Tesis de Licenciatura en Ciencias de la Computación

Secuencias completamente equidistribuidas basadas en secuencias de De Bruijn

Emilio Almansi

Directora: Verónica Becher
Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
4 de septiembre, 2019

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.
- Predicción del clima, medicina nuclear, simulación de proteínas.

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.
- Predicción del clima, medicina nuclear, simulación de proteínas.
- Aprendizaje automático, algoritmos probabilistas.

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.
- Predicción del clima, medicina nuclear, simulación de proteínas.
- Aprendizaje automático, algoritmos probabilistas.
- Juegos de azar, videojuegos, deportes.

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.
- Predicción del clima, medicina nuclear, simulación de proteínas.
- Aprendizaje automático, algoritmos probabilistas.
- Juegos de azar, videojuegos, deportes.

Generación de números aleatorios.

Sobre secuencias aleatorias

¿Qué tienen en común las siguientes disciplinas?

- Criptografía, seguridad informática.
- Predicción del clima, medicina nuclear, simulación de proteínas.
- Aprendizaje automático, algoritmos probabilistas.
- Juegos de azar, videojuegos, deportes.

Generación de números aleatorios.

Pero, ¿qué es una secuencia de números aleatorios?

Sobre secuencias aleatorias

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y cualquier número del 1 al 6 tiene que ser *equiprobable*.

Sobre secuencias aleatorias

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y cualquier número del 1 al 6 tiene que ser *equiprobable*.

Respecto a la parte de *impredecible*:

> *If "random" means that the sequence satisfies no predictable rules, the title of this paper is contradictory.*
>
> —*Donald Knuth, 1965*

Sobre secuencias aleatorias

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y cualquier número del 1 al 6 tiene que ser *equiprobable*.

Respecto a la parte de *impredecible*:

> *If "random" means that the sequence satisfies no predictable rules, the title of this paper is contradictory.*
>
> —*Donald Knuth, 1965*

En este trabajo, nos enfocamos en la parte de *equiprobable*.

Sobre secuencias aleatorias

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y cualquier número del 1 al 6 tiene que ser *equiprobable*.

Respecto a la parte de *impredecible*:

> *If "random" means that the sequence satisfies no predictable rules, the title of this paper is contradictory.*
>
> —*Donald Knuth, 1965*

En este trabajo, nos enfocamos en la parte de *equiprobable*. Es posible construir secuencias determinísticas que cumplen con esta propiedad.

Equidistribución

Definición

Dado un entero b, una secuencia de *números enteros* $x_1, x_2, \ldots$ del conjunto $\{0, 1, \ldots, b-1\}$ es **equidistribuida** si todo valor posible aparece con frecuencia asintótica igual a $\frac{1}{b}$:

Equidistribución

Definición

Dado un entero b, una secuencia de *números enteros* $x_1, x_2, \ldots$ del conjunto $\{0, 1, \ldots, b-1\}$ es **equidistribuida** si todo valor posible aparece con frecuencia asintótica igual a $\frac{1}{b}$:

$$Pr\,(x_i = j) = \frac{1}{b} \qquad \text{para } j = 0, \ldots, b-1,$$

donde $Pr(x_i = j) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \sigma(x_i = j)$.

Equidistribución

Definición

Dado un entero b, una secuencia de *números enteros* $x_1, x_2, \ldots$ del conjunto $\{0, 1, \ldots, b-1\}$ es **equidistribuida** si todo valor posible aparece con frecuencia asintótica igual a $\frac{1}{b}$:

$$Pr(x_i = j) = \frac{1}{b} \qquad \text{para } j = 0, \ldots, b-1,$$

donde $Pr(x_i = j) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \sigma(x_i = j)$.

Ahora, definimos una noción equivalente para secuencias de números reales.

Equidistribución

Definición

Una secuencia de *números reales* $x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es **equidistribuida** si la frecuencia de valores dentro de cualquier subconjunto I es igual a su tamaño:

Equidistribución

Definición

Una secuencia de *números reales* $x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es **equidistribuida** si la frecuencia de valores dentro de cualquier subconjunto I es igual a su tamaño:

$$Pr\,(x_i \in I) = |I| \qquad \text{para todo } I \in [0, 1)\,,$$

donde $Pr\,(x_i \in I) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \sigma(x_i \in I)$.

Sobre secuencias aleatorias

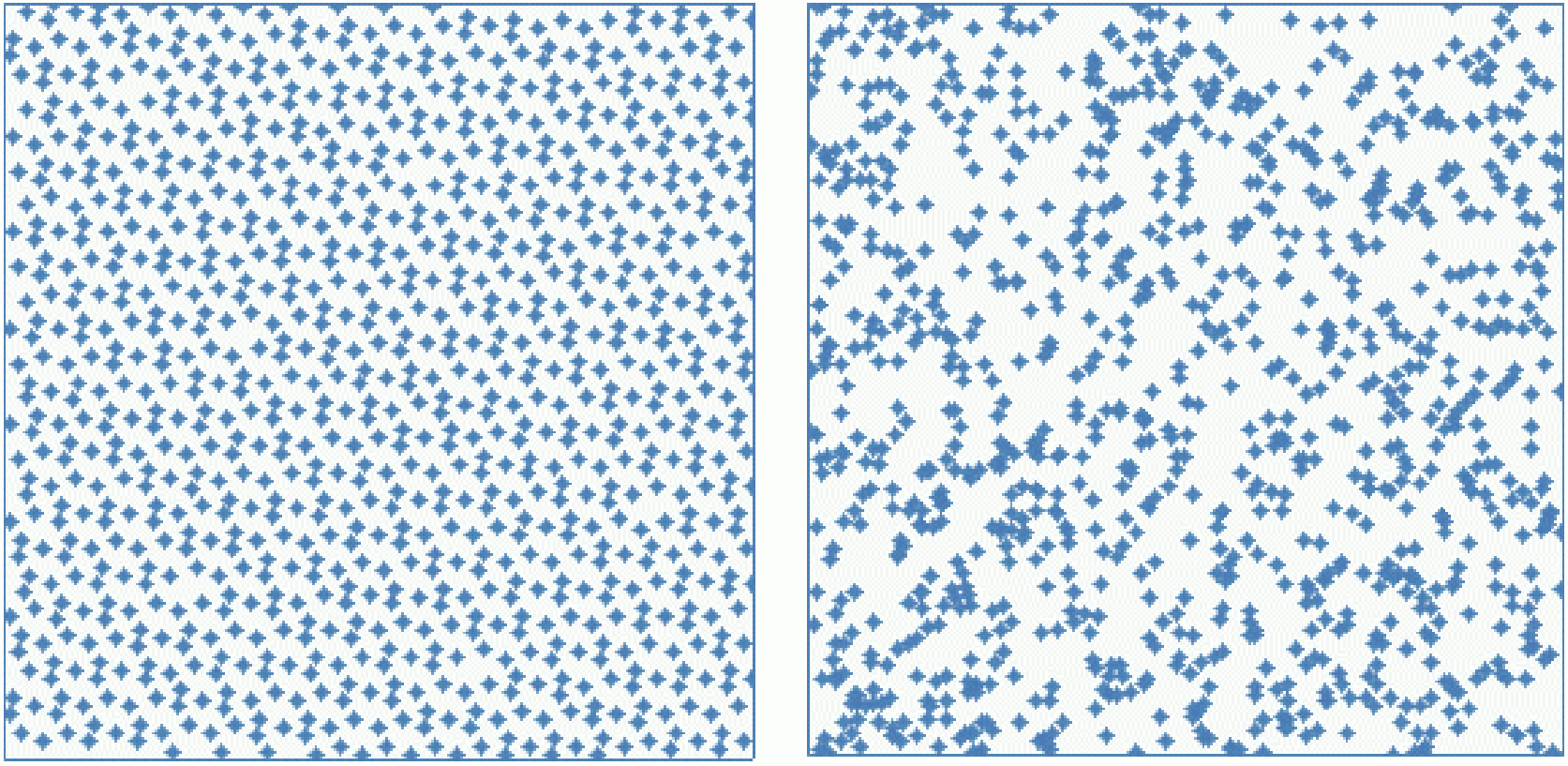

Figura 1: Baja y alta discrepancia.

Equidistribución completa

Aenean laoreet, ligula vel aliquet consectetur, mi magna rutrum urna, vel volutpat nulla purus sed lorem.

Equidistribución completa

Aenean laoreet, ligula vel aliquet consectetur, mi magna rutrum urna, vel volutpat nulla purus sed lorem.

Definición

Fusce sit amet lacus viverra, viverra massa sit amet, placerat neque. Integer ipsum sapien, efficitur quis dui vitae, facilisis tempus dolor.

Equidistribución completa

Aenean laoreet, ligula vel aliquet consectetur, mi magna rutrum urna, vel volutpat nulla purus sed lorem.

Definición

Fusce sit amet lacus viverra, viverra massa sit amet, placerat neque. Integer ipsum sapien, efficitur quis dui vitae, facilisis tempus dolor.

Duis ornare volutpat libero, at sodales dolor porttitor at.

Equidistribución completa

Aenean laoreet, ligula vel aliquet consectetur, mi magna rutrum urna, vel volutpat nulla purus sed lorem.

Definición

Fusce sit amet lacus viverra, viverra massa sit amet, placerat neque. Integer ipsum sapien, efficitur quis dui vitae, facilisis tempus dolor.

Duis ornare volutpat libero, at sodales dolor porttitor at.

In rutrum dapibus justo, at mattis lacus ultrices sed. Suspendisse suscipit luctus fermentum.

Secuencias de De Bruijn

Definición

[Borel, 1909] Mauris euismod neque a lorem rutrum, id molestie eros consequat. In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque:

$$\lim_{n\to\infty} \frac{\|u[1,\ell n]\|_v}{n} = \frac{1}{|A|^\ell}.$$

Secuencias de De Bruijn

Definición

[Borel, 1909] Mauris euismod neque a lorem rutrum, id molestie eros consequat. In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque:

$$\lim_{n\to\infty} \frac{\|u[1,\ell n]\|_v}{n} = \frac{1}{|A|^\ell}.$$

Donec nec ex id nisl venenatis semper. Curabitur erat mi, sagittis nec tortor vel, tempor porta magna. Cras at maximus orci, non viverra neque.

Secuencias de De Bruijn

Definición

[Borel, 1909] Mauris euismod neque a lorem rutrum, id molestie eros consequat. In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque:

$$\lim_{n\to\infty} \frac{\|u[1,\ell n]\|_v}{n} = \frac{1}{|A|^\ell}.$$

Donec nec ex id nisl venenatis semper. Curabitur erat mi, sagittis nec tortor vel, tempor porta magna. Cras at maximus orci, non viverra neque.

Problema (Borel, 1909)

In eget enim feugiat, cursus tellus eget, dapibus libero. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

La secuencia de Knuth (1)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna.

$$F^{(2^n,n)} = f_1, \ldots, f_{2^{n^2}}$$

La secuencia de Knuth (1)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna.

$$
\begin{aligned}
F^{(2^n,n)} &= f_1, \ldots, f_{2^{n^2}} \\
A^{(n)} &= \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n} \\
&= \left(\frac{f_i}{2^n} \right)_{i=1}^{2^{n^2}}
\end{aligned}
$$

La secuencia de Knuth (1)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna.

$$
\begin{aligned}
F^{(2^n,n)} &= f_1, \ldots, f_{2^{n^2}} \\
A^{(n)} &= \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n} \\
&= \left(\frac{f_i}{2^n} \right)_{i=1}^{2^{n^2}} \\
B^{(n)} &= \left\langle \underbrace{A^{(n)}; A^{(n)}; \ldots; A^{(n)}}_{n2^{2n} \text{ veces}} \right\rangle
\end{aligned}
$$

La secuencia de Knuth (1)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna.

$$
\begin{aligned}
F^{(2^n,n)} &= f_1, \ldots, f_{2^{n^2}} \\
A^{(n)} &= \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n} \\
&= \left(\frac{f_i}{2^n} \right)_{i=1}^{2^{n^2}} \\
B^{(n)} &= \left\langle \underbrace{A^{(n)}; A^{(n)}; \ldots; A^{(n)}}_{n2^{2n} \text{ veces}} \right\rangle
\end{aligned}
$$

Porta purus neque, ultrices vulputate orci ullamcorper eu.

La secuencia de Knuth (2)

For example, when $n = 2$:

$$F^{(4,2)} = 0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

La secuencia de Knuth (2)

For example, when $n = 2$:

$$F^{(4,2)} = 0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$
$$F^{(4,2)} = 0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

and $|A^{(2)}| = 16$, $|B^{(2)}| = 512$.

La secuencia de Knuth (3)

Curabitur varius in ligula nec laoreet.

$$K = \left\langle B^{(1)}; B^{(2)}; B^{(3)}; \ldots \right\rangle$$

La secuencia de Knuth (3)

Curabitur varius in ligula nec laoreet.

$$K = \left\langle B^{(1)}; B^{(2)}; B^{(3)}; \ldots \right\rangle$$

Teorema (Knuth, 1965)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna vulputate.

La secuencia de Knuth (3)

Curabitur varius in ligula nec laoreet.

$$K = \left\langle B^{(1)}; B^{(2)}; B^{(3)}; \ldots \right\rangle$$

Teorema (Knuth, 1965)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna vulputate.

Morbi euismod purus at cursus iaculis. Donec efficitur lorem rutrum, auctor justo id, rhoncus nibh.

La secuencia de Knuth (3)

Curabitur varius in ligula nec laoreet.

$$K = \left\langle B^{(1)}; B^{(2)}; B^{(3)}; \ldots \right\rangle$$

Teorema (Knuth, 1965)

Nam sagittis dolor in enim tincidunt, sit amet pellentesque urna vulputate.

Morbi euismod purus at cursus iaculis. Donec efficitur lorem rutrum, auctor justo id, rhoncus nibh.

Aenean ultricies eget mi quis maximus. Mauris ornare interdum vestibulum.

Tamaños de alfabeto linealmente crecientes

Teorema (Agafonov 1968)

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos

Tamaños de alfabeto linealmente crecientes

Teorema (Agafonov 1968)

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos

Corolario

Vestibulum quis dolor quam. Sed viverra, diam ac fringilla fringilla, ex dui consequat leo, nec tempus augue mi eu quam.

Tamaños de alfabeto linealmente crecientes

Teorema (Agafonov 1968)

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos

Corolario

Vestibulum quis dolor quam. Sed viverra, diam ac fringilla fringilla, ex dui consequat leo, nec tempus augue mi eu quam.

Teorema (Vandehey 2016)

Phasellus quis aliquam nulla, non rutrum lorem. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos.

Teorema principal

Nullam posuere tincidunt urna et elementum. Donec elementum at tellus sit amet tempus.

Teorema principal

Nullam posuere tincidunt urna et elementum. Donec elementum at tellus sit amet tempus.

Problema

Cras id accumsan risus, sed elementum elit. Suspendisse aliquet hendrerit gravida.

Teorema principal

Nullam posuere tincidunt urna et elementum. Donec elementum at tellus sit amet tempus.

Problema

Cras id accumsan risus, sed elementum elit. Suspendisse aliquet hendrerit gravida.

Teorema (Resultado principal de esta tesis)

Nullam vehicula erat ante, hendrerit euismod elit luctus nec. Duis sagittis tincidunt metus, in dapibus lorem ullamcorper ut.

Idea de la demostración

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Idea de la demostración

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Idea de la demostración

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Vestibulum aliquam augue et tortor pulvinar suscipit $w_n^\star$.

Idea de la demostración

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Vestibulum aliquam augue et tortor pulvinar suscipit $w_n^\star$.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed placerat nulla a vulputate ultrices. Ut et magna ac lacus elementum tincidunt a id ante.

Donec $u = v_1 v_2 \ldots v_m$ aenean ullamcorper odio vitae v_i erat ℓ_n rhoncus quis

$$e_n(u) = e_n(v_1) \ldots e_n(v_m)$$

Criterio de Weyl

Definición

Suspendisse ut hendrerit A, *finibus semper neque non congue tortor dictum* ℓ laoreet ex nec pulvinar $u \in A^*$ tellus

$$\Delta_{A,\ell}(u) = \max_{v \in A^\ell} \left(\left| \frac{\|u\|_v}{\lfloor |u|/\ell \rfloor} - \frac{1}{|A|^\ell} \right| \right).$$

Criterio de Weyl

Definición

Suspendisse ut hendrerit A, *finibus semper neque non congue tortor dictum* ℓ laoreet ex nec pulvinar $u \in A^*$ tellus

$$\Delta_{A,\ell}(u) = \max_{v \in A^\ell} \left(\left| \frac{\|u\|_v}{\lfloor |u|/\ell \rfloor} - \frac{1}{|A|^\ell} \right| \right).$$

Nam sagittis dolor in enim tincidunt $v \in A^\omega$ sit amet pellentesque urna vulputate ℓ

$$\lim_{n \to \infty} \Delta_{A,\ell}(v[1, \ell n]) = 0$$

Prueba alternativa

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Prueba alternativa

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Prueba alternativa

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Vestibulum aliquam augue et tortor pulvinar suscipit $w_n^\star$.

Prueba alternativa

Definición

Curabitur imperdiet tempus massa $A = \{0, 1, \ldots, b-1\}$, pellentesque id turpis at mauris tempor auctor at pellentesque ex.

Pellentesque urna arcu, pellentesque sit amet volutpat eget, venenatis sed leo. Phasellus tempus eu urna a lacinia.

Vestibulum aliquam augue et tortor pulvinar suscipit $w_n^\star$.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed placerat nulla a vulputate ultrices. Ut et magna ac lacus elementum tincidunt a id ante.

Donec $u = v_1 v_2 \ldots v_m$ aenean ullamcorper odio vitae v_i erat ℓ_n rhoncus quis

$$e_n(u) = e_n(v_1) \ldots e_n(v_m)$$

Problemas abiertos

Cras id accumsan risus, sed elementum elit.

Problemas abiertos

Cras id accumsan risus, sed elementum elit.

- Donec eu sollicitudin lacus. Vestibulum facilisis eu tellus quis gravida. Proin faucibus tellus nec tempus maximus.

Problemas abiertos

Cras id accumsan risus, sed elementum elit.

- Donec eu sollicitudin lacus. Vestibulum facilisis eu tellus quis gravida. Proin faucibus tellus nec tempus maximus.
- Proin at facilisis orci. Nunc at orci in ante semper elementum ullamcorper in est. Praesent maximus aliquet lorem, in tincidunt odio tempus vel.

Problemas abiertos

Cras id accumsan risus, sed elementum elit.

- Donec eu sollicitudin lacus. Vestibulum facilisis eu tellus quis gravida. Proin faucibus tellus nec tempus maximus.
- Proin at facilisis orci. Nunc at orci in ante semper elementum ullamcorper in est. Praesent maximus aliquet lorem, in tincidunt odio tempus vel.
- Etiam vulputate nunc eget mauris vestibulum, nec viverra massa lacinia. Donec volutpat tempus nunc, vitae malesuada odio ultricies nec.