elementales* tenemos que hacer para dar la respuesta? En este caso bastaría hacer 7 operaciones, una para obtener cada uno de los dígitos que aparecen en el algoritmo de multiplicación que todos aprendimos en el colegio:

$$\begin{array}{rcc} & 3 & 2 \\ \times & 2 & 1 \\ \hline & 3 & 2 \\ 6 & 4 & \\ \hline 6 & 7 & 2 \end{array}$$

¿Y si ahora quisiéramos multiplicar dos números, cada uno de n cifras? ¿Cuántas operaciones elementales habría que hacer? Como hay que multiplicar cada dígito del primer número con cada dígito del segundo, eso nos da n^2 operaciones. Luego hay que sumar, columna por columna, los n^2 dígitos obtenidos al multiplicar, lo que nos da otras n^2 operaciones. Concluimos por tanto que el algoritmo de multiplicar dos números de n cifras requiere $2n^2$ operaciones elementales. Como $2n^2$ es un polinomio en n, se dice que ese algoritmo tiene complejidad *polinomial*. [1]

Veamos ahora la operación inversa de multiplicar, que es *factorizar*. Supongamos que nos dan el número 403 y nos piden encontrar dos números a y b tales que su producto es 403. El algoritmo que nos enseñaron en el colegio para este problema era el más sencillo de todos: ir probando. Primero intentamos ver si la división de 403 entre 2 es exacta o no, luego la división de 403 entre 3, entre 4, y así hasta que lleguemos a una división exacta. En este caso, 403 entre 13 es 31 y nos da de resto 0, con lo que $13 \times 31 = 403$ y hemos resuelto el problema.

Nos podemos hacer ahora las mismas preguntas que antes: ¿Cuántas operaciones elementales hemos usado? ¿Cuántas habría que hacer si queremos factorizar un número de n cifras?

Incluso en el caso en que cada división realizada se considere una única operación elemental, el caso peor en el que el número de partida, llamémosle N, sea el cuadrado de un número primo ($N = p^2$), el número de operaciones sería $p = \sqrt{N}$ (ya que el algoritmo anterior requiere dividir N por todos los números hasta encontrar la primera división exacta). De hecho, el número real de operaciones sería aún mayor ya que cada división requiere en realidad de numerosas operaciones elementales.

Para poder comparar con el caso de la multiplicación, vamos a intentar dar el número de operaciones como función del número de cifras n del número N de partida que se quería factorizar. Para ello observamos que un número de n cifras está entre 10^{n-1} y 10^n. Por ejemplo, el número de siete cifras 4325214 está entre $10^6 = 1000000$ y $10^7 = 10000000$.

[1] En realidad la complejidad, siendo de orden n^2, es un poco mayor que $2n^2$, ya que en el análisis no hemos tenido en cuenta las operaciones entre dígitos que requieren "llevadas", como se decía coloquialmente en el colegio.

Por tanto, el número de operaciones para el algoritmo "ir probando" asociado a la factorización tiene complejidad al menos

$$\sqrt{N} \geq \sqrt{10^{n-1}} = 10^{\frac{n-1}{2}}.$$

En este caso, como la n se encuentra en el exponente, se dice que el algoritmo tiene complejidad *exponencial*.

Esto nos permite ya entender el concepto fundamental detrás de la teoría de la complejidad. Lo que se quiere entender es cómo *escala* la complejidad de un algoritmo para resolver un problema en función del tamaño (medido en número de dígitos o, más rigurosamente, en número de bits) de la entrada del problema. También podemos observar dos comportamientos bien distintos en esta dependencia. Puede ser *polinomial*, como en el caso de la multiplicación, o *exponencial*, como en el caso de la factorización.

Tener algoritmos polinomiales o exponenciales lo cambia todo a la hora de resolver instancias grandes. Por ejemplo, con una complejidad $2n^2$ como en el caso de la multiplicación, el número de operaciones elementales necesarias para multiplicar dos números de 161 dígitos es solo 51842. Sin embargo, con una complejidad de $10^{\frac{n-1}{2}}$ como en el algoritmo de factorización considerado, el número de operaciones elementales para factorizar un número de 161 dígitos es 10^{80}, mayor que el número de átomos estimado del Universo.

La siguiente observación es que, a la hora de entender la complejidad de un problema, estamos interesados en la complejidad del mejor algoritmo posible para resolverlo. Por supuesto, si conocemos, como en el caso de la multiplicación, un algoritmo polinomial, entonces podemos afirmar que el problema de la multiplicación tiene complejidad polinomial. A la clase que contiene esos problemas la llamamos P.

La clase de complejidad P captura, por tanto, la clase de problemas que se pueden resolver de forma eficiente con un ordenador, en el sentido de que la cantidad de tiempo requerida para resolver el problema si se aumenta el tamaño de la entrada escala de forma controlada. Naturalmente, esto no quiere decir que cualquier problema en P sea eficientemente resoluble *en la práctica*. Por ejemplo, si el tiempo de ejecución de un algoritmo escala como $n^{10^{1000}}$, siendo n el número de bits de la entrada, aunque el problema es *formalmente* polinomial, el tiempo de ejecución es irrealizable. Incluso para problemas que escalan de forma lineal, al no tener

en cuenta la clase P los posibles prefactores, un tiempo de ejecución que escale como $10^{10^{1000}}n$, aún siendo formalmente lineal, es también irrealizable. En cualquier caso, al menos en primera aproximación, se considera la clase P como el conjunto de problemas eficientemente resolubles con un ordenador.

¿Qué pasa en el caso de la factorización? ¿Podemos afirmar que no está en la clase P?

Pues del análisis anterior no podemos deducir si está en la clase P o no. Lo único que hemos visto es que *el algoritmo concreto* que nos enseñaron en el colegio de "ir probando" tiene complejidad exponencial. Pero podría ocurrir que existiera otro algoritmo que sí que fuera polinomial. Esto se cree que no es cierto, pero no está demostrado. De hecho, la seguridad del algoritmo de cifrado RSA, que es el estándar usado actualmente en básicamente todas las comunicaciones en internet, se basa precisamente en la hipótesis de que el problema de factorización no está en P.

¿Hay entonces alguna forma de capturar el tipo de complejidad asociado al problema de factorización?

La clave es darse cuenta de que, aunque no se sepa si existe un algoritmo polinomial que resuelva el problema, lo que sí existe es un algoritmo polinomial para *verificar* si una solución propuesta es correcta: basta multiplicar (que es polinomial) los factores propuestos como solución y verificar que recuperan el número de partida. Los problemas con esta propiedad conforman la clase de complejidad NP.

Para dar la definición de la clase NP de forma un poco más rigurosa conviene comentar que, normalmente, en teoría de la complejidad se suele trabajar con problemas *de decisión*, es decir, problemas en los que la respuesta es "sí" o "no". Así, un problema de decisión está en NP si, siempre que la respuesta al mismo sea afirmativa, existe un certificado de tamaño polinomial que permite verificarlo en tiempo polinomial. Una manera de convertir el problema de factorización en un problema de decisión en NP sería preguntar si, dados dos números naturales m, n, con $m > n$, existe un divisor propio de m mayor que n. En el caso de que tal divisor exista, ese es precisamente el certificado, pues basta dividir para verificar la solución, lo que requiere un número polinomial de operaciones en el número de dígitos de m.

Obviamente, todo problema en P está también en NP. La pregunta de si P es igual o no a NP ha sido identificada como uno de los problemas matemáticos del milenio [28], con un premio asociado de un millón de dólares. Como he comentado, ni siquiera se sabe si el problema de factorización (que sí está en NP) está en P o no.

La pregunta de si P = NP apareció ya explícitamente en los trabajos de Cook [27] y Levin [67] en los que se define la clase NP, aunque parece ser que ya Gödel era consciente de la importancia de ese problema 15 años antes [94].

Pero la contribución más importante de Cook y Levin fue el descubrimiento de un problema natural *NP-completo*, en el sentido de que el problema P = NP se reduce a ver si ese problema concreto, que está en NP, está también en P. El problema se conoce como SAT y consiste en decidir si existe una asignación de 0s y 1s para una cadena de bits $x_1, \ldots x_n$ que satisface una fórmula booleana dada, en el sentido de que le asigna el valor 1 a esa fórmula.

Una fórmula booleana no es más que una expresión lógica asociada a las variables x_i que usa los conectores $\vee, \wedge, \neg$ ("or", "and", "not"). El conector "or" asigna el valor 1 a $x_1 \vee x_2$ si y solo si x_1 ó x_2 son alguno 1. El conector "and" asigna el valor 1 a $x_1 \wedge x_2$ si y solo si x_1 y x_2 son ambos 1. La operación "not" simplemente cambia el valor del bit de 0 a 1 y viceversa, es decir $\neg 0 = 1$, $\neg 1 = 0$. Por ejemplo la fórmula booleana $(x_1 \vee x_2) \wedge \neg x_3$ se satisface con la asignación $x_1 = 1, x_2 = 0, x_3 = 0$ ya que $(1 \vee 0) \wedge \neg 0 = 1$.

El problema SAT sigue siendo NP-completo aunque restrinjamos el tipo de expresiones lógicas a familias de ternas booleanas unidas por $\wedge$, donde en cada terna aparecen solo tres bits y los conectores $\vee, \neg$. Esta variante del problema SAT se conoce como $3-$SAT. Como el conector $\wedge$ solo da el valor 1 si los bits que conecta tienen ambos el valor 1, satisfacer la fórmula booleana asociada a una instancia del problema $3-$SAT es equivalente a satisfacer *todas* las ternas booleanas unidas por $\wedge$ que contiene la fórmula.

Desde los trabajos fundacionales de Cook y Levin, numerosos problemas dentro de la clase NP han resultado ser NP-completos. Por ejemplo, a los pocos años ya aparecían cientos de ellos en el libro de Gary y Johnson

[44]. Los problemas que no están necesariamente en NP pero que, si estuvieran en P, las clases P y NP serían la misma, se conocen como NP-duros. Es decir, un problema es NP-completo si es NP-duro y está en NP.

Las enormes implicaciones filosóficas de suponer que P = NP hacen creer que ambas clases son distintas. Si fueran iguales, cualquier problema en el que se pudiera verificar eficientemente que una solución es correcta, se podría encontrar esa solución también de forma eficiente. Obviamente, esto significaría que la creatividad puede ser automatizada y que, por ejemplo, desde la perspectiva de las matemáticas, sería esencialmente igual de difícil verificar la demostración de un teorema matemático, algo que cualquier persona con la suficiente dedicación y formación matemática puede hacer, que la genialidad de obtener dicha demostración.

Tal y como ilustra muy bien Scott Aaronson en su blog:

> *Si P=NP, el mundo sería un lugar profundamente distinto de lo que creemos. No habría ningún valor especial en los "saltos creativos", ninguna diferencia notable entre resolver un problema y reconocer una solución una vez se ha encontrado. Cualquiera que pueda apreciar una sinfonía sería Mozart; cualquiera que pudiera seguir un argumento paso a paso sería Gauss; cualquiera que pudiera reconocer una buena estrategia de inversión sería Warren Buffet. Es posible remarcar este punto en términos darwinianos: si este es el tipo de universo que habitamos, ¿por qué no hemos evolucionado todavía para aprovecharnos de ello?*

Por tanto, se pueden catalogar como *problemas difíciles* aquellos que son NP-duros, ya que solo serían eficientemente resolubles en un ordenador en el improbable caso en que P = NP.

Teorema PCP

El Teorema PCP está considerado como uno de los hitos de la teoría de la complejidad. Su demostración original [6], debida a Arora, Lund, Motwani, Sudan y Szegedy, fue simplificada enormemente por Dinur en [32], que presentó esta simplificación como charla plenaria en el Congreso Internacional de Matemáticos (ICM) de 2010.

El nombre del Teorema PCP (*probabilistic checkable proof*) viene de su interpretación como una variante probabilista de NP. He comentado que NP es la clase de problemas para los que existe un certificado que permite verificar la corrección de una respuesta en tiempo polinomial. El Teorema PCP garantiza la propiedad sorprendente de que existen certificados para los que es suficiente chequear una cantidad constante de bits aleatorios para estar seguro, con una probabilidad arbitrariamente cercana a 1, de que la respuesta es correcta. Básicamente, esto prueba que cada teorema matemático tiene una demostración para la que verificar su corrección requiere solo leer unos pocos fragmentos aleatorios de la misma.

Como 3-SAT es un problema NP-completo, parece razonable pensar que exista una versión del Teorema PCP en términos de 3-SAT. En efecto, este es el caso:

Teorema 3.1 (Teorema PCP. Versión 3-SAT)**.** *Dada una instancia del problema 3-SAT, es decir una cantidad polinomial de formulas lógicas involucrando cada una a 3 bits de entre n posibles, salvo que* $\mathrm{P} = \mathrm{NP}$*, no existe un algoritmo polinomial que permita decidir entre las siguientes dos posibilidades, con la promesa de que una de las dos es cierta:*

> **Opción 1.** *Existe una asignación de* $\{0, 1\}$ *a cada bit que permite satisfacer todas las fórmulas.*
>
> **Opción 2.** *Para cada posible asignación de* $\{0, 1\}$ *a cada bit, hay una fracción constante* δ *de fórmulas que no se verifican.*

Básicamente, esta versión del Teorema PCP nos dice, no solo que es NP-duro decidir si existe una asignación $\{0, 1\}$ a cada bit que permite satisfacer todas las fórmulas (que es el problema $3-\mathrm{SAT}$ estándar), sino que sigue siendo NP-duro aunque sepamos que, si ese no es el caso, es porque todas las asignaciones posibles de $\{0, 1\}$ a cada bit fallan estrepitosamente a la hora de satisfacer la función booleana dada (pues fallarán en una fracción constante del número total de fórmulas). Es decir, si en vez de en resolver el problema $3-\mathrm{SAT}$ estuviéramos interesados en maximizar el número de cláusulas que se verifican (lo que se conoce como problema $\mathrm{MAX}-3\mathrm{SAT}$), el Teorema PCP nos dice precisamente que ese problema no es solo difícil de resolver, también es difícil de *aproximar* con cualquier precisión razonable; algo en lo que profundizaremos en breve.

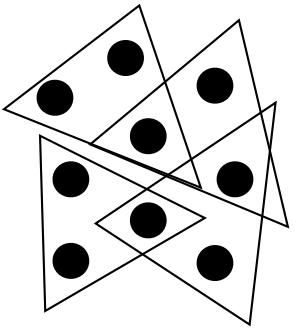

Figura 3.1: El Teorema PCP garantiza que no se puede aproximar a cualquier precisión razonable la energía fundamental de un sistema clásico de espines en los que las interacciones son tripartitas y pueden involucrar a cualquier terna de espines.

Antes de seguir, conviene hacer un breve paréntesis para aquellos con interés en la física, ya que se puede interpretar esta versión del Teorema PCP dentro del contexto de los sistemas (clásicos) de espín de muchos cuerpos. Si asociamos cada fórmula lógica a una interacción clásica entre espines, de forma que la energía de la interacción es 0 si los valores de los bits, que identificamos con los espines, satisfacen la fórmula, y la energía es 1 si no, podemos leer el Teorema PCP como sigue:

En un sistema de n espines en el que consideramos interacciones a tres cuerpos, de manera que cada terna de espines puede interactuar entre sí, es NP-duro decidir si la energía fundamental del sistema es 0 *o es mayor o igual que una constante por el número de interacciones, incluso con la promesa de que una de las dos opciones es cierta.*

La dificultad los juegos no locales

Podemos ya volver a nuestro objetivo de partida, que era entender la dificultad de computar el valor $\omega(G)$ de un juego no local. Para ello, dada una instancia del problema 3-SAT considerado en el Teorema PCP, para el que una de las opciones 1 o 2 es cierta, definimos el siguiente juego no local:

Se le asigna como pregunta a Alice un bit, elegido aleatoriamente entre todos los posibles, y a Bob una cláusula que contiene ese bit, también elegida aleatoriamente entre todas las posibles. Alice tiene que responder una asignación del bit asignado, y Bob una asignación de los tres bits involucrados en la fórmula que se le ha dado. La respuesta se considera correcta si la asignación de Bob satisface la cláusula que se le ha preguntado y si ambos asignan el mismo valor al bit que se ha preguntado a Alice.

Es claro que, si la opción 1 es cierta, la estrategia de responder con la asignación que permite satisfacer todas las fórmulas gana el juego con probabilidad 1. Sin embargo, si la opción 2 es cierta, entonces el valor del juego es como mucho $1 - \frac{\delta}{3}$

Como consecuencia del Teorema PCP obtenemos así esta variante del mismo para juegos no locales

Teorema 3.2 (Teorema PCP. Versión juegos no locales)**.** *Existe un $\delta > 0$ tal que, dado un juego no local G con la promesa de que su valor es $\omega(G) = 1$ o $\omega(G) \leq 1-\delta$, decidir cuál de las dos situaciones es cierta es* NP*-duro. Es decir, salvo que* P = NP*, no existe ningún algoritmo que proporcione la respuesta en un tiempo polinomial en el tamaño del juego, determinado por el cardinal del conjunto de preguntas y respuestas.*

El resultado, además, sigue siendo cierto si todos los pares de preguntas que se hacen se preguntan con la misma probabilidad.

El Teorema PCP se puede amplificar de manera que sea NP-duro incluso decidir si el valor de un juego no local es $= 1$ o arbitrariamente cercano a 0. Esto se deduce de otro de los principales logros en teoría de la complejidad de los últimos años: el teorema de repetición paralela de Raz [91].

Teorema de repetición paralela

Parece intuitivo que si Alice y Bob juegan al mismo juego r veces en paralelo con la exigencia de ganar los r juegos simultáneamente, el valor del juego resultante debería ser $\omega(G)^r$, que sería la probabilidad de ganar los r juegos si se juegan las r partidas de forma independiente con la estrategia óptima para una partida. Sin embargo, uno podría pensar que estrategias más sofisticadas, en las que se utiliza la información de las r preguntas

que se reciben simultáneamente, pueden permitir mejorar la estategia básica de jugar los r juegos de forma independiente. Esto es, de hecho, así y ocurre incluso en un juego tan sencillo como el CHSH [10]. Sin embargo, lo que sí es cierto es que la probabilidad de ganar los r juegos jugados en paralelo decrece exponencialmente a 0, salvo el caso en que $\omega(G) = 1$. Este resultado, altamente no trivial, es lo que se conoce como *Teorema de repetición paralela*, y fue demostrado por primera vez por Raz en 1998 [91]. Aplicado al Teorema PCP se obtiene el siguiente corolario:

Corolario 3.3 (PCP + Repetición paralela)**.** *Para todo $\varepsilon > 0$, dado un juego no local G con la promesa de que su valor es $\omega(G) = 1$ o $\omega(G) < \varepsilon$, es NP-duro decidir cuál de las dos situaciones es cierta.*

Inaproximabiliad en grafos

Una de las implicaciones más importantes del Teorema PCP, y de su versión amplificada, es en la demostración de que muchas de las principales cantidades de interés en teoría de grafos son NP-duras de aproximar a cualquier precisión razonable. Es decir, que salvo que $P = NP$, cualquier algoritmo eficiente que uno diseñe para aproximar dichas cantidades fracasará estrepitosamente en algún grafo.

Un grafo no es más que un conjunto de puntos, llamados vértices, con algunos pares de ellos unidos entre sí por una línea llamada arista. Una estructura tan sencilla engloba, como es normal, una gran diversidad de situaciones y problemas, como pueden ser:

- Una molécula, donde los vértices son los átomos y las aristas los enlaces entre ellos.
- Internet, donde los vértices son las páginas web y las aristas los hipervínculos entre ellas.
- Una red de transporte, donde los vértices son los puntos de entrega y las aristas las carreteras que los unen.
- Una comunidad de personas, donde cada persona es un vértice y las aristas reflejan, por ejemplo, una relación de amistad entre ellas.

No es de extrañar, por tanto, que la teoría de grafos juegue hoy en día un papel central en casi todas las áreas de la ciencia y la ingeniería, como se ilustra muy bien, por ejemplo, en [42].

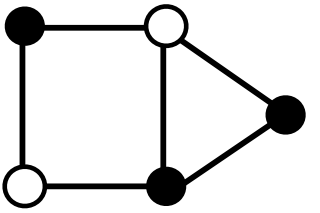

Figura 3.2: En el problema MAX-CUT, uno debe encontrar la manera de bicolorear un grafo que maximice el número de aristas que unen vértices de colores distintos. En este ejemplo, el valor de MAX-CUT es 5 y se consigue con la bicoloración blanco-negro dada en la figura.

El origen de la teoría de grafos [105] se suele situar en el famoso problema de los puentes de Königsberg, resuelto por Euler en 1735. Desde sus orígenes, la teoría de grafos surgió motivada por sus aplicaciones. Por ejemplo, ya en el siglo XIX, Kirchoff la utilizó para el cálculo de corrientes en redes eléctricas. Cayley y Sylvester, por su parte, utilizaron la teoría de grafos en el problema de enumerar todos los posibles isómeros de los alcanos. Por ejemplo, Cayley mostró en 1875 que hay 802 isómeros diferentes de la parafina $C_{13}H_{28}$.

Dependiendo del problema de interés, son distintas las propiedades de los grafos en que uno puede estar interesado. Por ejemplo, si el grafo representa una red de comunicaciones, la robustez de la red a fallos o ataques malintencionados estará dada por el mínimo número de aristas que, al ser eliminadas, hacen el grafo resultante disconexo. A este número se le conoce como MIN-CUT.

Uno puede considerar también el problema opuesto, MAX-CUT, de encontrar la manera de asignar un color, blanco o negro, a cada vértice del grafo, de forma que se maximice el número de aristas que unen un vértice blanco con uno negro. Este problema aparece de forma natural, por ejemplo, en el diseño de los chips que usan los ordenadores [9].

Uno puede también reenfocar este problema y preguntarse cuál es el menor número de colores que se necesitan para asignar a cada vértice del grafo un color de manera que las aristas solo unan vértices de colores distintos. El famoso teorema de los cuatro colores [4] establece que bastan

cuatro colores para colorear un grafo planar, es decir, aquel que puede ponerse en el plano sin que las aristas se corten. Interpretando los vértices como países en un mapa y las aristas uniendo países vecinos, este teorema prueba que se puede colorear cualquier mapa solo con cuatro colores.

La historia de este teorema es muy interesante [105]. La primera mención al problema aparece en una carta de De Morgan a Hamilton en 1852. Al parecer, la pregunta surgió de uno de sus estudiantes, Frederick Guthrie, que a su vez la atribuye a su hermano Francis. Aparece publicada por primera vez en la revista *The Athenaeum* en 1854. Tras numerosos artículos realizando progresos parciales en el problema, así como varias soluciones incorrectas, el problema fue resuelto en 1976 por Appel y Haken con una demostración asistida por ordenador.

Encontrar el *número cromático* de un grafo, es decir, el menor número de colores necesario para colorearlo en el sentido anterior, tiene aplicaciones en problemas de optimización de recursos con algún tipo de incompatibilidad [42]. Por ejemplo, si se quiere almacenar una serie de compuestos químicos de manera que, por seguridad, algunos pares de ellos no pueden estar en la misma habitación, ¿cuántas habitaciones serán necesarias para almacenarlos? Si uno considera el grafo que tiene por vértices los distintos compuestos y las aristas unen compuestos incompatibles, la solución al problema es precisamente el número cromático del grafo, donde cada color ahora corresponde a una habitación distinta.

El mismo tipo de problema surge, por ejemplo, si se quieren asignar los distintos aviones de una compañía aérea a los distintos vuelos que esta opera, donde por horario o localización, claramente algunos vuelos son incompatibles para un mismo avión.

Otra propiedad de interés en un grafo es entender sus *cliques*. Un clique es un subgrafo completo, es decir, una colección de vértices dentro del grafo que están todos unidos entre sí. Es de particular interés el tamaño del mayor clique dentro de un grafo, lo que se conoce como el problema MAX-CLIQUE. Esto es especialmente interesante en sociología, donde los vértices representan personas y las aristas relaciones entre ellas. Un clique es una comunidad de personas en la que todos están relacionados entre sí. La importancia de este concepto en sociología ya aparece en los trabajos pioneros de Festinger, Forsyth y Katz, a finales de los años 40 [38, 41].

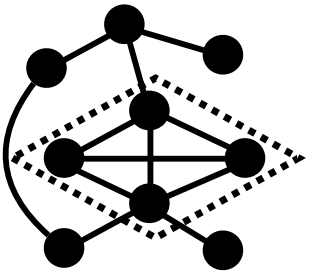

Figura 3.3: El problema MAX-CLIQUE consiste en determinar el tamaño del mayor subgrafo completo contenido en un grafo dado. En el ejemplo de la figura este valor sería 4.

Numerosas propiedades de los grafos, como es el caso de MAX-CUT, MAX-CLIQUE o el número cromático, son cantidades que, salvo que P=NP, no se pueden computar en tiempo polinomial. Una excepción es el caso de MIN-CUT, que sí que tiene un algoritmo polinomial [40].

Como consecuencia del Teorema PCP se tiene que, de hecho, tanto MAX-CUT, como MAX-CLIQUE o el número cromático, así como otras muchas propiedades de un grafo, son NP-duras *de aproximar*.

Por ejemplo, Feige y Kilian [37], mejorando un resultado anterior de Lund y Yannnakakis [72], probaron en 1996 que, salvo que P=NP, para cualquier $\varepsilon > 0$ y para cualquier algoritmo polinomial para determinar el número cromático de un grafo, existe un grafo de n vértices tal que el cociente entre la salida del algoritmo y el número cromático real del grafo es mayor que $n^{1-\varepsilon}$. Es importante notar que el mayor número cromático posible para un grafo es n, con lo que el algoritmo fallaría casi tanto como es posible. Poco después, Håstad demostró en 1999 [49] que el mismo resultado es cierto para MAX-CLIQUE. Ambos resultados se deducen, aunque de forma no trivial, del Teorema PCP (recuerdo que el Teorema PCP probaba precisamente la dificultad de dar una solución aproximada del problema MAX $-$ 3SAT).

Una manera sencilla de ilustrar la conexión entre el Teorema PCP en su versión para juegos no locales y las propiedades de un grafo, como por ejemplo el número cromático, es vía el problema conocido como LABEL-

COVER. En este problema, dado un grafo, un número fijo de colores y un conjunto de pares de colores válidos para cada arista, el objetivo es determinar una coloración de los vértices del grafo de manera que se maximice el número de aristas para las que la coloración dada es válida.

Dado un juego no local, se puede construir un grafo asociado de la siguiente manera. Hay dos tipos de vértices, los de Alice y los de Bob. Las aristas son los pares de preguntas posibles. El grafo resultante es, por tanto, bipartito (es decir, 2-coloreable): si coloreamos los vértices asociados a Alice de blanco y los de Bob de negro, todas las aristas unen un vértice blanco con uno negro. Los colores posibles del problema LABEL-COVER asociado van a ser las respuestas posibles, y las coloraciones válidas para cada arista (x, y) son precisamente los pares de respuestas ganadoras (a, b), es decir, tales que $V(a, b, x, y) = 1$. Es claro que, si todas las preguntas se hacen con la misma probabilidad, el valor del juego es exactamente la máxima fracción de aristas con una coloración válida que se pueden conseguir al colorear los vértices del grafo.

El Teorema PCP muestra, por tanto, que es NP-duro distinguir el caso en el que todas las aristas se puede verificar del caso en el que solo es posible hacerlo para una pequeña fracción de las mismas.

El problema MAX-CUT se comporta, sin embargo, de manera un poco distinta. Es de hecho NP-duro dar una aproximación con un error relativo menor que una cierta constante [50]. Sin embargo, existe un algoritmo eficiente, debido a Goemans y Williamson [46], que devuelve para cada grafo un valor $\alpha(G) \geq \text{MAX} - \text{CUT}(G)$ tal que

$$\min_{G} \frac{\text{MAX} - \text{CUT(G)}}{\alpha(G)} \geq \min_{0 \leq \theta \leq \pi} \frac{2}{\pi} \frac{\theta}{1 - \cos\theta} > 0{,}87856.$$

4. TODO EMPEZÓ CON EINSTEIN, COMO TANTAS OTRAS COSAS

He empezado hablando de los juegos no locales desde la perspectiva de la teoría de la complejidad, donde aparecieron bajo el nombre de *sistemas de demostración interactiva multiparte (multipartite interactive proof systems)* a finales de los años 80, gracias al trabajo pionero de Ben-Or, Goldwasser, Kilian y Wigderson [13]. Sin embargo, históricamente, su origen se debe a la física cuántica y, en concreto, al famoso artículo de Einstein, Podolsky y Rosen de 1935 "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?"[35]. Básicamente, Einstein, Podolsky y Rosen se dieron cuenta de que la mecánica cuántica era incompatible con el hecho de que las cantidades observadas estuvieran definidas de antemano y que, por tanto, pudieran interpretarse como "elementos de realidad". En física cuántica, el valor de una cantidad (la orientación del espín de un electrón, la dirección de polarización de la luz de un láser, la dirección de giro de la corriente en un superconductor, ...), no está definida de antemano, sino que se define, de forma probabilista, al observarla.

Esta observación, y el correspondiente debate filosófico, volvió al terreno de la ciencia cuando John Bell, en 1964, se dio cuenta de que había un experimento (en aquel momento no realizable todavía) que permitiría resolver el debate de forma concluyente [12].

El experimento propuesto no era más que un juego no local en el que, usando estregias cuánticas, se podría obtener una probabilidad de ganar estrictamente mayor que con la mejor estrategia clásica posible. Es decir, existen juegos para los que el valor cuántico $\omega^*(G)$ es estrictamente más grande que el valor clásico $\omega(G)$ considerado hasta ahora. De ahí que, en este contexto, a los juegos no locales se les conozca como *desigualdades de Bell*. La desigualdad viene de la cota $\omega(G)$ que el juego impone a la mejor estrategia clásica posible. Una estrategia cuántica con probabilidad de ganar mayor que $\omega(G)$ se llama, por tanto, una *violación* de la desigualdad de Bell. En el contexto de las desigualdades de Bell se suelen considerar, de hecho, *juegos generalizados* en los que la función de verificación $V(a, b, x, y)$ puede tomar valores reales que, en el contexto del juego de partida, uno puede interpretar como el premio en euros que los concursantes ganarán si contestan las respuestas a, b a las preguntas x, y.

Esta idea fue refinada cinco años después por Clauser, Horne, Shimony y Holt en su artículo "Proposed experiment to test local hidden-variable theories"[25], donde propusieron el juego CHSH que he descrito al principio de mi intervención. En ese juego el valor clásico es $\frac{3}{4}$, mientras que el valor cuántico es $\cos^2\left(\frac{\pi}{8}\right) \approx 0{,}85$.

Para poder explicar estas ideas, necesito comentar algunas nociones básicas sobre física cuántica que, por simplicidad, consideraré solo en dimensión finita.

Una propiedad de un sistema físico, como el espín de un electrón, viene dada por un espacio vectorial complejo, llamado *espacio de estados del sistema*, que se puede identificar, para un cierto n, con $\mathbb{C}^n$, es decir, el conjunto de todas las n-tuplas $(x_1, x_2, \ldots, x_n)$ de números complejos. La base canónica, que en general se denota por

$$|1\rangle = (1, 0, \ldots, 0) \ , \quad |2\rangle = (0, 1, \ldots, 0) \ , \ldots \ , \quad |n\rangle = (0, 0, \ldots, 1) \ ,$$

se corresponde con las posiciones básicas distinguibles de esa propiedad. Por ejemplo, en el caso del espín del electrón, el espacio sería $\mathbb{C}^2$ y la base vendría dada por la orientación hacia arriba $|\uparrow\rangle$ y la orientación hacia abajo $|\downarrow\rangle$, que se corresponderían, respectivamente, con los vectores

$$|\uparrow\rangle = (1, 0) \ , \quad |\downarrow\rangle = (0, 1) \, .$$

El *estado del sistema*, que codifica toda la información que se puede obtener del mismo, es un operador lineal, semidefinido positivo y de traza 1, que actúa en el espacio de estados del sistema ($\mathbb{C}^2$ en el caso del espín). El estado se llama puro si es un proyector de rango 1, definido por tanto por un vector normalizado (con la norma euclídea) del espacio. Un ejemplo sería el estado definido por el vector $|+\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$, que se correspondería [1] con la matriz (semidefinida positiva y de traza 1) dada por

$$\rho_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} .$$

Si se considera el vector $|-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$, el estado asociado vendría dado por la matriz

$$\rho_- = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} .$$

[1] Los operadores lineales T actuando en $\mathbb{C}^d$ se corresponden con las matrices A de tamaño $n \times n$, de manera que la acción de T en un vector de $\mathbb{C}^d$ no es más que la multiplicación de A por ese vector.

Para obtener información sobre la propiedad física en cuestión (por ejemplo el espín), se necesita medir el sistema. La medida más general posible, llamada POVM por sus siglas en inglés (positive operator-valued measure), viene dada por una colección de operadores lineales semidefinidos positivos $\{E_a\}_a$ actuando en el espacio de estados del sistema e indexados por el número de resultados posibles en la medida, con la condición de que $\sum_a E_a$ es el operador identidad $\mathbb{1}$.

La probabilidad de obtener el resultado a al medir el estado ρ viene dada por la regla de Born

$$p(a) = \mathrm{tr}(\rho E_a).$$

La magia de la física cuántica emerge cuando se tiene un sistema compuesto, por ejemplo, por los espines de dos electrones distintos. En este caso, el espacio del sistema estaría generado por todas las configuraciones distinguibles, que serían $\uparrow\uparrow, \uparrow\downarrow, \downarrow\uparrow, \downarrow\downarrow$. La noción matemática asociada es el producto tensorial que, a partir de dos copias del espacio $\mathbb{C}^n$, construye el espacio $\mathbb{C}^n \otimes \mathbb{C}^n$. Este espacio tiene por base *canónica* precisamente todas las posibilidades $|i\rangle \otimes |j\rangle$ con $i, j \in \{1, \dots n\}$ y, por tanto, es isomorfo a $\mathbb{C}^{n^2}$ (el producto tensorial multiplica las dimensiones). Por simplicidad en la notación, $|ij\rangle$ denotará $|i\rangle \otimes |j\rangle$.

La clave del producto tensorial es que existen vectores *entrelazados*, como por ejemplo el vector

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle \right),$$

en el espacio asociado a dos espines, que define el estado puro ρ_{EPR}. Un vector está entrelazado si no se puede escribir como un vector producto de la forma $v \otimes w$. [2]

Con estas breves indicaciones podemos pensar ya cómo podrían Alice y Bob usar la física cuántica para mejorar su probabilidad de ganar el juego que les plantean. Mientras están juntos en la habitación antes del juego, pueden generar un estado entrelazado ρ formado por dos sistemas, como por ejemplo el estado ρ_{EPR} asociado al espín de dos electrones, de forma que, al separarse en distintas habitaciones, cada uno de ellos se queda con

[2] La expresión del vector $v \otimes w$ en la base canónica $|ij\rangle$ viene unívocamente determinada por el hecho de que el operador $(v, w) \mapsto v \otimes w$ de $\mathbb{C}^n \times \mathbb{C}^n$ en $\mathbb{C}^n \otimes \mathbb{C}^n$ es bilineal.

uno de los dos subsistemas del sistema compuesto. Por ejemplo, cada uno podría llevarse uno de los dos electrones. Cuando reciben las preguntas x, y deciden implementar, en función de la pregunta, una medida, E_a^x para el caso de Alice y F_b^y para el caso de Bob, y dar como respuesta el resultado de dicha medida.

Por lo comentado anteriormente, la estrategia asociada $p(ab|xy)$ vendría dada por la fórmula

$$p(ab|xy) = \mathrm{tr}\left(\rho \left[E_a^x \otimes F_b^y\right]\right),$$

con lo que se puede definir el valor cuántico del juego $\omega^*(G)$ como la mayor probabilidad de ganar el juego G utilizando estrategias cuánticas de este tipo.

Es importante resaltar que estas estrategias cuánticas incluyen como caso particular a (pero son más generales que) las estrategias clásicas descritas al principio del discurso, es decir, aquellas que son de la forma:

$$p(ab|xy) = \sum_{\lambda} q(\lambda) p_A(a|x\lambda) p_B(b|y\lambda)$$

y que, en el contexto de las desigualdades de Bell, se conocen como *modelos de variables ocultas*.

En el caso del juego CHSH, por ejemplo, la estrategia cuántica óptima consiste en que Alice y Bob compartan el estado ρ_{EPR} y midan con los operadores de medida siguientes:

1. Si Alice recibe la pregunta $x = 0$, medirá con los operadores E_0^0, E_1^0 dados, respectivamente, por los proyectores en los vectores $|\uparrow\rangle$ y $|\downarrow\rangle$.

2. Si Alice recibe la pregunta $x = 1$, los operadores E_0^1, E_1^1 serán los proyectores en los vectores $|+\rangle$ y $|-\rangle$.

3. Si Bob recibe la pregunta $y = 0$, F_0^0, F_1^0 vendrán dados por los proyectores en los vectores $\cos\left(\frac{\pi}{8}\right)|\uparrow\rangle + \sin\left(\frac{\pi}{8}\right)|\downarrow\rangle$, en el caso de F_0^0, y $-\sin\left(\frac{\pi}{8}\right)|\uparrow\rangle + \cos\left(\frac{\pi}{8}\right)|\downarrow\rangle$, en el caso de F_1^0.

4. Por último, si Bob recibe la pregunta $y = 0$, F_0^1, F_1^1 serán los proyectores en los vectores $\cos\left(\frac{\pi}{8}\right)|\uparrow\rangle - \sin\left(\frac{\pi}{8}\right)|\downarrow\rangle$, en el caso de F_0^1, y $\sin\left(\frac{\pi}{8}\right)|\uparrow\rangle + \cos\left(\frac{\pi}{8}\right)|\downarrow\rangle$, en el caso de F_1^1.

Es un sencillo ejercicio ver que la probabilidad de éxito con esta estrategia es precisamente $\cos^2\left(\frac{\pi}{8}\right) \approx 0{,}85$.

La demostración de la optimalidad de esta estrategia es debida a Tsirelson [99], en lo que se conoce como *cota de Tsirelson*.

La idea subyacente a este fenónemo es ciertamente rompedora: si una estrategia cuántica permite ganar un juego no local (pongamos el CHSH) con una probabilidad mayor que la que permite la física clásica, entonces podemos concluir que, por un lado, los resultados de las medidas hechas por Alice y Bob están correlacionados y, por otro lado, que dichos resultados no estaban definidos de antemano, sino que se determinan probabilísticamente al hacer la medición.

Esto es, de alguna manera, el sueño de un criptógrafo: la garantía de correlaciones sin comunicación que se generan exactamente en el instante deseado. No es de extrañar que, ya en 1991, Artur Ekert propusiera en [36] esta idea para distribuir claves secretas que luego puedan ser utilizadas para comunicar información de forma segura mediante, por ejemplo, el "cuaderno de uso único".

La idea es aún más sorprendente puesto que no requiere fiarse de quien te provee de los equipos cuánticos necesarios para el protocolo, ni siquiera conocer los detalles internos de los aparatos, ya que la única información relevante son los resultados que los aparatos proporcionan (salidas a, b) a distintas configuraciones externamente controladas de los mismos (x, y). A esto se le conoce hoy en día como "criptografía cuántica independiente del dispositivo".

La clave para que esta idea funcione en la práctica es poder saber, solo a partir de la probabilidad de ganar un juego, qué es exactamente lo que hacen los aparatos cuánticos que están usando Alice y Bob para jugar; de los que no podemos asumir nada más que el conocimiento aproximado de la distribución de probabilidad $p(ab|xy)$ que generan.

Por tanto, es crucial que, de alguna manera, la distribución de probabilidad $p(ab|xy)$ o, mejor aún, la probabilidad de ganar un juego no local, determine la estructura cuántica interna de los dispositivos utilizados en el juego. Esta propiedad, conocida como rigidez o *self-testing*, la tiene, de hecho, el juego CHSH.

Primero Summers y Werner [97] para el caso exacto, y luego McKague, Yang y Scarani para el aproximado [77], probaron que si uno genera una estrategia cuántica que proporciona, para el juego CHSH, un valor ε-cercano a $\cos^2\left(\frac{\pi}{8}\right)$ es porque, salvo isometrías, han usado un estado cuántico y unas medidas $\sqrt{\varepsilon}$-cercanas a las que he explicitado anteriormente.

Recientemente se ha visto [103] cómo estas propiedades de rigidez se pueden deducir de un teorema de Gowers y Hatami [47] sobre representaciones aproximadas de grupos, que mejora a su vez un resultado clásico de Kazhdan [59].

La primera demostración completa de que es posible el intercambio de clave independiente del dispositivo fue debida a Vazirani y Vidick en [102], utilizando para ello un análisis muy sofisticado de la rigidez aproximada del juego CHSH. Esto fue mejorado posteriormente por Arnon-Friedman, Renner y Vidick [5], con una demostración basada en un teorema de acumulación de entropía de Renner, Dupuis y Fawzi [32].

Mención aparte merece la parte *experimental*. Al margen de las aplicaciones criptográficas, incluso únicamente para refutar la crítica de Einstein, Podolsky y Rosen y validar las predicciones de la física cuántica, es necesario poder garantizar la independencia causal de Alice y Bob. Hace falta, por tanto, que ambos estén suficientemente separados y que la distribución de estados entrelazados entre ellos se haga mediante fotones. El problema es que esto introduce el problema del ruido: con cierta probabilidad los fotones se pierden en el camino, o no hacen *click* en el detector correspondiente.

A pesar del éxito de los primeros experimentos de Aspect, Dalibard, Grangier y Roger [7, 8, 6] en los años 80, solo en 2015 [51] se ha conseguido finalmente cerrar lo que se conocía como el *detection loophole*, que era básicamente la posibilidad de que precisamente los fotones no detectados fueran responsables de una posible explicación clásica del resultado de los experimentos. Este hito, debido al grupo de Hanson en Delft, se ha reproducido después, incluso con mayor fiabilidad, en otros grupos de investigación [45, 93], zanjando por fin la crítica de Einstein, Podolsky y Rosen casi 100 años después.

Es natural preguntarse, por tanto, cuál es el ruido que soporta una distribución de probabilidad $P = p(ab|xy)$ antes de pasar a tener una explicación clásica. Para ello se define un parámetro $\pi(P)$ de tolerancia al

ruido como el ínfimo de los valores λ tales que la distribución $\lambda P + (1 - \lambda)P'$ no es clásica para cualquier P' clásica. Es decir, cuanto más próximo esté $\pi(P)$ a 0, más robusto es el contenido cuántico de la distribución de probabilidad P.

En [58] nosotros logramos probar que

$$\pi(P) = \frac{2}{\nu(P) + 1},$$

donde $\nu(P)$ es el mayor ratio posible entre la probabilidad de ganar un juego no local generalizado con la estrategia dada por P y su valor clásico. De ahí que interese encontrar ratios $\frac{\omega^*(G)}{\omega(G)}$ tan grandes como sea posible.

¿Cómo de grande puede llegar a ser este ratio en función del número de preguntas y respuestas?

Para responder a esta pregunta necesitaremos del análisis funcional.

5. ANÁLISIS FUNCIONAL PARA JUEGOS NO LOCALES

Mucho antes de que los juegos no locales aparecieran en el contexto de la complejidad computacional, e incluso antes de los trabajos fundacionales de Bell en física cuántica, se inició el estudio, dentro del análisis funcional, de lo que hoy se conoce como teoría local de los espacios de Banach.

Los espacios de Banach surgieron en la tesis de Banach en 1920 como abstracción de numerosos espacios infinito dimensionales de funciones y sucesiones estudiados anteriormente por Frechet, Hilbert, Lebesgue o Riesz, y que son conjuntos naturales en los que buscar soluciones de ecuaciones diferenciales e integrales. Los trabajos de Bombal [15] o Pietsch [86] son referencias obligadas sobre el origen de esta teoría. En la introducción de la tesis de Banach puede leerse:

> *El objetivo de este trabajo es demostrar algunos teoremas que son ciertos para diferentes espacios funcionales (champs fonctionneles). En lugar de probar los resultados para cada espacio funcional particular, he optado por un enfoque diferente: considero en general un conjunto de elementos abstractos, para los que postulo una serie de propiedades y demuestro los teoremas para esos conjuntos. Entonces pruebo que los distintos espacios funcionales particulares en los que estoy interesado satisfacen los axiomas postulados ...*

Desde su origen, por tanto, el análisis funcional se ha ocupado del estudio de espacios vectoriales de dimensión infinita. Sin embargo, el genio de Grothendieck en su "Résumé de la théorie métrique des produits tensoriels topologiques", publicado en 1956 [48], se dio cuenta de que muchas de las propiedades de los espacios de dimensión infinita dependían solo del comportamiento de sus subespacios de dimensión finita. Este enfoque, que se reduce a dar estimaciones y desigualdades asintóticas en la dimensión sobre espacios de dimensión finita, es lo que se conoce como *teoría local de los espacios de Banach*. Citando a Lindenstrauss y Milman [69]:

> *El nombre 'Teoría Local' se aplica a dos temas ligeramente distintos:*

(a) El estudio cuantitativo, cuando $n \to \infty$, de los espacios normados n–dimensionales.

(b) La relación de la estructura de un espacio infinito-dimensional con sus subespacios de dimensión finita.

Un espacio normado de dimensión finita no es más que $\mathbb{C}^n$ (o $\mathbb{R}^n$ si los coeficientes del vector son reales en vez de complejos) en el que se considera una noción de *longitud de un vector*, llamada norma, con buenas propiedades. Por ejemplo, se puede considerar la norma

$$\|(x_1, \ldots, x_n)\|_1 = |x_1| + |x_2| + \cdots + |x_n| \ ,$$

o la norma

$$\|(x_1, \ldots, x_n)\|_\infty = \text{máx}\{|x_1|, |x_2|, \ldots, |x_n|\} \ ,$$

o, por supuesto, la norma euclídea ya considerada antes

$$\|(x_1, \ldots, x_n)\|_2 = \sqrt{|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2}.$$

Cuando se quieren considerar esas normas en concreto, en vez de escribir $\mathbb{C}^n$ (o $\mathbb{R}^n$), se escribe, respectivamente, ℓ_1^n, ℓ_∞^n y ℓ_2^n.

Obviamente, un mismo vector puede tener longitudes distintas dependiendo de qué norma se use para medir su longitud. Así, el vector $(1, 1, 1)$ en $\mathbb{R}^3$ tiene longitud 3, 1 y $\sqrt{3}$, respectivamente, al considerar las normas $\|\cdot\|_1$, $\|\cdot\|_\infty$ y $\|\cdot\|_2$.

En espacios vectoriales de matrices $(x_{i,j})_{i,j=1}^n$, uno puede considerar también *mezclas* de estas normas, como por ejemplo

$$\max_i \sum_j |x_{i,j}| \quad \text{ó} \quad \sum_i \max_j |x_{i,j}|.$$

Los espacios asociados se denotan, respectivamente, por $\ell_\infty^n(\ell_1^n)$ y $\ell_1^n(\ell_\infty^n)$.

Asociado a cada espacio normado X de dimensión finita, se puede asignar su dual X^* como el mismo espacio base $\mathbb{C}^n$ con la norma definida por

$$\|(\phi_1, \phi_2, \ldots, \phi_n)\|_{X^*} = \max \left| \sum_{i=1}^n \phi_i x_i \right| \ ,$$

donde el máximo se toma entre todos los vectores $(x_1, x_2, \ldots, x_n)$ tales que $\|(x_1, x_2, \ldots, x_n)\|_X \leq 1$. Es muy fácil ver que $(X^*)^* = X$.

En los ejemplos anteriores, se verifica de forma muy sencilla que $(\ell_1^n)^* = \ell_\infty^n$, y por tanto $(\ell_\infty^n)^* = \ell_1^n$, y también que $(\ell_2^n)^* = \ell_2^n$. Para los espacios mezcla introducidos antes, se tiene también la dualidad

$$(\ell_\infty^n(\ell_1^n))^* = \ell_1^n(\ell_\infty^n).$$

De hecho, la definición de dual puede verse como el caso particular, para $Y = \mathbb{C}$, de la definición de norma para una aplicación lineal cualquiera $T : X \to Y$ entre dos espacios normados X e Y:

$$\|T\| = \max_{\|x\| \leq 1} \|T(x)\|_Y = \max_{x \neq 0} \frac{\|T(x)\|_Y}{\|x\|_X} \ .$$

Ya desde el *Résumé* de Grothendieck, la teoría local de los espacios de Banach ha estado ligada a la noción de norma tensorial que, por dualidad, no es más que una manera de definir clases de operadores lineales entre espacios de Banach.

En pocas palabras, una norma tensorial se puede entender como una forma de asignar, para cada par de normas $\|\cdot\|_\alpha$, $\|\cdot\|_\beta$ en el espacio $\mathbb{C}^n$, una extensión de ambas al espacio $\mathbb{C}^n \otimes \mathbb{C}^n$ que sea compatible con la estructura de producto tensorial (por ejemplo $\|v \otimes w\|$ debe ser igual a $\|v\|_\alpha \|w\|_\beta$).

La riqueza y potencia de esta idea pasó muchos años desapercibida, hasta que fue redescubierta por Pietsch, Lindenstrauss y Pelckzynski a finales de los años 60 [85, 70]. El excelente libro "Tensor norms and operator ideals"de Defant y Floret [30], ya en los años 90, ilustra de manera magistral cuán rica y potente es, en efecto, esa idea.

Especialmente relevante es el resultado que Grothendieck llamó *El teorema fundamental de la teoría métrica de los productos tensoriales*, reinterpretado por Lindenstrauus y Pelckzynski en 1968 [70] como un resultado sobre la mejora en la sumabilidad de series que se obtiene de aplicar una transformación lineal y continua entre determinados espacios funcionales. La importancia y el impacto de este resultado está todavía descubriéndose, tal y como se ilustra muy bien en el artículo de Pisier "Grothendieck's theorem: past and present"[88].

Para enunciar el Teorema de Grothendieck hace falta introducir la norma tensorial ε, que es la menor norma tensorial posible y, que por simplicidad, definiré solo en el caso finito dimensional:

Definición 5.1. *Dados k espacios normados de dimensión finita $X_1, \ldots, X_k$ y un elemento $x = \sum_i x_i^1 \otimes \cdots \otimes x_i^k \in X_1 \otimes \cdots \otimes X_k$, se define*

$$\varepsilon(x) = \sup |(\phi_1 \otimes \cdots \otimes \phi_k)(x)|$$

donde el supremo se toma en todos los ϕ_i de norma 1 del espacio dual X_i^* y

$$(\phi_1 \otimes \cdots \otimes \phi_k)(x) = \sum_i \phi_1(x_i^1) \cdots \phi_k(x_i^k)$$

No es difícil ver, por convexidad, que si consideramos el espacio ℓ_1^n (por simplicidad en el caso particular de coeficientes reales), un elemento $A \in \ell_1^n \otimes \ell_1^n$ se puede identificar con una matriz $A = (A_{i,j})_{i,j=1}^n$ (también de coeficientes reales) de forma que su norma ε viene dada por la expresión

$$\varepsilon(A) = \text{máx} \left\{ \sum_{i,j} A_{i,j}\ s_i t_j : s_i, t_j \in \{+1, -1\} \right\} . \tag{5.1}$$

El Teorema de Grothendieck establece que existe una constante universal, llamada constante de Grothendieck K_G, tal que la expresión (5.1) multiplicada por K_G acota superiormente a

$$\sup \left\{ \sum_{i,j} A_{i,j}\ v_i \cdot w_j \right\} , \tag{5.2}$$

donde v_i, w_j son vectores en el espacio ℓ_2^N para una dimensión N arbitraria y $v \cdot w$ denota el producto escalar usual de vectores: $v \cdot w = \sum_{k=1}^N v_k\, w_k$.

Esta última expresión (5.2) es, de hecho, el valor de otra norma tensorial, llamada γ_2^*, en la matriz A.

En pocas palabras, el Teorema de Grothendieck establece que $\varepsilon \leq \gamma_2^* \leq K_G\, \varepsilon$ en $\ell_1^n \otimes \ell_1^n$.

Normas tensoriales y juegos no locales

He comentado ya que hay una conexión muy estrecha entre los juegos no locales y la teoría de grafos. Antes de pasar a conectar de forma directa los juegos no locales y las normas tensoriales, es interesante remarcar que,

de hecho, algunos de los principales problemas NP-duros en teoría de grafos se pueden reformular como el cómputo de una determinada norma tensorial en un cierto espacio de dimensión finita.

Por ejemplo, se puede ver en [52] cómo, utilizando una reducción previa de Motzkin y Straus a una norma tensorial *simétrica* [39] (de las que, para evitar extender más aún este discurso, no hablaré), el problema MAX-CLIQUE se puede reducir a computar la norma ε de un cierto tensor $(T_{i,j,k})_{i,j,k=1}^{n}$ en el espacio $\ell_2^n \otimes \ell_2^n \otimes \ell_2^n$.

Otro ejemplo es el caso de MAX-CUT. Alon y Naor se dieron cuenta en 2004 [2] de que, dado un grafo G, se puede construir una matriz $(A_{i,j})_{i,j=1}^{n}$ tal que el MAX-CUT de G se reduce a calcular la norma de la matriz A en el espacio $\ell_1^n \otimes_\varepsilon \ell_1^n$. Por el teorema de Grothendieck, este valor se puede aproximar, salvo la constante de Grothendieck K_G, por el valor de la norma γ_2^* de A que, de hecho, se reduce a un problema de programación semidefinida, para los que existen algoritmos de complejidad polinomial. De hecho, el algoritmo de Goemans y Williamson ya comentado [46] se puede ver como una versión sencilla de la demostración de Krivine [65] del Teorema de Grothendieck para una clase muy particular de matrices $(A_{i,j})_{i,j=1}^{n}$. El teorema de Grothendieck va mucho más allá y se aplica para dar aproximaciones eficientes, como problemas de programación semidefinida, a cualquier problema cuadrático del tipo de la ecuación (5.1) [2].

De esta manera, 50 años después de su formulación inicial, se puede interpretar ahora el Teorema de Grothendieck como una aproximación eficiente con error multiplicativo K_G al problema de aproximar el MAX-CUT de un grafo y generalizaciones de ese problema. De hecho, gracias al trabajo de Raghavendra y Steurer [90], se sabe, si la *Unique Games Conjecture* es cierta y salvo que P sea igual a NP, que no puede haber una aproximación eficiente mejor para el problema de optimización (5.1). Se sabe también que, bajo esas hipótesis, la aproximación de Goemans y Williamson para MAX-CUT es óptima [63].

La Unique Games Conjecture está considerada una de las conjeturas principales en teoría de la complejidad [62]. Su formulación e implicaciones le valieron a Khot el premio Nevanlinna en el Congreso Internacional de Matemáticos (ICM) de 2014. La conjetura establece que un resultado

similar al Teorema PCP es cierto para una subfamilia concreta de juegos, llamados *unique games*, caracterizados por tener, para cada respuesta posible de Alice, una única respuesta ganadora posible de Bob, y viceversa.

Paso ya a conectar el valor de un juego no local con normas tensoriales. Esta conexión surgió de una colaboración con Junge, Palazuelos, Wolf y Villanueva al poco tiempo de acabar mi tesis doctoral, que dio como fruto los trabajos [84, 58, 57], que recogen buena parte de las ideas que voy a contar a continuación. Las cotas obtenidas en esos trabajos fueron luego mejoradas notablemente en un trabajo posterior de Junge y Palazuelos [56] utilizando el mismo tipo de herramientas.

Para conectar los juegos no locales con las normas tensoriales, hay que recordar primero lo que ya comenté al principio del discurso: que, de entre las estrategias clásicas, siempre existe una estrategia óptima que es de tipo producto, es decir, de la forma $p(ab|xy) = p_A(a|x)p_B(b|y)$.

Es importante notar ahora que $p_A(a|x)$, y análogamente $p_B(b|y)$, se puede ver como una matriz $(A_{x,a})_{x,a}$ en los índices x, a, que en el espacio $\ell_\infty^n(\ell_1^n)$ tiene norma

$$\|(A_{x,a})_{x,a}\| = \max_x \sum_a A_{x,a} = \max_x \sum_a p_A(a|x) = 1.$$

(Por simplicidad he asumido que el número de preguntas y respuestas posibles es el mismo, al que he denotado por n).

Por tanto, utilizando que los espacios $\ell_\infty^n(\ell_1^n)$ y $\ell_1^n(\ell_\infty^n)$ son duales entre sí, y definiendo a partir del juego el tensor

$$\left(G_{(x,a),(y,b)}\right)_{(x,a),(y,b)} \in \ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$$

dado por $G_{(x,a),(y,b)} = \pi(x,y)V(a,b,x,y)$, se tiene que el valor clásico del juego no es más que [57, 81]

$$\begin{aligned}\omega(G) &= \max_{p_A(a|x),p_B(b|y)} \sum_{a,b,x,y} p_A(a|x)p_B(b|y)\pi(x,y)V(a,b,x,y) \\ &= \max_{\phi_1,\phi_2} \left(\phi_1 \otimes \phi_2\right)(G)\end{aligned}$$

donde ϕ_1, ϕ_2 son elementos de norma 1 en el dual de $\ell_1^n(\ell_\infty^n)$, que es exactamente la norma ε del tensor G como elemento de $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$.

N.B.: Se ha hecho el abuso de notación de llamar G tanto al juego en sí como al tensor que lo define. Además, se ha utilizado el hecho de que, en este caso, el máximo entre los elementos ϕ_1, ϕ_2 de norma 1 en $\ell_\infty^n(\ell_1^n)$ se alcanza en distribuciones de probabilidad de la forma $p_A(a|x)$, $p_B(b|y)$.

Queda ver cómo identificar el valor cuántico del juego $\omega^*(G)$. Para ello necesitamos dar un paso más y estudiar una forma de *cuantizar* los espacios normados.

Espacios de operadores

A la hora de pensar cómo cuantizar los espacios normados, de cara a poder capturar las propiedades de los sistemas cuánticos, la clave reside en recordar que el producto tensorial modeliza los distintos subsistemas de un sistema cuántico global. Puesto que cualquier sistema se puede considerar siempre como un subsistema de otro más grande, que incluye también a su entorno, las normas consideradas, así como las transformaciones entre estados cuánticos, deben incluir de forma natural a dicho entorno.

Por ejemplo, en vez de considerar como transformaciones posibles entre estados cuánticos simplemente los operadores lineales que preservan la traza y que son positivos, en el sentido de que llevan matrices semidefinidas positivas a matrices semidefinidas positivas, uno necesita pedir que los operadores sean *completamente positivos*; es decir, que sigan siendo positivos al tensorizarlos con el operador identidad actuando en otro espacio de matrices cualquiera, que modeliza el entorno.

Esta forma de *cuantizar*, considerando la tensorización con otro espacio de matrices cualquiera, fue utilizada de forma magistral en la tesis de Ruan, dirigida por Effros, a finales de los años 80, para definir el concepto de *espacio de operadores* (*operator space* en inglés) [34, 87] como la *cuantización* natural de un espacio normado.

Así, si llamamos M_k al espacio de matrices con coeficientes complejos de tamaño $k \times k$, un espacio de operadores X (de dimensión finita r) no es más que el espacio vectorial $\mathbb{C}^r$ al que asignamos una sucesión de normas $\|\cdot\|_k$ en los espacios $M_k \otimes X$, de manera que dichas normas tienen buenas propiedades de compatibilidad con la norma y las operaciones producto y suma directa de la componente M_k del producto tensorial. En M_k se considera siempre la norma de operador, dada por el mayor valor singular,

que es la norma que hace de M_k una C^*-álgebra y que coincide con la norma asociada a ver las matrices de M_k como operadores lineales de ℓ_2^k en ℓ_2^k.

Es importante recalcar que un mismo espacio normado tiene varias (de hecho infinitas) estructuras de espacio de operadores compatibles con esa norma. Hay algunas, eso sí, que son más naturales que otras. Por ejemplo, M_r es trivialmente un espacio de operadores sin más que definir en $M_k \otimes M_r$ la norma inducida por la identificación $M_k \otimes M_r = M_{kr}$. Lo mismo ocurre, por tanto, con cualquier subespacio de M_r, como por ejemplo su diagonal, que como espacio de Banach es exactamente ℓ_∞^r, o su primera fila R_r y su primera columna C_r, que como espacios de Banach ambos son exactamente ℓ_2^r, pero que son distintos como espacios de operadores.

A la vista de la definición de espacio de operador, y por analogía con la definición usual de norma asociada a un operador lineal, dados dos espacios de operadores X, Y y un operador lineal entre ellos $T : X \to Y$, se define la norma completamente acotada de T como el supremo en k de las normas de los operadores lineales

$$\mathrm{Id}_k \otimes T : M_k \otimes X \to M_k \otimes Y.$$

Usando la identificación algebraica $M_k(\mathrm{CB}(X, Y)) = \mathrm{CB}(X, M_k \otimes Y)$, se puede dar una estructura de espacio de operadores al espacio normado de operadores lineales de X en Y con la norma completamente acotada $\mathrm{CB}(X, Y)$. En particular, para el caso en que $Y = \mathbb{C}$, esto dota de una estructura de espacio de operadores al dual X^* de X.

El papel central que el producto tensorial juega en la propia definición de espacio de operadores hace que la teoría de los espacios de operadores pueda verse como un análogo no conmutativo de la teoría local de los espacios de Banach.

De hecho, también en el caso de los espacios de operadores hay una norma tensorial minimal, llamada min, que juega el papel análogo a la norma ε introducida en la Definición 5.1. La definición, en este caso, es la siguiente, que por simplicidad formalizo solo en el caso de dos espacios de operadores de dimensión finita

Definición 5.2. *Dados dos espacios de operadores X, Y de dimensión finita, y un elemento $z \in X \otimes Y$, se define $\|z\|_{\min}$ como el supremo de*

$$\|(\alpha \otimes \beta)(z)\|_{M_{k^2}} ,$$

donde $\alpha : X \to M_k$ y $\beta : X \to M_k$ tienen norma completamente acotada ≤ 1.

A la luz de lo ya mencionado, no es sorprendente que el valor cúantico de un juego $\omega^*(G)$ coincida (en este caso salvo una constante), con el valor de la norma min en $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$ del tensor asociado al juego $G_{(x,a),(y,b)}$. La intuición de este resultado, que demostramos en el artículo [57], es la siguiente:

Lo primero que necesitamos es entender cuál es la estructura natural de espacio de operadores en $\ell_1^n(\ell_\infty^n)$. Esta será la obtenida de identificar $\ell_1^n(\ell_\infty^n)$ con el dual del espacio $\mathrm{CB}(\ell_\infty^n, \ell_\infty^n)$.

Con esta estructura, un conjunto de operadores de medida E_a^x define un operador $\alpha : \ell_1^n(\ell_\infty^n) \to M_r$ de norma completamente acotada $= 1$ sin más que definir E_a^x como la imagen por α del elemento (x, a) de la base canónica en $\ell_1^n(\ell_\infty^n)$. Por otro lado, dada una matriz hermítica A en M_{k^2}, la norma de A no es más que el supremo en todos los estados cuánticos bipartitos ρ de dimensión k de la expresión $\mathrm{tr}[\rho A]$.

Así, si evaluamos en el tensor del juego la expresión que aparece en la definición de la norma min para los α y β dados por operadores de medida E_a^x y F_b^y respectivamente, obtenemos

$$\left\|(\alpha \otimes \beta)\left((G_{(x,a),(y,b)})_{(x,a),(y,b)}\right)\right\|_{M_{k^2}} =$$

$$\sup_{\rho} \sum_{x,y,a,b} \pi(x,y) V(a,b,x,y) \mathrm{tr}\left[\rho\left(E_a^x \otimes F_b^y\right)\right] .$$

El supremo, entre los α, β de norma completamente acotada ≤ 1, de la primera expresión es, por la Definición 5.2, la norma min del tensor asociado al juego $G_{(x,a),(y,b)}$ en el espacio $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$. Por otro lado, el supremo, entre todos los operadores de medida E_a^x, F_b^y, de la segunda expresión es, exactamente, el valor cuántico del juego $\omega^*(G)$; ya que, tal y como he comentado antes, las expresiones $p(ab|xy) = \mathrm{tr}\left[\rho\left(E_a^x \otimes F_b^y\right)\right]$ definen precisamente el conjunto de estrategias cuánticas posibles.

Por tanto, si todos los operadores α y β de norma completamente acotada ≤ 1 proviniesen de operadores de medida, se tendría que el valor cuántico del juego sería exactamente la norma min del tensor del juego en el espacio $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$. Gracias al Teorema de descomposición de Wittstock, esto se puede conseguir salvo constantes [58].

La pregunta de partida sobre el valor máximo del ratio $\frac{\omega^*(G)}{\omega(G)}$ se puede reformular, por tanto, como calcular la norma de la identidad

$$\mathrm{Id} : \ell_1^n(\ell_\infty^n) \otimes_\varepsilon \ell_1^n(\ell_\infty^n) \longrightarrow \ell_1^n(\ell_\infty^n) \otimes_{\min} \ell_1^n(\ell_\infty^n)\,.$$

Para verlo, basta combinar las siguientes observaciones ya comentadas anteriormente. Por un lado, el espacio $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$ se puede identificar con el conjunto de juegos (generalizados). Por otro, la norma ε en ese espacio se puede identificar con el valor clásico del juego, mientras que la norma min refleja el valor cuántico. Finalmente, por la definición de norma de un operador lineal, la norma de la identidad es, precisamente, el valor máximo del cociente de la norma min por la ε entre todos los elementos de $\ell_1^n(\ell_\infty^n) \otimes \ell_1^n(\ell_\infty^n)$ que, por las observaciones anteriores, coincide (salvo constante) con el máximo ratio $\frac{\omega^*(G)}{\omega(G)}$ entre todos los juegos (generalizados) posibles G.

Esta reformulación nos permitió utilizar técnicas de espacios de operadores, así como de la teoría local de espacios de Banach, entre ellas el Teorema de Grothendieck. Tras una serie de trabajos [58, 57, 56], el estado actual del problema es que, salvo constantes universales,

$$\frac{\sqrt{n}}{\log n} \leq \|\mathrm{Id} : \ell_1^n(\ell_\infty^n) \otimes_\varepsilon \ell_1^n(\ell_\infty^n) \longrightarrow \ell_1^n(\ell_\infty^n) \otimes_{\min} \ell_1^n(\ell_\infty^n)\| \leq n\,.$$

En particular, el cociente entre el valor cuántico y clásico de un juego puede ser arbitrariamente grande. Además, para obtener la separación $\frac{\sqrt{n}}{\log n}$ solo es necesario utilizar un espacio de estados de dimensión n en las estrategias cuánticas.

Se cierra el círculo. MIP*=RE

Esto lleva a las siguientes preguntas generales:

¿Cómo de grande es la dimensión del espacio necesario para obtener $\omega^*(G)$? ¿Puede ser que haga falta dimensión infinita? De ser así, ¿existe un experimento que permita testar la necesidad de utilizar dimensión infinita en la formalización de la física cuántica?

Más aún, si consideramos dimensión infinita existen, de hecho, dentro de la física cuántica, dos maneras de modelizar la separación espacial. Una es con el producto tensorial, tal y como he esbozado en este discurso. Otra, que es la estándar en el contexto de la teoría cuántica de campos, es la condición, a priori menos restrictiva, de que los operadores de medida de Alice y Bob conmuten. Las estrategias asociadas a esta modelización serían, por tanto, de la forma

$$p(ab|xy) = \mathrm{tr}\left(\rho E_a^x F_b^y\right)$$

donde E_a^x, F_b^y actúan ahora en el mismo espacio, pero conmutan entre sí.

¿Pueden permitir estas estrategias con operadores que conmutan probabilidades de éxito mayores que las estrategias con productos tensoriales? Dicho de otra manera, ¿existen experimentos, aunque sean ideales, que permitirían descartar el modelo de producto tensorial y cuyo resultado solo fuera compatible con modelizar la separación espacial con un único espacio infinito dimensional y operadores que conmutan? Esto es lo que se conoce como *problema de Tsirelson*.

El problema de Tsirelson surge de una afirmación sin demostración hecha por Tsirelson en sus trabajos sobre desigualdades de Bell, en particular en el artículo de revisión que publicó en 1993 [101]. En él afirmaba sin demostración que las estrategias obtenidas con operadores que conmutan y aquellas obtenidas con el producto tensorial son exactamente las mismas. En 2006, tras recibir la solicitud de una demostración por parte de Antonio Acín, Tsirelson se dio cuenta de que, en realidad, la demostración que tenía en la cabeza solo funcionaba para el caso de dimensión finita, con lo que planteó el caso infinito dimensional como una pregunta abierta, que apareció después en la lista más famosa de problemas de información cuántica de la época, mantenida por Reinhard Werner.

Algunos años más tarde, en 2011, en colaboración con Junge, Navascués, Palazuelos, Scholtz y Werner, logramos probar que una solución negativa al problema de Tsirelson implicaría, de hecho, una solución negativa al *Connes' Embedding Problem* [55]; un problema planteado por Alain Connes en su artículo seminal de 1976 [26], que ha resultado jugar un

papel central en la teoría de álgebras de operadores, así como en teoría de grupos [89]. Nuestro resultado fue obtenido de forma independiente también por Fritz [43] y completado depués por Ozawa [80], probando que, de hecho, el problema de Tsirelson es equivalente al *Connes' Embedding Problem*.

Desde la perspectiva de teoría de la complejidad con la que iniciaba el discurso, la pregunta que surge es también clara. El Teorema PCP muestra que es NP-duro aproximar el valor clásico $\omega(G)$ de un juego no local. ¿Cuál es la complejidad computacional de aproximar el valor cuántico $\omega^*(G)$?

Sorprendentemente, todas estas preguntas están relacionadas entre sí.

La primera contribución crucial a estas preguntas fue debida a Solfstra en su trabajo pionero [96] y su continuación [95]. Solfstra consideró un tipo particular de juego no local asociado a sistemas de ecuaciones lineales en $\mathbb{Z}_2$ y probó que cualquier grupo definido por una cantidad finita de generadores y relaciones es, de hecho, un subgrupo del *grupo solución* de un sistema lineal. La clave es que las propiedades algebraicas del grupo solución determinan la existencia, o no, de estrategias cuánticas de tipo conmutativo o tensorial que permiten ganar el juego con probabilidad 1. Este potente resultado le dio acceso a todo el arsenal de la teoría de grupos, pudiendo probar, por ejemplo, que existen juegos para los que hace falta dimensión infinita para obtener $\omega^*(G)$, o que el problema de si $\omega^*(G) = 1$ o no es indecidible. Esto quiere decir que no existe ningún algoritmo, no importa cómo de ineficiente, que permita determinar si $\omega^*(G) = 1$ o no.

La construcción de Slofstra fue mejorada y simplificada poco después por Dykema, Paulsen y Prakash en [33], utilizando para ello técnicas de álgebras de operadores.

Sin embargo, ninguno de estos resultados permitía probar o refutar el *Connes' Embedding Problem* pues, para ello, había que obtener una separación entre el valor del juego con estrategias con operadores que conmutan y el valor del juego que uno puede *aproximar* con estrategias asociadas al producto tensorial. En todos los ejemplos anteriores, uno podía obtener una probabilidad de ganar el juego arbitrariamente cercana a 1, aunque no exactamente $= 1$, con estrategias de dimensión finita y en el paradigma tensorial.

Esto es precisamente lo que afirma el artículo "MIP* = RE" de Ji, Natarajan, Vidick, Wright y Yuen [53], aunque a fecha de hoy el resultado se encuentra todavía en proceso de revisión. El principal resultado, en la línea del Teorema PCP enunciado antes, es el siguiente:

Teorema 5.3 (RE $\subset$ MIP*)**.** *Existe un $\delta > 0$ tal que, dado un juego no local G con la promesa de que su valor cuántico es $\omega^*(G) = 1$ o $\omega^*(G) \leq 1 - \delta$, decidir cuál de las dos situaciones es cierta es indecidible. Es decir, no existe ningún algoritmo, no importa cómo de ineficiente, que proporcione la respuesta.*

Para entender por qué este resultado resuelve el problema de Tsirelson y, por tanto, el *Connes' Embedding Problem*, basta observar que existe un algoritmo que aproxima por abajo el valor cuántico del juego en el paradigma tensorial y otro, llamado jerarquía NPA [79], que permite aproximar por arriba el valor cuántico en el paradigma conmutativo. Si el valor de ambas aproximaciones pudiera hacerse arbitrariamente cercano, lo que sería el caso si el problema de Tsirelson tuviera una solución positiva, existiría un algoritmo para aproximar el valor cuántico de un juego a cualquier precisión constante, lo que contradice el teorema anterior. En el fabuloso artículo "From Operator Algebras to Complexity Theory and Back" de Thomas Vidick, se pueden encontrar más detalles de esta idea.

Es ciertamente sorprendente cómo un resultado de teoría de la complejidad, que puede verse como el análogo cuántico del Teorema PCP, al menos en su versión para juegos [1], permite resolver un problema central sobre álgebras de operadores para el que las técnicas usuales de la teoría habían resultado insuficientes. Esto enfatiza aún más, si cabe, mi observación inicial sobre los juegos no locales: "no son tan sencillos como parecen".

[1] Esto no es lo que se conoce normalmente en la literatura como *quantum PCP* [1], que hace referencia a una versión del Teorema PCP en su versión 3-SAT donde se cambia la clase de complejidad NP por su análogo cuántico QMA.

6. VARIANTES DEL JUEGO

He centrado la mayor parte del discurso en el juego no local de partida, pero existen numerosas variantes y generalizaciones del mismo, motivadas por distintos tipos de problemas.

Las generalizaciones más naturales corresponden a considerar juegos con más de dos participantes, pero con idénticas reglas. En este caso aparecen grandes diferencias incluso en la familia más sencilla de juegos: los juegos XOR.

Los juegos XOR

Un juego XOR es un juego en el que los concursantes tienen que responder un único bit y en el que, además, la dependencia en la función de verificación V de las respuestas es únicamente a través de su XOR (o suma módulo 2, denotada por $\oplus$). Este es el caso, por ejemplo, del juego CHSH con el que iniciaba el discurso, en el que $V(a, b, x, y) = 1$ si y solo si $xy = a \oplus b$. En este tipo de juego se suele considerar, en vez del valor, lo que se llama su *sesgo*, que no es más que la máxima diferencia entre la probabilidad de ganar el juego y la de perderlo.

Tsireslon [100] demostró que, para este tipo de juegos, uno puede identificar el sesgo clásico con la norma ε de un cierto tensor en el espacio $\ell_1^n \otimes \ell_1^n$, donde n es el número de preguntas posibles, mientras que el sesgo cuántico es precisamente la norma γ_2^* de ese tensor. Por tanto, el Teorema de Grothendieck garantiza que el cociente máximo posible entre el sesgo cuántico y el clásico de un juego XOR de dos jugadores está acotado por la constante de Grothendieck.

Analizar, por tanto, el caso de juegos XOR tripartitos requiere analizar la posibilidad de tener versiones multilineales del Teorema de Grothendieck.

Hay una extensa literatura sobre posibles versiones multilineales del Teorema de Grothendieck, que fue precisamente el tema central de mi tesis doctoral. Aparte de mis propias contribuciones [16, 82, 83], citaré como imprescindibles los trabajos de Carne [22] y Blei [14]. Lamentablemente, la mayor parte de las *posibles* generalizaciones posibles al contexto

multilineal de la desigualdad de Grothendieck son falsas. Recientemente, por ejemplo, Palazuelos y Briët [17] han dado un contraejemplo para una de ellas, que había sido propuesta como problema abierto por Pisier en [88].

Para los juegos XOR logramos demostrar en [84] que el sesgo clásico (resp. cuántico) está dado por la norma tensorial ε (resp. min) de un cierto tensor en el producto tensorial $\ell_1^n \otimes \cdots \otimes \ell_1^n$, para cualquier número de participantes. En este caso, la estructura de espacio de operadores natural en ℓ_1^n es la obtenida como espacio dual de ℓ_∞^n que, como he comentado antes, se identifica a su vez con la diagonal del espacio de matrices M_n. Por tanto, la desigualdad de Grothendieck multilineal buscada tendría como objeto acotar la norma del operador identidad

$$\mathrm{Id} : \ell_1^n \otimes_\varepsilon \cdots \otimes_\varepsilon \ell_1^n \longrightarrow \ell_1^n \otimes_{\min} \cdots \otimes_{\min} \ell_1^n \ . \tag{6.1}$$

Después, utilizando teoría de espacios de operadores, en combinación con técnicas probabilísticas, logramos ver que, ya en el caso de tres partes, la norma de la identidad (6.1) no está acotada en n [84], lo que muestra la gran diferencia existente entre el caso bipartito y el tripartito.

Los juegos XOR también han sido analizados recientemente desde la perspectiva de la teoría de la complejidad. Se cree que aproximar el sesgo cuántico del juego para juegos XOR tripartitos es NP-duro, pero la prueba original de ese aserto, debida a Thomas Vidick, contiene un error que todavía no se ha acabado de subsanar [104]. Nótese que para el sesgo clásico de juegos XOR, incluso el caso bipartito es NP-duro de aproximar, ya que hemos visto que aproximar la norma $\ell_1^n \otimes_\epsilon \ell_1^n$ permite aproximar la solución del problema MAX-CUT, que es un problema NP-duro.

Juegos con comunicación restringida

Uno podría plantearse relajar la regla de que Alice y Bob no pueden comunicarse en absoluto una vez que el juego empieza y dejar que puedan enviarse algo de comunicación. Por supuesto, si la comunicación que se les permite es arbitraria, ambos tendrían la información exacta del par de preguntas (x, y) y podrían responder siempre de forma correcta. Para que el juego tenga algo de interés, la comunicación permitida debe ser, por tanto, limitada.

Hay esencialmente dos formas de limitar la comunicación, que, además, se pueden combinar entre sí. Una es limitar el número total de bits de comunicación que se les permite intercambiar. Otra es limitar el tipo de comunicación; por ejemplo, permitir que Alice comunique información a Bob pero no al revés.

Centrémonos, para empezar, en el primer caso. Consideremos para ello una función booleana f en dos variables, cada una de ellas una cadena de n bits; es decir, $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Definamos el juego XOR en el que los participantes ganan si el XOR de sus respuestas $a \oplus b$ coincide con el valor de $f(x,y)$. Uno podría preguntarse:

¿Cuál es la menor cantidad de bits que Alice y Bob tienen que comunicarse para ganar el juego con certeza (o con probabilidad mayor que un valor fijo, e.g. $\frac{2}{3}$)?

Este valor coincide precisamente con la llamada *complejidad de la comunicación* de la función f.

La teoría de la complejidad de la comunicación [66] ha sido ampliamente estudiada en ciencias de la computación y tiene conexiones con numerosas áreas de estudio como, por ejemplo, la computación en paralelo, donde la comunicación entre los nodos es uno de los principales cuellos de botella en el tiempo total de cómputo.

El modelizar, tal y como hemos hecho, los problemas de complejidad de la comunicación como un juego no local permite analizar las posibles ganancias debidas al uso de comunicación cuántica (o entrelazamiento compartido que, via el protocolo de teleportación, son recursos esencialmente equivalentes).

Utilizando este punto de vista, tal y como se puede consultar en el excelente artículo de revisión [19], se pueden obtener distintas funciones para las que existen mejoras exponenciales en la cantidad de comunicación necesaria si se utilizan recursos cuánticos en vez de clásicos.

Es interesante observar además que, utilizando las conexiones existentes entre juegos no locales y análisis funcional, y entre juegos no locales y complejidad de la comunicación, recientemente Amr y Villanueva [3] han obtenido nuevas mejoras exponenciales en la complejidad de la comunicación dentro del contexto de los juegos XOR.

Juegos con preguntas cuánticas

Dada la ubicuidad con la que se encuentran los juegos no locales, no es de extrañar que varios protocolos cuánticos se puedan modelizar también desde esta perspectiva. Para ello hay que permitir que las preguntas y/o las respuestas puedan ser estados cuánticos. Un ejemplo particularmente interesante viene motivado por la *criptografía basada en la posición*.

Pensemos en un futuro (tal vez no tan lejano) en el que la movilidad en las ciudades esté dominada mayoritariamente por la circulación de coches autónomos. Sería conveniente, para una adecuada gestión del tráfico, que los vehículos autónomos puedan comunicarse entre sí, lo que plantea el problema crucial de la seguridad de dicha comunicación para evitar un jaqueo que pueda desencadenar accidentes o el colapso del tráfico.

En ese escenario el identificador relevante de un vehículo no es su matrícula, o la identidad de sus ocupantes, sino la posición GPS que ocupa. Un vehículo quiere estar seguro de estar comunicándose, por ejemplo, con el vehículo que está delante de él, al margen de quién lo ocupe.

La criptografía basada en la posición tiene por objeto diseñar sistemas de comunicación donde la seguridad se basa, precisamente, en la posición GPS. La primitiva fundamental en este contexto, que garantiza la existencia de sistemas de comunicación seguros, es el protocolo de verificación de la posición. Básicamente, es un reto que solo alguien en una posición GPS concreta puede resolver satisfactoriamente.

La idea de la criptografía basada en la posición se debe a Chandran, Goyal, Moriarty y Ostrovsky [23] y, cómo no, puede también modelizarse como un juego no local, en el que los jáquers potenciales son los participantes.

Vamos a pensar en el caso más sencillo, que es el uno dimensional, en el que suponemos que todas las personas involucradas en el análisis se sitúan en una recta. Un agente tiene que demostrar que está en una cierta posición P. Para ello, recibe el siguiente reto:

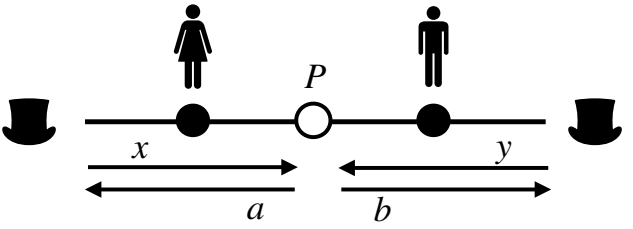

Figura 6.1: En la criptografía basada en la posición los agentes maliciosos Alice y Bob intentan contestar adecuadamente y en tiempo a las preguntas x, y que solo un participante honesto en la posición P debería poder contestar de forma satisfactoria.

Dos verificadores, que actúan de manera coordinada y que está situados a izquierda y derecha de P, envían cada uno una pregunta x e y, respectivamente, a la posición P, de manera que ambas preguntas llegan a la vez. El agente debe utilizar la información de ambas preguntas para enviar una respuesta válida a y b a cada verificador, respectivamente.

Para pasar el reto de forma satisfactoria, el agente debe responder de forma adecuada y, además, *las respuestas deben llegar a los verificadores exactamente en el tiempo que tarda una señal en ir y volver desde la posición de los verificadores a* P. Si las respuestas llegan más tarde, se consideran inválidas.

Este tipo de criptografía cuántica basada en el estudio de los tiempos de respuesta recibe el nombre genérico de criptografía cuántica relativista, precisamente porque utiliza la premisa básica de que la luz tiene una velocidad de tansmisión conocida y constante. Algunas de las primitivas criptográficas fundamentales, como *bit commitment* y *coin tossing*, son posibles en este contexto [60, 61] e, incluso, se han podido realizar experimentalmente [71, 73, 74].

Así, si un participante malicioso quiere hacer creer a los verificadores que está en la posición P sin estarlo, necesariamente su señal tardará más en llegar a uno de los dos verificadores: el que esté más lejos de él.

¿Qué pasaría, sin embargo, si dos jáquers situados a izquierda y derecha de P, entre P y los verificadores, actuaran de forma coordinada en este reto? No es difícil encontrar un protocolo donde pueden simular de forma

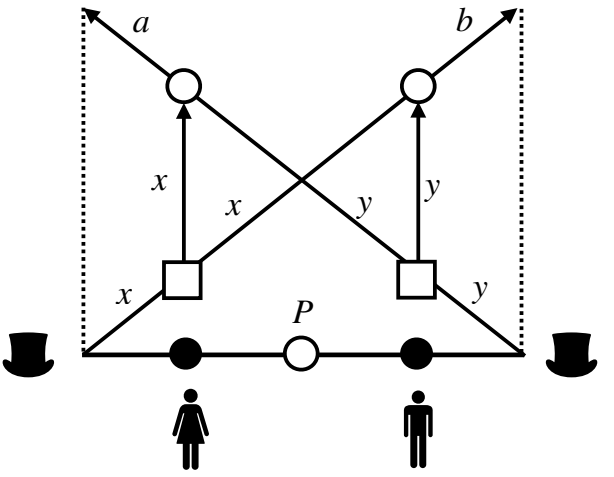

Figura 6.2: Ataque trivial a la criptografía *clásica* basada en la posición. Los agentes maliciosos solo tienen que copiar y transmitir la pregunta recibida del verificador más próximo y actuar como el participante honesto en el momento temporal en que ya tienen acceso al par de preguntas x, y.

exacta el comportamiento de un agente honesto. Basta con que cada uno de ellos, al recibir la pregunta del verificador más cercano, la copie, de forma que una de las dos copias la guarda en su memoria y la otra la envía al otro jáquer que, al recibirla, pasa a tener la misma información que un agente honesto y puede usarla para responder al verificador más cercano. Tal y como se aprecia en la Figura 6.2, los conos de luz asociados a los tiempos de este ataque permiten pasar el reto sin problemas.

¿Significa esto que la criptografía basada en la posición no es posible? En realidad no. El ataque presentado requiere *copiar* la información y, por el Teorema de no clonación [108], esto no es posible si las preguntas, en vez de cadenas de bits clásicos, son estados cuánticos. El protocolo resultante se puede modelizar como un juego no local en el que los participantes, Alice y Bob, son los jáquers y el verificador es el presentador que les plantea una pregunta *cuántica*, es decir, les envía un estado cuántico bipartito $\rho_{AB}^{\text{inicial}}$, donde el sistema A es enviado a Alice y el sistema B a Bob. La respuesta debe ser otro estado cuántico ρ_{AB}^{final}, donde A (resp. B) es el sistema que Alice (resp. Bob) devuelve como respuesta al presentador. La

necesidad de responder a tiempo permite a cada uno de los participantes enviar un mensaje al otro, pero sin la posibilidad de darle luego respuesta. A este modelo de comunicación lo llamamos comunicación simultánea unidireccional.

La pregunta de si la criptografía cuántica basada en la posición es posible puede por tanto reformularse como:

¿Existe un juego no local con preguntas y respuestas cuánticas que se pueda ganar con probabilidad 1 utilizando comunicación arbitraria (equivalente al caso honesto), pero para el que esto no sea posible si se puede utilizar solo comunicación simultánea unidireccional?

La respuesta, tal vez sorprendentemente, depende de la cantidad de entralazamiento compartido por los participantes [18]. El estado actual del arte es el siguiente:

- Si los participantes pueden compartir un estado entrelazado de dimensión *exponencial* comparada con la dimensión de los sistemas A y B asociados a las preguntas y respuestas, entonces Alice y Bob pueden simular el comportamiento de un agente honesto [11].
- Existen juegos para los que hace falta al menos una cantidad de entrelazamiento *lineal* para dar una respuesta válida [98].

Si existen juegos donde es *necesario* utilizar entrelazamiento exponencial, entonces uno podría afirmar que la criptografía cuántica basada en la posición es posible a todos los efectos prácticos. Sin embargo, si basta una cantidad polinomial de entrelazamiento para simular el comportamiento de un agente honesto, entonces la criptografía cuántica basada en la posición no sería posible, al menos sin hipótesis extra en las capacidades computacionales de los participantes.

A día de hoy sigue sin conocerse la respuesta, tal vez porque aún no se han desarrollado las técnicas matemáticas necesarias para ello.

En esa dirección, en el trabajo [54], hemos logrado extender la aplicabilidad de las técnicas de análisis funcional comentadas antes (normas tensoriales y espacios de operadores) al contexto de la comunicación simultánea unidireccional. En un trabajo previo [29], logramos hacerlo para los casos más sencillos de comunicación puramente unidireccional, o ausencia de comunicación (incluso en este caso los juegos son distintos al tener preguntas y respuestas cuánticas).

El resultado que mostramos como consecuencia del uso de estas técnicas de análisis funcional es que, bajo ciertas hipótesis en la regularidad de las estrategias empleadas por Alice y Bob, en el sentido de que dichas estrategias no varían mucho si se modifican ligeramente las preguntas, existen juegos para los que ganar con alta probabilidad requiere entrelazamiento exponencial.

Sorprendentemente, May, Penington y Sorce han argumentado recientemente [76] que el diccionario holográfico, conocido como correspondencia AdS-CFT, iniciado por Maldacena y Witten en los años 90 como solución para reconciliar gravedad y cuántica [75, 106], implicaría la existencia de ataques con entrelazamiento polinomial.

Dada la aparente contradicción entre este resultado y el nuestro, parece posible poder obtener nuevos resultados en el problema de la gravedad cuántica utilizando técnicas de normas tensoriales y espacios de operadores, lo que abre un nuevo campo apasionante de investigación en una de las preguntas centrales de la física. Nuevamente, son los juegos no locales los que actúan como puente entre ambos mundos; algo que, a estas alturas del discurso, ya ni siquiera debería sorprender.

Otra dirección interesante que surge de analizar la criptografía basada en la posición es una nueva definición de complejidad de la comunicación de una función booleana $f(x, y)$, conocida como complejidad *garden-hose*, que podría traducirse como complejidad *tipo manguera de jardín* [20]. El nombre es bastante gráfico y corresponde al siguiente problema, cuya descripción tomamos directamente de [20]:

> *En un agradable día soleado, Alice y Bob se relajan en sus respectivos jardines vecinos. Ocurre que sus dos jardines comparten s tuberías de agua, etiquetadas por los números $1, 2, \ldots, s$. Cada una de estas tuberías tiene un extremo abierto en el jardín de Alice y otro en el jardín de Bob. Por diversión, Alice y Bob juegan al siguiente juego. Alice utiliza trozos de manguera para conectar localmente entre sí algunos de los extremos abiertos de las tuberías que hay en su jardín. Por ejemplo, podría conectar la tubería 2 con la 5, la tubería 4 con la 9, etc. De forma similar, Bob conecta localmente algunos de los extremos abiertos de las tuberías que hay en su jardín; por ejemplo la tubería 1 con la 4, etc. Además, no se pueden usar piezas tipo T (o construcciones más complicadas) para conectar dos o más tuberías a una dada, o viceversa. Final-*

mente, Alice conecta un grifo de agua al extremo de su jardín de una de las tuberías, por ejemplo la 3*, y abre el grifo. Alice y Bob observan cuál de los dos jardines se acaba mojando. Es fácil ver que, como Alice y Bob solo utilizan conexiones simples uno-a-uno, el agua siempre acaba saliendo eventualmente en alguno de los dos lados. En cuál de ellos obviamente depende de las respectivas conexiones locales.*

Ahora pongamos que Alice conecta las tuberías y el grifo, no en unas posiciones fijas, sino dependiendo de una cadena de bits privada $x \in \{0,1\}^n$*; para distintas cadenas de bits* x, x'*, puede conectar sus extremos de las tuberías de forma diferente. Análogamente, la elección de Bob de cómo conectar las tuberías depende ahora de una cadena privada de bits* $y \in \{0,1\}^n$*. Estas estrategias especifican una función booleana* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *como sigue:* $f(x,y)$ *se define como* 0 *si, usando las conexiones determinadas por* x *e* y *respectivamente, el agua sale en el jardín de Alice, y* $f(x,y)$ *es* 1 *si el agua acaba saliendo en el lado de Bob.*

Cambiando el punto de vista, podemos ahora considerar una función booleana arbitraria $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *y preguntar: ¿Cómo se puede computar* f *en el modelo de mangueras de jardín? ¿Cómo tienen que elegir Alice y Bob sus conexiones locales, y cuántas tuberías hacen falta, para computar* f *en el modelo de mangueras de jardín? Recalcamos que la elección de Alice de qué tuberías conectar puede depender de* x*, pero no de* y*, y viceversa; esto es lo que hace no triviales las preguntas anteriores.*

Para una función booleana $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$*, su complejidad tipo manguera de jardín* $\mathrm{GH}(f)$ *se define como el menor número* s *de tuberías necesarias para computar* f *en el modelo de mangueras de jardín.*

La complejidad tipo manguera de jardín está motivada por el siguiente juego no local cuántico, llamado *qubit routing*, asociado a una función booleana $f(x,y)$. Alice recibe como pregunta una cadena clásica de bits x y un qubit en un cierto estado aleatorio $|\psi\rangle$. Bob recibe únicamente la cadena clásica de bits y. Para ganar el juego Alice debe enviar de vuelta el estado $|\psi\rangle$ como respuesta si $f(x,y) = 0$, mientras que si $f(x,y) = 1$ debe ser Bob quien envíe el estado $|\psi\rangle$ como respuesta.

Tal y como se demuestra en [20], la complejidad tipo manguera de jardín de $f(x, y)$ es una cota superior al logaritmo de la dimensión de entrelazamiento necesaria para ganar el juego utilizando comunicación simultánea unidireccional. Además, el resultado es constructivo, en el sentido de que la colocación de las mangueras en el cómputo de $\mathrm{GH}(f)$ proporciona un protocolo para ganar el juego.

Desde su definición, la complejidad tipo manguera de jardín ha ido ganando relevancia, como se puede ver por ejemplo en [24, 31, 64].

Otras variantes

Hay numerosas otras variantes y generalizaciones de los juegos no locales aquí presentados. En la mayoría de los casos la idea subyacente es similar a la propuesta por John Bell en respuesta a la crítica de la mecánica cuántica de Einstein, Podolsky y Rosen: tener un experimento que permita descartar un cierto modelo a partir únicamente de las distribuciones de probabilidad observadas.

De esta manera se pueden, por ejemplo, validar o refutar redes causales [107], en las que se quiere entender qué procesos son causa o consecuencia de otros. Se puede incluso diseñar un experimento para descartar la posibilidad de modelizar matemáticamente la mecánica cuántica con números reales, en vez de complejos [92]. En este caso, de hecho, el experimento se ha realizado [68], obteniendo que, en efecto, los números complejos son *necesarios*.

Que una propiedad tan fundamental como la necesidad de utilizar números complejos pueda obtenerse experimentalmente es algo que me resulta fascinante y que es una consecuencia más de la enorme riqueza de los juegos no locales como puente de unión entre las matemáticas, la física y las ciencias de la computación.

7. ALGUNOS DE LOS PRINCIPALES PROTAGONISTAS DE ESTA HISTORIA

Para no cortar el hilo argumental del discurso, he preferido no hacer los necesarios apuntes biográficos acerca de algunos de los grandes protagonistas del mismo. Es el momento de remediarlo. No es necesario decir que hay muchas más personas que han contribuido de forma crucial al tema en el que he centrado este discurso, algunos de cuyos nombres ya he mencionado antes. Pero, como una elección totalmente personal y por tanto subjetiva, he decidido resaltar a John Bell, como el origen de los juegos no locales; a Shafi Goldwasser, como una de las pioneras en el estudio de estos juegos en teoría de la complejidad; a Irit Dinur, por su demostración del teorema PCP; a Boris Tsirelson, por su desarrollo sistemático de las desigualdades de Bell; a Thomas Vidick, por todo el trabajo en juegos no locales que condujo a la resolución del problema de Tsirelson; a Alexander Grothendieck, por la creación de la teoría local de espacios de Banach; a Gilles Pisier, como principal impulsor de la teoría de los espacios de operadores y, por último, a Marius Junge, como uno de los principales investigadores en la interconexión entre la información cuántica y las álgebras de operadores.

Me centraré primero en los que ya han fallecido (John Bell, Alexander Grothendieck y Boris Tsirelson) a los que dedicaré algo más de tiempo a modo de pequeño homenaje. Curiosamente, en estos tres casos, las contribuciones clave asociadas a la temática de este discurso fueron marginales en sus carreras científicas, en las que se centraron mayoritariamente en otros temas completamente distintos. Mi fuente principal de información para la biografía de John Bell ha sido el extenso obituario que le dedicó la *Royal Society*, de la que era miembro, tras su fallecimiento [21]. En el caso de Grothendieck es difícil encontrar nada mejor que la fantástica charla impartida por Fernando Bombal en esta Real Academia: "Alexander Grothendieck: una mente maravillosa y una vida fascinante" (aunque el breve obituario de Mumford y Tate [78] es también muy recomendable). En cuanto a Boris Tsirelson, la información más relevante la he obtenido del obituario que le dedicó Gil Kalai titulado: "Trees not Cubes", el obituario de Mateus Araújo "Boris Tsirelson 1950-2020", la breve autobiografía que se puede encontrar en el blog del *Institute for Quantum Optics and Quantum Information* (IQOQI) de Viena y su propia web.

John Bell

John Stewart Bell nació en Belfast en 1928. Se graduó en física matemática en la Universidad de Queen, también en Belfast, en 1949. De allí marchó al Complejo de Investigación en Energía Atómica de Harwell, cerca de Oxford. Tras el arresto de su director Klaus Fuchs por espionaje, Bell se marchó al grupo de diseño de aceleradores que dirigía Bill Walkinshaw en el Complejo de Investigación en Telecomunicaciones de Malvern; complejo que un año después se trasladó también a Harwell.

En 1953, Bell obtuvo una licencia para investigar en la Universidad de Birmingham, bajo la supervisión de Sir Rudolf Peierls. Como parte de su tesis doctoral en la Universidad de Birmingham, Bell demostró la que seguramente sea la mayor contribución de su carrera: el Teorema CPT; obtenido también de forma independiente por Lüders y Pauli. En palabras de Peierls (sobre Bell):

> *En aquella época nos enteramos de experimentos que parecían revelar evidencia de una partícula cargada negativamente que era estable, pero con masa menor que la del protón. Los experimentales nos preguntaban si podría ser el anti-protón. Esto parecía poco probable, pero ¿quién podía descartarlo de forma rotunda? Todo el mundo esperaba que una partícula y su anti-partícula tuvieran la misma masa, pero ¿era eso estrictamente necesario? Este problema le tocó la fibra. A él no le gustaba dar por sentadas las creencias dominantes y solía preguntar: "¿Cómo lo sabes?". Enseguida obtuvo el "Teorema CPT", estableciendo que los resultados de una teoría de campos deben permanecer inalterados si se invierte el signo de las coordenades de espacio y tiempo y se intercambian partículas por anti-partículas [...]. El Teorema asegura en particular que cualquier partícula y su anti-partícula deben tener la misma masa. Cualquier evidencia que contradiga el teorema sería muy difícil de reconciliar con nuestro conocimiento básico actual de la física; hasta la fecha no se ha encontrado ninguna evidencia. De hecho, el experimento que había motivado la cuestión no se confirmó.*

Bell continuó trabajando toda su vida en física nuclear y de altas energías, así como en el diseño de aceleradores de partículas. Desde 1960 lo hizo en el CERN, donde permaneció hasta su fallecimiento en 1990. Para un resumen histórico detallado de sus contribuciones en este campo se puede consultar [21].

Su trabajo sobre juegos no locales y, en general, sobre los fundamentos de la física cuántica, era para él un pasatiempo que se remontaba incluso a su época del instituto y, muy especialmente, a las discusiones mantenidas con Franz Mandl en Harwell a principios de los años 50. De hecho, en su trabajo "On the problem of hidden variables in quantum mechanics" de 1966 en *Reviews in Modern Physics* escribe en los agradecimientos:

> *Las primeras ideas de este artículo surgieron en 1952. Estoy profundamente agradecido al Dr. F. Mandl por intensas discusiones en aquel período.*

Entre los muchos reconocimientos obtenidos por John Bell a lo largo de su carrera destacan la Medalla Dirac, el Premio Dannie Heineman o la Medalla Hughes.

Alexander Grothendieck

La vida y obra de Alexander Grothendieck valdrían para más de un discurso como este en exclusiva. Considerado como uno de los mejores y más influyentes matemáticos del siglo XX, su vida fue también intensa y fuera de lo común.

Grothendieck nació en Berlín en 1928. Sus padres eran ambos activos anarquistas y su padre era, además, judío. Por tanto, cuando los nazis llegaron al poder en Alemania en 1933, ambos huyeron a Paris, dejando a Grothendieck a cargo de una familia de acogida en Hamburgo. Grothendiek permaneció con ellos seis años, hasta que en 1939, ante la inminencia de la Segunda Guerra Mundial, fue enviado a Francia a reunirse con sus padres. Justo ese mismo año sus padres acababan de regresar a Francia de luchar en la Guerra Civil española.

Tras la caída de Francia, su padre fue deportado por el régimen de Vichy a Auschwitz, donde murió. Tanto Grothendieck como su madre se establecieron en Chambon sur Lignon, una pequeña ciudad símbolo de la resistencia francesa donde Grothendieck completó el bachillerato en el "Collège Cévenol", una escuela con un claro ideal en pos de la no-violencia y la solidaridad de todos los pueblos.

Entre 1945 y 1948 estudió matemáticas en la Universidad de Montpellier, tras lo cual marchó a París, y luego a Nancy, donde inició su tesis doctoral bajo la supervisión de Laurent Schwartz. Parte de la tesis doctoral

la realizó en Brasil, donde permaneció entre 1953 y 1955, y desde donde fue enviando por carta a Schwartz sus progresos. Su tesis doctoral, motivada por la teoría de distribuciones por la que Schwartz había recibido la medalla Fields, versó precisamente sobre las posibles topologías naturales en los productos tensoriales de espacios vectoriales topológicos. En palabras de Schwartz:

> *Es un monumento, una obra maestra de primer orden. Fue necesario leerla, comprenderla y aprender de ella, porque era difícil y profunda. Me llevó seis meses a plena dedicación. ¡Qué trabajo tan duro, pero qué felicidad! [...] Es la más bella de mis Tesis*"

Durante su estancia en Brasil escribió también su "Résumé de la théorie métrique des produits tensoriels topologiques", en el que probó el Teorema de Grothendieck del que he hablado largo y tendido en este discurso.

Tras su regreso a París cambió de tema y se centró en la geometría algebraica, área que revolucionó entre 1955 y 1970, primero en el CNRS y, tras 1959, como miembro del recién creado Instituto de Estudios Científicos Avanzados (IHES). En 1966 obtuvo la medalla Fields precisamente por sus trabajos en geometría algebraica.

En 1970 dejó el IHES por motivos que no están claros, aunque el motivo oficial fue que el IHES recibía financiación del Ministerio de Defensa, y abandonó las matemáticas para dedicarse al activismo medioambiental y pacifista. Según su amigo Jean Paul Cartier:

> *Llegó a considerar Bures sur Yvette (donde estaba situado el IHES) como una jaula dorada que le mantenía apartado de la vida real. A eso se añadió una profunda depresión, junto con dudas sobre el valor de su actividad científica. Me confió sus dudas y me dijo que estaba considerando dedicarse a otras actividades distintas de las matemáticas. Se podría añadir quizá el bien conocido efecto del "síndrome Nobel"que lleva a la perniciosa idea de que los 40 es la edad en que cesa la actividad matemática creativa.*

Para añadir después:

> *La guerra fría estaba en su apogeo, y el riesgo de una confrontación nuclear era muy real. Los problemas de sobrepoblación, contaminación y desarrollo descontrolado - todo lo que ahora se clasifica como ecología- comenzaban a atraer atención. ¡Había muchas razones para poner en cuestión la ciencia!*

Regresó al mundo académico en 1972, pero se dedicó ya casi exclusivamente a dar clases (de forma irregular) en la Universidad de Montpellier. Tras jubilarse en 1988 rechazó el Premio Crafoord de la Academia Sueca de Ciencias, dotado con medio millón de dólares, aduciendo que:

> *Dado el declive de la ética científica, participar en el juego de los premios significa aprobar un espíritu que me parece insano.*

Grothendieck había sido muy crítico en los años anteriores con la comunidad científica, en concreto con su competitividad y la presión por publicar.

Desde 1990 vivió de manera casi ermitaña en Laserre, un pequeño pueblo de los Pirineos, hasta su fallecimiento en 2014.

Boris Tsirelson

Boris Tsirelson nació en Leningrado en 1950, donde también estudió y obtuvo el doctorado en 1975. Fue uno de los numerosos judíos a los que no se permitió abandonar la URSS durante la guerra fría (los llamados *refusenik*), con lo que solo consiguió emigrar a Israel en 1991 con la "perestroika" y, según el propio Tsirelson, gracias también a la inestimable ayuda de Vitali Milman. Desde entonces ha sido catedrático de matemáticas de la Universidad de Tel-Aviv hasta su fallecimiento en 2020.

Su principal área de trabajo ha sido la teoría de la probabilidad, pero ha realizado contribuciones brillantes en numerosos otros campos, como el análisis funcional (con un único trabajo, construyendo lo que hoy en día se conoce como espacio de Tsirelson) o en desigualdades de Bell, donde sus trabajos pioneros de los años 80 fueron ignorados durante décadas, hasta el auge posterior de la teoría de la información cuántica. En sus propias palabras:

> *Obtuve mi cota (pobabilidad 0.85..., entre 0.75 y 1). Pasó totalmente inadvertida. Añadí algo más de matemáticas, generalizando el resultado, y en 1980 publiqué un artículo en "Letters in Mathematical Physics", que era ilegal para ciudadanos soviéticos sin afiliación académica; siendo un "refusenik" era afortunado de trabajar como programador para la industria. Como joven matemático soviético, creía ingenuamente que un artículo publicado en una revista de física de occidente debería ser leído por algunos físicos. No hubo ninguna reacción durante años [...]*

La falta de reconocimiento, en combinación con ser un "refusenik" durante largo tiempo me había llevado a publicar demostraciones esquemáticas, o a no publicar demostraciones en absoluto, de muchas de las afirmaciones hechas en mis artículos. Algunos cálculos hechos en mi primer trabajo (de 1980) contienen errores corregidos en un artículo de Elie Wolfe y Susanna Yelin (¡32 años después! [...]). Mucho peor, mi artículo de revisión de 1993 afirmaba un resultado que de hecho ¡fue un problema abierto durante décadas! Debería haberse llamado el fracaso escandaloso de Tsirelson, pero en vez de eso se conoce como "el Problema de Tsirelson" [...]

Por casualidades del destino, fue justo una semana antes de su muerte por suicidio asistido en Suiza (motivado por un estado avanzado de cáncer) cuando se anunció la solución del Problema de Tsirelson en el artículo MIP* = RE. Tsirelson se quedó fascinado por el resultado y comentó:

Envídienme. Soy muy afortunado. Me marcho cómodamente durante un pico de fama.

Shafi Goldwasser

Shafrira (Shafi) Goldwasser nació en Nueva York en 1958. Obtuvo el grado en matemáticas en la Universidad Carnegie Mellon, para luego realizar su máster y doctorado en Berkeley en ciencias de la computación, que finalizó en 1984. Desde entonces ha estado en el MIT, donde ostenta la Cátedra *RSA* de Ingeniería Electrónica y Ciencias de la Computación desde 1995. Desde 2018 es, además, la Directora del Instituto Simons de Teoría de la Computación en Berkeley.

Goldwasser recibió en 2012 el Premio Turing, considerado el Premio Nobel de ciencias de la computación, y posee numerosos otros premios y distinciones, entre los que podemos destacar el Premio Gödel (obtenido dos veces, la primera por introducir los juegos no locales en teoría de la computación y la segunda por su trabajo en inaproximabilidad y en el Teorema PCP), el Premio Grace Murray Hopper de la ACM, la Medalla Benjamin Franklin, el Premio Emanuel R. Piore de la IEEE, o el Premio BBVA Fronteras del Conocimiento. Es miembro de la Academia Nacional de Ciencias de los Estados Unidos.

Ha sido conferenciante plenaria en el Congreso Internacional de Matemáticos (ICM) de 2002 y conferenciante invitada en el ICM de 1990, así como en numerosos otros congresos, tanto en matemáticas como en criptografía y ciencias de la computación. Entre sus numerosos alumnos figura Johan Håstad, al que ya he mencionado al hablar de la dificultad de aproximar el MAX-CLIQUE de un grafo.

Irit Dinur

Irit Dinur nació en 1973. Se doctoró en la Universidad de Tel-Aviv en 2001 bajo la dirección de Shmuel Safra. Después de estancias postdoctorales en el Instituto de Estudios Avanzados de Princeton, en el Instituto de Investigación de NEC y en la Universidad de Berkeley (como *Miller Fellow*), se unió al Insituto Weizmann de Israel, donde es catedrática en ciencias de la computación.

Su demostración del Teorema PCP en 2006 le valió fama mundial y numerosos reconocimientos. Entre otros, fue conferenciante plenaria del ICM 2010 y ha obtenido los premios Gödel y Erdös.

Thomas Vidick

Thomas Vidick nació en 1982 en Bélgica. Estudió matemáticas en la *École Normale Supérieure* de París. Realizó un máster en París VII en ciencias de la computación, bajo la dirección de Julia Kempe, donde ya empezó a trabajar en juegos no locales, tema que continuó en su tesis doctoral en Berkeley bajo la dirección de Umesh Vazirani. Tras defender su tesis en 2011, obtuvo una plaza postdoctoral en el MIT, supervisada por Scott Aaronson. Desde el 2014 está en el Caltech, donde es catedrático en ciencias de la computación desde 2018. Es el director del Centro para las Matemáticas de la Información (CMI) del Caltech.

Ha obtenido numerosas distinciones, entre las que destacan el *Presidential Early-Career Award*, o el *Simons Investigator Award*. Ha sido conferenciante plenario del Congreso Internacional de Física Matemática (ICMP) en 2021 y conferenciante invitado del ICM en 2022.

Aunque no hemos llegado a colaborar juntos, he tenido el placer de hablar largo y tendido de juegos no locales con Thomas Vidick en numerosas ocasiones a lo largo de los últimos años. Su finura y profundidad de pensamiento solo son comparables con su carácter abierto, humilde y generoso.

Gilles Pisier

Gilles Pisier nació en 1950 en Nueva Caledonia. Tras licenciarse en la École Polytechnique de París en 1972 realizó posteriormente la tesis doctoral en París VII bajo la dirección de Laurent Schwartz, que finalizó en 1977. Para entonces ya había producido 16 artículos. Desde 1981 es catedrático de matemáticas en Paris VI, puesto que, desde 1985, combina con la Cátedra A.G. y M.E. Owen de Matemáticas en la Universidad A&M de Texas.

Entre sus numerosos reconocimientos figuran el Premio Salem, el Premio Ostrowski y la Medalla Stefan Banach. Fue conferenciante invitado en el ICM de 1983 y conferenciante plenario en el ICM de 1998, precisamente presentando la teoría de espacios de operadores y algunas de sus aplicaciones.

Conocí a Gilles Pisier por primera vez durante mi doctorado. Él visitaba la Universidad Complutense y le conté uno de los problemas en los que estaba trabajando, relacionado con la generalización de los resultados de Grothendieck a productos tensoriales de más de dos espacios. Recuerdo que le planteé un punto en el que estaba atascado y cuál era el resultado que esperaba que fuera cierto. Cuando me disponía a contarle el camino que estaba intentando seguir para probarlo me dijo: "Espera". Pensó durante no más de dos o tres minutos, al cabo de los cuales se levantó y me dijo: "Lo que intentas probar es cierto, y la demostración es esta" y escribió sin titubear una demostración nada sencilla, y muy elegante por cierto, del resultado. Como pueden imaginar, quedé maravillado.

Marius Junge

Marius Junge nació en 1962 en Hannover, Alemania. Estudió matemáticas en la Unviersidad Christian-Albrechts de Kiel, donde también realizó su doctorado bajo la supervisión de Hermann König, finalizando en

1991. Permaneció en la misma universidad hasta que en 1999 se trasladó a la Universidad de Illinois en Urbana Champaign, donde continúa actualmente y en la que es catedrático de matemáticas desde 2007.

Mi estrecha colaboración con Marius Junge se remonta al año 2003. Yo estaba haciendo mi tesis doctoral y acababa de volver de una estancia en la Universidad Estatal de Kent en Estados Unidos donde, por consejo de Andrew Tonge, había estado estudiando la teoría de los espacios de operadores. Entre otras cosas, había intentado probar (sin éxito) una versión para tres espacios del Teorema de Grothendieck que era natural en ese contexto. Con el objetivo de aprender más sobre espacios de operadores invitamos a Marius Junge a darnos un curso sobre el tema en la Universidad Complutense. Recuerdo que a mitad del curso nos preguntó: "Me gustaría saber por qué estoy aquí". Entonces le expliqué el problema que había estado intentando resolver y, para mi sorpresa, me dijo: "Yo lo he resuelto. Tengo un contraejemplo. Pero no me parece lo suficientemente interesante para publicarlo". Dos años después de aquello yo había cambiado ya de tema de investigación y estaba trabajando como investigador postdoctoral en el Instituto Max Planck de Óptica Cuántica, bajo la dirección de Ignacio Cirac, Académico de esta casa. Allí me di cuenta de que el contraejemplo de Marius Junge tenía, de hecho, un gran interés en el contexto de los juegos no locales. Así que iniciamos una primera colaboración que concluyó unos años después en el artículo [84]. Desde entonces, Marius Junge se fue interesando cada vez más por la aplicación de las técnicas de las que era experto en el área de la información cuántica, convirtiéndose en uno de los referentes mundiales del campo. He tenido la fortuna de colaborar con él en siete artículos hasta ahora y siempre quedo asombrado (y exhausto) de la enorme energía que derrocha en cada sesión de trabajo.

8. DESPEDIDA

Hablando de quedar exhausto, no quiero cansarles más. Creo que llegó el momento de poner el punto y final a este discurso, que espero hayan disfrutado. Pero no quiero despedirme sin agradecer antes a todas las personas que, de una manera u otra, han contribuído a que yo esté hoy aquí. "*De gente bien nacida es agradecer los beneficios que reciben y uno de los pecados que más a Dios ofende es la ingratitud*" decía Don Quijote.

En primer lugar, y por encima de todo, quiero agradecer a mi familia: a mis padres, Juan y Teresa; a mis hermanos, Lucas, Pablo y Jesús; a mis amigos, que siempre he considerado como parte de mi familia; y, cómo no, a mi mujer Rut y a mis hijos Irene y Juan. Gracias por apoyarme siempre y recordarme que, por mucho que me gusten las matemáticas, hay (muchas) cosas mucho más importantes. Gracias por los mil proyectos que hemos compartido juntos y por los que están por venir.

También quería agradecer a mis maestros, que han sido muchos y de los que tanto he aprendido: a José Luis Castaño, mi profesor de matemáticas y física en Bachillerato, que me inculcó el amor por ambas disciplinas; a Pilar Cembranos, que hizo que me enamorara del análisis matemático; a Ignacio Sols y José María Montesinos, que me enseñaron que matemática no hay más que una; a Ignacio Villanueva, Joe Diestel y Andreas Defant, que me ayudaron a descubrir la riqueza de la teoría local de los espacios de Banach; a Marius Junge, por enseñarme con enorme paciencia básicamente todo lo que sé sobre espacios de operadores; a Michael Wolf, que ha sido como un hermano mayor para mí desde que empecé a trabajar en teoría de la información cuántica; y por supuesto, a Fernando Bombal y a Ignacio Cirac, a los que ya he mencionado al principio del discurso. Sería imposible imaginar mi trayectoria científica sin todos ellos.

Es igualmente cierto que nada de lo que he hecho hubiera sido posible sin mis colaboradores, en los que incluyo, por supuesto, a los estudiantes de doctorado e investigadores postdoctorales a los que he tenido el privilegio de acompañar a lo largo de estos años. Y lo digo con total sinceridad. Echando la vista atrás y recordando cómo surgieron las ideas clave de muchos de nuestros artículos, creo que jamás hubiéramos llegado a ellas sin las numerosas sesiones de trabajo conjunto en la pizarra, algunas maratonianas. Son además esas sesiones de trabajo, precisamente, las que hacen

de este oficio nuestro un trabajo tan enriquecedor a nivel personal y humano. Hay pocas cosas tan gratificantes, y que unan tanto a las personas, como dar lo mejor de cada uno para crear algo juntos.

Por último, quiero acabar como empecé, agradeciendo de nuevo a los miembros de la Real Academia de Ciencias por el honor que me han concedido al acogerme entre ellos.

Muchas gracias por su atención.

Bibliografía

[1] Dorit Aharonov, Itai Arad, and Thomas Vidick, *Guest column: the quantum PCP conjecture*, ACM SIGACT News **44** (2013), no. 2, 47–79.

[2] Noga Alon and Assaf Naor, *Approximating the cut-norm via Grothendieck's inequality*, Proceedings of the thirty-sixth annual ACM symposium on Theory of Computing, 2004, pp. 72–80.

[3] Abderramán Amr and Ignacio Villanueva, *Quantum one-way versus classical two-way communication in XOR games*, Quantum Information Processing **20** (2021), no. 2, 1–17.

[4] Kenneth Appel and Wolfgang Haken, *Every Planar Map is Four Colorable*, Contemporary Mathematics, volume 98, AMS, 1989.

[5] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, *Simple and tight device-independent security proofs*, SIAM Journal on Computing **48** (2019), no. 1, 181–225.

[6] Alain Aspect, Jean Dalibard, and Gérard Roger, *Experimental test of Bell's inequalities using time-varying analyzers*, Physical Review Letters **49** (1982), no. 25, 1804.

[7] Alain Aspect, Philippe Grangier, and Gérard Roger, *Experimental tests of realistic local theories via Bell's theorem*, Physical Review Letters **47** (1981), no. 7, 460.

[8] _____, *Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities*, Physical Review Letters **49** (1982), no. 2, 91.

[9] Francisco Barahona, Martin Grötschel, Michael Jünger, and Gerhard Reinelt, *An application of combinatorial optimization to statistical physics and circuit layout design*, Operations Research **36** (1988), no. 3, 493–513.

[10] Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu, *Quantum nonlocality, Bell inequalities, and the memory loophole*, Physical Review A **66** (2002), no. 4, 042111.

[11] Salman Beigi and Robert König, *Simplified instantaneous non-local quantum computation with applications to position-based cryptography*, New Journal of Physics **13** (2011), no. 9, 093036.

[12] John S. Bell, *On the Einstein Podolsky Rosen paradox*, Physics Physique Fizika **1** (1964), no. 3, 195.

[13] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson, *Multi-prover interactive proofs: How to remove intractability assumptions*, Proceedings of the twentieth annual ACM symposium on Theory of Computing, ACM, 1988, pp. 113–131.

[14] Ron Blei, *Analysis in Integer and Fractional Dimensions*, Cambridge University Press, 2001.

[15] Fernando Bombal, *Análisis funcional: una perspectiva histórica*, Seminar of Mathematical Analysis: Proceedings, Universities of Malaga and Seville (Spain), September 2002-February 2003, no. 64, 2003.

[16] Fernando Bombal, David Pérez-García, and Ignacio Villanueva, *Multilinear extensions of Grothendieck's theorem*, The Quarterly Journal of Mathematics **55** (2004), no. 4, 441–450.

[17] Jop Briët and Carlos Palazuelos, *Failure of the trilinear operator space Grothendieck theorem*, Discrete Analysis (2019), 8805.

[18] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner, *Position-based quantum cryptography: Impossibility and constructions*, SIAM Journal on Computing **43** (2014), no. 1, 150–178.

[19] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf, *Nonlocality and communication complexity*, Reviews of Modern Physics **82** (2010), no. 1, 665.

[20] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman, *The garden-hose model*, Proceedings of the 4th conference on Innovations in Theoretical Computer Science, 2013, pp. 145–158.

[21] Philip G. Burke and Ian C. Percival, *John Stewart Bell. 28 July 1928 - 1 October 1990*, Biographical Memoirs of Fellows of the Royal Society **45** (1999), 3–17.

[22] Thomas Keith Carne, *Banach lattices and extensions of Grothendieck's inequality*, Journal of the London Mathematical Society **2** (1980), no. 3, 496–516.

[23] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky, *Position based cryptography*, Annual International Cryptology Conference CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, Springer, 2009, pp. 391–407.

[24] Well Y. Chiu, Mario Szegedy, Chengu Wang, and Yixin Xu, *The garden hose complexity for the equality function*, International Conference on Algorithmic Applications in Management, Lecture Notes in Computer Science, vol. 8546, Springer, 2014, pp. 112–123.

[25] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, *Proposed experiment to test local hidden-variable theories*, Physical Review Letters **23** (1969), no. 15, 880.

[26] Alain Connes, *Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$*, Annals of Mathematics **104** (1976), 73–115.

[27] Stephen A. Cook, *The complexity of theorem-proving procedures*, Proceedings of the third annual ACM symposium on Theory of Computing, 1971, pp. 151–158.

[28] _____, *The P versus NP problem. Description of the problem*, Clay Mathematics Institute (2000).

[29] Tom Cooney, Marius Junge, Carlos Palazuelos, and David Pérez-García, *Rank-one quantum games*, Computational Complexity **24** (2015), no. 1, 133–196.

[30] Andreas Defant and Klaus Floret, *Tensor Norms and Operator Ideals*, Elsevier, 1992.

[31] Yfke Dulek, Christian Schaffner, and Florian Speelman, *Quantum homomorphic encryption for polynomial-sized circuits*, Annual International Cryptology Conference CRYPTO 2016, Lecture Notes in Computer Science vol. 9816, Springer, 2016, pp. 3–32.

[32] Frederic Dupuis, Omar Fawzi, and Renato Renner, *Entropy accumulation*, Communications in Mathematical Physics **379** (2020), no. 3, 867–913.

[33] Ken Dykema, Vern I. Paulsen, and Jitendra Prakash, *Non-closure of the set of quantum correlations via graphs*, Communications in Mathematical Physics **365** (2019), no. 3, 1125–1142.

[34] Edward Effros and Zhong-Jin Ruan, *Operator Spaces*, Oxford University Press, 2000.

[35] Albert Einstein, Boris Podolsky, and Nathan Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Physical Review **47** (1935), no. 10, 777.

[36] Artur Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters **67** (1991), no. 6, 661–663.

[37] Uriel Feige and Joe Kilian, *Zero knowledge and the chromatic number*, Journal of Computer and System Sciences **57** (1998), no. 2, 187–199.

[38] Leon Festinger, *The analysis of sociograms using matrix algebra*, Human Relations **2** (1949), no. 2, 153–158.

[39] Klaus Floret, *Natural norms on symmetric tensor products of normed spaces*, Note di Matematica **17** (1997), 153–188.

[40] Lester Randolph Ford and Delbert R. Fulkerson, *Maximal flow through a network*, Canadian Journal of Mathematics **8** (1956), 399–404.

[41] Elaine Forsyth and Leo Katz, *A matrix approach to the analysis of sociometric data: preliminary report*, Sociometry **9** (1946), no. 4, 340–347.

[42] Leslie R. Foulds, *Graph Theory and Applications*, Springer-Verlag, New York, 1992.

[43] Tobias Fritz, *Tsirelson's problem and Kirchberg's conjecture*, Reviews in Mathematical Physics **24** (2012), no. 05, 1250012.

[44] Michael R. Garey and David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, W.H. Freeman and Co., New York, 1979.

[45] Marissa Giustina, Marijn A.M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al., *Significant-loophole-free test of Bell's theorem with entangled photons*, Physical Review Letters **115** (2015), no. 25, 250401.

[46] Michel X. Goemans and David P. Williamson, *Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming*, Journal of the ACM (JACM) **42** (1995), no. 6, 1115–1145.

[47] William Timothy Gowers and Omid Hatami, *Inverse and stability theorems for approximate representations of finite groups*, Sbornik: Mathematics **208** (2017), no. 12, 1784.

[48] Alexandre Grothendieck, *Résumé de la théorie métrique des produits tensoriels topologiques*, Boletim da Sociedade de Matemática de São Paulo **8** (1956), 1–79.

[49] Johan Håstad, *Clique is hard to approximate within* $n^{1-\varepsilon}$, Acta Mathematica **182** (1999), 105–142.

[50] _____, *Some optimal inapproximability results*, Journal of the ACM (JACM) **48** (2001), no. 4, 798–859.

[51] Bas Hensen, Hannes Bernien, Anaïs E. Dréau, Andreas Reiserer, Norbert Kalb, Machiel S. Blok, Just Ruitenberg, Raymond F.L. Vermeulen, Raymond N. Schouten, Carlos Abellán, et al., *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature **526** (2015), 682–686.

[52] Christopher J. Hillar and Lek-Heng Lim, *Most tensor problems are NP-hard*, Journal of the ACM (JACM) **60** (2013), no. 6, 1–39.

[53] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen, *MIP *= RE*, Communications of the ACM **64** (2021), no. 11, 131–138.

[54] Marius Junge, Aleksander M. Kubicki, Carlos Palazuelos, and David Pérez-García, *Geometry of Banach spaces: a new route towards position based cryptography*, Communications in Mathematical Physics **394** (2022), 1–54.

[55] Marius Junge, Miguel Navascues, Carlos Palazuelos, David Perez-Garcia, Volkher B. Scholz, and Reinhard F. Werner, *Connes' embedding problem and Tsirelson's problem*, Journal of Mathematical Physics **52** (2011), no. 1, 012102.

[56] Marius Junge and Carlos Palazuelos, *Large violation of Bell inequalities with low entanglement*, Communications in Mathematical Physics **306** (2011), no. 3, 695–746.

[57] Marius Junge, Carlos Palazuelos, David Pérez-García, Ignacio Villanueva, and Michael M. Wolf, *Operator space theory: a natural framework for Bell inequalities*, Physical Review Letters **104** (2010), no. 17, 170405.

[58] _____, *Unbounded violations of bipartite Bell inequalities via operator space theory*, Communications in Mathematical Physics **300** (2010), no. 3, 715–739.

[59] David Kazhdan, *On ε-representations*, Israel Journal of Mathematics **43** (1982), no. 4, 315–323.

[60] Adrian Kent, *Coin tossing is strictly weaker than bit commitment*, Physical Review Letters **83** (1999), no. 25, 5382.

[61] _____, *Unconditionally secure bit commitment*, Physical Review Letters **83** (1999), no. 7, 1447.

[62] Subhash Khot, *On the power of unique 2-prover 1-round games*, Proceedings of the thiry-fourth annual ACM symposium on Theory of Computing, 2002, pp. 767–775.

[63] Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O'Donnell, *Optimal inapproximability results for MAX-CUT and other 2-variable CSPs?*, SIAM Journal on Computing **37** (2007), no. 1, 319–357.

[64] Hartmut Klauck and Supartha Podder, *New bounds for the garden-hose model*, Proceedings of the 34th International Conference on Foundation of Software Technology and Theoretical Computer Science, 2014, pp. 481–492.

[65] Jean-Louis Krivine, *Sur la constante de Grothendieck*, Comptes Rendus de l'Académie des Sciences, Paris, Series AB **284** (1977), no. 8, A445–A446.

[66] Eyal Kushilevitz, *Communication Complexity*, Advances in Computers, vol. **44**, Elsevier, 1997, pp. 331–360.

[67] Leonid Anatolevich Levin, *Universal sequential search problems*, Problemy Peredachi Informatsii **9** (1973), no. 3, 115–116.

[68] Zheng-Da Li, Ya-Li Mao, Mirjam Weilenmann, Armin Tavakoli, Hu Chen, Lixin Feng, Sheng-Jun Yang, Marc-Olivier Renou, David Trillo, Thinh P Le, et al., *Testing real quantum theory in an optical quantum network*, Physical Review Letters **128** (2022), no. 4, 040402.

[69] Joram Lindenstrauss and Vitali D. Milman, *The local theory of normed spaces and its applications to convexity*, Handbook of Convex Geometry, Elsevier, 1993, pp. 1149–1220.

[70] Joram Lindenstrauss and Aleksander Pełczynski, *Absolutely summing operators in $\mathcal{L}_p$-spaces and their applications*, Studia Mathematica **29** (1968), no. 3, 275–326.

[71] Yang Liu, Yuan Cao, Marcos Curty, Sheng-Kai Liao, Jian Wang, Ke Cui, Yu-Huai Li, Ze-Hong Lin, Qi-Chao Sun, Dong-Dong Li, et al., *Experimental unconditionally secure bit commitment*, Physical Review Letters **112** (2014), no. 1, 010504.

[72] Carsten Lund and Mihalis Yannakakis, *On the hardness of approximating minimization problems*, Journal of the ACM (JACM) **41** (1994), no. 5, 960–981.

[73] Tommaso Lunghi, Jedrzej Kaniewski, Felix Bussieres, Raphael Houlmann, Marco Tomamichel, Adrian Kent, Nicolas Gisin, Stephanie Wehner, and Hugo Zbinden, *Experimental bit commitment based on quantum communication and special relativity*, Physical Review Letters **111** (2013), no. 18, 180504.

[74] Tommaso Lunghi, Jedrzej Kaniewski, Felix Bussieres, Raphael Houlmann, Marco Tomamichel, Stephanie Wehner, and Hugo Zbinden, *Practical relativistic bit commitment*, Physical Review Letters **115** (2015), no. 3, 030502.

[75] Juan Maldacena, *The large-N limit of superconformal field theories and supergravity*, International Journal of Theoretical Physics **38** (1999), no. 4, 1113–1133.

[76] Alex May, Geoff Penington, and Jonathan Sorce, *Holographic scattering requires a connected entanglement wedge*, Journal of High Energy Physics **2020** (2020), no. 8, 1–34.

[77] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani, *Robust self-testing of the singlet*, Journal of Physics A: Mathematical and Theoretical **45** (2012), no. 45, 455304.

[78] David Mumford and John Tate, *Alexander Grothendieck (1928–2014)*, Nature **517** (2015), 272–272.

[79] Miguel Navascués, Stefano Pironio, and Antonio Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*, New Journal of Physics **10** (2008), no. 7, 073013.

[80] Narutaka Ozawa, *About the Connes embedding conjecture*, Japanese Journal of Mathematics **8** (2013), no. 1, 147–183.

[81] Carlos Palazuelos and Thomas Vidick, *Survey on nonlocal games and operator space theory*, Journal of Mathematical Physics **57** (2016), no. 1, 015220.

[82] David Pérez-García, *The inclusion theorem for multiple summing operators*, Studia Mathematica **165** (2004), 275–290.

[83] David Pérez-García and Ignacio Villanueva, *Multiple summing operators on Banach spaces*, Journal of Mathematical Analysis and Applications **285** (2003), no. 1, 86–96.

[84] David Pérez-García, Michael M. Wolf, Carlos Palazuelos, Ignacio Villanueva, and Marius Junge, *Unbounded violation of tripartite Bell inequalities*, Communications in Mathematical Physics **279** (2008), no. 2, 455–486.

[85] Albrecht Pietsch, *Absolut p-summierende Abbildungenin normierten Raumen*, Studia Mathematica **28** (1967), 333–353.

[86] _____, *History of Banach spaces and linear operators*, Springer Science & Business Media, 2007.

[87] Gilles Pisier, *Introduction to Operator Space Theory*, Cambridge University Press, 2003.

[88] _____, *Grothendieck's theorem, past and present*, Bulletin of the American Mathematical Society **49** (2012), no. 2, 237–323.

[89] _____, *Tensor Products of C*—Algebras and Operator Spaces: The Connes–Kirchberg Problem*, London Mathematical Society Student Texts, Cambridge University Press, 2020.

[90] Prasad Raghavendra and David Steurer, *Towards computing the Grothendieck constant*, Proceedings of the Twentieth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, 2009, pp. 525–534.

[91] Ran Raz, *A parallel repetition theorem*, SIAM Journal on Computing **27** (1998), no. 3, 763–803.

[92] Marc-Olivier Renou, David Trillo, Mirjam Weilenmann, Thinh P. Le, Armin Tavakoli, Nicolas Gisin, Antonio Acín, and Miguel Navascués, *Quantum theory based on real numbers can be experimentally falsified*, Nature **600** (2021), 625–629.

[93] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, et al., *Strong loophole-free test of local realism*, Physical Review Letters **115** (2015), no. 25, 250402.

[94] Michael Sipser, *The history and status of the P versus NP question*, Proceedings of the twenty-fourth annual ACM symposium on Theory of Computing, 1992, pp. 603–618.

[95] William Slofstra, *The set of quantum correlations is not closed*, Forum of Mathematics, Pi **7** (2019).

[96] _____, *Tsirelson's problem and an embedding theorem for groups arising from non-local games*, Journal of the American Mathematical Society **33** (2020), no. 1, 1–56.

[97] Stephen J. Summers and Reinhard F. Werner, *Maximal violation of Bell's inequalities is generic in quantum field theory*, Communications in Mathematical Physics **110** (1987), no. 2, 247–259.

[98] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner, *A monogamy-of-entanglement game with applications to device-independent quantum cryptography*, New Journal of Physics **15** (2013), no. 10, 103002.

[99] Boris S. Tsirelson, *Quantum generalizations of Bell's inequality*, Letters in Mathematical Physics **4** (1980), no. 2, 93–100.

[100] _____, *Quantum analogues of the Bell inequalities. The case of two spatially separated domains*, Journal of Soviet Mathematics **36** (1987), no. 4, 557–570.

[101] _____, *Some results and problems on quantum Bell-type inequalities*, Hadronic Journal Supplement **8** (1993), no. 4, 329–345.

[102] Umesh Vazirani and Thomas Vidick, *Fully device independent quantum key distribution*, Communications of the ACM **62** (2019), no. 4, 133–133.

[103] Thomas Vidick, *Pauli braiding*, unpublished note (2017).

[104] _____, *Erratum: Three-player entangled XOR games are NP-hard to approximate*, SIAM Journal on Computing **49** (2020), no. 6, 1423–1427.

[105] Robin J. Wilson, *History of Graph Theory*, from: Handbook of Graph Theory, CRC Press, 2013.

[106] Edward Witten, *Anti-de Sitter space and holography*, Advances in Theoretical and Mathematical Physics **2** (1998), 253–291.

[107] Elie Wolfe, Alejandro Pozas-Kerstjens, Matan Grinberg, Denis Rosset, Antonio Acín, and Miguel Navascués, *Quantum inflation: A general approach to quantum causal compatibility*, Physical Review X **11** (2021), no. 2, 021043.

[108] William K. Wootters and Wojciech H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.

Parte II

CONTESTACIÓN DEL EXMO. SR. D. FERNANDO BOMBAL GORDÓN

Excmo. Sr. Presidente.
Excmas. Sras. Académicas.
Excmos. Sres. Académicos.
Señoras y señores.

Con profundo agradecimiento y una gran satisfacción he recibido el encargo de contestar a su magistral discurso y dar la bienvenida a esta Real Academia a mi querido amigo D. David Pérez García.

Nacido en Guadalajara el 14 de octubre de 1977, David fue el segundo de cuatro hermanos. Sus padres, Juan y Teresa, eran ambos profesores de matemáticas en el Instituto Brianda de Mendoza de Guadalajara, uno de los centros de educación secundaria más antiguos de España. David cursó sus estudios de educación primaria y secundaria en el Colegio de los Salesianos de Guadalajara. En 1995 inició sus estudios de Matemáticas en la Universidad Complutense de Madrid, que finalizó en 2000. Sus padres, muy queridos y respetados por sus compañeros y alumnos, inculcaron a sus hijos el valor del estudio y la cultura del esfuerzo. Y, ciertamente, a la vista está que consiguieron plenamente su objetivo.

Siempre he sentido un gran respeto y admiración por mis maestros y un indisimulado orgullo por mis discípulos, por lo que haya podido contribuir a su formación y hábitos de trabajo. Y este orgullo está más que justificado en el caso de David. Le conocí a finales del pasado siglo, cuando era alumno en la Facultad de Ciencias Matemáticas de la Universidad Complutense de Madrid y desde el principio pude apreciar su vocación entusiasta y su brillantez. Sus respuestas a las distintas pruebas y ejercicios destacaban por su elegancia y brevedad, abordando con precisión y originalidad los temas propuestos. Por ello no lo dudé cuando me propuso le avalara como Director en su solicitud de una Beca de Formación de Personal Investigador y después, para iniciar su Tesis Doctoral. Por entonces yo estaba interesado en el estudio y representación de polinomios y operadores multilineales continuos en distintos espacios funcionales, trabajando en colaboración con el profesor D. Ignacio Villanueva, al que había dirigido su Tesis Doctoral titulada *Operadores multilineales en espacios de funciones continuas*. En ella habían quedado diversos problemas pendientes, así que de mutuo acuerdo decidimos que este tema podía ser adecuado para David y codirigir su Tesis entre ambos. Pero pronto la enorme capacidad de trabajo de David nos hizo ir ampliando el objetivo, tratando ahora de encontrar una teoría satisfactoria de los operadores p-sumantes

que extendiera al caso multilineal los importantes resultados de la teoría iniciada por Grothendieck en su *Résumé de la théorie métrique des produits tensoriels topologiques* y reformulada por A. Pietsch, J. Lindenstrauss y A. Pelczynski a finales de los años 60 del pasado siglo. A partir de los años 80 hay un gran interés en trasladar al caso multilineal la teoría de ideales lineales de operadores, con relativo éxito en muchos casos, pero no en el de los operadores p-sumantes. En su Tesis, *Operadores multilineales absolutamente sumantes*, defendida en enero de 2004, David introduce la *buena* definición de operador *p*-sumante en el caso multilineal, que le permite recuperar gran parte de los resultados de la teoría lineal, y la compara con otras definiciones existentes poniendo de manifiesto sus diferencias y ventajas. En el desarrollo de la misma, David adquirió un enorme conocimiento y habilidad en el uso de las normas tensoriales, que le iban a resultar de gran utilidad en sus trabajos posteriores.

Poco antes de acabar la tesis doctoral, obtuvo una plaza de Ayudante, y más tarde de Ayudante Doctor, en la Universidad Rey Juan Carlos de Madrid, donde permaneció hasta finales de 2006.

Parafraseando a Haruki Murakami, *deambulamos sin rumbo fijo por el gran continente de la casualidad*, y a veces tenemos suerte y llegamos a un buen destino: Como cita David en su discurso, en el verano de 2004 asistió a un curso sobre información y computación cuántica en la Universidad Menéndez Pelayo, impartido por el profesor Ignacio Cirac. Supongo que asistiría por curiosidad intelectual, pues él mismo confiesa su total desconocimiento de los conceptos más básicos de la física cuántica. Sin embargo, David se percató de que algunas de las técnicas desarrolladas en su Tesis podían ser útiles para abordar ciertas cuestiones planteadas en el citado curso. Y sin dudarlo, aceptó la oferta del profesor Cirac de una posición postdoctoral en el Instituto Max Planck de Óptica Cuántica de Garching, solicitando y obteniendo una licencia por estudios de abril de 2005 a febrero de 2006. Allí empezó a trabajar en el área de las tecnologías cuánticas y los problemas matemáticos asociados a las mismas, su principal área de investigación desde entonces.

A su regreso, tiene lugar otro hito importante en la vida de David: en 2006 se casa con Rut, su novia de toda la vida (llevaban juntos desde 1993). Sus hijos Irene y Juan nacieron, respectivamente, en 2010 y 2013.

Y también obtiene un contrato Ramón y Cajal con el que se reincorporó al Departamento de Análisis Matemático de la UCM a finales de 2006. Obtuvo una de las plazas de Habilitación Nacional en el área de Análisis Matemático en 2007 y una plaza de Profesor Titular de Universidad en la UCM ese mismo año. Desde agosto de 2016 es Catedrático de Universidad en la UCM.

A lo largo de sus años de labor investigadora, David Pérez ha abordado muy variados y distintos temas, en los que ha dejado su impronta. A continuación, quisiera comentar brevemente algunos de ellos:

1.- Productos tensoriales topológicos y operadores multilineales.

Entre 2004 y 2009 David Pérez compaginó su interés en el área de la información cuántica con los temas de análisis funcional más relacionados con su Tesis. Además de resolver gran parte de los problemas planteados en la misma, obtuvo, con diversos coautores, importantes resultados sobre extensión de operadores multilineales, incondicionalidad de normas tensoriales, etc.

2.- Análisis complejo y geometría de espacios de Banach.

En colaboración con A. Defant, D. García y M. Maestre, en un extenso y profundo artículo publicado en Mathematische Annalen, obtuvieron una versión vectorial del famoso teorema de Bohr sobre la convergencia de las series de Dirichlet, que establece que la anchura de la banda (en el cuerpo de los números complejos) en el que una serie de Dirichlet dada converge uniforme pero no absolutamente, es a lo más 1/2. David y sus coautores probaron que para una serie de Dirichlet con coeficientes en un espacio de Banach X, esta banda tiene una anchura a lo más $1 - 1/\mathrm{Cot}(X)$, siendo Cot(X) el cotipo óptimo de X.

3.- Projected Entangled Pair States (PEPS) para describir y clasificar las fases cuánticas de la materia.

Junto con J.I. Cirac y N. Schuch, David inició en 2005 un programa para desarrollar la teoría matemática de los PEPS y utilizarla como herramienta para dar resultados matemáticos rigurosos sobre las fases cuánticas de la materia. Uno de los principales resultados ha sido el de caracterizar el orden topológico mediante ciertas simetrías en los tensores elementales que definen los PEPS. El orden topológico es una de las propiedades más interesantes y exóticas que pueden aparecer en los sistemas cuánticos y

está llamado a jugar un papel central en la actual carrera por construir un ordenador cuántico. El motivo es que los sistemas con orden topológico son inherentemente mucho más robustos al ruido y a imperfecciones. De hecho, David y sus coautores fueron pioneros en analizar el efecto de la temperatura en la robustez de las memorias cuánticas. La importancia del orden topológico ha venido reflejada por ejemplo, en la concesión del Premio Nobel de Física 2016.

4.- Teoría de la complejidad, desigualdades de Bell y criptografía.

Estos temas han ocupado gran parte de la actividad investigadora de David Pérez. El magnífico discurso que acabamos de escuchar está dedicado a explicar magistralmente el contenido y relaciones entre estos temas, así como las contribuciones más destacadas de David Pérez y sus coautores en estas áreas. Quizá la principal de estas contribuciones ha sido mostrar que la teoría local de espacios de Banach y los espacios de operadores son el lenguaje matemático apropiado para estudiar las desigualdades de Bell y los *Interactive Proof Systems*. Como ilustración de la potencia de dichas técnicas, según hemos escuchado en el Capítulo 5 de su discurso, David Pérez y sus coautores han logrado demostrar la posibilidad de encontrar dentro de la física cuántica violaciones arbitrariamente grandes de desigualdades de Bell, resolviendo así una antigua pregunta de Tsirelson. La conexión entre las desigualdades de Bell y el "*Connes embedding problem*" sobre la clasificación de las álgebras de von Neumann, descubierta por David Pérez y sus coautores, ha permitido el uso de técnicas de ciencias de la computación (asociadas al teorema PCP) para resolver finalmente ese problema fundamental en la teoría de las álgebras de operadores.

5.- Indecibilidad en problemas de física de la materia.

En 1931 K. Gödel sorprendió a la comunidad matemática con el artículo que lleva el expresivo título "*Sobre proposiciones formalmente indecidibles de Principia Mathematica y sistemas afines, I*". En él, Gödel prueba que todo sistema formal consistente y que contenga a la aritmética, es necesariamente *incompleto*, es decir, contiene enunciados legítimos del sistema que son *indecidibles*, esto es, ni su afirmación ni su negación son demostrables en el sistema. Unos años más tarde, en 1937, A. Turing muestra que los problemas de indecibilidad también se presentan en la teoría de la compu-

tación[1] al probar que el llamado *problema de la parada (halting problem)* es indecidible, es decir, que no existe un programa P que permita saber si cualquier programa concreto Q va a terminar tras un número finito de pasos o no[2].

Pues bien, un importante problema en mecánica cuántica, el llamado "*spectral gap problem*" consiste en determinar si dado un sistema cuántico formado por un gran número de partículas interactuando entre sí, la diferencia de energía entre el estado fundamental y el primer estado excitado del sistema está acotada inferiormente (es decir, el sistema es "*gapped*" en el lenguaje de los especialistas) o bien el sistema tiene un espectro continuo por encima del estado básico (el sistema es "*gapless*"). En un extenso trabajo titulado *Undecibility of the spectral gap* (publicado en Nature y en Forum of Mathematics Pi), David Pérez, junto con T. Cubitt y M. M. Wolf, han demostrado que el problema es algorítmicamente indecidible, es decir, dadas las matrices que describen las interacciones locales del sistema, no existe procedimiento (algoritmo) alguno para determinar si el sistema resultante será "*gapped*" o "*gapless*". Por tanto, existen interacciones microscópicas entre partículas para las que es imposible predecir el comportamiento macroscópico del material regido por dichas interacciones (en el sentido de que es indecidible decidir si el material es, por ejemplo, aislante o conductor). La prueba es muy técnica y consiste en demostrar que el problema en cuestión es equivalente al problema de la parada de Turing.

Una versión divulgativa de este trabajo fue la portada de Scientific American en Octubre de 2018, y fue incluido en el listado "*The Best Writing on Mathematics*" en 2019.

El profesor Pérez García ha publicado más de 100 artículos en revistas de primer orden en matemáticas, físicas y ciencias de la computación, incluyendo Nature, Nature Communications, PNAS, Physical Review Letters, Physical Review X, Communications in Mathematical Physics, Forum

[1] *On computable numbers, with an application to the Entscheidungsproblem*. Proc. London Math. Soc., vol **42** (1937), 230-265

[2] Por supuesto, para muchos programas concretos, pueden encontrarse pruebas de si se paran o no. Por ejemplo, el programa "*encontrar un número impar suma de dos pares*" no se para nunca; "*encontrar un número natural que no sea la suma de tres cuadrados*" se para para n=7; "*encontrar un número par mayor que 2 que no sea suma de dos primos*" nadie sabe a día de hoy si se parará o no (Conjetura de Goldbach).

of Mathematics Pi, Mathematische Annalen, Transactions of the AMS o IEEE Transactions of Information Theory. Sus contribuciones han recibido más de 8500 citas.

Su artículo de investigación "*Matrix Product State Representations*", con más de 1200 citas, ha sido seleccionado por Google Scholar como un "*classic paper*" en mecánica cuántica.

Como fruto de la calidad y relevancia de su investigación, David Pérez ha obtenido numerosos premios y reconocimientos, entre los que destacan:

- Premio Real Academia de Ciencias – Endesa 2012 a jóvenes matemáticos.
- Un proyecto Consolidator Grant del European Research Council (ERC).
- Premio Miguel Catalán (2017) a jóvenes investigadores.
- Premio Fundación Banco Sabadell en Ciencia y Tecnología (2019).
- Medalla Ramón y Cajal de la Real Academia de Ciencias (2021).

Desde 2018 es, además, Académico Correspondiente de esta Real Academia. En 2014 fue John Von Neumann Guest Professor de la Universidad Técnica de Múnich.

Es también el Editor de Sección en Información Cuántica de la revista Annales Henri Poincaré, y editor de Letters in Mathematical Physics. Ha formado parte del Comité de Programa del Congreso QIP, el más prestigioso en el área de la información cuántica, en sus ediciones de 2012, 2015, 2018, 2021 y 2022 (en este caso como Chair del Comité de Programa). Ha organizado también la sección de información cuántica en el International Congress of Mathematical Physics (ICMP) de 2021. Ha sido conferenciante invitado en el ICMP 2015, así como en numerosos congresos y workshops especializados (más de 50 charlas invitadas).

Ha realizado numerosas estancias en prestigiosos centros de investigación, como son Kent State University (EEUU), Oldenburg University (Alemania), California Institute of Technology (EEUU), Technical University Munich (Alemania), Kavli Institute for Theoretical Physics (EEUU), Institute Henri Poincaré (Francia), etc.

El grupo de investigación "*Matemáticas e Información Cuántica*", que David creó en 2007, no ha dejado de crecer desde entonces. Actualmente cuenta con 18 investigadores. El grupo ha recibido financiación de numerosos proyectos de investigación. David ha sido Investigador Principal de 12 de ellos.

Merece también destacar su labor de formación y dirección de investigación. David ha supervisado 9 tesis doctorales y a 14 investigadores postdoctorales.

Uno de los mayores méritos de David -que ha sido una constante en su investigación, como creo haber puesto de manifiesto en las líneas anteriores- ha sido la de introducir y desarrollar nuevas técnicas matemáticas en problemas centrales en otras áreas de las matemáticas, así como en física de la materia, teoría de la complejidad y, sobre todo, en el área de la información cuántica. Estas nuevas técnicas matemáticas han supuesto importantes avances, han permitido resolver preguntas abiertas muy antiguas y, tal vez lo más importante, han acabado consolidándose como técnicas centrales en los respectivos campos.

Quisiera ahora referirme brevemente al extraordinario discurso que nos acaba de regalar el profesor Pérez García. Se trata, a mi entender, de una verdadera exhibición de orfebrería científica, al mostrar de una manera rigurosa, clara y precisa las interrelaciones entre áreas tan aparentemente distintas como la teoría de la complejidad, los juegos no locales, la teoría de grafos y la mecánica cuántica, de la mano del análisis funcional. Ya me he referido anteriormente a parte del contenido del discurso, al citar algunos de los resultados relevantes del nuevo académico, y poco más podría añadir, tanto por mis limitados conocimientos en la mayoría de los temas tratados como por la claridad en su exposición.

Permítanme pues hacer una breve digresión en torno a las palabras de E. P. Wigner, Premio Nobel de Física de 1963 en su famoso artículo *The unreasonable effectiveness of Mathematics in the Natural Sciences*[3]:

> "*El milagro de la adecuación del lenguaje de las matemáticas para la formulación de las leyes físicas es un don maravilloso que ni entendemos ni merecemos.*"

[3]Commun. Appl. Math., 13 (1960), 1-14.

En efecto, es realmente sorprendente cómo las técnicas de productos tensoriales topológicos y la relación entre normas tensoriales, desarrolladas en el ámbito más abstracto de las matemáticas, aparecen ubicuamente en los distintos temas tratados en el discurso que acabamos de escuchar.

Muchos de los resultados citados y empleados por David Pérez tienen su origen en los trabajos de Alexander Grothendieck (un pequeño esquema biográfico aparece en el Capítulo 8 del discurso que estamos comentando), quizá más conocido por su revolucionario trabajo en Geometría Algebraica, que le valió la concesión de la Medalla Fields en 1966, que por sus contribuciones al Análisis Funcional, no menos revolucionarias[4].

El joven Grothendieck, siguiendo los consejos de H. Cartan y A. Weil, se incorpora a la Universidad de Nancy el curso 1950/51 para realizar sus estudios de doctorado con J. Dieudonné y L.Schwartz. Ambos estaban en la cúspide de su carrera académica. Schwartz acababa de recibir la medalla Fields por su fundamentación de la teoría de distribuciones. Y hete aquí que les llega un desconocido estudiante de provincias, con una limitada y poco ortodoxa educación matemática, pretendiendo estudiar con ellos. Probablemente para quitárselo de en medio, Schwartz le dio un artículo que acababa de publicar recientemente con Dieudonné ("*La dualité dans les espaces* $(\mathcal{F})$ *et* $(\mathcal{LF})$") y que incluía 14 cuestiones que no habían podido resolver, para que pensara sobre ellas. Al cabo de unas pocas semanas, según relata Schwartz en su autobiografía[5], Grothendieck volvió con la mitad de las cuestiones resueltas, utilizando técnicas e ideas realmente novedosas. Schwartz se dio cuenta rápidamente que había topado con un matemático de primer orden y le admitió en su Seminario.

El hecho de que Grothendieck no tuviera la nacionalidad francesa (sus documentos de identidad se perdieron en Alemania y durante muchos años viajó con un pasaporte de apátrida) dificultaban la posibilidad de otorgarle un puesto oficial de trabajo, por lo que los buenos oficios de Schwartz le consiguieron un puesto de profesor visitante en la Universidad de Sao Paulo en Brasil, donde permaneció entre 1953 y 1955.

---

[4] El lector interesado puede consultar el trabajo: F. Bombal, *Alexander Grothendieck's Work on Functional Analysis*, en "Advances Courses of Mathematical Analysis II", World Scientific Pub. (2007), 16-36.

[5] *Un mathématicien aux prises avec le siècle*. Editions Odile Jacob, 1997.

Por entonces Schwartz estaba iniciando la teoría de distribuciones vectoriales, esto es, el estudio del espacio $\mathcal{D}'(F) := L(\mathcal{D}, F)$ de los operadores lineales continuos del espacio *test* $D := D(\mathbb{R}^n)$ (el espacio de las funciones escalares C^∞ con soporte compacto, dotado de su topología límite inductivo usual) en el espacio localmente convexo F. La topología natural para este espacio era evidente, induciendo así una "buena" topología sobre su subespacio denso $\mathcal{D}' \otimes F$, pero esto no era obvio en general.

Así que Schwartz propuso a Grothendieck en la primavera de 1953, como problema de Tesis Doctoral, encontrar una "buena" topología en el producto tensorial $E \otimes F$ de dos espacios localmente convexos. Los productos tensoriales, aunque bien conocidos por sus propiedades algebraicas, apenas habían sido estudiados en el marco de los espacios vectoriales topológicos, por lo que Grothendieck tuvo que comenzar a explorar una "*terra incognita*".

A finales de julio Schwartz recibe de Grothendieck una carta, en cierto sentido decepcionante: en $E \otimes F$ hay *dos* topologías naturales, y son *diferentes* en general. Schwartz no sabe qué decir, ya que en $\mathcal{D}' \otimes F$ había solo *una* topología natural. Afortunadamente, dos semanas después llega una carta triunfal: ¡las dos topologías naturales coinciden en $\mathcal{D}' \otimes F$ (y con la usual)!

Las dos topologías naturales (que en el caso de espacios normados vienen dadas por sendas normas) son las que hoy conocemos como la topología *proyectiva* o topología π y la topología *inyectiva* o topología ε. La topología π es la "mayor" topología razonable (en un sentido preciso) y es la que linealiza a través del producto tensorial las aplicaciones bilineales *continuas*; la topología ε es la "menor" de las topologías razonables.

A lo largo de 1953 Grothendieck, desde Brasil, va remitiendo a Schwartz una imponente serie de resultados, que culminaron en la elaboración de su Tesis Doctoral: *Produits tensoriels topologiques et espaces nucléaires*, defendida en 1953 y publicada como volumen 16 en la prestigiosa colección "Memoirs of the American Mathematical Society" en 1955. Es un trabajo monumental de más de 300 páginas que contiene no solo los teoremas principales de la teoría de productos tensoriales topológicos, sino cantidad de nuevos métodos, técnicas e ideas seminales que iban a renovar el Análisis Funcional.

Grothendieck siguió trabajando intensamente en Análisis Funcional durante su estancia en Brasil. Publicó una serie de importantes artículos en revistas brasileñas, de los que hay que destacar su "*Résumé de la théorie métrique des produits tensoriels topologiques*", enviado al Boletín de la Sociedad Matemática de Sao Paulo en junio de 1954 y publicado en 1956. En opinión de A. Pietsch, "*el artículo más espectacular en la teoría moderna de los espacios de Banach*". Ignorado por su difícil redacción durante más de 10 años, en 1968 apareció un extenso artículo en Studia Mathematica de más de 50 páginas (Lindenstrauss & Pelczynski, 1968) intentando mostrar a la comunidad matemática algunas de las joyas ocultas en el *Résumé*. En su introducción, los autores declaran:

> "*The main purpose of the present paper is to give a new presentation as well as new applications of the results contained in Grothendieck's paper ...Though the theory of tensor products constructed in Grothendieck's paper has its intrinsic beauty we feel that the results of Grothendieck and their corollaries can be more clearly presented without the use of tensor products ...The paper of Grothendieck is quite hard to read and its results are not generally known even to experts in Banach space theory...*"

Y, en efecto, los autores evitaron el lenguaje de los productos tensoriales, usando sistemáticamente lo que ahora se conoce como *operadores p-sumantes*, que habían aparecido en otro artículo seminal de A. Pietsch publicado también en *Studia* en 1967.

Volviendo al *Resumé*, la idea subyacente en el trabajo es la de obtener nuevas clases de operadores entre espacios de Banach definiendo normas adecuadas en $E \otimes F$. Grothendieck establece un método para obtener normas tensoriales "razonables", que resulta ser precisamente las que están entre las normas ε y π. En el Capítulo 4 se establecen los resultados más profundos y de mayor alcance. En el Teorema 4.1, que Grothendieck llama *théorème fundamental de la théorie métrique des produits tensoriels*, establece que el operador identidad en un espacio de Hilbert cualquiera es lo que Grothendieck llama *preintegral* y que su norma preintegral está acotada por una constante universal K_G (*constante de Grothendieck*). Como cita David Pérez en su discurso, ese resultado se puede reinterpretar como

una desigualdad entre dos normas tensoriales en $\ell_1^n \otimes \ell_1^n$ [6]. Grothendieck no da ninguna justificación de la razón de designar como *fundamental* este teorema, aunque de él deriva importantes resultados.

Como acabamos de escuchar, muchos años después del trabajo de Grothendieck resulta que la formulación matemática correcta de aspectos fundamentales en la teoría de juegos no-locales, teoría de grafos o información cuántica involucra el uso de los productos tensoriales y el cómputo de diversas normas tensoriales y además el teorema de Grothendieck aparece por doquier. Se ha citado, por ejemplo, en el cálculo del MAX-CUT de un grafo G o bien cómo la constante de Grothendieck acota el cociente del sesgo cuántico y el clásico de un juego XOR de dos jugadores. También la importancia de obtener buenas versiones multilineales del teorema de Grothendieck, uno de los principales objetivos de la Tesis Doctoral de David Pérez.

Una vez más, la afirmación de Wigner aparece completamente justificada.

Querido amigo David, termino reiterándote la bienvenida a esta Real Academia, que a partir de ahora tendrá la suerte de contar con tu colaboración, tus conocimientos, entusiasmo y buen hacer.

Muchas gracias.

[6] La formulación que aparece en el discurso se encuentra en el citado artículo de Lindenstrauss y Pelczynski de 1968.