Resumen general de Matemáticas Discretas

Andrés Cabezas y Sebastián Poblete

28 de junio de 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 $\mathcal{I}(\text{dom})$
- 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 $\mathcal{I}(\text{dom})$, 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 $\mathcal{I}(\text{dom})$ 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 $\mathcal{I}(\text{dom})$ 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 $n = 2k + 1$.

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

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.

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

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

15.3. Demostración por Contradicción

Si se desea demostrar

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

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

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

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 $\sqrt{2} = \frac{p}{q}$.

$$\begin{array}{rcl} \sqrt{2} & = & \dfrac{p}{q} \\ 2 \cdot q^2 & = & p^2 \end{array}$$

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 $\mathbb{Z}$.

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

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:

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

- 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

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

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

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

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 $\frac{n \cdot (n+1)}{2}$.
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)

Esta es una paradoja enunciada por Bertrand Russell[1]. Para comenzar, se define el siguiente conjunto

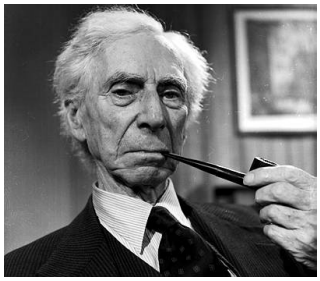
$$S^* = \{B \mid B \notin B\}$$

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

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



B. Russell (1872 - 1970)

[1] Esta sección contiene información extraída del siguiente artículo de Wikipedia.

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]

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

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

- 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]Todas las definiciones que se verán durante el curso son válidas, pero esto es una lección de que no siempre es así.

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 $\mathcal{S}$.

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

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

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

16.6. Conjunto Potencia

Para un conjunto A, el conjunto potencia $\mathcal{P}(A)$ de todos los subconjuntos de A es definido como:

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}$$

En palabras simples, el conjunto potencia de A corresponde al conjunto que contiene a todos los subconjuntos de A.

16.7. Cardinalidad de un conjunto

La cardinalidad del conjunto corresponde a la cantidad de elementos distintos contenidos en un conjunto

$$A = \#\text{ de elementos distintos en } A$$

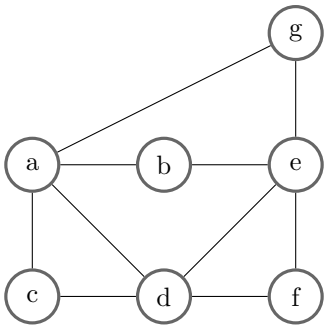
Teorema:

$$A = \{1, 2, 3, \ldots, n\} \rightarrow |\mathcal{P}(A)| = 2^n$$

En otras palabras, la cardinalidad del conjunto potencia de A corresponde a 2 elevado a la cardinalidad del conjunto A.

16.8. Grafos como conjuntos

Pero ... ¿qué es un grafo?[3]
Un grafo consiste en un conjunto de objetos llamados vertices y nodos, los cuales se encuentran unidos entre sí.
Definición: Un grafo G sobre el dominio V es un subconjunto $E \subseteq \mathcal{P}(V)$, tal que para todo $e \in E$ se cumple que $|e| = 2$.



V = {a, b, c, d, e, f, g}
E = { {a,b}, {a,c}, {a,d}, {a,g}, {b,e}, {c,d}, {d,e}, {d,f}, {e,f}, {e,g} }

En un grafo, los elementos que están presentes en V los llamamos *vértices o nodos*, y los elementos en E los llamamos *aristas*.

16.9. Pares Ordenados

Para dos elementos a y b se define el par ordenado (a, b) como

$$(a, b) = \{\{a\}, \{a, b\}\}$$

De forma mas informal, decimos que (a, b) es un par ordenado si es que el primer elemento (a) se distingue del segúndo elemento (b). Por esto, tenemos que $(a, b) \neq (b, a)$.
Generalización: Se define una *n-tupla ordenada* como

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

[3]Información extraida del siguiente artículo de Wikipedia

16.10. Producto Cartesiano

Sea A y B conjuntos. El producto cartesiano se define como

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

Si tenemos n conjuntos $A_1, A_2, \ldots, A_n$, el producto cartesiano generalizado es

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i\}$$

17. Relaciones

Considerando un conjunto A y B, R es una relación binaria sobre A y B si se cumple que

$$R \subseteq A \times B$$

Es posible que $B = A$, entonces se dice que R es una relación binaria sobre A

$$R \subseteq A \times A$$

Notación: Para una relación R y un par (a, b), se usará la siguiente notación

$$\left.\begin{array}{c} (a,b) \in R \\ \text{o} \\ a \ R \ b \end{array}\right\} \quad (a,b) \text{ pertenece a la relación } R$$

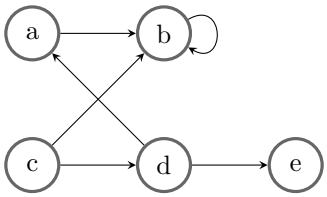
$$\left.\begin{array}{c} (a,b) \notin R \\ \text{o} \\ a \not R \ b \end{array}\right\} \quad (a,b) \text{ no pertenece a la relación } R$$

17.1. Representación de Relaciones

17.1.1. Grafos dirigidos

Toda relación binaria R sobre A se puede ver como un grafo dirigido $G_R = (A, R)$
Ejemplo:

$$A = \{a, b, c, d, e\} \quad ; \quad R = \{(a,b), (b,b), (c,b), (c,d), (d,a), (d,d), (d,e)\}$$



17.1.2. Matrices sobre bits / Representación Matricial

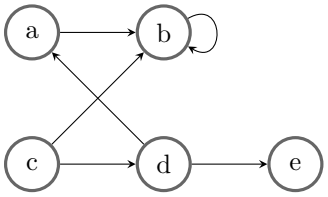
Sea $A = \{a_1, a_2, \ldots, a_n\}$ un conjunto y R una relación binaria sobre A. Definimos la matriz M_R que representa a la relación R como

$$M_R[i,j] = \begin{cases} 1 & \text{si } a_i \ R \ a_j \\ 0 & \text{si } a_i \not R \ a_j \end{cases}$$

Ejemplo:

$$A = \{a, b, c, d, e\} \quad ; \quad R = \{(a,b), (b,b), (c,b), (c,d), (d,a), (d,d), (d,e)\}$$

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



Operaciones sobre matrices: Dada dos matrices de bits M y N de tamaño n, entonces

$$\begin{array}{rcll} (M \vee N)[i,j] & = & M[i,j] \vee N[i,j] & \\ (M \wedge N)[i,j] & = & M[i,j] \wedge N[i,j] & \\ (\neg M)[i,j] & = & \neg M[i,j] & \\ M[i,j] & \leq & N[i,j] & \text{para todo } 1 \leq i \leq n \text{ y } 1 \leq j \leq n \text{ asumiendo que } 0 \leq 1. \end{array}$$

17.2. Operaciones entre relaciones

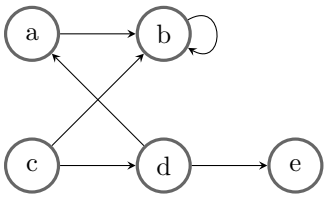
Sea A un conjunto y $R \subseteq A \times A$. Se definen las siguientes operaciones

- Proyección 1: $\pi_1(R)$ son todos los elementos que estan en la primera componente de R (No se consideran los duplicados).
$$\pi_1(R) = \{x \mid \exists y \in A.(x,y) \in R\}$$
- Proyección 2: $\pi_2(R)$ son todos los elementos que están en la segúnda componente de R (No se consideran los duplicados).
$$\pi_2(R) = \{y \mid \exists x \in A.(x,y) \in R\}$$
- Inverso: R^{-1} son todos los pares (x,y) de la relación R, pero al revés (como (y,x)). Más formalmente escrito como:
$$R^{-1} = \{(x,y) \mid (y,x) \in R\}$$
- Composición: $R_1 \circ R_2$ son todos los pares (x,y) que cumplen con que exista un z tal que $(x,z) \in R_1$ y $(z,y) \in R_2$
$$R_1 \circ R_2 = \{(x,y) \mid \exists z.(x,z) \in R_1 \wedge (z,y) \in R_2\}$$
- Unión: $R_1 \cup R_2$ son todos los pares que existen en R_1 o R_2. De forma más formal:
$$R_1 \cup R_2 = \{(x,y) | (x,y) \in R_1 \vee (x,y) \in R_2\}$$
- Intersección: $R_1 \cap R_2$ son todos los pares que existen en R_1 y R_2 de forma simultánea. Más formalmente expresado como:
$$R_1 \cap R_2 = \{(x,y) | (x,y) \in R_1 \wedge (x,y) \in R_2\}$$
- Relación identidad: I_A solamente contiene a los pares (x,x) para los x que existen en A.
$$I_A = \{(x,x) | x \in A\}$$

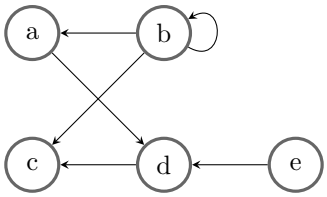
Debido a que esta parte puede llegar a ser un poco complicada de entender, vamos a mostrar una serie de ejemplos en base al conjunto y relación que tenemos de antes.

$$A = \{a,b,c,d,e\} \quad ; \quad R = \{(a,b),(b,b),(c,b),(c,d),(d,a),(d,d),(d,e)\}$$

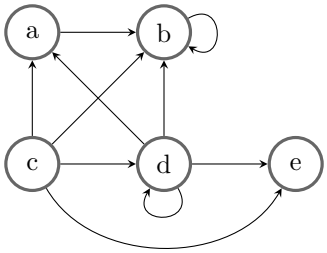
$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$



$$\pi_1(R) = \{a, b, c, d\} \quad ; \quad \pi_2(R) = \{a, b, d, e\}$$
$$R^{-1} = \{(b, a), (b, b), (b, c), (d, c), (a, d), (d, d), (e, d)\}$$



$$R \circ R = \{(a, b), (b, b), (c, b), (c, a), (c, d), (c, e), (d, b), (d, a), (d, d), (d, e)\}$$



17.3. Tipos de Relaciones

- Refleja: $\forall a \in A.(a, a) \in R$
- Irrefleja: $\forall a \in A.(a, a) \notin R$
- Simétrica: $\forall a, b \in A.(a, b) \in R \rightarrow (b, a) \in R$
- Asimétrica: $\forall a, b \in A.(a, b) \in R \rightarrow (b, a) \notin R$
- Antisimétrica: $\forall a, b \in A.((a, b) \in R \wedge (b, a) \in R) \rightarrow a = b$
- Transitiva: $\forall a, b, c \in A.((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$
- Conexa: $\forall a, b \in A.(a, b) \in R \vee (b, a) \in R$

17.3.1. Tipos de Relaciones caracterizadas con operaciones

Se considera un conjunto A y una relación binaria $R \subseteq A \times A$

- R es refleja si y solo si $I_A \subseteq R$.
- R es irrefleja si y solo si $R \cap I_A = \emptyset$.
- R es simétrica si y solo si $R = R^{-1}$.
- R es asimétrica si y solo si $R \cap R^{-1} = \emptyset$.
- R es antisimétrica si y solo si $R \cap R^{-1} \subseteq I_A$.
- R es transitiva si y solo si $R \circ R \subseteq R$.
- R es conexa si y solo si $R \cup R^{-1} = A \times A$.

17.4. Ordenes Parciales

Si tenemos un conjunto A y una relación $R \subseteq A \times A$, decimos que R es un orden parcial si es que cumple que

- R es refleja: $I_A \subseteq R$
- R es antisimétrica: $R \cap R^{-1} \subseteq I_A$
- R es transitiva: $R \circ R \subseteq R$

El orden parcial se denota como $(A, \preceq)$.

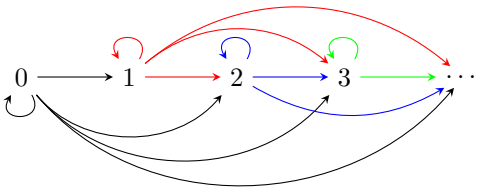
17.4.1. Ordenes Totales

Si tenemos un conjunto A y un orden parcial $(A, \preceq)$, se dice que este orden parcial es un orden total si es que se cumple que la relación $R \subseteq A \times A$ es conexa. En otras palabras, un orden total debe cumplir con

- R es refleja: $I_A \subseteq R$
- R es antisimétrica: $R \cap R^{-1} \subseteq I_A$
- R es transitiva: $R \circ R \subseteq R$
- R es conexa: $R \cup R^{-1} = A \times A$

17.4.2. Representación de un Orden Parcial

¿Cómo se ve un orden parcial representado con grafos?
Consideremos como ejemplo, el orden $\leq$ sobre $\mathbb{N}$



Este grafo queda demasiado enredado. Normalmente, para representar ordenes parciales, se usa el **Diagrama de Hasse**, el cual consiste en un diagrama de grafos, tal como el anterior, pero omitiendo los loops y las aristas transitivas[4].
Considerando la descripción anterior, el diagrama de Hasse del orden $\leq$ sobre $\mathbb{N}$ se vería así

$$0 \longrightarrow 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow \cdots$$

17.5. Elementos extremos

- Cotas superiores: $c \in A$ es una cota superior de S si y solo si $\forall y \in S.y \preceq c$
- Maximales: $\hat{x} \in S$ es un maximal si y solo si $\forall y \in S.\hat{x} \preceq y \to \hat{x} = y$
- Máximo: $x^{\uparrow} \in S$ es un máximo si y solo si $\forall y \in S.y \preceq x^{\uparrow}$
- Cotas inferiores: $c \in A$ es una cota inferior de S si y solo si $\forall y \in S.c \preceq y$
- Minimales: $\check{x} \in S$ es un minimal si y solo si $\forall y \in S.y \preceq \check{x} \to \check{x} = y$
- Mínimo: $x^{\downarrow} \in S$ es un máximo si y solo si $\forall y \in S.x^{\downarrow} \preceq y$

[4]Con esto nos referimos a que se omite $(a, b) \in \preceq$ si es que existe c de forma que $(a, c) \in \preceq$ y $(b, c) \in \preceq$

17.5.1. Sobre minimales y minimos

Sea $(a, \preceq)$ un orden parcial y $S \subseteq A$ distinto de $\emptyset$.

- Si S tiene un elemento mínimo, entonces ¿es único?
  Si. Es único.[5]
- ¿Tiene S siempre un mínimo?
  No. Es posible tener conjuntos que no tienen mínimos
- Si x es mínimo, entonces ¿es x minimal?
  Si. Un mínimo es siempre minimal también.[6]
- Si x es minimal, entonces ¿es x es mínimo?
  No necesariamente.
- ¿Tiene S siempre un elemento minimal?
  No necesariamente.

Con respecto a esto, también es verdadero respecto a maximales y máximos.

17.6. Ínfimos

Decimos que c^* es infimo si es una cota inferior de S y de todas las cotas inferiores de S, c^* es la cota inferior mayor.

17.7. Supremos

Decimos que c^* es supremo si es una cota superior de S y de todas las cotas superiores de S, c^* es la cota superior menor.

17.8. Clausuras

Sea A un conjunto y $R \subseteq A \times A$ una relación

17.8.1. Clausura Refleja

Una relación $R^r \subseteq A \times A$ es la clausura refleja de R si

- $R \subseteq R^r$
- R^r es refleja.
- Para toda relación refleja R' con $R \subseteq R'$ se cumple $R^r \subseteq R'$.

R^r es la menor relación refleja que contiene a R.

17.8.2. Clausura Transitiva

Una relación $R \subseteq A \times A$ es la clausura transitiva de R si

- $R \subseteq R^t$
- R^t es transitiva.
- Para toda relación refleja R' con $R \subseteq R'$ se cumple $R^t \subseteq R'$.

R^t es la menor relación transitiva que contiene a R.

[5] Se puede consultar la demostración en el anexo, subsección 2
[6] Se puede consultar la demostración en el anexo, subsección 3

17.8.3. Cálculo de clausuras

$$R^r = R \cup I_A \quad ; \quad R^t = \bigcup_{i=1}^{\infty} R^i$$

donde

Símbolo	Significa
I_A	Relación identidad
R^i	$R^{i-1} \circ R$
R^2	$R \circ R$

18. Relaciones de Equivalencia

Si se tiene que A un conjunto y $R \subseteq A \times A$ una relación binaria, se dice que R es una relación de equivalencia si cumple con ser una relación

- Refleja: $\forall a \in A.(a, a) \in R$
- Simétrica: $\forall a, b \in A.(a, b) \in R \rightarrow (b, a) \in R$
- Transitiva: $\forall a, b, c \in A.((a, b) \in R \wedge (b, c) \in R) \rightarrow (a, c) \in R$

Ejemplo práctico: Personas y cumpleaños

$$P = \{p | p \text{ es una persona}\}$$

$C \subseteq P \times P$ tal que $(p_1, p_2) \in C$ ssi p_1 está de cumpleaños el mismo día que p_2

18.1. Particiones

Sea A un conjunto y $\mathcal{S} \subseteq 2^A$. Se dice que $\mathcal{S}$ es una partición de A si

- Todos los elementos de $\mathcal{S}$ son distintos de vacío: $\forall X \in \mathcal{S}.X \neq \emptyset$
- La unión de todos los elementos de $\mathcal{S}$ es igual a A: $\cup\mathcal{S} = A$
- Todos los elementos de $\mathcal{S}$ son distintos de a pares: $X, Y \in \mathcal{S}.X \neq Y \rightarrow X \cap Y = \emptyset$

18.2. Clases de equivalencia

Sea A un conjunto, $\simeq \subseteq A \times A$ una relación de equivalencia y $x \in A$. La clase de equivalencia de x según $\simeq$ corresponde a

$$[x]_{\simeq} = \{y \in A | x \simeq y\}$$

En palabras simples, $[x]_{\simeq}$ corresponde a todos los elementos presentes en A que son iguales a x.

18.2.1. Propiedades de las clases de equivalencia

- $\forall x \in A.x \in [x]_{\simeq}$
- $x \simeq z \leftrightarrow [x]_{\simeq} = [z]_{\simeq}$
- $x \not\simeq z \rightarrow [x]_{\simeq} \cap [z]_{\simeq} = \emptyset$

18.3. Conjunto cuociente

Se tiene A un conjunto y $\simeq \subseteq A \times A$ una relación de equivalencia. El conjunto cuociente de A, expresado como $A/\simeq$ significa

$$A/\simeq = \{x \in A\}$$

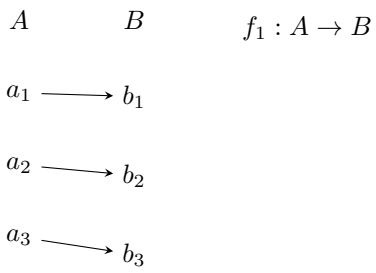
El conjunto cuociente de A corresponde a una partición de A.

19. Funciones

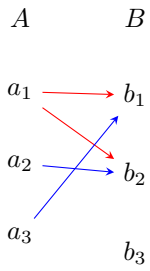
Las funciones son un tipo de relación. Más especificamente, $f \subseteq A \times B$ (con A y B conjuntos no vacios) es una función si es que

- $\forall a \in A.\exists b \in B.(a,b) \in f$ o que para todo elemento de A existe un elemento en B, tal que f los relacione.
- $\forall a \in A.\forall b_1, b_2 \in B.((a,b_1) \in f \wedge (a,b_2) \in f) \rightarrow b_1 = b_2$ o que todo elemento de A se relacione con solamente un elemento de B.

De forma más gráfica, una función se vería así

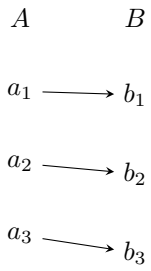


Por otro lado, estas cosas no serían funciones



$f_2 : A \to B$: Esto no es función, debido a que un elemento de A se relaciona con más de un elemento de B (También no relaciona todos los elementos de A)
$f_3 : A \to B$: Esto no es función, debido a que no todos los elementos de A se relacionan con algún elemento de B.
Una función siempre se puede ver como tabla, cosa que en la mayoría de casos hace que sea más facil

visualizarla y entenderla que los diagramas de antes. Por ejemplo, para la f_1 definida antes



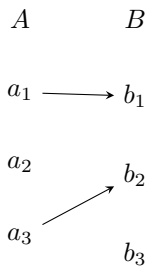
A	B
a_1	b_1
a_2	b_2
a_3	b_3

19.1. Función parcial

Una función parcial es similar a una función, sin embargo, podemos decir que es un poco más "permisiva", ya que a diferencia de la función, no exige que todos los elementos de A tengan relación con elementos de B. De manera más formal, $f \subseteq A \times B$ es una función parcial si

$$\forall a \in A. \forall b_1, b_2 \in B. ((a, b_1) \in f \wedge (a, b_2) \in f) \rightarrow b_1 = b_2$$

Un ejemplo sencillo de una función parcial que no es función



Todo elemento de A que se relaciona con un elemento de B, cumple con tener una unica relación, y no varias relaciones, como especificamos anteriormente. Sin embargo, hay un elemento de A que no se relaciona. Por esto, no es función, pero si es una función parcial.

19.2. Notación

Considerando $f \subseteq A \times B$, se usará la siguiente notación

$f : A \rightarrow B$	para f es una función de A a B.
$f : A \rightharpoonup B$	para f es una función parcial de A a B.
$f(a) = b$	para decir que $(a, b) \in f$.

19.3. Dominio e imagen de una función

$$\begin{array}{rrcccl} \text{Dominio:} & \text{dom}(f) & = & \pi_1(f) & = & \{a \in A | \exists b \in B. (a, b) \in f\} \\ \text{Imagen:} & \text{img}(f) & = & \pi_2(f) & = & \{b \in B | \exists a \in A. (a, b) \in f\} \end{array}$$

Proposición: Si se tiene una función parcial $f : A \rightharpoonup B$, entonces f será una función si $\text{dom}(f) = A$.

19.4. Tipos de funciones

Asumiendo una función $f : A \to B$, las funciones se clasifican como:

- Inyectiva: Una función es inyectiva si es que no existen dos elementos de A con la misma imagen.

$$\forall a_1, a_2 \in A. f(a_1) = f(a_2) \to a_1 = a_2$$

- Sobreyectiva: Una función es sobreyectiva si es que todo elemento de B tiene una preimagen.

$$\forall b \in B. \exists a \in A. (a, b) \in f$$

- Biyectiva: Inyectiva y sobreyectiva simultaneamente.

19.5. Función inversa, composición y caracterización

Similar a las relaciones, las funciones tienen una forma inversa y se puede componer.

- Función inversa: f^{-1} son todos los pares (a, b) tal que (b, a) existe en f.

$$f^{-1} = \{(a, b) | (b, a) \in f\}$$

- Composición de funciones: $f_1 \circ f_2$, con $f_1 : A \to B$ y $f_2 : B \to C$, son todos los elementos (a, c) tal que exista un c que permita crear un "puente" entre f_1 y f_2.

$$f_1 \circ f_2 = \{(a, c) | \exists b \in B. (a, b) \in f_1 \wedge (b, c) \in f_2\}$$

$$f_2(f_1(a)) = c$$

Esto nos entrega algunas propiedades interesantes. Si se tiene la función $f : A \to B$, entonces

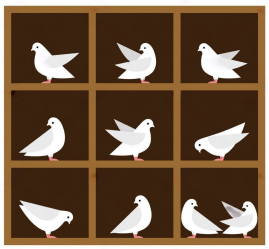
$$\begin{array}{rll} f \text{ es inyectiva} & \text{si, y solo si,} & f^{-1} \text{ es una función parcial.} \\ f \text{ es sobreyectiva} & \text{si, y solo si,} & \text{img}(f) = B. \\ f \text{ es biyectiva} & \text{si, y solo si,} & f^{-1} \text{ es una función.} \end{array}$$

$$\begin{array}{rl} \text{Si } f_1 \text{ y } f_2 \text{ son inyectivas,} & \text{entonces } f_1 \circ f_2 \text{ es inyectiva también.} \\ \text{Si } f_1 \text{ y } f_2 \text{ son sobreyectivas,} & \text{entonces } f_1 \circ f_2 \text{ es sobreyectiva también.} \end{array}$$

19.6. Principio del Palomar

"Si N palomas se distribuyen en M palomares, y tengo más palomas que palomares ($M > N$), entonces al menos habrá un palomar con más de una paloma."
Para las cosas con las que tendremos que lidiar en el curso, el principio del palomar dice que, considerando un $f : A \to B$ y $|B| < |A|$, entonces f **NO** es inyectiva.

$$\exists a_1, a_2 \in A. a_1 \neq a_2 \wedge f(a_1) = f(a_2)$$



20. Cardinalidad

Primero que nada, debemos recordar que el tamaño de un conjunto es definido como la cantidad de elementos presentes en el conjunto.

20.1. Equinumerosidad (Conjuntos equinumerosos)

Dos conjuntos A y B son equinumerosos si tienen la misma cantidad de elementos. Visto de otra forma, A y B son equinumerosos si es que existe una biyección $f : A \to B$. Si son equinumerosos, se denota como $|A| = |B|$.

20.2. Equinumerosidad como Relación de Equivalencia

La relación $|\cdot| = |\cdot|$ es una relación de equivalencia. Esto significa que es una relación refleja, simétrica y transitiva.
Entonces, para un conjunto A, se denotará su clase de equivalencia como $|A|$, según la relación $|\cdot| = |\cdot|$.

20.3. Cardinalidad de conjuntos finitos

Se dice que un conjunto es finito si es que existe un n tal que $|A| = |\{0, 1, 2, 3, \ldots, n-1\}|$. Cuando esto ocurre, se dice que su cardinalidad es n.

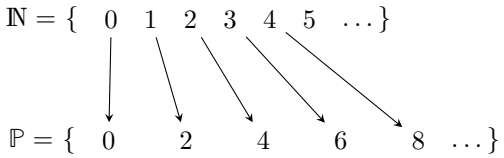
$$\exists n.|A| = |\{0, 1, 2, 3, \ldots, n-1\}| \to A \text{ es finito y } |A| = n$$

20.4. Cardinalidad de conjuntos infinitos

Hagamos un analisis de un ejemplo: Supongamos un conjunto $\mathbb{P}$ compuesto por todos los numeros pares

$$\mathbb{P} = \{0, 2, 4, 6, 8, \ldots\}$$

Este conjunto es infinito. Si lo pensamos, $\mathbb{N}$ (el conjunto de los naturales) también es infinito. ¿Tendrán $\mathbb{P}$ y $\mathbb{N}$ la misma cardinalidad? Nuestra definición de equinumerosidad nos será útil. Hay una biyección entre ambos conjuntos



Con la biyección $f : \mathbb{N} \to \mathbb{P}$, donde $f(n) = 2n$, se tiene que $|\mathbb{N}| = |\mathbb{P}|$

20.5. Conjuntos numerables

Se dice que un subconjunto A es numerable si tiene la misma cardinalidad que un subconjunto de $\mathbb{N}$. Más formalmente, un conjunto A es numerable si

$$\exists S \subseteq \mathbb{N}.|A| = |S|$$

También se puede decir que un conjunto A es numerable si y solo si existe una secuencia ordenada del tipo $a_1, a_2, a_3, \ldots$, en donde $\forall i \neq j.a_i \neq a_j$ y $\forall a \in A.\exists i \in \mathbb{N}.a = a_i$. En otras palabras, todos los elementos de la secuencia ordenada deben de ser diferentes entre si y todo elemento de la secuencia debe existir en A (y estar "indexado" con numeros naturales).
Destacar que **NO TODOS** los conjuntos son numerables. Por ejemplo, el conjunto $\mathbb{R}$ no es numerable.

20.6. Paradoja del Gran Hotel de Hilbert - Paradoja del Hotel Infinito

Esta paradoja fue enunciada por *David Hilbert (1862-1943)*, la cual habla de un hotel ficticio con una cantidad infinita de habitaciones, el cual se encuentra lleno. Llega un nuevo huésped al hotel y es su tarea entregarle una habitación. ¿Cómo puede asignarle una habitación? ¡Desplazando a cada uno de los huéspedes actuales a la habitación siguiente! El huésped de la habitación 1 se deberá ir a la habitación 2 y así.
Si está interesado en comprender mejor esta paradoja, aconsejo mirar este video de Veritasium[7] en donde se habla de algunas de las implicancias que tiene esta paradoja. Este video se encuentra en inglés, pero una versión en español[8] se encuentra disponible también.

[7]El link del video es: https://www.youtube.com/watch?v=OxGsU8oIWjY
[8]El link del video es: https://www.youtube.com/watch?v=4c8vG-mxuao

20.7. Teorema de Cantor

Teniendo un conjunto A no vacio, el Teorema de Cantor nos dice que no existe una biyección entre A y su conjunto potencia 2^A.
Para demostrar este teorema, *Georg Cantor (1845 - 1918)* creó una técnica la cual se conoce como el método de diagonalización de Cantor.[9]

20.8. ¿Hay algún infinito entremedio?

Se tiene la hipótesis siguiente
No existe ningún conjunto A tal que: $|\mathbb{N}| < |A| < |\mathbb{R}| \sim$ David Hilbert Actualmente no se ha logrado demostrar ni desmentir esta hipótesis, aunque cabe destacar que con los axiomas de teoria de conjuntos:

- 1940 - Kurt Gödel: No se puede demostrar que la hipótesis es falsa.
- 1963 - Paul Cohen: No se puede demostrar que la hipótesis es verdadera.

20.9. Solución a los problemas de decisión

Consideremos programas escritos en algunos lenguajes de programación, como *Python* o *C++*
Sea $\mathcal{I}$ un conjunto de inputs y $P : \mathcal{I} \to \{0, 1\}$ un problema de decisión.
Nos referimos a una solución `Program`, correspondiente a un programa computacional de Python o C++, el cual recibe inputs en $\mathcal{I}$ y retorna un output 0 o 1. Una solución `Program` es una solución a un problema de decisión P si para todo input $X \in \mathcal{I}$ se cumple que

$$P(X) = 1 \leftrightarrow \text{al ejecutar } \texttt{Program} \text{ con } X, \text{ este retorna 1}$$

Ejemplo: ¿Es este número primo?

$$\text{Primo} : \mathbb{N} \to \{0, 1\} \quad ; \quad \text{Primo}(n) = 1 \text{ si y solo si n es un número primo}$$

Se puede modelar el siguiente programa de Python para resolver el problema

```
def is_prime(n):
    if n % 2 == 0 and n > 2:
        return 0
    for i in range(3,n):
        if n % i == 0:
            return 0
    return 1
```

Recordemos que el codigo que vemos acá arriba corresponde a una abstracción solamente. El computador solamente entiende una secuencia de 1s y 0s, por lo que podemos representar todo programa computacional que es capaz de resolver un problema, usando solamente una palabra de ceros y unos. El conjunto de todas las palabras $\{0, 1\}^*$ es numerable, por lo que la cantidad de programas computacionales que son posibles también es numerable.
Ahora que sabemos que la cantidad de programas computacionales posibles es una cantidad numerable, *¿cuántos problemas de decisión existen?* Podemos decir que un problema de decisión se puede representar como una función $P : \{0, 1\}^* \to \{0, 1\}$. Se define $\mathcal{P}$ como el conjunto de todos los problemas de decisión, de forma que $\mathcal{P} = \{P : \{0, 1\}^* \to \{0, 1\}\}$. Se tiene que los conjuntos $\mathcal{P}$ y $2^{\{0,1\}^*}$ son equinumerosos, por lo que la cantidad de problemas de decisión no es numerable.
Es por esto que hay problemas de decisión los cuales no pueden ser modelados en un computador. Con esto, nos referimos a que hay problemas que no tienen algoritmo.

[9] Puede encontrar una demostración del Teorema de Cantor usando su método en el anexo de este resumen.

21. Notación Asintótica

Con $g : \mathbb{N} \to \mathbb{R}$ una función cualquiera, se pueden definir las siguientes notaciones...

21.1. Notación $\mathcal{O}$

El conjunto $\mathcal{O}(g)$ corresponde al conjunto de todas las funciones tales que

$$\exists c > 0. \exists n_0. \forall n \geq n_0. f(n) \leq c \cdot g(n)$$

En otras palabras, corresponde a todas las funciones tales que sean menores que $g(n)$ ponderado con un algún valor positivo, desde algún punto en adelante

21.1.1. Propiedades de la notación

1. $\forall a, b > 1. \log_a(n) \in \mathcal{O}(log_b(n))$
2. $\forall a < b \in \mathbb{N}. a^n \in \mathcal{O}(b^n) \wedge b^n \notin \mathcal{O}(a^n)$
3. $\forall a \in N. a^n \in \mathcal{O}(n!) \wedge n! \notin \mathcal{O}(a^n)$
4. $n! \in \mathcal{O}(2^{n \cdot \log(n)})$

21.1.2. Jerarquía de la notación

Notación	Nombre
$\mathcal{O}(1)$	Constante
$\mathcal{O}(\log(n))$	Logarítmico
$\mathcal{O}(n)$	Lineal
$\mathcal{O}(n \log(n))$	n log(n)
$\mathcal{O}(n^2)$	Cuadrático
$\mathcal{O}(n^3)$	Cúbico
$\mathcal{O}(n^m)$	Polinomial
$\mathcal{O}(k^n)$	Exponencial
$\mathcal{O}(n!)$	Factorial

21.2. Notación Ω

El conjunto $\Omega(g)$ corresponde al conjunto de todas las funciones tales que

$$\exists c > 0. \exists n_0. \forall n \geq n_0. f(n) \geq c \cdot g(n)$$

En palabras simples, es lo mismo que la notación $\mathcal{O}$, pero ahora, f debe ser mayor que g ponderado con un valor positivo.

21.3. Notación Θ

El conjunto $\Theta(g)$ corresponde al conjunto de todas las funciones tales que

$$\exists c_1, c_2 > 0. \exists n_0. \forall n \geq n_0. c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$$

En palabras simples, es la intersección entre $\mathcal{O}(g)$ y $\Omega(g)$.

22. Análisis de Algoritmos

22.1. ¿Qué es un algoritmo?

Un algoritmo corresponde a una secuencia finita de instrucciones para realizar una computación o resolver un problema. Los algoritmos se pueden dar en cualquier lenguaje o de cualquier forma, y estan presentes en un montón de lugares, incluso fuera de la matemática y la computación. (Por ejemplo: Una receta para cocinar brownies es un algoritmo.)
Cuando trabajamos con algoritmos, una cosa que nos interesa es saber la eficiencia de este. Hay muchos factores que pueden determinar que tan eficiente es nuestro algoritmo, pero el que estudiaremos aquí es el tiempo.

22.2. Eficiencia de un algoritmo con respecto al tiempo

Para un algoritmo A sobre un conjunto de inputs $\mathcal{I}$ se define la función

$$\text{tiempo}_A(I) : \mathcal{I} \to \mathbb{N} \quad ; \quad \text{tiempo}_A(I) = \text{Número de pasos realizados por } A \text{ con input } I$$

Considerando que ahora tenemos una función que nos dice cuanto tiempo se demora un algoritmo en resolver un problema, podemos definir un poco más a la eficiencia. Decimos que un algoritmo A es el más eficiente si se cumple que para todo algoritmo B que realiza el mismo cómputo o resuelve el mismo problema, logra cumplir que

$$\forall I \in \mathcal{I} \ . \ \text{tiempo}_A(I) \leq \text{tiempo}_B(I)$$

Destacar que esta definición no esta exenta de problemas, principalmente por el hecho de que no hemos definido como se puede medir el tiempo. El tiempo que demora un algoritmo puede verse definido por muchas cosas, como la cantidad de pasos a resolver y que tan complejo puede llegar a ser cada paso del algoritmo. Por ahora, para poder simplificar las cosas, para nosotros el tiempo va a consistir en la cantidad de pasos que tiene el algoritmo para lograr resolver un problema.

22.3. Uso de notación asintótica en algoritmos

La notación asintótica nos puede resultar útil para definir el tiempo de un algoritmo.
Por ejemplo, considere el siguiente algoritmo matemático escrito en Python.

```
for i in range(1, n):
    for j in range(1, i):
        x = x + 1
```

¿Cuántas veces se ejecuta la linea `x = x + 1` al cambiar `n`?
Analizando lo que ocurre en este código, el loop `for j in range(1, i)` es ejecutado `i` veces. Este se encuentra inmerso en un loop `for i in range(1, n)`, lo que significa que en la primera iteración se ejecutará 1 vez, en la siguiente 2 veces, en la siguiente 3 veces y así, hasta llegar a la iteración numero `n`, en donde se ejecutará `n` veces. Sumando todo...

$$\text{Tiempo}_{\text{for\_loop}}(n) = 1 + 2 + 3 + \ldots + n - 1 + n = \frac{n \cdot (n+1)}{2}$$

Resulta que

$$\frac{n \cdot (n+1)}{2} \in \Theta(n^2)$$

Entonces, la cantidad de veces que se ejecuta `x = x + 1` es $\Theta(n^2)$

22.4. Tamaño del input

Para un conjunto de inputs $\mathcal{I}$, se define su función tamaño como

$$|\cdot| : \mathcal{I} \to \mathbb{N} \quad ; \quad |I| = \text{Tamaño de } I \text{ según su representación}$$

Ejemplo: Para una palabra de bits $w \in \{0,1\}^*$; $|w|$ = largo de la palabra w o número de bits.

La definición más general que tenemos de $|I|$ es

$$|I| = \text{Número de bits de una codificación "razonable" de } I$$

22.5. Tipos de complejidad

Para todo algoritmo A y su conjunto de inputs I se puede tener un mejor caso y un peor caso.

$$\text{peor-caso}_A(n) = \max_{I \in \mathcal{I}}\{\text{tiempo}_A(I) \mid |I| = n\} \quad ; \quad \text{mejor-caso}_A(n) = \min_{I \in \mathcal{I}}\{\text{tiempo}_A(I) \mid |I| = n\}$$

23. Principio de Inducción

23.1. Principio de inducción simple

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

- $P(0)$, $P(1)$, ..., $P(k)$ son verdaderos
- Para todo $n \in \mathbb{N}$, si $P(n)$ es verdadero, entonces $P(n+1)$ también es verdadero.

entonces, para todo $n \in \mathbb{N}$ se tiene que $P(n)$ debe ser verdadero.
En lógica de predicados, esto se expresa como (forma general)

$$(\underbrace{P(0) \wedge P(1) \wedge P(2) \ldots \wedge P(k)}_{\text{Caso(s) base}} \wedge \underbrace{(\forall n \geq k . P(n) \to P(n+1))}_{\text{Hipótesis}}) \to \forall n \; . \; P(n)$$

23.1.1. Caso base único

$$(\; P(0) \wedge (\forall n \geq k . P(n) \to P(n+1)) \;) \to \forall n \; . \; P(n)$$

23.1.2. Caso base extendido

$$(\; P(k) \wedge (\forall n \geq k . P(n) \to P(n+1)) \;) \to \forall n \geq k \; . \; P(n)$$

23.2. Principio de inducción fuerte

Para una afirmación $P(n)$ sobre los naturales, si $P(n)$ cumple que para todo $n \in \mathbb{N}$

$$\text{Si } P(k) \text{ es verdadero para todo } k < n, \text{ entonces } P(n) \text{ es verdadero}$$

Entonces, para todo $n \in \mathbb{N}$ se tiene que $P(n)$ es verdadero.
En lógica de predicados, esto se ve como

$$(\; \forall n \; . \; (\forall k < n \; . \; P(k)) \to P(n) \;) \to \forall n . P(n)$$

23.3. Axiomas de $\mathbb{N}$ - Axiomas de Peano

1. El número $0 \in \mathbb{N}$
2. Si $n \in \mathbb{N}$, entonces $(n+1) \in \mathbb{N}$ donde $n+1$ es sucesor de n.
3. Todo $n \in \mathbb{N}$, a excepción de $n \neq 0$, tiene un antecesor en $\mathbb{N}$
4. Principio del Buen Orden: Todo subconjunto $A \subseteq \mathbb{N}$ tiene un elemento mínimo.

24. Definiciones Recursivas

Una definición recursiva consiste en una definición que cuenta con las siguientes caracteristicas

- Casos base sencillos
- Reglas que reducen la definición a casos anteriores (en otras palabras, una definición que se basa en el caso anterior para explicar el siguiente).

24.1. Definición recursiva de conjuntos

La definición recursiva de un conjunto $\mathbb{S}$ consiste en:

- Un conjunto de base tal que cada elemento del conjunto pertenece a $\mathbb{S}$.

$$B = \{b_1, b_2, \ldots, b_n\} \quad ; \quad \forall i < n \; . \; b_i \in \mathbb{S}$$

- Reglas recursivas R, donde mediante elementos que ya se sabe y se ha demostrado que existen dentro del conjunto, se puede demostrar que un nuevo elemento existe dentro del conjunto también.

$$s_1, s_2, \ldots, s_m \in \mathbb{S} \rightarrow R(s_1, s_2, \ldots, s_m) \in \mathbb{S}$$

- Una afirmación de exclusión, la cual se encarga de unir el conjunto base y las reglas recursivas definidas[10].

"El conjunto $\mathbb{S}$ son todos los elementos que se construyen solamente a partir de B y las reglas R"

24.2. Funciones sobre conjuntos definidos recursivamente

Se pueden definir funciones sobre conjuntos definidos de forma recursiva. Estas funciones generalmente quedarán en una forma recursiva también.
Ejemplo: Se define un conjunto Σ^* de la siguiente forma, considerando Σ un alfabeto

- $\epsilon \in \Sigma^*$ (definición de la palabra vacía)
- Si $w \in \Sigma^*$, entonces para todo $a \in \Sigma$ se tiene que $wa \in \Sigma^*$.

Ahora se define una función $f : \Sigma^* \rightarrow \mathbb{N}$ que obtiene el largo de una palabra de Σ^*

$$\begin{array}{rcl} f(\epsilon) & = & 0 \\ f(wa) & = & f(w) + 1 \quad \text{para } w \in \Sigma^* \text{ y } a \in \Sigma \end{array}$$

[10]Destacar que esto por lo general se omite y se asume que es de la forma mostrada debajo

24.3. Inducción estructural

La inducción estructural es practicamente una inducción pensada para demostrar una definición recursiva. Al igual que antes, se comienza con los casos base, para luego extrapolar mediante la regla recursiva de la definición a demostrar.
Ahora, de una forma más formal, se tiene un conjunto definido recusivamente $\mathbb{S}$, definido con un conjunto base B y reglas recursivas R. Se define la capa $\mathbb{S}[n]$ de $\mathbb{S}$ para todo $n \geq 0$ como:

$$\begin{aligned} \mathbb{S}[0] &= B \\ \mathbb{S}[n+1] &= \mathbb{S}[n] \cup \{T(s_1, \ldots, s_k) | T \in R \wedge s_1, \ldots, s_n \in \mathbb{S}[n]\} \end{aligned}$$

Entonces, el principio de inducción estructural dice que para todo predicado $P(\cdot)$ sobre $\mathbb{S}$, este es siempre verdadero si:

$$[(\forall s \in \mathbb{S}[0] \,.\, P(s)) \wedge \forall n \,.\, (\forall s \in \mathbb{S}[n] \,.\, P(s)) \rightarrow (\forall s' \in \mathbb{S}[n+1] \,.\, P(s'))] \rightarrow \forall s \in \mathbb{S} \,.\, P(s)$$

25. Teoría de Números

25.1. División

Considerando a $\mathbb{Z}$ como el conjunto de los números enteros, para $a, b \in \mathbb{Z}$ y $a \neq 0$, se dice que a divide a b si es que:

$$a|b \leftrightarrow \exists q \in \mathbb{Z} \,.\, a \cdot q = b$$

En el caso que esto no se cumpla, entonces a no divide b, expresado como $a \nmid b$

25.1.1. Propiedades de la división

- Si $a|b$ y $a|c$, entonces $a|(b+c)$
- Si $a|b$, entonces $a|(b \cdot c)$ para todo $c \in \mathbb{Z}$
- Si $a|b$ y $b|c$, entonces $a|c$

Corolario: Si $a|b$ y $b|c$, entonces $a|(b \cdot m + n \cdot c)$, para todo $m, n \in \mathbb{Z}$

25.2. Módulo

Con $a, b \in \mathbb{Z}$, $a > 0$ y $a|b$, entonces existe un único par $q, r \in \mathbb{Z}$ tal que $a \cdot q + r = b$. Esta corresponde a la definición de la división con resto. Mediante esta, se define el operador módulo ($\mod$) y el operador división (div).

$$\begin{aligned} b \text{ div } a &= q \\ b \mod a &= r \end{aligned}$$

25.3. Congruencia modular

Con $m \in \mathbb{Z}$ y $m > 0$, diremos que para todo $a, b \in \mathbb{Z}$, a es congruente con $b \mod m$ si:

$$a \equiv b(\mod m) \quad \text{si, y solo si} \quad m|(a-b)$$

25.3.1. Propiedades de la congruencia modular

Para todo $a, b, m \in \mathbb{Z}$, donde $m > 0$, se cumple que:

- $a \equiv b(\mod m)$
- $a = b + m \cdot s$, para algún $s \in \mathbb{Z}$
- $(a \mod m) = (b \mod m)$

25.3.2. Suma y multiplicación de la congruencia modular

Para todo $m > 0$, si $a \equiv b(\mod m)$ y $c \equiv d(\mod m)$ entonces:

$$\begin{aligned} a + c &\equiv b + d(\mod m) \\ a \cdot c &\equiv b \cdot d(\mod m) \end{aligned}$$

Adicionalmente...

$$\begin{aligned} (a+b) \mod m &= ((a \mod m) + (b \mod m)) \mod m \\ (a \cdot b) \mod m &= ((a \mod m) \cdot (b \mod m)) \mod m \end{aligned}$$

25.3.3. Aritmética módulo m - Aritmética modular

Con $m > 0$, se define $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Entonces, para todo $a, b \in \mathbb{Z}_m$, se definen las operaciones $+_m$ y $\cdot_m$

$$\begin{aligned} a +_m b &= (a + b) \mod m \\ a \cdot_m b &= (a \cdot b) \mod m \end{aligned}$$

La aritmética modular cumple con las siguientes propiedades:

$$\begin{aligned} \text{Clausura:} \quad & a +_m b \in \mathbb{Z}_m \quad ; \quad a \cdot_m b \in \mathbb{Z}_m \\ \text{Conmutatividad} \quad & a +_m b = b +_m a \quad ; \quad a \cdot_m b = b \cdot_m a \\ \text{Asociatividad} \quad & a +_m (b +_m c) = (a +_m b) +_m c \quad ; \quad a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c \\ \text{Identidad:} \quad & a +_m 0 = a \quad ; \quad a \cdot_m 1 = a \\ \text{Inverso aditivo:} \quad & a \neq 0,\ \exists a' \in \mathbb{Z}_m \ .\ a +_m a' = 0 \\ \text{Distributividad:} \quad & a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c) \end{aligned}$$

25.4. Representación de los números

Sea $b > 1$. Si $n \in \mathbb{N} - \{0\}$, entonces n se puede escribir de forma única como:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + a_{k-3}b^{k-3} + \ldots + a_2b^2 + a_1b^1 + a_0 = \sum_{i=0}^{k-1} a_i b^i$$

con

- $k \geq 1$
- Para todo $i < k$, $a_i < b$
- $a_{k-1} \neq 0$

Para poder simplificar un poco las cosas, vamos a establecer que todo número en representación de n en base b corresponde a la secuencia

$$(n)_b = a_{k-1} \ldots a_2 a_1 a_0$$

Como pequeño dato curioso, si esto le parece familiar al lector, es porque esto representa la forma en que nosotros escribimos los números normalmente, en donde la base $b = 10$.

25.4.1. Encontrando la representación de n en base b

Ahora que entendemos que podemos representar números usando distintas bases, ¿cómo podemos encontrar la representación de cualquier número en cualquier base?

Si se tiene un número $n \in \mathbb{N} - \{0\}$ y $b > 0$, sabiendo que su representación debe ser de la forma $(n)_b = a_{k-1} \ldots a_2 a_1 a_0$ y que por la división con resto, sabemos que $n = q \cdot b + r$, entonces tenemos que

$$\begin{aligned} r &= a_0 \\ (q)_b &= a_{k-1} \ldots a_1 \end{aligned}$$

25.4.2. Suma de números en base b

La forma de llegar al algoritmo para la suma de números en base b corresponde al siguiente, considerando que n y m son números en base b.

$$\begin{array}{lcll} n+m & = & (n_{k-1}+m_{k-1})\cdot b^{k-1}+\ldots+(n_2+m_2)\cdot b^2+(n_1+m_1)\cdot b+(n_0+m_0) & /(n_0+m_0)=c_0\cdot b+s_0 \\ n+m & = & (n_{k-1}+m_{k-1})\cdot b^{k-1}+\ldots+(n_2+m_2)\cdot b^2+(n_1+m_1+c_0)\cdot b+s_0 & /(n_1+m_1+c_0)=c_1\cdot b+s_1 \\ n+m & = & (n_{k-1}+m_{k-1})\cdot b^{k-1}+\ldots+(n_2+m_2+c_1)\cdot b^2+s_1\cdot b+s_0 & /(n_2+m_2+c_1)=c_2\cdot b+s_2 \\ & & & /\ \ldots \end{array}$$

Si se continua aplicando hasta terminar con toda la ecuación, se obtiene que

$$n+m=c_{k-1}\cdot b^k+s_{k-1}\cdot b^{k-1}+\ldots+s_1\cdot b+s_0$$

Estas son muchas letras y posiblemente confunde demasiado, por lo que es mejor trabajar con un ejemplo de como se usa este algoritmo. Supongamos que queremos realizar la suma $(11)_2+(14)_2$, donde $(11)_2=1011$ y $(14)_2=1110$.

$$\begin{array}{rrcll} \text{Se comienza con el primer dígito } (101\mathbf{1};\ 111\mathbf{0}): & 1+0 & = & 0\cdot 2+1 & \text{Resultado: } 1 \\ \text{Se continua con el segundo dígito } (10\mathbf{1}1;\ 11\mathbf{1}0): & 1+1+0 & = & 1\cdot 2+0 & \text{Resultado: } 01 \\ \text{Se continua con el tercer dígito } (1\mathbf{0}11;\ 1\mathbf{1}10): & 0+1+1 & = & 1\cdot 2+0 & \text{Resultado: } 001 \\ \text{Se continua con el cuarto dígito } (\mathbf{1}011;\ \mathbf{1}110): & 1+1+1 & = & 1\cdot 2+1 & \text{Resultado: } 1001 \\ \text{Siguiente dígito de la base (5° dígito acumulado):} & 0+0+1 & = & 0\cdot 2+1 & \text{Resultado: } 11001 \end{array}$$

Entonces, $(11)_2+(14)_2=11001$.
Este algoritmo es exactamente lo que se usa para realizar sumas de forma manual en base 10.

25.4.3. Multiplicación de números en base b

Considerando que n y m son números en base b, la multiplicación $m\cdot n$

$$n\cdot m=n(m_{k-1}b^{k-1}+\ldots+m_2b^2+m_1b+m_0)=n\cdot(m_{k-1}b^{k-1})+\ldots+n\cdot(m_2b^2)+n\cdot(m_1b)+n\cdot(m_0)$$

Considerando esto, se define p_i como

$$(p_i)_b=n\cdot(m_i\cdot b)=\begin{cases}0 & \text{si } m_i=0\\ n_{k-1}\ldots n_1n_00\ldots0 & \text{si } m_i=1.\text{ La cantidad de ceros es } i\end{cases}$$

25.5. Máximo común divisor

Sea $a,b\in\mathbb{Z}-\{0\}$. El máximo común divisor de a y b (o $\gcd(a,b)$) corresponde al mayor número d tal que $d|a$ y $d|b$, simultaneamente. El $\gcd(a,b)$ podemos decir, en otras palabras, que corresponde al máximo del conjunto $D_{a,b}$, definido como

$$D_{a,b}=\{c\in\mathbb{Z}\mid c|a\wedge c|b\}$$

25.5.1. Algoritmo del MCD - Algoritmo de Euclides[11]

Para obtener el $\gcd(a,b)$, se puede usar el algoritmo de Euclides, el cual permite descomponer el problema en un problema más pequeño.

$$\begin{array}{rl} \gcd(a,b) & /a=b\cdot q+r \\ \gcd(a,b)=\gcd(b,r) & /\text{Repetir de forma iterativa hasta poder determinar el MCD.} \end{array}$$

[11] Información obtenida desde KhanAcademy

25.6. Conjunto Generadores

Con $a, b \in \mathbb{Z} - \{0\}$, se define el conjunto generador de a y b ($\langle a, b \rangle$) como

$$\langle a, b \rangle = \{c \in \mathbb{Z} \mid \exists s, t \in \mathbb{Z} \ . \ c = a \cdot s + b \cdot t\}$$

De forma más general, el conjunto generado por $a_1, \ldots, a_n$ se define como

$$\langle a_1, \ldots, a_n \rangle = \{c \in \mathbb{Z} \mid \exists s_1, s_2, \ldots, s_n \in \mathbb{Z} \ . \ c = a_1 s_1 + a_2 s_2 + \ldots + a_n s_n\}$$

25.6.1. Identidad de Bézout

Para todo $a, b \in \mathbb{Z} - \{0\}$

- $\gcd(a, b)$ es el menor entero positivo tal que existe $s, t \in \mathbb{Z}$: $\gcd(a, b) = sa + tb$
- $\langle a, b \rangle = \langle \gcd(a, b) \rangle$

25.7. Ecuaciones de Congruencias

Esto sirve como una especie de "continuación" a la congruencia modular.
Se define una congruencia lineal como la ecuación de la siguiente forma

$$ax \equiv b(\mod m) \quad ; \quad m \in \mathbb{N} - \{0\};\ a, b \in \mathbb{Z};\ x \text{ variable}$$

25.7.1. Como resolver una ecuación de congruencia lineal

Para poder resolver $ax \equiv b(\mod m)$, se debe encontrar el inverso multiplicativo de a, o sea, a^{-1} (No necesariamente $a^{-1} = {}^1/_a$), de forma que

$$a \cdot a^{-1} \equiv b(\mod m)$$

Asumiendo que a^{-1} existe, significa que podemos resolver la ecuación de la siguiente forma

$$\begin{array}{rcll} ax & \equiv & b(\mod m) & /\cdot a^{-1} \\ (a \cdot a^{-1})x & \equiv & a^{-1}b(\mod m) & /a \cdot a^{-1} = 1 \\ x & \equiv & a^{-1}b(\mod m) & \end{array}$$

26. Anexo

26.1. 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.)

26.2. Demostración - Mínimo único

Si S tiene un elemento mínimo, entonces dicho elemento es único.
Sea $x_1^{\downarrow} \in S$ y $x_2^{\downarrow} \in S$ ambos mínimos y $x_1 \neq x_2$. ¿Es esto posible?
Mediante la definición de mínimo, llegamos a que

$$\forall y \in S.x_1^{\downarrow} \preceq y \quad ; \quad \forall y \in S.x_2^{\downarrow} \preceq y$$

Esto nos lleva a que

$$\left.\begin{array}{l} x_1^{\downarrow} \preceq x_2^{\downarrow} \\ x_2^{\downarrow} \preceq x_1^{\downarrow} \end{array}\right\} x_1^{\downarrow} = x_2^{\downarrow}$$

Así, queda demostrado que el mínimo debe ser único.

26.3. Demostración - Si es mínimo, es minimal

Si x es mínimo, entonces x es minimal

Sea $x^{\downarrow}$ un mínimo

Para realizar la demostración, se debe demostrar que $\forall z \in S. z \preceq x^{\downarrow} \rightarrow z = x$

Suponga que $z \preceq x^{\downarrow}$. Por definición de mínimo, se tiene que $x^{\downarrow} \preceq z$. Entonces, considerando toda la información, se llega a que

$$\left.\begin{array}{l} z \preceq x^{\downarrow} \\ x^{\downarrow} \preceq z \end{array}\right\} z = x^{\downarrow}$$

26.4. Demostración - Teorema de Cantor

Por demostrar: No existe biyección entre A y $2^A = \{S | S \subseteq A\}$

Para ayudar a que sea más sencillo entender la demostración, se puede demostrar primero que no existe biyección entre $\mathbb{N}$ y $2^{\mathbb{N}}$, para después extrapolarlo a cualquier conjunto A.

Por demostrar: No existe biyección entre $\mathbb{N}$ y $2^{\mathbb{N}} = \{S | S \subseteq \mathbb{N}\}$

Para comenzar la demostración, se supone que si existe una biyección $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$

	0	1	2	3	4	...
$f(0)$	1	1	0	1	0	...
$f(1)$	0	0	1	1	1	...
$f(2)$	1	1	1	1	0	...
$f(3)$	1	0	1	0	0	...
$f(4)$	0	0	1	1	0	...
...			...			

Aquí, la coordenada (i, j) es 1 si y solo si $j \in f(i)$. Si consideramos todos los elementos de la diagonal y los colocamos en un conjunto D...

	0	1	2	3	4	...
$f(0)$	1	1	0	1	0	...
$f(1)$	0	0	1	1	1	...
$f(2)$	1	1	1	1	0	...
$f(3)$	1	0	1	0	0	...
$f(4)$	0	0	1	1	0	...
...			...			

$$D = \{i \in \mathbb{N} | i \in f(i)\} \in 2^{\mathbb{N}} = \{0, 2, \ldots\}$$

Si pensamos en el complemento de D, llamese, el conjunto de elementos que no se encuentran contenidos en el conjunto D, obtenemos

$$\bar{D} = \{i \in \mathbb{N} | i \notin f(i)\} \in 2^{\mathbb{N}} = \{1, 3, 4, \ldots\}$$

Por la naturaleza de $\bar{D}$, no hay ninguna $f(x)$ para todo x, debido a que para que $x \in f(x)$, se debe cumplir que $x \notin \bar{D}$. Con esto se llega a que no existe una biyección entre $\mathbb{N}$ y $2^{\mathbb{N}}$.

Este mismo argumento se puede extrapolar a cualquier conjunto A, ya que el motivo por el que ocurre esto no esta relacionado con el conjunto en si, si no por la forma en la que funciona el conjunto potencia.

Si se mantiene escéptico, considere

$$\bar{D} = \{a \in A | a \notin f(a)\}$$

Ahora considere un $x^* \in A$, tal que $f(x^*) = \bar{D}$

- $x^* \in f(x^*) \Rightarrow x^* \in \bar{D} \Rightarrow x^* \notin f(x^*)$
- $x^* \notin f(x^*) \Rightarrow x^* \in \bar{D} \Rightarrow x^* \in f(x^*)$

Llegamos a una contradicción, lo que significa que dicho x^* no puede existir, llegando a que no existe una biyección.

26.5. Algoritmo de la suma de números en base b