Revista Colombiana de Matemáticas
Volumen 45(2011)2, páginas 137-146

Sobre conjuntos S_h de vectores binarios y códigos lineales

On S_h–Sequences of Binary Vectors and Lineal Codes

Carlos Alexis Gómez[1], Carlos Alberto Trujillo[2]

[1]Universidad del Valle, Cali, Colombia

[2]Universidad del Cauca, Popayán, Colombia

Resumen. Un subconjunto $\mathcal{A}$ de un grupo conmutativo G notado aditivamente, es un *conjunto S_h en G*, si todas las sumas de h elementos distintos de $\mathcal{A}$, omitiendo las permutaciones de los sumandos, determinan elementos diferentes en G.

En este artículo se muestra una relación entre conjuntos S_h en $\mathbb{F}_2^r$ y códigos binarios lineales.

Palabras y frases clave. Conjuntos S_h de vectores binarios, códigos correctores de errores.

2000 Mathematics Subject Classification. 11B, 11B75, 94B05.

Abstract. A subset $\mathcal{A}$ of a commutative group G with operation addition, is a *S_h–sequence in G*, if all the sums of h distinct elements of $\mathcal{A}$, omitting the permutations of the addends, determine different elements in G.

In this article, a relationship between S_h-sequences in $\mathbb{F}_2^r$ and binary linear codes, is established.

Key words and phrases. S_h–sequences of vectors binary, Error correcting codes.

1. Notación e introducción

Sea $\mathbb{F}_2$ el cuerpo con dos elementos. 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*.

Si $\mathcal{C}$ es un subespacio $k-$dimensional de $\mathbb{F}_2^n$ entonces $\mathcal{C}$ se llama un $[n,k]-$*código binario*. Las dos maneras más comunes de representar un código lineal es mediante una matriz generadora o una matriz de chequeo de paridad.

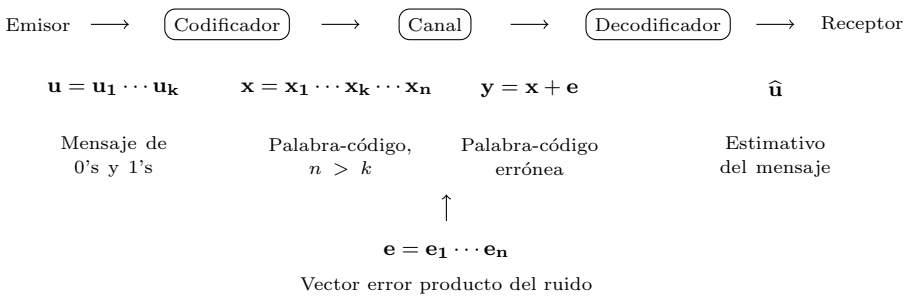
Una *matriz generadora* de un $[n,k]-$código binario $\mathcal{C}$ es una matriz binaria $\mathcal{G}$ de tamaño $k \times n$ cuyas filas forman una base de $\mathcal{C}$. Por otra parte, $\mathcal{C}$ también puede verse como el espacio nulo de una matriz binaria $\mathcal{H}$ de tamaño $(n-k)\times n$. La matriz $\mathcal{H}$ se llama *matriz de chequeo de paridad* del $[n,k]-$código binario $\mathcal{C}$. Es decir,

$$\mathcal{C} = \left\{\mathbf{x} \in \mathbb{F}_2^n : \mathcal{H}\mathbf{x}^t = \mathbf{0}\right\}.$$

En el año 1948, Claude E. Shannon publicó el artículo: *A Mathematical Theory of Communication* [1], que marcó el inicio de la teoría de la información y en ésta, la teoría de los códigos correctores de errores. El pilar de dicha 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.

A menudo se desea trasmitir un mensaje, el cual consiste de una secuencia de k símbolos que son elementos de un alfabeto finito, en este caso el cuerpo $\mathbb{F}_2$. El mensaje es transformado en una palabra de un código previamente conocido, agregando $r = n-k$ símbolos llamados *símbolos de redundancia* o *de chequeo de paridad* (esto se conoce como el proceso de codificación). Ahora, la transmisión de una palabra-código, sobre un canal de comunicación, no es necesariamente perfecta (en el sentido que cada símbolo no sufra alteración), de aquí que al canal se lo llame un canal de comunicación ruidoso.

El siguiente diagrama representa el proceso de transmisión de información.



Supóngase que el mensaje $\mathbf{u} = u_1 \cdots u_k$ es codificado en la palabra-código $\mathbf{x} = x_1 \cdots x_n$ la cual es enviada a través de un canal de comunicación. Debido al ruido del canal, la n-upla recibida $\mathbf{y} = y_1 \cdots y_n$ 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 $\mathbf{y}$ de la palabra-código $\mathbf{x}$, por lo cual aparece 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 $\delta : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{N}$ con

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

donde $|A|$ corresponde al cardinal del conjunto A.

Un parámetro muy importante en los códigos es la distancia mínima. Se define la *distancia mínima* de un código $\mathcal{C}$ como

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

Si $\mathcal{C} \subseteq \mathbb{F}_2^n$ es un código lineal $k-$dimensional con distancia mínima d, entonces $\mathcal{C}$ se llama un $[n, k, d]$-*código binario*. Si $\mathcal{C}$ es no lineal con M palabras-código, entonces $\mathcal{C}$ se llama un $(n, M, d)-$código binario. Ahora, es bien conocido en la teoría de códigos que si $\delta_{\mathcal{C}} = d$ entonces $\mathcal{C}$ puede corregir hasta $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores y detectar hasta $d-1$ errores.

Un problema básico en teoría de códigos es maximizar el cardinal de un código $\mathcal{C}$ de longitud n y distancia mínima al menos d. Este problema conduce a la función

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

Si adicionalmente se requiere que $\mathcal{C}$ sea un código lineal, se tendrá una nueva función que se denota como $B(n, d)$, donde claramente

$$B(n, d) \leq A(n, d).$$

En la sección 2, se presenta el concepto de conjunto S_h y su relación con los códigos binarios lineales, generalizando un resultado de H. Haanpää y P. Östergárd [5]. En la sección 3 se muestra como el problema, relacionado con la función $B(n, d)$, es equivalente a un problema combinatorio de conjuntos S_h en $\mathbb{F}_2^r$. En la sección 4, se discuten algunas observaciones y ejemplos que determinan la importancia del Teorema principal. Finalmente se plantean algunos problemas abiertos en la dirección de este tema de investigación.

2. Conjuntos S_h y códigos lineales

Sean, G un grupo conmutativo notado aditivamente, $h \geq 1$ entero y A un subconjunto de G. Una $h-$*suma débil* de A es una suma de h elementos distintos de A.

Se dice que A es un *conjunto* S_h *en* G, si todas las $h-$sumas débiles en 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. En particular todo subconjunto de G es un conjunto S_1 en G.

El uso de los conjuntos S_h en la teoría de códigos aparece por primera vez en el año 1980 con los trabajos de R. L. Graham y N. J. A. Sloane [7], relacionando los conjuntos S_h con los códigos binarios de peso constante. Posteriormente H. Derksen, en el año 2004 (véase [4]), retomo estas ideas construyendo nuevos códigos binarios de peso constante, y a partir de ellos nuevos códigos binarios no lineales.

Por otra parte, no es la primera vez que se encuentra una relación entre la Teoría de Códigos y la Teoría de Números Aditiva. En el año 1999, G. Cohen y G. Zémor presentaron el artículo: *Subset Sums and Coding Theory* [2], en el cual abordan tres problemas de teoría de números aditiva, relacionados con la representación de cada elemento de $\mathbb{F}_2^r$ como suma de t o menos elementos de un subconjunto de $\mathbb{F}_2^r$ dado. Dichos problemas son resueltos aplicando resultados de códigos lineales. Posteriormente, G. Cohen, G. Zémor y S. Litsyn, en el año 2000, estudiaron los conjuntos S_2 en $\mathbb{F}_2^r$ (véase [3]), centrando su atención en el problema de determinar el máximo número de elementos que puede tener un conjunto S_2 en $\mathbb{F}_2^r$.

Recientemente, en el año 2007, H. Haanpää y P. Östergárd [5], muestran una correspondencia biunívoca entre los $[n, n-r, 5]$-códigos binarios y los conjuntos S_2 en $\mathbb{F}_2^r$. De manera más precisa demostraron el siguiente teorema.

Teorema 1. *Existe un $[n, n-r, 5]-$código binario si y sólo si existe un conjunto S_2 en $\mathbb{F}_2^r$ con $n+1$ elementos.*

Primero que todo, nótese que si $A = \{a_1, \ldots, a_n\}$ es un subconjunto de $\mathbb{F}_2^r$ y se forma la matriz $H = [a_1, \ldots, a_n]$ de tamaño $r \times n$ con los elementos de A como columnas, entonces el código lineal binario $\mathcal{C}$ que tiene a H como matriz de chequeo de paridad está dado por el espacio nulo de la transformación lineal:

$$\begin{aligned} \sigma : \mathbb{F}_2^n &\longrightarrow \mathbb{F}_2^r \\ \mathbf{x} &\longmapsto \sigma(\mathbf{x}) = H\mathbf{x}^t. \end{aligned}$$

Como se mostrará en los siguientes resultados, las propiedades del código lineal binario $\mathcal{C}$ dependen de las propiedades del conjunto A. Por ejemplo si A es un conjunto generador de $\mathbb{F}_2^r$, entonces H tendrá rango r y la dimensión de $\mathcal{C}$ será $k = n - r$. Sin embargo, se requiere una propiedad adicional en A para poder determinar la distancia mínima de $\mathcal{C}$.

Los tres lemas siguientes son bien conocidos en Teoría de Códigos Correctores de Errores.

Lema 2. *[6, capítulo 1, teorema 9] Si $\mathcal{H}$ es una matriz de chequeo de paridad de un código de longitud n, entonces el código tiene dimensión $n-r$ si y sólo si existen r columnas de $\mathcal{H}$ que forman un conjunto linealmente independiente ($\mathcal{H}$ tiene rango r).*

Lema 3. *[6, capítulo 1, teorema 10] Si $\mathcal{H}$ es una matriz de chequeo de paridad de un código de longitud n, entonces el código tiene distancia mínima d si y sólo si cualquier conjunto con $d-1$ columnas de $\mathcal{H}$ es un conjunto linealmente independiente y existe un conjunto con d columnas de $\mathcal{H}$ que es linealmente dependiente.*

Lema 4. *[6, capítulo 1, teorema 11] Si $\mathcal{C}$ es un $[n,k,d]-$código, entonces*

$$k+d \leq n+1. \qquad (\textit{Cota Singleton})$$

A continuación se muestran algunas propiedades de los conjuntos S_h en $\mathbb{F}_2^r$, las cuales son fundamentales para garantizar el Teorema principal.

Lema 5. *Si A es un conjunto S_h en $\mathbb{F}_2^r$ con $\mathbf{0} \in A$, donde $|A| \geq r > 2h$, entonces:*

i) A es un conjunto S_{h-1}. Más aún A es un conjunto S_j, para todo $1 \leq j \leq h$.

ii) Todo subconjunto de A con $2h$ elementos no nulos es linealmente independiente en $\mathbb{F}_2^r$.

iii) Si A tiene un número óptimo de elementos en $\mathbb{F}_2^r$ (el máximo número de elementos posible que puede tener un conjunto S_h en $\mathbb{F}_2^r$) entonces A contiene una base de $\mathbb{F}_2^r$ como espacio vectorial sobre $\mathbb{F}_2$.

Demostración.

i) Si hay dos $(h-1)-$sumas débiles iguales en A, éstas requieren a lo más $2h-2 < |A|$ elementos distintos de A. Sumando en ambos lados un elemento de A, distinto a los usados antes, se obtienen dos $h-$sumas débiles iguales en A, lo cual contradice el hecho de que A es un conjunto S_h.

ii) Supóngase que $\{a_1, \ldots, a_{2h}\} \subset A$ es un conjunto linealmente dependiente. Entonces existen escalares $\lambda_1, \lambda_2, \ldots, \lambda_{2h} \in \mathbb{F}_2$, no todos nulos tales que

$$\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_{2h} a_{2h} = 0. \qquad (1)$$

Sea $t = \big|\{i : \lambda_i = 0\}\big|$. Si t es par, se pueden formar dos $(h-\frac{t}{2})$-sumas débiles iguales y se completan h-sumas débiles iguales sumando en ambos lados $\frac{t}{2}$ vectores binarios distintos tomados de aquellos que tienen coeficiente nulo en (1). Si t es impar, dado que $\mathbf{0} \in A$, se suma la r-upla nula para formar

dos $\left\lceil \frac{2h-t}{2} \right\rceil$-sumas débiles iguales y de nuevo se completan $h-$sumas débiles iguales sumando en ambos lados $\left\lfloor \frac{t}{2} \right\rfloor$ vectores binarios como antes. En ambos casos se tiene una contradicción con la definición de conjunto S_h y, en conclusión, $\{a_1, a_2, \ldots, a_{2h}\}$ es linealmente independiente.

iii) Finalmente, si A tiene un número óptimo de elementos y no contiene una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$, entonces $Gen(A) \subset \mathbb{F}_2^r$ y por tanto existe $\alpha \in \mathbb{F}_2^r \setminus Gen(A)$. Se mostrará bajo el supuesto anterior que $B = A \cup \{\alpha\}$ es un conjunto S_h en $\mathbb{F}_2^r$. Si existen dos h-sumas débiles iguales en B, entonces al menos una de ellas debe tener a α como sumando, pues en caso contrario A no seria un conjunto S_h. De otro lado, no es posible que ambas h-sumas débiles tengan a α como sumando porque en este caso se tendrían dos $(h-1)$-sumas débiles iguales en A contradiciendo i). En resumen sólo una h-suma tiene a α, de aquí que $\alpha \in Gen(A)$, lo cual es una contradicción. Pero que $B = A \cup \{\alpha\}$ sea un conjunto S_h contradice la maximalidad de A como conjunto S_h, por tanto A debe contener una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$. ☑

Los trabajos de R. L. Graham, N. J. A. Sloane y H. Derksen muestran como desde la Teoría de Números Aditiva, con los conjuntos S_h, se pueden construir códigos binarios no lineales. Sin embargo en estos trabajos no se considera la construcción de conjuntos S_h a partir de códigos binarios no lineales. De hecho no se sabe si existen.

En el caso de códigos lineales, el siguiente resultado, muestra una relación biunívoca entre conjuntos S_h y códigos lineales.

Teorema 6 (Teorema principal)**.** *Existe un $[n, k, d]$-código binario con $d \geq 2h+1$ si y sólo si existe un conjunto S_h con $n+1$ elementos en $\mathbb{F}_2^{n-k}$, donde $n - k \geq 2h$.*

Demostración. ($\Longrightarrow$) Sea $\mathcal{H}$ una matriz de chequeo de paridad de un $[n, k, d]$-código binario con distancia mínima $d \geq 2h+1$ y sea $r = n-k$. Entonces sus n columnas son no nulas y distintas (lema 3). Sea A el conjunto de las n columnas de $\mathcal{H}$ junto con la r-upla nula de $\mathbb{F}_2^r$. Si hubiesen dos h-sumas débiles iguales en A, es decir, si

$$\sum_{i=1}^{h} a_i = \sum_{i=1}^{h} b_i, \quad \text{con} \quad a_i \neq a_j, \quad b_i \neq b_j \quad \text{para} \quad i \neq j \quad \text{y} \quad \{a_i\} \neq \{b_i\}$$

entonces se tendrían $2h$ o menos columnas de $\mathcal{H}$ que forman un conjunto linealmente dependiente, contradiciendo el lema 3. Además, del lema 4 (*Cota Singleton*)

$$k + 2h + 1 \leq k + d \leq n + 1,$$

de donde $n - k \geq 2h$.

($\Longleftarrow$) Sea $r = n-k$. Supóngase que existe un conjunto S_h con $n+1$ elementos en $\mathbb{F}_2^r$, donde $n > r \geq 2h$; tal conjunto está contenido en un subconjunto A de $\mathbb{F}_2^r$ con un número óptimo de elementos y con la propiedad de ser un conjunto S_h. Si $b \in A$ entonces el conjunto

$$b + A = \{b + a : a \in A\}$$

es también un conjunto S_h con un número óptimo de elementos y tiene la r-upla nula. Del lema 5 parte iii), $b + A$ contiene una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$. Sea H la matriz binaria de tamaño $r \times n$, donde sus columnas son n elementos no nulos de $b + A$ incluyendo una base de $\mathbb{F}_2^r$ sobre $\mathbb{F}_2$. El código con matriz de chequeo de paridad H tiene distancia mínima $d \geq 2h + 1$ según el lema 3 y el lema 5 parte ii). Además tiene dimensión $k = n - r$, dado que H tiene rango r (lema 2). ☑

Del Teorema principal (teorema 6) se puede inferir que toda construcción de códigos lineales debe tener asociado un conjunto S_h en $\mathbb{F}_2^r$, para algún r. Unos de los primeros códigos que aparecieron con el resultado de C. Shannon fueron los *códigos de Hamming*, los cuales pueden corregir errores simples (un error). A continuación se mostrará que los códigos de Hamming, con sus parámetros respectivos, aparecen con los conjuntos S_1.

Para n fijo, sea r el mínimo número natural tal que $n + 1 \leq 2^r$. Tómese un conjunto A de $\mathbb{F}_2^r$ con $n + 1$ elementos, con la propiedad de que para al menos un par de elementos no nulos $a_1, a_2 \in A$ se cumpla que $a_1 + a_2 \in A$. Por el Teorema principal existe un $[n, n - r, 3]$-código binario, con distancia mínima 3, como consecuencia del lema 3 y la propiedad exigida al conjunto A que es además un conjunto S_1 en $\mathbb{F}_2^r$.

Si $n = 2^m - 1$, entonces $r = m$ y $A = \mathbb{F}_2^m$. Con lo cual se obtiene un $[2^m - 1, 2^m - m - 1, 3]$-código lineal binario (corrector de errores simples), el cual es un código de Hamming correspondiente a estos parámetros.

3. Una consecuencia del Teorema principal

Volviendo al problema principal de códigos lineales, representado por la función:

$$B(n, d) := \text{máx}\left\{|\mathcal{C}| : \mathcal{C} \quad \text{es un código lineal en } \mathbb{F}_2^n, \text{ con } \quad \delta_{\mathcal{C}} \geq d\right\},$$

el cual es equivalente a determinar la máxima dimensión de un código lineal binario de longitud n y distancia mínima $\geq d$; puede notarse del Teorema principal, que un código lineal binario de longitud n y distancia mínima $d \geq 2h+1$ con máxima dimensión, se puede obtener buscando la mínima redundancia $r = n - k$, para el cual $\mathbb{F}_2^r$ tiene un conjunto S_h con $n + 1$ elementos. Este problema aditivo se representa con la siguiente función:

$$\upsilon(h, n) := \min_{2h \leq r < n} \left\{r : \mathbb{F}_2^r \quad \text{contiene un conjunto } S_h \text{ con } \quad n+1 \quad \text{elementos}\right\}.$$

Así, el estudio de la función $\upsilon(h,n)$ resulta fundamental para dar estimativos de la función $B(n,d)$, como lo muestra el siguiente corolario.

Corolario 7. *Sean n y h enteros positivos tales que $n > 2h$. Si existe $\upsilon(h,n)$ entonces*

$$\log_2 B(n, 2h+1) = n - \upsilon(h,n).$$

Demostración. Sea $\gamma = \upsilon(h,n)$, entonces existe un conjunto S_h en $\mathbb{F}_2^{\gamma}$ con $n+1$ elementos tal que $n > \gamma \geq 2h$. Como consecuencia del Teorema principal, existe un $[n, n-\gamma, d]-$código binario con $d \geq 2h+1$. De esta forma, $\log_2 B(n, 2h+1) \geq n - \upsilon(h,n)$. Si existe un $[n,k,d]$-código binario con $d \geq 2h+1$ y $k > n - \upsilon(h,n)$ entonces de nuevo por el Teorema principal, existe un conjunto S_h con $n+1$ elementos en $\mathbb{F}_2^{n-k}$, donde $n-k < \upsilon(h,n)$, contradiciendo la minimalidad de $\upsilon(h,n)$. Luego $\log_2 B(n, 2h+1) = n - \upsilon(h,n)$. ☑

***Observación* 8.** Considérese el caso particular $h = 2$, es decir,

$$\upsilon(2,n) := \min_{4 \leq r < n} \big\{ r : \mathbb{F}_2^r \quad \text{contiene un conjunto } S_2 \text{ con } \quad n+1 \quad \text{elementos} \big\},$$

y A es un conjunto S_2 en $\mathbb{F}_2^r$ con $n+1$ elementos; entonces el número de $h-$sumas débiles distintas es menor que el cardinal de $\mathbb{F}_2^r$, por lo cual

$$\binom{n+1}{2} \leq 2^r,$$

de donde se tiene la identidad

$$n(n+1) \leq 2^{r+1}. \tag{2}$$

Teniendo en cuenta ésta observación, se presenta el siguiente ejemplo.

Ejemplo 9. Mediante el uso del sistema de computo MuPAD, se obtuvo

$$A = \big\{ [0,0,0,0,0,0], [1,0,0,0,0,0], [0,1,0,0,0,0], [0,0,1,0,0,0], \\ [0,0,0,1,0,0], [0,0,0,0,1,0], [0,0,0,0,0,1], [1,1,1,1,0,0], [1,1,0,0,1,1] \big\},$$

un conjunto S_2 en $\mathbb{F}_2^6$ con 9 elementos. Además, la ecuación (2) impide que exista un conjunto S_2 con 9 elementos en $\mathbb{F}_2^5$. De esta manera $\upsilon(2,9) = 6$.

Por otra parte, en las tablas más conocidas para estimar $A(n,d)$ [6, apéndice A], las cuales calculan la mejor cota inferior para la menor redundancia de un código binario, se tiene por ejemplo, para $n = 7$ y $n = 8$, la redundancia

$$r = n - \log_2 A(n,5) \geq 6,$$

mientras que en códigos lineales la redundancia es

$$r = n - \log_2 B(n,5) = \upsilon(2,9) = 6,$$

en virtud del conjunto S_2 dado anteriormente. Esto muestra que la cota inferior para la menor redundancia no puede ser mejorada con códigos lineales, en estos casos.

4. Problemas abiertos

Otra tabla de cotas inferiores para $A(n,d)$, $279 \leq n \leq 512$, y $3 \leq d \leq 29$, la presenta H. Derksen [4, sección V], la cual da cotas inferiores para $\log_2 A(n,d)$.

Por ejemplo, para $279 \leq n \leq 293$

$$r = n - \log_2 A(n,5) \geq 17.84, \tag{3}$$

obtenida con códigos no lineales.

Además, se observo mediante búsqueda computacional, con el sistema de computo MuPAD, que el máximo número de elementos de un conjunto S_2 en $\mathbb{F}_2^r$, es del orden de la raíz cuadrada de 2^r, para valores pequeños de r. Si esto fuese cierto en general, entonces en $\mathbb{F}_2^{17}$ habría un conjunto S_2 con aproximadamente 362 elementos, con lo cual se tendría un $[n,k,d]-$código binario con $d \geq 5$, para $279 \leq n \leq 293$ y redundancia

$$r = n - \log_2 A(n,5) = 17,$$

mejorando lo hecho por Derksen en la expresión (3).

Con la anterior observación y el Teorema principal se plantean los siguientes interrogantes:

Construcción de conjuntos S_h. Dar una construcción de conjuntos S_h en $\mathbb{F}_2^r$ con $n+1$ elementos (más aún, con un número óptimo de elementos), con la que se garantice que $v(h,n)$ siempre existe.

Conjuntos S_h desde Códigos lineales. Dado el hecho de que cada código lineal binario determina un conjunto S_h en $\mathbb{F}_2^r$, surge el interrogante acerca de los conjuntos S_h asociados a códigos lineales como los códigos BCH, códigos cíclicos, los códigos MDS entre otros.

Agradecimiento. El primer autor agradece a la Universidad del Valle por el tiempo otorgado para la investigación en el proyecto 7803 de convocatoria interna.

Referencias

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

[2] Cohen G. and Zémor G., *Subset Sums and Coding Theory*, Astérisque **258** (1999), 327–339.

[3] Cohen G., Litsyn S., and Zémor G., *Binary B_2-Sequences: A New Upper Bound*, Journal of Combinatorial Theory, Series A **94** (2001), 152–155.

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

[5] Haanpää H. and Östergárd P., *Set in Abelian Group with Distinct Sums of Pairs*, Journal of Number Theory **123** (2007), 144–153.

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

[7] Graham R. L. and Sloane N. J. A., *Lower Bounds for Constant Weight Codes*, IEEE Transations on Information Theory **26** (1980), 37–43.

(Recibido en septiembre de 2010. Aceptado en septiembre de 2011)

Departamento de Matemáticas
Universidad del Valle
A.A. 25360
Calle 13 No 100-00
Cali, Valle del Cauca, Colombia
e-mail: carlos.a.gomez@correounivalle.edu.co

Departamento de Matemáticas
Universidad del Cauca
Calle 5 No. 4 - 70
Popayán, Cauca, Colombia
e-mail: trujillo@unicauca.edu.co