

Otra mirada al lema de amplificación para BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Otra mirada al lema de amplificación para BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Dado $w \in \Sigma^*$ y $s \in \{0, 1\}^*$ tal que $t_M(|w|) \leq |s|$, decimos que $M(w, s)$ es incorrecto si:

$w \in L$ y $M(w, s)$ rechaza
o
 $w \notin L$ y $M(w, s)$ acepta

Otra mirada al lema de amplificación para BPP

Sea M una MT probabilística con alfabeto de entrada Σ

Dado $w \in \Sigma^*$ y $s \in \{0, 1\}^*$ tal que $t_M(|w|) \leq |s|$, decimos que $M(w, s)$ es incorrecto si:

$$\begin{aligned} &w \in L \text{ y } M(w, s) \text{ rechaza} \\ &\quad \text{o} \\ &w \notin L \text{ y } M(w, s) \text{ acepta} \end{aligned}$$

Vamos a utilizar esta noción para dar una mirada alternativa del lema de amplificación para BPP

Otra mirada al lema de amplificación para BPP

Versión alternativa del lema de amplificación para BPP

Sea L un lenguaje sobre un alfabeto Σ . Si $L \in \text{BPP}$, entonces para cada $\ell \in \mathbb{N}$, existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \left(\frac{3}{4}\right)^\ell$$

Segundo ingrediente: Una versión más fuerte del lema de amplificación

Proposición

Sea L un lenguaje sobre un alfabeto Σ . Si $L \in BPP$, entonces existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^$:*

$$Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Demostración de la versión más fuerte

Como $L \in \text{BPP}$, sabemos que existe una MT probabilística M_1 tal que $t_{M_1}(n)$ es $O(n^{k_1})$ y para cada $w \in \Sigma^*$:

$$\Pr_s(M_1(w, s) \text{ es incorrecto}) \leq \frac{1}{4}$$

Suponemos que $t_{M_1}(n)$ es $\Omega(n)$ y $t_{M_1}(n) \geq 2$ para todo $n \in \mathbb{N}$

► ¿Por qué podemos suponer esto?

Demostración de la versión más fuerte

Sea $a = \frac{4}{3}$

Como en la demostración del lema de amplificación, defina una MT probabilística M que con entrada $w \in \Sigma^*$ realiza los siguientes pasos:

1. realiza $(2\ell + 1)$ ejecuciones de la MT probabilística M_1 , donde $\ell = 2\lceil \log_a(t_{M_1}(|w|)) \rceil$
2. retorna **sí** si al menos $(\ell + 1)$ de las ejecuciones dieron respuesta **sí**, y **no** en caso contrario

Demostración de la versión más fuerte

Como en la demostración del lema de amplificación, obtenemos que:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \left(\frac{3}{4}\right)^\ell$$

Vamos a utilizar esta relación y la definición de ℓ para demostrar la versión más fuerte del lema de amplificación

Demostración de la versión más fuerte

Sea $k(n) = 2\lceil \log_a(t_{M_1}(n)) \rceil$

Tenemos que:

$$\begin{aligned} 3(2k(n) + 1)t_{M_1}(n) &= 3(4\lceil \log_a(t_{M_1}(n)) \rceil + 1)t_{M_1}(n) \\ &\leq 15\lceil \log_a(t_{M_1}(n)) \rceil t_{M_1}(n) \end{aligned}$$

puesto que $t_{M_1}(n) \geq 2$ para todo $n \in \mathbb{N}$.

Además, existe una constante n_0 tal que para todo $n \geq n_0$:

$$15\lceil \log_a(t_{M_1}(n)) \rceil t_{M_1}(n) \leq t_{M_1}(n)^2$$

puesto que $t_{M_1}(n)$ es $\Omega(n)$.

Demostración de la versión más fuerte

Por lo tanto para todo $n \geq n_0$:

$$\begin{aligned} 3(2k(n) + 1)t_{M_1}(n) &\leq t_{M_1}(n)^2 \\ &= a^{\log_a(t_{M_1}(n)^2)} \\ &= a^{2 \log_a(t_{M_1}(n))} \\ &\leq a^{2 \lceil \log_a(t_{M_1}(n)) \rceil} \\ &= a^{k(n)} \end{aligned}$$

Dado que $a = \frac{4}{3}$, concluimos que para todo $n \geq n_0$:

$$3(2k(n) + 1)t_{M_1}(n) \leq \left(\frac{4}{3}\right)^{k(n)}$$

Demostración de la versión más fuerte

Suponga que $|w| \geq n_0$

- Vamos a considerar el caso $|w| < n_0$ por separado

De la conclusión en la transparencia anterior obtenemos lo siguiente considerando que $\ell = k(|w|)$:

$$\begin{aligned} \Pr_s(M(w, s) \text{ es incorrecto}) &\leq \left(\frac{3}{4}\right)^\ell \\ &\leq \frac{1}{3(2\ell + 1)t_{M_1}(|w|)} \end{aligned}$$

Demostración de la versión más fuerte

Dado que $t_M(|w|) = (2\ell + 1)t_{M_1}(|w|)$, tenemos que:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Demostración de la versión más fuerte

Dado que $t_M(|w|) = (2\ell + 1)t_{M_1}(|w|)$, tenemos que:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Para concluir la demostración necesitamos considerar el caso $|w| < n_0$

Demostración de la versión más fuerte

Dado que $t_M(|w|) = (2\ell + 1)t_{M_1}(|w|)$, tenemos que:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Para concluir la demostración necesitamos considerar el caso $|w| < n_0$

En este caso podemos modificar M para que satisfaga la condición:

$$\Pr_s(M(w, s) \text{ es incorrecto}) = 0 < \frac{1}{3t_M(|w|)}$$

¿Por qué podemos hacer esto?



Demostración de $\text{BPP} \subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ , y suponga que $L \in \text{BPP}$

Demostración de $BPP \subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ , y suponga que $L \in BPP$

Por lema de amplificación existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Demostración de $\text{BPP} \subseteq \Sigma_2^P$

Sea L un lenguaje sobre un alfabeto Σ , y suponga que $L \in \text{BPP}$

Por lema de amplificación existe una MT probabilística M tal que $t_M(n)$ es $O(n^k)$ y para cada $w \in \Sigma^*$:

$$\Pr_s(M(w, s) \text{ es incorrecto}) \leq \frac{1}{3t_M(|w|)}$$

Además podemos suponer que $t_M(n) > 0$ para cada $n \in \mathbb{N}$

► ¿Por qué?

Demostración de $BPP \subseteq \Sigma_2^P$

Notación

Usamos $s \in \{0, 1\}^m$ para indicar que $s \in \{0, 1\}^*$ y $|s| = m$

Dados a y b en $\{0, 1\}$, la operación $a \oplus b$ es definida como $(a + b) \bmod 2$

► Vale decir, $\oplus$ es el o exclusivo

Dados $x, y \in \{0, 1\}^m$ con $x = a_1 a_2 \cdots a_m$ e $y = b_1 b_2 \cdots b_m$, la operación $x \oplus y$ da como resultado el siguiente string en $\{0, 1\}^m$:

$$(a_1 \oplus b_1)(a_2 \oplus b_2) \cdots (a_m \oplus b_m)$$

Demostración de $\text{BPP} \subseteq \Sigma_2^P$

Defina el lenguaje A de la siguiente forma:

$$A = \{(w, y_1, \dots, y_m, z) \mid w \in \Sigma^*, m = t_M(|w|), \\ y_i \in \{0, 1\}^m \text{ para cada } i \in \{1, \dots, m\}, z \in \{0, 1\}^m \\ \text{y } M(w, y_j \oplus z) \text{ acepta para algún } j \in \{1, \dots, m\} \}$$

Demostración de $BPP \subseteq \Sigma_2^P$

Defina el lenguaje A de la siguiente forma:

$$A = \{ (w, y_1, \dots, y_m, z) \mid w \in \Sigma^*, m = t_M(|w|), \\ y_i \in \{0, 1\}^m \text{ para cada } i \in \{1, \dots, m\}, z \in \{0, 1\}^m \\ \text{y } M(w, y_j \oplus z) \text{ acepta para algún } j \in \{1, \dots, m\} \}$$

Ejercicio

Demuestre que $A \in PTIME$

Demostración de $BPP \subseteq \Sigma_2^P$

Dada la caracterización de Σ_2^P en las transparencias anteriores, para demostrar que $L \in \Sigma_2^P$ basta demostrar la siguiente condición:

Para cada $w \in \Sigma^*$ tal que $t_M(|w|) = m$:

$w \in L$ si y sólo si

$$\exists y_1 \in \{0, 1\}^m \cdots \exists y_m \in \{0, 1\}^m \forall z \in \{0, 1\}^m (w, y_1, \dots, y_m, z) \in A$$

Demostración de $BPP \subseteq \Sigma_2^P$

Dada la caracterización de Σ_2^P en las transparencias anteriores, para demostrar que $L \in \Sigma_2^P$ basta demostrar la siguiente condición:

Para cada $w \in \Sigma^*$ tal que $t_M(|w|) = m$:

$w \in L$ si y sólo si

$$\exists y_1 \in \{0, 1\}^m \cdots \exists y_m \in \{0, 1\}^m \forall z \in \{0, 1\}^m (w, y_1, \dots, y_m, z) \in A$$

Para hacer esta demostración vamos a utilizar el método probabilístico.

- Para demostrar que un objeto con ciertas propiedades existe, en lugar de construirlo demostramos que la probabilidad de que exista es mayor que 0

La dirección ($\Rightarrow$) de la equivalencia

Suponga que $w \in L$ y $t_M(|w|) = m$

La dirección ($\Rightarrow$) de la equivalencia

Suponga que $w \in L$ y $t_M(|w|) = m$

Tenemos que:

$$\begin{aligned} \Pr_{y_1, \dots, y_m} \left(\exists z \in \{0, 1\}^m \bigwedge_{i=1}^m M(w, y_i \oplus z) \text{ rechaza} \right) &\leq \\ \sum_{z \in \{0, 1\}^m} \Pr_{y_1, \dots, y_m} \left(\bigwedge_{i=1}^m M(w, y_i \oplus z) \text{ rechaza} \right) &= \\ \sum_{z \in \{0, 1\}^m} \prod_{i=1}^m \Pr_{y_i} \left(M(w, y_i \oplus z) \text{ rechaza} \right) \end{aligned}$$

La dirección ($\Rightarrow$) de la equivalencia

Dado $a \in \{0, 1\}^m$, la función $f : \{0, 1\}^m \rightarrow \{0, 1\}^m$ definida como $f(x) = x \oplus a$ es **inyectiva**

La dirección ($\Rightarrow$) de la equivalencia

Dado $a \in \{0, 1\}^m$, la función $f : \{0, 1\}^m \rightarrow \{0, 1\}^m$ definida como $f(x) = x \oplus a$ es **inyectiva**

Por lo tanto dado que $w \in L$, concluimos que:

$$\Pr_{y_i} \left(M(w, y_i \oplus z) \text{ rechaza} \right) \leq \frac{1}{3m}$$

La dirección ($\Rightarrow$) de la equivalencia

Dado que $m > 0$ concluimos que:

$$\begin{aligned} \Pr_{y_1, \dots, y_m} \left(\exists z \in \{0, 1\}^m \bigwedge_{i=1}^m M(w, y_i \oplus z) \text{ rechaza} \right) &\leq \\ \sum_{z \in \{0, 1\}^m} \prod_{i=1}^m \Pr_{y_i} \left(M(w, y_i \oplus z) \text{ rechaza} \right) &\leq \\ \sum_{z \in \{0, 1\}^m} \prod_{i=1}^m \frac{1}{3^m} &= \\ \sum_{z \in \{0, 1\}^m} \frac{1}{(3^m)^m} &= \\ \frac{2^m}{(3^m)^m} &< 1 \end{aligned}$$

La dirección ($\Rightarrow$) de la equivalencia

Por lo tanto existen $y_1 \in \{0, 1\}^m, \dots, y_m \in \{0, 1\}^m$ tales que la siguiente condición es cierta:

$$\forall z \in \{0, 1\}^m \bigvee_{i=1}^m M(w, y_i \oplus z) \text{ acepta}$$

La dirección ($\Rightarrow$) de la equivalencia

Por lo tanto existen $y_1 \in \{0, 1\}^m, \dots, y_m \in \{0, 1\}^m$ tales que la siguiente condición es cierta:

$$\forall z \in \{0, 1\}^m \bigvee_{i=1}^m M(w, y_i \oplus z) \text{ acepta}$$

Concluimos que:

$$\exists y_1 \in \{0, 1\}^m \cdots \exists y_m \in \{0, 1\}^m \forall z \in \{0, 1\}^m (w, y_1, \dots, y_m, z) \in A$$

La dirección ($\Rightarrow$) de la equivalencia

¿Es necesario el uso de z para esta dirección de la demostración?

La dirección ($\Rightarrow$) de la equivalencia

¿Es necesario el uso de z para esta dirección de la demostración?

Dado que $w \in L$ y $m > 0$ tenemos que:

$$\begin{aligned} \Pr_{y_1, \dots, y_m} \left(\bigwedge_{i=1}^m M(w, y_i) \text{ rechaza} \right) &= \prod_{i=1}^m \Pr_{y_i} \left(M(w, y_i) \text{ rechaza} \right) \\ &\leq \prod_{i=1}^m \frac{1}{3^m} = \\ &= \frac{1}{(3^m)^m} < 1 \end{aligned}$$

La dirección ($\Rightarrow$) de la equivalencia

¿Es necesario el uso de z para esta dirección de la demostración?

Dado que $w \in L$ y $m > 0$ tenemos que:

$$\begin{aligned} \Pr_{y_1, \dots, y_m} \left(\bigwedge_{i=1}^m M(w, y_i) \text{ rechaza} \right) &= \prod_{i=1}^m \Pr_{y_i} \left(M(w, y_i) \text{ rechaza} \right) \\ &\leq \prod_{i=1}^m \frac{1}{3^m} = \\ &= \frac{1}{(3^m)^m} < 1 \end{aligned}$$

Por lo que el uso de z no es estrictamente necesario para esta parte de la demostración.

► Pero sí es necesario para la otra dirección

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

Además, suponga que $y_1 \in \{0, 1\}^m, \dots, y_m \in \{0, 1\}^m$

La dirección ($\Leftarrow$) de la equivalencia

Suponga que $w \notin L$ y $t_M(|w|) = m$

- Para demostrar la dirección ($\Leftarrow$) consideramos el contrapositivo

Además, suponga que $y_1 \in \{0, 1\}^m, \dots, y_m \in \{0, 1\}^m$

Dado que $w \notin L$ y $m > 0$ tenemos que:

$$\begin{aligned} \Pr_z \left(\bigvee_{i=1}^m M(w, y_i \oplus z) \text{ acepta} \right) &\leq \sum_{i=1}^m \Pr_z \left(M(w, y_i \oplus z) \text{ acepta} \right) \\ &\leq \sum_{i=1}^m \frac{1}{3^m} \\ &= \frac{m}{3^m} \\ &= \frac{1}{3} \end{aligned}$$

La dirección ($\Leftarrow$) de la equivalencia

Se concluye que:

$$\begin{aligned}\Pr_z\left(\bigwedge_{i=1}^m M(w, y_i \oplus z) \text{ rechaza}\right) &= 1 - \Pr_z\left(\bigvee_{i=1}^m M(w, y_i \oplus z) \text{ acepta}\right) \\ &\geq 1 - \frac{1}{3} \\ &= \frac{2}{3}\end{aligned}$$

La dirección ($\Leftarrow$) de la equivalencia

Se concluye que:

$$\begin{aligned}\Pr_z\left(\bigwedge_{i=1}^m M(w, y_i \oplus z) \text{ rechaza}\right) &= 1 - \Pr_z\left(\bigvee_{i=1}^m M(w, y_i \oplus z) \text{ acepta}\right) \\ &\geq 1 - \frac{1}{3} \\ &= \frac{2}{3}\end{aligned}$$

Por lo tanto tenemos que existe $z \in \{0, 1\}^m$ tal que $M(w, y_i \oplus z)$ rechaza para cada $i \in \{1, \dots, m\}$

La dirección ($\Leftarrow$) de la equivalencia

Dado que $y_1, \dots, y_m$ son elementos arbitrarios en el conjunto $\{0, 1\}^m$, tenemos finalmente que:

$$\forall y_1 \in \{0, 1\}^m \cdots \forall y_m \in \{0, 1\}^m \exists z \in \{0, 1\}^m (w, y_1, \dots, y_m, z) \notin A$$

La dirección ($\Leftarrow$) de la equivalencia

En esta dirección de la demostración si es necesario el uso de z

La dirección ($\Leftarrow$) de la equivalencia

En esta dirección de la demostración si es necesario el uso de z

Si existe $y \in \{0, 1\}^m$ tal que $M(w, y)$ acepta, entonces existen $y_1 \in \{0, 1\}^m$, $\dots$, $y_m \in \{0, 1\}^m$ tales que la siguiente condición es **falsa**:

$$\bigwedge_{i=1}^m M(w, y_i) \text{ rechaza}$$

La dirección ($\Leftarrow$) de la equivalencia

En esta dirección de la demostración si es necesario el uso de z

Si existe $y \in \{0, 1\}^m$ tal que $M(w, y)$ acepta, entonces existen $y_1 \in \{0, 1\}^m$, $\dots$, $y_m \in \{0, 1\}^m$ tales que la siguiente condición es **falsa**:

$$\bigwedge_{i=1}^m M(w, y_i) \text{ rechaza}$$

Concluimos que la idea de la demostración no funciona sin la utilización de z para m elementos arbitrarios $y_1, \dots, y_m$ del conjunto $\{0, 1\}^m$ □