CUBO, Vol. 2, Marzo 1986
Pág. 37-56

INTRODUCCION A LA TEORIA ALGEBRAICA DE CODIGOS

Oscar Barriga B.*

El estudio de códigos es una rama de la ciencia de la información y comunicación, que utiliza resultados de campos diversos de la matemática tales como álgebra lineal, álgebra abstracta, teoría de números, teoría combinatoria, probabilidades, estadística, etc. Representa en particular, para cualquier matemático dedicado a alguno de estos campos y orientado a las aplicaciones, una buena manera de usar sus conocimientos abstractos en el "mundo real".

La teoría de códigos se aplica a situaciones que tienen el siguiente razgo común: Información proveniente de

* Facultad de Ciencias, Universidad de Chile.

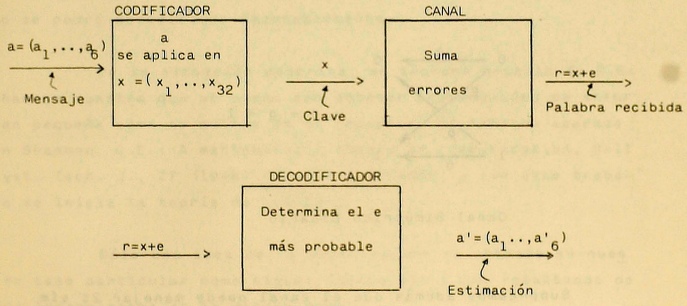
una fuente se transmite a través de un canal ruidoso a un receptor de información. (Conviene entender que "ruido" es genérico de perturbación, e.g. si la información es visual, el ruido puede ser alguna suciedad en los anteojos).

Ejemplos de tales situaciones son conversaciones telefónicas, información almacenada en un disco magnético que es alimentada a un computador, el telégrafo, la televisión, etc. Un ejemplo típico relativamente reciente es el que sigue: muchos de nosotros hemos visto excelentes imágenes tomadas de Marte, Saturno y otros planetas por los "Mariners", "Voyagers", etc. Para transmitir tales imágenes se ha dispuesto una fina malla sobre el objeto fotografiado y para cada cuadradito de la malla se ha medido el grado de luminosidad, digamos en una escala de 0 a 63. El número obtenido se ha escrito en sistema binario, es decir, cada cuadradito ha producido una hilera de seis 0's y 1's. Los 0's y los 1's se transmiten como dos señales diferentes al receptor en la tierra (Jet Propulsion Laboratory of the California Institute of Technology in Pasadena). Debido al efecto de ruido térmico sucede ocasionalmente que una señal transmitida como 0 es interpretada por el receptor como 1 y viceversa. Si los séxtuples de 0's y 1's mencionados fueran transmitidos como tales, entonces los errores cometidos por el receptor tendrían gran efecto en las imágenes finales. Para prevenir ésto, se introduce una así llamada redundancia en la señal, es decir, la sucesión transmitida consiste de más información que la necesaria. (Nótese que este principio es familiar en el lenguaje cotidiano: Un error de impresión en una palabra larga es fácilmente reconocible pues la palabra cambia a otra muy parecida). Las sucesiones más largas de 0's y 1's que son realmente transmitidas se llaman siempre palabras. De hecho, en el caso del Mariner 1969, las palabras consistían de 32 símbolos cada una.

Bastará por ahora entender que se ha diseñado un dispositivo que cambia las 64 informaciones posibles (séxtuples) en 64 posibles claves (palabras clave, palabras codificadas, codeword) cada una de las cuales es un 32-tuplo de 0's y 1's. Este dispositivo se llama codificador. La palabra codificada es transmitida, el ruido del canal introduce errores sumando módulo 2 alguna palabra al azar y el receptor tiene su propio dispositivo decodificador que cambia el 32-tuplo recibido, si no es una de las palabras clave, en la palabra clave más probable, lo que interpreta como la luminosidad del cuadradito correspondiente en su malla.

El código al que hemos hecho referencia tenía la propiedad de tomar la decisión correcta toda vez que no más de 7 de los 32 símbolos recibidos fueran incorrectos.

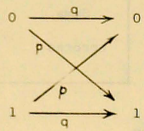
Podemos ilustrar la situación descrita así:



Tiene toda la razón quien objeta que la posibilidad de corregir errores ha cobrado peaje: El tiempo de transmisión necesario para la imagen del ejemplo es más de 5 veces el tiempo que habría tomado hacerlo sin la codificación descrita. Esto nos da una primera idea del interés en construir y analizar "buenos códigos".

Para acercarnos un poco más tanto a la idea como al origen de la teoría de códigos, consideremos el experimento que sigue:

Estamos en una pieza en que alguien lanza una moneda t veces por minuto. La pieza está conectada a otra pieza por una línea telegráfica. Supongamos que a través de este canal se puede enviar dos símbolos distintos, digamos 0 y 1. El canal es ruidoso y el efecto es que hay una probabilidad p que un símbolo transmitido 0 (respectivamente 1) sea recibido como 1 (respectivamente 0)



$p + q = 1$

Canal Simétrico Binario

Supongamos además que el canal puede manejar 2t símbolos por minuto y que podemos usarlo T minutos si el experimento dura T minutos.

Cada vez que la moneda cae cara transmitimos 0 y cada vez que cae sello transmitimos 1. Al final de la transmisión el receptor tendrá una fracción p de información incorrecta.

Si no tuviéramos la limitación del tiempo, podríamos obtener una probabilidad de error tan pequeña como quisiéramos fácilmente: Sea N natural impar, en lugar de 0 transmitimos N ceros y en lugar de 1 transmitimos N unos. Por ejemplo si p = 0.001, la probabilidad de error del decodificador es

$$\sum_{0<k<N/2} \binom{N}{k} q^k p^{N-k} < (0,07)^N$$

y para N ∞ esta probabilidad tiende a 0.

La limitación de tiempo es un problema serio. No tiene sentido enviar cada símbolo dos veces en lugar de una, pues no se podrá decodificar razonablemente.

En la situación descrita, un teorema notable de C.E. Shannon muestra que se puede aún obtener probabilidad de error tan pequeña como se quiera en el receptor. El teorema aparece en Shannon, C.E.: A mathematical theory of communication, Bell Syst. Tech. J., 27 (1948) 379-423 y 623-656, y con este trabajo se inicia la teoría de códigos.

Sólo una idea de la demostración se obtiene en nuestro caso particular como sigue: Transmitimos los resultados de dos lanzamientos de la moneda como

cara, cara $\longrightarrow$ 0 0 0 0

cara, sello $\longrightarrow$ 0 1 1 1

sello, cara $\longrightarrow$ 1 0 0 1

sello, sello $\longrightarrow$ 1 1 1 0

El decodificador usará el siguiente algoritmo completo: Si el cuádruple recibido no corresponde a una clave, supondrá que el cuarto símbolo es correcto y que uno de los primeros tres es incorrecto. Como la probabilidad de recibir correctamente una clave es q^4 y la probabilidad de recibirla con un error en uno de los primeros tres lugares es $3pq^3$, la probabilidad de decodificar correctamente es $q^4 + 3pq^3$, y basta que $p < \frac{1}{2}$ para que $q^4 + 3pq^3 > q^2$, que es la probabilidad de decodificar correctamente si no se usa el código descrito. El requisito sobre el tiempo de uso del canal se ha respetado.

Para mejorar nuevamente el resultado, transmitimos ahora tres lanzamientos de la moneda así: Si la información es el triple $a = (a_1, a_2, a_3)$ transmitimos el sextuple $(a_1, \ldots, a_6)$ en que $a_4 = a_2 + a_3$, $a_5 = a_1 + a_3$, $a_6 = a_1 + a_2$ (todas las sumas módulo 2). Hemos construído así un código que consiste de ocho claves, cada una de longitud 6. La palabra recibida es $b = a + e$ donde $e = (e_1, e_2, e_3, e_4, e_5, e_6)$ es el vector de error. Se tiene

$$e_2 + e_3 + e_4 = b_2 + b_3 + b_4 =: s_1 \quad \text{pues } a_2 + a_3 + a_4 = 0$$

$$e_1 + e_3 + e_5 = b_1 + b_3 + b_5 =: s_2 \quad \text{pues } a_1 + a_3 + a_5 = 0$$

$$e_1 + e_2 + e_6 = b_1 + b_2 + b_6 =: s_3 \quad \text{pues } a_1 + a_2 + a_6 = 0$$

Como el receptor conoce b, conoce s_1, s_2, s_3 y debe elegir el vector de error más probable, es decir aquél con el mínimo número de 1's. Si $(s_1, s_2, s_3) \neq (1,1,1)$ la elección es única, si $(s_1, s_2, s_3) = (1,1,1)$ el receptor debe elegir una de las tres posibilidades $(1,0,0,1,0,0), (0,1,0,0,1,0), (0,0,1,0,0,1)$ para e.

Se ve así que si e tiene un solo 1, es decir si hay un error entonces se decodifica correctamente. De los restantes hay uno con dos errores que también se decodifica correctamente. Así se tiene que la probabilidad es ahora $q^6 + 6pq^5 + p^2q^4 > q^4 + 3pq^3$, tan pronto $p < \frac{1}{2}$.

Tenemos ahora una idea de la importancia de las definiciones que siguen:

Si un código C consiste de claves de largo n, entonces $R = n^{-1} \log_2 |C|$ se llama la tasa de información del código.

En el caso del Mariner 1969 la tasa era entonces $\frac{6}{32}$, de acuerdo con la aseveración anterior que la transmisión tomaba más de 5 veces con el código que sin él.

Mencionamos también que dicho código tenía la propiedad de corregir hasta siete errores en una palabra recibida. La razón de ello es que dos claves de dicho código difieren al menos en 16 posiciones, de manera que la palabra recida con menos de 8 errores se parece a la clave correcta mucho más que a cualquiera otra.

Si x,y son dos n-tuplos de 0's y 1's, su distancia de Hamming es

$$d(x,y) = |\{ i \mid x_i \neq y_i , \quad 1 \leq i \leq n \}|$$

Las explicaciones anteriores están basadas en dos suposiciones: La primera es que durante la comunicación, todas las claves son equiprobables. La segunda es que si $n_1 > n_2$ entonces un vector de error con n_1 errores es menos probable que uno con n_2 errores.

Las suposiciones conducen a que, recibida una palabra "y" trataremos de encontrar una clave "x" tal que $d(x,y)$ sea minimal. Este principio se llama *principio de semejanza maximal*.

Los códigos descritos hasta ahora son ejemplos de una gran clase de códigos, llamados *códigos de bloques* y que podemos definir formalmente: Se tiene un alfabeto Q que consta de q símbolos distintos. Un código basado en este alfabeto es un código de bloques si la información codificada se puede dividir en bloques de n símbolos cada uno, que pueden ser decodificados independientemente. Los bloques son las claves y n se llama *longitud de bloque* o simplemente *longitud*.

Las definiciones anteriores se generalizan fácilmente: Si $x \in Q^n$, $y \in Q^n$ entonces la distancia $d(x,y)$ de x a y es

$$d(x,y) =: |\{ i \mid 1 \leq i \leq n, \quad x_i \neq y_i \}|$$

El *peso* de $x \in Q^n$ es

$$w(x) =: d(x,0)$$

(donde 0 denota $(0,\ldots,0)$ y $0 \in Q$ es un símbolo especial)

Naturalmente un código C es un subconjunto propio, no-vacío de Q^n. Si $|C| = 1$ el código se llama trivial. Si $q = 2$ el código es un código binario, si $q = 3$ es un código ternario, etc.

La distancia mínima de un código no trivial C es

$$\min \{d(x,y) \mid x \in C, \ y \in C, \ x \neq y\}$$

El peso mínimo de C es

$$\min \{w(x) \mid x \in C, \ x \neq 0\}$$

El radio de cubrimiento $\rho(C)$ del código C es

$$\max \{\min \{d(x,c) \mid c \in C\} \mid x \in Q^n\}$$

Si $B_\rho(x)$ denota la esfera de radio ρ y centro x, es decir $\{y \in Q^n \mid d(x,y) \leq \rho\}$, resulta claro que la distancia mínima del código C es el más grande ρ tal que las esferas $B_\rho(c)$ con $c \in C$ son disjuntas; en cambio el radio de cubrimiento es el más pequeño ρ tal que Q^n está contenido en la unión de las esferas $B_\rho(c)$ con $c \in C$. Si estos dos números coinciden el código C se llama un código perfecto.

Si el código C es perfecto, con distancia mínima $2e + 1$, entonces para cada $x \in Q^n$ hay una clave única en C a distancia menor o igual a e de x. Se dice que C corrige e errores.

Un simple cálculo muestra que un código perfecto C que corrige e errores satisface la siguiente condición de empaquetamiento de esferas:

$$|C| \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^n$$

Finalmente, para un código de bloques C con $|C|=M$, con $C \subseteq Q^n$ y distancia mínima d, se dice que se tiene un (n,M,d)-código y (n,M,d) se llaman los parámetros del código C.

Antes de continuar con más ideas generales completaremos un poco más los ejemplos. Para ello se necesita lo que sigue:

Definición: Una matriz cuadrada H de n filas y n columnas cuyos elementos son todos +1 ó -1 y tal que $H.H^t = nI$ se llama matriz de Hadamard.

Ejemplo: $$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Un buen ejercicio para un primer curso de Algebra Lineal es mostrar que el producto de Kronecker de dos matrices de Hadamard es nuevamente una matriz de Hadamard. Partiendo entonces con H_2 se puede conseguir matrices de Hadamard para n = potencia de 2. Para construir otras matrices de Hadamard el método más conocido se debe a R.E.A.C. Paley:

Recordemos que, si $\mathbb{F}_q$ denota el cuerpo con q elementos, el carácter cuadrático de $\mathbb{F}_q$ es la función X definida por (¡valores complejos!) $X(0) = 0$, $X(x) = 1$ si x es un cuadrado no-nulo en $\mathbb{F}_q$ y $X(x) = -1$ en los otros casos. Definiendo $s_{ij} = X(a_i - a_j)$ para a_i, a_j $\mathbb{F}_q$, la matriz $S = (s_{ij})$ se llama matriz de Paley y satisface

$$SJ = JS = 0$$

$$SS^t = qI - J$$

$$S^t = (-1)^{\frac{q-1}{2}} S$$

donde J es la matriz que consiste de elementos 1 enteramente.

Si a partir de la matriz de Paley S se construye la matriz de $q + 1$ filas y columnas

$$C = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ -1 & & & & \\ -1 & & & & \\ & & S & & \\ -1 & & & & \end{pmatrix}$$

la matriz C es una matriz de conferencia (es decir, tiene 0 en la diagonal, +1 o -1 fuera de ella y $CC^t = (n - 1)\mathbf{I}$.

En caso que $q \equiv 3 \pmod 4$ se puede considerar $H = I + C$ la cual, gracias a que $C^t = -C$ y -1 no es un cuadrado en $\mathbb{F}_q$, resulta ser una matriz de Hadamard.

Tomando $q = 11$, por ejemplo, se obtiene una matriz de Hadamard de 12 filas y columnas.

Es fácil probar que si H_n es una matriz de Hadamard de n filas y columnas, entonces n es un múltiplo de 4. Hasta 1978 no se conocía una matriz de Hadamard de orden 268, ni se sabía cuántas hay de orden 24.

El código descrito para el Mariner 1969 es un código en bloques construído a partir de H_{32} llamado código de Hadamard: En H_n y $-H_n$ se reemplaza cada -1 por 0, se tiene así $2n$ filas que son palabras en $\mathbb{F}_2^n$. Como dos filas cualesquiera de H_n difieren en la mitad de las posiciones, este es un código con parámetros $(n, 2n, \frac{1}{2}n)$, o bien $(32, 64, 16)$ en el caso descrito. Todos los detalles pueden ser recuperados ahora por el lector más interesado. En 1972, el Mariner 9 transmitió excelentes fotografías del Gran Cañón de Marte utilizando el código de Reed-Muller llamado $\mathbb{R}(1,5)$. En la construcción de éste código el papel principal lo juega el siguiente, hermoso teorema de Lucas (1878).

Teorema: Sea p primo y $n = \sum_{i=0}^{\ell} n_i p^i$, $k = \sum_{i=0}^{\ell} k_i p^i$ las representaciones de n y k en base p. Entonces

$$\binom{n}{k} \equiv \prod_{i=0}^{\ell} \binom{n_i}{k_i} \pmod{p}$$

En este punto pretendemos haber acumulado evidencia suficiente para justificar el deseo de construir códigos con alguna estructura algebraica. Una primera manera de lograrlo es eligiendo $Q = \mathbb{F}_q$, el cuerpo con q elementos como alfabeto ($q = p^r$, p primo). Entonces Q^n es un espacio vectorial de dimensión n, que se acostumbra denotar por $\mathbb{R}^{(n)}$ o simplemente $\mathbb{R}$ en teoría de códigos. Podemos definir ahora: Un código lineal C es un subespacio de $\mathbb{R}^{(n)}$. Si C tiene dimensión k entonces C es un $[n,k]$ - código y si la distancia mínima es d, es un $[n,k,d]$ - código. Nótese que en la notación anterior es un (n, q^k, d) - código.

Una matriz generadora G para el código lineal C es una matriz de k filas y n columnas, cuyas filas son una base del subespacio C.

Es claro que el código C se recupera a partir de G como $C = \{aG \mid a \in Q^k\}$.

G tiene forma standard si $G = (I_k P)$, en bloques donde I_k es la matriz identidad. En tal caso, los primeros k símbolos son símbolos de información y los restantes, llamados chequeos de paridad, están determinados por una clave.

Es claro que, en cuanto a capacidad de corregir errores, dos códigos C_1 y C_2 son igualmente buenos si C_2 se obtiene de C_1 aplicando una permutación fija a los símbolos de las palabras en C_1. Tales códigos se llaman equivalentes y el álgebra lineal elemental nos dice ahora que todo código lineal es equivalente a uno cuya matriz generadora tenga forma standard.

Sabemos que si la distancia mínima es 2e + 1 entonces C corrige hasta e errores. Si ella es 2e entonces detecta e errores.

En general, para calcular la distancia mínima se debe chequear $\binom{M}{2}$ pares de claves; pero si el código es lineal, el trabajo es menor:

Teorema: Para un código lineal, la distancia mínima es igual al peso mínimo.

Para demostrarlo basta observar que
$d(x,y) = d(x-y,0) = w(x-y)$ y que si $x,y \in C$ entonces $x-y \in C$.

Denotando por $\langle , \rangle$ el producto punto usual, se puede asociar a cada código C un código dual $C^{\perp}$ mediante

$$C^{\perp} = \{ y \in \mathbb{R}^{(n)} \mid \langle x, y \rangle = 0 \quad \forall\, x \in C \}$$

Nótese que éste no es necesariamente un "complemento" ortogonal en el sentido usual para espacios vectoriales sobre $\mathbb{R}$ ya que, sobre $\mathbb{F}_q$, C y $C^{\perp}$ pueden tener intersección no trivial, e incluso coincidir. El código C es auto - dual si $C = C^{\perp}$.

Nuevamente el álgebra lineal elemental muestra que si C es un $[n,k]$ - código entonces $C^{\perp}$ es un $[n,n-k]$ -código.

Si la matriz generadora de C es en forma standard $(I_k P)$ entonces la matriz $H = (-p^t I_{n-k})$ es generadora de $C^{\perp}$, pues tiene el rango y tamaño correcto y $GH^t = 0$ con lo cual cada fila de G es ortogonal a cada fila de H, i.e.

$$x \in C \Leftrightarrow x H^t = 0$$

Por esta razón H se llama la matriz de chequeo de paridad de C.

Para cada $x \in \mathbb{R}^{(n)}$ tiene sentido entonces llamar a xH^t el síndrome de x.

Para cada $x \in \mathbb{R}^{(n)}$ tiene sentido entonces llamar a Se tiene así que el síndrome de una clave es 0. Como C es un subespacio de $\mathbb{R}^{n)}$, el espacio $\mathbb{R}^{(n)}$ se particiona en clases laterales de $R^{n)}$. Nótese que x, y pertenecen a la misma clase lateral sí y solamente sí $x - y \in C$, lo que equivale a $(x - y) H^t = 0$ y esto ocurre sí y solamente sí $xH^t = yH^t$; i.e. x, y pertenecen a la misma clase lateral sí y solamente sí tienen el mismo síndrome. Si se recibe entonces la palabra $x = c + e$, con vector de error e, es claro que el síndrome de x y el de e son el mismo. De acuerdo al principio de semejanza maximal, se debe entonces encontrar un vector e de peso mínimo en la

clase lateral de x. Tal vector se llama vector líder de su clase lateral (coset leader).

Veamos como funciona ésto en la práctica, recordando el último código descrito para el experimento de lanzar la moneda: La información es un triple binario, se transmiten séxtuples y como los últimos tres símbolos son expresiones lineales en los tres primeros, el código es claramente lineal y su matriz generadora es (recordando $a_4 = a_2 + a_3$, etc.)

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{pues} \quad -p^t = P \text{ y } n - k = k = 3$$

$$H^t = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Si se recibe $b = (b_1, b_2, \ldots, b_6)$, se calcula

$$bH^t = (b_2 + b_3 + b_4,\ b_1 + b_3 + b_5,\ b_1 + b_2 + b_6).$$

Este es el síndrome, conocido al receptor. Supongamos por ejemplo que el síndrome es $(1,0,1)$. Se resuelve entonces el sistema

$$\begin{aligned} x_2 + x_3 + x_4 &= 1 \\ x_1 + x_3 + x_5 &= 0 \\ x_1 + x_2 + x_6 &= 1 \end{aligned}$$

La variedad de soluciones es $(0,1,0,0,0,0) +$ $+ (1,1,1,0,0,0), (1,1,0,1,1,0), (0,1,0,1,0,1)$ y se vé que el único vector líder posible es $0,1,0,0,0,0)$. Se decodifica entonces $x = (b_1, b_2 + 1, b_3, b_4, b_5, b_6)$. Un buen ejercicio de álgebra lineal es demostrar que para todo síndrome hay un único vector líder posible, salvo para $(1,1,1)$ para el cual hay tres vectores líderes posibles.

Resulta conveniente, a veces, agregar un símbolo extra a cada palabra de acuerdo a alguna regla bien establecida. La manera más usual de hacerlo, para un código C de longitud n sobre el alfabeto $\mathbb{F}_q$, es definiendo el código extendido $\bar{C}$ mediante

$$\bar{C} = \{(c_1, c_2, \dots c_n, c_{n+1}) \mid (c_1, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

Si C tenía matriz generadora G y matriz de chequeo de paridad H entonces $\bar{C}$ tiene matriz generadora $\bar{G}$ y matriz de chequeo de paridad $\bar{H}$ donde $\bar{G}$ se obtiene agregando una columna de manera que la suma de columnas de $\bar{G}$ sea 0 y donde

$$\bar{H} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ & & & 0 \\ & & & \vdots \\ & & H & \\ & & & 0 \end{pmatrix}$$

En caso que C sea un código binario con distancia mínima d entonces, si d es impar, la distancia mínima de $\bar{C}$ es $d + 1$ ya que todos los pesos y distancias para $\bar{C}$ son pares.

Si G es la matriz generadora de un $[n,k]$ - código C sobre $\mathbb{F}_q$, se dice que C es un código proyectivo cuando dos columnas cualesquiera de C son siempre linealmente independientes, es decir cuando las columnas de G representan puntos distintos de $PG(k-1,q)$.

Sea $n = \frac{q^k - 1}{q - 1}$. El $[n,n-k]$ - código de Hamming sobre $\mathbb{F}_q$ es un código para el cual la matriz de chequeo de paridad tiene columnas linealmente independiente a pares, i.e. las columnas son un conjunto maximal linealmente independiente a pares. Sea C un $[n,n-k]$ -código de Hamming. Si $c \in C$ y e es un vector de error de peso 1 entonces el síndrome de $c + e$ es $(c + e)H^t = cH^t + eH^t = eH^t = (0,\ldots,0,\ ,0,\ldots,0)H^t$ un múltiplo de una fila de H^t, es decir un múltiplo de una columna de H que determina claramente la columna de H primero y enseguida. Así C corrige un error. En consecuencia la distancia mínima de C es al menos 3. Por otra parte, una esfera de radio 1 alrededor de $c \in C$ contiene $1 + (q-1)n = 1 + (q-1)\frac{q^k - 1}{q - 1} = q^k$ palabras y como $q^k|C| = q^k.q^{n-k} = q^n$ resulta que C es perfecto y la distancia mínima es exactamente 3 (si fuera mayor, las esferas de radio 1 no podrían cubrir todo el espacio).

Como a veces no basta conocer la distancia mínima sino que se necesita saber más de todas las distancias posibles, se introduce los números

$$A_i = |\{ c \in C |\ w(c) = i\}|$$

La sucesión $\{A_i\}_{i=1}^{\infty}$ es la distribución de pesos de C y la función generatriz

$$A(z) =: \sum_{i=0}^{n} A_i z^i$$

se llama enumerador de pesos de C.

En 1963, F.J. Mac Williams demostró la hermosa, e importante relación siguiente entre el enumerados de pesos A(z) del código lineal C con parámetros [n,k] sobre $\mathbb{F}_q$ y el enumerador B(z) de su código dual $C^{\perp}$:

$$B(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right)$$

Posteriormente J.H. Van Lint ha encontrado una demostración relativamente simple de este hecho, que se puede encontrar en la bibliografía.

Un segundo tipo de ejemplos de códigos lineales se obtiene como sigue:

Un código C es un código cíclico si:

$$(c_0, c_1, \ldots, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in C$$

La herramienta algebraica es ahora el anillo cuociente del anillo de polinomios $\mathbb{F}_q[x]$ por el ideal principal $(x^n - 1)$. Considerados como grupos aditivos, hay un isomorfismo evidente entre $\mathbb{F}_q^n$ y $\mathbb{F}_q[x]/(x^n - 1)$ con la ventaja que el segundo tiene una estructura multiplicativa. El hecho importante aquí es el siguiente:

Un código lineal C en $\mathbb{F}_q^n$ es cíclico sí y solamente sí (bajo la identificación dada), C es un ideal en $\mathbb{F}_q[x]/(x^n - 1)$.

La Aritmética encuentra ahora una aplicación en teoría de códigos como sigue: Sea n un primo impar y sea $\mathbb{F}_q$ el alfabeto de tal manera que q sea un residuo cuadrático módulo n y sea α una raíz primitiva de la unidad en alguna extensión de $\mathbb{F}_q$. Sean

$$R_o = \{ i^2 \pmod{n} \mid i \in \mathbb{F}_n,\ i \neq 0 \}$$

$$R_1 = \mathbb{F}_n^* - R_o$$

$$g_o(X) = \prod_{r \in R_o} (X - \alpha^r),\quad g_1(X) = \prod_{r \in R_1} (x - \alpha^r)$$

Resulta que g_o y g_1 tienen coeficientes en $\mathbb{F}_q$ y que

$$x^n - 1 = (x - 1) g_o(X) g_1(X)$$

Los polinomios $g_o(X)$ y $(X - 1)g_1(X)$ generan ideales de $\mathbb{F}_q[X]$ que definen los códigos llamados <u>códigos de residuos cuadráticos</u>.

Para terminar con un ejemplo simple construyamos sobre $\mathbb{F}_3 = \{0,1,2\}$ un código de Hamming con

$$k = 2,\quad n = \frac{q^k - 1}{q - 1} = \frac{3^2 - 1}{3 - 1} = 4.$$

Para ello hay que escribir una matriz de dos filas y cuatro columnas linealmente independientes a pares, para lo cual basta escribir todas las columnas cuyo primer elemento no nulo es 1:

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Esta matriz, de chequeo de paridad, tiene la forma $(I_2 P)$. En consecuencia la matriz generadora, G es $(-P^t I_2)$ es decir

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}$$

El código es entonces $C = \{ xG \mid x \in \mathbb{F}_3^2 \}$ y podemos escribir explícitamente:

$(0,0)G = (0,0,0,0)$

$(0,1)G = (2,1,0,1)$

$(0,2)G = (1,2,0,2)$

$(1,0)G = (2,2,1,0)$

$(1,1)G = (1,0,1,1)$

$(1,2)G = (0,1,1,2)$

$(2,0)G = (1,1,2,0)$

$(2,1)G = (0,2,2,1)$

$(2,2)G = (2,0,2,2)$

Se puede ver ahora a simple vista que la distancia mínima es 3 y que C corrige un error, e.g. dándose un cuádruple cualquiera y encontrando en la lista un cuádruple a distancia a lo más 1 del dado.

Todos los tópicos apenas visualizados aquí, se encuentran en el excelente libro de J.H. Van Lint, Introduction to Coding Theory (Springer-Verlag, Graduate Texts in Mathematics 86 (1982)). Para una lectura más completa es recomendable además el de F.J. Mac Williams y N.J.A. Sloane, The Theory of error-correcting codes (North Holland Mathematical Library 16 1978)).