

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 $f : \Sigma^* \rightarrow \mathbb{N}$ 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 $\#$ CNF-SAT(φ) ≤ 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 $\# \text{CNF-SAT}$

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

$\# \text{U-CNF-SAT}$ es una restricción de $\# \text{CNF-SAT}$:

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

Obviamente U-CNF-SAT y $\# \text{U-CNF-SAT}$ tienen la misma complejidad.

- ▶ Para estudiar entonces la complejidad de $\# \text{U-CNF-SAT}$ vamos a considerar 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 $\text{CNF-SAT} \in \text{PTIME}^{\text{U-CNF-SAT}}$?

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

- ▶ 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)

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:

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

Ejercicio

Demuestre que $\text{CNF-SAT}^{\leq 1}$ 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 $\# \text{CNF-SAT}(\varphi) \geq 2$?

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

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

Teorema (Valiant & Vazirani)

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

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.

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 $\varphi_0, \varphi_1, \dots, \varphi_n, \varphi_{n+1}, \varphi_{n+2}$ en CNF tales que:

1. *Si φ es consistente, entonces*

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

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

U-CNF-SAT es tan difícil como CNF-SAT: la 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 $\varphi_0, \dots, \varphi_{n+2}$ a partir de φ

for $j := 1$ **to** n **do**

if $\varphi_j \in \text{U-CNF-SAT}_H$ **then return sí**

return no

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

U-CNF-SAT es tan difícil como CNF-SAT: la 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 $\varphi_0, \dots, \varphi_{n+2}$ generadas en cada iteración son todas inconsistentes

- ▶ Por lo tanto $\varphi_i \notin \text{U-CNF-SAT}$

Concluimos que $\Pr(\mathbf{Alg-CNF-SAT}(\varphi) \text{ retorne sí}) = 0$

U-CNF-SAT es tan difícil como CNF-SAT: la 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:

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

Concluimos que:

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

U-CNF-SAT es tan difícil como CNF-SAT: la demostración

Tenemos entonces que:

- ▶ Si φ es consistente: $\Pr(\mathbf{Alg}\text{-}\mathbf{CNF}\text{-}\mathbf{SAT}(\varphi) \text{ retorne } \mathbf{s\acute{i}}) \geq \frac{3}{4}$
- ▶ Si φ es inconsistente: $\Pr(\mathbf{Alg}\text{-}\mathbf{CNF}\text{-}\mathbf{SAT}(\varphi) \text{ retorne } \mathbf{s\acute{i}}) = 0$

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

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 $x_1, \dots, x_n$

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

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

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

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:

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

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

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

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

Algunas propiedades útiles del espacio vectorial

Lema

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

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 $\Pr_{\vec{b}}(\langle \vec{b}, \vec{a} \rangle = 0) = \frac{1}{2}$

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 $v_1, v_2 \in \{0, 1\}$:

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

Ejercicio

Demuestre el lema 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:

$$\Pr_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0 \wedge \langle \vec{c}, \vec{b} \rangle = 0) = \Pr_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0) \cdot \Pr_{\vec{c}}(\langle \vec{c}, \vec{b} \rangle = 0)$$

$$\Pr_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0 \mid \langle \vec{c}, \vec{b} \rangle = 0) = \Pr_{\vec{c}}(\langle \vec{c}, \vec{a} \rangle = 0)$$

La demostración del lema: continuación

Dado $\vec{v} \in \{0, 1\}^n$ tal que $\vec{v} = (v_1, \dots, v_n)$, 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 $\eta_{\vec{v}} = x_1 \oplus x_2 \oplus x_5$

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 $\vec{v}_1, \dots, \vec{v}_{n+2}$ en $\{0, 1\}^n$, y define:

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

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 $\varphi_0, \dots, \varphi_{n+2}$ en CNF mencionadas en el lema

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

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

Suponga entonces que φ es consistente.

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

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

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

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

Sea Γ el conjunto de valuaciones que satisfacen φ

- Sabemos que $\Gamma \neq \emptyset$

Tenemos que:

$$\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}(\# \text{CNF-SAT}(\psi_{k+2}) = 1) = \\ \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigvee_{\sigma \in \Gamma} \sigma \text{ es la \u00fanica valuaci\u00f3n que satisface } \psi_{k+2} \right)$$

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

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

$$\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}(\sigma \text{ es la \u00fanica valuaci\u00f3n que satisface } \psi_{k+2})$$

Tenemos que esta probabilidad es igual a:

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

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

Lo cual es igual a:

$$\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) .$$

$$\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right)$$

Utilizamos la siguiente notación:

$$p_{\sigma}^1 = \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right)$$

$$p_{\sigma}^2 = \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right)$$

Acotando inferiormente p_σ^1

Tenemos que:

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

Acotando inferiormente p_σ^1

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

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

Concluimos que:

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

Acotando inferiormente p_σ^2

Tenemos que:

$$\begin{aligned} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) = \\ 1 - \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigvee_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) \end{aligned}$$

Además, sabemos que:

$$\begin{aligned} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigvee_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) \leq \\ \sum_{\sigma' \in \Gamma \setminus \{\sigma\}} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) = \\ \sum_{\sigma' \in \Gamma \setminus \{\sigma\}} \Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right) \end{aligned}$$

Acotando inferiormente p_σ^2

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

$$\begin{aligned} \Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right) &= \\ \Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\left[\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \right] \wedge \left[\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right] \right) &= \\ \frac{\Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)}{\Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)} &= \\ \Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{i=1}^{k+2} \sigma'(\eta_{\vec{v}_i}) = 0 \wedge \sigma(\eta_{\vec{v}_i}) = 0 \right) &= \\ \frac{\Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)}{\Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)} &= \end{aligned}$$

Acotando inferiormente p_σ^2

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

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

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

Concluimos que $\Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right)$ es igual a:

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

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:

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

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

Concluimos que:

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

Acotando inferiormente p_σ^2

Tenemos entonces que:

$$\begin{aligned} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigvee_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) &\leq \\ \sum_{\sigma' \in \Gamma \setminus \{\sigma\}} \Pr_{\vec{v}_1, \dots, \vec{v}_{k+2}} \left(\bigwedge_{j=1}^{k+2} \sigma'(\eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\eta_{\vec{v}_i}) = 0 \right) &= \\ \sum_{\sigma' \in \Gamma \setminus \{\sigma\}} \frac{1}{2^{k+2}} &= \\ (|\Gamma| - 1) \cdot \frac{1}{2^{k+2}} &< \\ 2^{k+1} \cdot \frac{1}{2^{k+2}} &= \frac{1}{2} \end{aligned}$$

Acotando inferiormente p_σ^2

Finalmente concluimos que:

$$\begin{aligned} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigwedge_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigvee_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 0 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) &= \\ 1 - \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}} \left(\bigvee_{\sigma' \in \Gamma \setminus \{\sigma\}} \bigwedge_{j=1}^{k+2} \sigma'(\neg \eta_{\vec{v}_j}) = 1 \mid \bigwedge_{i=1}^{k+2} \sigma(\neg \eta_{\vec{v}_i}) = 1 \right) &\geq \\ 1 - \frac{1}{2} &= \frac{1}{2} \end{aligned}$$

Acotando inferiormente

$\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}$ (σ es la única valuación que satisface ψ_{k+2})

Sabemos que:

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

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

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

La conclusión ...

De los resultados en las transparencias anteriores tenemos que:

$$\begin{aligned}\Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}(\# \text{CNF-SAT}(\psi_{k+2}) = 1) &= \\ \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}\left(\bigvee_{\sigma \in \Gamma} \sigma \text{ es la \u00fanica valuaci\u00f3n que satisface } \psi_{k+2}\right) &= \\ \sum_{\sigma \in \Gamma} \Pr_{\vec{v}_1, \dots, \vec{v}_{n+2}}\left(\sigma \text{ es la \u00fanica valuaci\u00f3n que satisface } \psi_{k+2}\right) &\geq \\ \sum_{\sigma \in \Gamma} \frac{1}{2^{k+3}} &= \\ |\Gamma| \cdot \frac{1}{2^{k+3}} &\geq \\ 2^k \cdot \frac{1}{2^{k+3}} &= \frac{1}{8}\end{aligned}$$