Low-Density Parity-Check Codes

Bermúdez Piñero, Jeranfer
Departamento de Ciencia de Cómputos
UPR, Río Piedras

García Lebrón, Richard
Departamento de Ciencia de Cómputos
UPR, Río Piedras

López Roig, Reynaldo
Departamento de Ciencia de Cómputos
UPR, Río Piedras

Mentor
Dra. Ivelisse Rubio
Departamento de Ciencia de Cómputos
UPR, Río Piedras

30 de mayo de 2008

Resumen

Los códigos correctores de errores se utilizan en la comunicación digital para detectar y corregir errores en la transmisión o almacenamiento de la información. En esta investigación estudiamos códigos Low-Density Parity-Check (LDPC). Estos códigos son generados por grafos bipartitos construidos con permutaciones de cuerpos finitos dadas por monomios. Nuestro propósito es encontrar construcciones que resulten en códigos LDPC eficientes. Para esto estudiamos si existe relación entre la descomposición cíclica de la permutación y el girth del grafo.

1. Introducción

Los códigos de corrección de errores son comúnmente utilizados en las comunicaciones digitales para corregir errores en la transmisión de información. Estos se utilizan en la telefonía digital, los discos compactos (CD's), y en la comunicación interespacial entre otros.

En particular nos enfocamos en los códigos **Low-Density Parity-Check (LDPC)**. Estos códigos fueron creados por Robert G. Gallager en MIT (Massachusetts Institute of Technology) en el 1960. Estos fueron olvidados hasta aproximadamente en los 90's. Se relacionan con los Turbo Codes, pero su estructura algebráica es más conocida.

Pretendemos conseguir construcciones de códigos LDPC que sean eficientes debido a su buena capacidad para corregir errores. Esto se logra generando permutaciones de cuerpos finitos dadas por monomios, construyendo sus respectivos grafos y estudiando si existe una relación entre la descomposición cíclica de la permutación y el girth del grafo. Cuanto mejor sea el girth, más eficiente es el código.

2. Preliminares

Para poder entender la construcción de grafos por medio de permutaciones se tienen que entender primero los siguientes conceptos matemáticos.

2.1. Anillo

Un anillo es un conjunto no vacio R donde se satisfacen dos operaciones y tienen las siguientes propiedades. Para todo $a, b, c \in R$:

1. Si $a \in R$ y $b \in R$, entonces $a + b \in R$.
2. $a + (b + c) = (a + b) + c$.
3. $a + b = b + a$.
4. Existe un elemento 0_R en R tal que $a + 0_R = a = 0_R + a$ para cada $a \in R$.

5. Para cada $a \in R$, la equación $a + x = 0_R$ tiene una solucion en R.

6. Si $a \in R$ y $b \in R$, entonces $ab \in R$.

7. $a(bc) = (ab)c$.

8. $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$.

2.1.1. Anillo Conmutativo

Un anillo R es un anillo conmutativo si satisface el siguiente axioma:

1. $ab = ba$ para todo $a, b \in R$.

2.1.2. Anillo con Identidad

Un anillo R es un anillo con identidad si contiene un elemento 1_R que satisfazca el siguiente axioma:

1. $a1_R = a = 1_R a$ para todo $a \in R$.

Ejemplo 1

El conjunto de los enteros $\mathbb{Z}$, con sus propiedades de adición y multiplicación, es un anillo conmutativo con identidad.

Ejemplo 2

Considere el conjunto de los enteros impares con sus propiedades de adición y multiplicación . Este conjunto no es un anillo porque no satisface la propiedad número 1. La suma de dos números impares no es un número impar.

2.2. Cuerpos

Un cuerpo es un anillo conmutativo R con identidad $1_R \neq 0_R$ donde se satisface que para todo $a \neq 0_R \in R$, la ecuación $ax = 1_R$ tiene solución en R.

2.2.1. Cuerpos Finitos

Un cuerpo finito es un cuerpo con un número finito de elementos que tiene propiedades de los números reales. Suele denotarse $\mathbb{F}_q^n$ para indicar un cuerpo finito con q elementos.

Ejemplo 3

$\mathbb{Z}_p$ que representa los enteros módulo p donde p es un número primo.

2.3. Permutación

Una permutación es un rearreglo de los elementos de un conjunto dada por una función biyectiva.

Ejemplo 4

Sea A un conjunto donde $A = \{1, 2, 3, 4\}$ una posible permutación de A sería 3 4 1 2 .

Dada por $f : A \longrightarrow A$
$f(1) = 3$, $f(2) = 4$, $f(3) = 1$, $f(4) = 2$

Denotada: $\binom{1\ 2\ 3\ 4}{3\ 4\ 1\ 2}$

Descomposición Cíclica: $(1\ 3)\ (2\ 4)$

2.4. Permutación de cuerpos finitos

Un permutación de cuerpos finitos es una permutación con un número finito de elementos.

Teorema 1

$$x^i \text{ produce permutación en } \mathbb{Z}_p \longleftrightarrow mcd(i, p-1) = 1$$

Ejemplo 5

Considere el monomio x^2 con $p = 11$ produce $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{smallmatrix}\right)$ notar $mcd(2, 10) = 2$

Ejemplo 6

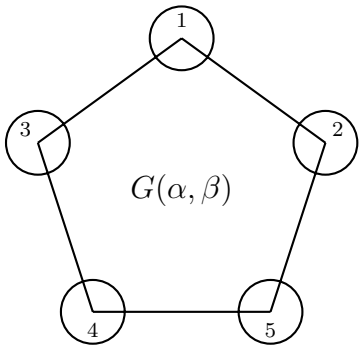
Considere el monomio x^3 con $p = 11$ produce $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & 10 \end{smallmatrix}\right)$ notar $mcd(3, 10) = 1$

2.5. Grafo

Un grafo es un par de conjuntos (α, β) donde α es un conjunto no vacío y los elementos de β son pares no ordenados de elementos de α.Denotado $G(\alpha, \beta)$. Los elementos de α se llaman vértices y los de β se llaman aristas.

Ejemplo 7

Sea $G(\alpha, \beta)$ donde $\alpha = \{1, 2, 3, 4, 5\}$ y $\beta = \{(1, 2), (2, 5), (3, 1), (4, 2), (5, 4)\}$.



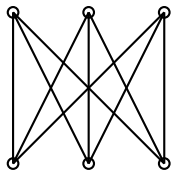
2.5.1. Grado de los vértices

Esta dado por la cantidad de aristas que van a un mismo vértice.

2.5.2. Grafo Bipartito

- Grafo donde el conjunto de vértices es separado en dos conjuntos disjuntos denotados M y C.
- Si $\mathbf{G_B} = (\alpha, \beta)$ donde $\alpha = M \cup C$ y $M \cap C = 0$, M tiene k elementos con grado mn y C tiene q elementos con grado cn. Existe $\phi = k \cdot mn = q \cdot cn$, donde ϕ es la cantidad de elementos de β.

Ejemplo 8



3. Construcción del Grafo

Sea Ω una permutación de cuerpos finitos , dada por una función biyectiva ρ(x) tal que $1 \leq x \leq n$ sobre $\mathbf{Z}_p$ donde p es primo. Si $n = p - 1$, podemos denotar y definir Ω como:

$$\Omega = \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ \rho(1) & \rho(2) & ... & \rho(n-1) & \rho(n) \end{pmatrix}$$

dada la permutación Ω podemos llamar y denotar al grafo bipartito de Ω como:

$$GB_\Omega(\alpha, \beta)$$

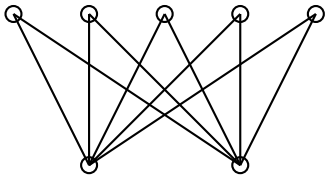
donde α es el conjunto de vértices y β el conjunto de aristas. Al $GB_\Omega(\alpha, \beta)$ ser bipartito entonces $\alpha = M \cup C$ y $M \cap C = 0$. M es el conjunto de los messege node con k elementos, denotado $M = \{m_1, m_2, m_3, ..., m_k\}$ con grado mn. C es el conjunto de los check nodes con q elementos, denotado $C = \{c_1, c_2, c_3, ...c_q\}$ y grado cn. Los aristas son el conjunto β con ϕ elementos, denotado $\beta = \{b_1, b_2, b_3, ..., b_\phi\}$ donde $\phi = mn \cdot k = cm \cdot q$. Los message nodes estan dados por: $m_a = \{(a \cdot mn + 1) - mn, a \cdot mn + 2) - mn, a \cdot mn + 3) - mn, ...a \cdot mn + mn) - mn, \}$ donde $1 \leq a \leq k$. Los check nodes estan dados por: $c_u = \{(u \cdot cn + 1) - cn, u \cdot cn + 2) - cn, u \cdot cn + 3) - cn, ...u \cdot cn + cn) - cn, \}$ donde $1 \leq u \leq q$. Los aristas estan dados por: $b_v = (v, \rho(v))$ donde $1 \leq v \leq \phi$, el elemento v pertence al message node y elemento $\rho(v)$ al check node.

Ejemplo 9 *Considere la función biyeciva sobre* $\mathbf{Z}_{11}$, $\rho(x) = x^3 mod\ 11$ *con* $1 \leq x \leq 10$ *la permutación* Ω *de la función* $\rho(x)$ *seria:*

$$\Omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 5 & 9 & 4 & 7 & 2 & 6 & 3 & 10 \end{pmatrix}$$

Si se establece que $mn = 2$, $k = 5$, $cn = 5$ *y* $q = 2$ *esto dice que los message node son de grado dos y los check node de grado cinco. Note que* $\phi = 2 \cdot 5 = 5 \cdot 2 = 10$. *El conjunto de los message node seria* $M = \{m_1, m_2, m_3, m_4, m_5\}$ *usando la formula para obtener los message node tendriamos que* $m_1 = \{1, 2\}, m_2 = \{3, 4\}, m_3 = \{5, 6\}, m_4 = \{7, 8\}, m_5 = \{9, 10\}$. *Los check nodes serian* $C = \{c_1, c_2\}$ *usando la formula para optener los check nodes tendriamos que* $c_1 = \{1, 2, 3, 4, 5\}, c_2 = \{6, 7, 8, 9, 10\}$. *El conjunto de arista seria* $\beta = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}\}$ *usando la formula para optener los aristas tendrianos que* $\beta_1 = (1, 1), \beta_2 = (2, 8), \beta_3 = (3, 5), \beta_4 = (4, 9), \beta_5 =$

$(5,4), \beta_6 = (6,7), \beta_7 = (7,2), \beta_8 = (8,6), \beta_9 = (9,3), \beta_{10} = (10,10)$ *la ilustración del grafo seria:*

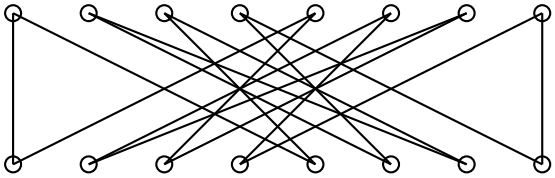


$GB_\Omega(\alpha, \beta)$

Ejemplo 10 *Considere la función biyeciva sobre* $\mathbf{Z}_{17}$*,* $h(x) = x^7 mod\ 17$ *con* $1 \leq x \leq 16$ *la permutación* χ *de la función* $h(x)$ *seria:*

$$\chi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 9 & 11 & 13 & 10 & 14 & 12 & 15 & 2 & 5 & 3 & 7 & 4 & 6 & 8 & 16 \end{pmatrix}$$

Si se establece que $mn = 2$*,* $k = 8$*,* $cn = 2$ *y* $q = 8$ *esto dice que los message node son de grado dos y los check node de grado dos. Note que* $\phi = 2 \cdot 8 = 2 \cdot 8 = 16$*. El conjunto de los message node seria* $M = \{m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8\}$ *usando la formula para obtener los message node tendriamos que* $m_1 = \{1,2\}, m_2 = \{3,4\}, m_3 = \{5,6\}, m_4 = \{7,8\}, m_5 = \{9,10\}, m_6 = \{11,12\}, m_7 = \{13,14\}, m_8 = \{15,16\}$*. Los check nodes serian* $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8\}$ *usando la formula para optener los check nodes tendriamos que* $c_1 = \{1,2\}, c_2 = \{3,4\}, c_3 = \{5,6\}, c_4 = \{7,8\}, c_5 = \{9,10\}, c_6 = \{11,12\}, c_7 = \{13,14\}, c_8 = \{15,16\}$*. El conjunto de arista seria:* $\beta = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{13}, b_{14}, b_{15}, b_{16}\}$ *usando la formula para optener los aristas tendrianos que* $\beta_1 = (1,1), \beta_2 = (2,9), \beta_3 = (3,11), \beta_4 = (4,13), \beta_5 = (5,10), \beta_6 = (6,14), \beta_7 = (7,12), \beta_8 = (8,15), \beta_9 = (9,2), \beta_{10} = (10,5), \beta_{11} = (11,3), \beta_{12} = (12,7), \beta_{13} = (13,4), \beta_{14} = (14,6), \beta_{15} = (15,8), \beta_{16} = (16,16)$ *la ilustración del grafo seria:*

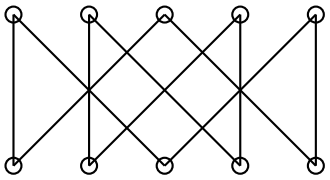


$GB_\chi(\alpha, \beta)$

4. Ciclos del Grafo

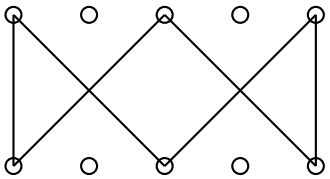
Se conoce como **ciclo del grafo** al recorrido entre la aristas del grafo donde se comienza en un vértice v y se termina en el mismo vértice v.

Ejemplo 11 *Considera el siguiente grafo*$GB(\alpha, \beta)$

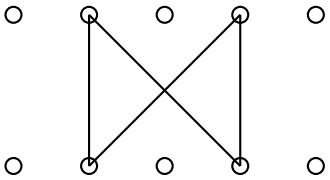


$GB(\alpha, \beta)$

Los ciclos del grafo serian los siguientes subgrafos:



ciclo 1

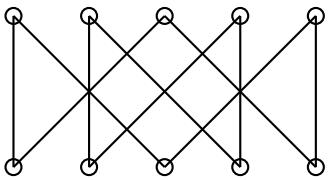


ciclo 2

5. Girth del Grafo

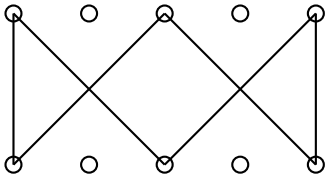
El girth del grafo seria el ciclo mas corto del grafo. Se dice que grafos con girth grande producen codificadores eficientes.

Ejemplo 12 *Considera el siguiente grafo*$GB(\alpha, \beta)$

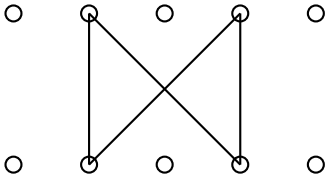


$GB(\alpha, \beta)$

Los ciclos del grafo serian los siguientes subgrafos:



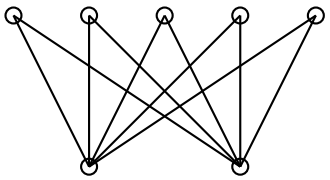
ciclo 1



ciclo 2

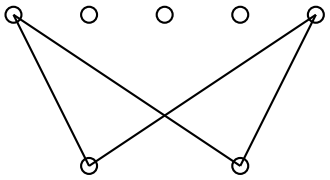
notar que el ciclo de menor largo es de largo 4 por lo tanto el $Girth = 4$.

Ejemplo 13 *Vea el grafo* $GB_\Omega(\alpha, \beta)$

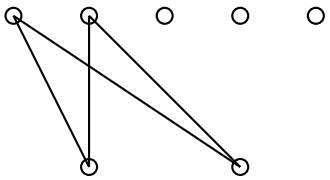


$GB_\Omega(\alpha, \beta)$

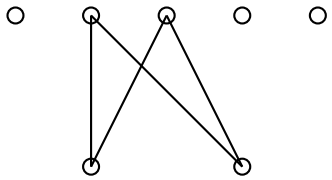
note que los diferentes ciclos del grafo serian los siguentes sub grafos:



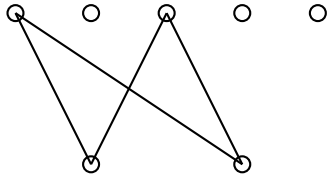
ciclo 1



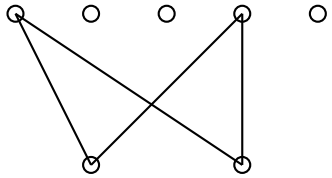
ciclo 2



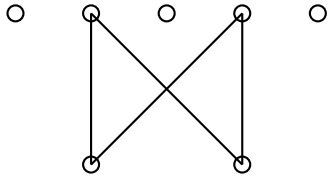
ciclo 3



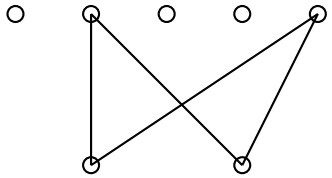
ciclo 4



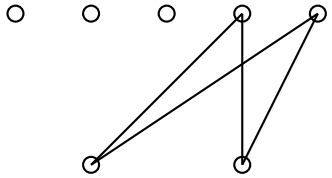
ciclo 5



ciclo 6

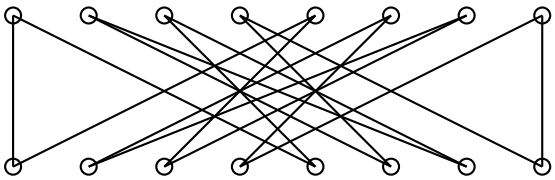


ciclo 7



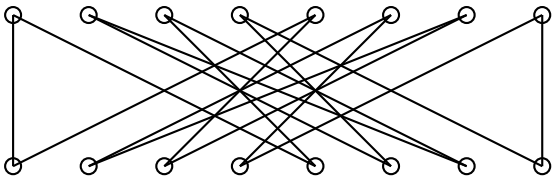
ciclo 8

Note que de los ocho diferentes ciclos del grafo $GB_\Omega(\alpha, \beta)$ son de largo cuatro por lo tanto como todos sus ciclos son de largo cuarto esto dice que el menor de sus ciclo es de largo cuatro entonces el girth es igual a cuatro (Girth = 4).



$GB_\chi(\alpha, \beta)$

A diferencia en el grafo $GB_\chi(\alpha, \beta)$(Ejemplo 2) todos sus ciclos son el mismo grafo. En ciclo del grafo $GB_\chi(\alpha, \beta)$ estan contenidos todos los aristas, de otra manera se dice que tiene girth maximo ya que el girth es igual a 16(Girth = 16). Todos los ciclos del grafo $GB_\chi(\alpha, \beta)$ son de la forma:

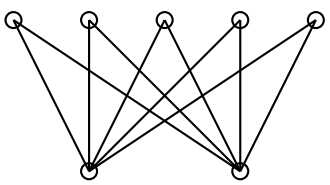


6. Matriz de Adjacencia

Si Gb es un grafo bipartito con k vértices llamados message node($M = \{m_1, m_2, m_3, ..., m_k\}$) y q vértices llamados check nodes($C = \{c_1, c_2, c_3, ..., c_q\}$). Los messege node serian las filas de la matriz y los check nodes las columnas de la matiz. La matiz de adyacencia M_{Gb} seria una matriz $k \times q$ Para i y j tal que $1 \leq i \leq k$ y $1 \leq j \leq q$, el subindice j dice la columna y el subindice i dice la fila. Donde a_{ij} son las entradas de la matriz M_{Gb} y estan definidas como:

$$a_{ij} = \begin{cases} 1, & \text{si } m_i, c_j \text{ es una arista;} \\ 0, & \text{si } m_i, c_j \text{ no es una arista;} \end{cases}$$

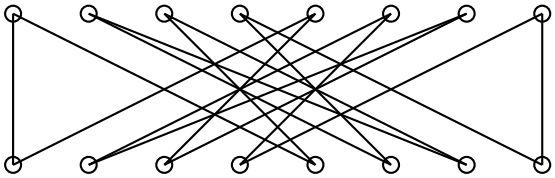
Ejemplo 14 *Considere el grafo* $GB_\Omega(\alpha, \beta)$



la matriz de adyacencia del grafo seria:

$$M_{GB_\Omega(\alpha,\beta)} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Ejemplo 15 *Dado el siguiente grafo*



$GB_\chi(\alpha, \beta)$

la matriz de adyacencia seria:

$$M_{GB_\chi(\alpha,\beta)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

7. Matriz Generadora

Sea ϵ es un especio vectorial con dimención n, existe un conjunto de n vectores que generan el código. Si $\{g_1, g_2, g_3, ..., g_n\}$ son las bases de espacio nulo de la matriz de adyacencia del grafo, entonces definimos y la matriz generadora G tal que $G \cdot H^T = \mathbf{0}$.

$$G = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \\ . \\ . \\ . \\ g_n \end{bmatrix}$$

Ejemplo 16 *Considere el grafo* $GB_\chi(\alpha,\beta)$ *dada la matriz de adyacencia* $M_{GB_\chi(\alpha,\beta)}$

$$M_{GB_\chi(\alpha,\beta)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

las base del nulo seria $Null\ M_{GB_\chi(\alpha,\beta)} = \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 1 \\ 1 \end{bmatrix}$ si $G_{GB_\chi(\alpha,\beta)} = \begin{bmatrix} 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}$

como $G_{GB_\chi(\alpha,\beta)} \cdot M^T_{GB_\chi(\alpha,\beta)} = \mathbf{0}$ entonces $G_{GB_\chi(\alpha,\beta)}$ se conoce como la matriz generadora.

Ejemplo 17 *Sea* M_{GB} *la matriz de adyacencia de un grafo donde* $M_{GB} =$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

las bases del espacio nulo de M_{GB} serian:

$$Null\ M_{GB} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -2 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ -1 \\ 1 \\ -1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

sea $G_{GB} =$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 2 & 0 & 0 & -1 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \end{bmatrix}$$

como $G_{GB} \cdot M_{GB}^T = \mathbf{0}$ entonces G_{GB} es la matriz generadora del grafo GB

8. Proceso de Codificar la informacion

El proceso de codificar la información (añadir redundacia a la información) ocure en el codificador, este proceso consiste en multiplicar el vector de la información por la matriz generadora G. Si la matriz generadora (G) es una matriz $n \times m$, esto dice que puede codificar un vector de información $1 \times n$. Sea i el vector de la información, C la palabra código (información codifiaca) donde $C = i \cdot G$ y C es $1 \times m$ donde $m > n$.

Ejemplo 18 *Sea* $i = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$ *y* G_{GB} *la matriz generadora donde* $G_{GB} =$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & 2 & 0 & 0 & -1 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \end{bmatrix}$$

la palabra código seria C *seria* $C = i \cdot G_{GB}$

$$C = \begin{bmatrix} -1 & 1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 1 & 1 & -1 & -1 & 0 & 1 & 1 & 0 & 0 & -2 & 1 & 0 \end{bmatrix}$$

8.1. Ejemplo 2

Sea $i = [1]$ y $G_{GB_{\chi(\alpha,\beta)}} = \begin{bmatrix} 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}$ la matriz generadora la palabra código C seria $C = i \cdot G_{GB_{\chi(\alpha,\beta)}}$

$$C = \begin{bmatrix} 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \end{bmatrix}$$

9. Trabajo Realizado

Se desarrollaron algoritmos para construir permutaciones según el teorema previamente descrito, hacer la descomposición cíclica de la permutación, construir su grafo con grados variantes y calcular su girth. Estos algoritmos se implementaron utilizando el simulador matemático Maple 11. Se corrió el programa para todos los primos desde el 11 al 211.

10. Resultados

No se encontró una relación entre el largo de ciclo de la permutación y el girth del grafo generado por esta. Esto no quiere decir que dicha relación no exista, sino que los resultados obtenidos no muestran un patrón claro que nos permita proponer un corolario formal.

Sin embargo, se observaron ciertas tendencias en cuanto a los grados de los nodos de los grafos y el girth. En los casos evaluados el girth máximo ha sido obtenido por grafos bipartitos donde sus dos conjuntos de nodos son de grado dos. Además, en la mayoría de los casos, los girth mayores a dos se consiguieron en grafos donde el grado de al menos uno de sus dos conjuntos de nodos es par.

11. Trabajo futuro

Cotejar la eficiencia de los códigos generados por las matrices de los grafos con sus grados dos y estudiar las permutaciones generadas por monomios ax^i donde a es un coeficiente diferente de uno.

Referencias

[1] Reinhard Diestel, Graph Theory, Secciones (1.3, 1.6) Springer-Verlag New York, 2004.

[2] Oscar Y. Takeshita, A New Construction for LDPC Codes using Permutation Polynomials over Integer Rings.

[3] http://www.cs.usask.ca/ resources/ tutorials/ csconcepts/ 1999-8/index.html

[4] Edgar G. Goodaire, Discrete Mathematics with Graph theory,(Cap 9).

[5] Amin Shokrollahi, LDPC Codes: An Introduction.

[6] Thomas W. Hungerford, Abstract Algebra, An Introduction Second edition, Sección(3.1)Thomson Learning, 1997.