

Dos nociones útiles

Decimos que una $\mathcal{L}$ -fórmula φ es **satisfacible** si existe una $\mathcal{L}$ -estructura $\mathfrak{A}$ y una asignación σ para $\mathfrak{A}$ tal que $(\mathfrak{A}, \sigma) \models \varphi$.

- Si φ es oración, entonces φ es satisfacible si existe $\mathfrak{A}$ tal que $\mathfrak{A} \models \varphi$

Dos nociones útiles

Decimos que una $\mathcal{L}$ -fórmula φ es **satisfacible** si existe una $\mathcal{L}$ -estructura $\mathfrak{A}$ y una asignación σ para $\mathfrak{A}$ tal que $(\mathfrak{A}, \sigma) \models \varphi$.

- ▶ Si φ es oración, entonces φ es satisfacible si existe $\mathfrak{A}$ tal que $\mathfrak{A} \models \varphi$

Decimos que una $\mathcal{L}$ -fórmula φ es **válida** si para toda $\mathcal{L}$ -estructura $\mathfrak{A}$ y toda asignación σ para $\mathfrak{A}$ se tiene que $(\mathfrak{A}, \sigma) \models \varphi$.

- ▶ Si φ es oración, entonces φ es válida si para todo $\mathfrak{A}$ se tiene que $\mathfrak{A} \models \varphi$

Dos nociones útiles

Decimos que una $\mathcal{L}$ -fórmula φ es **satisfacible** si existe una $\mathcal{L}$ -estructura $\mathfrak{A}$ y una asignación σ para $\mathfrak{A}$ tal que $(\mathfrak{A}, \sigma) \models \varphi$.

- ▶ Si φ es oración, entonces φ es satisfacible si existe $\mathfrak{A}$ tal que $\mathfrak{A} \models \varphi$

Decimos que una $\mathcal{L}$ -fórmula φ es **válida** si para toda $\mathcal{L}$ -estructura $\mathfrak{A}$ y toda asignación σ para $\mathfrak{A}$ se tiene que $(\mathfrak{A}, \sigma) \models \varphi$.

- ▶ Si φ es oración, entonces φ es válida si para todo $\mathfrak{A}$ se tiene que $\mathfrak{A} \models \varphi$

Ejercicio

Construya una fórmula válida.

Dos nociones útiles

Al igual que en la lógica proposicional, la lógica de primer orden tiene asociados algunos problemas de decisión:

$SAT = \{\varphi \mid \varphi \text{ es una oración satisfacible}\}$

$VAL = \{\varphi \mid \varphi \text{ es una oración válida}\}$

Dos nociones útiles

Al igual que en la lógica proposicional, la lógica de primer orden tiene asociados algunos problemas de decisión:

$SAT = \{\varphi \mid \varphi \text{ es una oración satisfacible}\}$

$VAL = \{\varphi \mid \varphi \text{ es una oración válida}\}$

¿Son estos problemas más difíciles que para el caso de la lógica proposicional?

- ▶ ¿Cómo se demuestra que son al menos tan difíciles?

Dos nociones útiles

Al igual que en la lógica proposicional, la lógica de primer orden tiene asociados algunos problemas de decisión:

$SAT = \{\varphi \mid \varphi \text{ es una oración satisfacible}\}$

$VAL = \{\varphi \mid \varphi \text{ es una oración válida}\}$

¿Son estos problemas más difíciles que para el caso de la lógica proposicional?

- ▶ ¿Cómo se demuestra que son al menos tan difíciles?

Vamos a mostrar una primera diferencia entre estas dos lógicas ...

La complejidad de VAL

Teorema (Church)

VAL es indecidible.

La complejidad de VAL

Teorema (Church)

VAL es indecidible.

Demostración: Vamos a reducir el siguiente problema a VAL:

$$L = \{w \in \{0,1\}^* \mid \text{existe una MT determinista } M$$

tal que $w = C(M)$ y M acepta $\varepsilon\}$.

¿Por qué es este problema indecidible?

La complejidad de VAL

Para cada MT M determinista, tenemos que construir una fórmula φ_M tal que:

M acepta ε si y sólo si φ_M es válida

La complejidad de VAL

Para cada MT M determinista, tenemos que construir una fórmula φ_M tal que:

M acepta ε si y sólo si φ_M es válida

Suponemos que $M = (Q, \{0, 1\}, q_0, \delta, F)$, donde

- ▶ $Q = \{q_0, \dots, q_m\}$
- ▶ $F = \{q_m\}$
- ▶ no existe una transición en δ para q_m

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

$P(t)$: t es el tiempo de partida de la máquina

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

$P(t)$: t es el tiempo de partida de la máquina

$C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t
- $B(t, p)$: M tiene un B en la posición p de la cinta en el tiempo t

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t
- $B(t, p)$: M tiene un B en la posición p de la cinta en el tiempo t
- $E_i(t)$: estado de M es q_i ($i \in [0, m]$) en el tiempo t

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t
- $B(t, p)$: M tiene un B en la posición p de la cinta en el tiempo t
- $E_i(t)$: estado de M es q_i ($i \in [0, m]$) en el tiempo t
- $T(t, p)$: la cabeza está en la posición p en el tiempo t

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t
- $B(t, p)$: M tiene un B en la posición p de la cinta en el tiempo t
- $E_i(t)$: estado de M es q_i ($i \in [0, m]$) en el tiempo t
- $T(t, p)$: la cabeza está en la posición p en el tiempo t
- $L(x, y)$: orden lineal en el dominio

La complejidad de VAL

Definimos un vocabulario $\mathcal{L}$ de la siguiente forma:

- $P(t)$: t es el tiempo de partida de la máquina
- $C(t, p)$: M tiene un 0 en la posición p de la cinta en el tiempo t
- $U(t, p)$: M tiene un 1 en la posición p de la cinta en el tiempo t
- $B(t, p)$: M tiene un B en la posición p de la cinta en el tiempo t
- $E_i(t)$: estado de M es q_i ($i \in [0, m]$) en el tiempo t
- $T(t, p)$: la cabeza está en la posición p en el tiempo t
- $L(x, y)$: orden lineal en el dominio

φ_M es definida como $(\varphi_P \wedge \varphi_L \wedge \varphi_I \wedge \varphi_C \wedge \varphi_\delta) \rightarrow \varphi_A$

La complejidad de VAL

φ_P : Hay un único punto de partida

$$\exists x(P(x) \wedge \forall y(x \neq y \rightarrow \neg P(y)))$$

La complejidad de VAL

φ_P : Hay un único punto de partida

$$\exists x(P(x) \wedge \forall y(x \neq y \rightarrow \neg P(y)))$$

φ_L : L es un orden lineal donde cada elemento tiene un sucesor y un predecesor

$$\begin{aligned} &\forall x \neg L(x, x) \wedge \forall x \forall y \forall z ((L(x, y) \wedge L(y, z)) \rightarrow L(x, z)) \wedge \\ &\quad \forall x \forall y (x = y \vee L(x, y) \vee L(y, x)) \wedge \\ &\quad \forall x \exists y (L(x, y) \wedge \neg \exists z (L(x, z) \wedge L(z, y))) \wedge \\ &\quad \forall x \exists y (L(y, x) \wedge \neg \exists z (L(y, z) \wedge L(z, x))) \end{aligned}$$

La complejidad de VAL

Usamos orden lineal L para definir un predicado auxiliar:

$$suc(x, y) = L(x, y) \wedge \neg \exists z (L(x, z) \wedge L(z, y))$$

La complejidad de VAL

Usamos orden lineal L para definir un predicado auxiliar:

$$suc(x, y) = L(x, y) \wedge \neg \exists z (L(x, z) \wedge L(z, y))$$

φ_I : Estado inicial

$$\forall x (P(x) \rightarrow (E_0(x) \wedge T(x, x) \wedge \forall y B(x, y)))$$

La complejidad de VAL

φ_C : La máquina funciona correctamente

La complejidad de VAL

φ_C : La máquina funciona correctamente

φ_C se define como la conjunción de cuatro fórmulas. Primero, cada celda siempre contiene un único símbolo:

$$\begin{aligned} \forall x \forall y \big(& (C(x, y) \wedge \neg U(x, y) \wedge \neg B(x, y)) \vee \\ & (U(x, y) \wedge \neg C(x, y) \wedge \neg B(x, y)) \vee \\ & (B(x, y) \wedge \neg C(x, y) \wedge \neg U(x, y)) \big). \end{aligned}$$

La complejidad de VAL

Segundo, la máquina siempre está en un único estado:

$$\forall x \left(\bigvee_{i=0}^m \left(E_i(x) \wedge \bigwedge_{j \in [0, m] \setminus \{i\}} \neg E_j(x) \right) \right)$$

La complejidad de VAL

Segundo, la máquina siempre está en un único estado:

$$\forall x \left(\bigvee_{i=0}^m \left(E_i(x) \wedge \bigwedge_{j \in [0, m] \setminus \{i\}} \neg E_j(x) \right) \right)$$

Tercero, la cabeza siempre está en una única posición:

$$\forall x \exists y (T(x, y) \wedge \forall z (y \neq z \rightarrow \neg T(x, z)))$$

La complejidad de VAL

Cuarto, el contenido de una celda no cambia si no es apuntada por la cabeza:

$$\forall x \forall y \forall z ((\neg T(x, y) \wedge \text{suc}(x, z)) \rightarrow ((C(x, y) \wedge C(z, y)) \vee (U(x, y) \wedge U(z, y)) \vee (B(x, y) \wedge B(z, y))))$$

La complejidad de VAL

φ_δ : función δ define como funciona la máquina

La complejidad de VAL

φ_δ : función δ define como funciona la máquina

Para cada transición en δ se define una fórmula, y φ_δ se define como la conjunción de estas fórmulas.

La complejidad de VAL

φ_δ : función δ define como funciona la máquina

Para cada transición en δ se define una fórmula, y φ_δ se define como la conjunción de estas fórmulas.

Ejemplo

Para $\delta(q_i, 0) = (q_j, 1, \leftarrow)$ se define la siguiente fórmula:

$$\forall x \forall y \forall u \forall v ((E_i(x) \wedge T(x, y) \wedge C(x, y) \wedge \\ \text{suc}(x, u) \wedge \text{suc}(v, y)) \rightarrow \\ (E_j(u) \wedge T(u, v) \wedge U(u, y)))$$

La complejidad de VAL

φ_A : La máquina acepta ε

$$\exists x \exists y (P(x) \wedge (x = y \vee L(x, y)) \wedge E_m(y))$$

La complejidad de VAL

φ_A : La máquina acepta ε

$$\exists x \exists y (P(x) \wedge (x = y \vee L(x, y)) \wedge E_m(y))$$

Para terminar sólo falta demostrar que M acepta ε si y sólo si φ_M es válida.

La complejidad de VAL

φ_A : La máquina acepta ε

$$\exists x \exists y (P(x) \wedge (x = y \vee L(x, y)) \wedge E_m(y))$$

Para terminar sólo falta demostrar que M acepta ε si y sólo si φ_M es válida.

- ¿Qué sucedería si φ_M es definida como $\varphi_P \wedge \varphi_L \wedge \varphi_I \wedge \varphi_C \wedge \varphi_\delta \wedge \varphi_A$?

La complejidad de SAT

Corolario

SAT es indecidible.

La complejidad de SAT

Corolario

SAT es indecidible.

Ejercicio

Demuestre el corolario.

La complejidad de SAT

Corolario

SAT es indecidible.

Ejercicio

Demuestre el corolario.

Para la lógica proposicional SAT era decidible (pero difícil). **¡Para la lógica de primer orden es indecidible!**

La noción de isomorfismo

Sean $\mathfrak{A} = \langle \mathbb{N}, 0^{\mathfrak{A}}, s^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle B, 0^{\mathfrak{B}}, s^{\mathfrak{B}} \rangle$ definida como:

- ▶ $B = \{0\}^*$
- ▶ $0^{\mathfrak{B}} = \varepsilon$
- ▶ $s^{\mathfrak{B}}(\underbrace{0 \cdots 0}_{n \text{ veces}}) = \underbrace{0 \cdots 0}_{n+1 \text{ veces}}$, para todo $n \geq 0$

La noción de isomorfismo

Sean $\mathfrak{A} = \langle \mathbb{N}, 0^{\mathfrak{A}}, s^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle B, 0^{\mathfrak{B}}, s^{\mathfrak{B}} \rangle$ definida como:

- ▶ $B = \{0\}^*$
- ▶ $0^{\mathfrak{B}} = \varepsilon$
- ▶ $s^{\mathfrak{B}}(\underbrace{0 \cdots 0}_{n \text{ veces}}) = \underbrace{0 \cdots 0}_{n+1 \text{ veces}}$, para todo $n \geq 0$

¿Son similares estas estructuras? ¿Por qué?

La noción de isomorfismo

Sean $\mathfrak{A} = \langle \mathbb{N}, 0^{\mathfrak{A}}, s^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle B, 0^{\mathfrak{B}}, s^{\mathfrak{B}} \rangle$ definida como:

- ▶ $B = \{0\}^*$
- ▶ $0^{\mathfrak{B}} = \varepsilon$
- ▶ $s^{\mathfrak{B}}(\underbrace{0 \cdots 0}_{n \text{ veces}}) = \underbrace{0 \cdots 0}_{n+1 \text{ veces}}, \text{ para todo } n \geq 0$

¿Son similares estas estructuras? ¿Por qué?

- ▶ Si identificamos $i \in \mathbb{N}$ con $\underbrace{0 \cdots 0}_{i \text{ veces}}$ podemos ver que estas estructuras son idénticas

La noción de isomorfismo

Dos estructuras son isomorfas si son idénticas excepto por sus dominios.

La noción de isomorfismo

Dos estructuras son isomorfas si son idénticas excepto por sus dominios.

Definición

Dado un vocabulario $\mathcal{L}$ y dos $\mathcal{L}$ -estructuras $\mathfrak{A}$ y $\mathfrak{B}$, decimos que $\mathfrak{A}$ y $\mathfrak{B}$ son isomorfas, denotado como $\mathfrak{A} \cong \mathfrak{B}$, si existe una biyección $h : A \rightarrow B$ tal que:

- ▶ $h(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$, para cada constante $c \in \mathcal{L}$
- ▶ $h(f^{\mathfrak{A}}(a_1, \dots, a_m)) = f^{\mathfrak{B}}(h(a_1), \dots, h(a_m))$, para cada función m -aria $f \in \mathcal{L}$ y elementos $a_1, \dots, a_m \in A$
- ▶ $(a_1, \dots, a_n) \in R^{\mathfrak{A}}$ si y sólo si $(h(a_1), \dots, h(a_n)) \in R^{\mathfrak{B}}$, para cada relación n -aria $R \in \mathcal{L}$ y elementos $a_1, \dots, a_n \in A$

La noción de isomorfismo: Ejemplos

Ejemplos

1. Sea $\mathfrak{A} = \langle \mathbb{N}, 0^{\mathfrak{A}}, 1^{\mathfrak{A}}, +^{\mathfrak{A}}, <^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle B, 0^{\mathfrak{B}}, 1^{\mathfrak{B}}, +^{\mathfrak{B}}, <^{\mathfrak{B}} \rangle$, donde B es el conjunto de los números pares y los demás símbolos son definidos de manera usual. ¿Son $\mathfrak{A}$ y $\mathfrak{B}$ isomorfos?
2. ¿Qué pasa en el caso anterior si además consideramos la multiplicación?
3. Sea $\mathcal{L} = \{E\}$ y $\mathfrak{A} = \langle A, E^{\mathfrak{A}} \rangle$, donde $A = \{1, 2, 3, 4\}$ y $E^{\mathfrak{A}} = \{(1, 2), (1, 3), (3, 2), (4, 1), (4, 2)\}$. Defina una oración φ tal que para toda $\mathcal{L}$ -estructura $\mathfrak{B}$ se tiene que $\mathfrak{B} \models \varphi$ si y sólo si $\mathfrak{A} \cong \mathfrak{B}$.
4. Sea $\mathfrak{Z} = \langle \mathbb{Z}, 0^{\mathfrak{Z}}, 1^{\mathfrak{Z}}, s^{\mathfrak{Z}}, +^{\mathfrak{Z}}, \cdot^{\mathfrak{Z}}, <^{\mathfrak{Z}} \rangle$. ¿Son $\mathfrak{N}$ y $\mathfrak{Z}$ isomorfos?
5. ¿Son $\mathfrak{N}$ y $\mathfrak{R}$ isomorfos?
6. Sea $\mathfrak{A} = \langle \mathbb{R}, +^{\mathfrak{A}}, \cdot^{\mathfrak{A}} \rangle$ y $\mathfrak{B} = \langle \mathbb{C}, +^{\mathfrak{B}}, \cdot^{\mathfrak{B}} \rangle$. ¿Son $\mathfrak{A}$ y $\mathfrak{B}$ isomorfos?