Resumen de Discretas 3

Elaborado por Christian Alexander Oliveros Labrador, Cohorte 13. Ing. Computación.

Actualizada: 08 de abril de 2016. El orden de los temas es basado en el cronograma del curso Enero-Marzo 2016.

Página web: oliveroschristian.wordpress.com

Índice

Primer Parcial

Números Enteros

Definición: ${}^{\mathbb{N}x\mathbb{N}}/_{\equiv} = \{[\langle n,0\rangle]: n \in \mathbb{N}^*\} \cup \{[\langle 0,n\rangle]: n \in \mathbb{N}^*\} \cup \{[\langle n,n\rangle]: n \in \mathbb{N}\} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}$

Aritmética:

- $[\langle a,b\rangle] + [\langle c,d\rangle] = [\langle a+c, b+d\rangle]$
- $[\langle a,b\rangle] * [\langle c,d\rangle] = [\langle a*c+b*d, a*d+b*d\rangle]$

Propiedades:

- *Cerradura/Clausura:*
  - $(\forall x,y \in \mathbb{Z})(x+y \in \mathbb{Z})$
  - $(\forall x,y \in \mathbb{Z})(x*y \in \mathbb{Z})$
- *Elemento Neutro:*
  - $(\forall x \in \mathbb{Z})\big((\exists y \in \mathbb{Z})(x+y=x)\big)$
  - $(\forall x \in \mathbb{Z})\big((\exists y \in \mathbb{Z})(x*y=x)\big)$
  - El elemento neutro de cada operador es único
- *Conmutatividad:*
  - $(\forall x,y \in \mathbb{Z})(x+y=y+x)$
  - $(\forall x,y \in \mathbb{Z})(x*y=y*x)$
- *Asociatividad:*
  - $(\forall x,y,z \in \mathbb{Z})(x+(y+z)=(x+y)+z)$
  - $(\forall x,y,z \in \mathbb{Z})(x*(y*z)=(x*y)*z)$
- *Distributividad (*/+):* $(\forall x,y,z \in \mathbb{Z})(x*(y+z)=x*y+x*z)$
- *Ley de Cancelación de la Multiplicación*: $(\forall x,y,z \in \mathbb{Z})(z \neq 0 \wedge z*x=z*y \Longrightarrow x=y)$
- *Divisor de Cero:* En los enteros no existen divisores de cero distintos de cero. $(\forall x,y \in \mathbb{Z})(x*y=0 \Longrightarrow x=0 \vee y=0)$

Orden en $\mathbb{Z}$:

- *Definición:* $[\langle a,b\rangle] \leq [\langle c,d\rangle] \Leftrightarrow a+d \leq b+c$
- *Propiedades*:
  - $m \leq m$
  - $m \leq n \wedge n \leq m \Longrightarrow m=n$
  - $m \leq n \wedge n \leq p \Longrightarrow m \leq p$
  - $m \leq n \wedge p \leq q \Longrightarrow m+p \leq n+q$
  - $m \leq n \wedge p > 0 \Longrightarrow m*p \leq n*p$
  - $m \leq n \wedge p < 0 \Longrightarrow n*p \leq m*p$
  - $m < n \vee n < m \vee m = n$

Valor Absoluto: $|x| = \begin{cases} x \; si \; x \geq 0 \\ x \; si \; x < 0 \end{cases}$

- *Propiedades:*
    - $|x| = |-x|$
    - $|x * y| = |x| * |y|$
    - $-|x| \leq x \leq |x|$
    - $p > 0 \Longrightarrow (|x| < p \Leftrightarrow -p < x < p)$
- *Desigualdad Triangular:* $(\forall x, y \in \mathbb{Z})(|x \pm y| \leq |x| + |y|)$

Orden Parcial: Una relación de orden parcial R de un conjunto A es tal que:

- $R \subseteq AxA$
- $R \; es \; Reflexiva$
- $R \; es \; Antisimetrica$
- $R \; es \; Transitiva$

Conjunto Bien Ordenado: Un conjunto parcialmente ordenado se dice bien ordenado si y solo si está linealmente (totalmente) ordenado y cada subconjunto no vacío tiene mínimo. Ejemplo: $\langle \mathbb{N}, \leq \rangle$.

Teorema: No existe entero positivo entre 0 y 1.

Divisibilidad en $\mathbb{Z}$

Definición: Dados dos enteros a y b decimos que "$a \; divide \; a \; b$" si y solo si existe un entero z, tal que $a * z = b$. Se denota divisibilidad como "$a|b$".

- *Teorema:* La relación de divisibilidad es Reflexiva y Transitiva.
- *Propiedades:*
    - $a|b \wedge a|c \Longrightarrow a|(b + c)$
    - $a|b \vee a|c \Longrightarrow a|(b * c)$
    - $a|(b \pm c) \wedge a|b \Longrightarrow a|c$
    - $c|c$
    - $c|0$
    - $1|b$
    - $c|1 \Longrightarrow c = \pm c$
    - $a > 0 \wedge b > 0 \wedge a|b \Longrightarrow a \leq b$
    - $d|c \wedge c|b \Longrightarrow d|b$
    - $b|c \wedge c|b \Leftrightarrow b = c \vee b = -c$
    - $b|c \Longrightarrow b|(c * d)$
    - $a|b \wedge a|c \Longrightarrow a|(b * x + c * y) \; (\forall x, y \in \mathbb{Z})$
    - $1 < b \wedge b|c \Longrightarrow \neg\big(b|(c + 1)\big)$

Unidad Multiplicativa: Se denominan unidades a los divisores de 1.

Teorema: Las únicas unidades en $\mathbb{Z}$ son ± 1. Corolario: Si los enteros a y b son mutuamente divisibles ($a|b \wedge b|a$) entonces $a = \pm b$.

Lema: Todo subconjunto no vacío de números enteros cerrado bajo la adición y sustracción contiene sólo al cero o contiene un número entero positivo mínimo del cual son múltiplos los demás.

Algoritmo de Euclides: Dados dos enteros a y b, con $b > 0$. Existen dos enteros únicos q, r tales que $a = b * q + r$ donde $0 \leq r < b$.

Máximo Común Divisor

Definición: Un entero positivo d se llama máximo común divisor de dos enteros a y b si y solo si:

1. $d|a \wedge d|b$
2. $(\forall e \in \mathbb{Z})(e|a \wedge e|b \Longrightarrow e|d)$

- *Notación:* Se denota $(a, b) = d = mcd(a, b)$.

Teorema: Dos enteros, no ambos nulos, a y b tienen un mcd, (a, b) no nulo. Este puede expresarse como combinación lineal de a y b con coeficientes enteros x, y. Es decir $(\exists x, y \in \mathbb{Z})(mcd(a, b) = d = ax + by)$.

Propiedades:

- $(a, 0) = |a|$
- $(a, b) = (b, a)$
- $(a, b) = (-a, b) = (a, -b)$
- $(a, b) = (|a|, |b|)$
- $(\forall k \in \mathbb{Z})\big((a * k, a) = |a|\big)$
- $(b, c) = (b, b + c) = (b, b - c)$
- $b = a * c + d \Longrightarrow (b, c) = (c, d)$

Recursión de Euclides: Si a, b son enteros positivos tales que $a = b * q + r$ con $0 \leq r < b$ entonces $(a, b) = (b, r)$.

Mínimo Común Múltiplo: Dados dos enteros positivos a y b, decimos que m es el mcm de a y b, denotado por $[a, b]$ o $mcm(a, b)$ si y solo si:

1. $a|m \wedge b|m$
2. $(\forall z \in \mathbb{Z})(a|z \wedge b|z \Longrightarrow m|z)$

Número Compuesto: Un entero positivo n, $n \neq 0$, es compuesto si existen enteros positivos x, y tales que $n = x * y$.

Número Primo: Un entero positivo, distinto de cero, p es primo si sus únicos divisores son 1 y p.

Teorema: Para p primo, $p|(b * c) \Longrightarrow p|b \vee p|c$.

Coprimos: Dos enteros a y b son coprimos o primos relativos si y solo si su mcd es 1. Se denota $a \perp b$.

Teorema: $b \perp c \wedge c|(b * d) \Longrightarrow c|d$.

Teorema Fundamental de la Aritmética: Cada entero positivo n puede ser escrito de forma única como producto de primos $n = p_0 * p_1 * p_2 * \ldots * p_{m-1}$ donde $p_0 \leq p_1 \leq p_2 \leq \cdots \leq p_{m-1}$.

Teorema: Existen infinitos números primos.

Álgebras

Definición: Consisten en un conjunto de elementos, llamado carrier y denotado por S, y operadores definidos sobre el conjunto. Los operadores son de la forma (tipo) $S^n \to S$ para $n \in \mathbb{N}$. El valor de n determina la aridad del operador, siendo Aridad-0 las constantes del álgebra. Un álgebra se denota de la siguiente forma $\langle S, \Phi \rangle$ donde Φ es una lista de operadores definidos en S. Por ejemplo:

- $\langle \mathbb{Z}, + \rangle$ es un álgebra.
- $\langle \{True, False\} = \mathbb{B}, \vee, \wedge, \neg \rangle$ es un álgebra.
- $\langle \mathbb{P}, *, \div \rangle$, siendo $\mathbb{P}$ el conjunto de los números pares, no es un álgebra ya que $a \div 0$ no está definido.

Firma: Manera estandarizada de escribir un álgebra, es escrita de operadores de mayor aridad a operadores de menor aridad, $\langle S^n \to S, S^n \to S, S^{n-1} \to S, \ldots, S^0 \to S \rangle$. Dos álgebras tienen la misma firma si:

1. Tienen el mismo número de operadores.
2. Operadores correspondientes del mismo tipo.

Ejemplo: $\langle \mathbb{B}, \vee, \wedge, \neg \rangle$ y $\langle \mathcal{P}(A), \cup, \cap, (\,)^c \rangle$ tienen la misma firma, pero $\langle \mathbb{B}, \vee, \wedge, \neg \rangle$ y $\langle \mathcal{P}(A), (\,)^c, \cup, \cap \rangle$ tienen firma distinta.

Identidad: Un elemento 1 en S (no es necesariamente el 1 de los números naturales), es una identidad izquierda de un operador binario $\circ$ sobre S si y solo si $(\forall b \in S)(1 \circ b = b)$. Se dice identidad derecha si y solo si $(\forall b \in S)(b \circ 1 = b)$. Si un elemento es identidad derecha e izquierda, entonces se dice el operador $\circ$ tiene identidad 1.

Teorema: Si c es identidad izquierda de $\circ$ y d es identidad derecha de $\circ$ entonces $c = d$.

Identidad: Un elemento 0 en S (no es necesariamente el 0 de los números naturales), es un cero o absorbente izquierdo de un operador binario $\circ$ sobre S si y solo si $(\forall b \in S)(0 \circ b = 0)$. Se dice cero o absorbente derecho si y solo si $(\forall b \in S)(b \circ 0 =)$. Si un elemento es absorbente derecho e izquierdo, entonces se dice el operador $\circ$ tiene cero o absorbente 0.

Teorema: Si c es un cero izquierdo de $\circ$ y d es un cero derecho de $\circ$ entonces $c = d$.

Inverso: Sea 1 la identidad de un operador binario sobre S. Entonces b tiene inverso derecho o izquierdo c con respecto al operador si:

- $b \circ c = 1$ (Inverso Derecho)
- $c \circ b = 1$ (Inverso Izquierdo)

Teorema: Si li es un inverso izquierdo y ri es un inverso derecho de un elemento b con respecto a un operador asociativo $\circ$, entonces $li = ri$. (Operador asociativo quiere decir $x \circ (y \circ z) = (x \circ y) \circ z$)

Tabla de Operador: Es una forma de representar un operador de un conjunto finito. Ejemplo: $\langle\{0,1\},*\rangle$

*	0	1
0	0	0
1	0	1

Operador Cerrado: Un subconjunto T de un conjunto S es cerrado bajo un operador si, aplicando el operador a los elementos de T produce un resultado en T.

Notación: $\langle S,\circ\rangle\ donde\ \circ: TxT \longrightarrow T$ El conjunto T es cerrado bajo el operador $\circ$.

Subálgebra: $\langle T,\Phi\rangle$ es Subálgebra de $\langle S,\Phi\rangle$ si:

1. $\phi \subset T \subseteq S$.
2. T es cerrado bajo cada operador en Φ.

Semigrupo: Es un álgebra $\langle S,\circ\rangle$ donde $\circ$ es un operador binario y asociativo.

Monoide: Es un semigrupo con identidad para el operador $\circ$, $\langle S,\circ,1\rangle$.

Submonoide: Un submonoide $\langle T,\circ,1\rangle$ de un monoide $\langle S,\circ,1\rangle$ es tal que:

1. $\phi \subset T \subseteq S$.
2. T es cerrado bajo cada operador en Φ.
3. $1 \in T$.
4. $\circ$ es binario y asociativo.

Grupos

Grupo: Es un monoide $\langle S,\circ,1\rangle$ en el cual cada elemento de S tiene un inverso con respecto al operador $\circ$, es decir $(\forall b \in S)(b^{-1} \in S)$. Una definición alternativa es:

1. $\langle S,\circ\rangle$ es un álgebra donde el operador es binario y asociativo.
2. Existe un elemento en S tal que es identidad del operador $\circ$.
3. Cada elemento de S tiene un inverso.

Grupo Abeliano: Es un grupo donde el operador $\circ$ es conmutativo (Abeliano).

Grupo Aditivo de los Enteros Modulo n: Sea $n > 0$. Se define $\oplus$ para b y c en $\{0,1,\dots,n-1\}$ como $b \oplus c = (b+c) mod\ n$ donde $mod\ n$ es el resto de dividir entre n. Entonces $Mn = \langle\{0,1,\dots,n-1\},\oplus,0\rangle$ es un grupo aditivo de los enteros modulo n.

Propiedades de Grupos:

- $b = (b^{-1})^{-1}$.
- *Cancelación:*
  - $b \circ d = c \circ d \equiv b = c$.
  - $d \circ b = d \circ c \equiv b = c$.

- *Solución Única:*
    - $b \circ x = c \equiv x = b^{-1} \circ c$.
    - $x \circ b = c \equiv x = c \circ b^{-1}$.
- *Uno a Uno:*
    - $b \neq c \equiv d \circ b \neq d \circ c$.
    - $b \neq c \equiv b \circ d \neq c \circ d$.
- *Sobre:*
    - $(\exists x \in S)(b \circ x = c)$.
    - $(\exists x \in S)(x \circ b = c)$.

Potencias Integrales: b^n de un elemento b de un grupo $G = \langle S, \circ, 1 \rangle$ con $n \in \mathbb{Z}$:

- $b^0 = 1$ (Identidad del Operador).
- $b^n = b^{n-1} \circ b$ (Para $n > 0$).
- $b^{-n} = (b^{-1})^n$ (Para $n > 0$).

Propiedades:

1. $b^n \circ b^m = b^{n+m}$ para $m, n \in \mathbb{Z}$.
2. $(b^m)^n = b^{m*n}$ para $m, n \in \mathbb{Z}$.
3. $b^n = b^p \equiv b^{n-p} = 1$ para $p, n \in \mathbb{Z}$.

Orden de un Elemento: El orden de un elemento b de un grupo con identidad 1, $ord.b$, es el menor entero positivo m tal que $b^m = 1$ o ∞ si tal m no existe.

Teorema: El orden de cada elemento de un grupo finito es finito.

Subgrupos: Una subálgebra $G' = \langle T, \circ, 1 \rangle$ de un grupo $G = \langle S, \circ, 1 \rangle$ es un subgrupo si cada elemento de T tiene inverso con respecto al operador $\circ$ y ese inverso está en T. Además, debe ser un submonoide de G y $1 \in T$.

Tipos:

- Triviales: G y $\langle \{e\}, \circ, e \rangle$.
- No triviales: Todos los que no son los dos anteriores.

Teorema: La relación "$es\ subgrupo\ de$" es una relación de orden parcial.

Teorema: Dado un grupo G, un subconjunto H de G es un subgrupo de G si y solo si:

1. H es cerrado bajo la operación $\circ$ de G.
2. El elemento neutro de G está en H.
3. Para todo $a \in H$ se cumple que $a^{-1} \in H$.

Propiedad de Grupos: Para un grupo $G = \langle S, \circ, 1 \rangle$: $(b \circ c)^{-1} = c^{-1} \circ b^{-1}$.

Propiedad de Grupos: Para un grupo $G = \langle S, \circ, 1 \rangle$, sean $a, b \in G$. Si $a^n = b^n$, $a^m = b^m$ y $(m, n) = 1$ entonces $a = b$.

Definición Débil de Grupo I: Un grupo $G = \langle S, \circ, e \rangle$ (e es identidad del operador) es un conjunto no vacío S con una operación binaria $\circ$ sobre G, tal que:

1. La operación $\circ$ es asociativa.
2. Existe un elemento $e \in G$ tal que $(\forall x \in G)(x \circ e = x)$.
3. Para cada g en G existe un g^{-1} en G tal que $g \circ g^{-1} = e$.

Lema: Si el operador $\circ$ es binario sobre un grupo G y $a, b, c, d \in G$ tal que $a = b \wedge c = d \Longrightarrow a \circ c = b \circ d$.

Definición Débil de Grupo II: Un grupo G es un álgebra $G = \langle S, \circ \rangle$ tal que para todo $a, b \in G$ $a \circ x = b \wedge y \circ a = b$ tienen solución única.

Idempotencia: Un álgebra $G = \langle S, \circ \rangle$ tienen un elemento idempotente si y solo si $(\exists a \in G)(a \circ a = e)$.

> *Observación:* Un álgebra puede tener más de un elemento idempotente, pero un grupo infinito tiene un único elemento idempotente, que es la identidad.

Finitud de Grupo: Un grupo G es finito si y solo si S es finito, de lo contrario es infinito.

Definición Débil de Subgrupo: Dado un grupo G, un subconjunto no vacío H de G es un subgrupo si y solo si:

1. H es cerrado bajo el operador $\circ$ de G.
2. $(\forall a \in H)(a^{-1} \in H)$

Teorema: Dado un grupo G. Un subconjunto, no vacío, H de G es subgrupo de G si y solo H es cerrado bajo la operación de G.

Teorema: Sea b un elemento de un grupo G, sea $Sb = \{b^k : k \in \mathbb{Z}\}$. Entonces Sb es subgrupo de G.

Teorema: Sea $G = \langle S, \circ, e \rangle$ un grupo. Sean $G_1 = \langle S_1, \circ, e \rangle$ y $G_2 = \langle S_2, \circ, e \rangle$ subgrupos de G. Entonces $G_1 \cap G_2$ es un subgrupo de G.

Teorema: Un subconjunto no vacío H de un grupo G, es subgrupo de G si y solo si $(\forall a, b \in H)(a \circ b^{-1} \in H)$.

Segundo Parcial (Posible Final de Materia del Primer Parcial)

Depende de cómo se esté dictando el curso.

Clases Laterales

Definición: Dado H un subgrupo de un grupo G, una clase lateral a derecha de H en G es un subconjunto de G de la forma $Hg = \{x \in G : x = h \circ g \wedge h \in H\}$. Una clase lateral izquierda de H en G es de la forma $Hg = \{x \in G : x = g \circ h \wedge h \in H\}$.

> *Observación:* $gH = g \circ H$ y $Hg = H \circ g$.

Definición de Partición: $P = \{P_1, \dots, P_n\}$ es una partición de un conjunto A si y solo si:

1. $(\forall i)(P_i \neq \phi)$.

2. $(\forall i, j \wedge 1 \leq i, j \leq n \wedge i \neq j)\big(P_i \cap P_j = \phi\big)$.
3. $\bigcup_{1 \leq i} P_i = A$.

Lema: Si H es un subgrupo de un grupo G, entonces las clases a derecha (también sucede con las clases a izquierda) de H en G forman una Partición de G.

Conjunto Cociente: Se define el Conjunto Cociente Derecho como ${}^{G}/_{H\sim} = \{Hg : g \in G\}$. El Conjunto Cociente Izquierdo ${}^{G}/_{\sim H} = \{gH : g \in G\}$. Cuando ${}^{G}/_{H\sim} = {}^{G}/_{\sim H}$ se llama Grupo Cociente.

Lema: Si G es un grupo y H es un subgrupo de G. Toda clase lateral a derecha (izquierda) de H en G tiene el mismo número de elementos.

Teorema de Lagrange: Si G es un grupo Finito y H es un subgrupo de G, entonces el orden de H (Número de elementos) divide el orden de G (Número de elementos), es decir $|G| = n * |H|$.

> *Corolario:* Si G es un grupo Finito y g es un elemento de G de orden m (menor $m > 0$ tal que $g^m = e$) entonces el orden de g divide al orden de G.
>
> *Corolario:* Si G es un grupo Finito de orden n y g un elemento de G, entonces $g^n = e$.
>
> *Uso:* Con este teorema se puede saber el tamaño de todos los subgrupos de un grupo, sólo hay que buscar los divisores del tamaño del grupo. Con esa información y con los elementos del grupo se pueden construir los subgrupos con relativa facilidad. El subgrupo de tamaño 1 es el que sólo contiene la identidad y el subgrupo del tamaño del grupo es el grupo como tal. Si el tamaño del grupo es par entonces como mínimo hay un elemento, distinto a la identidad, que es su propio inverso. Esto se debe a que si le restamos 1 a esa cantidad par de elementos, es decir quitamos la identidad, el resto de los elementos tiene que tener inverso, pero tenemos una cantidad impar de elementos. Suponiendo que tenemos el máximo número de elementos pares de inversos que son distintos entre ellos, siempre sobrará uno por lo que ese elemento que sobra tiene que ser su propio inverso y así mantener que todo elemento en un subgrupo tiene a su inverso en el subgrupo.

Índice de Subgrupo: Si H es un subgrupo de G, el Índice de H en G, $[G : H]$, es el número de clases laterales a derecha (izquierda) de H en G.

> *Corolario:* Si G es un grupo finito, entonces $|G| = [G : H] * |H|$.

Teorema: Si G es un grupo Abeliano y H es un subgrupo de G entonces toda clase lateral derecha de H en G es también clase lateral izquierda $Hg = gH$ ($g = h^{-1} \circ g \circ h$).

Subgrupos Normales: Un subgrupo H de un grupo G es normal en G si y solo si para todo $g \in G$ se tiene que su clase lateral a derecha de H en G es igual a su clase lateral a izquierda de H en G.

Segundo Parcial

Este es el comienzo de la materia del segundo parcial como tal.

Homomorfismos

Definición: Sean $A = \langle S, \Phi \rangle$ y $\hat{A} = \langle \hat{S}, \hat{\Phi} \rangle$ dos álgebras con la misma firma. Una función $h: S \to \hat{S}$ es un homomorfismo de A en $\hat{A}$ si y solo si:

1. Para cada par de operadores nulos (constantes) correspondientes c en Φ y $\hat{c}$ en $\hat{\Phi}$ se tiene que $h(c) = \hat{c}$.
2. Para cada par de operadores unarios $\sim$ en Φ y $\hat{\sim}$ en $\hat{\Phi}$ se tiene que $h(\sim b) = \hat{\sim} h(b)$.
3. Para cada par de operadores binarios $\circ$ en Φ y $\hat{\circ}$ en $\hat{\Phi}$ se tiene que $h(a \circ b) = h(a) \,\hat{\circ}\, h(b)$.

Tipos:

- Momomorfismo: homomorfismo inyectivo.
- Epimorfimso: homomorfismo sobreyectivo.
- Isomorfismo: homomorfismo biyectivo.
- Automorfismo: homomorfismo

Teorema: Sea h un homomorfismo de $A = \langle S, \Phi \rangle$ en $\hat{A} = \langle \hat{S}, \hat{\Phi} \rangle$. Entonces $\langle h.S, \hat{\Phi} \rangle$ es una subálgebra de $\hat{A}$, se llama la imagen homomórfica de A bajo h.
$(h.S = \{g \in \hat{S} : (\exists a \in S)(g = h(a))\})$.

Teorema: Un homomorfismo envía identidades en identidades e inversos en inversos.

Teorema: Si $\hat{A}$ es una imagen isomórfica de A entonces A es una imagen isomórfica de $\hat{A}$.

Grupos Cíclicos

Definición: Sea $G = \langle S, \circ, e \rangle$ un grupo, G es cíclico si y solo si $S = \{a^k : k \in \mathbb{Z}\}$, donde a es el generador. Se le llama Grupo Cíclico de Generador a.

Teorema: Todo grupo cíclico es Abeliano.

Teorema: Todo subgrupo de un grupo cíclico es cíclico.

Teorema: Sea G un grupo cíclico tal que $|G| = n$, con $n > 1$, y de generador a. Entonces:

- $(\forall d \in \mathbb{N})\left((d, n) = 1 \Longrightarrow a^d \; es \; generador \; de \; G\right)$
- $(\forall d \in \mathbb{Z})\left(d | n \wedge d \neq 1 \Longrightarrow a^d \; no \; es \; generador \; de \; G\right)$

Teorema: Un grupo cíclico **infinito** es isomorfo al grupo aditivo de los enteros ($\langle \mathbb{Z}, +, 0 \rangle$). Sea G un grupo cíclico infinito de generador a, el isomorfismo está definido de la siguiente forma:

$$h: S \to \mathbb{Z}$$

$$h.g = h(g) = h(a^m) = m$$

Teorema: Un grupo cíclico **finito** de n elementos es isomorfo al grupo aditivo de los enteros modulo n, $Mn = \langle \{0, 1, \ldots, n-1\}, \oplus, 0 \rangle$. El isomorfismo está definido de la siguiente forma:

$$h: S \to \{0, 1, \ldots, n-1\}$$

$$h.g = h(g) = h\left(a^k\right) = (k) mod \; n$$

Teorema: Sea G un grupo cíclico con identidad e y generador $b \in G$ de orden m. Entonces el elemento c de orden n genera al grupo si y solo si $(m,n) = 1$. Ejemplo: En $\langle \mathbb{Z}_6, +_6, \bar{0} \rangle$ el generador es 1, con $ord(\bar{1}) = 6$. Los coprimos de 6 menores que 6 son 1 y 5, $(\bar{1})^5 = c$ y genera a $\mathbb{Z}_6$.

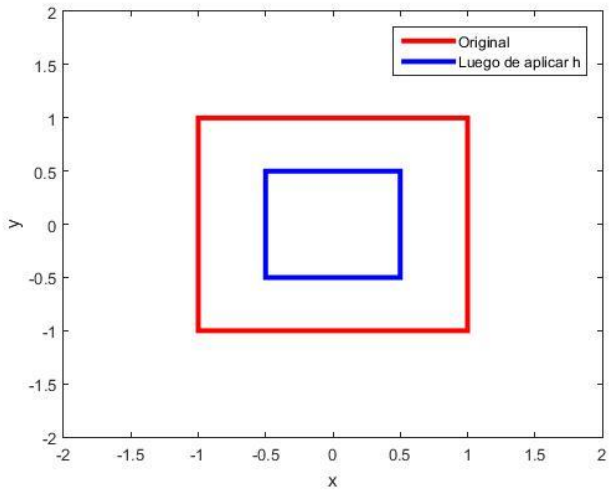
Grupo de Transformaciones

Definición: Vamos a considerar todas las funciones de un conjunto es si mismo que son biyectivas (En general una transformación es una función de un conjunto en otro).

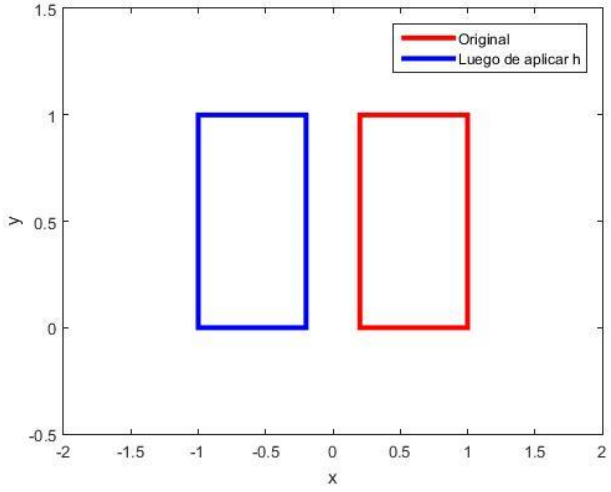
Si consideramos la operación de composición de funciones, $\circ$, $f \circ g = f(g)$. Sea $T = \{f: S \to S: f \ es \ biyectiva\}$ y sea Id la identidad de la composición de funciones, entonces $\langle T, \circ, Id \rangle$ es un grupo.

Ejemplos:

- $h(x,y) = (x/2, y/2)$ (Dividir entre dos todas las distancias).



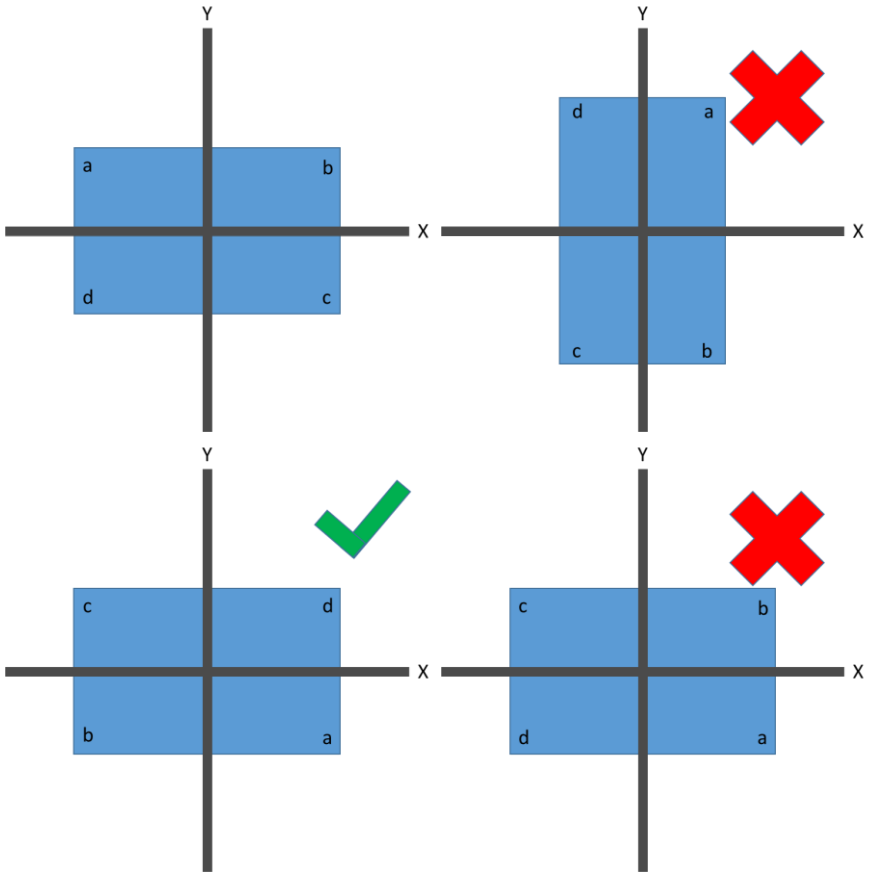
- $h(x,y) = (-x,y)$ (Reflejo contra eje X).



Simetrías: Son transformaciones que preservan la distancia de los puntos. Es decir, siendo ϕ una transformación, $distancia(p,q) = distancia(\phi(p), \phi(q))$.

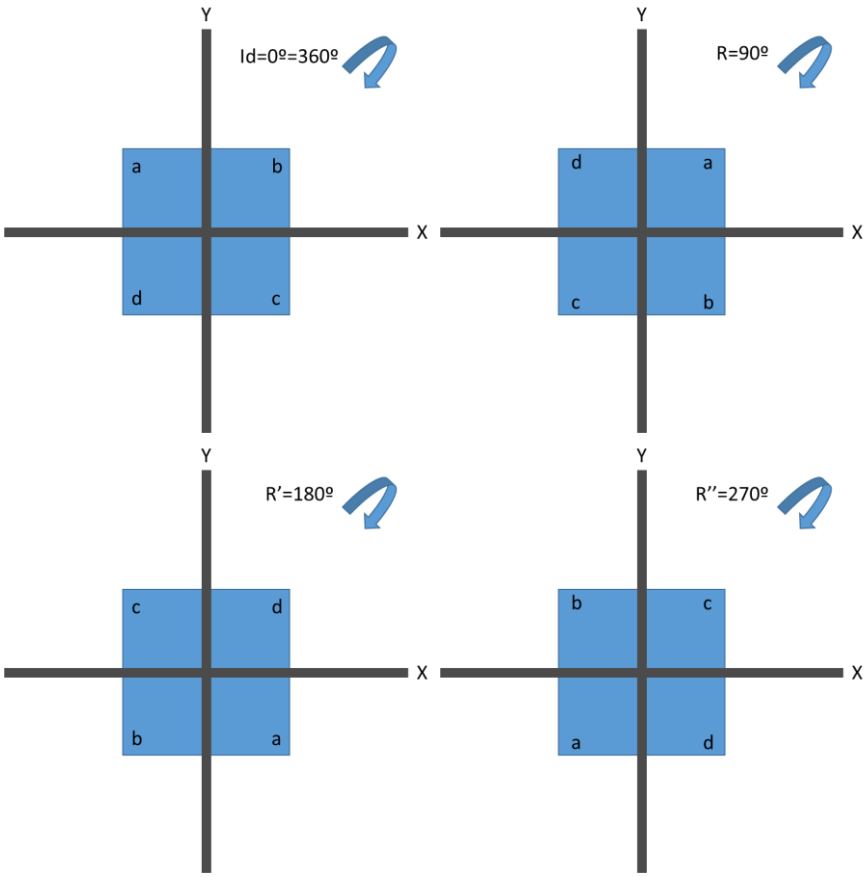
Simetrías de Figuras Geométricas:

Una simetría de una figura geométrica es una trasformación que toma la figura y la transforma en una figura igual, preservando las distancias (Vértices van a Vértices). Ejemplo:

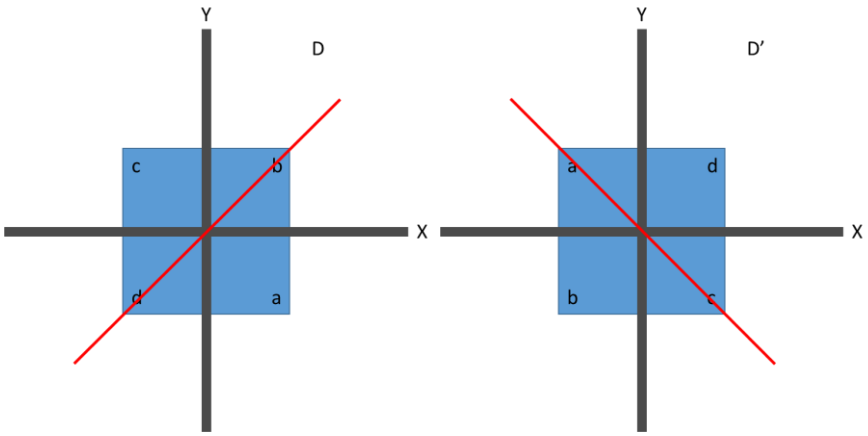


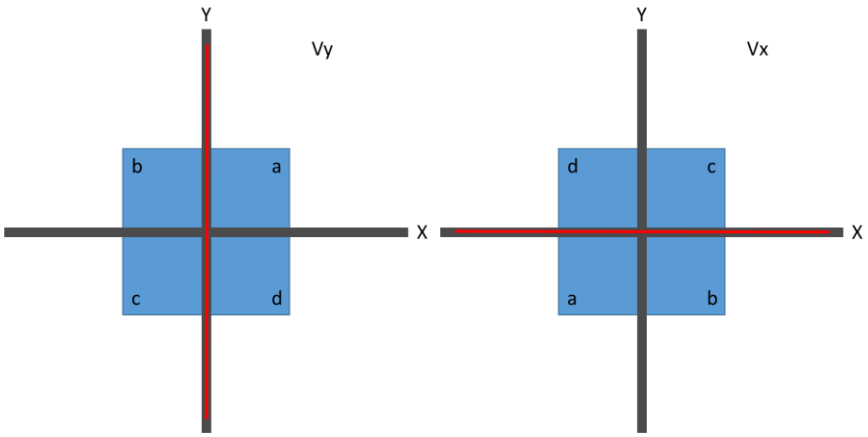
Simetrías del Cuadrado:

Rotaciones:



Reflexiones:





Grupo: $GS\square = \langle \{Id, R, R', R'', D, D', Vx, Vy\}, \circ, Id \rangle$.

Anillos

Definición: Un anillo $A = \langle S, \oplus, \otimes \rangle$ es un conjunto S con dos operadores binarios $\oplus$ y $\otimes$ tales que:

1. $\langle S, \oplus \rangle$ es un grupo Abeliano.
2. $\langle S, \otimes \rangle$ es un semigrupo (Asociatividad).
3. Distributividad: $\forall a, b, c \in A$
   a. $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
   b. $(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$

Teorema: Si $A = \langle S, \oplus, \otimes \rangle$ es un anillo con neutro aditivo e_+ e inversos aditivos denotados por $-$, entonces para todo $a, b \in A$:

- $e_+ \otimes a = a \otimes e_+ = e_+$
- $a \otimes (-b) = (-a) \otimes b = -(a \otimes b)$
- $(-a) \otimes (-b) = a \otimes b$

Teorema: Para todo $n \in \mathbb{Z}$ y para todo par $a, b \in A$ se tiene que (siendo na la potencia aditiva) $n(a \otimes b) = (na) \otimes b = a \otimes (nb)$.

Subanillos: Un subanillo $B = \langle S', \oplus, \otimes \rangle$ de un anillo $A = \langle S, \oplus, \otimes \rangle$ es un subconjunto B de A tal que B es un anillo con las operaciones que hereda de A.

Teorema: Dado un anillo $A = \langle S, \oplus, \otimes \rangle$ y un subconjunto S' de S , $B = \langle S', \oplus, \otimes \rangle$ es subanillo de A si y solo si $\langle S', \oplus \rangle$ es subgrupo de $\langle S, \oplus \rangle$ y la operación del producto es cerrada en $\langle S', \otimes \rangle$.

Teorema: Dado un anillo $A = \langle S, \oplus, \otimes \rangle$ y un subconjunto S' de S , un álgebra $B = \langle S', \oplus, \otimes \rangle$ es subanillo de A si y solo si $(\forall a, b \in S')(a \oplus (-b) \in S' \wedge a \otimes b \in S')$ (Recordar que – es inverso aditivo).

Homomorfismo de Anillos: Dado un anillo $A = \langle S, \oplus, \otimes \rangle$ y un anillo $A' = \langle S', \oplus', \otimes' \rangle$ una aplicación (función) $\varphi: S \to S'$ es homomorfismo de anillos si conserva las operaciones:

1. $\varphi(a \oplus b) = \varphi(a) \oplus' \varphi(b)$.
2. $\varphi(a \otimes b) = \varphi(a) \otimes' \varphi(b)$.
3. φ es un homomorfismo entre $\langle S, \oplus, 0 \rangle$ y $\langle S', \oplus', 0' \rangle$.

Teorema: Sean $A = \langle S, \oplus, \otimes \rangle$ y $A' = \langle S', \oplus', \otimes' \rangle$ anillos. Si $\varphi: S \to S'$ es un homomorfismo de anillos. Entonces para todo $a \in A$ y $n \in \mathbb{Z}$ se cumple:

1. $\varphi(0) = 0'$.
2. $\varphi(1) = 1'$.
3. $\varphi(n\ a) = n\ \varphi(a)$ (Potencia aditiva).
4. $\varphi(a^n) = [\varphi(a)]^n$ (Potencia multiplicativa).

Unidad: En un anillo con identidad se denominan unidades a los elementos del anillo con inverso multiplicativo.

Teorema: Sean A y A' anillos, si $\varphi: S \to S'$ es un epimorfismo de anillos:

1. Si A tiene identidad entonces A' tiene identidad (Identidad Multiplicativa). (Recomendación: Pensar por que no existe epimorfismo entre $\langle \mathbb{Z}, +, * \rangle$ y $\langle n\mathbb{Z} = \{n * z : z \in \mathbb{Z}\}, +, * \rangle$).
2. Si $a \in A$ es unidad entonces:
    a. $\varphi(a^{-1}) = [\varphi(a)]^{-1}$
    b. $(\forall n \in \mathbb{Z}^+)(\varphi(a^{-n}) = [\varphi(a)]^{-n})$

Divisores de Cero: Dado un anillo A y $a \in A$, a es divisor de cero si existe $b \neq 0$ ($0 = e_+$) tal que $a \otimes b = 0 \vee b \otimes a = 0$. Nótese que 0 es divisor de 0 por propiedades de anillos.

Dominio de Integridad: Un Dominio de Integridad (D.I.) es un anillo de conmutativo con identidad (Segunda operación) $1 \neq 0$ ($e_+ \neq e_*$), sin divisores de cero distintos de cero.

Anillo de División: Dado un anillo A con identidad distinto de cero. A es un anillo de división si todo elemento de A distinto de cero tiene inverso multiplicativo.

Cuerpos:

Definición I: Es un anillo de División conmutativo.

Definición II: Un Cuerpo es un anillo conmutativo con identidad en el que todo elemento distinto de cero tiene inverso multiplicativo.

Definición III: Un anillo $A = \langle S, \oplus, \otimes \rangle$ es un cuerpo si y solo si:

1. $\langle S, \oplus \rangle$ es un grupo.
2. $\langle S - \{0\}, \otimes \rangle$ es un grupo.

Teorema: En el anillo $\mathbb{Z}_n$ (enteros modulo n, $\langle \{\bar{0}, \bar{1} \ldots, \overline{n-1}\}, +_n, *_n \rangle$), los divisores de cero con elementos que no son coprimos con n.

Corolario: Si p es primo, entonces $\mathbb{Z}_p$ no tiene divisores de cero distintos de ceros.

Teorema: Las leyes cancelativas se cumplen en un anillo A si y solo si A no tiene divisores de cero distintos de cero:

- $(\forall a \in A - \{0\})(a \otimes b = a \otimes c \implies b = c)$
- $(\forall a \in A - \{0\})(b \otimes a = c \otimes a \implies b = c)$

Teorema: Todo Cuerpo es un Dominio de Integridad (No todo D.I. es un cuerpo).

Teorema: Todo Dominio de Integridad finito es un cuerpo.

Tercer Parcial

Reticulados

Relaciones Sobre un Conjunto: Una relación sobre un conjunto A es un subconjunto de AxA.

Relación de Orden: Una relación de orden sobre un conjunto A, es una relación R tal que:

- Reflexiva: $(\forall a \in A)(\langle a, a\rangle \in R)$.
- Antisimétrica: $(\forall a, b \in A)(\langle a, b\rangle \in R \wedge \langle b, a\rangle \in R \Longrightarrow a = b)$.
- Transitiva: $(\forall a, b, c \in A)(\langle a, b\rangle \in R \wedge \langle b, c\rangle \in R \Longrightarrow \langle a, c\rangle \in R)$.

Conjunto Parcialmente Ordenado: Un Conjunto Parcialmente Ordenado (CPO) es un par ordenado $\langle A, R\rangle$, donde A es un conjunto y R una relación de orden sobre A.

> *Ejemplos:* $\langle \mathbb{R}, \leq\rangle$, $\langle \mathcal{P}(A), \subseteq\rangle$, $\langle \mathbb{N}, \leq\rangle$, $\langle D_n, |\ \rangle$
> ($D_n = Conjunto\ de\ todos\ los\ divisores\ positivos\ de\ n$, "|" $es\ la\ relación$ "$divide\ a$").

Conjunto Linealmente (Totalmente) Ordenado: Es un CPO en el cual cualquier par de elementos es comparable.

> *Ejemplos:*
>
> - Si: $\langle \mathbb{R}, \leq\rangle$, $\langle \mathbb{N}, \leq\rangle$, $\langle \mathbb{Z}, \leq\rangle$.
> - No: $\langle \mathcal{P}(A), \subseteq\rangle$, $\langle D_n, |\ \rangle$.

De ahora en adelante tomaremos $\langle A, \leq\rangle$ como CPO, con $\leq$ una relación de orden cualquiera sobre A y $B \subseteq A$.

Minimales: Los Minimales de B son el conjunto de elementos "más pequeños" de B:

- $Min(B) = \{x \in B: (\nexists b \in B)(b < x)\}$.
- $Min(B) = \{x \in B: (\forall b \in B)(b \leq x \Longrightarrow x = b)\}$.

Maximales: Los Maximales de B son el conjunto de elementos "más grandes" de B:

- $Max(B) = \{x \in B: (\nexists b \in B)(x < b)\}$.
- $Max(B) = \{x \in B: (\forall b \in B)(x \leq b \Longrightarrow x = b)\}$.

Mínimo: El elemento x es el mínimo de B si y solo si $x \in B \wedge (\forall b \in B)(x \leq b)$ (Notar que la diferencia con los Minimales es que aquí se pide que todos los elementos de B tengan arco con x, es decir sean comparables con x). Si tal elemento no existe entonces se dice que B no tiene mínimo. En lógica: $\min(B) = x \Leftrightarrow x \in B \wedge (\forall b \in B)(x \leq b)$.

Máximo: El elemento x es el máximo de B si y solo si $x \in B \wedge (\forall b \in B)(b \leq x)$ (Notar que la diferencia con los Maximales es que aquí se pide que todos los elementos de B tengan arco con x,

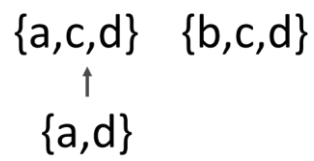
es decir sean comparables con x). Si tal elemento no existe entonces se dice que B no tiene máximo. En lógica: $\max(B) = x \Leftrightarrow x \in B \wedge (\forall b \in B)(b \leq x)$.

Cotas Superiores: Una cota superior es un elemento de A tal que es "mayor" a todo elemento de B ($x \in A \wedge (\forall b \in B)(b \leq x)$). El conjunto de las cotas superiores es $CotSup(B) = \{x \in A: (\forall b \in B)(b \leq x)\}$.

Cotas Inferiores: Una cota inferior es un elemento de A tal que es "menor" a todo elemento de B ($x \in A \wedge (\forall b \in B)(x \leq b)$). El conjunto de las cotas inferiores es $CotInf(B) = \{x \in A: (\forall b \in B)(x \leq b)\}$.

Ejemplo: De todo lo anterior:

$A = \{a, b, c, d\}$, $\langle \mathcal{P}(A), \subseteq \rangle$, $B = \{\{a, d\}, \{a, c, d\}, \{b, c, d\}\} \subseteq \mathcal{P}(A)$.



$Min(B) = \{\{a, d\}, \{b, c, d\}\}$.

$Max(B) = \{\{a, c, d\}, \{b, c, d\}\}$.

No existe $max(B)$ ni $min(B)$.

$CotSup(B) = \{A\}$.

$CotInf(B) = \{\phi, \{d\}\}$.

Supremo: Es la menor de las cotas superiores, es decir, $Sup(B) = min(CotSup(B))$.

Ínfimo: Es la mayor de las cotas inferiores, es decir, $Inf(B) = max(CotInf(B))$.

Notación de Ínfimo y Supremo:

- $Sup(\{x, y\}) = Sup(x, y) = x \vee y$.
- $Inf(\{x, y\}) = Inf(x, y) = x \wedge y$

Teorema: En todo CPO $\langle A, \leq \rangle$ se cumple que $(\forall x, y \in A)\big((x \leq y \Leftrightarrow x \vee y = y) \wedge (x \leq y \Leftrightarrow x \wedge y = x)\big)$.

Sub CPO: El par $\langle S, \underline{\propto} \rangle$ es un sub CPO de $\langle A, \leq \rangle$ si y solo si $S \subseteq A$, $\underline{\propto}$ es una relación de orden sobre S y $(\forall x, y \in S)\big(x \underline{\propto} y \Leftrightarrow x \leq y\big)$.

Cadena: Una cadena de un CPO $\langle A, \leq \rangle$ es un sub CPO totalmente ordenado.

Ejemplo:

- $\phi - \{a\} - \{a, b\} - A$
- $\phi - \{a\} - \{a, b\} - \{a, b, c\} - A$

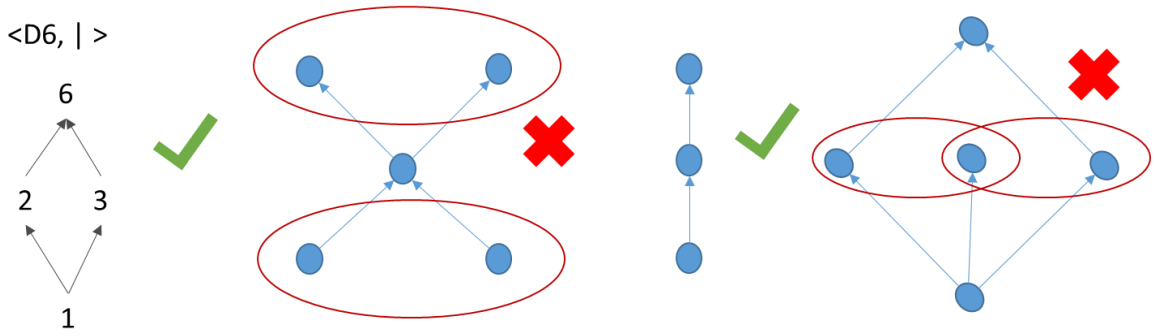
Finitud: Un CPO $\langle A, \leq \rangle$ es finito si y solo si A es finito, si A no es finito entonces es infinito.

Altura: La altura de una cadena finita $\langle B, \leq \rangle$ es $|B| - 1$.

Altura Finita: Un CPO $\langle A, \leq \rangle$ tiene altura finita si y solo si todas sus cadenas son de altura finita.

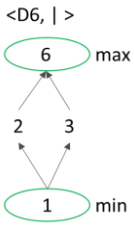
Reticulado: Es un CPO en el cual cualquier par de elementos tiene supremo e ínfimo.

Ejemplo:



Reticulado Acotado: Un reticulado es acotado si y solo si posee max (denotado $\hat{1}$) y min (denotado $\hat{0}$). Puede ser un reticulado infinito e igual estar acotado.

Ejemplo:

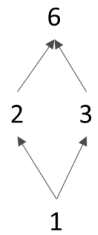


Complemento: Dado un reticulado acotado $\langle L, \leq \rangle$ y un elemento x de L se dice que y en L es el complemento de x si y solo si $Sup(\{x, y\}) = \hat{1}$ e $Inf(\{x, y\}) = \hat{0}$. Se denota $\sim x = y$.

Nota: Pueden existir múltiples complementos a un mismo elemento.

Ejemplo:

<D6, | >



~2=3
~3=2
~1=6
~6=1

Reticulado Complementado: Un reticulado $\langle L, \leq \rangle$ es complementado (todo elemento tiene un complemento) si y solo si para todo $x \in L$ existe $y \in L$ tal que $Sup(\{x, y\}) = \hat{1}$ e $Inf(\{x, y\}) = \hat{0}$.

Reticulado Distributivo: Un reticulado $\langle L, \leq \rangle$ es distributivo si y solo si para todo $x, y, z \in L$ se tiene que:

- $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.
- $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

Álgebras de Boole

Definición Algebraica: Un Álgebra de Boole es un reticulado $\langle L, \leq \rangle$ distributivo e inequívocamente complementado (es decir, es acotado y todos los elementos tienen un único complemento).

> *Ejemplos:* $\langle \mathcal{P}(A), \subseteq \rangle$, $\langle \mathbb{B} = \{0,1\}, \{\langle 0,0 \rangle, \langle 0,1 \rangle, \langle 1,1 \rangle\} \rangle$, $\langle D_n, | \, \rangle$, $\langle \mathbb{B}^n, \underline{\propto} \rangle$ con $\langle x_1, x_2, \dots, x_n \rangle \underline{\propto} \langle y_1, y_2, \dots, y_n \rangle \Leftrightarrow (\forall i \in [n] = [1..n])(x_i \leq y_i)$.

Definición Axiomática: Un Álgebra de Boole es un álgebra $\langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ tal que:

1. $\oplus, \otimes$ son asociativas.
2. $\oplus, \otimes$ son simétricas.
3. El elemento 0 es identidad de $\oplus$. El elemento 1 es identidad de $\otimes$.
4. El operado unario $\sim$, complemento, satisface que para todo $b \in S$: $b \oplus \sim b = 1$ y $b \otimes \sim b = 0$.
5. $\otimes$ se distribuye sobre $\oplus$: $(\forall a, b, c \in S)\big(a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)\big)$.
6. $\oplus$ se distribuye sobre $\otimes$: $(\forall a, b, c \in S)\big(a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)\big)$

> *Ejemplos:*

- $\langle \mathcal{P}(A), \subseteq \rangle \equiv \langle \mathcal{P}(A), \cup, \cap, (\,)^c, \phi, A \rangle$.
- $\langle \{1,2,3,6\}, mcm, mcd, 1,6 \rangle \equiv \langle D_6, | \, \rangle$.
- Para $n \in \mathbb{Z}^+$. Sea F_n el conjunto de las funciones del tipo $\mathbb{B}^n \to \mathbb{B}$ ($F_n = \{f : \mathbb{B}^n \to \mathbb{B}\}$). Sea s una secuencia de n valores booleanos ($s \in \mathbb{B}^n$). Se define $\oplus$, $\otimes$ y $\sim$ como:
  - $(f_1 \oplus f_2)s = f_1(s) \vee f_2(s)$ (Supremo).
  - $(f_1 \otimes f_2)s = f_1(s) \wedge f_2(s)$ (Ínfimo).
  - $(\sim f)s = \neg\big(f(s)\big)$.

Dual de una Proposición: El dual de una proposición es la proposición que resulta de sustituir todas las ocurrencias de $\wedge$ por $\vee$, las de $\vee$ por $\wedge$, las de $\hat{1}$ por $\hat{0}$ y las de $\hat{0}$ por $\hat{1}$.

> $\oplus \to \otimes$
>
> $\otimes \to \oplus$
>
> $0 \to 1$
>
> $1 \to 0$

Teorema: El dual de un teorema sobre Álgebras de Boole es un teorema.

Teoremas de Álgebras de Boole: Es importante el orden igual que lógica.

1. *Idempotencia:* $b \oplus b = b \wedge b \otimes b = b$.
2. *Cero:* $b \oplus 1 = 1 \wedge b \otimes 0 = 0$.
3. *Absorción:* $b \oplus (b \otimes c) = b \wedge b \otimes (b \oplus c) = b$.
4. *Cancelación:*
   - $(b \oplus c = b \oplus d) \wedge (\sim b \oplus c = \sim b \oplus d) \equiv (c = d)$
   - $(b \otimes c = b \otimes d) \wedge (\sim b \otimes c = \sim b \otimes d) \equiv (c = d)$
5. *Complemento Único:* $b \oplus c = 1 \wedge b \otimes c = 0 \equiv c = \sim b$.
6. *Doble Complemento:* $b = \sim (\sim b)$.
7. *Complemento Constante:* $\sim 0 = 1 \wedge \sim 1 = 0$.
8. *De Morgan:*
   a. $\sim (b \oplus c) = \sim b \otimes \sim c$.
   b. $\sim (b \otimes c) = \sim b \oplus \sim c$.
9. *Teoremas:*
   a. $b \oplus \sim c = 1 \equiv b \oplus c = b$.
   b. $b \otimes \sim c = 0 \equiv b \otimes c = b$.

Teorema: Toda imagen homomórfica de un Álgebra de Boole es un Álgebra de Boole. Es decir, sea $\langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ un álgebra de Boole, $\langle S', \oplus', \otimes', \sim', 0', 1' \rangle$ un álgebra y $h: S \to S'$ un homomorfismo, entonces $\langle h(S), \oplus', \otimes', \sim', 0', 1' \rangle$ es un álgebra de Boole.

Axiomas: Números de Gries.

Caracterización: $18.59)\ b \leq c \equiv b \otimes c = b$.

$18.60)\ b < c \equiv b \leq c \wedge b \neq c$.

Caracterización Alternativa: $18.62)\ b \leq c \equiv b \oplus c = c$.

Teorema: La relación $\leq$ (la del axioma anterior) es una relación de orden parcial.

Átomo: $18.63)\ atom(a) \equiv atom.a \equiv a \neq 0 \wedge (\forall b \in S |\ 0 \leq b \leq a : b = 0 \vee b = a)$.

Propiedades:

- $18.64)\ atom.a \Longrightarrow a \otimes b = 0 \vee a \otimes b = a$.
- $18.65)\ atom.a \wedge atom.b \wedge a \neq b \Longrightarrow a \otimes b = 0$.
- $18.66)\ (\forall a \in S |\ atom.a : a \otimes b = 0) \Longrightarrow b = 0$ (El contra recíproco también es importante).

Coátomos: Son los predecesores inmediatos del $\hat{1}$ en el Álgebra de Boole.
$coatom(a) \equiv coatom.a \equiv a \neq 1 \wedge (\forall b \in S |\ a \leq b \leq 1 : b = 1 \vee b = a)$.

Átomos: Son los sucesores inmediatos del $\hat{0}$ en el Álgebra de Boole.

Teorema: Cualquier elemento de un Álgebra de Boole finita puede ser escrito de manera única como suma de átomos o multiplicación de coátomos. Es decir, para A A.B. finita y $b \in A$ se tiene que $b = (\oplus a_i \in A |\ atom.\ a_i : a_i) \wedge b = (\otimes a_i \in A |\ coatom.\ a_i : a_i)$.

Teorema: Un álgebra de Boole con n átomos tiene 2^n elementos. La explicación de esto depende del teorema anterior, ya que en la representación como suma se puede ver que un átomo puede estar o no en la representación del elemento, es decir, hay 2 opciones; como hay n átomos y cada uno puede estar o no, entonces la cantidad de posibles elementos es $2 * 2 * 2 * \ldots * 2\ n$ veces, es decir, 2^n.

Teorema: Un álgebra de Boole finita $A = \langle S, \oplus, \otimes, \sim, 0, 1 \rangle$ con n átomos es isomorfa a un álgebra $\hat{A} = \langle \mathcal{P}(\hat{S}), \cup, \cap, (\ )^c, \phi, \hat{S} \rangle$ donde $\hat{S} = \{1, 2, \ldots, n\}$. Con el isomorfismo definido de la siguiente forma:

$h: S \to \hat{S}$

$h(b) = \{i \mid i \in S_k\}$ si $b = (\oplus i \mid i \in S_k : a_i)$, $S_k \subset S$, S_k es el conjunto de átomos que al sumarlos representan a b y a_i siendo el i-ésimo átomo de A (Ya que son finitos y contables son enumerarbles).

Átomos de un Elemento: Si x es un elemento de un álgebra de Boole, A, entonces $atom(x)$ es el conjunto de los átomos de A que se usan en la representación de x como suma de átomos.

Coátomos de un Elemento: Si x es un elemento de un álgebra de Boole, A, entonces $coatom(x)$ es el conjunto de los coátomos de A que se usan en la representación de x como multiplicación de coátomos.

Átomos de un Álgebra de Boole: Al conjunto de todos los átomos de un álgebra de Boole, A, se le denota como $Atom(A)$.

Coátomos de un Álgebra de Boole: Al conjunto de todos los coátomos de un álgebra de Boole, A, se le denota como $Coatom(A)$.

Isomorfismos de Álgebra de Boole: Se dice que dos Álgebras de Boole, A y B, de soportes (carrier) S y $\hat{S}$ respectivamente, son isomorfos si y solo si existe una función biyectiva $\varphi: S \to \hat{S}$ tal que:

1. $\varphi(a \vee b) = \varphi(a)\ \hat{\vee}\ \varphi(b)$.
2. $\varphi(a \wedge b) = \varphi(a)\ \hat{\wedge}\ \varphi(b)$.
3. $\varphi(\sim a) = \hat{\sim}\ \varphi(a)$.

Teorema:

Si $\langle A, \leq \rangle$ y $\langle \hat{A}, \hat{\leq} \rangle$ son Álgebras de Boole y $\varphi: A \to \hat{A}$ es un isomorfismo de Álgebras de Boole, entonces:

1. $\varphi(0) = \hat{0}$.
2. $\varphi(1) = \hat{1}$.
3. $x \leq y \Longrightarrow \varphi(x)\ \hat{\leq}\ \varphi(y)$.

4. $a \in Atom(A) \Longrightarrow \varphi(a) \in Atom(\hat{A})$ (Átomos en átomos).
5. $a \in Coatom(A) \Longrightarrow \varphi(a) \in Coatom(\hat{A})$ (Coátomos en coátomos).

Sub Álgebras de Boole: Dada un Álgebra de Boole $A = \langle S, \vee, \wedge, \sim, 0, 1 \rangle$. Se dice que $B = \langle S', \vee, \wedge, \sim, 0, 1 \rangle$ es sub álgebra de Boole si y solo si B es un álgebra de Boole con las mismas operaciones de A, $S \subseteq S'$ y todo $x \in S'$ tiene su complemento en S (Cerrado bajo el complemento).

Funciones Booleanas

Nota de ahora en adelante $xy = x * y$.

Variables Booleanas: Una variable x es booleana si y solo si toma valores en $\mathbb{B}$.

Funciones Booleanas: Una función Booleana (o de conmutación) de n variables es una función $f: \mathbb{B}^n \to \mathbb{B}$, con $\mathbb{B} = \{0,1\}$ y $\langle \mathbb{B}, +, *, \sim, 0, 1 \rangle$ siendo un Álgebra de Boole. Se denota el conjunto de todas las funciones booleanas de n variables como F_n.

Complemento de una Función Booleana: $\overline{f}(\vec{x}) = \overline{f(\vec{x})}$ (Complemento de $\mathbb{B}$) con $\vec{x} \in \mathbb{B}^n$.

Expresiones Booleanas: Se dice que e es una expresión booleana en las variables $x_1, x_2, \dots, x_n$ si y solo si satisface:

1. Es x_i o $\overline{x_i}$ con $i = 1, \dots, n$.
2. Es igual a $e_1 + e_2$ o a $e_1 * e_2$ donde $e1$ y e_2 son expresiones booleanas.
3. Es igual a $\overline{e_1}$ donde e_1 es una expresión booleana.

Ejemplo: $(x_1 + x_2) + x_3$.

Literal: Dado un conjunto de n variables booleanas $x_1, x_2, \dots, x_n$ se denomina literal a cada una de ellas o sus complementos.

Término: Un término es una conjunción (disyunción) de literales.

Ejemplos: $(x_1 x_2 x_3), (x_1 + x_2 + x_3)$.

Conjunción Fundamental: Una conjunción fundamental de un conjunto de n variables booleanas $x_1, x_2, \dots, x_n$ es un término de la forma $(y_1 y_2 \dots y_n)$ donde $y_i = x_i$ o $y_i = \overline{x_i}$ (Básicamente es un término con todos los literales).

Ejemplo: Para dos variables: $xy, x\bar{y}, \bar{x}y, \bar{x}\bar{y}$.

Forma Canónica Disyuntiva: Una representación de una función como una suma (disyunción) de conjunciones fundamentales se llama Forma Canónica Disyuntiva de f.

Ejemplos: Para dos variables: $xy + \bar{x}y + x\bar{y}$, $x\bar{y} + \bar{x}y$, $\bar{x}\bar{y}$.

Forma Normal Disyuntiva: Es una representación de una función f como suma (disyunción) de conjunciones.

Ejemplos:

Para dos variables: $x + y, xy + \bar{x}$.

Para cuatro variables: $x + y + z + w, xyzw + xyw + zw$.

Disyunción Fundamental: Una disyunción fundamental de un conjunto de n variables booleanas $x_1, x_2, \dots, x_n$ es un término de la forma $(y_1 + y_2 + \cdots + y_n)$ donde $y_i = x_i$ o $y_i = \overline{x_i}$ (Básicamente es un término con todos los literales).

Ejemplo: Para dos variables: $x + y, x + \bar{y}, \bar{x} + y, \bar{x} + \bar{y}$.

Forma Canónica Conjuntiva: Una representación de una función como una multiplicación (conjunción) de disyunciones fundamentales se llama Forma Canónica Conjuntiva de f.

Ejemplos: Para dos variables: $(x + y)(\bar{x} + y)(x + \bar{y})$, $(x + \bar{y})(\bar{x} + y)$, $(\bar{x} + \bar{y})$.

Forma Normal Conjuntiva: Es una representación de una función f como multiplicación (conjunción) de disyunciones.

Ejemplos:

Para dos variables: $(xy), (x + y)(\bar{x})$.

Para cuatro variables: $xyzw, (x + y + z + w)(x + y + w)(z + w)$.

Teorema: En el Álgebra de Boole de las Funciones Booleanas de n variables, F_n, los átomos son las conjunciones fundamentales y los coátomos son las disyunciones fundamentales. Las conjunciones fundamentales se les llama min-terms, min-términos o mini-términos. Las disyunciones fundamentales se les llaman máx-terms, maxi-términos o máx-términos. Cuando se trabaja con tablas de verdad, siendo importante el orden en que son puestas las variables, se cumplen las siguientes reglas para traducción de y a binario:

- Para min-terms: $x_i \leftrightarrow 1$ y $\overline{x_i} \leftrightarrow 0$.
- Para máx-terms: $x_i \leftrightarrow 0$ y $\overline{x_i} \leftrightarrow 1$.

Cómo Conseguir: Para conseguir las conjunciones fundamentales de una función f usando una tabla de verdad se toman los niveles donde la función de 1, luego se toma los valores de las variables asociada y se transforma en forma de variables usando las reglas anteriores; una vez conseguidas se suman todas las conjunciones fundamentales. Para conseguir las disyunciones fundamentales de una función f usando una tabla de verdad se toman los niveles donde la función de 0, luego se toma los valores de las variables asociada y se transforma en forma de variables usando las reglas anteriores; una vez conseguidas se multiplican todas las conjunciones fundamentales.

Ejemplo:

Valor en base 10	x	y	f	min	max
0	0	0	1	$\bar{x}\bar{y}$	$x + y$
1	0	1	0	$\bar{x}y$	$x + \bar{y}$
2	1	0	1	$x\bar{y}$	$\bar{x} + y$
3	1	1	0	xy	$\bar{x} + \bar{y}$

$f(x, y) = x\bar{y} + \bar{x}\bar{y} = \sum_m(0,2) = \prod_M(1,3)$.

Corolario: El Álgebra de Boole F_n tiene 2^n átomos y 2^{2^n} elementos.

Desarrollo de Shannon: Toda función booleana se puede expresar como suma única de min-terms (átomos).

Ejemplo:

Para una variable: $f(x) = \bar{x}f(0) + xf(1)$.

Para dos variables: $f(x_1, x_2) = \overline{x_1}f(0, x_2) + x_1 f(1, x_2) =$

$\overline{x_1}\,\overline{x_2}f(0,0) + \overline{x_1}\,x_2 f(0,1) + x_1\,\overline{x_2}f(1,0) + x_1\,x_2 f(1,1)$.

Desarrollo para n Variables:

$f(x_1, \dots, x_i, \dots, x_n) = \overline{x_i}\, f(x_1, \dots, 0, \dots, x_n) + x_i\, f(x_1, \dots, 1, \dots, x_n)$.

Desarrollo para cada Variable:

$f(x_1, \dots, x_n) = \overline{x_1} \dots \overline{x_n}\, f(0, \dots, 0) + x_1 \dots x_n f(1, \dots, 1)$.

Toda función booleana se puede expresar como multiplicación única de máx-terms (coátomos).

Ejemplo:

Para una variable: $f(x) = [\bar{x} + f(1)][x + f(0)]$.

Para dos variables: $f(x_1, x_2) = [\overline{x_1} + f(1, x_2)][x_1 + f(0, x_2)] =$

$[\overline{x_1} + \overline{x_2} + f(1,1)][\overline{x_1} + x_2 + f(1,0)][x_1 + \overline{x_2} + f(0,1)][x_1 + x_2 + f(0,0)]$.

Desarrollo para n Variables:

$f(x_1, \dots, x_i, \dots, x_n) = [\overline{x_i} + f(x_1, \dots, 1, \dots, x_n)][x_i + f(x_1, \dots, 0, \dots, x_n)]$.

Desarrollo para cada Variable:

$f(x_1, \dots, x_n) = [\overline{x_1} + \cdots + \overline{x_n} + f(1, \dots, 1)][x_1 + \cdots + x_n + f(0, \dots, 0)]$.

Pasar de una Forma a Otra por Método Sintáctico: Se usan las Leyes de A.B. y equivalencias. Existen dos casos:

Caso 1: La función está en Forma Normal (Conjuntiva o Disyuntiva). Se pasa a Forma Canónica (Conjuntiva o Disyuntiva) multiplicando por $1 = x_i + \overline{x_i}$ o sumando $0 = x_i * \overline{x_i}$ y se sigue con el Caso 2. Ejemplo: $f(x, y, z) = xyz + x = xyz + x * 1 = xyz + x(y + \bar{y}) = xyz + xy + x\bar{y} = \cdots = xyz + xy\bar{z} + x\bar{y}z + x\bar{y}\bar{z}$.

Caso 2: La función está en Forma Canónica (Conjuntiva o Disyuntiva), se siguen los siguientes pasos:

1. Se halla el complemento de la función de una forma especial, el complemento consiste en los términos que faltan para que la función sea completa, es decir, la función tenga 2^n términos. Ejemplo: $\bar{f}(x, y, z) = \bar{x}\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}y\bar{z}$.

2. Se halla el complemento del complemento (el calculado en el paso anterior) de la función usando De Morgan. Ejemplo: $\bar{\bar{f}}(x,y,z) = f(x,y,z) = \overline{(\bar{x}\bar{y}\bar{z} + \bar{x}yz + \bar{x}\bar{y}z + \bar{x}y\bar{z})} = (x+y+z)(x+\bar{y}+z)(x+y+\bar{z})(x+\bar{y}+z)$.

Pasar de una Forma a Otra por Método Semántico: Se usan tablas de verdad.

Mapas de Karnaugh

Adyacencia Lógica: Dos conjunciones (disyunciones) fundamentales son adyacentes lógicamente si y solo si difieren en solo uno de sus literales.

Ejemplos:

Para dos variables:

- Son Adyacencias: xy y $\bar{x}y$, $\bar{x}y$ y $\bar{x}\bar{y}$.
- No son Adyacencias: xy y $\bar{x}\bar{y}$.

Para tres variables:

- Son Adyacencias: xyz y $x\bar{y}z$, xyz y $\bar{x}yz$.
- No son Adyacencias: $\bar{x}\bar{y}z$ y xyz, $x\bar{y}z$ y $\bar{x}yz$.

Mapa de Karnaugh: Un mapa de Karnaugh para una función booleana $f: \mathbb{B}^n \to \mathbb{B}$ es una o más tablas rectangulares en las que las celdas representan a todos los átomos del álgebra de Boole de las funciones booleanas de n variables, ubicados de tal forma que aparezcan adyacentes físicamente si lo son lógicamente.

Cómo Construirlo:

1. A partir de una tabla de verdad de la función se toman los niveles donde la función toma el valor 1 para hacer el mapa de min-terms y los niveles donde la función toma el valor 0 para el mapa de máx-terms, no se pueden mezclar los dos tipos de mapa. Ejemplo:

x	y	z	f
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

x\yz	00	01	11	10
0	1		1	1
1	1			1

Para min-terms

x\yz	00	01	11	10
0		0		
1		0	0	

Para máx-terms

2. A partir de la Forma Canónica Disyuntiva se traduce a binario:
(Nota: es importante el orden de las variables. Los 0's y 1's arriba de las variables representan su traducción a binario)

$$f(w,x,y,z) = \frac{0000}{\bar{w}\bar{x}\bar{y}\bar{z}} + \frac{0001}{\bar{w}\bar{x}\bar{y}z} + \frac{0011}{\bar{w}\bar{x}yz} + \frac{0010}{\bar{w}\bar{x}y\bar{z}} + \frac{0101}{\bar{w}x\bar{y}z} + \frac{0111}{\bar{w}xyz} + \frac{1000}{w\bar{x}\bar{y}\bar{z}} + \frac{1010}{w\bar{x}y\bar{z}}$$

wx\yz	00	01	01	10
00	1	1	1	1
01		1	1	
01				
10				1

3. A partir de la Forma Canónica Conjuntiva se traduce a binario. Ejemplo:
(Nota: es importante el orden de las variables. Los 0's y 1's arriba de las variables representan su traducción a binario)

$$f(x,y,z) = \overset{000}{(x+y+z)}\ \overset{101}{(\bar{x}+y+\bar{z})}\ \overset{010}{(x+\bar{y}+\bar{z})}$$

x\yz	00	01	11	10
0	0			0
1		0		

4. A partir de la Forma Normal Disyuntiva o Conjuntiva:
   a. Se toma el término con menos literales que no se ha usado para hacer el mapa.
   b. Se convierte a binario los literales y todos los literales que no estén presenten se consideran como sus valores 1 y 0 y se buscan en el mapa sus combinaciones.

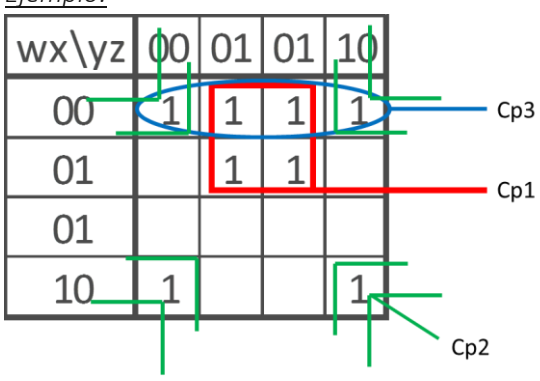
Ejemplo: $f(w,x,y,z) = \overset{1}{w} + \overset{00}{\bar{y}\bar{z}} + \overset{001}{\bar{w}\bar{x}y}$

wx\yz	00	01	01	10
00	1		1	1
01	1			
01	1	1	1	1
10	1	1	1	1

Cubo de Orden k: Un cubo de orden k (k-cubo) es un subconjunto de conjunciones fundamentales (o disyunciones fundamentales) de tamaño $\mathbf{2^k}$ en el que cada conjunción del subconjunto es adyacente a exactamente $\boldsymbol{k}$ conjunciones (disyunciones) del subconjunto.

Cubo Primo: Un cubo primo (o implicante primo) es un cubo que no está incluido dentro de ningún otro cubo.

Ejemplo:



Hay tres cubos primos de tamaño cuatro:

$Cp1 = \{0001,0011,0101,0111\}$.

$Cp2 = \{0000,0010,0100,0110\}$.

$Cp3 = \{0000,0001,0011,0010\}$.

Cubo Primo Esencial: Un cubo primo es esencial si y solo si dicho cubo cubre alguna conjunción (disyunción) fundamental que no cubre ningún otro cubo primo esencial.

Ejemplo: $Cp1$ y $Cp2$ del ejemplo anterior son Cubos Primos Esenciales.

Ejemplo:

x\yz	00	01	11	10
0	0		0	0
1	0			0

Ambos son cubos primos esenciales.

Expresión Mínima: Se usan los cubos primos esenciales para minimizar la expresión, cada dos adyacencias de un cubo primo esencial simplifican una variable de la siguiente forma:

Ejemplo 1: Usando $Cp1$ y $Cp2$ del primer ejemplo anterior:

Cubo $Cp1$: Por filas tomando adyacencias dos a dos.

$$\bar{w}\bar{x}\bar{y}z + \bar{w}\bar{x}yz = \bar{w}\bar{x}(\bar{y} + y)z = \bar{w}\bar{x}z$$

$$\bar{w}x\bar{y}z + \bar{w}xyz = \bar{w}xz$$

$$\bar{w}\bar{x}z + \bar{w}xz = \bar{w}z$$

Cubo $Cp2$: Por filas tomando adyacencias dos a dos.

$$\bar{w}\bar{x}\bar{y}\bar{z} + \bar{w}\bar{x}y\bar{z} = \bar{w}\bar{x}\bar{z}$$

$$w\bar{x}\bar{y}\bar{z} + w\bar{x}y\bar{z} = w\bar{x}\bar{z}$$

$$\bar{w}\bar{x}\bar{z} + w\bar{x}\bar{z} = \bar{x}\bar{z}$$

De $Cp1$ y $Cp2$: $f(w,x,y,z) = \bar{w}z + \bar{x}\bar{z}$.

Ejemplo 2: Usando el segundo mapa del ejemplo anterior y usando representación binaria:

Cubo Azul: $(0+1+1)(0+1+0) = (0+1+\_)$.

Cubo Rojo:

$(0+0+0)(0+1+0) = (0+\_+0)$ (Es importante mantener el orden, por eso se usa el "_")

$$(1+0+0)(1+1+0) = (1+\_+0)$$

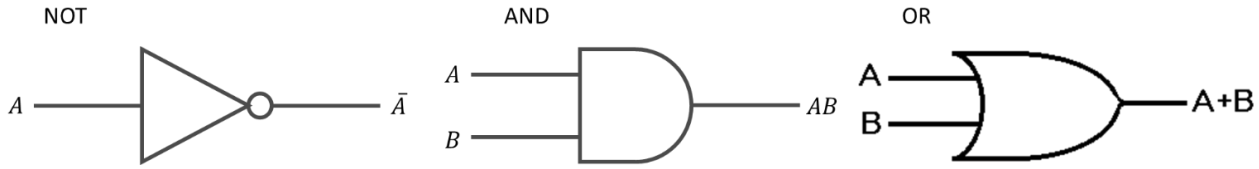
$$(0+\_+0) + (1+\_+0) = (\_+\_+0)$$

De Cubo Azul y Cubo Rojo: $f(x,y,z) = (\bar{x}+y)(\bar{z})$.

Don't Care: Se usan como comodines para rellenar la tabla, sirven como 0's o 1's dependiendo de lo que se necesite. Si quedan fuera de cubos primos esenciales no importa, pero se debe tratar de usarlos para tener cubos primos esenciales más grandes. Se les denota como x.

Circuitos Digitales

Puertas Digitales:



Dado un enunciado se siguen los siguientes pasos:

1. Se modela el enunciado como una o varias funciones booleanas, no tiene por qué ser una Forma Canónica.
2. Se genera la Tabla de Verdad de la función o funciones.
3. Se genera/n el/los Mapa/s Karnaugh asociado/s a la/s función/es.
4. Se busca la Expresión Mínima de todas las funciones.
5. Se genera el Circuito Digital asociado a esa expresión mínima.

Para ejercicios ver Guía y Problemario De Circuitos Lógicos de M en C. Rodolfo Romero Herrera.

Bibliografía

Clases de la Profesora Soraya Carrasquel.

Libro de Estructuras Algebraicas de Vicente Yriarte.

A Logical Approach to Discrete Math de David Gries y Fred B. Schneider.

Guía y Problemario De Circuitos Lógicos de M en C. Rodolfo Romero Herrera.

Notas

Elaborado por Christian Alexander Oliveros Labrador, Cohorte 13. Ing. Computación.

Página web: oliveroschristian.wordpress.com

Actualizada: 08 de abril de 2016. El orden de los temas es basado en el cronograma del curso Enero-Marzo 2016.

Para cualquier corrección o sugerencia enviar un correo a *christianol_01@hotmail.com*. Por favor añadir página, el error y lo que debería ser.