Introducción a los Algoritmos - 2do. cuatrimestre 2012

Guía 4: Demostraciones en Cálculo Proposicional

Docentes: Walter Alini, Luciana Benotti, Marcos Gómez y Gisela Rossi.

El objetivo principal de esta guía es lograr un buen entrenamiento de las habilidades necesarias para realizar una demostración formal en un sistema lógico sencillo, el Cálculo Proposicional.

Cálculo Proposicional

Una demostración en el Cálculo Proposicional que veremos en este curso consiste en probar la ***validez*** *de una fórmula mediante una serie de pasos justificados con* ***axiomas*** *y* ***teoremas*** *del Cálculo. Recordemos que una fórmula es válida si para toda asignación posible de las variables es equivalente a True; por lo tanto una demostración será una serie de fórmulas, equivalentes entre sí, donde la primera fórmula es la que queremos demostrar válida y la última es True. Por ejemplo:*

$$
\begin{array}{ll}
 & P \\
\equiv & \{ \texttt{Razón 1} \} \\
 & Q \\
\equiv & \{ \texttt{Razón 2} \} \\
 & (...) \\
\equiv & \{ \texttt{Razón n} \} \\
 & \mathit{True}
\end{array}
$$

$$
\begin{array}{ll}
 & (\underline{\neg\neg((p \Rightarrow r) \wedge s)}) \vee ((p \Rightarrow r) \wedge s) \equiv ((p \Rightarrow r) \wedge s) \\
\equiv & \{ \text{Doble negación } (\neg\neg P \equiv P),\ P := ((p \Rightarrow r) \wedge s) \ \} \\
 & \underline{((p \Rightarrow r) \wedge s) \vee ((p \Rightarrow r) \wedge s) \equiv ((p \Rightarrow r) \wedge s)} \\
\equiv & \{ \text{Idempotencia de } \vee\ (P \vee P \equiv P\ ),\ P := ((p \Rightarrow r) \wedge s) \ \} \\
 & \mathit{True}
\end{array}
$$

La regla general de la izquierda, donde se quiere demostrar que la fórmula P es válida, se puede leer de la siguiente manera: Debido a la `Razón 1`*, P es equivalente a Q, y debido a la* `Razón 2`*, Q es equivalente a True. Por lo tanto, como el equivalente es transitivo, se concluye que P es equivalente a True.*

El ejemplo de la derecha primero aplica el teorema llamado doble negación, y definido como $\neg\neg P \equiv P$, de la siguiente manera. Se sustituye $P := ((p \Rightarrow r) \wedge s)$ en el teorema obteniendo la instanciación $\neg\neg((p \Rightarrow r) \wedge s) \equiv ((p \Rightarrow r) \wedge s)$ y después reemplaza la parte izquierda del teorema sustituido $(\neg\neg((p \Rightarrow r) \wedge s))$ por la parte derecha $((p \Rightarrow r) \wedge s)$. Segundo, se aplica el axioma llamado idempotencia de la disyunción, y definido como $P \vee P \equiv P$, de la siguiente manera. Se sustituye $P := ((p \Rightarrow r) \wedge s)$ en el teorema obteniendo $((p \Rightarrow r) \wedge s) \vee ((p \Rightarrow r) \wedge s) \equiv ((p \Rightarrow r) \wedge s)$. Como obtuve toda la expresión que quería demostar al sustituir el teorema, y todos los teoremas son equivalentes a True, puedo reemplazar toda la expresión por True. Cuando aplico substituciones a un teorema obtengo una ***instanciación*** *del teorema. Todas las instanciaciones de teoremas son también teoremas.*

Si la fórmula que se quiere demostrar es de la forma $R \equiv S$, para demostrar la validez de la fórmula podemos seguir la estrategia seguida anteriormente transformando la expresión completa en True, o bien partir de la subexpresión R y transformarla en la subexpresión S (o viceversa). En ambos casos, cada paso de "transformación" consiste en "reescribir" la expresión en cuestión (o una subexpresión) en otra equivalente dada por uno de los Axiomas o Teoremas básicos. A continuación escribimos las mismas pruebas explicadas anteriormente siguiendo esta nueva estrategia.

$$
\begin{array}{ll}
 & R \\
\equiv & \{ \texttt{Razón 1} \} \\
 & T \\
\equiv & \{ \texttt{Razón 2} \} \\
 & (...) \\
\equiv & \{ \texttt{Razón n} \} \\
 & S
\end{array}
$$

$$
\begin{array}{ll}
 & (\underline{\neg\neg((p \Rightarrow r) \wedge s)}) \vee ((p \Rightarrow r) \wedge s) \\
\equiv & \{ \text{Doble negación } (\neg\neg P \equiv P),\ P := ((p \Rightarrow r) \wedge s) \ \} \\
 & \underline{((p \Rightarrow r) \wedge s) \vee ((p \Rightarrow r) \wedge s)} \\
\equiv & \{ \text{Idempotencia de } \vee\ (P \vee P \equiv P\ ),\ P := ((p \Rightarrow r) \wedge s) \ \} \\
 & \equiv ((p \Rightarrow r) \wedge s)
\end{array}
$$

Cada axioma o teorema nos habilita a reescribir una expresión de diversas maneras. Por ejemplo la Regla Dorada, cuya formulación es $P \wedge Q \equiv P \equiv Q \equiv P \vee Q$, nos permite reescribir la expresión $P \wedge Q$ por $P \equiv Q \equiv P \vee Q$, pero también:

$$
\begin{array}{rll}
P \wedge Q \equiv P \equiv Q \equiv P \vee Q & \textit{por} & \textit{True} \\
P \wedge Q \equiv P & \textit{por} & Q \equiv P \vee Q \\
Q \equiv P \vee Q & \textit{por} & P \wedge Q \equiv P \\
P \wedge Q \equiv P \vee Q & \textit{por} & P \equiv Q \\
P \wedge Q \equiv Q \equiv P \vee Q & \textit{por} & Q \\
P \equiv P \vee Q & \textit{por} & P \wedge Q \equiv Q \\
\textit{y demás combinaciones} \ldots & &
\end{array}
$$

Gracias a la sustitución el lugar de las variables P, Q y R en un axioma o teorema puede ser ocupado por cualquier expresión booleana (de tipo Bool), ya sean fórmulas proposicionales, como p, $(p \wedge q)$, $(p \Rightarrow q \vee r)$, etc, o expresiones aritméticas como $(2 * 2 = 4)$, $(x \leqslant 0)$, etc.

Sustitución y Regla de Leibniz

Las herramientas que venimos usando para hacer demostraciones se llaman: la sustitución y la regla de Leibniz.

Leibniz fue quien introdujo la regla de que es posible reemplazar en una fórmula una expresión por otra expresión equivalente, sin que esto altere el significado de la fórmula. Los sistemas de ecuaciones hacen uso de la regla de Leibniz, por ejemplo

$$
\left\{ \begin{array}{lcll} x & = & 5 & (1) \\ y & = & x+3 & (2) \end{array} \right. \xrightarrow{\textit{Utilizo (1) en (2)}} \left\{ \begin{array}{lcll} x & = & 5 & (1) \\ y & = & 5+3 & (2) \end{array} \right.
$$

En este ejemplo, ambos sistemas de ecuaciones son tienen el mismo significado porque el de la derecha reemplaza x por el valor al cual es equivalente en este sistema de ecuaciones, es decir, 5. En las demostraciones por inducción también usabamos la regla de Leibniz para reemplazar un lado de la hipótesis inductiva por el otro.

En las demostraciones del Cálculo Proposicional se utiliza todo el tiempo la regla de Leibniz para "transformar" fórmulas. Por ejemplo, como $p \vee p \equiv p$ es una ***instanciación*** *del axioma $P \vee P \equiv P$, se puede transformar la fórmula $p \wedge q$ a la fórmula $(p \vee p) \wedge q$ donde se reemplazó p por otra expresión equivalente, $p \vee p$.*

1. Encontrá el axioma o teorema que fue utilizado para transformar la primera expresión en la última y escribila entre las llaves. Subrayá la expresión que está siendo reemplazada e la primer expresión. Indicá la sustitución utilizada.

   Por ejemplo, si tenemos el enunciado:

$$
\begin{array}{ll}
 & q \equiv p \\
\equiv \{ & \qquad\qquad \} \\
 & q \equiv p \vee p
\end{array}
$$

   nos tenemos que dar cuenta que el axioma utilizado es $p \vee p \equiv p$, que se llama idempotencia de la disyunción. Como reeplazamos p la subrayamos.

$$
\begin{array}{ll}
 & q \equiv \underline{p} \\
\equiv \{ & \text{Idempotencia de la disyunción } (P \vee P \equiv P),\ P := p \ \} \\
 & q \equiv p \vee p
\end{array}
$$

   a)
$$
\begin{array}{ll}
 & p \\
\equiv \{ & \qquad\qquad \} \\
 & p \equiv \textit{True}
\end{array}
$$

   b)
$$
\begin{array}{ll}
 & p \Rightarrow q \\
\equiv \{ & \qquad\qquad \} \\
 & (p \equiv \textit{True}) \Rightarrow q
\end{array}
$$

   c)
$$
\begin{array}{ll}
 & p \vee (q \equiv r) \\
\equiv \{ & \qquad\qquad \} \\
 & p \vee q \equiv p \vee r
\end{array}
$$

   d)
$$
\begin{array}{ll}
 & q \Rightarrow p \vee q \\
\equiv \{ & \qquad\qquad \} \\
 & q \Rightarrow (p \equiv q \equiv p \wedge q)
\end{array}
$$

2. Encontrá las instanciaciones $\mathcal{E}$, $\mathcal{F}$ y $\mathcal{G}$ de forma que la sustitución $(P := \mathcal{E}, Q := \mathcal{F}, R := \mathcal{G})$ justifique cómo fue aplicado cada axioma o teorema para transformar una expresión en la otra, en cada una de las siguientes demostraciones. En todos los casos enunciá la fórmula cuya validez se demuestra. Por ejemplo, la siguiente demostración:

$\neg(p \Rightarrow q \equiv p)$
$\equiv$ { *(Definición de negación)*$(P := \mathcal{E}, Q := \mathcal{F})$ }
$\neg(p \Rightarrow q) \equiv p$

demuestra la validez de la fórmula $\neg(p \Rightarrow q \equiv p) \equiv \neg(p \Rightarrow q) \equiv p$ *utilizando el axioma "Definición de negación"* $(\neg(P \equiv Q) \equiv \neg P \equiv Q)$*, con la sustitución* $P := (p \Rightarrow q), Q := p$

Para encontrar la sustitución hay recetas, tenemos que conocer los axiomas y teoremas y saber qué queremos demostrar. Podemos pensar en las variables P, Q *y* R *de los axiomas como "comodines" diferentes, cada uno de los cuales puede representar una fórmula cualquiera (tan compleja como queramos). Lo importante es hacer la sustitución de forma coherente, es decir el lugar de un comodín es ocupado siempre por la* **misma** *fórmula. Una vez que tenemos sabemos qué se está demostrando, la ubicación de los paréntesis y de los operadores ayuda a encontrar la sustitución utilizada. A continuación la primera es la fórmula a demostrar, y la segunda el axioma visto con "comodines"* P *y* Q*:*

$$\neg(\ p \Rightarrow q \equiv p\ ) \equiv \neg(\ p \Rightarrow q\ ) \equiv p$$
$$\neg(\quad P \quad \equiv Q\ ) \equiv \neg(\quad P \quad) \equiv Q$$

Esto nos muestra que si usamos la sustitución $P := p \Rightarrow q$ *y* $Q := p$ *y el axioma "Definición de la negación", vamos a poder demostrar la fórmula que queríamos.*

Completá los siguientes ejercicios similares al ejemplo discutido. No te olvides de subrayar la expresión que se está reemplazando.

a) $p \equiv q \equiv r$
$\equiv$ { Conmutatividad de $\equiv$, $P := \mathcal{E}, Q := \mathcal{F}$ }
$r \equiv p \equiv q$

b) $p \vee q \vee (\mathit{False} \equiv \neg q)$
$\equiv$ { Distributividad $\vee$ con $\equiv$, $P := \mathcal{E}, Q := \mathcal{F}, R := \mathcal{G}$ }
$p \vee q \vee \mathit{False} \equiv p \vee q \vee \neg q$

c) $\neg p \wedge (r \Rightarrow s)$
$\equiv$ { Regla dorada, $P := \mathcal{E}, Q := \mathcal{F}$ }
$\neg p \equiv r \Rightarrow s \equiv \neg p \vee (r \Rightarrow s)$

d) $n \mod 4 = 0 \Rightarrow n \mod 2 = 0$
$\equiv$ { Definición de $\Rightarrow$, $P := \mathcal{E}, Q := \mathcal{F}$ }
$n \mod 4 = 0 \vee n \mod 2 = 0 \equiv n \mod 2 = 0$

e) $x > 2 \vee y > 5 \equiv x > 2 \vee \neg y > 5$
$\equiv$ { Teorema $*$, $P := \mathcal{E}, Q := \mathcal{F}$ }
$x > 2$

f) $\neg(p \wedge q \wedge r \Rightarrow p \wedge s)$
$\equiv$ { Negación de $\Rightarrow$, $P := \mathcal{E}, Q := \mathcal{F}$ }
$p \wedge q \wedge r \wedge \neg(p \wedge s)$

3. Completá las siguientes demostraciones especificando el axioma o teorema utilizado y la sustitución correspondiente; subrayá la subexpresión donde se aplica.

a) $\neg\neg\neg p \equiv q$
$\equiv$ { }
$\neg p \equiv q$
$\equiv$ { }
$\neg(p \equiv q)$
$\equiv$ { }
$p \not\equiv q$

b) $p \vee (q \equiv r \equiv s)$
$\equiv$ { }
$p \vee (q \equiv r) \equiv p \vee s$
$\equiv$ { }
$p \vee q \equiv p \vee r \equiv p \vee s$

c) $p \Rightarrow q$
$\equiv$ { }
$p \vee q \equiv q$
$\equiv$ { }
$q \equiv p \vee q$
$\equiv$ { }
$p \wedge q \equiv p$

d) $\neg p \equiv \neg q$
$\equiv$ { }
$\neg(p \equiv \neg q)$
$\equiv$ { }
$\neg(\neg q \equiv p)$
$\equiv$ { }
$\neg\neg(q \equiv p)$
$\equiv$ { }
$\neg\neg(p \equiv q)$
$\equiv$ { }
$p \equiv q$

Equivalencia, Discrepancia y Negación

4. Demostrá que las siguientes fórmulas son teoremas del Cálculo Proposicional, es decir, son fórmulas *válidas* utilizando sólo axiomas (no se pueden usar teoremas). Realizá la demostración justificando cada paso con un axioma y la sustitución utilizada en el mismo. Por ejemplo, demostramos el teorema *Asociatividad de la discrepancia*: $(p \not\equiv (q \not\equiv r)) \equiv ((p \not\equiv q) \not\equiv r)$, partiendo de la parte izquierda:

$$
\begin{array}{ll}
 & (p \not\equiv (q \not\equiv r)) \\
\equiv & \{ \text{ (Definición de } \not\equiv)(Q := (q \not\equiv r)) \ \} \\
 & \neg(p \equiv \underline{(q \not\equiv r)}) \\
\equiv & \{ \text{ (Definición de } \not\equiv)(P, Q := q, r) \ \} \\
 & \neg(p \equiv \underline{\neg(q \equiv r)}) \\
\equiv & \{ \text{ (Definición de } \neg)(P, Q := q, r) \ \} \\
 & \neg(p \equiv \neg q \equiv r) \\
\equiv & \{ \text{ (Definición de } \not\equiv)(P, Q := (p \equiv \neg q), r) \ \} \\
 & \underline{(p \equiv \neg q)} \not\equiv r \\
\equiv & \{ \text{ (Conmutatividad de } \equiv)(Q := \neg q) \ \} \\
 & \underline{(\neg q \equiv p)} \not\equiv r \\
\equiv & \{ \text{ (Definición de } \neg)(P, Q := q, p) \ \} \\
 & \neg\underline{(q \equiv p)} \not\equiv r \\
\equiv & \{ \text{ Conmutatividad de } \equiv \ \} \\
 & \underline{\neg(p \equiv q)} \not\equiv r \\
\equiv & \{ \text{ Definición de } \not\equiv \ \} \\
 & (p \not\equiv q) \not\equiv r
\end{array}
$$

a) *Reflexividad del equivalente*: $(p \equiv p) \equiv True$

b) *Doble negación*: $\neg\neg p \equiv p$

c) *Equivalencia y negación*: $p \equiv False \equiv \neg p$

d) *Neutro de la discrepancia*: $(p \not\equiv false) \equiv p$

e) *Absurdo*: $p \Rightarrow False \equiv \neg p$.

Disyunción y Conjunción

5. Demostrá que las siguientes fórmulas son teoremas, justificando cada paso con el axioma aplicado.

   a) *Distributividad de la disyunción con la disyunción*: $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$

   b) *Elemento absorbente de la disyunción*: $p \vee True \equiv True$

   c) *Elemento neutro de la disyunción*: $p \vee False \equiv p$

   d) *Teorema Estrella* : $p \vee q \equiv p \vee \neg q \equiv p$

6. Demostrá que las siguientes fórmulas son teoremas justificando cada paso con el axioma o teorema aplicado. **Aclaración:** Desde ahora en adelante, en cada ejercicio se pueden utilizar los teoremas del listado y los ya demostrados en los ejercicios anteriores.

   a) *Distributividad de la disyunción con la conjunción*: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

   b) *Asociatividad de la conjunción*: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

   c) *Idempotencia de la conjunción*: $p \wedge p \equiv p$

   d) *Conmutatividad de la conjunción*: $p \wedge q \equiv q \wedge p$

   e) *Elemento absorbente de la conjunción*: $p \wedge False \equiv False$

   f) *Elemento neutro de la conjunción*: $p \wedge True \equiv p$

   g) *De Morgan para la conjunción*: $\neg(p \wedge q) \equiv \neg p \vee \neg p$

   h) *Ley de absorción*: $p \wedge (p \vee q) \equiv p$

Implicación

La implicación es uno de los mecanismos más intuitivos para razonar, ya que de esta forma representamos la **causalidad**. *De la misma forma que la causalidad no es simétrica, tampoco lo es la implicación. Es decir, los dos elementos que componen una implicación no participan de igual forma en la relación. Por ejemplo, cuando como demasiado (causa) me duele la panza (efecto), pero no a la inversa (cuando me* *duele la panza no necesariamente es porque he comido demasiado, puede ser porque estoy nervioso). El elemento a la izquierda de la implicación se llama* **antecedente**, *y el de la derecha,* **consecuente**. *Esta asimetría también se pone de manifiesto en la tabla de verdad de la implicación:*

p	q	$p \Rightarrow q$
True	*True*	*True*
True	*False*	*False*
False	*True*	*True*
False	*False*	*True*

También las diferentes formas de reescribir la implicación nos muestran como sus dos elementos participan de forma distinta en la relación. En el próximo ejercicio tienen las dos definiciones más comunes de implicación, vean cómo el antecedente y el consecuente tienen reescrituras distintas.

7. Demostrá que las siguientes fórmulas son teoremas, justificando cada paso con el axioma o teorema aplicado.

   a) *Caracterización de implicación*: $p \Rightarrow q \equiv \neg p \vee q$

   b) *Definición dual de implicación*: $p \Rightarrow q \equiv p \wedge q \equiv p$

   c) *Negación de una implicación*: $\neg(p \Rightarrow q) \equiv p \wedge \neg q$

   d) *Absurdo*: $p \Rightarrow \mathit{False} \equiv \neg p$.

   e) *Debilitamiento para* $\wedge$: $p \wedge q \Rightarrow p$.

   f) *Debilitamiento para* $\vee$: $p \Rightarrow p \vee q$.

   g) *Modus Ponens* $(p \Rightarrow q) \wedge p \equiv p \wedge q$.

   h) *Modus Tollens* $(p \Rightarrow q) \wedge \neg q \equiv \neg p \wedge \neg q$.