Low-Density Parity-Check Codes

Jeranfer Bermúdez, Richard García, Reynaldo López
Universidad de Puerto Rico en Río Piedras Dept. Ciencia de Cómputo
Consejera: Dra. Ivelisse Rubio

Resumen:

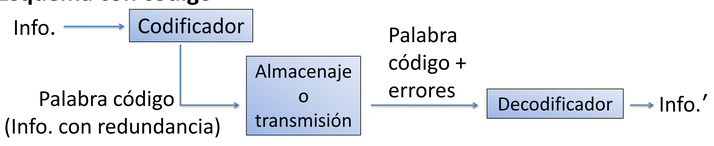
Los códigos correctores de errores se utilizan en la comunicación digital para detectar y corregir errores en la transmisión o almacenamiento de la información. En esta investigación estudiamos códigos Low-Density Parity-Check (LDPC). Estos códigos son generados por grafos bipartitos construidos con 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.

Preliminares:

Códigos de corrección de errores:

Esquema sin código

Esquema con código

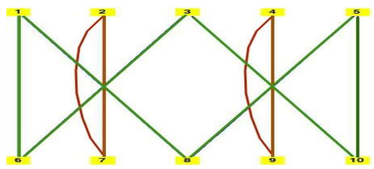


Permutación en cuerpos finitos - rearreglo de los elementos de un cuerpo finito.

Teorema: Con $1 \le x \le p-1$ x^i produce una permutación en Z_p si y solo si el $mcd(i,p-1)=1$.

Grafo - Es un par de conjuntos (α,β) donde no es un conjunto vaco y los elementos de son pares no ordenados de elementos.

Girth - es el ciclo más corto del grafo.



Los ciclos están dados por los colores marrón y verde. El girth sería el de color marrón.
En este caso el girth es igual a 2.

Girth máximo – es cuando el girth es igual a la cantidad de aristas del grafo.

Problema:

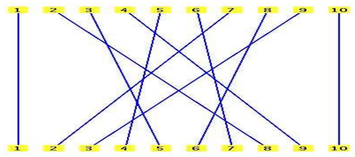
Construcción de códigos Low-Density Parity-Check eficientes.

Construcción del grafo:

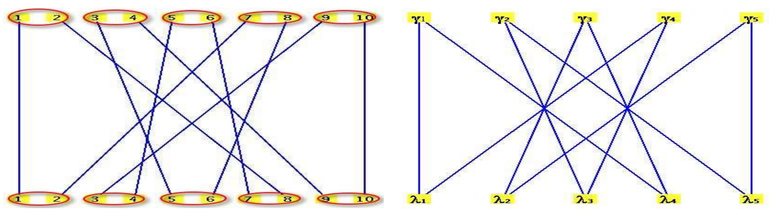
Paso 1:
Con x^3 módulo 11,
y $1 \le x \le 10$

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

Paso 2:
Trazado de la permutación



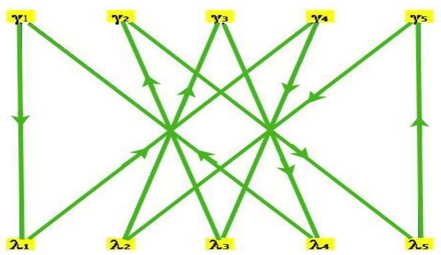
Paso 3:
Con G = (α,β), ga= 2, m= 5,gb= 2, n= 5, Φ = 10.
Con $1 \le i \le 5$ y $1 \le j \le 5$.
Los vertices serían:
γ1 = {1,2}, λ1 = {1,2}, γ2 = {3,4}, λ2= {3,4},
γ3= {5,6}, λ3 = {5,6}, γ4= {7,8}, λ4 = {7,8},
γ5= {9,10}, λ5 = {9,10}



En la izquierda la permutación con la representación de los vértices. En la derecha el grafo G generdo por la permutación.

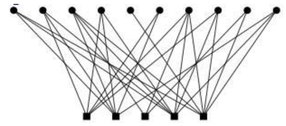
El grafo G = (α,β) tiene un girth máximo.

➢ girth = 10



Matriz generadora:

1) Considere el grafo:



2) Matriz de adyacencia:

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

3) Base del espacio nulo de H:

Null H = $\{g_1, g_2, g_3, g_4, g_5\}$

$$g_1 = [\,-1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\,]$$
$$g_2 = [\,0\ 0\ 0\ 0\ 0\ 0\ -1\ 0\ 1\ 0\,]$$
$$g_3 = [\,1\ -2\ -1\ 2\ 1\ 0\ -2\ 0\ 0\ 0\,]$$
$$g_4 = [\,0\ -1\ -1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\,]$$
$$g_5 = [\,-1\ 0\ 1\ -1\ 0\ 0\ 0\ 1\ 0\ 0\,]$$

4) Matriz generadora Mg , tal que $MgH^T = \mathbf{0}$.

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

5) Se multiplica *Info.* por Mg y se obtiene la palabra código.

Ej: Info. = [1 0 1 1 0];
Pal. Código= [-1 -2 1 0 1 0 -2 2 0 0]

Trabajo Realizado:

Utilizamos el simulador matemático Maple 11 donde hicimos programas para construir: la permutación, descomposición cíclica, hacer el grafo bipartito y calcular el girth. Evaluamos tods las posibles permutaciones de Z_p $11 \le p \le 211$ generadas por el monomio $x^i \bmod p$.

Conclusiones parciales:

En los casos evaluados el girth máximo ha sido obtenido por grafos bipartitos donde sus dos conjuntos de vértices son de grado 2. En la mayoría de los casos los girth mayores a 2 , al menos uno de los conjuntos de vértices del grafo es par.

Referencias:

- Reinhard Diestel, Graph Theory, Secciones (1.3, 1.6) Springer-Verlag, New York, 2004.
- Oscar Y. Takeshita, A New Construction for LDPC Codes using Permutation Polynomials over Integer Rings.
- http://www.cs.usask.ca/ resources/ tutorials/ csconcepts/ 1999-8/index.html
- Edgar G. Goodaire, Discrete Mathematics with Graph theory,(Cap 9).
- Amin Shokrollahi, LDPC Codes: An Introduction.

Agradecimientos: Dra. Ivelisse Rubio, Dr. Mariano Marcano, PRSLAM-AMP, Juan M. Font, Lab. Emmy Noether, Dept. Ciencia de Cómputos, CSI-CN.