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 $^{(1)}$

¿Qué tienen en común las siguientes áreas?

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

- Criptografía, seguridad informática.

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

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

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

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

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

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

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

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

Generación de números aleatorios.

Sobre secuencias aleatorias $^{(1)}$

¿Qué tienen en común las siguientes áreas?

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

Generación de números aleatorios.

Pero, ¿qué es una secuencia de números aleatorios?

Sobre secuencias aleatorias $^{(2)}$

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

Sobre secuencias aleatorias $^{(2)}$

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y todo 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.*
>
> *Construction of a Random Sequence*
> *Donald Knuth, 1965*

Sobre secuencias aleatorias $^{(2)}$

Intuición: si tiro un dado muchas veces seguidas, el resultado de cada tirada tiene que ser *impredecible* y todo 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.*
>
> *Construction of a Random Sequence*
> *Donald Knuth, 1965*

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

Equidistribución $^{(1)}$

Definición

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

Equidistribución $^{(1)}$

Definición

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

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

Equidistribución $^{(1)}$

Definición

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

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

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

Equidistribución $^{(1)}$

Definición

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

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

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 $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es **equidistribuida** si, dado cualquier conjunto $I \subseteq [0, 1)$, la frecuencia asintótica con la que la secuencia toma valores en I es igual a su tamaño:

Equidistribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es **equidistribuida** si, dado cualquier conjunto $I \subseteq [0, 1)$, la frecuencia asintótica con la que la secuencia toma valores en I es igual a su tamaño:

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

Equidistribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es **equidistribuida** si, dado cualquier conjunto $I \subseteq [0, 1)$, la frecuencia asintótica con la que la secuencia toma valores en I es igual a su tamaño:

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

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

Equidistribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0,1)$ es **equidistribuida** si, dado cualquier conjunto $I \subseteq [0,1)$, la frecuencia asintótica con la que la secuencia toma valores en I es igual a su tamaño:

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

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

Si X es equidistribuida en $[0,1)$, entonces para cualquier b la secuencia $Y = (\lfloor bx_i \rfloor)_{i=1}^{\infty}$ es equidistribuida en $\{0,1,\ldots,b-1\}$.

Equidistribución $^{(3)}$

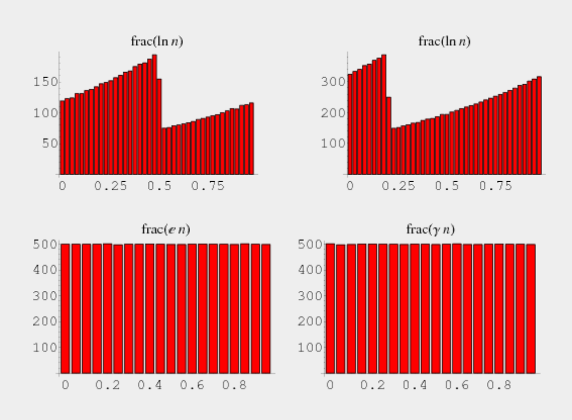

Figura 1: Secuencias de partes fraccionarias.

k-distribución [1]

Intuición: cualquier seguidilla de tiradas tiene que aparecer con igual frecuencia. Por ejemplo, (1, 1) aparece con la misma frecuencia que (2, 2) y que (6, 4).

k-distribución $^{(1)}$

Intuición: cualquier seguidilla de tiradas tiene que aparecer con igual frecuencia. Por ejemplo, (1, 1) aparece con la misma frecuencia que (2, 2) y que (6, 4).

Trabajamos con “ventanas“ de tamaño k de la secuencia. Si $X = x_1, x_2, \ldots$ es una secuencia de *números reales*, entonces:

k-distribución $^{(1)}$

Intuición: cualquier seguidilla de tiradas tiene que aparecer con igual frecuencia. Por ejemplo, (1, 1) aparece con la misma frecuencia que (2, 2) y que (6, 4).

Trabajamos con “ventanas“ de tamaño k de la secuencia. Si $X = x_1, x_2, \ldots$ es una secuencia de *números reales*, entonces:

$$
\begin{aligned}
w_1 &= (x_1, x_2, \ldots, x_k),\\
w_2 &= (x_2, x_3, \ldots, x_{k+1}),\\
w_3 &= (x_3, x_4, \ldots, x_{k+2}),\\
&\ldots
\end{aligned}
$$

es la secuencia de ventanas de X, que llamamos $W_k(X)$.

k-distribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es k-**distribuida** si, dado cualquier conjunto $I \subseteq [0, 1)^k$, la frecuencia asintótica con la que la secuencia de ventanas de X toma valores en I es igual a su tamaño:

k-distribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es k-**distribuida** si, dado cualquier conjunto $I \subseteq [0, 1)^k$, la frecuencia asintótica con la que la secuencia de ventanas de X toma valores en I es igual a su tamaño:

$$Pr(w_i \in I) = |I| \qquad \text{para todo } I \subseteq [0, 1)^k,$$

k-distribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es k-**distribuida** si, dado cualquier conjunto $I \subseteq [0, 1)^k$, la frecuencia asintótica con la que la secuencia de ventanas de X toma valores en I es igual a su tamaño:

$$Pr(w_i \in I) = |I| \qquad \text{para todo } I \subseteq [0, 1)^k,$$

$$\text{donde } W_k(X) = (w_i)_{i=1}^{\infty}$$
$$= (x_1, x_2, \ldots, x_k),\ (x_2, x_3, \ldots, x_{k+1}),\ \ldots\ .$$

k-distribución $^{(2)}$

Definición

Una secuencia de *números reales* $X = x_1, x_2, \ldots$ en el intervalo unitario $[0, 1)$ es k-**distribuida** si, dado cualquier conjunto $I \subseteq [0,1)^k$, la frecuencia asintótica con la que la secuencia de ventanas de X toma valores en I es igual a su tamaño:

$$Pr(w_i \in I) = |I| \qquad \text{para todo } I \subseteq [0,1)^k,$$

donde
$$\begin{aligned} W_k(X) &= (w_i)_{i=1}^{\infty} \\ &= (x_1, x_2, \ldots, x_k),\ (x_2, x_3, \ldots, x_{k+1}),\ \ldots\ . \end{aligned}$$

Si X es k-distribuida para todo k, entonces X es **completamente equidistribuida**.

Equidistribución completa $^{(1)}$

¿Por qué estudiar la propiedad de equidistribución?

- Requerimiento básico de pseudo-aleatoriedad. Propiedades de equipartición y autocorrelación con retraso.

Equidistribución completa (1)

¿Por qué estudiar la propiedad de equidistribución?

- Requerimiento básico de pseudo-aleatoriedad. Propiedades de equipartición y autocorrelación con retraso.
- Calidad de un generador de números aleatorios o PNRG. Pruebas de aleatoriedad.

Equidistribución completa [(1)]

¿Por qué estudiar la propiedad de equidistribución?

- Requerimiento básico de pseudo-aleatoriedad. Propiedades de equipartición y autocorrelación con retraso.
- Calidad de un generador de números aleatorios o PNRG. Pruebas de aleatoriedad.
- Integración de Montecarlo, criterio de la integral de Riemann.

Equidistribución completa $^{(1)}$

¿Por qué estudiar la propiedad de equidistribución?

- Requerimiento básico de pseudo-aleatoriedad. Propiedades de equipartición y autocorrelación con retraso.
- Calidad de un generador de números aleatorios o PNRG. Pruebas de aleatoriedad.
- Integración de Montecarlo, criterio de la integral de Riemann.
- Vínculo: teoría de números, computación, probabilidad y estadística.

Equidistribución completa [(1)]

¿Por qué estudiar la propiedad de equidistribución?

- Requerimiento básico de pseudo-aleatoriedad. Propiedades de equipartición y autocorrelación con retraso.
- Calidad de un generador de números aleatorios o PNRG. Pruebas de aleatoriedad.
- Integración de Montecarlo, criterio de la integral de Riemann.
- Vínculo: teoría de números, computación, probabilidad y estadística.

¿Qué **no** es la equidistribución?

Equidistribución completa $^{(2)}$

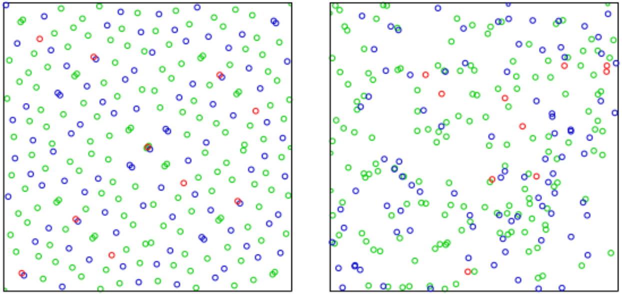

Figura 2: Izq.) Secuencia Sobol 2,3. Der.) Secuencia pseudo-aleat.

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, 1, 1, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$\mathbf{0, 0, 0}, 1, 0, 1, 1, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, \mathbf{0,\ 0,\ 1}, 0, 1, 1, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, \mathbf{0,\ 1,\ 0}, 1, 1, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, \mathbf{1,\ 0,\ 1}, 1, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, \mathbf{0,\ 1,\ 1}, 1$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, \mathbf{1,\ 1,\ 1}$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$\mathbf{0}, 0, 0, 1, 0, 1, \mathbf{1}, \mathbf{1}$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$\mathbf{0},\ \mathbf{0}, 0, 1, 0, 1, 1, \mathbf{1}$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, 1, 1, 1$$

Con $b = 4, k = 2$:

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, 1, 1, 1$$

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de "contener" a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, 1, 1, 1$$

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Notar que siempre tienen longitud b^k.

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Tienen la propiedad de “contener“ a todas las posibles combinaciones de secuencias de un alfabeto y tamaño dados. Ejemplos:

Con $b = 2, k = 3$:

$$0, 0, 0, 1, 0, 1, 1, 1$$

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Notar que siempre tienen longitud b^k. ¿Qué relación tienen con las secuencias equidistribuidas?

Secuencia de Knuth $^{(1)}$

Definición

Una **secuencia** A **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base 2^n y de órden n por su base:

Secuencia de Knuth $^{(1)}$

Definición

Una **secuencia** A **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base 2^n y de órden n por su base:

$$A^{(n)} = \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n}$$

donde $F^{(2^n,n)} = f_1, \ldots, f_{2^{n^2}}$ denota una secuencia de De Bruijn de base 2^n y de órden n.

Secuencia de Knuth (1)

Definición

Una **secuencia** A **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base 2^n y de órden n por su base:

$$A^{(n)} = \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n}$$

donde $F^{(2^n,n)} = f_1, \ldots, f_{2^{n^2}}$ denota una secuencia de De Bruijn de base 2^n y de órden n.

Una **secuencia** B **de órden** n es la secuencia que se obtiene de concatenar $n2^{2n}$ copias de una secuencia A de órden n:

Secuencia de Knuth (1)

Definición

Una **secuencia** A **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base 2^n y de órden n por su base:

$$A^{(n)} = \frac{f_1}{2^n}, \frac{f_2}{2^n}, \ldots, \frac{f_{2^{n^2}}}{2^n}$$

donde $F^{(2^n,n)} = f_1, \ldots, f_{2^{n^2}}$ denota una secuencia de De Bruijn de base 2^n y de órden n.

Una **secuencia** B **de órden** n es la secuencia que se obtiene de concatenar $n2^{2n}$ copias de una secuencia A de órden n:

$$B^{(n)} = \left\langle \underbrace{A^{(n)}; A^{(n)}; \ldots; A^{(n)}}_{n2^{2n} \text{ veces}} \right\rangle .$$

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

$$A^{(2)} = \frac{0}{4}, \frac{0}{4}, \frac{1}{4}, \frac{0}{4}, \frac{2}{4}, \frac{0}{4}, \frac{3}{4}, \frac{1}{4}, \frac{1}{4}, \frac{2}{4}, \frac{1}{4}, \frac{3}{4}, \frac{2}{4}, \frac{2}{4}, \frac{3}{4}, \frac{3}{4}$$

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

$$A^{(2)} = \frac{0}{4}, \frac{0}{4}, \frac{1}{4}, \frac{0}{4}, \frac{2}{4}, \frac{0}{4}, \frac{3}{4}, \frac{1}{4}, \frac{1}{4}, \frac{2}{4}, \frac{1}{4}, \frac{3}{4}, \frac{2}{4}, \frac{2}{4}, \frac{3}{4}, \frac{3}{4}$$

$$B^{(2)} = \left\langle \underbrace{A^{(2)}; \ldots ; A^{(2)}}_{2\times 2^{2\times 2}=32 \text{ veces}} \right\rangle$$

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

$$A^{(2)} = \frac{0}{4}, \frac{0}{4}, \frac{1}{4}, \frac{0}{4}, \frac{2}{4}, \frac{0}{4}, \frac{3}{4}, \frac{1}{4}, \frac{1}{4}, \frac{2}{4}, \frac{1}{4}, \frac{3}{4}, \frac{2}{4}, \frac{2}{4}, \frac{3}{4}, \frac{3}{4}$$

$$\begin{aligned} B^{(2)} &= \left\langle \underbrace{A^{(2)}; \ldots; A^{(2)}}_{2 \times 2^{2 \times 2} = 32 \text{ veces}} \right\rangle \\ &= \underbrace{\frac{0}{4}, \frac{0}{4}, \ldots, \frac{3}{4}, \frac{3}{4}}_{A^{(2)}}, \ldots, \underbrace{\frac{0}{4}, \frac{0}{4}, \ldots, \frac{3}{4}, \frac{3}{4}}_{A^{(2)}}. \end{aligned}$$

Secuencia de Knuth $^{(3)}$

Ahora sí, ya estamos en condiciones de definir la secuencia de Knuth.

Secuencia de Knuth $^{(3)}$

Ahora sí, ya estamos en condiciones de definir la secuencia de Knuth.

Definición

La secuencia de Knuth, que denominamos K, se define como la concatenación de todas las posibles secuencias B en órden creciente:

Secuencia de Knuth $^{(3)}$

Ahora sí, ya estamos en condiciones de definir la secuencia de Knuth.

Definición

La secuencia de Knuth, que denominamos K, se define como la concatenación de todas las posibles secuencias B en órden creciente:

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

Secuencia de Knuth $^{(3)}$

Ahora sí, ya estamos en condiciones de definir la secuencia de Knuth.

Definición

La secuencia de Knuth, que denominamos K, se define como la concatenación de todas las posibles secuencias B en órden creciente:

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

Teorema (Knuth, 1965)

La secuencia K es completamente equidistribuida.

Secuencia de Knuth $^{(4)}$

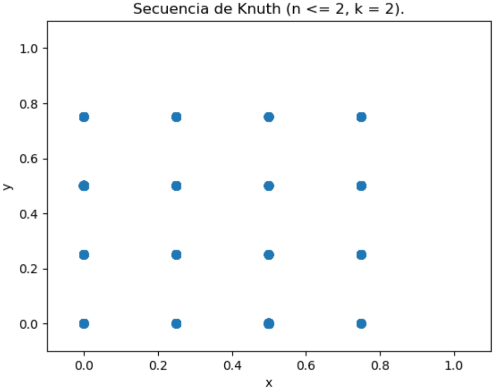

Figura 3: Secuencia de Knuth en dos dimensiones.

Secuencia de Knuth $^{(4)}$

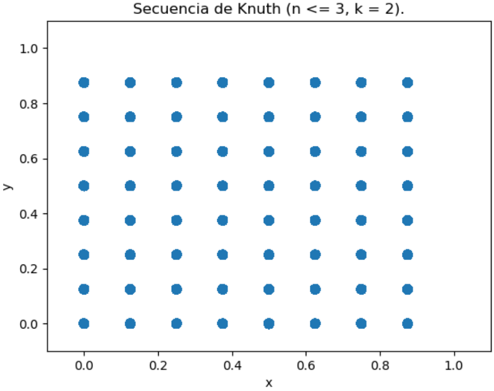

Figura 3: Secuencia de Knuth en dos dimensiones.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Definición

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

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Alfabetos linealmente crecientes

Definición

Una **secuencia** C **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base n y de órden n por su base:

Alfabetos linealmente crecientes

Definición

Una **secuencia** C **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base n y de órden n por su base:

$$C^{(n)} = \frac{f_1}{n}, \frac{f_2}{n}, \ldots, \frac{f_{n^n}}{n}$$

donde $F^{(n,n)} = f_1, \ldots, f_{n^n}$ denota una secuencia de De Bruijn de base n y de órden n.

Alfabetos linealmente crecientes

Definición

Una **secuencia** C **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base n y de órden n por su base:

$$C^{(n)} = \frac{f_1}{n}, \frac{f_2}{n}, \ldots, \frac{f_{n^n}}{n}$$

donde $F^{(n,n)} = f_1, \ldots, f_{n^n}$ denota una secuencia de De Bruijn de base n y de órden n.

Una **secuencia** D **de órden** n es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de órden n:

Alfabetos linealmente crecientes

Definición

Una **secuencia** C **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base n y de órden n por su base:

$$C^{(n)} = \frac{f_1}{n}, \frac{f_2}{n}, \ldots, \frac{f_{n^n}}{n}$$

donde $F^{(n,n)} = f_1, \ldots, f_{n^n}$ denota una secuencia de De Bruijn de base n y de órden n.

Una **secuencia** D **de órden** n es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de órden n:

$$D^{(n)} = \left\langle \underbrace{C^{(n)}; C^{(n)}; \ldots; C^{(n)}}_{t(n) \text{ veces}} \right\rangle .$$

Alfabetos linealmente crecientes

Definición

Una **secuencia** C **de órden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia de De Bruijn de base n y de órden n por su base:

$$C^{(n)} = \frac{f_1}{n}, \frac{f_2}{n}, \ldots, \frac{f_{n^n}}{n}$$

donde $F^{(n,n)} = f_1, \ldots, f_{n^n}$ denota una secuencia de De Bruijn de base n y de órden n.

Una **secuencia** D **de órden** n es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de órden n:

$$D^{(n)} = \left\langle \underbrace{C^{(n)}; C^{(n)}; \ldots; C^{(n)}}_{t(n) \text{ veces}} \right\rangle .$$

Secuencia L (1)

Definición

La secuencia L se define como la concatenación de todas las posibles secuencias D en órden creciente:

Secuencia L (1)

Definición

La secuencia L se define como la concatenación de todas las posibles secuencias D en órden creciente:

$$L = \left\langle D^{(1)}; D^{(2)}; D^{(3)}; \ldots \right\rangle .$$

Secuencia L $^{(1)}$

Definición

La secuencia L se define como la concatenación de todas las posibles secuencias D en órden creciente:

$$L = \left\langle D^{(1)}; D^{(2)}; D^{(3)}; \dots \right\rangle .$$

Ahora, enunciamos el aporte principal de esta tesis.

Secuencia L $^{(1)}$

Definición

La secuencia L se define como la concatenación de todas las posibles secuencias D en órden creciente:

$$L = \left\langle D^{(1)}; D^{(2)}; D^{(3)}; \ldots \right\rangle .$$

Ahora, enunciamos el aporte principal de esta tesis.

Teorema 1

Si $t : \mathbb{N} \mapsto \mathbb{N}$ *es una función no decreciente y* $\lim_{n\to\infty} n/t(n) = 0$*, entonces la secuencia* L *es completamente equidistribuida.*

Secuencia L (2)

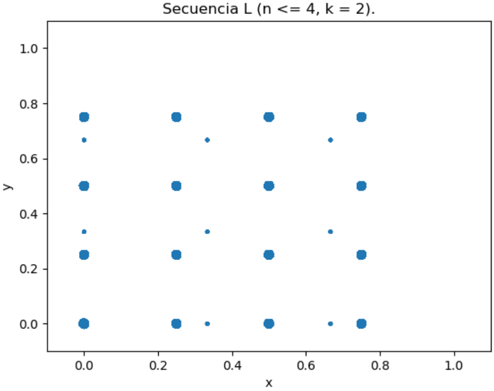

Figura 4: Secuencia L en dos dimensiones.

Secuencia $L^{(2)}$

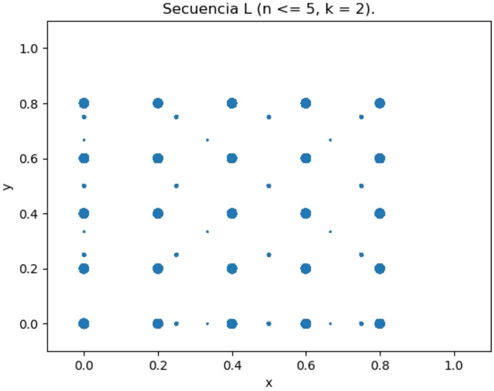

Figura 4: Secuencia L en dos dimensiones.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Definición

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

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Idea de la demostración

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Prueba alternativa $^{(1)}$

Presentamos una prueba alternativa más sencilla, basada en el criterio de Weyl y en una proposición de la teoría de congruencias lineales.

Prueba alternativa $^{(1)}$

Presentamos una prueba alternativa más sencilla, basada en el criterio de Weyl y en una proposición de la teoría de congruencias lineales.

Criterio de Weyl

Una secuencia $X = x_1, x_2, \ldots$ de números reales en $[0, 1)$ es k-distribuida si, y solo si, para cualquier vector de enteros no nulo $\bar{\ell} = (l_1, \ldots, l_k)$:

Prueba alternativa [(1)]

Presentamos una prueba alternativa más sencilla, basada en el criterio de Weyl y en una proposición de la teoría de congruencias lineales.

Criterio de Weyl

Una secuencia $X = x_1, x_2, \ldots$ de números reales en $[0, 1)$ es k-distribuida si, y solo si, para cualquier vector de enteros no nulo $\bar{\ell} = (l_1, \ldots, l_k)$:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i \bar{\ell} \cdot \bar{w}_n} = 0,$$

donde $W_k(X) = \bar{w}_1, \bar{w}_2, \ldots$ es la secuencia de ventanas de órden k de X.

Prueba alternativa $^{(1)}$

Presentamos una prueba alternativa más sencilla, basada en el criterio de Weyl y en una proposición de la teoría de congruencias lineales.

Criterio de Weyl

Una secuencia $X = x_1, x_2, \ldots$ de números reales en $[0, 1)$ es k-distribuida si, y solo si, para cualquier vector de enteros no nulo $\bar{\ell} = (l_1, \ldots, l_k)$:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i \bar{\ell}\cdot\bar{w}_n} = 0,$$

donde $W_k(X) = \bar{w}_1, \bar{w}_2, \ldots$ es la secuencia de ventanas de órden k de X.

Podemos reducir el problema a una cota sobre una suma exponencial.

Prueba alternativa $^{(2)}$

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

Prueba alternativa $^{(2)}$

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Prueba alternativa $^{(2)}$

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

Definición

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

Prueba alternativa $^{(2)}$

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Prueba alternativa [(2)]

Mauris euismod neque a lorem rutrum, id molestie eros consequat.

In facilisis magna eu libero commodo, id tincidunt ℓ purus pellentesque.

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.

Problemas abiertos

Quedan varias líneas claras de investigación futura:

Problemas abiertos

Quedan varias líneas claras de investigación futura:

- ¿Qué pasa cuando no se cumple que $\lim_{n\to\infty} n/t(n) = 0$? ¿La secuencia L sigue siendo completamente equidistribuida?

Problemas abiertos

Quedan varias líneas claras de investigación futura:

- ¿Qué pasa cuando no se cumple que $\lim_{n\to\infty} n/t(n) = 0$? ¿La secuencia L sigue siendo completamente equidistribuida?
- Para responder eso, es necesario entender mejor la discrepancia de la familia de secuencias de De Bruijn que se use para formar la secuencia L.

Problemas abiertos

Quedan varias líneas claras de investigación futura:

- ¿Qué pasa cuando no se cumple que $\lim_{n\to\infty} n/t(n) = 0$? ¿La secuencia L sigue siendo completamente equidistribuida?
- Para responder eso, es necesario entender mejor la discrepancia de la familia de secuencias de De Bruijn que se use para formar la secuencia L.
- Relacionado: ¿cumple la secuencia L la propiedad de correlación de pares de Poisson?