IIC1253 Matemáticas Discretas

Sasha Kozachinskiy

DCC UC

06.08.2025

Hoy...

Hoy...

- Lógica proposicional: formas normales, conectivos funcionalmente completos.

Repaso: conectivos

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$
1	1	0	1	1	1
1	0	0	0	1	0
0	1	1	0	1	1
0	0	1	0	0	1

Repaso: conectivos

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$
1	1	0	1	1	1
1	0	0	0	1	0
0	1	1	0	1	1
0	0	1	0	0	1

¿Son todos necesarios?

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, tenemos que con $\neg$ y cualquier otro conectivo se puede expresar los demas, pero para $\neg A$ no existe una fórmula proposicional equivalente que usa solo $\wedge, \vee, \rightarrow$.

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, *tenemos que con* $\neg$ *y cualquier otro conectivo se puede expresar los demas, pero para* $\neg A$ *no existe una fórmula proposicional equivalente que usa solo* $\wedge, \vee, \rightarrow$.

Demostración parte 1.

$$\neg, \wedge \longrightarrow \vee, \rightarrow$$

$$\neg, \vee \longrightarrow \wedge, \rightarrow$$

$$\neg, \rightarrow \longrightarrow \vee, \wedge$$

$$A \vee B = \neg\neg(A \vee B) = \neg(\neg A \wedge \neg B)$$

$$A \wedge B = \neg\neg(A \wedge B) = \neg(\neg A \vee \neg B)$$

$$A \rightarrow B = \neg A \vee B$$

$$A \vee B = \neg\neg A \vee B = \neg(\neg A) \vee B = \neg A \rightarrow B$$

$\square$

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$*, tenemos que con* $\neg$ *y cualquier otro conectivo se puede expresar los demas, pero para* $\neg A$ *no existe una fórmula proposicional equivalente que usa solo* $\wedge, \vee, \rightarrow$*.*

Demostración parte 2.

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, *tenemos que con* $\neg$ *y cualquier otro conectivo se puede expresar los demas, pero para* $\neg A$ *no existe una fórmula proposicional equivalente que usa solo* $\wedge, \vee, \rightarrow$.

Demostración parte 2.

- Sea ϕ cualquier fórmula proposicional con $\wedge, \vee, \rightarrow$ y con una variable proposicional A

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, *tenemos que con* $\neg$ *y cualquier otro conectivo se puede expresar los demas, pero para* $\neg A$ *no existe una fórmula proposicional equivalente que usa solo* $\wedge, \vee, \rightarrow$.

Demostración parte 2.

- Sea ϕ cualquier fórmula proposicional con $\wedge, \vee, \rightarrow$ y con una variable proposicional A
- Por ejemplo, $\phi = ((A \rightarrow A) \wedge (A \vee A)) \rightarrow (A \wedge A)$.

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, *tenemos que con* $\neg$ *y cualquier otro conectivo se puede expresar los demas, pero para* $\neg A$ *no existe una fórmula proposicional equivalente que usa solo* $\wedge, \vee, \rightarrow$.

Demostración parte 2.

- Sea ϕ cualquier fórmula proposicional con $\wedge, \vee, \rightarrow$ y con una variable proposicional A
- Por ejemplo, $\phi = ((A \rightarrow A) \wedge (A \vee A)) \rightarrow (A \wedge A)$.
- Queremos mostrar que $\neg A$ y ϕ no son equivalentes.

como se expresan los conectivos entre sí

Teorema

Entre $\neg, \wedge, \vee, \rightarrow$, tenemos que con $\neg$ y cualquier otro conectivo se puede expresar los demas, pero para $\neg A$ no existe una fórmula proposicional equivalente que usa solo $\wedge, \vee, \rightarrow$.

Demostración parte 2.

- Sea ϕ cualquier fórmula proposicional con $\wedge, \vee, \rightarrow$ y con una variable proposicional A
- Por ejemplo, $\phi = ((A \rightarrow A) \wedge (A \vee A)) \rightarrow (A \wedge A)$.
- Queremos mostrar que $\neg A$ y ϕ no son equivalentes.
- Si fijamos $A = 1$, el valor de cada conectivo en ϕ será 1.

$\square$

otros conectivos?

otros conectivos?

- ¿Existe un conectivo (a.k.a. *función Booleana*) $f(X_1, X_2, \dots, X_n)$ que no se expresa a través de $\neg, \wedge, \vee, \rightarrow$?

otros conectivos?

- ¿Existe un conectivo (a.k.a. *función Booleana*) $f(X_1, X_2, \ldots, X_n)$ que no se expresa a través de $\underbrace{\neg, \wedge, \vee, \rightarrow}$?

$$f(x,y) = x + y$$

Definición

Una función booleana de n variables es una función que mapea cada tupla de n 0s y 1s a 0 o 1.

otros conectivos?

- ¿Existe un conectivo (a.k.a. *función Booleana*) $f(X_1, X_2, \ldots, X_n)$ que no se expresa a través de $\neg, \wedge, \vee, \rightarrow$?

Definición

Una función booleana de n variables es una función que mapea cada tupla de n 0s y 1s a 0 o 1.

- ¡No existe!

Teorema

Para cada función booleana existe una fórmula proposicional equivalente con $\neg, \wedge, \vee, \rightarrow$.

Ejemplos

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

$$A \oplus B = \underline{\big((A \lor B) \land \neg(A \land B)\big)}$$

Ejemplos

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Ejemplos

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

X_1	X_2	X_3	$\mathrm{MAJ}_3(X_1, X_2, X_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$\mathrm{MAJ}_3(X_1, X_2, X_3)$

$= (X_1 \wedge X_2) \vee (X_1 \wedge X_3)$

$\vee (X_2 \wedge X_3)$

$\vdots$

C

DNFs

Definición (DNF)

- *Una cláusula conjutiva es una conjunción de los variables y su negaciones, por ejemplo:*

$$X_1 \wedge (\neg X_3), \qquad X_2 \wedge (\neg X_5) \wedge (X_7).$$

- *Una DNF (forma normal disyuntiva) es una disyunción de cláusulas conjuntivas, por ejemplo:*

$$\Big(X_1 \wedge (\neg X_3)\Big) \vee \Big(X_2 \wedge (\neg X_5) \wedge X_7)\Big) \vee \Big(X_1 \wedge X_3\Big)$$

DNFs

Definición (DNF)

- *Una cláusula conjutiva es una conjunción de los variables y su negaciones, por ejemplo:*

$$X_1 \wedge (\neg X_3), \qquad X_2 \wedge (\neg X_5) \wedge (X_7).$$

- *Una DNF (forma normal disyuntiva) es una disyunción de cláusulas conjuntivas, por ejemplo:*

$$\Big(X_1 \wedge (\neg X_3)\Big) \vee \Big(X_2 \wedge (\neg X_5) \wedge X_7)\Big) \vee \Big(X_1 \wedge X_3\Big)$$

Teorema

Para cada función booleana existe una DNF equivalente.

Pregunta DNF

$$\Big(X_1 \wedge (\neg X_3)\Big) \vee \Big(X_2 \wedge (\neg X_5) \wedge X_7)\Big) \vee \Big(X_1 \wedge X_3\Big) \tag{1}$$

Pregunta DNF

$$\Big(X_1 \wedge (\neg X_3)\Big) \vee \Big(X_2 \wedge (\neg X_5) \wedge X_7)\Big) \vee \Big(X_1 \wedge X_3\Big) \qquad (1)$$

- ¿Cuál es el valor de (1) cuando todos los variables son 0?

Pregunta DNF

$$\Big(X_1 \wedge (\neg X_3)\Big) \vee \Big(X_2 \wedge (\neg X_5) \wedge X_7)\Big) \vee \Big(X_1 \wedge X_3\Big) \qquad (1)$$

- ¿Cuál es el valor de (1) cuando todos los variables son 0? 0
- ¿Y cuando todos son 1? 1

Construyendo una DNF: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Construyendo una DNF: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

$$f = \big((\neg X_1) \wedge (\neg X_2) \wedge \neg X_3\big)$$
$$\vee \big((\neg X_1) \wedge (\neg X_2) \wedge X_3\big)$$
$$\vee \big((\neg X_1) \wedge X_2 \wedge (\neg X_3)\big)$$
$$\vee \big(X_1 \wedge (\neg X_2) \wedge (\neg X_3)\big)$$

DNFs expresan todo

Teorema

Para cada función booleana existe una DNF equivalente.

DNFs expresan todo

Teorema

Para cada función booleana existe una DNF equivalente.

Demostración.

- Sea $f(X_1, X_2, \ldots, X_n)$ una función Booleana de n variables.

DNFs expresan todo

Teorema

Para cada función booleana existe una DNF equivalente.

Demostración.

- Sea $f(X_1, X_2, \ldots, X_n)$ una función Booleana de n variables.
- Para cada tupla $\bar{\alpha} = (\alpha_1, \ldots, \alpha_n)$ de 0s y 1s, construimos una cláusula conjunctiva $C_{\bar{\alpha}}$:

$$C_{\bar{\alpha}}(X_1, \ldots, X_n) = \mathbb{I}\{(X_1, \ldots, X_n) = \bar{\alpha}\}$$
$$\left(\begin{cases} X_1 & \alpha_1 = 1 \\ \neg X_1 & \alpha_1 = 0 \end{cases}\right) \wedge \ldots \wedge \left(\begin{cases} X_n & \alpha_n = 1 \\ \neg X_n & \alpha_n = 0 \end{cases}\right)$$

DNFs expresan todo

Teorema

Para cada función booleana existe una DNF equivalente.

Demostración.

- Sea $f(X_1, X_2, \ldots, X_n)$ una función Booleana de n variables.
- Para cada tupla $\bar{\alpha} = (\alpha_1, \ldots, \alpha_n)$ de 0s y 1s, construimos una cláusula conjunctiva $C_{\bar{\alpha}}$:

$$C_{\bar{\alpha}}(X_1, \ldots, X_n) = \mathbb{I}\{(X_1, \ldots, X_n) = \bar{\alpha}\}$$
$$\left(\begin{cases} X_1 & \alpha_1 = 1 \\ \neg X_1 & \alpha_1 = 0 \end{cases}\right) \wedge \ldots \wedge \left(\begin{cases} X_n & \alpha_n = 1 \\ \neg X_n & \alpha_n = 0 \end{cases}\right)$$

- $f(X_1, \ldots, X_N) = \bigvee_{\bar{\alpha}: f(\bar{\alpha}) = 1} C_{\bar{\alpha}}(X_1, \ldots, X_N)$

□

CNFs

Definición (CNF)

- *una cláusula disyunctiva es una disyunción de variables y sus negaciones, por ejemplo:*

$$((\neg X_1) \vee X_2 \vee X_7), \qquad ((\neg Y) \vee (\neg Z)).$$

- *una CNF (forma normal conjunctiva) es una conjunción de cláusulas disyunctivas, por ejemplo,*

$$(X \vee Y) \wedge ((\neg X) \vee (\neg Y)). \tag{2}$$

CNFs

Definición (CNF)

- *una cláusula disyunctiva es una disyunción de variables y sus negaciones, por ejemplo:*

$$((\neg X_1) \vee X_2 \vee X_7), \qquad ((\neg Y) \vee (\neg Z)).$$

- *una CNF (forma normal conjunctiva) es una conjunción de cláusulas disyunctivas, por ejemplo,*

$$(X \vee Y) \wedge ((\neg X) \vee (\neg Y)). \tag{2}$$

Teorema

Para cada función booleana existe una CNF equivalente.

Pregunta CNF

?Existe la asignación de las variables tal que la CNF:

$$\underbrace{(X \vee Y)}_{C_1} \wedge \underbrace{(\neg X \vee \neg Y)}_{C_2} \wedge (X \vee Z) \wedge (\neg X \vee \neg Z) \wedge (Y \vee Z) \wedge (\neg Y \vee \neg Z)$$

toma valor 1?

$C_1 = 0 \iff X = Y = 0$

$C_2 = 0 \iff X = Y = 1$

No, porque siempre hay dos 0's o dos 1's

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Repaso: la ley de Morgan

$$\neg(A \vee B) = (\neg A) \wedge (\neg B), \qquad \neg(A \wedge B) = (\neg A) \vee (\neg B)$$

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Repaso: la ley de Morgan

$$\neg(A \vee B) = (\neg A) \wedge (\neg B), \qquad \neg(A \wedge B) = (\neg A) \vee (\neg B)$$

Lema

$\neg(A_1 \vee \ldots \vee A_n) = (\neg A_1) \wedge \ldots \wedge (\neg A_n)$

$\neg(A_1 \wedge \ldots \wedge A_n) = (\neg A_1) \vee \ldots \vee (\neg A_n)$ ✓

Demostración.

$\neg(A_1 \vee \ldots \vee A_n) = \neg(A_1 \vee \underbrace{(A_2 \vee \ldots \vee A_n)}) =$

$= \neg A_1 \wedge \neg(A_2 \vee \ldots \vee A_n) = \neg A_1 \wedge \neg A_2 \wedge \neg(A_3 \vee \ldots \vee A_n)$

$= \ldots = (\neg A_1) \wedge (\neg A_2) \ldots \wedge (\neg A_n)$

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Demostración.

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Demostración.

- sea f una función booleana.

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Demostración.

- sea f una función booleana.
- $\neg f = D$ para una DNF D:

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Demostración.

- sea f una función booleana.
- $\neg f = D$ para una DNF D:
- Entonces, $f = \neg\neg f = \neg D$.

CNFs expresan todo

Teorema

Para cada función booleana existe una CNF equivalente.

Demostración.

- sea f una función booleana.
- $\neg f = D$ para una DNF D:
- Entonces, $f = \neg\neg f = \neg D$.
- la negación de una DNF se transforma a una CNF según la ley de Morgan:

$$\neg \bigvee \bigwedge (X, \neg X) = \bigwedge \neg \bigwedge (X, \neg X) = \bigwedge \bigvee \neg (X, \neg X)$$
$$= \bigwedge \bigvee (X, \neg X).$$

$\square$

Construyendo una CNF: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Construyendo una CNF: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$	$\neg f$
0	0	0	1	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	0

Construyendo una CNF: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$	$\neg f$
0	0	0	1	0
0	0	1	0	1
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	0

$$\neg f =$$

$$= (\neg X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3)$$

$$f = \neg\neg f =$$

$$= \neg\big((\neg X_1 \wedge \neg X_2 \wedge X_3) \vee (X_1 \wedge \neg X_2 \wedge X_3)\big)$$

$$= \big(\neg(\neg X_1 \wedge \neg X_2 \wedge X_3)\big) \wedge \big(\neg(X_1 \wedge \neg X_2 \wedge X_3)\big)$$

$$= (X_1 \vee X_2 \vee \neg X_3) \wedge (\neg X_1 \vee X_2 \vee \neg X_3))$$

Comletitud funcional

Definición

Un conjunto $\{f_1, \ldots, f_m\}$ *de funciones booleanas es* **funcionalmente completo** *si para cada función booleana existe una formula equivalente que usa cómo conectivos solo elementos de* $\{f_1, \ldots, f_m\}$*.*

Comletitud funcional

Definición

Un conjunto $\{f_1, \dots, f_m\}$ *de funciones booleanas es* **funcionalmente completo** *si para cada función booleana existe una formula equivalente que usa cómo conectivos solo elementos de* $\{f_1, \dots, f_m\}$*.*

Proposición

$\{\wedge, \vee, \rightarrow\}, \{\neg\}$ *no son funcionalmente completos.*
$\{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \rightarrow\}$ *sí son funcionalmente completos.*

Dem $\neg A$ no se puede exp. a través $\wedge, \vee, \rightarrow$

$\neg\neg\dots\neg A \Rightarrow \{\neg\}$ no es func. comp.

$\{\neg, \wedge\} \Rightarrow \vee \Rightarrow$ DNFS $\Rightarrow$ todo

$A \vee B = \neg((\neg A)\wedge(\neg B))$

$\{\neg, \vee\} \Rightarrow \wedge \Rightarrow$ DNFs $\Rightarrow$ todo

$\{\neg, \rightarrow\} \Rightarrow \wedge, \vee \Rightarrow$ DNFs $\Rightarrow$ todos

Una función es suficiente

Teorema

$\{\text{nand}\}$ *es funcionalmente completo, donde* $\text{nand}(x, y) = \neg(x \wedge y)$.

Demostración.

Una función es suficiente

Teorema

$\{\text{nand}\}$ *es funcionalmente completo, donde* $\text{nand}(x, y) = \neg(x \wedge y)$.

Demostración.

Basta expresar, digamos, $\neg, \wedge$, a través de nand.

Para demostrar $\{f_1, \ldots, f_m\}$ es f.c., basta ver $\neg, \wedge$ se puede expres a través $f_1, \ldots, f_m$.

$\Leftrightarrow$ tmb. basta mostrar $\neg, \vee$ se puede exp. a través de $f_1, \ldots, f_m$.

$\square$

$\neg x = \text{nand}(x, x) = \neg(x \wedge x)$

$x \wedge y = \neg\, \text{nand}(x, y) = \text{nand}(\text{nand}(x, y), \text{nand}(x, y))$

¡Gracias!

XOR

Definición

$\oplus$ denota la siguiente función booleana

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

XOR

Definición

$\oplus$ *denota la siguiente función booleana*

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

Proposición

$A \oplus B = B \oplus A$, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

XOR

Definición

$\oplus$ *denota la siguiente función booleana*

A	B	$A \oplus B$
1	1	0
1	0	1
0	1	1
0	0	0

Proposición

$A \oplus B = B \oplus A$, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

Proposición

$A \wedge (B \oplus C) = (A \wedge B) \oplus (A \wedge C)$.

Proposición

$A \oplus B = B \oplus A$, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

Demostración.

$\square$

Proposición

$A \oplus B = B \oplus A$, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$.

Demostración.

$\square$

Proposición

$A \wedge (B \oplus C) = (A \wedge B) \oplus (A \wedge C)$.

Demostración.

$\oplus, \wedge, 1$

Teorema

$\{\oplus, \wedge, 1\}$ *es funcionalmente completo.*

$\oplus, \wedge, 1$

Teorema

$\{\oplus, \wedge, 1\}$ *es funcionalmente completo.*

Demostración.

$\neg X =$ $\square$

forma normal para $\{\oplus, \wedge, 1\}$ – polinomios de Zhegalkin

forma normal para $\{\oplus, \wedge, 1\}$ – polinomios de Zhegalkin

- un *monomio de Zhegalkin* es una conjunción de las variables (incluso constante 1), por ejemplo:

$$1, \qquad X_1 \wedge X_3, \qquad X_2 \wedge X_5 \wedge X_1.$$

forma normal para $\{\oplus, \wedge, 1\}$ – polinomios de Zhegalkin

- un *monomio de Zhegalkin* es una conjunción de las variables (incluso constante 1), por ejemplo:

$$1, \qquad X_1 \wedge X_3, \qquad X_2 \wedge X_5 \wedge X_1.$$

- un *polinomio de Zhegalkin* es un $\oplus$ de monomios de Zhegalkin, por ejemplo

$$(X \wedge Y) \oplus X \oplus Y$$

- ¿Que función calcula este polinomio?

Teorema

Para cada función booleana existe un polinomio de Zhegalkin equivalente.

Construyendo un polinomio de Zhegalkin: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Construyendo un polinomio de Zhegalkin: ejemplo

X_1	X_2	X_3	$f(X_1, X_2, X_3)$	
0	0	0	1	
0	0	1	1	
0	1	0	1	
0	1	1	0	1
1	0	0	1	$X_1,\ X_2,\ X_3$
1	0	1	0	$X_1 \wedge X_2,\ X_1 \wedge X_3,\ X_2 \wedge X_3$
1	1	0	0	$X_1 \wedge X_2 \wedge X_3$
1	1	1	0	