AzaR

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

Agosto 2014

Azar, aleatoriedad, "randomness"

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"...

- ¿Definición matemática de azar?

Azar, aleatoriedad, "randomness"

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"...

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

Azar, aleatoriedad, "randomness"

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"...

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

Azar, aleatoriedad, "randomness"

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"...

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

Azar, aleatoriedad, "randomness"

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"...

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

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

11111111111111111111111111111111...

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

11111111111111111111111111111111...

01001000100001000001000000100000001...

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

11111111111111111111111111111111...

01001000100001000001000000100000001...

00101001010001101110100010010101111...

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

11111111111111111111111111111111...

01001000100001000001000000100000001...

00101001010001101110100010010101111...

Azar es imposibilidad de predecir, es falta de patrón.

La suerte es loca

Echando una moneda, escribiendo 0 para cara y 1 para ceca.

11111111111111111111111111111111...

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

para secuencias infinitas o números reales.

- Émile Borel, 1900, números normales
  (azar es equifrequencia de todos los bloques de igual longitud)
- Per Martin Löf, 1965, tests algorítmico de (anti)aleatorieadad
  (azar es pasar todos los tests algoritmicos)
- Gregory Chaitin, 1975, medida de (in)compresibilidad algorítmica.
  (una secuencia aleatoria si la única forma de describirla es explicitamente).
- Martingalas algorítmicas (1975 en adelante).

Grados de azar

Azar básico (normalidad) ..... Azar puro (M.-Löf - Chaitin random)

grados de azar

¿Puede una computadora producir azar?

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

John von Neumann (1951)

Entonces π, e, $\sqrt{2}$ no son puramente aleatorios.

¿Puede una computadora producir azar?

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

John von Neumann (1951)

Entonces π, e, $\sqrt{2}$ no son puramente aleatorios. ¿Son normales?
Esta pregunta está abierta desde el 1900.

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/`

¿Ejemplos de números normales?

¿Ejemplos de números normales?

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

Existencia

Teorema (Borel 1909)

Casi todos los números reales son normales en toda base

Problem (Borel 1909)

Dar un ejemplo.

Conjetura (Borel 1950)

Los números algebraicos irracionales son normales en toda base.

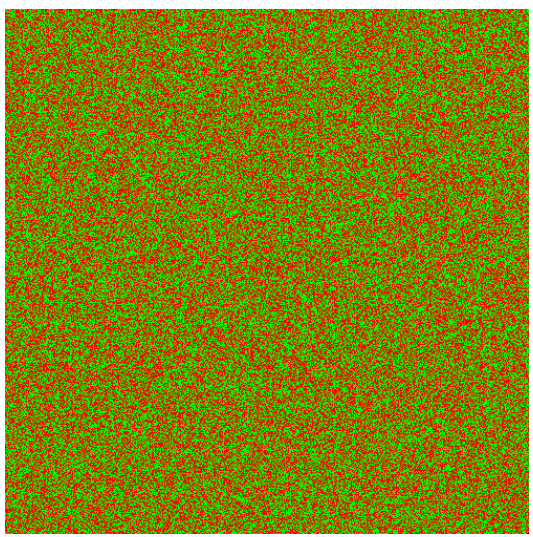
Normal en base 10: Champernowne

Teorema (Champernowne, 1933)

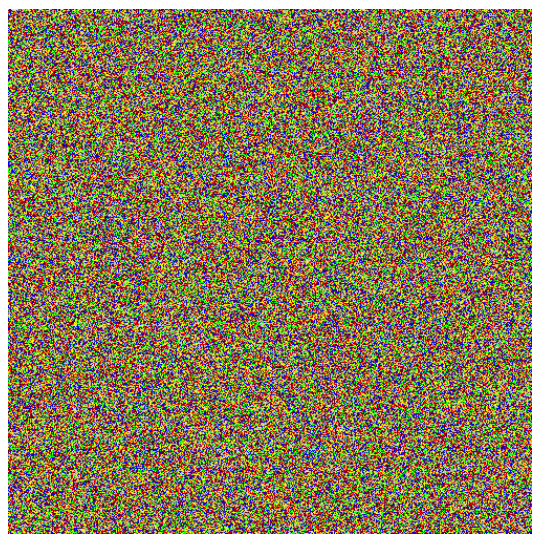
0,12345678910111213141516171819202122232425 . . . *es normal en base* 10.

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

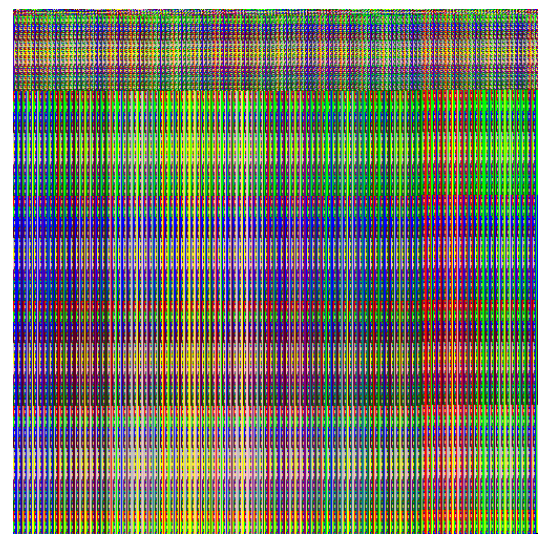
Los primeros 250000 dígitos del número de Champernowne.



base 2



base 6



base 10

Absolutamente normal

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

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

Hay un algoritmo que produce un número absolutamente normal.

Otros algoritmos Schmidt 1961/1962; Becher, Figueira 2002.

Absolutamente normales pero rapidito

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

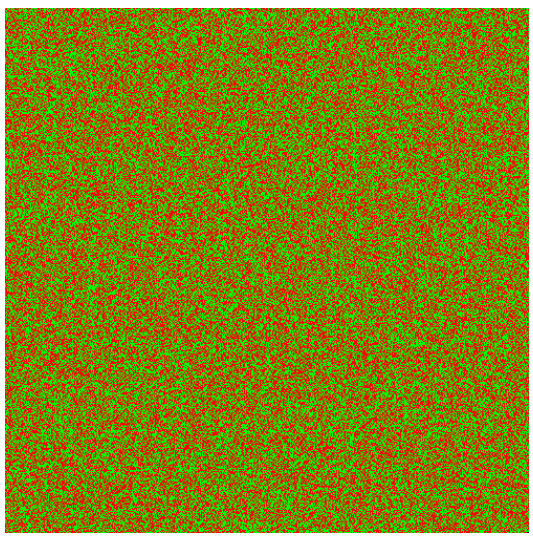
Hay un algoritmo que computa un número abslutamente normal en tiempo polinomial.

El algoritmo de Becher, Heiber, Slaman (2013), que forma parte de la tesis doctoral de Pablo Heiber (2014), tiene complejidad apenas arriba de cuadrática.

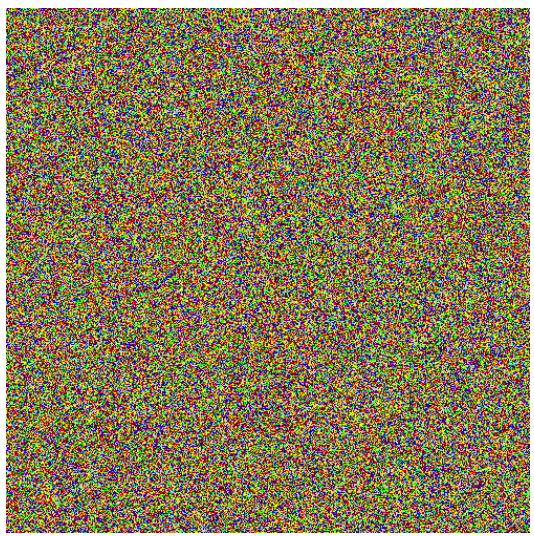
La salida de nuestro algoritmo

Programmed by Martin Epszteyn, tesis de licenciatura, 2013.

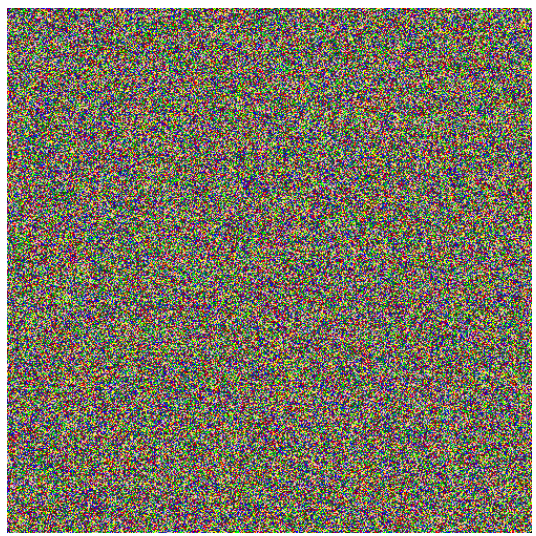
0,403129054200380913237142838082705910276511677762418977511089636 6...



base 2



base 6



base10

Parametros $t_i = (3 * \log(i)) + 3$; $\epsilon_i = 1/t_i$ Initial values $t_1 = 3$; $\epsilon_1 = 1$.

¿Dependencia de normalidad en distintas bases?

Dos números enteros positivos son *multiplicativamente dependientes* si uno es una potencia racional del otro.
Por ejemplo 2 y 8 son dependientes, pero 2 y 6 no.

Teorema (Maxfield 1953)

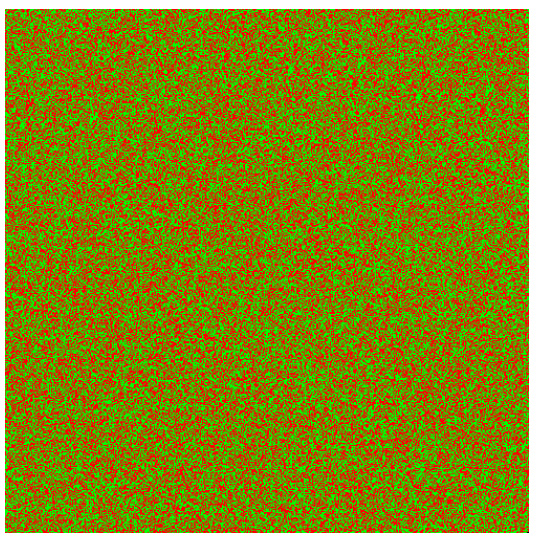
Si dos bases son multiplicativamente dependientes entonces, normalidad en una implica normalidad en la otra.

Normal en una base pero no en otra

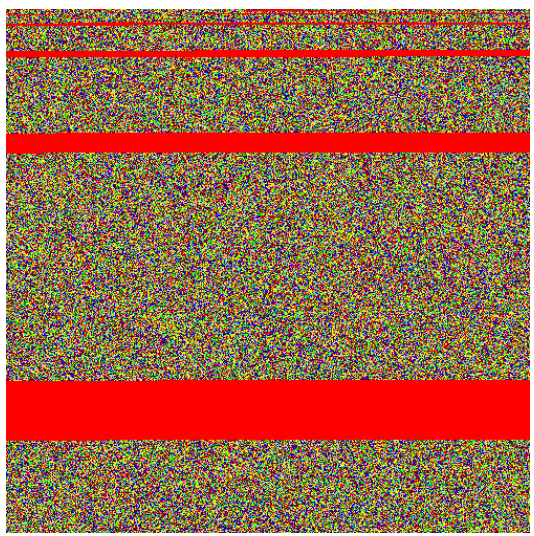
Bailey and Borwein (2012) demostraron que el número Stoneham $\alpha_{2,3}$,

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

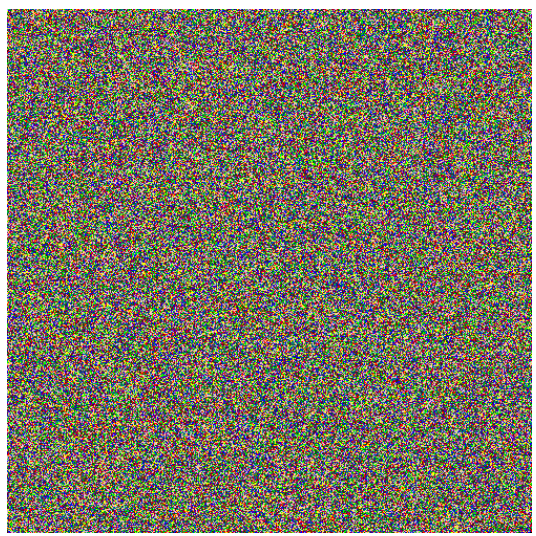
es normal en base 2 pero no es simplmente normal en base 6.



base 2



base 6



base 10

Normal en una base pero no en otra

Teorema (Cassels 1959, Schmidt 1961)

Para cualquier conjunto de bases cerrado por dependencia multiplicativa, hay números que son normales en cada base del conjunto pero no son normales en ninguna base del complemento.

En 2014 Becher y Slaman dimos un algoritmo que produce números normales en una base y no simplemente normales en otra.

Posible tesis de licenciatura

Implementar el algoritmo que produce un número normal en base 2 pero no en base 3.

Simplemente normal en una base pero no en otras

En 2014 Becher, Slaman y Bugeaud dimos condicones necesarias y suficientes para un conjunto de bases para que exista un numero que es simplemente normal exactamente en esas bases.

Posible tesis de licenciatura

Implementar el algoritmo que produce un número simplemente normal exactamente las bases dadas.

Nuevos números normales

En 2014 Becher, Heiber y Slaman dieron un algoritmo para producir un número de Liouville absolutamente normal.

Posible tesis de licenciatura

Implementar el algoritmo que arroja un número de Liouville absolutamente normal.

Secuencias de Bruijn y números normales

Consideremos un alfabeto, por ejemplo $\{0, 1\}$,y una longitud, por ejemplo 3.

Secuencias de Bruijn y números normales

Consideremos un alfabeto, por ejemplo $\{0, 1\}$,y una longitud, por ejemplo 3.

¿Es posible construir una secuencia que tenga toda las palabras distintas de longitud 3 exactamente una vez?

Secuencias de Bruijn y números normales

Consideremos un alfabeto, por ejemplo $\{0, 1\}$,y una longitud, por ejemplo 3.

¿Es posible construir una secuencia que tenga toda las palabras distintas de longitud 3 exactamente una vez? (por lo tanto de longitud $2^3 + 3 - 1$, o sea 10)

Secuencias de Bruijn y números normales

Consideremos un alfabeto, por ejemplo $\{0, 1\}$,y una longitud, por ejemplo 3.

¿Es posible construir una secuencia que tenga toda las palabras distintas de longitud 3 exactamente una vez? (por lo tanto de longitud $2^3 + 3 - 1$, o sea 10)

0001011100

Se llaman secuencias de Bruijn de orden 3.

Secuencias de Bruijn y números normales

Consideremos un alfabeto, por ejemplo $\{0, 1\}$,y una longitud, por ejemplo 3.

¿Es posible construir una secuencia que tenga toda las palabras distintas de longitud 3 exactamente una vez? (por lo tanto de longitud $2^3 + 3 - 1$, o sea 10)

0001011100

Se llaman secuencias de Bruijn de orden 3.

¿Es posible extender una secencia de Bruijn de orden 3 a una de orden 4? (tiene todas las palabras de longitud 4 exactamente una vez)

Secuencias de Bruijn y números normales

¿Es posible extender una secuencia de Bruijn de orden 3 a una de orden 4?

Sí, cuando el alfabeto es mayor que 2.

Secuencias de Bruijn y números normales

¿Es posible extender una secuencia de Bruijn de orden 3 a una de orden 4?

Sí, cuando el alfabeto es mayor que 2.

0120022110

Secuencias de Bruijn y números normales

¿Es posible extender una secuencia de Bruijn de orden 3 a una de orden 4?

Sí, cuando el alfabeto es mayor que 2.

0120022110001011121020212220 1

Pero se conoce un solo algoritmo para hacer la extensión (algoritmo de Fleury).

Posible tesis de licenciatura

Dar un algoritmo para extender secuencias de Bruijn de orden n a orden $(n+1)$,

Teorema

Las secuencias de Bruijn infinitas son normales respecto de su alfabeto.

Aleatoriedad factible

Calibrar, dar formulaciones equivalentes de aleatoriedad factible.

Santiago Figueira está desarrollando esta teoría.

Otros temas en KAPOW

- Discrepancia de normalidad

Otros temas en KAPOW

- Discrepancia de normalidad
- Problemas en secuencias biológicas (proteínas, ADN) ligados a repeticiones, azar y anti-azar.

  Pablo Turjanski

Otros temas en KAPOW

- Discrepancia de normalidad
- Problemas en secuencias biológicas (proteínas, ADN) ligados a repeticiones, azar y anti-azar.

  Pablo Turjanski
- Normalidad y autómatas

  Olivier Carton; INFINIS; Université Paris Diderot

Otros temas en KAPOW

- Discrepancia de normalidad
- Problemas en secuencias biológicas (proteínas, ADN) ligados a repeticiones, azar y anti-azar.

  Pablo Turjanski
- Normalidad y autómatas

  Olivier Carton; INFINIS; Université Paris Diderot
- Secuencias infinitas y autómatas, secuencias temporizadas

  Eugene Asarin, INFINIS, Université Paris Diderot

Otros temas en KAPOW

- Discrepancia de normalidad
- Problemas en secuencias biológicas (proteínas, ADN) ligados a repeticiones, azar y anti-azar.

  Pablo Turjanski
- Normalidad y autómatas

  Olivier Carton; INFINIS; Université Paris Diderot
- Secuencias infinitas y autómatas, secuencias temporizadas

  Eugene Asarin, INFINIS, Université Paris Diderot