Facultad de Ciencias Naturales y Exactas
Universidad del Valle

CÓDIGOS CORRECTORES DE ERRORES Y COMBINATORIA

Carlos Alexis Gómez Ruiz
Universidad del Valle

Recibido: marzo 28, 2011 Aceptado: mayo 25, 2011

Pág. 51-61

Resumen

Con los trabajos de R. L. Graham y N. J. A. Sloane [2], se obtuvo una relación entre los conjuntos S_h de la Teoría de Números Aditiva y los códigos binarios de peso constante. Recientemente, H. Derksen [3] extendió las ideas de Graham y Sloane a códigos binarios en general, presentando nuevas cotas inferiores para el máximo tamaño de los códigos binarios obtenidos. En este documento se dará esencialmente una demostración formal de una propiedad combinatoria que H. Derksen requirió y que determinó de manera heurística.

Palabras claves: Códigos binarios y cotas inferiores para $A(n, d)$.

Abstract

With the work by R. L. Graham and N. J. A. Sloane [2], we found a relationship between the S_h-sequences of the Additive Number Theory and the binary codes of constant weight. Recently, H. Derksen [3] extended the ideas of Graham and Sloane to binary codes in general, presenting new lower bounds for the maximum size of binary codes obtained. This document will be essentially a formal proof of a combinatorial property that H. Derksen required and determined heuristically.

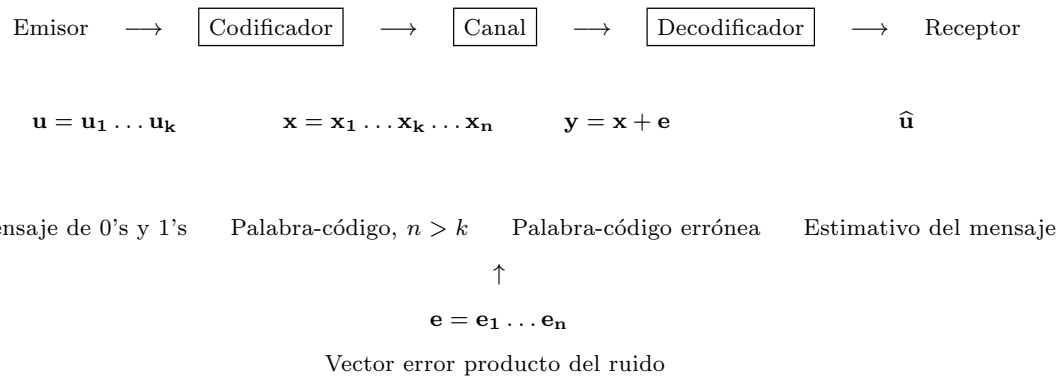
Keywords: Binary codes and lower bounds to $A(n, d)$.

1 Introducción

Los *Códigos Correctores de Errores* surgen de la necesidad de corregir errores en la transmisión de información a través de un canal de comunicación ruidoso.

El inicio de la teoría de la información data del año 1948 a partir de los trabajos de Claude E. Shannon quien publicó el artículo: *A mathematical theory of communication* [1].

El siguiente diagrama representa el proceso de transmisión de información.



El pilar de esta teoría se encuentra en el teorema que lleva su nombre, el cual garantiza la existencia de buenos códigos que permiten transmitir información, a través de un canal con una probabilidad de error tan pequeña como se quiera siempre que este canal tenga una capacidad de transmisión de información mayor que la tasa de transferencia del código.

Los resultados de Shannon afirman que los datos pueden ser codificados adecuadamente antes de ser transmitidos, de tal forma que los datos alterados recibidos pueden ser decodificados al mensaje enviado.

Un *código* de longitud n sobre $\mathbb{F}_2$ es un subconjunto $\mathcal{C} \subseteq \mathbb{F}_2^n$. Las $n-$uplas de $\mathcal{C}$ se llaman palabras-código y $\mathcal{C}$ un código binario. Cuando $\mathcal{C}$ es un subespacio vectorial se dice que $\mathcal{C}$ es un *código lineal*, de lo contrario se dice que $\mathcal{C}$ es un *código no lineal*.

Supóngase que el mensaje $\mathbf{u} = u_1 \dots u_k$ es codificado en la palabra-código $\mathbf{x} = x_1 \dots x_n$ la cual es enviada a través de un canal de comunicación. Debido al ruido del canal, la $n-$upla recibida $\mathbf{y} = y_1 \dots y_n$ puede ser diferente de $\mathbf{x}$ y en tal caso se dice que ha ocurrido un error en la transmisión del mensaje. De esta forma se define el error $\mathbf{e}$ en la transmisión de $\mathbf{x}$ mediante

$$\mathbf{e} = \mathbf{y} - \mathbf{x}.$$

Es natural preguntarse que tan diferente es la $n-$upla $\mathbf{y}$ de la palabra-código $\mathbf{x}$, por lo cual aparece de forma natural la siguiente función.

Para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, se define la *distancia de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$ como el número de coordenadas en las cuales $\mathbf{x}$ e $\mathbf{y}$ difieren. Es decir, la distancia de Hamming está dada por la función $\delta : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{N}_0$ definida como

$$\delta(\mathbf{x}, \mathbf{y}) := |\{\, i \ : \ x_i \neq y_i \,\}|,$$

donde $|A|$ corresponde al cardinal del conjunto A. Además se define el *peso* $\mathrm{wt}(\mathbf{x})$ de una $n-$upla $\mathbf{x} \in \mathbb{F}_2^n$, como el número de coordenadas no nulas de $\mathbf{x}$, es decir $\mathrm{wt}(\mathbf{x}) = \delta(\mathbf{x}, 0)$. Así, se dice que el código $\mathcal{C}$ tiene peso constante w, denotado por $\mathrm{wt}(\mathcal{C}) = w$, si $\mathrm{wt}(\mathbf{x}) = w$, para todo $\mathbf{x} \in \mathcal{C}$.

De esta manera, se define la *distancia mínima* de un código $\mathcal{C}$ como

$$\delta_{\mathcal{C}} := \text{mín}\{\, \delta(\mathbf{x}, \mathbf{y}) \,:\, \mathbf{x}, \mathbf{y} \in \mathcal{C},\, \mathbf{x} \neq \mathbf{y} \,\}.$$

El parámetro distancia mínima de un código $\mathcal{C}$ es de gran importancia, pues es bien conocido que si $\delta_{\mathcal{C}} = d$ entonces $\mathcal{C}$ puede corregir hasta $\lfloor \frac{d-1}{2} \rfloor$ errores y detectar hasta $d-1$ errores.

1.1 Problemas fundamentales en teoría de códigos

El Teorema de Shannon garantiza probabilísticamente que existen códigos con buenos parámetros, sin embargo en su demostración no se construye ninguno de ellos. Este hecho dio lugar a una amplia carrera y una intensa búsqueda de códigos que cumplan las especificaciones que predice el Teorema de Shannon.

Uno de los problemas principales en Teoría de Códigos es construir códigos con el mayor número posible de palabras-código, estableciendo un equilibrio entre la longitud n de las palabras-código y su distancia mínima d, es decir una vez fijo n, se quiere que d sea lo más grande posible para poder corregir el mayor número de errores que ocurran.

Sean n y d enteros positivos con $n \geq d$, el problema de determinar el máximo número de elementos de un código binario de longitud n y distancia mínima $\geq d$, se representa con la siguiente función:

$$A(n, d) := \text{máx}\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n,\ \delta_{\mathcal{C}} \geq d\}.$$

Un tipo particular de códigos son aquellos donde toda palabra-código tiene el mismo peso, llamados *códigos de peso constante*. De igual forma se está interesado en el máximo tamaño de un código de peso constante con determinados parámetros. Sean n, d y w enteros positivos con $n \geq w$, $n \geq d$, el último problema se representa mediante la siguiente función:

$$A(n, d, w) := \text{máx}\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n,\, \delta_{\mathcal{C}} \geq d,\ \text{wt}(\mathcal{C}) = w\}.$$

Para obtener cotas inferiores de las funciones $A(n, d)$ y $A(n, d, w)$ se han construido códigos a través de técnicas algebraicas como son los códigos de Hamming, códigos de Golay, códigos de Hadamard, códigos BCH, códigos cíclicos, códigos de Reed-Solomon, códigos alternantes, códigos geométricos de Goppa, códigos de Reed-Muller, códigos Preparata, códigos por residuos cuadráticos QR y modificaciones de estos. En cuanto a cotas superiores, se han usado variadas técnicas combinatorias, con las que se obtuvieron las cotas de Johnson. Además, se ha usado el método Simplex, con el que se obtuvo la cota de McEliece-Rodemich-Rumsey-Welch. Vale la pena notar que la labor hecha alrededor de estos problemas ha sido amplia, por lo cual se sugiere ver [4, capítulo 17] para más detalle sobre las cotas existentes.

En la sección 2, se presenta una cota inferior para $A(n, d)$ obtenida por H. Derksen [3], quien utiliza una construcción de códigos binarios de peso constante

a través de herramientas combinatorias. En la sección 3, se presentan algunas propiedades combinatorias y se muestra formalmente, mediante el Teorema principal, que cierta afirmación heurística que hace H. Derksen es correcta.

2 Códigos binarios no lineales

El siguiente teorema relaciona los códigos de peso constante con los códigos no lineales y permite dar una cota inferior de $A(n,d)$ a partir de cotas inferiores para $A(n,d,w)$.

Teorema 1. *Para n, d y $1 \leq u \leq n$ enteros positivos fijos, se cumple que*

$$A(n,d) \geq \sum_{w \equiv u \, mód \, d} A(n,d,w).$$

Demostración. Sean $\mathcal{C}_{d,w}$ códigos binarios de longitud n, distancia mínima $\geq d$, peso constante $w \equiv u \, mód \, d$ y óptimos en el sentido de un máximo número de elementos. Estos códigos son disjuntos según el peso y además $|\mathcal{C}_{d,w}| = |A(n,d,w)|$. Considérese la unión de estos códigos

$$\mathcal{C} = \bigcup_{w \equiv u \, mód \, d} \mathcal{C}_{d,w}. \tag{1}$$

Claramente $\mathcal{C}$ es un código binario de longitud n, resta probar que tiene distancia mínima $\geq d$. Sean $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ tal que $\mathrm{wt}(\mathbf{x}) = w_1$, $\mathrm{wt}(\mathbf{y}) = w_2$, donde $w_1, w_2 \equiv u \, mód \, d$. Si $w_1 = w_2$, entonces $\mathbf{x}, \mathbf{y} \in \mathcal{C}_{d,w_1}$ y $\delta(\mathbf{x},\mathbf{y}) \geq d$. Si $w_1 > w_2$, entonces

$$\begin{aligned} \delta(\mathbf{x},\mathbf{y}) &= \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2\,(\mathbf{x} * \mathbf{y}) \\ &\geq w_1 - w_2 \\ &\geq d, \end{aligned}$$

donde $\mathbf{x} * \mathbf{y}$ denota el número de unos en la misma posición en $\mathbf{x}$ e $\mathbf{y}$. Por lo tanto,

$$\begin{aligned} A(n,d) \geq |\mathcal{C}| &= \sum_{w \equiv u \, mód \, d} |\mathcal{C}_{d,w}| \\ &= \sum_{w \equiv u \, mód \, d} A(n,d,w). \end{aligned}$$

□

2.1 Códigos binarios de peso constante y Conjuntos S_h

Sean, G un grupo conmutativo notado aditivamente, $h \geq 2$ entero. Un subconjunto A del grupo G se llama un *conjunto S_h en G*, si todas las sumas de h elementos distintos de A, omitiendo las permutaciones de los sumandos, determinan elementos distintos en G. Es decir, si todas las expresiones de la forma

$$x_{i_1} + x_{i_2} + \cdots + x_{i_h}, \quad \text{con} \quad i_1 < i_2 < \cdots < i_h,$$

y $x_{i_1}, x_{i_2}, \ldots, x_{i_h} \in A$, producen elementos distintos en G.

La noción de conjunto S_h es propia de la Teoría de Números Aditiva, ver [5, capítulo 2], sin embargo aparece por primera vez relacionada con los códigos de peso constante en el año 1980 en los trabajos de R. L. Graham y N. J. A. Sloane [2, sección 3] y posteriormente en el trabajo de H. Derksen [3]. Esta relación se establece en el siguiente teorema.

Teorema 2. *[3, proposición 2]. Sea $\{g_1, \ldots, g_n\}$ un conjunto S_h en un grupo conmutativo G notado aditivamente. Si $\mathbb{F}_2$ se identifica con $\{0, 1\}$ y se considera la función $\phi : \mathbb{F}_2^n \to G$ definida como*

$$\phi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i g_i,$$

entonces se tiene que para todo w y cada $g \in G$, el conjunto

$$C_g^{(w)} = \phi^{-1}(g) \cap \{\mathbf{x} \in \mathbb{F}_2^n \ : \ \mathrm{wt}(\mathbf{x}) = w\}$$

es un código binario de longitud n, distancia mínima $\geq 2h + 2$ y peso constante w.

Una consecuencia de este teorema está en la cota inferior para $A(n, 2h + 2, w)$ que se obtiene. Más exactamente:

Corolario 1. *[3, Corolario 4]. Si existe un conjunto S_h de cardinalidad $n \geq 2h+2$, en un grupo conmutativo finito G, entonces*

$$A(n, 2h + 2, w) \geq |C_g^{(w)}| \geq \frac{1}{\mid G \mid} \binom{n}{w}.$$

Observación 1. Del Teorema 1 y el Corolario 1, se tiene la siguiente cota inferior

$$A(n, 2h + 2) \geq \frac{1}{\mid G \mid} \sum_{w \equiv u \, mód \ 2h+2} \binom{n}{w}, \tag{2}$$

para cualquier $1 \leq u \leq n$.

Nótese que para obtener mejores cotas inferiores de $A(n, 2h + 2)$ mediante la expresión (2), es necesario maximizar

$$\frac{1}{\mid G \mid} \sum_{w \equiv u \, mód \ 2h+2} \binom{n}{w}.$$

Esto sugiere determinar el mínimo cardinal de un grupo conmutativo finito G donde existe un conjunto S_h con n elementos y maximizar $\sum_{w \equiv u \, mód \ 2h+2} \binom{n}{w}$ respecto a u.

3 Combinatorio modular y su valor máximo

Sean n, l y m enteros positivos, con $1 \leq l, m \leq n$. El *Combinatorio Modular* "*n combinado l, módulo m*" se define como:

$$C_m(n : l) := \sum_{j \,\equiv\, l \,\mathrm{mód}\, m} \binom{n}{j}, \quad 0 \leq j \leq n.$$

Ejemplo 1. *Sea $n = 18$ y $m = 4$. El número $C_4(18 : l)$ determina una función sobre los enteros positivos.*

$$\begin{aligned} C_4(18 : 7) &= \sum_{j \,\equiv\, 7 \,\mathrm{mód}\, 4} \binom{18}{j} \\ &= \binom{18}{3} + \binom{18}{7} + \binom{18}{11} + \binom{18}{15} \\ &= 17544. \end{aligned}$$

El objetivo de esta sección es el de establecer algunas propiedades combinatorias satisfechas por estos números las cuales juegan un papel determinante en la demostración del resultado principal de este trabajo, el Teorema 3.

Lema 1. *Para n, l y m enteros positivos, con $1 \leq l, m \leq n$*

$$C_m(n : l) = C_m(n : n - l).$$

Demostración.

$$\begin{aligned} C_m(n : n - l) &= \sum_{j \,\equiv\, n-l \,\mathrm{mód}\, m} \binom{n}{j} \\ &= \sum_{n-j \,\equiv\, l \,\mathrm{mód}\, m} \binom{n}{n-j} \\ &= \sum_{i \,\equiv\, l \,\mathrm{mód}\, m} \binom{n}{i} \\ &= C_m(n : l). \end{aligned}$$

□

Lema 2. *Para n, l y m enteros positivos, con $1 \leq l, m \leq n$*

$$C_m(n : l) + C_m(n : l - 1) = C_m(n + 1 : l).$$

Demostración.

$$C_m(n : l) + C_m(n : l - 1) = \sum_{i \,\equiv\, l \,\mathrm{mód}\, m} \binom{n}{i} + \sum_{j \,\equiv\, l-1 \,\mathrm{mód}\, m} \binom{n}{j}.$$

□

Considérense los conjuntos

$$A = \{\, i \,:\, i \equiv\ l \bmod m \,\},\ B = \{\, j \,:\, j \equiv\ (l-1)\ \bmod m\}$$

y nótese que

$$\begin{aligned} i \in A, \text{ tal que } 1 \leq i \leq n &\iff i - 1 \equiv (l-1) \bmod m \\ &\iff i - 1 \in B. \end{aligned} \tag{3}$$

Caso I. $m \nmid l$.

a. Si $n \not\equiv\ (l-1) \bmod m$, entonces $0 \notin A$ y $n \notin B$, por tanto $|A| = |B|$ y de (3)

$$\begin{aligned} C_m(n:l) + C_m(n:l-1) &= \sum_{i \equiv l \bmod m} \left[\binom{n}{i} + \binom{n}{i-1} \right] \\ &= \sum_{i \equiv l \bmod m} \binom{n+1}{i} \\ &= C_m(n+1:l). \end{aligned}$$

b. Si $n \equiv\ (l-1) \bmod m$, entonces $0 \notin A$ y $n \in B$, por tanto $|B| = |A| + 1$ y de (3)

$$\begin{aligned} C_m(n:l) + C_m(n:l-1) &= \sum_{i \equiv l \bmod m} \left[\binom{n}{i} + \binom{n}{i-1} \right] + \binom{n}{n} \\ &= \left[\sum_{i \equiv l \bmod m} \binom{n+1}{i} \right] + \binom{n+1}{n+1} \\ &= C_m(n+1:l). \end{aligned}$$

Caso II. $m \mid l$.

a. Si $n \not\equiv\ (l-1) \bmod m$, entonces $0 \in A$ y $n \notin B$, por tanto $|A| = |B| + 1$ y de (3)

$$\begin{aligned} C_m(n:l) + C_m(n:l-1) &= \sum_{i \equiv l \bmod m} \left[\binom{n}{i} + \binom{n}{i-1} \right] + \binom{n}{0} \\ &= \left[\sum_{i \equiv l \bmod m} \binom{n+1}{i} \right] + \binom{n+1}{0} \\ &= C_m(n+1:l). \end{aligned}$$

b. Si $n \equiv (l-1) \operatorname{mód} m$, entonces $0 \in A$ y $n \in B$, por tanto $|B| = |A|$ y de (3)

$$\begin{aligned} C_m(n:l) + C_m(n:l-1) &= \sum_{i \equiv l \operatorname{mód} m} \left[\binom{n}{i} + \binom{n}{i-1} \right] + \binom{n}{0} + \binom{n}{n} \\ &= \left[\sum_{i \equiv l \operatorname{mód} m} \binom{n+1}{i} \right] + \binom{n+1}{0} + \binom{n+1}{n+1} \\ &= C_m(n+1:l). \end{aligned}$$

□

Observación 2. Nótese que para cada entero positivo l, existe un único entero r el cual cumple que $0 \leq r \leq m-1$ y $l \equiv r \operatorname{mód} m$. De donde $C_m(n:l) = C_m(n:r)$.

Además el conjunto $\lfloor \frac{n}{2} \rfloor + \{0, -1, -2, \ldots, -(m-1)\}$ igual a:

$$\left\{ \lfloor \tfrac{n}{2} \rfloor,\ \lfloor \tfrac{n}{2} \rfloor - 1,\ \lfloor \tfrac{n}{2} \rfloor - 2,\ \ldots, \lfloor \tfrac{n}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor, \lfloor \tfrac{n}{2} \rfloor - (\lfloor \tfrac{m}{2} \rfloor + 1), \ldots,\ \lfloor \tfrac{n}{2} \rfloor - (m-1) \right\}$$

es un sistema residual completo módulo m.

Así, para n y m fijo, el rango de la función $C_m(n:*) : \mathbb{N} \to \mathbb{N}$ está determinado por los valores $C_m(n : \lfloor \frac{n}{2} \rfloor - t)$, con $t = 0, 1, 2, \ldots, m-1$.

En el siguiente lema se determina de manera precisa las imagenes que toma la función $C_m(n:*)$.

Lema 3. *Para n, l y m enteros positivos, con $1 \leq l, m \leq n$, la función $C_m(n, *)$ toma exactamente los valores $C_m(n, \lfloor \frac{n}{2} \rfloor - j)$, con $0 \leq j \leq \lfloor \frac{m}{2} \rfloor$.*

Demostración. Por la observación 2 es suficiente considerar $l \in \{\lfloor \frac{n}{2} \rfloor - t : 0 \leq t \leq m-1\}$.

I. Para n impar. Si $1 \leq k \leq m - \lfloor \frac{m}{2} \rfloor - 1$, del lema 1.

$$\begin{aligned} C_m(n : \lfloor \tfrac{n}{2} \rfloor - (\lfloor \tfrac{m}{2} \rfloor + k)) &= C_m(n : n - \lfloor \tfrac{n}{2} \rfloor + \lfloor \tfrac{m}{2} \rfloor + k) \\ &= C_m(n : \lfloor \tfrac{n}{2} \rfloor + 1 + \lfloor \tfrac{m}{2} \rfloor + k) \\ &= C_m(n : \lfloor \tfrac{n}{2} \rfloor - (m - \lfloor \tfrac{m}{2} \rfloor - 1 - k)) \end{aligned}$$

luego tomando $j = m - \lfloor \frac{m}{2} \rfloor - 1 - k$, se tiene que $0 \leq j \leq \lfloor \frac{m}{2} \rfloor - 1$. Lo cual muestra que en este caso, el número $C_m(n, l)$ toma exactamente los valores $C_m(n, \lfloor \frac{n}{2} \rfloor - j)$, con $0 \leq j \leq \lfloor \frac{m}{2} \rfloor$.

II. Para n par. Si $1 \leq k \leq m - \lfloor \frac{m}{2} \rfloor - 1$, del lema 1.

$$\begin{aligned} C_m(n : \lfloor \tfrac{n}{2} \rfloor - (\lfloor \tfrac{m}{2} \rfloor + k)) &= C_m(n : n - \lfloor \tfrac{n}{2} \rfloor + \lfloor \tfrac{m}{2} \rfloor + k) \\ &= C_m(n : \lfloor \tfrac{n}{2} \rfloor + \lfloor \tfrac{m}{2} \rfloor + k) \\ &= C_m(n : \lfloor \tfrac{n}{2} \rfloor - (m - \lfloor \tfrac{m}{2} \rfloor - k)), \end{aligned}$$

y tomando $j = m - \lfloor \frac{m}{2} \rfloor - k$, se tiene que $1 \leq j \leq \lfloor \frac{m}{2} \rfloor$. Con lo cual, también en este otro caso, el número $C_m(n, l)$ toma exactamente los valores $C_m(n, \lfloor \frac{n}{2} \rfloor - j)$, con $0 \leq j \leq \lfloor \frac{m}{2} \rfloor$.

□

Con el objetivo de establecer buenas cotas inferiores para $A(n, d)$ desde la expresión (2), se observó que es necesario determinar el mínimo cardinal de un grupo conmutativo finito G donde existe un conjunto S_h con n elementos y maximizar $\sum_{w \equiv u \, m\acute{o}d \; 2h+2} \binom{n}{w}$ respecto a u.

Para determinar el mínimo cardinal de un grupo conmutativo finito G donde existe un conjunto S_h con n elementos, H. Derksen consideró el grupo de unidades del anillo cociente de polinomios $G = (\mathbb{F}_q[x]/\langle p(x)\rangle)^*$, donde $\mathbb{F}_q$ denota el cuerpo finito con q elementos, $\langle p(x)\rangle$ el ideal generado por $p(x)$ y R^* el grupo de unidades de un anillo R. De esta manera, minimizó el tamaño de G escogiendo adecuadamente q y $p(x)$. Para más detalle ver [3, Lema 6].

Observación 3. En cuanto a la optimización de $\sum_{w \equiv u \, m\acute{o}d \; 2h+2} \binom{n}{w}$, H. Derksen afirmó heuristicamente que la mejor escogencia para u es $\lfloor \frac{n}{2} \rfloor$, lo que es equivalente a decir que el número $C_m(n : l)$ es máximo cuando $l = \lfloor \frac{n}{2} \rfloor$.

En virtud del Lema 3, es suficiente considerar $C_m(n : \lfloor \frac{n}{2} \rfloor - j)$, con $0 \leq j \leq \lfloor \frac{m}{2} \rfloor$, con el fin de mostrar formalmente que la escogencia hecha por H. Derksen es correcta.

El siguiente teorema es el propósito esencial de este artículo.

Teorema 3. *(Teorema principal) Para $1 \leq m \leq n$ enteros, se tiene que*

$$C_m(n : \lfloor \tfrac{n}{2} \rfloor) \geq C_m(n : \lfloor \tfrac{n}{2} \rfloor - 1) \geq \cdots \geq C_m(n : \lfloor \tfrac{n}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor). \tag{4}$$

Es decir, $C_m(n, l)$ alcanza su valor máximo en $l = \lfloor \frac{n}{2} \rfloor$.

Demostración. Haciendo inducción sobre n, si $n = 1$ el resultado se tiene inmediatamente. Si $n \geq 2$ y $m = 1$ entonces

$$C_1(n, 1) = \sum_{j=0}^{n} \binom{n}{j} = 2^n,$$

para todo l, lo cual garantiza la conclusión del teorema.

En virtud del Lema 3, es suficiente considerar $C_m(n, \lfloor \frac{n}{2} \rfloor - t)$, con $0 \leq t \leq \lfloor \frac{m}{2} \rfloor$.

Supóngase como hipótesis de inducción que para todo $2 \leq m \leq k$, se cumple (4) y a partir de esto se verá que (4) también se tiene para $n = k + 1$. Es decir, se mostrará que

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - j) \geq C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - (j+1)), \text{ con } 0 \leq j \leq \lfloor \tfrac{m}{2} \rfloor - 1. \tag{5}$$

Si $m = k + 1$, entonces

$$C_{k+1}(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - j) = \binom{k+1}{\lfloor \frac{k+1}{2} \rfloor - j}, \quad \text{con} \quad 0 \leq j \leq \left\lfloor \tfrac{k+1}{2} \right\rfloor.$$

Así, (5) es consecuencia de las propiedad de los coeficientes binomiales. Para $2 \leq m \leq k$, se consideran algunos casos.

Caso I. Si k es par, entonces $\lfloor \frac{k+1}{2} \rfloor = \lfloor \frac{k}{2} \rfloor$. Además de la hipótesis de inducción, se tiene que para $0 \leq j \leq \lfloor \frac{m}{2} \rfloor - 2$

$$C_m(k : \lfloor \tfrac{k}{2} \rfloor - j) \geq C_m(k : \lfloor \tfrac{k}{2} \rfloor - (j+1))$$

y

$$C_m(k : \lfloor \tfrac{k}{2} \rfloor - (j+1)) \geq C_m(k : \lfloor \tfrac{k}{2} \rfloor - (j+2)).$$

Sumando los lado correspondientes, se sigue del Lema 2 que

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - j) \geq C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - (j+1)).$$

Resta considerar $j = \lfloor \frac{m}{2} \rfloor - 1$. Del Lema 3 y la hipótesis de inducción, se tiene que

$$\begin{aligned} C_m(k : \lfloor \tfrac{k}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor - 1) &= C_m(k : \lfloor \tfrac{k}{2} \rfloor - (m - \lfloor \tfrac{m}{2} \rfloor - 1)) \\ &\leq C_m(k : \lfloor \tfrac{k}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor + 1). \end{aligned}$$

Ahora, sumando $C_m(k : \lfloor \frac{k}{2} \rfloor - \lfloor \frac{m}{2} \rfloor)$ en ambos lados, de nuevo por el Lema 2 se concluye que

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor) \leq C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - \lfloor \tfrac{m}{2} \rfloor + 1).$$

Con esto termina la prueba de (5), en este caso.

Caso II. Si k es impar, entonces $\lfloor \frac{k+1}{2} \rfloor = \lfloor \frac{k}{2} \rfloor + 1$. De nuevo por la hipótesis de inducción, se tiene que para $0 \leq i \leq \lfloor \frac{m}{2} \rfloor - 2$

$$C_m(k : \lfloor \tfrac{k}{2} \rfloor - i) \geq C_m(k : \lfloor \tfrac{k}{2} \rfloor - (i+1))$$

y

$$C_m(k : \lfloor \tfrac{k}{2} \rfloor - (i+1)) \geq C_m(k : \lfloor \tfrac{k}{2} \rfloor - (i+2)).$$

Sumando los lado correspondientes, se sigue del Lema 2 que

$$C_m(k+1 : \lfloor \tfrac{k}{2} \rfloor - i) \geq C_m(k+1 : \lfloor \tfrac{k}{2} \rfloor - (i+1)),$$

lo cual es equivalente a

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - (i+1)) \geq C_m(k+1 : \tfrac{k+1}{2} \rfloor - (i+2)).$$

Así,

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - j) \geq C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - (j+1)),$$

para $1 \leq j \leq \lfloor \frac{m}{2} \rfloor - 1$.

Resta considerar $j = 0$. Del Lema 1 y la hipótesis de inducción se tiene que

$$\begin{aligned} C_m(k : \lfloor \tfrac{k}{2} \rfloor + 1) &= C_m(k : k - \lfloor \tfrac{k}{2} \rfloor - 1) \\ &= C_m(k : \lfloor \tfrac{k}{2} \rfloor) \\ &\geq C_m(k : \lfloor \tfrac{k}{2} \rfloor - 1). \end{aligned}$$

Sumando en ambos lados $C_m(k : \lfloor \frac{k}{2} \rfloor)$, una vez más por el Lema 2 se concluye que

$$C_m(k+1 : \lfloor \tfrac{k}{2} \rfloor + 1) \geq C_m(k+1 : \lfloor \tfrac{k}{2} \rfloor),$$

que equivale a

$$C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor) \geq C_m(k+1 : \lfloor \tfrac{k+1}{2} \rfloor - 1).$$

Con lo cual termina la prueba para (5), en este otro caso. □

Referencias bibliográficas

[1] Shannon C. E. *A mathematical Theory of Communication*, Bell System Tech. J. **27**,379-423, 623-656 (1948).

[2] Graham R. L. and Sloane N. J. A. *Lower bounds for constant weight codes*, IEEE Transations on Information Theory **26** (1980) No. 1, 37-43.

[3] Derksen H. *Error-Correcting Codes and B_h-Sequences*, IEEE Transations on Information Theory **50** 2004, No. 3, 476-485.

[4] MacWilliams F. J. and Sloane N. J. A. *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, (2006).

[5] Halberstam H. and Roth K. F. *Sequences*. Oxford, U.K.: Oxford Univ. Press, 1986, vol. 2.

[6] Gómez C. A. *Construcción de conjuntos B_h sobre grupos y Códigos.* Tesis de Maestría, Universidad del Valle, 2008.

Dirección del autor

Carlos Alexis Gómez Ruiz
Departamento de Matemáticas, Universidad del Valle, Cali - Colombia
carlos.a.gomez@correounivalle.edu.co