“Entrelazamiento, ergodicidad, aleatoriedad”

Alejandro Hnilo

Centro de Investigaciones en Láseres y Aplicaciones (CEILAP) (CITEDEF-CONICET).

9a Jornada de Lógica, Computación e Información Cuántica

CITEDEF, 24 de Octubre de 2019.

Ergodicidad:

La integral en el tiempo (para un tiempo "largo") de una variable dinámica es igual a su integral sobre el espacio de fases:

$$\langle x \rangle_t = (1/T) \int dt.x(t); \langle x \rangle_r = \int dr.x(r)$$

$$\langle x \rangle_t = \langle x \rangle_r$$

Entrelazamiento:

Propiedad de sistemas cuánticos (a menudo después de una interacción) en la que la descomposición en términos de las bases individuales deja de ser separable.

$$|A\rangle = \Sigma a_i |a_i\rangle, \; |B\rangle = \Sigma b_i |b_i\rangle, |\psi\rangle = \Sigma \varphi_i |b_i\rangle \otimes |a_i\rangle$$

$$|\psi\rangle \neq \{\Sigma a'_i |a_i\rangle\} \otimes \{\Sigma b'_i |b_i\rangle\}$$

A menudo $|A\rangle$ y $|B\rangle$ están espacialmente separados, lo que es el origen de paradojas: $|\varphi\rangle$ es un "átomo" de *tamaño* arbitrario.

Aleatoriedad es un término más difícil de definir.
(Martin-Löf, Borel normal, Kolmogorov, Turing incomputable…)

Desde el punto de vista práctico, hay dos definiciones principales :

• "Estadística": el número de 1 y 0 de diferente longitud (p.ej. 110101 for n=6) en la secuencia coincide con el que se obtendría tirando una moneda ideal (≈normal Borel). La batería de tests del NIST está en gran parte basada en esta definición.

• "Algorítmica" : Si no hay un programa (que corre una máquina de Turing clásica) capaz de reproducir la secuencia usando menos bits que la misma secuencia ("Complejidad", Kolmogorov, Chaitin and Solomonoff).

La aleatoriedad algorítmica se considera la forma más fuerte de aleatoriedad. PERO, no puede *calcularse*. Sólo puede *estimarse* mediante algoritmos compresores (como el de Lempel & Ziv).

Todo el mundo está de acuerdo en que:

Predecible ⇒ no aleatorio, luego:

Aleatorio ⇒ no *predecible*.

(pero…¿predecible por quién? ¿Contando con qué información?)

Nótese que todavía queda la posibilidad lógica de ser “no aleatorio” y a la vez “no predecible” (¿caótico?)

Todo el mundo está de acuerdo en que:

Predecible ⇒ no aleatorio, luego:

Aleatorio ⇒ no *predecible*.

(pero…¿predecible por quién? ¿Contando con qué información?)

Nótese que todavía queda la posibilidad lógica de ser "no aleatorio" y a la vez "no predecible" (¿caótico?)

Una solución atractiva:

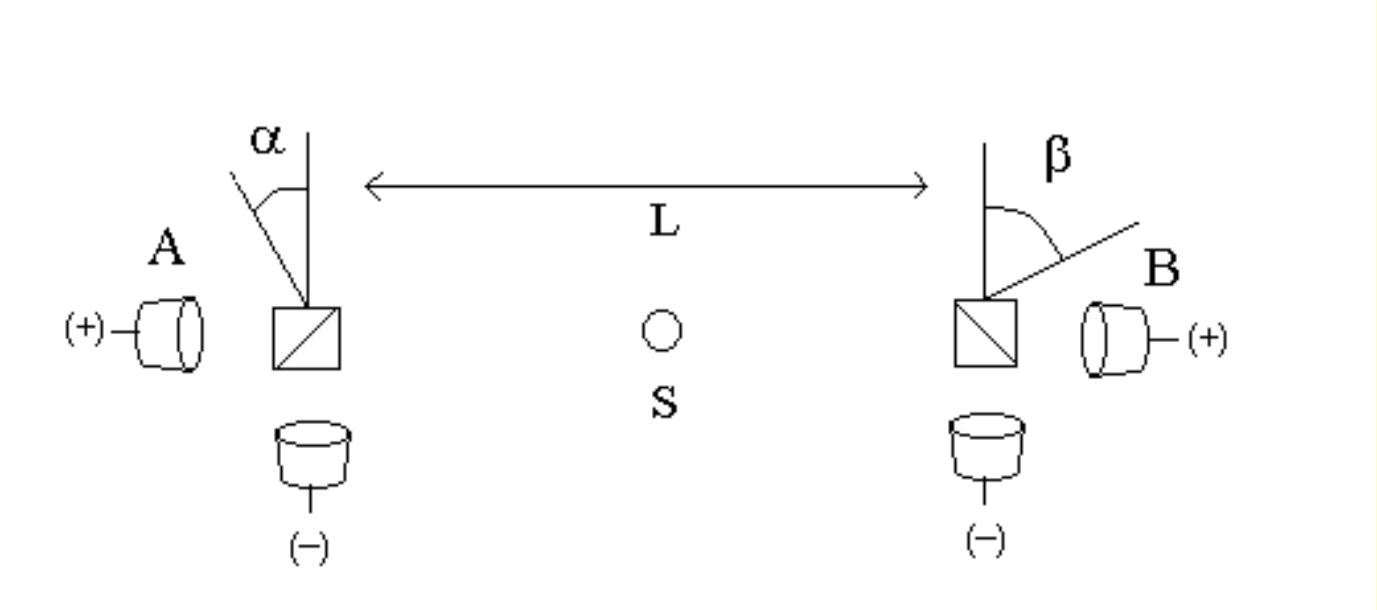
¡Los resultados de mediciones realizadas sobre (ciertos) sistemas cuánticos son **aleatorios**!

(pero…)

En esta charla voy a explorar la relación entre esas tres propiedades, y cómo su estudio es importante para generar números aleatorios, para la seguridad de QKD y para echar luz sobre aspectos fundamentales del mundo físico.

El bien conocido experimento que nos ocupa:

(S es una fuente de estados entrelazados)



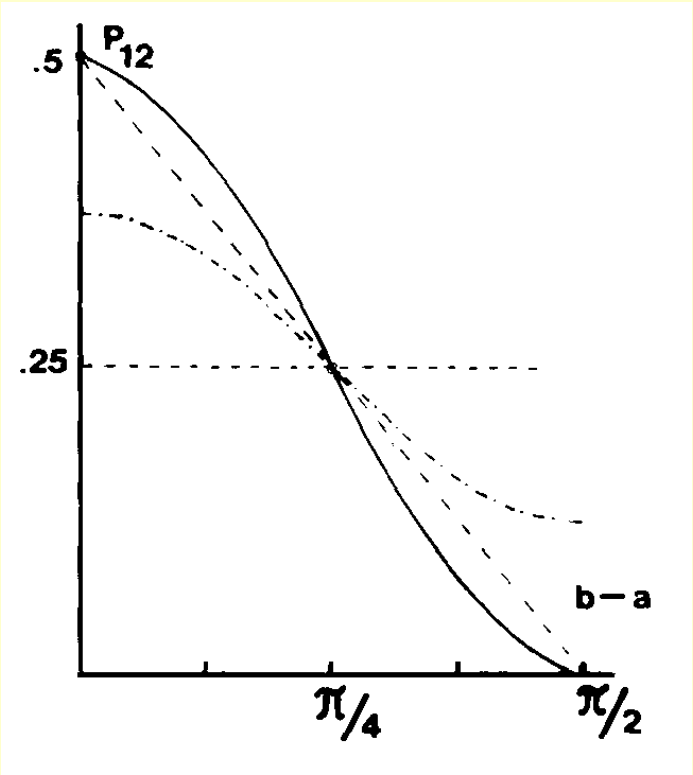
$$|\varphi^{+}\rangle = (1/\sqrt{2})\{\,|x_A,x_B\rangle + |y_A,y_B\rangle$$

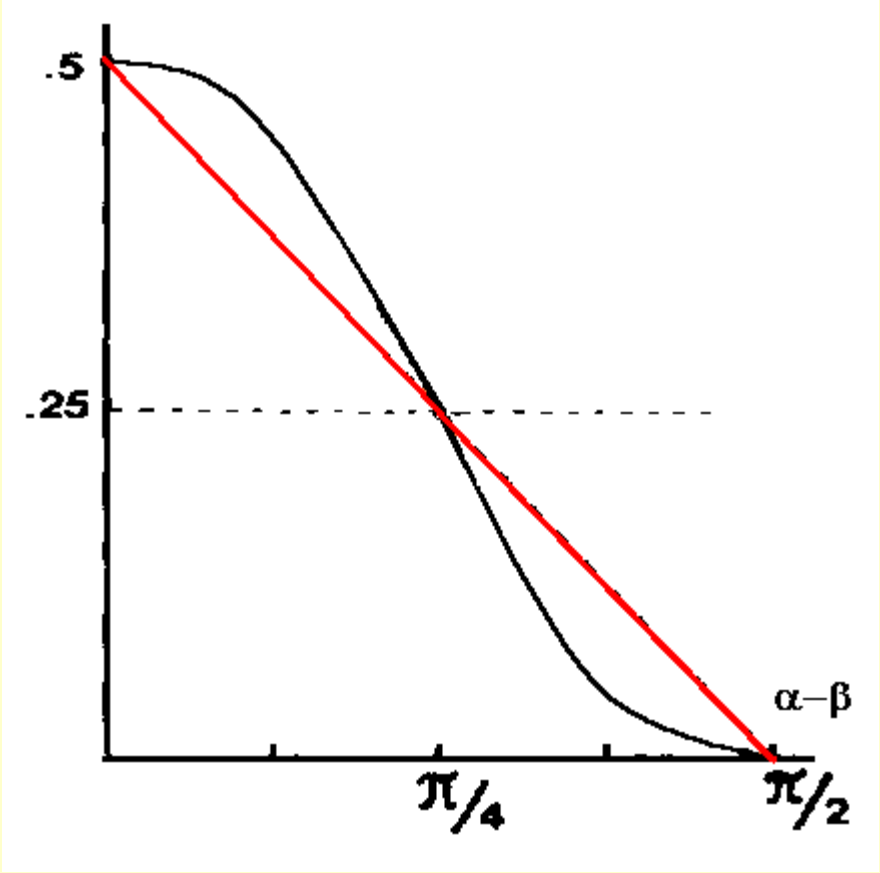
Un modelo simple que supone válidas las ideas intuitivas de “Localidad” y “Realismo” establece un límite a la magnitud de las correlaciones entre los resultados de observaciones realizadas en A y B.

Algunos estados entrelazados violan este límite.

$P_{AB}(\alpha,\beta) = \frac{1}{2} \cdot cos^2(\alpha-\beta)$

Viola el límite impuesto por las desigualdades de Bell (que se deducen a partir de suponer válidos "Localidad" + "Realismo").





El modelo semi-clásico de radiación no viola las desigualdades de Bell, pero la curva tiene la misma forma.

¿deficiencias instrumentales? ("l*oopholes*")

- *Detection (Fair-sampling)*
- *Locality (Predictability)*
- *Time-coincidence (falso Ergodic!)*

Un resumen de los principales experimentos *loophole-free*.

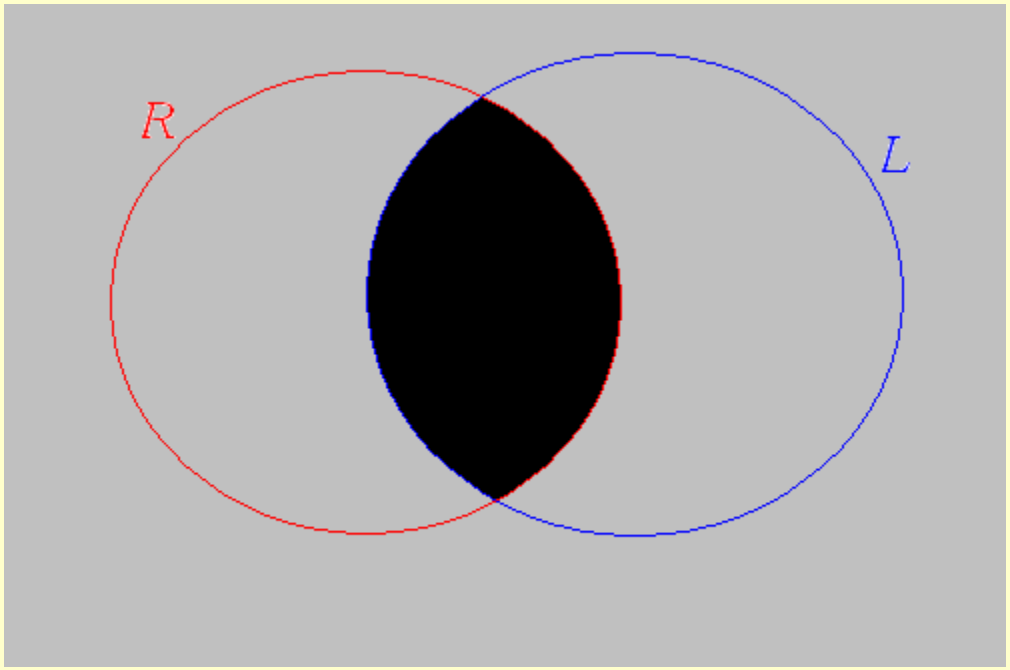
Phys.Rev.A **95**, 022102 (2017).

TABLE I. Summary of some parameters of interest; J_m is the experimentally obtained value of the left-hand side of the EI, J_{QM} is the QM ideal prediction, J_{corr} is the QM prediction but corrected by the separately measured efficiencies η_{meas}, η_{eq} is the efficiency value that makes $J_{corr} = J_m$, q_{QM} is the correlation probability between the hidden variable μ and the analyzers' settings the HV + DZ needs to reproduce J_{QM}, q_m is the same but to reproduce J_m, and q_{set} is the predictability of the RNG as estimated by the authors of the experiments.

	Giustina *et al.* [3]; see Sec. IV B	Christensen *et al.* [4]; see Sec. IV C	Giustina *et al.* [5]; see Sec. IV D	Shalm *et al.* [6]; see Sec. IV E	Hensen *et al.* [7]; see Sec. IV F
J_m	$5.24 \times 10^{-3} \pm 8 \times 10^{-5}$	$5.4 \times 10^{-5} \pm 7 \times 10^{-6}$	7.27×10^{-6}	1.41×10^{-5}	$S_m = 2.42 \pm 0.07$
J_{QM}	0.0701	0.0549	0.0671	0.0645	$S_{QM} = 2\sqrt{2}$
J_{corr}	8.53×10^{-3}	5.7×10^{-2}	1.03×10^{-2}	6.26×10^{-3}	$S_{corr} = 2.30$
η_{meas}	0.738 and 0.786	0.75	0.786 and 0.762	0.747 and 0.756	0.971 and 0.963
η_{eq}	0.745	0.710	0.719	0.715	Not applicable
η_{thr}	0.667	0.667	0.667 (?)	0.725	0.828
J_{corr}/J_m	1.6	106	1422	444	0.95
q_{QM}	0.785	0.787	0.783	0.776	0.769
q_m	$\frac{1}{2} + 2.1 \times 10^{-2}$	$\frac{1}{2} + 8 \times 10^{-3}$	$\frac{1}{2} + 7.6 \times 10^{-3}$	$\frac{1}{2} + 1.6 \times 10^{-2}$	0.659
q_{set}	1	1	$\frac{1}{2} + 1.2 \times 10^{-4}$	$\frac{1}{2} + 10^{-4}$	$\frac{1}{2} + 10^{-5}$
p Value	Not computed	1.16×10^{-10} [32]	3.74×10^{-31}	5.9×10^{-9}	0.039
Coincidence rate (min)	$232\,s^{-1}$	$1.7\,s^{-1}$	$9.6\,s^{-1}$	$0.059\,s^{-1}$	$\approx 2 \times 10^{-5}\,s^{-1}$
Coincidence rate (max)	$3970\,s^{-1}$	$31\,s^{-1}$	$162\,s^{-1}$	$3.60\,s^{-1}$	$\approx 1.3 \times 10^{-4}\,s^{-1}$

Para cerrar el *detection loophole*: $\eta_{eq} > \eta_{thr}$

Espacio de las teorías para describir la Naturaleza



Los experimentos recientes (*loophole-free*) han demostrado más allá de las dudas basadas en deficiencias instrumentales, que o bien la "Localidad" o bien el "Realismo" (o ambos) no son válidos en la Naturaleza.

En realidad hay una tercera hipótesis involucrada, que fue mencionada desde el principio pero olvidada casi por completo.

Redescubierta periódicamente, ha recibido diversos nombres a lo largo del tiempo: *ergodicity*, *homogeneous dynamics*, *uniform complexity*, *counterfactual stability*, etc.

No es necesaria para *deducir* las desigualdades de Bell, pero sí para poder *usarlas* en un experimento.

Veamos rápidamente por qué es necesaria, así como los significados precisos de “Localidad” y “Realismo”.

Ann. Inst. Henri Poincaré, Section A :
Vol. XXIX, n° 4, 1978, p. 379-394. *Physique théorique.*

A limitation on Bell's Inequality

by

V. BUONOMANO
Instituto de Matematica Universidade Estadual de Campinas,
Campinas, Sao Paulo, Brasil

ABSTRACT. — It is shown that Bell's Inequality does not characterize all local hidden variable explanations of the polarization correlation experiments. If one considers theories in which a single polarization measurement is not independent of previous particle-polarizer interactions then it is possible to manufacture local hidden variable theories which agree with quantum mechanics for any of the experiments performed to date.

A relevant property here is ergodicity, and we can say that Bell's Inequality characterizes all ergodic local hidden variable theories (i. e. all local theories that give the same time and ensemble average) but not all non-ergodic local hidden variable theories. It is further shown that the most physically reasonable class of non-ergodic local hidden variable theories must also satisfy Bell's Inequality.

It might be concluded from this article that if one insists on believing in both local hidden variable theories and the polarization correlation experiments supporting quantum mechanics then one must also believe in the existence of a field, medium or ether that permeates space and has relatively stable states (memory).

I. INTRODUCTION

A. In 1964 J. S. Bell [*1*], building on some work of Einstein, Podolsky and Rosen [*2*] and Bohm and Aharonov [*3*], proposed to show that any local hidden variable theory must necessarily be inconsistent with the quantum mechanical predictions for certain types of experiments that measure the polarization correlations of two separated particles which are originally together in some state. Several experiments [*4-8*] have since been

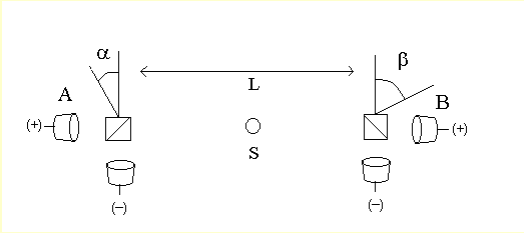
Deducción cortita de la desigualdad de Clauser y Horne:

Supongo que la probabilidad de observar (p.ej.) una detección en A es de la forma:

$$\mathbf{P^{+}_{A}(\alpha) = \int d\lambda.\rho(\lambda).\ P^{+}_{A}(\alpha,\lambda)}$$

(y lo mismo B, β, etc.). Supongo que $\rho(\lambda)$, $P_A(\alpha,\lambda) \in [0,1]$, que $\int d\lambda.\rho(\lambda) = 1$ y que las integrales son "bien comportadas" (= Riemann o Lebesgue) = **Realismo**.
La probabilidad de una coincidencia es entonces:

$$P^{++}_{AB}(\alpha,\beta) = \int d\lambda.\rho(\lambda).\ P^{++}_{AB}(\alpha,\beta,\lambda)$$



Donde supongo no contextualidad **(Localidad 1)**, es decir, es $\rho(\lambda)$, NO $\rho(\lambda,\alpha,\beta)$.

Uso que si: $x,y \geq 0;\ X \geq x';\ Y \geq y'$ entonces: $\mathbf{-1 \leq xy + x'y + x'y' - xy' - Yx' - Xy \leq 0}$
Llamo:

$X = Y = 1;$ $\quad x = P^{+}_{A}(\alpha,\lambda);$ $\quad x' = P^{+}_{A}(\alpha',\lambda)$
$\quad y = P^{+}_{B}(\beta,\lambda);$ $\quad y' = P^{+}_{B}(\beta',\lambda)$

(dejo de escribir los superíndices "+")

$$-1 \leq P_A(\alpha,\lambda)\times P_B(\beta,\lambda) + P_A(\alpha',\lambda)\times P_B(\beta,\lambda)\ P_A(\alpha',\lambda)\times P_B(\beta',\lambda)$$

$$- P_A(\alpha,\lambda)\times P_B(\beta',\lambda) - P_A(\alpha',\lambda) - P_B(\beta,\lambda) \leq 0$$

Ahora supongo **Localidad 2** (independencia estadística):

$$\mathbf{P_{AB}(\alpha,\beta,\lambda) = P_A(\alpha,\lambda)\times P_B(\beta,\lambda)}$$

Y tengo:

$$-1 \leq P_{AB}(\alpha,\beta,\lambda) + P_{AB}(\alpha',\beta,\lambda) + P_{AB}(\alpha',\beta',\lambda)$$

$$- P_{AB}(\alpha,\beta',\lambda) - P_A(\alpha',\lambda) - P_B(\beta,\lambda) \leq 0$$

Multiplico por $\rho(\lambda)$, **integro** y obtengo (desigualdad C-H):

$$-1 \leq P_{AB}(\alpha,\beta) - P_{AB}(\alpha,\beta') + P_{AB}(\alpha',\beta) + P_{AB}(\alpha',\beta') - P_A(\alpha') - P_B(\beta) \leq 0$$

Que quiero ver si se cumple o no *en los experimentos*.

Recordar que (p.ej.):

$$\mathbf{P_{AB}(\alpha,\beta) = \int d\lambda.\rho(\lambda).P_{AB}(\alpha,\beta,\lambda)}$$ *(ensemble average)*

Pero que yo siempre mido *en el tiempo*:

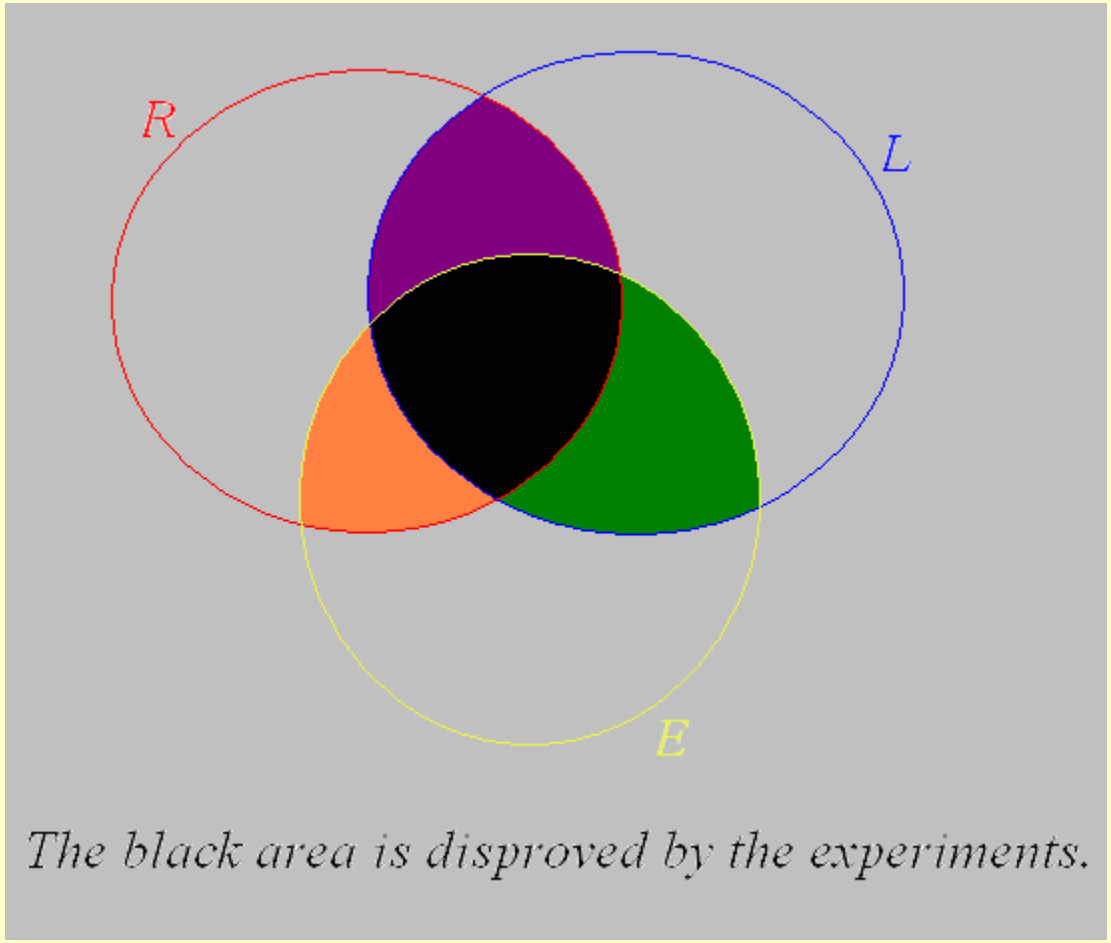
$$\mathbf{P_{AB}(\alpha,\beta) = (1/T) \int dt.\rho(t).P_{AB}(\alpha,\beta,t)}$$ *(time average)*

La igualdad entre las dos integrales es la hipótesis ergódica

Vale la pena aclarar que *ergodicidad* se refiere aquí a las propiedades del "mundo posible" implícito en la hipótesis de *counterfactual definiteness*, (que a su vez ya está incluída en "Realismo").

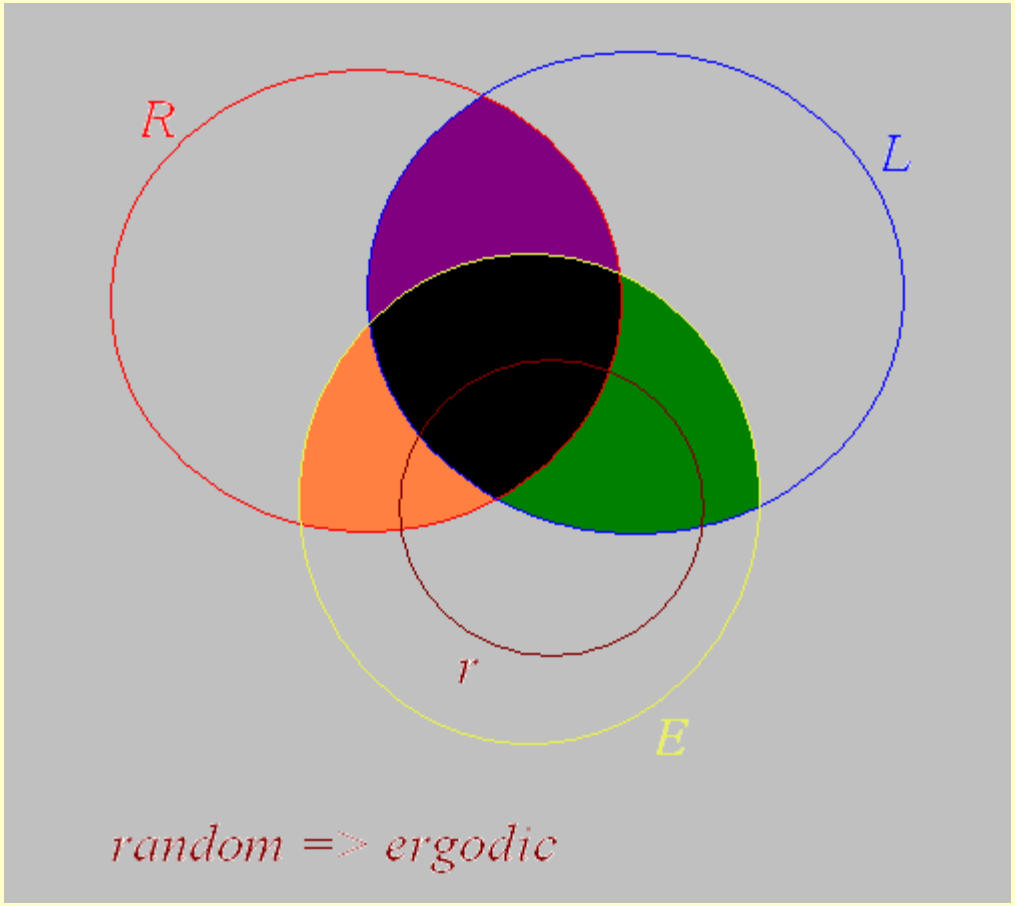
Es decir: aunque al suponer "Realismo" ya supuse que el mundo no-observado existe y está bien definido, todavía me falta definir *cómo* es ese mundo. Si supongo que en ese mundo no-observado vale *ergodicidad*, entonces recupero las desigualdades de Bell usuales. Si supongo otra cosa, las desigualdades toman *otras* formas, que a veces ni siquiera son violadas por QM.

Entropy 2017,19,80

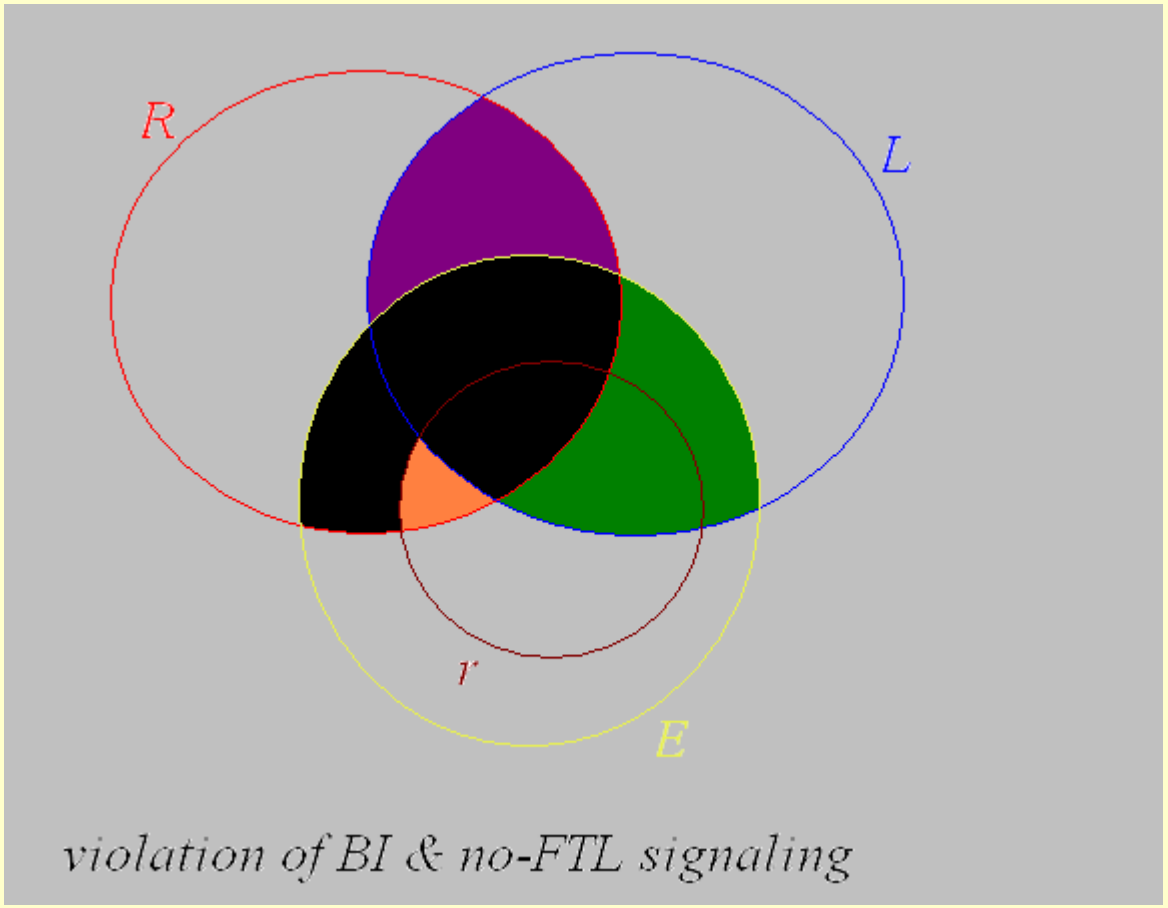


En lo que sigue voy a analizar los tres casos que surgen de suponer que *una* (no más de una) de las hipótesis involucradas es falsa, y las consecuencias para la aleatoriedad de series de observaciones.

random (bounded) ⇒ ergodic



Que un proceso aleatorio es ergódico es intuitivo, pero puede formalizarse (la manera precisa depende de cómo se defina “random”).



Un modelo “no Local” y “no aleatorio” permitiría enviar mensajes a velocidad instantánea (Popescu & Rohrlich) y debe ser descartado, ampliando el conjunto de modelos refutados.

Quedan así: modelos

“No realistas” (Copenhagen: random o no)

“No Locales” (⇒ Quantum certified randomness!)

“No ergódicos” (⇒ no random!)

Pero…¿no era que los resultados de mediciones cuánticas (hechas sobre una base de la que el estado observado no es autoestado) son aleatorios?
Las razones por las que esto se cree cierto:

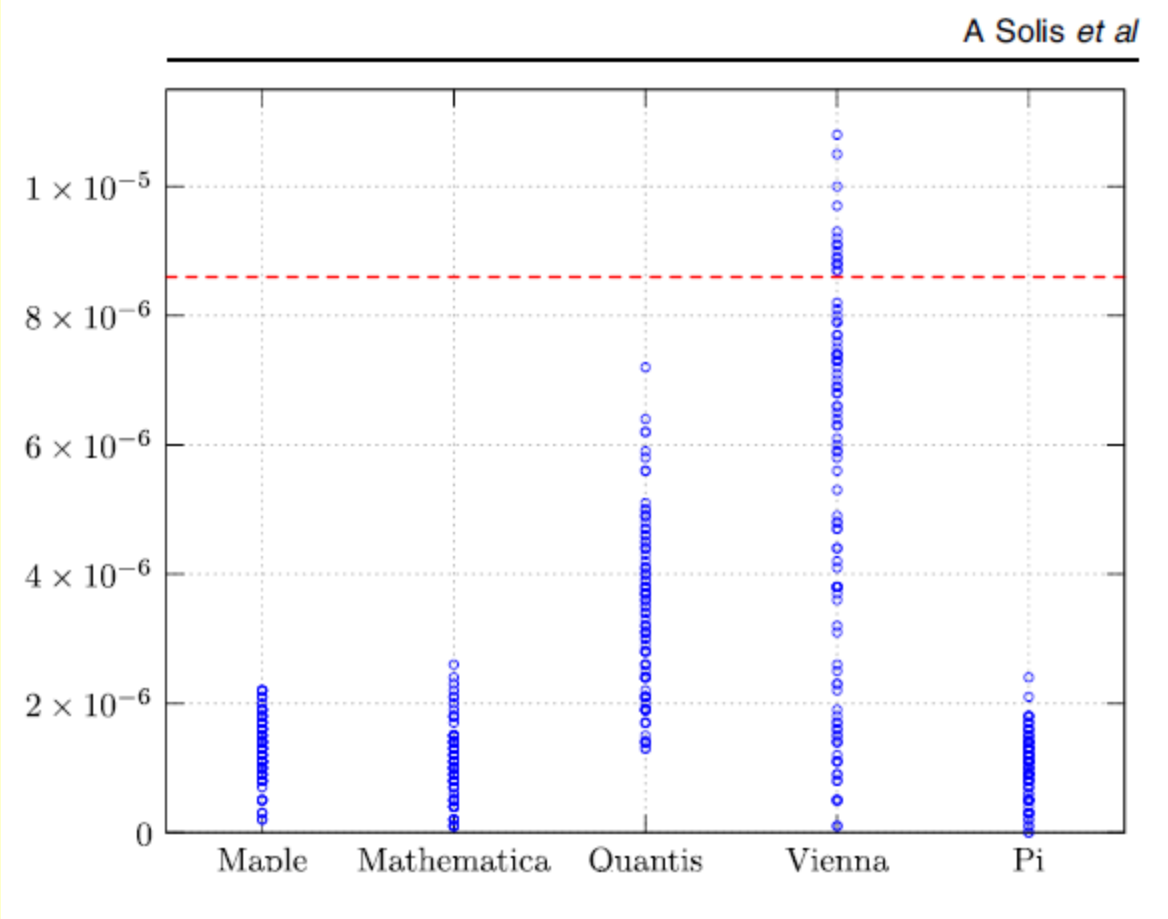
•Axioma de Von Neumann: *los resultados de mediciones en QM violan el principio de "razón suficiente" de Leibniz (formas* fuerte *y* débil*).*

• Resultado de Calude &Svozil (2008): *suponiendo la validez de la no-Localidad cuántica (y no-signaling), las secuencias de mediciones cuánticas deben ser "Turing non-computable".*

El dato importante es que, sometidas a tests estándar, las series de números generadas por mediciones cuánticas distan mucho de ser aleatorias en la práctica.

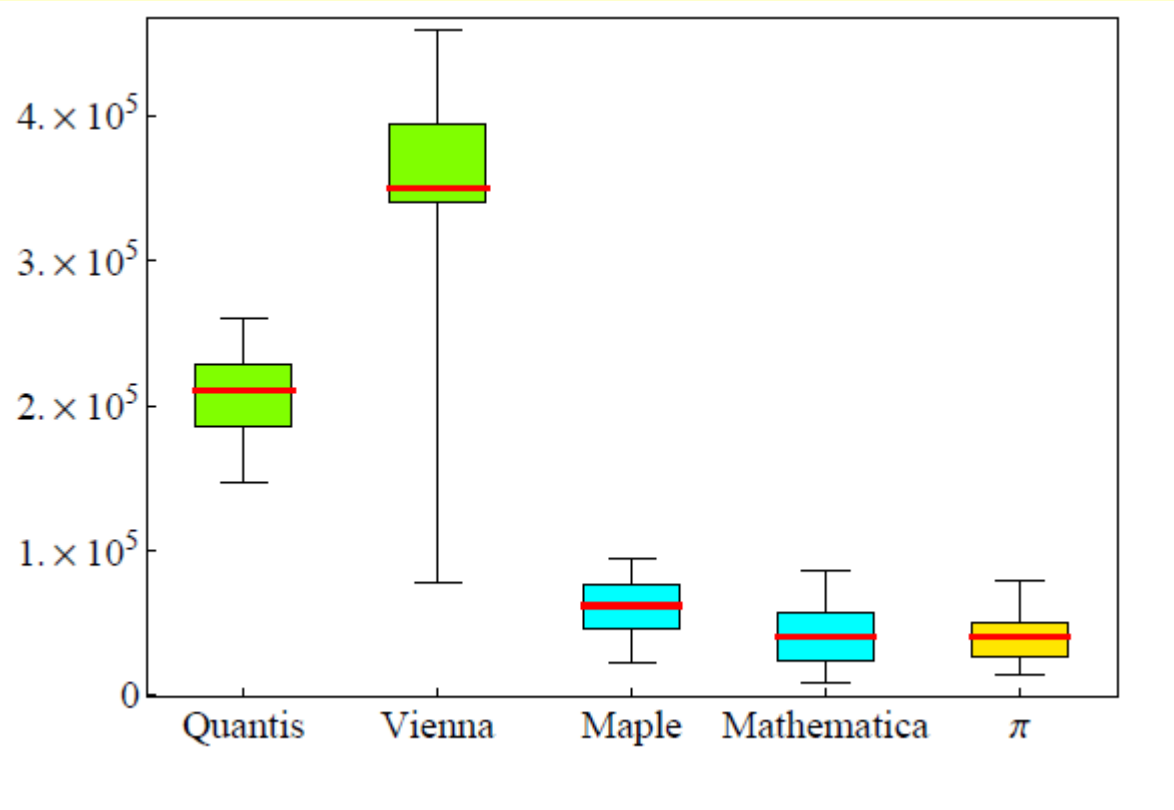
Se suele suponer que es por *deficiencias instrumentales*.
(*loopholes* otra vez, pero usados al revés)

Algunos ejemplos:



La línea roja representa la máxima desviación admisible de la condición de normalidad de Borel. Los círculos azules representan el valor absoluto de la desviación. Algunas secuencias producidas por RNG cuánticos no son siquiera “normales de Borel”.

From: Solis *et al.*, Phys. Scr. 90 (2015) 074034.



$$\left| \frac{N_j^m(x)}{|x|_m} - 2^{-m} \right| \leq \sqrt{\frac{\log_2 |x|}{|x|}},$$

Calude *et al.* 2010, otro test de normalidad de Borel. **Los RNG cuánticos tienen un desempeño peor que las series generadas por subrutinas incluidas en programas de uso corriente.**

El caso de QKD

En QKD, se genera dos series de números aleatorios idénticas en lugares distantes usando un estado entrelazado de fotones. Las series después se usan para codificar el mensaje.

- La "forma fuerte" del axioma de von Neumann garantiza que las series son aleatorias $\Rightarrow$ el mensaje no puede ser espiado (cifrado de Vernam).
- La Pureza del entrelazamiento pone un límite inferior a la entropía de las secuencias generadas (Pironio *et al.*, 2010) (pero sólo si la secuencia es *estacionaria* y vale no-localidad cuántica).
- Algunos experimentos "loophole-free" afirman haber generado secuencias "quantum certified" (Bierhorst *et al.*, 2018; Shen *et al.*, 2018). Estos experimentos usan estados de Eberhardt, que producen secuencias fuertemente desbalanceadas.

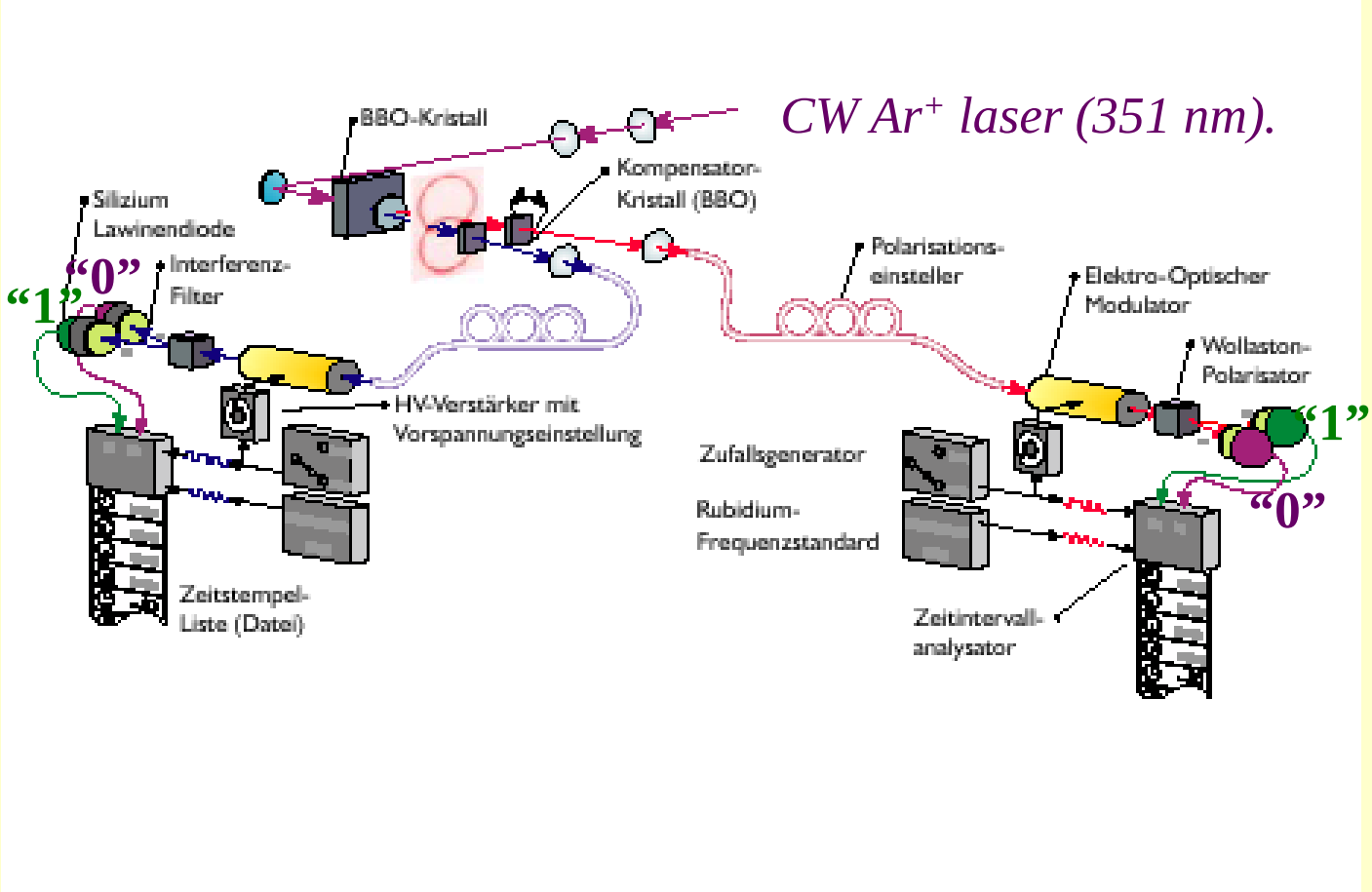
¿Y qué pasa con la aleatoriedad algorítmica?

(la forma más fuerte de aleatoriedad)

No hay datos disponibles de setups QKD, pero podemos usar experimentos parecidos.

El experimento de Innsbruck (Weihs *et al*. 1998).

No fue *loophole-free*, pero usó estados de Bell (= generó secuencias estadísticamente balanceadas) y hay muchos datos disponibles.



Basados en los resultados de Solis *et al*. estudiamos primero las series generadas por los *tiempos* entre coincidencias (su aleatoriedad es mejor que la de *outcomes*).

Un resultado viejo (*Found.Phys.* **37** p.80-102, 2007):
¡una de las series generadas en este experimento es *predecible*!

La corrida *longtime* (6 min de tiempo real, 95.797 puntos) tiene un objeto de baja dimensión en el espacio de fase (obtenido usando el teorema de reconstrucción de Takens, TISEAN software). Es posible predecir los bits "futuros" en la secuencia (hasta un promedio de ≈20 bits).

Esto implica una vulnerabilidad QKD de un tipo diferente (la correlación puede ser perfecta, pero…)

Se supone que la causa fue una variación (suave) de la frecuencia de los relojes de Alice y Bob.

El resultado es concluyente, pero el teorema de Takens puede aplicarse de manera confiable a sólo algunos casos (o corridas).

Una estimación de la complejidad de Kolmogorov *K(N)* provee una evaluación de "aleatoriedad" que es menos restrictiva (= más útil).

Extraemos series de tiempos entre coincidencias para casi todas las series disponibles en el experimento de Innsbruck's (con S>2) y calculamos *K(N)* con la realización del algoritmo de Lempel&Ziv desarrollada por Mihalovic *et al*.

Esto da una *estimación* de la complejidad de Kolmogorov normalizada:

$$K(N) \equiv c(N) \times \log_2(N)/N$$

Donde c(*N*) es el complexity counter, definido como el mínimo número de palabras distintas en la secuencia (la base para esta normalización es que si $N \to \infty$, $c(N) \to N/\log_2(N)$ en una serie aleatoria ideal).

Filename (description)	Complexity	NIST (RND=?)	S_{CHSH}	N
Longtime (remote, switched)	0.55	NO	2.51	95801
Longtime, subset {0,3}	0.65	NO	Not applicable	2122
Longdist0 (remote, switched)	0.97	yes	2.53	15501
Longdist0, singles	0.96	NO	Not applicable	471017
Longdist1	11.94	yes	2.63	16168
Longdist2	11.21	yes	1.98	26675
Longdist3	11.25	yes	2.67	24335
Longdist4	11.24	yes	2.66	25402
Longdist10	10.88	NO	2.20	26529
Longdist11	10.82	yes	2.41	25573
Longdist12	0.93	NO	2.37	27158
Longdist12, singles	0.97	yes	Not applicable	934979
Longdist13	10.84	yes	2.36	27160
Longdist20	10.37	yes	2.06	41549
Longdist22	0.59	NO	2.16	39915
Longdist22, singles	0.96	yes	Not applicable	1237058
Longdist23	10.37	yes	2.63	41058
Longdist30	12.24	yes	2.10	14145
Longdist31	0.97	yes	2.62	13022
Longdist32	12.24	yes	2.70	10992
Longdist33	12.18	yes	2.06	13004
Longdist34	12.26	yes	1.87	14289
→ **Longdist35**	0.34	NO *	2.73	14562
Longdist35, singles	0.96	yes	Not applicable	388455
Longdist36	11.0	yes	2.72	14573
Longdist36, singles	0.96	yes	Not applicable	388573
Longdist37	12.16	yes	2.05	14661
Loccorr1 (local, switched)	0.96	yes	2.74	72533
Loccorr3	0.96	yes	2.74	73269
Loccorr3, singles	0.96	yes	Not applicable	853985
Bluesin1 (local, static), $\alpha = 0^\circ$, $\beta = 7.5^\circ$	0.98	yes	Not applicable	6797
Bluesin2, $\alpha = 0^\circ$, $\beta = 15^\circ$	0.97	yes	Not applicable	6815
Bluesin3, $\alpha = 0^\circ$, $\beta = 22.5^\circ$	0.97	yes	Not applicable	6822
Bluesin4, $\alpha = 0^\circ$, $\beta = 30^\circ$	0.96	yes	Not applicable	6824
Bluesin5, $\alpha = 0^\circ$, $\beta = 37.5^\circ$	0.97	yes	Not applicable	6784
SL1722 (local, static) $\alpha = 0^\circ$, $\beta = 22.5^\circ$	0.96	yes	Not applicable	56913
Conlt3 (local, static, uncorrelated)	7.29	yes	Not applicable	4950

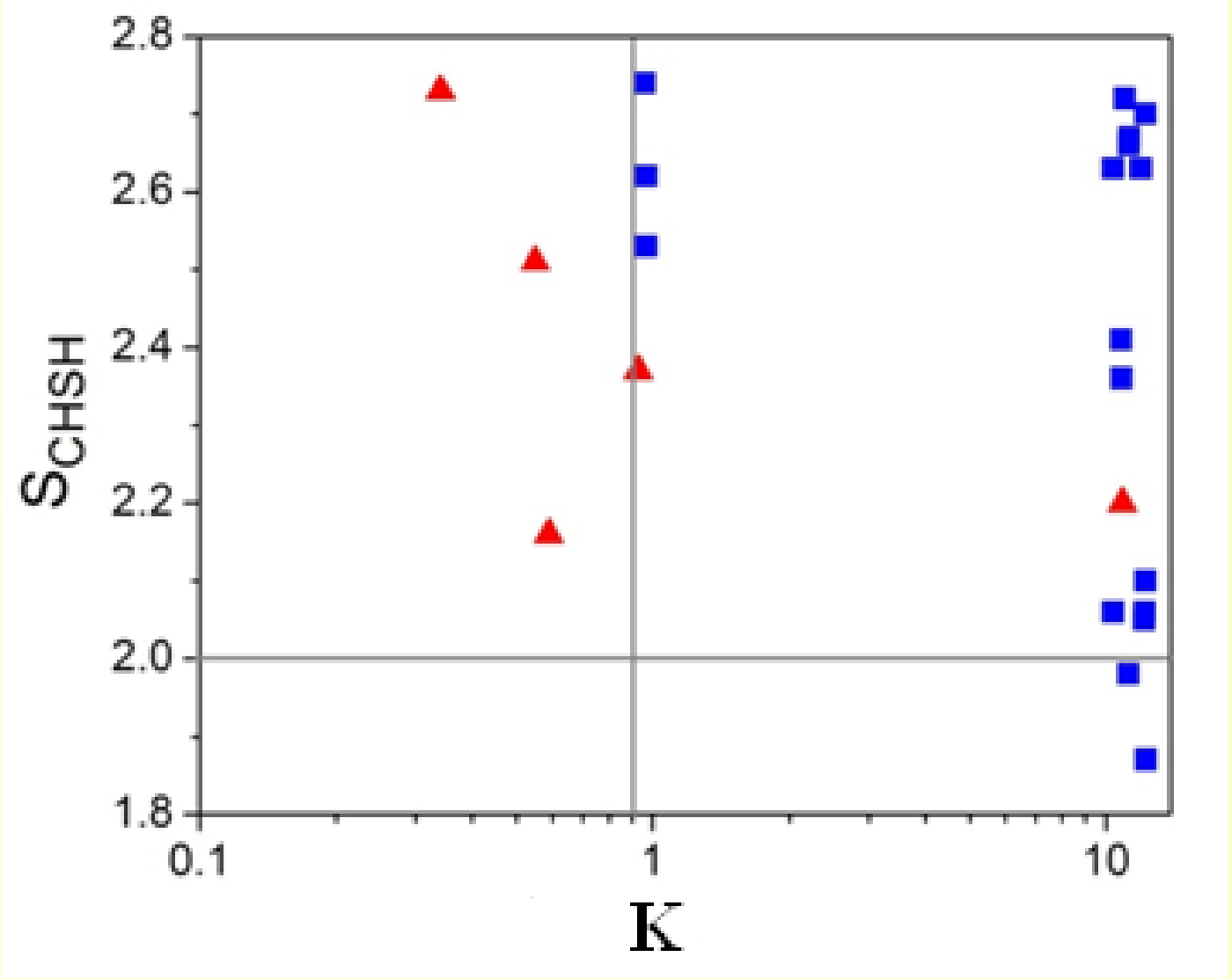


Gráfico resumen de los principales resultados en la tabla anterior. **Triángulos** (**cuadrados**) indican las corridas que **no pasan** (**pasan**) los tests del NIST. La línea horizontal indica el límite de Bell, la vertical es K=0.9 (límite arbitrario de complejidad algorítmica aceptable). *Parecería que a menor S, mayor K.*

Phys.Rev.A **98**, *042131 (2018).*

Teniendo en cuenta sólo las corridas “remote switched” (las que serían útiles para QKD), hay 5 entre 21 que *no* pueden ser consideradas random (≈25%)

Si nos restringimos a las 16 en las que la desigualdad de Bell es violada ampliamente, el porcentaje sube a **> 30%.**

(Incluyendo un caso en que la serie es **predecible**!)

Y esto es para el experimento de Innsbruck, que fue realizado en condiciones mucho mejor controladas que lo previsible para un dispositivo QKD operando en el mundo real.

La conclusión práctica importante es que no es seguro considerar que la aleatoriedad de series generadas en QKD está garantizada, aún si la desigualdad de Bell de control se viola por un amplio margen.

Se objetó que el estudio involucraba series de tiempos, y no de resultados (outcomes)

Usando outcomes…(da lo mismo, o peor)

Series of outcomes.	Complexity	NIST (RND=?)	S_{CHSH}	*N*
Longdist0, Alice, setting = 0	1.017	NO	2.53	9676
Longdist0, Alice, setting = 1	1.030	NO	2.53	10302
Longdist0, Bob, setting = 0	1.023	NO	2.53	9893
Longdist0, Bob, setting=1	1.023	NO	2.53	10085
Longdist1, Alice, setting = 0	1.025	NO	2.63	10848
Longdist1, Alice, setting = 1	1.027	yes (no)	2.63	9859
Longdist1, Bob, setting = 0	1.018	NO	2.63	10043
Longdist1, Bob, setting = 1	1.016	yes	2.63	10664
Longdist35, Alice, setting = 0	1.032	yes	2.73	8638
Longdist35, Alice, setting = 1	1.016	NO	2.73	6365
Longdist35, Bob, setting =0	1.033	yes (no)	2.73	7741
Longdist35, Bob, setting = 1	1.023	yes (no)	2.73	7262
Longdist35, all Alice outcomes	1.021	NO	2.73	15003
Longdist35, all Bob outcomes	1.026	yes	2.73	15003
Bierhorst *et al.*	1.044	yes	$J = 1.41 \times 10^{-5}$	1024

$K \approx 1$, $K >> 1$, $K < 1$, loophole-free.

Sólo **7 de las 15** series pueden ser consideradas estadísticamente aleatorias. La proporción de no-random (≈½) es mayor que para las series de tiempos (≈¼), resultado consistente con Solis *et al.* Si se aplica toda la batería de tests del NIST, sólo **4** series sobreviven (una de ellas es la loophole-free).

arxiv.org/1812.05926

Si para tener series verdaderamente aleatorias es imprescindible alcanzar la condición de loophole-free, entonces la idea de "quantum certification" (y también de QKD!) está muy lejos de ser practicable.

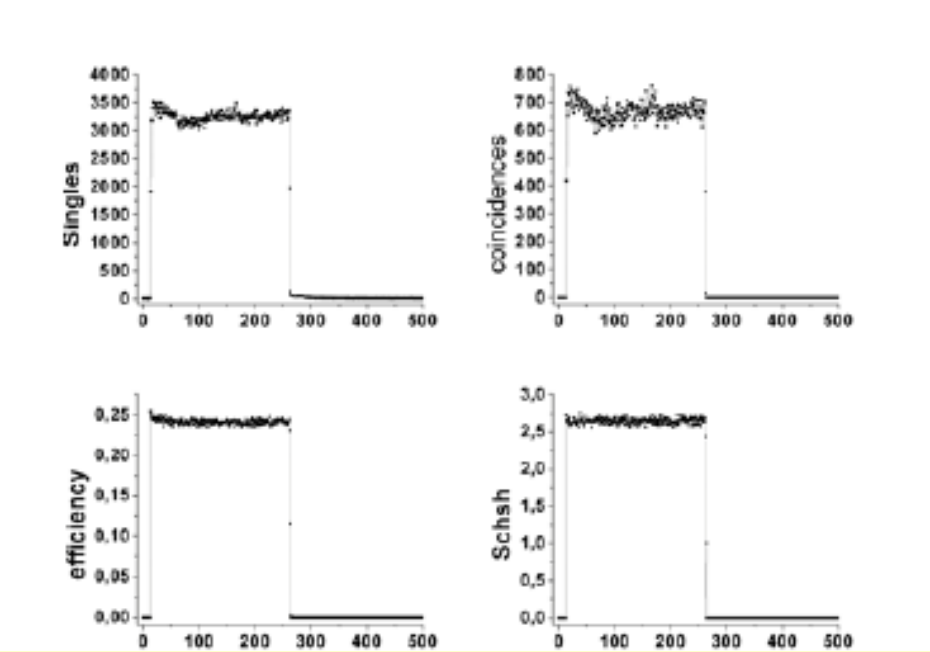
Una manera de explorar la factibilidad de estas ideas es tratar de "medir" la aleatoriedad de series generadas con estados de diferente entrelazamiento, para ver cuál es la tendencia.

Generamos series con S=1.41 (el valor del modelo semiclásico de radiación), S=2.04 (en el límite de Bell) y S=2.67 (fácilmente reproducible en un dispositivo de uso práctico), y les pasamos todos los tests de aleatoriedad que encontramos:

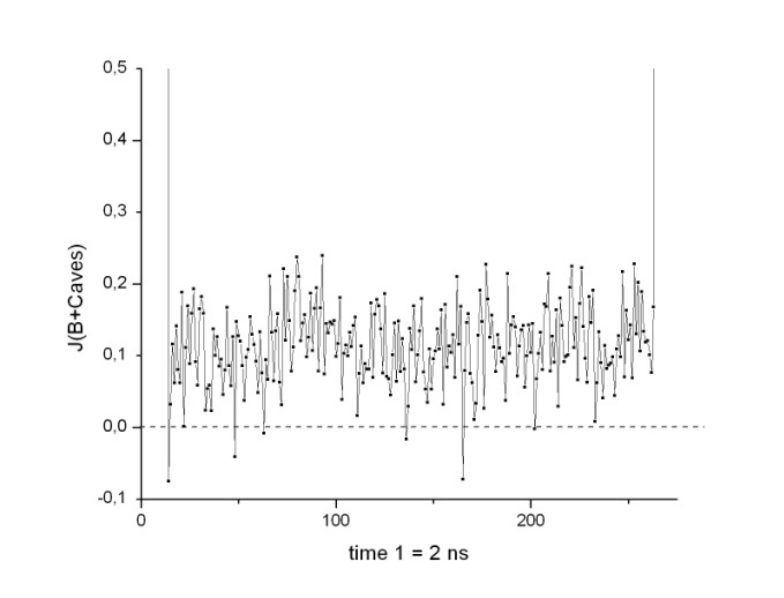
- Toda la batería del NIST.
- Complejidad de Kolmogorov.
- Test de estacionariedad: KPSS y ADF.
- Exponente de Hurst.

El dispositivo es pulsado (pulsos cuadrados de 500 ns a 50 KHz), lo que se parece a la situación de “tirar una moneda”. Sólo uno de cada 17 pulsos produce un fotón (single) detectado; prácticamente no hay “dos monedas por tiro”.

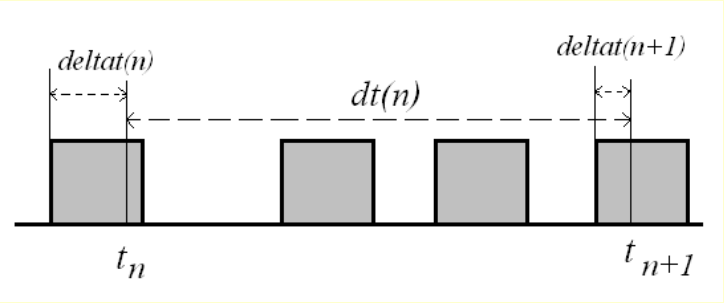
Esto permite generar varios tipos de series y también calcular (estroboscópicamente) la variación del entrelazamiento en el tiempo:



CHSH y η



Desigualdad informática
(Braunstein & Caves)



File type	*Kc*	*Km*	H
#1,θ=22.5°	0.947 ± 0.004	1.020 ± 0.004	0.497 ± 0.016
#2,θ=22.5°	1.022 ± 0.010	1.019 ± 0.004	0.493 ± 0.013
#1, θ=8.6°	0.966 ± 0.007	1.022 ± 0.008	0.493 ± 0.020
#2, θ=8.6°	1.020 ± 0.007	1.021 ± 0.007	0.491 ± 0.016
#3, θ=8.6°	1.015 ± 0.001	*not applicable*	0.505 ± 0.009

Table 1: Average values (over all files of the same type) and dispersion of Kolmogorov complexities and Hurst exponent, for files recorded with entangled state, S=2.67.

File type	*Kc*	*Km*	H
#1,θ=22.5°	0.965 ± 0.005	1.031 ± 0.025	0.501 ± 0.011
#2,θ=22.5°	1.019 ± 0.004	1.023 ± 0.015	0.498 ± 0.009
#1, θ=8.6°	0.965 ± 0.008	1.024 ± 0.013	0.504 ± 0.021
#2, θ=8.6°	1.020 ± 0.006	1.021 ± 0.007	0.499 ± 0.010
#3, θ=8.6°	1.019 ± 0.010	*not applicable*	0.503 ± 0.011

Table 2: Average values and dispersion of Kolmogorov complexities and Hurst exponent, for files recorded with marginally entangled state, S=2.06.

File type	*Kc*	*Km*	H
#1,θ=22.5°	0.962 ± 0.002	1.016 ± 0.003	0.496 ± 0.013
#2,θ=22.5°	1.016 ± 0.003	1.017 ± 0.004	0.497 ± 0.012
#1, θ=8.6°	0.964 ± 0.009	1.018 ± 0.010	0.496 ± 0.022
#2, θ=8.6°	1.017 ± 0.007	1.016 ± 0.008	0.496 ± 0.012
#3, θ=8.6°	0.972 ± 0.086	*not applicable*	0.501 ± 0.008

Table 3: Average values and dispersion of Kolmogorov complexities and Hurst exponent, for files recorded with no entangled state, S=1.42.

La aleatoriedad se “mide” por la proporción de series de coincidencias rechazadas (o no-aleatorias) usando varios indicadores bien establecidos. Dejando de lado las 24 series tipo #3 (que tienen algún problema sistemático, porque todas son rechazadas por el NIST), 8 de 64 series para S=2.67 son no-aleatorias, 14 de 64 para S=2.12, y 0 de 64 para S=1.42.

arXiv.org/abs/1908.10794

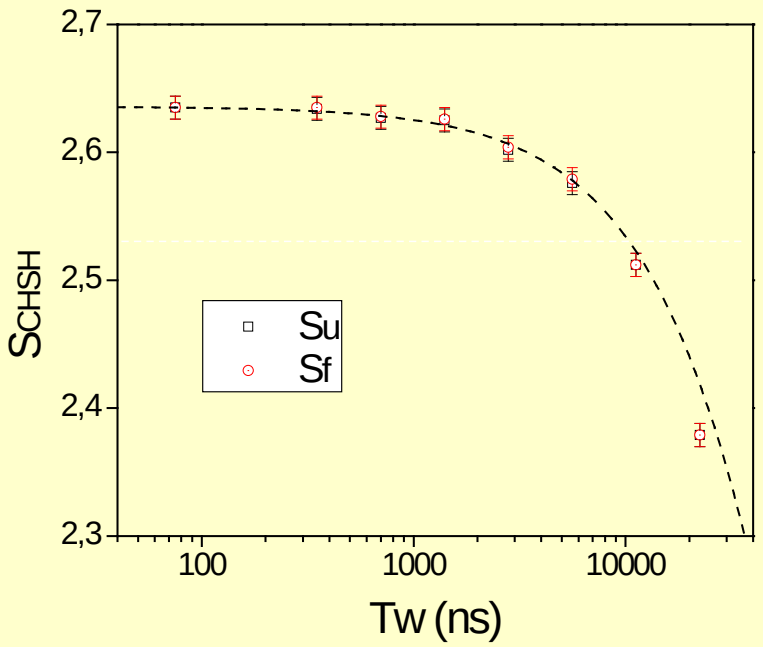
Las series generadas con el menor entrelazamiento son las “más aleatorias”. Esto es una buena noticia por un lado, porque son más fáciles de generar.

Por otro lado, un buen entrelazamiento es esencial para QKD.

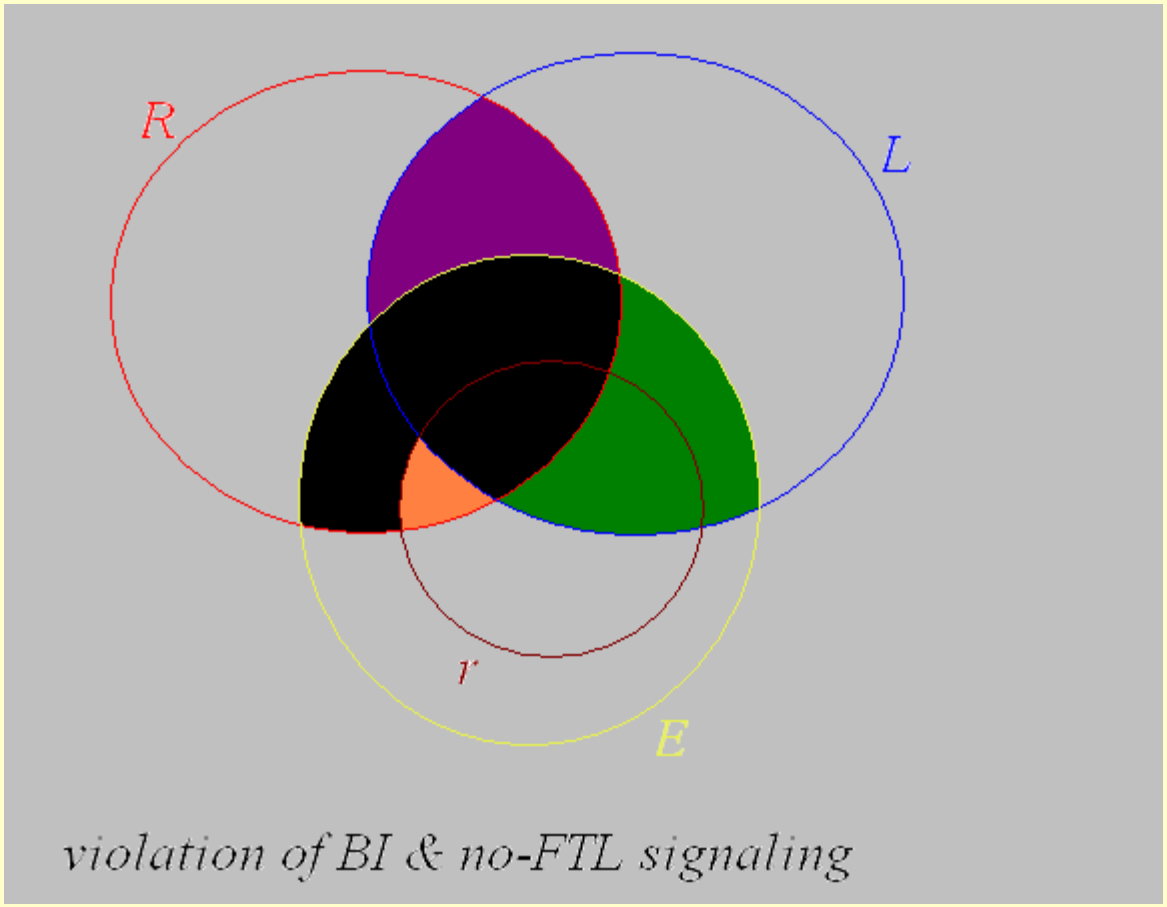
Pero en toda esta discusión ha quedado afuera un elemento esencial: *Localidad*, o la distancia *L* entre las estaciones.

Tal vez sea ésa la causa del desempeño pobre de algunos RNG no-loophole free.

Sabemos de experimentos anteriores que *los fotones detectados fuera del pulso no están correlacionados*.
Así que podemos suponer que los comienzos de los pulsos (tiempos menores que *L/c*) están en una zona donde la condición de Localidad se cumple.
Phys.Rev.A **86**, 052121 (2012).



Recordemos el gráfico de las propiedades de los modelos posibles después de los experimentos loophole-free:

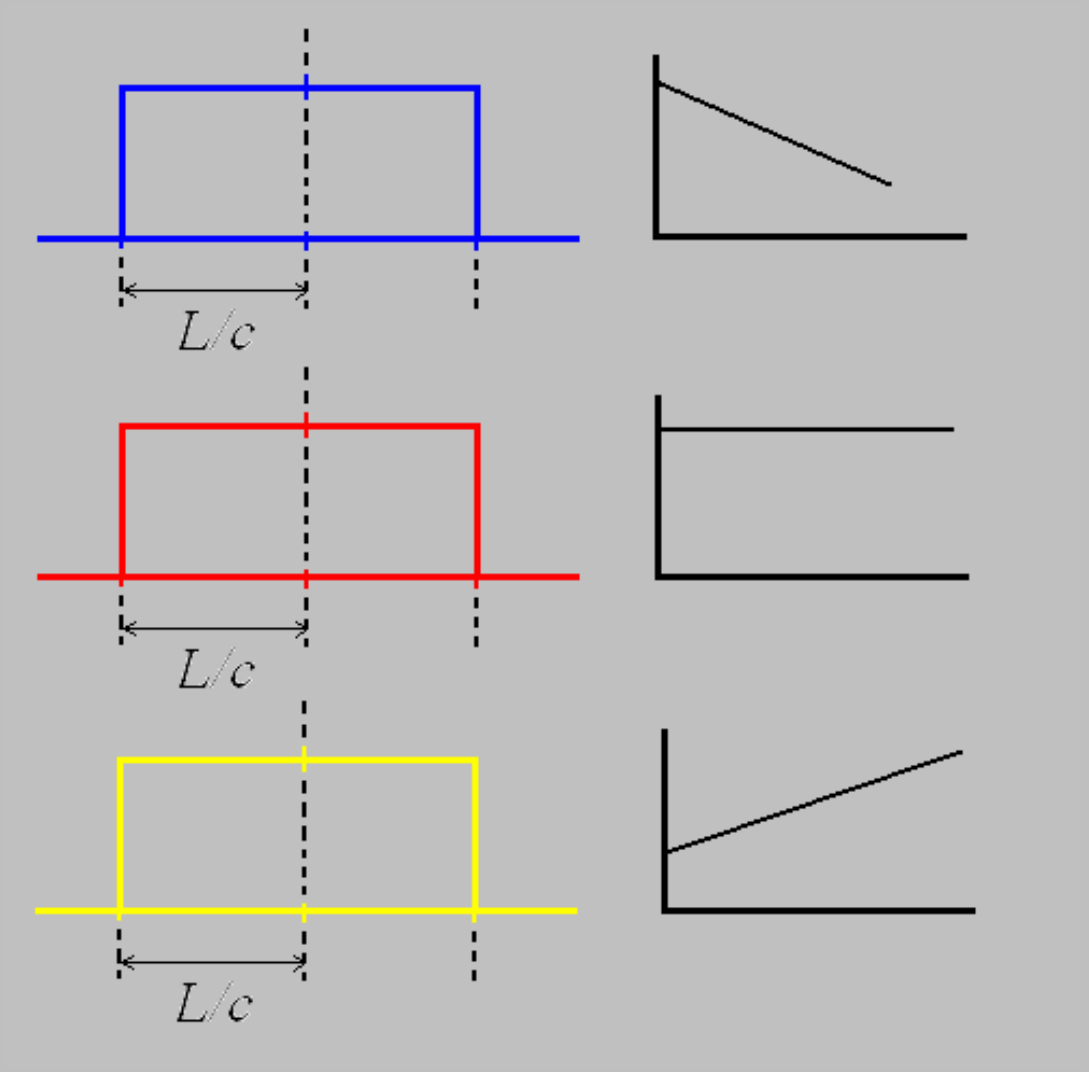


"No realistas" (Copenhagen: random o no)

"No Locales" (⇒ Quantum certified randomness!)

"No ergódicos" (⇒ no random!)

¿Qué mediría un “randómetro” en cada caso?



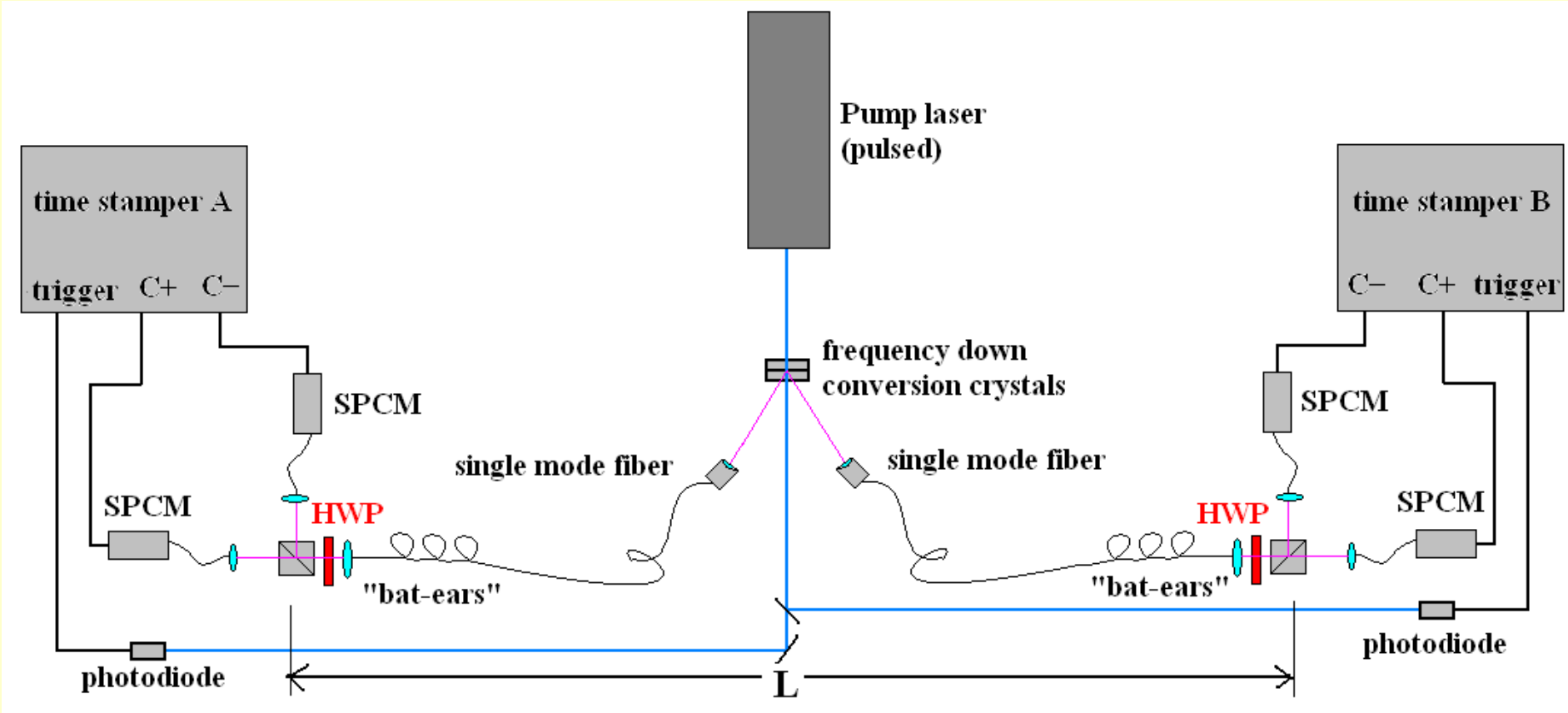
No se cumple Localidad
(Q. certified)

No se cumple Realismo
(Copenhagen)

No se cumple Ergodicidad
(no ergódico ⇒ no random)

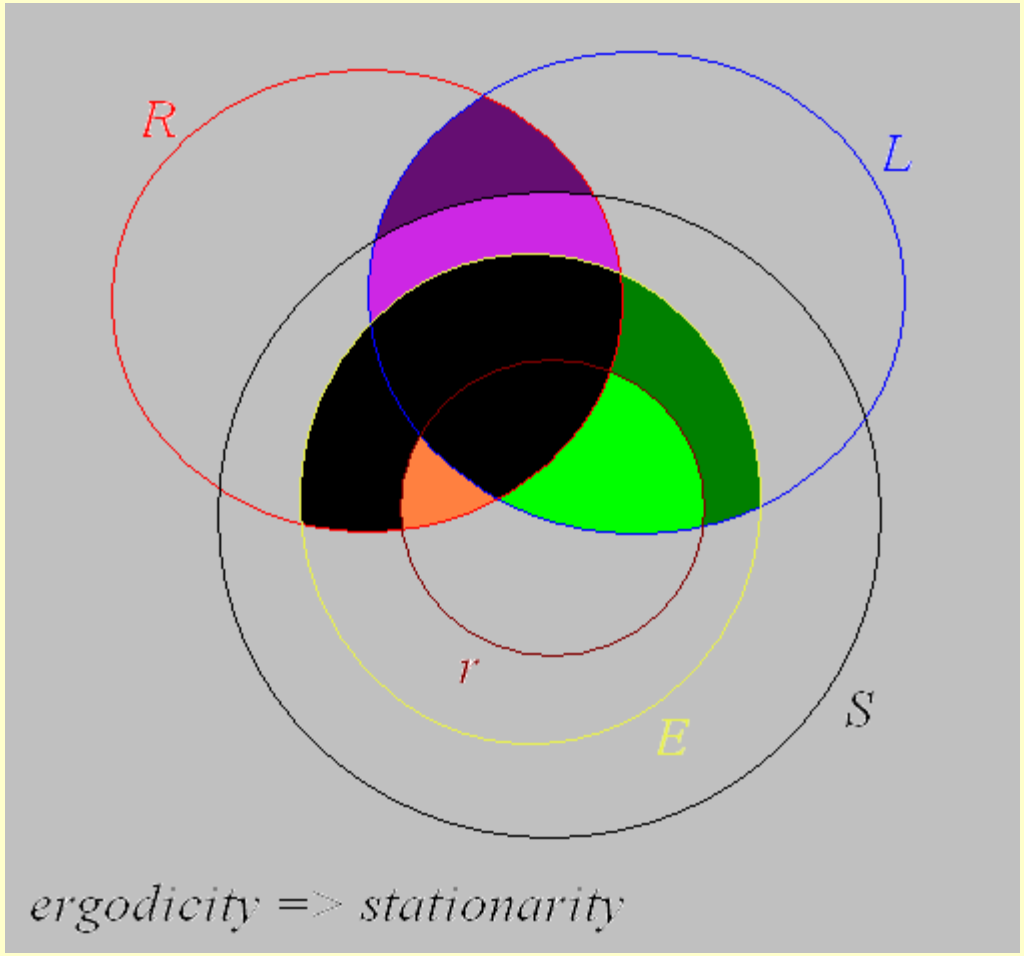
Lástima que los randómetros no existen…

(pero podemos contar la *proporción* de series no-random)



En un experimento como éste, variando *L* (y por lo tanto la parte del pulso que queda en la zona “Local”) es tal vez posible encontrar indicios de cuál de las tres hipótesis (Localidad, Realismo o Ergodicidad) es la que no se cumple en la violación de las desigualdades de Bell.

Finalmente, hay otra propiedad (estacionariedad) que puede ayudar:



Augmented Dickey-Fuller **(ADF)** y Kwiatkowski–Phillips–Schmidt–Shin **(KPSS)** son tests estándar de estacionariedad.

Volvemos a los datos del experimento de Innsbruck.

(que no me sorprendería que fuera no-estacionario)

En todas las series, ADF indica que se puede descartar *unit-root*.

KPSS = 0 indica que no se puede descartar *estacionariedad*.

Así, 6 de las 12 series "time" son en principio no estacionarias, *aunque todas las series de singles son estacionarias.*

En las series de "outcomes", 5 de 18 son no estacionarias.

Filename (description)	KPSS	K	Hurst	S_{CHSH} / C (est.)	*N*
Longtime (time)	1	0.55	0.73	2.51 / 0.83	95801
Longdist0 (time)	1	0.97	0.68	2.53 / 0.84	19978
Longdist0 (time, singles Alice)	0	0.96	0.49	Not applicable	471017
Longdist12 (time)	1	0.93	0.70	2.37 / 0.76	27158
Longdist12 (time, singles Alice)	0	0.97	0.50	Not applicable	934979
Longdist22 (time)	1	0.59	0.87	2.16 / 0.65	39915
Longdist23 (time)	0	10.37	0.49	2.63 / 0.89	41058
Longdist31 (time)	0	0.97	0.51	2.62 / 0.89	13022
Longdist32 (time)	0	12.24	0.48	2.70 / 0.93	10992
Longdist35 (time)	0	0.34	0.50	2.73 / 0.95	15003
Longdist35 (time, singles Alice)	0	0.96	0.51	Not applicable	388455
Longdist36 (time)	1	11.0	0.62	2.72 / 0.94	14573
Bluesin1 (time, static), $\alpha = 0^o$, $\beta = 7.5^o$	0	0.98	0.46	Not applicable	6797
Bellstat0 (time, static), $\alpha = 0^o$, $\beta = 0^o$	1	**falta**	0.56	Not applicable	10528
Bellstat0 (outcomes, static), $\alpha = 0^o$, $\beta = 0^o$	0	**falta**	0.51	Not applicable	10528
Longdist0 (outcomes Alice, total)	1	**falta**	0.58	2.53 / 0.84	19978
Longdist0 (outcomes Alice, V=0)	0	1.02	0.54	2.53 / 0.84	9676
Longdist0 (outcomes Alice, V=1)	1	1.03	0.61	2.53 / 0.84	10302
Longdist0 (outcomes Bob, total)	0	**falta**	0.52	2.53 / 0.84	19978
Longdist0 (outcomes Bob, V=0)	0	1.02	0.50	2.53 / 0.84	9893
Longdist0 (outcomes Bob, V=1)	0	1.02	0.51	2.53 / 0.84	10085
Longdist1 (outcomes Alice, total)	1	**falta**	0.52	2.63 / 0.89	20707
Longdist1 (outcomes Alice, V=0)	0	1.03	0.50	2.63 / 0.89	9859
Longdist1 (outcomes Alice, V=1)	0	1.03	0.51	2.63 / 0.89	10848
Longdist1 (outcomes Bob, total)	0	**falta**	0.51	2.63 / 0.89	20707
Longdist1 (outcomes Bob, V=0)	0	1.02	0.52	2.63 / 0.89	10043
Longdist1 (outcomes Bob, V=1)	0	1.02	0.49	2.63 / 0.89	10664
Longdist35 (outcomes Alice, total)	0	1.02	0.49	2.73 / 0.95	15003
Longdist35(outcomes Alice, V=0)	0	1.03	0.48	2.73 / 0.95	8638
Longdist35 (outcomes Alice, V=1)	0	1.02	0.52	2.73 / 0.95	6365
Longdist35 (outcomes Bob, total)	1	1.03	0.53	2.73 / 0.95	15003
Longdist35 (outcomes Bob, V=0)	0	1.03	0.51	2.73 / 0.95	7741
Longdist35 (outcomes Bob, V=1)	0	1.02	0.52	2.73 / 0.95	7262

CONCLUSIONES

CONCLUSIONES

- Muchas de las series de resultados (ya sea “tiempos” o “outcomes”) generadas por dispositivos cuánticos *no pasan* los tests estándar de aleatoriedad, (entre ¼ y ½ son rechazadas, aún para mediciones hechas sobre estados con buen entrelazamientos).

CONCLUSIONES

• Muchas de las series de resultados (ya sea “tiempos” o “outcomes”) generadas por dispositivos cuánticos *no pasan* los tests estándar de aleatoriedad, (entre ¼ y ½ son rechazadas, aún para mediciones hechas sobre estados con buen entrelazamientos).

• Esto abre un interrogante sobre la viabilidad de QNRG y QKD en la práctica. Hace falta más mediciones.

CONCLUSIONES

• Muchas de las series de resultados (ya sea “tiempos” o “outcomes”) generadas por dispositivos cuánticos *no pasan* los tests estándar de aleatoriedad, (entre ¼ y ½ son rechazadas, aún para mediciones hechas sobre estados con buen entrelazamientos).

• Esto abre un interrogante sobre la viabilidad de QNRG y QKD en la práctica. Hace falta más mediciones.

•Las series de mejor aleatoriedad fueron generadas por fuentes no-entrelazadas.

CONCLUSIONES

• Muchas de las series de resultados (ya sea “tiempos” o “outcomes”) generadas por dispositivos cuánticos *no pasan* los tests estándar de aleatoriedad, (entre ¼ y ½ son rechazadas, aún para mediciones hechas sobre estados con buen entrelazamientos).

• Esto abre un interrogante sobre la viabilidad de QNRG y QKD en la práctica. Hace falta más mediciones.

•Las series de mejor aleatoriedad fueron generadas por fuentes no-entrelazadas.

• Determinar el grado de aleatoriedad de las series *generadas para distintos L y en diferentes momentos de un pulso* puede echar luz sobre interrogantes fundamentales (¿cuál de las tres hipótesis involucradas en las desigualdades de Bell es falsa?) y cuál es el régimen en que QKD podría usarse de manera segura (p.ej.: sólo si $T_{pulso} < L/c$).

FIN

Muchas gracias!