# Códigos usando divisores de cero y unidades en anillos de grupo

Seminario de Álgebra

Autor:

**Oscar Andrés Suárez Porras**

Director:

**Prof. Alexander Holguín Villa**

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga, mayo 8 de 2018

# Contenido

# Introducción

El presente trabajo está basado en el artículo "**Codes from zero-divisors and units in group rings**" de los investigadores Paul Hurley y Ted Hurley.

Un nuevo método para la construcción de códigos usando codificaciones desde anillos de grupos será presentado. Consisten en dos tipos: los códigos divisores de cero y los códigos derivados de unidades. Los códigos procedentes de anillos de grupo se centraron en ideales; por ejemplo, los códigos cíclicos son ideales en el anillo de grupo sobre un grupo cíclico.

# Introducción

El presente trabajo está basado en el artículo "**Codes from zero-divisors and units in group rings**" de los investigadores Paul Hurley y Ted Hurley.

Un nuevo método para la construcción de códigos usando codificaciones desde anillos de grupos será presentado. Consisten en dos tipos: los códigos divisores de cero y los códigos derivados de unidades. Los códigos procedentes de anillos de grupo se centraron en ideales; por ejemplo, los códigos cíclicos son ideales en el anillo de grupo sobre un grupo cíclico.

El uso de un isomorfismo entre los anillos de grupo y un determinado anillo bien definido de matrices; se tiene que cada elemento del anillo de grupo es asociado a una matriz, haciendo posible la construcción de las matrices generadora y de verificación.

Los anillos de grupo son una fuente rica de unidades y divisores de cero, de los cuales nuevos códigos resultan. Muchas propiedades del código pueden expresarse fácilmente en términos de propiedades del anillo de grupo.

# Anillos de grupo y matrices

Sean $R$ un anillo con unidad $1_R$ y $G$ un grupo multiplicativo no necesariamente finito, se denota por $RG$ al conjunto de las sumas formales finitas $\mathbf{a} = \sum_{g \in G} \alpha_g g$, es decir,

$$RG = \left\{ \mathbf{a} = \sum_{g \in G} \alpha_g g : \alpha_g \in R, g \in G \right\},$$

donde $\alpha_g = 0$ casi siempre, esto es, solo un número finito de coeficientes son diferentes de cero en cada una de estas sumas. Este conjunto $RG$ es un anillo.

# Anillos de grupo y matrices

Sean $R$ un anillo con unidad $1_R$ y $G$ un grupo multiplicativo no necesariamente finito, se denota por $RG$ al conjunto de las sumas formales finitas $\mathbf{a} = \sum_{g \in G} \alpha_g g$, es decir,

$$RG = \left\{ \mathbf{a} = \sum_{g \in G} \alpha_g g : \alpha_g \in R, g \in G \right\},$$

donde $\alpha_g = 0$ casi siempre, esto es, solo un número finito de coeficientes son diferentes de cero en cada una de estas sumas. Este conjunto $RG$ es un anillo.

**Recordar:** Dado $R$ un anillo tenemos que:

1. $0 \neq z \in \mathcal{ZD}(R) \Leftrightarrow \exists 0 \neq r \in R$ tal que $zr = 0$.
2. Si $1 \in R$, $u \in \mathcal{U}(R) \Leftrightarrow \exists v \in R$ tal que $uv = vu = 1$.

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de $G$:

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de $G$:

$$RG \ni v = \sum_{i=1}^{n} \alpha_{g_i} g_i \underbrace{\Leftrightarrow}_{\varphi - iso} V \in \mathcal{M}_{RG}(R) \subset \mathcal{M}_n(R),$$

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de $G$:

$$RG \ni v = \sum_{i=1}^{n} \alpha_{g_i} g_i \underbrace{\Leftrightarrow}_{\varphi - iso} V \in \mathcal{M}_{RG}(R) \subset \mathcal{M}_n(R),$$

donde

$$V = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de $G$:

$$RG \ni v = \sum_{i=1}^{n} \alpha_{g_i} g_i \underbrace{\Leftrightarrow}_{\varphi - iso} V \in \mathcal{M}_{RG}(R) \subset \mathcal{M}_n(R),$$

donde

$$V = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

El conjunto $\mathcal{M}_{RG}(R)$ es llamado el conjunto de las $RG$-matrices.

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de $G$:

$$RG \ni v = \sum_{i=1}^{n} \alpha_{g_i} g_i \underbrace{\Leftrightarrow}_{\varphi - iso} V \in \mathcal{M}_{RG}(R) \subset \mathcal{M}_n(R),$$

donde

$$V = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

El conjunto $\mathcal{M}_{RG}(R)$ es llamado el conjunto de las $RG$-matrices.

**Teorema**

*Sea $R$ un cuerpo. $\mathbf{0} \neq \mathbf{u} \in \mathcal{ZD}(RG) \Leftrightarrow det(\varphi(\mathbf{u})) = 0$, en caso contrario $\mathbf{u}$ es una unidad.*

Para ello se necesitan los siguientes resultados.

Para ello se necesitan los siguientes resultados.

**Teorema**

*Suponga que $R$ tiene identidad. Entonces $\mathbf{u} \in RG$ es unidad si y sólo si $\varphi(\mathbf{u})$ es una unidad en $\mathcal{M}_n(R)$.*

Para ello se necesitan los siguientes resultados.

**Teorema**

*Suponga que $R$ tiene identidad. Entonces $\mathbf{u} \in RG$ es unidad si y sólo si $\varphi(\mathbf{u})$ es una unidad en $\mathcal{M}_n(R)$.*

**Corolario**

*Cuando $R$ es conmutativo, $\mathbf{u}$ es unidad en $RG \Leftrightarrow \varphi(\mathbf{u})$ es unidad en $\mathcal{M}_n(R)$ $\Leftrightarrow det(\varphi(\mathbf{u}))$ es unidad en $R$.*

Para ello se necesitan los siguientes resultados.

**Teorema**

*Suponga que $R$ tiene identidad. Entonces $\mathbf{u} \in RG$ es unidad si y sólo si $\varphi(\mathbf{u})$ es una unidad en $\mathcal{M}_n(R)$.*

**Corolario**

*Cuando $R$ es conmutativo, $\mathbf{u}$ es unidad en $RG \Leftrightarrow \varphi(\mathbf{u})$ es unidad en $\mathcal{M}_n(R)$ $\Leftrightarrow det(\varphi(\mathbf{u}))$ es unidad en $R$.*

**Corolario**

*Cuando $R$ es cuerpo, $\mathbf{z}$ es un divisor de cero en $RG \Leftrightarrow \varphi(\mathbf{z})$ es un divisor de cero en $\mathcal{M}_n(R) \Leftrightarrow det(\varphi(\mathbf{z})) = 0$.*

Sea $RG$ como antes, $G = \{g_1 g_2, \ldots, g_n\}$. Supongamos que $W$ es un submódulo de $RG$ y sea $\mathbf{u} \in RG$ dado.

Sea $RG$ como antes, $G = \{g_1 g_2, \ldots, g_n\}$. Supongamos que $W$ es un submódulo de $RG$ y sea $\mathbf{u} \in RG$ dado.

## Definición

*Sea $\mathbf{x} \in W$. Una **codificación de anillo de grupo** es una aplicación $\rho : W \to RG$, tal que $\rho(\mathbf{x}) = \mathbf{xu}$ o $\rho(\mathbf{x}) = \mathbf{ux}$. En el segundo caso, $\rho$ es una **codificación de anillo de grupo a izquierda**, y en el primero, una **codificación de anillo de grupo a derecha**.*

Sea $RG$ como antes, $G = \{g_1 g_2, \ldots, g_n\}$. Supongamos que $W$ es un submódulo de $RG$ y sea $\mathbf{u} \in RG$ dado.

**Definición**

*Sea $\mathbf{x} \in W$. Una **codificación de anillo de grupo** es una aplicación $\rho : W \to RG$, tal que $\rho(\mathbf{x}) = \mathbf{xu}$ o $\rho(\mathbf{x}) = \mathbf{ux}$. En el segundo caso, $\rho$ es una **codificación de anillo de grupo a izquierda**, y en el primero, una **codificación de anillo de grupo a derecha**.*

Un código $\mathcal{C}$ derivado de una codificación de anillo de grupo es entonces la imagen de una codificación de anillo de grupo, es decir, para $\mathbf{u} \in RG$ dado y $W$ un submódulo de $RG$, $\mathcal{C} = \{\mathbf{ux} : \mathbf{x} \in W\}$ o $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$.

Dado que el anillo de grupo $RG$ no es necesariamente conmutativo, entonces permitir grupos $G$ no conmutativos, posibilita la construcción de códigos no conmutativos. En el caso que $\mathbf{xu} = \mathbf{ux}$ para todo $\mathbf{x} \in W$, $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ es llamado código conmutativo.

# Códigos desde divisores de cero

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código divisor de cero**.

# Códigos desde divisores de cero

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código divisor de cero**.

En la práctica, el submódulo $W$ tiene dimensión $r < n$. Este puede tener la base $\{g_1, g_2, \ldots, g_r\}$. Otros submódulos también resultan útiles, como el generado por $\{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\}$ con $1 \leq t < n$ donde $\{k_1, k_2, \ldots, k_t\} \subseteq \{1, 2, \ldots, n\}$. Por lo tanto, el código va a tener longitud $n$ y su dimensión dependerá de la elección del submódulo $W$.

# Códigos desde divisores de cero

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código divisor de cero**.

En la práctica, el submódulo $W$ tiene dimensión $r < n$. Este puede tener la base $\{g_1, g_2, \ldots, g_r\}$. Otros submódulos también resultan útiles, como el generado por $\{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\}$ con $1 \leq t < n$ donde $\{k_1, k_2, \ldots, k_t\} \subseteq \{1, 2, \ldots, n\}$. Por lo tanto, el código va a tener longitud $n$ y su dimensión dependerá de la elección del submódulo $W$.

Si la codificación es a derecha, el código divisor de cero es dado por $\mathcal{C} = W\mathbf{u}$, decimos que $\mathbf{u}$ es un elemento generador relativo al submódulo $W$.

# Códigos desde divisores de cero

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código divisor de cero**.

En la práctica, el submódulo $W$ tiene dimensión $r < n$. Este puede tener la base $\{g_1, g_2, \ldots, g_r\}$. Otros submódulos también resultan útiles, como el generado por $\{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\}$ con $1 \leq t < n$ donde $\{k_1, k_2, \ldots, k_t\} \subseteq \{1, 2, \ldots, n\}$. Por lo tanto, el código va a tener longitud $n$ y su dimensión dependerá de la elección del submódulo $W$.

Si la codificación es a derecha, el código divisor de cero es dado por $\mathcal{C} = W\mathbf{u}$, decimos que $\mathbf{u}$ es un elemento generador relativo al submódulo $W$.

El caso cuando $W\mathbf{u} = RG\mathbf{u}$ es el caso clásico particular cuando el código es un ideal a la izquierda, al mismo tiempo, $rank(U) = rank(W\mathbf{u})$.

# Códigos desde divisores de cero

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código divisor de cero**.

En la práctica, el submódulo $W$ tiene dimensión $r < n$. Este puede tener la base $\{g_1, g_2, \ldots, g_r\}$. Otros submódulos también resultan útiles, como el generado por $\{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\}$ con $1 \leq t < n$ donde $\{k_1, k_2, \ldots, k_t\} \subseteq \{1, 2, \ldots, n\}$. Por lo tanto, el código va a tener longitud $n$ y su dimensión dependerá de la elección del submódulo $W$.

Si la codificación es a derecha, el código divisor de cero es dado por $\mathcal{C} = W\mathbf{u}$, decimos que $\mathbf{u}$ es un elemento generador relativo al submódulo $W$.

El caso cuando $W\mathbf{u} = RG\mathbf{u}$ es el caso clásico particular cuando el código es un ideal a la izquierda, al mismo tiempo, $rank(U) = rank(W\mathbf{u})$.

Cuando $\mathbf{u} \in \mathcal{ZD}(RG)$, entonces existe $\mathbf{0} \neq \mathbf{v} \in RG$ con $\mathbf{uv} = \mathbf{0}$ y así, $\mathbf{y} \in \mathcal{C}$ satisface $\mathbf{yv} = \mathbf{0}$.

Puede suceder que dicho elemento $\mathbf{v}$ también determine el código, caso donde $\mathbf{uv} = \mathbf{0}$ y $rank(U) + rank(V) = n = |G|$.

## Definición

*$\mathbf{v} \in RG$ es llamado un **elemento de verificación** para un código divisor de cero $\mathcal{C}$ si satisface que $\mathbf{y} \in \mathcal{C}$ si y sólo si $\mathbf{yv} = \mathbf{0}$. El código puede entonces ser escrito $\mathcal{C} = \{\mathbf{y} \in RG : \mathbf{yv} = \mathbf{0}\}$.*

## Definición

$\mathbf{v} \in RG$ *es llamado un* ***elemento de verificación*** *para un código divisor de cero* $\mathcal{C}$ *si satisface que* $\mathbf{y} \in \mathcal{C}$ *si y sólo si* $\mathbf{yv} = \mathbf{0}$. *El código puede entonces ser escrito* $\mathcal{C} = \{\mathbf{y} \in RG : \mathbf{yv} = \mathbf{0}\}$.

## Definición

*Un subconjunto de elementos* $T \subset RG$, *es llamado* ***linealmente independiente (L.I.)*** *si, para* $\alpha_{\mathbf{x}} \in R$, $\sum_{\mathbf{x} \in T} \alpha_{\mathbf{x}} \mathbf{x} = 0$, *solo cuando* $\alpha_{\mathbf{x}} = 0$ *para todo* $\mathbf{x} \in T$. *En caso contrario,* $T$ *es* ***linealmente dependiente (L.D.)***. *Definimos el* $\mathbf{rank}(T)$ *como el número máximo de elementos* ***L.I.*** *de* $T$. *Así,* $\mathbf{rank}(T) = |T|$ *si y sólo si* $T$ *es un conjunto* ***L.I.***.

## Definición

$\mathbf{v} \in RG$ *es llamado un* ***elemento de verificación*** *para un código divisor de cero* $\mathcal{C}$ *si satisface que* $\mathbf{y} \in \mathcal{C}$ *si y sólo si* $\mathbf{yv} = \mathbf{0}$. *El código puede entonces ser escrito* $\mathcal{C} = \{\mathbf{y} \in RG : \mathbf{yv} = \mathbf{0}\}$.

## Definición

*Un subconjunto de elementos* $T \subset RG$, *es llamado* ***linealmente independiente (L.I.)*** *si, para* $\alpha_{\mathbf{x}} \in R$, $\sum_{\mathbf{x} \in T} \alpha_{\mathbf{x}} \mathbf{x} = 0$, *solo cuando* $\alpha_{\mathbf{x}} = 0$ *para todo* $\mathbf{x} \in T$. *En caso contrario,* $T$ *es* ***linealmente dependiente (L.D.)***. *Definimos el* $\mathbf{rank}(T)$ *como el número máximo de elementos* ***L.I.*** *de* $T$. *Así,* $\mathbf{rank}(T) = |T|$ *si y sólo si* $T$ *es un conjunto* ***L.I.***.

## Observación

Note que un código divisor de cero $\mathcal{C} = W\mathbf{u}$, donde $W = \langle S \rangle$ es el submódulo de $RG$, consiste de todos los elementos de la forma $\sum_{g \in S} \alpha_g g\mathbf{u}$, luego

$dim(W\mathbf{u}) = \mathbf{rank}(S\mathbf{u})$.

La dimensión máxima de un código para un divisor cero dado $\mathbf{u}$ es $r = \mathbf{rank}(G\mathbf{u})$. Los códigos divisores de cero son así $(n, k)$-códigos donde $k = \mathbf{rank}(S\mathbf{u})$ y $k \leq r = \mathbf{rank}(G\mathbf{u})$.

La dimensión máxima de un código para un divisor cero dado $\mathbf{u}$ es $r = \mathbf{rank}(G\mathbf{u})$. Los códigos divisores de cero son así $(n, k)$-códigos donde $k = \mathbf{rank}(S\mathbf{u})$ y $k \leq r = \mathbf{rank}(G\mathbf{u})$.

## Observación

Un $(n, t)$ código divisor cero puede ser encontrado obteniendo $t$ filas linealmente independientes $i_1, i_2, \ldots, i_t$ de $U$. Luego, $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_t}\}$ es tal que $S\mathbf{u}$ es linealmente independiente y genera un $(n, t)$-código.
Decir que $S\mathbf{u}$ linealmente independiente equivale a decir que $W$ no contiene divisores de cero de $\mathbf{u}$.

La dimensión máxima de un código para un divisor cero dado $\mathbf{u}$ es $r = \mathbf{rank}(G\mathbf{u})$. Los códigos divisores de cero son así $(n, k)$-códigos donde $k = \mathbf{rank}(S\mathbf{u})$ y $k \leq r = \mathbf{rank}(G\mathbf{u})$.

## Observación

Un $(n, t)$ código divisor cero puede ser encontrado obteniendo $t$ filas linealmente independientes $i_1, i_2, \ldots, i_t$ de $U$. Luego, $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_t}\}$ es tal que $S\mathbf{u}$ es linealmente independiente y genera un $(n, t)$-código.
Decir que $S\mathbf{u}$ linealmente independiente equivale a decir que $W$ no contiene divisores de cero de $\mathbf{u}$.

## Ejemplo

Sea $RG$ el anillo de grupo donde $R$ es cuerpo y $G = C_n = \langle g : g^n = 1 \rangle$ el grupo cíclico de orden $n$. Supongamos que $\mathbf{u} \in RG$ es un divisor de cero. Sea $r \in \mathbb{N}$ el primer valor tal que el conjunto $\{\mathbf{u}, g\mathbf{u}, g^2\mathbf{u}, \ldots, g^r\mathbf{u}\}$ es linealmente dependiente. Luego $r$ es igual al $\mathbf{rank}(U)$ y el conjunto $S = \{1, g, g^2, \ldots, g^{r-1}\}$, genera $W$.

## Independencia lineal

La relación entre filas linealmente independientes (dependientes) de la $RG$-matriz $U$ y la independencia (dependencia) lineal del conjunto $S\mathbf{u}$ será evidenciada.

Suponga que $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_r}\} \subset \{g_1, g_2, \ldots, g_n\} = G$ y que $U$ es obtenida de esta lista de $G$. Tenemos:

## Independencia lineal

La relación entre filas linealmente independientes (dependientes) de la $RG$-matriz $U$ y la independencia (dependencia) lineal del conjunto $S\mathbf{u}$ será evidenciada.

Suponga que $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_r}\} \subset \{g_1, g_2, \ldots, g_n\} = G$ y que $U$ es obtenida de esta lista de $G$. Tenemos:

**Teorema**

1. *Suponga* $\mathbf{rank}(U) = t$. *Sea* $S \subset G$ *un conjunto de elementos de grupo tal que* $\mid S \mid = t + 1$. *Entonces,* $S\mathbf{u}$ *es linealmente dependiente.*
2. *Suponga que* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_s$ *son las primeras filas (o primeras columnas) de las* $RG$*-matrices* $U_1, U_2, \ldots, U_s$ *respectivamente. Entonces* $\alpha_1\underline{u}_1 + \alpha_1\underline{u}_2 + \ldots + \alpha_s\underline{u}_s = 0_{1\times n}$ *si y sólo si* $\alpha_1 U_1 + \alpha_1 U_2 + \ldots + \alpha_s U_s = 0_{n\times n}$.
3. $S\mathbf{u} = \{g_{i_1}\mathbf{u}, g_{i_2}\mathbf{u}, \ldots, g_{i_r}\mathbf{u}\}$ *es linealmente independiente si y sólo si* $\{\underline{u}_{i_1}, \underline{u}_{i_2}, \ldots, \underline{u}_{i_r}\}$ *es linealmente independiente.*

## Códigos dual y autodual

Por definición, el dual de un código $\mathcal{C}$, denotado por $\mathcal{C}^{\perp}$, considerado como vectores sobre $R^n$ es su complemento ortogonal, es decir

$$\mathcal{C}^{\perp} = \{v \in R^n : v \cdot u = 0, \forall u \in \mathcal{C}\}.$$

## Códigos dual y autodual

Por definición, el dual de un código $\mathcal{C}$, denotado por $\mathcal{C}^{\perp}$, considerado como vectores sobre $R^n$ es su complemento ortogonal, es decir

$$\mathcal{C}^{\perp} = \{v \in R^n : v \cdot u = 0, \forall u \in \mathcal{C}\}.$$

Sean $\mathbf{x} = \sum_{g \in G} \alpha_g g$, $\mathbf{y} = \sum_{h \in G} \beta_h h \in RG$. El producto interno o punto de $\mathbf{x}$ e $\mathbf{y}$ es dado por la expresión

$$\mathbf{x} \cdot \mathbf{y} = \sum_{g,h \in G} \alpha_g \beta_h.$$

## Códigos dual y autodual

Por definición, el dual de un código $\mathcal{C}$, denotado por $\mathcal{C}^{\perp}$, considerado como vectores sobre $R^n$ es su complemento ortogonal, es decir

$$\mathcal{C}^{\perp} = \{v \in R^n : v \cdot u = 0, \forall u \in \mathcal{C}\}.$$

Sean $\mathbf{x} = \sum_{g \in G} \alpha_g g$, $\mathbf{y} = \sum_{h \in G} \beta_h h \in RG$. El producto interno o punto de $\mathbf{x}$ e $\mathbf{y}$ es dado por la expresión

$$\mathbf{x} \cdot \mathbf{y} = \sum_{g,h \in G} \alpha_g \beta_h.$$

Así, el dual de un código a partir de una codificación de anillo de grupo viene dada por

$$\mathcal{C}^{\perp} = \{\mathbf{y} \in RG : \mathbf{y} \cdot (\mathbf{xu}) = \mathbf{0}, \forall \mathbf{x} \in W\}.$$

En el caso de un código divisor de cero tenemos.

**Teorema**

*Sean* $\mathbf{u}, \mathbf{v} \in RG$, *con* $U$ *y* $V$ *sus* $RG$*-matrices y tales que* $\mathbf{uv} = \mathbf{0}$, $\mathbf{rank}(U) = r$ *y* $\mathbf{rank}(V) = n - r$. *Sea* $W$ *un submódulo de* $RG$ *con base* $S \subset G$ *de dimensión* $r$ *tal que* $S\mathbf{u}$ *es linealmente independiente y denótese por* $W^{\perp}$ *el submódulo de* $RG$ *con base* $G \setminus S$. *Entonces el código* $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ *tiene código dual* $\mathcal{C}^{\perp} = \{\mathbf{xv}^T : \mathbf{x} \in W^{\perp}\} = \{\mathbf{y} \in RG : \mathbf{yu}^T = \mathbf{0}\}$.

En el caso de un código divisor de cero tenemos.

**Teorema**

*Sean* $\mathbf{u}, \mathbf{v} \in RG$, *con* $U$ *y* $V$ *sus* $RG$*-matrices y tales que* $\mathbf{uv} = \mathbf{0}$, $\mathbf{rank}(U) = r$ *y* $\mathbf{rank}(V) = n - r$. *Sea* $W$ *un submódulo de* $RG$ *con base* $S \subset G$ *de dimensión* $r$ *tal que* $S\mathbf{u}$ *es linealmente independiente y denótese por* $W^{\perp}$ *el submódulo de* $RG$ *con base* $G \setminus S$. *Entonces el código* $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ *tiene código dual* $\mathcal{C}^{\perp} = \{\mathbf{xv}^T : \mathbf{x} \in W^{\perp}\} = \{\mathbf{y} \in RG : \mathbf{yu}^T = \mathbf{0}\}$.

Como una consecuencia tenemos en el caso de códigos auto-duales que:

**Corolario**

$\mathcal{C}^{\perp} = \mathcal{C}$ *si y sólo si* $\mathbf{uu}^T = \mathbf{0}$ *y* $\mathbf{rank}(U) = n/2$.

# Códigos desde unidades

Cuando $\mathbf{u} \in \mathcal{U}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código derivado de unidad**.

Sea $W$ un submódulo de $RG$ generado (como un $R$-módulo) por $r$ elementos de grupo $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ con $r < n$, obtenemos el código $\mathcal{C} = W\mathbf{u}$.

# Códigos desde unidades

Cuando $\mathbf{u} \in \mathcal{U}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código derivado de unidad**.

Sea $W$ un submódulo de $RG$ generado (como un $R$-módulo) por $r$ elementos de grupo $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ con $r < n$, obtenemos el código $\mathcal{C} = W\mathbf{u}$.

Ahora $\mathbf{c} \in \mathcal{C}$ si y sólo si $\mathbf{cu}^{-1} \in W$ si y sólo si los coeficientes de elementos en $G \setminus S$ en la representación de $\mathbf{cu}^{-1}$ son cero. Como lo vemos multiplicar una palabra código por el inverso de la unidad permite recuperar la entrada original.

# Códigos desde unidades

Cuando $\mathbf{u} \in \mathcal{U}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código derivado de unidad**.

Sea $W$ un submódulo de $RG$ generado (como un $R$-módulo) por $r$ elementos de grupo $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ con $r < n$, obtenemos el código $\mathcal{C} = W\mathbf{u}$.

Ahora $\mathbf{c} \in \mathcal{C}$ si y sólo si $\mathbf{cu}^{-1} \in W$ si y sólo si los coeficientes de elementos en $G \setminus S$ en la representación de $\mathbf{cu}^{-1}$ son cero. Como lo vemos multiplicar una palabra código por el inverso de la unidad permite recuperar la entrada original.

Un código derivado de unidad también puede ser considerado como una aplicación de $R^r$ en $R^n$ de la siguiente manera:

1. $R^r \ni \underline{x} = (\alpha_1, \alpha_2, \ldots, \alpha_r) \mapsto \sum_{i=1}^{r} \alpha_i g_{k_i} = \mathbf{x} \in W$.

# Códigos desde unidades

Cuando $\mathbf{u} \in \mathcal{U}(RG)$, el código $\mathcal{C}$ que se genera es llamado **código derivado de unidad**.

Sea $W$ un submódulo de $RG$ generado (como un $R$-módulo) por $r$ elementos de grupo $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ con $r < n$, obtenemos el código $\mathcal{C} = W\mathbf{u}$.

Ahora $\mathbf{c} \in \mathcal{C}$ si y sólo si $\mathbf{cu}^{-1} \in W$ si y sólo si los coeficientes de elementos en $G \setminus S$ en la representación de $\mathbf{cu}^{-1}$ son cero. Como lo vemos multiplicar una palabra código por el inverso de la unidad permite recuperar la entrada original.

Un código derivado de unidad también puede ser considerado como una aplicación de $R^r$ en $R^n$ de la siguiente manera:

1. $R^r \ni \underline{x} = (\alpha_1, \alpha_2, \ldots, \alpha_r) \mapsto \sum_{i=1}^{r} \alpha_i g_{k_i} = \mathbf{x} \in W$.
2. $\mathcal{C} \ni \mathbf{xu} = \sum_{i=1}^{n} \beta_i g_i$. Esto da una codificación $\mathbf{x} \mapsto (\beta_1, \beta_2, \ldots, \beta_n)$ de $R^r$ a $R^n$

Sean $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$ en $RG$ y $U$ y $U^{-1}$ las correspondientes $RG$-matrices y consideremos $W$ el submódulo generado por $\{g_1, g_2, \ldots, g_r\}$ con $r < n$:

1. $W \ni \mathbf{x} = \sum_{i=1}^{r} \alpha_i g_i.$

Sean $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$ en $RG$ y $U$ y $U^{-1}$ las correspondientes $RG$-matrices y consideremos $W$ el submódulo generado por $\{g_1, g_2, \ldots, g_r\}$ con $r < n$:

1. $W \ni \mathbf{x} = \sum_{i=1}^{r} \alpha_i g_i$.
2. $U = \begin{pmatrix} A \\ B \end{pmatrix}$, donde $A$ es $r \times n$ y $B$ es $(n-r) \times n$.

Sean $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$ en $RG$ y $U$ y $U^{-1}$ las correspondientes $RG$-matrices y consideremos $W$ el submódulo generado por $\{g_1, g_2, \ldots, g_r\}$ con $r < n$:

1. $W \ni \mathbf{x} = \sum_{i=1}^{r} \alpha_i g_i$.
2. $U = \begin{pmatrix} A \\ B \end{pmatrix}$, donde $A$ es $r \times n$ y $B$ es $(n-r) \times n$.
3. $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$, donde $C$ es $n \times r$ y $D$ es $n \times (n-r)$.

Así como $UU^{-1} = I$ entonces $AD = 0$.

Sean $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$ en $RG$ y $U$ y $U^{-1}$ las correspondientes $RG$-matrices y consideremos $W$ el submódulo generado por $\{g_1, g_2, \ldots, g_r\}$ con $r < n$:

1. $W \ni \mathbf{x} = \sum_{i=1}^{r} \alpha_i g_i$.
2. $U = \begin{pmatrix} A \\ B \end{pmatrix}$, donde $A$ es $r \times n$ y $B$ es $(n-r) \times n$.
3. $U^{-1} = \begin{pmatrix} C & D \end{pmatrix}$, donde $C$ es $n \times r$ y $D$ es $n \times (n-r)$.

Así como $UU^{-1} = I$ entonces $AD = 0$.

**Resumiendo**

Los códigos derivados de unidades de longitud $n$ y de tamaño $r$ se pueden construir con total libertad como sigue: Seleccione un $G$ de orden $n$ y un $R$ sobre el que vamos a definir el código, encuentre una unidad $\mathbf{u} \in RG$ y su inverso $\mathbf{u}^{-1}$. Finalmente, una base para un submódulo $W$ de $r$ elementos genera un código derivado de $\mathbf{u}$.

## Códigos dual y autodual

A continuación veamos la obtención del código dual de un código derivado de la unidad $\mathbf{u}$, a partir de $\left(\mathbf{u}^{-1}\right)^T$.

## Códigos dual y autodual

A continuación veamos la obtención del código dual de un código derivado de la unidad $\mathbf{u}$, a partir de $\left(\mathbf{u}^{-1}\right)^T$.

**Teorema**

*Sean $W$ un submódulo con base de elementos de grupo $S \subset G$ y $W^{\perp}$ el submódulo con base $G \setminus S$. Sea $\mathbf{u} \in RG$ una unidad tal que $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$. Entonces el código dual de $\mathcal{C} = \{\mathbf{x}\mathbf{u} : \mathbf{x} \in W\}$ es $\mathcal{C}^{\perp} = \left\{\mathbf{x}\left(\mathbf{u}^{-1}\right)^T : \mathbf{x} \in W^{\perp}\right\}$.*

## Códigos dual y autodual

A continuación veamos la obtención del código dual de un código derivado de la unidad $\mathbf{u}$, a partir de $\left(\mathbf{u}^{-1}\right)^T$.

### Teorema

*Sean $W$ un submódulo con base de elementos de grupo $S \subset G$ y $W^{\perp}$ el submódulo con base $G \setminus S$. Sea $\mathbf{u} \in RG$ una unidad tal que $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$. Entonces el código dual de $\mathcal{C} = \{\mathbf{x}\mathbf{u} : \mathbf{x} \in W\}$ es $\mathcal{C}^{\perp} = \left\{\mathbf{x}\left(\mathbf{u}^{-1}\right)^T : \mathbf{x} \in W^{\perp}\right\}$.*

### Definición

*Una unidad $\mathbf{u} \in RG$ es **ortogonal** si y sólo si $\mathbf{u}\mathbf{u}^T = 1$. Es fácil ver que la $RG$-matriz de una unidad ortogonal $\mathbf{u}$ es una matriz ortogonal.*

## Códigos dual y autodual

A continuación veamos la obtención del código dual de un código derivado de la unidad $\mathbf{u}$, a partir de $\left(\mathbf{u}^{-1}\right)^T$.

### Teorema

*Sean $W$ un submódulo con base de elementos de grupo $S \subset G$ y $W^\perp$ el submódulo con base $G \setminus S$. Sea $\mathbf{u} \in RG$ una unidad tal que $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$. Entonces el código dual de $\mathcal{C} = \{\mathbf{x}\mathbf{u} : \mathbf{x} \in W\}$ es $\mathcal{C}^\perp = \left\{\mathbf{x}\left(\mathbf{u}^{-1}\right)^T : \mathbf{x} \in W^\perp\right\}$.*

### Definición

*Una unidad $\mathbf{u} \in RG$ es **ortogonal** si y sólo si $\mathbf{u}\mathbf{u}^T = 1$. Es fácil ver que la $RG$-matriz de una unidad ortogonal $\mathbf{u}$ es una matriz ortogonal.*

Como sabemos un código lineal $\mathcal{C}$ es auto-dual si $\mathcal{C} = \mathcal{C}^\perp$, por tanto usando el Teorema anterior, con $\mathbf{u}$ unidad ortogonal y un submódulo de dimensión $n/2$ obtenemos un código derivado de unidad auto-dual.

# Ejemplos

Presentamos algunos ejemplos ilustrativos de códigos desde codificaciones de anillos de grupos:

## Ejemplo

**Código divisor de cero auto-dual:** Podemos obtener códigos auto-duales en $RG$ de la siguiente manera. Suponga que $|G| = n = 2m$ y $G = \{g_1, g_2, \ldots, g_n\}$. Si $\mathbf{u} \in RG$ satisface

# Ejemplos

Presentamos algunos ejemplos ilustrativos de códigos desde codificaciones de anillos de grupos:

## Ejemplo

**Código divisor de cero auto-dual:** Podemos obtener códigos auto-duales en $RG$ de la siguiente manera. Suponga que $|G| = n = 2m$ y $G = \{g_1, g_2, \ldots, g_n\}$. Si $\mathbf{u} \in RG$ satisface

1. $\mathbf{u}^2 = \mathbf{0}$,
2. $\mathbf{u} = \mathbf{u}^T$, luego $\mathbf{u}\mathbf{u}^T = \mathbf{0}$,
3. $rank(U) = m$.

# Ejemplos

Presentamos algunos ejemplos ilustrativos de códigos desde codificaciones de anillos de grupos:

## Ejemplo

**Código divisor de cero auto-dual:** Podemos obtener códigos auto-duales en $RG$ de la siguiente manera. Suponga que $|G| = n = 2m$ y $G = \{g_1, g_2, \ldots, g_n\}$. Si $\mathbf{u} \in RG$ satisface

1. $\mathbf{u}^2 = \mathbf{0}$,
2. $\mathbf{u} = \mathbf{u}^T$, luego $\mathbf{u}\mathbf{u}^T = \mathbf{0}$,
3. $rank(U) = m$.

Entonces $\mathbf{u}$ genera un código auto-dual.

# Ejemplos

Presentamos algunos ejemplos ilustrativos de códigos desde codificaciones de anillos de grupos:

## Ejemplo

**Código divisor de cero auto-dual:** Podemos obtener códigos auto-duales en $RG$ de la siguiente manera. Suponga que $|G| = n = 2m$ y $G = \{g_1, g_2, \ldots, g_n\}$. Si $\mathbf{u} \in RG$ satisface

1. $\mathbf{u}^2 = \mathbf{0}$,
2. $\mathbf{u} = \mathbf{u}^T$, luego $\mathbf{u}\mathbf{u}^T = \mathbf{0}$,
3. $rank(U) = m$.

Entonces $\mathbf{u}$ genera un código auto-dual.
Por ejemplo, sea $G = C_2 \times C_4$ donde $C_4 = \langle a : a^4 = 1\rangle$ y $C_2 = \langle h : h^2 = 1\rangle$. Consideremos el anillo de grupo $\mathbb{Z}_2G$ y sea $\mathbf{u} = 1 + h(a + a^2 + a^3)$ elemento en este anillo. Entonces,

$$\mathbf{u}^2 = 1 + h^2(a^2 + a^4 + a^6) = 1 + a^2 + 1 + a^2 = 0,$$

$$\mathbf{u}^T = 1^{-1} + (ha)^{-1} + (ha^2)^{-1} + (ha^3)^{-1} = 1 + ha^3 + ha^2 + ha = \mathbf{u}$$

## Ejemplo

Así, $rank(U) \leq 4$ y la $RG$-matrix de $\mathbf{u}$ está dada por $U = \begin{pmatrix} I & B \\ B & I \end{pmatrix}$ de lo cual se sigue que $rank(U) = 4$.

## Ejemplo

Así, $rank(U) \leq 4$ y la $RG$-matrix de $\mathbf{u}$ está dada por $U = \begin{pmatrix} I & B \\ B & I \end{pmatrix}$ de lo cual se sigue que $rank(U) = 4$.

## Ejemplo

**Código derivado de unidad:** En el anillo de grupo $\mathbb{Z}_2G$, si $\mathbf{v}^2 = 0$, entonces $(1 + \mathbf{v})^2 = 1$. Consideremos el anillo de grupo $\mathbb{Z}_2C_{2n}$ con $C_{2n} = \langle g : g^{2n} = 1 \rangle$, sea $\mathbf{v}_i = g^i + g^{n-i} + g^{n+i} + g^{2n-i} \in \mathbb{Z}_2C_{2n}$.

## Ejemplo

Así, $rank(U) \leq 4$ y la $RG$-matrix de $\mathbf{u}$ está dada por $U = \begin{pmatrix} I & B \\ B & I \end{pmatrix}$ de lo cual se sigue que $rank(U) = 4$.

## Ejemplo

**Código derivado de unidad:** En el anillo de grupo $\mathbb{Z}_2G$, si $\mathbf{v}^2 = 0$, entonces $(1+\mathbf{v})^2 = 1$. Consideremos el anillo de grupo $\mathbb{Z}_2C_{2n}$ con $C_{2n} = \langle g : g^{2n} = 1 \rangle$, sea $\mathbf{v}_i = g^i + g^{n-i} + g^{n+i} + g^{2n-i} \in \mathbb{Z}_2C_{2n}$.
Entonces,

$$\begin{aligned} \mathbf{v}_i^2 &= (g^i)^2 + (g^{n-i})^2 + (g^{n+i})^2 + (g^{2n-i})^2 \\ &= g^{2i} + g^{2n-2i} + g^{2n+2i} + g^{4n-2i} \\ &= g^{2i} + g^{2n}g^{-2i} + g^{2n}g^{2i} + g^{4n}g^{-2i} \\ &= g^{2i} + g^{-2i} + g^{2i} + g^{-2i} = \mathbf{0}, \end{aligned}$$

## Ejemplo

y

$$\mathbf{v}_i^T = (g^i)^{-1} + (g^{n-i})^{-1} + (g^{n+i})^{-1} + (g^{2n-i})^{-1} = g^{2n-i} + g^{n+i} + g^{n-i} + g^i = \mathbf{v}_i.$$

Por lo tanto todos los $\mathbf{v}$, que son combinaciones de los $\mathbf{v}_i$'s, satisfacen que $\mathbf{v}^2 = \mathbf{v}\mathbf{v}^T = \mathbf{0}$. Finalmente, $\mathbf{u} = \mathbf{1} + \mathbf{v}$ satisface que $\mathbf{u}^2 = \mathbf{u}\mathbf{u}^T = \mathbf{1}$ y da una serie de unidades ortogonales. Como ya vimos, no hay problemas de rango ya que estos son códigos derivados de unidades.

## Ejemplo

y

$$\mathbf{v}_i^T = (g^i)^{-1}+(g^{n-i})^{-1}+(g^{n+i})^{-1}+(g^{2n-i})^{-1} = g^{2n-i}+g^{n+i}+g^{n-i}+g^i = \mathbf{v}_i.$$

Por lo tanto todos los $\mathbf{v}$, que son combinaciones de los $\mathbf{v}_i$'s, satisfacen que $\mathbf{v}^2 = \mathbf{v}\mathbf{v}^T = \mathbf{0}$. Finalmente, $\mathbf{u} = \mathbf{1} + \mathbf{v}$ satisface que $\mathbf{u}^2 = \mathbf{u}\mathbf{u}^T = \mathbf{1}$ y da una serie de unidades ortogonales. Como ya vimos, no hay problemas de rango ya que estos son códigos derivados de unidades.
Un ejemplo específico de lo anterior es el siguiente: tomando $n = 7$ tenemos el anillo de grupo $\mathbb{Z}_2C_{14}$ con $C_{14} = \langle g : g^{14} = 1\rangle$, si tomamos $i = 2$, entonces $\mathbf{v}_2 = g^2 + g^5 + g^9 + g^{12}$ y por lo tanto

$$\mathbf{u} = 1 + \mathbf{v}_2 = 1 + g^2 + g^5 + g^9 + g^{12},$$

satisface que $\mathbf{u}^2 = \mathbf{u}\mathbf{u}^T = \mathbf{1}$.

# Referencias



Hurley P. & Hurley T., *Codes from zero-divisors and units in group rings*. Int. J. Information and Coding Theory, Vol. **1**, No. **1**: 57-87, 2009.


Podestá R. A., *Introducción a la teoría de códigos autocorrectores*. Mathematics Subject Classification. CONICET y SecytUNC, 2006.


Polcino Milies C. & Sehgal S. K., *A Course in Group Rings*. Dordrecht: Kluwer Academic Publishers. Algebras and Applications, 2002.