La complejidad de una función acotada

IIC3810

Restringiendo las entradas de una función

Una alternativa para mejorar el tiempo de cálculo de una función es sólo considerar entradas de cierto tipo.

Restringiendo las entradas de una función

Una alternativa para mejorar el tiempo de cálculo de una función es sólo considerar entradas de cierto tipo.

Aunque esta idea puede funcionar bien, tiene como desventaja el hecho de que no tenemos una metodología general para restringir las entradas.

- Por ejemplo, no es cierto que una función $f : \Sigma^* \to \mathbb{N}$ siempre se pueda calcular de manera eficiente si nos restringimos al conjunto de entradas $x \in \Sigma^*$ tal que $f(x) \leq 1$

Restringiendo las entradas de una función

Una alternativa para mejorar el tiempo de cálculo de una función es sólo considerar entradas de cierto tipo.

Aunque esta idea puede funcionar bien, tiene como desventaja el hecho de que no tenemos una metodología general para restringir las entradas.

- Por ejemplo, no es cierto que una función $f : \Sigma^* \to \mathbb{N}$ siempre se pueda calcular de manera eficiente si nos restringimos al conjunto de entradas $x \in \Sigma^*$ tal que $f(x) \leq 1$

De hecho, vamos a ver un ejemplo fundamental donde una restricción severa no logra generar una función que se pueda calcular eficientemente.

Restringiendo las entradas de #CNF-SAT

Considere el siguiente problema: dada una fórmula proposicional φ en CNF tal que $\#\text{CNF-SAT}(\varphi) \leq 1$, determine si φ es satisfacible.

Restringiendo las entradas de #CNF-SAT

Considere el siguiente problema: dada una fórmula proposicional φ en CNF tal que #CNF-SAT$(\varphi) \leq 1$, determine si φ es satisfacible.

Este es el problema usual de satisfacibilidad pero con una **promesa** sobre la entrada

- La promesa es que la entrada consiste de una fórmula proposicional que puede ser hecha verdad por a lo más una valuación

Restringiendo las entradas de #CNF-SAT

Considere el siguiente problema: dada una fórmula proposicional φ en CNF tal que $\#\text{CNF-SAT}(\varphi) \leq 1$, determine si φ es satisfacible.

Este es el problema usual de satisfacibilidad pero con una **promesa** sobre la entrada

- La promesa es que la entrada consiste de una fórmula proposicional que puede ser hecha verdad por a lo más una valuación

Denotamos a este problema como U-CNF-SAT

Restringiendo las entradas de #CNF-SAT

U-CNF-SAT también puede verse como un problema de conteo.

- Dada una fórmula proposicional φ en CNF tal que #CNF-SAT(φ) ≤ 1, la función #U-CNF-SAT(φ) retorna el número de valuaciones que satisfacen φ

Restringiendo las entradas de #CNF-SAT

U-CNF-SAT también puede verse como un problema de conteo.

- Dada una fórmula proposicional φ en CNF tal que $\#\text{CNF-SAT}(\varphi) \leq 1$, la función $\#\text{U-CNF-SAT}(\varphi)$ retorna el número de valuaciones que satisfacen φ

#U-CNF-SAT es una restricción de #CNF-SAT:

$$\#\text{U-CNF-SAT} \quad = \quad \#\text{CNF-SAT}|_{\{\varphi \mid \#\text{CNF-SAT}(\varphi) \leq 1\}}$$

Restringiendo las entradas de #CNF-SAT

U-CNF-SAT también puede verse como un problema de conteo.

- Dada una fórmula proposicional φ en CNF tal que #CNF-SAT(φ) ≤ 1, la función #U-CNF-SAT(φ) retorna el número de valuaciones que satisfacen φ

#U-CNF-SAT es una restricción de #CNF-SAT:

$$\#\text{U-CNF-SAT} \quad = \quad \#\text{CNF-SAT}|_{\{\varphi \,\mid\, \#\text{CNF-SAT}(\varphi) \leq 1\}}$$

Obviamente U-CNF-SAT y #U-CNF-SAT tienen la misma complejidad.

- Para estudiar entonces la complejidad de #U-CNF-SAT vamos a consider U-CNF-SAT

Una pregunta fundamental

¿Es U-CNF-SAT un problema tan difícil como CNF-SAT?

Una pregunta fundamental

¿Es U-CNF-SAT un problema tan difícil como CNF-SAT?

¿Cómo podríamos demostrar que U-CNF-SAT es tan difícil como CNF-SAT?

Una pregunta fundamental

¿Es U-CNF-SAT un problema tan difícil como CNF-SAT?

¿Cómo podríamos demostrar que U-CNF-SAT es tan difícil como CNF-SAT?

- ¿Podemos demostrar que CNF-SAT $\in$ PTIME$^{\text{U-CNF-SAT}}$?

Una pregunta fundamental

¿Es U-CNF-SAT un problema tan difícil como CNF-SAT?

¿Cómo podríamos demostrar que U-CNF-SAT es tan difícil como CNF-SAT?

- ¿Podemos demostrar que CNF-SAT $\in$ PTIME$^{\text{U-CNF-SAT}}$?

Es un problema abierto si CNF-SAT $\in$ PTIME$^{\text{U-CNF-SAT}}$

Una pregunta fundamental

¿Es U-CNF-SAT un problema tan difícil como CNF-SAT?

¿Cómo podríamos demostrar que U-CNF-SAT es tan difícil como CNF-SAT?

- ¿Podemos demostrar que CNF-SAT $\in$ PTIME$^{\text{U-CNF-SAT}}$?

Es un problema abierto si CNF-SAT $\in$ PTIME$^{\text{U-CNF-SAT}}$

- Pero sí podemos demostrar que U-CNF-SAT es tan difícil como CNF-SAT si consideramos algoritmos aleatorizados

Máquinas de Turing probabilísticas con oráculo

Una Máquina de Turing probabilística puede tener un oráculo al igual que en el caso de las Máquinas de Turing usuales (deterministas o no deterministas)

Máquinas de Turing probabilísticas con oráculo

Una Máquina de Turing probabilística puede tener un oráculo al igual que en el caso de las Máquinas de Turing usuales (deterministas o no deterministas)

Ejercicios

Dado un problema de decisión A:

1. Defina la noción de Máquina de Turing probabilística M^A con oráculo para A
2. Defina las clases de complejidad RP^A y BPP^A

U-CNF-SAT es tan difícil como CNF-SAT

Defina el siguiente lenguaje de decisión:

$$\text{CNF-SAT}^{\leq 1} \quad = \quad \{\varphi \mid \varphi \text{ es una fórmula en CNF tal que } \#\text{CNF-SAT}(\varphi) \leq 1\}$$

Ejercicio

Demuestre que CNF-SAT$^{\leq 1}$ es co-NP-completo.

U-CNF-SAT es tan difícil como CNF-SAT

Defina el siguiente lenguaje de decisión:

$$\text{CNF-SAT}^{\leq 1} \quad = \quad \{\varphi \mid \varphi \text{ es una fórmula en CNF tal que } \#\text{CNF-SAT}(\varphi) \leq 1\}$$

Ejercicio

Demuestre que CNF-SAT$^{\leq 1}$ es co-NP-completo.

Sabemos entonces que la promesa sobre las entradas de U-CNF-SAT es difícil de verificar.

- Al demostrar que U-CNF-SAT es tan difícil como CNF-SAT no queremos sacar provecho de esta dificultad

U-CNF-SAT es tan difícil como CNF-SAT

Vamos a eliminar la promesa hecha sobre las entradas de U-CNF-SAT

- ¿Cómo debe funcionar un algoritmo para U-CNF-SAT sobre las fórmulas proposicionales φ en CNF tales que $\#\text{CNF-SAT}(\varphi) \geq 2$?

U-CNF-SAT es tan difícil como CNF-SAT

Vamos a eliminar la promesa hecha sobre las entradas de U-CNF-SAT

- ¿Cómo debe funcionar un algoritmo para U-CNF-SAT sobre las fórmulas proposicionales φ en CNF tales que $\#\text{CNF-SAT}(\varphi) \geq 2$?

Vamos a dejar abierto qué hacer con una entrada φ para U-CNF-SAT tal que $\#\text{CNF-SAT}(\varphi) \geq 2$

- Consideramos todas las posibilidades

U-CNF-SAT es tan difícil como CNF-SAT: el teorema

Sea $H \subseteq \{\varphi \mid \varphi$ es una fórmula en CNF tal que $\#\text{CNF-SAT}(\varphi) \geq 2\}$ y

$$\text{U-CNF-SAT}_H \quad = \quad \text{U-CNF-SAT} \cup H$$

U-CNF-SAT es tan difícil como CNF-SAT: el teorema

Sea $H \subseteq \{\varphi \mid \varphi$ es una fórmula en CNF tal que $\#\text{CNF-SAT}(\varphi) \geq 2\}$ y

$$\text{U-CNF-SAT}_H \quad = \quad \text{U-CNF-SAT} \cup H$$

Teorema (Valiant & Vazirani)

$\mathit{CNF\text{-}SAT} \in \mathit{RP}^{\mathit{U\text{-}CNF\text{-}SAT}_H}$

La pieza clave del resultado

Decimos que una fórmula proposicional es anulable si la valuación que asigna a cada variable proposicional el valor 0 la satisface.

La pieza clave del resultado

Decimos que una fórmula proposicional es anulable si la valuación que asigna a cada variable proposicional el valor 0 la satisface.

Lema (Valiant & Vazirani)

Existe un algoritmo aleatorizado de tiempo polinomial que, dada una fórmula proposicional φ en CNF con $n \geq 2$ variables y que no es anulable, genera una secuencia de fórmulas $\varphi_0, \varphi_1, \ldots, \varphi_n, \varphi_{n+1}, \varphi_{n+2}$ en CNF tales que:

1. *Si φ es consistente, entonces*

$$\mathbf{Pr}\left(\bigvee_{i=0}^{n+2} \#\mathit{CNF\text{-}SAT}(\varphi_i) = 1\right) \geq \frac{1}{8}$$

2. *Si φ es inconsistente, entonces cada fórmula φ_i $(0 \leq i \leq n+2)$ es inconsistente.*

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos que $\mathcal{A}$ es el algoritmo mencionado en el lema.

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos que $\mathcal{A}$ es el algoritmo mencionado en el lema.

Definimos entonces el siguiente algoritmo para CNF-SAT:

Alg-CNF-SAT(φ)
  if φ es anulable **then return sí**
  else
    $n :=$ número de variables en φ
    if $n = 1$ **then return VerificarExhaustivo**(φ)
    else
      for $i := 1$ **to** 11 **do**
        Utilice $\mathcal{A}$ para generar las fórmulas $\varphi_0, \ldots, \varphi_{n+2}$ a partir de φ
        for $j := 0$ **to** $n + 2$ **do**
          if $\varphi_j \in$ U-CNF-SAT$_H$ **then return sí**
      return no

En este algoritmo **VerificarExhaustivo**(φ) verifica utilizando tablas de verdad si φ es consistente.

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Dado que $\mathcal{A}$ funciona en tiempo polinomial, el algoritmo **Alg-CNF-SAT** funciona en tiempo polinomial.

- Tenemos que calcular la probabilidad de error de **Alg-CNF-SAT**

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Dado que $\mathcal{A}$ funciona en tiempo polinomial, el algoritmo **Alg-CNF-SAT** funciona en tiempo polinomial.

- Tenemos que calcular la probabilidad de error de **Alg-CNF-SAT**

Suponemos primero que φ es inconsistente.

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Dado que $\mathcal{A}$ funciona en tiempo polinomial, el algoritmo **Alg-CNF-SAT** funciona en tiempo polinomial.

- Tenemos que calcular la probabilidad de error de **Alg-CNF-SAT**

Suponemos primero que φ es inconsistente.

Por el lema sabemos que las fórmulas $\varphi_0, \ldots, \varphi_{n+2}$ generadas en cada iteración son todas inconsistentes

- Por lo tanto $\varphi_i \notin$ U-CNF-SAT$_H$

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Dado que $\mathcal{A}$ funciona en tiempo polinomial, el algoritmo **Alg-CNF-SAT** funciona en tiempo polinomial.

- Tenemos que calcular la probabilidad de error de **Alg-CNF-SAT**

Suponemos primero que φ es inconsistente.

Por el lema sabemos que las fórmulas φ_0, ..., φ_{n+2} generadas en cada iteración son todas inconsistentes

- Por lo tanto $\varphi_i \not\in$ U-CNF-SAT$_H$

Concluimos que **Pr**(**Alg-CNF-SAT**(φ) retorne **sí**) $= 0$

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos ahora que φ es consistente.

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos ahora que φ es consistente.

Para que **Alg-CNF-SAT**(φ) retorne **no**, en cada iteración de debe cumplir la siguiente condición:

$$\bigwedge_{i=0}^{n+2} \#\text{CNF-SAT}(\varphi_i) \neq 1$$

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos ahora que φ es consistente.

Para que **Alg-CNF-SAT**(φ) retorne **no**, en cada iteración de debe cumplir la siguiente condición:

$$\bigwedge_{i=0}^{n+2} \#\text{CNF-SAT}(\varphi_i) \neq 1$$

Por el lema tenemos que:

$$\mathbf{Pr}\left(\bigwedge_{i=0}^{n+2} \#\text{CNF-SAT}(\varphi_i) \neq 1 \right) \quad \leq \quad \frac{7}{8}$$

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Suponemos ahora que φ es consistente.

Para que **Alg-CNF-SAT**(φ) retorne **no**, en cada iteración de debe cumplir la siguiente condición:

$$\bigwedge_{i=0}^{n+2} \#\text{CNF-SAT}(\varphi_i) \neq 1$$

Por el lema tenemos que:

$$\mathbf{Pr}\left(\bigwedge_{i=0}^{n+2} \#\text{CNF-SAT}(\varphi_i) \neq 1\right) \quad \leq \quad \frac{7}{8}$$

Concluimos que:

$$\mathbf{Pr}(\textbf{Alg-CNF-SAT}(\varphi) \text{ retorne } \textbf{no}) \ \leq \ \left(\frac{7}{8}\right)^{11} \ < \frac{1}{4}$$

U-CNF-SAT$_H$ es tan difícil como CNF-SAT: demostración

Tenemos entonces que:

- Si φ es consistente: $\textbf{Pr}(\textbf{Alg-CNF-SAT}(\varphi) \text{ retorne } \textbf{sí}) \geq \frac{3}{4}$
- Si φ es inconsistente: $\textbf{Pr}(\textbf{Alg-CNF-SAT}(\varphi) \text{ retorne } \textbf{sí}) = 0$

Concluimos que CNF-SAT $\in \text{RP}^{\text{U-CNF-SAT}_H}$

La demostración del lema

Sea φ una fórmula proposicional en CNF con $n \geq 2$ variables y que no es anulable.

- Suponemos que las variables de φ son x_1, ..., x_n

Cada valuación $\sigma : \{x_1, \ldots, x_n\} \to \{0, 1\}$ puede ser considerada como un vector $\vec{\sigma} = (\sigma(x_1), \ldots, \sigma(x_n))$

Los vectores $\vec{\sigma}$ forman el conjunto $\{0, 1\}^n$

- $\{0, 1\}^n$ representa el producto cartesiano $\underbrace{\{0, 1\} \times \{0, 1\} \times \cdots \times \{0, 1\}}_{n \text{ veces}}$

La demostración del lema

$\{0,1\}^n$ naturalmente forma un espacio vectorial sobre el cuerpo $(\{0,1\}, \oplus, \wedge)$

- Recuerde que $\oplus$ es el o exclusivo

En particular, las siguientes son las operaciones en el espacio vectorial:

$$\begin{aligned} (a_1, \ldots, a_n) + (b_1, \ldots, b_n) &= (a_1 \oplus b_1, \ldots, a_n \oplus b_n) \\ \alpha \cdot (a_1, \ldots, a_n) &= (\alpha \wedge a_1, \ldots, \alpha \wedge a_n) \qquad \text{con } \alpha \in \{0,1\} \end{aligned}$$

Usamos la notación $\langle \cdot, \cdot \rangle$ para el producto interno en el espacio vectorial:

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle = (a_1 \wedge b_1) \oplus \cdots \oplus (a_n \wedge b_n)$$

Y denotamos como $\vec{0}$ el vector nulo.

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{0}$, *entonces* $|\{\vec{b} \in \{0,1\}^n \mid \langle \vec{b}, \vec{a} \rangle = 0\}| \ = \ 2^{n-1}$

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{0}$*, entonces* $|\{\vec{b} \in \{0,1\}^n \mid \langle \vec{b}, \vec{a} \rangle = 0\}| \ = \ 2^{n-1}$

Ejercicios

1. Demuestre por inducción que para cada $\ell \geq 1$:

   $$|\{\vec{c} \in \{0,1\}^\ell \mid \vec{c} \text{ tiene un número par de posiciones con valor } 1\}| \ = \ 2^{\ell-1}$$

2. Demuestre el lema a partir de la propiedad anterior.

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{0}$, *entonces* $|\{\vec{b} \in \{0,1\}^n \mid \langle \vec{b}, \vec{a} \rangle = 0\}| \ = \ 2^{n-1}$

Ejercicios

1. Demuestre por inducción que para cada $\ell \geq 1$:

   $$|\{\vec{c} \in \{0,1\}^\ell \mid \vec{c} \text{ tiene un número par de posiciones con valor } 1\}| \ = \ 2^{\ell-1}$$

2. Demuestre el lema a partir de la propiedad anterior.

Corolario 1

Si $\vec{a} \neq \vec{0}$, entonces $\mathbf{Pr}_{\vec{b}}(\langle \vec{b}, \vec{a} \rangle = 0) = \frac{1}{2}$

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{b}$, $\vec{a} \neq \vec{0}$, $\vec{b} \neq \vec{0}$ *y* $n \geq 2$, *entonces para cada* $v_1, v_2 \in \{0, 1\}$:

$$|\{\vec{c} \mid \langle \vec{c}, \vec{a} \rangle = v_1 \wedge \langle \vec{c}, \vec{b} \rangle = v_2\}| \quad = \quad 2^{n-2}$$

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{b}$, $\vec{a} \neq \vec{0}$, $\vec{b} \neq \vec{0}$ *y* $n \geq 2$, *entonces para cada* $v_1, v_2 \in \{0, 1\}$*:*

$$|\{\vec{c} \mid \langle \vec{c}, \vec{a} \rangle = v_1 \wedge \langle \vec{c}, \vec{b} \rangle = v_2\}| \quad = \quad 2^{n-2}$$

Ejercicio

Demuestre el lema por inducción en n

- También puede tratar de demostrarlo utilizando el lema anterior

Algunas propiedades útiles del espacio vectorial

Lema

Si $\vec{a} \neq \vec{b}$, $\vec{a} \neq \vec{0}$, $\vec{b} \neq \vec{0}$ *y* $n \geq 2$, *entonces para cada* $v_1, v_2 \in \{0, 1\}$*:*

$$|\{\vec{c} \mid \langle \vec{c}, \vec{a} \rangle = v_1 \wedge \langle \vec{c}, \vec{b} \rangle = v_2\}| \quad = \quad 2^{n-2}$$

Ejercicio

Demuestre el lema por inducción en n

- También puede tratar de demostrarlo utilizando el lema anterior

Corolario 2

Si $\vec{a} \neq \vec{b}$, $\vec{a} \neq \vec{0}$, $\vec{b} \neq \vec{0}$ y $n \geq 2$, entonces:

$$\begin{aligned}
\mathbf{Pr}_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0 \wedge \langle \vec{c}, \vec{b} \rangle = 0) \quad &= \quad \mathbf{Pr}_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0) \cdot \mathbf{Pr}_{\vec{c}}(\langle \vec{c}, \vec{b} \rangle = 0) \\
\mathbf{Pr}_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0 \mid \langle \vec{c}, \vec{b} \rangle = 0) \quad &= \quad \mathbf{Pr}_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0)
\end{aligned}$$

La demostración del lema: continuación

Dado $\vec{v} \in \{0,1\}^n$ tal que $\vec{v} = (v_1, \ldots, v_n)$, defina:

$$\eta_{\vec{v}} = \bigoplus_{i \,:\, v_i = 1} x_i$$

Nótese que $\eta_{\vec{0}} = \perp$, donde $\perp$ es una contradicción arbitraria.

Por ejemplo, si para un vector $\vec{v}$ tenemos que $v_1 = v_2 = v_5 = 1$ y $v_i = 0$ para toda otra posición i, entonces $\eta_{\vec{v}} = x_1 \oplus x_2 \oplus x_5$

La demostración del lema: continuación

Dado $\vec{v} \in \{0,1\}^n$ tal que $\vec{v} = (v_1, \ldots, v_n)$, defina:

$$\eta_{\vec{v}} \ = \ \bigoplus_{i \,:\, v_i = 1} x_i$$

Nótese que $\eta_{\vec{0}} = \bot$, donde $\bot$ es una contradicción arbitraria.

Por ejemplo, si para un vector $\vec{v}$ tenemos que $v_1 = v_2 = v_5 = 1$ y $v_i = 0$ para toda otra posición i, entonces $\eta_{\vec{v}} = x_1 \oplus x_2 \oplus x_5$

Dada una valuación σ, tenemos que:

$$\sigma(\eta_{\vec{v}}) = 0 \ \text{ si y sólo si } \ \langle \vec{\sigma}, \vec{v} \rangle = 0$$

Las fórmulas generadas por el algoritmo aleatorizado

El algoritmo aleatorizado escoge con distribución uniforme y de manera independiente $n+2$ vectores $\vec{v}_1, \ldots, \vec{v}_{n+2}$ en $\{0,1\}^n$, y define:

$$\begin{array}{rcl} \psi_0 & = & \varphi \\ \psi_{i+1} & = & \psi_i \wedge \neg \eta_{\vec{v}_{i+1}} \qquad 1 \leq i \leq n+1 \end{array}$$

Las fórmulas generadas por el algoritmo aleatorizado

El algoritmo aleatorizado escoge con distribución uniforme y de manera independiente $n + 2$ vectores $\vec{v}_1, \ldots, \vec{v}_{n+2}$ en $\{0,1\}^n$, y define:

$$\begin{array}{rcll} \psi_0 & = & \varphi & \\ \psi_{i+1} & = & \psi_i \wedge \neg \eta_{\vec{v}_{i+1}} & \qquad 1 \leq i \leq n+1 \end{array}$$

Las fórmulas definidas no están en CNF

- Vamos a demostrar que satisfacen las propiedades del lema
- Vamos a mostrar cómo a partir de ellas se pueden generar las fórmulas $\varphi_0, \ldots, \varphi_{n+2}$ en CNF mencionadas en el lema

Dos propiedades de ψ_0, . . ., ψ_{n+2}

Un primera observación importante es que si φ es inconsistente, entonces cada ψ_i es inconsistente.

Suponga entonces que φ es consistente.

- Existe $k \in \{0, \ldots, n\}$ tal que $2^k \leq \#\text{CNF-SAT}(\varphi) < 2^{k+1}$

Dos propiedades de ψ_0, ..., ψ_{n+2}

Un primera observación importante es que si φ es inconsistente, entonces cada ψ_i es inconsistente.

Suponga entonces que φ es consistente.

- Existe $k \in \{0, \ldots, n\}$ tal que $2^k \leq \#\text{CNF-SAT}(\varphi) < 2^{k+1}$

Vamos a demostrar que $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1) \geq \frac{1}{8}$

Dos propiedades de $\psi_0, \ldots, \psi_{n+2}$

Un primera observación importante es que si φ es inconsistente, entonces cada ψ_i es inconsistente.

Suponga entonces que φ es consistente.

- Existe $k \in \{0, \ldots, n\}$ tal que $2^k \leq \#\text{CNF-SAT}(\varphi) < 2^{k+1}$

Vamos a demostrar que $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1) \geq \frac{1}{8}$

- Se concluye que $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{i=0}^{n+2} \#\text{CNF-SAT}(\psi_i) = 1\right) \geq \dfrac{1}{8}$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1)$

Sea Γ el conjunto de valuaciones que satisfacen φ

- Sabemos que $\Gamma \neq \emptyset$

Tenemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1) \ = \\ \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\bigg(\bigvee_{\sigma \in \Gamma} \sigma \text{ es la única valuación que satisface } \psi_{k+2}\bigg)$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1)$

Entonces dado $\sigma \in \Gamma$, primero vamos a acotar inferiormente:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\sigma \text{ es la única valuación que satisface } \psi_{k+2})$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1)$

Entonces dado $\sigma \in \Gamma$, primero vamos a acotar inferiormente:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\sigma \text{ es la única valuación que satisface } \psi_{k+2})$$

Tenemos que esta probabilidad es igual a:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\left[\bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right] \wedge \left[\bigwedge_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg\eta_{\vec{v}_j}) = 0\right]\right)$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1)$

Lo cual es igual a:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right) \cdot$$
$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right)$$

Utilizamos la siguiente notación:

$$\begin{aligned} p^1_\sigma &= \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right) \\ p^2_\sigma &= \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right) \end{aligned}$$

Acotando inferiormente p_σ^1

Tenemos que:

$$
\begin{aligned}
p_\sigma^1 &= \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right) \\
&= \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\neg\eta_{\vec{v}_i}) = 1\right) \\
&= \prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma(\neg\eta_{\vec{v}_i}) = 1) \\
&= \prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma(\eta_{\vec{v}_i}) = 0) \\
&= \prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma} \rangle = 0)
\end{aligned}
$$

Acotando inferiormente p_σ^1

Dado que φ no es anulable tenemos que $\vec{\sigma} \neq \vec{0}$

Entonces por Corolario 1 deducimos que $\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma} \rangle = 0) = \frac{1}{2}$

Concluimos que:

$$\begin{aligned} p_\sigma^1 &= \prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma} \rangle = 0) \\ &= \prod_{i=1}^{k+2} \frac{1}{2} \\ &= \frac{1}{2^{k+2}} \end{aligned}$$

Acotando inferiormente p_σ^2

Tenemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\bigg(\bigwedge_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \ \bigg|\ \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \bigg) \ =$$

$$1 - \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\bigg(\bigvee_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \ \bigg|\ \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \bigg)$$

Acotando inferiormente p_σ^2

Tenemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) =$$

$$1 - \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right)$$

Además, sabemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) \leq$$

$$\sum_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) =$$

$$\sum_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)$$

Acotando inferiormente p_σ^2

Dado $\sigma' \in \Gamma \smallsetminus \{\sigma\}$, tenemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0\right) =$$

$$\frac{\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\left[\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0\right] \wedge \left[\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0\right]\right)}{\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0\right)} =$$

$$\frac{\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{i=1}^{k+2} \sigma'(\eta_{\vec{v}_i}) = 0 \wedge \sigma(\eta_{\vec{v}_i}) = 0\right)}{\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0\right)} =$$

Acotando inferiormente p_σ^2

$$\frac{\displaystyle\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma'(\eta_{\vec{v}_i}) = 0 \wedge \sigma(\eta_{\vec{v}_i}) = 0)}{\displaystyle\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma(\eta_{\vec{v}_i}) = 0)} =$$

$$\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma'(\eta_{\vec{v}_i}) = 0 \mid \sigma(\eta_{\vec{v}_i}) = 0) =$$

$$\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0)$$

Acotando inferiormente p_σ^2

$$\frac{\displaystyle\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma'(\eta_{\vec{v}_i}) = 0 \wedge \sigma(\eta_{\vec{v}_i}) = 0)}{\displaystyle\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma(\eta_{\vec{v}_i}) = 0)} =$$

$$\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\sigma'(\eta_{\vec{v}_i}) = 0 \mid \sigma(\eta_{\vec{v}_i}) = 0) =$$

$$\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0)$$

Concluimos que $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)$ es igual a:

$$\prod_{i=1}^{k+2} \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0)$$

Acotando inferiormente p_σ^2

Dado que φ no es anulable tenemos que $\vec{\sigma} \neq \vec{0}$ y $\vec{\sigma}' \neq \vec{0}$

Así, dado que $\vec{\sigma}' \neq \vec{\sigma}$ y $n \geq 2$, deducimos por Corolario 2 que:

$$\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0) \quad = \quad \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0)$$

Acotando inferiormente p_σ^2

Dado que φ no es anulable tenemos que $\vec{\sigma} \neq \vec{0}$ y $\vec{\sigma}' \neq \vec{0}$

Así, dado que $\vec{\sigma}' \neq \vec{\sigma}$ y $n \geq 2$, deducimos por Corolario 2 que:

$$\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0) \quad = \quad \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0)$$

Además, por Corolario 1 sabemos que $\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0) = \frac{1}{2}$

Acotando inferiormente p_σ^2

Dado que φ no es anulable tenemos que $\vec{\sigma} \neq \vec{0}$ y $\vec{\sigma}' \neq \vec{0}$

Así, dado que $\vec{\sigma}' \neq \vec{\sigma}$ y $n \geq 2$, deducimos por Corolario 2 que:

$$\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0 \mid \langle \vec{v}_i, \vec{\sigma} \rangle = 0) \quad = \quad \mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0)$$

Además, por Corolario 1 sabemos que $\mathbf{Pr}_{\vec{v}_i}(\langle \vec{v}_i, \vec{\sigma}' \rangle = 0) = \frac{1}{2}$

Concluimos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right) \quad = \quad \frac{1}{2^{k+2}}$$

Acotando inferiormente p_σ^2

Tenemos entonces que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) \leq$$

$$\sum_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right) =$$

$$\sum_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \frac{1}{2^{k+2}} =$$

$$(|\Gamma| - 1) \cdot \frac{1}{2^{k+2}} <$$

$$2^{k+1} \cdot \frac{1}{2^{k+2}} = \frac{1}{2}$$

Acotando inferiormente p_σ^2

Finalmente concluimos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigwedge_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) =$$

$$1 - \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{\sigma' \in \Gamma \smallsetminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \;\middle|\; \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) \geq$$

$$1 - \frac{1}{2} = \frac{1}{2}$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\sigma \text{ es la única valuación que satisface } \psi_{k+2})$

Sabemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\sigma \text{ es la única valuación que satisface } \psi_{k+2}) \ = \ p_\sigma^1 \cdot p_\sigma^2$$

Dado que $p_\sigma^1 = \frac{1}{2^{k+2}}$ y $p_\sigma^2 \geq \frac{1}{2}$, concluimos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\sigma \text{ es la única valuación que satisface } \psi_{k+2}) \ \geq \ \frac{1}{2^{k+3}}$$

La conclusión . . .

De los resultados en las transparencias anteriores tenemos que:

$$
\begin{aligned}
\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\psi_{k+2}) = 1) \ = \\
\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\left(\bigvee_{\sigma\in\Gamma} \sigma \text{ es la única valuación que satisface } \psi_{k+2}\right) \ = \\
\sum_{\sigma\in\Gamma} \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}\Big(\sigma \text{ es la única valuación que satisface } \psi_{k+2}\Big) \ \geq \\
\sum_{\sigma\in\Gamma} \frac{1}{2^{k+3}} \ = \\
|\Gamma| \cdot \frac{1}{2^{k+3}} \ \geq \\
2^k \cdot \frac{1}{2^{k+3}} \ = \ \frac{1}{8}
\end{aligned}
$$

Pero aún no estamos listos . . .

Nos falta indicar cómo generar $\varphi_0, \ldots, \varphi_{n+2}$ en CNF.

- Esta secuencia es construida de la misma forma que $\psi_0, \ldots, \psi_{n+2}$, pero reemplazando las fórmulas $(\neg\eta_{\vec{v}_i})$ por fórmulas en CNF

Pero aún no estamos listos ...

Nos falta indicar cómo generar φ_0, ..., φ_{n+2} en CNF.

- Esta secuencia es construida de la misma forma que ψ_0, ..., ψ_{n+2}, pero reemplazando las fórmulas $(\neg\eta_{\vec{v}_i})$ por fórmulas en CNF

Suponga que $\vec{v} = (v_1, \ldots, v_n)$ es un vector en $\{0, 1\}^n$

Pero aún no estamos listos . . .

Nos falta indicar cómo generar φ_0, . . ., φ_{n+2} en CNF.

- Esta secuencia es construida de la misma forma que ψ_0, . . ., ψ_{n+2}, pero reemplazando las fórmulas $(\neg\eta_{\vec{v}_i})$ por fórmulas en CNF

Suponga que $\vec{v} = (v_1, \ldots, v_n)$ es un vector en $\{0, 1\}^n$

No reemplazamos $(\neg\eta_{\vec{v}})$ por una fórmula lógicamente equivalente en CNF, puesto que construir tal fórmula toma tiempo exponencial.

- La reemplazamos por una fórmula relacionada (en un sentido que será definido), y que utiliza nuevas variables proposicionales $y_1^{\vec{v}}$, . . . , $y_n^{\vec{v}}$

Reemplazando $(\neg\eta_{\vec{v}})$ por una fórmula en CNF

Defina la fórmula $\xi_1^{\vec{v}}$ como:

$$\xi_1^{\vec{v}} \quad = \quad \begin{cases} y_1^{\vec{v}} \leftrightarrow x_1 & v_1 = 1 \\ y_1^{\vec{v}} \leftrightarrow \perp & v_1 = 0 \end{cases}$$

donde $\perp$ es una contradicción arbitraria.

Reemplazando $(\neg\eta_{\vec{v}})$ por una fórmula en CNF

Defina la fórmula $\xi_1^{\vec{v}}$ como:

$$\xi_1^{\vec{v}} \quad = \quad \begin{cases} y_1^{\vec{v}} \leftrightarrow x_1 & v_1 = 1 \\ y_1^{\vec{v}} \leftrightarrow \perp & v_1 = 0 \end{cases}$$

donde $\perp$ es una contradicción arbitraria.

Además, para cada $i \in \{2, \ldots, n\}$ defina:

$$\xi_i^{\vec{v}} \quad = \quad \begin{cases} y_i^{\vec{v}} \leftrightarrow (y_{i-1}^{\vec{v}} \oplus x_i) & v_i = 1 \\ y_i^{\vec{v}} \leftrightarrow y_{i-1}^{\vec{v}} & v_i = 0 \end{cases}$$

Reemplazando $(\neg\eta_{\vec{v}})$ por una fórmula en CNF

Finalmente, defina $\xi_{\vec{v}}$ como:

$$\xi_{\vec{v}} \quad = \quad \left(\bigwedge_{i=1}^{n} \xi_i^{\vec{v}}\right) \wedge \neg y_n^{\vec{v}}$$

Reemplazando $(\neg\eta_{\vec{v}})$ por una fórmula en CNF

Finalmente, defina $\xi_{\vec{v}}$ como:

$$\xi_{\vec{v}} \quad = \quad \left(\bigwedge_{i=1}^{n} \xi_i^{\vec{v}}\right) \wedge \neg y_n^{\vec{v}}$$

La fórmula $\xi_{\vec{v}}$ no es lógicamente equivalente a $(\neg\eta_{\vec{v}})$, de hecho no utilizan las mismas variables.

Reemplazando $(\neg\eta_{\vec{v}})$ por una fórmula en CNF

Finalmente, defina $\xi_{\vec{v}}$ como:

$$\xi_{\vec{v}} \quad = \quad \left(\bigwedge_{i=1}^{n} \xi_i^{\vec{v}}\right) \wedge \neg y_n^{\vec{v}}$$

La fórmula $\xi_{\vec{v}}$ no es lógicamente equivalente a $(\neg\eta_{\vec{v}})$, de hecho no utilizan las mismas variables.

- ¿Cuál es la relación entre estas fórmulas?

La relación entre $(\neg \eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Sea $X = \{x_1, \ldots, x_n\}$ e $Y^{\vec{v}} = \{y_1^{\vec{v}}, \ldots, y_n^{\vec{v}}\}$

Dos valuaciones $\sigma : X \to \{0,1\}$ y $\lambda : Y^{\vec{v}} \to \{0,1\}$ son $\vec{v}$-consistentes si $(\sigma \cup \lambda)(\xi_i^{\vec{v}}) = 1$ para cada $i \in \{1, \ldots, n\}$

- Donde $(\sigma \cup \lambda)(x_j) = \sigma(x_j)$ y $(\sigma \cup \lambda)(y_j^{\vec{v}}) = \lambda(y_j^{\vec{v}})$ para cada $j \in \{1, \ldots, n\}$

La relación entre $(\neg\eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Sea $X = \{x_1, \ldots, x_n\}$ e $Y^{\vec{v}} = \{y_1^{\vec{v}}, \ldots, y_n^{\vec{v}}\}$

Dos valuaciones $\sigma : X \to \{0,1\}$ y $\lambda : Y^{\vec{v}} \to \{0,1\}$ son $\vec{v}$-consistentes si $(\sigma \cup \lambda)(\xi_i^{\vec{v}}) = 1$ para cada $i \in \{1, \ldots, n\}$

- Donde $(\sigma \cup \lambda)(x_j) = \sigma(x_j)$ y $(\sigma \cup \lambda)(y_j^{\vec{v}}) = \lambda(y_j^{\vec{v}})$ para cada $j \in \{1, \ldots, n\}$

Lema

Para cada valuación $\sigma : X \to \{0,1\}$, existe una única valuación $\lambda : Y^{\vec{v}} \to \{0,1\}$ tal que σ y λ son $\vec{v}$-consistentes.

La relación entre $(\neg \eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Sea $X = \{x_1, \ldots, x_n\}$ e $Y^{\vec{v}} = \{y_1^{\vec{v}}, \ldots, y_n^{\vec{v}}\}$

Dos valuaciones $\sigma : X \to \{0, 1\}$ y $\lambda : Y^{\vec{v}} \to \{0, 1\}$ son $\vec{v}$-consistentes si $(\sigma \cup \lambda)(\xi_i^{\vec{v}}) = 1$ para cada $i \in \{1, \ldots, n\}$

- Donde $(\sigma \cup \lambda)(x_j) = \sigma(x_j)$ y $(\sigma \cup \lambda)(y_j^{\vec{v}}) = \lambda(y_j^{\vec{v}})$ para cada $j \in \{1, \ldots, n\}$

Lema

Para cada valuación $\sigma : X \to \{0, 1\}$, existe una única valuación $\lambda : Y^{\vec{v}} \to \{0, 1\}$ tal que σ y λ son $\vec{v}$-consistentes.

Ejercicio

Demuestre el lema.

La relación entre $(\neg \eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Lema

Si dos valuaciones $\sigma : X \to \{0, 1\}$ *y* $\lambda : Y^{\vec{v}} \to \{0, 1\}$ *son* $\vec{v}$*-consistentes, entonces* $\sigma(\neg \eta_{\vec{v}}) = (\sigma \cup \lambda)(\xi_{\vec{v}})$

La relación entre $(\neg\eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Lema

Si dos valuaciones $\sigma : X \to \{0,1\}$ *y* $\lambda : Y^{\vec{v}} \to \{0,1\}$ *son* $\vec{v}$*-consistentes, entonces* $\sigma(\neg\eta_{\vec{v}}) = (\sigma \cup \lambda)(\xi_{\vec{v}})$

Ejercicio

Demuestre el lema.

La relación entre $(\neg \eta_{\vec{v}})$ y $\xi_{\vec{v}}$

Lema

Si dos valuaciones $\sigma : X \to \{0,1\}$ *y* $\lambda : Y^{\vec{v}} \to \{0,1\}$ *son* $\vec{v}$*-consistentes, entonces* $\sigma(\neg \eta_{\vec{v}}) = (\sigma \cup \lambda)(\xi_{\vec{v}})$

Ejercicio

Demuestre el lema.

Las relaciones entre $(\neg \eta_{\vec{v}})$ y $\xi_{\vec{v}}$ mostradas en los lemas son las que necesitamos para terminar la demostración.

Definiendo $\varphi_0, \ldots, \varphi_{n+2}$

El algoritmo aleatorizado escoge con distribución uniforme y de manera independiente $n+2$ vectores $\vec{v}_1, \ldots, \vec{v}_{n+2}$ en $\{0,1\}^n$, y define:

$$
\begin{array}{rcll}
\varphi_0 & = & \varphi & \\
\varphi_{i+1} & = & \varphi_i \wedge \xi_{\vec{v}_{i+1}} & \qquad 1 \leq i \leq n+1
\end{array}
$$

Definiendo $\varphi_0, \ldots, \varphi_{n+2}$

El algoritmo aleatorizado escoge con distribución uniforme y de manera independiente $n+2$ vectores $\vec{v}_1, \ldots, \vec{v}_{n+2}$ en $\{0,1\}^n$, y define:

$$
\begin{array}{rcll}
\varphi_0 & = & \varphi & \\
\varphi_{i+1} & = & \varphi_i \wedge \xi_{\vec{v}_{i+1}} & \qquad 1 \leq i \leq n+1
\end{array}
$$

Las fórmulas $\varphi_0, \ldots, \varphi_{n+2}$ si están en CNF, puesto que podemos definir:

$$
\xi_1^{\vec{v}} \quad = \quad \begin{cases} (\neg y_1^{\vec{v}} \vee x_1) \vee (y_1^{\vec{v}} \vee \neg x_1) & v_1 = 1 \\ \neg y_1^{\vec{v}} & v_1 = 0 \end{cases}
$$

y para cada $i \in \{2, \ldots, n\}$ podemos definir:

$$
\xi_i^{\vec{v}} \quad = \quad \begin{cases} (\neg y_i^{\vec{v}} \vee y_{i-1}^{\vec{v}} \vee x_i) \wedge (y_i^{\vec{v}} \vee \neg y_{i-1}^{\vec{v}} \vee x_i) \wedge & \\ (y_i^{\vec{v}} \vee y_{i-1}^{\vec{v}} \vee \neg x_i) \wedge (\neg y_i^{\vec{v}} \vee \neg y_{i-1}^{\vec{v}} \vee \neg x_i) & v_i = 1 \\ (\neg y_i^{\vec{v}} \vee y_{i-1}^{\vec{v}}) \wedge (y_i^{\vec{v}} \vee \neg y_{i-1}^{\vec{v}}) & v_i = 0 \end{cases}
$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Sea Λ el conjunto de valuaciones $\lambda : (X \cup Y^{\vec{v}_1} \cup \cdots \cup Y^{\vec{v}_{k+2}}) \to \{0,1\}$ tal que:

Para cada $i \in \{1, \ldots, k+2\}$, se tiene que $\lambda|_X$ y $\lambda|_{Y^{\vec{v}_i}}$ son $\vec{v}_i$-consistentes

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Sea Λ el conjunto de valuaciones $\lambda : (X \cup Y^{\vec{v}_1} \cup \cdots \cup Y^{\vec{v}_{k+2}}) \to \{0,1\}$ tal que:

Para cada $i \in \{1, \ldots, k+2\}$, se tiene que $\lambda|_X$ y $\lambda|_{Y^{\vec{v}_i}}$ son $\vec{v}_i$-consistentes

Tenemos que:

$$\begin{aligned}
\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1) \ &= \\
&\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1) \ = \\
&\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\Bigg(\bigvee_{\lambda \in \Lambda} \lambda \text{ es la única valuación que satisface } \varphi_{k+2} \Bigg) \ = \\
&\sum_{\lambda \in \Lambda} \mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\Bigg(\lambda \text{ es la única valuación que satisface } \varphi_{k+2} \Bigg)
\end{aligned}$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Y tenemos que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\Big(\lambda \text{ es la única valuación que satisface } \varphi_{k+2}\Big) \ =$$

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\left[\bigwedge_{i=1}^{k+2} \lambda(\xi_{\vec{v}_i}) = 1\right] \wedge \left[\bigwedge_{\lambda' \in \Lambda \smallsetminus \{\lambda\}} \bigvee_{j=1}^{k+2} \lambda'(\xi_{\vec{v}_j}) = 0\right]\right) \ =$$

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{i=1}^{k+2} \lambda(\xi_{\vec{v}_i}) = 1\right) \cdot$$

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{k+2}}\left(\bigwedge_{\lambda' \in \Lambda \smallsetminus \{\lambda\}} \bigvee_{j=1}^{k+2} \lambda'(\xi_{\vec{v}_j}) = 0 \ \middle|\ \bigwedge_{i=1}^{k+2} \lambda(\xi_{\vec{v}_i}) = 1\right)$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Dado que φ no es anulable, tenemos que $\vec{\lambda|_X} \neq \vec{0}$. Así, dado que $\lambda \in \Lambda$ concluimos para $i \in \{1, \ldots, k+2\}$ que:

$$\begin{aligned}
\mathbf{Pr}_{\vec{v}_i}(\lambda(\xi_{\vec{v}_i}) = 1) &= \mathbf{Pr}_{\vec{v}_i}(\lambda|_X(\neg\eta_{\vec{v}_i}) = 1) \\
&= \mathbf{Pr}_{\vec{v}_i}(\langle \vec{\lambda|_X}, \vec{v}_i \rangle = 0) \color{red}{= \frac{1}{2}}
\end{aligned}$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Dado que φ no es anulable, tenemos que $\vec{\lambda|}_X \neq \vec{0}$. Así, dado que $\lambda \in \Lambda$ concluimos para $i \in \{1, \ldots, k+2\}$ que:

$$\begin{aligned}
\mathbf{Pr}_{\vec{v}_i}(\lambda(\xi_{\vec{v}_i}) = 1) &= \mathbf{Pr}_{\vec{v}_i}(\lambda|_X(\neg\eta_{\vec{v}_i}) = 1) \\
&= \mathbf{Pr}_{\vec{v}_i}(\langle \vec{\lambda|}_X, \vec{v}_i \rangle = 0) \color{red}{=} \color{red}{\frac{1}{2}}
\end{aligned}$$

Sea $\lambda' \in \Lambda \setminus \{\lambda\}$. Dado que φ no es anulable y $\lambda \neq \lambda'$, tenemos que $\vec{\lambda|}_X \neq \vec{0}$, $\vec{\lambda'|}_X \neq \vec{0}$ y $\vec{\lambda|}_X \neq \vec{\lambda'|}_X$, por lo que concluimos para $i \in \{1, \ldots, k+2\}$ que:

$$\begin{aligned}
\mathbf{Pr}_{\vec{v}_i}(\lambda'(\xi_{\vec{v}_i}) = 1 \mid \lambda(\xi_{\vec{v}_i}) = 1) &= \mathbf{Pr}_{\vec{v}_i}(\lambda'|_X(\neg\eta_{\vec{v}_i}) = 1 \mid \lambda|_X(\neg\eta_{\vec{v}_i}) = 1) \\
&= \mathbf{Pr}_{\vec{v}_i}(\langle \vec{\lambda'|}_X, \vec{v}_i \rangle = 0 \mid \langle \vec{\lambda|}_X, \vec{v}_i \rangle = 0) \\
&= \mathbf{Pr}_{\vec{v}_i}(\langle \vec{\lambda'|}_X, \vec{v}_i \rangle = 0) \color{red}{=} \color{red}{\frac{1}{2}}
\end{aligned}$$

Acotando inferiormente $\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1)$

Utilizando los resultados anteriores y considerando que $|\Lambda| = |\Gamma|$, concluimos como en el caso de ψ_0, ..., ψ_{n+2} que:

$$\mathbf{Pr}_{\vec{v}_1,\ldots,\vec{v}_{n+2}}(\#\text{CNF-SAT}(\varphi_{k+2}) = 1) \quad \geq \quad \frac{1}{8}$$

Esto concluye la demostración del teorema. $\square$