El método Markov chain Monte Carlo

IIC3810

Marcelo Arenas y Luis Alberto Croquevielle

La noción de p-relación

Será conveniente ver las funciones de #P como relaciones.

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ es una p-relación si:

- *Existe un polinomio q tal que si $(x, y) \in R$, entonces $|y| \leq q(|x|)$*
- *$R \in PTIME$, vale decir, existe un algoritmo de tiempo polinomial que, dado $(x, y) \in \Sigma^* \times \Sigma^*$, verifica si $(x, y) \in R$*

Cada p-relación representa una función en #P

Dada una relación $R \subseteq \Sigma^* \times \Sigma^*$, defina la función $f_R : \Sigma^* \to \mathbb{N}$ como:

$$f_R(x) = \begin{cases} |\{y \mid (x,y) \in R\}| & \text{si } \{y \mid (x,y) \in R\} \text{ es finito} \\ 0 & \text{en otro caso} \end{cases}$$

Cada p-relación representa una función en #P

Dada una relación $R \subseteq \Sigma^* \times \Sigma^*$, defina la función $f_R : \Sigma^* \to \mathbb{N}$ como:

$$f_R(x) = \begin{cases} |\{y \mid (x,y) \in R\}| & \text{si } \{y \mid (x,y) \in R\} \text{ es finito} \\ 0 & \text{en otro caso} \end{cases}$$

Proposición

Si R es una p-relación, entonces $f_R \in \#P$

Cada p-relación representa una función en #P

Dada una relación $R \subseteq \Sigma^* \times \Sigma^*$, defina la función $f_R : \Sigma^* \to \mathbb{N}$ como:

$$f_R(x) = \begin{cases} |\{y \mid (x,y) \in R\}| & \text{si } \{y \mid (x,y) \in R\} \text{ es finito} \\ 0 & \text{en otro caso} \end{cases}$$

Proposición

Si R es una p-relación, entonces $f_R \in \#P$

Ejercicio

Demuestre la proposición.

Cada función en #P puede ser representada como una p-relación

Sea $f : \Sigma^* \to \mathbb{N}$ una función en #P

- Existe una MT no determinista M tal que para todo $x \in \Sigma^*$ se tiene que $f(x) = \text{accept}_M(x)$

Cada función en #P puede ser representada como una p-relación

Sea $f : \Sigma^* \to \mathbb{N}$ una función en #P

- Existe una MT no determinista M tal que para todo $x \in \Sigma^*$ se tiene que $f(x) = \text{accept}_M(x)$

Cada ejecución de M se puede codificar usando el alfabeto Σ

Cada función en #P puede ser representada como una p-relación

Sea $f : \Sigma^* \to \mathbb{N}$ una función en #P

- Existe una MT no determinista M tal que para todo $x \in \Sigma^*$ se tiene que $f(x) = \text{accept}_M(x)$

Cada ejecución de M se puede codificar usando el alfabeto Σ

Utilizando las codificaciones de las ejecuciones de M definimos:

$$R_f = \{(x, y) \in \Sigma^* \times \Sigma^* \mid y \text{ codifica una ejecución de } M \text{ con entrada } x \text{ que termina en un estado final}\}$$

Cada función en #P puede ser representada como una p-relación

Proposición

Si f está en $\#P$, entonces R_f es una p-relación

Cada función en #P puede ser representada como una p-relación

Proposición

Si f está en $\#P$, entonces R_f es una p-relación

Demostración: Como la MT no determinista M en la transparencia anterior es de tiempo polinomial, para una entrada x se puede:

- Codificar cualquier ejecución de M que acepta usando un string de largo polinomial en $|x|$
- Verificar si una ejecución termina en estado final (simulando el funcionamiento de M) en tiempo polinomial

Funciones en #P y p-relaciones

Por lo tanto, de ahora en adelante trabajamos con p-relaciones.

Estudiaremos los problemas de conteo y de generación uniforme asociados a p-relaciones, sabiendo que los resultados se extienden de manera natural a funciones en #P

Un generador uniforme para una p-relación

Dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$, sea:

$$N_R(x) \quad = \quad |\{y \in \Sigma^* \mid (x, y) \in R\}|$$

Además, suponga que $\perp$ es un símbolo reservado que no es usado en Σ

Un generador uniforme para una p-relación

Dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$, sea:

$$N_R(x) \quad = \quad |\{y \in \Sigma^* \mid (x, y) \in R\}|$$

Además, suponga que $\perp$ es un símbolo reservado que no es usado en Σ

Un algoritmo aleatorizado $\mathcal{G} : \Sigma^* \to \Sigma^* \cup \{\perp\}$ es un generador uniforme para R si para todo $x, y \in \Sigma^*$:

- si $(x, y) \notin R$, entonces $\mathbf{Pr}(\mathcal{G}(x) = y) = 0$
- si $(x, y) \in R$, entonces $\mathbf{Pr}(\mathcal{G}(x) = y) = \frac{1}{N_R(x)}$

Un generador casi uniforme para una p-relación

Las herramientas que veremos más adelante no nos permitirán obtener generadores uniformes, sino que una versión más débil

- Consideramos nuevamente una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Un generador casi uniforme para una p-relación

Las herramientas que veremos más adelante no nos permitirán obtener generadores uniformes, sino que una versión más débil

- Consideramos nuevamente una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Un algoritmo aleatorizado $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R si para todo $x, y \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$:

Un generador casi uniforme para una p-relación

Las herramientas que veremos más adelante no nos permitirán obtener generadores uniformes, sino que una versión más débil

- Consideramos nuevamente una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Un algoritmo aleatorizado $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R si para todo $x, y \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$:

- si $(x, y) \notin R$, entonces $\mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) = 0$

Un generador casi uniforme para una p-relación

Las herramientas que veremos más adelante no nos permitirán obtener generadores uniformes, sino que una versión más débil

- Consideramos nuevamente una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Un algoritmo aleatorizado $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R si para todo $x, y \in \Sigma^*$ y $\varepsilon \in \mathbb{R}^+$:

- si $(x, y) \notin R$, entonces $\mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) = 0$
- si $(x, y) \in R$, entonces:

$$\frac{1}{(1+\varepsilon) \cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) \leq (1+\varepsilon) \cdot \frac{1}{N_R(x)}$$

Una definición alternativa de generador casi uniforme

Vamos a considerar una definición alternativa de generador casi uniforme para una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Una definición alternativa de generador casi uniforme

Vamos a considerar una definición alternativa de generador casi uniforme para una p-relación $R \subseteq \Sigma^* \times \Sigma^*$

Un algoritmo aleatorizado $\mathcal{H} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R si para todo $x, y \in \Sigma^*$ y $\delta \in \mathbb{R}^+$:

- si $(x, y) \notin R$, entonces $\mathbf{Pr}(\mathcal{H}(x, \delta) = y) = 0$
- si $(x, y) \in R$, entonces:

$$(1 - \delta) \cdot \frac{1}{N_R(x)} \leq \mathbf{Pr}(\mathcal{H}(x, \delta) = y) \leq (1 + \delta) \cdot \frac{1}{N_R(x)}$$

Las definiciones son equivalentes

Vamos a demostrar que las definiciones dadas en las dos transparencias anteriores son equivalentes.

De manera precisa, dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$, vamos a demostrar que:

Si hay un generador casi uniforme para R bajo la primera definición, entonces hay un generador casi uniforme para R bajo la segunda definición, y viceversa

La primera definición implica la segunda

Suponga que $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la primera definición.

- Y sea $(x, y) \in R$

Para todo $\varepsilon \in \mathbb{R}^+$ tenemos que:

$$\frac{1}{(1+\varepsilon) \cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) \leq (1+\varepsilon) \cdot \frac{1}{N_R(x)} \qquad (\dagger)$$

La primera definición implica la segunda

Suponga que $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la primera definición.

- Y sea $(x, y) \in R$

Para todo $\varepsilon \in \mathbb{R}^+$ tenemos que:

$$\frac{1}{(1+\varepsilon) \cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) \leq (1+\varepsilon) \cdot \frac{1}{N_R(x)} \qquad (\dagger)$$

En este caso consideramos $\mathcal{H} = \mathcal{G}$

La primera definición implica la segunda

Suponga que $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la primera definición.

- Y sea $(x, y) \in R$

Para todo $\varepsilon \in \mathbb{R}^+$ tenemos que:

$$\frac{1}{(1+\varepsilon) \cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x, \varepsilon) = y) \leq (1+\varepsilon) \cdot \frac{1}{N_R(x)} \qquad (\dagger)$$

En este caso consideramos $\mathcal{H} = \mathcal{G}$

Dado $\delta > 0$, tenemos que demostrar que:

$$(1-\delta) \cdot \frac{1}{N_R(x)} \leq \mathbf{Pr}(\mathcal{H}(x, \delta) = y) \leq (1+\delta) \cdot \frac{1}{N_R(x)}$$

La primera definición implica la segunda

Pero tenemos que:

$$
\begin{aligned}
\delta > 0 \quad &\Rightarrow \quad \delta^2 > 0 \\
&\Rightarrow \quad -\delta^2 < 0 \\
&\Rightarrow \quad 1 - \delta^2 < 1 \\
&\Rightarrow \quad (1-\delta) \cdot (1+\delta) < 1 \\
&\Rightarrow \quad (1-\delta) < \frac{1}{(1+\delta)}
\end{aligned}
$$

La primera definición implica la segunda

Pero tenemos que:

$$\begin{aligned}
\delta > 0 &\Rightarrow \delta^2 > 0 \\
&\Rightarrow -\delta^2 < 0 \\
&\Rightarrow 1 - \delta^2 < 1 \\
&\Rightarrow (1-\delta)\cdot(1+\delta) < 1 \\
&\Rightarrow (1-\delta) < \frac{1}{(1+\delta)}
\end{aligned}$$

Por lo tanto considerando $\varepsilon = \delta$ en $(\dagger)$ y el hecho que $\mathcal{H}(x,\delta) = \mathcal{G}(x,\delta) = \mathcal{G}(x,\varepsilon)$ obtenemos:

$$(1-\delta)\cdot\frac{1}{N_R(x)} < \frac{1}{(1+\varepsilon)\cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{H}(x,\delta) = y) \leq (1+\varepsilon)\cdot\frac{1}{N_R(x)} = (1+\delta)\cdot\frac{1}{N_R(x)}$$

La segunda definición implica la primera

Suponga que $\mathcal{H} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la segunda definición.

- Y sea $(x, y) \in R$

Para todo $\delta \in \mathbb{R}^+$ tenemos que:

$$(1-\delta) \cdot \frac{1}{N_R(x)} \;\leq\; \mathbf{Pr}(\mathcal{H}(x,\delta) = y) \;\leq\; (1+\delta) \cdot \frac{1}{N_R(x)} \qquad (\ddagger)$$

La segunda definición implica la primera

Suponga que $\mathcal{H} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la segunda definición.

- Y sea $(x, y) \in R$

Para todo $\delta \in \mathbb{R}^+$ tenemos que:

$$(1-\delta) \cdot \frac{1}{N_R(x)} \;\leq\; \mathbf{Pr}(\mathcal{H}(x,\delta) = y) \;\leq\; (1+\delta) \cdot \frac{1}{N_R(x)} \qquad (\ddagger)$$

En este caso consideramos $\mathcal{G}$ definido como $\mathcal{G}(x, \varepsilon) = \mathcal{H}\left(x, \frac{\varepsilon}{(1+\varepsilon)}\right)$

La segunda definición implica la primera

Suponga que $\mathcal{H} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ es un generador casi uniforme para R según la segunda definición.

- Y sea $(x, y) \in R$

Para todo $\delta \in \mathbb{R}^+$ tenemos que:

$$(1-\delta) \cdot \frac{1}{N_R(x)} \leq \mathbf{Pr}(\mathcal{H}(x,\delta) = y) \leq (1+\delta) \cdot \frac{1}{N_R(x)} \qquad (\ddagger)$$

En este caso consideramos $\mathcal{G}$ definido como $\mathcal{G}(x,\varepsilon) = \mathcal{H}\left(x, \frac{\varepsilon}{(1+\varepsilon)}\right)$

Dado $\varepsilon > 0$, tenemos que demostrar que:

$$\frac{1}{(1+\varepsilon) \cdot N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x,\varepsilon) = y) \leq (1+\varepsilon) \cdot \frac{1}{N_R(x)}$$

La primera definición implica la segunda

Tenemos que:

$$
\begin{aligned}
\delta = \frac{\varepsilon}{(1+\varepsilon)} \quad &\Rightarrow \quad \delta + \delta \cdot \varepsilon = \varepsilon \\
&\Rightarrow \quad 0 = \varepsilon - \delta - \delta \cdot \varepsilon \\
&\Rightarrow \quad 1 = 1 + \varepsilon - \delta - \delta \cdot \varepsilon \\
&\Rightarrow \quad 1 = (1-\delta) \cdot (1+\varepsilon) \\
&\Rightarrow \quad \frac{1}{(1+\varepsilon)} = (1-\delta)
\end{aligned}
$$

La primera definición implica la segunda

Tenemos que:

$$\begin{aligned}
\delta = \frac{\varepsilon}{(1+\varepsilon)} \quad &\Rightarrow \quad \delta + \delta \cdot \varepsilon = \varepsilon \\
&\Rightarrow \quad 0 = \varepsilon - \delta - \delta \cdot \varepsilon \\
&\Rightarrow \quad 1 = 1 + \varepsilon - \delta - \delta \cdot \varepsilon \\
&\Rightarrow \quad 1 = (1-\delta) \cdot (1+\varepsilon) \\
&\Rightarrow \quad \frac{1}{(1+\varepsilon)} = (1-\delta)
\end{aligned}$$

Por lo tanto considerando $\delta = \frac{\varepsilon}{(1+\varepsilon)}$ en $(\ddagger)$ y los hechos que $\frac{\varepsilon}{(1+\varepsilon)} \leq \varepsilon$ y $\mathcal{G}(x,\varepsilon) = \mathcal{H}(x, \frac{\varepsilon}{(1+\varepsilon)}) = \mathcal{H}(x,\delta)$ obtenemos:

$$\frac{1}{(1+\varepsilon)\cdot N_R(x)} = (1-\delta)\cdot\frac{1}{N_R(x)} \leq \mathbf{Pr}(\mathcal{G}(x,\varepsilon)=y) \leq (1+\delta)\cdot\frac{1}{N_R(x)} \leq (1+\varepsilon)\cdot\frac{1}{N_R(x)}$$

Un esquema de generación casi uniforme

Desde ahora en adelante consideramos la primera definición de generador casi uniforme.

Un esquema de generación casi uniforme

Desde ahora en adelante consideramos la primera definición de generador casi uniforme.

Definición

Dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$, *un algoritmo aleatorizado* $\mathcal{G} : \Sigma^* \times \mathbb{R}^+ \to \Sigma^* \cup \{\perp\}$ *es un* **fully polynomial almost uniform generator (FPAUG)** *para* R *si*

1. $\mathcal{G}$ *es un generador casi uniforme para* R
2. *Existe un polinomio* $q(u, v)$ *tal que para todo* $x \in \Sigma^*$ *y* $\varepsilon \in \mathbb{R}^+$, *el número de pasos ejecutados por* $\mathcal{G}(x, \varepsilon)$ *es menor o igual a* $q(|x|, \log(\frac{1}{\varepsilon}))$

Una definición alternativa de FPRAS

Definición

Dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$*, un algoritmo aleatorizado* $\mathcal{A} : \Sigma^* \times \mathbb{R}^+ \to \mathbb{N}$ *es un* **fully polynomial randomized approximation scheme (FPRAS)** *para* R *si existe un polinomio* $q(u, v)$ *tal que para cada* $x \in \Sigma^*$ *y* $\varepsilon \in \mathbb{R}^+$*:*

1. *El número de pasos ejecutados por* $\mathcal{A}(x, \varepsilon)$ *es menor o igual a* $q(|x|, \frac{1}{\varepsilon})$
2. $\mathbf{Pr}\left(\frac{N_R(x)}{(1+\varepsilon)} \leq \mathcal{A}(x, \varepsilon) \leq (1+\varepsilon) \cdot N_R(x) \right) \geq \frac{3}{4}$

Una definición alternativa de FPRAS

Definición

Dada una p-relación $R \subseteq \Sigma^* \times \Sigma^*$*, un algoritmo aleatorizado* $\mathcal{A} : \Sigma^* \times \mathbb{R}^+ \to \mathbb{N}$ *es un* **fully polynomial randomized approximation scheme (FPRAS)** *para* R *si existe un polinomio* $q(u, v)$ *tal que para cada* $x \in \Sigma^*$ *y* $\varepsilon \in \mathbb{R}^+$*:*

1. *El número de pasos ejecutados por* $\mathcal{A}(x, \varepsilon)$ *es menor o igual a* $q(|x|, \frac{1}{\varepsilon})$
2. $\mathbf{Pr}\left(\frac{N_R(x)}{(1+\varepsilon)} \leq \mathcal{A}(x, \varepsilon) \leq (1+\varepsilon) \cdot N_R(x) \right) \geq \frac{3}{4}$

Observación

Dada una función f en #P representada como R_f, se puede demostrar que esta definición de FPRAS es equivalente a la vista en el capítulo anterior utilizando las mismas ideas usadas en la demostración que las definiciones de generador casi uniforme son equivalentes.

Un comentario sobre las definiciones anteriores

La noción de algoritmo aleatorizado se formaliza usando MT probabilísticas.

- Estas máquinas funcionan con cintas de bits, por lo que las probabilidades resultantes son de la forma $\frac{n}{2^k}$

Un comentario sobre las definiciones anteriores

La noción de algoritmo aleatorizado se formaliza usando MT probabilísticas.

- Estas máquinas funcionan con cintas de bits, por lo que las probabilidades resultantes son de la forma $\frac{n}{2^k}$

Por lo tanto, al describir un algoritmo aleatorizado, en teoría no podemos decir algo como "la probabilidad de error del algoritmo es $\frac{1}{3}$"

Algunos comentarios sobre las definiciones anteriores

Tratar de tener algoritmos aleatorizados con probabilidades arbitrarias no entrega intuiciones nuevas

- Y hace mucho más técnicas y complicadas las demostraciones

Algunos comentarios sobre las definiciones anteriores

Tratar de tener algoritmos aleatorizados con probabilidades arbitrarias no entrega intuiciones nuevas

- Y hace mucho más técnicas y complicadas las demostraciones

Supuesto

Todas las probabilidades que vamos a considerar (por ejemplo, la probabilidad $\frac{1}{N_R(x)}$) son de la forma $\frac{n}{2^k}$

La relación entre FPAUG y FPRAS

Pasaremos ahora a enunciar y demostrar que la existencia de un FPAUG implica la existencia de un FPRAS.

- Este resultado es válido para una amplia clase de relaciones
- Esto nos va a permitir utilizar una gran cantidad de herramientas desarrolladas para el muestreo de variables aleatorias en la construcción de FPRAS

La relación entre FPAUG y FPRAS

Pasaremos ahora a enunciar y demostrar que la existencia de un FPAUG implica la existencia de un FPRAS.

- Este resultado es válido para una amplia clase de relaciones
- Esto nos va a permitir utilizar una gran cantidad de herramientas desarrolladas para el muestreo de variables aleatorias en la construcción de FPRAS

Primero debemos formalizar la noción de p-relación auto-reducible, la cual es necesaria al demostrar la relación entre FPAUG y FPRAS.

Relaciones auto-reducibles

Intuitivamente, un problema se dice auto-reducible si es que se puede solucionar mediante la resolución de instancias más simples del mismo problema.

Relaciones auto-reducibles

Intuitivamente, un problema se dice auto-reducible si es que se puede solucionar mediante la resolución de instancias más simples del mismo problema.

Ejemplo

Sea φ una fórmula proposicional con variables $x_1, \ldots, x_n$

Utilizamos la notación $\varphi[\frac{x_i}{v}]$ para indicar que la variable x_i es reemplazada por $v \in \{0, 1\}$

- Reemplazar por 0 y 1 equivale a reemplazar por una contradicción y una tautología, respectivamente

El problema de determinar si φ es satisfacible se reduce al problema de determinar si $\varphi[\frac{x_1}{0}]$ o $\varphi[\frac{x_1}{1}]$ es satisfacible

- Así, una instancia de SAT se reduce a instancias más simples de SAT

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$
2. *Existen funciones* $\psi : \Sigma^* \times \Sigma^* \to \Sigma^*$ *y* $\sigma : \Sigma^* \to \mathbb{N}$ *tales que:*

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$
2. *Existen funciones* $\psi : \Sigma^* \times \Sigma^* \to \Sigma^*$ *y* $\sigma : \Sigma^* \to \mathbb{N}$ *tales que:*
   - $\sigma(x) \in O(\log(|x|))$

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$
2. *Existen funciones* $\psi : \Sigma^* \times \Sigma^* \to \Sigma^*$ *y* $\sigma : \Sigma^* \to \mathbb{N}$ *tales que:*
   - $\sigma(x) \in O(\log(|x|))$
   - $\forall x \in \Sigma^*$*: si* $g(x) > 0$*, entonces* $\sigma(x) > 0$

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$
2. *Existen funciones* $\psi : \Sigma^* \times \Sigma^* \to \Sigma^*$ *y* $\sigma : \Sigma^* \to \mathbb{N}$ *tales que:*
   - $\sigma(x) \in O(\log(|x|))$
   - $\forall x \in \Sigma^*$*: si* $g(x) > 0$*, entonces* $\sigma(x) > 0$
   - $\forall x, w \in \Sigma^*$*:* $|\psi(x, w)| \leq |x|$

Relaciones auto-reducibles: formalización

Definición

Una relación $R \subseteq \Sigma^* \times \Sigma^*$ *es auto-reducible si:*

1. *Existe función* $g : \Sigma^* \to \mathbb{N}$ *tal que* $g \in FP$ *y para cada* $(x, y) \in R$ *se tiene que* $|y| = g(x)$
2. *Existen funciones* $\psi : \Sigma^* \times \Sigma^* \to \Sigma^*$ *y* $\sigma : \Sigma^* \to \mathbb{N}$ *tales que:*
   - $\sigma(x) \in O(\log(|x|))$
   - $\forall x \in \Sigma^*$*: si* $g(x) > 0$*, entonces* $\sigma(x) > 0$
   - $\forall x, w \in \Sigma^*$*:* $|\psi(x, w)| \leq |x|$
   - $\forall x, y \in \Sigma^*$ *con* $y = a_1 \cdots a_n$*:*

     $(x, y) \in R$ *si y sólo si* $(\psi(x, a_1 \cdots a_{\sigma(x)}), a_{\sigma(x)+1} \cdots a_n) \in R$

Relaciones auto-reducibles: ejemplos

Ejercicios

Demuestre que las siguientes relaciones son auto-reducibles:

1. $R_{\mathsf{SAT}} = \{(\varphi, \sigma) \mid \varphi$ es una fórmula proposicional y σ es una valuación tal que $\sigma(\varphi) = 1\}$

2. $R_{\mathsf{IS}} = \{(G, S) \mid G$ es un grafo y S es un conjunto independiente de $G\}$

Una relación natural no auto-reducible

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un conjunto independiente maximal de G si:

1. S es un conjunto independiente de G
2. Para todo conjunto independiente S' de G, no se cumple que $S \subsetneq S'$

Una relación natural no auto-reducible

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un conjunto independiente maximal de G si:

1. S es un conjunto independiente de G
2. Para todo conjunto independiente S' de G, no se cumple que $S \subsetneq S'$

Considere la relación:

$R_{\text{MIS}} = \{(G, S) \mid G \text{ es un grafo y } S \text{ es un conjunto independiente maximal de } G\}$

Una relación natural no auto-reducible

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un conjunto independiente maximal de G si:

1. S es un conjunto independiente de G
2. Para todo conjunto independiente S' de G, no se cumple que $S \subsetneq S'$

Considere la relación:

$R_{\text{MIS}} = \{(G, S) \mid G \text{ es un grafo y } S \text{ es un conjunto independiente maximal de } G\}$

¿Es R_{MIS} auto-reducible?

Una relación natural no auto-reducible

Dado un grafo $G = (N, A)$, decimos que $S \subseteq N$ es un conjunto independiente maximal de G si:

1. S es un conjunto independiente de G
2. Para todo conjunto independiente S' de G, no se cumple que $S \subsetneq S'$

Considere la relación:

$R_{\text{MIS}} = \{(G, S) \mid G \text{ es un grafo y } S \text{ es un conjunto independiente maximal de } G\}$

¿Es R_{MIS} auto-reducible?

- ¿Cómo se puede demostrar que no lo es?

Una propiedad de las relaciones auto-reducibles

Para demostrar que R_{MIS} no es auto-reducible identificamos una propiedad de las relaciones auto-reducibles que no es cumplida por R_{MIS}

- Bajo una suposición de complejidad

Una propiedad de las relaciones auto-reducibles

Para demostrar que R_{MIS} no es auto-reducible identificamos una propiedad de las relaciones auto-reducibles que no es cumplida por R_{MIS}

- Bajo una suposición de complejidad

Dado un alfabeto Σ, suponga dado un orden lineal en Σ

- Este orden lineal induce un orden lexicográfico $\leq$ en Σ^*

Una propiedad de las relaciones auto-reducibles

Para demostrar que R_{MIS} no es auto-reducible identificamos una propiedad de las relaciones auto-reducibles que no es cumplida por R_{MIS}

- Bajo una suposición de complejidad

Dado un alfabeto Σ, suponga dado un orden lineal en Σ

- Este orden lineal induce un orden lexicográfico $\leq$ en Σ^*

Definición

Dada una relación $R \subseteq \Sigma^* \times \Sigma^*$*:*

$$
\begin{aligned}
\mathit{Exists}(R) &= \{x \mid \exists y : (x, y) \in R\} \\
\mathit{Min}(R) &= \{(x, y) \mid x \in \mathit{Exists}(R) \wedge y = \arg\min_{\leq} \{z \mid (x, z) \in R\}\} \\
\mathit{Max}(R) &= \{(x, y) \mid x \in \mathit{Exists}(R) \wedge y = \arg\max_{\leq} \{z \mid (x, z) \in R\}\}
\end{aligned}
$$

Una propiedad de las relaciones auto-reducible

Teorema

Si R es una p-relación auto-reducible tal que $Exists(R) \in PTIME$, entonces $Min(R) \in PTIME$ y $Max(R) \in PTIME$

Una propiedad de las relaciones auto-reducible

Teorema

Si R es una p-relación auto-reducible tal que $Exists(R) \in PTIME$, entonces $Min(R) \in PTIME$ y $Max(R) \in PTIME$

Ejercicio

Demuestre el teorema

R_{MIS} no es auto-reducible

Proposición

Si R_{MIS} es auto-reducible, entonces PTIME = NP

R_{MIS} no es auto-reducible

Proposición

Si R_{MIS} es auto-reducible, entonces PTIME = NP

Ejercicio

Demuestre las siguientes propiedades:

1. R_{MIS} es una p-relación y Exists(R_{MIS}) $\in$ PTIME
2. Min(R_{MIS}) es co-NP-completo

R_{MIS} no es auto-reducible

Proposición

Si R_{MIS} es auto-reducible, entonces PTIME = NP

Ejercicio

Demuestre las siguientes propiedades:

1. R_{MIS} es una p-relación y Exists(R_{MIS}) $\in$ PTIME
2. Min(R_{MIS}) es co-NP-completo

A partir de estas propiedades y del teorema demuestre la proposición.