Universidad de Buenos Aires
Facultad de Ciencias Exactas y Naturales
Departamento de Computación

Collares Aritméticos

Tesis de Licenciatura en Ciencias de la Computación

Alan Solowieiczyk

Directora: Verónica Becher

Buenos Aires, Octubre 2025

COLLARES ARITMÉTICOS

Fijemos un alfabeto. Un collar (n, k)-perfecto es una secuencia circular de símbolos del alfabeto donde cada bloque de longitud n ocurre k veces, pero en posiciones con distinta congruencia modulo k, para cualquier convención de la posición inicial. Una clase particular de collares perfectos es la de los collares aritméticos. Son collares (n, n)-perfectos generados a partir de una progresión aritmética. En esta tesis nos concentramos en collares aritméticos en el alfabeto de dos símbolos e investigamos cuán balanceados están los dos símbolos en distintas partes del collar. Identificamos el collar aritmético mágico que admite una partición en segmentos totalmente balanceados. Damos una formula cerrada para el máximo desbalance en el collar aritmético ordenado. Además damos propiedades que cumplen todos los collares aritméticos.

Palabras claves: collares aritméticos, collares perfectos, secuencias De Bruijn, progresiones aritméticas, discrepancia discreta.

Índice general

1. INTRODUCCIÓN

Esta tesis forma parte de las investigaciones sobre la equidistribución de símbolos y de bloques de símbolos en secuencias sobre un alfabeto dado. Por ejemplo, las secuencias pueden ser códigos de la teoría de la información, o representaciones de números en bases enteras. Las investigaciones en la década de 1970 mostraron que es imposible una distribución totalmente justa: fijado un alfabeto, es imposible que una secuencia infinita de símbolos tenga en sus segmentos iniciales, todos los símbolos del alfabeto con exactamente la misma frecuencia, y todos los bloques de símbolos de igual tamaño con exactamente la misma frecuencia. Sin embargo, es posible construir secuencias con una distribución casi justa y es un problema de investigación construir secuencias con la distribución más justa posible, ver [3, 5].

En el caso de las secuencias finitas también es necesario dar construcciones donde los símbolos del alfabeto estén equidistribuidos y los distintos bloques de símbolos de cada tamaño también lo estén. Nos interesa dar construcciones donde sepamos cuánto es el máximo desbalance que se puede alcanzar a lo largo de la secuencia.

En esta tesis nos dedicamos a los *collares aritméticos*, que son un subconjunto propio de los collares perfectos definidos en [1], que a su vez son variantes de las clásicas secuencias de Bruijn [7, 9, 13].

Comencemos con la definición de las secuencias de Bruijn y algunos de sus aspectos salientes. Fijemos un alfabeto finito A. Una palabra es una secuencia finita de símbolos del alfabeto A. Una palabra circular, o collar, es la clase de equivalencia de una palabra bajo rotaciones. Una secuencia de Bruijn de orden n es un collar tal que todas las palabras de longitud n ocurren exactamente un vez. Por ejemplo,

$$0000111101100101$$

es una secuencia de Bruijn de orden 4 en el alfabeto $A = \{0, 1\}$. Nicholaas de Bruijn [7] demostró que hay una correspondencia uno a uno entre secuencias de Bruijn y ciclos eulerianos en los llamado grafos de Bruijn. Para una presentación de la secuencias de Bruijn ver el libro de Knuth [12].

Para enteros positivos n y k, un collar es (n, k)-perfecto si cada palabra de longitud n ocurre exactamente k veces en posiciones con distinta congruencia módulo k, para cualquier convención de posición inicial. Los collares $(n, 1)$-perfectos son exactamente las secuencias de Bruijn de orden n. Los collares (n, k)-perfectos se corresponden con los ciclos eulerianos en los grafos que son el producto entre el grafo de Bruijn y un ciclo simple. Los collares perfectos fueron definidos por Álvarez, Becher, Ferrari y Yuhjtman en [1].

En lo que sigue, dado un alfabeto A, llamamos b a su cantidad de símbolos. Sin périda de generalidad todo alfabet de b símbolos se puede representar como $\{0, 1, \dots b - 1\}$.

Los llamados collares perfectos anidados son un conjunto particular de collares perfectos que

tienen un balance sorprendente tanto de símbolos, como de bloques de simbolos. Un collar es (n, k)-perfecto anidado si $n = 1$ o es la concatenación de b collares $(n-1, k)$-perfectos anidados. Por ejemplo, este es un collar $(2, 2)$-perfecto anidado en el alfabeto $A = \{0, 1\}$,

$$\underbrace{0011}_{\text{(1,2)-perfecto}}\overbrace{0110}^{\text{(1,2)-perfecto}}$$

Los collares perfectos anidados fueron concebidos por Becher y Carton en [4].

Los collares aritméticos de orden n son collares que se construyen concatenando uno tras otro los b^n bloques de longitud n que surgen de los términos sucesivos de una progresión aritmética de diferencia coprima con la cardinalidad del alfabeto. Cada término debe ser escrito como un número entero en base b en un bloque de n símbolos.

Un collar aritmético de orden n es la concatenación de b^n bloques de longitud n, el j-ésimo bloque es la representación en base b del número $dj \mod b^n$, para un valor de d coprimo con b. En [1, Teorema 5] se demuestra que los collares aritméticos de orden n son collares (n, n)-perfectos.

Así, para todo entero positivo n, la concatenación de todas las palabras de longitud n en orden lexicográfico es un collar aritmético que proviene de la progresión aritmética de diferencia 1. Por ejemplo para el alfabeto de $A = \{0, 1\}$ es 000 001 010 011 100 101 110 111. A este collar lo llamamos el collar ordenado.

Nos interesa aqui una propiedad de las secuencias de Bruijn y en los collares perfectos llamada *discrepancia discreta*, que mide cuánto difiere la secuencia de ser completamente balanceada respecto de las ocurrencias de distintos símbolos y los distintos bloques de símbolos de la misma longitud [3]. Hasta el momento sólo se conocen la mínima y la máxima discrepancia discreta alcanzables de secuencias de Bruijn, cuando contamos solamente símbolos [6, 8, 2], En cambio, sí se conoce la discrepancia discreta de los collares perfectos anidados [14, 11, 10, 4].

Esta tesis da un primer paso en el problema de determinar la discrepancia discreta de los collares aritméticos.

2. DEFINICIONES

Sea A un alfabeto finito. Una palabra es una secuencia finitas de símbolos. Escribimos A^* para el conjunto de todas las palabras sobre A, y A^ℓ para el conjunto de palabras de longitud exactamente ℓ.

Sea $s \in A^*$ una palabra , numeramos sus posiciones desde 1 hasta $|s|$. Para $1 \leq M \leq N \leq |s|$, denotamos por $s[M, N]$ al *substring* (intervalo) de s comprendido entre las posiciones M y N (ambos inclusive).

Para una palabra $s \in A^*$ y otra palabra $B \in A^*$, denotamos por $|S|_B$ la cantidad de *ocurrencias* de B en S. Por ejemplo, $|0001|_{00} = 2$.

Definición (Collares aritméticos)**.** *Sea A un alfabeto finito y sea b su cardinalidad. Sea d un entero positivo coprimo con b. La* secuencia aritmética *generada por d es*

$$0, d, 2d, 3d, \ldots \pmod{b^n}.$$

Llamamos collar aritmético de orden n de diferencia d a la secuncia circular que resulta de la concatenación de b^n bloques de longitud n, el j-ésimo bloque es la representación en base b del número $d\ j \mod b^n$.

En [1, Teorema] se demuestra que para todo entero positivo d coprimo con $|A|$ la secuencia aritmética generada por d induce un collar perfecto. En particular, los collares aritméticos son collares (n, n)-perfectos.

Para estudiar el desbalance en collares perfectos usamos la noción clásica de discrepancia discreta.

Definición (Discrepancia discreta)**.** *Sea $s \in A^*$ y sean $M, N \in \mathbb{N}$, $1 \leq M \leq N \leq |s|$.*

$$D(s, M, N) = \max_{1 \leq \ell \leq n} \left(\max_{B \in A^\ell} |s[M, N]|_B \ - \ \min_{B \in A^\ell} |s[M, N]|_B \right),$$

$$D(s) = \max_{(M,N):1 \leq M \leq N} D(s, M, N)$$

Definición (Discrepancia de símbolo)**.**

$$\Delta(s, M, N) = \max_{a \in A} |s[M, N]|_a \ - \ \min_{a \in A} |s[M, N]|_a,$$

Es la discrepancia discreta para $\ell = 1$ y nos da la diferencia entre la cantidad de veces que aparece el símbolo que más aparece y el que menos, en las posiciones desde M hasta N.

$$\Delta(s) = \max_{(M,N):1 \leq M \leq N} \Delta(s, M, N)$$

En particular $A = \{0, 1\}$:

$$\Delta(s, M, N) = | \, |s[M, N]|_0 - |s[M, N]|_1 \, |$$

3. EL COLLAR ARITMÉTICO ORDENADO

Llamamos *collar ordenado* de orden n, al collar aritmético de orden n con diferencia $d = 1$. .

Teorema 1. *Sea s el collar ordenado de orden n para el alfabeto $\{0,1\}$. Entonces, para $n \cdot q$ con $1 \leq q \leq 2^n$ es*

$$\Delta(s, 1, n \cdot q) \;=\; (n - \lceil \log_2 q \rceil)\, q \;+\; \sum_{i=0}^{\lceil \log_2 q \rceil - 1} \Big(2^i - \big|\, (q \bmod 2^{i+1}) - 2^i \,\big| \Big) \;.$$

Corolario 1. $\big(n - \lceil \log_2 q \rceil\big)\, q \;\leq\; \Delta(S, 1, n \cdot q) \;\leq\; \big(n + 2 - \lceil \log_2 q \rceil\big)\, q$

Del Teorema 1 deducimos que el máximo valor de $\Delta(s, 1, n \cdot q)$ es 2^{n-1} y se alcanza con $q = 2^{n-1}$, es decir, exactamente q es el bloque que está en la mitad del collar aritmético ordenado.

3.1. Demostración del Teorema 1

Dados $n > 0$ y q con $1 \leq q \leq 2^n$ tenemos:

$$\Delta(s, 1, n \cdot q) \;=\; |s[1, n \cdot q]|_0 \; - |s[1, n \cdot q]|_1$$

donde $|s[1, n \cdot q]|_0$ y $|s[1, n \cdot q]|_1$ denotan, respectivamente, la cantidad de ceros y unos que hay hasta la posición $n \cdot q$ de S. Por lo que:

$$n \cdot q = |s[1, n \cdot q]|_0 \; + |s[1, n \cdot q]|_1$$

Además, como el collar ordenado es el orden lexicografico, vale que $s[1, n \cdot q]|_0 \geq s[1, n \cdot q]|_1$, luego:

$$\Delta(s, 1, n \cdot q) \;=\; 2\,|s[1, n \cdot q]|_0 \;-\; n \cdot q.$$

Fijado un bit i entre 0 y $n - 1$, al enumerar $j = 0, 1, 2, \ldots$ en binario usando n bits si en cada bloque miramos el bit en la posición i, se observa el patrón

$$\underbrace{0\,0 \cdots 0}_{2^i \text{ veces}}\;\underbrace{1\,1 \cdots 1}_{2^i \text{ veces}}$$

Es decir, si miramos la posición i de cada bloque de longitud n , vemos que aparece el cero 2^i veces y luego el uno 2^i veces, y esto se repite indefinidamente.

Definimos, para cada i entre 0 y $n - 1$,

$$c_i \;=\; \Big\lfloor \frac{q}{2^{i+1}} \Big\rfloor \qquad \text{y} \qquad t_i \;=\; q \bmod 2^{i+1} \;\in\; \{0, 1, \ldots, 2^{i+1} - 1\}.$$

Es decir, c_i es la cantidad de veces del patrón $0^{2^i}1^{2^i}$ dentro de los primeros q valores de j, y t_i es el *resto* que queda al final.

En resumen, hay exactamente 2^i ceros si contamos la posición i de cada bloque, lo que produce un aporte de $c_i\,2^i$ ceros. En el resto de longitud t_i, el conteo adicional de ceros es:

$$\text{ceros extra} = \begin{cases} t_i, & \text{si } t_i \le 2^i \quad \text{(todo dentro del bloque de ceros);} \\ 2^i, & \text{si } t_i > 2^i \quad \text{(se cubre todo el bloque de ceros y se entra en unos).} \end{cases}$$

Esto se resume como un mínimo:

$$\text{ceros extra} \;=\; \text{mín}(2^i,\, t_i).$$

Luego, el número exacto de ceros en el bit i entre $0 \le j < q$ es

$$Z_i(q) \;=\; c_i\,2^i \;+\; \text{mín}\big(2^i,\; t_i\big).$$

Sumando sobre todos los bits:

$$|s[1, n\cdot q]|_0 \;=\; \sum_{i=0}^{n-1} Z_i(q).$$

Por definición,

$$\Delta(s, 1, n\cdot q) \;=\; \sum_{i=0}^{n-1} \big(2Z_i(q) - q\big).$$

usando $q = c_i\,2^{i+1} + t_i$ y la fórmula de $Z_i(q)$,

$$2Z_i(q) \;=\; c_i\,2^{i+1} + 2\,\text{mín}(2^i, t_i) \quad\Rightarrow\quad 2Z_i(q) - q \;=\; 2\,\text{mín}(2^i, t_i) - t_i.$$

Por lo tanto,

$$\Delta(s, 1, n\cdot q) \;=\; \sum_{i=0}^{n-1} \Big(2\,\text{mín}(2^i, t_i) - t_i\Big).$$

Observación: para cada i, el término está acotado por $0 \le 2\,\text{mín}(2^i, t_i) - t_i \le 2^i$, con máximo en $t_i = 2^i$.

En la suma que define $\Delta(s, 1, n\cdot q)$,

$$\Delta(s, 1, n\cdot q) \;=\; \sum_{i=0}^{n-1} \big(2\,\text{mín}(2^i, t_i) - t_i\big), \quad \text{con} \quad t_i = q \bmod 2^{i+1},$$

aparece un fenómeno que simplifica el cálculo para los bits de índice grande.

Idea: si i es suficientemente grande como para que $2^i \ge q$, el *bit* i **nunca cambia a 1** en los bloques correspondientes a j con $0 \le j < q$. En otras palabras, los 2^i ceros que forman parte del patrón $0^{2^i}1^{2^i}$ son más que todo el rango considerado. Por lo tanto:

$$Z_i(q) = q,$$

ya que para todos esos j el bit i vale 0.

Sea

$$m = \lceil \log_2 q \rceil.$$

Entonces:

Para $i \geq m$, se cumple $2^i \geq q$, por lo que *bit* i es siempre 0.

Para $i < m$, el bit alterna entre 0 y 1 dentro del rango $0 \leq j < q$, y requiere el cálculo general.

Si $i \geq m$ tenemos $t_i = q$ (ya que $q < 2^{i+1}$) y, por ende,

$$2\,\text{mín}(2^i, t_i) - t_i = 2q - q = q.$$

Esto significa que cada *bit alto* ($i \geq m$) aporta exactamente q a la suma.

Podemos entonces separar la contribución de los bits altos de la de los bits bajos:

$$\Delta(S, n \cdot q) = (n - m) \cdot q \; + \; \sum_{i=0}^{m-1} \left(2\,\text{mín}(2^i, t_i) - t_i\right)$$

Aquí:

El término $(n - m) \cdot q$ corresponde a la suma de todos los bits altos, que aportan q cada uno.

La suma de $i = 0$ a $m - 1$ corresponde a los bits *bajos* que sí alternan y cuyo aporte depende de t_i.

Dado que

$$2\,\text{mín}(2^i, t_i) - t_i \; = \; 2^i - \left| \, t_i - 2^i \, \right|,$$

obtenemos

$$\Delta(s, 1, n \cdot q) \; = \; (n - m)\, q \; + \; \sum_{i=0}^{m-1} \left(2^i - \left| \, t_i - 2^i \, \right|\right) .$$

Es decir,

$$\Delta(s, 1, n \cdot q) \; = \; (n - \lceil \log_2 q \rceil)\, q \; + \; \sum_{i=0}^{\lceil \log_2 q \rceil - 1} \left(2^i - \left| \, (q \bmod 2^{i+1}) - 2^i \, \right|\right) .$$

Queda demostrado el Teorema 1 □

3.2. Demostración de Corolario 1

Demostración. Sea q entre 1 y 2^n. Para $0 \leq i < \lceil \log_2 q \rceil - 1$ tenemos

$$0 \; \leq \; 2^i - \left| \, (q \bmod 2^{i+1}) - 2^i \, \right| \; \leq \; 2^i.$$

Por lo tanto,

$$\sum_{i=0}^{\lceil \log_2 q \rceil - 1} \Big(2^i - \big|\, (q \bmod 2^{i+1}) - 2^i \,\big| \Big)$$

se acota por abajo con 0 y por arriba con $2^{\lceil \log_2 q \rceil} - 1$. La cota superior se obtiene observando que cada término de la suma cumple

$$2^i - |(q \bmod 2^{i+1}) - 2^i| \leq 2^i.$$

Al sumar estos valores para $i = 0, \ldots, \lceil \log_2 q \rceil - 1$, se tiene

$$\sum_{i=0}^{\lceil \log_2 q \rceil - 1} \big(2^i - |(q \bmod 2^{i+1}) - 2^i|\big) \leq \sum_{i=0}^{\lceil \log_2 q \rceil - 1} 2^i = 2^{\lceil \log_2 q \rceil} - 1$$

por ser una suma geométrica.

Luego,

$$\begin{aligned}
\big(n - \lceil \log_2 q \rceil\big) q \;&\leq\; \Delta(s, 1, n \cdot q) \;\leq\; \big(n - \lceil \log_2 q \rceil\big) q + \big(2^{\lceil \log_2 q \rceil} - 1\big) \\
\big(n - \lceil \log_2 q \rceil\big) q \;&\leq\; \Delta(s, 1, n \cdot q) \;\leq\; \big(n - \lceil \log_2 q \rceil\big) q + 2q \\
\big(n - \lceil \log_2 q \rceil\big) q \;&\leq\; \Delta(s, 1, n \cdot q) \;\leq\; \big(n + 2 - \lceil \log_2 q \rceil\big) q
\end{aligned}$$

□

4. EL COLLAR ARITMÉTICO MÁGICO

Fijamos el alfabeto $\{0, 1\}$. Para n par definimos el *collar mágico* orden n, como el collar aritmético de orden n y diferencia $d = 2^{n/2} + 1$.

Sea k un entero positivo, sea $n = 2k$, y sea $d = 2^k + 1$. Sea $S = (d\ x \mod 2^n)_{0 \le x < 2^n}$.

A continuación definimos una partición del conjunto $\{0, \ldots 2^n - 1\}$ en d conjuntos $S(0), \ldots, S(d-1)$ a los que llamamos *segmentos*. Para $i = 0, \ldots d - 1$,

$$S(i) \ = \ \left\{ (d\ x) \bmod 2^n \ \middle|\ 0 \le x < 2^n,\ \left\lfloor \frac{d\ x}{2^n} \right\rfloor = i \right\}.$$

Asociamos cada $S(i)$ con un segmento del collar S, identificando cada elemento de $S(i)$ con un bloque binario de longitud n.

Teorema 2. *Sea n par. El collar mágico de orden n tiene $d = 2^{n/2} + 1$ segmentos, y cada uno tiene exactamente la misma cantidad de ceros que de unos.*

Ejemplo Caso mágico $k = 2$, por lo que $n = 4$ y $d = 5$. Sea $f(x) = 5x \bmod 16$ para $x = 0, \ldots, 15$. La secuencia generada es:

$$0, 5, 10, 15,\ 4, 9, 14,\ 3, 8, 13,\ 2, 7, 12,\ 1, 6, 11.$$

Segmentos $S(i) = \{5x \mod 16 : \lfloor 5x/16 \rfloor = i\}$:

$$\begin{aligned} S(0) &= \{0, 5, 10, 15\}, \\ S(1) &= \{4, 9, 14\}, \\ S(2) &= \{3, 8, 13\}, \\ S(3) &= \{2, 7, 12\}, \\ S(4) &= \{1, 6, 11\}. \end{aligned}$$

Segmento	**Valores en binario (4 bits)**	**#1 = #0**
$S(0)$	`0000, 0101, 1010, 1111`	$8 = 8$
$S(1)$	`0100, 1001, 1110`	$6 = 6$
$S(2)$	`0011, 1000, 1101`	$6 = 6$
$S(3)$	`0010, 0111, 1100`	$6 = 6$
$S(4)$	`0001, 0110, 1011`	$6 = 6$

Tabla 4.1: Segmentos $S(i)$ para $n = 4$, $d = 5$. En cada segmento, el total de unos y ceros (sumando los 4 bits de todos sus elementos) es el mismo; por tanto la discrepancia de símbolo es 0.

4.1. Demostración del Teorema 2

Sea un entero positivo k, sea $n = 2k$ y sea $d = 2^k + 1$. Sea $S = (d\ x \mod 2^n)_{0 \le x < 2^n}$. El tamaño de $S(0)$ es 2^k y para $i = 1, \ldots, 2^k$ el tamaño de $S(i)$ es $2^k - 1$. Demostramos aqui que para cada i, el número total de ceros en las representaciones binarias en n de todos los elementos de $S(i)$ es igual al número total de unos.

La estrategia de la demostracion consite en expresar cada $S(i)$, para $i = 1, \ldots, 2^k - 1$, en función de conjuntos $T(i)$, $D(i)$ y $D(i-1)$, y $S(2^k) = D(2^k - 1)$. Mostraremos que estos conjuntos tienen balance de ceros y unos. Dado que $S(i)$ de define a partir de estos conjuntos mediante operaciones de union y diferencia que preservan el balance, concluiremos que $S(i)$ está balancedo. Damos un ejemplo de como se ven los conjuntos antes de comenzar:

Para cada i, $0 \le i < 2^k$ definamos

$$T(i) = \{2^k \cdot ((i + j) \mod 2^k) + j : 0 \le j < 2^k\}.$$

Proposición 1. *Para $i = 0, \ldots 2^k - 1$, $\#ceros(T(i)) = \#unos(T(i))$.*

Demostración. Sea $k > 0$ entero, $i \in \{0, 1, \ldots, 2^k - 1\}$. Cada $t \in T(i)$ se escribe en binario con $2k$ bits (con ceros a la izquierda si es necesario). Sea $C(i)$ el conjunto de estos strings.

Cada $t \in T(i)$ corresponde a un par (m, j) con $m \equiv i + j \pmod{2^k}$, $m, j \in \{0, \ldots, 2^k - 1\}$, y $t = 2^k m + j$. En binario, t es la concatenación de los bits de m (mitad izquierda) y los bits de j (mitad derecha). Definimos la función $f : C(i) \to C(i)$ como la composición de:

- s: intercambiar las dos mitades de $2k$ bits: $s(2^k m + j) = 2^k j + m$.
- c: complemento a 1 (invertir todos los bits).

Es decir, $f(t) = c(s(t))$.

Verifiquemos que $f(t) \in T(i)$:

$$\begin{aligned} t &= 2^k m + j, \quad m \equiv i + j \pmod{2^k}, \\ s(t) &= 2^k j + m, \\ f(t) &= c(s(t)) = 2^k(2^k - 1 - j) + (2^k - 1 - m). \end{aligned}$$

Sean $M = 2^k - 1 - j$, $J = 2^k - 1 - m$. Entonces $f(t) = 2^k M + J$. Queremos $M \equiv i + J \pmod{2^k}$:

$$\begin{aligned} M = 2^k - 1 - j &\equiv -1 - j \pmod{2^k}, \\ i + J = i + 2^k - 1 - m &\equiv i - 1 - m \pmod{2^k}. \end{aligned}$$

De $m \equiv i + j$ tenemos $i - m \equiv -j$, luego $i - 1 - m \equiv -1 - j$. Así, $M \equiv i + J \pmod{2^k}$, por tanto $f(t) \in T(i)$.

Claramente f es una involución ($f(f(t)) = t$) y biyectiva. Además, f intercambia 0s y 1s en cada string. Luego, al sumar sobre todos los elementos de $C(i)$, el número total de 0s coincide con el total de 1s. □

Proposición 2. *Para todo* $i = 0, \dots 2^k - 1$,

1. $T(i) \subset S(i) \cup S(i+1)$.
2. $\bigcup_{\ell=0}^{i} S(\ell) \subseteq \bigcup_{\ell=0}^{i} T(\ell)$

Demostración. Por la definición de $S(\ell)$, un elemento de $S(\ell)$ es de la forma $(d \cdot y)$ mód 2^n con $\lfloor (d \cdot y)/2^n \rfloor = \ell$. Sea $y = 2^k u + v$ (con $0 \le u, v < 2^k$) y usando $d = 2^k + 1$,

$$(d \cdot y) \text{ mód } 2^n \equiv 2^k \big((u+v) \text{ mód } 2^k\big) + v \ \in \ T(u), \tag{4.1}$$

$$\left\lfloor \tfrac{d\ y}{2^n} \right\rfloor = u + \left\lfloor \tfrac{u+v}{2^k} \right\rfloor = \begin{cases} u, & v < 2^k - u \\ u+1, & v \ge 2^k - u \end{cases} \tag{4.2}$$

Item 1. Por (4.1) y (4.2) $T(u) \subset S(u) \cup S(u+1)$.

Item 2. Sea $x \in S(\ell)$ con $\ell \le i$. Entonces existe y tal que

$$x \equiv (d\, y) \text{ mód } 2^n, \qquad \left\lfloor \tfrac{d\, y}{2^n} \right\rfloor = \ell.$$

Escribimos $y = 2^k u + v$ con $0 \le u, v < 2^k$ y usamos $d = 2^k + 1$, $n = 2k$ y por (4.1) y (4.2) $\ell \in \{u, u+1\}$ y por tanto $u \in \{\ell, \ell - 1\}$ (si $\ell = 0$, forzosamente $u = 0$).

Luego, $x \in T(u) \subseteq T(\ell) \cup T(\ell - 1) \subseteq \bigcup_{m=0}^{\ell} T(m) \subseteq \bigcup_{m=0}^{i} T(m)$. Como $x \in S(\ell)$ con $\ell \le i$, concluimos

$$\bigcup_{\ell=0}^{i} S(\ell) \ \subseteq \ \bigcup_{\ell=0}^{i} T(\ell).$$

□

Para cada $i = 0, \dots, 2^k - 1$ definamos

$$D(i) = \left(\bigcup_{0 \le \ell \le i} T(\ell) \right) \setminus \left(\bigcup_{0 \le \ell \le i} S(\ell) \right).$$

Proposición 3. *Sean* k, $n = 2k$ *y* $d = 2^k + 1$. *Para* $i = 0, \dots, 2^k - 1$ *se cumple*

$$D(i) \ = \ \Big\{ 2^k \big((i+j) \text{ mód } 2^k\big) + j : \ 2^k - i \le j < 2^k \Big\}.$$

Demostración. (Pertenencia). Sea $x \in D(i)$. Luego, $x = 2^k((i+j) \text{ mód } 2^k) + j$ con $2^k - i \le j < 2^k$. Claramente $x \in T(i)$. Debemos ver que $x \notin \bigcup_{\ell=0}^{i} S(\ell)$.

Si $\ell < i$: entonces $T(i) \cap S(\ell) = \varnothing$ por Proposición 2. Entonces $x \notin S(\ell)$.

Si $\ell = i$: $x \in S(i) \iff \left\lfloor \frac{i+j}{2^k} \right\rfloor = 0 \iff i + j < 2^k \iff j < 2^k - i$. Dado que $x \in D(i)$ entonces $x = 2^k\big((i+j) \bmod 2^k\big) + j$ para $2^k - i \le j < 2^k$ por lo que $x \notin S(i)$.

(Cardinalidad). El conjunto de índices $\{j : 2^k - i \le j < 2^k\}$ tiene exactamente i valores. La aplicación $j \mapsto x = 2^k((i+j) \bmod 2^k) + j$ es inyectiva (los k bits bajos de x son exactamente los de j), así que la imagen tiene i elementos. Por otra parte,

$$\left|\bigcup_{\ell=0}^{i} T(\ell)\right| = (i+1)\,2^k \quad \text{(los } T(\ell) \text{ son disjuntos y cada uno tiene } 2^k \text{ elementos)},$$
$$\left|\bigcup_{\ell=0}^{i} S(\ell)\right| = |S(0)| + \sum_{\ell=1}^{i} |S(\ell)| = 2^k + i\,(2^k - 1) = (i+1)\,2^k - i,$$

pues los segmentos $S(\ell)$ son disjuntos y sus tamaños son 2^k para $\ell = 0$ y $2^k - 1$ para $1 \le \ell \le i$. Por Proposición 2 tenemos que $\bigcup_{\ell=0}^{i} S(\ell) \subseteq \bigcup_{\ell=0}^{i} T(\ell)$, por lo tanto

$$|D(i)| = \left|\bigcup_{\ell=0}^{i} T(\ell)\right| - \left|\bigcup_{\ell=0}^{i} S(\ell)\right| = (i+1)2^k - \big((i+1)2^k - i\big) = i.$$

Hemos probado que todo elemento de la fórmula pertenece a $D(i)$ y la fórmula produce i elementos, que coincide con $|D(i)|$. Por lo tanto, la fórmula describe exactamente $D(i)$. □

Volviendo al Ejemplo Caso mágico $k = 2$, por lo que $n = 4$ y $d = 5$. Sea $f(x) = 5x \bmod 16$ para $x = 0, \ldots, 15$. La secuencia generada es:

$$0, 5, 10, 15,\ 4, 9, 14,\ 3, 8, 13,\ 2, 7, 12,\ 1, 6, 11.$$

Segmentos $S(i) = \{5x \bmod 16 : \lfloor 5x/16 \rfloor = i\}$:

$$S(0) = \{0, 5, 10, 15\},$$
$$S(1) = \{4, 9, 14\},$$
$$S(2) = \{3, 8, 13\},$$
$$S(3) = \{2, 7, 12\},$$
$$S(4) = \{1, 6, 11\}.$$

Segmentos $T(i) = \{\, 2^k((i+j) \bmod 2^k) + j : 0 \le j < 2^k \,\}$:

$$T(0) = \{0, 5, 10, 15\},$$
$$T(1) = \{4, 9, 14, 3\},$$
$$T(2) = \{8, 13, 2, 7\},$$
$$T(3) = \{12, 1, 6, 11\}.$$

Segmentos $\big(D(i) = \bigcup_{\ell \le i} T(\ell) \setminus \bigcup_{\ell \le i} S(\ell)\big)$:

$$D(0) = \varnothing, \qquad D(1) = \{3\}, \qquad D(2) = \{2, 7\}, \qquad D(3) = \{1, 6, 11\}.$$

Proposición 4. *$S(2^k) = D(2^k - 1)$ y para $i = 1, \dots, 2^k - 1$,*

$$S(i) = (D(i-1) \cup T(i)) \setminus D(i).$$

Demostración. Denotemos

$$\mathcal{T}_{\le i} := \bigcup_{\ell=0}^{i} T(\ell), \qquad \mathcal{S}_{\le i} := \bigcup_{\ell=0}^{i} S(\ell).$$

Por definición de $D(i)$,

$$D(i) = \mathcal{T}_{\le i} \setminus \mathcal{S}_{\le i} \quad \Longleftrightarrow \quad \mathcal{S}_{\le i} = \mathcal{T}_{\le i} \setminus D(i).$$

Caso $S(2^k) = D(2^k - 1)$. Como $\{T(0), \dots, T(2^k - 1)\}$ particiona $U := \{0, \dots, 2^{2k} - 1\}$, se tiene $\mathcal{T}_{\le 2^k - 1} = U$; además $\mathcal{S}_{\le 2^k} = U$ (los $S(\ell)$ también particionan U). Luego

$$S(2^k) = \mathcal{S}_{\le 2^k} \setminus \mathcal{S}_{\le 2^k - 1} = U \setminus \mathcal{S}_{\le 2^k - 1} = \mathcal{T}_{\le 2^k - 1} \setminus \mathcal{S}_{\le 2^k - 1} = D(2^k - 1).$$

Caso $1 \le i \le 2^k - 1$. Escribimos $S(i) = \mathcal{S}_{\le i} \setminus \mathcal{S}_{\le i-1}$ y sustituimos:

$$S(i) = \big(\mathcal{T}_{\le i} \setminus D(i)\big) \ \setminus \ \big(\mathcal{T}_{\le i-1} \setminus D(i-1)\big).$$

Notar que:

$$D(i) = \Big(T(i) \ \cup \ \mathcal{T}_{\le i-1}\Big) \setminus \mathcal{S}_{\le i}$$

Usando $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$,

$$D(i) = \Big(T(i) \setminus \mathcal{S}_{\le i}\Big) \ \cup \ \Big(\mathcal{T}_{\le i-1} \setminus \mathcal{S}_{\le i}\Big).$$

Para cada $\ell < i$ ya vimos que

$$T(\ell) \subset S(\ell) \cup S(\ell + 1) \subset \mathcal{S}_{\le i},$$

luego $T(\ell) \setminus \mathcal{S}_{\le i} = \varnothing$. Por tanto,

$$D(i) = T(i) \setminus \mathcal{S}_{\le i} \ \subseteq \ T(i).$$

Aplicamos la identidad:

$$(A \setminus C) \setminus (B \setminus D) = \big((A \setminus B) \setminus C\big) \ \cup \ \big((A \cap D) \setminus C\big), \quad \text{válida cuando } B \subseteq A,$$

con $A = \mathcal{T}_{\leq i}$, $B = \mathcal{T}_{\leq i-1}$, $C = D(i)$, $D = D(i-1)$ (nótese que $B \subseteq A$). Obtenemos

$$S(i) = \underbrace{\big((\mathcal{T}_{\leq i} \setminus \mathcal{T}_{\leq i-1}) \setminus D(i)\big)}_{= T(i)\setminus D(i)} \cup \underbrace{\big((\mathcal{T}_{\leq i} \cap D(i-1)) \setminus D(i)\big)}_{= D(i-1)}$$

donde usamos que $\mathcal{T}_{\leq i} \setminus \mathcal{T}_{\leq i-1} = T(i)$ (los Ts son disjuntos), que $D(i-1) \subseteq \mathcal{T}_{\leq i-1} \subseteq \mathcal{T}_{\leq i}$, y que $D(i-1) \cap D(i) = \varnothing$ (pues $D(i-1) \subseteq T(i-1)$ y $D(i) \subseteq T(i)$, con $T(i-1) \cap T(i) = \varnothing$). Finalmente, dado que los Ds son disjuntos entre si:

$$S(i) = \big(T(i) \setminus D(i)\big) \cup D(i-1) = \big(D(i-1) \cup T(i)\big) \setminus D(i).$$

□

Dado un entero m entre 0 y $2^k - 1$, #ceros(m) es la cantidad de ceros en la representación binaria de m en k dígitos y análogamente definimos #unos(m).

Proposición 5. *Para $i = 0, \dots 2^k - 1$, $j = 0, \dots 2^k - 1$,*

$$\sum_{m=0}^{i-1} \#ceros(m) - \sum_{j=0}^{2^k-i-1} \#ceros(j) = \sum_{m=0}^{i-1} \#unos(m) - \sum_{j=0}^{2^k-i-1} \#unos(j).$$

Demostración. Definimos

$$\begin{aligned} A &= \{0, 1, \dots, i-1\}, \\ B &= \{i, i+1, \dots, 2^k - i - 1\}, \\ C &= \{2^k - i, \dots, 2^k - 1\}. \end{aligned}$$

Notemos que $A \cup B = \{0, 1, \dots, 2^k - i - 1\}$. Para cualquier $x \in \{0, 1, \dots, 2^k - 1\}$, la representación binaria de $2^k - 1 - x$ intercambia de ceros y unos de la de x. Por lo tanto

$$\begin{aligned} \sum_{x\in A} \#\text{ceros}(x) &= \sum_{x\in C} \#\text{unos}(x), \\ \sum_{x\in A} \#\text{unos}(x) &= \sum_{x\in C} \#\text{ceros}(x) \\ \sum_{x=0}^{2^k-1} \#\text{ceros}(x) &= \sum_{x=0}^{2^k-1} \#\text{unos}(x) = k \cdot 2^{k-1}. \end{aligned}$$

Expresando en términos de A, B, C,

$$\sum_{x\in A} \#\text{ceros}(x) + \sum_{x\in B} \#\text{ceros}(x) + \sum_{x\in C} \#\text{ceros}(x) = k \cdot 2^{k-1},$$

$$\sum_{x\in A} \#\text{unos}(x) + \sum_{x\in B} \#\text{unos}(x) + \sum_{x\in C} \#\text{unos}(x) = k \cdot 2^{k-1}.$$

Restando

$$\left(\sum_A \#\text{ceros} - \sum_A \#\text{unos}\right) + \left(\sum_B \#\text{ceros} - \sum_B \#\text{unos}\right) + \left(\sum_C \#\text{ceros} - \sum_C \#\text{unos}\right) = 0.$$

Usando la simetría

$$\sum_C \#\text{ceros} - \sum_C \#\text{unos} = -\left(\sum_A \#\text{ceros} - \sum_A \#\text{unos}\right).$$

Sustituyendo

$$\left(\sum_A \#\text{ceros} - \sum_A \#\text{unos}\right) + \left(\sum_B \#\text{ceros} - \sum_B \#\text{unos}\right) - \left(\sum_A \#\text{ceros} - \sum_A \#\text{unos}\right) = 0,$$

lo que implica

$$\sum_B \#\text{ceros} = \sum_B \#\text{unos}.$$

Por lo tanto se cumple la igualdad. □

Escribamos $\#\text{ceros}(D(i))$ para la suma de la totalidad de ceros necesarios para escribir cada elemento de $D(i)$ en n bits. Análogamente definimos $\#\text{unos}(D(i))$.

Proposición 6. *Para todo $i = 0, \dots 2^k - 1$, $\#ceros(D(i)) = \#unos(D(i))$.*

Demostración. Para $i = 0, 1, \dots, 2^k - 1$,

$$D(i) = \{2^k \cdot ((i+j) \mod 2^k) + j : 2^k - i \leq j < 2^k\}.$$

Cada $a \in D(i)$ tiene forma $a = 2^k \cdot a_h + a_\ell$, con $a_h \in \{0, \dots, i-1\}$, $a_\ell \in [2^k - i, 2^k - 1]$.

$$\#\text{ceros}(D(i)) = \sum_{m=0}^{i-1} \#\text{ceros}(m) + \sum_{j=2^k-i}^{2^k-1} \#\text{ceros}(j),$$

$$\#\text{unos}(D(i)) = \sum_{m=0}^{i-1} \#\text{unos}(m) + \sum_{j=2^k-i}^{2^k-1} \#\text{unos}(j).$$

Usando el balance de $\{0, \dots, 2^k - 1\}$ es decir, usando que

$$\sum_{j=0}^{2^k-1} \#\text{ceros}(j) = \sum_{j=0}^{2^k-1} \#\text{unos}(j) = k \cdot 2^{k-1}$$

tenemos que

$$\sum_{j=2^k-i}^{2^k-1} \#\text{ceros}(j) = k \cdot 2^{k-1} - \sum_{j=0}^{2^k-i-1} \#\text{ceros}(j),$$

$$\sum_{j=2^k-i}^{2^k-1} \#\text{unos}(j) = k \cdot 2^{k-1} - \sum_{j=0}^{2^k-i-1} \#\text{unos}(j).$$

Luego,

$$\#\text{ceros}(D(i)) = \sum_{m=0}^{i-1} \#\text{ceros}(m) + k \cdot 2^{k-1} - \sum_{j=0}^{2^k-i-1} \#\text{ceros}(j),$$

$$\#\text{unos}(D(i)) = \sum_{m=0}^{i-1} \#\text{unos}(m) + k \cdot 2^{k-1} - \sum_{j=0}^{2^k-i-1} \#\text{unos}(j).$$

Por Proposición 5

$$\sum_{m=0}^{i-1} \#\text{ceros}(m) - \sum_{j=0}^{2^k-i-1} \#\text{ceros}(j) = \sum_{m=0}^{i-1} \#\text{unos}(m) - \sum_{j=0}^{2^k-i-1} \#\text{unos}(j).$$

Concluimos que $\#\text{ceros}(D(i) = \#\text{unos}(D(i))$. □

Demostración del Teorema 2. Decimos que un conjunto de números es balanceado si al representar cada número en n bits, la cantidad total de ceros es igual cantidad total de unos. La unión de conjuntos balanceados es balanceada y que la diferencia de conjuntos balanceado también es balanceada. Las Proposiciones 1 y 6 nos dicen que, para $i = 0, \dots 2^k - 1$, tanto $D(i)$ como $T(i)$ son balanceados. Por lo tanto cada $S(i)$ lo es. Concluimos que para $i = 0, \dots 2^k$, $\#\text{ceros}(S(i)) = \#\text{unos}(S(i))$. □

5. SOBRE COLLARES ARITMÉTICOS

5.1. Los collares aritméticos son un juego de opuestos

Sea n un entero positivo y sea d impar entre 1 y $2^n - 1$. Sea S el collar aritmético de orden n y diferencia d. Para $i = 0, \ldots, d-1$ definimos los segmentos

$$S(i) \;=\; \left\{ (d\ x) \text{ mód } 2^n \;\middle|\; 0 \le x < 2^n,\ \left\lfloor \frac{dx}{2^n} \right\rfloor = i \right\}.$$

Asociamos cada $S(i)$ con un segmento del collar S. El orden en que aparecen los segmentos en el collar S se puede escribir fácilmente. Llamamos cabeza del segmento $S(i)$ al elemento $(d\ x) \mod 2^n$ donde $x = \min\limits_{0 \le y < 2^n} \left\lfloor \dfrac{d\ y}{2^n} \right\rfloor = i$.

Si escribimos $r = 2^n \mod d$, entonces las cabezas de los segmentos van recorriendo los residuos de a pasos de $-r$ módulo d. Es decir, el primer segmento arranca en 0, el segundo en $d - r$, el siguiente en $d - 2r$, y así sucesivamente hasta recorrer exactamente todos los números entre 0 y $d - 1$, siempre tomando módulo d.

Decimos que dos segmentos $\{u_0, \ldots u_m\}$ y $\{v_1, \ldots v_m\}$ son opuestos cuando para cada $\ell = 0, \ldots, m$,

$$u_\ell = 2^n - 1 - v_{m-\ell}.$$

Dado $S(i) = \{u_0, \ldots u_m\}$, definimos

$$S(i)^{\complement} = \{2^n - 1 - u_{m-j} : 0 \le j \le m\}.$$

A continuación demostramos que cada segmento tiene un segmento opuesto. Primero mostramos que si un segmento tiene cabeza s entonces termina con $2^n - k$ con k entre 1 y d y el opuesto empieza en $k - 1$.

Proposición 7 (Orden de los segmentos)**.** *Sea $r = 2^n \mod d$. Entonces las cabezas de los segmentos forman la sucesión*

$$s_0 = 0, \qquad s_{i+1} \equiv s_i - r \pmod d,$$

y en consecuencia

$$s_i \equiv -\,i\,r \pmod d, \qquad i = 0, 1, \ldots, d-1.$$

Es decir, las cabezas recorren los residuos de a pasos de $-r$ módulo d:

$$0,\ d-r,\ d-2r,\ \ldots,\ d-(d-1)r \pmod d,$$

hasta cubrir exactamente todos los números de 0 a $d - 1$.

Demostración. Cada elemento consecutivo de la secuencia aritmética suma d módulo 2^n. Por lo tanto, cada vez que la suma parcial $d \cdot x$ pasa un múltiplo de 2^n, el cociente $\lfloor d\, x/2^n \rfloor$ aumenta en 1 y comienza un nuevo segmento. El residuo al dividir 2^n por d es r, de modo que el *desplazamiento* entre cabezas consecutivas es exactamente $-r \pmod d$. Iterando, obtenemos $s_i \equiv -ir \pmod d$, lo que recorre una permutación completa de $\{0, \ldots, d-1\}$ porque r es coprimo con d. □

Lemma 1 (Forma interna de un segmento)**.** *Sea $n \in \mathbb{N}$ y d impar. El segmento $S(i)$ es una progresión aritmética módulo 2^n con razón d y longitud $L_i \in \{2^k - 1, 2^k\}$. Si s es la cabeza de $S(i)$, entonces el último elemento de $S(i)$ es $s + (L_i - 1)d$ y $s + (L_i - 1)d \equiv 2^n - k \pmod{2^n}$ con $1 \le k \le d$, y $k \equiv 2^n - s \pmod d$.*

Proposición 8 (Opuesto por complemento y orden inverso)**.** *Sea S un collar aritmético de orden n y diferencia d. Para todo i tal que $0 \le i \le d-1$ existe ℓ tal que $0 \le \ell \le d-1$ y $S(i)^{\complement} = S(\ell)$.*

Demostración. Escribamos $S(i)$ como en el Lema 1,

$$y_j \equiv s + jd \pmod{2^n}, \qquad j = 0, 1, \ldots, L_i - 1,$$

con $y_{L_i-1} \equiv 2^n - k \pmod{2^n}$ y $1 \le k \le d$. Consideremos ahora la sucesión

$$y'_j \;:=\; 2^n - 1 - y_{L_i-1-j}, \qquad j = 0, \ldots, L_i - 1.$$

Tenemos, módulo 2^n,

$$y'_0 \equiv 2^n - 1 - y_{L_i-1} \equiv 2^n - 1 - (2^n - k) \equiv k - 1,$$

y para todo j,

$$y'_{j+1} - y'_j \equiv \big(2^n - 1 - y_{L_i-2-j}\big) - \big(2^n - 1 - y_{L_i-1-j}\big) \equiv y_{L_i-1-j} - y_{L_i-2-j} \equiv d.$$

Es decir, (y'_j) es también una progresión aritmética módulo 2^n con la *misma* razón d y cabeza $k-1$,

$$y'_j \equiv (k-1) + jd \pmod{2^n}.$$

Como la aplicación $x \mapsto (dx)$ mód 2^n es una permutación de $\{0, \ldots, 2^n - 1\}$ (pues $\gcd(d, 2^n) = 1$), toda progresión de razón d y longitud L_i con cabeza entre 0 y $d-1$ coincide con *un único* segmento. Por lo tanto, $S(i)^{\complement}$ coincide con el segmento $S(\ell)$ cuya cabeza es $k-1$ y cuya longitud es L_i. □

Corolario 2 (Segmentos auto-opuestos y discrepancia nula)**.** *En el contexto de la Proposición 8, puede ocurrir que un segmento $S(i)$ sea opuesto de sí mismo, es decir,*

$$S(i)^{\complement} = S(i).$$

Esto ocurre exactamente cuando el último elemento del segmento es $2^n - 1 - s$, siendo s la cabeza del segmento. Es decir, el segmento termina en el complemento de su punto inicial. Como, por definición, el último valor de $S(i)$ cumple

$$s + (L_i - 1)d \equiv 2^n - k \pmod{2^n},$$

además

$$s + (L_i - 1)d \equiv 2^n - 1 - s \pmod{2^n},$$

por lo que $k \equiv 2^n - s \pmod{d}$*, es decir,* $s \equiv k - 1 \pmod{d}$*. En tal caso, la cabeza del segmento y la de su opuesto coinciden, por lo que ambos comienzan en el mismo valor y recorren exactamente la misma progresión. El segmento es entonces su propio opuesto y su discrepancia de símbolo es* 0*.*

Demostración. Si un segmento coincide con su complemento, entonces invertir el orden y cambiar 0 por 1 no altera su secuencia de símbolos. Esa simetría sólo es posible si el segmento contiene la misma cantidad de 0s y 1s, de modo que toda contribución positiva y negativa a la discrepancia se anula. Por lo tanto, su discrepancia de símbolo es nula. □

Corolario 3 (Paridad y discrepancia nula)**.** *Como d es impar, el numero de segmentos es impar y el emparejamiento por opuestos deja un segmento sin pareja. Por lo que hay siempre al menos un segmento que es opuesto de si mismo (ya que todos los segmentos tienen opuesto).*

Ejemplo [Orden y opuestos para $n = 4$, $d = 5$]
Tenemos $2^n = 16$ y $r = 2^n \bmod d = 1$. Por la Proposición (orden), las cabezas recorren $s_i \equiv -i\, r \pmod{d}$, es decir:

$$s_0 = 0,\ s_1 = 4,\ s_2 = 3,\ s_3 = 2,\ s_4 = 1,$$

el orden de segmentos es

$$S(0),\ S(4),\ S(3),\ S(2),\ S(1).$$

Cada segmento es progresión de razón d *mód* 2^n dentro de su tramo (Lema):

$$S(i) = \{(s + jd) \bmod 16 :\ j = 0, \ldots, L_i - 1\}.$$

En Tabla 5.1 listamos sus valores en `binario (4 bits)`. Además, para una cabeza s, el opuesto comienza en

$$s^\star \equiv k - 1 \pmod{d}, \qquad k \equiv 16 - s \pmod{5}.$$

Segmentos (valores en binario) y sus opuestos: En la Tabla 5.1 vemos que $S(0)$ es auto-opuesto; $S(4)$ y $S(1)$ son opuestos y, $S(3)$ y $S(2)$ son opuestos. Notemos que la discrepanca de símbolo de la concatenacion de opuestos es nula. ya que complementar intercambia 0s y 1s
.

Segmento	`Valores` $S(i)$	**Final** / k	`Opuesto` $S(i)^{\mathtt{C}}$
$S(0)$	`0000, 0101, 1010, 1111`	final $= 1111 = 16 - 1$ $k = 1$	`0000, 0101, 1010, 1111`
$S(4)$	`0100, 1001, 1110`	final $= 1110 = 16 - 2$ $k = 2$	`0001, 0110, 1011`
$S(3)$	`0011, 1000, 1101`	final $= 1101 = 16 - 3$ $k = 3$	`0010, 0111, 1100`
$S(2)$	`0010, 0111, 1100`	final $= 1100 = 16 - 4$ $k = 4$	`0011, 1000, 1101`
$S(1)$	`0001, 0110, 1011`	final $= 1011 = 16 - 5$ $k = 5$	`0100, 1001, 1110`

Tabla 5.1: Relación entre segmentos $S(i)$, su valor final y sus opuestos $S(i)^{\mathtt{C}}$.

6. EXPERIMENTOS SOBRE DISCREPANCIA DE COLLARES ARITMÉTICOS

En este capítulo mostramos varios cómputos de discrepancia de collares aritméticos. Como se aprecia en la Figura 6.1, la discrepancia $D(S)$ no presenta un comportamiento uniforme en función de d. Luego de un valor inicial muy alto para $d = 1$ —registrado explícitamente en la Tabla 6.2— la discrepancia cae de manera abrupta y se mantiene relativamente baja para la mayoría de los valores de d, con picos pronunciados en posiciones muy específicas.

La Tabla 6.1 muestra que los valores mínimos de discrepancia se repiten en varios d distintos para un mismo n, lo que indica que hay múltiples configuraciones que generan collares altamente balanceados. Por otro lado, la Tabla 6.3 destaca una familia particular de d de la forma $d = 2^k + 1$ (con $n = 2k$), que produce discrepancias intermedias con un patrón muy regular.

Además, al superponer distintos valores de n, estos picos se repiten en escalas sucesivas, sugiriendo una estructura *similar* o semi-fractal: los máximos para $n = 10$ aparecen cerca de los mismos d que para $n = 9$, y así sucesivamente, manteniendo su forma y altura relativa. Este patrón indica que ciertos d actúan como resonancias para la secuencia, mientras que la mayoría de los d produce collares mucho más equilibrados.

Más allá de la similitud visible en la Figura 6.1 y en las Tablas 6.1–6.3, se observan ciertos patrones empíricos que ayudan a caracterizar la aparición de picos y valles en la discrepancia:

- **Simetrías aproximadas en d.** Para módulo 2^n, los collares generados por d y por $2^n - d$ no son idénticos pero presentan una estructura muy similar: ambos comienzan en 0 y sus segmentos se recorren en órdenes casi opuestos. Empíricamente, esto hace que sus discrepancias $D(S_d)$ y $D(S_{2^n-d})$ tengan magnitudes muy parecidas, con picos y valles que aparecen en posiciones especulares respecto de $d = 2^{n-1}$.
- **Escalamiento con n.** Si se fija d y se aumenta n, las posiciones relativas de los picos se replican a escalas 2-ádicas: lo que es un pico para $(n-1)$ reaparece cerca de d y de $d+2^{n-1}$ para n, conservando la forma (auto-similitud observada en las superposiciones).
- **Caída inicial.** $D(S_d)$ para $d = 1$ es e máximo. Refleja que $d = 1$ recorre los bloques en orden lexicográfico puro (máxima alineación de patrones) mientras que $d > 1$ rompe alineaciones y mezcla bloques, por lo que $D(S_d)$ es menor que $D(S_1)$.
- **Los d "mágicos" no son óptimos.** Aunque los valores $d = 2^k + 1$ (caso mágico) tienen la propiedad teórica de balance perfecto por segmento, las tablas muestran que su discrepancia $D(S_d)$ no necesariamente es la mínima global: otros valores de d dan discrepancias más bajas.
- **Múltiples mínimos posibles.** En algunos n distintos valores de d alcanzan la misma discrepancia mínima lo que indica que no existe un único generador sino posiblemnete varios.

- **Crecimiento en $d = 1$.** Con los resultados que obtenemos de la Tabla 6.1 la discrepancia para $d = 1$ parece ser del orden de $\mathcal{O}(2^n)$.
- **Conjetura sobre la discrepancia mínima $D(S_d)$.** A partir de los valores presentados en la Tabla 6.1, conjeturamos que la mínima discrepancia de un collar aritmético de orden n $D(S_d)$ es $\mathcal{O}(n \log n)$.

n	d **que alcanzan la discrepancia mínima**	$D(S_d)$ **Discrepancia mínima**
4	5, 13	5
5	27, 29	6
6	41	8
7	83	9
8	231	11
9	157, 165, 181, 217, 437, 467	14
10	143	16

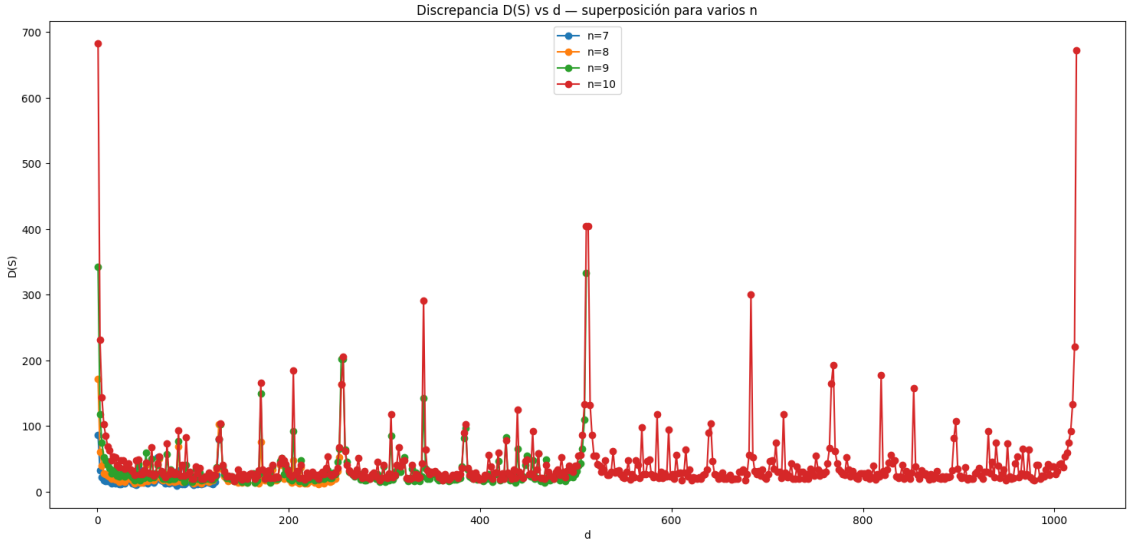
Tabla 6.1: Para cada n, listamos d tal que tal que para todo d', $D(S_d) \leq D(S_{d'})$.

n	$D(S_{d=1})$
4	11
5	22
6	43
7	86
8	171
9	342
10	683

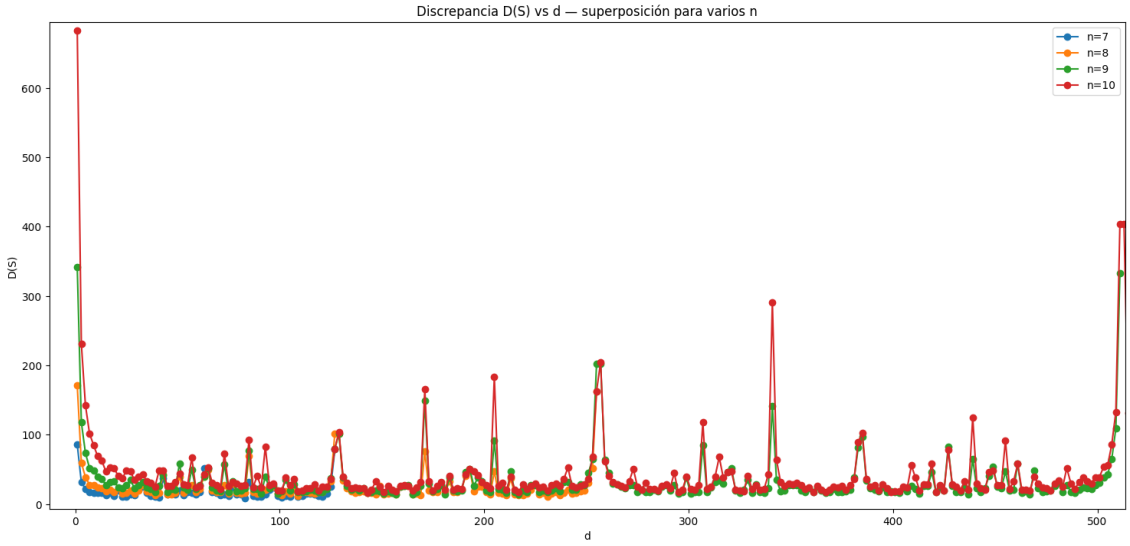
Tabla 6.2: Discrepancia $D(S)$ para $d = 1$ en cada n.

$n = 2k$	$d = 2^k + 1$	$D(S)$	$\Delta(S)$
4	5	7	5
6	9	13	11
8	17	27	21
10	33	53	43

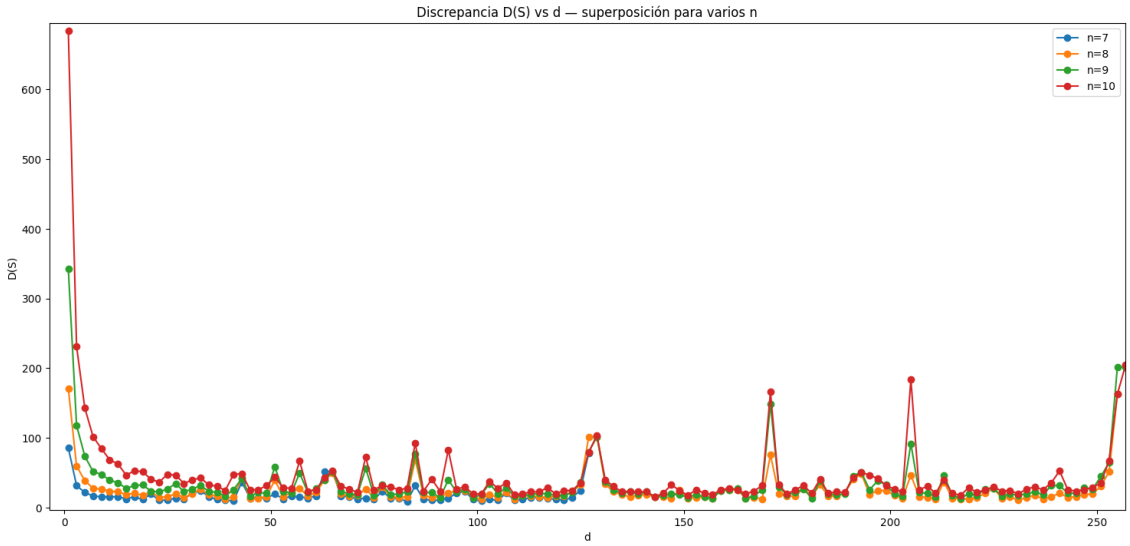
Tabla 6.3: Discrepancia $D(S_d)$ y $\Delta(S_d)$ para el caso "mágico" $d = 2^k + 1$ con $n = 2k$.



(a) Exhibe $D(S_d)$ para todos los d.



(b) Limita los d de $n = 10$ a la mitad.



(c) Limita los d hasta 2^8

Figura 6.1: $D(S)$ para $n = 7, 8, 9, 10$ en función de d.

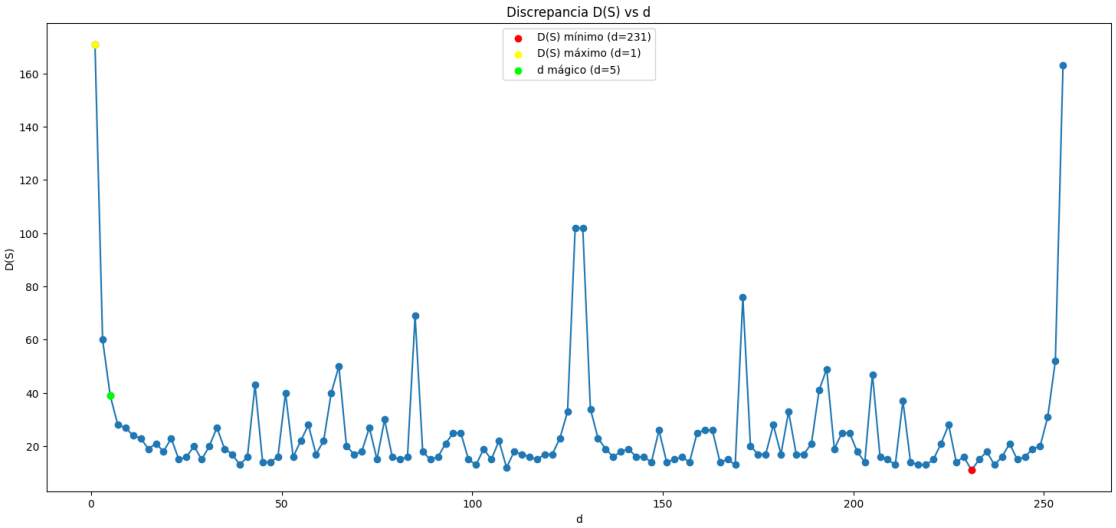


Figura 6.2: Gráfico $D(S_d)$ $n = 8$, para todos los d.

Bibliografía

[1] N. Alvarez, V. Becher, P. Ferrari, and S. Yuhjtman. Perfect necklaces. *Advances in Applied Mathematics*, 80:48–61, 2016.

[2] N. Alvarez, V. Becher, M. Mereb, I. Pajor, and C. S. Soto. De Bruijn sequences with minimum discrepancy. *arXiv:2407.17367*, 2025. Aparecerá en Mathematics of Computation.

[3] V. Becher and O. Carton. Normal numbers and computer science. In Valérie Berthé and Michel Rigó, editors, *Sequences, Groups, and Number Theory*, Trends in Mathematics Series, pages 233–269. Birkhauser/Springer, 2018.

[4] V. Becher and O. Carton. Normal numbers and nested perfect necklaces. *Journal of Complexity*, 54(101403), 2019.

[5] V. Becher and N. Graus. The discrepancy of the Champernowne constant. *arXiv:2407.13114*, 2024. Aparecerá en American Mathematical Monthly en Febrero 2026.

[6] J. Cooper and C. Heitsch. The discrepancy of the lex-least de Bruijn sequence. *Discrete Math.*, 310(6-7):1152–1159, 2010.

[7] N.G. de Bruijn. A combinatorial problem. *Proc. Nederl. Akad. Wetensch.*, 49:758–764, 1946.

[8] D. Gabric and J. Sawada. Investigating the discrepancy property of de Bruijn sequences. *Discrete Mathematics*, 345(4):112780, 2022.

[9] I.J. Good. Normal recurring decimals. *Journal of London Mathematical Society*, 21:167–169, 1946.

[10] R. Hofer and G. Larcher. Discrepancy bounds for normal numbers generated by necklaces in arbitrary base. *Journal of Complexity*, 78:101767, 2023.

[11] R. Hofer and G. Larcher. The exact order of discrepancy for levin's normal number in base 2. *Journal de Théorie des Nombres de Bordeaux*, 35(3):pp. 999–1023, 2023.

[12] D. Knuth. *The Art of Computer Programming. Volumen 4, Combinatorial algorithms.* Addison-Wesley, 1973.

[13] N. Korobov. *Bulletin of the Academy of Sciences of the USSR. Mathematical Series*, 15:16–46, 1951.

[14] M. B. Levin. On the discrepancy estimate of normal numbers. *Acta Arithmetica*, 88(2):99–111, 1999.