

# Teorema de Valiant-Vazirani

Martín Muñoz<sup>1</sup>

<sup>1</sup>Departamento de Ciencias de la Computación  
Pontificia Universidad Católica de Chile

TATC, 2016

## 1 Introducción

- El Resultado
- Motivación

## 2 Demostración del teorema

- Hiperplanos
- Construcción
- Demostración del teorema

Definimos la función  $\#SAT : \Sigma^* \rightarrow \mathbb{N}$  como:

$$\#SAT(\varphi) = |\{\sigma : \sigma \text{ es una valuación sobre las variables de } \varphi \text{ y } \sigma(\varphi) = 1.\}|$$

Dada una función  $Q : \Sigma^* \rightarrow \{0, 1\}$ , definimos la función  $USAT_Q : \Sigma^* \rightarrow \{0, 1\}$ :

$$USAT_Q(\varphi) = \begin{cases} 0 & \text{si } \#SAT(\varphi) = 0, \\ 1 & \text{si } \#SAT(\varphi) = 1, \\ Q(\varphi) & \text{si } \#SAT(\varphi) \geq 2 \end{cases}$$

## Teorema (Valiant-Vazirani [2])

*Existe un procedimiento aleatorizado que funciona en tiempo polinomial que, dado una fórmula  $\varphi$  con  $n$  variables, genera  $n + 1$  fórmulas  $\varphi_0, \dots, \varphi_n$  tales que:*

- *Si  $\varphi$  es satisfacible, existe algun  $\varphi_i$  tal que  $\#SAT(\varphi_i) = 1$  con probabilidad  $\geq \frac{1}{8}$ .*
- *Si  $\varphi$  no es satisfacible, para cada  $\varphi_i$  se tiene que  $\#SAT(\varphi_i) = 0$ .*

## Corolario

*Si para alguna función  $Q$  se tiene que  $USAT_Q \in RP$ , entonces  $NP = RP$ .*

¿Por qué nos interesa?

- Evidencia de que la dificultad de SAT no está en el número de soluciones.

Parity-P -  $\oplus P$ :

$L \in \oplus P$  si existe una máquina no determinista que funciona en tiempo polinomial  $M$  tal que para cada  $w \in \{0, 1\}^*$ :

- Si  $w \in L$ , entonces  $M(w)$  tiene un  $\#$  de rutas de aceptación impar.
- Si  $w \notin L$ , entonces  $M(w)$  tiene un  $\#$  de rutas de aceptación par.
- Corolario del teorema:  $NP \subseteq BPP^{\oplus P}$

Mostraremos la demostración del teorema de Valiant-Vazirani hecha por Ilya Posov para la TU de München [1].

# Hiperplanos

Sea  $H \subseteq \{x_1, \dots, x_n\}$ . El hiperplano  $\eta_H$  es una fórmula tal que para cada valuación  $\sigma$  se cumple que  $\sigma(\eta_H) = 1$  si y sólo si  $|\{x_i : \sigma(x_i) = 1\}|$  es par. La fórmula misma es

$$\eta_H = \left( \bigoplus_{x_i \in H} x_i \right) \oplus 1.$$

Ejemplo: si  $H = \{x_1, x_4, x_5\}$ , entonces  $\eta_H = x_1 \oplus x_4 \oplus x_5 \oplus 1$ .

Por simpleza, notaremos subconjuntos de  $\{x_1, \dots, x_n\}$  y valuaciones como vectores en  $\{0, 1\}^n$ .

- $H = (a_1, \dots, a_n)$  donde  $a_i = 1$  ssi  $x_i \in H$ .
- $\sigma = (a_1, \dots, a_n)$  donde  $a_i = 1$  ssi  $\sigma(x_i) = 1$ .

Por la construcción de  $\eta_H$  se puede entender que  $\sigma(\eta_H) = 1$  si los vectores  $\sigma$  y  $H$  son ortogonales.

# Construcción de $\varphi_0, \dots, \varphi_n$

Elegimos  $n$  conjuntos  $H_1, \dots, H_n \in \{0, 1\}^n$  aleatoriamente. Las fórmulas son:

$$\varphi_0 = \varphi$$

$$\varphi_1 = \varphi \wedge \eta_{H_1}$$

$$\varphi_2 = \varphi \wedge \eta_{H_1} \wedge \eta_{H_2}$$

$$\vdots$$

$$\varphi_n = \varphi \wedge \eta_{H_1} \wedge \eta_{H_2} \wedge \dots \wedge \eta_{H_n}$$

Supongamos que  $\varphi$  es satisfacible. Sea  $k$  tal que  $2^k \leq \#\text{SAT}(\varphi) \leq 2^{k+1}$ . A continuación vamos a demostrar que  $\#\text{SAT}(\varphi_{k+2}) = 1$  con probabilidad  $p \geq \frac{1}{8}$ .



# Demostración del teorema

## Lema

*Dada una valuación  $\sigma$ , sea  $\Gamma_\sigma = \{H \mid H \in \{0,1\}^n \text{ y } \sigma(\eta_H) = 1\}$  y sea  $\overline{\Gamma}_\sigma = \{0,1\}^n \setminus \Gamma_\sigma$ . Para toda valuación  $\sigma \neq 0^n$ , se tiene que  $|\Gamma_\sigma| = |\overline{\Gamma}_\sigma|$ . Además, para cada par de valuaciones  $\sigma_1, \sigma_2$  distintas a  $0^n$  se tiene que  $|\Gamma_{\sigma_1} \cap \Gamma_{\sigma_2}| = |\overline{\Gamma}_{\sigma_1} \cap \Gamma_{\sigma_2}|$ .*

## Corolario

- *Dada una valuación  $\sigma \neq 0^n$ , al elegir  $H \in \{0,1\}^n$  aleatoriamente se tiene  $P_H(\sigma(\eta_H) = 1) = \frac{1}{2}$ .*
- *Dadas dos valuaciones distintas  $\sigma_1, \sigma_2$ , se tiene que  $P_H(\sigma_1(\eta_H) = 1)$  y  $P_H(\sigma_2(\eta_H) = 1)$  son independientes.*

# Demostración del teorema

Sea  $\Sigma = \{\sigma \mid \sigma(\varphi) = 1\}$ . Tomemos un  $\sigma^* \in \Sigma$ . Definimos:

$$p_{\sigma^*} = P_{H_1, \dots, H_n}(\sigma^* \text{ es la \u00fanica valuaci\u00f3n que satisface } \varphi_{k+2}),$$

que es igual a

$$p_{\sigma^*} = P_{H_1, \dots, H_n}(\text{Para todo } i \leq k+2 \text{ se tiene que } \sigma^*(\eta_{H_i}) = 1 \\ \text{y para cada otro } \sigma' \in \Sigma \text{ existe un } i \leq k+2 \text{ tal que } \sigma'(\eta_{H_i}) = 0).$$

Ahora, por la segunda parte del corolario, tenemos que

$$p_{\sigma^*} = P_{H_1, \dots, H_n}(\forall i \leq k+2, \sigma^*(\eta_{H_i}) = 1) \\ \cdot P_{H_1, \dots, H_n}(\forall \sigma' \in \Sigma \setminus \{\sigma^*\} \exists i \leq k+2, \sigma'(\eta_{H_i}) = 0))$$

# Demostración del teorema

Llamemos:

- $P_1 = P_{H_1, \dots, H_n}(\text{Para todo } i \leq k+2 \text{ se tiene que } \sigma^*(\eta_{H_i}) = 1),$
- $P_2 = P_{H_1, \dots, H_n}(\forall \sigma' \in \Sigma \setminus \{\sigma^*\} \exists i \leq k+2 \text{ tal que } \sigma'(\eta_{H_i}) = 0).$

Luego

$$p_{\sigma^*} = P_1 \cdot P_2.$$

Como cada  $H_i$  es independiente a los demás,  $P_1$  se puede calcular considerando que se elige solo un  $H \in \{0, 1\}^n$  aleatoriamente. Usando la primera parte del corolario,

$$P_1 = (P_H(\sigma^*(\eta_H) = 1))^{k+2} \geq \frac{1}{2^{k+2}}.$$

# Demostración del teorema

Ahora, tenemos que

$$P_2 = P_{H_1, \dots, H_n}(\forall \sigma' \in \Sigma \setminus \{\sigma^*\} \exists i \leq k+2 \text{ tal que } \sigma'(\eta_{H_i}) = 0) = \\ 1 - P_{H_1, \dots, H_n}(\exists \sigma' \in \Sigma \setminus \{\sigma^*\} \forall i \leq k+2 \text{ tal que } \sigma'(\eta_{H_i}) = 1).$$

Luego para cualquier  $\sigma' \in \Sigma \setminus \{\sigma^*\}$ ,

$$P_2 \geq 1 - (|\Sigma| - 1)P_{H_1, \dots, H_n}(\forall i \leq k+2, \sigma'(\eta_{H_i}) = 1),$$

y por la construcción del  $k$  y usando nuevamente la primera parte del corolario,

$$P_2 \geq 1 - 2^{k+1}(P_H(\sigma'(\eta_H) = 1))^{k+2} \geq 1 - 2^{k+1} \frac{1}{2^{k+2}} = \frac{1}{2},$$

# Demostración del teorema

Finalmente, tenemos que

$$\begin{aligned} p_{\sigma^*} &= P_{H_1, \dots, H_n}(\sigma^* \text{ es la única valuación que satisface } \varphi_{k+2}) \\ &= P_1 \cdot P_2 \\ &\geq \frac{1}{2^{k+2}} \cdot \frac{1}{2} = \frac{1}{2^{k+3}} \end{aligned}$$

Para terminar, notar que  $|\Sigma| \geq 2^k$ , y por el principio de inclusión-exclusión,

$$P_{H_1, \dots, H_n}(\exists \sigma \in \Sigma \text{ tal que } \sigma \text{ es la única valuación para } \varphi_{k+2}) \geq \frac{2^k}{2^{k+3}}.$$

Concluimos que

$$p = P_{H_1, \dots, H_n}(\#SAT(\varphi_{k+2}) = 1) \geq \frac{2^k}{2^{k+3}} = \frac{1}{8}. \quad \square$$

-  Ilya Posov.  
Valiant-vazirani theorem, June 2006.
-  Leslie G. Valiant and Vijay V. Vazirani.  
NP is as easy as detecting unique solutions.  
*Theor. Comput. Sci.*, 47(3):85–93, 1986.