

Matemáticas Discretas I

Lógica proposicional - Aparato deductivo

Juan Francisco Díaz Frias

Profesor Titular (1993-hoy)
juanfco.diaz@correounivalle.edu.co
Edif. B13 - 4009



Universidad del Valle

Noviembre 2021

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Motivación

- Hasta ahora: A es correcto (o válido) si A es una tautología, i.e. la tabla de verdad asociada da V en todas las filas.
- Impráctico, pues el número de filas de la tabla depende exponencialmente del número de variables proposicionales, y el número de columnas depende del número de subexpresiones de la fórmula.
- Deducir la verdad en lugar de calcularla. A partir de axiomas y de la aplicación de reglas de inferencia establecer la validez de nuevas fórmulas.
- Notación: $\vdash \alpha$ se leerá como α es un teorema.

Motivación

- Hasta ahora: A es correcto (o válido) si A es una tautología, i.e. la tabla de verdad asociada da V en todas las filas.
- Impráctico, pues el número de filas de la tabla depende exponencialmente del número de variables proposicionales, y el número de columnas depende del número de subexpresiones de la fórmula.
- Deducir la verdad en lugar de calcularla. A partir de axiomas y de la aplicación de reglas de inferencia establecer la validez de nuevas fórmulas.
- Notación: $\vdash \alpha$ se leerá como α es un teorema.

Motivación

- Hasta ahora: A es correcto (o válido) si A es una tautología, i.e. la tabla de verdad asociada da V en todas las filas.
- Impráctico, pues el número de filas de la tabla depende exponencialmente del número de variables proposicionales, y el número de columnas depende del número de subexpresiones de la fórmula.
- **Deducir la verdad** en lugar de calcularla. A partir de **axiomas** y de la aplicación de **reglas de inferencia** establecer la **validez** de nuevas fórmulas.
- Notación: $\vdash \alpha$ se leerá como α es un teorema.

Motivación

- Hasta ahora: A es correcto (o válido) si A es una tautología, i.e. la tabla de verdad asociada da V en todas las filas.
- Impráctico, pues el número de filas de la tabla depende exponencialmente del número de variables proposicionales, y el número de columnas depende del número de subexpresiones de la fórmula.
- **Deducir la verdad** en lugar de calcularla. A partir de **axiomas** y de la aplicación de **reglas de inferencia** establecer la **validez** de nuevas fórmulas.
- Notación: $\vdash \alpha$ se leerá como α es un teorema.

Generalidades

- Los **axiomas** en el aparato deductivo de un sistema lógico son **fórmulas válidas** a partir de las cuales se pueden deducir nuevas fórmulas válidas.
- Cualquier fórmula válida puede ser un axioma.
- Los axiomas no se demuestran, pero se justifican. En lógica proposicional, la **justificación** de que una fórmula sea un axioma es su **tabla de verdad**.

Generalidades

- Los **axiomas** en el aparato deductivo de un sistema lógico son **fórmulas válidas** a partir de las cuales se pueden deducir nuevas fórmulas válidas.
- Cualquier fórmula válida puede ser un axioma.
- Los axiomas no se demuestran, pero se justifican. En lógica proposicional, la **justificación** de que una fórmula sea un axioma es su **tabla de verdad**.

Generalidades

- Los **axiomas** en el aparato deductivo de un sistema lógico son **fórmulas válidas** a partir de las cuales se pueden deducir nuevas fórmulas válidas.
- Cualquier fórmula válida puede ser un axioma.
- Los axiomas no se demuestran, pero se justifican. En lógica proposicional, la **justificación** de que una fórmula sea un axioma es su **tabla de verdad**.

Axiomas (Equivalencias)(1)

Verdadero, Falso y doble negación

Regla	Nombre
$\neg\neg p \equiv p$	doble negación
$false \equiv \neg true$	definición de false
$\neg false \equiv true$	negación de false

Axiomas de \wedge

Regla	Nombre
$p \wedge true \equiv p$	identidad de \wedge
$p \wedge false \equiv false$	dominación \wedge
$p \wedge p \equiv p$	idempotencia \wedge
$p \wedge q \equiv q \wedge p$	comutatividad \wedge
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	asociatividad \wedge
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	distributividad \wedge sobre \vee
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	de Morgan de \wedge
$p \wedge (p \vee q) \equiv p$	absorción de \wedge sobre \vee
$p \wedge \neg p \equiv false$	contradicción

Axiomas (Equivalencias)(1)

Verdadero, Falso y doble negación

Regla	Nombre
$\neg\neg p \equiv p$	doble negación
$false \equiv \neg true$	definición de false
$\neg false \equiv true$	negación de false

Axiomas de \wedge

Regla	Nombre
$p \wedge true \equiv p$	identidad de \wedge
$p \wedge false \equiv false$	dominación \wedge
$p \wedge p \equiv p$	idempotencia \wedge
$p \wedge q \equiv q \wedge p$	comutatividad \wedge
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	asociatividad \wedge
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	distributividad \wedge sobre \vee
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	de Morgan de \wedge
$p \wedge (p \vee q) \equiv p$	absorción de \wedge sobre \vee
$p \wedge \neg p \equiv false$	contradicción



Axiomas (Equivalencias)(2)

Axiomas de \vee

Regla	Nombre
$p \vee \text{false} \equiv p$	identidad \vee
$p \vee \text{true} \equiv \text{true}$	dominación \vee
$p \vee p \equiv p$	idempotencia \vee
$p \vee q \equiv q \vee p$	comutatividad \vee
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	asociatividad \vee
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributividad \vee sobre \wedge
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	de Morgan \vee
$p \vee (p \wedge q) \equiv p$	absorción \vee sobre \wedge
$p \vee \neg p \equiv \text{true}$	tautología (medio excluido)

Definición de \implies, \oplus, \equiv

Regla	Nombre
$p \implies q \equiv \neg p \vee q$	Definición \implies
$(p \equiv q) \equiv (p \implies q) \wedge (q \implies p)$	Definición \equiv
$p \oplus q \equiv \neg(p \equiv q)$	Definición \oplus

Axiomas (Equivalencias)(2)

Axiomas de \vee

Regla	Nombre
$p \vee \text{false} \equiv p$	identidad \vee
$p \vee \text{true} \equiv \text{true}$	dominación \vee
$p \vee p \equiv p$	idempotencia \vee
$p \vee q \equiv q \vee p$	comutatividad \vee
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	asociatividad \vee
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributividad \vee sobre \wedge
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	de Morgan \vee
$p \vee (p \wedge q) \equiv p$	absorción \vee sobre \wedge
$p \vee \neg p \equiv \text{true}$	tautología (medio excluido)

Definición de \implies, \oplus, \equiv

Regla	Nombre
$p \implies q \equiv \neg p \vee q$	Definición \implies
$(p \equiv q) \equiv (p \implies q) \wedge (q \implies p)$	Definición \equiv
$p \oplus q \equiv \neg(p \equiv q)$	Definición \oplus

Axiomas (Equivalencias)(3)

Más axiomas de \Rightarrow y \equiv

Regla	Nombre
$true \equiv (p \equiv p)$	Identidad \equiv
$(p \equiv q) \equiv (q \equiv p)$	Commutatividad \equiv
$((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$	Asociatividad \equiv
$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$	contrapositiva
$p \vee q \equiv \neg p \Rightarrow q$	Definición de \vee con \Rightarrow
$p \wedge q \equiv \neg(p \Rightarrow \neg q)$	Definición de \wedge con \Rightarrow
$\neg(p \Rightarrow q) \equiv p \wedge \neg q$	Negación de \Rightarrow
$(p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \Rightarrow (q \wedge r))$	Distributividad izquierda de \Rightarrow sobre \wedge
$(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow (q \vee r))$	Distributividad izquierda de \Rightarrow sobre \vee
$(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q) \Rightarrow r$	Distributividad derecha de \Rightarrow sobre \wedge (note que al distribuir se cambia \wedge por \vee)
$(p \Rightarrow r) \vee (q \Rightarrow r) \equiv (p \wedge q) \Rightarrow r$	Distributividad derecha de \Rightarrow sobre \wedge (note que al distribuir se cambia \vee por \wedge)
$p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q) \Rightarrow r$	Asociatividad izquierda de \Rightarrow (note que al asociar se cambia \Rightarrow por \wedge)
$p \equiv q \equiv \neg p \equiv \neg q$	Contrapositiva \equiv
$\neg(p \equiv q) \equiv \neg p \equiv q$	Negacion ₁ \equiv
$\neg(p \equiv q) \equiv p \equiv \neg q$	Negación ₂ \equiv
$p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$	Definición ₃ \equiv
$p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$	Definición ₂ \oplus

Reglas de inferencia

- Una **regla de inferencia** tiene la forma:

$$\langle \text{Identificador} \rangle \frac{\overbrace{\text{Hipótesis}}^{\langle \text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \rangle} \quad | \quad \langle \text{Condiciones} \rangle}{\underbrace{C}_{\text{Conclusión}}}$$

- $\text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \vdash C$
- Las reglas de inferencia no se demuestran, pero si se justifican:

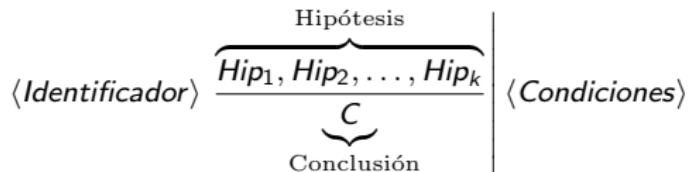
$$\text{Hip}_1 \wedge \text{Hip}_2 \wedge \dots \wedge \text{Hip}_k \implies C$$

es una tautología.

- $E[x := p]$ denota reemplazar en E todas las apariciones de x por p .
- **Deducir** es aplicar reglas.

Reglas de inferencia

- Una **regla de inferencia** tiene la forma:



- $\text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \vdash C$
- Las reglas de inferencia no se demuestran, pero si se justifican:

$$\text{Hip}_1 \wedge \text{Hip}_2 \wedge \dots \wedge \text{Hip}_k \implies C$$

es una tautología.

- $E[x := p]$ denota reemplazar en E todas las apariciones de x por p .
- **Deducir** es aplicar reglas.

Reglas de inferencia

- Una **regla de inferencia** tiene la forma:

$$\langle \text{Identificador} \rangle \frac{\overbrace{\text{Hipótesis}}^{\langle \text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \rangle} \quad | \quad \langle \text{Condiciones} \rangle}{\underbrace{C}_{\text{Conclusión}}}$$

- $\text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \vdash C$
- Las reglas de inferencia no se demuestran, pero si se justifican:

$$\text{Hip}_1 \wedge \text{Hip}_2 \wedge \dots \wedge \text{Hip}_k \implies C$$

es una tautología.

- $E[x := p]$ denota reemplazar en E todas las apariciones de x por p .
- **Deducir** es aplicar reglas.

Reglas de inferencia

- Una **regla de inferencia** tiene la forma:

$$\langle \text{Identificador} \rangle \frac{\overbrace{\text{Hipótesis}}^{\langle \text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \rangle} \quad | \quad \langle \text{Condiciones} \rangle}{\underbrace{C}_{\text{Conclusión}}}$$

- $\text{Hip}_1, \text{Hip}_2, \dots, \text{Hip}_k \vdash C$
- Las reglas de inferencia no se demuestran, pero si se justifican:

$$\text{Hip}_1 \wedge \text{Hip}_2 \wedge \dots \wedge \text{Hip}_k \implies C$$

es una tautología.

- $E[x := p]$ denota reemplazar en E todas las apariciones de x por p .
- **Deducir** es aplicar reglas.

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Reglas ecuacionales

- Las usaremos para demostrar **equivalencias**: $E \equiv F$

- Idea: $E = E_0 \overset{r_1}{\equiv} E_1 \overset{r_2}{\equiv} E_2 \dots \overset{r_{i-1}}{\equiv} E_{i-1} \overset{r_i}{\equiv} E_i \dots \overset{r_k}{\equiv} E_k = F$, donde r_1, \dots, r_k son las reglas usadas para justificar cada una de las equivalencias deducidas.
- Para que se lea fácil la prueba se presentará así:

Exp.	Regla (razón)
E_0	
\equiv	E_1
\equiv	r_1
E_2	
\vdots	\vdots
\vdots	\vdots
E_{i-1}	
\equiv	r_{i-1}
E_i	
\vdots	\vdots
\vdots	\vdots
E_k	
\equiv	r_k

- r_i justifica la equivalencia $E_{i-1} \equiv E_i$. Es un axioma o una regla o, a veces, varias reglas que se pueden aplicar en un paso sin generar confusión

Reglas ecuacionales

- Las usaremos para demostrar **equivalencias**: $E \equiv F$

- Idea: $E = E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k = F$, donde r_1, \dots, r_k son las reglas usadas para justificar cada una de las equivalencias deducidas.
- Para que se lea fácil la prueba se presentará así:

Exp.	Regla (razón)
E_0	
\equiv	E_1
\equiv	r_1
E_2	
\vdots	\vdots
\vdots	\vdots
E_{i-1}	
\equiv	r_{i-1}
E_i	
\vdots	\vdots
\vdots	\vdots
E_k	
\equiv	r_k

- r_i justifica la equivalencia $E_{i-1} \equiv E_i$. Es un axioma o una regla o, a veces, varias reglas que se pueden aplicar en un paso **sin generar confusión**

Reglas ecuacionales

- Las usaremos para demostrar **equivalencias**: $E \equiv F$

- Idea: $E = E_0 \stackrel{r_1}{\equiv} E_1 \stackrel{r_2}{\equiv} E_2 \dots \stackrel{r_{i-1}}{\equiv} E_{i-1} \stackrel{r_i}{\equiv} E_i \dots \stackrel{r_k}{\equiv} E_k = F$, donde r_1, \dots, r_k son las reglas usadas para justificar cada una de las equivalencias deducidas.
- Para que se lea fácil la prueba se presentará así:

Exp.	Regla (razón)
E_0	
$\equiv E_1$	r_1
$\equiv E_2$	r_2
\vdots	\vdots
$\equiv E_{i-1}$	r_{i-1}
$\equiv E_i$	r_i
\vdots	\vdots
$\equiv E_k$	r_k

- r_i justifica la equivalencia $E_{i-1} \equiv E_i$. Es un axioma o una regla o, a veces, varias reglas que se pueden aplicar en un paso **sin generar confusión**

Reglas ecuacionales

- Las usaremos para demostrar **equivalencias**: $E \equiv F$

- Idea: $E = E_0 \stackrel{r_1}{\equiv} E_1 \stackrel{r_2}{\equiv} E_2 \dots \stackrel{r_{i-1}}{\equiv} E_{i-1} \stackrel{r_i}{\equiv} E_i \dots \stackrel{r_k}{\equiv} E_k = F$, donde r_1, \dots, r_k son las reglas usadas para justificar cada una de las equivalencias deducidas.
- Para que se lea fácil la prueba se presentará así:

Exp.	Regla (razón)
E_0	
\equiv	E_1
\equiv	r_1
E_2	
\equiv	r_2
⋮	⋮
⋮	⋮
E_{i-1}	
\equiv	r_{i-1}
E_i	
\equiv	r_i
⋮	⋮
⋮	⋮
E_k	
\equiv	r_k

- r_i justifica la equivalencia $E_{i-1} \equiv E_i$. Es un axioma o una regla o, a veces, varias reglas que se pueden aplicar en un paso **sin generar confusión**

Reglas ecuacionales (2)

- ⟨Reflexividad- \equiv ⟩: $\frac{p \equiv p}{\text{true}}$

- ⟨Simetría- \equiv ⟩: $\frac{p \equiv q}{q \equiv p}$

Es la que permite concluir que $E \equiv F$ si

$$F = E_0 \equiv E_1 \equiv \dots \equiv E_k = E$$

- ⟨Transitividad- \equiv ⟩: $\frac{p \equiv q, q \equiv r}{p \equiv r}$

Es la que permite concluir que $E \equiv F$ si

$$E = E_0 \equiv E_1 \equiv \dots \equiv E_k = F$$

Reglas ecuacionales (2)

- ⟨Reflexividad- \equiv ⟩: $\frac{p \equiv p}{\text{true}}$
- ⟨Simetría- \equiv ⟩: $\frac{p \equiv q}{q \equiv p}$

Es la que permite concluir que $E \equiv F$ si

$$F = E_0 \equiv E_1 \equiv \dots \equiv E_k = E$$

- ⟨Transitividad- \equiv ⟩: $\frac{p \equiv q, q \equiv r}{p \equiv r}$

Es la que permite concluir que $E \equiv F$ si

$$E = E_0 \equiv E_1 \equiv \dots \equiv E_k = F$$

Reglas ecuacionales (2)

- ⟨Reflexividad- \equiv ⟩: $\frac{p \equiv p}{\text{true}}$
- ⟨Simetría- \equiv ⟩: $\frac{p \equiv q}{q \equiv p}$

Es la que permite concluir que $E \equiv F$ si

$$F = E_0 \equiv E_1 \equiv \dots \equiv E_k = E$$

- ⟨Transitividad- \equiv ⟩: $\frac{p \equiv q, q \equiv r}{p \equiv r}$

Es la que permite concluir que $E \equiv F$ si

$$E = E_0 \equiv E_1 \equiv \dots \equiv E_k = F$$

Regla de sustitución

- **(Sustitución):** $\frac{E}{E[x:=p]}$ | p : proposición
 E : Expresión proposicional
- Si $E = x \vee (\neg x \wedge \text{true})$ entonces

$$E[x := (q \implies \neg s)] = (q \implies \neg s) \vee (\neg(q \implies \neg s) \wedge \text{true})$$

Regla de sustitución

- **(Sustitución):** $\frac{E}{E[x:=p]}$ | p : proposición
 E : Expresión proposicional
- Si $E = x \vee (\neg x \wedge \text{true})$ entonces

$$E[x := (q \implies \neg s)] = (q \implies \neg s) \vee (\neg(q \implies \neg s) \wedge \text{true})$$

Regla de Leibniz

- **(Leibniz)**:
$$\frac{E_1 \equiv E_2}{E[x:=E_1] \equiv E[x:=E_2]} \quad | \quad \begin{array}{l} E_1, E_2: \text{proposiciones} \\ E: \text{Expresión proposicional sobre } x \end{array}$$
- Intuitivamente: se pueden **reemplazar iguales por iguales**.
- Si $E = \underbrace{\neg(p \wedge q)}_x \vee (p \vee q)$ y $\underbrace{\neg(p \wedge q)}_{E_1} \equiv \underbrace{\neg p \vee \neg q}_{E_2}$ entonces
$$\neg(p \wedge q) \vee (p \vee q) \equiv (\neg p \vee \neg q) \vee (p \vee q)$$

Regla de Leibniz

- $\langle \text{Leibniz} \rangle: \frac{E_1 \equiv E_2}{E[x:=E_1] \equiv E[x:=E_2]} \quad | \quad E_1, E_2: \text{proposiciones}$
 $E: \text{Expresión proposicional sobre } x$
- Intuitivamente: se pueden **reemplazar iguales por iguales.**
- Si $E = \underbrace{\neg(p \wedge q)}_x \vee (p \vee q)$ y $\underbrace{\neg(p \wedge q)}_{E_1} \equiv \underbrace{\neg p \vee \neg q}_{E_2}$ entonces
 $\neg(p \wedge q) \vee (p \vee q) \equiv (\neg p \vee \neg q) \vee (p \vee q)$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- **Ejemplos de demostración con equivalencias**

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Analogía con la aritmética

Demostrar que $a^2 - b^2 = (a + b) * (a - b)$

Teo: $a^2 - b^2 = (a + b) * (a - b)$

Dem:

$$\begin{aligned} & (a + b) * (a - b) \\ = & a * (a - b) + b * (a - b) \quad \text{Distributividad} \\ = & a * a - a * b + b * a - b * b \quad \text{Distributividad} \\ = & a^2 - a * b + b * a - b^2 \quad \text{Definición de } x^2 \\ = & a^2 + a * b - a * b - b^2 \quad \text{Commutatividad } * \text{ y } + \\ = & a^2 + 0 - b^2 \quad \text{Teorema } x - x = 0 \\ = & a^2 - b^2 \quad \text{Teorema } x + 0 = 0 \end{aligned}$$



Esquema de demostración: *Video1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overset{r_1}{\overbrace{\equiv}} E_1 \overset{r_2}{\overbrace{\equiv}} E_2 \dots \overset{r_{i-1}}{\overbrace{\equiv}} E_{i-1} \overset{r_i}{\overbrace{\equiv}} E_i \dots \overset{r_k}{\overbrace{\equiv}} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_0 es un teorema ($\alpha \vdash \alpha \equiv \text{true}$); o
- $E_0 = \alpha$ y E_0 es un teorema ($\alpha \vdash \alpha \equiv \text{false}$); o
- $E_0 = \alpha$ y E_0 es una constante ($\alpha \vdash \alpha \equiv \text{const}$); o
- $E_0 = \alpha$ y E_0 es una variable ($\alpha \vdash \alpha \equiv \text{var}$); o
- $E_0 = \alpha$ y E_0 es una fórmula ($\alpha \vdash \alpha \equiv \text{formula}$); o

- La información asociada a la razón r_i debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{i-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video 1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
- $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
- $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
- $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
- La información asociada a la razón r_j debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{j-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video 1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
- $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
- $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
- $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
- La información asociada a la razón r_j debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{j-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
 - $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
 - $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
 - $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
-
- La información asociada a la razón r_i debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{i-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
 - $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
 - $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
 - $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
- La información asociada a la razón r_i debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{i-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video 1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overbrace{\equiv}^{r_1} E_1 \overbrace{\equiv}^{r_2} E_2 \dots \overbrace{\equiv}^{r_{i-1}} E_{i-1} \overbrace{\equiv}^{r_i} E_i \dots \overbrace{\equiv}^{r_k} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
 - $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
 - $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
 - $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
- La información asociada a la razón r_i debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{i-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

Esquema de demostración: *Video1.4*

- Sea $\alpha = E \equiv F$. Se quiere demostrar $\vdash \alpha$.
- La secuencia

$$E_0 \overset{r_1}{\equiv} E_1 \overset{r_2}{\equiv} E_2 \dots \overset{r_{i-1}}{\equiv} E_{i-1} \overset{r_i}{\equiv} E_i \dots \overset{r_k}{\equiv} E_k$$

es una **demostración de α** si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \dots \equiv \text{true}$); o
- $E_k = \alpha$ y E_0 es un teorema ($\text{true} \equiv \dots \equiv \alpha$); o
- $E = E_0$ y $E_k = F$ ($E \equiv \dots \equiv F$); o
- $F = E_0$ y $E_k = E$ ($F \equiv \dots \equiv E$)
- La información asociada a la razón r_i debe contener (en lo posible):
 - identificador de la regla de inferencia o del teorema que se aplica
 - enunciado de la regla de inferencia o del teorema que se aplica
 - parte de la fórmula E_{i-1} sobre la que se aplica el teorema o la regla de inferencia
 - sustitución de variables (del teorema o de la regla de inferencia)

$p \wedge q \implies p \vee q$: *Video 1.4*

Teo: $p \wedge q \implies p \vee q$

Dem:

$$\begin{aligned} & p \wedge q \implies p \vee q \\ \equiv & \neg(p \wedge q) \vee (p \vee q) && \text{Definición de } \implies \\ \equiv & \neg p \vee \neg q \vee p \vee q && \text{De Morgan } \wedge, \text{ Simplificación} \\ \equiv & p \vee \neg p \vee q \vee \neg q && \text{Comutatividad } \vee, \text{ varias veces} \\ \equiv & \text{true} \vee q \vee \neg q && \text{Medio excluido } \vee \\ \equiv & \text{true} && \text{Dominación } \vee \end{aligned}$$

◊

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

Teo: $p \wedge (\neg q \implies p) \equiv p$

Dem:

$$\begin{aligned} & p \wedge (\neg q \implies p) \equiv p \\ \equiv & p \wedge (\neg \neg q \vee p) \equiv p && \text{Definición de } \implies \\ \equiv & p \wedge (q \vee p) \equiv p && \text{Doble negación} \\ \equiv & \underbrace{p \wedge (p \vee q)}_{\text{Teorema absorción}} \equiv p && \text{Comutatividad } \vee \end{aligned}$$



$p \wedge (\neg q \implies p) \equiv p$, otra demostración (*Video 1.5*)

Teo: $p \wedge (\neg q \implies p) \equiv p$

Dem:

$$\begin{aligned} & p \wedge (\neg q \implies p) \\ \equiv & p \wedge (\neg \neg q \vee p) && \text{Definición de } \implies \\ \equiv & p \wedge (q \vee p) && \text{Doble negación} \\ \equiv & p \wedge (p \vee q) && \text{Comutatividad } \vee \\ \equiv & p && \text{absorción } \wedge \\ & & \diamondsuit & \end{aligned}$$

$$\neg p \implies q \equiv p \vee q$$

Teo: $\neg p \implies q \equiv p \vee q$

Dem:

$$\begin{aligned} & \neg p \implies q \\ \equiv & \quad \neg\neg p \vee q \\ \equiv & \quad p \vee q \end{aligned}$$

Definición de \implies
Doble negación

◊

Ejercicio en clase

[Socrative]

Demuestre que

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

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

• Lemas

- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Lemas

- La justificación de un paso en la demostración de un teorema α puede requerir usar un teorema β que no está en la lista de teoremas conocidos.
- Se hace necesario demostrar β para demostrar α :

Lema: β

Dem:

...

Teo: α

Dem:

E_0

$\equiv E_1 r_1$

$\equiv E_2 r_2$

.

.

$\equiv E_{i-1} \beta$

$\equiv E_i r_i$

.

.

$\equiv E_k r_k$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- **El metateorema de la deducción**
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

El metateorema de la deducción

- Es un teorema que relaciona **deducción** con **implicación** (es decir aparato deductivo y semántica):

$$\alpha_1, \dots, \alpha_k \vdash \beta \text{ si y solo si } \vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$$

- Modo de uso: Si le piden demostrar

$$\vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$$

basta con demostrar

$$\beta$$

suponiendo las hipótesis

$$\alpha_1, \dots, \alpha_k$$

como fórmulas válidas o teoremas.

- Demostrar $p \wedge q \implies p \vee q$.

Teo: $p \wedge q \implies p \vee q$

Hip: p, q

Dem:

$$p \vee q$$

$$\equiv \text{true} \vee q$$

$$\equiv \text{true}$$

// A demostrar $p \vee q$

Hipótesis p

Dominación y Comutatividad \vee



El metateorema de la deducción

- Es un teorema que relaciona **deducción** con **implicación** (es decir aparato deductivo y semántica):
 $\alpha_1, \dots, \alpha_k \vdash \beta$ si y solo si $\vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$

- Modo de uso:** Si le piden demostrar

$$\vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$$

basta con demostrar

$$\beta$$

suponiendo las hipótesis

$$\alpha_1, \dots, \alpha_k$$

como fórmulas válidas o teoremas.

- Demostrar $p \wedge q \implies p \vee q$.

Teo: $p \wedge q \implies p \vee q$

Hip: p, q

Dem:

$$p \vee q$$

$$\equiv \text{true} \vee q$$

$$\equiv \text{true}$$

// A demostrar $p \vee q$

Hipótesis p

Dominación y Comutatividad \vee



El metateorema de la deducción

- Es un teorema que relaciona **deducción** con **implicación** (es decir aparato deductivo y semántica):
 $\alpha_1, \dots, \alpha_k \vdash \beta$ si y solo si $\vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$

- Modo de uso:** Si le piden demostrar

$$\vdash \alpha_1 \wedge \dots \wedge \alpha_k \implies \beta$$

basta con demostrar

$$\beta$$

suponiendo las hipótesis

$$\alpha_1, \dots, \alpha_k$$

como fórmulas válidas o teoremas.

- Demostrar $p \wedge q \implies p \vee q$.

Teo: $p \wedge q \implies p \vee q$

Hip: p, q

Dem:

$$p \vee q$$

$$\equiv \text{true} \vee q$$

$$\equiv \text{true}$$

// A demostrar $p \vee q$

Hipótesis p

Dominación y Comutatividad \vee



Relajación esquema de pruebas (1) (*Video 1.6*)

- Usando el teorema de la deducción se puede probar que:

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

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

$$\vdash ((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$$

- Esto da lugar a tres reglas de inferencia **no ecuacionales**:

$$p \Rightarrow q, q \equiv r \vdash p \Rightarrow r$$

$$p \equiv q, q \Rightarrow r \vdash p \Rightarrow r$$

$$p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$$

Relajación esquema de pruebas (1) (*Video 1.6*)

- Usando el teorema de la deducción se puede probar que:

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

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

$$\vdash ((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$$

- Esto da lugar a tres reglas de inferencia **no ecuacionales**:

$$p \Rightarrow q, q \equiv r \vdash p \Rightarrow r$$

$$p \equiv q, q \Rightarrow r \vdash p \Rightarrow r$$

$$p \Rightarrow q, q \Rightarrow r \vdash p \Rightarrow r$$

Relajación esquema de pruebas (2) (*Video 1.6*)

- Ahora una prueba puede tener la forma:

Exp.	Regla (razón)
E_0	
(\equiv, \implies)	E_1
(\equiv, \implies)	r_1
⋮	⋮
(\equiv, \implies)	E_2
⋮	⋮
(\equiv, \implies)	E_{i-1}
(\equiv, \implies)	r_{i-1}
⋮	⋮
(\equiv, \implies)	E_i
⋮	⋮
(\equiv, \implies)	r_i
⋮	⋮
(\equiv, \implies)	E_k
	r_k

en cuyo caso el teorema demostrado es

$$E_0 \implies E_k$$

Nótese que la prueba ya no es ecuacional.

- Una forma de demostrar $E \equiv F$ es demostrando $E \implies F$ y $F \implies E$

Relajación esquema de pruebas (2) (*Video 1.6*)

- Ahora una prueba puede tener la forma:

Exp.		Regla (razón)
E_0		
(\equiv, \implies)	E_1	r_1
(\equiv, \implies)	E_2	r_2
⋮	⋮	⋮
(\equiv, \implies)	E_{i-1}	r_{i-1}
(\equiv, \implies)	E_i	r_i
⋮	⋮	⋮
(\equiv, \implies)	E_k	r_k

en cuyo caso el teorema demostrado es

$$E_0 \implies E_k$$

Nótese que la prueba ya no es ecuacional.

- Una forma de demostrar $E \equiv F$ es demostrando $E \implies F$ y $F \implies E$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- **Debilitamiento/Fortalecimiento**
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Debilitamiento/Fortalecimiento: más reglas no ecuacionales

- Si $\alpha \implies \beta$ es válida, se dice que β es más débil que α o que α es más fuerte que β
- Otros teoremas con la implicación:

$$\vdash p \implies p \vee q$$

$$\vdash p \wedge q \implies p$$

$$\vdash p \wedge q \implies p \vee q$$

$$\vdash p \vee (q \wedge r) \implies p \vee q$$

$$\vdash p \wedge q \implies p \wedge (q \vee r)$$

- dan lugar a otras reglas de inferencia **no ecuacionales**:

$$p \vdash p \vee q$$

$$p \wedge q \vdash p$$

$$p \wedge q \vdash p \vee q$$

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

$$p, q \vdash p \wedge (q \vee r)$$

Debilitamiento/Fortalecimiento: más reglas no ecuacionales

- Si $\alpha \implies \beta$ es válida, se dice que β es más débil que α o que α es más fuerte que β
- Otros teoremas con la implicación:

$$\vdash p \implies p \vee q$$

$$\vdash p \wedge q \implies p$$

$$\vdash p \wedge q \implies p \vee q$$

$$\vdash p \vee (q \wedge r) \implies p \vee q$$

$$\vdash p \wedge q \implies p \wedge (q \vee r)$$

- dan lugar a otras reglas de inferencia **no ecuacionales**:

$$p \vdash p \vee q$$

$$p \wedge q \vdash p$$

$$p \wedge q \vdash p \vee q$$

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

$$p, q \vdash p \wedge (q \vee r)$$

Debilitamiento/Fortalecimiento: más reglas no ecuacionales

- Si $\alpha \implies \beta$ es válida, se dice que β es más débil que α o que α es más fuerte que β
- Otros teoremas con la implicación:

$$\vdash p \implies p \vee q$$

$$\vdash p \wedge q \implies p$$

$$\vdash p \wedge q \implies p \vee q$$

$$\vdash p \vee (q \wedge r) \implies p \vee q$$

$$\vdash p \wedge q \implies p \wedge (q \vee r)$$

- dan lugar a otras reglas de inferencia **no ecuacionales**:

$$p \vdash p \vee q$$

$$p \wedge q \vdash p$$

$$p \wedge q \vdash p \vee q$$

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

$$p, q \vdash p \wedge (q \vee r)$$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- **Modus Ponens**
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Modus Ponens

- Otro teorema muy conocido de la implicación:

$$p \wedge (p \implies q) \implies q$$

- da lugar a una regla muy conocida: **Modus Ponens**:

$$\langle \text{Modus Ponens} \rangle p, p \implies q \vdash q$$

Modus Ponens

- Otro teorema muy conocido de la implicación:

$$p \wedge (p \implies q) \implies q$$

- da lugar a una regla muy conocida: **Modus Ponens**:

$$\langle \text{Modus Ponens} \rangle p, p \implies q \vdash q$$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos**
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Prueba por casos

- Recuerde el axioma de **Distributividad derecha de \Rightarrow sobre \wedge** :

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

- Si $q = \neg p$: $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv ((p \vee \neg p) \Rightarrow r) \equiv (\text{true} \Rightarrow r) \equiv r$
 Por tanto, para demostrar r se puede proceder por casos así:

Caso 1: Demostrar $p \Rightarrow r$

Caso 2: Demostrar $\neg p \Rightarrow r$

- En general se puede usar el esquema de prueba siguiente:

Teo: r

Dem:

Casos: p_1, \dots, p_m

Demostración de $p_1 \vee \dots \vee p_m$ (si no es obvio)

Caso 1:

Demostración de $p_1 \Rightarrow r$

⋮

⋮

⋮

Caso m:

Demostración de $p_m \Rightarrow r$



Prueba por casos

- Recuerde el axioma de **Distributividad derecha de \Rightarrow sobre \wedge** :

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

- Si $q = \neg p$: $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv ((p \vee \neg p) \Rightarrow r) \equiv (\text{true} \Rightarrow r) \equiv r$
 Por tanto, para demostrar r se puede proceder por casos así:

Caso 1: Demostrar $p \Rightarrow r$

Caso 2: Demostrar $\neg p \Rightarrow r$

- En general se puede usar el esquema de prueba siguiente:

Teo: r

Dem:

Casos: p_1, \dots, p_m

Demostración de $p_1 \vee \dots \vee p_m$ (si no es obvio)

Caso 1:

Demostración de $p_1 \Rightarrow r$

⋮

⋮

⋮

Caso m:

Demostración de $p_m \Rightarrow r$



Prueba por casos

- Recuerde el axioma de **Distributividad derecha de \Rightarrow sobre \wedge** :

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

- Si $q = \neg p$: $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv ((p \vee \neg p) \Rightarrow r) \equiv (\text{true} \Rightarrow r) \equiv r$
 Por tanto, para demostrar r se puede proceder por casos así:

Caso 1: Demostrar $p \Rightarrow r$

Caso 2: Demostrar $\neg p \Rightarrow r$

- En general se puede usar el esquema de prueba siguiente:

Teo: r

Dem:

Casos: p_1, \dots, p_m

Demostración de $p_1 \vee \dots \vee p_m$ (si no es obvio)

Caso 1:

Demostración de $p_1 \Rightarrow r$

⋮ ⋮ ⋮

Caso m:

Demostración de $p_m \Rightarrow r$

Plan

1 Motivación

2 Axiomas

3 Reglas de inferencia

- Reglas de inferencia ecuacional, sustitución y Leibniz
- Ejemplos de demostración con equivalencias

4 Otras formas de demostración

- Lemas
- El metateorema de la deducción
- Debilitamiento/Fortalecimiento
- Modus Ponens
- Prueba por casos
- Pruebas por contrarecíproca y contradicción

5 Ejemplos de demostraciones

Pruebas por contrarecíproca y contradicción

Contrarecíproca: $(p \implies q) \equiv (\neg q \implies \neg p)$

Cuando no se sabe cómo deducir q a partir de p , el camino puede ser deducir $\neg p$ a partir de $\neg q$.

Teo: $p \implies q$

Hip: $\neg q$ // A demostrar $\neg p$

Demostración de $\neg p$

◊

Contradicción: $\neg p \implies \text{false} \equiv (\neg \text{false} \implies \neg \neg p) \equiv (\text{true} \implies p) \equiv p$

Cuando no se sabe cómo deducir p , el camino puede ser deducir $\neg p \implies \text{false}$ es decir deducir **una contradicción** a partir de $\neg p$.

Teo: r

Hip: $\neg r$

Demostración de *false*

◊



Pruebas por contrarecíproca y contradicción

Contrarecíproca: $(p \implies q) \equiv (\neg q \implies \neg p)$

Cuando no se sabe cómo deducir q a partir de p , el camino puede ser deducir $\neg p$ a partir de $\neg q$.

Teo: $p \implies q$

Hip: $\neg q$ // A demostrar $\neg p$

Demostración de $\neg p$

◊

Contradicción: $\neg p \implies \text{false} \equiv (\neg \text{false} \implies \neg \neg p) \equiv (\text{true} \implies p) \equiv p$

Cuando no se sabe cómo deducir p , el camino puede ser deducir $\neg p \implies \text{false}$ es decir deducir **una contradicción** a partir de $\neg p$.

Teo: r

Hip: $\neg r$

Demostración de *false*

◊



Recuerden el ejemplo: ¿Superman existe? ([Video 1.7](#))

Considere el siguiente razonamiento:

Si Supermán fuera capaz y quisiera prevenir el mal, él lo prevendría.

Si Supermán fuera incapaz de prevenir el mal, sería impotente; si él no quisiera prevenir el mal, sería malévolο.

Supermán no previene el mal.

Si Supermán existe, no es impotente ni malévolο.

Entonces, Supermán no existe.

- Variables proposicionales:

a: Supermán es capaz de prevenir el mal w: Supermán quiere prevenir el mal p: Supermán previene el mal

i: Supermán es impotente m: Supermán es malévolο

e: Supermán existe

- Traducción:

$p_0: a \wedge w \Rightarrow p$ $p_1: (\neg a \Rightarrow i) \wedge (\neg w \Rightarrow m)$

$p_2: \neg p$ $p_3: e \Rightarrow \neg i \wedge \neg m$

$p_4: \neg e$

$A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \Rightarrow p_4$

- Deducir: $A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \Rightarrow p_4$ es demostrar $p_0, p_1, p_2, p_3 \vdash p_4$

Recuerden el ejemplo: ¿Superman existe? ([Video 1.7](#))

Considere el siguiente razonamiento:

Si Supermán fuera capaz y quisiera prevenir el mal, él lo prevendría.

Si Supermán fuera incapaz de prevenir el mal, sería impotente; si él no quisiera prevenir el mal, sería malévolο.

Supermán no previene el mal.

Si Supermán existe, no es impotente ni malévolο.

Entonces, Supermán no existe.

- Variables proposicionales:

a: Supermán es capaz de prevenir el mal w: Supermán quiere prevenir el mal p: Supermán previene el mal

i: Supermán es impotente m: Supermán es malévolο

e: Supermán existe

- Traducción:

$p_0: a \wedge w \Rightarrow p$ $p_1: (\neg a \Rightarrow i) \wedge (\neg w \Rightarrow m)$

$p_2: \neg p$ $p_3: e \Rightarrow \neg i \wedge \neg m$

$p_4: \neg e$

$A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \Rightarrow p_4$

- Deducir: $A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \Rightarrow p_4$ es demostrar $p_0, p_1, p_2, p_3 \vdash p_4$

Recuerden el ejemplo: ¿Superman existe? ([Video 1.7](#))

Considere el siguiente razonamiento:

Si Supermán fuera capaz y quisiera prevenir el mal, él lo prevendría.

Si Supermán fuera incapaz de prevenir el mal, sería impotente; si él no quisiera prevenir el mal, sería malévolο.

Supermán no previene el mal.

Si Supermán existe, no es impotente ni malévolο.

Entonces, Supermán no existe.

- Variables proposicionales:

a: Supermán es capaz de prevenir el mal w: Supermán quiere prevenir el mal p: Supermán previene el mal

i: Supermán es impotente m: Supermán es malévolο

e: Supermán existe

- Traducción:

$p_0: a \wedge w \implies p$ $p_1: (\neg a \implies i) \wedge (\neg w \implies m)$

$p_2: \neg p$ $p_3: e \implies \neg i \wedge \neg m$

$p_4: \neg e$

$A : p_0 \wedge p_1 \wedge p_2 \wedge p_3 \implies p_4$

- Deducir: $A : p_0 \wedge p_1 \wedge p_2 \wedge p_3 \implies p_4$ es demostrar $p_0, p_1, p_2, p_3 \vdash p_4$



Recuerden el ejemplo: ¿Superman existe? ([Video 1.7](#))

Considere el siguiente razonamiento:

Si Supermán fuera capaz y quisiera prevenir el mal, él lo prevendría.

Si Supermán fuera incapaz de prevenir el mal, sería impotente; si él no quisiera prevenir el mal, sería malévolο.

Supermán no previene el mal.

Si Supermán existe, no es impotente ni malévolο.

Entonces, Supermán no existe.

- Variables proposicionales:
 - a: Supermán es capaz de prevenir el mal w: Supermán quiere prevenir el mal p: Supermán previene el mal
 - i: Supermán es impotente m: Supermán es malévolο
 - e: Supermán existe
- Traducción:
 - $p_0: a \wedge w \implies p$ $p_1: (\neg a \implies i) \wedge (\neg w \implies m)$
 - $p_2: \neg p$ $p_3: e \implies \neg i \wedge \neg m$
 - $p_4: \neg e$
 - $A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \implies p_4$
- Deducir: $A: p_0 \wedge p_1 \wedge p_2 \wedge p_3 \implies p_4$ es demostrar $p_0, p_1, p_2, p_3 \vdash p_4$

$p_0, p_1, p_2, p_3 \vdash p_4 \text{ (1) } (\text{Video 1.7})$

$$\begin{array}{ll} p_0: a \wedge w \implies p & p_1: (\neg a \implies i) \wedge (\neg w \implies m) \\ p_2: \neg p & p_3: e \implies \neg i \wedge \neg m \\ & p_4: \neg e \end{array}$$

Intuición

- Hay que llegar a $\neg e$
- La contrapositiva de p_3 serviría para esto:
 $\neg(\neg i \wedge \neg m) \implies \neg e$
- Necesitamos entonces demostrar $i \vee m$
- i se puede lograr de p_1 si tenemos $\neg a$
- m se puede lograr de p_1 si tenemos $\neg w$
- La contrapositiva de p_0 permitiría concluir $\neg a \vee \neg w$ si se tiene $\neg p$
- $\neg p$ es un hecho por p_2

Plan de la demostración

- Observar que $\neg p$ es un hecho por p_2
- Deducir $\neg a \vee \neg w$ por contrapositiva de p_0 y (DeMorgan)
- Usar esto con p_1 para deducir $i \vee m$
- Deducir $\neg e$ por contrapositiva de p_3

$p_0, p_1, p_2, p_3 \vdash p_4 \text{ (1) } (\text{Video 1.7})$

$$\begin{array}{ll} p_0: a \wedge w \implies p & p_1: (\neg a \implies i) \wedge (\neg w \implies m) \\ p_2: \neg p & p_3: e \implies \neg i \wedge \neg m \\ p_4: \neg e & \end{array}$$

Intuición

- Hay que llegar a $\neg e$
- La contrapositiva de p_3 serviría para esto:
 $\neg(\neg i \wedge \neg m) \implies \neg e$
- Necesitamos entonces demostrar $i \vee m$
- i se puede lograr de p_1 si tenemos $\neg a$
- m se puede lograr de p_1 si tenemos $\neg w$
- La contrapositiva de p_0 permitiría concluir $\neg a \vee \neg w$ si se tiene $\neg p$
- $\neg p$ es un hecho por p_2

Plan de la demostración

- Observar que $\neg p$ es un hecho por p_2
- Deducir $\neg a \vee \neg w$ por contrapositiva de p_0 y *(DeMorgan)*
- Usar esto con p_1 para deducir $i \vee m$
- Deducir $\neg e$ por contrapositiva de p_3

$p_0, p_1, p_2, p_3 \vdash p_4$ (2) (Video 1.7)

$$\begin{array}{ll} p_0: a \wedge w \implies p & p_1: (\neg a \implies i) \wedge (\neg w \implies m) \\ p_2: \neg p & p_3: e \implies \neg i \wedge \neg m \\ & p_4: \neg e \end{array}$$

$$L_0 : \neg p \implies (\neg a \vee \neg w)$$

Lema: $\neg p \implies (\neg a \vee \neg w)$

Hip: p_0, p_1, p_2, p_3

Dem:

true

$$\begin{array}{lll} \equiv & a \wedge w \implies p & \text{Hipótesis } p_0 \\ \equiv & \neg p \implies \neg(a \wedge w) & \langle \text{Contrapositiva} \rangle \\ \equiv & \neg p \implies \neg a \vee \neg w & \langle \text{DeMorgan} \rangle \\ & \diamond & \end{array}$$

$$L_1 : \neg a \vee \neg w$$

Lema: $\neg a \vee \neg w$

Hip: p_0, p_1, p_2, p_3

Dem:

true

$$\begin{array}{lll} \equiv & \neg p & \text{Hipótesis } p_2 \\ \implies & \neg a \vee \neg w & \langle L_0; \text{ModusPonens} \rangle \\ & \diamond & \end{array}$$

$p_0, p_1, p_2, p_3 \vdash p_4$ (2) (Video 1.7)

$$\begin{array}{ll} p_0: a \wedge w \implies p & p_1: (\neg a \implies i) \wedge (\neg w \implies m) \\ p_2: \neg p & p_3: e \implies \neg i \wedge \neg m \\ & p_4: \neg e \end{array}$$

$$L_0 : \neg p \implies (\neg a \vee \neg w)$$

Lema: $\neg p \implies (\neg a \vee \neg w)$

Hip: p_0, p_1, p_2, p_3

Dem:

true

$$\begin{array}{lll} \equiv & a \wedge w \implies p & \text{Hipótesis } p_0 \\ \equiv & \neg p \implies \neg(a \wedge w) & \langle \text{Contrapositiva} \rangle \\ \equiv & \neg p \implies \neg a \vee \neg w & \langle \text{DeMorgan} \rangle \\ & \diamond & \end{array}$$

$$L_1 : \neg a \vee \neg w$$

Lema: $\neg a \vee \neg w$

Hip: p_0, p_1, p_2, p_3

Dem:

true

$$\begin{array}{lll} \equiv & \neg p & \text{Hipótesis } p_2 \\ \implies & \neg a \vee \neg w & \langle L_0; \text{ModusPonens} \rangle \\ & \diamond & \end{array}$$

$p_0, p_1, p_2, p_3 \vdash p_4 \text{ (3) (Video 1.7)}$

$p_0: a \wedge w \implies p$ $p_1: (\neg a \implies i) \wedge (\neg w \implies m)$ $p_2: \neg p$ $p_3: e \implies \neg i \wedge \neg m$ $p_4: \neg e$

$L_2 : i \vee m$

Lema: $i \vee m$

Hip: $p_0, p_1, p_2, p_3, L_0, L_1$

Dem:

Casos: $\neg a, \neg w$

Demostración de $\neg a \vee \neg w$

$$\text{true} \equiv \neg a \vee \neg w \quad \langle L_1 \rangle$$

Caso: $\neg a$

Demostración de $\neg a \implies i \vee m$

$$\text{true}$$

$$\begin{aligned} \equiv & (\neg a \implies i) \\ & \wedge (\neg w \implies m) \quad \langle p_1 \rangle \end{aligned}$$

$$\begin{aligned} \implies & (\neg a \implies i) \quad \langle p \wedge q \implies q \rangle \\ \implies & (\neg a \implies (i \vee m)) \quad \langle p \implies p \vee q \rangle \end{aligned}$$

Caso: $\neg w$

Demostración de $\neg w \implies i \vee m$

$$\text{true}$$

$L_2 : i \vee m \text{ (cont)}$

$$\begin{aligned} \equiv & (\neg a \implies i) \\ & \wedge (\neg w \implies m) \quad \langle p_1 \rangle \\ \implies & (\neg w \implies m) \quad \langle p \wedge q \implies q \rangle \\ \implies & (\neg w \implies (m \vee i)) \quad \langle p \implies p \vee q \rangle \\ & \diamond \end{aligned}$$

Teorema: $\neg e$

Dem:

Hip: $p_0, p_1, p_2, p_3, L_0, L_1, L_2$
 true

$$\begin{aligned} \equiv & e \implies \neg i \wedge \neg m \quad \langle p_3 \rangle \\ \equiv & \neg(\neg i \wedge \neg m) \implies \neg e \quad \langle \text{Contrapositiva} \rangle \\ \equiv & i \vee m \implies \neg e \quad \langle \text{DeMorgan} \rangle \\ \implies & \neg e \\ & \diamond \end{aligned}$$

$p_0, p_1, p_2, p_3 \vdash p_4 \text{ (3) (Video 1.7)}$

$p_0: a \wedge w \implies p$ $p_1: (\neg a \implies i) \wedge (\neg w \implies m)$ $p_2: \neg p$ $p_3: e \implies \neg i \wedge \neg m$ $p_4: \neg e$

$L_2 : i \vee m$

Lema: $i \vee m$

Hip: $p_0, p_1, p_2, p_3, L_0, L_1$

Dem:

Casos: $\neg a, \neg w$

Demostración de $\neg a \vee \neg w$

$$\text{true} \equiv \neg a \vee \neg w \quad \langle L_1 \rangle$$

Caso: $\neg a$

Demostración de $\neg a \implies i \vee m$

$$\text{true}$$

$$\equiv (\neg a \implies i) \\ \wedge (\neg w \implies m) \quad \langle p_1 \rangle$$

$$\implies (\neg a \implies i) \quad \langle p \wedge q \implies q \rangle$$

$$\implies (\neg a \implies (i \vee m)) \quad \langle p \implies p \vee q \rangle$$

Caso: $\neg w$

Demostración de $\neg w \implies i \vee m$

$$\text{true}$$

$L_2 : i \vee m \text{ (cont)}$

$$\begin{aligned} &\equiv (\neg a \implies i) \\ &\quad \wedge (\neg w \implies m) \quad \langle p_1 \rangle \\ &\implies (\neg w \implies m) \quad \langle p \wedge q \implies q \rangle \\ &\implies (\neg w \implies (m \vee i)) \quad \langle p \implies p \vee q \rangle \\ &\quad \diamond \end{aligned}$$

Teorema: $\neg e$

Dem:

Hip: $p_0, p_1, p_2, p_3, L_0, L_1, L_2$
 true

$$\begin{aligned} &\equiv e \implies \neg i \wedge \neg m \quad \langle p_3 \rangle \\ &\equiv \neg(\neg i \wedge \neg m) \implies \neg e \quad \langle \text{Contrapositiva} \rangle \\ &\equiv i \vee m \implies \neg e \quad \langle \text{DeMorgan} \rangle \\ &\implies \neg e \quad \langle L_2; MP \rangle \\ &\quad \diamond \end{aligned}$$

$p_0, p_1, p_2, p_3 \vdash p_4 \text{ (3) (Video 1.7)}$

$p_0: a \wedge w \implies p$ $p_1: (\neg a \implies i) \wedge (\neg w \implies m)$ $p_2: \neg p$ $p_3: e \implies \neg i \wedge \neg m$ $p_4: \neg e$

$L_2 : i \vee m$

Lema: $i \vee m$

Hip: $p_0, p_1, p_2, p_3, L_0, L_1$

Dem:

Casos: $\neg a, \neg w$

Demostración de $\neg a \vee \neg w$

$$\text{true} \equiv \neg a \vee \neg w \quad \langle L_1 \rangle$$

Caso: $\neg a$

Demostración de $\neg a \implies i \vee m$

$$\text{true}$$

$$\equiv (\neg a \implies i) \wedge (\neg w \implies m) \quad \langle p_1 \rangle$$

$$\begin{aligned} \implies & (\neg a \implies i) && \langle p \wedge q \implies q \rangle \\ \implies & (\neg a \implies (i \vee m)) && \langle p \implies p \vee q \rangle \end{aligned}$$

Caso: $\neg w$

Demostración de $\neg w \implies i \vee m$

$$\text{true}$$

$L_2 : i \vee m$ (cont)

$$\begin{aligned} \equiv & (\neg a \implies i) \\ & \wedge (\neg w \implies m) && \langle p_1 \rangle \\ \implies & (\neg w \implies m) && \langle p \wedge q \implies q \rangle \\ \implies & (\neg w \implies (m \vee i)) && \langle p \implies p \vee q \rangle \\ & & & \diamond \end{aligned}$$

Teorema: $\neg e$

Dem:

Hip: $p_0, p_1, p_2, p_3, L_0, L_1, L_2$

true

$$\begin{aligned} \equiv & e \implies \neg i \wedge \neg m && \langle p_3 \rangle \\ \equiv & \neg(\neg i \wedge \neg m) \implies \neg e && \langle \text{Contrapositiva} \rangle \\ \equiv & i \vee m \implies \neg e && \langle \text{DeMorgan} \rangle \\ \implies & \neg e && \langle L_2; MP \rangle \\ & & & \diamond \end{aligned}$$

Ejercicio en clase

Considere el siguiente razonamiento:

La policía le está siguiendo el rastro a un posible delincuente que usó el transmilenio para escaparse. De acuerdo a sus investigaciones la policía ha podido establecer que el delincuente tomó rutas que pasaron por las estaciones Aguas, ClI26, Prado y Virrey, donde el delincuente pudo bajarse o no. Y se sabe lo siguiente:

- 1 El delincuente se bajó en al menos una de esas estaciones.
- 2 El delincuente no se bajó en Virrey si se bajó antes en Aguas o ClI26.
- 3 Si el delincuente se bajó en Prado entonces también se bajó en Aguas
- 4 Si el delincuente no se bajó en Prado entonces tampoco se bajó en ClI26
- 5 El delincuente se bajó Prado y Virrey o no se bajó en ninguna de ellas.

Un policía de inteligencia concluyó que el delincuente sólo se bajó en Aguas. Demuéstre que esa conclusión es correcta

- Haga la demostración siguiendo los esquemas y reglas de la lógica proposicional
- [Socrative]

Ejercicio en clase

Considere el siguiente razonamiento:

La policía le está siguiendo el rastro a un posible delincuente que usó el transmilenio para escaparse. De acuerdo a sus investigaciones la policía ha podido establecer que el delincuente tomó rutas que pasaron por las estaciones Aguas, ClI26, Prado y Virrey, donde el delincuente pudo bajarse o no. Y se sabe lo siguiente:

- 1 El delincuente se bajó en al menos una de esas estaciones.
- 2 El delincuente no se bajó en Virrey si se bajó antes en Aguas o ClI26.
- 3 Si el delincuente se bajó en Prado entonces también se bajó en Aguas
- 4 Si el delincuente no se bajó en Prado entonces tampoco se bajó en ClI26
- 5 El delincuente se bajó Prado y Virrey o no se bajó en ninguna de ellas.

Un policía de inteligencia concluyó que el delincuente sólo se bajó en Aguas. Demuéstre que esa conclusión es correcta

- Haga la demostración siguiendo los esquemas y reglas de la lógica proposicional
- [Socrative]