Resumen general de Matemáticas Discretas

Andrés Cabezas y Sebastián Poblete

April 24, 2022

1 ¿Qué son las matemáticas discretas?

"El lenguaje necesario para entender y modelar la computación". Las matemáticas discretas usan conjuntos finitos e infinitos al momento de estudio. Modelan los objetos y conceptos abstractos de las matemáticas que pueden ser representados dentro de un computador.

1.1 Lógica

La lógica consiste en el uso y estudio del razonamiento válido. Para esto, es necesario un lenguaje, pero esto también supone un problema: Los lenguajes que los humanos hablan tiene ciertas subjetividades y diferencias entre si, lo que conduce a errores al momento de usar la lógica. Para resolver esto, es necesario usar un lenguaje formal.
Durante el curso, se estudiarán dos lógicas (o lenguajes), sin embargo, existen muchos más

- Lógica Proposicional
- Lógica de Predicados

¿Para qué son necesarias estas lógicas? Recordemos nuestro objetivo. Queremos usar esto para realizar nuestro razonamiento matemático. De esta forma, podemos definir correctamente objetos matemáticos, teorías matemáticas y realizar demostraciones más formales

2 Lógica Proposicional (LP)

2.1 Proposición

Una proposición consiste en una afirmación, la cual puede ser *verdadera (1)* o *falsa (0)*.
Para denotar proposiciones básicas, usaremos letras mayusculas (Ej.: P, Q, R...)

2.2 Conectivos Lógicos

La LP usa conectivos sencillos para conseguir formar proposiciones más complejas.

Conectivos	Nombre	Uso	Significado
$\wedge$	Conjunción	$P \wedge Q$	P y Q
$\vee$	Disyunción	$P \vee Q$	P o Q
$\neg$	Negación	$\neg P$	No P
$\rightarrow$	Condicional	$P \rightarrow Q$	Si P, entonces Q
$\leftrightarrow$	Bicondicional	$P \leftrightarrow Q$	P, si y solo si, Q

2.2.1 Conjunción ($\wedge$)

El valor de verdad de una conjunción es *verdadero* si ambas proposiciones (a cada lado del signo) son verdaderas. En cualquier otro caso, es *falso*.

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

2.2.2 Disyunción ($\vee$)

El valor de verdad de una disyunción es *verdadero* si al menos una de las proposiciones (a cada lado del signo), es verdadera.

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

2.2.3 Negación ($\neg$)

El valor de verdad corresponde al opuesto del valor entregado (a la derecha del signo)

P	$\neg P$
1	0
0	1

2.2.4 Condicional ($\rightarrow$)

El valor de verdad de una condicional del tipo $P \rightarrow Q$ es *falso* si P es verdadero, pero Q es falso. En cualquier otro caso, es *verdadero*.

P	Q	$P \rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

Hint: *"Si P es verdadero, entonces necesariamente Q es verdadero"*. Si P es verdadero, entonces Q deberá ser verdadero para tener un valor de verdad *verdadero*. Si P es falso, entonces de forma automática el valor de verdad es *verdadero*.

2.2.5 Bicondicional ($\leftrightarrow$)

El valor de verdad de una bicondicional es verdadero si ambas proposiciones (a ambos lados del signo) son iguales (en otras palabras, ambas verdaderas o ambas falsas).

P	Q	$P \leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

2.3 Proposición Compuesta

Una proposición es compuesta si corresponde a la negación ($\neg$), conjunción ($\wedge$), disyunción($\vee$), condicional($\rightarrow$) o bicondicional($\leftrightarrow$) de proposiciones compuestas.
Como por ejemplo

$$P \wedge (Q \vee R)$$
$$\neg(P \vee (\neg R \wedge Q))$$
$$(P \rightarrow Q) \leftrightarrow (P \wedge Q)$$

Si se desea obtener el valor de verdad de alguna proposición compuesta, se debe evaluar de forma recursiva cada uno de los conectivos lógicos presentes.
Por ejemplo:

$$\neg(P \vee (\neg R \wedge Q)) \text{ con P} = 0, \text{ Q} = 1 \text{ y R} = 0$$
$$\neg(0 \vee (\neg 0 \wedge 1))$$
$$\neg(0 \vee (1 \wedge 1))$$
$$\neg(0 \vee 1)$$
$$\neg 1$$
$$0$$

$$(P \rightarrow Q) \leftrightarrow (P \wedge Q) \text{ con P} = 1 \text{ y Q} = 0$$
$$(1 \rightarrow 0) \leftrightarrow (1 \wedge 0)$$
$$0 \leftrightarrow 0$$
$$1$$

2.3.1 Paréntesis y prioridad

El orden de prioridad entre conectivos lógicos, al momento de evaluar proposiciones compuestas, será el siguiente:

Conectivo	Precedencia
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

3 Formulas y Valuaciones

3.1 Variables Proposicionales

Una variable proposicional es una variable que puede ser reemplazada con los valores 1 o 0. Generalmente son representadas con una letra minúscula (Amiga eri boolean)

3.2 Formulas Proposicionales

Una formula proposicional es una formula que puede ser

- Una variable proposicional
- Los valores 1 o 0
- Una combinación con conectivos lógicos

Generalmente son representadas con letras griegas (Ej.: α)
Ejemplos:

$$\alpha(p, q, r) := p \wedge (q \rightarrow r)$$
$$\beta(p, q) := (p \wedge \neg q) \vee (\neg p \wedge 1)$$

4 Equivalencia Lógica

4.1 Definición

Si tenemos dos formulas proposicionales con las mismas variables proposicionales

$$\alpha(p_1, \ldots, p_n) \text{ y } \beta(p_1, \ldots, p_n)$$

Entonces, α y β serán logicamente equivalentes

$$\alpha \equiv \beta$$

si para toda valuación posible $(v_1, \ldots, v_n)$ se cumple que:

$$\alpha(v_1, \ldots, v_n) = \beta(v_1, \ldots, v_n)$$

Ejemplo: Para las fórmulas $p \wedge (q \vee r)$ y $(p \wedge q) \vee (p \wedge r)$ se tiene la siguiente tabla de verdad:

p	q	r	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Como ambas formulas son equivalentes para toda valuación, entonces:

$$p \wedge (q \vee r) \equiv (p \wedge q) \wedge (p \wedge r)$$

4.2 Equivalencias útiles

1. Conmutatividad:

$$p \wedge q \equiv q \wedge p$$
$$p \vee q \equiv q \vee p$$

2. Asociatividad:

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$
$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$

3. Idempotente:

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

4. Doble negación:

$$\neg\neg p \equiv p$$

5. Distributividad:

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

6. De Morgan:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

7. Implicación:

$$p \to q \equiv \neg p \vee q$$
$$p \to q \equiv \neg q \to \neg p$$
$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$

8. Absorción:

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

9. Identidad:

$$p \vee 0 \equiv p$$
$$p \wedge 1 \equiv p$$

10. Dominación:

$$p \wedge 0 \equiv 0$$
$$p \vee 1 \equiv 1$$

5 Operadores Generalizados

Debido a que $\vee$ y $\wedge$ son operadores asociativos, podemos escribir las siguientes generalizaciones

$$\bigvee_{i=1}^{n} p_i \equiv p_1 \vee p_2 \vee \ \ldots \ \vee p_n$$

$$\bigwedge_{i=1}^{n} p_i \equiv p_1 \wedge p_2 \wedge \ \ldots \ \wedge p_n$$

Además, podemos saltarnos los parentesis al momento de escribir estas operaciones. Por ejemplo:

$$(p_1 \vee p_2) \vee p_3 \equiv p_1 \vee (p_2 \vee p_3) \equiv p_1 \vee p_2 \vee p_3$$

$$(p_1 \wedge p_2) \wedge p_3 \equiv p_1 \wedge (p_2 \wedge p_3) \equiv p_1 \wedge p_2 \wedge p_3$$

6 Formas normales

Primero, consideremos que un *literal* es una variable proposicional o la negación de una variable.

6.1 Forma Normal Disyuntiva (DNF)

Una formula α está en DNF si es una disyunción de conjunciones de literales.

$$\alpha = \beta_1 \vee \beta_2 \vee \ldots \vee \beta_k$$

donde $\beta_i = (l_{i_1} \wedge \ldots \wedge l_{i_{k_i}})$ y $l_{i_1}, \ldots, l_{i_{k_i}}$ son literales.
Por si esta forma de anotarlo es muy complicada de entender, en palabras más simples, nos referimos a que α está en DNF si es que es una formula proposicional tal que este compuesta por disyunciones de otras formulas, las cuales son conjunciones de variables proposicionales.
Ejemplo:

$$(p \wedge \neg q) \vee (\neg p \wedge p \wedge s) \vee (r \wedge \neg s)$$

6.2 Forma Normal Conjuntiva (CNF)

Una formula α está en CNF si es una conjuncion de disyunciones de literales.

$$\alpha = \beta_1 \wedge \beta_2 \wedge \ldots \wedge \beta_k$$

donde $\beta_i = (l_{i_1} \vee \ldots \vee l_{i_{k_i}})$ y $l_{i_1}, \ldots, l_{i_{k_i}}$ son literales.
Al final, la idea de la CNF es algo así como una "forma inversa" de la DNF, ya que se invierte que es lo que se encuentra en disyunción y lo que se encuentra en conjunción.
Ejemplo:

$$(p \vee \neg q) \wedge (\neg p \vee p \vee s) \wedge (r \vee \neg s)$$

6.3 Formas normales y Equivalencia lógica

Tenemos el siguiente teorema:

1. Toda formula α es lógicamente equivalente a una formula en DNF.
2. Toda formula α es lógicamente equivalente a una formula en CNF.

Debido a las limitadas herramientas de demostración que tenemos por el momento, la demostración será escrita a futuro en esta parte del resumen. En caso de estar estudiando con este resumen, no considere la demostración hasta tener las herramientas suficientes como para demostrar.

7 Consecuencia Lógica

Sea $\Sigma = \{\alpha_1, \ldots, \alpha_m\}$ un conjunto de formulas con variables $p_1, \ldots, p_n$. Diremos que α es *consecuencia lógica* de Σ si, y solo si, para toda valuación $v_1, \ldots, v_n$ se tiene que

$$\text{si } [\bigwedge_{i=1}^{m} \alpha_i](v_1, \ldots, v_n) = 1, \text{ entonces } \alpha(v_1, \ldots, v_n) = 1$$

Esto se denota como $\Sigma \models \alpha$ (leido como α *es consecuencia lógica de* Σ)
Posiblemente no quede del todo claro el significado de esta formula, pero en palabras, lo que queremos decir es que si tenemos una valuación, tal que al aplicarla a toda formula presente en el conjunto retorne 1, entonces si una formula es consecuencia lógica del conjunto, esta debe también retornar 1.

Si lo intentamos ver con una tabla de verdad, a modo de ejemplo, una consecuencia lógica se vería de la siguiente forma:

v_1	$\cdots$	v_n	α_1	α_2	$\cdots$	α_m	α
$\cdots$	$\cdots$	$\cdots$	1	1	$\cdots$	0	1
$\cdots$	$\cdots$	$\cdots$	1	1	$\cdots$	1	1
$\cdots$	$\cdots$	$\cdots$	0	0	$\cdots$	1	0

En donde tenemos una fila marcada en gris, en donde podemos ver que todas las formulas del conjunto Σ son iguales a 1 y tambien que α es 1. Si esto se cumple y no sucede que tenemos todas las formulas de la izquierda con unos, y el alpha de la derecha con un 0, entonces tenemos consecuencia lógica.
Otro ejemplo:

v_1	$\cdots$	v_n	α_1	α_2	$\cdots$	α_m	α
$\cdots$	$\cdots$	$\cdots$	1	1	$\cdots$	0	1
$\cdots$	$\cdots$	$\cdots$	1	1	$\cdots$	1	0
$\cdots$	$\cdots$	$\cdots$	0	0	$\cdots$	1	0

En este caso, ya no hay consecuencia lógica, debido a que no se cumple la condición establecida antes. La fila marcada en gris, tiene un 0 en la formula final, lo que nos dice que no es consecuencia lógica.
NOTA: Si tenemos un conjunto Σ tal que es imposible obtener una fila con solo unos, entonces **cualquier cosa** puede ser consecuencia lógica de Σ. ¡Usar con sabiduria para demostraciones!

7.1 Consecuencias lógicas clásicas

7.1.1 Modus ponens

$$\{p, p \to q\} \models q$$

p	q	p	$p \to q$	q
0	0	0	1	0
0	1	0	1	0
1	0	1	0	0
1	1	1	1	1

7.1.2 Modus tollens

$$\{\neg q, p \to q\} \models \neg p$$

p	q	p	$p \to q$	q
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	1	0

7.1.3 Resolución

$$\{p \vee q, \neg q \vee r\} \models p \vee r$$

p	q	r	$p \vee q$	$\neg q \vee r$	$p \vee r$
0	0	0	0	1	0
0	0	1	0	1	1
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	0	1
1	1	1	1	1	1

7.2 Trucos de consecuencia lógica

1. $\{1\} \models \alpha$, entonces α es una tautología
2. Si α es una contradicción, entonces $\{\alpha\} \models \beta$
3. Si $\Sigma \models \alpha$, entonces $\Sigma \cup \{\beta\} \models \alpha$ para todo β
4. Si $\Sigma \cup \{\alpha\} \models \beta$ y $\Sigma \models \alpha$, entonces $\Sigma \models \beta$

7.3 Más consecuencias lógicas clásicas

A continuación, vamos a mostrar más consecuencias lógicas, sumando a la lista en 7.1

1. Modus ponens: $\{p, p \to q\} \models q$
2. Modus tollens: $\{\neg q, p \to q\} \models \neg p$
3. Resolución: $\{p \vee q, \neg q \vee r\} \models p \vee r$
4. Silogismo: $\{p \to q, q \to r\} \models p \to r$
5. Silogismo disyuntivo: $\{p \vee q, \neg p\} \models q$
6. Conjunción: $\{p, q\} \models p \wedge q$
7. Simplificación Conjuntiva: $\{p \wedge q\} \models p$
8. Amplificación Disyuntiva: $\{p\} \models p \vee q$
9. Demostración Condicional: $\{p \wedge q, p \to (q \to r)\} \models r$
10. Demostración por casos: $\{p \to r, q \to r\} \models (p \vee q) \to r$

7.4 Composición y Consecuencia lógica

7.4.1 Definición

Considerando un conjunto $\Sigma = \{\alpha_1(p_1, \ldots, p_n), \ldots, \alpha_m(p_1, \ldots, p_n)\}$ y $\beta_1, \ldots, \beta_n$ como formulas proposicionales.
Una composición $\Sigma(\beta_1, \ldots, \beta_n)$, consiste en el conjunto resultante de valuar cada formula de Σ con $\beta_1, \ldots, \beta_n$.
En otras palabras:

$$\Sigma(\beta_1, \ldots, \beta_n) = \{\alpha_1(\beta_1, \ldots, \beta_n), \ldots, \alpha_m(\beta_1, \ldots, \beta_n)\}$$

7.4.2 Teorema

Sea Σ un conjunto de formulas (similar al de antes), y $\alpha, \beta_1, \ldots, \beta_n$, formulas proposicionales. Si $\Sigma \models \alpha$, entonces $\Sigma(\beta_1, \ldots, \beta_n) \models \alpha(\beta_1, \ldots, \beta_n)$.

8 Satisfacibilidad

8.1 Satisfacción de un conjunto de formulas

Se dice que una formula proposicional $\alpha(p_1, \ldots, p_n)$ es satisfacible si existe una valuación $v_1, \ldots, v_n$ tal que

$$\alpha(v_1, \ldots, v_n) = 1$$

Un conjunto $\Sigma = \{\alpha_1, \ldots, \alpha_m\}$ con variables $p_1, \ldots, p_n$ se dice que es satisfacible si existe una valuación $v_1, \ldots, v_n$ tal que

$$[\bigwedge_{i=1}^{m} = \alpha_i](v_1, \ldots, v_n) = 1$$

Si un conjunto o formula no es satisfacible, entonces se dice que es inconsistente.

8.2 Consecuencia lógica vs satisfacibilidad

Teorema: $\{\alpha_1, \ldots, \alpha_m\} \models \alpha$ si y solo si $\{\alpha_1, \ldots, \alpha_m, \neg\alpha\}$ es inconsistente.

8.3 Satisfacibilidad y representación de problemas

Problema: Dada una formula α, verificar si es o no satisfacible.
¿Como podemos resolver este problema? Si bien es posible ir probando todas las posibles valuaciones para verificar, es un proceso largo y poco eficiente. Tristemente, la respuesta a este problema, es que no es posible. No existe ningun otro método al momento de verificar si una formula es o no es consistente.

9 Lógica de Predicados

Hasta ahora, se ha trabajado unicamente con Lógica Proposicional. Esta funciona bien, pero tiene algunas limitaciones que vuelven imposible modelar algunas situaciones.

- No tiene objetos. Solo se pueden usar proposiciones.
- No tiene predicados.
- No tiene cuantificadores.

9.1 ¿Y qué tiene la Lógica de Predicados?

La lógica de predicados es una parte de la lógica de primer orden. La lógica de predicados nos va a permitir expresar ciertas estructuras las cuales no eramos capaces de expresar usando la lógica proposicional.

9.2 Predicados

Un predicado consiste en una proposicion abierta. El valor de verdad de un predicado dependerá del valor usado en la valuación. Generalmente, estos se simbolizan usando letras mayúsculas (Ej.: $P(x)$)
Ejemplos de predicados:

- $P(x)$:= x es par
- $R(x)$:= x es primo
- $M(x)$:= x es mortal

9.2.1 Predicados n-arios

Los predicados n-arios consisten en predicados los cuales usan más de una variable para verificar su valor de verdad.
Ejemplo: $O(x, y) := x \leq y$. Si $x = 2$ e $y = 3$, entonces $O(2, 3) = 1$

9.2.2 Dominio de predicado

Todo predicado está restringido a un cierto dominio de evaluación. Esto significa que sus valores de verdad solo se pueden evaluar cuando las variables que se usan en el predicado estan dentro del dominio designado.
Ej.: $O(x, y) := x \leq y$ sobre $\mathbb{N}$

9.2.3 Predicado 0-ario / Predicado degenerado

Corresponde a un predicado que no tiene ninguna variable libre. Tiene un valor de verdad el cual es totalmente independiente de su valuación.

9.2.4 Predicados compuestos

Un predicado compuesto corresponde a la combinación de diversos predicados básicos, usando distintos operadores para mezclarlos en la sentencia, o la cuantificación universal o existencial de algun predicado (Véase sección 9.3). Todos los predicados deben tener el mismo dominio.

9.3 Cuantificadores

9.3.1 Cuantificador Universal

Consideremos $P(x, y_1, \ldots, y_n)$ un predicado compuesto de dominio D.
El cuantificador universal corresponde a

$$P'(y_1, \ldots, y_n) := \forall x.P(x, y_1, \ldots, y_n)$$

donde x es la variable cuantificada e $y_1, \ldots, y_n$ son las variables libres.
Si para cierta valuación se cumple que $P'(\ldots) = 1$ significa que para toda variable libre se cumple lo especificado anteriormente.
Ejemplo

$$O(x, y) := x \leq y \text{ sobre } \mathbb{N}$$

$$O'(y) := \forall x.O(x, y)$$

$$O'(2) = \forall x.O(x, 2) = 0$$

Podemos notar que para $y = 2$, no se cumple para todo valor de x lo dictado en el predicado $O(x, y)$

$$O''(x) := \forall y.O(x, y)$$

$$O''(0) := \forall y.O(0, y) = 1$$

Si $x = 0$, debido a que estamos considerando a los naturales, entonces para todo valor de y se cumple siempre el predicado.

9.3.2 Cuantificador Existencial

Consideremos $P(x, y_1, \ldots, y_n)$ un predicado compuesto de dominio D.
El cuantificador existencial corresponde a

$$P'(y_1, \ldots, y_n) := \exists x.P(x, y_1, \ldots, y_n)$$

donde x es la variable cuantificada e $y_1, \ldots, y_n$ son las variables libres.
Si para cierta valuación se cumple que $P'(\ldots) = 1$ significa que para alguna combinación de variables libres se cumple lo especificado anteriormente.
Ejemplo

$$O(x, y) := x \leq y \text{ sobre } \mathbb{N}$$
$$O'(y) := \exists x.O(x, y)$$
$$O'(2) = \exists x.O(x, 2) = 1$$

9.4 Interpretaciones

En algunos casos, puede ocurrir que algún predicado o formula, dependiendo de ciertas condiciones, sea verdadero(a) o falso(a). Debido a esto, vamos a definir las *interpretaciones*.
Para comenzar, es importante destacar que desde ahora diremos que $P(x_1, \ldots, x_n)$ es un símbolo de predicado.
Una interpretación $\mathcal{I}$ para símbolo de predicado $P_1, \ldots, P_m$ se compone de

- Un dominio $\mathcal{I}$(dom)
- Para cada símbolo P_i, un predicado $\mathcal{I}(P_i)$

Sea $\alpha(x_1, \ldots, x_n)$ una formula y $\mathcal{I}$ una interpretación de los símbolos en α. Se dice que la interpretación $\mathcal{I}$ satisface α sobre $a_1, \ldots, a_n$ en $\mathcal{I}$(dom), expresado como

$$\mathcal{I} \models \alpha(a_1, \ldots, a_n)$$

si $\alpha(a_1, \ldots, a_n)$ es verdadero al evaluar cada símbolo en α según $\mathcal{I}$. En el caso que $\mathcal{I}$ no logre satisfacer a α, se anotará como

$$\mathcal{I} \not\models \alpha(a_1, \ldots, a_n)$$

Ejemplo

$$\mathcal{I}_1(\text{dom}) := \mathbb{N}$$
$$\mathcal{I}_1(P) := \text{x es par}$$
$$\mathcal{I}_1(O) := x < y$$
$$\alpha(x) := \exists y.P(y) \wedge O(x, y)$$
$$\mathcal{I}_1 \models \alpha(1) := \exists y.\text{y es par} \wedge 1 < y$$

10 Equivalencia lógica en Lógica de Predicados

Se tiene $\alpha(x_1, \ldots, x_n)$ y $\beta(x_1, \ldots, x_n)$ dos oraciones en lógica de predicados (no tienen variables libres). α y β serán logicamente equivalentes, escrito como:

$$\alpha \equiv \beta$$

si para toda interpretación $\mathcal{I}$ y para todo $a_1, \ldots, a_n$ se cumple que:

$$\mathcal{I} \models \alpha(a_1, \ldots, a_n) \text{ si, y solo si, } \mathcal{I} \models \beta(a_1, \ldots, a_n)$$

En otras palabras, funciona practicamente igual a la equivalencia lógica en lógica proposicional.

10.1 Equivalencias lógicas

Todas las equivalencias de lógica proposicional aplican aquí. Simplemente se tienen que cambiar las variables proposicionales por predicados de lógica de predicados. Aquí se muestra un ejemplo:
Conmutatividad (para operador $\wedge$)

En lógica proposicional	En lógica de predicados
$p \wedge q \equiv q \wedge p$	$\alpha \wedge \beta \equiv \beta \wedge \alpha$

Ahora, además de estas equivalencias, nos encontraremos con algunas nuevas

1. $\neg \forall x.\alpha \equiv \exists x.\neg\alpha$
2. $\neg \exists x.\alpha \equiv \forall x.\neg\alpha$
3. $\forall x.(\alpha \wedge \beta) \equiv (\forall x.\alpha) \wedge (\forall x.\beta)$
4. $\forall x.(\alpha \vee \beta) \equiv (\forall x.\alpha) \vee (\forall x.\beta)$

11 Tautología en Lógica de Predicados

Sea $\alpha(x_1, \ldots, x_n)$ una fórmula con variables libres $(x_1, \ldots, x_n)$. α es tautología si para toda interpretación $\mathcal{I}$ y para todo $(a_1, \ldots, a_n)$ en $\mathcal{I}$(dom) se tiene que:

$$\mathcal{I} \models \alpha(a_1, \ldots, a_n)$$

12 Consecuencia lógica en Lógica de Predicados

Una oración de lógica de predicados α es consecuencia lógica de un conjunto de oraciones Σ si para toda interpretación $\mathcal{I}$ y para todo $(a_1, \ldots, a_n)$ en $\mathcal{I}$(dom) se cumple que

$$\text{si } \mathcal{I} \models \Sigma(a_1, \ldots, a_n) \text{ entonces } \mathcal{I} \models \alpha(a_1, \ldots, a_n)$$

Si α es consecuencia lógica de Σ, entonces se denota como

$$\Sigma \models \alpha$$

13 Inferencia en Lógica de Predicados

1. **Instanciación Universal**
$$\frac{\forall x.\alpha(x)}{\alpha(a) \text{ para cualquier a}}$$
2. **Generalización Universal**
$$\frac{\alpha(a) \text{ para cualquier a}}{\forall x.\alpha(x)}$$
3. **Instanciación Existencial**
$$\frac{\exists x.\alpha(x)}{\alpha(a) \text{ para algún a (nuevo)}}$$
4. **Generalización Existencial**
$$\frac{\alpha(a) \text{ para algún a}}{\exists x.\alpha(x)}$$

14 Demostraciones

14.1 Afirmación matemática

Una afirmación matemática consiste en una proposición en lógica de predicados

Tipos de afirmaciones matemáticas

- Teorema: Afirmación matemática verdadera y demostrable.
- Proposición: Similar a un Teorema, pero de menor importancia.
- Definición: Sentencia usada para explicar la naturaleza de algún objeto matemático.
- Axioma: Suposición que se considera cierta, y se usa como base para demostrar algo.
- Lema: Proposición demostrada, usada como herramienta para demostrar un teorema.
- Corolario: Teorema que se deduce de un axioma
- Conjetura: Afirmación que es intuitivamente correcta, pero que no ha sido demostrada.
- Problema: Conjetura, que podría ser verdadera o falsa. No se sabe su valor de verdad.

14.2 ¿Qué es una demostración?

Una demostración es un argumento válido que permite establecer la verdad de una afirmación matemática. Con argumento válido, nos referimos a una secuencia de argumentos que puede estar compuesta por

- Axiomas.
- Hipótesis o supuestos.
- Afirmaciones implicadas por argumentos previos.

Cada argumento en la secuencia lógica de argumentos está conectado con el anterior por una *regla de inferencia* (consecuencia lógica).
El último paso de la secuencia establece la verdad de la afirmación.

¿Qué NO es una demostración?

- Una secuencia de símbolos.
- Una secuencia disconexa o imprecisa de argumentos.

Al final, la secuencia de argumentos debe ser lo más clara, precisa y completa posible, para así, convencer al lector u oyente, sin dar lugar a dudas acerca de la veracidad de la demostración.

14.3 ¿Cómo puedo encontrar una secuencia de argumentos?

Si lo que se desea es encontrar una secuencia de argumentos que logre demostrar un teorema se requiere de las siguientes cosas

- *Experiencia*: La práctica hace al maestro.
- *Intuición*: Coloquialmente conocida como *La cachativa*
- *Creatividad*: Pensar fuera de la caja
- *Perseverancia*: If at first you don't succeed, try, try again.
- **Métodos de demostración**

15 Métodos de demostración

15.1 Demostración Directa

Si se desea demostrar

$$\forall x.P(x) \to Q(x)$$

entonces se supone que $P(n)$ es verdadero para un n cualquiera, y demostramos que $Q(n)$ es verdadero.

Ejemplo

- Un entero n en $\mathbb{Z}$ se dice **par** si existe k en $\mathbb{Z}$ tal que $n = 2k$.
- Un entero n en $\mathbb{Z}$ se dice **impar** si existe k en $\mathbb{Z}$ tal que $n = 2k + 1$.

Teorema: Para todo $n \in \mathbb{Z}$, si n es impar, entonces n^2 es impar.
Para realizar la demostración, primero suponemos que n es impar. Por definición, existe un $n \in \mathbb{Z}$ tal que $n = 2k + 1$.

$$\begin{array}{lcl} n^2 & = & (2k+1)^2 \\ n^2 & = & 4k^2 + 4k + 1 \\ n^2 & = & 2 \cdot (2k^2 + 2k) + 1 \end{array}$$

Al definir $k' = 2k^2 + 2k$, entonces $n^2 = 2k' + 1$. Esto corresponde a la definición de un número impar, por lo que n^2 es impar.

15.2 Demostración por Contrapositivo

Si se desea demostrar

$$\forall x.P(x) \to Q(x) \equiv \forall x.\neg Q(x) \to \neg P(x)$$

entonces se supone que $Q(n)$ es falso para un n cualquiera, y demostramos que $P(n)$ es falso también.

Ejemplo

Teorema: Suponga a y b son positivos. Si $n = ab$, entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.
Para realizar la demostración por contrapositivo, debemos considerar que si $a > \sqrt{n}$ y $b > \sqrt{n}$, entonces $n \neq ab$, considerando la información entregada en el enunciado. Supongamos que $a > \sqrt{n}$ y $b > \sqrt{n}$ con n positivo.

$$\begin{array}{lcll} n & = & \sqrt{n} \cdot \sqrt{n} & \\ n & < & a \cdot \sqrt{n} & (\text{por } a > \sqrt{n}) \\ n & < & a \cdot b & (\text{por } b > \sqrt{n}) \end{array}$$

Tenemos que $n < ab$, lo que automáticamente significa que $n \neq ab$.

15.3 Demostración por Contradicción

Si se desea demostrar

$$(\neg R) \to (S \wedge \neg S)$$

entonces se supone que $\neg R$ es verdadero e inferimos una contradicción. En este caso, R debe ser verdadero. Otro caso podría ser que se quiera demostrar

$$R := \forall x.P(x) \to Q(x)$$

Entonces, para realizar la demostración, consideramos la negación de la expresión anterior:

$$\neg R := \exists x.P(x) \wedge \neg Q(x)$$

y suponemos que existe un n tal que $P(n)$ es verdadero y $Q(n)$ es falso, e inferimos una contradicción.

Ejemplo

- Un número r en $\mathbb{R}$ se dice racional si existen enteros p y q tales que:

$$r = \frac{p}{q}$$

  con $q \neq 0$ y p, q no tienen divisores en común, exceptuando al 1.

- Un número r en $\mathbb{R}$ se dice irracional si no es racional.

Teorema: $\sqrt{2}$ es irracional.
Para comenzar la demostración, se supone que $\sqrt{2}$ es racional. Entonces, existen p y q que pertenecen a $\mathbb{Z}$, sin divisores en común, tal que $\sqrt{2} = \frac{p}{q}$.

$$\begin{aligned} \sqrt{2} &= \frac{p}{q} \\ 2 \cdot q^2 &= p^2 \end{aligned}$$

Entonces, p^2 es par, por lo que p es par (debido a una propiedad existente en los numeros pares).
Como p es par, entonces $p = 2k$ para algún k en $\mathbb{Z}$.

$$\begin{aligned} 2 \cdot q^2 &= p^2 \\ 2 \cdot q^2 &= (2k)^2 \\ q^2 &= 2 \cdot k^2 \end{aligned}$$

Entonces, q^2 es par, por lo que q es par también.
¡Esto es una contradicción! Se supone que si es irracional, p y q no pueden tener divisores comunes, y al ser pares, tienen como común divisor al 2. Como no es racional, significa que es irracional, y así, *Q.E.D.*

15.4 Demostración por Análisis de Casos

Si se desea demostrar

$$\forall x \in D.P(x)$$

entonces se va a dividir el dominio de posibilidades D en una cantidad finita de casos $D_1, D_2, \ldots, D_k$, de forma que

$$D = D_1 \cup D_2 \cup \ldots \cup D_k$$

Por ultimo, se demuestra que para todo subdominio D_i se cumple que

$$\forall x \in D_i.P(x)$$

con i desde 1 hasta k.

Ejemplo

Teorema: Para todo entero n se cumple que $n^2 \geq n$.
Para realizar la demostración, consideremos que

- Si $n = 0$, entonces $0^2 = 0$. Por lo tanto, $0^2 \geq 0$
- Si $n \geq 1$, entonces:

$$\begin{aligned} n &\geq 1 \\ n^2 &\geq n \quad \text{(multiplicando ambos lados por } n \geq 0) \end{aligned}$$

- Si $n \leq -1$, como $n^2 \geq 0$, por lo que se tiene que $n^2 \geq n$

Recomendación: *Cuando todos los métodos anteriores han fallado y no se sabe por donde empezar, una 'estrategia' es empezar demostrando los casos simples para así ganar intuición en la demostración general.*

15.5 Demostración de Doble Implicación

Si se desea demostrar

$$\forall x.(P(x) \leftrightarrow Q(x))$$

entonces se deben demostrar dos afirmaciones

$$\forall x.(P(x) \rightarrow Q(x)) \land \forall x.(P(x) \leftarrow Q(x))$$

Ejemplo

Teorema: Para todo numero natural n, se tiene que n es impar si, y solo si, n^2 es impar.
Entonces, para demostrar debemos

- ($\rightarrow$) Si n es impar, entonces n^2 es impar. Esta demostración se realizó previamente en 15.1.
- ($\leftarrow$) Si n^2 es impar, entonces n es impar.
  Mediante contrapositivo, si n^2 no es impar, entonces n tampoco es impar. El no ser impar significa ser par. Por lo tanto, podemos demostrar la afirmación n es par, entonces n^2 es par. Trivialmente, esto es algo que ya sabemos (en una prueba, deberías demostrarlo igual). De esta forma, queda demostrado que si n^2 es impar, entonces n es impar.

Como hemos demostrado que la teoría se cumple para ambos lados, Q.E.D.

15.6 Demostración por contra-ejemplo

Si se desea demostrar

$$\forall x.P(x)$$

entonces se debe encontrar un elemento n cualquiera tal que $P(n)$ es falso.

Ejemplo

Teorema: Es falso que todo número mayor a 1 es la suma de dos cuadrados perfectos.
Para demostrar, probamos con los dos primeros números mayores que 1

$$\begin{array}{lcl} 2 & = & 1^2 + 1^2 \\ 3 & \neq & 1^2 + 1^2 \\ 3 & \neq & 2^2 + 1^2 \end{array}$$

Nos damos cuenta de inmediato que para el 3 esto ya no se cumple. Así, se logra demostrar correctamente que la afirmación es falsa.

15.7 Demostración Existencial

Si se desea demostrar

$$\exists x.P(x)$$

entonces se debe demostrar que existe un elemento n tal que $P(n)$ es verdadero. No es estrictamente necesario mostrar n de forma explícita.

Ejemplo

Teorema: Existen dos números irracionales a y b tal que a^b es racional.
Consideremos $\sqrt{2}$, ya que este es un numero irracional. Entonces, $a = \sqrt{2}$, $b = \sqrt{2}$ y $a^b = \sqrt{2}^{\sqrt{2}}$. Nosotros no sabemos que es lo que ocurre con $\sqrt{2}^{\sqrt{2}}$, asi que pongamonos en los casos posibles.

- Si $\sqrt{2}^{\sqrt{2}}$ es racional, entonces $a = \sqrt{2}$ y $b = \sqrt{2}$ logra demostrar de forma satisfactoria el teorema.
- Si $\sqrt{2}^{\sqrt{2}}$ es irracional, entonces debemos considerar otro ejemplo. Un ejemplo que podemos analizar y comprobar con facilidad sería $a = \sqrt{2}^{\sqrt{2}}$ y $b = \sqrt{2}$. Entonces...

$$\begin{aligned}(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} &= \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} \\ (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} &= \sqrt{2}^{2} \\ (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} &= 2\end{aligned}$$

Asi, logramos comprobar que a^b es racional, y esto demuestra de que al menos existe un valor de a y de b que permiten que el teorema se cumpla.

15.8 Demostración por Inducción

Supongamos que queremos demostrar que

$$\forall x.P(x) \text{ sobre } \mathbb{N}$$

Para una afirmación $P(x)$ sobre los naturales, si $P(x)$ cumple que:

- $P(0)$ es verdadero. *(Caso base)*
- Si $P(n)$ *(Hipótesis de inducción)* es verdadero, entonces $P(n+1)$ *(Tesis de inducción)* es verdadero.

entonces para todo n en los naturales se tiene que $P(n)$ es verdadero.

Ejemplo

Teorema: La suma de los primeros n números naturales es igual a $\dfrac{n\cdot(n+1)}{2}$.
Primero, demostremos que se cumple para un caso base. En este caso, usaremos $n = 0$

$$\textbf{Caso base } (n=0): \quad 0 = \frac{0\cdot(0+1)}{2} = 0$$

Ahora supongamos que nuestro teorema se cumple para un n cualquiera. Demostremos que se cumple para $n+1$

$$\begin{aligned}\textbf{Hipótesis:} \quad 0+1+\ldots n &= \frac{n\cdot(n+1)}{2} \\ \textbf{Inducción:} \quad 0+1+\ldots n+(n+1) &= 0+1+\ldots n+(n+1) \quad \text{esto es [caso n]} + (n+1) \\ 0+1+\ldots n+(n+1) &= \frac{n\cdot(n+1)}{2}+(n+1) \\ 0+1+\ldots n+(n+1) &= \frac{(n+1)\cdot((n+1)+1)}{2}\end{aligned}$$

Podemos notar como la ultima fórmula es igual a la del teorema, pero reemplazando n por $n+1$. Esto demuestra que la formula si es válida para n, entonces si es válida para $n+1$, demostrando correctamente el teorema.

16 Conjuntos

16.1 ¿Qué es un conjunto?

Un conjunto corresponde a una colección bien definida de objetos. Estos objetos son denominados como **elementos del conjunto** y se dice que estos **pertenecen** (expresado con el simbolo $\in$) a él.
Cuando definimos un conjunto, se usan símbolos de llaves y dentro se colocan todos los objetos que pertenecen al conjunto.
Ejemplo:

$$S = \{1, 2, 3, 4\}$$

16.2 Nociones básicas de los conjuntos

16.2.1 Pertenencia ($\in$)

Si tenemos un conjunto S y un objeto a, se dice que

- $a \in S$ cuando el objeto a se encuentra dentro del conjunto S.
- $a \notin S$ cuando el objeto a **no** se encuentra dentro del conjunto S.

NOTA: Un objeto puede ser un conjunto. Esto significa que un conjunto puede pertenecer a otro conjunto.

16.2.2 Subconjunto ($\subseteq$)

Considerando a un conjunto A y un conjunto B, se dice que A es subconjunto de B si

$$\forall x.x \in A \rightarrow x \in B$$

En otras palabras, A es subconjunto de B si todo elemento presente en A está presente en B también. Cuando esto ocurre, se denota como $A \subseteq B$ (y cuando no, lógicamente se escribe como $A \nsubseteq B$)

16.2.3 Igualdad de conjuntos

Diremos que dos conjuntos A y B son iguales si se cumple que

$$A \subseteq B \land B \subseteq A \quad \text{o, escrito de otra forma} \quad \forall x.x \in A \leftrightarrow x \in B$$

En palabras simples, dos conjuntos son iguales cuando ambos conjuntos tienen exactamente los mismos objetos, sin ninguno que pertenezca a un conjunto y no a otro. Esto se expresa como $A = B$ (y cuando no, $A \neq B$).

16.2.4 Conjunto vacío

Existe un conjunto único $\emptyset$, el cual llamamos *conjunto vacío*, el cual cumple que

$$\forall x.x \notin \emptyset$$

16.3 Descripción de un conjunto

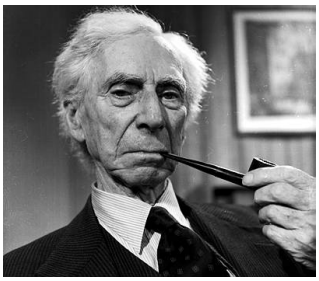
1. Por extensión: Este es el método más básico y el cual se describió anteriormente. Simplemente se listan todos los contenidos del conjunto entre llaves.
   Ejemplo:
   $$S = \{1, 2, 3, 4\}$$

2. Por comprensión: Se define una propiedad $\delta(x)$ en algún lenguaje formal que solo cumplen los elementos del conjunto.
   Ejemplo:
   $$S = \{x | \delta(x) \text{ es verdadero}\}$$
   Ejemplo un poco más creativo:
   $$P = \{x | \forall x.x \text{ es par}\}$$

16.4 Paradoja de Russell o Paradoja del Barbero (1901)[1]

Esta es una paradoja enunciada por Bertrand Russell. Para comenzar, se define el siguiente conjunto

$$S^* = \{B \mid B \notin B\}$$


B. Russell (1872 - 1970)

S^* corresponde al "conjunto de todos los conjuntos que no se contienen a si mismos como miembros". Ahora, recordemos que por la definición de lo que es un conjunto, esto es equivalente a

$$\forall B.B \in S^* \leftrightarrow B \notin B$$

O sea, "cada conjunto es elemento de B si y solo si no es elemento de si mismo". Debido a que B es un conjunto, lo podemos sustituir de la siguiente forma

$$S^* \in S^* \leftrightarrow S^* \notin S^*$$

lo cual es una contradicción.
Esto puede ser un poco complicado de entender así. Intentemos entenderlo con la historia del Barbero.

Una definición como esta es bastante problemática. El problema aquí es *"considerar definiciones que se referencian a si mismas"*. Esto nos deja de lección que no todas las definiciones son válidas en la teoría de conjuntos.[2]

[1] Esta sección contiene información extraída del siguiente artículo de Wikipedia.
[2] Todas las definiciones que se verán durante el curso son válidas, pero esto es una lección de que no siempre es así.

16.5 Operaciones sobre conjuntos

- Unión ($\cup$): $A \cup B$ son todos los elementos que se encuentran en A o en B.

$$A \cup B = \{x | x \in A \vee x \in B\}$$

- Intersección ($\cap$): $A \cap B$ son todos los elementos que se encuentran en A y B al mismo tiempo.

$$A \cap B = \{x | x \in A \wedge x \in B\}$$

- Diferencia ($\backslash$): $A \backslash B$ son todos los elementos que se encuentran en A y no en B.

$$A \backslash B = \{x | x \in A \wedge x \notin B\}$$

- Complemento (A^C): A^C corresponde a todos los elementos que no se encuentran en A.

$$A^C = \{x | x \notin A\}$$

16.5.1 Propiedades de las operaciones sobre conjuntos

Para conjuntos A, B y C y un universo $\mathcal{U}$ tenemos las siguientes propiedades

1. Asociatividad:
$$\begin{aligned} A \cup (B \cup C) &= (A \cup B) \cup C \\ A \cap (B \cap C) &= (A \cap B) \cap C \end{aligned}$$

2. Conmutatividad:
$$\begin{aligned} A \cup B &= B \cup A \\ A \cap B &= B \cap A \end{aligned}$$

3. Idempotencia:
$$\begin{aligned} A \cup A &= A \\ A \cap A &= A \end{aligned}$$

4. Absorción:
$$\begin{aligned} A \cup (A \cap B) &= A \\ A \cap (A \cup B) &= A \end{aligned}$$

5. Distributividad:
$$\begin{aligned} A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \end{aligned}$$

6. De Morgan
$$\begin{aligned} (A \cup B)^C &= A^C \cap B^C \\ (A \cap B)^C &= A^C \cup B^C \end{aligned}$$

7. Elemento neutro:
$$\begin{aligned} A \cup \emptyset &= A \\ A \cap \mathcal{U} &= A \end{aligned}$$

8. Dominación:
$$\begin{aligned} A \cap \emptyset &= \emptyset \\ A \cup \mathcal{U} &= \mathcal{U} \end{aligned}$$

9. Elemento inverso:
$$\begin{aligned} A \cup A^C &= \mathcal{U} \\ A \cap A^C &= \emptyset \end{aligned}$$

16.5.2 Paréntesis y precedencia

Se asumirá el siguiente orden de precedencia entre operadores

Operadores	Precedencia
$\cdot^C$	1
$\cap$	2
$\cup$	3

16.5.3 Operaciones generalizadas

- Unión generalizada: $\bigcup \mathcal{S}$ son todos los elementos que pertenecen a algún elemento de $\mathcal{S}$.

$$\bigcup \mathcal{S} = \{x \mid \exists A.\ A \in \mathcal{S} \land x \in A\} = \bigcup_{A \in \mathcal{S}} A = \bigcup_{i=1}^{k} A_i$$

- Intersección generalizada: $\bigcap \mathcal{S}$ son todos los elementos que pertenecen a todos los elementos de $\mathcal{S}$

$$\bigcap \mathcal{S} = \{x \mid \forall A.\ A \in \mathcal{S} \to x \in A\} = \bigcap_{A \in \mathcal{S}} A = \bigcap_{i=1}^{k} A_i$$

17 Anexo

17.1 Ejercicio - Inferencia lógica de predicados

Algún estudiante en la sala no estudió para el examen.
Todos los estudiantes de la sala pasaron el examen.

Algún estudiante pasó el examen y no estudió.

¿Cómo modelamos este problema?

$$S(x) := x \text{ está en la sala}$$

$$E(x) := x \text{ estudió para el examen}$$

$$X(x) := x \text{ pasó el examen}$$

Entonces, la consecuencia lógica quedaría así:

$$\frac{\begin{array}{l}\exists x.S(x) \wedge \neg E(x) \\ \forall x.S(x) \rightarrow X(x)\end{array}}{\exists x.X(x) \wedge \neg E(x)}$$

¿Cómo inferimos esta consecuencia lógica?

1. $\exists x.S(x) \wedge \neg E(x)$ (Premisa)
2. $S(a) \wedge \neg E(a)$ (Instanciación Existencial 1.)
3. $S(a)$ (Simplificación Conjuntiva 2.)
4. $\forall x.S(x) \rightarrow X(x)$ (Premisa)
5. $S(a) \rightarrow X(a)$ (Instanciación Universal 4.)
6. $X(a)$ (Modus ponens 3. y 5.)
7. $\neg E(a)$ (Simplificación Conjuntiva 2.)
8. $X(a) \wedge \neg E(a)$ (Conjunción 6. y 7.)
9. $\exists x.X(x) \wedge \neg E(x)$ (Generalización Existencial 8.)