Circuitos Lógicos no Clásicos

Juan Carlos Agudelo Agudelo

Grupo de Lógica y Computación
Universidad EAFIT

12 de febrero de 2010

Contenido

Contenido

Circuitos Booleanos

Definición

Un circuito booleano es una colección finita de variables de entrada y puertas lógicas conectadas de manera direccionada e acíclica, donde las variables de entrada toman valores en $\{0,1\}$ y cada puerta calcula una operación booleana (usualmente *AND*, *OR* o *NOT*).

- Circuitos booleanos computan funciones de la forma $f\colon \{0,1\}^n \to \{0,1\}^m$ (con tamaño de entrada n fijo).
- Para computar una función con tamaño da entrada variable se debe definir una familia uniforme de circuitos booleanos.
- La clase de lenguajes decidibles por familias uniformes de circuitos booleanos con número polinomial de puertas lógicas ($\mathbf{P}_{/poly}$) es igual a la clase **P**.

Circuitos Booleanos

- Generalizar los circuitos booleanos para lógicas finitamente valoradas es simple: valores de entrada/salida corresponden a los valores de verdad y las puertas lógicas realizan las funciones asociadas a los conectivos lógicos.
- Como generalizar para lógicas no caracterizables por matrices finitas (como es el caso de varias lógicas paraconsistentes)? Cuales serian los valores de entrada? Cuales serian las operaciones de las puertas lógicas?

Contenido

Cálculo de Anillos de Polinomios

- El Cálculo de Anillos de Polinômios (CAP) consiste básicamente en traducir fórmulas de una lógica en polinomios con coeficientes en un cuerpo finito (o cuerpo de Galois), y en realizar deducciones a través de operaciones sobre esos polinomios.
- A través de la introducción de varibles ocultas pueden ser definidos CAPs para lógicas no caracterizables por matrices finitas, como es el caso de la lógica paraconsistente *mbC* y a lógica modal *S5*.

CAP para lógica proposicional clásica

Definición (CAP para la lógica proposicional clásica (*LPC*))

- **Función de traducción** ($*$: $ForLPC \to \mathbb{Z}_2[X]$):

$$p_i^* = x_i \text{ si } p_i \text{ es una variable proposicional;}$$
$$(\varphi \wedge \psi)^* = \varphi^* \cdot \psi^*;$$
$$(\varphi \vee \psi)^* = \varphi^* \cdot \psi^* + \varphi^* + \psi^*;$$
$$(\neg\varphi)^* = \varphi^* + 1.$$

- **Reglas de reducción**: $x + x = 0$ y $x \cdot x = x$.

CAP para lógica proposicional clásica

Teorema

$\vdash_{LPC} \varphi$ *sii* φ^* *reduce en el CAP al polinomio constante* 1*.*

Ejemplo (Deducción usando el CAP para *LPC*)

$$\begin{aligned}(\varphi \vee \neg\varphi)^* &= \varphi^* \cdot (\neg\varphi)^* + \varphi^* + (\neg\varphi)^* \\ &= \varphi^* \cdot (\varphi^* + 1) + \varphi^* + \varphi^* + 1 \\ &= \varphi^* \cdot \varphi^* + \varphi^* + \varphi^* + \varphi^* + 1 \\ &= \varphi^* + \varphi^* + \varphi^* + \varphi^* + 1 \\ &= 1\end{aligned}$$

CAP para *mbC*

mbC no es caracterizable por una matriz finita, pero puede ser caracterizada por una semántica bivalorada no veritativo-funcional:

$v(\varphi \wedge \psi) = 1$ iff $v(\varphi) = 1$ and $v(\psi) = 1$;
$v(\varphi \vee \psi) = 1$ iff $v(\varphi) = 1$ or $v(\psi) = 1$;
$v(\varphi \rightarrow \psi) = 1$ iff $v(\varphi) = 0$ or $v(\psi) = 1$;
$v(\neg\varphi) = 0$ implies $v(\varphi) = 1$;
$v(\circ\varphi) = 1$ implies $v(\varphi) = 0$ or $v(\neg\varphi) = 0$.

CAP para *mbC*

Definición (CAP para *mbC*)

- **Función de traducción** ($*$: *FormbC* $\to \mathbb{Z}_2[X]$):

  $p_i^* = x_i$ si p_i es una variable proposicional;
  $(\varphi \wedge \psi)^* = \varphi^* \cdot \psi^*$;
  $(\varphi \vee \psi)^* = \varphi^* \cdot \psi^* + \varphi^* + \psi^*$;
  $(\varphi \to \psi)^* = \varphi^* \cdot \psi^* + \varphi^* + 1$;
  $(\neg\varphi)^* = \varphi^* \cdot x_\varphi + 1$ (x_φ es una variable oculta);
  $(\circ\varphi)^* = (\varphi^* \cdot (x_\varphi + 1) + 1) \cdot x_{\varphi'}$ ($x_\varphi, x_{\varphi'}$ son variables ocultas);

- **Reglas de reducción**: $x + x = 0$ y $x \cdot x = x$.

Teorema

$\vdash_{mbC} \varphi$ *sii* φ^* *reduce en el CAP al polinomio constante* 1.

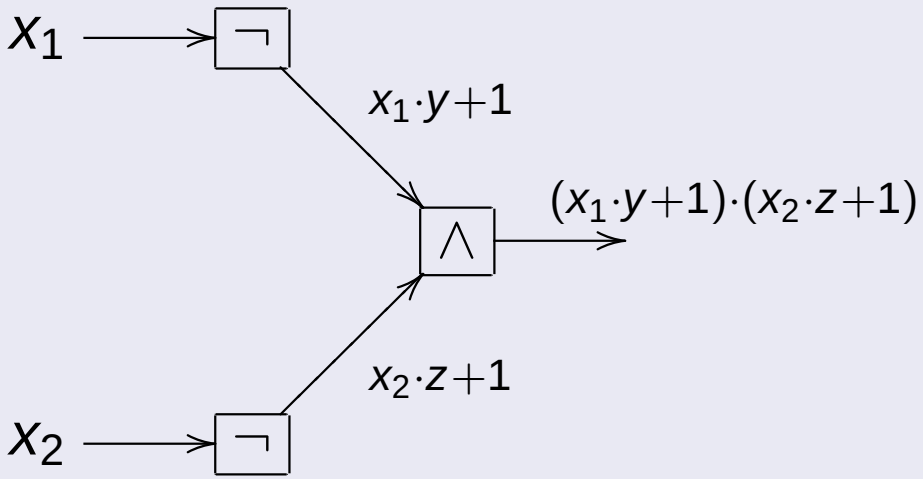
Contenido

Definición

Sea L una lógica proveída de CAP sobre un cuerpo F. Un L-circuito es una colección finita de variables de entrada y puertas lógicas conectadas de manera direccionada y acíclica, donde las variables de entrada toman valores en F e cada puerta lógica calcula el polinomio asociado al conectivo en el CAP.

- Variables ocultas pueden ser introducidas por conectivos lógicos.
- Las variables ocultas producen indeterminismo, aunque las entradas sean deterministas.
- El indeterminismo puede ser usado para simular cierto tipo de procesamiento en paralelo.

Ejemplo (*mbC*-circuito)



x_1	x_2	$\neg x_1$	$\neg x_2$	$\neg x_1 \wedge \neg x_2$
0	0	1	1	1
0	1	1	$z+1$	$z+1$
1	0	$y+1$	1	$y+1$
1	1	$y+1$	$z+1$	$(y+1)\cdot(z+1)$

Circuitos Paraconsistentes *mbC*

mbC-circuitos:

- Permiten cambiar variables de entrada por variables ocultas, dando la posibilidad de traducir computaciones deterministas a no-deterministas sin necesidad de considerar entradas aleatorias.
- No existe ningún tipo de correlación entre variables.

Definición

$$\mathbf{BPmbC}_{/poly} = \{L \mid \text{existe un } mbC\text{-circuito que decide } L \text{ con número de puertas } f(c) = c^k, \text{ para alguna constante } k \in \mathbb{N}\}.$$

Teorema

$$\mathbf{BPmbC}_{/poly} = \mathbf{BPP}_{/poly}.$$