Matemáticas Discretas I

Lógica proposicional - Aparato deductivo

Juan Francisco Díaz Frias

Profesor Titular (1993-hoy)
juanfco.diaz@correounivalle.edu.co
Edif. 331 - 2111
Universidad del Valle

Septiembre 2018

Plan

Plan

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 $\wedge$
$p \wedge q \equiv q \wedge p$	conmutatividad $\wedge$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	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 $\wedge$
$p \wedge q \equiv q \wedge p$	conmutatividad $\wedge$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	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
$p \vee false \equiv p$	identidad $\vee$
$p \vee true \equiv true$	dominación $\vee$
$p \vee p \equiv p$	idempotencia $\vee$
$p \vee q \equiv q \vee p$	conmutatividad $\vee$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	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 $\wedge$
$p \vee \neg p \equiv true$	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
$p \vee false \equiv p$	identidad $\vee$
$p \vee true \equiv true$	dominación $\vee$
$p \vee p \equiv p$	idempotencia $\vee$
$p \vee q \equiv q \vee p$	conmutatividad $\vee$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	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 $\wedge$
$p \vee \neg p \equiv true$	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 $\Longrightarrow$ y $\equiv$

Regla	Nombre
$true \equiv (p \equiv p)$	Identidad $\equiv$
$(p \equiv q) \equiv (q \equiv p)$	Conmutatividad $\equiv$
$((p \equiv q) \equiv r)) \equiv (p \equiv (q \equiv r))$	Asociatividad $\equiv$
$p \Longrightarrow q \equiv \neg q \Longrightarrow \neg p$	contrapositiva
$p \vee q \equiv \neg p \Longrightarrow q$	Definición de $\vee$ con $\Longrightarrow$
$p \wedge q \equiv \neg(p \Longrightarrow \neg q)$	Definición de $\wedge$ con $\Longrightarrow$
$\neg(p \Longrightarrow q) \equiv p \wedge \neg q$	Negación de $\Longrightarrow$
$(p \Longrightarrow q) \wedge (p \Longrightarrow r) \equiv (p \Longrightarrow (q \wedge r))$	Distributividad izquierda de $\Longrightarrow$ sobre $\wedge$
$(p \Longrightarrow q) \vee (p \Longrightarrow r) \equiv (p \Longrightarrow (q \vee r))$	Distributividad izquierda de $\Longrightarrow$ sobre $\vee$
$(p \Longrightarrow r) \wedge (q \Longrightarrow r) \equiv (p \vee q) \Longrightarrow r$	Distributividad derecha de $\Longrightarrow$ sobre $\wedge$ (note que al distribuir se cambia $\wedge$ por $\vee$)
$(p \Longrightarrow r) \vee (q \Longrightarrow r) \equiv (p \wedge q) \Longrightarrow r$	Distributividad derecha de $\Longrightarrow$ sobre $\wedge$ (note que al distribuir se cambia $\vee$ por $\wedge$)
$p \Longrightarrow (q \Longrightarrow r) \equiv (p \wedge q) \Longrightarrow r$	Asociatividad izquierda de $\Longrightarrow$ (note que al asociar se cambia $\Longrightarrow$ 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$_2$ $\equiv$
$p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$	Defnción$_3$ $\equiv$
$p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$	Defnción$_2 \oplus$

Reglas de inferencia

- Una regla de inferencia tiene la forma:

$$\langle Identificador \rangle \; \frac{\overbrace{Hip_1, Hip_2, \ldots, Hip_k}^{\text{Hipótesis}}}{\underbrace{C}_{\text{Conclusión}}} \Bigg| \; \langle Condiciones \rangle$$

  o

$$Hip_1, Hip_2, \ldots, Hip_k \vdash C$$

- Las reglas de inferencia no se demuestran, pero si se justifican:

$$Hip_1 \wedge Hip_2 \wedge \ldots \wedge Hip_k \implies C$$

  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:

$$\langle \mathit{Identificador} \rangle \; \frac{\overbrace{Hip_1, Hip_2, \ldots, Hip_k}^{\text{Hipótesis}}}{\underbrace{C}_{\text{Conclusión}}} \; \Bigg| \; \langle \mathit{Condiciones} \rangle$$

  o

$$Hip_1, Hip_2, \ldots, Hip_k \vdash C$$

- Las reglas de inferencia no se demuestran, pero si se justifican:

$$Hip_1 \wedge Hip_2 \wedge \ldots \wedge Hip_k \implies C$$

  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:

$$\langle Identificador \rangle \; \frac{\overbrace{Hip_1, Hip_2, \ldots, Hip_k}^{\text{Hipótesis}}}{\underbrace{C}_{\text{Conclusión}}} \Bigg| \; \langle Condiciones \rangle$$

  o

$$Hip_1, Hip_2, \ldots, Hip_k \vdash C$$

- Las reglas de inferencia no se demuestran, pero si se justifican:

$$Hip_1 \wedge Hip_2 \wedge \ldots \wedge Hip_k \implies C$$

  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:

$$\langle \mathit{Identificador} \rangle \; \left. \frac{\overbrace{Hip_1, Hip_2, \ldots, Hip_k}^{\text{Hipótesis}}}{\underbrace{C}_{\text{Conclusión}}} \right| \; \langle \mathit{Condiciones} \rangle$$

  o

$$Hip_1, Hip_2, \ldots, Hip_k \vdash C$$

- Las reglas de inferencia no se demuestran, pero si se justifican:

$$Hip_1 \wedge Hip_2 \wedge \ldots \wedge Hip_k \implies C$$

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

Plan

Reglas ecuacionales

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

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

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

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

- 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)

- $\langle$Reflexividad- $\equiv\rangle$: $\frac{p\equiv p}{true}$
- $\langle$Simetría- $\equiv\rangle$: $\frac{p\equiv q}{q\equiv p}$
  Es la que permite concluir que $E \equiv F$ si

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

- $\langle$Transitividad- $\equiv\rangle$: $\frac{p\equiv q, q\equiv r}{p\equiv r}$
  Es la que permite concluir que $E \equiv F$ si

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

Reglas ecuacionales (2)

- ⟨Reflexividad- $\equiv$⟩: $\frac{p \equiv p}{true}$
- ⟨Simetría- $\equiv$⟩: $\frac{p \equiv q}{q \equiv p}$
  Es la que permite concluir que $E \equiv F$ si
  $$F = E_0 \equiv E_1 \equiv \ldots \equiv E_k = E$$
- ⟨Transitividad- $\equiv$⟩: $\frac{p \equiv q, q \equiv r}{p \equiv r}$
  Es la que permite concluir que $E \equiv F$ si
  $$E = E_0 \equiv E_1 \equiv \ldots \equiv E_k = F$$

Reglas ecuacionales (2)

- $\langle$Reflexividad- $\equiv\rangle$: $\frac{p\equiv p}{true}$
- $\langle$Simetría- $\equiv\rangle$: $\frac{p\equiv q}{q\equiv p}$
  Es la que permite concluir que $E \equiv F$ si

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

- $\langle$Transitividad- $\equiv\rangle$: $\frac{p\equiv q, q\equiv r}{p\equiv r}$
  Es la que permite concluir que $E \equiv F$ si

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

Regla de sustitución

- ⟨Sustitución⟩: $\dfrac{E}{E[x{:=}p]}$ | p: proposición; E: Expresión proposicional
- Si $E = x \vee (\neg x \wedge true)$ entonces

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

Regla de sustitución

- ⟨Sustitución⟩: $\dfrac{E}{E[x{:=}p]}$ | p: proposición; E: Expresión proposicional
- Si $E = x \vee (\neg x \wedge true)$ entonces

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

Regla de Leibniz

- $\langle$Leibniz$\rangle$: $\dfrac{E_1 \equiv E_2}{E[x:=E_1] \equiv E[x:=E_2]}$ | E_1, E_2: proposiciones; E: 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

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

Regla de Leibniz

- $\langle$Leibniz$\rangle$: $\dfrac{E_1 \equiv E_2}{E[x:=E_1] \equiv E[x:=E_2]}$ E_1, E_2: proposiciones; E: 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

Analogía con la aritmética

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

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

Dem:

	$(a+b)*(a-b)$	
$=$	$a*(a-b)+b*(a-b))$	Distributividad
$=$	$a*a-a*b+b*a-b*b$	Distributividad
$=$	$a^2-a*b+b*a-b^2$	Definición de x^2
$=$	$a^2+a*b-a*b-b^2$	Conmutatividad $*$ y $+$
$=$	a^2+0-b^2	Teorema $x-x=0$
$=$	a^2-b^2	Teorema $x+0=0$
		$\diamond$

Esquema de demostración: *Video1.4*

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

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

es una demostración de α si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
- $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); 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: *Video1.4*

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

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

es una demostración de α si:

  - $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
  - $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
  - $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
  - $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)

- 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

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

es una demostración de α si:

- $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
- $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
- $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
- $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)

- 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

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

es una demostración de α si:

  - $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
  - $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
  - $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
  - $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)

- 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

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

  es una demostración de α si:

  - $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
  - $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
  - $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
  - $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)

- 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

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

  es una demostración de α si:

  - $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
  - $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
  - $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
  - $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)
- 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

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

es una demostración de α si:

  - $E_0 = \alpha$ y E_k es un teorema ($\alpha \equiv \ldots \equiv true$); o
  - $E_k = \alpha$ y E_0 es un teorema ($true \equiv \ldots \equiv \alpha$); o
  - $E = E_0$ y $E_k = F$ ($E \equiv \ldots \equiv F$); o
  - $F = E_0$ y $E_k = E$ ($F \equiv \ldots \equiv E$)

- 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)

$p \wedge q \implies p \vee q$: *Video1.4*

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

Dem:

	$p \wedge q \implies p \vee q$	
$\equiv$	$\neg(p \wedge q) \vee (p \vee q)$	Definición de $\implies$
$\equiv$	$\neg p \vee \neg q \vee p \vee q$	De Morgan $\wedge$, Simplificación
$\equiv$	$p \vee \neg p \vee q \vee \neg q$	Conmutatividad $\vee$, varias veces
$\equiv$	$true \vee q \vee \neg q$	Medio excluido $\vee$
$\equiv$	$true$	Dominación $\vee$

$\diamond$

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

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

Dem:

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

$\diamond$

$p \wedge (\neg q \implies p) \equiv p$, otra demostración (*Video1.5*)

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

Dem:

	$p \wedge (\neg q \implies p)$	
$\equiv$	$p \wedge (\neg\neg q \vee p)$	Definición de $\implies$
$\equiv$	$p \wedge (q \vee p)$	Doble negación
$\equiv$	$p \wedge (p \vee q)$	Conmutatividad $\vee$
$\equiv$	p	absorción $\wedge$
		$\diamond$

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

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

Dem:

	$\neg p \implies q$	
$\equiv$	$\neg\neg p \vee q$	Definición de $\implies$
$\equiv$	$p \vee q$	Doble negación

$\diamond$

Ejercicio en clase

[Socrative]

Demuestre que

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

Plan

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:

$$
\begin{array}{lll}
 & E_0 & \\
\equiv & E_1 & r_1 \\
\equiv & E_2 & r_2 \\
\vdots & \vdots & \vdots \\
\equiv & E_{i-1} & \beta \\
\equiv & E_i & r_i \\
\vdots & \vdots & \vdots \\
\equiv & E_k & r_k \\
 & & \diamond
\end{array}
$$

Plan

El metateorema de la deducción

- Es un teorema que relaciona deducción con implicación (es decir aparato deductivo y semántica):
  $\alpha_1, \ldots, \alpha_k \vdash \beta$ si y solo si $\vdash \alpha_1 \wedge \ldots \wedge \alpha_k \implies \beta$
- Modo de uso: Si le piden demostrar

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

  basta con demostrar

  $$\beta$$

  suponiendo las hipótesis

  $$\alpha_1, \ldots, \alpha_k$$

  como fórmulas válidas o teoremas.
- Demostrar $p \wedge q \implies p \vee q$.

Teo:	$p \wedge q \implies p \vee q$	
Hip:	p, q	// A demostrar $p \vee q$
Dem:		
	$p \vee q$	
$\equiv$	$true \vee q$	Hipótesis p
$\equiv$	$true$	Dominación y Conmutatividad $\vee$

$\diamond$

El metateorema de la deducción

- Es un teorema que relaciona deducción con implicación (es decir aparato deductivo y semántica):
  $\alpha_1, \ldots, \alpha_k \vdash \beta$ si y solo si $\vdash \alpha_1 \wedge \ldots \wedge \alpha_k \implies \beta$
- Modo de uso: Si le piden demostrar

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

  basta con demostrar

$$\beta$$

  suponiendo las hipótesis

$$\alpha_1, \ldots, \alpha_k$$

  como fórmulas válidas o teoremas.
- Demostrar $p \wedge q \implies p \vee q$.

Teo:	$p \wedge q \implies p \vee q$	
Hip:	p, q	// A demostrar $p \vee q$
Dem:		
	$p \vee q$	
$\equiv$	$true \vee q$	Hipótesis p
$\equiv$	$true$	Dominación y Conmutatividad $\vee$

$\diamond$

El metateorema de la deducción

- Es un teorema que relaciona deducción con implicación (es decir aparato deductivo y semántica):
  $\alpha_1, \ldots, \alpha_k \vdash \beta$ si y solo si $\vdash \alpha_1 \wedge \ldots \wedge \alpha_k \implies \beta$
- Modo de uso: Si le piden demostrar

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

  basta con demostrar

  $$\beta$$

  suponiendo las hipótesis

  $$\alpha_1, \ldots, \alpha_k$$

  como fórmulas válidas o teoremas.
- Demostrar $p \wedge q \implies p \vee q$.

Teo:	$p \wedge q \implies p \vee q$	
Hip:	p, q	// A demostrar $p \vee q$
Dem:		
	$p \vee q$	
$\equiv$	$true \vee q$	Hipótesis p
$\equiv$	$true$	Dominación y Conmutatividad $\vee$

$\diamond$

Relajación esquema de pruebas (1) (*Video1.6*)

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

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

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

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

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

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

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

$$p \implies q, q \implies r \vdash p \implies r$$

Relajación esquema de pruebas (1) (*Video1.6*)

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

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

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

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

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

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

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

$$p \implies q, q \implies r \vdash p \implies r$$

Relajación esquema de pruebas (2) (*Video1.6*)

- Ahora una prueba puede tener la forma:

$$
\begin{array}{lll}
 & \text{Exp.} & \text{Regla (razón)} \\
 & E_0 & \\
(\equiv, \Longrightarrow) & E_1 & r_1 \\
(\equiv, \Longrightarrow) & E_2 & r_2 \\
\vdots & \vdots & \vdots \\
(\equiv, \Longrightarrow) & E_{i-1} & r_{i-1} \\
(\equiv, \Longrightarrow) & E_i & r_i \\
\vdots & \vdots & \vdots \\
(\equiv, \Longrightarrow) & E_k & r_k
\end{array}
$$

  en cuyo caso el teorema demostrado es

$$E_0 \Longrightarrow E_k$$

  Nótese que la prueba ya no es ecuacional.

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

Relajación esquema de pruebas (2) (Video1.6)

- Ahora una prueba puede tener la forma:

$$
\begin{array}{lll}
 & \text{Exp.} & \text{Regla (razón)} \\
 & E_0 & \\
(\equiv, \implies) & E_1 & r_1 \\
(\equiv, \implies) & E_2 & r_2 \\
\vdots & \vdots & \vdots \\
(\equiv, \implies) & E_{i-1} & r_{i-1} \\
(\equiv, \implies) & E_i & r_i \\
\vdots & \vdots & \vdots \\
(\equiv, \implies) & E_k & r_k
\end{array}
$$

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 $F \implies G$

Plan

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

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

Prueba por casos

- Recuerde el axioma de Distributividad derecha de $\implies$ sobre $\wedge$:

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

- Si $q = \neg p$: $(p \implies r) \wedge (\neg p \implies r) \equiv ((p \vee \neg p) \implies r) \equiv (true \implies r) \equiv r$
  Por tanto, para demostrar r se puede proceder por casos así:
  Caso 1: Demostrar $p \implies r$ Caso 2: Demostrar $\neg p \implies r$
- En general se puede usar el esquema de prueba siguiente:

Teo: r
Dem:
Casos: $p_1, \ldots, p_m$
Demostración de $p_1 \vee \ldots \vee p_m$ (si no es obvio)
Caso 1:
Demostración de $p_1 \implies r$
⋮ ⋮ ⋮
Caso m:
Demostración de $p_m \implies r$
◇

Prueba por casos

- Recuerde el axioma de Distributividad derecha de $\implies$ sobre $\wedge$:

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

- Si $q = \neg p$: $(p \implies r) \wedge (\neg p \implies r) \equiv ((p \vee \neg p) \implies r) \equiv (true \implies r) \equiv r$
Por tanto, para demostrar r se puede proceder por casos así:
Caso 1: Demostrar $p \implies r$ Caso 2: Demostrar $\neg p \implies r$
- En general se puede usar el esquema de prueba siguiente:

Teo: r
Dem:
Casos: $p_1, \ldots, p_m$
Demostración de $p_1 \vee \ldots \vee p_m$ (si no es obvio)
Caso 1:
Demostración de $p_1 \implies r$
$\vdots$ $\vdots$ $\vdots$
Caso m:
Demostración de $p_m \implies r$
$\diamond$

Prueba por casos

- Recuerde el axioma de Distributividad derecha de $\implies$ sobre $\wedge$:

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

- Si $q = \neg p$: $(p \implies r) \wedge (\neg p \implies r) \equiv ((p \vee \neg p) \implies r) \equiv (true \implies r) \equiv r$
  Por tanto, para demostrar r se puede proceder por casos así:
  Caso 1: Demostrar $p \implies r$ Caso 2: Demostrar $\neg p \implies r$
- En general se puede usar el esquema de prueba siguiente:

Teo: r
Dem:
Casos: $p_1, \ldots, p_m$
Demostración de $p_1 \vee \ldots \vee p_m$ (si no es obvio)
Caso 1:
Demostración de $p_1 \implies r$
⋮ ⋮ ⋮
Caso m:
Demostración de $p_m \implies r$
◇

Plan

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 $\neg p$
$\diamond$

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

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

Teo: r
Hip: $\neg r$
Demostración de *false*
$\diamond$

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 $\neg p$
$\diamond$

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

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

Teo: r
Hip: $\neg r$
Demostración de *false*
$\diamond$

Recuerden el ejemplo: ¿Superman existe?(*Video1.7*)

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 malévolo.
Supermán no previene el mal.
Si Supermán existe, no es impotente ni malévolo.
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 malévolo
  e: Supermán existe
- Traducción:
  p_0: $a \wedge w \implies p$ $\quad p_1$: $(\neg a \implies i) \wedge (\neg w \implies m)$
  p_2: $\neg p$ $\quad p_3$: $e \implies \neg i \wedge \neg m$
  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?(*Video1.7*)

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 malévolo.
Supermán no previene el mal.
Si Supermán existe, no es impotente ni malévolo.
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 malévolo
  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?(*Video1.7*)

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 malévolo.
Supermán no previene el mal.
Si Supermán existe, no es impotente ni malévolo.
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 malévolo
  e: Supermán existe
- Traducción:
  p_0: $a \wedge w \implies p$ $\quad$ p_1: $(\neg a \implies i) \wedge (\neg w \implies m)$
  p_2: $\neg p$ $\quad$ 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?(*Video1.7*)

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 malévolo.
Supermán no previene el mal.
Si Supermán existe, no es impotente ni malévolo.
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 malévolo
  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 $p_0, p_1, p_2, p_3 \vdash p_4$

$p_0, p_1, p_2, p_3 \vdash p_4$ (1) (*Video1.7*)

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

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 $\langle DeMorgan \rangle$
- Usar esto con p_1 para deducir $i \vee m$
- Deducir $\neg e$ por contrapositiva de p_3

$p_0, p_1, p_2, p_3 \vdash p_4$ (1) (Video1.7)

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: $\neg e$

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 $\langle DeMorgan \rangle$
- 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) (Video1.7)

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: $\neg e$

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

Lema: $\neg p \implies (\neg a \vee \neg w)$
Hip: p_0, p_1, p_2, p_3
Dem:

	$true$	
$\equiv$	$a \wedge w \implies p$	Hipótesis p_0
$\equiv$	$\neg p \implies \neg(a \wedge w)$	$\langle Contrapositiva \rangle$
$\equiv$	$\neg p \implies \neg a \vee \neg w$	$\langle DeMorgan \rangle$
		$\diamond$

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

Lema: $\neg a \vee \neg w$
Hip: p_0, p_1, p_2, p_3
Dem:

	$true$	
$\equiv$	$\neg p$	Hipótesis p_2
$\implies$	$\neg a \vee \neg w$	$\langle L_0; ModusPonens \rangle$
		$\diamond$

$p_0, p_1, p_2, p_3 \vdash p_4$ (2) (Video1.7)

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: $\neg e$

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

Lema: $\neg p \implies (\neg a \vee \neg w)$
Hip: p_0, p_1, p_2, p_3
Dem:

	$true$	
$\equiv$	$a \wedge w \implies p$	Hipótesis p_0
$\equiv$	$\neg p \implies \neg(a \wedge w)$	$\langle Contrapositiva \rangle$
$\equiv$	$\neg p \implies \neg a \vee \neg w$	$\langle DeMorgan \rangle$
		$\diamond$

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

Lema: $\neg a \vee \neg w$
Hip: p_0, p_1, p_2, p_3
Dem:

	$true$	
$\equiv$	$\neg p$	Hipótesis p_2
$\implies$	$\neg a \vee \neg w$	$\langle L_0; ModusPonens \rangle$
		$\diamond$

$p_0, p_1, p_2, p_3 \vdash p_4$ (3) (*Video1.7*)

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 $\neg a \vee \neg w$

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

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

	$true$	
$\equiv$	$(\neg a \implies i)$	
	$\wedge(\neg w \implies m)$	$\langle p_1 \rangle$
$\implies$	$(\neg a \implies i)$	$\langle p \wedge q \implies q \rangle$
$\implies$	$(\neg a \implies (i \vee m))$	$\langle p \implies p \vee q \rangle$

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

$true$

$L_2 : i \vee m$ (cont)

$\equiv$	$(\neg a \implies i)$	
	$\wedge(\neg w \implies m)$	$\langle p_1 \rangle$
$\implies$	$(\neg w \implies m)$	$\langle p \wedge q \implies q \rangle$
$\implies$	$(\neg w \implies (m \vee i))$	$\langle p \implies p \vee q \rangle$

$\diamond$

Teorema: $\neg e$

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

	$true$	
$\equiv$	$e \implies \neg i \wedge \neg m$	$\langle p_3 \rangle$
$\equiv$	$\neg(\neg i \wedge \neg m) \implies \neg e$	$\langle Contrapositiva \rangle$
$\equiv$	$i \vee m \implies \neg e$	$\langle DeMorgan \rangle$
$\implies$	$\neg e$	$\langle L_2; MP \rangle$

$\diamond$

$p_0, p_1, p_2, p_3 \vdash p_4$ (3) (Video1.7)

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 $\neg a \vee \neg w$

$true \equiv \neg a \vee \neg w$ $\langle L_1 \rangle$

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

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

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

$true$

$L_2 : i \vee m$ (cont)

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

Teorema: $\neg e$

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

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

$p_0, p_1, p_2, p_3 \vdash p_4$ (3) (Video1.7)

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 $\neg a \vee \neg w$

$true \equiv \neg a \vee \neg w$ $\langle L_1 \rangle$

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

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

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

$true$

$L_2 : i \vee m$ (cont)

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

$\diamond$

Teorema: $\neg e$

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

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

$\diamond$

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 la estaciones Aguas, Cll26, 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 Cll26.*
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 Cll26*
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 la estaciones $Aguas$, $Cll26$, $Prado$ 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 $Cll26$.*
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 $Cll26$*
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]