UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

DEPARTAMENTO DE INFORMÁTICA

Estructuras Discretas - Técnicas de Demostración

Versión 220223

Capítulos

Inferencia

Teoremas

Definición: teorema

Una expresión que se ha demostrado como verdadera con respecto a axiomas, teoremas existentes.

¿Cómo se demuestra un teorema?

Teoremas

Definición: teorema

Una expresión que se ha demostrado como verdadera con respecto a axiomas, teoremas existentes.

¿Comó se demuestra un teorema?

- Debemos construir un argumento lógico (una *demostración*)
- Queremos demostrar que si las hipótesis del teorema se cumplen . . .
- . . . entonces podemos deducir la conclusión del teorema.

Para construir un demostración, primero tenemos que saber como derivar nuevas expresiones a partir de las conocidas – estas son las reglas de inferencia.

Reglas de Inferencia

Son reglas que justifican los pasos de una demostración:

- Estas reglas se derivan de tautologías básicas de la forma "$A \Rightarrow B$"
- Esto es porque si asumimos que A es **V**, entonces el único caso en que $A \Rightarrow B$ es **V** es cuando B también es **V**

$$
\begin{array}{c}
p \\
q \\
\hline
p \wedge q
\end{array}
\qquad
\begin{array}{l}
\longleftarrow \text{hipótesis} \\
\\
\longleftarrow \text{conclusión}
\end{array}
$$

Significado: Si p es **V**, y además q es **V**, entonces podemos inferir que $p \wedge q$ es **V**

Tautología: $p \wedge q \Rightarrow p \wedge q$

Ejemplo:

- Hipótesis:
  - Hoy comí tostadas (p)
  - Hoy tomé café (q)
- Conclusión:

$$\begin{array}{c} p \\ q \\ \hline p \wedge q \end{array} \qquad \begin{array}{l} \longleftarrow \text{hipótesis} \\ \\ \longleftarrow \text{conclusión} \end{array}$$

Significado: Si p es **V**, y además q es **V**, entonces podemos inferir que $p \wedge q$ es **V**

Tautología: $p \wedge q \Rightarrow p \wedge q$

Ejemplo:

- Hipótesis:
  - Hoy comí tostadas (p)
  - Hoy tomé café (q)
- Conclusión: hoy comí tostadas y tomé café ($p \wedge q$)

$$\frac{p \wedge q}{p}$$

Significado: Si $p \wedge q$ es **V**, podemos inferir que p debe ser **V** (y lo mismo para q)

Tautología: $p \wedge q \Rightarrow p$

Ejemplo:

- Hipótesis: Tome café y tome té $(p \wedge q)$
- Conclusión:

$$\frac{p \wedge q}{p}$$

Significado: Si $p \wedge q$ es **V**, podemos inferir que p debe ser **V** (y lo mismo para q)

Tautología: $p \wedge q \Rightarrow p$

Ejemplo:

- Hipótesis: Tome café y tome té ($p \wedge q$)
- Conclusión: tome café (p)

$$\frac{p}{p \vee q}$$

Significado: Si p es **V**, podemos inferir que $p \vee q$ debe ser **V** (q puede ser cualquier cosa)

Tautología: $p \Rightarrow p \vee q$

Ejemplo:

- Hipótesis: Le eché leche a mi café (p)
- Conclusión:

$$\frac{p}{p \vee q}$$

Significado: Si p es **V**, podemos inferir que $p \vee q$ debe ser **V** (q puede ser cualquier cosa)

Tautología: $p \Rightarrow p \vee q$

Ejemplo:

- Hipótesis: Le eché leche a mi café (p)
- Conclusión: hay leche o azúcar en mi café ($p \vee q$)

Reglas de Inferencia
Modus Ponens

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline q \end{array}$$

Significado: Si tanto la implicancia ($p \Rightarrow q$) como su antecedente (p) son **V**, entonces la conclusión de la implicancia (q) tiene que ser **V**

Tautología: $(p \wedge (p \Rightarrow q)) \Rightarrow q$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces vamos a la playa ($p \Rightarrow q$)
  - Hoy hay sol (p)
- Conclusión:

Reglas de Inferencia
Modus Ponens

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline q \end{array}$$

Significado: Si tanto la implicancia ($p \Rightarrow q$) como su antecedente (p) son **V**, entonces la conclusión de la implicancia (q) tiene que ser **V**

Tautología: $(p \wedge (p \Rightarrow q)) \Rightarrow q$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces vamos a la playa ($p \Rightarrow q$)
  - Hoy hay sol (p)
- Conclusión: vamos a la playa (q)

$$\begin{array}{c} \neg q \\ p \Rightarrow q \\ \hline \neg p \end{array}$$

Significado: Similar a Modus Ponens, pero con respecto a la contrarecíproca (recordar que $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$)

Tautología: $(\neg q \wedge (p \Rightarrow q)) \Rightarrow \neg p$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces vamos a la playa ($p \Rightarrow q$)
  - Hoy no fuimos a la playa ($\neg q$)
- Conclusión:

$$\begin{array}{c} \neg q \\ p \Rightarrow q \\ \hline \neg p \end{array}$$

Significado: Similar a Modus Ponens, pero con respecto a la contrarecíproca (recordar que $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$)

Tautología: $(\neg q \wedge (p \Rightarrow q)) \Rightarrow \neg p$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces vamos a la playa ($p \Rightarrow q$)
  - Hoy no fuimos a la playa ($\neg q$)
- Conclusión: hoy no hizo sol ($\neg p$)

Reglas de Inferencia
Silogismo Hipotético

$$\begin{array}{c} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$$

Significado: la implicancia es transitiva

Tautología: $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces haremos un asado ($p \Rightarrow q$)
  - Si hacemos un asado hoy, entonces hay que ir al supermercado ($q \Rightarrow r$)
- Conclusión:

$$\begin{array}{c} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$$

Significado: la implicancia es transitiva

Tautología: $[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$

Ejemplo:

- Hipótesis:
  - Si hoy hay sol, entonces haremos un asado ($p \Rightarrow q$)
  - Si hacemos un asado hoy, entonces hay que ir al supermercado ($q \Rightarrow r$)
- Conclusión: si hoy hay sol, entonces hay que ir al supermercado ($p \Rightarrow r$)

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}$$

Significado: Similar a Modus Ponens, dado que $p \vee q \equiv \neg p \Rightarrow q$

Tautología: $[(p \vee q) \wedge \neg p] \Rightarrow q$

Ejemplo:

- Hipótesis:
  - Le eché azúcar o leche a mi café $(p \vee q)$
  - No le eché azúcar a mi café $(\neg p)$
- Conclusión:

$$\begin{array}{l} p \vee q \\ \underline{\neg p \quad\quad} \\ q \end{array}$$

Significado: Similar a Modus Ponens, dado que $p \vee q \equiv \neg p \Rightarrow q$

Tautología: $[(p \vee q) \wedge \neg p] \Rightarrow q$

Ejemplo:

- Hipótesis:
  - Le eché azúcar o leche a mi café ($p \vee q$)
  - No le eché azúcar a mi café ($\neg p$)
- Conclusión: le eché leche a mi café (q)

$$\begin{array}{l} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$$

Significado:

- Si p es **V**, entonces r tiene que ser **V** ... y si p es **F**, entonces q tiene que ser **V**
- Entonces, para que ambas hipótesis sean verdadera, no importa el valor de p, lo que necesitamos es que q o r sean **V**

Tautología: $[(p \vee q) \wedge (\neg p \vee r)] \Rightarrow (q \vee r)$

Ejemplo:

- Hipótesis:
  - Hace calor o Pedro juega fútbol $(p \vee q)$
  - No hace calor o Juan esta en la playa $(\neg p \vee r)$
- Conclusión:

$$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline q \vee r \end{array}$$

Significado:

- Si p es **V**, entonces r tiene que ser **V** . . . y si p es **F**, entonces q tiene que ser **V**
- Entonces, para que ambas hipótesis sean verdadera, no importa el valor de p, lo que necesitamos es que q o r sean **V**

Tautología: $[(p \vee q) \wedge (\neg p \vee r)] \Rightarrow (q \vee r)$

Ejemplo:

- Hipótesis:
  - Hace calor o Pedro juega fútbol $(p \vee q)$
  - No hace calor o Juan esta en la playa $(\neg p \vee r)$
- Conclusión: Pedro juega fútbol o Juan esta en la playa $(q \vee r)$

Ejemplo

Demuestre que el siguiente argumento lógico es válido:

$$\begin{array}{l} \neg p \wedge q \\ r \Rightarrow p \\ \neg r \Rightarrow s \\ s \Rightarrow t \\ \hline t \end{array}$$

En otras palabras, deben mostrar que es posible deducir la conclusión de las hipótesis, usando las reglas de inferencia.

Ejemplo

Demuestre que el siguiente argumento lógico es válido:

$$\begin{array}{l} \neg p \wedge q \\ r \Rightarrow p \\ \neg r \Rightarrow s \\ s \Rightarrow t \\ \hline t \end{array}$$

En otras palabras, deben mostrar que es posible deducir la conclusión de las hipótesis, usando las reglas de inferencia.

Solución:

1.	$\neg p \wedge q$	hipótesis	5.	$\neg r \Rightarrow s$	hipótesis
2.	$\neg p$	simplificación (linea 1)	6.	s	m. ponens (lineas 4, 5)
3.	$r \Rightarrow p$	hipótesis	7.	$s \Rightarrow t$	hipótesis
4.	$\neg r$	m. tollens (lineas 2, 3)	8.	t	m. ponens (lineas 6, 7)

$\therefore$ El argumento es correcto.

$$\frac{\forall x P(x)}{P(c)}$$

Significado: Si $P(x)$ es **V** para todo x, entonces $P(c)$ es **V**, donde c es un valor particular de x

Ejemplo:

- Hipótesis: Todos los cursos en la UTFSM son difíciles ($\forall x P(x)$)
- Conclusión: INF-152 es difícil ($P(c)$)

$$\frac{P(c) \text{ para } c \text{ arbitrario}}{\forall x P(x)}$$

Significado: Si podemos demostrar que $P(c)$ es **V**, donde c es un elemento arbitrario, entonces $P(x)$ es **V**, $\forall x$

Esta regla usualmente se aplica de la siguiente forma:

1. Definir un elemento arbitrario c
2. Demostrar que $P(c)$ es **V**. Como el elemento c es arbitrario, no pueden usar propiedades de c para demostrar que $P(c)$ es **V**
3. Como c representa a cualquier elemento, podemos concluir que $\forall x P(x)$ es **V**

Ejemplo:

Si $P(x) : x > x - 1$, ¿cuál de los dos argumentos lógicos es correcto?

$$\frac{P(3)}{\forall x\, P(x)} \qquad\qquad \frac{P(n)}{\forall x\, P(x)}$$

La misma pregunta, donde $C(p)$: persona p tiene cumpleaños

$$\frac{C(Maria)}{\forall p\, C(p)} \qquad\qquad \frac{C(q)}{\forall p\, C(p)}$$

Reglas de Inferencia con Cuantificadores
Generalización Universal

Ejemplo:

Si $P(x) : x > x - 1$, ¿cuál de los dos argumentos lógicos es correcto?

$$\cancel{\frac{P(3)}{\forall x\, P(x)}} \qquad\qquad \frac{P(n)}{\forall x\, P(x)}$$

La misma pregunta, donde $C(p)$: persona p tiene cumpleaños

$$\frac{C(Maria)}{\forall p\, C(p)} \qquad\qquad \frac{C(q)}{\forall p\, C(p)}$$

Ejemplo:

Si $P(x) : x > x-1$, ¿cuál de los dos argumentos lógicos es correcto?

$$\cancel{\dfrac{P(3)}{\forall x P(x)}} \qquad\qquad \dfrac{P(n)}{\forall x P(x)}$$

La misma pregunta, donde $C(p)$: persona p tiene cumpleaños

$$\cancel{\dfrac{C(Maria)}{\forall p\, C(p)}} \qquad\qquad \dfrac{C(q)}{\forall p\, C(p)}$$

$$\frac{\exists x\, P(x)}{P(c) \text{ para un elemento } c}$$

Significado: Si sabemos que existe un x tal que $P(x)$ es **V**, entonces le podemos dar nombre a este elemento

- Ojo que c debe ser una nueva variable, no puede ser una ya en uso en la demostración
- Generalmente, solo se sabe que existe, y no su valor. Como existe, se le puede dar nombre y continuar el argumento.

Ejemplo:

- Hipótesis: Alguien ha inscrito este ramo ($\exists x\, P(x)$)
- Conclusión:

$$\frac{\exists x\, P(x)}{P(c) \text{ para un elemento } c}$$

Significado: Si sabemos que existe un x tal que $P(x)$ es **V**, entonces le podemos dar nombre a este elemento

- Ojo que c debe ser una nueva variable, no puede ser una ya en uso en la demostración
- Generalmente, solo se sabe que existe, y no su valor. Como existe, se le puede dar nombre y continuar el argumento.

Ejemplo:

- Hipótesis: Alguien ha inscrito este ramo ($\exists x\, P(x)$)
- Conclusión: entonces, sea "Pedrito" ese alguien.

$$\frac{P(c) \text{ para un elemento } c}{\exists x\, P(x)}$$

Significado: Si conocemos un elemento c donde $P(c)$ es **V**, entonces podemos concluir que $\exists x\, P(x)$ es **V**

Ejemplo:

- Hipótesis: Juan ha comido pizza ($P(c)$)
- Conclusión:

$$\frac{P(c) \text{ para un elemento } c}{\exists x\, P(x)}$$

Significado: Si conocemos un elemento c donde $P(c)$ es **V**, entonces podemos concluir que $\exists x\, P(x)$ es **V**

Ejemplo:

- Hipótesis: Juan ha comido pizza ($P(c)$)
- Conclusión: Por lo tanto, alguien ha comido pizza ($\exists x\, P(x)$)

Ejemplos

¿Es válido el siguiente argumento?

$D(p)$: p es alumno de INF-152
$C(p)$: p es alumno de Ing. Civil Informática

$$\begin{array}{l} \forall p\,(D(p) \Rightarrow C(p)) \\ D(\text{Juan}) \\ \hline C(\text{Juan}) \end{array}$$

Ejemplos

¿Es válido el siguiente argumento?

$D(p)$: p es alumno de INF-152
$C(p)$: p es alumno de Ing. Civil Informática

$$\begin{array}{l} \forall p\,(D(p) \Rightarrow C(p)) \\ D(\text{Juan}) \\ \hline C(\text{Juan}) \end{array}$$

Solución:

1.	$\forall p\,(D(p) \Rightarrow C(p))$	hipótesis
2.	$D(\text{Juan}) \Rightarrow C(\text{Juan})$	part. universal, Juan es de tipo p
3.	$D(\text{Juan})$	hipótesis
4.	$C(\text{Juan})$	modus ponens, lineas 2 y 3

$\therefore$ El argumento es correcto.

Ejercicio

Si los siguientes argumentos son correctos:

- Un alumno de este curso no ha bajado la guía de ejercicios
- Todos los alumnos aprobaron el primer certamen

Mostrar que lo anterior implica:

- Alguien quien aprobó el primer certamen no bajó la guía de ejercicios

Ejercicio

Si los siguientes argumentos son correctos:

- Un alumno de este curso no ha bajado la guía de ejercicios
- Todos los alumnos aprobaron el primer certamen

Mostrar que lo anterior implica:

- Alguien quien aprobó el primer certamen no bajó la guía de ejercicios

Primer paso: formalizar

- x : persona
- $E(x)$: x es alumno de este curso
- $G(x)$: x ha bajado la guía de ejercicios
- $P(x)$: x ha aprobado el primer certamen

Ejemplo

x : persona
$G(x)$: x ha bajado la guía de ejercicios
$E(x)$: x es alumno de este curso
$P(x)$: x ha aprobado el primer certamen

Entonces:

$$\begin{array}{l} \exists x\,(E(x) \wedge \neg G(x)) \\ \forall x\,(E(x) \Rightarrow P(x)) \\ \hline \exists x\,(P(x) \wedge \neg G(x)) \end{array}$$

Solución: demostrar de que el argumento es válido

Ejemplo

x : persona

$G(x)$: x ha bajado la guía de ejercicios

$E(x)$: x es alumno de este curso

$P(x)$: x ha aprobado el primer certamen

Entonces:

$$\begin{array}{l} \exists x\,(E(x) \land \neg G(x)) \\ \forall x\,(E(x) \Rightarrow P(x)) \\ \hline \exists x\,(P(x) \land \neg G(x)) \end{array}$$

Solución: demostrar de que el argumento es válido

1.	$\exists x\,(E(x) \land \neg G(x))$	hipótesis
2.	$E(a) \land \neg G(a)$	part. existencial de linea 1, a es alumno
3.	$E(a)$	simplificación de linea 2
4.	$\forall x\,(E(x) \Rightarrow P(x))$	hipótesis
5.	$E(a) \Rightarrow P(a)$	part. universal de linea 4
6.	$P(a)$	modus ponens de lineas 3, 5
7.	$\neg G(a)$	simplificación de linea 2
8.	$P(a) \land \neg G(a)$	combinación de linea 6, 7
9.	$\exists x\,(P(x) \land \neg G(x))$	gen. existencial de linea 8

$\therefore$ El argumento es correcto.

Técnicas de demostración

Teoremas

Definición: teorema

Una expresión que se ha demostrado como verdadera con respecto a axiomas, teoremas existentes.

- Muchos teoremas se escriben como implicaciones: si $p_1, p_2, p_3, \ldots p_n$ son todas verdaderas (hipótesis), entonces q también lo es
- En otras palabras, queremos demostrar teoremas de la forma

$$p_1 \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_n \Rightarrow q$$

Terminología

Definición: conjetura

Expresión cuyo valor de verdad es desconocido. Si podemos demostrar una conjetura, entonces esta se convierte en teorema

Definición: lema

Teorema sencillo usado en la demostración de otros teoremas (un resultado útil, pero no suficientemente “interesante” como para ponerle nombre)

Definición: corolario

Proposición que se puede establecer directamente a partir de un teorema ya demostrado

Técnicas de Demostración

Para teoremas de la forma $p \Rightarrow q$:

- Demostración Directa
- Demostración Indirecta
- Demostración Vacua
- Demostración Trivial
- Reducción al Absurdo (también conocida como “Demostración por Contradicción”)
- Demostración por Casos
- Demostración de Equivalencia

Demostración Directa

Para demostrar $p \Rightarrow q$ de forma directa:

1. Asumir que p es **V**
2. Usar las reglas de inferencia y teoremas ya demostrados para demostrar que q también debe ser **V**

Ejemplo: Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Notar que:

- un entero n es par si $\exists k$ tal que $n = 2k$ ...
- ... y es impar si $\exists k$ tal que $n = 2k + 1$

Demostración Directa
Ejemplo

Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Demostración:

1. Primero, SIEMPRE especificar lo que se va a demostrar

Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Demostración:

1. Primero, SIEMPRE especificar lo que se va a demostrar
   - p : n es un entero impar
   - q : n^2 es un entero impar
   - Queremos demostrar que $p \Rightarrow q$
2. Asumir que p es **V**.

Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Demostración:

1. Primero, SIEMPRE especificar lo que se va a demostrar
   - p : n es un entero impar
   - q : n^2 es un entero impar
   - Queremos demostrar que $p \Rightarrow q$
2. Asumir que p es **V**. Es decir, n es impar, lo que significa que $\exists k$ tal que $n = 2k + 1$
3. Ahora, tratar de deducir que q es **V** de lo que ya sabemos:

Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Demostración:

1. Primero, SIEMPRE especificar lo que se va a demostrar
   - $p : n$ es un entero impar
   - $q : n^2$ es un entero impar
   - Queremos demostrar que $p \Rightarrow q$
2. Asumir que p es **V**. Es decir, n es impar, lo que significa que $\exists k$ tal que $n = 2k + 1$
3. Ahora, tratar de deducir que q es **V** de lo que ya sabemos:
   $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2\ell + 1$
4. Conclusión:

Demostrar que si n es un entero impar, entonces n^2 es un entero impar. Demostración:

1. Primero, SIEMPRE especificar lo que se va a demostrar
   - p : n es un entero impar
   - q : n^2 es un entero impar
   - Queremos demostrar que $p \Rightarrow q$
2. Asumir que p es **V**. Es decir, n es impar, lo que significa que $\exists k$ tal que $n = 2k+1$
3. Ahora, tratar de deducir que q es **V** de lo que ya sabemos:
   $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2\ell + 1$
4. Conclusión: como $\exists \ell$ tal que $n^2 = 2\ell + 1$, podemos concluir que n^2 es entero impar si n es impar $\square$

Como este es un teorema simple, bastó con un poco de álgebra para inferir q, pero usualmente se deben aplicar reglas de inferencia

Demostración Indirecta

Para demostrar $p \Rightarrow q$ de forma indirecta:

1. Como $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ (contrarecíproca)
2. Asumir que $\neg q$ es **V**
3. Usar las reglas de inferencia y teoremas ya demostrados para demostrar que $\neg p$ también debe ser **V**

Es decir, una demostración indirecta de $p \Rightarrow q$ es una demostración directa de $\neg q \Rightarrow \neg p$

Ejemplo: Demostrar que si $3n+2$ es entero impar, entonces n es entero impar

Demostrar que si $3n+2$ es entero impar, entonces n es entero impar. Demostración:

Demostrar que si $3n+2$ es entero impar, entonces n es entero impar. Demostración:

1. Especificar lo que se va a demostrar
   - $p: 3n+2$ es un entero impar
   - $q: n$ es un entero impar
   - Queremos demostrar que $\neg q \Rightarrow \neg p$

Demostrar que si $3n+2$ es entero impar, entonces n es entero impar. Demostración:

1. Especificar lo que se va a demostrar
   - $p : 3n+2$ es un entero impar
   - $q : n$ es un entero impar
   - Queremos demostrar que $\neg q \Rightarrow \neg p$
2. Asumir que $\neg q$ es **V**. Es decir, n es par, lo que significa que $\exists k$ tal que $n = 2k$

Demostrar que si $3n+2$ es entero impar, entonces n es entero impar. Demostración:

1. Especificar lo que se va a demostrar
   - $p : 3n+2$ es un entero impar
   - $q : n$ es un entero impar
   - Queremos demostrar que $\neg q \Rightarrow \neg p$
2. Asumir que $\neg q$ es **V**. Es decir, n es par, lo que significa que $\exists k$ tal que $n = 2k$
3. Se sigue entonces que $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) = 2\ell$

Demostrar que si $3n+2$ es entero impar, entonces n es entero impar. Demostración:

1. Especificar lo que se va a demostrar
   - $p : 3n+2$ es un entero impar
   - $q : n$ es un entero impar
   - Queremos demostrar que $\neg q \Rightarrow \neg p$
2. Asumir que $\neg q$ es **V**. Es decir, n es par, lo que significa que $\exists k$ tal que $n = 2k$
3. Se sigue entonces que $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) = 2\ell$
4. Conclusión: como $\exists \ell$ tal que $3n+2 = 2\ell$, podemos concluir que $3n+2$ es entero par (entonces, $\neg p$ es **V**) $\square$

Demostración Vacua

Para demostrar $p \Rightarrow q$ de forma vacua:

1. ¿Que sucede si p siempre es **F**?

Demostración Vacua

Para demostrar $p \Rightarrow q$ de forma vacua:

1. ¿Que sucede si p siempre es **F**?
2. En ese caso, $p \Rightarrow q$ es siempre **V**, sin importar el valor de q
3. Entonces, si podemos demostrar que p es siempre **F**, hemos demostrado que $p \Rightarrow q$ por vacuidad

Ejemplo: Muestre que la proposición $P(0)$ es **V**, donde $P(n)$ es el predicado “si $n > 1$, entonces $n^2 > n$”

Demostración Vacua

Para demostrar $p \Rightarrow q$ de forma vacua:

1. ¿Que sucede si p siempre es **F**?
2. En ese caso, $p \Rightarrow q$ es siempre **V**, sin importar el valor de q
3. Entonces, si podemos demostrar que p es siempre **F**, hemos demostrado que $p \Rightarrow q$ por vacuidad

Ejemplo: Muestre que la proposición $P(0)$ es **V**, donde $P(n)$ es el predicado "si $n > 1$, entonces $n^2 > n$"

Demostración:

1. $P(0)$ es la implicación "si $0 > 1$, entonces $0^2 > 0$", donde $p : 0 > 1$ y $q : 0^2 > 0$
2. Conclusión: como p siempre es **F**, $P(0)$ es **V** de forma vacua $\square$

Demostración Trivial

Para demostrar $p \Rightarrow q$ de forma trivial:

1. ¿Que sucede si q siempre es **V**?
2. En ese caso, $p \Rightarrow q$ es siempre **V**, sin importar el valor de p
3. Entonces, si podemos demostrar que q es siempre **V**, hemos demostrado que $p \Rightarrow q$ por trivialidad

Ejemplo: Demuestre que si n es la suma de dos números primos, entonces n es par o impar

Demostración Trivial

Para demostrar $p \Rightarrow q$ de forma trivial:

1. ¿Que sucede si q siempre es **V**?
2. En ese caso, $p \Rightarrow q$ es siempre **V**, sin importar el valor de p
3. Entonces, si podemos demostrar que q es siempre **V**, hemos demostrado que $p \Rightarrow q$ por trivialidad

Ejemplo: Demuestre que si n es la suma de dos números primos, entonces n es par o impar

Demostración:

1. $p : n$ es la suma de dos números primos, y $q : n$ es par o impar
2. Pero impar $\equiv \neg$ par, así que q siempre es **V**
3. Conclusión: como q siempre es **V**, $p \Rightarrow q$ es trivialmente **V** $\square$

Caso simple: demostrar que p es **V** por reducción al absurdo

- Asumir que $\neg p$ es **V**
- Usar las reglas de inferencia y teoremas ya demostrados para llegar a una contradicción, es decir, $\neg p \Rightarrow \mathbf{F}$
- Si $\neg p \Rightarrow \mathbf{F}$ es **V**, esto significa que $\neg p$ es **F** (es decir, nuestro supuesto inicial fue incorrecto), y que entonces p es **V**

Ejemplo: Muestre que $\sqrt{2}$ es número irracional

Caso simple: demostrar que p es **V** por reducción al absurdo

- Asumir que $\neg p$ es **V**
- Usar las reglas de inferencia y teoremas ya demostrados para llegar a una contradicción, es decir, $\neg p \Rightarrow \mathbf{F}$
- Si $\neg p \Rightarrow \mathbf{F}$ es **V**, esto significa que $\neg p$ es **F** (es decir, nuestro supuesto inicial fue incorrecto), y que entonces p es **V**

Ejemplo: Muestre que $\sqrt{2}$ es número irracional

Demostración:

1. $p : \sqrt{2}$ es número irracional. Queremos demostrar p por contradicción
2. Asumir que $\neg p$ es **V**, es decir, $\sqrt{2}$ es número racional
3. Si $\sqrt{2}$ es número racional, entonces existen dos enteros a, b tales que $\sqrt{2} = \frac{a}{b}$, donde a, b no tienen factores comunes
4. ...continúa

Reducción al Absurdo
Ejemplo

Ejemplo: Muestre que $\sqrt{2}$ es número irracional

Ejemplo: Muestre que $\sqrt{2}$ es número irracional

Demostración:

4. Como $\sqrt{2} = \frac{a}{b}$, tenemos que $2 = \frac{a^2}{b^2}$, así que $a^2 = 2b^2$, lo que implica que a^2 es un número par
5. Teo. 1: si n^2 es par, entonces n es par (propuesto: demostrar)
6. Usando Teo. 1, tenemos que a es par, es decir, $\exists c$ tal que $a = 2c$
7. Entonces, $2b^2 = (2c)^2$, por lo que $b^2 = 2c^2$
8. Usando Teo. 1, tenemos que b también es par
9. Esto es una contradicción, nuestro supuesto en el paso 3 es que a y b no tienen factores comunes
10. Conclusión: como $\neg p$ es **F** por contradicción, podemos concluir que $\sqrt{2}$ es irracional $\square$

Veamos como demostrar que $p \Rightarrow q$ es **V** por reducción al absurdo

- Asumir que $\neg(p \Rightarrow q)$ es **V**, es decir, que $p \wedge \neg q$ es **V**
- Usar las reglas de inferencia y teoremas ya demostrados para llegar a una contradicción, es decir, $p \wedge \neg q \Rightarrow \mathbf{F}$
- Una contradicción significa que nuestro supuesto de que $\neg q$ es **V** es incorrecto. Entonces, como q es **V**, tenemos que $p \Rightarrow q$ es **V**

Ejemplo: Mostrar que si m es un entero par, entonces $m+7$ es impar

Ejemplo: Mostrar que si m es un entero par, entonces $m+7$ es impar

Ejemplo: Mostrar que si m es un entero par, entonces $m+7$ es impar

Demostración:

1. $p : m$ es entero par, $q : m+7$ es entero impar. Quiero demostrar $p \Rightarrow q$ por contradicción
2. Asumir que $p \wedge \neg q$ es **V**, es decir, $\exists k, \ell$ tal que $m = 2k$ y $m+7 = 2\ell$
3. Si $m+7 = 2\ell$, entonces $m = 2\ell - 7 = 2\ell - 8 + 1 = 2(\ell - 4) + 1 = 2h + 1$. Es decir, m es impar
4. Esto contradice nuestro supuesto inicial, entonces fue incorrecto asumir que $\neg q$ es **V**
5. Conclusión: como q es **V**, podemos concluir que $p \Rightarrow q$ es **V** $\square$

Demostración por Casos

¿Cómo podemos demostrar algo de la forma $(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q$?

- $p_1, p_2, \ldots p_n$ representan distintos casos
- Usemos equivalencias lógicas:
  $(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots (p_n \Rightarrow q)$
- Es decir, si demostramos $p_i \Rightarrow q$, $\forall i = 1 \ldots n$ (usando las técnicas que quieran), hemos demostrado la implicación original

Ejemplo: Demostrar que si x, y son números reales, entonces $\max(x,y) + \min(x,y) = x + y$

Demostración por Casos

¿Cómo podemos demostrar algo de la forma $(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q$?

- $p_1, p_2, \ldots p_n$ representan distintos casos
- Usemos equivalencias lógicas:
  $(p_1 \vee p_2 \vee \cdots \vee p_n) \Rightarrow q \equiv (p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \ldots (p_n \Rightarrow q)$
- Es decir, si demostramos $p_i \Rightarrow q$, $\forall i = 1 \ldots n$ (usando las técnicas que quieran), hemos demostrado la implicación original

Ejemplo: Demostrar que si x, y son números reales, entonces $\max(x,y) + \min(x,y) = x + y$

Demostración:

- Identificar casos que sirvan para hacer la demostración. Por ejemplo, si hay mínimos y máximos, es útil saber cual número es mayor/menor, por lo que definiré: $p_1 : x < y$, $p_2 : x > y$, $p_3 : x = y$
- Quiero demostrar que si $(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q)$, donde $q : \max(x,y) + \min(x,y) = x + y$

sigue ...

Demostrar que $(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q)$

Demostración por Casos
Ejemplo

Demostrar que $(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q)$

- Caso 1: $(x < y \Rightarrow q)$
  1. Si $x < y$, sabemos que $\max(x,y) = y$, $\min(x,y) = x$ (def. de *max*, *min*)
  2. Entonces, $\max(x,y) + \min(x,y) = y + x = x + y$ (conmut. +)
  3. Conclusión: $(x < y \Rightarrow q)$, por demostración directa $\square$
- Caso 2: $(x > y \Rightarrow q)$. Demostración similar a la anterior, solo que $\max(x,y) = x$ y $\min(x,y) = y$ $\square$
- Caso 3: $(x = y \Rightarrow q)$
  1. Si $x = y$, sabemos que $\max(x,y) = x = y$, $\min(x,y) = x = y$
  2. Entonces, $\max(x,y) + \min(x,y) = x + y$
  3. Conclusión: $(x = y \Rightarrow q)$, por demostración directa $\square$

Conclusión: como $(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge (p_3 \Rightarrow q)$ es **V**, podemos concluir que $p \Rightarrow q$ es **V** $\square$

Demostración de Equivalencia

Para demostrar cosas de la forma $p \Leftrightarrow q$

- Podemos usar la tautología $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
- Usando las técnicas de demostración que quieran, deben demostrar las dos implicaciones para demostrar que $p \Leftrightarrow q$ es **V**

Ejemplo: Demostrar que el entero n es impar si, y solo si, n^2 es impar

Demostración de Equivalencia

Para demostrar cosas de la forma $p \Leftrightarrow q$

- Podemos usar la tautología $p \Leftrightarrow q \equiv (p \Rightarrow q) \land (q \Rightarrow p)$
- Usando las técnicas de demostración que quieran, deben demostrar las dos implicaciones para demostrar que $p \Leftrightarrow q$ es **V**

Ejemplo: Demostrar que el entero n es impar si, y solo si, n^2 es impar

Demostración:

1. $p : n$ es impar, $q : n^2$ es impar, queremos demostrar que $p \Leftrightarrow q$
2. Ya demostramos que $p \Rightarrow q$, ver ejemplo de *Demostración Directa*
3. Falta probar que $q \Rightarrow p$

Ejemplo

Demostrar que n^2 es impar $\Rightarrow$ n es impar $(q \Rightarrow p)$

Ejemplo

Demostrar que n^2 es impar $\Rightarrow$ n es impar $(q \Rightarrow p)$

- Intento 1: demostración directa
  1. Asumir que n^2 es impar, demostrar que n es impar
  2. Si n^2 es impar, significa que $\exists k$ tal que $n^2 = 2k+1$
  3. Entonces, $n = \pm\sqrt{2k+1}$ ... ¿y que mas podemos inferir?

Ejemplo

Demostrar que n^2 es impar $\Rightarrow n$ es impar $(q \Rightarrow p)$

- Intento 1: demostración directa
  1. Asumir que n^2 es impar, demostrar que n es impar
  2. Si n^2 es impar, significa que $\exists k$ tal que $n^2 = 2k+1$
  3. Entonces, $n = \pm\sqrt{2k+1}$ ... ¿y que mas podemos inferir? esto parece ser un camino sin salida, cambiemos de técnica
- Intento 2: demostración indirecta
  1. Asumir que n es par, demostrar que n^2 es par
  2. Si n es par, entonces $\exists k$ tal que $n = 2k$
  3. Entonces, $n^2 = (2k)^2 = 2(2k^2) = 2\ell$, es decir, n^2 es número par
  4. Conclusión: hemos demostrado que la contrareciproca de $q \Rightarrow p$ es **V**, así que la implicación original es **V**

Conclusión: como $p \Rightarrow q$ y $q \Rightarrow p$ son **V**, sabemos que $p \Leftrightarrow q$ es **V** $\square$

OJO: Si no logran completar una demostración, intenten con otra técnica, otra formalización de p, q, otros casos, etc.

Técnicas de Demostración

Para teoremas con cuantificadores:

- Para demostrar que $\forall x P(x)$ es **V**:
  1. Aplicar particularización universal: $P(c)$, donde c es elemento arbitrario
  2. Demostrar que $P(c)$ es **V**, tal como lo hemos hecho en las diapos anteriores
  3. Generalizar el resultado para concluir que $\forall x P(x)$ es **V**
- Demostración de Existencia
- Demostración de Unicidad
- Contraejemplos

Demostración de Existencia

Existen dos estrategias para demostrar teoremas de la forma $\exists x P(x)$:

1. Encontrar un elemento a tal que $P(a)$ es **V**. No siempre se conoce el valor de a, solo hay que demostrar que existe
2. Demostrar que tal elemento no existe, es decir, que $\forall x \neg P(x)$ es **V**

Ejemplo: Muestre que existen dos números irracionales x, y tales que x^y es racional

Demostración de Existencia

Existen dos estrategias para demostrar teoremas de la forma $\exists x P(x)$:

1. Encontrar un elemento a tal que $P(a)$ es **V**. No siempre se conoce el valor de a, solo hay que demostrar que existe
2. Demostrar que tal elemento no existe, es decir, que $\forall x \neg P(x)$ es **V**

Ejemplo: Muestre que existen dos números irracionales x, y tales que x^y es racional

Demostración:

1. Del ejemplo de *Reducción al Absurdo*, sabemos que $\sqrt{2}$ es número irracional
2. Consideremos el número $\sqrt{2}^{\sqrt{2}}$:
   - Caso 1: si $\sqrt{2}^{\sqrt{2}}$ es racional, hemos encontrado valores de x, y que hacen que el teorema sea verdadero $\square$
   - Caso 2: ¿y si $\sqrt{2}^{\sqrt{2}}$ es irracional?

Ejemplo: Muestre que existen dos números irracionales x, y tales que x^y es racional

Demostración:

- Sabemos que $\sqrt{2}$ es número irracional
- Caso 1: si $\sqrt{2}^{\sqrt{2}}$ es racional, hemos encontrado valores de x, y que hacen que la expresión sea verdadera $\square$
- Caso 2: ¿y si $\sqrt{2}^{\sqrt{2}}$ es irracional?

Ejemplo: Muestre que existen dos números irracionales x, y tales que x^y es racional

Demostración:

- Sabemos que $\sqrt{2}$ es número irracional
- Caso 1: si $\sqrt{2}^{\sqrt{2}}$ es racional, hemos encontrado valores de x, y que hacen que la expresión sea verdadera $\square$
- Caso 2: ¿y si $\sqrt{2}^{\sqrt{2}}$ es irracional? Tomemos $x = \sqrt{2}^{\sqrt{2}}$ e $y = \sqrt{2}$. Entonces, $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}.\sqrt{2}} = \sqrt{2}^2 = 2$, que claramente es racional $\square$

Conclusión: en ambos casos encontramos valores de x, y irracionales tales que x^y es racional, así que la expresión es **V** $\square$

Demostración de Unicidad

Algunos teoremas afirman la existencia de un único elemento con cierta propiedad ($\exists! x\, P(x)$). Para demostrar esto, debemos probar dos cosas:

1. Existencia: existe un elemento que cumple la condición
2. Unicidad: este elemento es único

Esto es lo mismo que demostrar $\exists x\, (P(x) \wedge \forall y\, (y \neq x \Rightarrow \neg P(y)))$

Técnica común para estas demostraciones:

- Demostrar que $\exists x\, P(x)$
- Asumir que que existe $y \neq x$ tal que $P(y)$ sea **V**, y llegar a una contradicción

Ejemplo: si a y b son números reales y $a \neq 0$, entonces existe un único número real r tal que $ar + b = 0$

Demostración:

Demostración de Unicidad
Ejemplo

Ejemplo: si a y b son números reales y $a \neq 0$, entonces existe un único número real r tal que $ar + b = 0$

Demostración:

- Existencia: es fácil ver que $r = -\frac{b}{a}$ es la solución de la ecuación $ar + b = 0$, así que existe un número real r tal que $ar + b = 0$ $\square$

Ejemplo: si a y b son números reales y $a \neq 0$, entonces existe un único número real r tal que $ar + b = 0$

Demostración:

- Existencia: es fácil ver que $r = -\frac{b}{a}$ es la solución de la ecuación $ar + b = 0$, así que existe un número real r tal que $ar + b = 0$ $\square$
- Unicidad:
  1. Asumir que existe un número real $s \neq r$ tal que $as + b = 0$
  2. Como $ar + b = 0$ y $as + b = 0$, tenemos que $ar + b = as + b$
  3. Restando b a ambos lados, nos queda que $ar = as$
  4. Como $ar = as$ y $a \neq 0$ (parte de la premisa), la única posibilidad es que $r = s$, lo que contradice nuestro supuesto inicial
  5. Conclusión: no existe $s \neq r$ tal que $as + b = 0$, es decir, si $s \neq r$, entonces $as + b \neq 0$ $\square$

Conclusión: como hemos demostrado la existencia y unicidad de r, podemos concluir que la expresión es **V** $\square$

Contraejemplos

Quieren demostrar una expresión de la forma $\forall x\, P(x)$

- Pero encuentran un valor de x tal que $P(x)$ es **F** ...
- ... por lo que $\forall x\, P(x)$ es **F**. Este x es un *contraejemplo*

Ejemplo: para todo n, si n es entero impar, entonces $\frac{n+1}{2}$ también es entero impar

Demostración:

- ¿Existe un n_0 tal que n_0 es impar pero $\frac{n_0+1}{2}$ sea **par**?

Contraejemplos

Quieren demostrar una expresión de la forma $\forall x P(x)$

- Pero encuentran un valor de x tal que $P(x)$ es **F** ...
- ... por lo que $\forall x P(x)$ es **F**. Este x es un *contraejemplo*

Ejemplo: para todo n, si n es entero impar, entonces $\frac{n+1}{2}$ también es entero impar

Demostración:

- ¿Existe un n_0 tal que n_0 es impar pero $\frac{n_0+1}{2}$ sea **par**?
- ¿Qué tal $n_0 = 7$? Es fácil ver que $\frac{n_0+1}{2} = \frac{8}{2} = 4$, que es par
- Conclusión: la expresión es falsa $\square$

Recomendación: antes de intentar demostrar un $\forall$, intenten ver si existe algún contraejemplo. **Importante**: no pueden demostrar que un $\forall$ es **V** usando solo ejemplos