Semana 15: Polinomios de Boole

1. Polinomios y funciones de Boole

En muchas ocasiones, es interesante hablar de variables. En esta sección lo haremos de una manera formal considerando las variables simplemente como elementos de un conjunto y por lo regular usaremos los símbolos $x, y, z, x_1, \ldots$ para denotarlas.

Definición 14.1. Sea V un conjunto de variables. *Un polinomio de Boole* es una secuencia de objetos definida de manera recursiva como sigue:

- Si $p \in V \cup \{0,1\}$ entonces p es un polinomio de Boole.
- Si p es un polinomio de Boole, entonces lo es también $(\neg p)$.
- Si p y q son polinomios de Boole, entonces los son también $(p \vee q)$ y $(p \wedge q)$.

Es una consecuencia de la definición que cada polinomio de Boole p involucra un número finito de variables. Para indicar esto escribiremos $p(x_1, \ldots, x_n)$. Es importante observar que los paréntesis funcionan como símbolos auxiliares e indican de alguna forma el proceso de *construcción* del polinomio.

Ejemplo. Debemos observar que la expresión

$$p(x,y,z) = ((x \vee ((\neg z) \wedge y)) \wedge z)$$

es un polinomio de Boole. Para verificarlo, debemos considerar que x, y y z son variables, por lo que podemos observar el proceso constructivo notando que las siguientes expresiones son todas polinomios de Boole: $(\neg z)$, $((\neg z) \wedge y)$, $(x \vee ((\neg z) \wedge y))$, $((x \vee ((\neg z) \wedge y)) \wedge z)$.

El ejemplo anterior ilustra lo incómodo que resulta tener tantos paréntesis en la expresión de un polinomio de Boole. En la mayoría de los casos estos pueden ser omitidos sin mucho problema a condición que se deje claro el orden en que la expresión es construida.

Realizaremos ahora algunas observaciones acerca de la forma en que hemos definido los polinomios de Boole. Si $p \notin V \cup \{0,1\}$, entonces sólo puede darse una de las siguientes opciones: $p = \neg q$, $p = q \vee r$ o $p = q \wedge r$. Si $p = \neg q$ y p involucra las variables $x_1, \ldots x_n$, entonces el polinomio q debe involucrar exactamente las mismas variables. Esto puede ser expresado escribiendo

$$p(x_1, \ldots, x_n) = \neg q(x_1, \ldots x_n).$$

Si por otro lado $p = q \vee r$ y p involucra las variables $x_1, \ldots, x_n$, entonces las variables involucradas en q y r deben ser un subconjunto de éstas. Supogamos que $x_{i_1}, \ldots x_{i_k}$ son las variables involucradas

en q y $x_{j_1}, \dots x_{j_l}$ las variables involucradas en r. En ese caso, para dejar constancia de las variables involucradas, escribiremos

$$p(x_1, \dots, x_n) = q(x_{i_1}, \dots, x_{i_k}) \vee r(x_{j_1}, \dots, x_{j_l}).$$

De manera similar, si $p = q \wedge r$ escribiremos

$$p(x_1, \dots, x_n) = q(x_{i_1}, \dots, x_{i_k}) \wedge r(x_{j_1}, \dots, x_{j_l}).$$

Los polinomios, así expresados, nos permiten «sustituir» sus variables por elementos de un álgebra de Boole y obtener expresiones que indiquen operaciones de manera coherente. Vamos a precisar esto teniendo cuidado de distinguir los símbolos involucrados en un polinomio de Boole y las operaciones en un álgebra de Boole. No abundaremos en la distinción pues en este punto debe parecer una trivialidad.

Definición 14.2. Sea L un álgebra de Boole con conjunto base A y sea también p un polinomio de Boole cualquiera. Definimos *la función determinada por p para L*, en símbolos $\varphi_{L,p}$, con las siguientes posibilidades:

- Si $p = 0$, entonces $\varphi_{L,p} \colon A \to A$ donde $\varphi_{L,p}(a) = 0_L$.
- Si $p = 1$, entonces $\varphi_{L,p} \colon A \to A$ donde $\varphi_{L,p}(a) = 1_L$.
- Si $p \in V$, entonces $\varphi_{L,p} \colon A \to A$ donde $\varphi_{L,p}(a) = a$.
- Si $p(x_1, \dots, x_n) = \neg q(x_1, \dots, x_n)$, entonces $\varphi_{L,p} \colon A^n \to A$ donde
$$\varphi_{L,p}(a_1, \dots, a_n) = \neg \varphi_{L,q}(a_1, \dots, a_n)$$
- Si $p(x_1, \dots, x_n) = q(x_{i_1}, \dots, x_{i_k}) \vee r(x_{j_1}, \dots, x_{j_l})$, entonces $\varphi_{L,p} \colon A^n \to A$ donde
$$\varphi_{L,p}(a_1, \dots, a_n) = \varphi_{L,q}(a_{i_1}, \dots, a_{i_k}) \vee \varphi_{L,r}(a_{j_1}, \dots, a_{j_l}).$$
- Si $p(x_1, \dots, x_n) = q(x_{i_1}, \dots, x_{i_k}) \wedge r(x_{j_1}, \dots, x_{j_l})$, entonces $\varphi_{L,p} \colon A^n \to A$ donde
$$\varphi_{L,p}(a_1, \dots, a_n) = \varphi_{L,q}(a_{i_1}, \dots, a_{i_k}) \wedge \varphi_{L,r}(a_{j_1}, \dots, a_{j_l}).$$

Por voluminosa y arcana que parezca la anterior definición, ésta trata simplemente de cambiar las apariciones de los símbolos en el polinomio por la estructura correspondiente en el álgebra de Boole utilizando una definición recursiva. Sin embargo, no debe pensarse que es una labor estéril y que podríamos haber simplemente definido el concepto de manera sencillo. Al contrario, ahora podemos estudiar las funciones asociadas con total pulcritud y sin necesidad de particularizar. Eso es motivo suficiente para esta presentación.

Ejemplo. Consideremos el polinomio $p = x \wedge (y \vee z)$ y el álgebra 2^A para algún conjunto de A. En ese caso, la función asociada a p en esta retícula tiene como regla de correspondencia

$$(S, T, U) \mapsto S \cap (T \cup U).$$

Esto se debe simplemente a la estructura del álgebra de un conjunto potencia y a la construcción que se da en la definición de función asociada.

Definición 14.3. Una función $\beta\colon \{0,1\}^n \to \{0,1\}$ se dice *una función de Boole*. Para un polinomio p, la función determinada por p para **2** se denomina *la función de Boole inducida por* p, la cual se denota por β_p. Además, diremos que los polinomios p y q son *equivalentes*, en símbolos $p \cong q$, si inducen la misma función de Boole.

De manera alegórica, podemos afirmar que dos polinomios de Boole son equivalente si podemos transformar uno en el otro usando solamente propiedades válidas de todas las álgebras de Boole. Esta idea, sin embargo, no será la gobierne nuestro resultados.

Ejemplo. Consideremos los polinomios $p = x \vee (y \wedge z)$ y $q = (x \vee y) \wedge (x \vee y)$. Podemos afirmar que p y q resultan equivalentes al tener

$$\begin{aligned}\beta_p(a,b,c) &= a \vee (b \wedge c)\\ &= (a \vee b) \wedge (a \vee c)\\ &= \beta_q(a,b,c).\end{aligned}$$

Este ejemplo en particular muestra que una de las leyes de DeMorgan se mantiene a través de la equivalencia en polinomios de Boole. Debe notarse que estos son símbolos y no operaciones pero de igual forma, podemos dar expresiones, sino iguales, equivalentes que obedezcan las mismas reglas.

Es quizá interesante observar, que las funciones de Boole son una forma general de presentar las denominadas tablas de verdad. En realidad, las tablas de verdad son representaciones exhaustivas de una función de Boole y en muchas ocasiones podemos recurrir a ellas para representar y comparar dos polinomios de Boole.

Ejemplo.

Teorema 14.1. *Sea β una función de Boole y para cada $a = (a_1, \ldots, a_n) \in \{0,1\}^n$ sea p_a el polinomio de Boole definido por*

$$p_a(x_1, \ldots, x_n) = x_1^{\epsilon_1} \wedge \cdots \wedge x_k^{\epsilon_k}$$

donde

$$x_k^{\epsilon_k} = \begin{cases} x_k & si\ a_k = 1 \\ \neg x_k & si\ a_k = 0. \end{cases}$$

Entonces, β es la función de Boole asociada al polinomio

$$p(x_1, \ldots, x_n) = \bigvee \{p_a(x_1, \ldots, x_n) \mid F(a) = 1\}.$$

Corolario 14.2. *Para cualquier función de Boole β, existe un polinomio de Boole p de forma que $\beta = \beta_p$. En particular, existe un número menor de funciones de Boole con n entradas que polinomios de Boole con n variables.*

2. Formas normales

Definición 14.4. Por *literal*, entenderemos un polinomio de Boole que sea una variable o una negación de una variable, i.e., un polinomio de la forma

$$x^{\epsilon} = \begin{cases} x & \text{si } \epsilon = 1 \\ \neg x & \text{si } \epsilon = 0. \end{cases}$$

Es importante notar que las literales son simplemente variables o negaciones de una variable. Esto quiere decir que, sin importar quien sea la literal l, la función $\beta_l \colon \{0,1\} \to \{0,1\}$, inducida por la literal l, es o la identidad o la negación. Por esta razón, a pesar de que no necesariamente $\neg l$ es una literal, la tomaremos como una, i.e., si $l = \neg x$ tomaremos $\neg l = x$. Esta convención acerca de las literales, se mantendrá en lo que resta del capítulo.

Definición 14.5. Un polinomio $p(x_1, \ldots, x_n)$ se dice un *mintérmino sobre las variables* $x_1, \ldots, x_n$ si podemos expresarlo como la conjunción de literales que involucren a estas variables, i.e., si podemos expresarlo como

$$p = x_1^{\epsilon_1} \wedge \cdots \wedge x_n^{\epsilon_n}.$$

Definición 14.6. Sea $p(x_1, \ldots, x_n)$ un polinomio de Boole. En ese caso, p se dice que está en *forma normal disyuntiva*, abreviando FND, si $p = 0$ o si existen mintérminos $m_1, \ldots, m_k$ en las variables $x_1, \ldots, x_n$ y todos distintos entre sí, de forma que

$$p = m_1 \vee \cdots \vee m_k.$$

Según el teorema 14.1, cada función de Boole es inducida por un polinomio de Boole en la forma normal disjuntiva. Esto implica que si p es cualquier polinomio de Boole y β_p la función de Boole inducida por p, entonces existe un polinomio q en forma normal disyuntiva tal que $\beta_p = \beta_q$. Lo anterior permite concluir que p es equivalente a q, lo que da pie al siguiente teorema.

Teorema 14.3. *Todo polinomio de Boole es equivalente a un polinomio en FND.*

La prueba que hemos dado a este teorema, en realidad oculta el proceso por el cual conseguimos un polinomio en forma normal disyuntiva. Podemos, sin embargo, recrearlo sin mucho esfuerzo. Tomemos para esto un polinomio $p(x_1, \ldots, x_n)$ y consideremos los siguientes pasos:

1. Si $\neg$ ocurre en cualquier lugar que no sea directamente en las variables $x_1, \ldots, x_n$, lo reducimos usando las leyes de DeMorgan, las cuales en este caso son

   $$x \vee (y \wedge z) \cong (x \vee y) \wedge (x \vee z)$$

   y

   $$x \wedge (y \vee z) \cong (x \wedge y) \vee (x \wedge z).$$

2. Utilizando la ley distributiva, se expresa a p como una disyunción de conjunciones, eliminando las posibles repeticiones. Esto es posible pues $x \vee x \cong x$.

3. Requerimos finalmente que las variables aparezcan en una y sólo una de las literales involucradas en cada conjunción resultante. Si la variable está repetida, simplemente removemos la repetición. Si por otro lado, la conjunción contiene tanto a x_j como a $\neg x_j$ simplemente la descartamos. Finalmente, si la variable x_j no ocurriera en la conjunción

   $$x_{i_1}^{\epsilon_{i_1}} \wedge \cdots \wedge x_{i_k}^{\epsilon_{i_k}}$$

   entonces,

   $$\begin{aligned} x_{i_1}^{\epsilon_{i_1}} \wedge \cdots \wedge x_{i_k}^{\epsilon_{i_k}} &\cong \left(x_{i_1}^{\epsilon_{i_1}} \wedge \cdots \wedge x_{i_k}^{\epsilon_{i_k}}\right) \wedge (x_j \vee \neg x_j) \\ &\cong \left(x_{i_1}^{\epsilon_{i_1}} \wedge \cdots \wedge x_{i_k}^{\epsilon_{i_k}} \wedge x_j\right) \vee \left(x_{i_1}^{\epsilon_{i_1}} \wedge \cdots \wedge x_{i_k}^{\epsilon_{i_k}} \wedge \neg x_j\right). \end{aligned}$$

   Repitiendo este paso para todas las variables y todas las conjunciones, obtendremos un polinomio equivalente a p que será una disyunción de mintérminos.

Ejemplo. Vamos a expresar el polinomio de Boole $p = x \wedge \neg(y \wedge \neg z)$ en forma normal disjuntiva. Usando la ley de DeMorgan y luego la propiedad distributiva, tenemos que $p = x \wedge (\neg y \vee z) = (x \wedge \neg y) \vee (x \wedge z)$ que expresa a p como una disyunción de conjunciones. El primer término $x \wedge \neg y$ en esta disyunción no contiene z o $\neg z$, y el segundo término $x \wedge z$ es libre de y, $\neg y$. Por lo tanto, haciendo conjunción entre el primero y $z \vee \neg z$, y entre el segundo junto con $y \vee \neg y$, resulta

$$\begin{aligned} p &= ((x \wedge \neg y) \wedge (z \vee \neg z)) \vee (x \wedge (y \vee \neg y) \wedge z) \\ &= (x \wedge \neg y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z) \vee (x \wedge \neg y \wedge z) \end{aligned}$$

El término $x \wedge \neg y \wedge z$ ocurre dos veces. Borrando uno de estos (usando la propiedad de idempotencia), tenemos la forma normal disjuntiva de p dada por

$$p = (x \wedge \neg y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z).$$

Vamos ahora a describir los conceptos duales de lo anterior. Los resultados asociados, por supuesto, serán resultado del principio de dualidad.

Definición 14.7. Un polinomio $p(x_1, \ldots, x_n)$ se dice un *maxtérmino sobre las variables* $x_1, \ldots, x_n$ si podemos expresarlo como la disyunción de literales que involucren a estas variables, i.e., si podemos expresarlo como

$$p = x_1^{\epsilon_1} \vee \cdots \vee x_n^{\epsilon_n}.$$

Definición 14.8. Sea $p(x_1, \ldots, x_n)$ un polinomio de Boole. En ese caso, p se dice que está en *forma normal conjuntiva*, abreviando FNC, si $p = 0$ o si existen maxtérminos $m_1, \ldots, m_k$ en las variables $x_1, \ldots, x_n$ y todos distintos entre sí, de forma que

$$p = m_1 \wedge \cdots \wedge m_k.$$

No debe ser difícil dar con la versión del teorema 14.1. En ésta, debe observarse, que en lugar de mintérminos estarán involucrado máxterminos y bajo el mismo argumento que se usó para garantizar el teorema 14.3, podemos formular un teorema análogo.

Teorema 14.4. *Todo polinomio Booleano puede ser expresado en FNC.*

Tampoco debe ser difícil adaptar el procedimiento descrito para obtener de manera mecánica la forma normal conjuntiva. Realmente, todos estos resultados son consecuencia el principio de dualidad y, bajo la óptica adecuada, basta cambiar obtener los enunciados duales de cada uno para obtener el resultado adecuado.

Referencias

[DP02] Davey, Brian A. y Priestley, Hilary A.: *Introduction to lattices and order*. Cambridge University Press, 2002.

[Gri97] Grimaldi, Ralph P.: *Matemáticas discreta y combinatoria*. Addison Wesley Iberoamericana, 3ª edición, 1997.

[Gó07] Gómez Laveaga, Carmen: *Introducción a la teoría intuitiva de conjuntos*. Las Prensas de Ciencias, 2007.

Considerar notas el texto precedente es producto de la imaginación febril de autor. El único propósito al que sirven es dar una interpretación personal de algunos textos que han sido usados para preparar el curso de «Matemáticas discretas» impartido en la carrera de Matemáticas Aplicadas y Computación de la FES Acatlán. Es muy probable que el presente texto esté lleno de errores gramaticales, imprecisiones técnicas y sea sujeto a cambios constantes.