

La demostración general

Vamos a extender las ideas utilizadas para $\#SAT$ y $\#KS$ al caso general.

Vale decir, dada una p -relación R auto-reducible, vamos a demostrar que si existe un FPAUG para R , entonces existe un FPRAS para R

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Sean $g : \Sigma^* \rightarrow \mathbb{N}$, $\psi : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ y $\sigma : \Sigma^* \rightarrow \mathbb{N}$ funciones que muestran que R es auto-reducible.

- De acuerdo a la definición vista en las transparencias anteriores

Además, sea $\mathcal{G} : \Sigma^* \times (0, 1) \rightarrow \Sigma^* \cup \{\perp\}$ un FPAUG para R

Algunos supuestos para la relación R

Suponemos que $R \subseteq \Sigma^* \times \Sigma^*$, y dados $x, w \in \Sigma^*$ definimos:

$$\text{Ext}_R(x, w) = \{y \in \Sigma^* \mid (x, y) \in R \text{ y existe } z \in \Sigma^* \text{ tal que } y = wz\}$$

Sean $g : \Sigma^* \rightarrow \mathbb{N}$, $\psi : \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ y $\sigma : \Sigma^* \rightarrow \mathbb{N}$ funciones que muestran que R es auto-reducible.

- De acuerdo a la definición vista en las transparencias anteriores

Además, sea $\mathcal{G} : \Sigma^* \times (0, 1) \rightarrow \Sigma^* \cup \{\perp\}$ un FPAUG para R

Finalmente, sean $c, d \in \mathbb{R}^+$ tales que $|\Sigma|^{\sigma(x)} \leq |x|^c + d$ para todo $x \in \Sigma^*$

- Sabemos que existe porque $\sigma(x) \in O(\log(|x|))$

Un esquema de aproximación para R

```
EAR( $x, \varepsilon$ )  
  if  $\mathcal{G}(x, \varepsilon) = \perp$  then return 0  
  else  
     $N := 1$   
     $m := g(x)$   
     $t := \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$   
    while  $g(x) > 0$  do  
      for  $j := 1$  to  $t$  do  
         $y_j := \mathcal{G}\left(x, \frac{\varepsilon}{5m}\right)$   
        Sea  $w \in \Sigma^{\sigma(x)}$  el prefijo de largo  $\sigma(x)$  más común en  $\{y_1, \dots, y_t\}$   
         $\alpha := \frac{|\{j \in \{1, \dots, t\} \mid y_j \in \text{Ext}_R(x, w)\}|}{t}$   
         $x := \psi(x, w)$   
         $N := \frac{1}{\alpha} \cdot N$       /* se tiene que  $\alpha > 0$  */  
  return  $N$ 
```

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

Si $N_R(x) = 0$, tenemos que **EAR**(x, ε) retorna el resultado correcto 0 dado que $\mathcal{G}$ es un FPAUG para R

- ▶ En el resto de la demostración suponemos que $N_R(x) > 0$

EAR es un FPRAS para R

Vamos a demostrar que **EAR** es un FPRAS para R

- ▶ Sean $x \in \Sigma^*$ y $\varepsilon \in (0, 1)$ una entrada de **EAR**

Si $N_R(x) = 0$, tenemos que **EAR**(x, ε) retorna el resultado correcto 0 dado que $\mathcal{G}$ es un FPAUG para R

- ▶ En el resto de la demostración suponemos que $N_R(x) > 0$

De la misma forma, **EAR**(x, ε) retorna el resultado correcto si $g(x) = 0$

- ▶ ¿Por qué?

En el resto de la demostración suponemos que $g(x) > 0$

EAR es un FPRAS para R

Tenemos que el valor de la función g disminuye en cada iteración

- ▶ ¿Por qué?

EAR es un FPRAS para R

Tenemos que el valor de la función g disminuye en cada iteración

- ¿Por qué?

Sea s la cantidad total de iteraciones realizadas por el algoritmo.

- Tenemos que $s \leq g(x) = m$

EAR es un FPRAS para R

EAR funciona en tiempo polinomial en $|x|$ y $\frac{1}{\varepsilon}$

- ▶ Dado que R es una p -relación, sabemos que existe un polinomio fijo $p(u)$ tal que $m = g(x) \leq p(|x|)$
- ▶ Además, sabemos que m puede ser calculado en tiempo polinomial dada la definición de relación auto-reducible
- ▶ Finalmente, tenemos que $\mathcal{G}$ es un FPAUG para R , y **EAR** realiza a lo más $m \cdot \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$ llamadas a la función $\mathcal{G}$

EAR es un FPRAS para R

EAR funciona en tiempo polinomial en $|x|$ y $\frac{1}{\varepsilon}$

- ▶ Dado que R es una p -relación, sabemos que existe un polinomio fijo $p(u)$ tal que $m = g(x) \leq p(|x|)$
- ▶ Además, sabemos que m puede ser calculado en tiempo polinomial dada la definición de relación auto-reducible
- ▶ Finalmente, tenemos que $\mathcal{G}$ es un FPAUG para R , y **EAR** realiza a lo más $m \cdot \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$ llamadas a la función $\mathcal{G}$

Nos queda entonces por demostrar:

$$\Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)\right) \geq \frac{3}{4}$$

La propiedad central

Dado $i \in \{1, \dots, s\}$, para la iteración i del algoritmo sean:

- ▶ x_i, N_i los valores de las variables x y N al principio de la iteración
 - ▶ Tenemos que $x_1 = x$ y $N_1 = 1$
- ▶ w_i, α_i los valores de las variables w y α calculados en la iteración

La propiedad central

Dado $i \in \{1, \dots, s\}$, para la iteración i del algoritmo sean:

- ▶ x_i, N_i los valores de las variables x y N al principio de la iteración
 - ▶ Tenemos que $x_1 = x$ y $N_1 = 1$
- ▶ w_i, α_i los valores de las variables w y α calculados en la iteración

Propiedad de aproximación

Para cada $i \in \{1, \dots, s\}$:

$$\frac{\alpha_i}{1 + \frac{\varepsilon}{2m}} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i$$

Usando la propiedad de aproximación

Tenemos que:

$$\begin{aligned} \Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)\right) &= \\ \Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \text{propiedad de aproximación}\right) &\cdot \\ \Pr\left(\text{propiedad de aproximación}\right) + & \\ \Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \overline{\text{propiedad de aproximación}}\right) &\cdot \\ \Pr\left(\overline{\text{propiedad de aproximación}}\right) \geq & \\ \Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \text{propiedad de aproximación}\right) &\cdot \\ \Pr\left(\text{propiedad de aproximación}\right) & \end{aligned}$$

Usando la propiedad de aproximación

Por lo tanto, para demostrar que **EAR** es un FPRAS para R basta acotar inferiormente la siguiente probabilidad:

$$\Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \text{propiedad de aproximación}\right) \cdot \Pr(\text{propiedad de aproximación})$$

Usando la propiedad de aproximación

Por lo tanto, para demostrar que **EAR** es un FPRAS para R basta acotar inferiormente la siguiente probabilidad:

$$\Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \text{propiedad de aproximación}\right) \cdot \Pr(\text{propiedad de aproximación})$$

Primero vamos a demostrar que la propiedad de aproximación es suficiente para tener una buena aproximación de $N_R(x)$

- Después de esto vamos a acotar inferiormente la probabilidad de que la propiedad de aproximación se cumpla

La propiedad de aproximación es suficiente

Definimos x_{s+1} y N_{s+1} como los valores de las variables x y N al final de la iteración s del algoritmo.

La propiedad de aproximación es suficiente

Definimos x_{s+1} y N_{s+1} como los valores de las variables x y N al final de la iteración s del algoritmo.

- ▶ Tenemos que $g(x_{s+1}) = 0$, $N_R(x_{s+1}) = 1$ y el valor retornado por el algoritmo es N_{s+1}
 - ▶ ¿Por qué?

La propiedad de aproximación es suficiente

Definimos x_{s+1} y N_{s+1} como los valores de las variables x y N al final de la iteración s del algoritmo.

- ▶ Tenemos que $g(x_{s+1}) = 0$, $N_R(x_{s+1}) = 1$ y el valor retornado por el algoritmo es N_{s+1}
 - ▶ ¿Por qué?

Dado $i \in \{1, \dots, s\}$, tenemos que:

$$\begin{aligned}x_{i+1} &= \psi(x_i, w_i) \\ N_R(x_{i+1}) &= |\text{Ext}_R(x_i, w_i)| \\ N_{i+1} &= \frac{1}{\alpha_i} \cdot N_i\end{aligned}$$

La propiedad de aproximación es suficiente

Además, tenemos que:

$$\begin{aligned}\frac{\alpha_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i \\ \Rightarrow \frac{N_R(x_i)}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq \frac{|\text{Ext}_R(x_i, w_i)|}{\alpha_i} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \\ \Rightarrow \frac{N_R(x_i) \cdot N_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq |\text{Ext}_R(x_i, w_i)| \cdot \frac{N_i}{\alpha_i} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \cdot N_i \\ \Rightarrow \frac{N_R(x_i) \cdot N_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq N_R(x_{i+1}) \cdot N_{i+1} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \cdot N_i\end{aligned}$$

La propiedad de aproximación es suficiente

Además, tenemos que:

$$\begin{aligned}\frac{\alpha_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i \\ \Rightarrow \frac{N_R(x_i)}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq \frac{|\text{Ext}_R(x_i, w_i)|}{\alpha_i} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \\ \Rightarrow \frac{N_R(x_i) \cdot N_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq |\text{Ext}_R(x_i, w_i)| \cdot \frac{N_i}{\alpha_i} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \cdot N_i \\ \Rightarrow \frac{N_R(x_i) \cdot N_i}{\left(1 + \frac{\varepsilon}{2m}\right)} &\leq N_R(x_{i+1}) \cdot N_{i+1} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot N_R(x_i) \cdot N_i\end{aligned}$$

Así, la cantidad $N_R(x_i) \cdot N_i$ es *casi* una invariante del ciclo **while**

La propiedad de aproximación es suficiente

Suponiendo que la propiedad de aproximación es cierta concluimos que:

$$\frac{N_R(x_1) \cdot N_1}{\left(1 + \frac{\varepsilon}{2m}\right)^s} \leq N_R(x_{s+1}) \cdot N_{s+1} \leq \left(1 + \frac{\varepsilon}{2m}\right)^s \cdot N_R(x_1) \cdot N_1$$

La propiedad de aproximación es suficiente

Suponiendo que la propiedad de aproximación es cierta concluimos que:

$$\frac{N_R(x_1) \cdot N_1}{\left(1 + \frac{\varepsilon}{2m}\right)^s} \leq N_R(x_{s+1}) \cdot N_{s+1} \leq \left(1 + \frac{\varepsilon}{2m}\right)^s \cdot N_R(x_1) \cdot N_1$$

Por lo tanto, dado que $s \leq m$ tenemos que:

$$\frac{N_R(x_1) \cdot N_1}{\left(1 + \frac{\varepsilon}{2m}\right)^m} \leq N_R(x_{s+1}) \cdot N_{s+1} \leq \left(1 + \frac{\varepsilon}{2m}\right)^m \cdot N_R(x_1) \cdot N_1$$

Algunas propiedades de $N_R(x_i) \cdot N_i$

Dado que $x_1 = x$ y $N_1 = 1$, tenemos que $N_R(x) = N_R(x_1) \cdot N_1$

- Recuerde que queremos calcular $N_R(x)$

Algunas propiedades de $N_R(x_i) \cdot N_i$

Dado que $x_1 = x$ y $N_1 = 1$, tenemos que $N_R(x) = N_R(x_1) \cdot N_1$

- Recuerde que queremos calcular $N_R(x)$

Dado que $N_R(x_{s+1}) = 1$, tenemos que $N_R(x_{s+1}) \cdot N_{s+1} = N_{s+1}$

- Además, sabemos que **EAR**(x, ε) = N_{s+1}

La propiedad de aproximación es suficiente: conclusión

Juntando los resultados anteriores obtenemos:

$$\frac{N_R(x)}{\left(1 + \frac{\varepsilon}{2m}\right)^m} \leq \mathbf{EAR}(x, \varepsilon) \leq \left(1 + \frac{\varepsilon}{2m}\right)^m \cdot N_R(x)$$

La propiedad de aproximación es suficiente: conclusión

Juntando los resultados anteriores obtenemos:

$$\frac{N_R(x)}{\left(1 + \frac{\varepsilon}{2m}\right)^m} \leq \mathbf{EAR}(x, \varepsilon) \leq \left(1 + \frac{\varepsilon}{2m}\right)^m \cdot N_R(x)$$

Dado que $\varepsilon \in (0, 1)$, tal como el caso de $\#KS$ obtenemos:

$$\left(1 + \frac{\varepsilon}{2m}\right)^m \leq e^{\frac{\varepsilon}{2}} \leq \varepsilon + 1$$

La propiedad de aproximación es suficiente: conclusión

Juntando los resultados anteriores obtenemos:

$$\frac{N_R(x)}{\left(1 + \frac{\varepsilon}{2m}\right)^m} \leq \mathbf{EAR}(x, \varepsilon) \leq \left(1 + \frac{\varepsilon}{2m}\right)^m \cdot N_R(x)$$

Dado que $\varepsilon \in (0, 1)$, tal como el caso de #KS obtenemos:

$$\left(1 + \frac{\varepsilon}{2m}\right)^m \leq e^{\frac{\varepsilon}{2}} \leq \varepsilon + 1$$

Ejercicio

Demuestre que $e^{\frac{\varepsilon}{2}} \leq \varepsilon + 1$ considerando que $0 < \varepsilon < 1$ y el intervalo donde la función $f(x) = e^{\frac{x}{2}} - x - 1$ es negativa.

La propiedad de aproximación es suficiente: conclusión

Así, suponiendo que la propiedad de aproximación se cumple obtenemos:

$$\frac{N_R(x)}{(1 + \varepsilon)} \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)$$

La propiedad de aproximación es suficiente: conclusión

Así, suponiendo que la propiedad de aproximación se cumple obtenemos:

$$\frac{N_R(x)}{(1 + \varepsilon)} \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)$$

Sabemos que $(1 - \varepsilon) \leq \frac{1}{1 + \varepsilon}$, puesto que $\varepsilon > 0$

La propiedad de aproximación es suficiente: conclusión

Así, suponiendo que la propiedad de aproximación se cumple obtenemos:

$$\frac{N_R(x)}{(1 + \varepsilon)} \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)$$

Sabemos que $(1 - \varepsilon) \leq \frac{1}{1 + \varepsilon}$, puesto que $\varepsilon > 0$

Suponiendo que la propiedad de aproximación se cumple, obtenemos entonces:

$$(1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x)$$

La propiedad de aproximación es suficiente: conclusión

Vale decir, hemos demostrado que:

$$\Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \begin{array}{l} \text{propiedad de aproximación} \end{array} \right) = 1$$

La propiedad de aproximación es suficiente: conclusión

Vale decir, hemos demostrado que:

$$\Pr\left((1 - \varepsilon) \cdot N_R(x) \leq \mathbf{EAR}(x, \varepsilon) \leq (1 + \varepsilon) \cdot N_R(x) \mid \begin{array}{l} \text{propiedad de aproximación} \end{array} \right) = 1$$

De esta forma, para terminar la demostración tenemos que demostrar:

$$\Pr\left(\text{propiedad de aproximación} \right) \geq \frac{3}{4}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$

Fije $i \in \{1, \dots, s\}$

► i corresponde a una iteración de **EAR**

Para cada $u \in \Sigma^{\sigma(x_i)}$ definimos la variable aleatoria:

$$X_u = \frac{|\{j \in \{1, \dots, t\} \mid \exists z \in \Sigma^* : y_j = uz\}|}{t}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$

Fije $i \in \{1, \dots, s\}$

- ▶ i corresponde a una iteración de **EAR**

Para cada $u \in \Sigma^{\sigma(x_i)}$ definimos la variable aleatoria:

$$X_u = \frac{|\{j \in \{1, \dots, t\} \mid \exists z \in \Sigma^* : y_j = uz\}|}{t}$$

X_u es un promedio de t variables aleatorias que toman valor 0 ó 1, las cuales denotamos como $X_{j,u}$ para $j \in \{1, \dots, t\}$

- ▶ $X_{j,u}(y_j) = 1$ si $y_j = uz$ para algún $z \in \Sigma^*$, y $X_{j,u}(y_j) = 0$ en otro caso

Vale decir, tenemos que $X_u = \frac{1}{t} \sum_{j=1}^t X_{j,u}$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$

Tenemos que:

$$\mathbf{Var}[X_u] = \mathbf{Var}\left[\frac{1}{t} \sum_{j=1}^t X_{j,u}\right] = \frac{1}{t^2} \sum_{j=1}^t \mathbf{Var}[X_{j,u}] \leq \frac{1}{t^2} \sum_{j=1}^t 1 = \frac{1}{t}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$

Tenemos que:

$$\mathbf{Var}[X_u] = \mathbf{Var}\left[\frac{1}{t} \sum_{j=1}^t X_{j,u}\right] = \frac{1}{t^2} \sum_{j=1}^t \mathbf{Var}[X_{j,u}] \leq \frac{1}{t^2} \sum_{j=1}^t 1 = \frac{1}{t}$$

Dado que $t = \lceil 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2} \rceil$, por la desigualdad de Chebyshev concluimos que:

$$\begin{aligned} \Pr\left(|X_u - \mathbf{E}[X_u]| \geq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m}\right) &\leq \frac{36 \cdot (|x|^c + d)^2 \cdot m^2 \cdot \mathbf{Var}[X_u]}{\varepsilon^2} \\ &\leq \frac{36 \cdot (|x|^c + d)^2 \cdot m^2}{\varepsilon^2 \cdot t} \\ &\leq \frac{36 \cdot (|x|^c + d)^2 \cdot m^2}{\varepsilon^2 \cdot 180 \cdot (|x|^c + d)^3 \cdot m^3 \cdot \varepsilon^{-2}} \\ &= \frac{1}{5 \cdot (|x|^c + d) \cdot m} \end{aligned}$$

Definiendo α_i en términos de las variables aleatorias X_u

El valor de cada variable aleatoria X_u es una función de las variables $y_1, \dots, y_t$

- Podemos entonces hablar de $X_u(y_1, \dots, y_t)$

Definiendo α_i en términos de las variables aleatorias X_u

El valor de cada variable aleatoria X_u es una función de las variables $y_1, \dots, y_t$

- Podemos entonces hablar de $X_u(y_1, \dots, y_t)$

De la misma forma, el valor de la variable aleatoria α_i es una función de $y_1, \dots, y_t$, y podemos hablar de $\alpha_i(y_1, \dots, y_t)$

Definiendo α_i en términos de las variables aleatorias X_u

Suponga que v es el valor de w_i . Si los valores de las variables $y_1, \dots, y_t$ en la iteración i son $a_1, \dots, a_t$, respectivamente, entonces tenemos que:

$$\alpha_i(a_1, \dots, a_t) = X_v(a_1, \dots, a_t)$$

Definiendo α_i en términos de las variables aleatorias X_u

Suponga que v es el valor de w_i . Si los valores de las variables $y_1, \dots, y_t$ en la iteración i son $a_1, \dots, a_t$, respectivamente, entonces tenemos que:

$$\alpha_i(a_1, \dots, a_t) = X_v(a_1, \dots, a_t)$$

Además, en general tenemos que:

$$\alpha_i(y_1, \dots, y_t) = \max_{u \in \Sigma^{\sigma(x_i)}} X_u(y_1, \dots, y_t)$$

Definiendo α_i en términos de las variables aleatorias X_u

Suponga que v es el valor de w_i . Si los valores de las variables $y_1, \dots, y_t$ en la iteración i son $a_1, \dots, a_t$, respectivamente, entonces tenemos que:

$$\alpha_i(a_1, \dots, a_t) = X_v(a_1, \dots, a_t)$$

Además, en general tenemos que:

$$\alpha_i(y_1, \dots, y_t) = \max_{u \in \Sigma^{\sigma(x_i)}} X_u(y_1, \dots, y_t)$$

Es importante notar que **no** podemos concluir que:

$$\alpha_i(y_1, \dots, y_t) = X_v(y_1, \dots, y_t),$$

dado que v es un string **fijo** calculado en la iteración i

No podemos concluir que $\alpha_i(y_1, \dots, y_t) = X_v(y_1, \dots, y_t)$

Suponga que ejecutamos el algoritmo nuevamente obteniendo v' como el valor de w_i

- ▶ Además, suponga que los valores de las variables $y_1, \dots, y_t$ en la iteración i de esta nueva ejecución son $b_1, \dots, b_t$, respectivamente.

No podemos concluir que $\alpha_i(y_1, \dots, y_t) = X_v(y_1, \dots, y_t)$

Suponga que ejecutamos el algoritmo nuevamente obteniendo v' como el valor de w_i

- ▶ Además, suponga que los valores de las variables $y_1, \dots, y_t$ en la iteración i de esta nueva ejecución son $b_1, \dots, b_t$, respectivamente.

Sabemos que $\alpha_i(b_1, \dots, b_t) = X_{v'}(b_1, \dots, b_t)$

No podemos concluir que $\alpha_i(y_1, \dots, y_t) = X_v(y_1, \dots, y_t)$

Suponga que ejecutamos el algoritmo nuevamente obteniendo v' como el valor de w_i

- ▶ Además, suponga que los valores de las variables $y_1, \dots, y_t$ en la iteración i de esta nueva ejecución son $b_1, \dots, b_t$, respectivamente.

Sabemos que $\alpha_i(b_1, \dots, b_t) = X_{v'}(b_1, \dots, b_t)$

Pero si $v \neq v'$ y $X_v(b_1, \dots, b_t) < X_{v'}(b_1, \dots, b_t)$, entonces tenemos que:

$$\alpha_i(b_1, \dots, b_t) \neq X_v(b_1, \dots, b_t)$$

Acotando superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Queremos entender cuán cerca está α_i de $\mathbf{E}[X_{w_i}]$

- ▶ Vale decir, queremos acotar superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Acotando superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Queremos entender cuán cercar está α_i de $\mathbf{E}[X_{w_i}]$

- ▶ Vale decir, queremos acotar superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Dado que $\alpha_i = \max_{u \in \Sigma^{\sigma(x_i)}} X_u$, no podemos utilizar la desigualdad de

Chebyshev para acotar superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

- ▶ ¿Por qué?

Acotando superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Si $|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta$ en la iteración i , entonces se debe tener que $|X_{w_i} - \mathbf{E}[X_{w_i}]| \geq \delta$

- Y si esperamos que esto se cumpla en la iteración i de cada ejecución de **EAR**, entonces en cada ejecución debe ser posible encontrar $u \in \Sigma^{\sigma(x_i)}$ tal que $|X_u - \mathbf{E}[X_u]| \geq \delta$

Acotando superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta)$

Si $|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta$ en la iteración i , entonces se debe tener que $|X_{w_i} - \mathbf{E}[X_{w_i}]| \geq \delta$

- Y si esperamos que esto se cumpla en la iteración i de cada ejecución de **EAR**, entonces en cada ejecución debe ser posible encontrar $u \in \Sigma^{\sigma(x_i)}$ tal que $|X_u - \mathbf{E}[X_u]| \geq \delta$

Por lo tanto, tenemos que:

$$\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \delta) \leq \Pr\left(\bigvee_{u \in \Sigma^{\sigma(x_i)}} |X_u - \mathbf{E}[X_u]| \geq \delta\right)$$

Acotando superiormente $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m})$

Utilizando la conclusión de la transparencia anterior:

$$\begin{aligned} \Pr\left(|\alpha_i - \mathbf{E}[X_{w_i}]| \geq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m}\right) &\leq \\ \Pr\left(\bigvee_{u \in \Sigma^{\sigma(x_i)}} \left[|X_u - \mathbf{E}[X_u]| \geq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m}\right]\right) &\leq \\ \sum_{u \in \Sigma^{\sigma(x_i)}} \Pr\left(|X_u - \mathbf{E}[X_u]| \geq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m}\right) &\leq \\ \sum_{u \in \Sigma^{\sigma(x_i)}} \frac{1}{5 \cdot (|x|^c + d) \cdot m} &= \\ \frac{1}{5 \cdot (|x|^c + d) \cdot m} \cdot |\Sigma|^{\sigma(x_i)} &\leq \\ \frac{1}{5 \cdot (|x|^c + d) \cdot m} \cdot (|x_i|^c + d) &= \frac{1}{5m} \cdot \left(\frac{|x_i|^c + d}{|x|^c + d}\right) \leq \frac{1}{5m} \end{aligned}$$

¿Por qué **EAR** elige el prefijo de largo $\sigma(x)$ más común en $\{y_1, \dots, y_t\}$?

Como w_i se elige como el prefijo de largo $\sigma(x_i)$ más común en $\{y_1, \dots, y_t\}$, sabemos que:

$$\alpha_i = \frac{|\{j \in \{1, \dots, t\} \mid y_j \in \text{Ext}_R(x_i, w_i)\}|}{t} \geq \frac{t}{|\Sigma|^{\sigma(x_i)}} \cdot \frac{1}{t} = \frac{1}{|\Sigma|^{\sigma(x_i)}} \geq \frac{1}{|x_i|^c + d} \geq \frac{1}{|x|^c + d}$$

¿Por qué **EAR** elige el prefijo de largo $\sigma(x)$ más común en $\{y_1, \dots, y_t\}$?

Como w_i se elige como el prefijo de largo $\sigma(x_i)$ más común en $\{y_1, \dots, y_t\}$, sabemos que:

$$\alpha_i = \frac{|\{j \in \{1, \dots, t\} \mid y_j \in \text{Ext}_R(x_i, w_i)\}|}{t} \geq \frac{t}{|\Sigma|^{\sigma(x_i)}} \cdot \frac{1}{t} = \frac{1}{|\Sigma|^{\sigma(x_i)}} \geq \frac{1}{|x_i|^c + d} \geq \frac{1}{|x|^c + d}$$

Concluimos entonces que:

$$\begin{aligned} \Pr\left(|\alpha_i - \mathbf{E}[X_{w_i}]| \leq \alpha_i \cdot \frac{\varepsilon}{6m}\right) &\geq \Pr\left(|\alpha_i - \mathbf{E}[X_{w_i}]| \leq \frac{\varepsilon}{6 \cdot (|x|^c + d) \cdot m}\right) \\ &\geq 1 - \frac{1}{5m} \end{aligned}$$

Dos desigualdades útiles

Tenemos que $1 + \frac{\varepsilon}{5m} \geq 1 + \frac{\varepsilon}{6m}$

Dos desigualdades útiles

Tenemos que $1 + \frac{\varepsilon}{5m} \geq 1 + \frac{\varepsilon}{6m}$

Por otra parte, para $\varepsilon \in (0, 1)$ también se tiene que:

$$\frac{1}{1 + \frac{\varepsilon}{5m}} \leq 1 - \frac{\varepsilon}{6m},$$

puesto que $m \geq 1$ y:

$$\begin{aligned} \frac{1}{1 + \frac{\varepsilon}{5m}} \leq 1 - \frac{\varepsilon}{6m} &\Leftrightarrow \frac{5m}{5m + \varepsilon} \leq \frac{6m - \varepsilon}{6m} \\ &\Leftrightarrow 30 \cdot m^2 \leq 30 \cdot m^2 + 6 \cdot m \cdot \varepsilon - 5 \cdot m \cdot \varepsilon - \varepsilon^2 \\ &\Leftrightarrow \varepsilon^2 \leq m \cdot \varepsilon \\ &\Leftrightarrow \varepsilon \leq m \end{aligned}$$

Una cota inferior para $\Pr(|\alpha_i - \mathbf{E}[X_{w_i}]| \leq \alpha_i \cdot \frac{\varepsilon}{6m})$

Usando todas las desigualdades anteriores concluimos que:

$$\begin{aligned} \Pr\left(\frac{1}{(1 + \frac{\varepsilon}{5m})} \cdot \alpha_i \leq \mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \alpha_i\right) &\geq \\ \Pr\left(\left(1 - \frac{\varepsilon}{6m}\right) \cdot \alpha_i \leq \mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{6m}\right) \cdot \alpha_i\right) &= \\ \Pr\left(|\alpha_i - \mathbf{E}[X_{w_i}]| \leq \alpha_i \cdot \frac{\varepsilon}{6m}\right) &\geq \\ 1 - \frac{1}{5m} \end{aligned}$$

Acotando $\mathbf{E}[X_{w_i}]$

Por definición de X_{w_i} , se tiene que:

$$\begin{aligned}\mathbf{E}[X_{w_i}] &= \mathbf{E}\left[\frac{1}{t} \sum_{j=1}^t X_{j,w_i}\right] \\&= \frac{1}{t} \sum_{j=1}^t \mathbf{E}[X_{j,w_i}] \\&= \frac{1}{t} \sum_{j=1}^t \left(1 \cdot \mathbf{Pr}(X_{j,w_i} = 1) + 0 \cdot \mathbf{Pr}(X_{j,w_i} = 0)\right) \\&= \frac{1}{t} \sum_{j=1}^t \sum_{y \in \text{Ext}_R(x_i, w_i)} \mathbf{Pr}\left(\mathcal{G}\left(x_i, \frac{\varepsilon}{5m}\right) = y\right) \\&= \sum_{y \in \text{Ext}_R(x_i, w_i)} \mathbf{Pr}\left(\mathcal{G}\left(x_i, \frac{\varepsilon}{5m}\right) = y\right)\end{aligned}$$

Acotando $\mathbf{E}[X_{w_i}]$

Como $\mathcal{G}$ es un FPAUG para R , tenemos que:

$$\left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)} \leq \mathbf{Pr}\left(\mathcal{G}\left(x_i, \frac{\varepsilon}{5m}\right) = y\right) \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)}$$

Acotando $\mathbf{E}[X_{w_i}]$

Como $\mathcal{G}$ es un FPAUG para R , tenemos que:

$$\left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)} \leq \Pr\left(\mathcal{G}\left(x_i, \frac{\varepsilon}{5m}\right) = y\right) \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)}$$

Por lo tanto:

$$\sum_{y \in \text{Ext}_R(x_i, w_i)} \left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)} \leq \mathbf{E}[X_{w_i}] \leq \sum_{y \in \text{Ext}_R(x_i, w_i)} \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)}$$

Acotando $\mathbf{E}[X_{w_i}]$

Como $\mathcal{G}$ es un FPAUG para R , tenemos que:

$$\left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)} \leq \Pr\left(\mathcal{G}\left(x_i, \frac{\varepsilon}{5m}\right) = y\right) \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)}$$

Por lo tanto:

$$\sum_{y \in \text{Ext}_R(x_i, w_i)} \left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)} \leq \mathbf{E}[X_{w_i}] \leq \sum_{y \in \text{Ext}_R(x_i, w_i)} \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{1}{N_R(x_i)}$$

De lo cual concluimos que:

$$\left(1 - \frac{\varepsilon}{5m}\right) \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)}$$

Acotando $\mathbf{E}[X_{w_i}]$

Dado que:

$$\begin{aligned} \left(1 + \frac{\varepsilon}{5m}\right) &\leq \left(1 + \frac{\varepsilon}{4m}\right) \\ \frac{1}{1 + \frac{\varepsilon}{4m}} &\leq \left(1 - \frac{\varepsilon}{5m}\right) \end{aligned}$$

Concluimos que:

$$\frac{1}{1 + \frac{\varepsilon}{4m}} \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{4m}\right) \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)}$$

Otra desigualdad útil

Para $\varepsilon \in (0, 1)$, se tiene que:

$$1 + \frac{\varepsilon}{2m} \geq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \left(1 + \frac{\varepsilon}{4m}\right)$$

Otra desigualdad útil

Para $\varepsilon \in (0, 1)$, se tiene que:

$$1 + \frac{\varepsilon}{2m} \geq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \left(1 + \frac{\varepsilon}{4m}\right)$$

Puesto que $\varepsilon \in (0, 1)$ y:

$$\begin{aligned} 1 + \frac{\varepsilon}{2m} \geq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \left(1 + \frac{\varepsilon}{4m}\right) &\Leftrightarrow 1 + \frac{\varepsilon}{2m} \geq 1 + \frac{\varepsilon}{4m} + \frac{\varepsilon}{5m} + \frac{\varepsilon^2}{20m} \\ &\Leftrightarrow \frac{\varepsilon}{2m} \geq \frac{\varepsilon}{4m} + \frac{\varepsilon}{5m} + \frac{\varepsilon^2}{20m} \\ &\Leftrightarrow 10\varepsilon \geq 5\varepsilon + 4\varepsilon + \varepsilon^2 \\ &\Leftrightarrow \varepsilon \geq \varepsilon^2 \\ &\Leftrightarrow 1 \geq \varepsilon \end{aligned}$$

Acotando inferiormente $\Pr\left(\frac{\alpha_i}{(1+\frac{\varepsilon}{2m})} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq (1 + \frac{\varepsilon}{2m}) \cdot \alpha_i\right)$

Usando las desigualdades anteriores, tenemos que:

$$\begin{aligned} \frac{1}{(1 + \frac{\varepsilon}{5m})} \cdot \alpha_i \leq \mathbf{E}[X_{w_i}] &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{5m})} \cdot \alpha_i \leq \left(1 + \frac{\varepsilon}{4m}\right) \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \\ &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{5m}) \cdot (1 + \frac{\varepsilon}{4m})} \cdot \alpha_i \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \\ &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{2m})} \cdot \alpha_i \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \end{aligned}$$

Acotando inferiormente $\Pr\left(\frac{\alpha_i}{(1+\frac{\varepsilon}{2m})} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq (1 + \frac{\varepsilon}{2m}) \cdot \alpha_i\right)$

Usando las desigualdades anteriores, tenemos que:

$$\begin{aligned} \frac{1}{(1 + \frac{\varepsilon}{5m})} \cdot \alpha_i \leq \mathbf{E}[X_{w_i}] &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{5m})} \cdot \alpha_i \leq \left(1 + \frac{\varepsilon}{4m}\right) \cdot \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \\ &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{5m}) \cdot (1 + \frac{\varepsilon}{4m})} \cdot \alpha_i \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \\ &\Rightarrow \frac{1}{(1 + \frac{\varepsilon}{2m})} \cdot \alpha_i \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \end{aligned}$$

De la misma forma obtenemos:

$$\mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \alpha_i \Rightarrow \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i$$

Acotando inferiormente $\Pr\left(\frac{\alpha_i}{(1+\frac{\varepsilon}{2m})} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i\right)$

Juntando todo lo anterior, finalmente concluimos que:

$$\Pr\left(\frac{\alpha_i}{(1 + \frac{\varepsilon}{2m})} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i\right) \geq$$
$$\Pr\left(\frac{\alpha_i}{(1 + \frac{\varepsilon}{5m})} \leq \mathbf{E}[X_{w_i}] \leq \left(1 + \frac{\varepsilon}{5m}\right) \cdot \alpha_i\right) \geq 1 - \frac{1}{5m}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$: el paso final

Recuerde que nuestro objetivo es demostrar que:

$$\Pr(\text{propiedad de aproximación}) \geq \frac{3}{4}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$: el paso final

Recuerde que nuestro objetivo es demostrar que:

$$\Pr(\text{propiedad de aproximación}) \geq \frac{3}{4}$$

Tenemos que:

$$\Pr(\text{propiedad de aproximación}) =$$

$$\begin{aligned} & \Pr\left(\bigwedge_{i=1}^s \left[\frac{\alpha_i}{\left(1 + \frac{\varepsilon}{2m}\right)} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i \right]\right) = \\ & \prod_{i=1}^s \Pr\left(\frac{\alpha_i}{\left(1 + \frac{\varepsilon}{2m}\right)} \leq \frac{|\text{Ext}_R(x_i, w_i)|}{N_R(x_i)} \leq \left(1 + \frac{\varepsilon}{2m}\right) \cdot \alpha_i\right) \geq \\ & \prod_{i=1}^s \left(1 - \frac{1}{5m}\right) = \left(1 - \frac{1}{5m}\right)^s \geq \left(1 - \frac{1}{5m}\right)^m \end{aligned}$$

Acotando inferiormente $\Pr(\text{propiedad de aproximación})$: el paso final

Dado que $m \geq 1$, tenemos que $\left(1 - \frac{1}{5m}\right)^m \geq \frac{4}{5} > \frac{3}{4}$

Concluimos finalmente que:

$$\Pr(\text{propiedad de aproximación}) \geq \left(1 - \frac{1}{5m}\right)^m \geq \frac{3}{4}$$

Esto termina la demostración del teorema. □