AzaR y AutómataS

Verónica Becher

Grupo KAPOW (Knowledgeable Algorithms for Problems on Words)
Departamento Computación, Facultad de Ciencias Exactas y Naturales, UBA
Laboratoire International Associé INFINIS Université Paris Diderot-CNRS/UBA-CONICET

Octubre 2017

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los “juegos de azar” o con la “suerte”. . .

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los “juegos de azar” o con la “suerte”...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los “juegos de azar” o con la “suerte”...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

- ¿Definición matemática de azar?

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los "juegos de azar" o con la "suerte"...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

- ¿Definición matemática de azar?
- ¿Hay grados de azar?

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los "juegos de azar" o con la "suerte"...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

- ¿Definición matemática de azar?
- ¿Hay grados de azar? ¿Hay anti-azar?

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los "juegos de azar" o con la "suerte"...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

- ¿Definición matemática de azar?
- ¿Hay grados de azar? ¿Hay anti-azar?
- ¿Puede una computadora producir una secuencia realmente al azar? ¿Ejemplos?

Azar - aléatoire - Zufall - rasgelelik - satunnaisuuden - slumpmässighet - randomness - aleatorietà

Todos tenemos una idea intuitiva acerca de lo que es el azar; una idea muchas veces relacionada con los "juegos de azar" o con la "suerte"...

En castellano azar y aleatoriedad son sinónimos. En adelante diré azar.

- ¿Definición matemática de azar?
- ¿Hay grados de azar? ¿Hay anti-azar?
- ¿Puede una computadora producir una secuencia realmente al azar? ¿Ejemplos?
- ¿Podemos garantizar azares independientes?

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111...

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗

01001000100001000001000000100000001...

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗
01001000100001000001000000100000001... ✗

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗
01001000100001000001000000100000001... ✗

00101001010001101110100010010101111...

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗

01001000100001000001000000100000001... ✗

00101001010001101110100010010101111... ✓

La suerte es loca

Azar es no poder distinguir entre la secuencia y echar una moneda para cada posición.

11111111111111111111111111111111111... ✗
01001000100001000001000000100000001... ✗

00101001010001101110100010010101111... ✓

Azar es imposibilidad de predecir, es falta de patrón.

Azar es imposibilidad de predecir

Entonces cara y ceca deben ocurrir con la misma frecuencia, en el límite,

Azar es imposibilidad de predecir

Entonces cara y ceca deben ocurrir con la misma frecuencia, en el límite, sino, ¡ podríamos predecir!.

Azar es imposibilidad de predecir

Entonces cara y ceca deben ocurrir con la misma frecuencia, en el límite, sino, ¡ podríamos predecir!.

Y lo mismo vale para combinaciones de caras y cecas.

Esta es la propiedad más básica del azar.

Definición matemática de azar

Azar es imposibilidad de predecir.

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

¿Un ser humano?

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

¿Un ser humano?
¿Una computadora? (máquina de Turing universal)

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

¿Un ser humano?
¿Una computadora? (máquina de Turing universal)
¿Un algoritmo de complejidad polinomial?

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

¿Un ser humano?
¿Una computadora? (máquina de Turing universal)
¿Un algoritmo de complejidad polinomial?
¿Un autómata de pila?

Definición matemática de azar

Azar es imposibilidad de predecir.
Equivalentemente, azar es imposibilidad de abreviar.
Pero . . . ¿Para quién?

¿Un ser humano?
¿Una computadora? (máquina de Turing universal)
¿Un algoritmo de complejidad polinomial?
¿Un autómata de pila?
¿Un autómata finito?

Definición matemática de azar

Definición

Fijemos una alfabeto. Sea $\mathcal{C}$ una clase de autómatas. Una secuencia x de símbolos es azarosa para la clase $\mathcal{C}$ si ningún automata de $\mathcal{C}$ comprime x.

Es decir,

Una secuencia es azarosa repecto de la clase de autómatas $\mathcal{C}$ cuando, esencialmente, la única forma de describirla mediante un atómata de $\mathcal{C}$ es explicitamente.

Grados de azar

Distintos modelos de cómputo tienen distintas capacidad de resolver problemas. Por ejemplo:

Grados de azar

Distintos modelos de cómputo tienen distintas capacidad de resolver problemas. Por ejemplo:

Máquinas de Turing

Grados de azar

Distintos modelos de cómputo tienen distintas capacidad de resolver problemas. Por ejemplo:

Máquinas de Turing
Autómatas de pila

Grados de azar

Distintos modelos de cómputo tienen distintas capacidad de resolver problemas. Por ejemplo:

Máquinas de Turing
Autómatas de pila
Autómatas finitos

Grados de azar

Azar puro: incompresibilidad mediante máquinas de Turing.

Grados de azar

Azar puro: incompresibilidad mediante máquinas de Turing.

Azar básico: incompresibilidad mediante autómatas finitos.

Grados de azar

Azar puro: incompresibilidad mediante máquinas de Turing.

Azar básico: incompresibilidad mediante autómatas finitos.

¿Azar intermedio: incompresibilidad mediante autómatas de pila?

Azar puro

Per Martin Löf, 1965, tests algorítmico de no aleatorieadad :
Azar es pasar todos los tests algoritmicos en base máquinas de Turing.

Azar puro

Per Martin Löf, 1965, tests algorítmico de no aleatorieadad :
Azar es pasar todos los tests algoritmicos en base máquinas de Turing.

Gregory Chaitin, 1975, medida de incompresibilidad algorítmica:
Azar es casi máxima incompresibilidad por máquinas de Turing.

Azar puro

Per Martin Löf, 1965, tests algorítmico de no aleatorieadad :
Azar es pasar todos los tests algoritmicos en base máquinas de Turing.

Gregory Chaitin, 1975, medida de incompresibilidad algorítmica:
Azar es casi máxima incompresibilidad por máquinas de Turing.

Teorema (Schnorr 1975)

Las secuencias azarosas segun Martin-Löf son exactamente las secuencias incompresibles mediante máquinas de Turing.

¿Puede una computadora producir azar puro?

¿Puede una computadora producir azar puro?

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."

John von Neumann, 1951

¿Puede una computadora producir azar puro?

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin."

John von Neumann, 1951 (cita Knuth, The Art of Computing Programming)

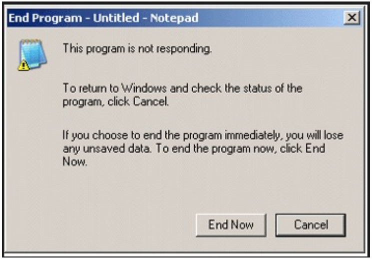
Examples of random sequences

Examples of random sequences

¿Te pasó que se te cuelga la computadora?

Examples of random sequences

¿Te pasó que se te cuelga la computadora?



Ω-numbers

Teorema (Chaitin 1975)

La probabilidad de que una computadora universal no se cuelgue,
$\Omega = \sum_{U(p) halts} 2^{-|p|}$, *is puramente aleatoria.*

Ω-numbers

Teorema (Chaitin 1975)

La probabilidad de que una computadora universal no se cuelgue,
$\Omega = \sum_{U(p) halts} 2^{-|p|}$*, is puramente aleatoria.*

Las probabilidades de otros comportamientos también

Becher,Chaitin, Daicz 2001; Becher, Chaitin 2003; Becher,Grigorieff 2005,2009:

Becher,Figueira,Grigorieff,Miller 2006; Barmpalias 2016,2017

Azar básico

Azar básico

Émile Borel, 1900, normalidad:
Azar es equifrequencia de todos los bloques de igual longitud.

Azar básico

Émile Borel, 1900, normalidad:
Azar es equifrequencia de todos los bloques de igual longitud.

Teorema (Schnor, Stimm 1972; Dai,Lothrup,Lutz,Mayordomo 2004; Becher, Heiber 2013: Becher, Heiber, Carton 2015: Carton, Heiber 2015)

Las secuencias normales son exactamente las secuencias incompresibles mediante autómatas finitos (transductores uno a uno).

Azar básico

Émile Borel, 1900, normalidad:
Azar es equifrequencia de todos los bloques de igual longitud.

Teorema (Schnor, Stimm 1972; Dai,Lothrup,Lutz,Mayordomo 2004; Becher, Heiber 2013: Becher, Heiber, Carton 2015: Carton, Heiber 2015)

Las secuencias normales son exactamente las secuencias incompresibles mediante autómatas finitos (transductores uno a uno).

Proposición (Boasson 2014)

Hay secuencias normales compresibles mediante autómatas de pila no determinísticos.

Azar básico

Émile Borel, 1900, normalidad:
Azar es equifrequencia de todos los bloques de igual longitud.

Teorema (Schnor, Stimm 1972; Dai,Lothrup,Lutz,Mayordomo 2004; Becher, Heiber 2013: Becher, Heiber, Carton 2015: Carton, Heiber 2015)

Las secuencias normales son exactamente las secuencias incompresibles mediante autómatas finitos (transductores uno a uno).

Proposición (Boasson 2014)

Hay secuencias normales compresibles mediante autómatas de pila no determinísticos.

Problema

¿Hay alguna secuencia normal que se pueda comprimir mediante autómatas de pila determinístico?

¿Ejemplos de números normales?

¿Ejemplos de números normales?

Sí

¿Ejemplos de números normales?

Sí

`http://kapow.dc.uba.ar`

Hace más de 100 años

Teorema (Borel 1909)

Casi todos los números reales son normales en toda base

Problema (Borel 1909)

Dar un ejemplo. Es π normal en alguna base? ¿Y e? ¿Y $\sqrt{2}$?

Hace más de 100 años

Teorema (Borel 1909)

Casi todos los números reales son normales en toda base

Problema (Borel 1909)

Dar un ejemplo. Es π normal en alguna base? ¿Y e? ¿Y $\sqrt{2}$?

Conjetura (Borel 1950)

Los números algebraicos irracionales son normales en toda base.

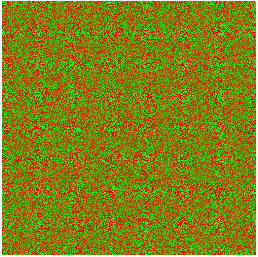
Normal en base 10

Teorema (Champernowne, 1933)

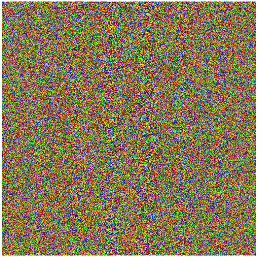
0,12345678910111213141516171819202122232425 26 ... *es normal en base* 10*.*

No se sabe si es normal en bases que no son potencias de 10.

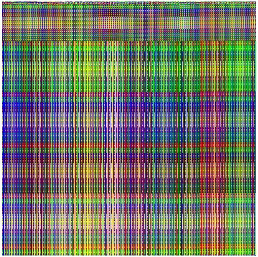
Los primeros 250000 dígitos del número de Champernowne.



base 2



base 6



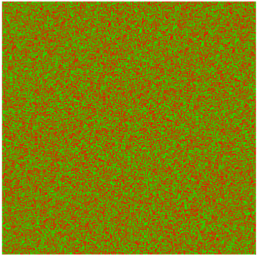
base 10

Normal en una base pero no en otra

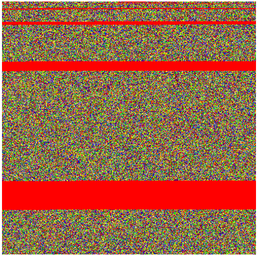
Bailey and Borwein (2012) demostraron que el número Stoneham $\alpha_{2,3}$,

$$\alpha_{2,3} = \sum_{k \geq 1} \frac{1}{3^k \ 2^{3^k}}$$

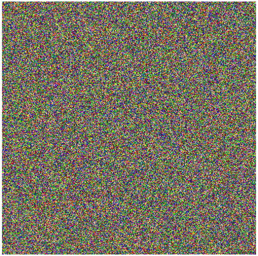
es normal en base 2 pero no es simplmente normal en base 6.



base 2

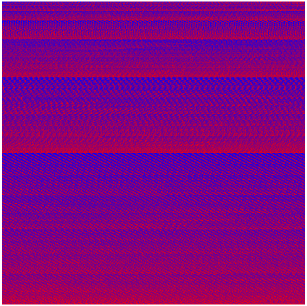


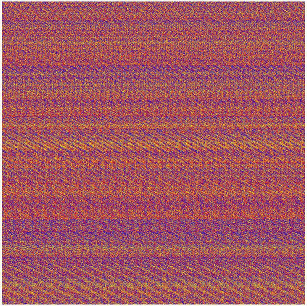
base 6



base 10

Otras normales





de Bruijn lexicográficamente mínima
de orden 1,2, 3 etc.

$x[n] = x[2n]$

Problema

Clasificar las distintas de Bruijn infinitas según su velocidad de convergencia a normalidad.
Computar la secuencias de Levin 1999 y calcular su complejidad computacional

Absolutamente normal

Significa normal en toda base entera mayor o igual que 2.

Absolutamente normal

Significa normal en toda base entera mayor o igual que 2.

Construcciones de Lebesgue and Sierpiński, independientemente, 1917.
No son computables.

Teorema (Turing 1937; Becher, Figueira, Picchi 2007)

Hay un algoritmo que produce un número absolutamente normal.

Otros algoritmos Schmidt 1961/1962; Becher, Figueira 2002, Scheerer 2017; Beche, Heiber Slaman 2016; Aistleitner, Becher, Scheerer, Slaman 2017

Absolutamente normales pero rapidito

Teorema (Lutz,Mayordomo 2013/16;Figueira,Nies 2013;Becher,Heiber,Slaman 2013)

Hay un algoritmo que computa un número abslutamente normal en tiempo polinomial.

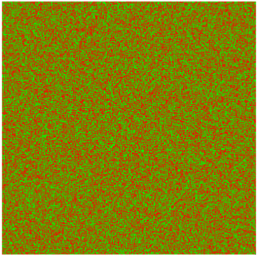
El algoritmo de Lutz, Mayordomo 2016 tiene complejidad polilog lineal.

El algoritmo de Becher, Heiber, Slaman 2013, tiene complejidad apenas arriba de cuadrática, tesis doctoral de Pablo Heiber 2014.

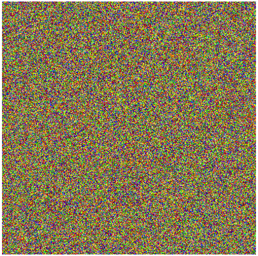
La salida de nuestro algoritmo

Programado por Martin Epszteyn, tesis de licenciatura, 2013.

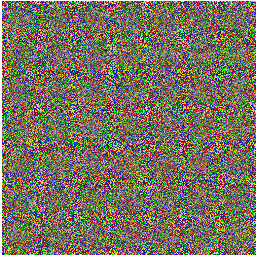
0,4031290542003809132371428380827059102765116777624189775110896366...



base 2



base 6



base10

Números pseudoaleatorios

John Von Neumann 1951. Various techniques used in connection with random digits. *Applied Math Series* 12 (1): 36–38.

National Institute of Standards and Technology
`http://csrc.nist.gov/groups/ST/toolkit/rng/`

`http://www.random.org/`

Problema (para tesis doctoral)

Investigar números pseudoaleatorios normales.

La noción de independencia entre secuencias

Dos secuencias son independientes si ninguna ayuda a comprimir la otra.

La noción de independencia entre secuencias

Dos secuencias son independientes si ninguna ayuda a comprimir la otra.

¡Hoy no tengo tiempo de contarlo!

Investigadores externos

Theodore Slaman, University California Berkeley

Olivier Carton, Université Paris Diderot

Otros temas en KAPOW

- Problemas en secuencias biológicas (proteínas, ADN) ligados a repeticiones, azar y anti-azar. Lidera Pablo Turjanski