## TEMA I – INTRODUCCIÓN A MATEMÁTICA DISCRETA Y LÓGICA MATEMÁTICA

**Lógica**

-Nos permite representar de manera más formal las cosas.

Sintaxis: cómo se describen las cosas.

Semántica: significado de la sintaxis.

**La lógica formal se usa para:**

-Formalizar propiedades del mundo.

-Interpretar; es decir, asociar a enunciados un significado.

-Deducción formal: demostrar que una cierta propiedad es verdaderas a partir de unas propiedades anteriores.

**Aplicaciones de la lógica a la informática.**

-Especificación y verificación de programas.

-Derivación de programas.

-Reducción automática.

-Lógica como paradigma de programación: PROGRAMACIÓN LÓGICA (Prolog).

-Inteligencia artificial (comienzo).

**Lenguaje: Oraciones, enunciados y proposiciones.**

-Nos vamos a restringir a oraciones declarativas (verdaderas o falsas).

**Ejemplo:** El 3 es primo, Todos los números racionales son mayores que 7.

También existen oraciones no declarativas, no son verdaderas ni falsas. **Ejemplo:** ¿Llueve?

**Insuficiencia del lenguaje natural. Lenguajes formales.**

LÓGICA PROPOSICIONAL

-Símbolo de proposición: p, q, r….

Representa un cierto enunciado y como tal puede evaluarse a dos valores posibles (V o F).

* SINTAXIS

φ::= p | T | ⊥ | φ^φ | φvφ | φφ | φφ | ¬φ

Semántica informal: prop. |verdad | falso| y | o | implica | sí y solamente sí| negación

**Ej. fórmula:** ((p^q)n) v ¬s / ⊥(p^¬r)

**Semántica formal. Tablas de verdad.**

Evaluar una fórmula da verdadero o falso.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| φ1 | φ2 | φ1^φ2 | φ1vφ2 | φ1φ2 | φ1φ2 | ¬φ1 |
| V | V | V | V | V | V | F |
| V | F | F | V | F | F | F |
| F | V | F | V | V | F | V |
| F | F | F | F | V | V | V |

LÓGICA DE PRIMER ORDEN

Objetivo: ampliar lógica proposicional para representar propiedades de forma más adecuada.

Características:

Constantes: A, B, C…

Predicados: M(\_), evalúa a Verdadero o Falso dependiendo de que los parámetros cumplan la pdad.

Cuantificadores:

-Bruto mató a César (p)

-Tito pagó a Bruto (q)

**-Tito pagó a uno que mató a César** (r)

B=Bruto, T=Tito, C=César

-Alguien mató a Trotski

-Stalin pagó a alguien

**-Stalin pagó a alguien que mató a Trotski**

T’=Trotski, S= Stalin

**Ejemplo de lógica proposicional**

-Algunos poetas escribieron libros de ensayo

-El autor del poema del Mío Cid era poeta

-**El autor del poema del Mío Cid escribió libros de ensayo** **No se deduce.**

P=poetas, E=escribieron ensayos, A= Autor Mío Cid

-Si Pablo era monoteísta, entonces, Sócrates y Jantipa no contrajeron matrimonio

-Sócrates y Jantipa no contrajeron matrimonio

-**Pablo era monoteísta** **No se deduce.**

p=Pablo era monoteísta, q= Sócrates y Jantipa no contrajeron matrimonio

-Todos los revolucionarios usan uniforme

-Mussolini no usaba uniforme

-**Mussolini no era revolucionario** **Correcto.**

R=revolucionarios, U=usan Uniforme, M=Mussolini

1. Los políticos pueden pertenecer a 3 grupos: honrados, hipócritas y tontos. x{P(x)[Ho(x)Hi(x)T(x)]}
2. Todo intelectual es amigo de un político inteligente.x{I(x)[y(A(x,y) P(y) ¬T(y))]}
3. Algunos intelectuales no tienen ningún amigo honrado. x{I(x)y[A(x,y)¬Ho(y)]}
4. **Luego no faltan intelectuales con amigos hipócritas.** . x{I(x)y[A(x,y)Hi(y)]}

P=políticos, Ho=Honrados, Hi=Hipócritas, T=tontos, I=Intelectual, A=amigo

## TEMA II – Sistemas Numéricos

Se forman a partir de un valor inicial (0) y aplicando la función sucesor se obtienen los siguientes: 0, s(0), s(s(0)), s(s(s(0)))…  **.**

**.**

**.**

**2.1 Axiomas de Peano. Principio de Inducción.**

Construimos a partir de un valor (0) y la aplicación de la función sucesor.

Los axiomas de Peano permiten formalizar la construcción de .

P1

P2

P3 *Principio de Inducción*

Sea P propiedad definida sobre y quiero probar : P(n). Demostramos P(0) y que : P(k)P(k+1)

Sea P propiedad sobre : si PASO BASE P(0) y PASO INDUCTIVO P(k)P(s(K)) : P(n).

|  |
| --- |
|  |

**Ejemplo**. Demuestra que : 2+4+6+…+2n=n·(n+1)

Paso base P(0):

Hipótesis de Inducción: asumimos que la propiedad para k es ciertapara (k+1) también lo es.

(k+1)(k+2)=(k+1)(k+2) DEMOSTRADO

|  |
| --- |
|  |

**Ejemplo.** Demuestra que 1+2+22+…+2n=2n+1-1

Paso base P(0):

Hipótesis de Inducción: asumimos que la propiedad para k es ciertapara (k+1) también lo es.

DEMOSTRADO

**Ejemplo.** Demuestra que (32n+4n+1) es múltiplo de 5 (32n+4n+1)=5·j

Paso base P(0):

3­2·0+40+1=1+4=5 (múltiplo de 5)

Hipótesis de Inducción: asumimos que para k0 ; 32k+4k+1=5j

Demostramos \32(k+1)+4(k+1)+1=5j’=9·32k+4·4k+1=(4+5) ·32k+4·4k+1=4(32k+4k+1)+ 5 ·32k (32k+4k+1)=5j

4·5j+ 5 ·32k=5(4j+32k)

**Principio de Inducción completa**

Sea P propiedad sobre:

Si paso base P(0) y paso inductivo completo

SEGMENTO DE

**(Def.)** Sea m . Definimos

Por el principio de inducción completo:

Sea P propiedad sobre :

Si paso base P(m) y paso inductivo completo

**Ejemplo.** Demuestra que z admite descomposición por factores.

Paso base P(2)2=2·1 **√**

Inducción completa:

Consideramos k+1

Si (k+1) es primo. **√**

Si (k+1) no es primo

Aplicando la Hipótesis de inducción a x, y tenemos que x, y se puede descomponer en números primos se puede descomponer en números primos.

**Ejemplo.** Demuestra que la suma de los primeros n números impares es n2

1+3+5+…+(2n-1)=n2

Paso base P(0)

Paso inductivo. H.I.

**Ejemplo.** Demuestra que

Paso base P(24)

24=5·0+6·4 (x=0, y=4)

Paso inductivo. H.I. , entonces, k+1

k+1= 5x+6y+1 = 5x+6y+6-5 = 5(x-1)+6(y+1)

\ Demostrado x’=5 , y’=(y-4)

**Principio de Inducción completa sobre con varios casos base**

1. Demostrar todos los pasos base.
2. Dado un k+1 relativamente grande (kel último caso base).
3. Asumir que se cumple hasta el primer caso base.
4. Demostrar que se cumple para k+1

Sea P una proposición sobre

Caso base SI tenemos P(j): P(m), P(m+1),…, P(l-1), P(l)

Ind. Compl. ((

Entonces .

**2.2 Definiciones Recursivas.**

**Esquema de definiciones recursivas sobre**.

Sea m , para definir una función **f**: , podemos utilizar el siguiente esquema.

Sea caso base 1. Consideramos Definimos:

f(n)=an

f(m)=am f(l)=al

f(m+1)=am+1

Caso Recursivo: f(n)=e·(…n…f(i))·(n>1, mi<n)

**Definiciones Recursivas**

FUNCIÓN DE FIBONACCI

f:

f(1)=1

f(2)=1

Recursivo para n2: f(n)=f(n-1)+f(n-2)

**Definición recursiva con varios argumentos**

* Hacemos recursión sobre un argumento, dejando los otros constantes.
* Esquema limitado (existen funciones recursivas que no siguen este esquema) pero fácil de obtener.

f(x,0)=x g(x,0)=0

f(x,s(y))=s(f(x,y)) SUMA g(x,s(y))=f(g(x,y),x) PRODUCTO

**Funciones recursivas con varios argumentos**

|  |  |  |
| --- | --- | --- |
| Elegir el “mejor” argumento  f:  f(k+1)=1+k  [n>0]g(k,n)=(n+k)n+f(k,n-1) | Def. Rec. De sumatorios  g(0)=f(0)  [x>0] g(x)=f(x)+g(x-1) | g:  x,yx· y (definición)  g(x,0)=0  g(x,s(y))=f(g(x,y)x) |

**2.3 DIVISÓN ENTERA Y DIVISIBILIDAD**

Sean a, b , si cII a=b·c, decimos que “a” divide a “b” ó que “a” es múltiplo de “b”

Notación: x/y= x divide a y

Teorema.Sean a, b , a0 y b0; c, r unívocamente determinados II a=b·c+r, 0|r|b

**Bases de numeración**

Teorema. Sea b2 y sea a0, entonces se puede representar de forma unívoca:

a=rnbn+r­­n-1bn-1+…+r1b+r0

**Máximo común divisor**

Sean a, b ; a, b. Decimos que d+(-) es el máximo común divisor de a y b si y solamente si:

**d/a** y **d/b**

c+: **c/a** y **c/b** entonces **c/d**

(a, b) es único.

DEMOSTRACIÓN. Supongamos que existen 2, d1 yd2

d1/d2 d1, d2 + d1=d2

d2/d1

Nota: (a, 0)= |a|

**Algoritmo de Euclides**

LEMA. Sean ab>0mcd (a, b)=mcd (b,r); r=resto de división a/b.

TEOREMA. a b>0; a, b

TEOREMA Sean a, b y d=mcd(a,b). Entonces m, n / d=ma+nb.

mcd (a, b)=mcd (|a|, |b|)

COROLARIO si mcd (a, b)=1, Entonces m, n / 1=ma+nb.

-Nota. Si mcd (a, b)=1, decimos que a y b son primos entre sí.

**Números primos**

(Def.) sea p , decimos que **p** es primo si y solo si p2 y sus únicos divisores positivos son 1 y p.

-Nota. 1 no es primo.

TEOREMA. Sea p primo y sean x1·····xn con n1. Entonces si p/ x1·····xn tenemos , 1: p/xi

Demostración por hipótesis de inducción:

Caso base, n=1. Evidente.

H.I para n=k, k1, p/ x1·····xk, , 1 / p/xi

Para n=k+1, / y1·····yk·yk+1 , ¿, 1 / p/yi ?

Llamemos Y= y1·····yk, tal que y1·····yk·yk+1 = Y·yk+1

Dos posibles casos.

* p/Y, demostrado.
* ¬p/Y 1=p+ yk+1= yk+1·1=p+· yk+1=

=p· yk+1+· yk+1=p· yk+1+p=p(· yk+1+)p/ yk+1. DEMOSTRADO.

**Teorema fundamental de la aritmética**

Sea n, n2. La descomposición en factores primos de n es única salvo su orden de factores.

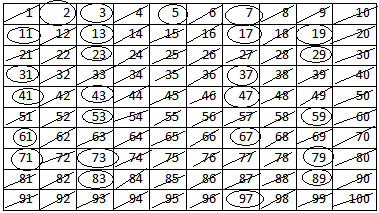
TEOREMA. Sea p primo, entonces cualquier factor primo de p!+1 es mayor que p.

Demostración, supongamos que es falso y q primo,, [q/(1+p!)] A y qp[q/p!]B

* De A tenemos: 1+p!=q·
* De B tenemos: p!=q·

1=1+p!-p!=q·-q·=q(-)q/±1 (absurdo)

**Criba de Eratóstenes**



**Consecuencias de la aritmética modular**

Dados a, b, b>0 c, r unívocamente determinados tal que: a= b · c + r

Podemos definir **“mod”** (notación interfija): ( se corresponde (a, b) y es el resto de dividir a/b)

* NOTA: mod (a, b)a mod b

DEFINICIÓN: Sean a, b y sea m>0, decimos que a es congruente en módulo m con b, denotada amb, si a-b es divisible entre m.

TEOREMA. Sean a, b y sea m>0, amb si y solo si a mod m = b mod m.

TEOREMA. Sea m>0 amb si y solo si k , a = b +k·m

Congruentes con 0 módulo m {…-3m, -2m, -m, 0, m, 2m, 3m…}

Congruentes con 1 módulo m {…1-3m, 1-2m, 1-m, 1, 1+m, 1+2m, 1+3m…}

Congruentes con 2 módulo m {……….}

…………………………………………….

Congruentes con m-1 módulo m {…-1-2m, -1-m, -1, m-1, 2m-1, 3m-1…}

Congruentes con m módulo m {…-2m, -m, 0, m, 2m, 3m…}=0

TEOREMA. Sean a, b, c d, m , con m>0

Si amb y cmd, (a+c)m(b+d)

Si amb y cmd, (a·c)m(b·d)

Nota: es posible definir operaciones sobre clases de congruencia.

A +­­­ mb = (a + b) mod m

A · ­­­mb = (a · b) mod m

## TEMA III – CONJUNTOS NUMÉRICOS

La idea de conjuntos es básica; es decir, no admite una definición formal.

Podemos usar la “definición” de Cantor: Cualquier colección considerada como un todo de objetos bien definidos de nuestro pensamiento e intuición.

Dos nociones básicas a partir del concepto de elemento: (el elemento pertenece al conjunto )

Nota: Podemos definir un conjunto sin más que numerar sus elementos.

**Principio de Extensionalidad**

Sean y dos conjuntos. Si se cumple:

Si no podemos enumerar todos los elementos de un conjunto enumeraremos una función característica.

**Principio de Comprehesión**

Sea un conjunto y una propiedad definida sobre A, podemos definir el conjunto

**(Def.)** Sean y dos conjuntos, decimos que está incluido en si:

-Notación: ^

**(Def.)** Decimos A contenido estricto en B ( ) si:

-Notación:

**Representación gráfica: diagramas de Venn**

Usaremos diagramas de Venn para mostrar propiedades pero usualmente NO servirán para demostrarlas.

PROPOSICIÓN. Sean tres conjuntos A, B, C:

* ^
* ^
* Si ^

^

NOTAS: Usando comprehesión podemos definir conjuntos sin elementos.

Dado que tienen los mismos elementos, estos conjuntos son iguales y vacíos ()

-Los conjuntos con un único elemento los llamamos unitarios.

**Principio de abstracción**

Si p, propiedad bien definida, se puede formar el conjunto de todos los objetos x que cumplan p

**Paradoja de Russell**

R=, entonces R no es un conjunto.

Dado y vamos a ver que asumir y nos lleva a una contradicción.

- (1) Por definición, cumple la propiedad

*-*  (2) Por definición, cumple la propiedad

Si definiéramos RA=, sí es un conjunto.

No existe como conjunto aquel que tiene como elementos todos los conjuntos.

**Demostración de que dos enunciados demuestran un tercero.**

**-**A y B disjuntos () --A=

Dem. 3 a partir de 1 y 2: y A=

Dem. 1 a partir de 2 y 3: supongamos que (absurdo)

Dem. 2 a partir de 1 y 3: Trivial.

**Operaciones de formación de conjuntos**

(**Def**.) Sean A y B conjuntos:

Unión: =

Intersección: =

Diferencia: A\B =

Ejemplo. Sea A = y B = :

**Familias de conjuntos**

(**Def**.) Sea un conjunto, decimos que es una familia de conjuntos si todos sus elementos son conjuntos.

(**Def**.) Sea una familia de conjuntos, definimos:

para algún

para todo

Ejemplo

=

(**Def**.) Sea A conjunto, definimos **el conjunto potencia** o conjunto de las partes de A como:

NOTA. Sea A conjunto, se cumple siempre:

-

-A

NOTA. Acerca de la notación,

**Producto Cartesiano**

(**Def**.) Sean A, B conjuntos. Definimos AxB como el conjunto de pares AxB = {(a,b)\aA y bB}

NOTA. (a, b) es un par ordenado; es decir, importa el orden: (a, b)(b, a)

NOTA.

-Si A= ó B=, AxB=

-Si A=B, escribiremos A2 en lugar de AxA.

(**Def.**) Sean A1, A2,…,An (n>2) conjuntos, entonces:

A1xA2x…xAn = {(x1,x2,…, xn)\ xi Ai}

NOTA. Si Ai son iguales escribiremos An.

**Leyes algebraicas de Boole**

Suponemos un conjunto que contiene a los conjuntos que aparecen en estas leyes.

Definimos el complementario de un conjunto, denotado , como .

NOTA. Si consideramos y tenemos A, B , entonces

* Asociatividad:
* Conmutatividad:
* Distributividad:
* De Morgan:
* Idempotencia:
* Doble Complementación:
* Absorción:
* Complementación:

Para demostrar las leyes tenemos dos métodos.

1. Demostraciones algebraicas.
2. Tablas de pertenencia.

NOTA. Para “mostrar” una ley podemos usar representación gráfica.

Ejemplo: demostración

Demostración algebraica

Para demostrar que S1=S2 haremos:

1. Probamos primero que .

Si

Si

Entonces .

1. Ahora demostramos que

Si

Si (**Caso 1**)

Si (**Caso 2**)

Entonces, sabemos que ó 1 ó 2 debe cumplirse, por tanto siempre y si caso 1 es verdadero o si caso 2 es verdadero, entonces ; Es decir, se cumple .

Demostración por tablas de pertenencia

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C |  |  |  |  |  |
| T | T | T | T | T | T | T | T |
| T | T | F | T | T | T | F | T |
| T | F | T | T | T | F | T | T |
| T | F | F | F | F | F | F | F |
| F | T | T | T | F | F | F | F |
| F | T | F | T | F | F | F | F |
| F | F | T | T | F | F | F | F |
| F | F | F | F | F | F | F | F |

Por la tabla anterior queda demostrado que

Una vez demostrado que todas las leyes son ciertas, podemos usar estas leyes para demostrar otras igualdades.

Relaciones

Aparecen tanto en el mundo real como en las matemáticas.

En informática:

-En programación establecemos relaciones entre inputs y outputs.

-Bases de datos: cálculo relacional.

**Relación binaria**

(**Def**.) Una relación binaria es un conjunto *R* de pares ordenados.

Si tenemos que R AxB, R es una relación entre A y B.

Si R AxA, R es una relación sobre A.

Notación. Si (x, y) R normalmente escribiremos R(x, y) ó xRy.

Normalmente definiremos relaciones mediante una condición característica:

xRy condición depende de x e y.

Ejemplo.

xRy x/y, R AxA

**xRy expresión sobre x e y**

(**Def.**) Sea una relación binaria:

|  |
| --- |
| -El dominio de |
| -El rango de |

Definimos:

**Operaciones entre relaciones**

Dado que las relaciones son conjuntos, podemos considerar unión e intersección de relaciones. Además si entonces

Otras operaciones propias de relaciones

* Inversa de
* Composición de R y S:
* Sea A un conjunto de identidad sobre A:

**Ejemplo.**

xRy x es hermano de y.

xSy x es progenitor de y.

x(y x es hermano de z z es progenitor de y x es tío de y.

xS-1y x es hijo de y.

**Proposición:** Sean relaciones:

* , además la composición de relaciones es asociativa

(**Def**.) Un conjunto R de n-tuplas ordenadas (x1,… ,xn) se llama relación n-aria (binaria, ternaria…)

* Si decimos que R es relación entre
* Si decimos que R es relación n-aria sobre A.

**Ejemplo.**

Una relación ternaria sobre es mcd(x, y, z) mcd(x, y) = z.

Funciones

(**Def**.) Una relación binaria *R* decimos que es función si

**Ejemplo.**

Sea

Dom(R)= cuadrados perfectos, por lo tanto R no es función (Dos valores de y cumplen xRy).

**Dominio, imágenes y rango**

Usualmente usaremos las letras *f*, *g*, y *h* para designar funciones

Sea f una función y el único objeto y tal que xfy , lo denotamos f(x).

xfyf’(x)

**Funciones parciales de A en B**

(**Def**.)

Si decimos que f es una función parcial de A en B.

Si decimos que f es una función total.

**Ejemplo.**

es parcial porque

**Definición de funciones**

(**Def**.)

Podemos definir como expresión dependiente de :

**Ejemplo:**

|  |
| --- |
|  |
|  |

Podemos definir mediante casos:

**Ejemplo:**

Para que los casos estén bien definidos los casos deben ser mutuamente excluyentes.

**Igualdad entre funciones**

(**Def**.)

Dadas dos funciones y : decimos que

**Ejemplo.**

|  |
| --- |
|  |

g

**Funciones especiales**

(**Def**.)

Sea un conjunto, definimos como Identidad en A.

Nota: si , entonces hablamos de aplicación de inclusión de A en B

Consideremos la relación vacía:

(Función total)

( (Función parcial)

Consideremos (f no total)

**Operaciones entre funciones**

(**Def**.) Sea función y Definimos la restricción de a como la función cuyo dominio

Notación:

|  |
| --- |
|  |
|  |

**Ejemplo.** Sea

(**Def**.) y sea entonces

(**Def**.) Consideremos la composición de funciones como comparación de relaciones.

Sean y funciones:

xz

**Teorema.**

Sean y funciones:

**Teorema.**

Sean y

1. =

**Inversa de una función**

Mientras que la inversa de una relación es otra relación, la inversa de una función no tiene por qué ser otra función.

(**Def**.) Sea una función. Definimos Sean inyectiva es una función.

NOTA. Sean es inyectiva