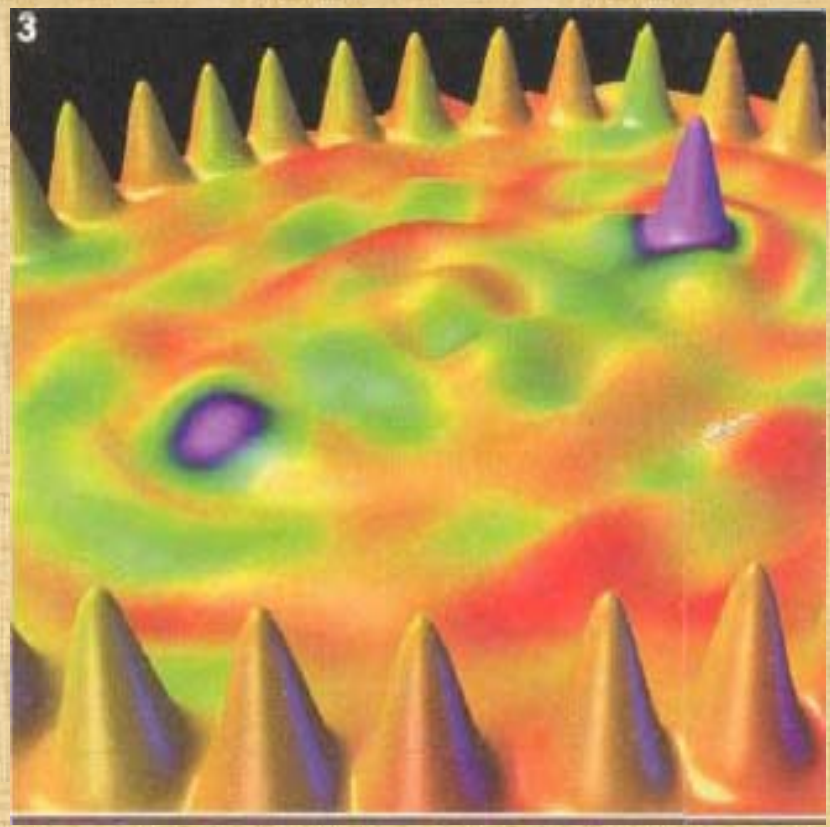
De la escritura secreta a la Criptografía Cuántica

Grabado antiguo con un retrato de Julio César



LA ESCRITURA SECRETA

- Los testimonios más antiguos se remontan a Herodoto.
- En “Las Historias” hizo una crónica de los conflictos entre Grecia y Persia en el siglo V a.C.
- Según Herodoto fue el “arte de la escritura secreta lo que salvó a Grecia de ser ocupada por Jerjes.

LA ESCRITURA SECRETA

- El prolongado enfrentamiento entre Grecia y Persia alcanzó su punto culminante cuando Jerjes comenzó a construir una ciudad en Persépolis.
- Llegaron tributos y regalos de todo el imperio y de los estados vecinos, con las notables excepciones de Atenas y Esparta.

LA ESCRITURA SECRETA

- Para vengar esta insolencia, Jerjes comenzó a movilizar una fuerza, declarando que “extenderemos el imperio de Persia de tal manera que sus límites serán el propio cielo de Dios, de forma que el Sol no brillará en ninguna tierra más allá de los límites de lo que es nuestro”.

LA ESCRITURA SECRETA

- Pasó los cinco años siguientes reuniendo en secreto la mayor fuerza de lucha de la Historia, y en el año 480 a.C. estuvo listo para lanzar un ataque sorpresa.

LA ESCRITURA SECRETA

- Sin embargo, la proliferación militar persa había sido presenciada por Demarato, un griego que había sido expulsado de su patria y vivía en la ciudad persa de Susa.

LA ESCRITURA SECRETA

- A pesar de estar exiliado, aún sentía cierta lealtad hacia Grecia, y decidió enviar un mensaje para advertir a los espartanos del plan de invasión de Jerjes.
- El desafío consistía en cómo enviar el mensaje sin que fuera interceptado por los guardas persas.

LA ESCRITURA SECRETA

- Herodoto escribió:
- *Como el peligro de que lo descubrieran era muy grande, sólo había una manera en que podía contribuir a que pasara el mensaje: retirar la cera de un par de tablillas de madera, escribir en la madera lo que Jerjes planeaba y luego volver a cubrir el mensaje con cera. De esta forma, las tablillas, al estar aparentemente en blanco, no ocasionarían problemas con los guardas del camino. Cuando el mensaje llegó a su destino, nadie fue capaz de adivinar el secreto, hasta que, según tengo entendido, la hija de Cleomenes, Gorgo, que era la esposa de Leónidas, lo vaticinó y les dijo a los demás que si quitaban la cera encontrarían algo escrito debajo, en la madera. Se hizo así; el mensaje quedó revelado y fue leído, y después fue comunicado a los demás griegos.*

LA ESCRITURA SECRETA

- Como resultado de esta advertencia, los hasta entonces indefensos griegos comenzaron a armarse.
- Los beneficios de las minas de plata pertenecientes al estado, que normalmente se distribuían entre los ciudadanos, fueron ahora transferidos a la Marina para la construcción de doscientas naves de guerra.

LA ESCRITURA SECRETA

- Jerjes había perdido el vital elemento de la sorpresa y, el 23 de septiembre del año 480 a.C., cuando la flota persa se aproximó a la bahía de Salamina, cerca de Atenas, los griegos estaban preparados.
- Aunque Jerjes creía que había atrapado a la marina griega, los griegos estaban incitando deliberadamente a las naves persas para que entraran en la bahía.

LA ESCRITURA SECRETA

- Los griegos sabían que sus naves, más pequeñas y menores en número, serían destruidas en el mar abierto, pero se dieron cuenta que entre los confines de la bahía podrían superar estratégicamente a los persas.
- Cuando el viento cambió de dirección, los persas fueron llevados por el viento al interior de la bahía, forzados a un enfrentamiento en los términos de los griegos.

LA ESCRITURA SECRETA

- La princesa persa Artemisa quedó rodeada por tres lados y trató de volver hacia el mar abierto, consiguiendo tan sólo chocar con una de sus propias naves.
- Entonces cundió el pánico, más naves persas chocaron entre sí y los griegos lanzaron un sangriento ataque.
- En menos de un día, las formidables fuerzas de Persia habían sido humilladas.

LA ESCRITURA SECRETA

- **La cabeza del mensajero.**
- La estrategia de Demarato para la comunicación secreta se basaba simplemente en la ocultación del mensaje.
- Herodoto narró también otro incidente en el que la ocultación fue suficiente para conseguir el paso seguro de un mensaje.

LA ESCRITURA SECRETA

- Él hizo la crónica de la historia de Histaiaeo, que quería alentar a Aristágoras de Mileto para que se rebelara contra el rey de Persia.

Grabado antiguo con un retrato de Julio César

Histaiaeo afeitó la cabeza del mensajero, escribió el mensaje en su cuero cabelludo y esperó a que le creciera el pelo

LA ESCRITURA SECRETA

- Para transmitir sus instrucciones de forma segura, Histaiaeo afeitó la cabeza de su mensajero, escribió el mensaje en su cuero cabelludo y luego esperó a que le volviera a crecer el pelo.
- Evidentemente, aquél era un período de la Historia que toleraba una cierta falta de urgencia.

LA ESCRITURA SECRETA

- El mensajero, que aparentemente no llevaba nada conflictivo, pudo viajar sin ser molestado.
- Al llegar a su destino, se afeitó la cabeza y se la mostró al receptor al que iba destinado el mensaje.

LA ESCRITURA SECRETA

- La comunicación secreta lograda mediante la ocultación de la existencia de un mensaje se conoce como esteganografía, derivado de la palabra griega «steganos», que significa «encubierto» y «graphein», que significa «escribir».

LA ESCRITURA SECRETA

- En los dos mil años que han transcurrido desde Herodoto, diversas formas de estenografía han sido utilizadas por todo el mundo.
- Por ejemplo, en la China antigua se escribían mensajes sobre seda fina, que luego era aplastada hasta formar una pelotita diminuta que se recubría de cera.
- Entonces el mensajero tragaba la bola de cera.

LA ESCRITURA SECRETA

- En el siglo XV, el científico italiano Giovanni Porta describió cómo esconder un mensaje dentro de un huevo cocido haciendo una tinta con una mezcla de una onza de alumbre y una pinta de vinagre, y luego escribiendo en la cáscara.

LA ESCRITURA SECRETA

- La solución penetra en la cáscara porosa y deja un mensaje en la superficie de la albúmina del huevo duro, que sólo se puede leer si se pela el huevo.
- La esteganografía incluye también la práctica de escribir con tinta invisible.

LA ESCRITURA SECRETA

- Ya en el siglo I, Plinio el Viejo explicó como la «leche» de la planta *Thithymallus* podía usarse como tinta invisible.
- Aunque se vuelve transparente al secarse, al calentarla suavemente se chamusca y se pone marrón.

LA ESCRITURA SECRETA

- Muchos fluidos orgánicos se comportan de manera similar, porque son ricos en carbono y se chamuscan fácilmente.
- De hecho, es sabido que los espías modernos a los que se les ha acabado su tinta invisible habitual improvisan utilizando su propia orina.
- La longevidad de la esteganografía corrobora que ofrece sin duda un nivel de seguridad, pero padece de una debilidad fundamental.

LA ESCRITURA SECRETA

- Si registran al mensajero y descubren el mensaje, el contenido de la comunicación secreta se revela en el acto.
- La interceptación del mensaje compromete inmediatamente toda la seguridad.

LA ESCRITURA SECRETA

- Un guarda concienzudo podría registrar rutinariamente a cualquier persona que cruce una frontera y raspar cualquier tablilla cubierta de cera, calentar cualquier hoja de papel en blanco, pelar huevos cocidos, afeitar la cabeza de alguien, y así sucesivamente, e inevitablemente se producirían ocasiones en las que el mensaje quedaría revelado.

LA ESCRITURA SECRETA

- Por eso, paralelamente al desarrollo de la esteganografía, se produjo la evolución de la criptografía, término derivado de la palabra griega «kryptos», que significa «escondido».

LA ESCRITURA SECRETA

- El objetivo de la criptografía no es ocultar la existencia de un mensaje, sino más bien ocultar su significado, un proceso que se conoce como codificación.
- Para hacer que el mensaje sea inteligible se codifica siguiendo un protocolo específico, sobre el cual se han puesto de acuerdo de antemano el emisor y el receptor a quien va dirigido.

LA ESCRITURA SECRETA

- De esta forma, dicho receptor puede invertir el protocolo codificador y hacer que el mensaje sea comprensible.
- La ventaja de la criptografía es que si el enemigo intercepta un mensaje cifrado, éste es ilegible.
- Sin conocer el protocolo codificador, al enemigo le resultaría difícil, cuando no imposible, recrear el mensaje original a partir del texto cifrado.

LA ESCRITURA SECRETA

- Aunque la criptografía y la esteganografía son independientes, es posible codificar y ocultar un mismo mensaje para aumentar al máximo la seguridad.
- Por ejemplo, el micropunto es una forma de esteganografía que se hizo popular durante la Segunda Guerra Mundial.

LA ESCRITURA SECRETA

- Agentes alemanes en Latinoamérica reducían fotográficamente una página de texto a un punto de menos de 1 milímetro de diámetro y luego escondían este micropunto sobre un punto y aparte de una carta aparentemente inocua.

LA ESCRITURA SECRETA

- La primera vez que el FBI descubrió un micropunto fue en 1941, siguiendo un soplo que decía que los norteamericanos debían buscar en la superficie de una carta un brillo diminuto, indicativo de un minúsculo film.
- Después de eso, los norteamericanos pudieron leer el contenido de la mayoría de los micropuntos interceptados, excepto cuando los agentes alemanes habían tomado la precaución extra de codificar su mensaje antes de reducirlo.

LA ESCRITURA SECRETA

- En tales casos de criptografía combinada con esteganografía, a veces los norteamericanos pudieron bloquear las comunicaciones, pero no lograron averiguar nueva información sobre la actividad del espionaje alemán.
- De las dos ramas de la comunicación secreta, la criptografía es la más poderosa a causa de su habilidad para evitar que la información caiga en manos enemigas.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- A su vez, la criptografía misma puede ser dividida en dos ramas, conocidas como «trasposición» y «sustitución».
- En la «trasposición», las letras del mensaje simplemente se colocan de otra manera, generando así un anagrama.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Para mensajes muy cortos, como los de una sola palabra, este método es relativamente inseguro porque sólo hay un número limitado de maneras de combinar un puñado de letras.
- Por ejemplo, tres letras sólo pueden ser combinadas de seis manera diferentes: por ejemplo, ron, rno, orn, onr, nro, nor.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Sin embargo, según el número de letras va incrementándose, el número de posibles combinaciones se dispara rápidamente, haciendo imposible volver al mensaje original a no ser que se conozca el proceso codificador exacto.
- Por ejemplo, considérese esta breve frase.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Contiene solamente 35 letras, y, sin embargo, existen más de 50.000.000.000.000.000.000.000.000.000.000 de combinaciones distintas entre ellas.
- Si una persona pudiera revisar una combinación por segundo y si todas las personas del mundo trabajaran día y noche, aún se necesitarían más de mil veces los siglos de vida del universo para revisar todas las combinaciones.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Una trasposición de letras realizada al azar parece ofrecer un nivel muy alto de seguridad, porque a un interceptor enemigo le resultaría muy poco práctico descodificar, incluso una breve frase.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Pero hay un inconveniente:
- La trasposición genera eficazmente un anagrama increíblemente difícil, y si las letras se mezclan al azar, sin pies ni cabeza, la descodificación del anagrama es tan imposible para el recipiente a quien va dirigido como para un interceptor enemigo.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Para que la trasposición sea efectiva, la combinación de letras necesita seguir un sistema sencillo, que haya sido acordado previamente por el emisor y el receptor, pero que se mantenga secreto frente al enemigo.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Por ejemplo, los niños en la escuela a veces envían mensajes utilizando la trasposición de «riel», en la que el mensaje se escribe alternando las letras en dos líneas separadas.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- A continuación, la secuencia de letras de la línea inferior se añade al final de la secuencia de letras de la línea inferior se añade al final de la secuencia de la línea superior, creándose así el mensaje cifrado final.
- Por ejemplo:

LA ESCRITURA SECRETA: Combinar un puñado de letras

TU SECRETO ES TU PRISIONERO; SI LO SUELTAS, TÚ ERES SU PRISIONERO

↓

TSCEOSUROEOIOULATEESPIINR
UERTETPIINRSLSETSURSURSOEO

↓

TSCEOSUROEOIOULATEESPIINRUERTETPIINRSLSETSURSURSOEO

- El receptor puede recuperar el mensaje simplemente invirtiendo el proceso.

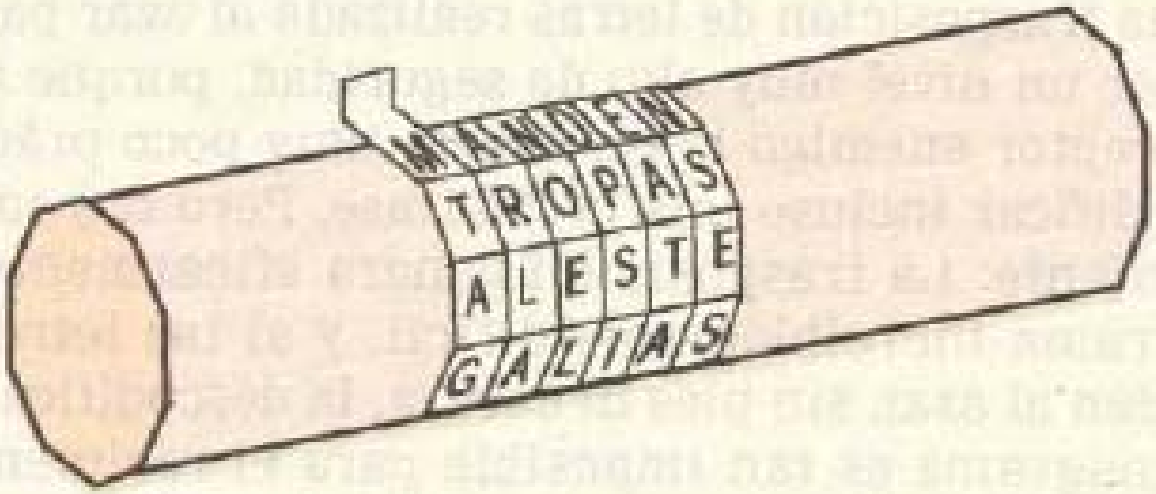
LA ESCRITURA SECRETA: Combinar un puñado de letras

- Hay otras formas de traposición sistemática, incluida la cifra de «riel» de tres líneas, en la que primero se escribe el mensaje en tres líneas separadas en vez de dos.
- Como alternativa se podría cambiar cada par de letras, de forma que la primera y la segunda cambien de lugar, así como la tercer y la cuarta, y así sucesivamente.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Otra forma de trasposición es la producida en el primer aparato criptográfico de la Historia, el escitalo espartano, que se remonta al siglo V a.C.
- El escitalo es una vara de madera sobre la que se enrosca una tira de cuero o un pergamino, tal como se muestra bajo estas líneas.

LA ESCRITURA SECRETA: Combinar un puñado de letras



Cuando se desenrosca del escitalo (vara de madera) del emisor, la tira de cuero parece llevar una lista de letras al azar: M,T,A,G... Sólo al volver a enroscar la tira alrededor de otro escitalo con el diámetro correcto reaparecerá el mensaje.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- El emisor escribe un mensaje a lo largo de la longitud del escitalo y luego desenrosca la tira, que ahora parece llevar una lista de letras sin sentido.
- El mensaje ha sido codificado.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- El mensajero llevaba la tira de cuero y, en un nuevo giro esteganográfico, a veces la llevaba de cinturón, con las letras ocultas en la parte interna.
- Para recuperar el mensaje, el receptor simplemente enrosca la tira de cuero en torno a un escitalo del mismo diámetro que el usado por el emisor.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- En el año 404 a.C. se presentó ante Lisandro de Esparta un mensajero, maltrecho y ensangrentado, uno de los cinco únicos supevivientes del arduo viaje desde Persia.
- El mensajero le dio su cinturón, y Lisandro lo enrolló en su escitalo, enterándose así de que Farnabazo de Persia planeaba atacarlo.
- Gracias al escitalo, Lisandro se preparó para afrontar ese ataque y lo repelió.

LA ESCRITURA SECRETA: Combinar un puñado de letras

«Combate en un pantano» (siglo VII a.C.)

Una de las descripciones más antiguas de codificación por sustitución aparece en el Kamasutra, en el siglo IV a.C.

- La alternativa a la trasposición es la sustitución.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Una de las descripciones más antiguas de codificación por sustitución aparece en el Kamasutra, un texto escrito en el siglo IV por el erudito Brahmin Vatsyayana, pero que se basa en manuscritos que se remontan al siglo IV a.C.

LA ESCRITURA SECRETA: Combinar un puñado de letras

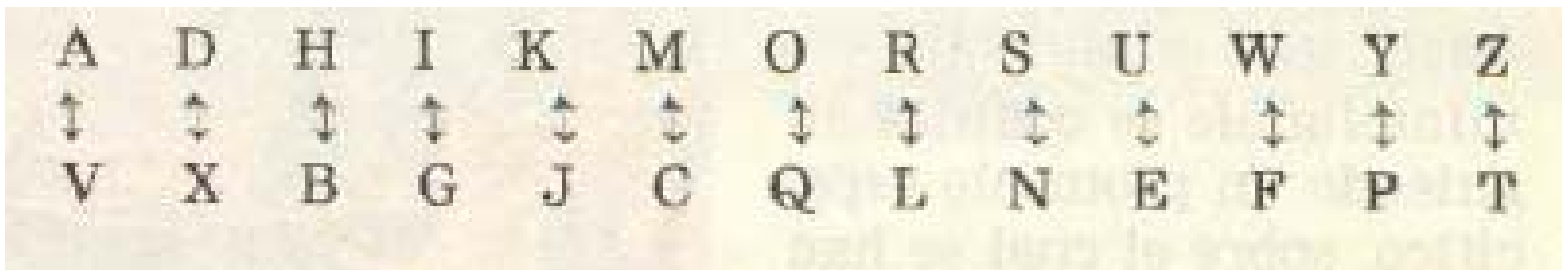
- El Kamasutra recomienda que las mujeres deberían estudiar 64 artes, como cocinar, saber vestirse, dar masajes y preparar perfumes.
- La lista incluye también algunas artes menos obvias, como la prestidigitación, el ajedrez, la encuadernación de libros y la carpintería.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- El número 45 de la lista es mlecchita-vikalpa, el arte de la escritura secreta, preconizado para ayudar a las mujeres a ocultar los detalles de sus relaciones amorosas.
- Una de las técnicas recomendadas es emparejar al azar las letras del alfabeto y luego sustituir cada letra del mensaje original por su pareja.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Si aplicamos este principio al alfabeto romano podríamos emparejar las letras de esta manera.



LA ESCRITURA SECRETA: Combinar un puñado de letras

Entonces, en vez de:

«encontrémonos a medianoche»,

el emisor escribiría

USMQSZLUCQSQN V CUXGVSQMBU.

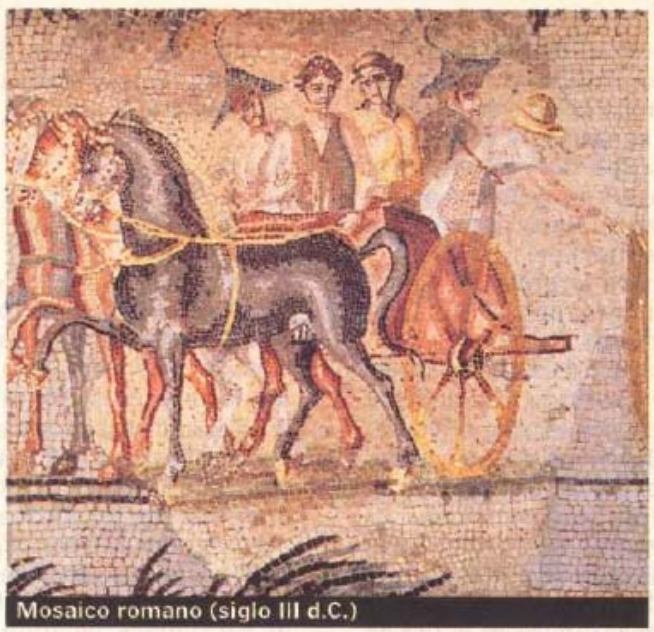
LA ESCRITURA SECRETA: Combinar un puñado de letras

- Esta forma de escritura secreta se conoce como cifra de sustitución porque cada letra del texto llano se sustituye por una letra diferente, funcionando así de manera complementaria a la cifra por trasposición.
- En la trasposición, cada letra mantiene su identidad pero cambia su posición, mientras que en la sustitución, cada letra cambia su identidad pero mantiene su posición.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- El primer uso documentado de una cifra de sustitución con propósitos militares aparece en la «Guerra de las Galias», de Julio César.
- César describe cómo envió un mensaje a Cicerón que se encontraba sitiado y a punto de rendirse.

LA ESCRITURA SECRETA: Combinar un puñado de letras



Mosaico romano (siglo III d.C.)

César utilizó la escritura secreta son tanta frecuencia que Valerio Probo escribió un tratado entero que, tristemente, no ha sobrevivido

LA ESCRITURA SECRETA: Combinar un puñado de letras

- La sustitución reemplazó las letras romanas por letras griegas, haciendo que el mensaje resultara ininteligible para el enemigo.
- César describió la dramática entrega del mensaje.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- *Se dieron instrucciones al mensajero para que si no pudiese acercarse, arrojara una lanza, con la carta sujeta a la correa, al atrincheramiento del campamento. Temiendo el peligro, el galo arrojó la lanza, tal como se le había dicho. Por casualidad, la lanza se clavó en la torre, y durante dos días nuestras tropas no la vieron; al tercer día fue divisada por un soldado, que la bajó y la llevó a Cicerón. Después de leerla detalladamente, éste la narró en un desfile de las tropas, proporcionando a todos la mayor de las alegrías.*

LA ESCRITURA SECRETA: Combinar un puñado de letras

- César utilizó la escritura secrete tan frecuentemente que Valerio Probo escribió un tratado entero acerca de sus cifras, que desgraciadamente no ha sobrevivido.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Sin embargo, gracias a la obra de Suetonio «Vidas de los Césares LVI», escrita en el siglo segundo de nuestra era, tenemos una descripción detallada de uno de los tipos de cifra de sustitución utilizado por César.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- El emperador sencillamente sustituía cada letra del mensaje con la letra que está tres lugares más adelante en el alfabeto.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Los criptógrafos a menudo piensan en términos de alfabeto llano, el alfabeto que se usa para escribir el mensaje original, y alfabeto cifrado, las letras que sustituyen a las del alfabeto llano.

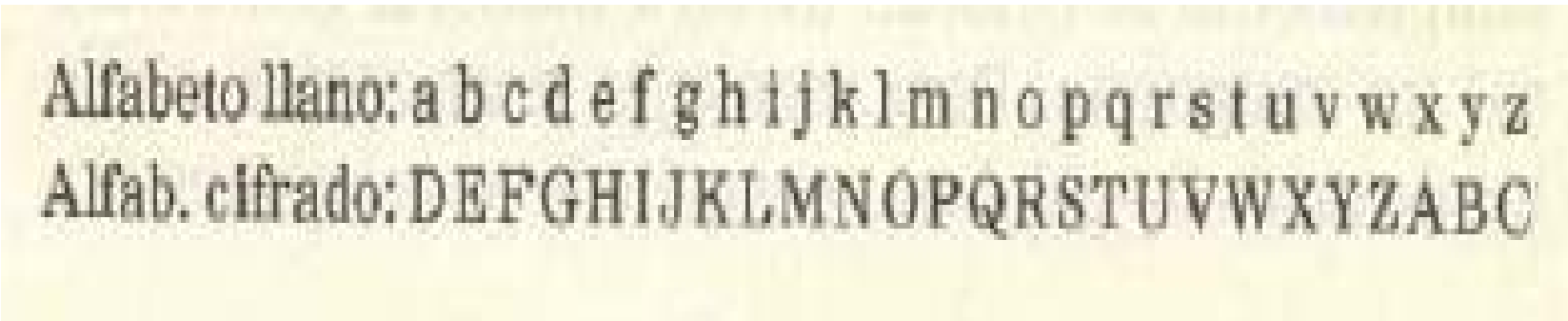
LA ESCRITURA SECRETA: Combinar un puñado de letras

- Cuando el alfabeto llano se coloca sobre el alfabeto cifrado, tal como se muestra más abajo, queda claro que el alfabeto cifrado ha sido movido tres lugares, por lo que esta forma de sustitución a menudo es llamada la cifra de cambio del César, o simplemente la cifra del César.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Una cifra es el nombre que se da a cualquier forma de sustitución criptográfica en la que cada letra es reemplazada por otra letra o símbolo.

LA ESCRITURA SECRETA: Combinar un puñado de letras



- Texto llano:

veni, vidi, vici

- Texto cifrado:

YHQL, YLGL, YLFL

LA ESCRITURA SECRETA: Combinar un puñado de letras

- *La cifra del César se basa en un alfabeto cifrado que se ha movido un cierto número de lugares (en este caso, tres) con respecto al alfabeto llano. La convención en la criptografía es escribir el alfabeto llano en letras minúsculas, y el alfabeto cifrado en mayúsculas. De manera similar, el mensaje original, el texto llano, se escribe en minúsculas y el texto cifrado, en mayúsculas.*

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Aunque Suetonio sólo menciona un «cambio del César» de tres lugares, es evidente que al utilizar cualquier cambio de entre 1 y 25 lugares es posible generar 25 cifras distintas.
- De hecho, si no nos limitamos a cambiar ordenadamente el alfabeto y permitimos que el alfabeto cifrado sea cualquier combinación del alfabeto llano, podemos generar un número aún mayor de cifras distintas.
- Hay más de 400.000.000.000.000.000.000.000.000 combinaciones posibles y, por tanto, de cifras diferentes.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- **Sospechas y claves exactas.**
- Cada una de las cifras puede ser considerada en términos de un método de codificación general, conocido como el algoritmo, y una clave, que especifica los detalles exactos de una codificación particular.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- En este caso, el algoritmo conlleva sustituir cada letra del alfabeto llano por una letra procedente de un alfabeto cifrado, y el alfabeto cifrado puede consistir de cualquier combinación del alfabeto llano.
- La clave define el alfabeto cifrado exacto que hay que usar para una codificación particular.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Un enemigo que estudie un mensaje codificado interceptado puede tener una fuerte sospecha de la existencia del algoritmo, pero quizá no conozca la clave exacta.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Por ejemplo, puede muy bien sospechar que cada letra del texto llano ha sido reemplazada por una letra diferente según un alfabeto cifrado particular, pero es improbable que sepa qué alfabeto cifrado ha sido utilizado.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Si el alfabeto cifrado, la clave, se mantiene como secreto bien guardado entre el emisor y el receptor, el enemigo no podrá descifrar el mensaje interceptado.
- La importancia de la clave, a diferencia del algoritmo, es un principio estable de la criptografía.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Fue expuesto definitivamente en 1883 por el lingüista holandés Augusto Kerckhoffs von Nieuwenhof en su libro «La Cryptographie Militaire».

LA ESCRITURA SECRETA: Sospechas y claves exactas

- «El Principio de Kerckhoffs:
- La seguridad de un cripto-sistema no debe depender de mantener secreto el cripto-algoritmo.
- La seguridad depende sólo de mantener secreta la clave».

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Además de mantener secreta la clave, un sistema de cifra seguro debe tener también una amplia gama de claves potenciales.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Por ejemplo, si el emisor utiliza la cifra de «cambio del César» para cifrar un mensaje, la codificación es relativamente débil, porque sólo hay 25 claves potenciales.

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Desde el punto de vista del enemigo, si éste intercepta el mensaje y sospecha que el algoritmo utilizado es «el cambio del César», entonces sólo tiene que revisar las 25 posibilidades.

LA ESCRITURA SECRETA: Sospechas y claves exactas

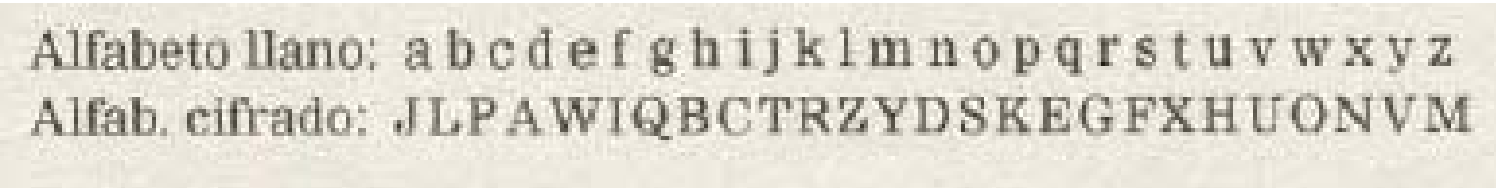
- Sin embargo, si el emisor utiliza el algoritmo de sustitución más general, que permite que el alfabeto cifrado sea cualquier combinación del universo llano, entonces hay $4 \cdot 10^{26}$ claves posibles entre las que elegir.
- Una de ellas es:

Alfabeto llano:	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfab. cifrado:	J L P A W I Q B C T R Z Y D S K E G F X H U O N V M

LA ESCRITURA SECRETA: Sospechas y claves exactas

- Desde el punto de vista del enemigo, si el mensaje es interceptado y se conoce el algoritmo, queda aún la horrenda tarea de revisar todas las claves posibles.
- Si un agente enemigo fuese capaz de revisar una de las $4 \cdot 10^{26}$ claves posibles por segundo le llevaría aproximadamente un billón de veces los siglos de vida del universo revisar todas ellas y descifrar el mensaje.

LA ESCRITURA SECRETA: Combinar un puñado de letras



- Texto llano: et tu, brute?
- Texto cifrado: WX XH, LGHXW?
- *Un ejemplo de algoritmo de sustitución general, en el que cada letra del texto llano se sustituye por otra letra según una clave. La clave se define mediante el alfabeto cifrado, que puede ser cualquier combinación del alfabeto llano.*

LA ESCRITURA SECRETA: Combinar un puñado de letras

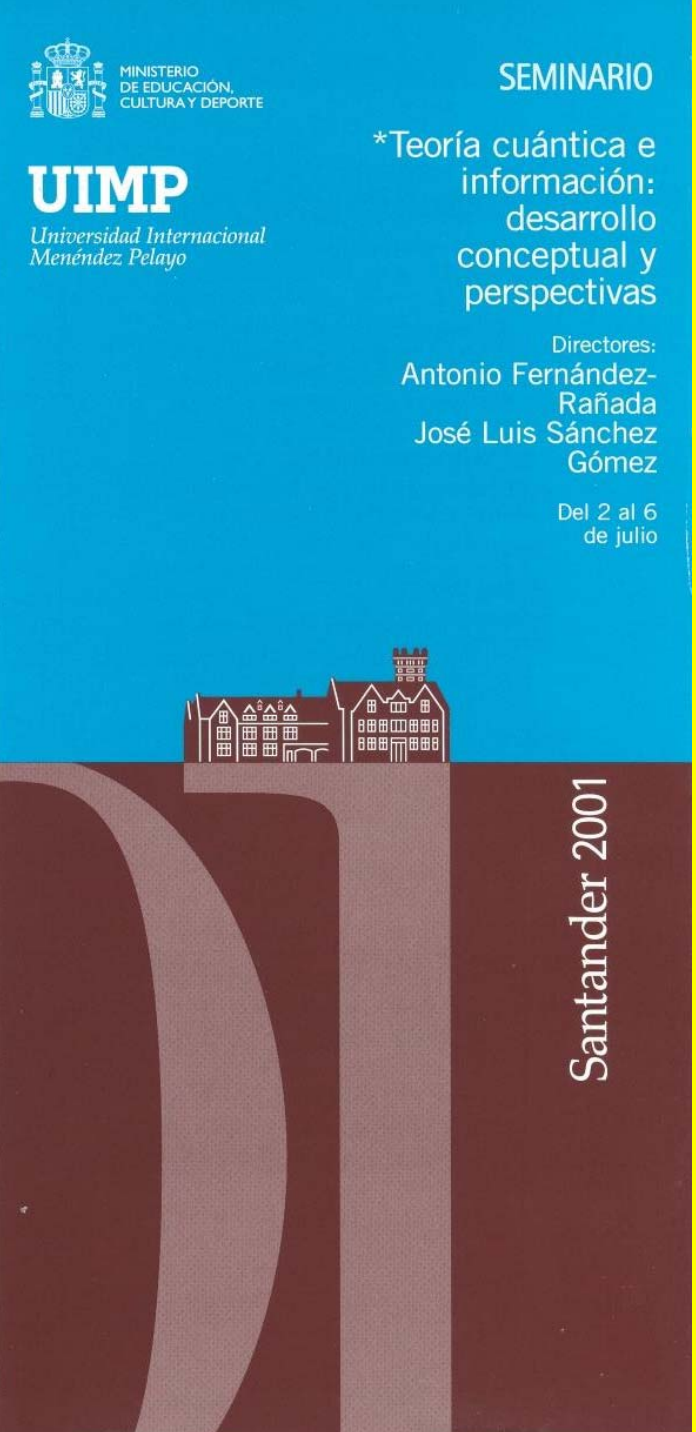
- La ventaja de este tipo de cifra radica en que es fácil de poner en práctica, a la vez que ofrece un alto nivel de seguridad.

LA ESCRITURA SECRETA: Combinar un puñado de letras

- Para el emisor es fácil definir la clave, que consiste meramente en determinar el orden de las 26 letras en el alfabeto cifrado elegido, y, sin embargo, al enemigo le será prácticamente imposible revisar todas las claves posibles por el denominado «ataque por la fuerza bruta».

LA ESCRITURA SECRETA: Combinar un puñado de letras

- La simplicidad de la clave es importante, porque el emisor y el receptor tienen que compartir el conocimiento de la clave, y cuanto más simple sea esta, menor será la posibilidad de un malentendido.



- TEORÍA DE LA INFORMACIÓN Y LEYES DE LA FÍSICA

Teoría de la Información y Leyes de la Física

- En 1948, Claude E. Shannon publicó un artículo seminal titulado "A mathematical theory of communication", transformado en libro un año más tarde, que fundó una nueva disciplina, *la teoría de la comunicación* o *de la información*, como se tiende a llamarla hoy.

Teoría de la Información y Leyes de la Física

- Desde entonces su importancia no ha dejado de crecer.
- Aunque es necesaria para el análisis de cómo se procesa el pensamiento, surge de un dispositivo creado por los humanos, la telegrafía (algo parecido ocurrió antes con la máquina de vapor, los aviones o los circuitos eléctricos).

Teoría de la Información y Leyes de la Física

- En la teoría de la información es central el concepto de entropía, idea que los físicos estudian desde sus cursos de termodinámica.
- Pero conviene decir desde el principio que la entropía de que vamos a hablar es distinta, al menos en su forma, de la de la termodinámica, pareciéndose en cambio a la de Boltzmann propia de la Mecánica Estadística.

Teoría de la Información y Leyes de la Física

- Consideremos un gas que se expande contra un pistón dentro de un cilindro.
- Si el proceso es lo bastante lento y no hay flujo de calor desde o hacia el gas, se trata de un proceso *reversible* que se puede deshacer volviendo el gas al mismo estado de presión, energía y temperatura que al principio.

Teoría de la Información y Leyes de la Física

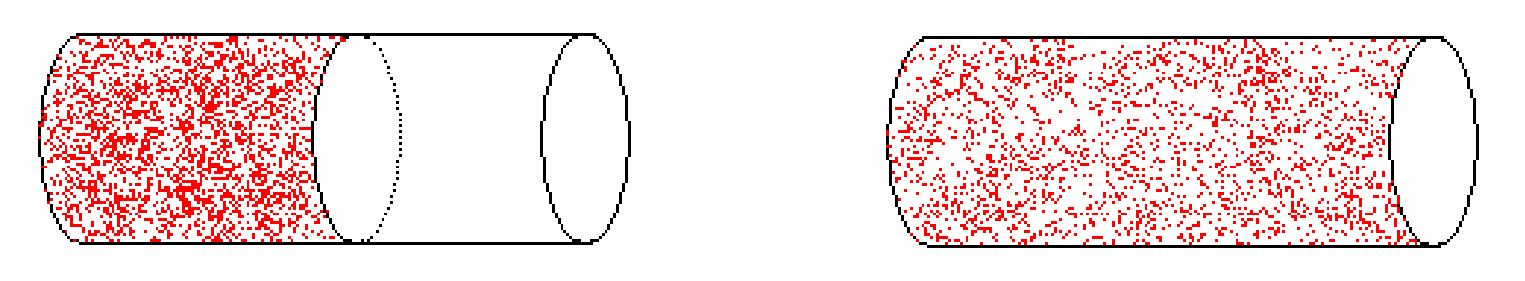
- En los procesos reversibles, la entropía permanece constante.
- Por eso el cambio de entropía es un indicador de la reversibilidad.
- Los estados reversibles son la excepción, no la regla.

Teoría de la Información y Leyes de la Física

- Supongamos que, en el ejemplo anterior, el cilindro estuviese dividido en dos mediante una pared y que todo el gas se encontrase a la izquierda de esta pared.

Teoría de la Información y Leyes de la Física

- Si la pared desaparece de manera súbita, el gas se expande y llena el cilindro rápidamente.



Teoría de la Información y Leyes de la Física

- En este proceso, su energía permanece constante, pero la entropía crece.
- Antes de la partición, era posible obtener energía mecánica del gas, dejándolo salir a través de un agujero en la pared y haciéndole mover un pequeño motor.

Teoría de la Información y Leyes de la Física

- Pero tras la expansión y el consiguiente aumento de la entropía eso no es ya posible.
- Un aumento de la entropía implica una disminución de nuestra capacidad de transformar energía térmica en energía mecánica.

Teoría de la Información y Leyes de la Física

- Esto se refiere al concepto de entropía según la termodinámica.
- Nos interesa más aquí el de la mecánica estadística, en la que aparece como proporcional al logaritmo de la extensión en el espacio de las fases del conjunto de los microestados que son compatibles con un cierto macroestado.

Teoría de la Información y Leyes de la Física

- En términos matemáticos

$$S = k \log W$$

ecuación, por cierto, grabada en la tumba de Boltzmann en el cementerio de Viena.

Teoría de la Información y Leyes de la Física

- Se suele decir que la entropía es una medida del desorden, afirmación que suele ser muy imprecisa pues no se suele explicar bien qué cosa es desorden, aunque suele asociarse de modo no explícito con la complejidad del estado.
- La mejor manera de dar sentido a esta frase tópica es hacer corresponder orden con conocimiento.

Teoría de la Información y Leyes de la Física

- El desorden estaría entonces relacionado con la *imprevisibilidad* (o *impredecibilidad*).
- O sea, que un aumento del desorden es una disminución de nuestro conocimiento de los detalles de un sistema, lo que hace más difícil la predicción (así ocurre de modo notable con los sistemas caóticos).

Teoría de la Información y Leyes de la Física

- Volvamos al ejemplo anterior.
- Hemos visto que si sabemos que las moléculas están a un lado de la pared, la entropía es menor que si se reparten por todo el cilindro.

Teoría de la Información y Leyes de la Física

- Sin duda sabemos más sobre las moléculas en el primer caso que en el segundo, lo que muestra que cuanto más detallado sea nuestro conocimiento de un sistema, menor será su entropía y menor será también nuestra incertidumbre sobre él.

Teoría de la Información y Leyes de la Física

- Este es el sentido de la entropía que nos interesa: es una medida de nuestra *incertidumbre*, de modo que un crecimiento de la entropía significa un decrecimiento del orden (aunque este concepto es ambiguo) y también una disminución de nuestro conocimiento.

Teoría de la Información y Leyes de la Física

- En la definición de Boltzmann es claramente así.
- Si aumenta la extensión en el espacio de las fases W, disminuye nuestro conocimiento del sistema.

Teoría de la Información y Leyes de la Física

- Lo mismo ocurre en teoría de la información (o de la comunicación).
- Tenemos en este caso una fuente de mensajes (una persona que escribe o habla, por ejemplo), que puede producir en cada ocasión uno cualquiera de un cierto número de posibles mensajes.

Teoría de la Información y Leyes de la Física

- Se entiende bien de modo intuitivo que la cantidad de información que proporciona cada mensaje aumenta con el grado de incertidumbre sobre cuál será ese mensaje.
- Si sólo hay uno posible, por ejemplo la letra A, no se añade ningún conocimiento al recibirlo.

Teoría de la Información y Leyes de la Física

- Del mismo modo, un mensaje entre 10 posibles transmite menos información que uno entre mil.
- Por eso la entropía de la teoría de la información tiene mucho parecido con la de la mecánica estadística (no así con la de la termodinámica): es también una medida de la incertidumbre.

Teoría de la Información y Leyes de la Física

- La incertidumbre, es decir, la entropía, se toma como medida de la información aportada por un mensaje.
- Cuanto más sepamos sobre los mensajes que puede producir la fuente, menor será nuestra incertidumbre, menor la entropía y menor la información.

Teoría de la Información y Leyes de la Física

- Hay que tener cuidado aquí con la manera de hablar, especialmente con el uso de la palabra información.
- Debe distinguirse entre la información que tenemos ya sobre un sistema y la información al hacer un experimento.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Mientras hacía un viaje trasatlántico en 1832, Samuel Morse discutió con unos amigos sobre algunos experimentos recientes de Ampère.
- Se le ocurrió entonces la idea de un código para la comunicación telegráfica.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Al principio constaba de secuencias de rayas largas y cortas en una banda de papel, que no representaban letras sino números asignados a palabras en un diccionario que el mismo Morse elaboró.
- Curiosamente era un sistema eficiente aunque poco práctico.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Más tarde elaboró la forma conocida, en la que las letras del alfabeto y algunos signos ortográficos se representaron por espacio, puntos y rayas.
- El espacio es ausencia de corriente eléctrica, el punto es una corriente breve, la raya, una más larga.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Morse asignó combinaciones de puntos y rayas a las letras, adecuadamente teniendo en cuenta la frecuencia relativa de las letras.
- Por eso a la E, la letra más frecuente en inglés, le fue asignada la combinación más simple, el punto, y a las letras menos frecuentes se les asoció combinaciones más largas.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Por ejemplo, la Z (--..), la W (.--) o la Q (--.-).
- Morse consiguió así un código muy eficaz, la velocidad de transmisión de un mensaje sólo se podría aumentar en un 15% con otras asignaciones, según se comprobó después.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Esta cuestión de la eficacia de un código es una de las más importantes de la teoría de la información.
- Más adelante se consiguieron sistemas más eficaces aún, por ejemplo con cuatro posibilidades en vez de las dos punto y raya, como en la telegrafía cuadruplex de Edison.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- El punto y la raya podían representarse como +1 y -1 o como 0 y 1.
- En el sistema cuadruplex, las posibilidades se representaban por +3, +1, -1 y -3

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- En 1924 otro protagonista de la teoría de la información, Harry Nyquist, que trabajaba para la American Telephone an Telegraph Company se planteó la cuestión de como calcular la velocidad de transmisión de un mensaje de una fuente que envía símbolos a ritmo constante, elegidos entre *m* posibilidades.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

- Su conclusión fue que la velocidad de transmisión está dada por

$$V = K \log m$$

siendo K una constante que depende de las características del aparato.

- Lo más conveniente es tomar logaritmos binarios, es decir, en base 2.

Teoría de la Información y Leyes de la Física
El Alfabeto Morse

m	$\log_2 m$
1	0
2	1
3	1,6
4	2
8	3
16	4

Teoría de la Información y Leyes de la Física

- Nyquist acertó con el logaritmo para su fórmula.
- Si la máquina puede enviar sucesiones de “unos” y “ceros”, tomando cada signo un tiempo t, entonces m = 2 y la velocidad V = K.

Teoría de la Información y Leyes de la Física

- Supongamos que puede enviar un par de esos símbolos cada t, o sea que su velocidad será V = 2K.
- Esto significa que puede elegir entre cuatro pares de dos símbolos (00, 01, 10, 11), o sea que m = 4.
- Si puede enviar tripletes de “unos” y “ceros”, m = 8 y V = 3K.

Teoría de la Información y Leyes de la Física

- Más adelante, en 1928, el americano Hartley publicó un artículo clásico titulado "Transmission of information" en el que argumentaba que debe definirse la cantidad de información contenida en un mensaje como:

$$H = n \log s$$

donde n es el número de símbolos del mensaje y s es el número de símbolos diferentes con los que se puede construir el mensaje.

Teoría de la Información y Leyes de la Física

- Para entender mejor la teoría de la información conviene aplicarla a mensajes con letras, como los de nuestras comunicaciones.
- Para ello conviene saber las frecuencias de aparición de las diferentes 26 letras.
- La más frecuente, tanto en español como en inglés, es la E, cuya frecuencia es $p(E) = 0,13$, con una diferencia de milésimas entre los dos idiomas.

Teoría de la Información y Leyes de la Física

- Ya vimos que Morse consiguió una gran eficacia por haber elegido sabiamente las combinaciones de puntos y rayas que representan las letras (más cortas las de las más frecuentes).
- Curiosamente, esas frecuencias varían muy poco entre los distintos autores o tipos de texto, aunque hay, claro está, excepciones.

Teoría de la Información y Leyes de la Física

- Hubo un poeta alemán, Gottlob Burmann (1737-1805), que fue famoso porque escribió 130 poemas sin usar nunca la R e incluso aprendió a hablar sin usarla durante los últimos diecisiete años de su vida.
- Un escritor español, Alonso Alcalá y Herrera, escribió en 1641 un libro titulado "Varios efectos de amor", que es un conjunto de cinco cuentos en cada uno de los cuales falta una de las vocales.

Teoría de la Información y Leyes de la Física

- También hay un cuento de Mark Twain, en el que a un periódico le roban los tipos de la letra E.
- Un artículo publicado al día siguiente tiene un gran efecto cómico por los circunloquios a que se ve obligado el periodista para no usar esa letra.

Teoría de la Información y Leyes de la Física

- Shannon se ocupó de esa cuestión, construyendo varias aproximaciones a un texto en inglés.
- Consideró, en primer lugar sucesiones de letras y espacios, en las que cada símbolo tenía la misma probabilidad, o sea 1/27.
- A eso lo llamó aproximación de orden cero al inglés (símbolos independientes y equiprobables).

Teoría de la Información y Leyes de la Física

Un ejemplo:

- XFOML RXKHRJFFJUJ ZLPWCFWKCYJ FFJEYVKCQSGHYD
- Tomó luego sucesiones en las que cada letra y el espacio tenían la misma probabilidad que en un texto en inglés.

Teoría de la Información y Leyes de la Física

- O sea, la E aparecía 130 veces cada 1000 símbolos [p(E) = 0,13], la W, 20 veces [p(W) = 0,02], etc.
- Un ejemplo de esta aproximación de orden uno (símbolos independientes con la frecuencia de un texto inglés) es
- OCRO HLI RGWR NMIEL WIS EU LL NBNESEBYA...

Teoría de la Información y Leyes de la Física

- Como se ve, no se parece mucho a un texto inglés, porque una característica de un idioma es la frecuencia de pares y triplos de letras.
- Por ejemplo, la Q aparece siembre seguida de una U, nunca de una B.

Teoría de la Información y Leyes de la Física

- Por eso Shannon construyó aproximaciones en las que no sólo letras, sino los pares y triplos de letras tienen la misma frecuencia que en un texto inglés.
- Luego tomó sucesiones de palabras con la frecuencia inglesa y hasta secuencias de palabras en la que cada par de dos sucesivas tenía la frecuencia adecuada.

Teoría de la Información y Leyes de la Física

- He aquí un ejemplo de esa aproximación:
- THE HEAD AND IN FRONTAL ATTACK ON AN ENGLISH WRITER THAT THE CHARACTER OF THIS POINT IS THEREFORE ANOTHER...

Teoría de la Información y Leyes de la Física

- Como se ve, aunque el mensaje no tiene ningún sentido discernible, su aspecto recuerda al inglés.
- Lo que nos interesa de este esquema de Shannon es que la entropía de cada símbolo depende del tipo de aproximación usado.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- La teoría de la información se ocupa de mensajes generados por fuentes, en un sentido muy general que no tiene en cuenta, en un principio, su significado: se dice que no es semántica, aunque sí es sintáctica en un sentido.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Por ejemplo, trata de textos escritos en cualquier idioma, de una canción o de una interpretación instrumental grabada, fotografías, imágenes quietas o en movimiento, ...
- Cada uno de esos objetos puede codificarse, es decir, representarse por una sucesión de símbolos que permitan luego recuperar el texto, la voz, la música o la imagen.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- En general se consideran *fuentes ergódicas*.
- Para saber qué es una tal fuente tomemos primero la idea de *fuente estacionaria* que es aquella en la que las probabilidades de los diferentes símbolos no varían en el tiempo.
- Por ejemplo, las frecuencias de las letras que usamos en nuestro lenguaje cotidiano son bastante constantes (aunque no fuera el caso de Burmann pues la frecuencia de la R decayó para él a cero al final de su vida).

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Una sucesión de tiradas de dado o de lotería es estacionaria, si no se hacen trampas o no cambian el número de billetes distintos.
- En un idioma, la probabilidad de aparición de una letra en un lugar depende de la letra que hay en el lugar inmediatamente anterior.
- Por tanto podría ocurrir que las probabilidades de aparición en un mensaje dependiesen de por qué letra empieza.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Conviene por ello introducir el concepto de *conjunto* de mensajes.
- En el caso de un idioma sería un conjunto muy grande de mensajes cuya primera letra tiene la misma frecuencia que la de un texto.
- Por ejemplo, si es en inglés, la primera letra sería la E con frecuencia 0,13, la W con frecuencia 0,02.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Pues bien una fuente es ergódica si es estacionaria y además la frecuencia de cada letra, o de cada par o trío de letras, etc. en el conjunto es la misma que en cada mensaje.
- Un ejemplo de fuente no ergódica es la que sólo puede generar los tres mensajes siguientes con igual probabilidad.
- 1. ABABABAB, etc. 2. BABABABA, etc. 3. EEEEEEEE, etc

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Las tres letras aparecen con frecuencia 1/3 en el conjunto, pero sus frecuencias en los mensajes particulares son diferentes.
- Nótese la correspondencia de esta definición con la usada en Física a veces, basada en la igualdad de los valores medios en el tiempo en cada trayectoria y en el espacio de las fases.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Volvamos a la codificación, que aparece en contextos muy distintos, por ejemplo en Genética.
- La herencia biológica funciona al transmitir un texto consistente en una ordenación lineal de cuatro símbolos diferentes (o bases) en la molécula de ADN, o sea, una codificación.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- A su vez, este texto produce otro equivalente en la molécula de ARN, mediante el cual se sintetizan las proteínas mediante los veinte aminoácidos.
- De hecho los genetistas han llegado a ese lenguaje por la existencia previa de la teoría de la información.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Como vimos un texto se codifica en el sistema Morse mediante puntos y rayas.
- Desde esa perspectiva, las ondas electromagnéticas que transmiten una música por la radio son una codificación de esa música, lo mismo que la variación de la presión del aire, lo que llamamos sonido, que sirve para comunicarnos, y naturalmente la grabación en un disco u otro sistema.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Estos ejemplos nos explican claramente que uno de los objetivos de la teoría de la información es diseñar sistemas eficientes de codificación, para conseguir un almacenamiento más compacto de datos (pensemos en el incremento espectacular de la capacidad de los discos de los ordenadores) o una representación lo más fiel posible de la música para mejor disfrutar de ella.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Para todos los propósitos y otros parecidos, se usa una medida de la cantidad de información llamada ***entropía*** y una unidad de esa medida llamada ***bit***.

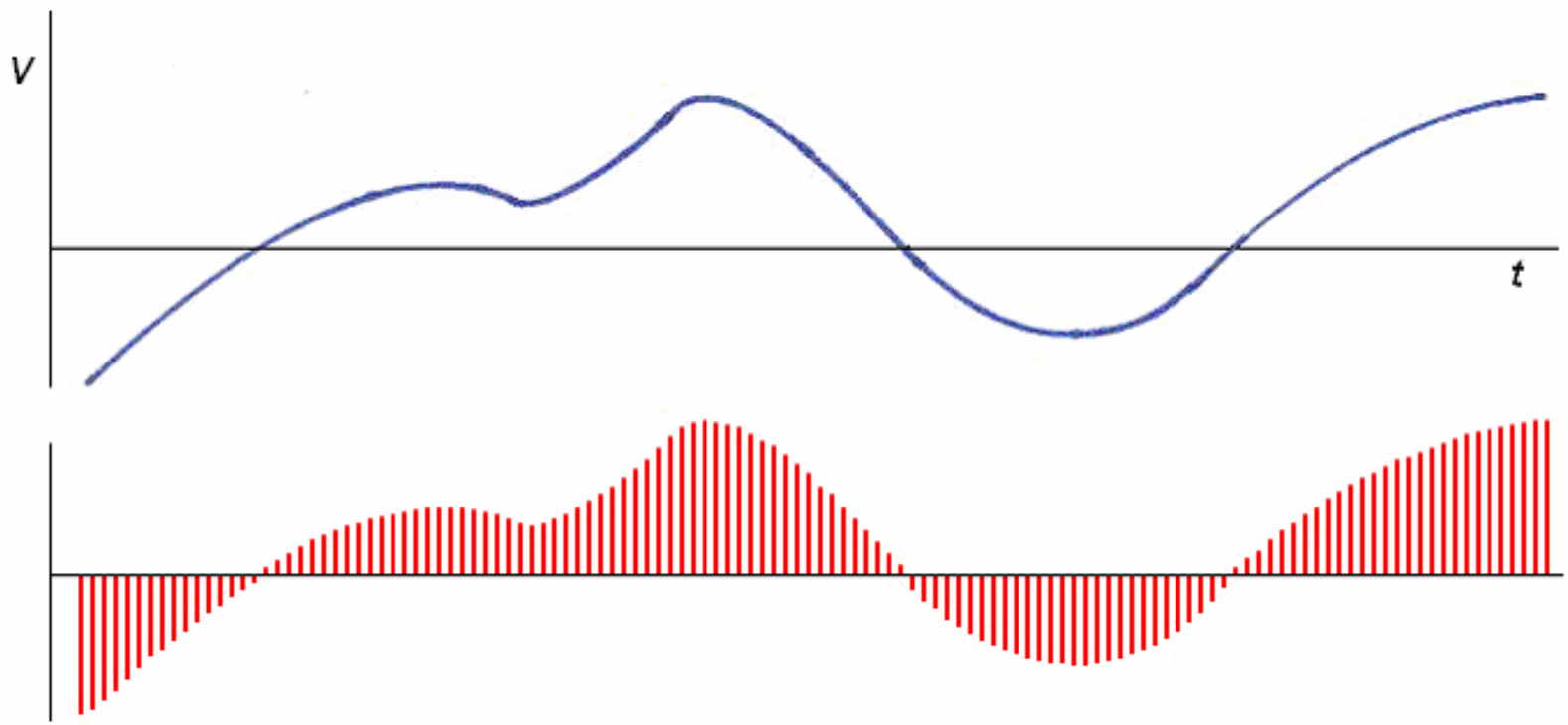
Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Los mensajes pueden ser discretos o continuos.
- Un ejemplo de los primeros es un texto escrito, constituido por un conjunto discreto de letras, de los segundos es una música representada por la variación continua de un voltaje V(t).

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Lo que se hace es “discretizar” esa señal tomando muestras, es decir, valores de su amplitud a intervalos iguales de tiempo.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios



Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Un teorema matemático asegura que podemos reconstruir la señal perfectamente mediante un tal muestreo, si el intervalo temporal es menor que la mitad del período de la frecuencia más alta presente en la señal.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Para la señal de una voz que incluye frecuencias de 0 a 4.000 Hz hay que hacer al menos 8.000 muestras por segundo.
- En el caso de una señal de TV, cuyas frecuencias llegan a 4 MHz, hay que tomar 8 millones de muestras por segundo.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Eso no resuelve completamente el problema, pues las muestras son continuas.
- El paso siguiente (una vez discretizado el tiempo) es discretizar la intensidad, aproximándola por uno de entre 100 niveles por ejemplo, o 50 u 80.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- De este modo se tiene una sucesión de números discretos (que son aproximaciones al valor de la señal cada intervalo de tiempo) que codifican la música o el sonido de una manera comparable a lo que hace un alfabeto con el lenguaje.
- Nótese que la calidad del sonido va a depender del número de niveles que usemos.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Esos números se pueden representar mediante sucesiones de espacios (voltaje nulo) y pulsos eléctricos de igual intensidad.
- Cada sucesión de varios pulsos y espacios equivale a un número en base 2.
- Por ejemplo, cuando usamos el número 285 en base 10 significamos

$$2 \times 10^2 + 8 \times 10^1 + 5 \times 10^0 = 285$$

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- El mismo número se escribe en base 2 como 100011101, pues

$$1 \times 2^8 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 1 \times 2^0 =$$
$$256 + 16 + 8 + 4 + 1 = 285$$

- O sea, que podemos representar cualquier número con cadenas de dígitos binarios (de ahí viene la palabra **bit**, de **bi**nary digi**t**)

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- De esta forma, cualquier número puede representarse por una cadena de dígitos binarios.
- El número de dígitos de la cadena es esencialmente el logaritmo del número.
- Podemos hacer lo mismo con las letras.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Mediante cadenas de tres dígitos podemos representar ocho símbolos distintos, por ejemplo los números entre 0 y 7; con cadenas de cuatro, hasta 16, con cadenas de cinco hasta 32; con cadenas de 10 dígitos hasta 1024 y con cadenas de 20 dígitos hasta 1.048.576.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Antes consideramos cadenas de las 26 letras y el espacio, o sea de 27 símbolos.
- Eso corresponde a 4,755 bits por cada uno, pues 4,755 es el logaritmo binario de 27, o sea 4,7552 = 27 (con 4 dígitos no hay bastante, con 5 sobran algunas combinaciones).

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Un teclado normal tiene 48 teclas de símbolos, cada una de ellas con dos posibilidades y alguna con tres, o sea, unos 100 símbolos.
- Con cadenas de 6 hay 64 posibilidades (no basta), con cadenas de 7 hay 128, sobra algo.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Si se quieren incluir otros símbolos, otros signos ortográficos o letras de otros alfabetos como el griego, necesitamos cadenas de ocho (256 posibilidades) pues 7 no es bastante.
- Por eso los ordenadores usan cadenas de ocho “0” y “1”, llamadas **bytes** que no se suelen dividir y son sus unidades prácticas de información.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Una manera formalmente eficiente es tomar las 16.384 cadenas de 14 dígitos (214 = 16.384) y representar con ellas otras tantas palabras.
- Cada una tendría 14 bits.
- En inglés cada palabra tiene en promedio 4,5 letras.
- Como hay que usar un espacio serían 5,5 símbolos, lo que hace a cinco bits por carácter 5,5 x 5 = 27,5 bits por palabra.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- En español el promedio de letras por palabra es aproximadamente 5,1, con lo que se necesitan 30,5 bits por palabra.
- Tomando la palabra como unidad de codificación se necesitarían 14 bits por cada una, o sea que la ventaja es grande.

Teoría de la Información y Leyes de la Física: Codificación y dígitos binarios

- Pero codificar por palabras tiene inconvenientes, no admite neologismos o préstamos de otros idiomas, onomatopeyas nuevas o palabras escritas deformadas a propósito.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- La entropía de la teoría de la información se mide en bits.
- Se dice que una fuente de mensajes tiene tantos bits por letra, por palabra o por mensaje.
- Si produce símbolos a ritmo constante, se dice que su velocidad es de tantos bits por segundo.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- La entropía crece si crece el número de mensajes posibles.
- También crece si aumenta la libertad de elección de mensajes (es decir, si aumenta la incertidumbre del receptor) y recíprocamente disminuye si lo hace la libertad de elección.
- Si se impone la restricción de que algunos mensajes se envíen muy frecuentemente o muy infrecuentemente, la entropía decrece.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Tomemos un ejemplo sencillo.
- Sea una fuente que puede enviar mensajes formados sólo con dos símbolos A y B, de modo que el dispositivo elige entre ellos sin que la probabilidad de hacerlo depende de cuáles fueron los símbolos anteriores.
- Supongamos que A es elegido con probabilidad p_o y B, con probabilidad p_1.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- El sistema es ergódico.
- En este caso sencillo, la entropía se define como:

$$H = -(p_o \log p_o + p_1 \log p_1)$$

en bits por símbolo

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Supongamos ahora que la fuente consiste en un jugador que tira sucesivamente una moneda.
- A sería cara, B sería cruz.
- Si la moneda no está amañada, las dos probabilidades son iguales, $p_o = p_1 = ½$.
- En ese caso:

$H = -(½ \log ½ + ½ \log ½) = 1$ bit por tirada

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Se dice que al saber cómo cayó la moneda en una tirada *ganamos 1 bit de información.*
- Nótese que si representamos cara por 0 y cruz por 1, una sucesión de tiradas se representa por una sucesión de dígitos binarios.
- El número de dígitos binarios por mensaje es la entropía de la fuente por mensaje.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Saber el resultado de una tirada es como determinar entre dos alternativas binarias.
- ¿Qué ocurre si la moneda está cargada y es más probable la cara que la cruz?
- Sea por ejemplo $p_o = 0,6$ y $p_1 = 0,4$.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Sustituyendo estos valores en la ecuación se tiene

  $H = - (0{,}6 \log 0{,}6 + 0{,}4 \log 0{,}4) = 0{,}971$ bit por tirada

- En este caso sabemos algo más sobre el resultado de la tirada que si las dos probabilidades fuesen iguales.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

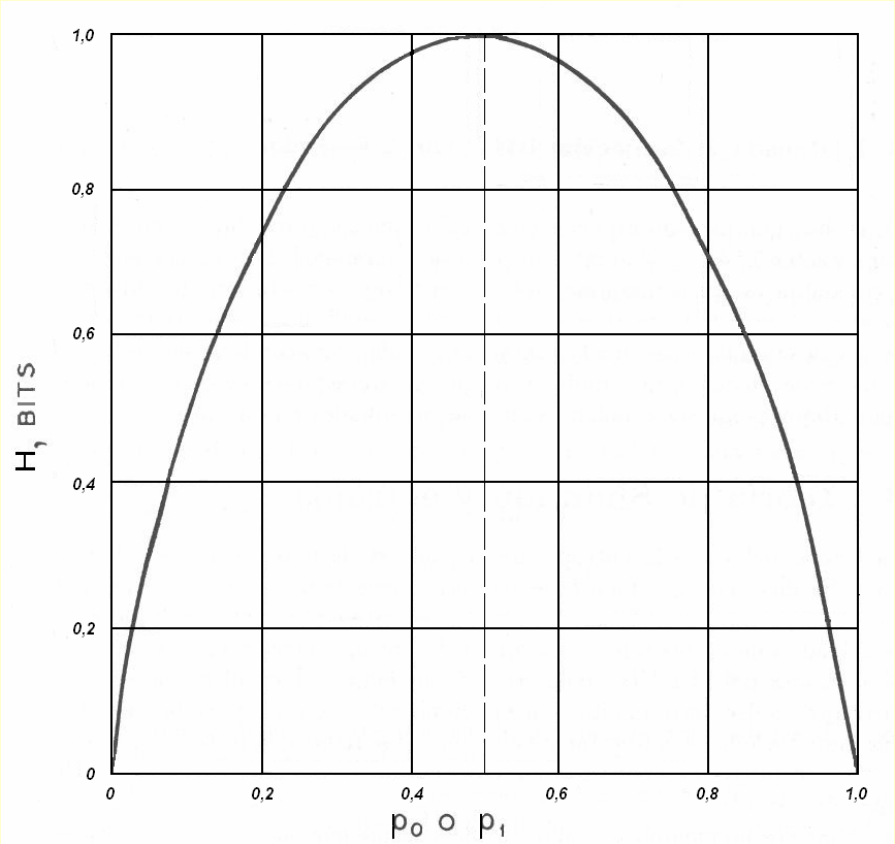
- Nuestra incertidumbre es menor (hay más orden) y por eso la entropía es también menor.
- Intuitivamente comprendemos que cada tirada tiene ahora menos de un bit, aunque sea difícil imaginarse cuánto.

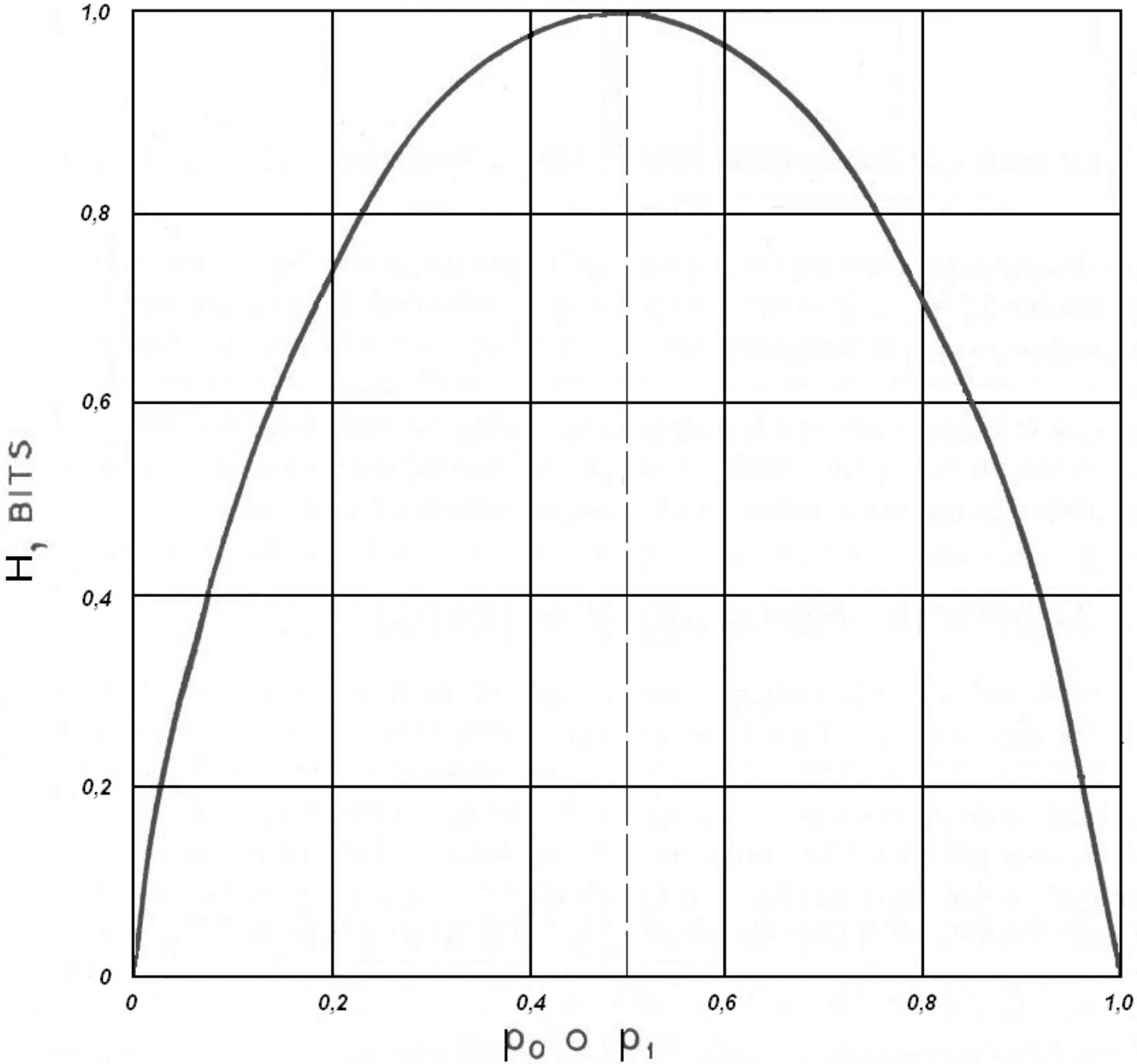
Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- La curva

  $H(p_o, p_1)$ está representada en la figura.
- Como vemos, es simétrica entre p_o y p_1 y tiene un máximo para

  $p_o = p_1 = ½$.




1,0
0,8
0,6
0,4
0,2
0
H, BITS
0
0,2
0,4
0,6
0,8
1,0
p0 o p1

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Una fuente puede generar mensajes eligiendo entre los diez dígitos arábigos, entre las 26 letras o entre los siete colores.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Si lo hace eligiendo entre n símbolos, con probabilidades independientes de las elecciones anteriores, la entropía por símbolo es

$$H = -\sum_{i=1}^{n} p_i \log p_i$$

bits por símbolo

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- En el caso de que cada símbolo consista en dos tiradas de una moneda, la fórmula anterior dice que H = 2 bits por símbolo.
- Tomando un dado honesto que se tira sucesivamente, resulta

$$H = \log_2 6 = 2{,}58 \text{ por tirada.}$$

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- En general, si hay n alternativas equiprobables,

  $H = \log n$ bits por símbolo.

- Nótese que en ese caso se parece mucho a la entropía de Boltzmann.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- Si hacemos una partición en grano grueso del espacio de fases de volumen δw (por ejemplo $\delta w = \hbar^N$ en el caso de un gas siendo N el número de partículas) y $n = W/dw$, se tiene

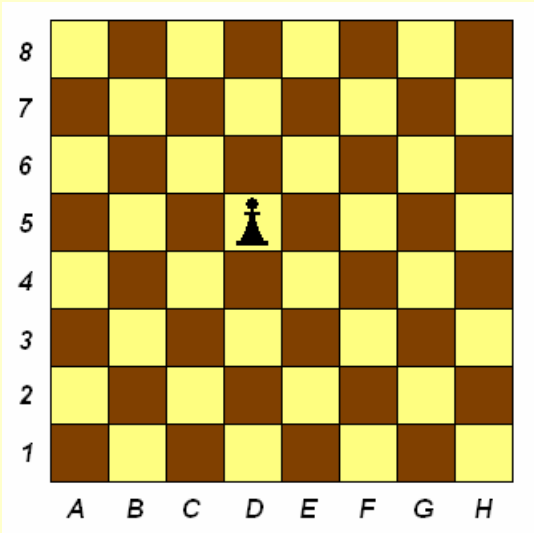
$$S = H_B = k\,(\log n + \log \delta w)$$

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- De aquí resulta que la diferencia entre las entropías de Shannon y Boltzmann es una constante.
- Nótese que estos razonamientos justifican la fórmula de Hartley.

Teoría de la Información y Leyes de la Física: Teoría de Shannon y entropía

- ¿Codificar palabras: 14 dígitos ⇨ 16.384 palabras (eficaz, pero incómodo)



64 = 26 ⇨ 6 bits

Teoría de la Información y Leyes de la Física: *It from bit*

- En una ocasión en que John Archibald Wheeler asistía a un seminario en que se hablaba de las leyes de la Física le oyeron musitar de manera oscura "It from bit".

Teoría de la Información y Leyes de la Física: *It from bit*

- Al principio no le entendían hasta que explicó que estaba considerando la posibilidad de que las leyes de la Física expresen, de una manera que no entendemos aún, que la realidad consiste en flujos de información.

Teoría de la Información y Leyes de la Física: *It from bit*

- O sea, con “It from bit” significaba que ello (la cosa) se sigue del bit (la información).
- La idea encaja en lo que Wheeler llama un *universo participativo.*

Teoría de la Información y Leyes de la Física: *It from bit*

- Normalmente consideraremos que el mundo está constituido por elementos básicos, partículas elementales, por ejemplo que podemos organizar de modo que se transmita información con ellas.

Teoría de la Información y Leyes de la Física: *It from bit*

- Pero la importancia de las comunicaciones y la información en la sociedad de hoy ha provocado el nacimiento de una idea extraña que conviene examinar: quizá la realidad más profunda sea un complejo entramado de flujos fluctuantes de información y la materia tal como la conocemos sea simplemente una manifestación secundaria.

Teoría de la Información y Leyes de la Física: *It from bit*

- La idea es extraña, pero no es una locura completa.
- Al fin y al cabo la Física es una ciencia experimental, lo que significa que se basa en experimentos, en los que se interroga a la naturaleza: medir una cantidad es en cierto modo como recibir un mensaje o averiguar cómo ha caído un dado o qué número ha salido en un sorteo de lotería.

Teoría de la Información y Leyes de la Física: *It from bit*

- Si refinamos el valor de una constante, por ejemplo de G, podemos decir que ha aumentado nuestra información sobre ella.
- Desde este punto de vista se llega a decir que los fenómenos se dan como consecuencia de nuestras preguntas mediante experimentos.

Teoría de la Información y Leyes de la Física: *It from bit*

- La naturaleza sería una fuente de mensajes como los que hemos considerado antes.
- En el universo participativo de Wheeler la acción de los humanos es decisiva y no puede eliminarse de las leyes físicas.

Teoría de la Información y Leyes de la Física: *It from bit*

- Estas frases resumen la idea:
- *“All things physical are information-theoretic in origin and this is a participatory universe...*
- *Observer participancy gives rise to information; and information gives rise to physics”*

Teoría de la Información y Leyes de la Física: *It from bit*

- Más o menos mientras Schrödinger, Heisenberg, Dirac y otros fundaban su nueva mecánica ondulatoria, de matrices o cuántica, en la que la interpretación estadística de Born juega un papel tan importante, el gran matemático inglés Ronald Fischer desarrollaba la estadística mediante el análisis de la variancia, el método de estimación de la máxima verosimilitud ("likelihood") y una medida de la incertidumbre conocida como la *información de Fischer*.

Teoría de la Información y Leyes de la Física: *It from bit*

- Curiosamente hay una relación muy estrecha entre esa información de Fischer y el término cinético en el método variacional para obtener la ecuación de Schrödiunger, pero los dos campos se mantuvieron muy lejanos, pues Fischer propuso sus métodos para analizar problemas de demografía humana y animal, de genética y de eugenesia.

Teoría de la Información y Leyes de la Física: *It from bit*

- Pero medio siglo más tarde muchos han empezado a aplicar sus ideas a la Física.
- La primera indicación en favor de hacerlo así vino de un trabajo del matemático holandés Stam, quien probó en 1959 que las incertidumbres de Heisenberg se pueden probar como una consecuencia de un resultado de la teoría de la información conocido como *desigualdad de Cramer-Rao* aplicado a la información de Fischer.

Teoría de la Información y Leyes de la Física: *It from bit*

- Sin duda esto influyó en Wheeler.
- Más recientemente, Roy Frieden, un físico de Arizona que había trabajado mucho tiempo en limpiado de imágenes, desarrolló una teoría que pretende unificar toda la Física (¡palabras mayores!) basándose en un principio variacional sobre la información de Fischer que tiene una gran semejanza formal con el principio variacional de Hamilton.

Teoría de la Información y Leyes de la Física: *It from bit*

- Aparte de la interpretación de las incertidumbres dada por Stam, a Fischer le impresionó mucho darse cuenta de que la integral del gradiente al cuadrado,

$$\nabla\psi^* \cdot \nabla\psi$$

que aparece en el estudio de todos los campos tiene una gran semejanza formal con la información de Fischer.

MECÁNICA CUÁNTICA E INFORMACIÓN

- *El interés de los físicos por los estados entrelazados nace con un trabajo de Einstein, Podolsky y Rosen (EPR) en el que describen un sistema de partículas que según la Mecánica Cuántica (MC) tiene propiedades globales perfectamente definidas, pero en el que las propiedades de las partículas individuales están totalmente indefinidas.*
- *Esta situación llevó a EPR a la conclusión de que la MC era una teoría "Incompleta".*

MECÁNICA CUÁNTICA E INFORMACIÓN

- *Sin embargo, Bell demostró que cualquier intento de "completar" la MC conduce, en ciertos casos, a predicciones diferentes de las de la MC.*
- *Hasta la fecha, todos los experimentos realizados han confirmado las predicciones de la MC.*

MECÁNICA CUÁNTICA E INFORMACIÓN

- *En los últimos años se ha descubierto que otros estados entrelazados de dos y tres partículas permiten demostrar el teorema de Bell de una forma particularmente simple, usando sólo las correlaciones perfectas entre resultados que predice la MC, sin recurrir a otras predicciones estadísticas.*

MECÁNICA CUÁNTICA E INFORMACIÓN

- *Recientemente se ha obtenido una demostración de este tipo para los estados entrelazados del tipo considerado por EPR.*

MECÁNICA CUÁNTICA E INFORMACIÓN

- Hay tres situaciones en las que las palabras "Mecánica Cuántica" (MC) e "información" aparecen asociadas.
- La primera y más fundamental, está relacionada con una característica de la MC:
- "La teoría cuántica (...) es realmente una teoría, no de **cosas** físicas, sino de **información** física."

MECÁNICA CUÁNTICA E INFORMACIÓN

- La segunda situación tiene que ver con el hecho de que la teoría clásica de la información puede considerarse que es un caso particular de una teoría más general, a la que ya se ha bautizado como *teoría cuántica de la información.*

MECÁNICA CUÁNTICA E INFORMACIÓN

- Esta teoría más general nace de la observación de que la MC permite formas de codificar, transmitir y procesar información inconcebibles sin herramientas cuánticas.
- Una de estas herramientas es el entrelazamiento.

MECÁNICA CUÁNTICA E INFORMACIÓN

- "El entrelazamiento es un recurso que se encuentra en la mecánica cuántica y del que no existe ninguna analogía en nuestro mundo clásico diario; es acero en la edad del bronce del mundo clásico."

Michael Nielsen,
http://www.physics.uq.edu.au/people/nielsen/pubs.html

MECÁNICA CUÁNTICA E INFORMACIÓN

- Existe una tercera situación en la que la MC e información aparecen relacionadas.
- Tiene que ver con la (escasa) presencia de la MC en la cultura de principios del siglo XXI.

MECÁNICA CUÁNTICA E INFORMACIÓN

- Ello resulta preocupante ya que, por un lado
- “Más del 25% del producto mundial bruto depende de nuestra comprensión de la mecánica cuántica; donde esté un transistor, un láser, una resonancia magnética, ahí está la presencia de la Mecánica Cuántica!
- *Luis A. Orozco, El País, 13 de diciembre de 2000, página 39.*

MECÁNICA CUÁNTICA E INFORMACIÓN

- Pero sobre todo porque la MC conduce a una comprensión más profunda de qué es y como funciona la naturaleza.

MECÁNICA CUÁNTICA E INFORMACIÓN

- “Yo diría que existe una diferencia mucho mayor entre un humano que sabe mecánica cuántica y uno que no sabe mecánica cuántica, que la que existe entre uno que no sabe mecánica cuántica y los otros grandes simios.”

Murray Gell-Mann,

Reunión anual de la American Association for the Advancement of Science, Chicago, 11 de febrero de 1992 /// Premio Nobel de Física en 1969

MECÁNICA CUÁNTICA E INFORMACIÓN

- Pese a todo esto, la MC es prácticamente desconocida para el público general.
- En un reciente artículo con motivo del centenario de la explicación de Planck de la distribución de la energía en la radiación del cuerpo negro –que marca el comienzo de la MC-, Rolf Tarrach hacía la siguiente reflexión:

MECÁNICA CUÁNTICA E INFORMACIÓN

- *"En este mundo ahogado en la información, ¿cómo es [posible] que casi nadie sepa nada de la revolución científica del siglo XX más profunda y más determinante de nuestro mundo actual?*

MECÁNICA CUÁNTICA E INFORMACIÓN

- *Quizá sea un problema de formación, o acaso de dificultad, pero es una pena que la sociedad no disfrute más con algo tan relevante para nuestra actualidad tecnológica y, a la vez, tan irreal, tan sorprendente y provocador como el mundo de los fenómenos cuánticos.”*

Rolf Tarrach, El Cultural (ABC), 20 de diciembre de 2000, pp. 64-65

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- **El argumento de Einstein, Podolsky y Rosen.**
- ***La mecánica cuántica es "incompleta".***
- El sábado 4 de mayo de 1935, el *New York Times* incluía una noticia con el titular "Einstein ataca la teoría cuántica". La noticia, fechada en Princeton, New Jersey, comienza:

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- "El Profesor Albert Einstein atacará la importante teoría científica de la mecánica cuántica... Su conclusión es que aunque es "correcta", no es "completa".

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Junto con dos colegas aquí en el Instituto de Estudios Avanzados [Institute for Advance Study, en Princeton], el destacado científico está a punto de informar a la Sociedad Física Americana [American Physical Society] de qué está mal en... la mecánica cuántica.”

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Los dos colegas de Einstein (1879-1955) en Princeton eran Boris Podolsky (¿-1966) y Nathan Rosen (1909-1995).
- Podolsky era un físico ruso graduado en el California Institute of Technology de Pasadena en 1929 y con el que Einstein ya había trabajado en un artículo en 1931.
- En 1935 Podolsky estaba en Princeton con una beca (él trabajaba en el Instituto Físico-Técnico Ucraniano en Kharkow –o Jarkov-).

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Podolsky fue quien, al parecer, redactó el criterio de elemento de realidad del que hablaremos después.
- Rosen, nacido en Brooklyn, New York, graduado en el M.I.T. en 1939, master en Física en 1931 y Doctor en 1932, ya había usado estados entrelazados en un artículo de 1931 sobre la estructura de la molécula de hidrógeno.

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Él fue quien llamó la atención de Einstein sobre las curiosas propiedades de los estados entrelazados.
- Se fue a la Unión Soviética en 1936 (Kiev) y volvió a los Estados Unidos en 1941 (a la Universidad de North Carolina), donde estuvo hasta 1952.
- En 1953 emigró a Israel.

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- El trabajo al que se refiere el *New York Times* salió publicado en el número del 15 de mayo de 1935 de *Physical Review,* bajo el título de
- "¿Puede considerarse completa la descripción mecano-cuántica de la realidad?".

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Los puntos esenciales de este artículo se resumen ya en el artículo del *New York Times*.
- Según EPR, cualquier teoría física satisfactoria debe cumplir dos requisitos:

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Debe ser "correcta"; lo que implica que debe permitir calcular y predecir hechos comprobables experimentalmente.

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Puede ser "completa":
- "Una teoría satisfactoria debe, como una buena imagen del mundo objetivo, contener una contrapartida para las cosas encontradas en el mundo objetivo."

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- O como escriben EPR en *Physical Review, "cada elemento de la realidad física debe tener una contrapartida en la teoría física."*

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- ¿Qué es un elemento de ralidad para EPR?
- "Los elementos de realidad física no pueden determinarse por consideraciones filosóficas *a prio*ri, sino que deben encontrarse apelando a los resultados de experimentos y mediciones.

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- Una definición global de realidad es, sin embargo, innecesaria para nuestro propósito.
- Nos conformaremos con el siguiente criterio que consideraremos razonable.

MECÁNICA CUÁNTICA E INFORMACIÓN
El argumento de Einstein, Podolsky y Rosen

- *Si, sin perturbar de ninguna manera un sistema, podemos predecir con certeza (i.e., con probabilidad igual a la unidad) el valor de una cantidad física, entonces existe un elemento de realidad física correspondiente a esa cantidad física.”*

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- **El experimento de Bohm para ilustrar el argumento de EPR**
- El argumento que demuestra la incompletitud de la MC se basa en un experimento hipotético sobre un sistema de dos partículas preparado en un estado en el que la posición relativa de ambas partículas y el momento lineal total están perfectamente definidos.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- En 1951, David Bohm propuso un experimento hipotético diferente, que es conceptualmente equivalente al de EPR y mucho más sencillo de analizar matemáticamente en MC.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- El experimento de PR-Bohm es el siguiente:

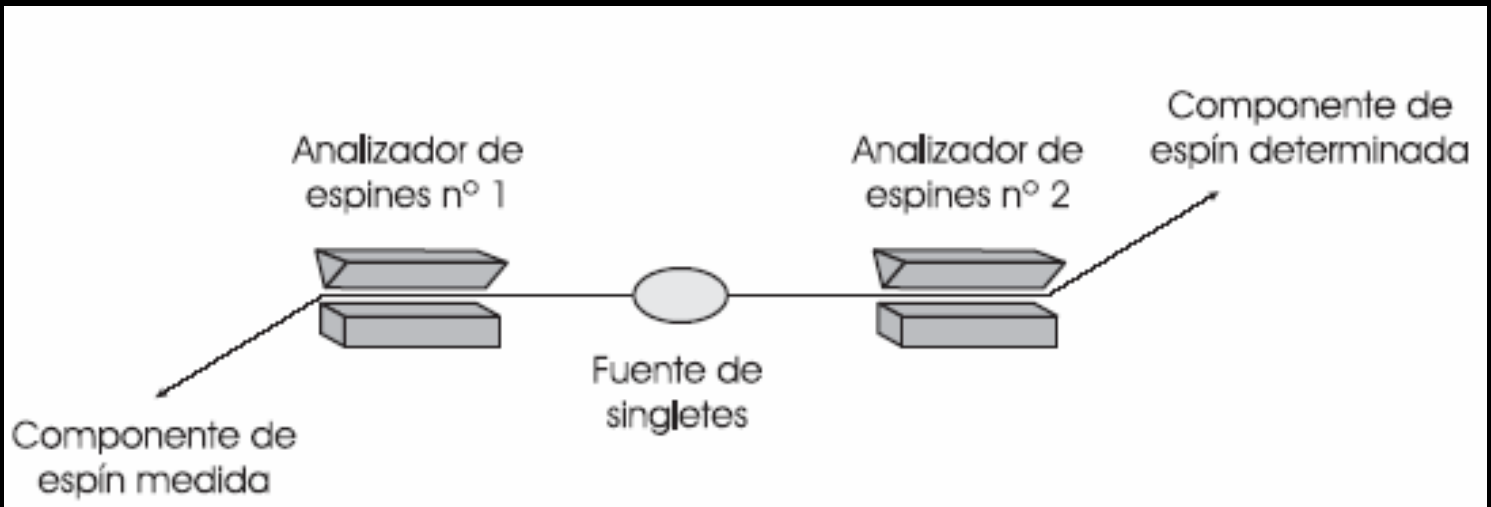


Figura 1: Esquema del experimento de Bohm para ilustrar el argumento de EPR.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Supongamos que tenemos una molécula que contiene dos átomos en un estado en el que el espín total es cero y que el espín de cada átomo es $\hbar/2$.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Ahora supongamos que la molécula se desintegra mediante un proceso que no cambia el momento angular total.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Los dos átomos empezarán a separarse y pronto dejarán de interactuar de forma apreciable.
- Sin embargo, su momento angular conjunto sigue siendo cero ya que, por hipótesis, no han actuado pares de fuerzas sobre el sistema.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Si el espín fuese un momento angular clásico, la interpretación de este proceso sería la siguiente:
- Mientras que los dos átomos están juntos formando una molécula, cada componente del momento angular de cada átomo tendría un valor definido que es siempre opuesto al del otro, haciendo cero de esta manera el momento angular total.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Cuando los átomos se separan, cada átomo continuaría teniendo cada componente de su momento angular opuesta a la del otro.
- Por tanto, los dos vectores momento angular estarían correlacionados.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Supongamos que uno mide el momento angular de espín de una cualquiera de las partículas (átomos), digamos la número 1.
- Debido a la existencia de correlaciones, uno puede concluir que el vector momento angular de la otra partícula (la número 2) es igual y opuesto al de la partícula número 1.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Ahora veamos cómo describe este experimento la mecánica cuántica.
- Aquí, el investigador puede medir la componente *x,* o la componente *y* o la componente *z* del espín de la partícula número 1, pero no más de una de estas componentes en un experimento (sin “perturbar” la otra componente, según nos dice el principio de Heisenberg).

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

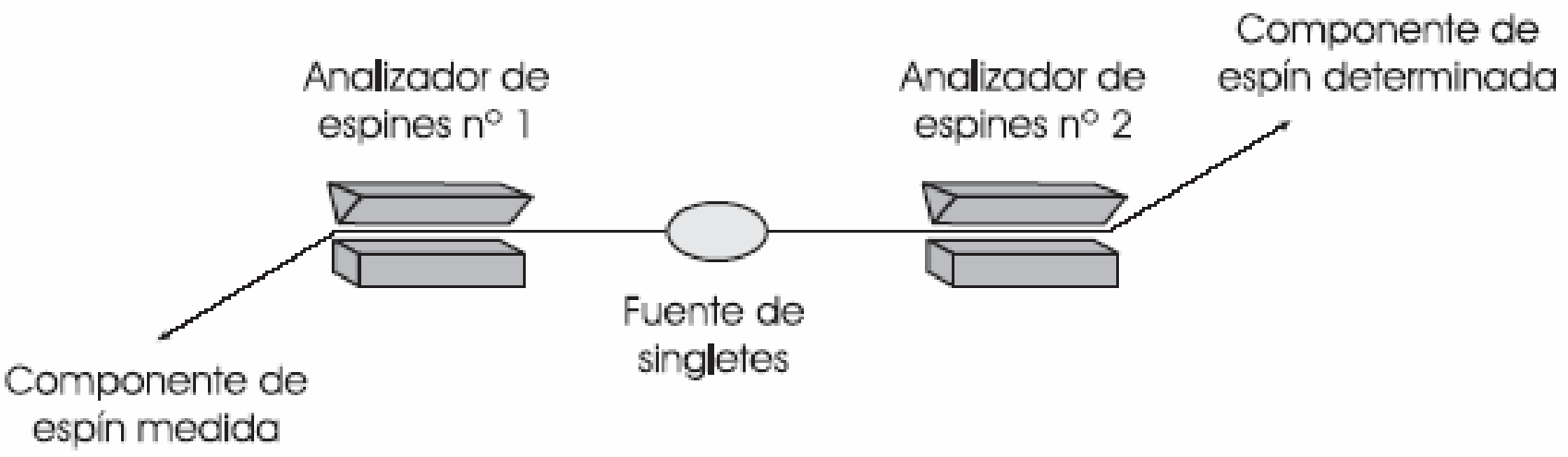


Figura 1: Esquema del experimento de Bohm para ilustrar el argumento de EPR.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- No obstante, todavía sucede que cualquiera que sea la componente medida, los resultados están correlacionados, de manera que si medimos la misma componente del espín del átomo número 2, siempre tendrá el valor opuesto.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Es decir, que una medición de cualquier componente del espín del átomo número 1 proporciona, lo mismo que en una teoría clásica, una medida indirecta de la misma componente de espín del átomo número 2.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Como, por hipótesis, las dos partículas no interactúan, hemos obtenido una forma de medir una componente arbitraria del espín de la partícula número 2 sin perturbarla en modo alguno.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Si aceptamos la definición de elemento de realidad sugerida por EPR, es claro que después de medir la componente σ_z para la partícula número 1, la componente σ_z de la partícula número 2 debe considerarse un elemento de realidad, que existe separadamente sólo en la partícula número 2.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Sin embargo, si esto es cierto, este elemento de realidad debe haber existido en la partícula número 2 incluso antes de que la medida de σ_z de la partícula número 1 tuviese lugar.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Ya que como, por hipótesis, no hay interacción con la partícula número 2, el proceso de medida no puede haber afectado de ninguna manera a esta partícula.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Pero recordemos que, en cada caso, el observador es libre para reorientar el aparato en una dirección arbitraria mientras que los átomos están todavía en vuelo y, por tanto, de obtener un valor definido (pero impredecible) de la componente de espín en cualquier dirección que elija.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Como esto puede hacerse sin perturbar de ninguna manera el segundo átomo, llegamos a la conclusión de que, si el criterio de EPR es aplicable, entonces deben existir elementos de realidad precisos en el segundo átomo, que corresponden a cualesquiera tres componentes de su espín.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- Como un estado cuántico permite especificar con total precisión sólo una de esas componentes como mucho, llegamos a la conclusión de que el estado cuántico no proporciona una descripción completa de todos los elementos de realidad que existen en el segundo átomo.

MECÁNICA CUÁNTICA E INFORMACIÓN

El experimento de Bohm para ilustrar el argumento EPR

- En resumen, según EPR, la descripción cuántica de este sistema es incompleta.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- **La descripción cuántica del experimento de EPR-Bohm.**
- Veamos ahora cómo describe este experimento la MC.
- El estado de espín de una partícula de espín ½ se representa en MC mediante un vector (o un operador) bidimensional.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- El estado de espín de una partícula de espín ½ es un ejemplo de lo que hoy se llama un ***qubit***, un sistema cuántico de dos niveles y, por tanto, la unidad mínima de información cuántica.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- El estado de espín de dos partículas se describe mediante el producto tensorial de dos vectores bidimensionales; esto es, mediante un vector de dimensión cuatro.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- El estado cuántico del sistema completo (no sólo de su parte de espín) se obtiene haciendo el producto tensorial del estado de espín por el estado espacial, que depende de las coordenadas espaciales de las dos partículas.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Cualquier estado de espín de dos partículas de espín ½ se puede expresar como una combinación lineal de una base de estados.
- Por ejemplo, una base puede ser la formada por los vectores:

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

$$|++\rangle = |+\rangle \otimes |+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad [1]$$

$$|+-\rangle = |+\rangle \otimes |-\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad [2]$$

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

$$|-+\rangle = |-\rangle \otimes |+\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad [3]$$

$$|--\rangle = |-\rangle \otimes |-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad [4]$$

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

Ddonde $|+\rangle$ y $|-\rangle$ son estados de espín de una sola partícula, que representan, respectivamente, que la partícula tiene componente de espín igual a $\hbar/2$ ó $-\hbar/2$ en la dirección z.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Así, por ejemplo, el estado $|+-\rangle$ representa que la partícula número 1 tiene la componente *z* de su espín con valor $\hbar/2$ y la partícula número 2 tiene la componente *z* de su espín con valor $-\hbar/2$.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- O eligiendo un sistema de unidades en el que $\hbar/2 = 1$, que la componente z tiene, respectivamente, el valor +1 ó -1.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Para construir el estado cuántico que representa la situación en la que el espín total del sistema es cero hay que percatarse de que los estados de la base anterior, los únicos en los que cada partícula tiene la componente de espín opuesta a la de la otra son $|+-\rangle$ y $|-+\rangle$.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Por tanto, el estado buscado debe ser una combinación lineal de esos dos estados.
- De las diferentes combinaciones lineales posibles, la única en la que el espín total del sistema conjunto es cero resulta ser

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+-\right\rangle - \left|-+\right\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \qquad [5]$$

que es el estado buscado.

- El estado [5] se llama estado ***singlete*** de espín.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- La primera observación importante sobre este estado es que el espín total del sistema está completamente definido pero que la componente *z* del espín de cada partícula está *completamente indefinida.*

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- De hecho, si usamos las reglas de la MC para calcular cuál es la probabilidad de obtener $\hbar/2$ al medir la componente z de la partícula número 1, obtendremos ½, que es la misma probabilidad de obtener el otro resultado (el resultado opuesto).

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- La segunda observación importante es que si expresamos el singlete en otra base ortogonal formada por los estados propios de las componentes de espines individuales en otra dirección, digamos *n* (formada por los cuatro vectores:

$$\left|\mathrm{n}+\mathrm{n}+\right\rangle,\ \left|\mathrm{n}+\mathrm{n}-\right\rangle,\ \left|\mathrm{n}-\mathrm{n}+\right\rangle \quad \mathrm{y} \quad \left|\mathrm{n}-\mathrm{n}-\right\rangle$$

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Y, el singlete se escribe

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|n+n-\right\rangle - \left|n-n+\right\rangle\right) \qquad [6]$$

- Es decir, la primera observación es válida no sólo para las componentes en la dirección *z* sino también para las componentes en cualquier dirección *n*.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- La tercera observación es que, además de tener un valor definido del espín total, si se mide la misma componente de espín en cada partícula, los resultados estarán correlacionados: serán opuestos.
- Exactamente igual que en la teoría clásica.

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Por ejemplo, si se miden las componentes en la dirección *z*, si el resultado de la partícula número 1 es $-\hbar/2$, el resultado de la partícula número 2 será $\hbar/2$, y lo mismo si medimos las componentes en la dirección *x* o *y*.
- Esto lo expresaremos:

MECÁNICA CUÁNTICA E INFORMACIÓN

Descripción cuántica del experimento de EPR-Bohm

$$Z_1 = -Z_2 \qquad [7]$$

$$X_1 = -X_2 \qquad [8]$$

$$Y_1 = -Y_2 \qquad [9]$$

MECÁNICA CUÁNTICA E INFORMACIÓN
Descripción cuántica del experimento de EPR-Bohm

- Como curiosidad diremos que, según el *Science Citation Index*, el artículo de EPR se ha convertido en el más citado en la literatura científica de entre todos los trabajos de Einstein.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

"El entrelazamiento no es *un* sino más bien *el* rasgo característico de la mecánica cuántica, el que obliga a desviarse completamente de las líneas clásicas del pensamiento."

Erwin Schrödinger

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- El sustantivo “entrelazamiento” y el adjetivo “entrelazado” (o en alemán “Verschränkung” (cruzamiento) y “verwickelten” (enredado, enmarañado) –que eran los que usó Schrödinger para bautizarlos- o en inglés “entanglement” y “entangled”) son ejemplos de algo muy común en física: términos que nos dan la impresión de que sabemos lo que significan pero que en realidad son palabras cifradas que necesitan una aclaración algo más amplia.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- En este caso, esa aclaración requiere unos conocimientos mínimos de MC.
- Se dice que un sistema se halla en un **estado cuántico *puro*** si la información que se posee sobre ese sistema es la máxima permitida por la MC.
- Los estados puros de sistemas físicos discretos se representan por vectores (en un cierto espacio de Hilbert).

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- Un estado puro de un sistema de dos partículas se dice que se halla en un *estado entrelazado* si ese estado no se puede expresar como un producto de estados puros de cada una de las partículas.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- Es decir $|\psi\rangle$ es un estado entrelazado si no se puede escribir como

$$|\alpha\rangle \otimes |\beta\rangle$$

donde $|\alpha\rangle$ es un estado puro de la partícula número 1 y $|\beta\rangle$ es un estado puro de la partícula número 2.

- El símbolo $\otimes$ denota producto tensorial.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- Un estado puro que no es entrelazado se dice que es un *estado factorizable* o un *estado puro*.
- Un estado puro entrelazado de dos partículas se dice que es *máximamente entrelazado* si el estado del sistema conjunto está perfectamente definido pero los estados de las partículas están completamente indefinidos.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- Una forma de expresar esto es diciendo que la información contenida en ese estado es toda ella sobre las correlaciones entre las partículas y no se dice nada de los estados individuales de las partículas.
- El singlete es un estado máximamente entrelazado.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- Hay estados que son entrelazados pero no máximamente entrelazados.
- Por ejemplo, consideremos los estados de la forma:

$$\left|\Psi\right\rangle = \cos\theta\left|+-\right\rangle - \operatorname{sen}\theta\left|-+\right\rangle \quad [10]$$

- Si $\theta = n\pi/2$ con n entero, el estado $\left|\Psi\right\rangle$ es factorizable.
- Si $\theta = \pi/4 + n\pi/2$ el estado $\left|\Psi\right\rangle$ es máximamente entrelazado.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- En los restantes casos el estado $|\Psi\rangle$ es entrelazado pero no máximamente.
- En los estados entrelazados no máximamente las probabilidades de obtener los dos posibles resultados al medir una componente particular del espín ya no son siempre iguales.

MECÁNICA CUÁNTICA E INFORMACIÓN
Estados entrelazados y máximamente entrelazados

- La noción de entrelazamiento se puede extender a sistemas con más de dos partículas.
- Por ejemplo, un estado puro de un sistema de tres partículas se dice que es entrelazado si no se puede escribir como:

$$|\alpha\rangle \otimes |\beta\rangle \otimes |\gamma\rangle$$

LAS DESIGUALDADES DE BELL
El teorema de Bell

- En un artículo de 1964 Bell demuestra que para el estado singlete las predicciones *estadísticas* de la MC resultan incompatibles con una "predeterminación separable" (i.e., con los elementos de realidad de EPR).

LAS DESIGUALDADES DE BELL
El teorema de Bell

- Bell viene a decir que la MC no sólo es “incompleta” sino que también debe ser “incorrecta”.
- En otras palabras, una teoría “completa” a la manera de EPR conduce a predicciones diferentes.

LAS DESIGUALDADES DE BELL
El teorema de Bell

- ¿Cuáles son las “predicciones estadísticas” de la MC para el singlete?
- Esencialmente que si A es una componente de espín de la partícula número 1 y B de la partícula 2 y las direcciones de A y B forman un ángulo θ_{AB}, entonces en el singlete el valor esperado de AB (el producto de ambas componentes) es $-\cos\theta_{AB}$ (en unidades en las que $\hbar/2 = 1$).

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- La desigualdad de Clauser, Horne, Shimony y Holt (CHSH), de 1969, es diferente de la desigualdad de Bell de 1964, pero incluye ésta como caso particular y, además, es muy fácil de derivar.
- Sean *A, a, B* y *b* cuatro cantidades cuyos posibles valores son -1 y 1.
- Consideremos las expresiones *A* + *a* y *A* - *a*: necesariamente una de ellas es cero y la otra -2 ó 2.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Por tanto, la expresión

$$B(A + a) + b(A - a)$$

  necesariamente vale -2 ó 2.
- Supongamos ahora que *A, a, B* y *b* fuesen observables físicos cuyos valores estuviesen predefinidos para cada sistema individual y supongamos que disponemos de muchos sistemas individuales sobre los que medir esas cantidades.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Entonces, por lo dicho antes, está claro que al promediar los resultados de esas medidas deberá suceder que

$$-2 \leq (AB + Ab + aB - ab) \leq 2 \qquad [11]$$

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Supongamos ahora que los sistemas físicos son pares de partículas de espín ½ preparados en el estado singlete, y que *A* y *a* son dos componentes de espín de la partícula número 1, mientras que *B* y *b* son componentes de espín de la partícula número 2.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Supongamos además que las partículas 1 y 2 están lo suficientemente alejadas entre sí para que nada que se haga sobre la partícula número 1 pueda influir causalmente (i.e., a velocidades no superiores a la de la luz en el vacío) sobre la partícula número 2.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Entonces, *A, a, B* y *b* verifican cada uno de ellos el criterio de elemento de realidad de EPR.

Experimento de Bell-CHSH

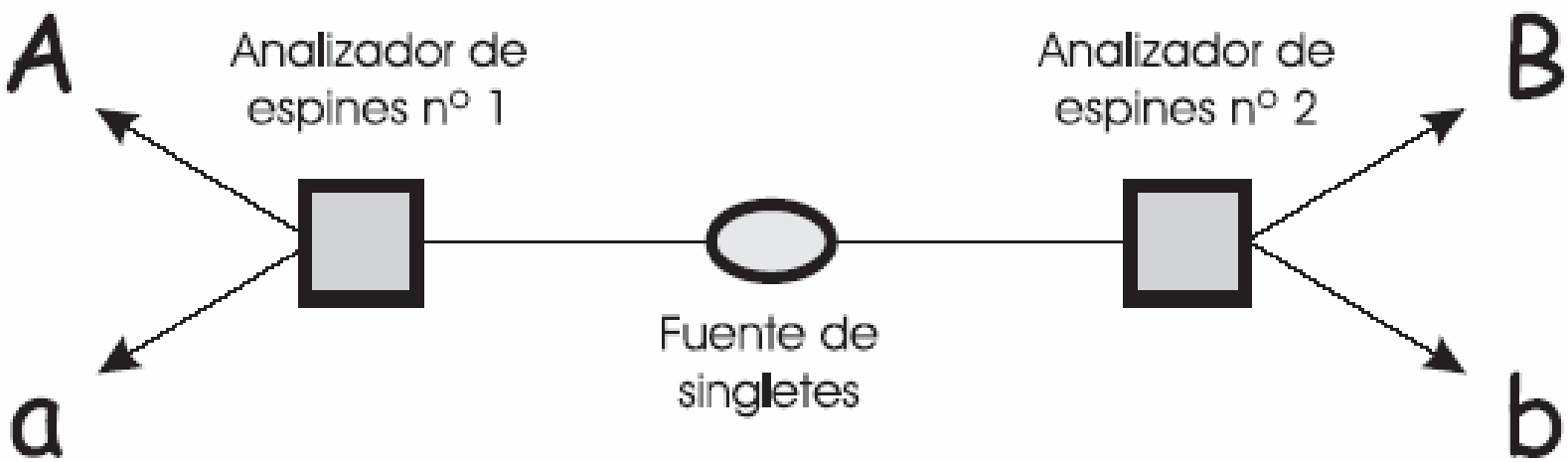


Figura 2: Esquema del experimento para comprobar las desigualdades de Bell-CHSH. A y a son dos experimentos alternativos sobre las partículas de la izquierda, B y b son dos experimentos alternativos sobre las partículas de la derecha.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- En MC no podemos medir simultáneamente *A* y *a*, ni *B* y *b*, sin embargo sí podemos hacer experimentos en los que midamos *A* y *B*, otros en los que midamos *A* y *b*, otros en los que midamos *a* y *B*, y otros en los que midamos *a* y *b*.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Suponiendo que los valores de los observables medidos no dependen de los no medidos, también debe ocurrir que los promedios de los cuatro experimentos alternativos cumplan

$$-2 \leq \langle AB \rangle + \langle Ab \rangle + \langle aB \rangle - \langle ab \rangle \leq 2 \quad [12]$$

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Sin embargo, la MC dice que si *A* y *B* son componentes de espín que forman un ángulo θ_{AB}, entonces en el singlete el valor esperado de *AB* es $-\cos\theta_{AB}$.
- Por tanto

$$\langle AB\rangle + \langle Ab\rangle + \langle aB\rangle - \langle ab\rangle = -\cos\theta_{AB} - \cos\theta_{Ab} - \cos\theta_{aB} + \cos\theta_{ab} \quad [13]$$

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- Eligiendo

  $cos\theta_{AB} = cos\theta_{Ab} = cos\theta_{aB} = cos\theta_{ab} = \sqrt{2}/2$

  Por ejemplo, midiendo las componentes

  $A = \sigma_z$, $a = \sigma_Y$,

  $B = (-\sigma_x - \sigma_y)/\sqrt{2}$

  $b = (-\sigma_x + \sigma y)/\sqrt{2}$

  se obtiene $2\sqrt{2}$ que es mayor que 2.

LAS DESIGUALDADES DE BELL

La demostración de Clauser, Horne, Shimony y Holt.

- En resumen: en ciertas situaciones la MC viola la desigualdad [12].
- Las desigualdades de CHSH se violan para cualquier estado entrelazado de dos partículas, pero la máxima violación, $2\sqrt{2}$, se obtiene para los estados máximamente entrelazados (también llamados “estados de Bell”) como el singlete.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- En 1989, Greenberger, Horne y Zeilinger (GHZ) obtuvieron una extraordinaria demostración de la incompatibilidad entre la MC y los elementos de realidad de EPR.
- Esta demostración fue luego simplificada por David Mermin.
- Las características de la demostración de GHZ-Mermin del teorema de Bell son:

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Sólo usa *correlaciones perfectas* (y no predicciones estadísticas, como en las demostraciones de Bell y CHSH), lo cual la hace fantásticamente sencilla (en otras palabras, es una demostración “sin probabilidades”).
- Sirve sólo para un tipo particular de estados de *tres o más partículas* que, desde entonces, se conocen como *estados de GHZ.*

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Un estado de GHZ para un sistema de tres qubits es, por ejemplo,

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}\left(|+++\rangle - |---\rangle\right) \quad [14]$$

ESQUEMA DEL EXPERIMENTO GHZ

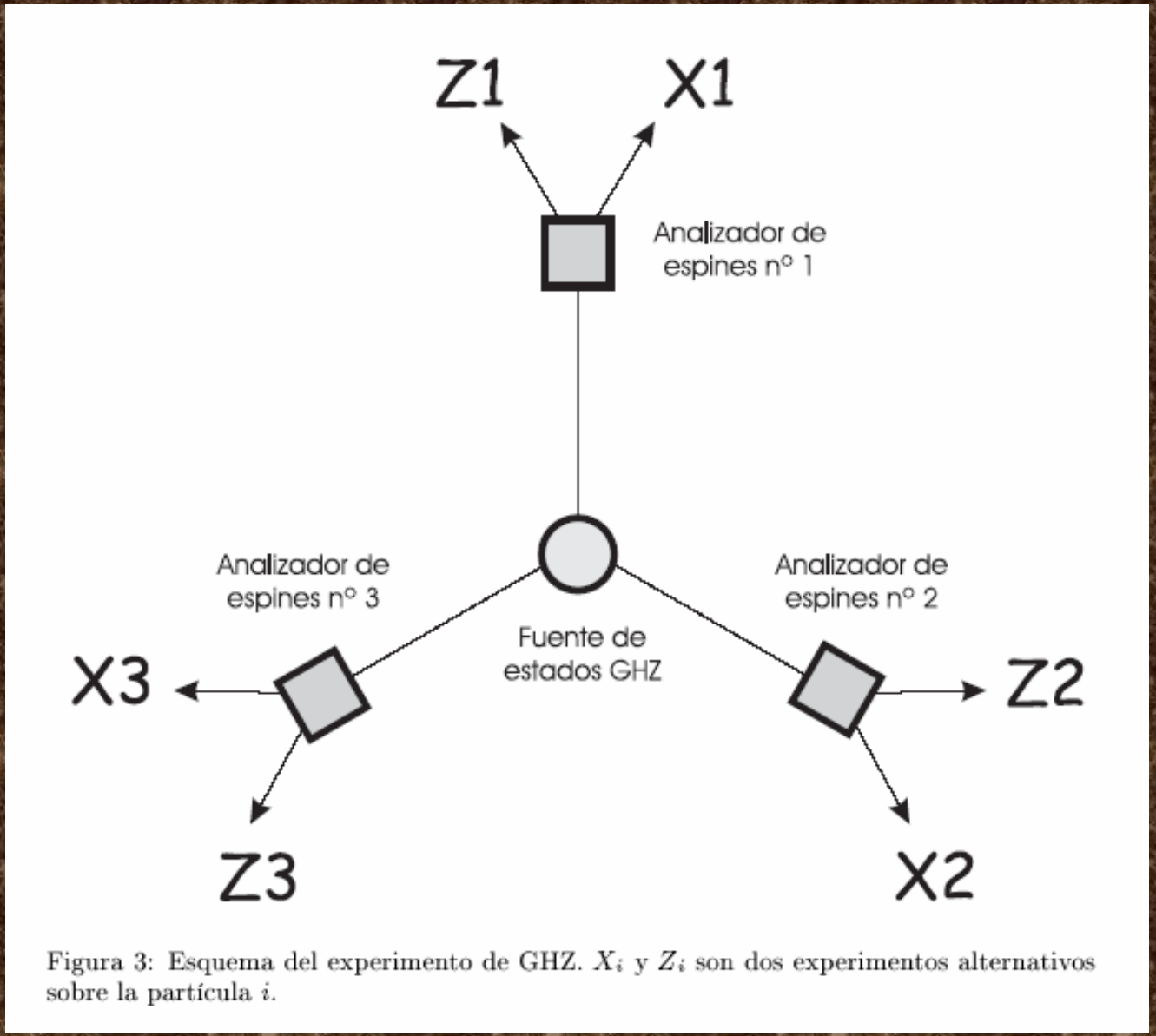


Figura 3: Esquema del experimento de GHZ. X_i y Z_i son dos experimentos alternativos sobre la partícula i.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Si de manera similar a como hicimos antes, llamamos X_1 al resultado de medir la componente *x* del espín de la partícula número 1, Y_2 al resultado de medir la componente *y* del espín de la partícula número 2, Y_3 al resultado de medir la componente *y* de la partícula número 3, etc. (pero ahora en unidades tales que $\hbar/2 = 1$).

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Las correlaciones entre los resultados que nos interesan para la demostración se pueden resumir en las siguientes ecuaciones:

$$X_1 Y_2 Y_3 = 1 \qquad [15]$$

$$Y_1 X_2 Y_3 = 1 \qquad [16]$$

$$Y_1 Y_2 X_3 = 1 \qquad [17]$$

$$X_1 X_2 X_3 = -1 \qquad [18]$$

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- De ellas se deduce que X_1, Y_1, X_2, Y_2, X_3 e Y_3 cumplen el criterio de EPR de elementos de realidad puesto que cualquiera de ellos se puede predecir con certeza a partir de medidas sobre las otras dos partículas.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Si hacemos la hipótesis de que las tres partículas están lo suficientemente alejadas entre sí como para que nada que se haga sobre ellas pueda afectar causalmente a las demás, ello implica que las medidas sobre las partículas 1 y 2 que permiten determinar, por ejemplo, X_3, no pueden perturbar la tercera partículas.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Sin embargo, las cuatro ecuaciones anteriores también demuestran que es imposible que existan todos esos elementos de realidad.
- La demostración es muy sencilla por reducción al absurdo:

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Supongamos que X_1, Y_1, X_2, Y_2, X_3 e Y_3 tuviesen predefinidos -1 ó 1 (que equivalen, en los ejemplos anteriores, a $-\hbar/2$ y $\hbar/2$).
- Entonces el valor de, por ejemplo, X_1 sería el mismo en la primera ecuación y en la cuarta.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Sin embargo, es imposible completar esa asignación de valores por el sencillo motivo de que cada valor aparece exactamente dos veces, por lo que al multiplicar las cuatro ecuaciones necesariamente obtendríamos un 1 a la izquierda del signo igual, mientras que obtendríamos un -1 a la derecha.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- En 2000, PAN y sus colaboradores han hecho un experimento con fotones en el que han verificado, dentro de un razonable error experimental, estas predicciones de la MC.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Hardy

- En 1993, Lucien Hardy propuso una demostración del teorema de Bell sin desigualdades (pero “con probabilidades”) válida para dos qubits en un estado no máximamente entrelazado.
- La de Hardy es probablemente la demostración más sencilla posible del teorema de Bell.

D. Bouwmeester, L. Hardy, J. Eisert y A. Cabello.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Hardy demostró que cualquier estado no máximamente entrelazado $|\eta\rangle$

  de dos qubits, existen dos observables (componentes de espín, por ejemplo) *A* y *a* para la partícula 1 y dos observables *B* y *b* para la partícula 2, tales que el estado se puede expresar en las correspondientes cuatro bases ortogonales de las siguientes formas:

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

$$|\eta\rangle = c_{++}|A+B+\rangle + c_{+-}|A+B-\rangle + c_{-+}|A-B+\rangle + c_{--}|A-B-\rangle \qquad [19]$$

$$= d_{++}|A+b+\rangle + d_{-+}|A-b+\rangle + d_{--}|A-b-\rangle \qquad [20]$$

$$= f_{++}|a+B+\rangle + f_{+-}|a+B-\rangle + f_{--}|a-B-\rangle \qquad [21]$$

$$= g_{++}|a+b-\rangle + g_{-+}|a-b+\rangle + g_{--}|a-b-\rangle \qquad [22]$$

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Los coeficientes c_i, d_i, f_i y g_i son todos distintos de cero.
- De esas cuatro ecuaciones se deduce que cualquier estado tiene las siguientes propiedades

$$P_\eta(A = +1,\ B = +1) = |c_{++}|^2 \qquad [23]$$

$$P_\eta(b = +1;\ A = +1) = 1 \qquad [24]$$

$$P_\eta(a = +1;\ B = +1) = 1 \qquad [25]$$

$$P_\eta(a = +1,\ b = +1) = 0 \qquad [26]$$

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Consideremos ahora un experimento en el que se hayan medido *A* (sobre la partícula número 1) y *B* (sobre la número 2) y fijémonos en un suceso en el que se haya obtenido en ambas mediciones el resultado +1.
- Esto puede ocurrir, según nos dice la propiedad [23].

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Imaginemos ahora que en ese mismo suceso hubiésemos medido sobre la partícula número 2 el observable *b* en lugar del observable *B*.
- Según la propiedad [24] el resultado de esa medición habría sido, con total certeza $b = +1$.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- De hecho, desde el momento que en la partícula número 1 se obtiene $A = +1$ es posible predecir con certeza y sin perturbar la partícula número 2 (si asumimos que las partículas están suficientemente alejadas) que el valor de b es +1.
- Entonces, según EPR, en ese suceso la segunda partícula tiene un elemento de realidad correspondiente a $b = +1$.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Mediante un argumento similar, a partir de la propiedad [25] podemos concluir que en ese suceso la partícula número 1 tiene un elemento de realidad correspondiente a $a = +1$.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

- Por tanto, si en ese suceso hubiésemos medido *a* sobre la partícula número 1 y *b* sobre la partícula número 2, habríamos obtenido $a = +1$ y $b = +1$.
- Sin embargo, esto contradice la propiedad [26].
- Por tanto, para un sistema preparado en un estado no máximamente entrelazado (o *estado de Hardy*) no pueden existir elementos de realidad.

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración de Greenberger, Horne y Zeilinger

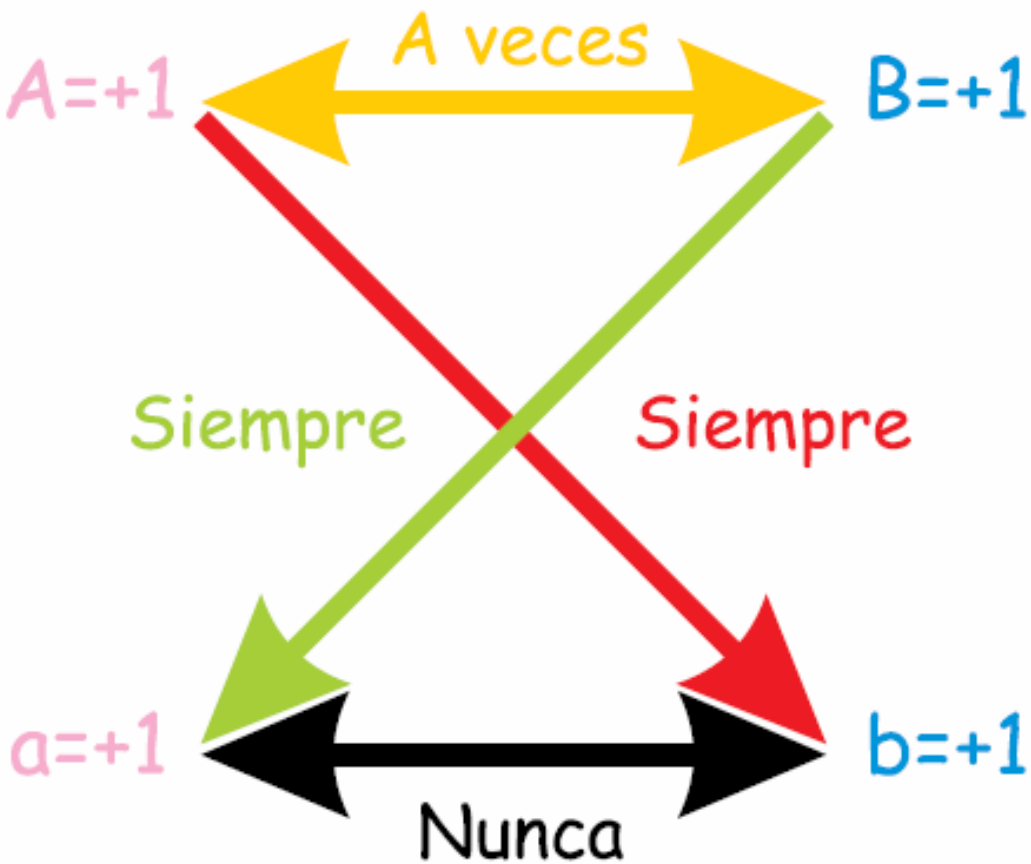


Figura 4: Esquema lógico de la demostración de Hardy.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- La demostración de GHZ usa sólo correlaciones perfectas, pero sólo vale para ciertos estados entrelazados de tres o más partículas.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- La demostración de Hardy vale para estados entrelazados de dos partículas pero, curiosamente, no para los estados máximamente entrelazados (como el singlete), que son precisamente aquellos para los que la violación de las desigualdades de Bell es máxima.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- En este punto surgen de manera natural dos preguntas:
- ¿Se puede extender la demostración de Hardy a estados máximamente entrelazados como el singlete?
- ¿Se puede demostrar el teorema de Bell para el singlete usando sólo correlaciones perfectas?

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- La respuesta es sí para ambas preguntas.
- La respuesta a la primera pregunta se puede encontrar en la primera página del número del 5 de marzo de 2001 de *Physical Review Letters*, y la respuesta a la segunda en el número de 2 de julio.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- De hecho, las dos respuestas están estrechamente relacionadas y las demostraciones de tipo (a) y (b) son en realidad dos formas distintas de una misma demostración.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- El “truco” de estas demostraciones del teorema de Bell consiste en preparar *dos* parejas de partículas en el estado singlete y en permitir mediciones no sólo de componentes de espín (en las direcciones *z* o *x*) sino también de observables de dos partículas, como por ejemplo (cuyo resultado representaremos por Z_1Z_2).

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- A continuación, vamos a ver la demostración del teorema de Bell para el singlete usando sólo correlaciones perfectas.

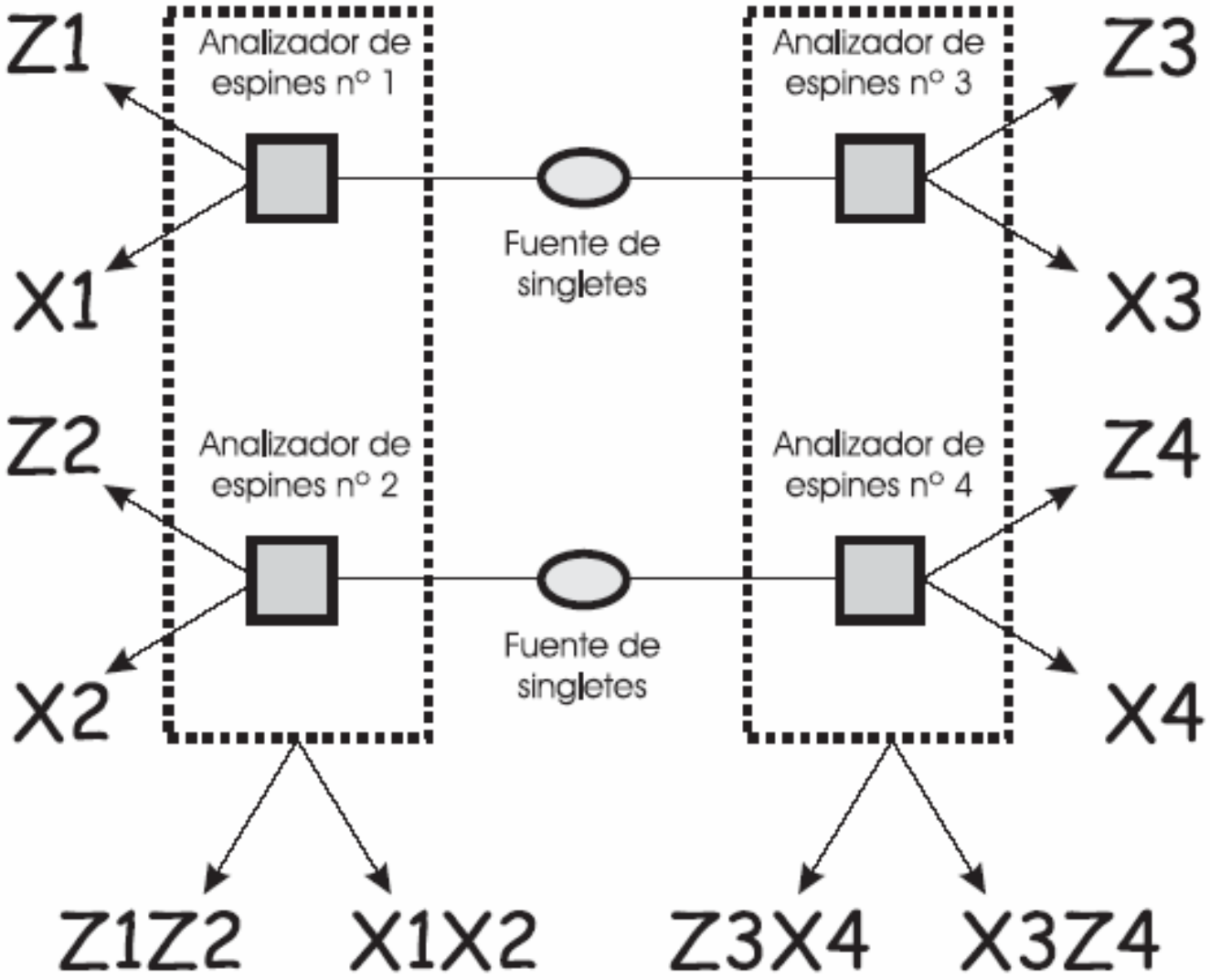


Figura 5: Esquema del experimento para demostrar el teorema de Bell sin desigualdades para el singlete. X_i y Z_i son dos experimentos alternativos sobre la partícula i, Z_1Z_2 es un experimento conjunto sobre las partículas 1 y 2, etc.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- Supongamos que las partículas número 1 y número 3 están en el estado singlete y que también lo están las partículas número 2 y número 4.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- Supongamos también que un observador puede hacer mediciones sobre las partículas número 1 y número 2, mientras que otro observador suficientemente alejado puede hacer mediciones sobre las partículas número 2 y número 4.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- En ese caso, usando sólo correlaciones perfectas se puede demostrar que no existen elementos de realidad.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- La demostración es fruto de una contradicción algebraica similar a la que se obtenía en la demostración de GHZ y se resume en que es imposible asignar valores definidos, -1 ó 1, a los 12 observables que aparecen en las siguientes nueve ecuaciones (seis para la pareja formada por las partículas número 1 y número 2, 6 para la pareja formada por las partícula número 3 y número 4):

EL TEOREMA DE BELL SIN DESIGUALDADES

La demostración para estados máximamente entrelazados.

$$Z_1 = -Z_3 \quad [27]$$

$$X_1 = -X_3 \quad [28]$$

$$Z_2 = -Z_4 \quad [29]$$

$$X_2 = -X_4 \quad [30]$$

$$Z_1Z_2 = Z_3 \cdot Z_4 \quad [31]$$

$$X_1X_2 = X_3 \cdot X_4 \quad [32]$$

$$Z_1 \cdot X_2 = Z_3X_4 \quad [33]$$

$$X_1 \cdot Z_2 = X_3Z_4 \quad [34]$$

$$Z_1Z_2 \cdot X_1X_2 = -Z_3X_4 \cdot X_3Z_4 \quad [35]$$

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- La demostración es muy similar a la de antes: cada observable aparece en dos ecuaciones y siempre en el mismo lado de la ecuación.
- Por tanto, el producto de los lados izquierdos es 1 mientras que el producto de los lados derechos es -1.

EL TEOREMA DE BELL SIN DESIGUALDADES
La demostración para estados máximamente entrelazados.

- Por tanto, aunque existen correlaciones perfectas entre los resultados de esos experimentos nos vemos obligados a concluir que los resultados no estaban determinados antes de los experimentos

Epílogo: “It from bit”

- “Llegué a la frase “ello del bit” intentando casar en mi cerebro la idea de la teoría de la información como base de la existencia.
- El universo y todo lo que contiene (“ello”) puede surgir de la mirada de elecciones sí-no de la medición (los “bits”).

Epílogo: “It from bit”

- Niels Bohr pasó gran parte de su vida luchando con la pregunta de cómo los actos de medida (o “registro”) pueden afectar la realidad.
- El registro (...) es lo que cambia la potencialidad en actualidad.

Epílogo: “It from bit”

- Yo sólo he construido un poco sobre la estructura del pensamiento de Bohr cuando sugiero que nunca entenderemos esta extraña cosa, el cuanto, hasta que no entendamos cómo la información puede servir de base a la realidad.
- La información puede no sólo ser simplemente lo que *aprendemos* del mundo sino lo que *hace* el mundo.

Epílogo: “It from bit”

- Un ejemplo de la idea de ello del bit.
- Cuando se absorbe un fotón y de se modo se “mide” –hasta su absorción, no tiene verdadera realidad- se añade un bit indivisible de información a lo que conocemos del mundo, *y*, al mismo tiempo, ese bit de información determina la estructura de una pequeña parte del mundo.
- *Crea* la realidad del momento y lugar de esa interacción del fotón.”