Algoritmos y Estructuras de Datos I

Digesto de Axiomas y Teoremas Básicos del Cálculo Proposicional y Expresiones Cuantificadas

Axiomas del cálculo proposicional

A1 Asociatividad de la Equivalencia:
$$((P \equiv Q) \equiv R) \equiv (P \equiv (Q \equiv R))$$

A2 Conmutatividad de la Equivalencia:
$$P \equiv Q \equiv Q \equiv P$$

A3 Neutro de la Equivalencia:
$$P \equiv True \equiv P$$

A4 Definición de la Negación:
$$\neg(P \equiv Q) \equiv \neg P \equiv Q$$

A5 Definición de $False$:
$$False \equiv \neg True$$

A6 Definición de la Discrepancia:
$$P \not\equiv Q \equiv \neg(P \equiv Q)$$

A7 Asociatividad de la Disyunción:
$$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$$

A8 Conmutatividad de la Disyunción:
$$P \vee Q \equiv Q \vee P$$

A9 Idempotencia de la Disyunción:
$$P \vee P \equiv P$$

A10 Distributividad de la Disyunción respecto a la Equivalencia:
$$P \vee (Q \equiv R) \equiv (P \vee Q) \equiv (P \vee R)$$

A11 Tercero excluido:
$$P \vee \neg P$$

A12 Regla Dorada:
$$P \wedge Q \equiv P \equiv Q \equiv P \vee Q$$

A13 Leibniz:
$$e = f \Rightarrow E(z := e) = E(z := f)$$

A14 Definición de la Implicación:
$$P \Rightarrow Q \equiv P \vee Q \equiv Q$$

A15 Definición de la Consecuencia:
$$P \Leftarrow Q \equiv P \vee Q \equiv P$$

Teoremas del cálculo proposicional

T1 Metateorema de $True$:
Si P está demostrado, $P \equiv True$

T2 Doble Negación:
$$\neg\neg P \equiv P$$

T3 Equivalencia y Negación:
$$P \equiv \neg P \equiv False$$

T4 Elemento absorbente de la Disyunción:
$$P \vee True \equiv True$$

T5 Elemento neutro de la Disyunción:
$$P \vee False \equiv P$$

T6 Conmutatividad de la Conjunción:
$$P \wedge Q \equiv Q \wedge P$$

T7 Asociatividad de la Conjunción:
$$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$$

T8 Teorema $(*)$:
$$P \vee Q \equiv P \vee \neg Q \equiv P$$

Precedencia

4. $\neg$
3. $\vee$, $\wedge$
2. $\Rightarrow$, $\Leftarrow$
1. $\equiv$, $\not\equiv$

Axiomas de cuantificadores

A16 (Rango vacío): $\langle \oplus i \ : False : \ T \rangle = e$

– e el elemento neutro de $\oplus$.

A17 (Rango unitario): $\langle \oplus i \ : i = N : \ T.i \rangle = T.N$

A18 (Partición de rango): $\langle \oplus i \ : R \vee S : \ T \rangle = \langle \oplus i \ : R : \ T \rangle \oplus \langle \oplus i \ : S : \ T \rangle$

– $\oplus$ es idempotente o R y S son disjuntos.

A19 (Partición de rango generalizada):

$$\langle \oplus i \ : \langle \exists j \ : S.i.j : \ R.i.j \rangle : \ T.i \rangle = \langle \oplus i, j \ : S.i.j \wedge R.i.j : \ T.i \rangle$$

– $\oplus$ es idempotente.

A20 (Regla del término): $\langle \oplus i \ : R : \ T \oplus G \rangle = \langle \oplus i \ : R : \ T \rangle \oplus \langle \oplus i \ : R : \ G \rangle$

A21 (Término constante): $\langle \oplus i \ : R : \ C \rangle = C$

– i no aparece en C
– $C \oplus C = C$ ($\oplus$ es idempotente para C)
– R es no vacío.

A22 (Distributividad): $\langle \oplus i \ : R : \ x \otimes T \rangle = x \otimes \langle \oplus i \ : R : \ T \rangle$

– $\otimes$ distributivo a izquierda con $\oplus$
– R es no vacío o el neutro de $\oplus$ es absorbente para $\otimes$
– i no aparece en x.

Análogamente, $\langle \oplus i \ : R : \ T \otimes x \rangle = \langle \oplus i \ : R : \ T \rangle \otimes x$

– $\otimes$ distributivo a derecha con $\oplus$
– R es no vacío o el neutro de $\oplus$ es absorbente para $\otimes$
– i no aparece en x.

A23 (Anidado): $\langle \oplus i, j \ : R.i \wedge S.i.j : \ T.i.j \rangle = \langle \oplus i \ : R.i : \ \langle \oplus j \ : S.i.j : \ T.i.j \rangle \rangle$

A24 (Intercambio): $\langle \forall i \ : R.i : \ T.i \rangle \equiv \langle \forall i \ :: \ R.i \Rightarrow T.i \rangle$
$\langle \exists i \ : R.i : \ T.i \rangle \equiv \langle \exists i \ :: \ R.i \wedge T.i \rangle$

A25 (De Morgan): $\neg \langle \forall i \ : R.i : \ T.i \rangle \equiv \langle \exists i \ : R.i : \ \neg T.i \rangle$
$\neg \langle \exists i \ : R.i : \ T.i \rangle \equiv \langle \forall i \ : R.i : \ \neg T.i \rangle$

A26 (Definición de conteo): $\langle N i \ : R.i : \ T.i \rangle = \langle \sum i \ : R.i \wedge T.i : \ 1 \rangle$

A27 (Definición de máximo y mínimo): Si el rango R es no vacío entonces

$$z = \langle \text{Max} \ i \ : R.i : \ F.i \rangle \equiv \langle \exists i \ : R.i : \ z = F.i \rangle \wedge \langle \forall i \ : R.i : \ F.i \leq z \rangle$$
$$z = \langle \text{Min} \ i \ : R.i : \ F.i \rangle \equiv \langle \exists i \ : R.i : \ z = F.i \rangle \wedge \langle \forall i \ : R.i : \ z \leq F.i \rangle$$

Teoremas sobre cuantificadores

T9 (Cambio de variable): $\langle \oplus i \ : R.i : \ T.i \rangle = \langle \oplus j \ : R.(f.j) : \ T.(f.j) \rangle$

– f tiene inversa en R
– j no aparece en R y T.

T10 (Separación de un término): Si $n : Nat$ $(n \geq 0)$

$$\langle \oplus i \ : 0 \leq i < n+1 : \ T.i \rangle = T.0 \oplus \langle \oplus i \ : 0 \leq i < n : \ T.(i+1) \rangle$$
$$\langle \oplus i \ : 0 \leq i < n+1 : \ T.i \rangle = \langle \oplus i \ : 0 \leq i < n : \ T.i \rangle \oplus T.n$$