Matemática Discreta

Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana

Lic en Sistemas de Información - FCyT - UADER

2023

Grupos y teoría de codificación.

Definiciones, ejemplos y propiedades elementales.

Grupo

Si G es un conjunto no vacío y $\circ$ es una operación binaria en G, entonces $(G, \circ)$ es un grupo si cumple las siguientes condiciones:

1. $\forall a, b \in G$,$a \circ b \in G$. (ley de cierre)
2. $\forall a, b, c \in G$, $a \circ (b \circ c) = (a \circ) b \circ c$. (asociativa)
3. Existe $e \in G$ tal que $a \circ e = e \circ a = a$, para todo $a \in G$. (neutro)
4. Para todo $a \in G$ existe un elemento $b \in G$ tal que $a \circ b = b \circ a = e$. (inversos)

Si además se verifica para todo $a, b \in G$ que $a \circ b = b \circ a$, entonces el grupo es *abeliano o conmutativo*.

Con la suma ordinaria, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$ con cada uno grupo abeliano.

Sin el cero, $\mathbb{Q}^*, \mathbb{R}^*$ y $\mathbb{C}^*$ son grupos abelianos multiplicativos.

En general: Si $(R, +, .)$ es un anillo, entonces $(R, +)$ es un grupo abeliano. Los elementos distintos de cero de un *cuerpo* forman un grupo abeliano multiplicativo.

Orden de un grupo

Para cualquier grupo G, el número de elementos de G es el *orden* de G, y se denota con $|G|$. Cuando el número de elementos de un grupo no es finito, su orden es infinito.

Ejemplos
Para $c \in Z^+$, $n > 1$, $(\mathbb{Z}_n, +)$ es un grupo abeliano. $|(\mathbb{Z}_n, +)| = n$
Si p es primo, $(\mathbb{Z}_p^*, .)$ es un grupo abeliano. $|(\mathbb{Z}_p^*, .)| = p - 1$
Veamos el ejemplo de $(\mathbb{Z}_6, +)$ y $(\mathbb{Z}_7^*, .)$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Ejemplo

Sea $(\mathbb{Z}_n, +, .)$ un anillo, el conjunto formado por las unidades de dicho anillo forman un grupo multiplicativo $(U_n, .)$. Además $|(U_n, .)| = \varphi(n)$

Veamos el ejemplo de U_9

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Teorema

Sean $(G, \circ)$ y $(H, *)$ grupos. Definimos la operación binaria $\cdot$ en $G \times H$ como $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2)$. Entonces $(G \times H, \cdot)$ es un grupo llamado *producto directo* de G y H.

Ejemplo

Sea $(\mathbb{Z}_2, +)$ y $(\mathbb{Z}_3, +)$. Entonces $(\mathbb{Z}_2 \times \mathbb{Z}_3, \cdot)$ es un grupo donde el neutro es $(0, 0)$ y, por ejemplo, $(1, 2)$ y $(1, 1)$ son inversos.

Teorema

Para cualquier grupo G,

- el neutro de G es único.
- el inverso de cada elemento de G es único.
- $\forall a, b, c \in G$ y $ab = ac$, entonces $b = c$. (cancelativa por izquierda)
- $\forall a, b, c \in G$ y $ba = ca$, entonces $b = c$. (cancelativa por derecha)

Subgrupo

Sea G un grupo y H un subconjunto no vacío de G. Si H es un grupo mediante la operación binaria de G, entonces H es un subgrupo de G.

Teorema

Si H es un subconjunto no vacío de un grupo G, entonces H es subgrupo de G si y sólo si $\forall a, b \in H$: (a) $ab \in H$ y (b) $a^{-1} \in H$.

Teorema

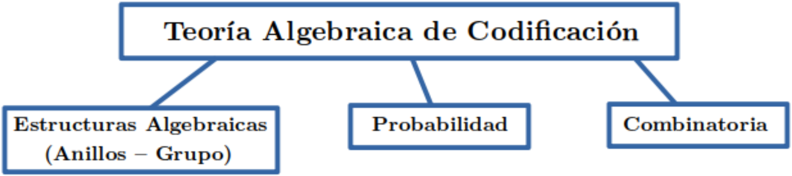
Si H es un subconjunto finito no vacío de un grupo G, entonces H es subgrupo de G si y sólo si $\forall a, b \in H$ se verifica que $ab \in H$.

Ejemplos de subgrupo

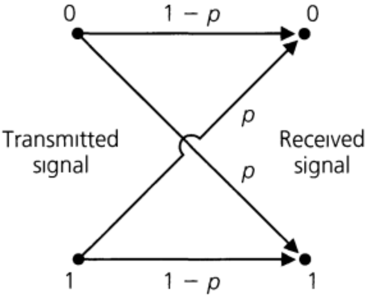
- Todo grupo G tiene como subgrupos a G y e. (subgrupos triviales).
- $H = \{0, 2, 4\}$ y $K = \{0, 3\}$ son subgrupos de $(\mathbb{Z}_6, +)$.
- $H = \{1, 8\}$ y $K = \{1, 4, 7\}$ son subgrupos de $(U_9, .)$.
- El grupo $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$ que a su vez en subgrupo de $(\mathbb{R}, +)$

Grupos y teoría de codificación.

Elementos de la teoría de la codificación.



Canal Simétrico Binario



Ejemplo:

Sea $\mathbb{Z}_2^5$ formado a partir del *producto directo* de cinco copias de $(\mathbb{Z}_2, +)$. Un elemento de $\mathbb{Z}_2^5$, por ejemplo, es $c = (1, 0, 1, 1, 0)$ que de ahora en más escribiremos $c = 10110$.

Al enviar cada *bit* de c si la probabilidad de transmición incorrecta es $p = 0,05$, la probabilidad de transmitir sin errores es $0,95^5 \approx 0,77$ ya que consideraremos que la transmición de cada *bit* es un suceso independiente.

Si se envía $c = 10110$:

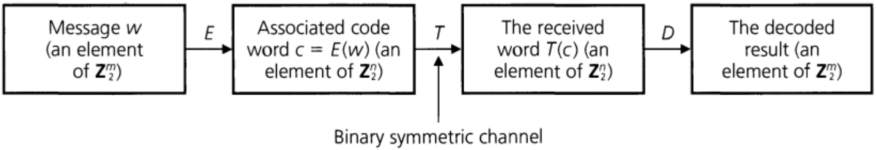
- ¿cuál es la probabilidad de recibir $r = 00110$?
  Se puede escribir $r = c + e$, donde e es un patrón de error. Como operamos en $(\mathbb{Z}_2^5, +)$, resulta $c = r + e$ y $e = c + r$. Para nuestro ejemplo:
  $e = 10110 + 00110 = 10000$, un patrón de error en la primera posición, por lo que la probabilidad de recibir r es $0,05 \cdot 0,95^4 \approx 0,041$.
- ¿cuál es la probabilidad de recibir $r = 00100$?
  $e = 10010$ y la probabilidad de recibir r es $0,05^2 \cdot 0,95^3 \approx 0,002$
- ¿cuál es la probabilidad de recibir una cadena r con dos errores respecto de c?
  Como el error estará en 2 de los 5 posiciones, la probabilidad buscada es
  $$\binom{5}{2} 0,05^2 \cdot 0,95^3 \approx 0,021$$

Teorema

Sea $c \in \mathbb{Z}_2^n$. Para la transmición de c a través de un canal simétrico binario con probabilidad de transmición incorrecta p,

- La probabilidad de recibir $r = c + e$, donde e es un patrón de error particular, formado por k unos y $(n-k)$ ceros, es $p^k \cdot (1-p)^{n-k}$
- La probabilidad de que ocurra k errores en la transmición es $\binom{n}{k} p^k \cdot (1-p)^{n-k}$

Para mejorar la precisión en un canal simétrico binario pueden usarse ciertos tipos de esquema de codificación. Sea $W \subseteq \mathbb{Z}_2^m$ el conjunto de mensajes (w) por transmitir, $E : W \to \mathbb{Z}_2^n$ la función de codificación tal que $E(w) = c$, $T(c) = r$ la función de transmición y $D(r)$ la función de decodificación con $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. En este esquema, llamaremos al par ordenado (n, m) *código de bloque*.



Ejemplos:

Código de verificación de paridad

Código de bloque $(m+1,m)$ para $m=8$, $E:\mathbb{Z}_2^8\to\mathbb{Z}_2^9$ con $E(w)=w_1w_2w_3w_4w_5w_6w_7w_8w_9$ tal que $w_9\equiv(w_1+w_2+w_3+w_4+w_5+w_6+w_7+w_8)(mod 2)$

Podríamos detectar errores sencillos en la transmición, pero parece que no hay manera de corregirlos. Porque si, por ejemplo, $w=11010110$, $E(w)=110101101$ y recibimos $r=T(c)=T(E(w))=100101101$ sabemos que ha ocurrido al menos un error de transmición pero, de ser un error sencillo, no sabemos en qué posición ha ocurrido.

Para $p=0,001$, la probabilidad de enviar 110101101 y cometer a lo sumo un error en la transmición es

$$0,999^9+\binom{9}{1}0,001\cdot 0,999^8\approx 0,999964$$

Si detectamos un error y podemos retransmitir una señal de regreso al transmisor para que repita la palabra codificada, y continuamos este proceso hasta que la palabra recibida tenga un número par de unos, entonces la probabilidad de enviar y recibir 110101101 es aproximadamente igual a $0,999964$. Lo que es una mejora respecto a la probabilidad sin este esquema de codificación, la cual es $0,999^8=0,992028$.

Ejemplos:

Código de triple repetición

Código de bloque $(3m, m)$. Permite detectar y corregir errores simples en la transmición. Si $m = 8$, $E : \mathbb{Z}_2^8 \to \mathbb{Z}_2^{24}$ con $E(w) = w_1w_2w_3 \cdots w_8w_1w_2w_3 \cdots w_8w_1w_2w_3 \cdots w_8$

La función decodificadora $D : \mathbb{Z}_2^{24} \to \mathbb{Z}_2^8$ se guía por la regla de la mayoría. No puede detectar errores dobles (o más).

por ejemplo: $T(c) = 101001110011011110110110 \to d = 10110111$

Respecto a la probabilidad, si $p = 0,001$, la probabilidad de transmitir correctamente 1 bit es $0,999^3 + \binom{3}{1}0,001 \cdot 0,999^2 \approx 0,999997$. Por lo que la de transmitir 8 bits es $(0,999997)^8 \approx 0,999976$, a penas un poco mejor que el código de verificación de paridad, aunque este último a veces necesita de la retransmición del mensaje.

Grupos y teoría de codificación.

Homomorfismos, isomorfismos y grupos cíclicos

Homomorfismo e isomorfismo

Si $(G, \circ)$ y $(H, *)$ son grupos y $f : G \to H$, entonces f es un *homomorfismo de grupos* si $\forall a, b \in G$ se verifica que
$f(a \circ b) = f(a) * f(b)$.
Si además f es biyectiva, f es un *isomorfismo de grupos*. En tal caso, se dice que H y G son isomorfos.

Teorema

Sean $(G, \circ)$ y $(H, *)$ grupos con neutros respectivos e_G y e_H. Si $f : G \to H$ es un homomorfismo, entonces

- $f(e_G) = e_H$.
- $f(a^{-1}) = [f(a)]^{-1}$, para todo a en G.
- $f(a^n) = [f(a)]^n$ para todo a en G, con n entero.
- $f(S)$ es un subgrupo de H para cada subgrupo S de G.

Ejemplos

- Sean $(\mathbb{Z},+)$ y $(\mathbb{Z}_4,+)$, con $f(x)=[x]$ es homomorfismo de grupo porque: $f(x+y)=[x+y]=[x]+[y]=f(x)+f(y)$ para todo x e y en G.
- $f:(\mathbb{R}^+,.)\to(\mathbb{R},+)$, con $f(x)=log(x)$ es isomorfismo de grupo porque f es biyectiva, y $f(xy)=log(ab)=log(a)+log(b)=f(x)+f(y)$ para todo x e y en G.
- También es isomorfismo de grupo $f:(\{1,-1,i,-i\},.)\to(\mathbb{Z}_4,+)$, con f definida por

$$f(1)=[0] \qquad f(-1)=[2] \qquad f(i)=[1] \qquad f(-i)=[3]$$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Como se puede observar $i^1=i, \quad i^2=-1, \quad i^3=-i, \quad i^4=1$, tenemos que todo elemento de G es una potencia de i, y decimos, i genera a G. Se denota $G=<i>$.

Grupos cíclicos

Un grupo G es *cíclico* si existe un elemento $x \in G$ tal que para todo $a \in G$,$a = x^n$ para algún n entero.

Ejemplos

- Sean $(\mathbb{Z}_4, +)$ es cíclico porque [1] y [3] lo generan. Para el caso de [3]: 1.[3] = [3], 2.[3] = [2], 3.[3] = [1] y 4.[3] = [0]. Escibimos $H =< [3] >=< [1] >$.
- U_9 es cíclico porque 2 lo genera. Verificar.

Si un elemento no genera a todo el grupo, generará un subgrupo distinto al grupo.

Orden de un generador

Si G es un grupo y $a \in G$, el *orden de a*, que denotamos con $o(a)$, $| < a > |$.

Así por ejemplo, para U_9, $< 4 >= \{1, 4, 7\}$ por lo que $o(7) = 3$.

Teorema

Sea $a \in G$ con $o(a) = n$. Si $k \in \mathbb{Z}$ y $a^k = e$, entonces $n|k$.

Teorema

Sea G un grupo cíclico:

- Si $|G|$ es infinito, entonces G es isomorfo a $(\mathbb{Z}, +)$.
- Si $|G| = n$, con $n > 1$, entonces G es isomorfo a $(\mathbb{Z}_n, +)$.

Teorema

Cualquier subgrupo de un grupo cíclico es cíclico.

Ejemplo

Verificar que $f : U_9 \to (\mathbb{Z}_6, +)$ son isomorfos.

Grupos y teoría de codificación.

Clases laterales y el teorema de Lagrange

Clase lateral

Si H es un subgrupo de G, entonces para cualquier $a \in G$, el conjunto $aH = \{ah/h \in H\}$ es una *clase lateral izquierda* de H en G. El conjunto $Ha = \{ha/h \in H\}$ es una *clase lateral derecha* de H en G. Si la operación en G es suma, escribimos $a + H$ en vez de aH.

Lema

Si H es un subgrupo de un grupo finito G, entonces para cualquier $a, b \in G$:

(a) $|aH| = |H|$ (b) $aH = bH$ o $aH \cap bH = \emptyset$.

Ejemplo

Verificar el lema para $G = (\mathbb{Z}_{12}, +)$ y $H = \{0, 4, 8\}$.

Teorema de Lagrange

Si G es un grupo finito de orden n y H es un subgrupo de orden m, entonces $m|n$.

Corolario 1

Si G es un grupo finito de orden n y $a \in G$, entonces $o(a)|n$.

Corolario 1

Cualquier grupo de orden primo es cíclico.

Grupos y teoría de codificación.

Métrica de Hamming.

Definición de distancia

Para cualquier elemento $x = x_1 x_2 \cdots x_n \in \mathbb{Z}_2^n$, el *peso de* x, que se denota con $p(x)$, es el número de componentes x_i de x, para $1 \leq i \leq n$, tales que $x_i = 1$. Si $y \in \mathbb{Z}_2^n$, la *distancia entre* x *e* y, que se denota con $d(x, y)$, es el número de componentes tales que $x_i \neq y_i$, para $1 \leq i \leq n$.

Lema

Para todos $x, y \in \mathbb{Z}_2^n$, $p(x + y) \leq p(x) + p(y)$.

Ejemplo: Para $n = 5$, sean $x = 01001$ e $y = 11101$, calcular $p(x)$, $p(y)$, $p(x + y)$, $d(x, y)$

Teorema

La función distancia d definida en $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ satisfase lo siguientes $\forall x, y, z \in \mathbb{Z}_2^n$.

a) $d(x, y) \geq 0$

b) $d(x, y) = 0 \Leftrightarrow x = y$

c) $d(x, y) = d(y, x)$

d) $d(x, z) \leq d(x, y) + d(y, z)$

Cuando una función satisface estas cuatro propiedades, recibe el nombre de *función distancia o métrica*, y decimos que $(\mathbb{Z}_2^n, d)$ es un *espacio métrico*. A la distancia definida anteriormente se la conoce como *Métrica de Hamming*.

Esfera

Para $n, k \in \mathbb{Z}^+$ y $x \in \mathbb{Z}_2^n$, la *esfera* de radio k con centro en x se define como $S(x, k) = \{y \in \mathbb{Z}_2^n \diagup d(x, y) \leq k\}$.

Teorema

Sea $E : W \to C$ una función de codificación con el conjunto de mensajes $W \subseteq \mathbb{Z}_2^m$ y el conjunto de palabras codificadas $E(W) = C \subseteq \mathbb{Z}_2^n$, donde $m < n$. Para $k \in \mathbb{Z}^+$, podemos:

- detectar errores de transmición de peso menor o igual a k si y sólo si la distancia mínima entre palabras codificadas es al menos $k + 1$.
- corregir errores de transmición de peso menor o igual a k si y sólo si la distancia mínima entre palabras codificadas es al menos $2k + 1$.

Ejemplo:
Si $W = \mathbb{Z}_2^2$, sea $E : W \to \mathbb{Z}_2^6$. Hallar:

- el conjunto de palabras codificadas.
- evaluar la capacidad de detección y de corrección de errores.
- la esfera de radio 1 y centro 000000. Analizar $D(x)$ para los x de esta esfera.
- la esfera de radio 1 y centro 010101. Analizar $D(x)$ para los x de esta esfera.

Grupos y teoría de codificación.

Verificación de paridad y matrices generadoras.

Matriz de codificación

Para $m, n \in \mathbb{Z}^+$ con $m < n$, la función $E : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ está dada por la matriz G de orden $m \times n$ sobre $\mathbb{Z}_2$ a la que llamaremos *matriz generadora del código.*

$$G = [I_m|A] \text{ tal que } E(w) = wG, \forall w \in \mathbb{Z}_2^m.$$

Matriz de verificación de paridad

Es una matriz H de orden $(n - m) \times n$ sobre $\mathbb{Z}_2$.

$H = [A^{tr}|I_{n-m}]$ tal que $H.(E(w))^{tr} = \mathbf{0}$ determinan las ecuaciones de verificación de paridad.

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

Cuando H no contiene una columna de ceros y ningún par de columnas iguales, se puede aplicar el siguiente algorítmo de decodificación.
Para cualquier $r \in \mathbb{Z}_2^n$, si $T(c) = r$, entonces analizaremos su síndrome, $H.r^{tr}$. De esta manera confrontaremos a r con la lista de palabras codificadas:

1. Si $H.r^{tr} = \mathbf{0}$ pensaremos que la transmición fue correcta y que r es la palabra codificada que fue transmitida. El mensaje decodificado consta entonces de las primeras m componentes de r.
2. Si $H.r^{tr}$ es igual a la i-ésima columna de H, pensaremos que hubo un error simple en la transmición y cambiamos la i-ésima componente de r para obtener la palabra codificada c. Esto se debe a que $H.r^{tr} = H.(c+e)^{tr} = H.c^{tr} + H.e^{tr}$.
   En este caso, las primeras m componentes de c producen el mensaje original.
3. Si no ocurre ninguno de los dos casos anteriores, pensaremos que hubo más de un error de transmición y que no podemos corregirlo.

Ejemplo: Sea $E : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$, G y H dadas en el ejemplo; resolver:

1. Hallar C, el conjunto de palabras codificadas.
2. Calcular la distancia mínima entre palabras y realice un comentario sobre la capacidad de detectar y corregir errores.
3. Hallar las ecuaciones de verificación de paridad.
4. Suponga que recibimos $r = 110110$, hallar $H.r^{tr}$ (llamado *síndome de* r). Si es posible, decodificar r.
5. Idem para $r = 000111$.