Introducción a los Algoritmos
Cálculo Proposicional

Pedro Sánchez Terraf

CIEM-FaMAF — Universidad Nacional de Córdoba

FaMAF
UNC
28 de abril de 2014

Contenido

1. Demostraciones
   - Repaso
   - Demostraciones con expresiones booleanas
   - Fórmulas Proposicionales: Más Variantes
   - Axiomas y Teoremas

2. Tarea.

Repaso (I)

Justificación

$$
\begin{aligned}
& 5 * (x+3) = 20 \\
\equiv \{ & \text{ Conmutativa } + \} \\
& 5 * (3+x) = 20
\end{aligned}
$$

Repaso (I)

$$
\begin{aligned}
& 5 * (x + 3) = 20 \\
\equiv \{ & \text{ Conmutativa + } \} \\
& 5 * (3 + x) = 20
\end{aligned}
$$

Justificación

Conmutativa de +:

$$a + b = b + a$$

Sustituyo a por x
Sustituyo b por 3
para obtener

$$x + 3 = 3 + x.$$

Repaso (II)

$$
\begin{aligned}
& \underline{S.(1+1)} = S.1 + S.1 \\
\equiv \{ & \text{ Definición de } S \ \} \\
& 1+1+1 = S.1 + S.1
\end{aligned}
$$

Justificación

Definición de S

$$S.x \doteq x + 1$$

Sustituyo x por

para obtener

$$S.(1+1) = 1+1+1$$

- Debo justificar usando propiedades **válidas** o **definiciones**.

Repaso (II)

$$
\begin{array}{rl}
& \underline{S.(1+1)} = S.1 + S.1 \\
\equiv & \{ \text{ Definición de } S \ \} \\
& 1+1+1 = S.1 + S.1
\end{array}
$$

Justificación

Definición de S

$$S.x \doteq x+1$$

Sustituyo x por $1+1$
para obtener

$$S.(1+1) = 1+1+1$$

- Debo justificar usando propiedades **válidas** o **definiciones**.

Cálculo Proposicional (I)

Justificaremos ahora usando expresiones booleanas válidas. Un ejemplo es la *Conmutatividad de* $\equiv$.

$$\begin{array}{ll} & r \equiv p \wedge q \equiv r \\ \equiv & \{ \text{ Conmutatividad } \equiv \} \\ & p \wedge q \equiv r \equiv r \end{array}$$

Justificación

Conmutatividad de $\equiv$:

$$(P \equiv Q) \equiv (Q \equiv P)$$

Justificaremos ahora usando expresiones booleanas válidas. Un ejemplo es la *Conmutatividad de* $\equiv$.

$$r \equiv p \wedge q \equiv r$$
$$\equiv \{ \text{ Conmutatividad } \equiv \}$$
$$p \wedge q \equiv r \equiv r$$

Justificación

Conmutatividad de $\equiv$:

$$(P \equiv Q) \equiv (Q \equiv P)$$

Sustituyo P por r
Sustituyo Q por $p \wedge q$; obtengo

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

Cálculo Proposicional (II)

Otra expresión booleana válida es la *Definición* $\Rightarrow$.

Justificación

Definición $\Rightarrow$:

$$(P \Rightarrow Q) \equiv (P \vee Q \equiv Q)$$

$$\begin{aligned} & q \equiv r \Rightarrow q \equiv r \\ \equiv & \{ \text{ Definición } \Rightarrow \} \\ & q \equiv r \vee q \equiv q \equiv r \end{aligned}$$

Cálculo Proposicional (II)

Otra expresión booleana válida es la *Definición* $\Rightarrow$.

$$
\begin{array}{ll}
 & q \equiv r \Rightarrow q \equiv r \\
\equiv & \{ \text{ Definición } \Rightarrow \} \\
 & q \equiv r \vee q \equiv q \equiv r
\end{array}
$$

Justificación

Definición $\Rightarrow$:

$$(P \Rightarrow Q) \equiv (P \vee Q \equiv Q)$$

Sustituyo P por r
Sustituyo Q por q; obtengo

$$(r \Rightarrow q) \equiv (r \vee q \equiv q).$$

Asociatividad y Conmutatividad de $\equiv$

Hasta ahora todo es igual. Pero las demostraciones con fórmulas proposicionales (las expresiones booleanas hechas con $\equiv$, $\wedge$, $\vee$,... y variables de tipo $Bool$) permiten mucha más flexibilidad.

Asociatividad de $\equiv$

Puedo agrupar las expresiones separadas por $\equiv$ de la manera que quiera, poniendo paréntesis

Ejemplo

Para la *Conmutatividad de* $\equiv$, tenemos

$$(P \equiv Q) \equiv (Q \equiv P)$$
$$P \equiv (Q \equiv Q \equiv P)$$
$$(P \equiv Q \equiv Q) \equiv P$$

Asociatividad y Conmutatividad de $\equiv$

Hasta ahora todo es igual. Pero las demostraciones con fórmulas proposicionales (las expresiones booleanas hechas con $\equiv$, $\wedge$, $\vee$,... y variables de tipo $Bool$) permiten mucha más flexibilidad.

Asociatividad de $\equiv$

Puedo agrupar las expresiones separadas por $\equiv$ de la manera que quiera, poniendo paréntesis

Ejemplo

Para la *Conmutatividad de* $\equiv$, tenemos

$$(P \equiv Q) \equiv (Q \equiv P)$$
$$P \equiv (Q \equiv Q \equiv P)$$
$$(P \equiv Q \equiv Q) \equiv P$$

$$
\begin{array}{ll}
 & r \equiv p \wedge q \equiv r \\
\equiv & \{ \text{ Conmutatividad } \equiv \} \\
 & p \wedge q \equiv r \equiv r \\
\equiv & \{ \text{ Conmutatividad } \equiv \} \\
 & p \wedge q
\end{array}
$$

Justificación

Conmutatividad de $\equiv$:

$$(P \equiv Q) \equiv (Q \equiv P)$$

Sustituyo P por r
Sustituyo Q por $p \wedge q$; obtengo

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

Cálculo Proposicional (III)

$$
\begin{aligned}
& r \equiv p \wedge q \equiv r \\
\equiv \{ & \text{ Conmutatividad } \equiv \} \\
& p \wedge q \equiv r \equiv r \\
\equiv \{ & \text{ Conmutatividad } \equiv \} \\
& p \wedge q
\end{aligned}
$$

Justificación

Conmutatividad de $\equiv$:

$$(P \equiv Q \equiv Q) \equiv P$$

Sustituyo P por $p \wedge q$
Sustituyo Q por r ; obtengo

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

Cálculo Proposicional (IV)

$$
\begin{aligned}
& q \equiv r \Rightarrow q \equiv r \\
\equiv & \{ \text{ Definición } \Rightarrow \} \\
& q \equiv r \vee q \equiv q \equiv r
\end{aligned}
$$

Justificación

Definición $\Rightarrow$:

$$(P \Rightarrow Q) \equiv (P \vee Q \equiv Q)$$

Sustituyo P por r
Sustituyo Q por q; obtengo

$$(r \Rightarrow q) \equiv (r \vee q \equiv q).$$

Cálculo Proposicional (IV)

$$\begin{array}{ll} & \underline{q \equiv r \Rightarrow q} \equiv r \\ \equiv & \{ \text{ Definición } \Rightarrow \} \\ & r \vee q \equiv r \end{array}$$

Justificación

Definición $\Rightarrow$:

$$(P \Rightarrow Q) \equiv (P \vee Q \equiv Q)$$

$$\begin{aligned} & \underline{q \equiv r \Rightarrow q} \equiv r \\ \equiv \{ & \text{ Definición } \Rightarrow \} \\ & r \vee q \equiv r \end{aligned}$$

Justificación

Definición $\Rightarrow$:

$$P \Rightarrow Q \equiv P \vee Q \equiv Q$$

Cálculo Proposicional (IV)

$$\begin{aligned} & \underline{q \equiv r \Rightarrow q} \equiv r \\ \equiv \; & \{ \text{ Definición } \Rightarrow \} \\ & r \vee q \equiv r \end{aligned}$$

Justificación

Definición $\Rightarrow$:

$$Q \equiv P \Rightarrow Q \equiv P \vee Q$$

$$\begin{array}{ll} & \underline{q \equiv r \Rightarrow q} \equiv r \\ \equiv \{ & \text{Definición} \Rightarrow \} \\ & r \vee q \equiv r \end{array}$$

Justificación

Definición $\Rightarrow$:

$$Q \equiv P \Rightarrow Q \equiv P \vee Q$$

Sustituyo P por r
Sustituyo Q por q; obtengo

$$q \equiv r \Rightarrow q \equiv r \vee q.$$

Axiomas y Teoremas

Fijaremos un conjunto de fórmulas proposicionales válidas y justificaremos nuestras pruebas usando al principio sólo ellas.
Los axiomas que usaremos están listados en el Práctico 4 (ir al Aula Virtual).
Definimos intuitivamente (de manera "recursiva") la noción de *teorema*.

Definición

Un **teorema** es:

1. un axioma; o sino
2. una fórmula proposicional equivalente a un axioma o a un teorema ya demostrado.

Fijaremos un conjunto de fórmulas proposicionales válidas y justificaremos nuestras pruebas usando al principio sólo ellas.
Los axiomas que usaremos están listados en el Práctico 4 (ir al Aula Virtual).
Definimos intuitivamente (de manera “recursiva”) la noción de *teorema*.

Definición

Un **teorema** es:

1. un axioma; o sino
2. una fórmula proposicional equivalente a un axioma o a un teorema ya demostrado.

Teoremas: Cómo demostrarlos

En la práctica, admitiremos un par de reglas extra (que, de todos modos, son correctas desde el punto de vista del libro).

1. Todo teorema es equivalente a $True$.
2. Si pruebo que algo es equivalente a $True$, entonces es un teorema.
3. Si salgo de una fórmula E y llego a otra F justificando con teoremas, entonces $E \equiv F$ es un teorema.

Por ejemplo, en último ejemplo probamos que

$$q \equiv r \Rightarrow q \equiv r \equiv r \vee q \equiv r$$

es un teorema.

Teoremas: Cómo demostrarlos

En la práctica, admitiremos un par de reglas extra (que, de todos modos, son correctas desde el punto de vista del libro).

1. Todo teorema es equivalente a $True$.
2. Si pruebo que algo es equivalente a $True$, entonces es un teorema.
3. Si salgo de una fórmula E y llego a otra F justificando con teoremas, entonces $E \equiv F$ es un teorema.

Por ejemplo, en último ejemplo probamos que

$$q \equiv r \Rightarrow q \equiv r \equiv r \vee q \equiv r$$

es un teorema.

Teoremas: Cómo demostrarlos

En la práctica, admitiremos un par de reglas extra (que, de todos modos, son correctas desde el punto de vista del libro).

1. Todo teorema es equivalente a $True$.
2. Si pruebo que algo es equivalente a $True$, entonces es un teorema.
3. Si salgo de una fórmula E y llego a otra F justificando con teoremas, entonces $E \equiv F$ es un teorema.

Por ejemplo, en último ejemplo probamos que

$$q \equiv r \Rightarrow q \equiv r \equiv r \vee q \equiv r$$

es un teorema.

Cálculo Proposicional (IV)

$$\underline{q \equiv r \Rightarrow q} \equiv r$$
$$\equiv \{ \text{ Definición } \Rightarrow \}$$
$$r \vee q \equiv r$$

Justificación

Definición $\Rightarrow$:

$$Q \equiv P \Rightarrow Q \equiv P \vee Q$$

Sustituyo P por r
Sustituyo Q por q; obtengo

$$q \equiv r \Rightarrow q \equiv r \vee q.$$

Tareas para ahora mismo

1. ¿Qué teorema demostramos en la filmina 8 (página 14)?
2. Leer los axiomas, poniendoles paréntesis de acuerdo a la precedencia.
3. ¿De cuántas maneras se puede leer la *Definición de* $\neg$? (es el axioma **A4**).
4. Completar los espacios en blanco, justificando con los axiomas:

$$
\begin{array}{ll}
 & \neg p \equiv q \vee r \\
\equiv & \{ \qquad\qquad\qquad\qquad \} \\
 & \neg(p \equiv q \vee r) \\
\equiv & \{ \qquad\qquad\qquad\qquad \} \\
 & p \not\equiv q \vee r
\end{array}
$$

5. Leer el ejemplo en el ejercicio 1 del Práctico 4. Preguntar las dudas.