UNIVERSIDAD DE MURCIA

FACULTAD DE MATEMÁTICAS

TRABAJO FIN DE MÁSTER

TÉCNICAS ALGEBRAICAS EN CÓDIGOS CORRECTORES DE ERRORES

Autor:
Juan Adrián Vargas Alemañy
Tutor:
Juan Jacobo Simón Pinero

28 de Junio de 2019

Declaración de originalidad

Juan Adrián Vargas Alemañy autor del Trabajo de Fin de Máster *Técnicas algebraicas en códigos correctores de errores*, bajo la tutela del profesor Juan Jacobo Simón Pinero,

DECLARA

que el trabajo que se presenta es original, en el sentido de que ha puesto el mayor empeño posible en citar debidamente todas las fuentes utilizadas.

En Murcia, a 28 de Junio de 2019.

Fdo.: Juan Adrián Vargas Alemañy

Nota. En la Secretaría de la Facultad de Matemáticas se ha depositado una copia firmada de esta declaración.

Introducción

Uno de los tipos de Códigos Correctores de Errores más clásicos y estudiados es el de los códigos cíclicos. Muchas familias de códigos como por ejemplo los códigos de Golay, los códigos binarios de Hamming o los códigos Reed-Muller son, o bien códigos cíclicos, o bien una extensión de estos. El cálculo de la distancia mínima de un código cíclico, o de una cota inferior para ella, es uno de los principales problemas en el estudio de los códigos cíclicos (véase, por ejemplo, [2]). La cota inferior para la distancia mínima de un código cíclico más antigua es la cotas BCH [1]. Como veremos en este trabajo, un código cíclico puede tener asociadas varias cotas BCH.

El objetivo de este trabajo es tratar dos problemas relacionados con el máximo de las cotas BCH. El primero es dar condiciones necesarias y suficientes para que en un código cíclico dado, su distancia mínima coincida con el máximo de sus cotas BCH. El segundo problema es obtener un método que nos permita construir códigos cíclicos que cumplan dicha propiedad. En los Capítulos 2 y 3 mostramos la resolución de ambos problemas.

En el Capítulo 4, extendemos nuestros resultados a códigos abelianos de dos variables. Para ello, introducimos la noción de distancia aparente fuerte de un código abeliano, la cual veremos que es una cota inferior para la distancia mínima. Posteriormente, al igual que en el caso de los códigos cíclicos con el máximo de las cotas BCH, veremos condiciones necesarias y suficientes para que en un código abeliano su distancia mínima coincida con su distancia aparente fuerte, y estudiaremos un método para construir códigos abelianos de dos variables que cumplan dicha propiedad.

Índice general

Capítulo 1

Notación y preliminares

Sea q una potencia de un número primo p y n un entero positivo tal que $mcd(q, n) = 1$. Denotamos con $\mathbb{F}_q$ al cuerpo de q elementos, con R_n al conjunto de las raíces n-ésimas de la unidad y con U_n al conjunto de las raíces n-ésimas primitivas de la unidad, las cuales viven en una extensión $\mathbb{L} \mid \mathbb{F}_q$.

Denotamos con $\mathbb{F}_q[x]$ al anillo de polinomios con coeficientes en $\mathbb{F}_q$. Para un polinomio $g = g(x) \in \mathbb{F}_q[x]$, denotamos con deg(g) a su grado, con supp(g) a su soporte y con $w(g) = |supp(g)|$ a su peso.

Sea n un entero positivo. Denotamos el anillo cociente $\mathbb{F}_q[x]/(x^n - 1) = \mathbb{F}_q(n)$ e identificamos a los representantes canónicos $g \in \mathbb{F}_q(n)$ con polinomios, por lo que podemos escribir también $g \in \mathbb{F}_q[x]$, siempre que $deg(g) < n$. Cuando necesitemos ser más específicos con un polinomio $f \in \mathbb{F}_q[x]$, denotaremos con $\overline{f}$ a su representante canónico en $\mathbb{F}_q(n)$.

En $\mathbb{Z}_n$ consideramos siempre a los representantes canónicos. Si habiendo realizado operaciones aritméticas con representantes canónicos de $\mathbb{Z}_n$ obtenemos un elemento $y \notin \{0, \ldots, n-1\}$, denotaremos con $\overline{y}$ a su representante canónico. En el conjunto de los representantes canónicos de $\mathbb{Z}_n$ definimos el siguiente orden. Sean $i, j \in \{0, \ldots, n-1\}$ representantes canónicos. Entonces $i \leq j$ como elementos de $\mathbb{Z}_n$ si $i \leq j$ con el orden usual de los números enteros. Nótese que esto nos permite extender la noción de orden a todo $\mathbb{Z}_n$.

Un código abeliano cíclico (que llamaremos código cíclico) C

de longitud n en el alfabeto $\mathbb{F}_q$ es un ideal del anillo $\mathbb{F}_q(n)$. Si $mcd(q,n) = 1$, el anillo cociente $\mathbb{F}_q(n)$ es semisimple y por tanto cada código cíclico tiene un único polinomio generador mónico divisor de $x^n - 1$ ([1], Theorem 7.1) y un único polinomio generador idempotente ([1], Theorem 8.1). En particular, todo polinomio generador es divisor de $x^n - 1$ ([1], Theorem 7.1).

Por lo anterior, cada código cíclico C en $\mathbb{F}_q(n)$ está determinado por su conjunto de ceros definido como $Z(C) = \{\alpha \in R_n \mid c(\alpha) = 0,\ \forall c \in C\}$; así, para todo polinomio $f \in \mathbb{F}_q(n)$, tenemos que $f \in C$ si y solo si $f(\alpha) = 0\ \forall \alpha \in Z(C)$. Denotamos con $\overline{Z(C)}$ a su complemento, es decir, $\overline{Z(C)} = R_n \setminus Z(C)$. Fijado $\alpha \in U_n$, el conjunto de definición de C con respecto de α es $D_\alpha(C) = \{i \in \mathbb{Z}_n \mid \alpha^i \in Z(C)\}$. De manera análoga, podemos definir el conjunto de ceros y el conjunto de definición respecto de α para un polinomio $f \in \mathbb{F}_q(n)$.

Observación 1.0.1 *Nótese que* $Z(f) = Z(< f >)$ *y* $D_\alpha(f) = D_\alpha(< f >)$. *La inclusión* $Z(< f >) \subseteq Z(f)$ *es inmediata. Veamos ahora que* $Z(f) \subseteq Z(< f >)$. *Sea* $f' \in < f >$. *Si* $\alpha \in Z(f)$, *entonces* $f(\alpha) = 0$ *y como* $f \mid f'$, *se tiene que* $f'(\alpha) = 0$. *Esto implica* $Z(f) \subseteq Z(< f >)$. *Sabiendo que* $Z(f) = Z(< f >)$ *la igualdad* $D_\alpha(f) = D_\alpha(< f >)$ *es inmediata.*

Lema 1.0.2 *En un código cíclico* C *en* $\mathbb{F}_q(n)$ *con polinomio generador* $g(x)$, $D_\alpha(C) = D_\alpha(g)$.

Demostración. Inmediata por el hecho de que $C =< g >$ y por la Observación 1.0.1. ■

Dado un elemento $a \in \mathbb{Z}_n$, su clase q-ciclotómica módulo n es el conjunto $C_q(a) = \{\overline{q^i a} \in \mathbb{Z}_n \mid i \in \mathbb{N}\}$. Sabemos que para todo polinomio $f \in \mathbb{F}_q[x]$ y para todo elemento a de una extensión $\mathbb{L} \mid \mathbb{F}_q$, tenemos que si $f(a) = 0$ entonces $f(a^q) = 0$. De aquí se desprende que si $mcd(q,n) = 1$, el conjunto de definición de todo código cíclico C es unión de clases q-ciclotómicas módulo n, ya que si $i \in D_\alpha(C)$ entonces $qi \in D_\alpha(C)$ por el Lema 1.0.2 y lo anteriormente expuesto. Además, si $mcd(q,n) = 1$, las clases q-cilotómicas forman una partición de $\mathbb{Z}_n$. Vamos a verlo. Sean $a, b \in$

$\mathbb{Z}_n$ tales que $C_q(a) \neq C_q(b)$ pero $C_q(a) \cap C_q(b) \neq \emptyset$. Entonces existen $i, j \in \mathbb{N}$ tales que $q^i a \equiv q^j b \bmod n$. Como $mcd(n, q) = 1$, esto implica que $a \equiv q^{j-i} b \bmod n$ y por lo tanto $C_q(a) = C_q(q^{j-i}b) = C_q(b)$, lo que es una contradicción. Además, es inmediato ver que $\mathbb{Z}_n = \bigcup_{i=1}^{h} C_q(a_i)$ siendo $\{a_1, \ldots, a_h\}$ un conjunto completo de los representantes de las clases q-ciclotómicas.

Observación 1.0.3 *Hemos visto que para cualquier código C en $\mathbb{F}_q(n)$ su conjunto de definición con respecto a α es unión de clases q-ciclotómicas. Veamos ahora que para cualquier conjunto $D \subset \mathbb{Z}_n$, con D unión de clases q-ciclotómicas, existe un código C en $\mathbb{F}_q(n)$ tal que $D_\alpha(C) = D$.*

Sea $\alpha \in U_n$, $\mathbb{L} \mid \mathbb{F}_q$ una extensión tal que $U_n \subset \mathbb{L}$ y sea $s \in \{0, \ldots, n-1\}$. El polinomio mínimo de α^s en $\mathbb{F}_q$, el cual denotamos con m_{α^s}, se factoriza en $\mathbb{L}[x]$ como $m_{\alpha^s} = \prod_{i \in C_q(s)} (x - \alpha^i)$ ([2], Theorem 4.1.1). Sean $C_q(a_1), \ldots, C_q(a_h)$ las clases q-ciclotómicas módulo n siendo $\{a_1, \ldots, a_h\}$ un conjunto completo de los representantes de dichas clases. La factorización de $x^n - 1$ en $\mathbb{F}_q[x]$ es $x^n - 1 = \prod_{a_i \in \{a_1, \ldots, a_h\}} m_{a^{a_i}}(x)$ ([2], Theorem 4.1.1). Sea ahora C un código en $\mathbb{F}_q(n)$, con conjunto definición $D_\alpha(C) = C_q(a_{i_1}) \cup C_q(a_{i_2}) \cup \cdots \cup C_q(a_{i_s})$, con $\{a_{i_1}, a_{i_2}, \ldots, a_{i_s}\} \subset \{a_1, \ldots, a_h\}$. Entonces el polinomio generador mónico de C es $g = \prod_{a_{i_j} \in \{a_{i_1}, a_{i_2}, \ldots, a_{i_s}\}} m_{\alpha^{a_{i_j}}}$ ([2], Theorem 4.2.1).

Por lo tanto, si tenemos un conjunto unión de clases q-ciclotómicas $D = \bigcup_{j=1}^{t} C_q(a_{i_t})$, con $\{a_{i_1}, a_{i_2}, \ldots, a_{i_t}\} \subset \{a_1, \ldots, a_h\}$ y tomamos el polinomio $g = \prod_{a_{i_j} \in \{a_{i_1}, a_{i_2}, \ldots, a_{i_t}\}} m_{\alpha^{a_{i_j}}}$, entonces el código $C =< g >$ tiene como conjunto definición $D_\alpha(C) = D_\alpha(g) = D$.

En resumen, para cualquier código C en $\mathbb{F}_q(n)$ su conjunto definición es unión de clases q-ciclotómicas y para cualquier conjunto D unión de clases q-ciclotómicas existe un único código C tal que $D_\alpha(C) = D$; es decir, hay una relación uno a uno entre los có-

digos en $\mathbb{F}_q(n)$ *y los conjuntos* $D \subset \mathbb{Z}_n$ *que son unión de clases q-ciclotómicas.*

Ejemplo 1.0.4 *Sea* $q = 2$, $n = 15$. *Las clases* 2*-ciclotómicas módulo* 15 *son*

$$C_2(0) = \{0\},$$
$$C_2(1) = \{1, 2, 4, 8\},$$
$$C_2(3) = \{3, 6, 9, 12\},$$
$$C_2(5) = \{5, 10\},$$
$$C_2(7) = \{7, 11, 13, 14\}.$$

Puesto que hay 5 clases 2*-ciclotómicas distintas podemos formar* $2^5 = 32$ *conjuntos unión de clases* 2*-ciclotómicas distintos y por lo tanto hay* 32 *códigos cíclicos distintos en* $\mathbb{F}_2(15)$.

Veamos que esta última observación no es cierta si estamos en el caso no semisimple, es decir, si $mcd(n, q) \neq 1$.

Ejemplo 1.0.5 *Sea* $q = 2$, $n = 4$. *Tenemos que* $mcd(4, 2) = 2 \neq 1$. *Es fácil comprobar que* $x^4 - 1$ *se factoriza en* $\mathbb{F}_2[x]$ *como* $x^4 - 1 = (x + 1)^4$, *por lo tanto* $\{1\}$ *es la única raíz cuarta de la unidad y tiene multiplicidad cuatro. Por otro lado, tenemos que* $C_2(0) = \{0\}$ *y* $C_2(1) = \{1, 2, 0\}$, *por lo que las clases* 2*-ciclotómicas no forman una partición de* $\mathbb{Z}_4$. *Como* $D_\alpha(C) = \{0\}$ *para cualquier código* C *en* $\mathbb{F}_2(4)$ *tenemos que no podemos tener un código con conjunto definición* $D_\alpha(C) = \{0, 1, 2\}$.

Denotamos con $d(C)$ a la distancia mínima de cualquier código C. El teorema de la cota BCH establece que para cualquier código cíclico en $\mathbb{F}_q(n)$ que tenga una lista de longitud $\delta - 1$ de enteros consecutivos $\{i_1, \ldots, i_{\delta-1}\}$, con $i_j + 1 = i_{j+1}$ para todo $j \in \{1, \ldots, \delta - 2\}$, tal que, para un cierto $\alpha \in R_n$, $\alpha^i \in Z(C)$ $\forall i \in \{i_1, \ldots, i_{\delta-1}\}$, se cumple que $d(C) \geq \delta$ ([1], Theorem 7.8).

Veamos cómo expresar esto último en términos de los conjuntos de definición. Sea $\{i_1, \ldots, i_k\}$ un subconjunto de representantes canónicos de $\mathbb{Z}_n$. Decimos que estos elementos son una lista de longitud k de enteros consecutivos módulo n si $\overline{i_j + 1} = i_{j+1}$ para todo $j \in \{1, \ldots, k - 1\}$. En términos de los conjuntos de definición, el teorema de la cota BCH establece entonces que si existe una lista de longitud $\delta - 1$ de enteros consecutivos módulo n en $D_\alpha(C)$, para

algún $\alpha \in U_n$, entonces $d(C) \geq \delta$. A cada número δ que podamos encontrar que cumpla las condiciones anteriores le denominaremos una cota BCH del código. Para cualquier código cíclico C denotamos con $\Delta(C)$ al máximo de sus cotas BCH.

Observación 1.0.6 *Tenemos que tener en cuenta que diferentes raíces de la unidad pueden dar lugar a diferentes conjuntos definición y por lo tanto a diferentes cotas BCH. Para calcular* $\Delta(C)$ *no es necesario calcular el conjunto de definición respecto de todos los elementos de* U_n *ya que, fijado un* $\alpha \in U_n$*, para calcular una cota BCH distinta, necesitamos un elemento* $\beta \in U_n$ *tal que* $D_\alpha(C) \neq D_\beta(C)$*. Queremos, por lo tanto, identificar los elementos* $\beta \in U_n$ *tales que* $D_\alpha(C) \neq D_\beta(C)$*. Sea* $\beta \in U_n$ *tal que* $D_\alpha(C) \neq D_\beta(C)$*. Veamos qué condiciones debe cumplir* β*.*
Sean $C_q(a_1), \ldots, C_q(a_h)$ *las clases q-ciclotómicas módulo n siendo* $\{a_1, \ldots, a_h\}$ *un conjunto completo de los representantes de las clases. El elemento* β *debe satisfacer la igualdad* $\beta^{a_i q^j} = \alpha$ *para algún* $a_i \in \{a_1, \ldots, a_h\}$ *y* $j \in \mathbb{Z}$*. Puesto que* $\beta^{a_i q^j} = \alpha \in U_n$ *tenemos que* $mcd(a_i q^j, n) = 1$*, lo que implica que* $mcd(a_i, n) = 1$*. Además, tomando un* $j' \in \mathbb{Z}_n$ *adecuado,* $\beta^{a_i} = \beta^{a_i q^j q^{j'}} = \alpha^{j'}$*. Puesto que* $mcd(a_i q^j, n) = 1$*, tenemos que* $\alpha^{q^{j'}} = \beta^{a_i} \in U_n$*. Como* $D_\alpha(C) = D_{\alpha^{q^{j'}}}(C)$*, tenemos que cualquier elemento* $\beta \in U_n$ *tal que* $D_\alpha(C) \neq D_\beta(C)$ *tiene que cumplir que* $\beta^{a_i} = \alpha$ *para algún* $a_i \in \{a_1, \ldots, a_h\}$ *con* $mcd(a_i, n) = 1$*. Además* $D_\beta(C) = a_i \cdot D_\alpha(C) = \{a_i \cdot j \mid j \in D_\alpha(C)\}$ *. Definimos el conjunto*

$$A(n) = \{(a_i \mid mcd(a_i, n) = 1\}. \tag{1.1}$$

Ejemplo 1.0.7 *Sea* $n = 41$ *y* $q = 2$*. Las clases 2-ciclotómicas módulo 41 son*

$C_2(0) = \{0\}$,
$C_2(1) = \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}$,
$C_2(2) = \{3, 6, 7, 11, 12, 13, 14, 15, 17, 19, 22, 24, 26, 27, 28, 29, 30, 34, 35, 38\}$.

Sea $\alpha \in U_{41}$ *y tomamos el código cíclico* C *tal que* $D_\alpha(C) = C_2(1)$*. Las cotas BCH que podemos encontrar en este conjunto de definición* $D_\alpha(C)$ *son* $\delta_1 = 3$*, tomando, por ejemplo, las listas de longitud* 2 *de enteros consecutivos módulo* 41 $\{1, 2\}, \{4, 5\}, \{20, 21\} \subset$

$D_\alpha(C)$ y $\delta_2 = 4$, tomando $\{8,9,10\},\{31,32,33\} \subset D_\alpha(C)$. Para calcular $\Delta(C)$ tenemos que calcular las cotas BCH que podemos encontrar en los conjuntos de definición $D_\beta(C)$ con $D_\beta(C) \neq D_\alpha(C)$. Puesto que $A(41) = \{1,3\}$ tan solo tenemos que considerar el conjunto $D_\beta(C) = 3 \cdot D_\alpha(C) = C_2(3)$. En este conjunto, podemos encontrar una cota BCH mayor que las que hemos obtenido anteriormente ya que $\{26,27,28,29,30\} \subset D_\beta(C)$, con lo que obtenemos una cota BCH $\delta_3 = 6$. Por lo tanto, tenemos que $\Delta(C) = 6$.

Un código cíclico C en $\mathbb{F}_q(n)$, con polinomio generador $g(x)$, es un código BCH de distancia designada δ si existe $\alpha \in U_n$ y $b \in \{0,\ldots,n-1,\}$ tales que $g(x)$ es el polinomio mónico de menor grado en $\mathbb{F}_q$ tal que $g(\alpha^{b+j}) = 0\ \forall j \in \{0,\ldots,\delta-2\}$, de hecho $g = mcd(m_{\alpha^b}, m_{\alpha^{b+1}},\ldots,m_{\alpha^{b+\delta-2}})$. Es decir, $g(x)$ es el polinomio mónico de menor grado en $\mathbb{F}_q$ tal que $\{\alpha^{b+j} \mid j = 0,\ldots,\delta-2\} \subseteq Z(g) \underset{\text{Lema 1.0.2}}{=} Z(C)$. Puesto que $g(\alpha^{b+j}) = 0\ \forall j \in \{0,\ldots,\delta-2\}$ se tiene que $\{b,\ldots,\overline{b+\delta-2}\}$ es una lista de longitud $\delta-1$ de enteros consecutivos módulo n en $D_\alpha(C)$ y por el teorema de la cota BCH, tenemos que $d(C) \geq \delta$. De aquí que, en términos del conjunto de definición, C es un código *BCH* de distancia δ si para toda clase q-ciclotómica $Q \subseteq D_\alpha(C)$ tenemos que $Q \cap \{\overline{b+j} \mid j = 0,\ldots,\delta-2\} \neq \emptyset$.

Sea $\mathbb{L} \mid \mathbb{F}_q$ una extensión de cuerpos tal que $U_n \subseteq \mathbb{L}$ y sea $\alpha \in U_n$. La transformada de Fourier discreta de un polinomio $f \in \mathbb{F}_q(n)$ con respecto a α (conocido también como el polinomio de Mattson-Solomon), que denotamos con $\varphi_{\alpha,f}$, se define como

$$\varphi_{\alpha,f}(x) = \sum_{j=0}^{n-1} f(\alpha^j)x^j.$$

Claramente, $\varphi_{\alpha,f} \in \mathbb{L}(n)$; es más, podemos ver a esta función como un isomorfismo de álgebras $\varphi_\alpha : \mathbb{L}(n) \longrightarrow (\mathbb{L}^n, \star)$, donde la operación "$\star$" en $\mathbb{L}^n$ es la multiplicación componente a componente ([1], Theorem 8.22). De esta manera podemos ver a $\varphi_{\alpha,f}$ como un vector en $\mathbb{L}^n$ o como un polinomio en $\mathbb{L}(n)$.

La inversa de la transformada de Fourier discreta viene dada por $\varphi^{-1}_{\alpha,g}(x) = \frac{1}{n}\sum_{i=0}^{n-1} g(\alpha^{-i})x^i$ ([1], Theorem 8.20) donde $g \in \mathbb{L}(n)$.

Para cualquier $i \in \{0, \ldots, n-1\}$ denotamos $\varphi_{\alpha,f}[i] = f(\alpha^i)$ al coeficiente de x^i.

Observación 1.0.8 *Para cualquier $\alpha \in U_n$, $f \in \mathbb{F}_q(n)$ y $g \in \mathbb{L}(n)$ tenemos que:*

1. *$supp(\varphi_{\alpha,f}) = \{i \in \{0, \ldots, n-1\} \mid f(\alpha^i) \neq 0\}$ y por lo tanto $\mathbb{Z}_n \setminus supp(\varphi_{\alpha,f}) = D_\alpha(f)$.*

2. *Puesto que $f = \varphi^{-1}_{\alpha,\varphi_{\alpha,f}}(x)$, $supp(f) = \{i \in \{0, \ldots, n-1\} \mid \varphi_{\alpha,f}(\alpha^{-i}) \neq 0\}$, por lo que $|supp(f)| = n - |Z(\varphi_{\alpha,f})| = \left|\overline{Z(\varphi_{\alpha,f})}\right|$.*

3. *$\varphi^{-1}_{\alpha,g} \in \mathbb{F}_q(n)$ si y solo si $(g(\alpha^j))^q = g(\alpha^j)\ \forall\ j \in \{0, \ldots, n-1\}$.*

4. *$\varphi^{-1}_{\alpha,g} \in \mathbb{F}_q(n)$ si y solo si $\varphi^{-1}_{\beta,g} \in \mathbb{F}_q(n)\ \forall \beta \in U_n$.*

Demostración.

1. y 2. Triviales por la definición de la transformada de Fourier discreta.

3. Directa por la propiedad de que un elemento $a \in \mathbb{L}$ cumple que $a \in \mathbb{F}_q$ si y solo si $a^q = a$.

4. Basta observar que para dos elementos $\alpha, \beta \in U_n$ con $\alpha \neq \beta$, los coeficientes de $\varphi^{-1}_{\alpha,g}$ son los mismos que los de $\varphi^{-1}_{\beta,g}$ pero permutados; es decir, aparecerán en monomios posiblemente de otros grados.

■

Capítulo 2

La distancia aparente de un código cíclico.

Vamos a introducir ahora una definición que nos será útil posteriormente para calcular la cota $\Delta(C)$ de un código cíclico C.

Definición 2.0.1 *Sea $\mathbb{L}$ un cuerpo. Para cualquier elemento $g \in \mathbb{L}(n)$ definimos la distancia aparente de g, que denotamos con $d^*(g)$, como*

1. *Si $g = 0$ entonces $d^*(g) = 0$.*

2. *Si $g \neq 0$ entonces*

$$d^*(g) = máx\{n - deg(\overline{x^h g}) \mid \quad 0 \leq h \leq n-1\}.$$

Ejemplo 2.0.2 *Sea $f = 1 + x + x^4 \in \mathbb{F}_2(5)$. Tenemos que $\overline{x^0 f} = 1 + x + x^4$; $\overline{xf} = 1 + x + x^2$; $\overline{x^2 f} = x + x^2 + x^3$; $\overline{x^3 f} = x^2 + x^3 + x^4$; $\overline{x^4 f} = 1 + x^3 + x^4$. Por lo tanto $d^*(f) = 5 - deg(\overline{xf}) = 3$.*

Definición 2.0.3 *Sea un vector $a = (a_0, \ldots, a_{n-1}) \in \mathbb{L}^n$ y sea $\{i_1, \ldots, i_k\} \subseteq \mathbb{Z}_n$ una lista de enteros consecutivos módulo n. Si $a_{i_j} = 0$ para todo $j \in \{i_1, \ldots, i_k\}$, decimos que las componentes $\{a_{i_1}, \ldots, a_{i_k}\}$ forman una cadena de ceros de longitud k.*

Definición 2.0.4 *Sea $a \in \mathbb{L}^n$. Definimos la distancia aparente de a, que denotamos también con $d^*(a)$, como la longitud máxima de las cadenas de ceros módulo n en a más 1.*

Ejemplo 2.0.5 *Sea* $a = (10010001) \in \mathbb{F}_2^8$. *Tenemos que* $\{a_1, a_2\}$ *forman una cadena de ceros módulo* 8 *de longitud* 2 *y que* $\{a_4, a_5, a_6\}$ *forman una cadena de ceros módulo* 8 *de longitud* 3. *La longitud máxima de las cadenas de ceros módulo* 8 *en* a *es 3 y por lo tanto* $d^*(a) = 4$.

El siguiente lema nos proporciona una forma rápida de calcular la distancia aparente de un polinomio.

Lema 2.0.6 *Sea* $g = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q(n)$. *Si asociamos el polinomio* g *a su vector de coeficientes* $M(g) = (a_0, \ldots, a_{n-1})$ *entonces* $d^*(g) = d^*(M(g))$.

Demostración. Sea $g = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q(n)$ y sea $k \in \{0, \ldots, n-1\}$ tal que $d^*(g) = n - deg(\overline{x^k g})$. Esto implica que $deg(\overline{x^k g}) \leq deg(\overline{x^h g})\ \forall\ h,\ 1 \leq h \leq n-1$.
Sea $deg(\overline{x^k g}) = l$ y sea a_{i_0} tal que $i_0 + k \equiv 0$ módulo n. Tenemos entonces, tomando los exponentes en $\mathbb{Z}_n$,

$$\overline{x^k g} = a_{i_0} + a_{i_0+1}x + \cdots + a_0 x^k + a_1 x^{\overline{1+k}} + \cdots + a_{i_0-1} x^{\overline{i_0-1+k}}.$$

Tomando $b_0 = a_{i_0}, b_1 = a_{i_0+1}, \ldots, b_k = a_0, \ldots, b_{n-1} = a_{i_0-1}$ podemos escribir $\overline{x^k g}$ como

$$\overline{x^k g} = b_0 + b_1 x + \cdots + b_k x^k + \cdots + b_{n-1} x^{n-1}.$$

Sea ahora a_{i_1} tal que $\overline{i_1 + k} = l$. Puesto que $deg(\overline{x^k g}) = l$ tenemos que $b_l \neq 0$ y $b_i = 0,\ \forall\ i \in \{l+1, \ldots, n-1\}$. En términos de las a_i, tenemos que $a_{i_1} \neq 0$ y que $a_i = 0,\ \forall i \in \{i_1 + 1, \ldots, i_0 - 1\}$, siendo $\{i_1 + 1, \ldots, i_0 - 1\}$ una lista de enteros consecutivos módulo n. Tenemos entonces que $M(g)$ tiene una cadena de ceros consecutivos módulo n de longitud $L = n - l - 1$.

Supongamos que $M(g)$ tiene otra cadena de ceros de longitud M, con $M > L$. Sea a_j tal que $a_j \neq 0$ y $a_{\overline{j+j'}} = 0$, con $j' \in \{1, \ldots, M\}$. Tomamos ahora k' tal que $\overline{j + M + k'} = n$, esto implica que $deg(\overline{x^{k'} g}) = n - M$. De esta forma tenemos:

$$deg(\overline{x^{k'} g}) = n - M < n - L = l + 1 < l = deg(\overline{x^k g}),$$

lo que es una contradicción pues habíamos supuesto $deg(\overline{x^k g}) \leq deg(\overline{x^h g})\ \forall\ h,\ 1 \leq h \leq n-1$.

Por lo tanto la cadena módulo n de ceros más larga tiene longitud L, con $L+1 = n-l = n-deg(\overline{x^k}g) = d^*(g)$. ■

Ejemplo 2.0.7 *Siguiendo el Ejemplo 2.0.2 tenemos que* $M(f) = (11001)$ *entonces* $d^*(f) = d^*(M(f)) = 2+1 = 3$.

Obsérvese que si aplicamos el razonamiento que hemos utilizado en la demostración del lema anterior tenemos que $k = 1$ *ya que, como hemos visto en el Ejemplo 2.0.2,* $d^*(f) = 5 - deg(\overline{xf})$. *Además,* $l = 2$, $i_0 = 4$ *e* $i_1 = 2$. *Como*

$$\overline{xf} = 1 + x + x^2,$$

tenemos que $b_0 = a_4$, $b_1 = a_0$, $b_2 = a_1$, $b_3 = a_2$ *y* $b_4 = a_3$. *Así,* $b_2 \neq 0$ *y* $b_3 = b_4 = 0$ *y por lo tanto* $M(f)$ *tiene una cadena de ceros de longitud* 2.

Observación 2.0.8 *Hay que destacar que* $\left|\overline{Z(f)}\right| \geq d^*(f)$. *Esto es fácil de ver ya que* $\overline{Z(x^h f)} = \overline{Z(f)}\ \forall\ h,\ 0 \leq h \leq n-1$ *y* $\left|\overline{Z(x^h f)}\right| \geq n - deg(\overline{x^h f})$.

Sea ahora $f \in \mathbb{L}(n)$. Puesto que, como hemos dicho antes, $\overline{Z(x^h f)} = \overline{Z(f)}$, tenemos que $deg(\overline{x^h f}) \geq |D_\alpha(f)|$ para cualquier $\alpha \in U_n$. Esto implica que

$$d^*(f) \leq n - |D_\alpha(f)|\ ,\ \forall\ \alpha \in U_n. \tag{2.1}$$

Ahora, por la definición de la inversa de la transformada de Fourier discreta y lo visto en la Observación 1.0.8 tenemos que

$$w(f) = n - |D_\alpha(\varphi_{\alpha,f})|$$

Y por lo tanto,

$$d^*(\varphi_{\alpha,f}) \leq n - |D_\alpha(\varphi_{\alpha,f})| = w(f),\ \forall\ f \in \mathbb{F}_q(n)\ y\ \forall\ \alpha \in U_n. \tag{2.2}$$

Esto implica que la distancia aparente de la transformada de Fourier discreta de las palabras código distintas de cero es una cota inferior de la distancia mínima de un código cíclico. Esto nos lleva a la siguiente definición.

Definición 2.0.9 *Sea C un código cíclico en $\mathbb{F}_q(n)$ y sea $\alpha \in U_n$. La distancia aparente de C con respecto a α es*

$$d^*_\alpha(C) = \min_{c\in C,\, c\neq 0}\{d^*(\varphi_{\alpha,f})\}$$

y la distancia aparente de C es

$$d^*(C) = \max_{\alpha\in U_n}\{d^*_\alpha(C)\}.$$

También definimos el conjunto de raíces óptimas de C como:

$$R(C) = \{\beta \in U_n \mid d^*_\beta(C) = d^*(C)\}.$$

Esta definición de la distancia aparente de un código cíclico es una definición teórica y nunca la calcularemos de esta manera. Calcular la distancia aparente de esta forma sería un proceso más laborioso que calcular los pesos de todas las palabras de nuestro código, es decir, calcular la distancia mínima del código a través del método de "fuerza bruta". A lo largo del resto de esta sección veremos una serie de resultados que nos permitirán calcular la distancia aparente de un código de una forma mucho más sencilla y eficaz.

Hasta el momento hemos visto dos cotas inferiores para la distancia mínima de un código C, la máxima de las cotas BCH ($\Delta(C)$) y la distancia aparente de C ($d^*(C)$). El siguiente resultado nos muestra la relación que existe entre estas dos cotas.

Proposición 2.0.10 *En un código cíclico C se cumple la igualdad $\Delta(C) = d^*(C)$.*

Demostración. Sea $X = d^*(C)$ y $Y = \Delta(C)$. Veamos primero que $d^*(C) \leq \Delta(C)$.

Sea g el polinomio generador de C. Por el Lema 1.0.2, sabemos que $D_\alpha(g) = D_\alpha(C)$. Sea $\alpha \in U_n$.

Como $\varphi_{\alpha,g}[i] = g(\alpha^i) = \begin{cases} 0 & si \quad i \in D_\alpha(g) = D_\alpha(C) \\ & \\ \neq 0 & si \quad i \notin D_\alpha(g) = D_\alpha(C) \end{cases}$, tenemos que $D_\alpha(C)$ tiene una lista de longitud $d^*(\varphi_{\alpha,g}) - 1$ de enteros consecutivos módulo n. Sea k_α la longitud máxima de las listas de enteros

consecutivos módulo n que podemos encontrar en $D_\alpha(C)$. Entonces

$$k_\alpha + 1 \geq d^*(\varphi_{\alpha,g}) \geq d^*_\alpha(C).$$

De esta forma

$$\Delta(C) = \text{máx}_{\alpha \in U_n}\{k_\alpha + 1\} \geq \text{máx}_{\alpha \in U_n}\{d^*_\alpha(C)\} = d^*(C).$$

Veamos ahora $Y \leq X$.

Sea $\beta \in U_n$ tal que $D_\beta(C)$ tiene una lista de enteros consecutivos módulo n de longitud $Y-1$. Esto implica que $d^*(\varphi_{\beta,c}) \geq Y \ \forall c \in C$, por lo que $d^*_\beta(C) \geq Y$ y por lo tanto $Y \leq X$.

■

El valor $d^*(\varphi_{\alpha,c})$ depende del soporte de $\varphi_{\alpha,c}$; es decir, de cómo están distribuidos los ceros de c con respecto a α. Puesto que $\varphi_{\alpha,c}[i] = c(\alpha^i) = 0$ si $i \in D_\alpha(C)$, tenemos que $d^*(\varphi_{\alpha,c})$ está relacionado con el conjunto $D_\alpha(C)$. Por lo tanto, el mínimo $d^*_\alpha(C)$ depende también del conjunto $D_\alpha(C)$. Es por ello que, fijado un elmento $\alpha \in U_n$, para calcular $d^*(C)$, tenemos considerar los elementos $\beta \in U_n$ tales que $D_\alpha(C) \neq D_\beta(C)$. Como hemos visto en la Observación 1.0.6, si $\beta \in U_n$ es tal que $D_\alpha(C) \neq D_\beta(C)$ y $\{a_1, \ldots, a_h\}$ es un conjunto de representantes de las clases q-ciclotómicas módulo n entonces $\beta^{a_i q^j} = \alpha$ para algún $j \in \mathbb{Z}$ y algún a_i coprimo con n. Puesto que $D_{\beta^{q^j}}(C) = D_\beta(C)$, solo tenemos que considerar las raíces $\beta \in U_n$ tales que $\beta^{a_i} = \alpha$ para algún a_i coprimo con n. De esta forma, para cada $\alpha \in U_n$ definimos el conjunto

$$R_\alpha = \{\beta \in U_n \mid \beta^a = \alpha,\ a \in A(n)\}, \tag{2.3}$$

donde $A(n)$ es el conjunto definido en (1.1).

Por lo tanto, en la práctica, para calcular la distancia aparente de un código cíclico C en $\mathbb{F}_q(n)$ basta con fijar $\alpha \in U_n$ y calcular $d^*(C) = \text{máx}\{d^*_\beta(C) \mid \beta \in R_\alpha\}$.

Lema 2.0.11 *Sean $e, g \in C$ el idempotente generador y el polinomio generador de C, respectivamente, entonces $d^*_\beta(C) = d^*(\varphi_{\beta,e}) = d^*(\varphi_{\beta,g})\ \forall \beta \in U_n$.*

Demostración. Para cualesquiera $f, h \in \mathbb{F}_q(n)$, tenemos que $supp(\varphi_{\beta,fh}) \subseteq supp(\varphi_{\beta,f})$ ya que $\varphi_{\beta,fh} = \varphi_{\beta,f} \star \varphi_{\beta,h}$ y por lo tanto, $\forall c \in C$ y $\forall \beta \in U_n$ tenemos que $supp(\varphi_{\beta,c}) \subseteq supp(\varphi_{\beta,g}) = supp(\varphi_{\beta,e})$. Esto implica que $d^*(\varphi_{\beta,g}) = d^*(\varphi_{\beta,e}) \leq d^*(\varphi_{\beta,c})$. Así, $d^*_\beta(C) = d^*(\varphi_{\beta,e}) = d^*(\varphi_{\beta,g})$. ■

Si $\beta \in R(C)$ y $e, g \in C$ son el idempotente generador y el polinomio generador de C, respectivamente, por los resultados vistos hasta ahora obtenemos la siguiente desigualdad

$$\Delta(C) \underset{\text{Proposición 2.0.10}}{=} d^*(C) \underset{\beta \in R(C)}{=} d^*_\beta(C) \underset{\text{Lema 2.0.11}}{=} d^*(\varphi_{\beta,e}) \underset{\text{Lema 2.0.11}}{=} d^*(\varphi_{\beta,g}) \underset{(2.4)}{\leq} d(C),\ \forall \beta \in R(C). \quad (2.4)$$

Siguiendo la última desigualdad, tenemos el siguiente corolario, que nos da una condición suficiente para que la distancia mínima de un código coincida con su cota BCH (o su distancia aparente).

Corolario 2.0.12 *Sea C un código cíclico en $\mathbb{F}_q(n)$ y sean $e, g \in C$ el idempotente generador y el polinomio generador de C, respectivamente. Para $f \in \{e, g\}$ tenemos que si $d^*(\varphi_{\alpha,f}) = w(f)$ para algún $\alpha \in U_n$, entonces $d(C) = \Delta(C)$ y $\alpha \in R(C)$.*

Demostración. Por hipótesis, $d^*(\varphi_{\alpha,f}) = w(f) \geq d(C)$. Por otro lado, si tomamos $\beta \in R(C)$ tenemos que $d^*(\varphi_{\alpha,f}) \leq d^*(\varphi_{\beta,f})$ y como $f \in \{e, g\}$ utilizando (2.4) concluimos.

■

Veamos cómo estos resultados nos permiten construir códigos cíclicos y calcular su distancia aparente. En primer lugar, para cualquier código cíclico C con idempotente generador $e \in \mathbb{F}_q(n)$, $\varphi_{\alpha,e}$ es también idempotente en $(\mathbb{L}^n, \star)$; así que

$$e(\alpha^i) = \varphi_{\alpha,e}[i] = \begin{cases} 0 & si \quad i \in D_\alpha(e) \\ \\ 1 & si \quad i \notin D_\alpha(e) \end{cases}. \quad (2.5)$$

Ahora, sea $\{a_1, \ldots, a_n\}$ un conjunto completo de representantes de las clases q-ciclotómicas módulo n. Para cualquier conjunto $D =$

$\cup_{j=1}^{t} C_q(a_{i_j})$, con $i_j \in \{1, \ldots, h\}$ y $1 \leq t \leq h$, denotamos $F_D \in \mathbb{F}_q^n$ al vector tal que $F_D[i] = 0$ si $i \in D$ y 1 si $i \notin D$.

Lema 2.0.13 *Sea F_D como hemos definido en el párrafo anterior. Podemos ver F_D como la imagen por la transformada de Fourier discreta del generador idempotente de un código cíclico C en $\mathbb{F}_q(n)$ tal que $D = D_\alpha(C)$ con respecto a algún $\alpha \in U_n$. Es decir, si C es un código cíclico con conjunto definición $D_\alpha(C) = D$, para algún $\alpha \in U_n$, y e es su idempotente generador, entonces tenemos que $F_D = M(\varphi_{\alpha,e}) \in \mathbb{F}_q(n)$.*

Demostración. Como e es el idempotente generador de C, por el Lema 1.0.2 sabemos que $D_\alpha(C) = D_\alpha(e)$. Además tenemos que

$$\varphi_{\alpha,e}[i] = e(\alpha^i) = \begin{cases} 0 & si \quad i \in D_\alpha(e) \\ \\ 1 & si \quad i \notin D_\alpha(e) \end{cases},$$

que coincide con la definición de F_D y por lo tanto $F_D = M(\varphi_{\alpha,e})$.

■

Podemos utilizar este último lema para calcular $d^*(C)$. Para ello, primero consideramos el conjunto $A(n) = \{a_{i_1}, \ldots, a_{i_k}\} \subseteq \{a_1, \ldots, a_h\}$. Para cada $j = 1, \ldots, k$, sea $\beta_j \in U_n$ tal que $\beta_j^{a_{i_j}} = \alpha$. (Recuérdese que esto implica que $D_{\beta_j} = a_{i_j} \cdot D_\alpha(C)$.) La distancia aparente de $\varphi_{\beta_j,e}$ es la cadena más larga de ceros consecutivos módulo n en $F_{D_{\beta_j}(C)}$ más 1; esto implica, utilizando el Lema 2.0.11, que $d^*(C) = \max\limits_{j=1,\ldots,k} d^*(F_{D_{\beta_j}(C)})$.

Ejemplo 2.0.14 *Sea $n = 21$ y $q = 2$. Tomamos las clases 2-ciclotómicas módulo 21; a saber, $C_2(0) = \{0\}$, $C_2(1) = \{1, 2, 4, 8, 11, 16\}$, $C_2(3) = \{3, 6, 12\}$, $C_2(5) = \{5, 10, 13, 17, 19, 20\}$, $C_2(7) = \{7, 14\}$ y $C_2(9) = \{9, 15, 18\}$. Observamos que $\{0, 1, 3, 5, 7, 9\}$ es un conjunto completo de representantes de las clases 2-ciclotómicas módulo 21 y que $A(21) = \{1, 5\}$. Si tomamos $D = C_2(1) \cup C_2(3) \cup C_2(7) = \{1, 2, 3, 4, 6, 7, 8, 11, 12, 14, 16\}$, entonces*

$$F_D = (10000100011001010111).$$

Sea $C =< e >$ el código cíclico tal que $D_\alpha(C) = D$ para algún $\alpha \in U_{21}$, entonces $d^*(\varphi_{\alpha,e}) = d^*(F_D) = 5$. Para comprobar que ésta

es la distancia aparente del código C tan solo necesitamos considerar $\beta \in U_{21}$ tal que $\beta^5 = \alpha$. En ese caso, $D_\beta(C) = 5 \cdot D_\alpha(C) = C_2(5) \cup C_2(9) \cup C_2(7) = \{5, 7, 9, 10, 13, 14, 15, 17, 18, 19, 20\}$. Entonces, tenemos que

$$F_{D_\beta(C)} = (11111010100110001000 0),$$

y por lo tanto $d^*(F_{D_\beta(C)}) = 5$. De esta forma hemos visto que $d^*(C) = 5$ y que $R(C) = \{\beta, \beta^5\}$.

Capítulo 3

La distancia mínima y el máximo de las cotas BCH

Para un elemento arbitrario $g \in \mathbb{L}(n)$, el cual podemos ver como un polinomio con $deg(g) \leq n-1$, la igualdad $mcd(g, x^n - 1) = mcd(x^h g, x^n - 1)$ se cumple $\forall\ h \in \{0, \ldots, n-1\}$, ya que x^h y $x^n - 1$ son polinomios primos entre sí. Además, podemos definir

$$m_g = mcd(x^h g, x^n - 1), \tag{3.1}$$

donde, por lo anterior, m_g no depende de h. Para cualquier $h \in \{0, \ldots, n-1\}$ escribimos

$$x^h g = (x^n - 1) f_{g,h} + \overline{x^h g}, \tag{3.2}$$

donde $0 \leq deg(\overline{x^h g}) < n$.

Lema 3.0.1 *Sea $g \in \mathbb{L}(n)$ y sea m_g como hemos definido en* (3.1). *Entonces*

1. *$d^*(g) \leq n - deg(m_g)$.*
2. *Si $g \mid x^n - 1$, entonces $d^*(g) = n - deg(g)$.*

Demostración.

1. Puesto que $m_g \mid x^n - 1$ y $m_g \mid x^h g\ \forall h \in \{0, \ldots, n-1\}$, tenemos que

$$\overline{x^h g} = x^h g - (x^n - 1) f_{g,h} = m_g t\ \forall h \in \{0, \ldots, n-1\},$$

siendo t un elemento de $\mathbb{L}(n)$, es decir, $m_g \mid \overline{x^h g}$. Esto implica que $n - deg(\overline{x^h g}) \leq n - deg(m_g)\ \forall h \in \{0, \ldots, n-1\}$. Por la definición de $d^*(g)$, tenemos que $d^*(g) \leq n - deg(m_g)$.

2. $d^*(g) \geq n - deg(g)$ es trivial por la definición de distancia aparente ya que

$$d^*(g) = max\{n - deg(\overline{x^h g}),\ 0 \leq h \leq n-1\} \underset{h=0}{\geq} n - deg(g).$$

Para ver $d^*(g) \leq n - deg(g)$, basta observar que si $g \mid x^n - 1$, entonces $g = sm_g$ con $s \in \mathbb{F}_q$. Por lo tanto, aplicando (1.), $d^*(g) \leq n - deg(sm_g) = n - deg(g)$.

■

Sea c una palabra de un código cíclico C en $\mathbb{F}_q(n)$. Por la desigualdad (2.2) sabemos que $d^*(\varphi_{\alpha,c}) \leq w(c)$. Nos preguntamos bajo qué condiciones se da la igualdad. El siguiente resultado nos será de ayuda para encontrar estas condiciones.

Lema 3.0.2 *Sea C un código cíclico en $\mathbb{F}_q(n)$ y $c \in C$. Entonces $n - deg(m_{\varphi_{\alpha,c}}) = w(c)$, $\forall\ \alpha \in U_n$.*

Demostración. Tenemos que $n - deg(m_{\varphi_{\alpha,c}}) = |\{\alpha^j \mid \varphi_{\alpha,c}(\alpha^j) \neq 0\}|$. Por la Observación 1.0.8 y la desigualdad (2.1) tenemos que $w(c) = n - |D_\alpha(\varphi_{\alpha,c})| = n - n + |\{\alpha^j \mid \varphi_{\alpha,c}(\alpha^j) \neq 0\}| = n - deg(m_{\varphi_{\alpha,c}})$. ■

Observamos que por el Lema 3.0.1, para cualquier elemento $f \in \mathbb{L}(n)$ su distancia aparente es menor o igual que el "número de no ceros" de m_f. El siguiente resultado nos muestra cuándo se cumple la igualdad.

Proposición 3.0.3 *Sea $f \in \mathbb{L}(n)$ y sea m_f como hemos definido en (3.1). Tenemos que $d^*(f) = n - deg(m_f)$ si y solo si existe $h \in \{0, \ldots, n-1\}$ tal que $\overline{x^h f} \mid x^n - 1$, (equivalentemente, $\overline{x^h f}$ y m_f son polinomios asociados en $\mathbb{L}[x]$).*

Demostración.

"$\Longrightarrow$"

Por definición de $d^*(f)$, existe $h \in \{0, \ldots, n-1\}$ tal que $d^*(f) = n -$

$deg(\overline{x^h f})$. Puesto que $d^*(f) = n - deg(m_f)$, tenemos que $deg(\overline{x^h f}) = deg(m_f)$. Por (3.2) tenemos que si α pertenece al conjunto de ceros de m_f, entonces α también pertenece al conjunto de ceros de $\overline{x^h f}$. Como $deg(\overline{x^h f}) = deg(m_f)$ tenemos que m_f y $\overline{x^h f}$ tienen exactamente el mismo conjunto de ceros y por lo tanto son polinomios asociados.

"$\Longleftarrow$"

Sea $h \in \{0, \ldots, n-1\}$ tal que $\overline{x^h f} \mid x^n - 1$. Por (3.2), tenemos que $\overline{x^h f} \mid x^h f$. Puesto que además sabemos que $\overline{x^h f} \mid x^n - 1$, tenemos que $\overline{x^h f} \mid m_f$. Por otro lado, por (3.1), tenemos que $m_f \mid \overline{x^h f}$. Esto implica que m_f y $\overline{x^h f}$ son asociados y por lo tanto $deg(\overline{x^h f}) = deg(m_f)$. Por la definición de distancia aparente y por el Lema 3.0.1 (2.), tenemos que $d^*(f) = d^*(\overline{x^h f}) = n - deg(\overline{x^h f}) = n - deg(m_f)$.

■

Utilizando el Lema 3.0.2 y la Proposición 3.0.3 obtenemos las condiciones bajo las cuales se da la igualdad $d^*(\varphi_{\alpha,c}) = w(c)$. Este resultado nos es de gran utilidad para caracterizar los códigos cíclicos que cumplen la igualdad $d(C) = \Delta(C)(= d^*(C))$.

Teorema 3.0.4 *Sea n un entero positivo, p un número primo y q una potencia de p. Supongamos que $mcd(n, q) = 1$. Sea el cuerpo $\mathbb{F}_q$ y $\mathbb{L} \mid \mathbb{F}_q$ una extensión tal que $U_n \subseteq \mathbb{L}$. Sea C un código cíclico en $\mathbb{F}_q(n)$. Entonces $d(C) = \Delta(C)(= d^*(C))$ si y solo si existe un polinomio $f \in \mathbb{L}(n)$ tal que*

1. $d^*(f) = d^*(C)$.
2. $d^*(f) = n - deg(m_f)$.
3. $\varphi^{-1}_{\alpha,f} \in C$, *para algún* $\alpha \in R(C)$.

Mas aún, en este caso, existe $h \in \{0, \ldots, n-1\}$ tal que $\overline{x^h f} \mid x^n - 1$.

Demostración.

"$\Longrightarrow$"

Sea $c \in C$ tal que $w(c) = d(C)$ y sea $\alpha \in R(C)$. Tomamos $m_{\varphi_{\alpha,c}} = mcd(\varphi_{\alpha,c}, x^n - 1)$. Por la definición de distancia aparente y aplicando

resultados previos tenemos que

$$w(c) \underset{(2.2)}{\geq} d^*(\varphi_{\alpha,c}) \geq d^*_\alpha(C) \underset{\alpha \in R(C)}{=} d^*(C) = d(C) = w(c) \underset{\text{Lema 3.0.2}}{=} n - deg(m_{\varphi_{\alpha,c}}).$$

Tomando $f = \varphi_{\alpha,c}$ se cumplen las tres condiciones requeridas.
"$\Longleftarrow$"
Supongamos que existe $f \in \mathbb{L}(n)$ que cumple las condiciones $(1-3)$.
Por el Lema 3.0.2 y la condición (2.) tenemos que

$$w(\varphi^{-1}_{\alpha,f}) = n - deg(m_{\varphi_{\alpha,\varphi^{-1}_{\alpha,f}}}) = n - deg(m_f) = d^*(f).$$

Por la condición (3.) tenemos que $\varphi^{-1}_{\alpha,f} \in C$ lo que implica que $w(\varphi^{-1}_{\alpha,f}) = d^*(f) \geq d(C)$. Ahora por la condición (1.) tenemos que $d^*(C) \geq d(C)$ y por (2.4) concluimos que $d^*(C) = d(C)$. La última afirmación del teorema es directa al utilizar la Proposición 3.0.3. ■

Obsérvese que este resultado es teórico, ya que es imposible de llevar a la práctica. Sin embargo, este resultado nos servirá para obtener condiciones necesarias y suficientes más fáciles de comprobar para que en un código cíclico su distancia mínima coincida con el máximo de sus cotas BCH.

Para comprobar si se cumplen las condiciones de este teorema, por la Proposición 3.0.3, tenemos que comprobar si los divisores de $x^n - 1$ cumplen ciertas propiedades. El siguiente resultado nos ofrece condiciones sobre los divisores más simples de comprobar para que se de la igualdad $d(C) = \Delta(C)$.

Corolario 3.0.5 *Sea C un código cíclico en $\mathbb{F}_q(n)$. Entonces $d(C) = \Delta(C)$ si y solo si existe $k \in \{0, \ldots, n-1\}$ y un divisor $g \mid x^n - 1$ en $\mathbb{L}[x]$ tal que $f = \overline{x^k g}$ cumple las siguientes condiciones*

1. *$d^*(f) = d^*(C)$.*
2. *$\varphi^{-1}_{\alpha,f} \in C$, para algún $\alpha \in R(C)$.*

Demostración. Sea $h = n - k$,entones $g = \overline{x^h f}$.
"$\Longrightarrow$"

Por el Teorema 3.0.4, condiciones (1.) y (3.), existe $f \in \mathbb{L}(n)$ tal que $d^*(f) = d^*(C)$ y $\varphi_{\alpha,f}^{-1} \in C$. Además, por la condición (2.), tenemos que $d^*(f) = n - deg(m_f)$ y, por la Proposición 3.0.3, esto implica que existe un $h \in \{0, \ldots, n-1\}$ tal que $\overline{x^h f} \mid x^n - 1$. Si tomamos $g = \overline{x^h f}$ hemos terminado.

"$\Longleftarrow$"

Queremos ver que se cumplen las tres condiciones del Teorema 3.0.4. Por hipótesis tenemos que se cumplen (1.) y (3.). Veamos (2.). Puesto que $g = \overline{x^h f} \mid x^n - 1$, por la Proposición 3.0.3 tenemos que

$$d^*(f) = d^*(\overline{x^h f}) = n - deg(m_{\overline{x^h f}}) = n - deg(m_f).$$

■

Nótese que, como mostramos en el siguiente ejemplo, en las condiciones del corolario anterior, puede que existan $\alpha, \beta \in U_n$ tales que $\varphi_{\alpha,f}^{-1} \in C$ pero $\varphi_{\beta,f}^{-1} \notin C$.

Ejemplo 3.0.6 *Sea $q = 2$ y $n = 15$. Sea $\alpha \in U_{15}$, cuyo polinomio mínimo es $m_\alpha = x^4 + x + 1$, y sea $\beta = \alpha^7 \in U_{15}$, cuyo polinomio mínimo es $m_\beta = x^4 + x^3 + 1$. Además, tenemos que $D_\alpha(m_\alpha) = C_2(1) = \{1, 2, 4, 8\}$. Puesto que*

$$\alpha^7 = \beta \Rightarrow \beta^2 = \alpha^{14} = \alpha^{-1} \Rightarrow \beta^{-2} = \alpha \Rightarrow \alpha = \beta^{17},$$

tenemos que $D_\beta(m_\alpha) = C_2(7)$. Por otro lado, por el punto (1.) de la Observación 1.0.8, $supp(\varphi_{\alpha,m_\alpha}) = \mathbb{Z}_{15} \setminus C_2(1)$ y $supp(\varphi_{\beta,m_\alpha}) = \mathbb{Z}_{15} \setminus C_2(7)$.

Sea $f = \varphi_{\alpha,m_\alpha}$, por la inversa de la transformada de Fourier discreta sabemos que $\varphi_{\alpha,f}^{-1} = m_\alpha$. Sea $g = \varphi_{\beta,f}^{-1}$. Veamos que $m_\alpha \neq g$. Para ello, por reducción al absurdo, supongamos que $m_\alpha = g$. Puesto que la transformada de Fourier discreta es un isomorfismo tenemos que

$$\varphi_{\beta,m_\alpha} = \varphi_{\beta,g} = f = \varphi_{\alpha,m_\alpha},$$

que es una contradicción, pues habíamos visto que $supp(\varphi_{\alpha,m_\alpha}) = \mathbb{Z}_{15} \setminus C_2(1) \neq \mathbb{Z}_{15} \setminus C_2(7) = supp(\varphi_{\beta,m_\alpha})$. Es decir, hemos encontrado un polinomio f con $\varphi_{\alpha,f}^{-1} \neq \varphi_{\beta,f}^{-1}$. Esto implica que $< \varphi_{\alpha,f}^{-1} > \neq < \varphi_{\beta,f}^{-1} >$ y por lo tanto si tomamos $C =< \varphi_{\alpha,f}^{-1} >$, $\varphi_{\alpha,f}^{-1} \in C$ pero $\varphi_{\beta,f}^{-1} \notin C$.

Podemos reescribir la condición (2.) del Corolario 3.0.5 de la siguiente forma.

Corolario 3.0.7 *Sea C un código cíclico en $\mathbb{F}_q(n)$. Entonces $d(C) = \Delta(C)$ si y solo si existe $k \in \{0, \ldots, n-1\}$ y un divisor $g \mid x^n - 1$ en $\mathbb{L}[x]$ tal que, si tomamos $f = \overline{x^k g}$, se cumplen las siguientes condiciones:*

1. $d^*(f) = d^*(C)$.
2. $supp(f) \subseteq \mathbb{Z}_n \setminus D_\alpha(C)$, *para algún* $\alpha \in R(C)$.
3. $(f(\alpha^j))^q = f(\alpha^j)$ *para cualquier* $j \in \{0, \ldots, n-1\}$.

Demostración.
"$\Longrightarrow$"
Basta ver que la condición (2.) del Corolario 3.0.5 implica las condiciones (2.) y (3.).
$\varphi_{\alpha,f}^{-1} \in C$ implica que $\varphi_{\alpha,f}^{-1} \in \mathbb{F}(n)$ y por la Observación 1.0.8 (4.) $(f(\alpha^j))^q = f(\alpha^j)$ para cualquier $j \in \{0, \ldots, n-1\}$..
Para ver (2.) utilizamos el punto 4 de la Observación 1.0.8 y que $\varphi_{\alpha,f}^{-1} \in C$.

$$supp(f) = supp(\varphi_{\alpha,\varphi_{\alpha,f}^{-1}}) = \{i \in \{0, \ldots, n-1\} \mid \varphi_{\alpha,f}^{-1}(\alpha^i) \neq 0\} = \mathbb{Z}_n \setminus \{i \in \{0, \ldots, n-1\} \mid \varphi_{\alpha,f}^{-1}(\alpha^i) = 0\} \subseteq \mathbb{Z}_n \setminus D_\alpha(C).$$

"$\Longleftarrow$"
Puesto que $(f(\alpha^j))^q = f(\alpha^j)$ para cualquier $j \in \{0, \ldots, n-1\}$, tenemos que $\varphi_{\alpha,f}^{-1} \in \mathbb{F}_q(n)$. Veamos que $\varphi_{\alpha,f}^{-1} \in C$.

$$supp(f) = \mathbb{Z}_n \setminus \{i \in \{0, \ldots, n-1\} \mid \varphi_{\alpha,f}^{-1}(\alpha^i) = 0\} \subseteq \mathbb{Z}_n \setminus D_\alpha(C),$$

lo que implica que $D_\alpha(C) \subseteq \{i \in \{0, \ldots, n-1\} \mid \varphi_{\alpha,f}^{-1}(\alpha^i) = 0\}$, de esta forma $\varphi_{\alpha,f}^{-1}(\alpha^i) = 0$, $\forall i \in D_\alpha(C)$ por lo que $\varphi_{\alpha,f}^{-1} \in C$. ■

En el siguiente resultado vemos que comprobar la condición (3.) del corolario anterior es muy simple si estamos en el caso $q = 2$.

Lema 3.0.8 *Sea* $\mathbb{F}_2$ *y* $f \in \mathbb{F}_2[x]$. *Si* $supp(f)$ *es unión de clases 2-ciclotómicas entonces* $(f(\alpha^j))^2 = f(\alpha^j)$, $\forall j \in \{0, \ldots, n-1\}$ *y* $\forall\, \alpha \in U_n$.

Demostración. Podemos escribir f como $f = \sum_{i \in supp(f)} x^i$. Sea $\alpha \in U_n$ y $j \in \{0, \ldots, n-1\}$,

$$(f(\alpha^j))^2 = \left(\sum_{i \in supp(f)} (\alpha^j)^i \right)^2 = \sum_{i \in supp(f)} (\alpha^{2j})^i$$
$$= \underset{\substack{supp(f) \text{ es unión} \\ \text{de clases 2-ciclotómicas}}}{=} \sum_{i \in supp(f)} (\alpha^j)^i = f(\alpha^j)$$

Es decir $(f(\alpha^j))^2 = f(\alpha^j)$, $\forall j \in \{0, \ldots, n-1\}$ y $\forall\, \alpha \in U_n$. ■

El siguiente resultado es una generalización para un q cualquiera del lema anterior.

Lema 3.0.9 *Sea* $f \in \mathbb{L}(n)$. *Si* $\varphi_{\alpha,f}^{-1} \in \mathbb{F}_q(n)$ *para cualquier* $\alpha \in U_n$ *entonces* $supp(f)$ *es unión de clases q-ciclotómicas. Si* f *es idempotente en* $(\mathbb{L}^n, \star)$ *el recíproco también es cierto, es decir, si* $supp(f)$ *es unión de clases q-ciclotómicas entonces* $\varphi_{\alpha,f}^{-1} \in \mathbb{F}_q(n)$.

Demostración. Sea $f \in \mathbb{L}(n)$ tal que $\varphi_{\alpha,f}^{-1} \in \mathbb{F}_q(n)$. Por el punto (2.) de la Observación 1.0.8, sabemos que $supp(\varphi_{\alpha,\varphi_{\alpha,f}^{-1}}) = \mathbb{Z}_n \setminus D_\alpha(\varphi_{\alpha,f}^{-1})$. Por lo tanto $supp(f)$ es unión de clases q-ciclotómicas.

Veamos ahora la otra implicación. Supongamos que $f \in (\mathbb{L}^n, \star)$ es idempotente. Sea C el código con conjunto definición $D_\alpha(C) = \mathbb{Z}_n \setminus supp(f)$. Sea e el generador idempotente de C, por el Lema 1.0.2 tenemos que $D_\alpha(e) = \mathbb{Z}_n \setminus supp(f)$. Puesto que e es idempotente en $\mathbb{F}_q(n)$ y la transformada de Fourier discreta es un isomorfismo, $\varphi_{\alpha,e}$ es idempotente en $(\mathbb{L}^n, \star)$. Como $supp(\varphi_{\alpha,e}) = supp(f)$ y ambos son idempotentes tenemos que $\varphi_{\alpha,e} = f$ y por lo tanto $\varphi_{\alpha,f}^{-1} \in \mathbb{F}_q(n)$. ■

El siguiente corolario nos proporciona otra condición suficiente para determinar los códigos cíclicos cuya distancia aparente coincide con su distancia mínima.

Corolario 3.0.10 *Sea C un código cíclico en $\mathbb{F}_q(n)$ con un idempotente generador $e \in C$. Si existe $h \in \{0, \ldots, n-1\}$ y $\alpha \in U_n$ tal que $\overline{x^h \varphi_{\alpha,e}} \mid x^n - 1$ entonces $d(C) = \Delta(C)$ y $\alpha \in R(C)$.*

Demostración. Puesto que $\overline{x^h \varphi_{\alpha,e}} \mid x^n - 1$, por la Proposición 3.0.3, tenemos que $d^*(\varphi_{\alpha,e}) = n - deg(m_{\varphi_{\alpha,e}})$ y por el Lema 3.0.2 tenemos que $n - deg(m_{\varphi_{\alpha,e}}) = w(e)$. Por lo tanto $d^*(\varphi_{\alpha,e}) = w(e)$ y aplicando el Corolario 2.0.12 concluimos la demostración. ■

Los resultados previos nos muestran algunas condiciones que puede cumplir un código cíclico C para que se satisfaga la igualdad $d(C) = \Delta(C)$. El siguiente corolario nos ofrece un método para construir códigos cíclicos que tengan esta propiedad.

Corolario 3.0.11 *Sea un cuerpo intermedio $\mathbb{F}_q \subseteq \mathbb{K} \subseteq \mathbb{L}$ y sea $g \in \mathbb{K}[x]$ un divisor de $x^n - 1$ y $\beta \in U_n$. Si $\varphi^{-1}_{\beta,\overline{x^k g}} \in \mathbb{F}_q(n)$, para algún $k \in \{0, \ldots, n-1\}$, entonces la familia de códigos cíclicos permutación equivalentes $\{C_\alpha = (\varphi^{-1}_{\alpha,\overline{x^k g}}) \mid \alpha \in U_n\}$ satisface $d(C_\alpha) = \Delta(C_\alpha)$ para todo $\alpha \in U_n$. Mas aún, $dim_{\mathbb{F}_q}(C_\alpha) = |supp(g)|$, para todo $\alpha \in U_n$.*

Demostración. Sea $f = \overline{x^k g}$ y sea $e \in \mathbb{F}_q(n)$ el idempotente generador del código $C = (\varphi^{-1}_{\alpha,f})$ en $\mathbb{F}_q(n)$.

Puesto que e es idempotente, $\varphi_{\alpha,e}[i] = e(\alpha^i) = \begin{cases} 0 & si \quad i \in D_\alpha(c) \\ \\ 1 & si \quad i \notin D_\alpha(c) \end{cases}$,

y por tanto $supp(\varphi_{\alpha,e}) = \mathbb{Z}_n \setminus D_\alpha(C)$. Además, por la Observación 1.0.8 (1.), tenemos que

$$\mathbb{Z}_n \setminus supp(f) = \mathbb{Z}_n \setminus supp(\varphi_{\alpha,\varphi^{-1}_{\alpha,f}}) = D_\alpha(\varphi^{-1}_{\alpha,f}) = D_\alpha(C),$$

por lo que $supp(f) = \mathbb{Z}_n \setminus D_\alpha(C)$. Es decir, $supp(f) = supp(\varphi_{\alpha,e})$ lo que implica que $d^*(f) = d^*(\varphi_{\alpha,e})$. Ahora, si tomamos $h = n - k$, tenemos que $\overline{x^h f} = g \mid x^n - 1$, y por la Proposición 3.0.3 tenemos que

$$d^*(f) \underset{\text{Proposición 3.0.3}}{=} n - deg(m_f) \underset{\text{Lema 3.0.2}}{=} w(\varphi^{-1}_{\alpha,f}) \geq d(C).$$

Por otro lado, por (2.4), tenemos que $d^*(f) = d^*(\varphi_{\alpha,e}) \underset{\text{Lema 2.0.11}}{=}$

$d^*_\alpha(C) \leq d^*(C) \leq d(C)$, por lo que hemos terminado. ■

Utilizando este último corolario, si queremos construir un código cíclico C con $d(C) = \Delta(C)$ tenemos que encontrar un divisor g de $x^n - 1$ y un elemento $k \in \mathbb{Z}_n$ tales que, si tomamos $f = \overline{x^k g}$, $\varphi^{-1}_{\alpha,f} \in \mathbb{F}_q(n)$ para algún $\alpha \in U_n$ o, equivalentemente, utilizando el punto (3.) de la Observación 1.0.8, $(f(\alpha^j))^q = f(\alpha^j)$, $\forall j \in \{0, \ldots, n-1\}$ y para algún $\alpha \in U_n$. Veamos esto con un ejemplo.

Ejemplo 3.0.12 *Sea $q = 2$, $n = 45$. Tenemos que $A(45) = \{1, 7\}$. Sea $g = x^{40}+x^{39}+x^{38}+x^{36}+x^{35}+x^{32}+x^{30}+x^{25}+x^{24}+x^{23}+x^{21}+x^{20}+x^{17}+x^{15}+x^{10}+x^9+x^8+x^6+x^5+x^2+1$. Se puede comprobar que $g \mid x^{45} - 1$ en $\mathbb{F}_2[x]$ (por lo que $\mathbb{F} = \mathbb{K}$). Necesitamos encontrar un $k \in \{0, \ldots, 44\}$ tal que, al tomar $f = \overline{x^k g}$, $(f(\alpha^j))^2 = f(\alpha^j)$, $\forall j \in \{0, \ldots, 44\}$ y para algún $\alpha \in U_{45}$. Puesto que nos encontramos en el caso $q = 2$ podemos utilizar el Lema 3.0.8 y comprobar si $supp(f)$ es unión de clases 2-ciclotómicas. Sin embargo, en este ejemplo vamos a comprobar directamente la propiedad $(f(\alpha^j))^2 = f(\alpha^j)$. Para ello fijamos $\beta \in U_{45}$ tal que $min_\beta = x^{12} + x^3 + 1$. Se puede comprobar que $D_\beta(g) = \mathbb{Z}_{45} \setminus (C_2(0) \cup C_2(3))$, siendo $C_2(3) = \{3, 6, 12, 24\}$. Puesto que $g(1) = 1$ y $g(\beta) = \beta^{30}$, veamos que $f = \overline{x^5 g}$ cumple la propiedad. Por un lado tenemos que $f(\beta^j) = 0, \forall\ j \in D_\beta(C)$ por la definición de conjunto definición. Por otro lado $f(1) = 1$ y $f(\beta^3) = \overline{(\beta^3)^5 \beta^{30}} = \overline{\beta^{45}} = 1$ por lo que $f(\beta^6) = f(\beta^{12}) = f(\beta^{24}) = 1$. Por lo tanto tenemos que $f(\beta^j) = 0$ si $j \in D_\beta(C)$ y $f(\beta^j) = 1$ si $j \in C_2(0) \cup C_2(3)$, lo que implica que $(f(\beta^j))^2 = f(\beta^j)$, $\forall j \in \{0, \ldots, 44\}$ y, utilizando los puntos (3.) y (4.) de la Observación 1.0.8, $\varphi^{-1}_{\alpha,f} \in \mathbb{F}_2(45)$, $\forall \alpha \in U_{45}$.*

Sea $C =< \varphi^{-1}_{\beta,f} >$. Utilizando el punto (1.) de la Observación 1.0.8, $D_\beta(C) = D_\beta(\varphi^{-1}_{\beta,f}) = \mathbb{Z}_{45} \setminus supp(f) = C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21)$. Analizando

$$\begin{aligned} M(f) = F_{D_\beta(C)} \quad = \quad & (1,0,0,0,0,1,0,1,0,0,1,1,0,1,1, \\ & 1,0,0,0,0,1,0,1,0,0,1,1,0,1,1, \\ & 1,0,0,0,0,1,0,1,0,0,1,1,0,1,1) \end{aligned}$$

como en el Ejemplo 2.0.14 y utilizando el último corolario, tenemos

que $\Delta(C) = d(C) = 5$ *y* $dim(C) = 21$.

Capítulo 4

La distancia aparente en códigos abelianos de dos variables

4.1. Notación

El lector notará que la notación que usaremos en este caso es una extensión natural a dos variables de la notación que hemos utilizado en la sección anterior para códigos de una variable.

Al igual que antes, $\mathbb{F}_q$ es el cuerpo de q elementos, donde q es potencia de un primo p. Sean $r_x, r_y \in \mathbb{N}$. Sea $T \subseteq \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, denotamos con $\pi_x(T)$ a la proyección de T en $\mathbb{Z}_{r_x}$ y con $\pi_x(T)$ a la proyección de T en $\mathbb{Z}_{r_y}$.

Un código abeliano es un ideal en el álgebra

$$\mathbb{F}_q(r_x, r_y) = \mathbb{F}_q[x, y]/ < x^{r_x} - 1, y^{r_y} - 1 > .$$

Identificamos las palabras código con polinomios en dos variables $f(x, y)$, para los cuales cada monomio satisface que el grado de la indeterminada x pertenece a $\mathbb{Z}_{r_x}$ y el grado de la indeterminada y pertenece a $\mathbb{Z}_{r_y}$. Un polinomio $f \in \mathbb{F}_q(r_x, r_y)$ lo expresamos de la forma

$$f = f(x, y) = \sum_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} a_{(i,j)} Z^{(i,j)}, \text{ donde } Z^{(i,j)} = x^i y^j.$$

Dado un polinomio $f \in \mathbb{F}_q(r_x, r_y)$ denotamos por $\overline{f}$ a la proyección canónica de f en $\mathbb{F}_q(r_x, r_y)$. Suponemos siempre que estamos en el caso semisimple, es decir, $mcd(r_x, q) = mcd(r_y, q) = 1$.

Recordemos que, para cada $s \in \mathbb{N}$ denotamos con R_s a las raíces s-ésimas de la unidad y con U_s a las raíces s-ésimas primitivas de la unidad. Para r_x, r_y, a su vez, definimos los conjuntos $R = \{\alpha = (\alpha_x, \alpha_y) \mid \alpha_x \in R_{r_x}, \alpha_y \in R_{r_y}\}$ y $U = \{\alpha = (\alpha_x, \alpha_y) \mid \alpha_x \in U_{r_x}, \alpha_y \in U_{r_y}\}$. Sea $\mathbb{L} \mid \mathbb{F}_q$ una extensión de cuerpos tal que U_{r_x} y U_{r_y} están contenidos en $\mathbb{L}$. Para un código cíclico C en $\mathbb{F}_q(r_x, r_y)$ definimos el conjunto de ceros como $Z(C) = \{\alpha \in U \mid f(\alpha) = 0 \ \forall f \in C \text{ y } \alpha^{(r_x, r_y)} = 1\}$. Fijado $\alpha = (\alpha_x, \alpha_y) \in U$, el conjunto de definición con respecto de α está definido como $D_\alpha(C) = \{(a_x, a_y) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y} \mid f(\alpha_x^{a_x}, \alpha_y^{a_y}) = 0 \ \forall f \in C\}$. Nótese que si $(i, j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, $f(\alpha^{(i,j)}) = \sum_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} a_{(i,j)} \alpha_x^i \alpha_y^j$.

Dado un elemento $a = (a_x, a_y) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, definimos su q^t-órbita módulo(r_x, r_y) como $Q_{q^t}(a) = \{(a_x \cdot q^{ti}, a_y \cdot q^{ti}) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y} \mid i \in \mathbb{N}\}$. Obsérvese que la definición de q^t-órbita es la extensión a dos variables de la definición de clase q^t-ciclotómica. Sabemos que para todo polinomio $f \in \mathbb{F}_q[x, y]$ y para todo elemento $(a_x, a_y) \in \mathbb{L}$, tenemos que si $f(a_x, a_y) = 0$ entonces $f(a_x^q, a_y^q) = 0$. Esto implica que, al igual que en el caso de una variable donde los conjuntos definición son unión de clases q^t-ciclotómicas, en dos variables los conjuntos definición son unión de q^t-órbitas.

Sea ahora una matriz $M = (a_{ij})_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}}$, con $a_{ij} \in R$, siendo R un determinado conjunto. Para $b \in \mathbb{Z}_{r_x}$, denotamos por $f_M(b) = \{a_{(b,j)} \mid j \in \mathbb{Z}_{r_y}\}$ a la fila b-ésima de M y para $b \in \mathbb{Z}_{r_y}$ por $c_M(b) = \{a_{(i,b)} \mid i \in \mathbb{Z}_{r_x}\}$ a la columna b-ésima de M.

Sea $D \subseteq \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$. La matriz dada por D está definida como

$$M = (a_{ij})_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}}, \text{ con } a_{ij} = \begin{cases} 0 & si \quad (i,j) \in D \\ \\ 1 & si \quad (i,j) \notin D \end{cases}.$$

Si D es unión de q^t-órbitas, decimos que M es una matriz de q^t-órbitas y la denotamos como $M = M(D)$.

Observación 4.1.1 *Sea $b \in \mathbb{Z}_{r_x}$ y sea D unión de q^t-órbitas, con*

$D \subset \{b\} \times \mathbb{Z}_{r_y}$. Sea $M = M(D)$. Decimos que el vector $A = f_M(b)$ es un vector de q^t-órbitas. Análogamente, Sea $b' \in \mathbb{Z}_{r_y}$ y sea D unión de q^t-órbitas, con $D \subset \mathbb{Z}_{r_y} \times \{b'\}$. Sea $M = M(D)$. Decimos que el vector $A = c_M(b')$ es un vector de q^t-órbitas

Ejemplo 4.1.2 *Sea $q = 2, r_x = 5, r_y = 7$. El conjunto de 2-órbitas módulo $(5, 7)$ es el siguiente*

$$\begin{aligned}
Q_2((0,0)) &= \{(0,0)\},\\
Q_2((0,1)) &= \{(0,1),(0,2),(0,4)\},\\
Q_2((0,3)) &= \{(0,3),(0,5),(0,6)\},\\
Q_2((1,0)) &= \{(1,0),(2,0),(3,0),(4,0)\},\\
Q_2((1,1)) &= \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(3,1),(3,2),\\
&\quad (3,4),(4,1),(4,2),(4,4)\},\\
Q_2((1,3)) &= \{(1,3),(1,5),(1,6),(2,3),(2,5),(2,6),(3,3),(3,5),\\
&\quad (3,6),(4,3),(4,5),(4,6)\}.
\end{aligned}$$

Si tomamos $D = Q_2((0,0)) \cup Q_2((0,1)) \cup Q_2((1,3))$ entonces la matriz dada por D es

$$M(D) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1\\ 1 & 1 & 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 1 & 0 & 1 & 0 & 0\\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Para cualquier matriz M, definimos el soporte de M como $supp(M) = \{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y} \mid a_{ij} \neq 0\}$. Denotamos $D(M)$ a su complemento, es decir, $D(M) = \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y} \setminus supp(M)$. Destacar que si M es una matriz de q^t-órbitas definida por D entonces $D(M(D)) = D$.

Sea L_t un conjunto de q^t-órbitas en $\mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, para algún $t \in \mathbb{N}$. Definimos el siguiente orden parcial en el conjunto de todas las matrices de q^t-órbitas $\{M(D) \mid D = \cup Q, \text{ para algunos } Q \in L_t\}$

$$M(D) \leq M(D') \Leftrightarrow supp(M(D)) \subseteq supp(M(D')). \tag{4.1}$$

Claramente, esta condición es equivalente a $D' \subseteq D$.

Sea $\mathbb{L} \mid \mathbb{F}_q$ una extensión de cuerpos tal que $U \subset \mathbb{L}^2$. Al igual que en el caso de una variable, definimos la transformada de Fourier

discreta de $f \in \mathbb{F}_q(r_x, r_y)$ con respecto a $\alpha \in U$ como el polinomio

$$\varphi_{\alpha,f}(Z) = \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} f(\alpha^{(i,j)})Z^{(i,j)} \in \mathbb{L}(r_x, r_y).$$

La inversa de la transformada de Fourier discreta es

$$\varphi^{-1}_{\alpha,f}(Z) = \frac{1}{r_x \cdot r_y} \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} f(\alpha^{-(i,j)})Z^{(i,j)} \in \mathbb{L}(r_x, r_y).$$

También como en el caso de una variable, podemos ver la transformada de Fourirer discreta como un isomorfismo de álgebras

$$\varphi_\alpha : \mathbb{L}(r_x, r_y) \longrightarrow (\mathbb{L}^{|\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}|}, \star),$$

donde $\star$ es la multiplicación coordenada a coordenada.

Observación 4.1.3 *Como* $f = \varphi^{-1}_{\alpha,\varphi_{\alpha,f}}$, *tenemos que* $supp(f) = \{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y} \mid \varphi_{\alpha,f}(\alpha^{-(i,j)}) \neq 0\}$. *Esto implica que* $w(f) = \left|\overline{Z(\varphi_{\alpha,f})}\right|$.

4.2. La distancia aparente fuerte

Vamos a introducir ahora el concepto de distancia aparente fuerte para polinomios en dos variables y para matrices. Al igual que con la distancia aparente en códigos de una variable, la distancia aparente fuerte nos servirá para calcular una cota inferior para la distancia mínima de un código abeliano.

Todos los conceptos que vamos a ver a lo largo de este capítulo tienen una versión para varias variables, pero, puesto que los resultados de caracterización de códigos abelianos en los que su distancia aparente fuerte coincide con su distancia mínima y los resultados que nos permiten construir códigos con esta propiedad solo se conocen para dos variables, en este trabajo solo desarrollamos la versión para dos variables.

La distancia aparente fuerte de un polinomio

Sea $f = \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} a_{(i,j)}Z^{(i,j)}$ un polinomio en $\mathbb{L}(r_x, r_y)$. Podemos ver f como un polinomio en $(\mathbb{L}[y])[x]$. Basta con escribir f

como $f = f_x = \sum_{b=0}^{r_x-1} f_{x,b}x^b$, con $f_{x,b} = \sum_{j\in\mathbb{Z}_{r_y}} a_{(b,j)}y^j$. Análogamente, también lo podemos ver como un polinomio en $(\mathbb{L}[x])[y]$. En este caso escribimos f como $f = f_y = \sum_{b=0}^{r_y-1} f_{y,b}y^b$, con $f_{y,b} = \sum_{i\in\mathbb{Z}_{r_x}} a_{(i,b)}y^i$.

Definimos el grado x como $deg(f_x)$ y el grado y como $deg(f_y)$. Para cualquier $h = (h_x, h_y) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, definimos $d_x[h] = d_x[h](f)$ como el grado x de $\overline{Z^h f}$ y $c_x[h] = c_x[h](f)$ al coeficiente de $x_k^{d_k[h]}$ (nótese que $c_x[h]$ es un polinomio en la indeterminada y). Las definiciones de $d_y[h]$ y de $c_y[h]$ son análogas.

Definición 4.2.1 *Sea $f \in \mathbb{L}(r_x, r_y)$. La distancia aparente de f; denotada, al igual que el el caso de una variable, con $d^*(f)$, es*

1. *Si $f = 0$, entonces $d^*(f) = 0$.*
2. *Si $f \neq 0$,*

$$d^*(f) = \max\{\max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{d^*(c_x[h])(r_x - d_x[h])\}, \max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{d^*(c_y[h])(r_y - d_y[h])\}\}$$

Ejemplo 4.2.2 *Sea $q = 2, r_x = 15$ y $r_y = 3$. Sea $f = y + x^{10}y + x^{11}y + x^{13}y^2 + x^{14}y + y^2 + x^5y^2 + x^7y^2$. Tenemos que*

- $f_x = (y+y^2)+(y^2)x^5+(y^2)x^7+(y)x^{10}+(y)x^{11}+(y^2)x^{13}+(y)x^{14}$.
- $f_y = (1 + x^{10} + x^{11} + x^{14})y + (1 + x^5 + x^7 + x^{13})y^2$.

El máximo para la variable x se alcanza en $d_x[(10, 2)] = 10$, con $c_x[(10, 2)] = 1+y$, $d^*(c_x[(10, 2)]) = 2$. Para la variable y el máximo se alcanza en $d_y[(0, 2)] = 1$, con $c_y[(0, 1)] = 1 + x^5 + x^7 + x^{13}$, $d^*(c_y[(0, 2)]) = 6$. Por lo que $d^*(f) = \max\{(15-10)\cdot 2, (3-1)\cdot 6\} = 12$.

Más adelante, se podrá observar que la distancia aparente es una cota inferior para el número de no-ceros de un polinomio. Para obtener una mejor cota modificamos la definición de distancia aparente, obteniendo la definición de distancia aparente fuerte.

Definición 4.2.3 *Sea $f \in \mathbb{L}(r_x, r_y)$. Sea $b \in \mathbb{Z}_{r_x}$, el conjunto de coeficientes cero x asociados a b es el conjunto de coeficientes (que son polinomios en $\mathbb{L}[y]$)*

$$ZC_f(k, b) = \{f_{k,b_0}, \ldots, f_{k,b_l}\}, \text{ con } b = b_0$$

tal que $f_{k,b_j} = 0 \; \forall j \in \{0, \ldots, l\}$ siendo $b_0, \ldots, b_l$ una lista de enteros consecutivos módulo r_x y $f_{k,b_l^+} \neq 0$, con $b_l^+ = \overline{b_l + 1}$. Denotamos por $w_f(x, b)$ a $|ZC_f(x, b)|$

El conjunto de coeficientes cero y asociados a b tiene una definición análoga.

Definición 4.2.4 *Sea $f \in \mathbb{L}(r_x, r_y)$. La distancia aparente fuerte de f, denotada por $sd^*(f)$, esta definida como sigue*

1. $sd^*(0) = 0$

2. *Definimos*

$$\varepsilon_f(x) = \max_{b \in \mathbb{Z}_{r_x}} \{d^*(f_{x,b})\},$$

$$\varepsilon_f(y) = \max_{b \in \mathbb{Z}_{r_y}} \{d^*(f_{y,b})\},$$

$$w_f(x) = \max_{b \in \mathbb{Z}_{r_x}} \{w_f(x, b) + 1\},$$

$$w_f(y) = \max_{b \in \mathbb{Z}_{r_y}} \{w_f(y, b) + 1\}.$$

   a) *La distancia aparente fuerte de f con respecto a x es $sd_x^*(f) = \varepsilon(x) \cdot w_f(x)$.*

   b) *La distancia aparente fuerte de f con respecto a y es $sd_y^*(f) = \varepsilon(y) \cdot w_f(y)$.*

3. *La distancia aparente fuerte de f es $sd^*(f) = \max\{sd_x^*(f), sd_y^*(f)\}$.*

Observación 4.2.5 *Podemos ver $w_f(x)$ como la distancia aparente del polinomio f_x ya que estamos contando la cadena de coeficientes cero más larga más 1. (En este caso los coeficientes son polinomios en la indeterminada y y vemos cuáles de estos polinomios son idénticamente cero). Para $w_f(y)$ seguimos un razonamiento análogo.*

Ejemplo 4.2.6 *Vamos a calcular la distancia aparente fuerte del polinomio del Ejemplo 4.2.2. Calculemos primero la distancia aparente fuerte con respeto a x. Recordamos que $f \in \mathbb{F}_2(15,3)$ se puede escribir como*

$$f_x = \underbrace{(y+y^2)}_{f_{x,0}} + \underbrace{(y^2)}_{f_{x,5}} x^5 + \underbrace{(y^2)}_{f_{x,7}} x^7 + \underbrace{(y)}_{f_{x,10}} x^{10} + \underbrace{(y)}_{f_{x,11}} x^{11} + \underbrace{(y^2)}_{f_{x,13}} x^{13} + \underbrace{(y)}_{f_{x,14}} x^{14}.$$

Podemos comprobar que $\varepsilon_f(x) = 3$, que se alcanza en los coeficientes $f_{x,10} = f_{x,11} = f_{x,14} = y$ así como en los coeficientes $f_{x,5} = f_{x,7} = f_{x,13} = y^2$. También se puede comprobar que $w_f(x) = 5$ ya que, si tomamos $b = 1$, tenemos que $f_{x,1} = f_{x,2} = f_{x,3} = f_{x,4} = 0$. Por lo tanto $sd^*_x(f) = 3 \cdot 5 = 15$. Calculemos ahora la distancia aparente fuerte con respecto a y. Recordemos que

$$f_y = \underbrace{(1 + x^{10} + x^{11} + x^{14})}_{f_{y,1}} y + \underbrace{(1 + x^5 + x^7 + x^{13})}_{f_{y,2}} y^2.$$

Puesto que $d^*(f_{y,1}) = 10$ y $d^*(f_{y,2}) = 6$, tenemos que $\varepsilon_f(y) = d^*(f_{y,1}) = 10$. Para calcular $w_f(y)$ basta observar que el único coeficiente que es idénticamente nulo es $f_{y,0}$, por lo que $w_f(y) = 1 + 1 = 2$. De esta forma $s^*_y(f) = 10 \cdot 2 = 20$. Por lo tanto $sd^*(f) = \max\{15, 20\} = 20$.

El siguiente teorema nos muestra cómo se relaciona la distancia aparente fuerte de un polinomio con su distancia aparente y con su número de no-ceros.

Teorema 4.2.7 *Sea $f \in \mathbb{L}(r_x, r_y)$. Entonces $d^*(f) \leq sd^*(f) \leq \left|\overline{Z(f)}\right|$.*

Demostración. Veamos primero que $d^*(f) \leq sd^*(f)$. Para ello, veamos que

$$\max_{h \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} \{d^*(c_x[h])(r_x - d_x[h])\} \leq sd^*_x(f).$$

Por un lado, tenemos que $\max\limits_{h \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} \{d^*(c_x[h])\} = \max\limits_{b \in \mathbb{Z}_{r_x}} \{d^*(f_{x,b})\} = \varepsilon_f(x)$. Ya que, multiplicando por el $h \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$ adecuado, $f_{x,b} = c_x[h]$ para cualquier $b \in \mathbb{Z}_{r_x}$. Por otro lado, tenemos que $\max\limits_{h \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} \{(r_x - d_x[h])\} = w_f(x)$, ya que, como hemos dicho en la Observación 4.2.5,

podemos ver $w_f(x)$ como la distancia aparente del polinomio f_x. De esta forma, tenemos que

$$\max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{d^*(c_x[h])(r_x-d_x[h])\}\leq$$
$$\max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{d^*(c_x[h])\}\cdot\max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{(r_x-d_x[h])\}=\varepsilon_f(x)\cdot w_f(x)=sd_x^*(f).$$

Análogamente tenemos que

$$\max_{h\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}\{d^*(c_y[h])(r_y-d_y[h])\}\leq sd_y^*(f).$$

Por lo tanto $d^*(f)\leq sd^*(f)$.

Veamos ahora que $sd^*(f)\leq\left|\overline{Z(f)}\right|$. Para ello veamos que $sd_x^*(f)\leq\left|\overline{Z(f)}\right|$.
Sea $b\in\{0,\ldots,r_x-1\}$ tal que $d^*(f_{x,b})=\varepsilon_f(x)$ y sea $\beta\in\overline{Z(f_{x,b})}$. Tenemos que $f(x,\beta)=\sum_{j=0}^{r_x-1}f_{x,j}(\beta)x^j\neq 0$, pues al menos $f_{x,b}(\beta)\neq 0$. Sea ahora $\gamma\in\overline{Z(f(x,\beta))}$, entonces $f(\gamma,\beta)\neq 0$, que implica $\sum_{\beta\in\overline{Z(f_{x,b})}}\left|\overline{Z(f(x,\beta))}\right|\leq\overline{Z(f(x,y))}$. Por otro lado tenemos que

$$\sum_{\beta\in\overline{Z(f_{x,b})}}\left|\overline{Z(f(x,\beta))}\right|\geq\sum_{\beta\in\overline{Z(f_{x,b})}}(w_f(x))=w_f(x)\cdot\left|\overline{Z(f_{x,b})}\right|$$
$$\geq w_f(x)\cdot d^*(f_{x,b})=w_f(x)\cdot\varepsilon_f(x)=sd_x^*(f).$$

Lo que implica, junto con lo anterior, que $sd_x^*(f)\leq\left|\overline{Z(f(x,y))}\right|$. Análogamente tenemos que $sd_y^*(f)\leq\left|\overline{Z(f(x,y))}\right|$, por lo que $sd^*(f)\leq\left|\overline{Z(f)}\right|$. ■

La distancia aparente fuerte de una matriz

Definición 4.2.8 *Sea M una matriz de orden $r_x\times r_y$ con entradas en $\mathbb{F}_q$. El conjunto de filas cero asociado a $b\in\mathbb{Z}_{r_x}$ es el conjunto*

$$Cf_M(b)=\{f_M(b_0),\ldots,f_M(b_l)\}\ \textit{con}\ b=b_0,$$

tal que $f_M(b_j) = 0\ \forall j \in \{0, \ldots, l\}$, $b_0, \ldots, b_l$ *es una lista de enteros consecutivos módulo* r_x *y* $f_M(\overline{b_l + 1}) \neq 0$. *Denotamos* $w_M(f, b) = |Cf_M(b)|$.

Análogamente, el conjunto de columnas asociado a $b \in \mathbb{Z}_{r_y}$ *es el conjunto*

$$Cc_M(b) = \{c_M(b_0), \ldots, c_M(b_l)\} \text{ con } b = b_0,$$

tal que $c_M(b_j) = 0\ \forall j \in \{0, \ldots, l\}$, $b_0, \ldots, b_l$ *es una lista de enteros consecutivos módulo* r_y *y* $c_M(\overline{b_l + 1}) \neq 0$. *Denotamos* $w_M(c, b) = |Cc_M(b)|$.

Definición 4.2.9 *Sea* M *una matriz con entradas en* $\mathbb{F}_q$. *La distancia aparente fuerte de* M, *denotada* $sd^*(M)$, *se define como*

1. $sd^*(0) = 0$

   a) $d^*(0) = 0$

   b) $d^*(f_M(b))$ *es la distancia aparente del vector* $f_M(b)$.

   c) $d^*(c_M(b))$ *es la distancia aparente del vector* $c_M(b)$.

2. *Definimos*

$$\varepsilon_M(x) = \max_{b \in \mathbb{Z}_{r_x}} \{d^*(f_M(b))\},$$

$$\varepsilon_M(y) = \max_{b \in \mathbb{Z}_{r_y}} \{d^*(c_M(b))\},$$

$$w_M(x) = \max_{b \in \mathbb{Z}_{r_x}} \{w_M(f, b) + 1\},$$

$$w_M(y) = \max_{b \in \mathbb{Z}_{r_y}} \{w_M(c, b) + 1\}.$$

   a) *La distancia aparente fuerte de* M *con respecto a* x *es* $sd^*_x(M) = \varepsilon(x) \cdot w_M(x)$.

   b) *La distancia aparente fuerte de* M *con respecto a* y *es* $sd^*_y(f) = \varepsilon(y) \cdot w_M(y)$.

3. *La distancia aparente fuerte de* M *es* $sd^*(M) = \max\{sd^*_M(f), sd^*_y(M)\}$.

Observación 4.2.10 *Veamos otra forma de calcular* $w_M(x)$. *Sea* $A_x = (a_0, \ldots, a_{r_x - 1})$ *con* $a_j = 0$ *si* $f_M(j) = 0$ *y* $a_j = 1$ *si* $f_M(j) \neq 0$. *Al vector* A_x *le denominamos un vector testigo de la matriz* M.

Es inmediato ver que $d^*(A_x) = w_M(x)$. *Análogamente, sea* $A_y = (a_0, \ldots, a_{r_y-1})$ *con* $a_j = 0$ *si* $c_M(j) = 0$ *y* $a_j = 1$ *si* $c_M(j) \neq 0$, *es inmediato ver que* $d^*(A_y) = w_M(y)$.

Definición 4.2.11 *Sea* M *una matriz no nula. Decimos que la fila* $f_M(b)$, *con* $b \in \mathbb{Z}_{r_x}$ *es una fila involucrada si* $sd^*(M) = d^*(f_M(b)) \cdot w_M(x)$. *Análogamente, decimos que la columna* $c_M(b)$, *con* $b \in \mathbb{Z}_{r_y}$ *es una columna involucrada si* $sd^*(M) = d^*(c_M(b)) \cdot w_M(y)$. *Denotamos por* $I_p(M)$ *al conjunto de filas y columnas de* M *involucradas.*

Ejemplo 4.2.12 *Calculemos la distancia aparente fuerte de la siguiente matriz* 5×15 *con entradas en* $\mathbb{F}_2$

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

Calculemos primero la distancia aparente fuerte con respecto a x. *Tenemos que* $\varepsilon_M(x) = 10$, *dado por la fila*

$$f_M(1) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Por otro lado, $w_M(x) = 2$ *ya que hay una única fila cuyas entradas sean todas nulas, la fila* $f_M(0)$. *Por lo tanto* $sd^*_x(M) = 10 \cdot 2 = 20$.

Veamos ahora la distancia aparente fuerte con respecto a y. *En este caso,* $\varepsilon_M(y) = 4$, *dado, entre otras, por la fila* $c_M(6) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \end{pmatrix}$. *Por otro lado,* $w_M(y) = 4$, *dado por el conjunto* $Cc_M(13)$ *ya que las columnas* $C_M(13), C_M(14), C_M(0)$ *son nulas. De esta forma,* $sd^*_y(M) = 4 \cdot 4 = 16$.

Así, $sd^*(M) = \max\{sd^*_M(f), sd^*_y(M)\} = sd^*_x(M) = 20$ *e* $I_p = \{f_M(1)\}$.

Veamos ahora que relación hay entre la distancia aparente fuerte de un polinomio y la distancia aparente fuerte de una matriz. Para un polinomio $f = \sum_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}} a_{(i,j)} Z^{(i,j)} \in \mathbb{F}_q(r_x, r_y)$ la matriz de coeficientes de f es $M(f) = (a_{(i,j)})_{(i,j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}}$. Si escribimos $f = f_x = \sum_{b=0}^{r_x - 1} f_{x,b} x^b$, observamos que $M(f_{x,b}) = f_{M(f)}(b)$. Análoga-

mente, si escribimos $f = f_y = \sum_{b=0}^{r_y-1} f_{y,b}y^b$, $M(f_{y,b}) = c_{M(f)}(b)$. En el siguiente lema vemos la relación entre las distancias aparentes fuertes de f y $M(f)$.

Lema 4.2.13 *Para cualquier polinomio $f \in \mathbb{F}_q(r_x, r_y)$ con matriz de coeficientes $M(f)$ se da la igualdad $sd^*(f) = sd^*(M(f))$,*

Demostración. Inmediato por la definición de distancia aparente para polinomios y matrices. ■

La distancia aparente fuerte de un código abeliano

Veamos ahora la definición de distancia aparente fuerte para un código abeliano.

Definición 4.2.14 *Sea C un código en $\mathbb{F}_q(r_x, r_y)$. La distancia aparente fuerte de C con respecto a α es $sd^*_\alpha(C) = \min\{sd^*(M(\varphi_{\alpha,c})) \mid c \in C\}$. La distancia aparente fuerte de C es $sd^*(C) = \max\{sd^*_\beta(C) \mid \beta \in U\}$.*

Definimos el conjunto de raíces óptimas de C como $SR(C) = \{\beta \in U \mid sd^*(C) = sd^*_\beta(C)\}$.

Obsérvese que, al igual que ocurría con la definición de distancia aparente para un código cíclico, esta definición es teórica e imposible de llevar a la práctica. En el resto del capítulo, veremos resultados que nos permitirán calcular la distancia aparente fuerte de un código de una forma más sencilla.

En la sección anterior, en (2.4), vimos que la distancia aparente de un código es menor o igual que la distancia mínima. El siguiente teorema nos muestra la relación entre la distancia aparente fuerte de un código y su distancia mínima.

Teorema 4.2.15 *Para cualquier código abeliano C en $\mathbb{F}_q(r_x, r_y)$ se cumple la desigualdad $sd^*(C) \leq d(C)$.*

Demostración. Para cualquier palabra código $f \in C$, por la definición de la transformada de Fourier sabemos que $w(f) = \left|\overline{Z(\varphi_{\alpha,f})}\right|$.

Por el Teorema 4.2.7 y el Lema 4.2.13 tenemos que

$$sd^*(M(\varphi_{\alpha,f})) = sd^*(\varphi_{\alpha,f}) \leq \left|\overline{Z(\varphi_{\alpha,f})}\right| = w(f).$$

Por lo tanto, $sd^*_\alpha(C) = \min\{sd^*(M(\varphi_{\alpha,f})) \mid f \in C\} \leq min\{w(f) \mid f \in C\} = d(C)$. Así, $sd^*(C) = \max\{sd^*_\beta(C) \mid \beta \in U\} \leq D(C)$. ■

Observamos que, al igual que ocurre en el caso de una variable, si $e \in \mathbb{F}_q(r_x, r_y)$ es idempotente y E es el ideal generado por e entones para cualquier $\alpha \in U$ tenemos que $\varphi_{\alpha,e} \star \varphi_{\alpha,e} = \varphi_{\alpha,e}$. Si $\varphi_{\alpha,e} = \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} a_{(i,j)}Z^{(i,j)}$, entonces $a_{(i,j)} \in \{1,0\}$ y $a_{(i,j)} = 0$ si y solo si $(i,j) \in D_\alpha(E)$. De esta forma, $M(\varphi_{\alpha,e}) = M(D_\alpha(E))$. Por otro lado, sea M una matriz dada por D, siendo D unión de q-órbitas. Sabemos que D define un único ideal C en $\mathbb{F}_q(r_x, r_y)$ tal que $D_\alpha(C) = D$. Sea $e \in C$ el generador idempotente, está claro que $M(\varphi_{\alpha,e}) = M(D)$.

Sea ahora C un código abeliano, $\alpha \in U$ y M una matriz dada por $D_\alpha(C)$. Por lo que hemos visto en la página 28, para cualquier matriz de q-órbitas P con $P \leq M$ existe un idempotente $e' \in C$ tal que $P = M(\varphi_{\alpha,e'})$ y para cualquier palabra código $f \in C$ existe un único idempotente $e(f)$ tal que $sd^*(M(\varphi_{\alpha,f})) = sd^*(M(\varphi_{\alpha,e(f)}))$. Por este motivo, podemos calcular la distancia aparente fuerte de un código abeliano por medio de las matrices de q-órbitas $P \leq M(\varphi_{\alpha,e})$, es decir

$$\begin{aligned}\min\{sd^*(P) \mid 0 \neq P \leq M\} &= \min\{sd^*(M(\varphi_{\alpha,e})) \mid 0 \neq e^2 = e \in C\} \\ &= sd^*_\alpha(C). \quad (4.2)\end{aligned}$$

Esto nos motiva a dar la siguiente definición.

Definición 4.2.16 *Sea M una matriz de q^t-órbitas. La distancia aparente fuerte mínima de M es $msd(M) = \min\{sd^*(P) \mid 0 \neq P \leq M\}$.*

Ejemplo 4.2.17 *Siguiendo el Ejemplo 4.1.2 tomamos el conjunto $D = Q_2((0,1)) \cup Q_2((0,3)) \cup Q_2((1,3))$. La matriz de 2-órbitas dada*

por D es

$$M = M(D) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

La distancia aparente fuerte de M es

$$sd^*(M) = sd^*_x(M) = d^*(f_M(0)) \cdot (w_M(f, 0) + 1) = 7 \cdot 1 = 7.$$

Si tomamos $D' = D \cup Q((0, 0))$, la matriz de 2-órbitas dada por D' es

$$P = M(D') = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Puesto que $D' \subset D$, $P < M$ además

$$sd^*(P) = sd^*_y(P) = d^*(c_P(0)) \cdot (w_P(c, 5) + 1) = 2 \cdot 3 = 6.$$

Por lo tanto $sd^*(P) < sd^*(M)$, es más, se puede comprobar que $msd(M) = sd^*(P) = 6$.

Observación 4.2.18 *En el caso de una variable tenemos que si $f, g \in \mathbb{L}(n)$ con $supp(f) \subseteq supp(g)$ entonces $d^*(g) \leq d^*(f)$. Esto implica, como hemos visto en el Lema 2.0.11, que $d^*_\alpha(C) = d^*(\varphi_{\alpha,e})$. El ejemplo anterior nos muestra que esto no es cierto en el caso de dos variables ya que tenemos que $P \leq M$, y por lo tanto $supp(P) \subseteq supp(M)$, pero $sd^*(P) = 6 < 7 = sd^*(M)$. Este fenómeno es lo que nos impide extender directamente los resultados que hemos obtenido en códigos cíclicos a códigos abelianos de dos variables.*

En el siguiente teorema vemos la relación que hay entre la distancia aparente fuerte de un código abeliano y la distancia aparente fuerte mínima de la matriz dada por la transformada de Fourier discreta del idempotente generador.

Teorema 4.2.19 *Sea C un código abeliano en $\mathbb{F}_q(r_x, r_y)$, e su generador idempotente y $\alpha \in U$. Entonces $sd^*_\alpha(C) = msd(M(\varphi_{\alpha,e}))$. Así, $sd^*(C) = \max\{msd(M(\varphi_{\alpha,e})) \mid \alpha \in U\}$.*

Demostración. Por (4.2) tenemos que $msd(M(\varphi_{\alpha,e})) = \min\{sd^*(P) \mid 0 \neq P \leq M(\varphi_{\alpha,e}\} = sd^*_\alpha(C)$. Así, $\max\{msd(M(\varphi_{\alpha,e})) \mid \alpha \in U\} = \max\{sd^*_\alpha(C) \mid \alpha \in U\} = sd^*(C)$. ■

Observación 4.2.20 *Veamos que, al igual que ocurría en el caso de una variable al calcular la distancia aparente de un código, para calcular la distancia aparente fuerte de un código abeliano no necesitamos calcular $sd^*_\alpha(C)$ $\forall \alpha \in U$. Sea $\{Q(a_1), Q(a_2), \ldots, Q(a_h)\}$ un conjunto completo de todas las q-órbitas módulo (r_x, r_y). Fijemos los representantes $a_1, \ldots, a_h$ y sea $\alpha \in U$ que nos da el conjunto de definición $D_\alpha(C)$. Buscamos los elementos $\beta \in U$ tales que $D_\beta(C) \neq D_\alpha(C)$. Entonces $\beta \in U$ debe cumplir $\beta^{a_i q^t} = \alpha$, para algún $t \in \mathbb{Z}$ y $a_i = (a_{ix}, a_{iy})$ tal que $mcd(a_{ix}, r_x) = mcd(a_{iy}, r_y) = 1$. En este caso está claro que $D_\beta(C) = a_i \cdot D_\alpha(C)$, donde la multiplicación es componente a componente.*

Denotamos por $K(r_x, r_y) = \{a_i = (a_{ix}, a_{iy}) \mid mcd(a_{ix}, r_x) = mcd(a_{iy}, r_y) = 1\}$. Fijado $\alpha \in U$, definimos $R_\alpha = \{\beta \in U \mid \beta^{a_i} = \alpha, a_i \in K(r_x, r_y)\}$. Por lo que, para calcular la distancia aparente de un código, fijado un $\alpha \in C$, necesitamos calcular $sd^*(C) = \max\{sd^*_\beta(C) \mid \beta \in R_\alpha\}$.

4.2.1. Cómo calcular la distancia aparente fuerte mínima de una matriz

Sea q, r_x y r_y y sea L_t el conjunto de q^t-órbitas en $\mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, para algún $t \in \mathbb{N}$. Para un subconjunto arbitrario $L' \subseteq L_t$ definimos $D = \bigcup_{Q \in L'} Q$ y construimos $M = M(D)$, la matriz de q^t-órbitas dada por D. Sea $f_M(b)$ una fila cualquiera de M, con $b \in \mathbb{Z}_{r_x}$. Definimos $Df_M(b) = \{b\} \times \mathbb{Z}_{r_y} \setminus supp(f_M(b))$.

Lema 4.2.21 *Podemos ver $f_M(b)$ como un vector de $q^{t'}$-órbitas, con $t' = t\,|C_{q^t}(b)|$ y donde $C_{q^t}(b)$ es la clase q^t-ciclotómica módulo*

r_x *(recordemos que* $C_{q^t}(a) = \{q^i a \mid i \in \mathbb{N}\}$*). Mas aún,* $f_M(b)$ *es el vector generado por* $Df_M(b)$*.*

Demostración. Sea $(b, j) \in \{b\} \times \mathbb{Z}_{r_y}$. Observamos que

$$q^{t'} b = q^{t|C_{q^t}(b)|} = b.$$

Por lo tanto $q^{t'}(b, j) = (q^{t'} b, q^{t'} j) = (b, q^{t'} j) \in \{b\} \times \mathbb{Z}_{r_y}$, lo que implica que $\{b\} \times \mathbb{Z}_{r_y}$ es cerrado bajo $q^{t'}$-órbitas, es decir, podemos escribir $\{b\} \times \mathbb{Z}_{r_y}$ como unión de $q^{t'}$-órbitas. Sea ahora $(b, j) \in \{b\} \times \mathbb{Z}_{r_y}$ tal que $a_{(b,j)} = 0$. Puesto que $(b, j) \in \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$, existe un $Q \in L_t$ tal que $(b, j) \in Q$. Además, $q^{t'}(b, j) = (b, q^{t'} j)$ y por lo tanto $q^{t'}(b, j) \in Q$ por ser Q una q^t-órbita. Esto implica que $a_{q^{t'}(b,j)} = 0$, ya que M es una matriz de q^t-órbitas. Hemos visto que $\{b\} \times \mathbb{Z}_{r_y}$ es unión de $q^{t'}$-órbitas y que si $a_{(b,j)} \in f_M(b)$, con $a_{(b,j)} = 0$, entonces $a_{q^{t'}(b,j)} \in \{b\} \times \mathbb{Z}_{r_y}$ y $a_{q^{t'}(b,j)} = 0$, esto implica que $f_M(b)$ es un vector de $q^{t'}$-órbitas. El hecho de que $D(f_M(b)) = Df_M(b)$ es inmediato. ■

Análogamente, si $c_M(b)$ es una columna cualquiera de M con $b \in \mathbb{Z}_{r_y}$, podemos ver $c_M(b)$ como un vector de $q^{t'}$-órbitas, con $t' = t\,|C_{q^t}(b)|$ y donde $C_{q^t}(b)$ es la clase q^t-ciclotómica módulo r_y. Además $c_M(b)$ es el vector generado por $Dc_M(b)$, siendo $Dc_M(b) = \mathbb{Z}_{r_x} \times \{b\} \setminus supp(c_M(b))$.

Proposición 4.2.22 *Sea* M *una matriz de* q^t*-órbitas, y sea* $N < M$*. Entonces para todo* $b \in \mathbb{Z}_{r_x}$*,* $f_N(b) < f_M(b)$*, viendo* $f_N(b)$ *y* $f_M(b)$ *como vectores de* $q^{t'}$*-órbitas, donde* $t = t'\,|C_{q^t}(b)|$ *y* $C_{q^t}(b)$ *es la clase* q^t*-ciclotómica módulo* r_x*. Análogamente, para todo* $b \in \mathbb{Z}_{r_y}$*,* $c_N(b) < c_M(b)$*, viendo* $c_N(b)$ *y* $c_M(b)$ *como vectores de* $q^{t'}$*-órbitas, donde* $t = t'\,|C_{q^t}(b)|$ *y* $C_{q^t}(b)$ *es la clase* q^t*-ciclotómica módulo* r_y*.*

Demostración. Vemos la demostración para las filas ya que para las columnas es análoga. Puesto que $N < M$, tenemos que $D(M) \subset D(N)$ por lo que $Df_N(b) \subseteq Df_M(b)$. Utilizando el lema anterior, esto implica que $f_N(b) \leq f_M(b)$ como vectores de $q^{t'}$-órbitas. ■

Lema 4.2.23 *Sea* M *una matriz de* q^t*-órbitas no nula. Sea* $b \in \mathbb{Z}_{r_x}$

y A un vector indexado por $\{b\}\times\mathbb{Z}_{r_y}$ (es decir, $A=(a_{(i,j)})_{(i,j)\in\{b\}\times\mathbb{Z}_{r_y}}$) tal que $supp(A)\subseteq supp(f_M(b))$. Entonces existe $N\leq M$ tal que:

1. *$supp(f_N(b))\subseteq supp(A)$.*
2. *Si una matriz de q^t-órbitas $P<M$ es tal que $supp(f_P(b))\subseteq supp(A)$, entonces $P\leq N$.*
3. *Si A es un vector de $q^{t|C_{q^t}(b)|}$-órbitas entonces $A=f_N(b)$.*

Así, N es la máxima matriz de q^t-órbitas (con respecto al orden definido en (4.1)) tal que $supp(f_N(b))\subseteq supp(A)$.

Demostración. Sea $\overline{A}=supp(f_M(b))\setminus supp(A)$ y sea N la matriz de q^t-órbitas tal que $D(N)=D(M)\cup(\cup_{(b,j)\in\overline{A}}Q_t((b,j)))$. Puesto que $D(M)\subseteq D(N)$, tenemos que $N\leq M$ y $supp(f_N(b))\subseteq supp(f_M(b))$. Veamos que N cumple las tres condiciones del lema.

1. Sea $(b,j)\in supp(f_N(b))$. Tenemos que $Q_t((b,j))\cap D(N)=\emptyset$ y por lo tanto $Q_t((b,j))\cap\overline{A}=\emptyset$. Puesto que $(b,j)\in supp(f_M(b))$ ya que $N\leq M$, tenemos que $Q_t(b,j)\subseteq supp(A)$ y por lo tanto $(b,j)\in supp(A)$.

2. Sea P una matriz de q^t-órbitas con $P<M$, tal que $supp(f_P(b))\subseteq supp(A)$. Sea $(i,j)\in supp(P)$ esto implica que $Q_t((i,j))\cap D(P)=\emptyset$. Veamos ahora que $Q_t((i,j))\cap D(N)=\emptyset$. Puesto que $P<M$, tenemos que $D(M)\subset D(P)$ y por lo tanto $Q_t((i,j))\cap D(M)=\emptyset$, lo que implica que $(i,j)\notin D(M)$. Supongamos que $Q_t((i,j))\cap D(N)\neq\emptyset$. Puesto que $D(N)=D(M)\cup(\cup_{(b,j)\in\overline{A}}Q_t((b,j)))$ y $Q_t((i,j))\cap D(M)=\emptyset$ tenemos que $Q_t((i,j))\cap(\cup_{(b,j)\in\overline{A}}Q_t((b,j)))\neq\emptyset$ y por lo tanto existe un $(b,j')\in\overline{A}$ tal que $Q_t((i,j))=Q_t((b,j'))$. Esto implica que $(b,j')\in supp(P)$ ya que $Q_t((b,j'))\cap D(P)=Q_t((i,j))\cap D(P)=\emptyset$. Además, $(b,j')\in supp(f_P(b))\subseteq supp(A)$, lo que es una contradicción pues $(b,j')\in\overline{A}$. De esta forma hemos visto que $Q_t((i,j))\cap D(N)=\emptyset$, lo que implica que $(i,j)\in supp(N)$ y por lo tanto $supp(P)\subseteq sup(N)$, es decir, $P\leq N$.

3. Supongamos que A es un vector de $q^{t|C_{q^t(b)}|}$-órbitas y supongamos que $supp(A)\setminus supp(f_N(b))\neq\emptyset$. Sea $(b,j)\in supp(A)\setminus$

$supp(f_N(b))$. Puesto que $(b,j) \notin supp(f_N(b))$, $(b,j) \notin supp(N)$ lo que implica que $(b,j) \in D(N)$ y por lo tanto $Q_t((b,j)) \subseteq D(N)$. Sea N' el vector generado por $D(N) \setminus Q_t(b,j)$. Puesto que $D(N') = D(N) \setminus Q_t((b,j)) \subseteq D(N)$, $N < N'$. Además, puesto que A es un vector de $q^{t|C_{q^t(b)}|}$-órbitas y que $(b,j) \in supp(A)$, por el Lema 4.2.21 tenemos que $Q_{t|C_{q^t(b)}|}((b,j)) \subset supp(A)$ y por lo tanto

$$\{b\}\times\mathbb{Z}_{r_y}\setminus supp(f_{N'}(b)) = (\{b\}\times\mathbb{Z}_{r_y}\setminus supp(f_N(b)))\setminus Q_{t|C_{q^t(b)}|}((b,j))$$
$$\supseteq (\{b\}\times\mathbb{Z}_{r_y}\setminus supp(A))\setminus Q_{t|C_{q^t(b)}|}((b,j)) \supseteq \{b\}\times\mathbb{Z}_{r_y}\setminus supp(A).$$

Así, $supp(f_{N'}(b)) \subseteq supp(A)$ que implica $f_{N'}(b) \leq A$, lo que contradice el punto (2.). Por lo tanto, $supp(A)\setminus supp(f_N(b)) = \emptyset$ y utilizando el punto (1.), $A = f_N(b)$.

■

Análogamente, podemos enunciar el Lema 4.2.23 para columnas.

Lema 4.2.24 *Sea M una matriz de q^t-órbitas no nula. Sea $b \in \mathbb{Z}_{r_y}$ y A un vector indexado por $\mathbb{Z}_{r_x}\times\{b\}$ (es decir, $A = (a_{(i,j)})_{(i,j)\in\mathbb{Z}_{r_x}\times\{b\}}$) tal que $supp(A) \subseteq supp(c_M(b))$. Entonces existe $N \leq M$ tal que:*

1. *$supp(c_N(b)) \subseteq supp(A)$.*
2. *Si una matriz de q^t-órbitas $P < M$ es tal que $supp(c_P(b)) \subseteq supp(A)$, entonces $P \leq N$.*
3. *Si A es un vector de $q^{t|C_{q^t(b)}|}$-órbitas entonces $A = c_N(b)$.*

Así, N es la máxima matriz de q^t-órbitas tal que $supp(c_N(b)) \subseteq supp(A)$.

Demostración. Análoga a la demostración del Lema 4.2.23. ■

Corolario 4.2.25 *Sea M una matriz de q^t-órbitas no nula. Sean $b_1,\ldots,b_l \in \mathbb{Z}_{r_x}$ y $b'_1,\ldots,b'_r \in \mathbb{Z}_{r_y}$. Existe una matriz de q^t-órbitas $N \leq M$ con soporte máximo, es decir, máxima con respecto al orden definido en (4.1), tal que $f_N(b) = 0, \forall b \in \{b_1,\ldots,b_l\}$ y $c_N(b) = 0, \forall b \in \{b'_1,\ldots,b'_r\}$.*

Demostración. Es inmediata utilizando repetidamente el Lema 4.2.23 y el Lema 4.2.24 con $A = 0$. ■

El siguiente resultado nos proporciona una condición suficiente para calcular la distancia aparente mínima de una matriz.

Proposición 4.2.26 *Sea D un conjunto unión de q^t-órbitas y sea $M = M(D) \neq 0$. Sea $f_M(b)$, con $b \in \mathbb{Z}_{r_x}$, una fila involucrada en el cálculo de $sd^*(M)$. Si $d^*(f_M(b)) = 1$ entonces $msd(M) = sd^*(M)$.*

Análogamente, si $c_M(b)$, con $b \in \mathbb{Z}_{r_y}$, una columna involucrada en el cálculo de $sd^*(M)$ y $d^*(c_M(b)) = 1$ entonces $msd(M) = sd^*(M)$

Demostración. Veamos la prueba para las filas ya que para las columnas es análoga.

Por hipótesis tenemos que $sd^*(M) = d^*(f_M(b))\cdot w_M(x) \underset{d^*(f_M(b))=1}{=} w_M(x)$. Sea $b' \in \{0, \ldots, r_x - 1\}$ tal que $w_M(x) = w_M(f, b') + 1$. Sea ahora una matriz M' con $0 \neq M' \leq M$. Puesto que $M' \leq M$ y por lo tanto $supp(M') \subseteq supp(M)$, si $l \in \mathbb{Z}_{r_x}$ es tal que $f_M(l) = 0$, entonces $f_{M'}(l) = 0$. Puesto que $f_M(b') = 0$, tenemos que $Cf_M(b') \subseteq Cf_{M'}(b')$ y así $sd^*(M') \geq (w_{M'}(f, b') + 1)\varepsilon_{M'}(x) \geq w_M(f, b') + 1 = sd^*(M)$. Por lo tanto tenemos que $\forall\ M'$ con $M' \leq M$, $sd^*(M') \geq sd^*(M)$, por la definición de distancia aparente mínima tenemos que $sd^*(M) = msd(M)$. ■

El siguiente ejemplo muestra que la condición de la proposición anterior no es una condición necesaria.

Ejemplo 4.2.27 *Sea $q = 2, r_x = 3, r_y = 9$. El conjunto de 2-*

órbitas módulo $(3,9)$ *es el siguiente*

$$\begin{aligned}
&Q_2((0,0)) = \{(0,0)\},\\
&Q_2((0,1)) = \{(0,1),(0,2),(0,4),(0,5),(0,7),(0,8)\},\\
&Q_2((0,3)) = \{(0,3),(0,6)\},\\
&Q_2((1,0)) = \{(1,0),(2,0)\},\\
&Q_2((1,1)) = \{(1,1),(1,4),(1,7),(2,2),(2,5),(2,8)\},\\
&Q_2((1,2)) = \{(1,2),(1,5),(1,8),(2,1),(2,4),(2,7)\},\\
&Q_2((1,3)) = \{(1,3),(2,6)\},\\
&Q_2((1,6)) = \{(1,6),(2,3)\}.
\end{aligned}$$

Si tomamos $D = Q_2((0,1)) \cup Q_2((1,0)) \cup Q_2((1,3)) \cup Q_2((2,3))$, *la matriz de* 2*-órbitas dada por* D *es*

$$M = M(D) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Se puede comprobar que $sd^*(M) = 3$ *siendo*

$$I_p(M) = \{f_M(0), c_M(0), c_M(3), c_M(6)\}$$

el conjunto de filas y columnas de M *involucradas. También se puede comprobar que* $msd(M) = sd^*(M) = 3$, *sin embargo, ninguna de las filas o columnas involucradas tiene distancia aparente 1.*

Lema 4.2.28 *Sea* D *un conjunto unión de* q^t*-órbitas y sea* $M = M(D) \neq 0$. *Sea* $f_M(b)$, *con* $b \in \mathbb{Z}_{r_x}$, *una fila involucrada en el cálculo de* $sd^*(M)$. *Si* $P < M$ *y* $sd^*(P) < sd^*(M)$ *entonces* $d^*(f_P(b)) < d^*(f_M(b))$. *Análogamente si* $c_M(b)$, *con* $b \in \mathbb{Z}_{r_y}$, *es una columna involucrada en el cálculo de* $sd^*(M)$, *entonces* $d^*(c_P(b)) < d^*(c_M(b))$.

Demostración. Veamos la prueba para las filas ya que para las columnas es análoga.

Si $f_P(b) = 0$ la demostración es directa por lo tanto supongamos que $f_P(b) \neq 0$. Como $P < M$, tenemos que $w_M(x) \leq w_P(x)$. Así,

$$\begin{aligned}
sd^*(M) = d^*(f_M(b)) \cdot w_M(x) &\underset{\text{Hipótesis}}{>} sd^*(P) \geq d^*(f_P(b)) \cdot w_P(x)\\
&\underset{w_M(x) \leq w_P(x)}{\geq} d^*(f_P(b)) \cdot w_M(x),
\end{aligned}$$

lo que implica que $d^*(f_P(b)) < d^*(f_M(b))$. ■

Proposición 4.2.29 *Sea L_t el conjunto de todas las q^t-órbitas módulo (r_x, r_y), $\mu \in \{1, \ldots, |L_t| - 1\}$ y $\{Q_j\}_{j=1}^{\mu}$ un subconjunto de L_t. Sea $D = \bigcup_{j=1}^{\mu} Q_j$ y $M = M(D)$. Entonces existen dos sucesiones: la primera formada por matrices de q^t-órbitas no nulas,*

$$M = M_0 > \cdots > M_l \neq 0$$

y la segunda formada por enteros positivos

$$m_0 \geq \cdots \geq m_l,$$

con $l \leq \mu$ y $m_i \leq sd^*(M_i)$ para $0 \leq i \leq l$, que satisfacen la siguiente propiedad:

(*I*) *Si P es una matriz de q^t-órbitas tal que $0 \neq P \leq M$, entonces $sd^*(P) \geq m_l$ y si $sd^*(P) < m_{i-1}$ entonces $P \leq M_i$, donde $0 < i < l$.*

Mas aún, si $l' \in \{0, \ldots, l\}$ es el primer elemento tal que $m_{l'} = m_l$ entonces $sd^*(M_{l'}) = msd(M)$.

Demostración. Obsérvese que $M \neq 0$ ya que $\mu \leq |L_t| - 1$. Veamos cómo construir de forma recursiva dos sucesiones que cumplan la condición (I). Sea $M_0 = M$, $m_0 = sd^*(M)$ e $I_p(M)$ el conjunto de filas y columnas involucradas. Si existe alguna fila involucrada $f_M(b)$ con $b \in \mathbb{Z}_{r_x}$ o alguna columna involucrada $c_M(b')$ con $b' \in \mathbb{Z}_{r_y}$ tales que $d^*(f_M(b)) = 1$ o $d^*(c_M(b')) = 1$ entonces por la Proposición 4.2.26 hemos terminado (en este caso $l = 0$); por lo tanto, supongamos que $d^*(f_M(b)) \neq 1$ para todo $f_M(b) \in I_p(M)$ y $d^*(c_M(b')) \neq 1$ para todo $c_M(b') \in I_p(M)$. Por el Corolario 4.2.25 podemos construir una matriz de q^t-órbitas $M_1 < M$ con soporte máximo tal que $f_M(b) = 0$ para todo $f_M(b) \in I_p(M)$ y $c_M(b') = 0$ para todo $c_M(b') \in I_p(M)$.

Afirmamos que para cualquier matriz de q^t-órbitas $P < M$, si $sd^*(P) < m_0$ entonces $P \leq M_1$. Supongamos que P es una matriz

de q^t-órbitas con $P < M$ y $sd^*(P) < m_0$. Sea $f_M(b) \in I_p(M)$ (si no hay filas involucradas tomamos una columna y procedemos de la misma manera). Por el Lema 4.2.28 sabemos que $d^*(f_P(b)) < d^*(f_M(b))$. Por otro lado, por la Proposición 4.2.22 tenemos que $f_P(b) < f_M(b)$ como vectores de q^t-órbitas, es decir, $f_P(b)$ tiene un mayor número de coordenadas nulas que $f_M(b)$. Como $d^*(f_P(b)) < d^*(f_M(b))$, esto implica que $f_P(b) = 0$. Análogamente, para todo $c_M(b') \in I_p(M)$ tenemos que $c_P(b') = 0$. Así, por cómo hemos construido M_1, $P \leq M_1$.

Si $M_1 = 0$, tomando de nuevo $l = 0$, hemos terminado. Si $M_1 \neq 0$, tomamos $m_1 = min\{m_0, sd^*(M_1)\}$ y por lo tanto obtenemos M_1 y m_1 que satisfacen la condición (I) debido al razonamiento que hemos seguido en el párrafo anterior.

Supongamos que tenemos las sucesiones $M = M_0 > \cdots > M_\delta \neq 0$ y $m_0 \geq \cdots \geq m_\delta$ tales que $m_i = min\{m_{i-1}, sd^*(M_i)\}$ $\forall i \in \{0, \ldots, \delta\}$ con $1 \leq \delta \leq \mu - 1$. Supongamos también que si P es una matriz de q^t-órbitas con $P \leq M$ y $sd^*(P) < m_{i-1}$ entonces $P < M_i$.

Para obtener los elementos $M_{\delta+1}$ y $m_{\delta+1}$ razonamos con M_δ de forma análoga a como hemos razonado con M_0 al principio de la prueba. Si existe alguna fila involucrada de M_δ, $f_{M_\delta}(b)$ con $d^*(f_{M_\delta}(b)) = 1$ o alguna columna involucrada de M_δ, $c_{M_\delta}(b')$ con $d^*(c_{M_\delta}(b')) = 1$, entonces, por la Proposición 4.2.26 hemos terminado (en este caso $l = \delta$). Por lo tanto, supongamos que $d^*(f_{M_\delta}(b)) \neq 1$ para todo $f_{M_\delta}(b) \in I_p(M_\delta)$ y que $d^*(c_{M_\delta}(b')) \neq 1$ para todo $c_{M_\delta}(b') \in I_p(M_\delta)$. Al igual que hemos razonado antes, el Corolario 4.2.25 nos permite construir una matriz de q^t-órbitas $M_{\delta+1}$ de soporte máximo tal que $M_{\delta+1} < M_\delta$ y con $f_{M_{\delta+1}}(b) = 0$ para todo $f_{M_\delta}(b) \in I_p(M_\delta)$ y $c_{M_{\delta+1}}(b') = 0$ para todo $c_{M_\delta}(b') \in I_p(M_\delta)$. Si $M_{\delta+1} = 0$, tomamos $l = \delta$ y hemos terminado; si $M_{\delta+1} \neq 0$, por la Proposición 4.2.22 y por el Lema 4.2.28 tenemos que para cualquier matriz de q^t-órbitas $0 \neq P < M$ tal que $P \leq M_{\delta+1}$ se verifica que $P \leq M_{\delta+1}$. Definimos $m_{\delta+1} = \{m_\delta, sd^*(M_{\delta+1})\}$. De esta forma podemos añadir un elemento más a nuestras sucesiones las cuales siguen cumpliendo la condición (I).

Obsérvese que este proceso concluye en, como mucho, $|L_t| - \mu$

pasos ya que $supp(M_i)$ difiere de $supp(M_{i+1})$ en al menos una q^t-órbita. Es decir, en cada paso necesitamos al menos una q^t-órbita que no hayamos utilizado anteriormente para construir la nueva matriz que continúa la sucesión, como al principio tenemos $|L_t| - \mu$ q^t-órbitas disponibles realizamos como mucho $|L_t| - \mu$ pasos.

Supongamos que la sucesión termina en el paso l. En este paso $d^*(f_{M_l}(b)) = 1$ para algún $f_{M_l}(b) \in I_p(M_l)$ (o $d^*(c_{M_l}(b')) = 1$ para algún $c_{M_l}(b') \in I_p(M_l)$) o bien $M_{l+1} = 0$. Sea $l' \in \{0, \ldots, l\}$ el primer elemento tal que $m_{l'} = m_l$. Afirmamos que $m_{l'} = sd^*(M_{l'})$. Como $m_{l'} = min\{m_{l'-1}, sd^*(M_{l'})\}$, basta ver que $m_{l'} \neq m_{l'-1}$. Si $m_{l'} = m_{l'-1}$, entonces $m_{l'-1} = m_{l'} = m_l$ lo que contradice que l' es el menor elemento tal que $m_{l'} = m_l$. Por lo tanto $m_{l'} = sd^*(M_{l'})$. Veamos ahora que $msd(M) = sd^*(M_{l'})$. Supongamos que existe una matriz de q^t-órbitas $0 \neq P \leq M$ con $sd^*(P) < m_{l'} = m_l$. Como las sucesiones que hemos construido cumplen la condición (I), entonces $P \leq M_{l+1} \leq M_l$. Ahora, si la sucesión de matrices de q^t-órbitas se ha detenido porque $d^*(f_{M_l}(b)) = 1$ para algún $f_{M_l}(b) \in I_p(M_l)$ (o $d^*(c_{M_l}(b')) = 1$ para algún $c_{M_l}(b') \in I_p(M_l)$) entonces $msd(M_l) = sd^*(M_l)$ y por lo tanto $P = 0$. Si la sucesión de matrices se ha detenido porque $M_{l+1} = 0$ entonces también ocurre que $P = 0$. En ambos casos ocurre que $P = 0$ lo que es una contradicción. Así $msd(M) = sd^*(M_{l'})$. ■

A continuación, vemos, de forma esquemática, el algoritmo que hemos utilizado para construir las sucesiones de la proposición anterior.

Algoritmo 4.2.30 *Sea* $M = (m_{ij})_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}$.

Paso 1. *Tomamos* $m_0 = sd^*(M)$.

Paso 2. a) *Si existe alguna fila involucrada* $f_M(b)$ *con* $b \in \{0, \ldots, r_x - 1\}$ *o alguna columna involucrada* $c_M(b')$ *con* $b' \in \{0, \ldots, r_y - 1\}$ *tales que* $d^*(f_M(b)) = 1$ *o* $d^*(c_M(b')) = 1$ *entonces por la Proposición se termina el proceso con 4.2.26* $M = M_0$ *y* $m_0 = sd^*(M)$.

b) *En el caso de que* $d^*(f_M(b)) \neq 1$ *para todo* $f_M(b) \in$

$I_p(M)$ y $d^*(c_M(b')) \neq 1$ para todo $c_M(b') \in I_p(M)$ tomamos

$$S_x = \cup\{supp(f_M(b)) \mid b \in \mathbb{Z}_{r_x} \text{ con } f_M(b) \in I_p(M)\},$$

$$S_y = \cup\{supp(c_M(b')) \mid b' \in \mathbb{Z}_{r_y} \text{ con } c_M(b') \in I_p(M)\}$$

y construimos la matriz $M_1 = (a_{ij})_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}$ tal que

$$a_{ij} = \begin{cases} 0 & si \quad (i,j) \in (\cup\{Q(b,k) \mid (b,k) \in S_x\}) \\ & \quad \cup (\cup\{Q(k',b') \mid (k',b') \in S_y\}), \\ m_{ij} & en\ otro\ caso. \end{cases}$$

Paso 3. a) *Si $M_1 = 0$, finalizamos dando las sucesiones $M = M_0$ y $m_0 = sd^*(M)$.*

b) *Si $M_1 \neq 0$, tomamos $m_1 = min\{m_0, sd^*(M_1)\}$ y obtenemos las sucesiones $M = M_0 > M_1$ y $m_0 \geq m_1$. Volvemos al Paso 1 con M_1 en lugar de M y m_1 en lugar de m.*

Ejemplo 4.2.31 *Sea $q = 2$, $r_x = 3$, $r_y = 15$. Vamos a calcular la distancia aparente fuerte del código C con $D_\alpha(C) = \mathbb{Z}_3 \times \mathbb{Z}_{15} \setminus \{Q_2((1,0)) \cup Q_2((1,10)) \cup Q_2((1,11))\}$.*

Las 2-órbitas módulo $(3,15)$ son

$$\begin{aligned}
&Q_2((0,0)) = \{(0,0)\},\\
&Q_2((1,0)) = \{(1,0),(2,0)\},\\
&Q_2((0,1)) = \{(0,1),(0,2),(0,4),(0,8)\},\\
&Q_2((0,3)) = \{(0,3),(0,6),(0,9),(0,12)\},\\
&Q_2((0,5)) = \{(0,5),(0,10)\},\\
&Q_2((0,7)) = \{(0,7),(0,11),(0,13),(0,14)\},\\
&Q_2((1,1)) = \{(1,1),(1,4),(2,2),(2,8)\},\\
&Q_2((1,2)) = \{(1,2),(1,8),(2,1),(2,4)\},\\
&Q_2((1,3)) = \{(1,3),(1,12),(2,6),(2,9)\},\\
&Q_2((1,5)) = \{(1,5),(2,10)\},\\
&Q_2((1,6)) = \{(1,6),(1,9),(2,3),(2,12)\},\\
&Q_2((1,7)) = \{(1,7),(1,13),(2,11),(2,14)\},\\
&Q_2((1,10)) = \{(1,10),(2,5)\},\\
&Q_2((1,11)) = \{(1,11),(1,14),(2,7),(2,13)\}.
\end{aligned}$$

La matriz generada por $D_\alpha(C)$ *es*

$$M = M(D_\alpha(C)) \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Calculamos $msd(M)$ *utilizando el Algoritmo 4.2.30.*

Paso 1. *Calculamos* $sd^*(M)$. *Es fácil comprobar que* $sd^*(M) = sd^*_x(M) = \varepsilon_M(x) \cdot w_M(x) = 10 \cdot 2 = 20$, *donde* $\varepsilon_M(x) = d^*(f_M(1)) = 10$. *Tomamos* $m_0 = 20$.

Paso 2*a*. *Como* $I_p(M) = \{f_M(1)\}$ *y* $d^*(f_M(1)) \neq 1$ *vamos al paso* 2*b*.

Paso 2*b*. *Tenemos que* $S_x = supp\{f_M(1)\} = \{(1,0),(1,10),(1,11),(1,14)\}$ *y que* $S_y = \emptyset$. *Construimos la matriz* $M_1 = (a_{ij})_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}$ *tal que*

$$a_{ij} = \begin{cases} 0 & si \quad (i,j) \in (Q_2((1,0)) \cup Q_2((1,10)) \\ & \qquad \cup Q_2((1,11))) \\ m_{ij} & en\ otro\ caso. \end{cases}$$

Obsérvese que $M_1 = 0$, *por lo que vamos al paso* 3*a*

Paso 3*a*. *Damos las sucesiones* $M = M_0$,$m_0 = sd^*(M)$. *Además, tenemos que* $msd(M) = sd^*(M) = 20$ *lo que implica que* $sd^*(C) = 20$.

4.3. Códigos abelianos en los que su distancia aparente fuerte coincide con su distancia mínima

Veamos primero qué condiciones tiene que cumplir un código abeliano para que su distancia aparente fuerte coincida con su distancia mínima. Por la Observación 4.2.18, el tratamiento de este problema va a diferir del que hemos utilizado en el caso de códigos cíclicos.

Teorema 4.3.1 *Sea C un código abeliano en $\mathbb{F}_q(r_x, r_y)$. Las siguientes condiciones son equivalentes:*

1. $sd^*(C) = d(C)$.
2. *Existe un elemento $\alpha \in U$ y una palabra $c \in C$ tal que $g = \varphi_{\alpha,c}$ verifica:*
   a) $sd^*(M(g)) = sd^*_\alpha(C)$.
   b) $sd^*(M(g)) = \left|\overline{Z(g)}\right|$.

Demostración.
"$1 \Longrightarrow 2$"
Sea $c \in C$ tal que $w(c) = d(C)$ y $\alpha \in U$ tal que $sd^*_\alpha(C) = sd^*(C)$. Sea $g = \varphi_{\alpha,c}$. Tenemos que

$$d(C) \underset{\text{Hipótesis}}{=} sd^*(C) = sd^*_\alpha(C) \leq sd^*(M(g)) \underset{\substack{\text{Lema 4.2.13 y} \\ \text{Teorema 4.2.7}}}{\leq} \left|\overline{Z(g)}\right| \underset{\text{Observación 4.1.3}}{=} w(g) = d(C),$$

lo que implica que $sd^*(M(g)) = sd^*_\alpha(C)$ y $sd^*(M(g)) = \left|\overline{Z(g)}\right|$.
"$2 \Longrightarrow 1$"
Considérese una palabra $c \in C$ tal que su imagen por la transformada de Fourier discreta $g = \varphi_{\alpha,c}$ verifica los puntos $(2a.)$ y $(2b.)$. Entonces

$$d(C) \leq w(c) = \left|\overline{Z(g)}\right| = sd^*(M(g)) = sd^*_\alpha(C) \leq sd^*(C) \leq d(C),$$

lo que implica que $sd^*(C) = d(C)$. ■

Al igual que ocurre en el caso de una variable, para un código abeliano dado, encontrar una palabra código que cumpla la condición (2) del Teorema 4.3.1 es un problema muy difícil de resolver. En el caso de que la palabra código que cumpla estas condiciones sea un idempotente seremos capaces de encontrarla utilizando la Proposición 4.2.29 para el cálculo de la distancia aparente fuerte mínima. El siguiente resultado nos proporciona un método para encontrar este idempotente.

Proposición 4.3.2 *Sea C un código abeliano en $\mathbb{F}_q(r_x, r_y)$, $\alpha \in U$ y M la matriz dada por el conjunto definición $D_\alpha(C)$. Sea $P \leq M$ una matriz de q-órbitas con $e \in C$ un idempotente con $g = \varphi_{\alpha,e} \in \mathbb{L}(r_x, r_y)$ tal que $P = M(g)$. Si P verifica*

1. $sd^*(P) = msd(M)$ *y*
2. $sd^*(P) = \left|\overline{Z(g)}\right|$.

Entonces $d(C) = msd(M) = sd^*(C)$.

Demostración. Tenemos que $\varphi_{\alpha,g}^{-1} = e \in C$, así $w(e) \geq d(C) \geq sd^*(C) \underset{\text{Teorema 4.2.15}}{\geq} d(C)$. Por otro lado tenemos que

$$w(\varphi_{\alpha,g}^{-1}) = \left|\overline{Z(g)}\right| \underset{\text{Condición (1.)}}{=} sd^*(P) \underset{\text{Condición (2.)}}{=} msd(M) \leq sd^*(C) \leq d(C).$$

Por lo tanto, $d(C) = msd(M) = sd^*(C)$. ■

Así, dado un código abeliano C con matriz dada M, si queremos saber si $d(C) = sd^*(C)$, por la Proposición 4.3.2, en caso de que la palabra código que satisface la condición (2.) del Teorema 4.3.1 sea idempotente, tenemos que analizar todas las matrices de q-órbitas $P \leq M$ y comprobar si cumplen las condiciones (1.) y (2.) de la Proposición 4.3.2. Si $\left|\overline{D_\alpha(C)}\right| = t$ tenemos que analizar, como mucho, 2^t matrices de q-órbitas $P \leq M$.

Nos preguntamos si será posible reducir la búsqueda de esta matriz P analizando la sucesión de matrices que hemos utilizado en la Proposición 4.2.29 para calcular la distancia aparente fuerte mínima de M. Consideramos las sucesiones

$$M = M_0 > M_1 > \cdots > M_{j_0-1} > M_{j_0} > \cdots > M_l > 0,$$

$$m_0 \geq m_1 \geq \cdots \geq m_{j_0-1} \geq m_{j_0} \geq \cdots \geq m_l,$$

que cumplen la condición (I) de la Proposición 4.2.29 y donde j_0 es el primer índice tal que $m_{j_0} = m_l$. Como hemos visto en la demostración de la Proposición 4.2.29, $m_{j_0} = m_l$ implica que $sd^*(M_{j_0}) = msd(M)$. Si $m_0 = m_l$, entonces $P \leq M$ y no podemos reducir la búsqueda. Sin embargo, si $m_0 > m_l$, entonces

$sd^*(P) = m_l < m_{j_0-1}$ lo que implica que $P \leq M_{j_0}$, de esta forma solo necesitamos analizar las matrices de q-órbitas $P \leq M_{j_0}$; es decir, tenemos que analizar, como mucho, 2^{t-j_0} matrices de q-órbitas.

Nos preguntamos si la existencia de una matriz $P \leq M$ que satisfaga las condiciones de la Proposición 4.3.2 implica la existencia de una matriz en la sucesión $M = M_0 > M_1 > \cdots > M_{j_0-1} > M_{j_0} > \cdots > M_l > 0$ que satisfaga también dichas condiciones. El siguiente ejemplo muestra que esto no tiene por qué ocurrir.

Ejemplo 4.3.3 *Veamos que existe un código abeliano C y una matriz M dada por $D_\alpha(C)$ tales que*

1. *Para cada matriz de q-órbitas en la sucesión $M = M_0 > \ldots M_l > 0$, tenemos que $sd^*(M_j) \neq \left|\overline{Z(e_j)}\right|$, con $e_j \in \mathbb{L}(r_x, r_y)$ el idempotente tal que $M_j = M(e_j)$.*

2. *$d(C) = sd^*(C)$.*

Sea $q = 2$, $r_x = r_y = 7$. Las 2-órbitas módulo $(7,7)$ son

$Q_2((0,0)) = \{(0,0)\}$,
$Q_2((1,0)) = \{(1,0),(2,0),(4,0)\}$, $Q_2((0,1)) = \{(0,1),(0,2),(0,4)\}$,
$Q_2((3,0)) = \{(3,0),(5,0),(6,0)\}$, $Q_2((0,3)) = \{(0,3),(0,5),(0,6)\}$,
$Q_2((1,1)) = \{(1,1),(2,2),(4,4)\}$,
$Q_2((1,2)) = \{(1,2),(2,4),(4,1)\}$, $Q_2((2,1)) = \{(2,1),(4,2),(1,4)\}$,
$Q_2((1,3)) = \{(1,3),(2,6),(4,5)\}$, $Q_2((3,1)) = \{(3,1),(6,2),(5,4)\}$,
$Q_2((1,4)) = \{(1,4),(2,1),(4,2)\}$, $Q_2((4,1)) = \{(4,1),(1,2),(2,4)\}$,
$Q_2((1,5)) = \{(1,5),(2,3),(4,6)\}$, $Q_2((5,1)) = \{(5,1),(3,2),(6,4)\}$,
$Q_2((1,6)) = \{(1,6),(2,5),(4,3)\}$, $Q_2((6,1)) = \{(6,1),(5,2),(3,4)\}$,
$Q_2((3,1)) = \{(3,1),(6,2),(5,4)\}$, $Q_2((1,3)) = \{(1,3),(2,6),(4,5)\}$,
$Q_2((3,2)) = \{(3,2),(6,4),(5,1)\}$, $Q_2((2,3)) = \{(2,3),(4,6),(1,5)\}$,
$Q_2((3,3)) = \{(3,3),(6,6),(5,5)\}$,
$Q_2((3,4)) = \{(3,4),(6,1),(5,2)\}$, $Q_2((4,3)) = \{(4,3),(1,6),(2,5)\}$,
$Q_2((3,5)) = \{(3,5),(6,3),(5,6)\}$, $Q_2((5,3)) = \{(5,3),(3,6),(6,5)\}$,
$Q_2((3,6)) = \{(3,6),(6,5),(5,3)\}$, $Q_2((6,3)) = \{(6,3),(5,6),(5,3)\}$.

Sea $\alpha \in U$ y sea el código C con $D_\alpha(C) = Q_2((0,3)) \cup Q_2((1,3)) \cup Q_2((1,5)) \cup Q_2((1,6)) \cup Q_2((3,0)) \cup Q_2((3,2)) \cup Q_2((3,3)) \cup Q_2((3,4)) \cup Q_2((3,5)) \cup Q_2((3,6))$.

Sea $a(x) = (1+x)(1+x^2+x^3)$, $b(y) = (1+y)(1+y^2+y^3)$ *y* $e \in C$ *el idempotente generador de* C. *Se puede comprobar que* $\varphi_{\alpha,e} = a(x)b(y) + x^3y + x^6y^2 + x^5y^4$ *y que* $\left|\overline{Z(\varphi_{\alpha,e})}\right| = 25$.

Ahora, calculemos $msd(M)$, *con* $M = M(D_\alpha(C))$, *utilizando la Proposición 4.2.29. Tenemos que*

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

Para construir la sucesión de matrices que necesitamos utilizamos el Algoritmo 4.2.30. Calculamos primero $m_0 = sd^*(M)$. *Es fácil comprobar que* $sd^*(M) = sd^*_y(M) = \varepsilon_M(y) \cdot w_M(y) = d^*(c_M(1)) \cdot (w_M(c,5)+1) = 3 \cdot 3 = 9$. *Además,* $I_p(M) = \{c_M(0) \cup c_M(1)\}$. *Puesto que* $d^*(c_M(0)) \neq 1$, *vamos al paso 2b del Algoritmo 4.2.30. Tenemos* $S_x = \emptyset$ *y* $S_y = supp(c_M(0)) \cup supp(c_M(1)) = \{(0,0),(1,0),(2,0),(4,0)\} \cup \{(0,1),(1,1),(2,1),(3,1),(4,1)\}$. *Construimos la matriz* $M_1 = (a_{ij})_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}}$ *con*

$$a_{ij} = \begin{cases} 0 \quad si & (i,j) \in Q_2((0,0)) \cup Q_2((1,0)) \\ & \cup Q_2((0,1)) \cup Q_2((1,1)) \cup Q_2((2,1)) \\ & \cup Q_2(3,1)) \cup Q_2((4,1)) \\ m_{ij} \quad en\ otro\ caso. \end{cases}$$

Por lo tanto, $M_1 = 0$ *y damos las sucesiones* $M_0 > 0$ *y* $m_0 > 0$, *además,* $msd(M) = sd^*(M) = 9$. *Ahora consideramos la matriz de q-órbitas*

$$P = M(ab) = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

con $0 < P < M$. *Obsérvese que* P *no pertenece a la sucesión* $M_0 > 0$. *Sin embargo, como veremos más adelante,* $g_1 = ab$ *cumple las hipótesis de la Proposición 4.3.11 por lo que* C *satisface la condición* $(2b)$ *del Teorema 4.3.1. Por otro lado, es muy fácil comprobar que* $sd^*(P) = 9$ *y por lo tanto la condición* $(2a)$ *del Teorema 4.3.1 también se satisface. Así,* $d(C) = sd^*(C)$.

Como hemos visto, aunque la Proposición 4.3.2 nos da una condición suficiente, no nos garantiza que podamos encontrar la palabra código adecuada que cumpla la condición del Teorema 4.3.1 si esta no es un idempotente. Es por ello que, para construir códigos abelianos C con $d(C) = sd^*(C)$, intentamos utilizar otro razonamiento en el cual intentaremos caracterizar los polinomios que cumplen la condición $(2b)$ del Teorema 4.3.1, es decir, los polinomios $g \in \mathbb{L}(r_x, r_y)$ tales que $sd^*(M(g)) = \left|\overline{Z(g)}\right|$.

Queremos identificar los polinomios $g \in \mathbb{L}(r_x, r_y)$ tales que $sd^*(M(g)) = \left|\overline{Z(g)}\right|$. Vamos a suponer que $g \in \mathbb{L}(r_x, r_y)$ cumple esta igualdad, es más, vamos a suponer que cumple la siguiente condición, que aunque es más fueret nos permite manejar mejor la situación.

$$sd_x^*(M) = sd_y^*(M) = sd^*(M) = g \in \mathbb{L}(r_x, r_y), \tag{4.3}$$

con $M = M(g)$.

Recordemos que podemos ver g como un polinomio en $(\mathbb{L}[y])[x]$, basta con escribir g como $g = g_x = \sum_{k=0}^{r_x-1} g_{x,k}x^k$. Análogamente, escribiendo $g = g_y = \sum_{k=0}^{r_y-1} g_{y,k}y^k$, lo podemos ver como un polinomio en $(\mathbb{L}[x])[y]$.

Para todo $u \in \mathbb{L}$, los polinomios de la forma $g(u, y)$ y $g(x, u)$ tienen el significado obvio.

Definimos ahora los siguientes conjuntos

$$M_x = \{k \in \{0, \ldots, r_x - 1\} \mid f_M(k) \in I_p(M)\},$$

$$M_y = \{k \in \{0, \ldots, r_y - 1\} \mid c_M(k) \in I_p(M)\},$$

donde $I_p(M)$ es el conjunto de filas y columnas de M involucradas. Obsérvese que $I_p(M) = M_x \cup M_y$.

Ahora, para cada $k \in M_x$ definimos el conjunto

$$D_{x,k} = \{(u,v) \in R \mid v \in \overline{Z(g_{x,k})} \text{ y } u \in \overline{Z(g(x,v))}\}.$$

Análogamente, para cada $k \in M_y$ definimos el conjunto

$$D_{y,k} = \{(u,v) \in R \mid u \in \overline{Z(g_{y,k})} \text{ y } v \in \overline{Z(g(u,y))}\}.$$

Definimos ahora $min(x,k) = \min\{\left|\overline{Z(g(x,v))}\right| \mid v \in \overline{Z(g_{x,k})}\}$. Análogamente, $min(y,k) = \min\{\left|\overline{Z(g(u,y))}\right| \mid u \in \overline{Z(g_{y,k})}\}$.

En las siguientes observaciones vemos que relación guardan estos elementos que acabamos de definir.

Observación 4.3.4 *Obsérvese que*

$$|D_{x,k}| = \sum_{v \in \overline{Z(g_{x,k})}} \left|\overline{Z(g(x,v))}\right| \geq \sum_{v \in \overline{Z(g_{x,k})}} min(x,b) = min(x,b) \cdot \left|\overline{Z(g_{x,k})}\right|,$$

y por lo tanto, $\left|\overline{Z(g_{x,k})}\right| \cdot min(x,k) \leq |D_{x,k}|$.

Observación 4.3.5 *Para todo* $k \in M_x$*, tenemos que* $\varepsilon_M(x) = d^*(f_M(k)) \underset{\text{Observación 2.0.8}}{\leq} \left|\overline{Z(g_{x,k})}\right|$*. Por otro lado,*

$$w_M(x) = \max\{w_M(x,k) + 1 \mid k \in \mathbb{Z}_{r_x}\} \leq d^*(M(g(x,v))) \underset{\text{Observación 2.0.8}}{\leq} \left|\overline{Z(g(x,v))}\right|,$$

y por lo tanto $w_M(x) \leq min(x,k)$*. (Nótese que la desigualdad* $\max\{w_M(x,k) + 1 \mid k \in \mathbb{Z}_{r_x}\} \leq d^*(M(g(x,v))$ *proviene de la Observación 4.2.10 y del hecho de que* $f_{M(g)}(k) = M(g_{x,k})$*. Puede ocurrir que* $f_{M(g)}(k) \neq 0$ *pero que* $g_{x,k}(v) = 0$ *y por lo tanto* $\max\{w_M(x,k) + 1 \mid k \in \mathbb{Z}_{r_x}\} = d^*(A_x) \leq d^*(M(g(x,v))$*.) Así,* $\varepsilon_M(x) \cdot w_M(x) \leq \left|\overline{Z(g_{x,k})}\right| \cdot min(x,k) \leq |D_{x,k}|$*. Análogamente,* $\varepsilon_M(y) \cdot w_M(y) \leq |D_{y,k}|$.

Observación 4.3.6 *Teniendo en cuenta que* g *cumple la condición* (4.3) *y por la observación anterior, tenemos que* $\left|\overline{Z(g)}\right| = sd_x^*(M) = \varepsilon_M(x) \cdot w_M(x) \leq |D_{x,k}|$*. Por otro lado, por definición de*

$D_{x,k}$, *tenemos que* $D_{x,k} \leq \overline{Z(g)}$. *Esto implica que* $D_{x,k} = \overline{Z(g)}\ \forall k \in M_x$. *Además, puesto que* $\left|\overline{Z(g)}\right| = |D_{x,k}| = sd_x^*(M) = \varepsilon_M(x) \cdot w_M(x) \leq \left|\overline{Z(g_{x,k})}\right| \cdot min(x,k) \leq |D_{x,k}|$, *tenemos que* $\varepsilon_M(x) \cdot w_M(x) = \left|\overline{Z(g_{x,k})}\right| \cdot min(x,k)$. *Análogamente,* $D_{y,k} = \overline{Z(g)}\ \forall y \in M_x$ *y* $\varepsilon_M(y) \cdot w_M(y) = \left|\overline{Z(g_{y,k})}\right| \cdot min(y,k)$.

Observación 4.3.7 *En la última observación hemos visto que* $\varepsilon_M(x) \cdot w_M(x) = \left|\overline{Z(g_{x,k})}\right| \cdot min(x,k)$. *Veamos ahora que* $\varepsilon_M(x) = \left|\overline{Z(g_{x,k})}\right|$ *y* $w_M(x) = min(x,k)$. *Tenemos que*

$$\varepsilon_M(x) \leq \left|\overline{Z(g_{x,k})}\right| \Rightarrow$$

$$\varepsilon_M(x) \cdot min(x,k) \leq \left|\overline{Z(g_{x,k})}\right| \cdot min(x,k) \underset{\text{Observación 4.3.6}}{=} \varepsilon_M(x) \cdot w_M(x) \Rightarrow$$

$$min(x,k) \leq w_M(x) \Rightarrow min(x,k) = w_M(x)\ y\ \varepsilon_M(x) = \left|\overline{Z(g_{x,k})}\right|.$$

Por lo tanto, tenemos que que $\varepsilon_M(x) = \left|\overline{Z(g_{x,k})}\right|$, $w_M(x) = min(x,k)$ *y análogamente* $\varepsilon_M(y) = \left|\overline{Z(g_{y,k})}\right|$ *y* $w_M(y) = min(y,k)$.

Teniendo en cuenta las igualdades que hemos obtenido en la Observación 4.3.6 y en la Observación 4.3.7 vamos a probar los dos siguientes resultados.

Lema 4.3.8 *Sea* $g = g(x,y) \in \mathbb{L}(r_x, r_y)$ *un polinomio tal que* $M = M(g)$ *satisface la condición* (4.3), *entonces.*

1. *Para todo* $k \in M_x$, $d^*(M(g_{x,k})) = \left|\overline{Z(g_{x,k})}\right| = \left|\pi_y\left(\overline{Z(g)}\right)\right|$.
2. *Para todo* $k \in M_y$, $d^*(M(g_{y,k})) = \left|\overline{Z(g_{y,k})}\right| = \left|\pi_x\left(\overline{Z(g)}\right)\right|$.

Demostración. Veamos que se cumple (1.) pues la prueba de (2.) es análoga. Puesto que g cumple la condición (4.3) tenemos que la Observación 4.3.6 y la Observación 4.3.7 se cumplen. Por lo tanto tenemos que $\varepsilon_M(x) = d^*(M(g_{x,k})) = \left|\overline{Z(g_{x,k})}\right|$. Además, como $D_{x,k} = \overline{Z(g)}$, tenemos que $\left|\pi_y\left(\overline{Z(g)}\right)\right| = |\pi_y(D_{x,k})| = \left|\overline{Z(g_{x,k})}\right|$. Asi, $d^*(M(g_{x,k})) = \left|\overline{Z(g_{x,k})}\right| = \left|\pi_y\left(\overline{Z(g)}\right)\right|$. ■

Proposición 4.3.9 *Sea* $g = g(x,y) \in \mathbb{L}(r_x, r_y)$ *un polinomio tal que* $M = M(g)$ *satisface la condición* (4.3). *Entonces existen* $a =$

$a(x) \in \mathbb{L}(r_x)$, $b = b(y) \in \mathbb{L}(r_y)$ y $F = F(x,y) \in \mathbb{L}(r_x, r_y)$ tales que $g = abF$ y

1. *$\overline{x^{h_x} a} \mid x^{r_x} - 1$ para algún $h_x \in \mathbb{Z}_{r_x}$ con $d^*(M(a)) = \varepsilon_M(y)$.*
2. *$\overline{y^{h_y} b} \mid y^{r_y} - 1$ para algún $h_y \in \mathbb{Z}_{r_y}$ con $d^*(M(b)) = \varepsilon_M(x)$.*

Mas aún, $a = mcd(g_{y,0}, \ldots, g_{y,r_y-1}, x^{r_x}-1)$ y $b = mcd(g_{x,0}, \ldots, g_{x,r_x-1}, y^{r_y}-1)$.

Demostración. Para cada $k \in M_y$, denotamos $m_k = mcd(g_{y,k}, x^{r_x}-1)$ (obsérvese que $m_k = m_{g_{y,k}} = mcd(g_{y,k}, x^n - 1)$ como hemos definido en (3.1)). Entonces

$$d^*(M(m_k)) \underset{\text{Proposición 3.0.3}}{=} r_x - |Z(m_k)| = r_x - |Z(g_{y,k})| = \left|\overline{Z(g_{y,k})}\right| \underset{\text{Lema 4.3.8}}{=} d^*(M(g_{y,b})).$$

Por la definición de distancia aparente para polinomios de una variable, existe un $k' \in \{0, \ldots, r_x - 1\}$ tal que $d^*(M(g_{y,k})) = r_x - deg(\overline{x^{k'} g_{y,k}})$. Por otro lado, por el Lema 3.0.1 tenemos que $d^*(M(m_k)) = r_x - deg(m_k)$. Así, $d^*(M(g_{y,k})) = d^*(M(m_k)) = r_x - deg(m_k)$ y por la Proposición 3.0.3 tenemos que $\overline{x^{k'} g_{y,k}}$ y m_k son polinomios asociados.

Veamos ahora que $m_k \mid g_{y,j}\ \forall j \in \{0, \ldots, r_y - 1\}$. Para ello basta ver que $Z(g_{y,k}) \subseteq Z(g_{y,j})$. Por la Observación 4.3.6 tenemos que $D_{y,k} = \overline{Z(g)}$. Ahora, para $u \in \overline{Z(g_{y,j})}$ tenemos que $g(u,y) \neq 0$ y para $v \in \overline{Z(g(u,y))}$, tenemos que $(u,v) \in \overline{Z(g)} = D_{y,k}$ lo que implica que $\overline{Z(g_{y,j})} \subseteq \overline{Z(g_{y,k})}$. Así $Z(g_{y,k}) \subseteq Z(g_{y,j})$ y por lo tanto $m_k \mid g_{y,j}\ \forall j \in \{0, \ldots, r_y - 1\}$.

Denotamos $g'_{y,j} = \frac{g_{y,j}}{m_k}\ \forall j \in \{0, \ldots, r_y - 1\}$ y $a(x) = m_k$. Podemos escribir g de la siguiente forma

$$g(x,y) = a(x) \sum_{j=0}^{r_y - 1} g'_{y,j} y^j,$$

con $d^*(a) = d^*(m_k) = d^*(g_{y,k}) \underset{\text{Lema 4.3.8}}{=} \left|\overline{Z(g_{y,k})}\right| \underset{\text{Observación 4.3.7}}{=} \varepsilon_M(y)$. Análogamente, podemos escribir g como

$$g(x,y) = b(y) \sum_{j=0}^{r_x - 1} g'_{x,j} x^j,$$

con $g'_{x,j} = \frac{g_{x,j}}{b(y)}$ $\forall j \in \{0, \ldots, r_x - 1\}$ y con $d^*(M(b(y))) = \varepsilon_M(x)$.

Es importante destacar que $1 = mcd(x^{r_x} - 1, g'_{y,0}, \ldots, g'_{y,r_y-1})$, ya que si $mcd(x^{r_x} - 1, g'_{y,0}, \ldots, g'_{y,r_y-1}) = t$ con $t \in \mathbb{L}(r_x)$, $t \neq 1$, entonces tenemos que $t \mid x^{r_x} - 1$ y que $t \mid g'_{y,k} = \frac{g_{y,k}}{m_k}$, lo que contradice que $m_k = mcd(g_{y,k}, x^{r_x} - 1)$. Análogamente, $1 = mcd(y^{r_y} - 1, g'_{x,0}, \ldots, g'_{x,r_x-1})$.

Sea ahora $f(x,y) = \sum_{j=0}^{r_y-1} g'_{y,j} y^j$ y $h(x,y) = \sum_{j=0}^{r_x-1} g'_{x,j} x^j$, tenemos que $g(x,y) = a(x)f(x,y) = b(y)h(x,y)$.

Veamos que $\pi_y\left(\overline{Z(g)}\right) = \overline{Z(b)}$. Sea $v \in \pi_y\left(\overline{Z(g)}\right)$, existe $u \in \pi_x\left(\overline{Z(g)}\right)$ tal que $(u,v) \in \overline{Z(g)} = D_{x,k}$, lo que implica que $v \in \overline{Z(g_{x,k})} = \overline{Z(b)}$. Tenemos que $\pi_y\left(\overline{Z(g)}\right) \subseteq \overline{Z(b)} = \overline{Z(g_{x,k})}$ y por el Lema 4.3.8 tenemos que $\left|\overline{Z(g_{x,k})}\right| = \left|\pi_y\left(\overline{Z(g)}\right)\right|$. Por lo tanto, $\pi_y\left(\overline{Z(g)}\right) = \overline{Z(b)}$.

Se afirma que $v \in \overline{Z(b)} = \pi_y\left(\overline{Z(g)}\right)$ si y solo si $g(x,v) \neq 0$. Para $v \in \overline{Z(b)} = \pi_y\left(\overline{Z(g)}\right)$, tenemos que $g(x,v) = b(v)h(x,v) = b(v) = \sum_{j=0}^{r_x-1} g'_{x,j}(v)x^j$. Como $b(v) \neq 0$, entonces $g(v) \neq 0$, ya que si $g(v) = 0$ tendríamos que $g'_{x,j}(v)$ $\forall j \in \{0, \ldots, r_x - 1\}$, es decir, todos los $g'_{x,j}$ tendrían un cero en común, lo que contradice $1 = mcd(x^{r_x} - 1, g'_{y,0}, \ldots, g'_{y,r_y-1})$. La otra implicación es inmediata, pues como $b(v) \neq 0$ implica que $g(x,v) \neq 0$, tenemos que $g(x,v) = 0$ implica que $b(v) = 0$, y por lo tanto $v \in \overline{Z(b)} = \pi_y\left(\overline{Z(g)}\right)$.

Ahora, miramos al polinomio f como un polinomio en $(\mathbb{L}[y])[x]$ es decir, escribimos $f = \sum_{i=0}^{r_x-1} f_{x,i} x^i$. Análogamente, escribimos $h = \sum_{j=0}^{r_y-1} h_{y,j} y^j$, es decir, vemos h como un polinomio en $(\mathbb{L}[x])[y]$.

Sea $v \in Z(b)$, entonces $g(x,v) = a(x)f(x,v) = b(v)h(x,v) = 0$, lo que implica $f(x,v) = 0$. Esto quiere decir que $f_{x,i}(v) = 0$ $\forall i \in \{0, \ldots, r_x - 1\}$. Puesto que $b(y) = mcd(g_{x,k}, y^{r_y} - 1)$ y $f_{x,i}(v) = 0$ $\forall i \in \{0, \ldots, r_x - 1\}$ y $\forall v \in Z(b)$, tenemos que $b \mid f_{x,i}$ $\forall i \in$

$\{0,\dots,r_x-1\}$. Por otro lado, si $f_{x,i}(v)=0\ \forall i\in\{0,\dots,r_x-1\}$ tenemos que $f(x,v)=0$ y por lo tanto $g(x,v)=0$, lo que implica, por lo que hemos visto anteriormente, que $v\in Z(b)$. Por lo tanto $\forall i\in\{0,\dots,r_x-1\}$, tenemos que $b\mid f_{x,i}$ y si v es tal que $f_{x,i}(v)=0$ entonces $v\in Z(b)$. Esto implica que $b(y)=mcd(y^{r_y}-1,f_{x,i})\ \forall i\in\{0,\dots,r_x-1\}$. Así, $f(x,y)=b(y)f'(x,y)$ y $g(x,y)=a(x)b(y)f'(x,y)$.

Análogamente, podemos ver que $a(x)\mid h_{y,j}\ \forall j\in\{0,\dots,r_y-1\}$. De esta manera, $h(x,y)=a(x)h'(x,y)$ y $g(x,y)=a(x)b(y)h'(x,y)$.

Finalmente, tenemos que las descomposiciones $g=abf'$ y $g=abh'$ las hemos realizado en $\mathbb{L}[x,y]$, que es un dominio y por tanto $f'(x,y)=h'(x,y)$. De esta manera, si escribimos $F(x,y)=f'(x,y)=h'(x,y)$ tenemos que $g(x,y)=a(x)b(y)F(x,y)$. ■

En el Teorema 4.3.1 hemos visto qué condiciones (teóricas) debe de cumplir un código para que su distancia aparente fuerte sea igual a su distancia mínima. Para comprobar estas condiciones necesitamos encontrar una palabra código c tal que $g=\varphi_{\alpha,c}$ cumpla los puntos $(2a)$ y $(2b)$ del Teorema 4.3.1. Puesto que necesitamos comprobar que $sd^*(M(g))=\overline{Z(g)}$, hemos impuesto la condición (4.3) y hemos visto qué propiedades cumplen los polinomios que satisfacen esta condición (Proposición 4.3.9.). Ahora nos preguntamos si un polinomio g que satisface las condiciones del Teorema 4.3.1 cumple necesariamente la condición (4.3). A continuación mostramos un ejemplo de que esto no tiene por qué ocurrir.

Ejemplo 4.3.10 *Sea $q=2$, $r_x=5$, $r_y=9$. Sea C un código con $D_\alpha(C)=Q_2((1,3))$, para un cierto $\alpha\in U$, con idempotente generador $e(x,y)=x^4y^7+x^3y^8+x^4y^6+x^2y^8+x^3y^6+x^4y^4+x^3y^5+x^2y^6+xy^7+x^4y^3+x^2y^5+xy^6+x^3y^3+x^4y+x^3y^2+x^2y^3+xy^4+x^4+x^2y^2+xy^3+x^3+x^2+xy$. Se puede comprobar que $d(C)=24$ y que $\varphi_{\alpha,e}=xy^3+x^4y^3+x^2y^6+x^3y^6$. Sea $g=\varphi_{\alpha,e}$, vamos a calcular*

$sd^*(M(g))$. *Tenemos que*

$$M(g) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Calculemos primero $sd_x^*(M(g))$. *Obsérvese que* $\varepsilon_{M(g)}(x) = d^*(f_{M(g)}(4)) = 9$ *y que* $w_{M(g)}(x) = w_{M(g)}(f, 0) + 1 = 2$, *por lo que* $sd_x^*(M(g)) = 2 \cdot 9 = 18$. *Calculemos ahora* $sd_y^*(M(g))$. *Obsérvese que* $\varepsilon_{M(g)}(y) = d^*(c_{M(g)}(6)) = 4$ *y que* $w_{M(g)}(xy = w_{M(g)}(c, 7) + 1 = 6$, *por lo que* $sd_y^*(M(g)) = 4 \cdot 6 = 24$.. *Así,* $sd^*(M(g)) = 24$ *pero* $sd_x^*(M(g)) \neq sd_y^*(M(g))$ *por lo que* g *no satisface la condición* (4.3).

Por otro lado, como $w(e) = 24$, *tenemos, por la Observación 1.0.8, que* $sd^*(M(g)) = \left|\overline{Z(g)}\right|$. *Además se puede comprobar que* $sd^*(M(g)) = msd(M(g))$. *Por lo tanto,* $g = \varphi_{\alpha,e}$ *cumple las condiciones del Teorema 4.3.1 pero no cumple la condición* (4.3).

Por la Proposición 4.3.9, sabemos que si g cumple la condición (4.3), podemos escribir $g = abF$ donde a, f y F cumplen ciertas condiciones. A continuación vemos un resultado análogo a la Proposición 4.3.9; en que se establece qué condiciones cumple g si lo podemos expresar de la forma $g = ab$.

Proposición 4.3.11 *Sea* $g \in \mathbb{L}(r_x, r_y)$ *tal que* $g(x, y) = a(x)b(y)$, *y existen* $h_x \in \{0, \ldots, r_x - 1\}$ *y* $h_y \in \{0, \ldots, r_y - 1\}$ *tales que* $\overline{x^{h_x}a} \mid x^{r_x} - 1$ *y* $\overline{y^{h_y}b} \mid y^{r_y} - 1$. *Sea* $M = M(g)$. *Entonces*

1. $\overline{Z(g)} = \overline{Z(a)} \times \overline{Z(b)}$.
2. $sd^*(M) = d^*(M(a)) \cdot d^*(M(b)) = \left|\overline{Z(g)}\right|$.
3. $sd^*(M) = sd_x^*(M) = sd_y^*(M) = \left|\overline{Z(g)}\right|$ *(Obsérvese que es la condición* (4.3)*)*.
4. $d^*(M(a)) = \varepsilon_M(y) = w_M(x)$.
5. $d^*(M(b)) = \varepsilon_M(x) = w_M(y)$.

Demostración. Veamos primero el punto (1.). Sea $(u,v) \in \overline{Z(g)}$, entonces $g(u,v) = a(u)b(v) \neq 0$ y por lo tanto $a(u) \neq 0$ y $b(v) \neq 0$. Esto implica que $(u,v) \in \overline{Z(a)} \times \overline{Z(b)}$. Sea ahora $(u,v) \in \overline{Z(a)} \times \overline{Z(b)}$, tenemos que $a(u) \neq 0$ y $b(v) \neq 0$. Así $g(u,v) = a(u)b(v) \neq 0$ y por lo tanto $(u,v) \in \overline{Z(g)}$.

Veamos ahora los puntos (4.) y (5.). Para ello veamos que $\varepsilon_M(x) = d^*(M(b))$ y que $w_M(x) = d^*(M(a))$.

Veamos primero que $\varepsilon_M(x) = d^*(M(b))$. Sea $M(a) = (a_0, \ldots, a_{r_x-1})$. Si escribimos g como un polinomio en $(\mathbb{L}[y])[x]$ tenemos

$$g = \sum_{i=0}^{r_x-1} g_{x,i}x^i = \sum_{i=0}^{r_x-1} a_i \cdot b(y)x^i.$$

Así $g_{x,i} = a_i \cdot b(y)\ \forall i \in \{0, \ldots, r_x - 1\}$, por lo que, $f_M(i) = M(g_{x,i}) = M(a_i \cdot b(y))$. Además si $a_i \neq 0$, $supp(a_i \cdot b(y)) = supp(b(y))$. Por lo tanto tenemos que, $\varepsilon_M(x) = \max\{d^*(f_M(i)) \mid i \in \{0, \ldots, r_x - 1\}\} = \max\{d^*(a_i \cdot b(y)) \mid i \in \{0, \ldots, r_x - 1\}\} = d^*(M(b))$.

Ahora veamos $w_M(y) = d^*(M(a))$. En la Observación 4.2.10, hemos visto que $w_M(x) = d^*(A_x)$, siendo A_x un vector testigo de la matriz M tal que $A_x = (a'_0, \ldots, a'_{r_x-1})$ con $a'_i = 0$ si $f_M(i) = 0$ y $a'_i = 1$ si $f_M(i) \neq 0$. Puesto que $f_M(i) = M(g_{x,i}) = M(a_i \cdot b(y))\ \forall i \in \{0, \ldots, r_y - 1\}$, tenemos que $a'_i = 0$ si $a_i = 0$ y $a'_i = 1$ si $a_i \neq 0$. Por lo tanto, $supp(A_x) = supp(M(a))$, lo que implica que $w_M(y) = d^*(A_x) = d^*(M(a))$. Análogamente podemos ver $\varepsilon_M(y) = d^*(M(a))$ y $w_M(y) = d^*(M(b))$.

Como ya hemos demostrado los puntos (4.) y (5.) se cumple la siguiente igualdad

$$\begin{aligned} sd^*_x(M) = \varepsilon_M(x) \cdot w_M(x) &= d^*(M(b)) \cdot d^*(M(a)) \\ &= w_M(y) \cdot \varepsilon_M(y) = sd^*_y(M), \end{aligned}$$

que implica $sd^*(M) = sd^*_x(M) = sd^*_y(M) = \varepsilon_M(y) \cdot w_M(y) = d^*(M(a)) \cdot d^*(M(b))$. Para demostrar los puntos (3.) y (4.) nos basta ver $d^*(M(a)) \cdot d^*(M(b)) = \left|\overline{Z(g)}\right|$. Como a cumple la Proposición 3.0.3, tenemos que $d^*(M(a)) = n - deg(m_a) = \left|\overline{Z(a)}\right|$. Análogamente tenemos que $d^*(M(b)) = \left|\overline{Z(b)}\right|$. Así, por el punto (1.), tenemos

que $d^*(M(a)) \cdot d^*(M(b)) = \left|\overline{Z(a)}\right| \cdot \left|\overline{Z(b)}\right| = \left|\overline{Z(g)}\right|$. ■

Usando la Proposición 4.3.9 y la Proposición 4.3.11 seremos capaces de construir códigos abelianos C tales que $d(C) = sd^*(C)$. Para ello necesitamos definir primero un nuevo tipo de matriz.

Definición 4.3.12 *Una matriz P de orden $r_y \times r_y$ con entradas en $\mathbb{L}$ se denomina una matriz polinómica compuesta o CP-matriz, si existen polinomios $a = a(x) \in \mathbb{L}(r_x)$ y $b = b(y) \in \mathbb{L}(r_y)$ tales que $P = M(ab)$, con $ab \in \mathbb{L}(r_x, r_y)$. Los polinomios a y b se denominan los factores polinómicos de P.*

Observación 4.3.13 *Sea P una CP-matriz con $P = M(ab)$. Veamos que $\pi_x(supp(P)) = supp(M(a))$. Siguiendo el mismo razonamiento que hemos utilizado en la demostración de los puntos* (4.) *y* (5.) *de la Proposición 4.3.11, tenemos que $c_P(j) = M(b)$ $\forall j \in \{0, \ldots, r_y - 1\}$ con $c_P(j) \neq 0$. Ahora, sean $i \in \pi_x(supp(P))$ y $j \in \{0, \ldots, r_y - 1\}$ tal que $(i, j) \in supp(M)$. Entonces, $i \in supp(c_P(j))$ con $c_P(j) \neq 0$, lo que implica $i \in supp(M(a))$. Por otro lado, sea $i \in supp(M(a))$. Esto implica que $i \in supp(c_P(j))$ $\forall j \in \{0, \ldots, r_y - 1\}$ con $c_P(j) \neq 0$. Sea $j' \in \{0, \ldots, r_y - 1\}$ tal que $c_M(j') \neq 0$. Entonces $(i, j') \in supp(P)$ y por lo tanto $i \in \pi_x(supp(P))$. Análogamente podemos ver que $\pi_y(supp(P)) = supp(M(b))$.*

Observación 4.3.14 *Sea P una CP-matriz con $P = M(ab)$. Veamos que $supp(P) = \pi_x(supp(P)) \times \pi_y(supp(P))$. Es inmediato ver que $supp(P) \subseteq \pi_x(supp(P)) \times \pi_y(supp(P))$, por lo tanto, basta ver $\pi_x(supp(P)) \times \pi_y(supp(P)) \subseteq supp(P)$. Sea $(i, j) \in \pi_x(supp(P)) \times \pi_y(supp(P))$. Puesto que $j \in \pi_y(supp(P))$ tenemos que $c_P(j) \neq 0$. Por otro lado,*

$$i \in \pi_x(supp(P)) \underset{\text{Observación 4.3.13}}{=} \pi_x(supp(M(a))) \underset{c_P(j) \neq 0}{=} supp(c_P(j)),$$

lo que implica que $(i, j) \in supp(P)$.

En la observación anterior hemos visto que si P es una CP-matriz entonces $supp(P) = \pi_x(supp(P)) \times \pi_y(supp(P))$. En el siguiente ejemplo mostramos que la implicación contraria no tiene por qué cumplirse.

Ejemplo 4.3.15 *Sea $q = 3$,$r_x = 5$,$r_y = 3$ y sea P la siguiente*

matriz

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

Tenemos que $supp(P) = \{(0,0),(3,0),(0,6),(3,6)\}$, $\pi_x(supp(P)) = \{0,3\}$ *y* $\pi_y(supp(P)) = \{0,6\}$, *por lo que* $supp(P) = \pi_x(supp(P)) \times \pi_y(supp(P))$. *Supongamos que* $P = M(ab)$ *con* $a = a(x)$ *y* $b = b(y)$. *Sea*

$$a(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4,$$

$$b(y) = b_0 + b_1y + b_2y^2 + b_3y^3 + b_4y^4 + b_5^5 + b_6y^6.$$

Para que se cumpla $P = M(ab)$ *se tienen que dar las siguientes igualdades*

$$a_0b_0 = 1,$$

$$a_3b_0 = 1,$$

$$a_0b_6 = 1,$$

$$a_3 = b_6 = 2,$$

$$a_1 = a_2 = a_4 = 0,$$

$$b_1 = b_2 = b_3 = b_4 = b_5 = 0.$$

De las primeras tres igualdades obtenemos que $a_0 = b_0 = a_3 = b_6$, *lo que implica que* $a_3b_6 = 1$ *que es una contradicción. Por lo tanto* P *no es una CP-matriz.*

Corolario 4.3.16 *Sea* $P = M(g)$, *con* $g(x,y) = a(x)b(y)$, *una CP-matriz. Si* $\overline{x^{h_x}a} \mid x^{r_x} - 1$ *y* $\overline{y^{h_y}b} \mid y^{r_y} - 1$ *para ciertos* $h_x \in \{0,\dots,r_x - 1\}$, $h_y \in \{0,\dots,r_y - 1\}$, *entonces*

1. $\overline{Z(ab)} = \overline{Z(a)} \times \overline{Z(b)}$.
2. $sd^*(P) = d^*(M(a)) \cdot d^*(M(b)) = \left|\overline{Z(g)}\right|$.
3. $sd^*(P) = sd_x^*(P) = sd_y^*(P) = \left|\overline{Z(g)}\right|$.
4. $d^*(M(a)) = \varepsilon_P(y) = w_P(x)$.

5. $d^*(M(b)) = \varepsilon_P(x) = w_P(y)$.

Demostración. Tenemos que $P = M(g)$, con $g(x,y) = a(x)b(y)$. Puesto que $\overline{x^{h_x}a} \mid x^{r_x} - 1$ y $\overline{y^{h_y}b} \mid y^{r_y} - 1$ para ciertos $h_x \in \{0, \ldots, r_x - 1\}$, $h_y \in \{0, \ldots, r_y - 1\}$, tenemos que a y b satisfacen la Proposición 3.0.3. Puesto que se cumplen las hipótesis de la Proposición 4.3.11 basta aplicarla para concluir la demostración. ■

En el siguiente ejemplo mostramos que las condiciones que tienen que cumplir los polinomios a y b del corolario anterior no son superfluas.

Ejemplo 4.3.17 *Sea $q = 2$, $r_x = 5$ y $r_y = 7$. Sea P la CP-matriz con factores polinómicos $a = x+x^2+x^3+x^4$, $b = y+y^2+y^4$. Se puede comprobar que $\overline{y^6b} \mid y^7 - 1$ pero $\overline{x^{h_x}a} \nmid x^5 - 1\ \forall h_x \in \{0, \ldots, r_x - 1\}$. Tenemos que $M(a) = (01111)$ y por lo tanto $d^*(M(a)) = 2$ y que $M(b) = (0110100)$ y así $d^*(M(b)) = 4$. Calculemos ahora $sd^*(P) = sd^*(M(ab))$. Como*

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

es fácil comprobar que $sd_x^*(M) = 4 \cdot 2 = 8$ y que $sd_y^*(M) = 2 \cdot 4 = 8$. Así, tenemos que $sd^*(P) = d^*(M(a)) \cdot sd^*(M(b))$ y que $sd^*(P) = sd_x^*(P) \cdot sd_y^*(P)$, pero, se puede comprobar que $\left|\overline{Z(ab)}\right| = 16$, por lo que los puntos (2.) *y* (3.) *del Corolario 4.3.16 no se cumplen.*

Veamos ahora un método para construir códigos abelianos en los que su distancia mínima coincide con su distancia aparente fuerte. Para ello necesitamos el siguiente lema técnico.

Lema 4.3.18 *Sea $D \subset \mathbb{Z}_{r_x} \times \mathbb{Z}_{r_y}$ una unión de q-órbitas y $M = M(D)$ la matriz dada por D. Si $supp(M) = \pi_x(supp(M)) \times \pi_y(supp(M))$ entonces $sd^*(M) = msd(M)$.*

Demostración. Por la demostración de la Proposición 4.3.11, si M es una CP-matriz todas las filas y columnas cuyo soporte es

distinto de cero son filas y columnas involucradas. Si $d^*(f_M(i)) = d^*(M(b)) = 1\ \forall i \in \{0,\dots,r_x-1\}$ o $d^*(c_M(i)) = d^*(M(a)) = 1\ \forall j \in \{0,\dots,r_y-1\}$, por el paso $(2a)$ del Algoritmo 4.2.30,tenemos que $msd(M) = sd^*(M)$. Si $d^*(M(b)) \neq 1$ y $d^*(M(a)) \neq 1$, por el paso $(2b)$ del Algoritmo 4.2.30 y puesto que todas las filas y columnas con soporte no nulo son filas involucradas, tenemos que $M_1 = 0$. Esto implica que $sd^*(M) = msd(M)$. ■

Teorema 4.3.19 *Sea $a = a(x) \in \mathbb{L}(r_x)$ y $b = b(y) \in \mathbb{L}(r_y)$ tales que $a \mid x^{r_x} - 1$ y $b \mid y^{r_y} - 1$. Si existen $(\alpha_x, \alpha_y) \in U$, $h_x \in \mathbb{Z}_{r_x}$ y $h_y \in \mathbb{Z}_{r_y}$ para los cuales $\varphi^{-1}_{\alpha_x, \overline{x^{h_x}a}} \in \mathbb{F}_q(r_x)$ y $\varphi^{-1}_{\alpha_y, \overline{y^{h_y}b}} \in \mathbb{F}_q(r_y)$, entonces el código abeliano $C = \left\langle \varphi^{-1}_{\alpha_x, \overline{x^{h_x}a}} \cdot \varphi^{-1}_{\alpha_y, \overline{y^{h_y}b}} \right\rangle$ en $\mathbb{F}_q(r_x, r_y)$ verifica $sd^*(M(ab)) = sd^*(C) = d(C)$.*

Mas aún, en ese caso, para cualquier $\beta_x \in U_{r_x}$ y $\beta_y \in U_{r_y}$ el código abeliano $C_{(\beta_x,\beta_y)} = \left\langle \varphi^{-1}_{\beta_x, \overline{x^{h_x}a}} \cdot \varphi^{-1}_{\beta_y, \overline{y^{h_y}b}} \right\rangle$ verifica $sd^*(M(ab)) = sd^*(C_{(\beta_x,\beta_y)}) = d(C_{(\beta_x,\beta_y)}) = d(C)$.

Demostración. Sea $g(x,y) = \overline{x^{h_x}a(x) \cdot y^{h_y}b(y)}$ y $\alpha = (\alpha_x, \alpha_y)$. Por definición de la inversa de la transformada de Fourier discreta,

$$\begin{aligned}\varphi^{-1}_{g,\alpha} &= \frac{1}{r_x r_y} \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} g(\alpha^{-(i,j)}) Z^{(i,j)} \\ &= \frac{1}{r_x r_y} \sum_{(i,j)\in\mathbb{Z}_{r_x}\times\mathbb{Z}_{r_y}} \overline{x^{h_x}(\alpha_x^{-i})a(\alpha_x^{-i})x^i \cdot y^{h_y}(\alpha_y^{-j})b(\alpha_y^{-j})} y^j \\ = \frac{1}{r_x} \sum_{i\in\mathbb{Z}_{r_x}} \overline{x^{h_x}(\alpha_x^{-i})a(\alpha_x^{-i})} x^i \cdot \frac{1}{r_y} \sum_{j\in\mathbb{Z}_{r_y}} \overline{y^{h_y}(\alpha_y^{-j})a(\alpha_y^{-j})} y^j &= \varphi^{-1}_{\alpha_x, \overline{x^{h_x}a}} \cdot \varphi^{-1}_{\alpha_y, \overline{y^{h_y}b}}\end{aligned}$$

Por otro lado $M(g)$ es una CP-matriz que satisface las hipótesis del Corolario 4.3.16 y por lo tanto, $sd^*(M(g)) = \left|\overline{Z(g)}\right|$, es decir, cumple la condición $(2b.)$ del Teorema 4.3.1.

Sea M la matriz dada por $D_\alpha(C)$. Puesto que $C =< \varphi^{-1}_{\alpha,g} >$ entonces $supp(M) = supp(M(g))$. Por el Lema 4.3.18 , $msd(M) = sd^*(M)$ y por lo tanto se cumple la condición $(2a.)$ del Teorema 4.3.1. Así, puesto que g cumple las dos condiciones del Teorema 4.3.1, tenemos que $d(C) = sd^*(C)$. La última afirmación es cierta por el punto (4.) de la Observación 1.0.8 junto con el hecho de que,

bajo las hipótesis del corolario, todas las matrices dadas por este tipo de conjuntos de definición son CP-matrices. ■

Corolario 4.3.20 *Sea* $a = a(x) \in \mathbb{L}(r_x)$ *y* $b = b(y) \in \mathbb{L}(r_y)$ *tales que* $a \mid x^{r_x} - 1$ *y* $b \mid y^{r_y} - 1$. *Si existen* $(\alpha_x, \alpha_y) \in U$, $h_x \in \mathbb{Z}_{r_x}$ *y* $h_y \in \mathbb{Z}_{r_y}$ *para los cuales* $\left[\left(\overline{x^{h_x}a}(\alpha_x^i)\right)\right]^q = \overline{x^{h_x}a}(\alpha_x^i)\ \forall i \in \{0, \ldots, r_x - 1\}$ *y* $\left[\left(\overline{y^{h_y}b}(\alpha_y^j)\right)\right]^q = \overline{y^{h_y}b}(\alpha_y^j)\ \forall j \in \{0, \ldots, r_y - 1\}$ *entonces la familia de códigos abelianos*

$$\left\{C_{(\beta_1,\beta_2)} = \left\langle \varphi^{-1}_{\beta_x, \overline{x^{h_x}a}} \cdot \varphi^{-1}_{\beta_y, \overline{y^{h_y}b}} \right\rangle \mid \beta_x \in U_{r_x} \text{ y } \beta_2 \in U_{r_y}\right\}$$

en $\mathbb{F}_q(r_x, r_y)$ *verifica que* $sd^*(M(ab)) = sd^*(C_{(\beta_1,\beta_2)}) = d(C_{(\beta_1,\beta_2)})$.

Demostración. Por el punto (3.) de la Observación 1.0.8 tenemos que $\varphi^{-1}_{\alpha_x, \overline{x^{h_x}a}} \in \mathbb{F}_q(r_x)$ y $\varphi^{-1}_{\alpha_y, \overline{y^{h_y}b}} \in \mathbb{F}_q(r_y)$ y por lo tanto se cumplen las hipótesis del Teorema 4.3.19. ■

En el siguiente ejemplo vemos cómo usar este último corolario.

Ejemplo 4.3.21 *Sea* $q = 2$, $r_x = 3$, $r_y = 45$. *Sea* $\alpha_x \in U_3$ *y* $\alpha_y \in U_{45}$. *Tomamos los polinomios* $a = x + 1$ *y* $b = y^{40} + y^{39} + y^{38} + y^{36} + y^{35} + y^{32} + y^{30} + y^{25} + y^{24} + y^{23} + y^{21} + y^{20} + y^{17} + y^{15} + y^{10} + y^9 + y^8 + y^6 + y^5 + y^2 + 1$.

Tenemos que $a \mid x^3 - 1$. *Si tomamos* $h_x = 1$, $supp(x \cdot a(x)) = \{1, 2\} = C_2(1)$. *Entonces, por el Lema 3.0.8 y por la Observación 1.0.8, tenemos que* $\varphi^{-1}_{\alpha_x, xa} \in \mathbb{F}_q(2)$. *Por otro lado, el polinomio* b *es el mismo que hemos utilizado en el Ejemplo 3.0.12, en el cual hemos visto que si tomamos* $h_y = 5$, $\varphi^{-1}_{\alpha_y, y^5 b} \in \mathbb{F}_q(45)$. *Sea* $C = < \varphi^{-1}_{\alpha_x, xa} \cdot \varphi^{-1}_{\alpha_y, y^5 b} > \subset \mathbb{F}_2(3, 45)$, *con* $D_{\alpha_x, \alpha_y}(C) = C_2(1) \times (C_2(1) \cup C_2(3) \cup C_2(9) \cup C_2(21))$. *Se puede comprobar que* $sd^*(M(ab)) = 10$ *y por lo tanto* $d(C) = 10$.

Bibliografía

[1] F.J. Macwilliams and N.J.A Sloane, *The Theory of Error-Correcting Codes*, North-Holland,1977.

[2] W.C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, 2003.

[3] D.H. Bueno-Carreño, J.J. Bernal, and J.J. Simón, *Cyclic and BCH codes whose minimun distances equals their maximun BCH bound*. Advances in Mathematics of Communications 10(2016), 459-474

[4] J.J Bernal, D.H. Bueno-Carreño, J.J. Simón, *Apparent distance and a notion of BCH multivariate codes*. IEEE Transactions on Information Theory, **62**(2) (2016), 655-668.

[5] J.J. Bernal, M. Gerreiro, and J.J. Simón, *From ds-bounds for cyclic codes to true minimus distance for abelian codes*. IEEE Transactions on Information Theory.

[6] D.H. Bueno-Carreño. *Cálculo de la Distancia Aparente de Códigos Abelianos. Códigos BCH Multivariables.*