¿Dónde estamos?

La demostración de que GRAPH-ISO $\in L_2^P$ tiene tres partes:

1. Definición de la clase de complejidad AM ✓
2. Demostración que GRAPH-ISO $\in$ co-AM ✓
3. Demostración que NP $\cap$ co-AM $\subseteq L_2^P$

Un resultado útil para la demostración

Lema

Sea $p : \mathbb{N} \to \mathbb{N}$ *un polinomio no nulo. Entonces existe* $n_0 \in \mathbb{N}$ *tal que para todo* $n \in \mathbb{N}$ *con* $n \geq n_0$ *y* $E \subseteq \{0,1\}^{p(n)}$ *con* $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$, *las siguientes afirmaciones son ciertas:*

1. $\exists u_1 \in \{0,1\}^{p(n)} \ldots \exists u_{p(n)} \in \{0,1\}^{p(n)} \forall v \in \{0,1\}^{p(n)}$
   $\exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

2. $\forall u_1 \in \{0,1\}^{p(n)} \ldots \forall u_{p(n)} \in \{0,1\}^{p(n)} \exists v \in \{0,1\}^{p(n)}$
   $\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v \in E)$

La demostración del lema

Como $p(n)$ es un polinomio, existe $n_1 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_1) : (p(n) < 2^n)$$

Como $p : \mathbb{N} \to \mathbb{N}$ es un polinomio no nulo, existe $n_2 \in \mathbb{N}$ tal que:

$$(\forall n \in \mathbb{N} : n \geq n_2) : (1 \leq p(n))$$

A partir de estos números definimos $n_0 = \text{máx}\{1, n_1, n_2\}$

La demostración del lema

En la demostración del lema consideramos:

- $n \geq n_0$
- $E \subseteq \{0,1\}^{p(n)}$ tal que $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$

Demostración de la parte 1 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Entonces se tiene que:

$$\forall u_1 \in \{0,1\}^{p(n)} \cdots \forall u_{p(n)} \in \{0,1\}^{p(n)} \\ \exists v \in \{0,1\}^{p(n)} \forall i \in \{1,\ldots,p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 1 del lema

Sea v_j el j-ésimo elemento de $\{0,1\}^{p(n)}$ en orden lexicográfico.

Definimos:

$$U = \{(u_1, \ldots, u_{p(n)}) \mid \forall i \in \{1, \ldots, p(n)\} : u_i \in \{0,1\}^{p(n)}\}$$

Podemos reescribir la condición inicial como:

$$\forall (u_1, \ldots, u_{p(n)}) \in U \; \exists j \in \{1, \ldots, 2^{p(n)}\}$$
$$\forall i \in \{1, \ldots, p(n)\} : (u_i \oplus v_j \notin E)$$

Demostración de la parte 1 del lema

Para cada $j \in \{1, \ldots, 2^{p(n)}\}$ definimos:

$$U_j \quad = \quad \{(u_1, \ldots, u_{p(n)}) \in U \mid \forall i \in \{1, \ldots, p(n)\} : u_i \oplus v_j \notin E\}$$

Tenemos entonces que:

$$U \quad = \quad \bigcup_{j=1}^{2^{p(n)}} U_j$$

Entonces existe $\ell \in \{1, \ldots, 2^{p(n)}\}$ tal que:

$$|U_\ell| \;\geq\; \frac{|U|}{2^{p(n)}} \;=\; \frac{2^{p(n)^2}}{2^{p(n)}} \;=\; 2^{p(n)^2 - p(n)}$$

Demostración de la parte 1 del lema

Considere la función $f : U \to U$ definida como:

$$f(u_1, \ldots, u_{p(n)}) \quad = \quad (u_i \oplus v_\ell, \ldots, u_{p(n)} \oplus v_\ell)$$

Tenemos que f es una biyección.

Además, para cada $(u_1, \ldots, u_{p(n)}) \in U_\ell$ se tiene que $f(u_1, \ldots, u_{p(n)}) \in \overline{E}^{p(n)}$

- Concluimos que $|U_\ell| \leq |\overline{E}^{p(n)}| = |\overline{E}|^{p(n)}$

Demostración de la parte 1 del lema

Tenemos entonces que $2^{p(n)^2-p(n)} \leq |U_\ell| \leq |\overline{E}|^{p(n)}$, de lo cual concluimos:

$$2^{p(n)-1} \leq |\overline{E}|$$

Dado que $E \cup \overline{E} = \{0,1\}^{p(n)}$, sabemos que $|E| = 2^{p(n)} - |\overline{E}|$

- Tenemos entonces que $|E| \leq 2^{p(n)} - 2^{p(n)-1} = (1 - \frac{1}{2}) \cdot 2^{p(n)}$

Pero esto contradice el hecho que $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$

- Puesto que $|E| \leq (1 - \frac{1}{2}) \cdot 2^{p(n)} \leq (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$ ya que $n \geq n_0 \geq 1$

Demostración de la parte 2 del lema

Para obtener una contradicción suponemos que la condición es falsa.

Entonces se tiene que:

$$\exists u_1 \in \{0,1\}^{p(n)} \cdots \exists u_{p(n)} \in \{0,1\}^{p(n)}$$
$$\forall v \in \{0,1\}^{p(n)} \exists i \in \{1,\ldots,p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 2 del lema

Sea $u_1, \ldots, u_{p(n)}$ una secuencia de strings en $\{0,1\}^{p(n)}$ que satisfacen la condición anterior.

Definimos $V = \{0,1\}^{p(n)}$, y reescribimos la condición anterior como:

$$\forall v \in V \, \exists i \in \{1, \ldots, p(n)\} : (u_i \oplus v \notin E)$$

Demostración de la parte 2 del lema

Para cada $j \in \{1, \ldots, p(n)\}$ definimos:

$$V_j \quad = \quad \{v \in V \mid u_j \oplus v \notin E\}$$

Tenemos entonces que:

$$V \quad = \quad \bigcup_{j=1}^{p(n)} V_j$$

Entonces existe $\ell \in \{1, \ldots, p(n)\}$ tal que:

$$|V_\ell| \ \geq \ \frac{|V|}{p(n)} \ = \ \frac{2^{p(n)}}{p(n)}$$

Demostración de la parte 2 del lema

Considere la función $g : V \to V$ definida como:

$$g(v) \quad = \quad u_\ell \oplus v$$

Tenemos que g es una biyección.

Además, para cada $v \in V_\ell$ se tiene que $g(v) \in \overline{E}$

- Concluimos que $|V_\ell| \leq |\overline{E}|$

Demostración de la parte 2 del lema

Tenemos entonces que $\frac{2^{p(n)}}{p(n)} \leq |V_\ell| \leq |\overline{E}|$

Dado que $|E| = 2^{p(n)} - |\overline{E}|$, tenemos que:

$$|E| \leq 2^{p(n)} - \frac{2^{p(n)}}{p(n)} = (1 - \frac{1}{p(n)}) \cdot 2^{p(n)}$$

Demostración de la parte 2 del lema

Dado que $n \geq n_0$ tenemos que:

$$
\begin{aligned}
1 \leq p(n) < 2^n \quad &\Rightarrow \quad \frac{1}{2^n} < \frac{1}{p(n)} \\
&\Rightarrow \quad -\frac{1}{p(n)} < -\frac{1}{2^n} \\
&\Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) < \left(1 - \frac{1}{2^n}\right) \\
&\Rightarrow \quad \left(1 - \frac{1}{p(n)}\right) \cdot 2^{p(n)} < \left(1 - \frac{1}{2^n}\right) \cdot 2^{p(n)}
\end{aligned}
$$

Obtenemos una contradicción dado que $|E| \leq (1 - \frac{1}{p(n)}) \cdot 2^{p(n)}$ y por hipótesis $|E| > (1 - \frac{1}{2^n}) \cdot 2^{p(n)}$ □