

# Aleatoriedad por Diseño

## William A. Dembski, Ph.D.

---

El matemático y filósofo William A. Dembski es profesor asociado de investigación de los fundamentos conceptuales de la ciencia en la Universidad de Baylor y miembro distinguido del Centro del Instituto Discovery para la Renovación de la Ciencia y la Cultura en Seattle. El Dr. Dembski fue previamente catedrático de la Northwestern University, la Universidad de Notre Dame y la Universidad de Dallas. Ha realizado trabajo post-doctoral en matemáticas en el MIT, en física en la Universidad de Chicago, y en ciencia computacional en la Universidad Princeton. Es graduado de la Universidad de Illinois en Chicago, donde obtuvo el grado de Licenciatura en Psicología, el grado de Maestría en Ciencias en Estadística y el Ph.D. en Filosofía, también recibió un doctorado en matemáticas de la Universidad de Chicago en 1988 y un grado de maestro en divinidad del Seminario Teológico de Princeton en 1996. Ha sostenido confraternidad de posgrado y post-doctorado de la Fundación Nacional de Ciencia. El Dr. Dembski ha publicado artículos en *journals* de matemáticas, filosofía y teología y es autor/editor de 7 libros. En *La Inferencia de Diseño: Eliminando al Azar a Través de Probabilidades Pequeñas* (Cambridge University Press, 1998), examina el argumento de diseño en un contexto post-Darwiniano y analiza las conexiones que enlazan el azar, la probabilidad y la causalidad inteligente. La secuela de *La Inferencia de Diseño* saldrá el próximo diciembre del 2001 con Rowman's and Littlefield's y critica la postura Darwiniana y otras posturas también evolucionistas. Se titula *No hay Comida Gratis: Porqué no puede Conseguirse una Complejidad Específica sin Inteligencia*.

### 1. Introducción

“Cualquiera que considere métodos aritméticos para producir dígitos aleatorios está, por supuesto, en estado de pecado”.<sup>1</sup> La famosa frase de John von Neumann lanza un dedo acusador a todos aquellos que dedican sus mentes ordenadas a engendrar desorden. Así como en tiempos pasados ladrones, alcahuetes y actores llevaban a cabo su profesión con un cargo de conciencia, así en estos tiempos los científicos que diseñan generadores de números aleatorios sufren ataques de culpa. George Masaglia, quizás el más preeminente trabajador en el campo, bromea cuando pregunta a sus colegas. “¿Quién de entre nosotros no ha pecado?” El trabajo de Marsaglia en el Instituto de Investigación en Supercomputadoras es bastante conocido. Por mucho que el trabajo de diseño y prueba de generadores de números aleatorios depende de la computación, y por mucho que la computación es fundamentalmente aritmética, Marsaglia es de acuerdo a la perspectiva personal de von Neumann un grosero pecador. Y trabajando de la forma en que lo hace en computación, Marsaglia de hecho es un gran pecador. El lo admite libremente. Escribiendo acerca de los mejores generadores de números aleatorios que conoce, Marsaglia dice, “son el resultado de métodos aritméticos y todos aquellos que los usan deben, como todos los pecadores,

enfrentar el día de Redención [*sic*]. Pero quizás con un mejor entendimiento podemos posponerlo”.<sup>2</sup>

A pesar del peligro de ser marcado como hereje, quiero argumentar que la aleatoriedad no exige ninguna deficiencia moral. Incluso abogaré por que los generadores de números aleatorios sean construidos con un abandono imprudente, aunque un abandono imprudente bien pensado. La aleatoriedad, para ser propiamente aleatoriedad, no debe dejar nada al azar. Debe parecer como azar, como hija del caos primitivo. Pero por debajo, una aguzada inteligencia debe manipular y calcular, tomando ventaja de este y aquel hecho conveniente de forma sistemática para causar confusión. Recuerdo a los foto-periodistas en Vietnam que reacomodaron escenas de carnicería simplemente para incrementar el sentimiento de violencia indiscriminada. Aquí, por supuesto, hubo una falta moral, pero no con aleatoriedad intrínseca. Vale decir, la aleatoriedad, para ser aleatoriedad, debe ser diseñada.

En su ahora clásico, aunque un poco anticuado estudio acerca de los números aleatorios Donald Knuth (1981, pp. 4-6) describe su ingenuo intento para construir un generador de números aleatorios a prueba de tontos. Su generador de números “super-aleatorio” (las vibrantes comillas son suyas) era una enredada red de subrutinas que construyeran complicación sobre complicación. Su razonamiento era un algoritmo increíblemente complicado que nadie podía seguir, que producía una increíblemente complicada secuencia de números que otra vez, nadie podía seguir, es decir, por medio de la cual no se podía encontrar ningún patrón sistemático. El no poder encontrar dichos patrones era visto como una señal de aleatoriedad. Inescrutabilidad tanto de entrada como de salida era el razonamiento de Knuth. Su razonamiento probó ser mortalmente incorrecto. En lugar de encontrar desorden y caos, Knuth descubrió la peor forma de no-aleatoriedad: su algoritmo tomó una semilla particular (es decir, una entrada inicial que inicia el generador de números aleatorios) y sólo siguió repitiéndola. La semilla era 6065038420. El generador de números aleatorios de Knuth repitió 6065038420 una y otra vez:

6065038420 6065038420 6065038420 6065038420 6065038420

6065038420 6065038420 6065038420 6065038420 ....

Lo que sea que se entienda por aleatoriedad, no es esto ciertamente. Knuth (1981, p. 5) rápidamente concluyó lo siguiente: “La moraleja de esta historia es que *los números aleatorios no deben ser generados con un método elegido al azar*. Debe usarse alguna teoría” (las itálicas son suyas).

Knuth y yo estamos de acuerdo en que generar aleatoriedad involucra pensamiento y diseño. Knuth, sin embargo, todavía sufre de remordimientos de conciencia, los cuales yo no tengo. Los generadores de números aleatorios deben ser cuidadosamente diseñados. Sobre este punto no hay controversia. La aleatoriedad es fundamentalmente una cuestión de diseño. Este punto es más ambicioso y abierto a controversia. La aleatoriedad recae en un diseño, no la probabilidad. Aquí radica una partida sin precedentes. La forma típica de entender la aleatoriedad es la siguiente: un objeto que se supone que exhibe aleatoriedad es propuesto (ej., una secuencia de números). Luego uno examina al objeto contra una colección de patrones (ej., pruebas estadísticas). Si el objeto se ajusta a cualquier patrón de la colección, no es aleatorio. Si viola todos los patrones de la colección de datos, entonces es aleatorio. Yo propongo lo contrario a esto. Consideremos *primero* una colección fija de patrones. Cualquier

objeto que viole todos los patrones de esa colección es aleatorio. Aquellos que satisfacen un patrón en la colección son no-aleatorios. De esta forma, la aleatoriedad se convierte en una noción relativa, es decir, *con respecto* a una colección de patrones.

En la práctica el primer enfoque sobre la aleatoriedad es fundamentalmente probabilística: secuencias de dígitos constituyen los objetos aleatorios, y pruebas estadísticas constituyen los patrones. Cuando el patrón inducido por una prueba estadística es violado, decimos que la secuencia pasa la prueba.<sup>3</sup> Cuando la cadena pasa suficientes pruebas, se dice que es aleatoria. Las pruebas, sin embargo, están formuladas de tal forma que la mayoría de las secuencias generadas de acuerdo a una distribución de probabilidad dada pasen exitosamente. Esto propone un problema. Para una secuencia cualquiera hay una prueba estadística que la cadena no puede pasar. Por tanto, siempre podemos preparar pruebas que produzcan una cadena supuestamente aleatoria que en realidad no lo sea.<sup>4</sup> Es dentro de este contexto que von Neumann formuló su sentencia. Secuencias verdaderamente aleatorias se supone que son generadas de acuerdo a alguna distribución de probabilidad y por esta única razón pasan las pruebas estadísticas. Los generadores de números aleatorios, por otra parte, son puramente determinísticos y sólo pueden imitar el pasar pruebas estadísticas. De acuerdo a von Neumann, secuencias generadas por algoritmos computacionales pueden a lo más pretender ser aleatorias pero son impostoras.

Pero cuando la probabilidad es repudiada, la aleatoriedad no es más una cuestión de imitar al azar. Cuando la aleatoriedad recae en el diseño, los patrones se convierten en el objeto fundamental de estudio. Un objeto aleatorio es entonces un objeto que sistemáticamente viola una colección fija de patrones. En contraste con el enfoque probabilístico convencional, este enfoque alternativo no tiene engaño. Con aleatoriedad premeditada uno no trata de imitar al azar como se hace con aleatoriedad probabilística. En lugar de eso, uno conduce una búsqueda metódica por un objeto que satisface ciertas restricciones. Estas restricciones comprenden todos los patrones que deben ser violados.

Para clarificar estos pensamientos necesito revisar un poco de teoría de probabilidad lo mismo que algunos pensamientos del pasado acerca de la aleatoriedad. Al analizar casos concretos de aleatoriedad, deberé limitarme a secuencias de 0's y 1's. Esta limitación no involucra una pérdida real de generalidad. Aleatoriedad—lo que he llamado probabilidad aleatoria—no es. En una conferencia interdisciplinaria sobre aleatoriedad, atendida entre otros, por los estadísticos George Marsaglia y Persi Diaconis como por los filósofos Brian Skyrms y Richard Jeffrey, la conclusión general fue la siguiente: *Sabemos lo que la aleatoriedad no es, no lo que es*. Yo atribuyo esta conclusión poco atractiva al matrimonio de la aleatoriedad con la probabilidad. Las dos experimentan diferencias irreconciliables. La aleatoriedad probabilística ha soportado consistentemente una formulación teórica precisa. Por otro lado, la aleatoriedad premeditada que esbozaré no se presta a una formulación teórica.

## ***2. Un poco de historia y motivación***

La idea de probabilidad para la imaginación popular siempre a residido en la ley de los grandes números. Desde que los mecanógrafos simiescos de Thomas Huxley le dieron al mundo un juego completo de Shakespeare, la gente ha contemplado esta ley con admiración. Su postulado básico es que si un evento tiene una probabilidad positiva de ocurrir, no importa que tan pequeña esta sea, y si uno repite las circunstancias bajo las cuales dicho

evento puede ocurrir *con una frecuencia suficiente*, entonces ese evento definitivamente ocurrirá.<sup>5</sup> Por supuesto, si el evento tiene una probabilidad “cero” de ocurrir, entonces nunca ocurrirá.

Por ejemplo, suponga estar confinado en una prisión y que se le da una moneda justa. Se le informa que si hace girar la moneda en el aire y obtiene 100 “caras” seguidas, será liberado. Dado que cada experimento es independiente, las probabilidades se multiplican. De esta forma, usted espera “caras” con una probabilidad de  $\frac{1}{2}$ , dos caras seguidas con una probabilidad de  $\frac{1}{2} \times \frac{1}{2} = \frac{1}{2^2}$ , ... y 100 “caras” seguidas con probabilidad  $\frac{1}{2} \times \frac{1}{2} \times \dots \times \frac{1}{2}$  [100 veces] =  $\frac{1}{2^{100}}$ , lo cual es aproximadamente 1 en  $10^{30}$ . Esta probabilidad es tan pequeña que lo deja con poca esperanza de salir pronto de prisión. Si pudiera, por ejemplo, hacer 10 billones de intentos cada año para obtener 100 caras seguidas, entonces tendría usted una probabilidad razonable de salir de prisión en  $10^{20}$  años. Pero, no se desespere, la fuerte ley de los grandes números garantiza que *eventualmente* usted saldrá libre.<sup>6</sup>

Suponga ahora que se le da un mazo estándar de cartas. Esta vez para salir de prisión usted tiene que conseguir flor imperial de espadas, cada vez barajando completamente el juego. Este evento tiene una probabilidad del orden de 1 en un millón. De esa forma, en cerca de un millón de oportunidades, usted saldrá de la cárcel. Su carcelero, sin embargo, gusta de su compañía y quiere mantenerlo cerca. Consecuentemente, decide eliminar el as de espadas del juego. Este movimiento deshace sus esperanzas de libertad. Con el mazo alterado su probabilidad de conseguir la flor imperial adecuada es precisamente cero.

En cualquier interpretación probabilística, el tiempo juega un papel. El girar una moneda es realmente el ejemplo básico en teoría de probabilidad; hay un sentido en el que si uno entiende el giro de la moneda en todas sus ramificaciones, se entiende la teoría de probabilidad.<sup>7</sup> Digamos que se le da una moneda justa. Usted está a punto de girar la moneda. No está seguro del resultado. Hay una probabilidad igual de que salga cara o cruz. Ahora usted gira la moneda. Sale cara. De pronto toda la incertidumbre queda fuera. La incertidumbre y la probabilidad aplican sólo para el futuro, para eventos que aún no suceden. Una vez que el evento ha ocurrido y ha sido presenciado, toda la incertidumbre desaparece.

Los eventos raros son causa de sorpresa sólo si el tiempo es el adecuado. Imagine, por ejemplo, que ante usted se encuentra un gran campo lleno de pasto. Tiene 100 piedras y 100 banderas, cada una de ellas marcadas del 1 al 100. Usted vuela sobre el campo con un helicóptero, liberando las piedras indiscriminadamente. Después de haber soltado la última piedra, aterriza el helicóptero en un lugar seguro y alejado del campo, deja el helicóptero y examina donde han aterrizado las piedras y coloca una bandera enseguida de cada piedra con su número correspondiente. Hay un número excesivamente grande de maneras en como pudieron haber aterrizado las piedras. Ellas tuvieron que haber aterrizado de alguna forma. Usted la está viendo y no está sorprendido o impresionado. Usted no lo ve como un milagro por el hecho de estar presenciando la ocurrencia de una probabilidad excesivamente pequeña. Algún evento improbable tenía que ocurrir. El colocar las banderas enseguida de las piedras *después* de que las piedras han caído no cambia las conclusiones.

Ahora modifique la situación. Como antes, usted tiene un campo, piedras y un helicóptero. Como antes, usted toma el helicóptero y piedras, y vuela sobre el campo, dejando caer las





tiene una descripción corta,

repetir '10' 50 veces.

La secuencia (R) no tiene una descripción corta y sencilla. Por esta razón Kolmogorov la consideraría más aleatoria que las secuencias (N), (H) y (A).

Como notamos, uno puede siempre describir una secuencia en términos de sí misma. Mientras (R) tiene la descripción

copiar '1100001101011000110111111010001100011011001110111

00011001000010111101110110011111010010100101011110'.

Dado que la secuencia (R) fue construida por los giros de la moneda, es muy probable que esta sea la descripción más corta de (R). Es un hecho que la vasta mayoría de secuencias de 0's y 1's tienen que su descripción más corta es la secuencia misma, es decir, la mayoría de las secuencias son aleatorias en el sentido computacional de Kolmogorov. En el lenguaje de mecánica estadística, hay una gran cantidad de secuencias de alta entropía, y aquellas cuyas descripciones computacionales son muy pequeñas, constituyen eventos raros, y la observancia de cualquier secuencia tal como resultado del azar es causa de sorpresa. No solo eso, sino que es causa para buscar explicaciones diferentes al azar.

Consideremos ahora una aplicación práctica de las ideas de Kolmogorov. Considere a una persona que se le acerca en la calle y le informa que ha hecho girar una moneda en el aire 100 veces. Si él le proporciona una secuencia (R), usted la examina y trata de salir con una descripción corta (el hacer esto es análogo a hacerle pruebas estadísticas). Después de eventos repetidos usted encuentra que no puede describir la secuencia de ninguna forma mejor de que la secuencia se describe a sí misma. Por tanto usted concluye que esta es una secuencia genuinamente aleatoria, es decir, un tipo de secuencia que esta persona pudo haber obtenido al hacer girar una moneda justa. Usted no está particularmente sorprendido o impresionado.

Suponga ahora que esta persona le proporciona una secuencia (R) en un pedazo de papel y luego desaparece. Una semana después reaparece y dice: "¿Adivine qué? Recuerde la secuencia que le pasé la semana pasada. Bueno, anoche estaba haciendo girar esta moneda y aunque usted no lo crea, obtuve la misma secuencia que le pasé en un pedazo de papel". Usted examina la moneda y está convencido de que es genuina. Además, esta persona insiste en que cada vez que hizo girar la moneda, ella dio giros bastante amplios (es decir, no alterados). ¿Qué concluye usted ahora? Como antes, usted no podrá encontrar ninguna secuencia más corta que la secuencia misma y la considera una secuencia aleatoria. A menos de que crea en los milagros, sin embargo, usted actuaría tontamente si concluye que esta persona está diciendo la verdad. La sincronización está al revés. Cuando le pasó la secuencia, hace una semana, el preestableció la secuencia. De esta forma, el orden está ya establecido. Cuando él regresa y le dice que *subsecuentemente* reprodujo la secuencia que le había pasado a usted, se engaña a sí mismo. Porque lo que realmente está diciendo es que sabía cual secuencia conseguiría la semana próxima. Esto es profecía. Si alguien no cree que la profecía

es algo milagroso (léase sobrenatural, estrictamente fuera del reino material), sólo necesita ir a Wall Street o Las Vegas donde todos los profetas genuinos son millonarios.

Suponga finalmente que esta persona llega con usted y dice: “¿Puede creerlo? Acabo de hacer girar la moneda 100 veces, y cada vez me dio como resultado cara”. Como antes, la moneda que le muestra es genuina y él es enfático en que los giros no fueron alterados. Esta vez él no fijó el patrón. Más bien, tal patrón es dado intrínsecamente. La secuencia (N) tiene la mínima entropía posible. Hay muy pocas secuencias con descripciones tan pequeñas como “repetir ‘1’ 100 veces”. Otra vez, a no ser de que ocurriera un milagro, usted actuaría ingenuamente al creer que esta persona dice la verdad. Las mentes razonables explican tales eventos considerando eventos diferentes al azar. El problema no es que tales secuencias constituyan eventos extremadamente raros. El problema es que hay muchos otros eventos que violan los pocos patrones preestablecidos que los humanos pueden retener en sus mentes. Lo básico aquí es la noción de un orden intrínseco. En el sentido del ejemplo de nuestras banderas y piedras, nuestra cognición preestablece las banderas de una manera muy limitada de formas diferentes. Cuando las piedras caen y se acomodan enseguida de las banderas preestablecidas, tenemos el derecho de sorprendernos y buscar explicaciones diferentes al azar. Los argumentos probabilísticos de este tipo son circunstanciales. Nuestro amigo “gira-monedas” que dice haber obtenido cara 100 veces seguidas (con una moneda justa, sin alterar los giros) sería acusado de mentir en una sociedad educada, así como un gerente de la lotería cuyos parientes ganan todos el sorteo sería acusado de fraude.<sup>8</sup>

### ***3. Complejidad y aleatoriedad***

La teoría de la complejidad computacional es quizás el tema de actualidad más candente en la ciencia computacional teórica. La complejidad computacional se enfoca en los recursos computacionales requeridos para que un algoritmo complete su tarea. La gran pregunta en complejidad computacional es si los algoritmos de tipo tiempo-polinomio coinciden con los algoritmos no-determinísticos tiempo-polinomio—si P es igual a NP (ver Garey and Johnson, 1979). Esta es una cuestión de tiempo-complejidad. El recurso es el tiempo y la cuestión es si los problemas en el NP se pueden resolver en tiempo-polinomio. Pero el tiempo no es el único recurso computacional. El espacio, o la memoria equivalente, también entra. ¿Cuánta memoria se necesita para resolver un problema dado? Esto también se convierte en una consideración importante. En la construcción de algoritmos eficientes, las interacciones tiempo-memoria siempre deben ser tenidas en cuenta. Por esto, un algoritmo tiempo-polinomio puede requerir demasiada memoria como para ser práctico, mientras que un programa que requiera poca memoria puede correr interminablemente.

Ahora, ¿qué tiene todo esto que ver con la aleatoriedad? Si recordamos el enfoque de Kolmogorov sobre la aleatoriedad, entendemos que dentro de este marco, una cadena de números es aleatoria al grado en que el programa que la genere sea máximo. Pero, ¿máximo en que sentido? Máximo en el sentido de la longitud del programa. Los generadores de aleatorios de Kolmogorov son programas que satisfacen dos condiciones: (1) no debe existir un programa de longitud estrictamente corta que genere la secuencia aleatoria propuesta, esto es, el programa no puede ser abreviado y aún generar la secuencia. Llamemos a estos programas “concisos”. Este requerimiento es esencial debido a que para cualquier programa es posible agregar algunas iteraciones vacuas que incrementan la longitud del programa, pero dejan el trabajo efectivo sin cambio, es decir, dejan las entradas-salidas de la misma forma.

(2) Dentro de todos los programas tersos, los generadores de aleatorios son los de longitud máxima. Los generadores de aleatorios de Kolmogorov son realmente soluciones a un problema mínimax: dentro de los programas tersos (aquellos que satisfacen la condición de minimalidad) eligen aquellos de longitud máxima. La noción de Kolmogorov de aleatoriedad se apega en la complejidad del espacio—el parámetro clave es la longitud del programa. Para generar secuencias aleatorias, estos programas deben estar almacenados en la memoria de un dispositivo computacional. Aquellos que consuman la mayor cantidad de memoria, pero que no puedan ser abreviados sin afectar las entradas-salidas, son los generadores de aleatorios de Kolmogorov.

Más recientemente, la relación tiempo-complejidad ha sido usada para definir aleatoriedad. En este caso un busca secuencias de dígitos cuyos algoritmos tiempo-polinomio no pueden distinguirse de cadenas aleatorias genuinas (es decir, aquellas cuyos dígitos son derivados al muestrear aleatoriamente de una distribución de probabilidad fija). Uno habla de cadenas que son P-indistinguibles respecto a cadenas genuinamente aleatorias. La idea básica aquí es que los únicos algoritmos humanos que se pueden manejar legítimamente son algoritmos tiempo-polinomio; algoritmos que no son tiempo-polinomial están afuera de nuestro rango de acción. Por tanto, si todos nuestros algoritmos tiempo-polinomio no pueden distinguir una supuesta cadena aleatoria de una genuina, entonces de hecho no existe ninguna distinción. La identidad de Leibniz de lo indiscernible es implícita aquí—distinciones que aparecen a través de algoritmos no polinomiales son indiscernibles.

Los matemáticos han encontrado estos enfoques de complejidad tiempo-espacio sobre la aleatoriedad altamente estimulantes, por lo menos inicialmente. Sin duda las ideas son lindas. Además, hay algo genuinamente profundo sucediendo aquí. Martin-Löf (1966<sup>a</sup>), un estudiante de Kolmogorov, derivó una buena cantidad de teoría clásica de probabilidad a partir del enfoque espacio-complejidad sobre la aleatoriedad (es decir, la ley de los grandes números y la ley del logaritmo iterado). Andrew Yao (1982) y Silvio Micali (Goldreich, Goldwasser y Micali, 1986) han usado el enfoque tiempo-complejidad sobre la aleatoriedad con algún éxito en criptografía (ej., las funciones de un solo sentido y “trampilla” en la criptografía moderna).

Aún, hay problemas. Después de que el entusiasmo inicial y éxitos se han desgastado, uno encuentra que los enfoques de complejidad sobre aleatoriedad no cumplen sus promesas. Esto es especialmente cierto en el enfoque de Kolmogorov vía espacio-complejidad. Tiempo-complejidad, siendo un enfoque mucho más reciente sobre la aleatoriedad, tiene aún que enfrentar desaprobación. Sin embargo, los dos enfoques enfrentan dificultades similares. Ciertamente las complejidades con respecto al tiempo y al espacio proveen de intuiciones maravillosas para la aleatoriedad, y sin ellas es improbable que este artículo pudiera haber sido escrito. Pero no ambas fallan al entregar una teoría de aleatoriedad en el sentido de que uno puede apuntar una secuencia concreta de ceros y unos y llamarla aleatoria.<sup>9</sup>

Hay dos razones para este fracaso práctico. La primera tiene que ver con la elección del lenguaje de programación. No me refiero con este término a BASIC, Lisp o Fortran, sino a la forma en que el dispositivo computacional interpreta una secuencia de 0's y 1's como programa y luego usa tal cadena para generar las secuencias (salida) aleatorias que estamos buscando. Alternativamente, podemos preguntar, ¿qué máquina universal Turing vamos a usar? Ni los enfoques de complejidad de espacio ni de tiempo sobre la aleatoriedad





responsable es el papel aún sin resolver de la probabilidad. Las secuencias aleatorias son, después de todo, supuestamente semejantes a secuencias derivadas de procesos aleatorios. Por ello es que cualquier secuencia generada por una computadora demanda validación probabilística. Y esto, como hemos visto, nos aterriza en un pantano probabilístico, puesto que debemos sujetar una secuencia aleatoria propuesta a pruebas estadísticas. Ahora, una prueba estadística es entre otras cosas un procedimiento de decisión; debe decidir entre diferentes salidas cuales pasan la prueba y cuales no. Ninguna de estas categorías debe estar vacía, de otra forma la prueba estadística es vacua. Por tanto, cualquier prueba tal debe pasar algunas pruebas y reprobar otras. ¿Pero cómo deben las pruebas elegirse a sí mismas? ¿Cuáles pruebas son suficientes para garantizar aleatoriedad?

La confusión aquí ha conducido a manadas de generadores abismales de números aleatorios, los cuales, dado su amplio uso en investigación experimental han llenado la literatura científica con errores tipo I. Este es un hecho muy reconocido. Frecuentemente ha sido echado en cara a programadores que, siendo competentes con la computadora, dejan mucho que desear como estadísticos. Sin embargo, el problema de los malos generadores de números aleatorios persiste incluso entre altamente competentes trabajadores en el campo. Por eso Donald Knuth promociona un generador aditivo de números que luego George Marsaglia desacredita. ¿Cómo logra esto Marsaglia? Inventa una prueba estadística en la cual las secuencias producidas por el generador aditivo pasan si son derivadas de un proceso aleatorio, pero que de hecho no pueden pasar.<sup>11</sup>

La escena es que un programador y un estadístico luchan sobre un cuadrilátero. El programador quiere un programa eficiente que genere números aleatorios. El estadístico quiere una prueba estadística simple que desacredite los números generados. El programador propone, el estadístico dispone. Mientras que el estadístico no tenga una prueba estadística para desacreditar las secuencias aleatorias generadas por el programa, el programador gana; en cuanto una prueba estadística se “cocine”, el estadístico gana. El juego es sin duda divertido, y responsable de incontables artículos de investigación. Pero nunca puede ofrecer una teoría concluyente de aleatoriedad—el juego no tiene resolución.

#### ***4. La aleatoriedad como teoría***

A lo largo de este ensayo he distinguido deliberadamente entre aleatoriedad, probabilidad y azar. El azar lo dejo a lanzar monedas y a eventos cuánticos. Si el azar es reducible a determinismo o si es fundamentalmente indeterminístico o simplemente ilusorio es un debate al que no me aventuraré aquí. La probabilidad, la medida probabilidad teórica de Kolmogorov de los 30's es una teoría matemática bien definida inspirada por procesos aleatorios y diseñada para modelar al azar. La aleatoriedad, hasta la fecha, ha sido el intento de los científicos de imitar al azar utilizando métodos determinísticos.<sup>12</sup>

Ahora repudiamos todas las pretensiones del azar y la probabilidad y requiramos sólo una cosa de la aleatoriedad: la violación sistemática de un juego fijo de patrones. ¿Cómo se vería tal teoría? Primero necesitamos delimitar una colección de objetos potencialmente aleatorios. Llamemos a tal colección un *espacio candidato* y denotémoslo por  $\Omega$ . Los elementos de  $\Omega$  son candidatos participando para la candidatura—el honor de ser llamados aleatorios. Enseguida necesitamos delimitar una colección de patrones. Los patrones son, si Ud., quiere, obstáculos

que los candidatos deben brincar para recibir la distinción de ser llamados aleatorios. Más precisamente, un candidato  $\omega$  en  $\Omega$  es aleatorio si viola todos los patrones de una colección dada de patrones. Llamemos a tal colección de patrones un *espacio patrón* y denotarlo por  $P$ . Observe que esta es una noción relativa de aleatoriedad— $w$  es aleatorio relativo a  $P$ .

Para cada patrón  $p$  en  $P$ , un candidato  $w$  violará o se ajustará al patrón. Por tanto, un patrón no es más que una separación del espacio  $\Omega$  entre dos subconjuntos no vacíos, desunidos y exhaustivos, donde la inclusión dentro de uno de estos subconjuntos significa ajustarse a  $p$ , y la inclusión en el otro, el violar a  $p$ . Ahora esto puede ser para algunas matemáticas excesivamente bobas, si no somos cuidadosos. Porque, iniciando con el espacio del candidato  $\Omega$ , podemos reducir patrones a nada más que una colección de subconjuntos de  $\Omega$ , digamos,  $A_1, A_2, \dots, A_n$ . Luego para algún objeto  $w$  violar todos estos patrones es simplemente caer fuera de  $A_1, A_2, \dots, A_n$ . Por tanto,  $w$  es aleatorio si cae en el complemento de  $A_1 \cup A_2 \cup \dots \cup A_n$ . Además, si este complemento es nulo, entonces no tiene elementos aleatorios con respecto al espacio de patrones  $\{A_1, A_2, \dots, A_n\}$ . Al nivel más alto de generalidad esto es todo lo que estamos haciendo cuando construimos o encontramos un objeto aleatorio. Por tanto, si el marco que estoy proponiendo para la aleatoriedad ofrece alguna posibilidad interesante, debe hacerlo a un nivel menor de generalidad, donde algunos análisis razonados justifican la elección de patrones relativo a los cuales los candidatos sean juzgados como aleatorios (es decir, consideraciones de complejidad).

Sin embargo, incluso a un nivel puramente teórico se pueden obtener algunos razonamientos útiles. Estamos buscando objetos aleatorios en el espacio candidato  $\Omega$  con respecto al espacio patrón  $P$ . Tomamos los patrones en  $P$  como subconjuntos de tal forma que ajustarse a un patrón  $p$  en  $P$  coincide con el hecho de ser parte de  $p$ . Denotemos los objetos aleatorios de  $\Omega$  relativos a  $P$  por:

$$\Omega/P =_{\text{def}} \{\omega \in \Omega \mid \omega \notin p \text{ para todo } p \in P\} \quad (4.1)$$

Considere ahora dos espacios patrón  $P$  y  $P'$ . Si  $P'$  incluye a  $P$ , entonces el  $\Omega/P'$  no puede contener más elementos aleatorios que  $\Omega/P$ . Esto va de acuerdo con la intuición, pues entre más patrones debe violar un elemento potencialmente aleatorio, lo menos probable es que consiga ganar esa distinción. Los patrones ponen obstáculos que los candidatos deben brincar para calificar como aleatorios. Dado que  $P'$  contiene más obstáculos que  $P$ , los candidatos tienen más problemas para calificar en relación a  $P'$  que a  $P$ .

También es claro a partir de esta formulación general que puede haber muchos patrones, o que los patrones pueden ser elegidos de tal forma que  $\Omega/P$  esté vacío. Por tanto podemos poner demasiados obstáculos, de tal forma que ningún candidato califique como aleatorio. Este era precisamente el problema con los *colectivos* de von Mises (1936). Su idea era delinear las secuencias aleatorias infinitas de 0's y 1's modeladas sobre la secuencia interminable de giros de una moneda justa. El espacio candidato  $\Omega$  era por tanto  $\{0,1\}^\infty$  y una secuencia aleatoria propuesta debería tener 0's y 1's distribuidos aleatoriamente (es decir, la misma proporción de 0's y 1's). Von Mises quería forzar esta noción de distribución uniforme lo más lejos que pudiera. Por tanto quería requerir una distribución uniforme de 0's y 1's a

través de todas las subsecuencias de una secuencia potencialmente aleatoria. Esto provó ser un requerimiento muy riguroso.

Más formalmente, von Mises consideraba la siguiente esperanza: sus candidatos  $w$  comprendían todas las funciones desde los números naturales  $\mathbf{N} = \{0,1,2,\dots\}$  hasta el set binario  $\{0,1\}$ , es decir, las secuencias infinitas de 0's y 1's. Sus patrones fueron inducidos por subconjuntos infinitos de  $\mathbf{N}$  como  $\mathbf{S} = \{s_0 < s_1 < s_2 < \dots\}$ . Como von Mises lo vio, para que  $\omega$  fuera aleatorio debería estar uniformemente distribuido en cualquier  $\mathbf{S}$  tal –la aleatoriedad después de todo era el imitar el giro de una moneda justa. Por tanto, un aleatorio  $\omega$  debería satisfacer

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \omega(s_i) = \frac{1}{2} \quad (4.2)$$

para todos los subconjuntos infinitos  $\mathbf{S}$  de  $\mathbf{N}$ .

Pero esto presenta un problema. Hay simplemente demasiados subconjuntos  $\mathbf{S}$  para que cualquier candidato  $\omega$  pueda satisfacer (4.2) para toda  $\mathbf{S}$ . Esto puede verse fácilmente. Un aleatorio  $\omega$  debe ciertamente estar uniformemente distribuido a lo largo de  $\mathbf{N}$  y debe por tanto satisfacer

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \omega(i) = \frac{1}{2} \quad (4.3)$$

Ahora, si escogemos  $\mathbf{S}$  como tal subconjunto (infinito) de  $\mathbf{N}$  en el cual  $w$  es idénticamente 1, entonces en  $\mathbf{S}$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \omega(i) = 1 \quad (4.4)$$

$w$  ciertamente no puede estar uniformemente distribuido en esta  $\mathbf{S}$ . De ahí que para cualquier  $w$  presumiblemente aleatorio siempre podemos encontrar un subconjunto de  $\mathbf{N}$  en el cual  $w$  parece todo menos aleatorio.

Al permitir demasiados patrones, en efecto cometemos el ahora familiar error de la aleatoriedad, es decir, inventamos patrones para probar la aleatoriedad de un objeto después de que el objeto ha sido presentado. En el ejemplo, precedente, para obtener el límite en la ecuación (4.4) necesitábamos construir  $\mathbf{S}$  con la base del objeto presumiblemente aleatorio mismo  $-\omega$ . Esto, como hemos observado, es análogo al viejo error estadístico de seleccionar hipótesis estadísticas después de que hubo terminado el experimento y que sus resultados se han examinado. Tal metodología es siempre incorrecta.

Debido a que la idea original de von Mises no pudo ponerse a trabajar, se hicieron intentos de salvarla. El movimiento obvio sería restringir los subconjuntos  $\mathbf{S}$  que  $\omega$  debería satisfacer (4.2). Por tanto se sugirió que (4.2) fuera requerida sólo para los subconjuntos infinitos de  $\mathbf{N}$

que fueran recursivamente numerables (r.e., por sus siglas en inglés) (ver Church, 1940). Dado que sólo contablemente hay muchos programas que generan estos juegos, la colección de juegos r.e., es susceptible de contarse. Además, la medición de consideraciones teóricas implica que casi cada candidato  $w$  satisface (4.2) para todos los  $S$ s en tal colección.<sup>13</sup> Por tanto los patrones inducidos por los juegos r.e., infinitos dejan muchas secuencias infinitas que son aleatorias con respecto este espacio contable de patrones.

Mientras que este ejemplo ilustra la teoría de aleatoriedad que persigo, no es el mejor anuncio para mi teoría. El problema con secuencias aleatorias infinitas es que permanecen siendo aleatorias independientemente de los segmentos iniciales finitos. Por tanto para una secuencia infinita de 0's y 1's, uno puede cambiar las primeras  $10^{1000}$  entradas a 0 sin afectar la aleatoriedad de la secuencia. La aleatoriedad de una secuencia infinita sólo puede ser comprobada al tomar en cuenta el comportamiento limitante completo de la cadena. Estas son malas noticias para cualquiera interesado en las aplicaciones prácticas de la aleatoriedad. Por tanto a continuación me concentraré en la aleatoriedad en contextos infinitos.

Entonces, ¿cómo se vería una teoría sobre aleatoriedad? Ciertamente uno debe iniciar con una colección de objetos potencialmente aleatorios, el espacio candidato  $\Omega$ . Enseguida debemos encontrar un espacio de patrones  $P$  con respecto al cual los objetos en  $\Omega$  Pueden ser aleatorios.  $P$  es directo y problemático al mismo tiempo.  $P$  es directo porque sus patrones nos permiten decidir rápidamente si un objeto presumiblemente aleatorio se ajusta al patrón o no (de esta forma los patrones reducen las particiones binarias de  $\Omega$ ).  $P$  es problemático porque sus patrones deben ser seleccionados de acuerdo a un razonamiento que justifique el llamar a los elementos de  $\Omega/P$  objetos aleatorios. Las consideraciones teóricas fijadas entran aquí:  $P$  debe ser lo suficientemente grande y lo suficientemente pequeño. Debe ser lo suficientemente pequeño para evitar que  $\Omega/P$  esté vacío— $P$  siempre puede ser aumentado para que  $\Omega/P$  esté vacío. Por otra parte, si  $P'$  incluye a  $P$ , y si  $P'$  no está vacío, entonces  $P'$  es el  $P$  preferible. Por tanto  $P$  debe contener todos los patrones que los objetos aleatorios no pueden legítimamente fracasar en romper.

### ***5. La aleatoriedad en la práctica***

La aleatoriedad como el rompimiento sistemático de patrones fijos ha estado implícita en la investigación pasada. Justo antes de introducir su enfoque de complejidad computacional sobre aleatoriedad, Kolmogorov (1965a) escribió un artículo titulado “Sobre Tablas de Números Aleatorios”, cuyo contenido matemático eran sólo combinaciones. En este documento, Kolmogorov se enfocó al problema de construir secuencias numéricas aleatorias de una longitud fija finita. Habiendo decidido la longitud  $n$  (algún número natural positivo), entonces procedió sistemáticamente a eliminar secuencias que no pudieran ser aleatorias de acuerdo a cierto criterio frecuentista sobre aleatoriedad. Estas exclusiones sistemáticas constituyeron los patrones que las secuencias no aleatorias no pudieron violar. En esta sección incorporaré el trabajo de Kolmogorov sobre secuencias aleatorias finitas en el marco que estoy desarrollando. Mi tratamiento introducirá suposiciones simplificadoras que no involucran una pérdida de generalidad, sino que también extenderán ciertas ideas implícitas en el trabajo original de Kolmogorov.

Nuestro espacio candidato es la colección de  $2^n$  secuencias de 0's y 1's de longitud  $n$ . Un candidato  $\omega$  es por lo tanto una función de  $\{1, 2, \dots, n\}$  a  $\{0, 1\}$ . Como con los colectivos de von Mises, nuestra motivación por la aleatoriedad es una distribución uniforme: la proporción de 0's y 1's para candidatos aleatorios  $\omega$  debe ser aproximadamente la misma. Por tanto, hasta ahora las frecuencias han fallado al no estar uniformemente distribuidas, se han ajustado a patrones y se ha evidenciado una falta de aleatoriedad. La totalidad de los patrones que nos pueden interesar es inducida por la colección  $\Sigma$  que comprende todos los subconjuntos no vacíos del juego indicante para  $\Omega$ , es decir, los subconjuntos no vacíos de  $\{1, 2, \dots, n\}$ . Para cualquier  $\mathbf{S}$  en  $\Sigma$  la extensión a la cual un candidato  $w$  es aleatorio corresponde a que tan cerca

$$\frac{1}{|\mathbf{S}|} \sum_{i \in \mathbf{S}} \omega(i) \quad (5.1)$$

está a  $1/2$ . En la expresión (5.1)  $|\mathbf{S}|$  denota la cardinalidad de  $\mathbf{S}$  (la cual es mayor que cero por la forma en que definimos  $\Sigma$ ). La expresión (5.1) es la proporción de 1's que  $\omega$  tiene en el juego  $\mathbf{S}$ .

Ahora, requerir que esa expresión (5.1) sea igual a  $1/2$ , es una condición muy restrictiva. Si por ejemplo la cardinalidad de  $\mathbf{S}$  es un número primo diferente a 2, entonces ningún candidato  $w$  puede ser aleatorio con respecto a  $\mathbf{S}$ —la expresión (5.1) nunca podría tomar el valor de  $1/2$ . Por tanto queremos a (5.1) cerca de  $1/2$  mientras al mismo tiempo nos permitimos algo de holgura. Por tanto fijamos una  $\epsilon$  positiva y estipulamos que un candidato  $\omega$  rompa el patrón prescrito por  $\mathbf{S}$  si

$$\left| \frac{1}{|\mathbf{S}|} \sum_{i \in \mathbf{S}} \omega(i) - \frac{1}{2} \right| < \epsilon. \quad (5.2)$$

Estas observaciones son la raíz de las secuencias binarias (n,e)-aleatorias de Kolmogorov.

Una cuestión natural aparece ahora: Dados  $n$  y  $\epsilon$ , ¿para cuáles subcolecciones de  $\mathbf{S}$  y candidatos de  $\Omega$  es satisfecha la desigualdad (5.2)? Realmente dos cuestiones están involucradas aquí: (1) Dada una colección de  $\mathbf{S}$ s, ¿podemos encontrar un candidato  $w$  que satisfaga (5.2) para cada una de estas  $\mathbf{S}$ s? Dado  $\omega$ , ¿para cuál  $\mathbf{S}$  es satisfecha (5.2)? La primera cuestión se refiere a si podemos encontrar un objeto aleatorio con respecto a una colección preestablecida de patrones. La segunda se refiere a los patrones que producen un candidato aleatorio  $\omega$ . La segunda cuestión es nueva y no aparece en el trabajo de Kolmogorov ni en el de sus sucesores. Kolmogorov se enfoca en la primera pregunta, aunque desde una perspectiva limitada. Examinemos estas cuestiones en turno.

Para una colección fija de  $\mathbf{S}$ s, ¿existe algún candidato  $\omega$  que viole todos los patrones inducidos y por tanto sea aleatorio? Un número de restricciones están luchando una con la otra. Si  $\epsilon$  es mayor que  $1/2$ , (5.2) siempre es satisfecha y todo es aleatorio. Por tanto queremos que  $\epsilon$  sea menor a  $1/2$ . Una vez que se ha fijado a  $\epsilon$ , es generalmente cierto que el número de

juegos  $S$  con respecto al cual el candidato  $\omega$  es aleatorio (es decir, rompe al patrón indicado en (5.2) se incrementará con respecto a la longitud  $n$  de la secuencia. Pero si  $\epsilon$  es muy pequeño, entonces cometemos la culpa de requerir que (5.1) sea igual a  $1/2$  (un  $\epsilon$  muy cercano a cero en la desigualdad (5.2) es equivalente a que la expresión (5.1) iguale a  $1/2$  exactamente).

Otras restricciones son menos obvias. Por ejemplo, los juegos  $S$  cuya cardinalidad es muy pequeña con respecto a  $n$ , generalmente no serán adecuados para revisar la aleatoriedad de un candidato. Por tomar un ejemplo extremo, si  $S$  es un singulete (es decir, un conjunto que contiene un solo elemento), entonces la expresión (5.1) será ya sea 0 o 1 implicando que para cualquier  $\epsilon$  razonable, la desigualdad (5.2) será violada. Por tanto, con respecto a  $S$ s que son singuletes ningún candidato puede ser aleatorio. Dentro de nuestro marco, cualquier patrón  $P$  que incluye por lo menos un singulete no tiene elementos aleatorios; en este caso  $\Omega/P$  estará vacío.

Para un ejemplo más complicado, considere juegos  $S$  conteniendo dos elementos. Para simplificar los cálculos asumamos que  $n$  es par ( $n=2k$ ) y restrinjamos nuestra atención a los candidatos  $\omega$  que tienen el mismo número de 0s y 1s (ej.,  $k$ ). (Estas condiciones pueden ser eliminadas sin afectar las conclusiones generales.)

Encontramos que

$$\frac{1}{n} \sum_{i=1}^n \omega(i) = \frac{1}{2}, \quad (5.3)$$

$$\binom{2k}{2} \text{ juegos } S \text{ tienen 2 elementos,} \quad (5.4)$$

$$2 \binom{k}{2} \text{ juegos } S \text{ con 2 elementos satisfacen } \frac{1}{|S|} \sum_{i \in S} \omega(i) = 0 \text{ o } 1, \quad (5.5)$$

$$k^2 \text{ juegos } S \text{ con 2 elementos satisfacen } \frac{1}{|S|} \sum_{i \in S} \omega(i) = \frac{1}{2}, \text{ y} \quad (5.6)$$

$$\binom{2k}{2} = 2 \binom{k}{2} + k^2. \quad (5.7)$$

Por tanto para cerca de la mitad de los juegos  $S$  con dos elementos las frecuencias son exactamente correctas (cuando (5.6) se obtiene), mientras que para la otra mitad las frecuencias son exactamente incorrectas (cuando (5.5) se obtiene). Además, por un argumento trivial de inclusión-exclusión uno puede elegir  $k$  cuyos juegos  $S$  (es decir,  $\{1,2\}$ ,

$\{1,3\}, \dots, \{1,k\}$  y  $\{1, k+1\}$  para los cuales por lo menos uno de estos juegos satisfará (5.5) sin importar el candidato. En otras palabras, uno puede encontrar  $k$  patrones inducidos por juegos  $\mathbf{S}$  de cardinalidad 2 los cuales todos producen candidatos no aleatorios. Si relajamos nuestras suposiciones iniciales, observamos que para una  $n$  arbitraria y  $\epsilon < 1/2$ , podemos encontrar aproximadamente  $n/2$  juegos con 2 elementos para los cuales ningún candidato puede ser aleatorio (ningún candidato puede violar todos los patrones inducidos). Dentro de nuestro marco, para un espacio de patrones  $P$  tal,  $\Omega/P$  está vacío.

Los juegos  $\mathbf{S}$  en  $\Sigma$  que realmente interesaron a Kolmogorov fueron aquellos que, a diferencia de los dos ejemplos precedentes, incluyeron una porción sustancial del juego indicante  $\{1, 2, \dots, n\}$ . Tales juegos  $\mathbf{S}$  fueron generados algorítmicamente, y tendieron a inducir patrones que a uno le gustaría ver a secuencias “genuinamente aleatorias” romper. Por tanto el primer  $\mathbf{S}$  que fue considerado fue el ser indicante entero  $\{1, 2, \dots, n\}$  –cualquier objeto  $\omega$  debería estar uniformemente distribuido dentro de  $\epsilon$  en este juego. Enseguida, uno debería considerar juegos  $\mathbf{S}$  conteniendo términos alternativos del juego indicante:  $\{1, 3, 5, \dots, 2[(n+1)/2] - 1\}$  y  $\{2, 4, 6, \dots, 2[n/2]\}$  (los corchetes indican la mayor función entera). Kolmogorov encontró que al generar juegos de esta forma podría obtener

$$\frac{1}{2} e^{2n\epsilon^2(1-\epsilon)} \quad (5.8)$$

juegos en  $\Sigma$  para los cuales por lo menos un candidato  $\omega$  fuera aleatorio.<sup>15</sup> Por tanto el número de patrones para los cuales un objeto aleatorio existe es exponencial en la longitud  $n$  de la secuencia.<sup>16</sup>

Con (5.8) Kolmogorov determinó un límite superior en el número de patrones con los que podría salir y aún obtener un candidato aleatorio. Su algoritmo fijó los patrones, (5.8) limitó el número de patrones, y con esta información Kolmogorov procedió a buscar un candidato aleatorio. Nuestra segunda pregunta revierte todo esto: dado un candidato fijo  $w$ , ¿para cuáles patrones ( $\mathbf{S}$ s) es  $\omega$  aleatorio? ¿Cuáles espacios  $P$  de patrones interpretan a  $w$  como aleatorio? Kolmogorov fracasó al dirigirse a esta pregunta. Sin embargo, ella ofrece nuevas introspecciones acerca de la aleatoriedad y marca el papel distinguido que las permutaciones (y más generalmente las acciones de grupo) juegan en cualquier teoría sobre aleatoriedad basada en patrones.

Para indicar porqué es esta segunda pregunta importante consideremos el siguiente ejemplo. Suponga que la secuencia

$$\omega = 0011100101 \quad (5.9)$$

es una secuencia  $(n, \epsilon)$ -aleatoria para  $n = 10$  y  $\epsilon > 1/10$ . Encontramos que en  $\mathbf{S}_0 = \{1, 2, \dots, 10\}$ .  $\omega$  está uniformemente distribuida. En  $\mathbf{S}_1 = \{1, 3, 5, 7, 9\}$ ,  $\mathbf{S}_2 = \{2, 4, 6, 8, 10\}$ ,  $\mathbf{S}_3 = \{1, 2, 3, 4, 5\}$ , y  $\mathbf{S}_4 = \{6, 7, 8, 9, 10\}$   $w$  está dentro de  $1/10$  de estar uniformemente distribuida. Considere ahora las siguientes permutaciones del set indicante  $\mathbf{S}_0 = \{1, 2, \dots, 10\}$

$$\sigma = (1 \ 8)(2 \ 10) \quad (5.10)$$

$$\tau = (2\ 3)(5\ 6) \quad (5.11)$$

$\sigma$ , por ejemplo, permuta  $\{1, 2, \dots, 10\}$  al intercambiar 1 y 8, lo mismo que 2 y 10. Si nosotros ahora modificamos  $w$  aplicando  $s$  y  $t$ , encontramos que la secuencia resultante de 0's y 1's es cualquier cosa menos aleatoria:

$$\omega \circ \sigma = 1111100000 \quad (5.12)$$

$$\omega \circ \tau = 0101010101 \quad (5.13)$$

En  $S_3$  y  $S_4$  los  $\omega \circ \sigma$  fallan lo más posible en estar uniformemente distribuidos; en  $S_1$  y  $S_2$  pasa lo mismo para  $\omega \circ \tau$ . Pero las permutaciones que alteraron a  $\omega$  también alteran los juegos (patrones) de  $S_1$  a  $S_4$ . Por lo tanto  $\sigma$  transforma a  $S_3$  y a  $S_4$  y a  $S_4$  en  $\sigma S_3 = \{3, 4, 5, 8, 10\}$  y en  $\sigma S_4 = \{1, 2, 6, 7, 9\}$  en los cuales  $\omega \circ \sigma$  está uniformemente distribuido dentro de  $1/10$ , mientras que  $\tau$  transforma a  $S_1$  y  $S_2$  en  $\tau S_1 = \{1, 2, 6, 7, 9\}$  y  $\tau S_2 = \{3, 4, 5, 8, 10\}$  en los cuales  $\omega \circ \tau$  está uniformemente distribuido dentro de  $1/10$ .

Hay una lección que aprender. Dentro de 0-1 secuencias de longitud 10 que tienen el mismo número de 0's y 1's,  $\omega \circ \sigma$  es tan no-aleatorio como es posible. Y aún con respecto a algunas  $S$ s  $\omega \circ \sigma$  es justo tan aleatorio como  $\omega$ . De hecho, cuando sea que  $w$  es aleatorio con respecto a  $S$ ,  $\omega \circ \sigma$  es aleatorio con respecto a  $\sigma S$ , y  $\omega \circ \tau$  es aleatorio con respecto a  $\tau S$ . La aleatoriedad realmente depende de cómo vemos las cosas. Los patrones  $S_0, S_1, S_2, S_3, S_4$  son los tipos de patrones con los que los humanos se sienten cómodos, son con los cuales nuestros aparatos visuales y preceptuales razonan. Nosotros esperamos que las secuencias aleatorias se encuentren distribuidas aleatoriamente a lo largo de tales patrones agradables. Si por otro lado, nuestros aparatos perceptivos estuvieran configurados de tal forma que alguna permutación de estos patrones apareciera como más natural (es decir,  $\sigma S_0, \sigma S_1, \sigma S_2, \sigma S_3, \sigma S_4$ ), entonces nuestro sentido de aleatoriedad estaría alterado.<sup>17</sup>

## 6. *El papel de las Acciones de Grupo*

Resumamos ahora nuestro trabajo sobre aleatoriedad desde un punto de vista abstracto. Nos ha sido dada una colección de objetos, el *espacio candidato*  $\Omega$ , donde queremos encontrar objetos aleatorios. La aleatoriedad es entendida como el violar patrones. Generalmente habrá una colección que comprende todos los patrones concebibles que pudieran interesarnos (ver  $S$  en la sección anterior). Refirámonos a tal colección como un *espacio patrón completo* y denotémoslo por  $F$ . Mientras que un espacio patrón completo contendrá todos los patrones que pudieran concebiblemente interesarnos, usualmente este será tan amplio como para dejar espacio para aleatoriedad —es seguro que cada candidato dentro de  $\Omega$  se ajustará a algún patrón en  $F$ , de tal forma que ningún candidato puede ser aleatorio con respecto a  $F$  completo. Por tanto  $\Omega/F$  típicamente está vacío (si no, especifique  $\Omega/F$  y sus problemas se acaban).

Por esta razón normalmente consideraremos *espacios patrón*  $P$  que son subconjuntos propios de  $F$ . Si tenemos confianza en que el espacio patrón  $P$  captura adecuadamente lo que nosotros queremos de aleatoriedad en  $\Omega$ , y si es cierto que  $\Omega/P$  no está vacío, entonces nuestra tarea se reduce a especificar  $\Omega/P$ , es decir, a encontrar a aquellos candidatos  $\omega$  que violan todos los patrones en  $P$ . En la última sección el algoritmo de Kolmogorov para generar patrones proporcionó justo el espacio patrón  $P$  que Kolmogorov consideró relevante para la aleatoriedad de secuencias finitas 0-1. El límite dado en la expresión (5.8) reflejó que tan grande podría ser tomado  $\Omega/P$  manteniendo a  $\Omega/P$  no vacío.

Aunque es seguro que el espacio patrón  $F$  completo contendría todos los patrones de interés, generalmente no está claro si un espacio patrón  $P$  dado proporcionará la noción “correcta” de aleatoriedad para el propósito de un juego, mucho menos una noción universalmente correcta de aleatoriedad. Los espacios patrón no están grabados en piedra. No vienen con un orden de rango natural que nos permita decidir que patrón ofrece “mejor” aleatoriedad que otro. No vienen con banderas que los marquen como los verdaderos portadores de aleatoriedad. Si por alguna razón  $P$  estuviera grabado en piedra, entonces la única tarea por hacer sería el delinear los miembros de  $\Omega/P$ . Pero dado que generalmente ese no es el caso, es conveniente revertir la fotografía. Por tanto podemos iniciar con un candidato  $\omega$  que es aleatorio para  $F(\omega)$ . Llamemos a este el *espacio patrón en  $F$  inducido por  $\omega$* .  $\omega$  viola todos los patrones en  $F(\omega)$  y es un miembro (posiblemente el único) de  $\Omega/F(\omega)$ .

El problema obvio ahora es relacionar los espacios patrón inducidos  $F(\omega)$  para varios candidatos  $\omega$ . Esto creo yo que es logrado mejor por medio de acciones de grupo. Consideramos la acción de un grupo  $\Gamma$  en el espacio candidato. Representemos el grupo  $\Gamma$  multiplicativamente, denotando al elemento identidad por  $\epsilon$ . Al decir que  $\Gamma$  actúa en  $\Omega$ , queremos decir que cada elemento del grupo induce una función para sí mismo tal que

- 1)  $\epsilon$  es la identidad de la transformación en  $\Omega$ .
- 2) Para cada  $g$  y  $b$  en  $\Gamma$   $g(b\omega) = (gb)\omega$ , es decir, composición de las funciones inducidas por  $\Gamma$  espejos en la multiplicación de grupo.

Se deduce de (1) y (2) que las funciones inducidas son de hecho permutaciones (bisecciones) en  $\Omega$ .<sup>18</sup>

Desde nuestra perspectiva, la acción de grupo de  $\Gamma$  en  $\Omega$  se hace interesante cuando el elemento en turno induce una acción de grupo en el espacio patrón completo  $F$ . Para ver que una acción de grupo en  $\Omega$  inducirá una acción de grupo en patrones y espacios patrón, es suficiente notar que un patrón individual  $p$  es ultimadamente sólo un subconjunto de  $\Omega$ . Por lo tanto, para un elemento  $g$  del grupo  $\Gamma$  es natural considerar el patrón  $gp = \{g\omega \mid \omega p\}$ . Los espacios patrón  $P$  y el espacio patrón completo  $F$  están por supuesto compuestos de tales patrones  $p$ . Por tanto para  $g$  en  $\Gamma$  y un espacio patrón  $P$  tiene sentido considerar  $gP = \{gp \mid pP\}$ . Dado que la característica distintiva de  $F$  como espacio patrón es que contiene todo –debe contener todos los patrones concebiblemente relevantes para la aleatoriedad– no hay problema en elegir que  $F$  sea tan grande de forma que esté cerrado bajo la operación de

grupo. Por tanto podemos asumir que para todo  $g$  en  $\Gamma$ , y todo  $p$  en  $F$ ,  $gp$  está también en  $F$ . Con esta propiedad de encierro,  $\Gamma$  de hecho induce una acción de grupo en el espacio patrón completo  $F$ , y manda a los espacios patrón  $P$  a los espacios patrón  $gP$ .

Con un grupo  $\Gamma$  actuando en ambos  $\Omega$  y  $F$ , se hace posible comparar la aleatoriedad de los candidatos  $\omega$  y  $\omega'$  con respecto a los patrones inducidos  $F(\omega)$  y  $F(\omega')$ . Si por ejemplo  $\omega'$  está en la órbita de  $\omega$  (es decir, si hay algún elemento  $g$  para el cual  $g\omega = \omega'$ ), entonces podemos preguntar como  $F(\omega)$ ,  $gF(\omega)$  y  $F(\omega')$  pueden compararse. Si  $\Gamma$  es transitivo en  $\Omega$ , entonces todos los candidatos pueden ser comparados de esta forma. Una pregunta interesante es si  $gF(\omega)$  iguala a  $F(g\omega)$ . Si es así, entonces la aleatoriedad de  $\omega$  y la de  $\omega' = g\omega$  son enteramente simétricas –los patrones que rompe  $\omega$  para ser aleatorio y los que rompe  $\omega'$  son imágenes en un espejo bajo la acción de grupo.

Notemos que esta explicación abstracta de las acciones de grupo estaba implícita en el ejemplo de Kolmogorov de las secuencias aleatorias finitas descritas en la sección anterior. Existía la colección de secuencias aleatorias finitas de 0-1 con longitud finita  $n$ . El grupo actuando era el grupo simétrico en  $n$  caracteres,  $S_n$ , lo cual sirve como nuestro  $G$ . Un elemento  $g$  en  $\Gamma (=S_n)$  es por supuesto sólo una biyección en  $\{1, 2, \dots, n\}$ . Por tanto, el que  $g$  induzca una función en él debe ser interpretado como sigue:  $g(\omega) = \omega \circ g$ . En efecto,  $g$  toma cualquier secuencia  $\omega$  de 0's y 1's y rearregla estos 0's y 1's en un orden diferente.

$\Gamma$  también induce una acción de grupo en el espacio patrón completo  $\mathbf{S}$ , el cual comprende los subconjuntos vacíos  $\mathbf{S}$  de  $\{1, 2, \dots, n\}$ . Bajo la acción de un elemento  $g$ ,  $\mathbf{S}$  es enviado a su imagen natural bajo el grupo simétrico, a saber  $g\mathbf{S}$ . Note que  $\mathbf{S}$  en  $\Sigma$  no es en sí mismo un subconjunto del espacio candidato  $\Sigma$ . Pero cuando tal  $\mathbf{S}$  es usado para seleccionar candidatos  $\omega$  vía la desigualdad (5.2),  $\mathbf{S}$  especifica un patrón (es decir, un subconjunto) en  $\Omega$ , el cual podemos denotar por  $p(\mathbf{S})$ . Encontramos una consistencia perfecta en la forma en que la acción de grupo transforma los elementos  $\mathbf{S}$  de  $\Sigma$ , y la forma en que la acción transforma los patrones inducidos por tales  $\mathbf{S}$ :  $gp(\mathbf{S}) = p(g\mathbf{S})$  para todo  $g$  en  $\Gamma$ , es decir, el patrón inducido por  $g\mathbf{S}$  es sólo el patrón inducido por  $\mathbf{S}$  y traducido por  $g$ .

Esto concluye nuestro resumen sobre aleatoriedad. He descrito desde un punto de vista abstracto nuestra teoría sobre aleatoriedad en el estado en que se encuentra actualmente. Mi objetivo es el de hacer explícitas las intuiciones calladas que motivan los ejemplos en las secciones 4 y 5. Con esta exposición abstracta en la mano, quiero ahora enfocarme en las acciones de grupo y argumentar que pueden ser usadas para extender nuestra noción sobre aleatoriedad. Una intuición primaria sobre aleatoriedad es la idea de mezclar. Un set de cartas, por ejemplo, no es “aleatorio” hasta que ha sido barajado completamente, es decir, hasta que las cartas han sido adecuadamente mezcladas.<sup>19</sup> En teoría ergódica uno considera transformaciones de mezclado que toman distintos eventos y los unen de forma que sean probabilísticamente independientes.<sup>20</sup> En ambos ejemplos, aparecen consideraciones probabilísticas, haciendo imposible el hablar de un objeto fijo dado como objeto aleatorio de la forma en que estoy proponiendo. Pero las intuiciones aquí son fuertes, y vale la pena considerar como esas intuiciones pueden trabajar para nosotros.

Por el momento pensemos en un grupo  $\Gamma$  como una bolsa de artefactos para mezclar cosas. Para ser concretos, uno puede imaginar una colección de mezcladoras. Algunas de las mezcladoras no funcionan bien, de modo que no logran un mezclado efectivo. Algunas sólo pueden cortar y pulverizar. Otras pueden licuar. Pero las mezcladoras que son mejores al mezclar son las que tienen fuerza industrial que operan a 20,000 rpm. De forma similar, los elementos de  $\Gamma$  variarán en que tan bien se mezclan bajo una acción de grupo. Por ejemplo, la identidad  $\omega$  será completamente inútil para mezclar cosas. A lo largo de estas contemplaciones no tomo en cuenta los objetos que  $\Gamma$  está mezclando. Al final queremos que  $\Gamma$  mezcle al espacio candidato  $\Omega$ . Pero por ahora estoy interesado en establecer criterios objetivos sobre que tan bien los elementos de  $\Gamma$  se mezclan, independientemente de cual espacio  $\Gamma$  esté actuando. Suponga que este es el caso –suponga que podemos enlistar a los elementos de  $\Gamma$  de acuerdo a lo bien que se mezclen. Además, asumamos que sea lo que sea que queramos decir por mezclar en  $\Gamma$ , esta noción está bien definida y es intuitivamente plausible. En particular, nuestras intuiciones para mezclar y la aleatoriedad deben corresponder. ¿Cómo entonces podemos explotar las propiedades de mezclado inherentes en  $\Gamma$  para extender nuestra teoría sobre aleatoriedad?

Para ser concretos, imaginemos una función limitada  $\mu$  del grupo  $\Gamma$  en los reales no negativos  $[0, \infty)$  la cual toma valores más altos conforme los elementos del grupo se mezclen mejor. Por tanto para los elementos  $g$  y  $h$ , si  $\mu(g) < \mu(h)$ , entonces  $h$  es mejor en mezclarse que  $g$ . Dado que  $\mu$  modela la intuición,  $\mu$  obtiene su valor menor en  $\mu(\epsilon)$ , y es simétrica con respecto a la inversión de grupo, es decir,  $\mu(g) = \mu(g^{-1})$  para  $g$  en  $\Gamma$ . Llamemos a  $\mu$  una *medición de mezclado* en  $\Gamma$ .<sup>21</sup> Dado que nuestras intuiciones acerca del mezclado y la aleatoriedad corresponden, queremos especificar esos elementos  $h$  que son los mejores al mezclarse, es decir, aquellos  $h$  para los que  $\mu(h)$  es igual o está muy cerca de

$$\sup_{g \in \Gamma} \mu(g). \tag{6.1}$$

Observar que este máximo existe mientras que se asuma que  $\mu$  está limitado. Con una medición de mezclado como  $\mu$ , el problema de encontrar a las mejores mezcladoras en  $\Gamma$ , si usted quiere, se convierte en un problema directo de optimización.<sup>22</sup>

Suponga ahora que hemos resuelto el problema de optimización y encontrado un elemento de  $\Gamma$  mezclado óptimamente, llamémoslo  $h$ . Suponga además que  $\Gamma$  está actuando en el espacio candidato  $\Omega$ . Nuestra tarea es encontrar un elemento aleatorio en  $\Omega$  (tomado aleatoriamente en su sentido intuitivo sin una referencia explícita hacia patrones aún). ¿Cómo lo haremos? Un primer intento algo ingenuo puede ser el de tomar un candidato aleatorio  $\omega$ , aplicarle  $h$  y llamar al resultado  $h\omega$  aleatorio. Pero esto presenta un problema: si  $\omega$  es (intuitivamente) no aleatorio y  $\omega'$  es igual a  $(\omega)$ , entonces  $h\omega'$  es sólo el no aleatorio  $\omega$ . Por este truco, cualquier elemento  $h$  óptimamente mezclado tiene imágenes bajo la acción de grupo que son no aleatorias. Aún de forma sorprendente, este truco indica una forma de usar  $h$  para obtener elementos aleatorios de  $\Omega$ . Si podemos encontrar un candidato  $w$  que es intuitivamente lo más no aleatorio posible, y si aplicamos un elemento mezclado





rompimiento o la explosión de esta estructura.<sup>25</sup> Por ejemplo,  $\{1, 2, 3, 100\}$  posee una estructura métrica  $d$  dada por el valor absoluto de la diferencia:  $d(m,n) = |mn|$ . Uno se puede imaginar una permutación  $g$  en  $\Gamma$  explotando la estructura métrica  $d$  si acerca a  $m$  y  $n$  (resp. lejos) y los manda a números lejanos (resp. cerca), es decir, si  $d(m,n)$  es pequeña (resp. grande), entonces  $d(gm,gn)$  es grande (resp. pequeño). Esta propiedad explosiva puede ser capturada por la siguiente medición de mezclado

$$\xi(g) = \sum_{1 \leq m < n \leq 100} \left[ \frac{d(gm, gn)}{d(m,n)} + \frac{d(m,n)}{d(gm, gn)} \right], \quad (6.3)$$

la cual define  $\xi$  para toda  $g$  en  $\Gamma$ .<sup>26</sup>  $\xi$  es mínima en la identidad  $\epsilon$  y se hace grande precisamente para esas  $g$  que rompen la estructura métrica. Un elemento de grupo íntimamente mezclado  $h$  de acuerdo con esta medida de mezclado es un que satisfice

$$\xi(h) = \sup_{g \in \Gamma} \xi(g). \quad (6.4)$$

Aún pueden proponerse otras mediciones de mezclado. En  $\{1,2,3,100\}$  considere la métrica  $d\zeta(m,n) = \min(|mn|, 100|mn|)$ . Esta medida alternativa en  $\{1,2,3,100\}$  trata a los números naturales entre 1 y 100 como puntos uniformemente distribuidos alrededor de un círculo. Con esta medición 1 y 100 son adyacentes. En la ecuación (6.3), si sustituimos  $d$  por  $d\zeta$  obtenemos una medición de mezclado alternativa, la que podemos denotar como  $\zeta$ . Pueden introducirse otras modificaciones también. El grupo  $\Gamma$  puede incluir un subconjunto  $\Delta$  que a nosotros nos gustaría definitivamente excluir de consideración como elementos de mezclado. Por tanto en  $\Gamma (= \mathbf{S}_{100})$  quisiéramos excluir permutaciones con ciertas estructuras cíclicas. En este caso encontrar elementos de grupo óptimamente mezclados en  $\Gamma$  exige encontrar valores supremos para  $\tau$ ,  $\xi$  y  $\zeta$  sobre el juego reducido  $\Gamma\Delta$ .

Es evidente que cualquier promedio ajustado (combinación lineal convexa) de mediciones de mezclado en un grupo dado es otra vez una medida de mezclado. Por tanto podemos combinar las mediciones de mezclado  $\tau$ ,  $\xi$  y  $\zeta$  en una super-medición  $w_1\tau + w_2\xi + w_3\zeta$ , donde las proporciones son números reales positivos que suman 1. La forma en que las proporciones deben elegirse dependerá de la importancia relativa de las mediciones  $\tau$ ,  $\xi$  y  $\zeta$  con respecto al mezclado, de la misma forma que los tamaños relativos de las mediciones de mezclado ( $\xi$  es siempre por lo menos  $n^2 - n$  mientras que  $\tau$  nunca es más que  $n$ ). Habiendo escogido las mediciones de mezclado, las proporciones, y el juego  $\Delta$  con cuidado, ahora buscamos un  $h$  en  $\Gamma$  que satisfaga

$$w_1\tau(h) + w_2\xi(h) + w_3\zeta(h) = \sup_{g \in \Gamma - \Delta} [w_1\tau(g) + w_2\xi(g) + w_3\zeta(g)] \quad (6.5)$$

y por tanto transforme un número intuitivamente aleatorio  $\omega$  en uno intuitivamente no aleatorio  $h\omega$ . Por supuesto,  $\omega$  será formalmente aleatorio con respecto a  $F(\omega)$ , mientras que  $h\omega$  será formalmente aleatorio con respecto a  $F(h\omega) = hF(\omega)$ . Esto concluye el ejemplo.

Al cerrar esta sección quiero decir una palabra respecto a la construcción de mediciones de mezclado, y más generalmente acerca de los criterios para los elementos de grupo óptimamente mezclados. Mi enfoque en el ejemplo pasado fue estrictamente ad hoc -imaginé propiedades que pensé que elementos de grupo óptimamente mezclados debían poseer para el grupo dado  $\Gamma$ , y luego construí mediciones de mezclado para modelar dichas propiedades. Tales mediciones de mezclado establecen los criterios para un mezclado óptimo. Qué tan buenos son esos criterios, qué tan bien hechos pueden ser, y cómo implementar esos criterios computacionalmente son preguntas que dejo para otra ocasión. En el ejemplo precedente ni siquiera he computado un  $h$  óptimamente “explosivo” en línea con (6.3). La solución a estos problemas no es directa y requiere un análisis más profundo que lo que es posible en este artículo expositivo. Aún así, espero haber convencido al lector no sólo de que los grupos pueden poseer propiedades intrínsecas de mezclado relevantes a la aleatoriedad, sino también de que estas propiedades de mezclado pueden ser efectivamente especificadas.

## 7. *Posdata filosófico*

¿Qué ha pasado con la alegación de von Neumann sobre el pecado? Francamente ha perdido su sazón. La redefinición es siempre una forma efectiva de alterar estructuras morales, y el caso presente no es la excepción. La consciencia de culpabilidad de von Neumann se derivó de una paradoja: sistemas determinísticos modelaban sistemas aleatorios, y por tanto, los sistemas aleatorios en la medida en que fueran modelados por sistemas determinísticos por definición no podrían ser aleatorios. En esta paradoja von Neumann combinó la aleatoriedad con el azar. Con esta identificación la paradoja es de hecho no tiene solución. Pero cuando la aleatoriedad es redefinida en términos de romper patrones, la paradoja desaparece. Cuestiones de determinismo, azar y probabilidad no tienen cabida. El problema ahora es si un objeto existe y si puede encontrarse que rompe los patrones.

Algo parecido a la revolución copérmica de Kant está pasando aquí. Ciertamente no intento colocar este ensayo en compañía de la primera *Crítica* de Kant. Pero hay un paralelo en la forma en que la revolución de Kant cambió la relación entre el objeto y el conocimiento, y la forma en que mi redefinición cambió la relación entre objeto aleatorio y patrón. Antes a Kant el conocimiento se había conformado al objeto con el objeto casualmente influenciando el conocimiento. Pero con Kant (1927, p. 22) los objetos deben en adelante adecuarse al conocimiento. Como Allison (1983, p. 30) observa,

El punto a ser enfatizado es si este “punto de vista cambiado” trae con él una concepción radicalmente nueva de un objeto. Un objeto debe ahora ser entendido como lo que sea que se adecue a nuestro conocimiento, y esto... significa cualquier cosa que se adecue a las condiciones de la mente (ambas sensible e intelectual) para la representación de ella como un objeto. Consecuentemente, un objeto es por su misma naturaleza algo representado...

Similarmente, los objetos aleatorios de los que hablo representan un punto de vista cambiado. En tiempos pasados, los objetos aleatorios eran aleatorios porque imitaban al azar. Eran falsificaciones. Mientras que la falsificación pareciera plausible, uno podría decir

que eran el producto del azar. Pero la tecnología para descubrir estas falsificaciones fue siempre mejorando. La prueba estadística más reciente siempre era una amenaza para descubrir al “bien establecido” objeto aleatorio. Sin embargo, dentro de este nuevo marco conceptual, las “condiciones para la posibilidad” de tales objetos, para usar una frase kantiana, de ahora en adelante descansan con los patrones que juzgan a estos objetos como aleatorios, y no con los objetos mismos. Los patrones se convierten estrictamente en anteriores a los objetos aleatorios. Sin patrones, los objetos son sólo objetos, no objetos aleatorios.

## REFERENCIAS

- [1] Allison, Henry E., *Kant's Transcendental Idealism* (New Haven, Conn.: Yale University Press, 1983).
- [2] Bauer, Heinz, *Probability Theory and Elements of Measure Theory* (London: Academic Press, 1981).
- [3] Chaitin, Gregory J., *Algorithmic Information Theory* (Cambridge: Cambridge University Press, 1987).
- [4] Church, Alonzo, "On the Concept of a Random Sequence," *Bulletin of the American Mathematical Society* 46 (1940): 130–35.
- [5] Dembski, William A., "Uniform Probability," *Journal of Theoretical Probability* 3(4) (1990): 611–26.
- [6] Diaconis, Persi, "On the Statistics of Vision: The Julesz Conjecture," *Journal of Mathematical Psychology* 24 (1981): 112–38.
- [7] ———, *Group Representations in Probability and Statistics* (Hayward, Calif.: Institute of Mathematical Statistics, 1988).
- [8] Garey, Michael R. and David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (New York: Freeman, 1979).
- [9] Goldreich, Oded, Shafi Goldwasser and Silvio Micali, "How to Construct Random Functions," *Journal of the Association for Computing Machinery* 33(4) (1986): 792–807.
- [10] Hungerford, Thomas W., *Algebra* (New York: Springer-Verlag, 1974).
- [11] Kant, Immanuel, *Critique of Pure Reason*, translated by N. K. Smith (New York: St Martin's, 1929).
- [12] Knuth, Donald E., *Seminumerical Algorithms*, 2nd ed., in *The Art of Computer Programming*, vol. 2 (Reading: Addison-Wesley, 1981).

- [13] Kolmogorov, Andrei N., *Foundations of the Theory of Probability* (New York: Chelsea, 1950).
- [14] ———, “On Tables of Random Numbers,” *Sankhya* (The Indian Journal of Statistics: Series A) 25(4) (1965a): 369–76.
- [15] ———, “Three Approaches to the Quantitative Definition of Information,” *Problemy Peredachi Informatsii* (in translation) 1(1) (1965b): 3–11.
- [16] Kolmogorov, Andrei N. and V. A. Uspensky, “Algorithms and Randomness,” *SIAM Theory of Probability and Applications* 32 (1988): 389–412.
- [17] Kranakis, Evangelos, *Primality and Cryptography* (Stuttgart: Wiley-Teubner, 1986).
- [18] Lasota, Andrzej and Michael C. Mackey, *Probabilistic Properties of Deterministic Systems* (Cambridge: Cambridge University Press, 1985).
- [19] Martin-Löf, Per, “The Definition of Random Sequences,” *Information and Control* 9 (1966a): 600–619.
- [20] ———, “Algorithmen und zufällige Folgen,” four lectures delivered at the Mathematical Institute of the Erlangen-Nürnberg University, 1966b.
- [21] Mises, Richard von, *Wahrscheinlichkeit, Statistik und Wahrheit* (Vienna: Springer-Verlag, 1936).
- [22] Parthasarathy, K. R., *Probability Measures on Metric Spaces* (New York: Academic Press, 1967).
- [23] van Lambalgen, Michiel, “Algorithmic Information Theory,” *Journal of Symbolic Logic* 54(4) (1989): 1389–1400.
- [24] ———, “The Axiomatization of Randomness,” *Journal of Symbolic Logic* 55(3), (1990): 1143–67.
- [25] Weihrauch, Kurt, *Computability* (Berlin: Springer-Verlag, 1987).
- [26] Wilder-Smith, A. E., *Man's Origin, Man's Destiny* (Minneapolis, Minn.: Bethany House, 1975).
- [27] Yao, Andrew C., “Theory and Applications of Trapdoor Functions,” *Twenty-third IEEE Symposium on Foundations of Computer Science* (Foundations of Computer Science) (1982): 80–91.

## NOTAS

1 Citado en Knuth (1981, p.1). Es sorprendente como esta casi ligera observación ha sido elevada al nivel de dogma. Además de su estado canónico, esta observación funciona como una de las bromas locales del archivo de los científicos computacionales.

2 Estos comentarios se derivan de la Conferencia Interdisciplinaria sobre la Aleatoriedad en la Ohio State University, 11-16 de Abril de 1988. Este evento fue significativo por reunir a filósofos, matemáticos, psicólogos, científicos computacionales, físicos y estadísticos a compartir sus pensamientos sobre la aleatoriedad. En referencia a este evento usaré las iniciales *ICR*.

3 La fraseología aquí puede parecer al lector como antinatural, porque violar un patrón es igualado a pasar una prueba estadística. Las dos nociones de hecho corresponden: el pasar una prueba estadística es la salida normal esperada; sólo cuando sucede algo inusual esperamos que falle una prueba estadística. El que un evento aleatorio se ajuste a un patrón es inusual; cualquier patrón se piensa que es suficientemente restrictivo de tal forma que romper el patrón se convierte en la salida normal, esperada.

4 Precisamente dado que las pruebas estadísticas abundan y pueden descalificar a cualquier secuencia supuestamente aleatoria, la noción no calificada de von Mises de los colectivos fundó –ninguna secuencia infinita mantiene las frecuencias correctas sobre todas las subsecuencias. Ver von Mises (1936).

5 Para la ley fuerte sobre los grandes números ver Bauer (1981, p. 172); para una mirada poco convencional sobre los simios de Huxley ver Wilder-Smith (1975, p.63).

6 Este ejemplo inspira una revisión masiva del sistema de justicia criminal: con el requerimiento de que todos los giros de la moneda sean justos y se hayan registrado debidamente, sentenciar a un criminal convicto a servir tiempo en prisión hasta que obtenga  $n$  giros seguidos, donde  $n$  es seleccionado de acuerdo a la severidad de la ofensa. Por tanto, para una sentencia de 10 años en prisión, si asumimos que el prisionero puede hacer girar una moneda una vez cada cinco segundos (esto parece razonable), ocho horas al día, seis días a la semana, y dado que el intento promedio para obtener una secuencia de  $n$  soles antes de águilas es  $2^{n+1}$ , entonces él en promedio intentará obtener una cadena de  $n$  soles una vez cada 10 segundos, o 6 intentos por minuto, o 360 intentos por hora, o 2880 intentos en un día de ocho horas de trabajo, o 901440 intentos en un año (asumiendo una semana de trabajo de seis días), o aproximadamente 9 millones de intentos en 10 años. 9 millones es aproximadamente 223. Por tanto si requiriéramos que un prisionero obtuviera 23 soles seguidos antes de ser liberado, podríamos esperar verlo libre en aproximadamente 10 años. Por supuesto que los casos específicos variarían y algunos prisioneros saldrían libres sólo después de una pequeña estancia, y algunos otros nunca obtendrían los elusivos 23 soles!

7 Hay algunos teoremas profundos de isomorfismo sobre espacios pulidos, en los cuales el espacio que modela el girar de la moneda es un ejemplo clave. La mayor parte de la teoría de probabilidad moderna puede ser ajustada al marco conceptual abstracto provisto por espacios pulidos. La razón por la que el girar monedas es fundamental es porque todos los

espacios pulidos son (Borel) isomórficos uno con respecto al otro, y por tanto también con respecto al espacio que modela el giro de una moneda. Ver Parthasarathy (1967, pp. 7-15).

8 Dado que las reglas de la evidencia en la corte requieren una historia causal para condenar a un individuo y no en meras improbabilidades, es concebible que un abogado defendería al administrador de la lotería apelando a la probabilidad infinitamente pequeña de “las cosas simplemente sucedieron así” – después de todo, cualquier cosa es posible. Pero con improbabilidades severas del tipo descrito las historias causales generalmente están inmediatamente disponibles. Por ejemplo, una investigación del mecanismo de azar de la lotería puede bien indicar un ajuste por parte del administrador de la lotería.

9 Esto no es para negar que el trabajo de Kolmogorov y Martin-Löf en los 60s ha dejado de inspirar a los matemáticos. Tanto en lógica (ver van Lambalgen, 1989 y Chaitin, 1987) y en propiedades de aleatoriedad (ver Kolmogorov y Uspensky, 1988 y van Lambalgen, 1990) sus ideas continúan dando fruto. Pero en la raíz de ambos enfoques tanto de complejidad tiempo-espacio sobre aleatoriedad es un marco de trabajo teórico de repetición donde la aleatoriedad existe sólo como límite, permitiendo cadenas arbitrariamente largas, programas arbitrariamente largos y tiempos de corrida arbitrariamente largos.

10 Esto es realmente una apelación a la tesis de Church, es decir, la afirmación de que la computabilidad matemática e intuitiva coinciden. Ver Weihrauch (1987, p. 87).

11 Ver Knuth (1981, p. 27) para sus observaciones generalmente brillantes sobre el generador aditivo de números. El desafecto de Marsaglia con este generador fue publicado en *ICR*.

12 Por métodos determinísticos quiero decir métodos que son obviamente determinísticos, como el correr un programa computacional. El girar una moneda es determinístico en el sentido de que la mecánica newtoniana ofrece predicciones precisas y exactas. Sin embargo, yo tomo el girar monedas como el paradigma del azar e ignoro cualquier determinismo subyacente.

13 Estoy asumiendo el modelo probabilístico estándar para el girar de una moneda: el espacio producto infinito de  $\{0,1\}$  junto con la medición uniforme del producto.

14 Puede parecer contraintuitivo el hablar de  $w$  como el romper el patrón inducido por  $S$  si esta desigualdad es satisfecha. Sin embargo, la intuición subyacente deriva de la probabilidad de girar una moneda la cual dicta que  $w$  debería estar distribuida uniformemente si es aleatoria. Dado que hemos definido la aleatoriedad como el romper patrones, para que  $w$  satisfaga la desigualdad (5.2) debe por tanto estar identificada con el rompimiento de un patrón. Este punto es estrictamente una cuestión de terminología. Ver también la nota 3.

15 El número en (5.8) es esencialmente el recíproco de la probabilidad limitada en la ley de Bernstein de los grandes números, una aguda desigualdad combinatoria que sale de la distribución binomial –ver Kranakis (1986, p. 94).

16 Compare esto con el enfoque tiempo-complejidad a la aleatoriedad para el cual las funciones tiempo-polinomial son insuficientes para distinguir la pseudo-aleatoriedad de

aleatoriedad genuina. En el presente ejemplo una secuencia potencialmente aleatoria de longitud  $n$  debe ser confrontada contra una colección de patrones cuya cardinalidad es exponencial en  $n$ , no meramente polinomial en  $n$ .

17 Debería enfatizar que después de todo que estoy tras una teoría matemática sobre aleatoriedad, no una perceptual. Aún así, estas son paralelas –ver Diaconis (1981).

18 Ver Hungerford (1974, pp. 88-92) para más detalles.

19 El estadístico Persi Diaconis, un organizador clave de ICR, ha hecho un trabajo significativo en el área de acciones de grupo y aleatoriedad. Al mismo tiempo un mago y un estadístico profesional, ha obtenido resultados en las matemáticas del barajado de cartas (lo cual no es nada más que una acción de grupo disfrazada) lo cual ha traído recientemente a él y a su colega Dave Bayer al ojo público (ver *Time Magazine*, 22 Enero 1990, p. 62). Sus hallazgos generales eran que 7 barajadas eran necesarias para llevar un mazo de cartas de un estado no aleatorio a uno aleatorio. Ver Diaconis (1988) para su enfoque general sobre aleatoriedad via grupos. Permítame enfatizar que su enfoque es fundamentalmente probabilístico.

20 Ver Mackey y Lasota (1985, pp. 63-65) para algunas fotografías impactantes generadas por computadora que refuerzan las intuiciones abstractas que motivan la teoría ergódica.

21 Las mediciones de mezclado no son mediciones en el sentido de funciones aditivas contables de juego. En lugar de eso, son funciones en un grupo cuyos extremos proveen elementos de grupo óptimamente mezclados.

22 Por lo menos conceptualmente tales problemas de optimización son directos. En la práctica pueden ser difíciles.

23 Esto surge directamente de la descomposición de la estructura cíclica de las permutaciones. Ver Hungerford (1974, pp. 46-51).

24 La permutación  $(1\ 2\ 3\ 100)$  puede ser expresada más brevemente como el producto de 99 transposiciones:  $(1\ 2)(1\ 3)(1\ 4)(1\ 100)$ .

25 Esto es claramente evocador del rompimiento de patrones en la aleatoriedad, pero hay algunas diferencias.

26 Esta sumatoria tiene una formulación como integral para espacios métricos compactos usando probabilidades (semi-) uniformes. Ver Dembski (1990) para el uso apropiado de mediciones en la integración.

---

## Limitaciones de Reproducción/Copyright

A menos de que sea precedido por otro copyright en el texto del artículo previo, este documento es propiedad solamente de **Leadership U**. No puede ser alterado o editado de ninguna forma. Puede ser reproducido solamente de forma completa para su circulación como “programa de libre acceso”, sin cargo alguno. Todas las reproducciones de este archivo y/o documento deben contener el aviso de Copyright (es decir, *Copyright © 1995-2002 Leadership U*) y este aviso de limitación de copyright/reproducción.

Este archivo/documento no puede ser usado sin el permiso de **Leadership U.**, para reventa o el mejoramiento de algún otro producto vendido.

El contenido de algunos archivos también está protegido bajo *copyrights* adicionales.