5 CÓDIGOS DE GOLAY

En 1949, Marcel Golay en un trabajo de una página de extensión dio la definición de una familia de cuatro códigos lineales, dos binarios y dos ternarios, dando las matrices generadoras de dichos códigos, sin ninguna indicación de cómo las obtuvo. Sin embargo, existen formas más naturales de definir estos códigos, pero esos métodos requieren más conceptos matemáticos de los desarrollados hasta el momento.

5.1. CÓDIGO DE GOLAY BINARIO G_{24}

El código de Golay binario G_{24} es un código sobre Z_2 cuyos parámetros son $(24, 12, 8)$, su matriz generadora es de la forma $G = (I_{12}\ A)$ siendo I_{12} la matriz identidad de orden 12 y A la matriz cuadrada 12×12

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Una forma fácil de recordar la matriz A, que además permite ahorrar cálculos en las demostraciones de las propiedades de G_{24}, es observar que la matriz de orden 11×11, A_1, obtenida de la matriz A eliminando la primera fila y la primera columna tiene una estructura cíclica. La primera fila de A_1 es *11011100010*. La segunda fila se obtiene de la primera desplazando cada dígito una posición a la izquierda y moviendo el primero a la última posición. La tercera fila se obtiene de la segunda de la misma forma, y así sucesivamente para las restantes filas. De esta forma, la matriz A puede recordarse como la matriz

$$A = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^{tr} & A_1 \end{pmatrix}.$$

donde $\mathbf{1}$ representa la palabra de longitud 11 cuyas entradas tiene todas el valor *1*.

La matriz A es una matriz simétrica, $A = A^{tr}$. Aplicando el teorema 2.3.4 la matriz 12×24, $H = (A\ I_{12})$ es una matriz control de paridad para G_{24}.

Otra matriz control de paridad para G_{24} es la propia matriz G. Por el teorema 2.3.2 sólo falta comprobar que el producto $G\ G^{tr}$ es la matriz nula. Para ello observemos que cada fila de la matriz A tiene peso impar (la primera 11 y las restantes 7). El producto de cada fila de A por sí misma es 1. A continuación, una comprobación manual muestra que el producto de la segunda fila de A por cualquier otra fila es nulo. Del carácter cíclico de A_1 se obtiene que el producto de dos filas cualesquiera de A es nulo. Así, $A\ A = A^2 = I_{12}$. Por tanto,

$$G\ G^{tr} = (I_{12}\ A)\ (I_{12}\ A)^{tr} = (I_{12})^2 + A^2 = I_{12} + I_{12} = (0).$$

En consecuencia, G_{24} es un código dual de sí mismo y el código lineal cuya matriz generadora es $(A\ I_{12})$ tiene el mismo conjunto de palabras código que G_{24}.

Teorema 5.1.1 La distancia mínima del código de Golay binario G_{24} es *8*.

Demostración. La demostración de este resultado se realiza en dos partes. En primer lugar se verá que toda palabra código de G_{24} tiene un peso múltiplo de 4; seguidamente, se descarta la existencia de palabras código cuyo peso sea 4, dado que las palabras código que forman la matriz G, excepto la primera, tienen peso 8 se obtiene el resultado.

El peso de cualquier palabra código $\boldsymbol{c}$ de G_{24} es un múltiplo de 4. Puesto que toda palabra código de G_{24} es suma finita de las palabras código que forman la matriz generadora G, demostraremos el resultado por inducción en el número de sumandos. Si la palabra código $\boldsymbol{c}$ es una fila de la matriz G, una simple observación de la matriz basta para concluir que $w(\boldsymbol{c}) = 8$ ó 12, en ambos casos un múltiplo de 4. Supongamos el resultado cierto si la palabra $\boldsymbol{c}$ es suma de i filas distintas de G; es decir, $w(\boldsymbol{c})$ es un múltiplo de 4; y demostrémoslo para el caso de que $\boldsymbol{c}$ sea suma de $i + 1$ filas. Sea $\boldsymbol{c} = \boldsymbol{v}_1 + \boldsymbol{v}_2 + \ldots + \boldsymbol{v}_i + \boldsymbol{v}_{i+1}$, con cada $\boldsymbol{v}_j$ una fila distinta de G. Denotemos por $\boldsymbol{c}_1$ la palabra código de G_{24}, $\boldsymbol{c}_1 = \boldsymbol{v}_1 + \boldsymbol{v}_2 + \ldots + \boldsymbol{v}_i$, cuyo peso es un múltiplo de 4 por la hipótesis de inducción. Por ser G una matriz control de paridad de G_{24}, $\boldsymbol{c}_1\ G^{tr} = (0)$, en particular el producto $\boldsymbol{c}_1\ \boldsymbol{v}_{i+1} = 0\ (mod\ 2)$, es decir las palabras $\boldsymbol{c}_1$ y $\boldsymbol{v}_{i+1}$ tienen un número par, pongamos 2λ, de posiciones en común con valor *1*. En consecuencia,

$$w(\boldsymbol{c}) = w(\boldsymbol{c}_1 + \boldsymbol{v}_{i+1}) = w(\boldsymbol{c}_1) + w(\boldsymbol{v}_{i+1}) - 2(2\lambda),$$

nuevamente el peso de $\boldsymbol{c}$ es un múltiplo de 4.

Para demostrar que ninguna palabra código de G_{24} tiene peso 4 utilizamos el hecho de que las matrices $G = (I_{12}A)$ y (AI_{12}) generan el mismo conjunto de palabras código. Así, para cada palabra código $\boldsymbol{c}$ de G_{24} existen dos palabras binarias de longitud 12, $\boldsymbol{u}_1$ y $\boldsymbol{u}_2$, tales que $\boldsymbol{c} = \boldsymbol{u}_1 (I_{12}A) = \boldsymbol{u}_2 (AI_{12})$. Si $w(\boldsymbol{c}) = 4$; entonces, entre las doce primeras componentes o entre las doce últimas componentes de $\boldsymbol{c}$, hay a lo sumo dos entradas no nulas de $\boldsymbol{c}$. Por tanto $w(\boldsymbol{u}_1) \leq 2$ ó $w(\boldsymbol{u}_2) \leq 2$. Sin embargo, cualquier fila y la suma de dos filas cualesquiera de la matriz A tiene un peso mayor que tres. Por tanto, $w(\boldsymbol{c}) = w(\boldsymbol{u}_i) + w(\boldsymbol{u}_i A) > 4$.

Por los parámetros de código, G_{24} es un código corrector de errores triples. La descodificación por medio de la tabla de síndromes requiere construir y comprobar una tabla con $2^{24-12} = 2^{12} = 4096$ síndromes; o al menos de 2324, si se utiliza la descodificación incompleta. Sin embargo, utilizando la estructura del código es posible definir un algoritmo de descodificación más simple.

Como se vio anteriormente, las matrices $G = (I_{12}\, A)$ y $H = (A\, I_{12})$ son matrices control de paridad del código G_{24}. Supongamos que en la transmisión de una palabra código de G_{24} se producen a lo sumo tres errores, siendo $\boldsymbol{r}$ la palabra recibida y $\boldsymbol{e}$ el vector error producido, con $w(\boldsymbol{e}) \leq 3$. La palabra $\boldsymbol{r}$ se divide en dos partes $\boldsymbol{r} = (\boldsymbol{r}_1,\boldsymbol{r}_2)$ siendo $\boldsymbol{r}_1$ la palabra de longitud 12 formada por las 12 primeras componentes de $\boldsymbol{r}$ y $\boldsymbol{r}_2$ la palabra de longitud 12 formada por las 12 últimas componentes de $\boldsymbol{r}$. De forma análoga, $\boldsymbol{e} = (\boldsymbol{e}_1,\boldsymbol{e}_2)$, con $\boldsymbol{e}_1$ y $\boldsymbol{e}_2$ palabras de longitud 12.

Como el peso del vector $\boldsymbol{e}$ es a lo sumo 3, entonces el peso de $\boldsymbol{e}_1$ o el peso de $\boldsymbol{e}_2$ es a lo sumo 1. Sea $\boldsymbol{s}_1 = \boldsymbol{e}\, G^{tr} = (\boldsymbol{e}_1,\boldsymbol{e}_2)\, (I_{12}\, A)^{tr} = \boldsymbol{e}_1 + \boldsymbol{e}_2 A$. Si $w(\boldsymbol{e}_2) \leq 1$, entonces $\boldsymbol{s}_1$ es una palabra de peso menor o igual que 3 (cuando $w(\boldsymbol{e}_2) = 0$) o una fila de la matriz A con a lo sumo dos de sus dígitos cambiados (cuando $w(\boldsymbol{e}_2) = 1$). Análogamente, si $w(\boldsymbol{e}_1) \leq 1$, entonces $\boldsymbol{s}_2 = \boldsymbol{e}\, H^{tr} = (\boldsymbol{e}_1,\boldsymbol{e}_2)\, (A\, I_{12})^{tr} = \boldsymbol{e}_1 A + \boldsymbol{e}_2$, es una palabra de peso menor o igual que 3 (cuando $w(\boldsymbol{e}_1) = 0$) o una fila de la matriz A con a lo sumo dos de sus dígitos cambiados (cuando $w(\boldsymbol{e}_1) = 1$).

En cualquier caso, si se producen hasta tres errores en la transmisión podemos localizar, en alguna de las matrices control de paridad, las columnas (tres a lo sumo) cuya suma es el síndrome correspondiente del error producido. Utilizando este hecho, obtenemos el algoritmo de descodificación buscado. Para evitar la utilización de dos matrices control de paridad observemos que $\boldsymbol{s}_2 = \boldsymbol{e}_1 A + \boldsymbol{e}_2 = (\boldsymbol{e}_1 + \boldsymbol{e}_2 A) A = \boldsymbol{s}_1 A$, pues $A^2 = I_{12}$. De esta forma, sólo se utiliza la matriz G. Por supuesto, una vez determinado el vector error $\boldsymbol{e}$, la palabra recibida se descodifica como la palabra código $\boldsymbol{c} = \boldsymbol{r} + \boldsymbol{e}$. Sea $\boldsymbol{u}_i$ la palabra de longitud 12 con un *1* en la i-ésima componente y *0* en las restantes y $\boldsymbol{a}_i$ la i-ésima fila o columna de la matriz A.

Algoritmo 5.1.2 Recibida una palabra binaria $\boldsymbol{r}$ de longitud 24,

(i) Se calcula el síndrome de la palabra recibida, $\boldsymbol{s} = \boldsymbol{r}\, G^{tr}$.

(ii) Si $w(\boldsymbol{s}) \leq 3$, entonces el vector error es $\boldsymbol{e} = (\boldsymbol{s},\boldsymbol{0})$.

(iii) Si $w(\boldsymbol{s} + \boldsymbol{a}_i) \leq 2$ para alguna fila $\boldsymbol{a}_i$ de la matriz A, entonces el vector error es $\boldsymbol{e} = (\boldsymbol{s} + \boldsymbol{a}_i,\boldsymbol{u}_i)$.

(iv) Se calcula el segundo síndrome de la palabra $\boldsymbol{r}$, $\boldsymbol{s}A$.

(v) Si $w(\boldsymbol{s}A) \leq 3$, entonces el vector error es $\boldsymbol{e} = (\boldsymbol{0},\boldsymbol{s}A)$.

(vi) Si $w(\boldsymbol{s}A + \boldsymbol{a}_i) \leq 2$ para alguna fila $\boldsymbol{a}_i$ de la matriz A, entonces el vector error es $\boldsymbol{e} = (\boldsymbol{u}_i,\boldsymbol{s}A + \boldsymbol{a}_i)$.

(vii) Si todavía no se ha determinado el vector error $\boldsymbol{e}$, solicitar una retransmisión pues se han producido más de tres errores.

Por las observaciones anteriores, si el peso del vector error es menor o igual que 3 se verifica alguna de las condiciones de los pasos (ii), (iii), (v) y (vi) del algoritmo. En cualquiera de ellas, se obtiene un vector de peso a lo sumo 3 cuyo síndrome coincide con el correspondiente síndrome de la palabra recibida $\boldsymbol{r}$. Dicho vector es pues el representante de la clase a la que pertenece $\boldsymbol{r}$. Este algoritmo requiere calcular, como mucho, el peso de 26 palabras de longitud 12 para realizar el proceso de descodificación. Evidentemente, una vez determinado el vector error $\boldsymbol{e}$ no es necesario realizar los siguientes pasos del algoritmo.

Ejemplo 5.1.3 Descodificar la palabra $\boldsymbol{r} = (101111101111,010010010010)$.

El síndrome es $\boldsymbol{s} = \boldsymbol{r}G^{tr} = 101111101111 + 010011111011 = 111100010100$, cuyo peso es 6. Sin embargo $\boldsymbol{s} + \boldsymbol{a}_5 = 111100010100 + 111100010110 = 000000000010$, de peso 1. Por tanto $\boldsymbol{e} = (\boldsymbol{s} + \boldsymbol{a}_5, \boldsymbol{u}_5) = (000000000010,000010000000)$, la palabra código enviada es $\boldsymbol{c} = (101111101101,010000010010)$. Como G_{24} es un código sistemático, el símbolo fuente es $\boldsymbol{m} = 101111101101$.

5.2. CÓDIGO DE GOLAY BINARIO G_{23}

Un nuevo código corrector de errores triples se puede conseguir acortando el código de Golay G_{24}. Esto es, considerar como conjunto de palabras código las palabras obtenidas eliminando la misma coordenada de todas las palabras código de G_{24}. En este caso, eliminamos la última.

Sea A' la matriz 12×11 obtenida de la matriz A eliminando la última columna. El código binario cuya matriz generadora es $G = (I_{12}\ A')$ se denomina código de Golay binario G_{23}, su longitud es 23, su dimensión sigue siendo 12 y su distancia mínima es 7. Es obvio que acortar un código no puede aumentar su distancia mínima ni disminuirla en más de una unidad, que es lo que ocurre en nuestro caso pues la matriz G tiene filas cuyo peso es 7.

El código G_{23} verifica la igualdad de Hamming,

$$2^{12} \times \left(1 + 23 + \binom{23}{2} + \binom{23}{3}\right) = 2^{23}$$

por tanto, es un código 3–perfecto.

Es inmediato comprobar que si el código G_{23} se amplia de forma análoga a la realizada con los códigos de Hamming binarios se obtiene el código G_{24}.

El proceso de descodificación para G_{23} se basa en el algoritmo definido para G_{24} y en el siguiente lema.

Lema 5.2.1 Sea $\boldsymbol{r}$ una palabra binaria de longitud 23 a la que se le añade un bit i de forma que la palabra de longitud 24 resultante $\boldsymbol{ri}$ tiene peso impar. Existe una única palabra código de G_{24} cuya distancia Hamming a la palabra $\boldsymbol{ri}$ es a lo sumo 3.

Demostración. El código G_{23} es un código 3–perfecto; por tanto, para toda palabra $\boldsymbol{r}$ de $(Z_2)^{23}$ existe una única palabra código $\boldsymbol{c}$ de G_{23} tal que $d(\boldsymbol{r},\boldsymbol{c}) \leq 3$.

Si $d(\boldsymbol{r},\boldsymbol{c}) \leq 2$, independientemente del valor de i, $d(\boldsymbol{r}i,\boldsymbol{c}0) \leq 3$ y $d(\boldsymbol{r}i,\boldsymbol{c}1) \leq 3$, siendo $\boldsymbol{c}0$ o $\boldsymbol{c}1$ una palabra código de G_{24}.

Si $d(\boldsymbol{r},\boldsymbol{c}) = 3$, $w(\boldsymbol{c})$ y $w(\boldsymbol{r})$ tienen distinta paridad pues,

$$3 = d(\boldsymbol{r},\boldsymbol{c}) = w(\boldsymbol{c}) + w(\boldsymbol{r}) - 2\, w(\boldsymbol{c} \wedge \boldsymbol{r}).$$

Siendo $\boldsymbol{c} \wedge \boldsymbol{r}$ la palabra binaria de longitud 23, cuya i-ésima componente vale *1* si las correspondientes componente de las palabras $\boldsymbol{c}$ y $\boldsymbol{r}$ valen *1* y *0* en los demás casos. Si $w(\boldsymbol{r})$ es par; por una parte, la palabra completada es $\boldsymbol{r}1$, por otra, el peso de $\boldsymbol{c}$ es impar y la palabra $\boldsymbol{c}1 \in G_{24}$. Por tanto, $d(\boldsymbol{r}1,\boldsymbol{c}1) = 3$. Si $w(\boldsymbol{r})$ es impar entonces $\boldsymbol{r}0$ es la palabra completada y la palabra $\boldsymbol{c}0 \in G_{24}$. De nuevo, $d(\boldsymbol{r}0,\boldsymbol{c}0) = 3$.

La unicidad es consecuencia inmediata de la unicidad de la existencia de la palabra código de G_{23}.

Recibida una palabra $\boldsymbol{r}$ de longitud 23, se le añade un dígito más *(0 ó 1)* de forma que la palabra $\boldsymbol{r}i$ *(i = 0 ó 1)* tenga peso impar. De esta forma la palabra $\boldsymbol{r}i$ se encuentra a una distancia menor o igual que 3 de un única palabra código de G_{24}. Descodificando la palabra $\boldsymbol{r}0$ o $\boldsymbol{r}1$ (según el caso) como la palabra código $\boldsymbol{c}'$ de G_{24} obtenida aplicando el algoritmo 5.1.2 y eliminando a continuación el último dígito de $\boldsymbol{c}'$ se obtiene la palabra código de G_{23} más próxima a la palabra $\boldsymbol{r}$. Por todo lo dicho, podemos definir el siguiente algoritmo para la descodificación del código G_{23}.

Algoritmo 5.2.2 Recibida una palabra binaria $\boldsymbol{r}$ de longitud 23,

(i) Añadir un *0* ó un *1* a la palabra recibida $\boldsymbol{r}$ de forma que la palabra $\boldsymbol{r}i$ *(i = 0 ó 1)* tenga peso impar.

(ii) Descodificar la palabra $\boldsymbol{r}i$ utilizando el algoritmo 5.1.2 como una palabra código $\boldsymbol{c}'$ de G_{24}.

(iii) La palabra $\boldsymbol{r}$ se descodifica como la palabra código $\boldsymbol{c}$ de G_{23} obtenida suprimiendo el último dígito de la palabra $\boldsymbol{c}'$.

En la práctica, la palabra recibida $\boldsymbol{r}$ es normalmente una palabra código; sin embargo, la palabra $\boldsymbol{r}i$ formada en el paso (i) nunca es una palabra código de G_{24} (su peso es impar y las palabras código de G_{24} tiene peso múltiplo de 4). Si $\boldsymbol{r}$ es una palabra código entonces el síndrome de $\boldsymbol{r}i$ será la última columna de la matriz G (pues se trata de un error simple en la última posición), esto puede comprobarse fácilmente antes de implementar el algoritmo descrito.