Demostraciones en la lógica proposicional

Matemática estructural y lógica

ISIS-1104

Nombres, nombres everywhere

Nombres, nombres everywhere

- Un **axioma** es una proposición que se **asume** cierta.

Nombres, nombres everywhere

- Un **axioma** es una proposición que se **asume** cierta.
- Un **teorema** es una proposición que se **demuestra**.

Nombres, nombres everywhere

- Un **axioma** es una proposición que se **asume** cierta.
- Un **teorema** es una proposición que se **demuestra**.
- Un **lema** es un teorema **chiquito**.

Nombres, nombres everywhere

- Un **axioma** es una proposición que se **asume** cierta.
- Un **teorema** es una proposición que se **demuestra**.
- Un **lema** es un teorema **chiquito**.
- Una **demostración** es una **derivación**.

Axiomas... y eso para qué?

Axiomas... y eso para qué?

Los axiomas que vamos a ver acá son equivalencias

$$LHS \equiv RHS$$

Axiomas... y eso para qué?

Los axiomas que vamos a ver acá son equivalencias

$$LHS \equiv RHS$$

y se utilizan de la siguiente forma:

Siempre que vea LHS lo puedo reemplazar por RHS

Siempre que vea RHS lo puedo reemplazar por LHS

Axiomas... y eso para qué?

Los axiomas que vamos a ver acá son equivalencias

$$LHS \equiv RHS$$

y se utilizan de la siguiente forma:

Siempre que vea *LHS* lo puedo reemplazar por *RHS*

Siempre que vea *RHS* lo puedo reemplazar por *LHS*

Es decir, son como **reglas de inferencia** pero **bidireccionales**.

Axiomas de la lógica proposicional

Axiomas de la lógica proposicional

- Conmutatividad

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

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

Axiomas de la lógica proposicional

- Conmutatividad

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

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

- Asociatividad

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

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

Axiomas de la lógica proposicional

- Conmutatividad

$$p \lor q \equiv q \lor p$$
$$p \land q \equiv q \land p$$

- Asociatividad

$$(p \lor q) \lor r \equiv q \lor (p \lor r)$$
$$(p \land q) \land r \equiv q \land (p \land r)$$

- Absorción

$$p \land (p \lor q) \equiv p$$
$$p \lor (p \land q) \equiv p$$

Axiomas de la lógica proposicional

Axiomas de la lógica proposicional

- Distribución

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

Axiomas de la lógica proposicional

- Distribución

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

- Todo o nada

$$p \wedge \neg p \equiv \mathit{False}$$
$$p \vee \neg p \equiv \mathit{True}$$

Axiomas de la lógica proposicional

- Distribución

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

- Todo o nada

$$p \wedge \neg p \equiv False$$
$$p \vee \neg p \equiv True$$

- Identidad

$$p \vee False \equiv p$$
$$p \wedge True \equiv p$$

Axiomas de la lógica proposicional

Axiomas de la lógica proposicional

- Piso, techo

$$p \wedge \mathit{False} \equiv \mathit{False}$$

$$p \vee \mathit{True} \equiv \mathit{True}$$

Axiomas de la lógica proposicional

- Piso, techo

$$p \wedge False \equiv False$$

$$p \vee True \equiv True$$

- Idempotencia

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

Axiomas de la lógica proposicional

- Piso, techo

$$p \wedge \mathit{False} \equiv \mathit{False}$$
$$p \vee \mathit{True} \equiv \mathit{True}$$

- Idempotencia

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

- Doble negación

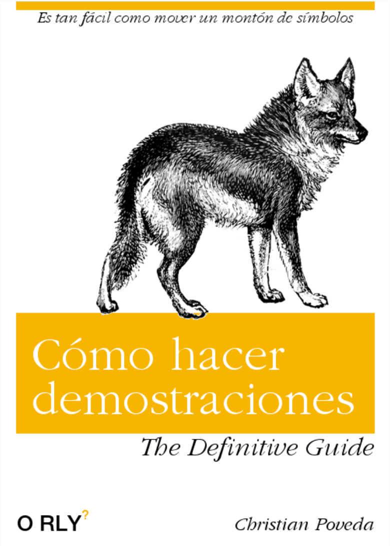
$$\neg\neg p \equiv p$$

Axiomas de la lógica proposicional

Axiomas de la lógica proposicional

- Leyes de De Morgan

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


Es tan fácil como mover un montón de símbolos
Cómo hacer demostraciones
The Definitive Guide
O RLY?
Christian Poveda

Ejemplo: Probando una equivalencia

Ejemplo: Probando una equivalencia

Demuestre que $p \equiv (p \land q) \lor (p \land \neg q)$

Ejemplo: Probando una equivalencia

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

Demostración:

Ejemplo: Probando una equivalencia

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

Demostración:

Tenemos dos opciones

Ejemplo: Probando una equivalencia

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

Demostración:

Tenemos dos opciones

- Partiendo de p usar axiomas hasta llegar a $(p \wedge q) \vee (p \wedge \neg q)$.

Ejemplo: Probando una equivalencia

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

Demostración:

Tenemos dos opciones

- Partiendo de p usar axiomas hasta llegar a $(p \wedge q) \vee (p \wedge \neg q)$.
- Partiendo de $(p \wedge q) \vee (p \wedge \neg q)$ usar axiomas hasta llegar a p.

Ejemplo: Probando una equivalencia

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

Demostración:

Tenemos dos opciones

- Partiendo de p usar axiomas hasta llegar a $(p \wedge q) \vee (p \wedge \neg q)$.
- Partiendo de $(p \wedge q) \vee (p \wedge \neg q)$ usar axiomas hasta llegar a p.

Usualmente la segunda es más fácil.

Ejemplo: Probando una equivalencia

Ejemplo: Probando una equivalencia

- Partimos de

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

Ejemplo: Probando una equivalencia

- Partimos de

$$(p \land q) \lor (p \land \neg q)$$

- Usando distribución

$$(p \land q) \lor (p \land \neg q) \equiv p \land (q \lor \neg q)$$

Ejemplo: Probando una equivalencia

- Partimos de

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

- Usando distribución

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

- Usando todo o nada

$$p \wedge (q \vee \neg q) \equiv p \vee \mathit{True}$$

Ejemplo: Probando una equivalencia

- Partimos de

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

- Usando distribución

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

- Usando todo o nada

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

- Usando identidad

$$p \wedge True \equiv p$$

Ejemplo: Probando una equivalencia

- Partimos de

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

- Usando distribución

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

- Usando todo o nada

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

- Usando identidad

$$p \wedge True \equiv p$$

- Luego concluimos que

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

Ejemplo: Probando una equivalencia

Ejemplo: Probando una equivalencia

- Otra forma de escribir esta prueba es

$$\begin{aligned}
(p \wedge q) \vee (p \wedge \neg q) &\equiv p \wedge (q \vee \neg q) && \text{(distribución)} \\
&\equiv p \wedge \mathit{True} && \text{(todo o nada)} \\
&\equiv p && \text{(identidad)}
\end{aligned}$$

Ejemplo: Probando una equivalencia

- Otra forma de escribir esta prueba es

$$
\begin{aligned}
(p \wedge q) \vee (p \wedge \neg q) &\equiv p \wedge (q \vee \neg q) && \text{(distribución)} \\
&\equiv p \wedge \mathit{True} && \text{(todo o nada)} \\
&\equiv p && \text{(identidad)}
\end{aligned}
$$

- Tras bastidores simplemente estamos mostrando que $p \equiv (p \wedge q) \vee (p \wedge \neg q)$ es **verdadera** sin importar que valores puedan llegar a tomar p y q.

Ejemplo: Probando una equivalencia

- Otra forma de escribir esta prueba es

$$\begin{aligned}
(p \land q) \lor (p \land \neg q) &\equiv p \land (q \lor \neg q) && \text{(distribución)}\\
&\equiv p \land \mathit{True} && \text{(todo o nada)}\\
&\equiv p && \text{(identidad)}
\end{aligned}$$

- Tras bastidores simplemente estamos mostrando que $p \equiv (p \land q) \lor (p \land \neg q)$ es **verdadera** sin importar que valores puedan llegar a tomar p y q.
- Cuando una proposición es verdadera **siempre**, decimos que es una **tautología**.

Ejercicio: Probando otra equivalencia

Ejercicio: Probando otra equivalencia

- Ahora ustedes demuestren que $\neg q \lor (p \land q) \equiv \neg q \lor p$

...que pasa cuando me piden probar algo que no es una equivalencia?

Pruebas en general

Pruebas en general

- Pedir una demostración de p es lo mismo que pedir una demostración de que p es una **tautología**.

Pruebas en general

- Pedir una demostración de p es lo mismo que pedir una demostración de que p es una **tautología**.
- En otras palabras, basta mostrar que a partir de p puedo llegar a *True* usando **equivalencias**.

$$p \equiv True$$

Ejemplo

Ejemplo

Demuestre que $p \wedge (p \Rightarrow q) \Rightarrow q$

Ejemplo

Demuestre que $p \wedge (p \Rightarrow q) \Rightarrow q$

Demostración:

$$\begin{aligned}
p \wedge (p \Rightarrow q) \Rightarrow q &\equiv p \wedge (\neg p \vee q) \Rightarrow q && \text{(def. } \Rightarrow\text{)} \\
&\equiv (p \wedge \neg p) \vee (p \wedge q) \Rightarrow q && \text{(distribución)} \\
&\equiv \mathit{False} \vee (p \wedge q) \Rightarrow q && \text{(todo o nada)} \\
&\equiv (p \wedge q) \Rightarrow q && \text{(identidad)} \\
&\equiv \neg(p \wedge q) \vee q && \text{(def. } \Rightarrow\text{)} \\
&\equiv (\neg p \vee \neg q) \vee q && \text{(De Morgan)} \\
&\equiv \neg p \vee (\neg q \vee q) && \text{(asociatividad)} \\
&\equiv \neg p \vee \mathit{True} && \text{(todo o nada)} \\
&\equiv \mathit{True} && \text{(piso, techo)}
\end{aligned}$$

Ejercicio

Ejercicio

- Ahora ustedes demuestren que $p \wedge q \Rightarrow p$

Reglas de inferencia

Reglas de inferencia

- Las reglas de inferencia en lógica son expresiones de la forma

$$\frac{P_1 \wedge P_2 \wedge \ldots \wedge P_n}{C}$$

Reglas de inferencia

- Las reglas de inferencia en lógica son expresiones de la forma

$$\frac{P_1 \wedge P_2 \wedge ... \wedge P_n}{C}$$

- Una regla de inferencia es cierta si la siguiente **proposición** es una **tautología**

$$(P_1 \wedge P_2 \wedge ... \wedge P_n) \Rightarrow C \tag{1}$$

Reglas de inferencia

- Las reglas de inferencia en lógica son expresiones de la forma

$$\frac{P_1 \wedge P_2 \wedge ... \wedge P_n}{C}$$

- Una regla de inferencia es cierta si la siguiente **proposición** es una **tautología**

$$(P_1 \wedge P_2 \wedge ... \wedge P_n) \Rightarrow C \tag{1}$$

- Se usan de la siguiente manera:

Si tengo $P_1 \wedge P_2 \wedge ... \wedge P_n$ puedo derivar C

Reglas de inferencia

- Las reglas de inferencia en lógica son expresiones de la forma

$$\frac{P_1 \wedge P_2 \wedge \ldots \wedge P_n}{C}$$

- Una regla de inferencia es cierta si la siguiente **proposición** es una **tautología**

$$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \Rightarrow C \tag{1}$$

- Se usan de la siguiente manera:

Si tengo $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ puedo derivar C

- Dado que (1) **no** es una **equivalencia**, sólo puedo usarla en **un sentido**.

Reglas de inferencia

Reglas de inferencia

- Modus Ponens:

$$\frac{(p) \wedge (p \Rightarrow q)}{q}$$

Reglas de inferencia

- Modus Ponens:

$$\frac{(p) \wedge (p \Rightarrow q)}{q}$$

- Modus Tollens:

$$\frac{(\neg q) \wedge (p \Rightarrow q)}{\neg p}$$

Reglas de inferencia

- Modus Ponens:

$$\frac{(p) \wedge (p \Rightarrow q)}{q}$$

- Modus Tollens:

$$\frac{(\neg q) \wedge (p \Rightarrow q)}{\neg p}$$

- Silogismo hipotético:

$$\frac{(p \Rightarrow q) \wedge (q \Rightarrow r)}{p \Rightarrow r}$$

Reglas de inferencia

- Modus Ponens:

$$\frac{(p) \land (p \Rightarrow q)}{q}$$

- Modus Tollens:

$$\frac{(\neg q) \land (p \Rightarrow q)}{\neg p}$$

- Silogismo hipotético:

$$\frac{(p \Rightarrow q) \land (q \Rightarrow r)}{p \Rightarrow r}$$

- Silogismo disyuntivo:

$$\frac{(p \lor q) \land (\neg p)}{q}$$

Reglas de inferencia

Reglas de inferencia

- Adición:

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

Reglas de inferencia

- Adición:

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

- Simplificación:

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

Reglas de inferencia

- Adición:
$$\frac{(p)}{p \vee q}$$
- Simplificación:
$$\frac{(p \wedge q)}{p}$$
- Resolución:
$$\frac{(p \vee q) \wedge (\neg p \vee r)}{q \vee r}$$

Cuando usarlas?

Cuando usarlas?

- Si queremos demostrar una proposición de la forma

$$p \Rightarrow q$$

Cuando usarlas?

- Si queremos demostrar una proposición de la forma

$$p \Rightarrow q$$

- Usamos reglas de inferencia partiendo de p hasta llegar a q.

Cuando usarlas?

- Si queremos demostrar una proposición de la forma

$$p \Rightarrow q$$

- Usamos reglas de inferencia partiendo de p hasta llegar a q.
- Nos referimos a p como la/las **hipótesis**.

Cuando usarlas?

- Si queremos demostrar una proposición de la forma

$$p \Rightarrow q$$

- Usamos reglas de inferencia partiendo de p hasta llegar a q.
- Nos referimos a p como la/las **hipótesis**.
- Nos referimos a q como la **conclusión**.

Ejemplo: Una prueba estructurada

Ejemplo: Una prueba estructurada

Demuestre que

$$(\neg p \land q) \land (r \Rightarrow p) \land (\neg r \Rightarrow s) \land (s \Rightarrow t) \Rightarrow t$$

Ejemplo: Una prueba estructurada

Demuestre que

$$(\neg p \wedge q) \wedge (r \Rightarrow p) \wedge (\neg r \Rightarrow s) \wedge (s \Rightarrow t) \Rightarrow t$$

Demostración:

Ejemplo: Una prueba estructurada

Demuestre que

$$(\neg p \wedge q) \wedge (r \Rightarrow p) \wedge (\neg r \Rightarrow s) \wedge (s \Rightarrow t) \Rightarrow t$$

Demostración:

- Primero nombramos nuestras hipótesis:

$$(\neg p \wedge q) \tag{1}$$
$$(r \Rightarrow p) \tag{2}$$
$$(\neg r \Rightarrow s) \tag{3}$$
$$(s \Rightarrow t) \tag{4}$$

Ejemplo: Una prueba estructurada

Demuestre que

$$(\neg p \land q) \land (r \Rightarrow p) \land (\neg r \Rightarrow s) \land (s \Rightarrow t) \Rightarrow t$$

Demostración:

- Primero nombramos nuestras hipótesis:

$$(\neg p \land q) \tag{1}$$
$$(r \Rightarrow p) \tag{2}$$
$$(\neg r \Rightarrow s) \tag{3}$$
$$(s \Rightarrow t) \tag{4}$$

- Ahora usando reglas de inferencia tratamos de derivar la conclusión t.

Ejemplo: Una prueba estructurada

Ejemplo: Una prueba estructurada

- Aplicando silogismo hipotético entre (3) y (4):

$$\frac{(\neg r \Rightarrow s) \wedge (s \Rightarrow t)}{\neg r \Rightarrow t} \tag{5}$$

Ejemplo: Una prueba estructurada

- Aplicando silogismo hipotético entre (3) y (4):

$$\frac{(\neg r \Rightarrow s) \wedge (s \Rightarrow t)}{\neg r \Rightarrow t} \tag{5}$$

- Aplicando simplificación a (1):

$$\frac{(\neg p \wedge q)}{\neg p} \tag{6}$$

Ejemplo: Una prueba estructurada

- Aplicando silogismo hipotético entre (3) y (4):

$$\frac{(\neg r \Rightarrow s) \wedge (s \Rightarrow t)}{\neg r \Rightarrow t} \tag{5}$$

- Aplicando simplificación a (1):

$$\frac{(\neg p \wedge q)}{\neg p} \tag{6}$$

- Aplicando modus tollens entre (6) y (2):

$$\frac{(\neg p) \wedge (r \Rightarrow p)}{\neg r} \tag{7}$$

Ejemplo: Una prueba estructurada

- Aplicando silogismo hipotético entre (3) y (4):

$$\frac{(\neg r \Rightarrow s) \wedge (s \Rightarrow t)}{\neg r \Rightarrow t} \tag{5}$$

- Aplicando simplificación a (1):

$$\frac{(\neg p \wedge q)}{\neg p} \tag{6}$$

- Aplicando modus tollens entre (6) y (2):

$$\frac{(\neg p) \wedge (r \Rightarrow p)}{\neg r} \tag{7}$$

- Aplicando modus ponens entre (7) y (5):

$$\frac{(\neg r) \wedge (\neg r \Rightarrow t)}{t}$$

Ejercicio: Otra prueba estructurada

Ejercicio: Otra prueba estructurada

Ahora ustedes, demuestren que

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