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

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$\mathbf{0,\ 0}, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, \mathbf{0,\ 1}, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, \mathbf{1,\ 0}, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, \mathbf{0,\ 2}, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, \mathbf{2,\ 0}, 3, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k "contiene" a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, \mathbf{0,\ 3}, 1, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, \mathbf{3,\ 1}, 1, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, \mathbf{1,\ 1}, 2, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, \mathbf{1, 2}, 1, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, \mathbf{2,\ 1}, 3, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, \mathbf{1,\ 3}, 2, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, \mathbf{3}, \mathbf{2}, 2, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, \mathbf{2,\ 2}, 3, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, \mathbf{2}, \mathbf{3}, 3$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$0, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, \mathbf{3,\ 3}$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. Ejemplos:

Con $b = 2, k = 3$:

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

Con $b = 4, k = 2$:

$$\mathbf{0}, 0, 1, 0, 2, 0, 3, 1, 1, 2, 1, 3, 2, 2, 3, \mathbf{3}$$

Secuencias de De Bruijn

Son secuencias muy estudiadas en combinatoria. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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. Una secuencia b-aria de De Bruijn de orden k “contiene“ a cada posible secuencia b-aria de longitud k exactamente una vez. 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.

Estas secuencias tienen una relación con la noción de equidistribución.

Sobre secuencias aleatoriash $^{(1)}$

¿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 $^{(1)}$

Dado un entero $b \geq 2$, una secuencia de *números enteros* $X = x_1, x_2, \ldots$ del conjunto $\{1, \ldots, b\}$ es **equidistribuida** si todo valor posible aparece con la misma frecuencia asintótica:

Equidistribución $^{(1)}$

Dado un entero $b \geq 2$, una secuencia de *números enteros* $X = x_1, x_2, \ldots$ del conjunto $\{1, \ldots, b\}$ es **equidistribuida** si todo valor posible aparece con la misma frecuencia asintótica:

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

Equidistribución $^{(1)}$

Dado un entero $b \geq 2$, una secuencia de *números enteros* $X = x_1, x_2, \ldots$ del conjunto $\{1, \ldots, b\}$ es **equidistribuida** si todo valor posible aparece con la misma frecuencia asintótica:

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

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

Equidistribución [1]

Dado un entero $b \geq 2$, una secuencia de *números enteros* $X = x_1, x_2, \ldots$ del conjunto $\{1, \ldots, b\}$ es **equidistribuida** si todo valor posible aparece con la misma frecuencia asintótica:

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

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

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

Equidistribución $^{(2)}$

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 $^{(2)}$

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 $^{(2)}$

Una secuencia de *números reales* $X = x_1, x_2, \dots$ 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 $^{(2)}$

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

Equidistribución $^{(3)}$

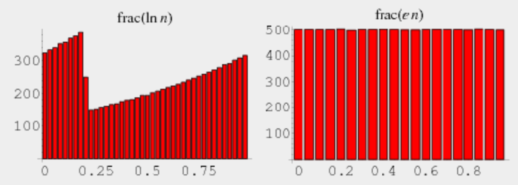

Figura 1: Secuencias de partes fraccionarias.

k-distribución $^{(1)}$

Intuición: cualquier seguidilla de tiradas tiene que aparecer con igual frecuencia. Por ejemplo, (1, 2, 3) aparece con la misma frecuencia que (3, 2, 1) y que (6, 6, 6).

k-distribución $^{(1)}$

Intuición: cualquier seguidilla de tiradas tiene que aparecer con igual frecuencia. Por ejemplo, (1, 2, 3) aparece con la misma frecuencia que (3, 2, 1) y que (6, 6, 6).

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, 2, 3) aparece con la misma frecuencia que (3, 2, 1) y que (6, 6, 6).

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

$$\begin{aligned}
\bar{w}_1 &= (x_1, x_2, \ldots, x_k), \\
\bar{w}_2 &= (x_2, x_3, \ldots, x_{k+1}), \\
\bar{w}_3 &= (x_3, x_4, \ldots, x_{k+2}), \\
&\ldots
\end{aligned}$$

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

k-distribución $^{(2)}$

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 $^{(2)}$

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:

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

k-distribución $^{(2)}$

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:

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

$$\text{donde } W_k(X) = \bar{w}_1, \bar{w}_2, \ldots$$
$$= (x_1, x_2, \ldots, x_k),\ (x_2, x_3, \ldots, x_{k+1}),\ \ldots\ .$$

k-distribución $^{(2)}$

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:

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

$$\text{donde } W_k(X) = \bar{w}_1, \bar{w}_2, \ldots$$
$$= (x_1, x_2, \ldots, x_k),\ (x_2, x_3, \ldots, x_{k+1}),\ \ldots .$$

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 PRNG. 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 PRNG. 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 PRNG. Pruebas de aleatoriedad.
- Integración de Montecarlo, criterio de la integral de Riemann.

¿Qué **no** es la equidistribución?

Equidistribución completa $^{(2)}$

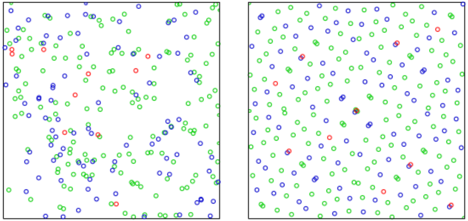

Figura 2: Izq.) Sec. pseudo-aleatoria Der.) Sec. Sobol 2,3.

Secuencia de Knuth $^{(1)}$

Secuencia de Knuth $^{(1)}$

Definición

Una **secuencia** A **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia 2^n-aria de De Bruijn de orden n por 2^n:

Secuencia de Knuth [1]

Definición

Una **secuencia** A **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia 2^n-aria de De Bruijn de orden n por 2^n:

$$A^{(n)} = \frac{x_1}{2^n}, \frac{x_2}{2^n}, \ldots, \frac{x_{2^{n^2}}}{2^n}$$

donde $x_1, \ldots, x_{2^{n^2}}$ es una secuencia 2^n-aria de De Bruijn de orden n.

Secuencia de Knuth $^{(1)}$

Definición

Una **secuencia** A **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia 2^n-aria de De Bruijn de orden n por 2^n:

$$A^{(n)} = \frac{x_1}{2^n}, \frac{x_2}{2^n}, \ldots, \frac{x_{2^{n^2}}}{2^n}$$

donde $x_1, \ldots, x_{2^{n^2}}$ es una secuencia 2^n-aria de De Bruijn de orden n.

Definición

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

Secuencia de Knuth $^{(1)}$

Definición

Una **secuencia** A **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia 2^n-aria de De Bruijn de orden n por 2^n:

$$A^{(n)} = \frac{x_1}{2^n}, \frac{x_2}{2^n}, \ldots, \frac{x_{2^{n^2}}}{2^n}$$

donde $x_1, \ldots, x_{2^{n^2}}$ es una secuencia 2^n-aria de De Bruijn de orden n.

Definición

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

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

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

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

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

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

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

Secuencia de Knuth $^{(2)}$

Ejemplo para $n = 2$:

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

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

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

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 (Knuth, 1965)

La secuencia de Knuth, que denominamos K, se define como la concatenación de las secuencias $B^{(n)}$ para $n = 1, 2, 3, \ldots$:

Secuencia de Knuth $^{(3)}$

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

Definición (Knuth, 1965)

La secuencia de Knuth, que denominamos K, se define como la concatenación de las secuencias $B^{(n)}$ para $n = 1, 2, 3, \ldots$:

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

Secuencia de Knuth $^{(3)}$

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

Definición (Knuth, 1965)

La secuencia de Knuth, que denominamos K, se define como la concatenación de las secuencias $B^{(n)}$ para $n = 1, 2, 3, \ldots$:

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

Teorema (Knuth, 1965)

La secuencia K es completamente equidistribuida.

Secuencia de Knuth $^{(4)}$

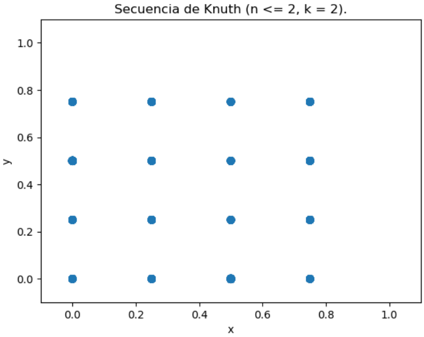

Figura 3: Secuencia de Knuth en dos dimensiones.

Secuencia de Knuth $^{(4)}$

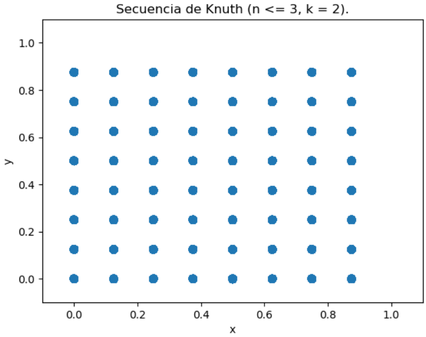

Figura 3: Secuencia de Knuth en dos dimensiones.

Comentarios sobre la demostración

Knuth da una prueba elemental de este teorema.

Comentarios sobre la demostración

Knuth da una prueba elemental de este teorema.

Dos decisiones en la construcción de K parecen arbitrarias, pero juegan un rol importante en la demostración:

Comentarios sobre la demostración

Knuth da una prueba elemental de este teorema.

Dos decisiones en la construcción de K parecen arbitrarias, pero juegan un rol importante en la demostración:

- La cantidad $n2^{2n}$ de repeticiones de una secuencia A en una secuencia B.

Comentarios sobre la demostración

Knuth da una prueba elemental de este teorema.

Dos decisiones en la construcción de K parecen arbitrarias, pero juegan un rol importante en la demostración:

- La cantidad $n2^{2n}$ de repeticiones de una secuencia A en una secuencia B.
- El uso de secuencias de De Bruijn 2^n-arias de orden n.

Comentarios sobre la demostración

Knuth da una prueba elemental de este teorema.

Dos decisiones en la construcción de K parecen arbitrarias, pero juegan un rol importante en la demostración:

- La cantidad $n2^{2n}$ de repeticiones de una secuencia A en una secuencia B.
- El uso de secuencias de De Bruijn 2^n-arias de orden n.

Si usamos secuencias de De Bruijn con alfabetos que crecen linealmente en tamaño, ¿sigue siendo completamente equidistribuida la secuencia? ¿Cuántas repeticiones son necesarias?

Alfabetos linealmente crecientes [1]

Alfabetos linealmente crecientes [1]

Definición

Una **secuencia** C **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia n-aria de De Bruijn de orden n por n:

Alfabetos linealmente crecientes [1]

Definición

Una **secuencia** C **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia n-aria de De Bruijn de orden n por n:

$$C^{(n)} = \frac{x_1}{n}, \frac{x_2}{n}, \ldots, \frac{x_{n^n}}{n}$$

donde $x_1, \ldots, x_{n^n}$ es una secuencia n-aria de De Bruijn de orden n.

Alfabetos linealmente crecientes $^{(1)}$

Definición

Una **secuencia** C **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia n-aria de De Bruijn de orden n por n:

$$C^{(n)} = \frac{x_1}{n}, \frac{x_2}{n}, \ldots, \frac{x_{n^n}}{n}$$

donde $x_1, \ldots, x_{n^n}$ es una secuencia n-aria de De Bruijn de orden n.

Definición

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, una **secuencia** D **de orden** n es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de orden n:

Alfabetos linealmente crecientes [1]

Definición

Una **secuencia** C **de orden** n es la secuencia que se obtiene al dividir cada elemento de una secuencia n-aria de De Bruijn de orden n por n:

$$C^{(n)} = \frac{x_1}{n}, \frac{x_2}{n}, \ldots, \frac{x_{n^n}}{n}$$

donde $x_1, \ldots, x_{n^n}$ es una secuencia n-aria de De Bruijn de orden n.

Definición

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, una **secuencia** D **de orden** n es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de orden n:

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

Alfabetos linealmente crecientes [1]

Definición

Una **secuencia C de orden n** es la secuencia que se obtiene al dividir cada elemento de una secuencia n-aria de De Bruijn de orden n por n:

$$C^{(n)} = \frac{x_1}{n}, \frac{x_2}{n}, \ldots, \frac{x_{n^n}}{n}$$

donde $x_1, \ldots, x_{n^n}$ es una secuencia n-aria de De Bruijn de orden n.

Definición

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, una **secuencia D de orden n** es la secuencia que se obtiene de concatenar $t(n)$ copias de una secuencia C de orden n:

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

Alfabetos linealmente crecientes $^{(2)}$

Ejemplo para $n = 3$, $t(n) = n$:

Alfabetos linealmente crecientes $^{(2)}$

Ejemplo para $n = 3$, $t(n) = n$:

$$X^{(3,3)} = 0, 0, 0, 1, 0, 0, 2, 0, 1, 1, 0, 1, 2, 0, 2, 1, 0, 2, 2, 1, 1, 1, 2, 1, 2, 2, 2;$$

Alfabetos linealmente crecientes $^{(2)}$

Ejemplo para $n = 3$, $t(n) = n$:

$$X^{(3,3)} = 0, 0, 0, 1, 0, 0, 2, 0, 1, 1, 0, 1, 2, 0, 2, 1, 0, 2, 2, 1, 1, 1, 2, 1, 2, 2, 2;$$

$$\begin{aligned} C^{(3)} = \; & \frac{0}{3}, \frac{0}{3}, \frac{0}{3}, \frac{1}{3}, \frac{0}{3}, \frac{0}{3}, \frac{2}{3}, \frac{0}{3}, \frac{1}{3}, \frac{1}{3}, \frac{0}{3}, \frac{1}{3}, \frac{2}{3}, \frac{0}{3}, \\ & \frac{0}{3}, \frac{2}{3}, \frac{1}{3}, \frac{0}{3}, \frac{2}{3}, \frac{2}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3}; \end{aligned}$$

Alfabetos linealmente crecientes $^{(2)}$

Ejemplo para $n = 3,\ t(n) = n$:

$$X^{(3,3)} = 0,0,0,1,0,0,2,0,1,1,0,1,2,0,2,1,0,2,2,1,1,1,2,1,2,2,2;$$

$$C^{(3)} = \frac{0}{3},\frac{0}{3},\frac{0}{3},\frac{1}{3},\frac{0}{3},\frac{0}{3},\frac{2}{3},\frac{0}{3},\frac{1}{3},\frac{1}{3},\frac{0}{3},\frac{1}{3},\frac{2}{3},\frac{0}{3},$$
$$\frac{0}{3},\frac{2}{3},\frac{1}{3},\frac{0}{3},\frac{2}{3},\frac{2}{3},\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3};$$

$$D^{(3)} = \underbrace{\frac{0}{3},\frac{0}{3},\ldots,\frac{2}{3},\frac{2}{3}}_{C^{(3)}},\underbrace{\frac{0}{3},\frac{0}{3},\ldots,\frac{2}{3},\frac{2}{3}}_{C^{(3)}},\underbrace{\frac{0}{3},\frac{0}{3},\ldots,\frac{2}{3},\frac{2}{3}}_{C^{(3)}}.$$

Secuencia L (1)

Definición (Esta tesis)

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, la secuencia $L^{(t)}$ se define como la concatenación de las secuencias $D^{(n,t)}$ para $n = 1, 2, 3, \ldots$:

Secuencia L (1)

Definición (Esta tesis)

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, la secuencia $L^{(t)}$ se define como la concatenación de las secuencias $D^{(n,t)}$ para $n = 1, 2, 3, \ldots$:

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

Secuencia L (1)

Definición (Esta tesis)

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, la secuencia $L^{(t)}$ se define como la concatenación de las secuencias $D^{(n,t)}$ para $n = 1, 2, 3, \ldots$:

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

Ahora, enunciamos el aporte principal de esta tesis.

Secuencia L (1)

Definición (Esta tesis)

Dada $t : \mathbb{N} \mapsto \mathbb{N}$, la secuencia $L^{(t)}$ se define como la concatenación de las secuencias $D^{(n,t)}$ para $n = 1, 2, 3, \ldots$:

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

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 $L^{(t)}$ es completamente equidistribuida.

Secuencia $L^{(2)}$

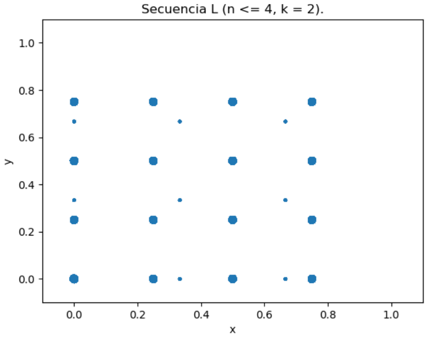

Figura 4: Secuencia $L^{(t)}$ con $t(n) = n^2$ en dos dimensiones.

Secuencia $L^{(2)}$

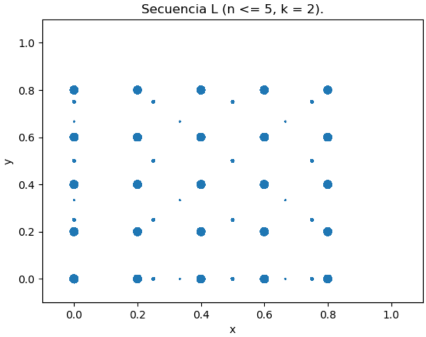

Figura 4: Secuencia $L^{(t)}$ con $t(n) = n^2$ en dos dimensiones.

Idea de la demostración $^{(1)}$

Recordando la definición, queremos probar que para cualquier k vale:

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

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

Idea de la demostración [1]

Recordando la definición, queremos probar que para cualquier k vale:

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

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

Queremos contar cuántas ventanas $\bar{w}_i$ caen adentro de un I arbitrario.

Idea de la demostración $^{(1)}$

Recordando la definición, queremos probar que para cualquier k vale:

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

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

Queremos contar cuántas ventanas $\bar{w}_i$ caen adentro de un I arbitrario.

Pensemos en los primeros N elementos de la secuencia L. Este prefijo $L_{1:N}$ se puede partir en cuatro partes:

Idea de la demostración $^{(1)}$

Recordando la definición, queremos probar que para cualquier k vale:

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

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

Queremos contar cuántas ventanas $\bar{w}_i$ caen adentro de un I arbitrario.

Pensemos en los primeros N elementos de la secuencia L. Este prefijo $L_{1:N}$ se puede partir en cuatro partes:

$$L_{1:N} = \left\langle S^{(1)}; S^{(2)}; S^{(3)}; S^{(4)} \right\rangle$$

Idea de la demostración $^{(2)}$

Calculamos cuántas ventanas pertenecen a I en cada parte. Después sumamos, dividimos por N, y tomamos el límite. El resultado es $Pr(\bar{w}_i \in I)$.

Idea de la demostración $^{(2)}$

Calculamos cuántas ventanas pertenecen a I en cada parte. Después sumamos, dividimos por N, y tomamos el límite. El resultado es $Pr(\bar{w}_i \in I)$.

Para las partes $S^{(1)}$ y $S^{(4)}$, podemos acotar la cantidad de ventanas por la longitud del segmento. Para las partes $S^{(2)}$ y $S^{(3)}$, necesitamos el siguiente lema:

Idea de la demostración $^{(2)}$

Calculamos cuántas ventanas pertenecen a I en cada parte. Después sumamos, dividimos por N, y tomamos el límite. El resultado es $Pr(\bar{w}_i \in I)$.

Para las partes $S^{(1)}$ y $S^{(4)}$, podemos acotar la cantidad de ventanas por la longitud del segmento. Para las partes $S^{(2)}$ y $S^{(3)}$, necesitamos el siguiente lema:

Lema

Dado un entero positivo k y un conjunto $I \subseteq [0,1)^k$, sea $n \in \mathbb{N}$ tal que $k \leq n$. Luego, para algún $\varepsilon \in (-1,1)$:

$$\sum_{i=1}^{n^n} \sigma\Big(\big(W_k^c(C^{(n)}) \big)_i \in I \Big) = n^n |I| + n^{n-1}(2^k - 1)\varepsilon.$$

Comentarios sobre la demostración

La prueba de Knuth usa la propiedad de que los denominadores son potencias de 2. Con el lema previo, podemos hacer la cuenta para cualquier denominador arbitrario.

Comentarios sobre la demostración

La prueba de Knuth usa la propiedad de que los denominadores son potencias de 2. Con el lema previo, podemos hacer la cuenta para cualquier denominador arbitrario.

Transformamos los números racionales en $C^{(n)}$ a enteros. La condición $\bar{w}_i \in I$ se transforma en un sistema de inecuaciones. Podemos contar la cantidad de soluciones dentro de $C^{(n)}$ gracias a la propiedad de De Bruijn.

Comentarios sobre la demostración

La prueba de Knuth usa la propiedad de que los denominadores son potencias de 2. Con el lema previo, podemos hacer la cuenta para cualquier denominador arbitrario.

Transformamos los números racionales en $C^{(n)}$ a enteros. La condición $\bar{w}_i \in I$ se transforma en un sistema de inecuaciones. Podemos contar la cantidad de soluciones dentro de $C^{(n)}$ gracias a la propiedad de De Bruijn.

Las condiciones sobre t surgen como medio para garantizar que el límite sobre la parte $S^{(4)}$ se vaya a 0.

Comentarios sobre la demostración

La prueba de Knuth usa la propiedad de que los denominadores son potencias de 2. Con el lema previo, podemos hacer la cuenta para cualquier denominador arbitrario.

Transformamos los números racionales en $C^{(n)}$ a enteros. La condición $\bar{w}_i \in I$ se transforma en un sistema de inecuaciones. Podemos contar la cantidad de soluciones dentro de $C^{(n)}$ gracias a la propiedad de De Bruijn.

Las condiciones sobre t surgen como medio para garantizar que el límite sobre la parte $S^{(4)}$ se vaya a 0.

También damos una prueba alternativa más sencilla, aunque no es elemental ya que se basa en el criterio de Weyl.

Problemas abiertos

Líneas de investigación futura:

Problemas abiertos

Líneas 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

Líneas 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?
- ¿Qué pasa si cambiamos las secuencias de De Bruijn por alguna de sus variantes?

Problemas abiertos

Líneas 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?
- ¿Qué pasa si cambiamos las secuencias de De Bruijn por alguna de sus variantes?
- Relacionado: ¿cumple la secuencia L la propiedad de correlación de pares de Poisson?

¿Preguntas?

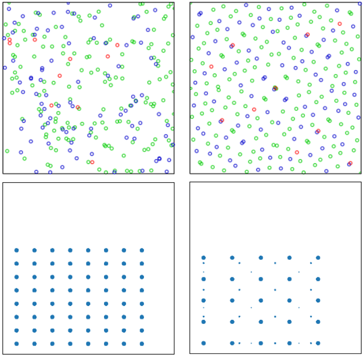

Figura 5: Secuencias 2-distribuidas.