Motivación: la complejidad de algunos problemas

IIC3810

El problema de factorización de números naturales

Factorizar un número natural n consiste en encontrar un divisor de n

- Este divisor debe ser no trivial, vale decir, mayor que 1 y menor que n

Es importante considerar que el problema de verificar si un número es primo se puede resolver en tiempo polinomial.

- Al factorizar un número n primero verificamos si es primo. Si n es primo indicamos que no hay divisores no triviales, en caso contrario debemos entregar uno de estos divisores

El problema de factorización de números enteros

Como problema de decisión el problema de factorización mostrado en la transparencia anterior es modelado de la siguiente forma:

$$\text{FACT} = \{(n,k) \mid n \text{ y } k \text{ son números naturales y existe } \ell \text{ tal que } 1 < \ell \leq k \text{ y } \ell \text{ divide a } n\}$$

El problema de factorización de números enteros

Como problema de decisión el problema de factorización mostrado en la transparencia anterior es modelado de la siguiente forma:

$$\text{FACT} = \{(n,k) \mid n \text{ y } k \text{ son números naturales y existe } \ell \text{ tal que } 1 < \ell \leq k \text{ y } \ell \text{ divide a } n\}$$

¿Por qué FACT se considera equivalente al problema de factorización?

El problema de factorización de números enteros

Como problema de decisión el problema de factorización mostrado en la transparencia anterior es modelado de la siguiente forma:

$$\text{FACT} = \{(n,k) \mid n \text{ y } k \text{ son números naturales y existe } \ell \text{ tal que } 1 < \ell \leq k \text{ y } \ell \text{ divide a } n\}$$

¿Por qué FACT se considera equivalente al problema de factorización?

- ¿Es cierto que si uno puede resolver FACT en tiempo polinomial también puede resolver el problema de factorización en tiempo polinomial? ¿Es cierta la dirección opuesta?

La complejidad exacta de FACT

Ejercicio

Demuestre que FACT está en NP.

La complejidad exacta de FACT

Ejercicio

Demuestre que FACT está en NP.

Ejercicio

Demuestre que FACT está en co-NP.

La complejidad exacta de FACT

Ejercicio

Demuestre que FACT está en NP.

Ejercicio

Demuestre que FACT está en co-NP.

¿Puede ser FACT un problema NP-completo?

- ¿Qué consecuencias tendría esto?

El problema de isomorfismo de grafos

Dados: grafos $G_1 = (N_1, A_1)$ y $G_2 = (N_2, A_2)$

Una función $f : N_1 \to N_2$ es un isomorfismo de G_1 en G_2 si

1. f es una biyección
2. Para cada par $(a, b) \in N_1 \times N_1$, se tiene que $(a, b) \in A_1$ si y sólo si $(f(a), f(b)) \in A_2$

El problema de isomorfismo de grafos

El problema de isomorfismo de grafos se define de la siguiente forma:

$$\text{GRAPH-ISO} = \{(G_1, G_2) \mid G_1 \text{ y } G_2 \text{ son grafos y existe un isomorfismo de } G_1 \text{ en } G_2\}$$

La complejidad exacta de GRAPH-ISO

Ejercicio

Demuestre que GRAPH-ISO está en NP.

La complejidad exacta de GRAPH-ISO

Ejercicio

Demuestre que GRAPH-ISO está en NP.

¿Qué más sabemos sobre la complejidad de este problema?

La complejidad exacta de GRAPH-ISO

Ejercicio

Demuestre que GRAPH-ISO está en NP.

¿Qué más sabemos sobre la complejidad de este problema?

- ¿Es GRAPH-ISO un problema NP-completo?
- ¿Está GRAPH-ISO en co-NP?

¿Por qué son importantes estos problemas?

- FACT:
- GRAPH-ISO:

¿Por qué son importantes estos problemas?

- FACT: Es unos de los problemas en los que se basa la criptografía moderna.

- GRAPH-ISO:

¿Por qué son importantes estos problemas?

- FACT: Es unos de los problemas en los que se basa la criptografía moderna.

- GRAPH-ISO: Es el problema que está detrás de la idea de tener una representación canónica de un grafo.

¿Por qué son importantes estos problemas?

- FACT: Es unos de los problemas en los que se basa la criptografía moderna.
- GRAPH-ISO: Es el problema que está detrás de la idea de tener una representación canónica de un grafo.
  - Y además de tener una representación canónica de estructuras generales.

¿Y qué tienen en común estos problemas?

¿Y qué tienen en común estos problemas?

El estudio de su complejidad no está basado en técnicas usuales.

¿Y qué tienen en común estos problemas?

El estudio de su complejidad no está basado en técnicas usuales.

- Por ejemplo, no se puede concluir que son difíciles porque son NP-completos.

¿Y qué tienen en común estos problemas?

El estudio de su complejidad no está basado en técnicas usuales.

- Por ejemplo, no se puede concluir que son difíciles porque son NP-completos.

Se necesita entonces desarrollar otro tipo de herramientas para estudiar su complejidad.

¿Y qué tienen en común estos problemas?

El estudio de su complejidad no está basado en técnicas usuales.

- Por ejemplo, no se puede concluir que son difíciles porque son NP-completos.

Se necesita entonces desarrollar otro tipo de herramientas para estudiar su complejidad.

- Algunas de estas herramientas las veremos en este curso.