

Pruebas de Conocimiento Cero y sus Aplicaciones

José Luis Cánovas Sánchez

Tutores:

Antonio José Pallarés Ruiz

Leandro Marín Muñoz

13 de julio de 2017

Universidad de Murcia

Facultad de Matemáticas

Decision Problems

Residuos Cuadráticos

Pruebas Interactivas

Pruebas de Conocimiento Cero

Aplicaciones

Decision Problems

Decision Problem

Definition (Decision Problem)

General description of a task which depend on some parameters and which possible answers are in the set $\{True, False\}$.

Name *A characteristic name.*

Parameters *Arguments the problem depends on.*

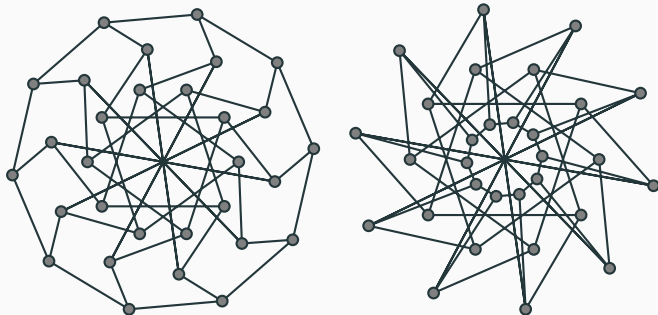
Question *Question such the possible answers are True or False.*

Graph Isomorphism

Name Graph Isomorphism Problem (GI).

Parameters Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ with $|V_1| = |V_2| = n$.

Question Is there a permutation $\tau : V_1 \rightarrow V_2$ such that an edge $(u, v) \in E_1$ if and only if $(\tau(u), \tau(v)) \in E_2$?



Complexity classes

Definition (Class P)

The set of decision problems which can be solved in polynomial time.

Definition (Class NP)

The set of decision problems where a *True* answer can be verified in polynomial time, given some extra information (certificate).

Fact

$$P \subset NP$$

Millennium Problem

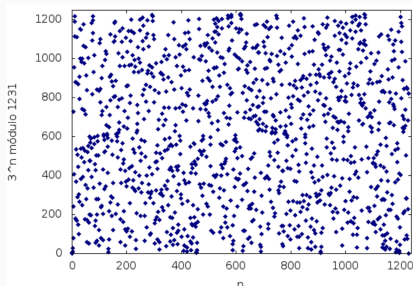
$$P \stackrel{?}{=} NP$$

Discrete Logarithm

Name Discrete Logarithm problem (DL).

Parameters A cyclic group $G = \langle g \rangle$ of prime order q , an element $y \in G$.

Question Does P know $s \in \mathbb{Z}_q$ such that $g^s = y$, or $\log_g y = s$?



Discrete Logarithm with

$G = \mathbb{Z}_{1231}$, $g = 3$.

Adolfo Quirós Gracián. *Grupos y criptografía: de Julio César a las curvas elípticas*.

Definition (Polynomial-time reduction $L_1 \leq_P L_2$)

Be L_1 and L_2 two decision problems. L_1 can be reduced in polynomial time to L_2 if L_1 can be solved using L_2 as a subroutine plus a polynomial time.

Definition (Class NP-complete or NPC)

A decision problems L is in **NPC** if:

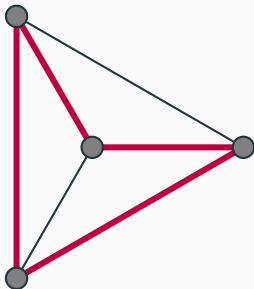
1. $L \in \mathbf{NP}$, and
2. $L_1 \leq_P L \quad \forall L_1 \in \mathbf{NP}$.

Hamiltonian Cycle ^{NPC}

Name Hamiltonian Cycle Problem (HC).

Parameters Given graph $G = (V, E)$.

Question Does there exist a Hamiltonian cycle in G ?

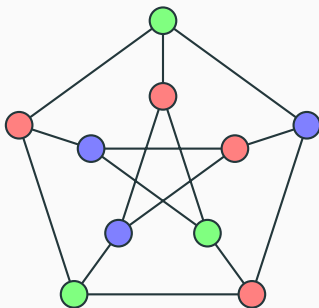


Graph 3-colorability ^{NPC}

Name Graph 3-colorability Problem (G3C).

Parameters Given graph $G = (V, E)$.

Question Is there a function $\phi : V \rightarrow \{1, 2, 3\}$ such that
 $\phi(u) \neq \phi(v) \quad \forall (u, v) \in E$?



Quadratic residue

Name Factorization problem (FACT).

Parameters Positive integer N .

Question Are there integers $p, q \geq 2$ such that $N = pq$?

Name Quadratic residue problem (QR).

Parameters Given a composite integer $N = pq$ and the integer x with Jacobi Symbol $\left(\frac{x}{N}\right) = 1$.

Question Is x a quadratic residue in \mathbb{Z}_N ? $\exists a \in \mathbb{Z}_N : x \equiv a^2(N)$?

Theorem

$QR \leq_P FACT$

Residuos Cuadráticos

Definición

Sea $x \in \mathbb{Z}_n^*$. Se dice que x es un *residuo cuadrático* módulo n , o un *cuadrado* módulo n , si existe un $a \in \mathbb{Z}_n^*$ tal que

$$x \equiv a^2 \pmod{n}.$$

Si no existe dicho a , entonces x se llama un *no-residuo cuadrático* módulo n .

Al conjunto de los residuos cuadráticos módulo n los denotaremos como Q_n . Al de los no-residuos cuadráticos, como $\overline{Q_n}$.

Ejemplo

Si tomamos $n = 4$, los no-residuos cuadráticos son 2 y 3, y el único residuo cuadrático es 1:

$$1^2 \equiv 1 \pmod{4} \quad 2^2 \equiv 0 \pmod{4} \quad 3^2 \equiv 1 \pmod{4}$$

Por definición $0 \notin \mathbb{Z}_n^*$, y por tanto $0 \notin Q_n$ ni $0 \notin \overline{Q_n}$.

Residuos Cuadráticos: Propiedades

- Sea $p > 1$ un número primo, entonces $|Q_p| = |\overline{Q_p}| = \frac{p-1}{2}$.
- Sean n, m coprimos. $x \in \mathbb{Z}_{mn}$ es un residuo cuadrático si y sólo si $x \bmod m$ y $x \bmod n$ son residuos cuadráticos en \mathbb{Z}_m y \mathbb{Z}_n respectivamente.
- Si a y b son raíces cuadradas de $x \bmod m$ y $x \bmod n$ en sus correspondientes anillos, podemos combinarlas mediante el **Teorema Chino de los Restos** para obtener una raíz cuadrada de x en \mathbb{Z}_{mn} .
- Sea $n = pq$ el producto de dos primos distintos, entonces el número de residuos cuadráticos módulo n es $\frac{(p-1)(q-1)}{4}$.

Definición (Símbolo de Legendre)

Dados un primo impar p y un entero a , se define el *Símbolo de Legendre* como

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } a \equiv 0 \pmod{p} \\ 1, & \text{si } a \in Q_p \\ -1, & \text{si } a \in \overline{Q_p} \end{cases}$$

Definición (Símbolo de Jacobi)

Sea n un entero impar positivo cuya descomposición en factores primos es $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ y sea a un entero. Entonces definimos el *símbolo de Jacobi* de a y n como

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_t}\right)^{e_t}$$

- El Símbolo de **Legendre** nos indica si un entero es residuo cuadrático módulo un **primo** mayor que 2.
- Podemos calcular una **raíz** cuadrada módulo un primo en tiempo polinomial con el **Algoritmo de Tonelli**.
- El Símbolo de **Jacobi** se puede calcular en tiempo polinomial **sin** conocer la **factorización** del módulo.
- Un Símbolo de **Jacobi** -1 nos indica *no-residuo*, pero un 1 ya no indica necesariamente *residuo cuadrático*.
- Conociendo la **factorización** del módulo, podemos calcular la **raíz** modular en tiempo **polinomial** con el **Teorema Chino de los Restos** y el **Algoritmo de Tonelli**.

Nombre Problema de los residuos cuadráticos (QR).

Parámetros N un entero impar tal que $N = pq$ para p y q primos, y el entero x tal que $\left(\frac{x}{N}\right) = 1$.

Pregunta ¿Es x un residuo cuadrático en \mathbb{Z}_N^* ?

Pruebas Interactivas

Probador (P) computacionalmente *todopoderosa*.

Verificador (V) cómputo limitado, probabilístico de tiempo de polinomial.

$$P \stackrel{*}{\rightleftharpoons} V$$

Objetivo: P quiere probar *algo* a V, p. ej., que una instancia de un problema es *Verdadera*.

Definición (Sistema de Prueba Interactiva)

Un problema de decisión Q tiene un *sistema de prueba interactiva* si tiene un protocolo de interacción polinomialmente acotado en número de mensajes que cumple:

- *Complejidad* Para toda instancia q Verdadera, del problema Q , V acepta q como Verdadera.
- *Robustez* Para cada instancia q Falsa, V rechaza la prueba de q con una probabilidad no menor que $\epsilon = 1 - n^{-c}$, para cualquier constante $c > 0$ y donde n es el tamaño de la instancia.

Ejemplo Pruebas Interactivas: Problema QR

Teorema

El problema QR tiene un sistema de prueba interactivo.

Nombre Problema de los residuos cuadráticos (QR).

Parámetros N un entero impar tal que $N = pq$ para p y q primos, y el entero x tal que $\left(\frac{x}{N}\right) = 1$.

Pregunta ¿Es x un residuo cuadrático en \mathbb{Z}_N^* ?

Ejemplo Pruebas Interactivas: Problema QR

Prueba interactiva para QR (x, N)

Sea $t(n)$ un polinomio en n , el tamaño de la instancia (x, N) . P y V repiten $t(n)$ veces los siguientes pasos.

1. $P \rightarrow V$: $u \in_R \mathbb{Z}_N^{Q+}$, un residuo cuadrático en \mathbb{Z}_N .
2. $V \rightarrow P$: $b \in_R \{0, 1\}$.
3. $P \rightarrow V$: w , una raíz cuadrada aleatoria de $u \cdot x^b$.
4. V comprueba si:

$$w^2 \stackrel{?}{\equiv} \begin{cases} u \bmod N, & \text{si } b = 0 \\ xu \bmod N, & \text{si } b = 1. \end{cases}$$

Si la comparación falla, V termina en rechazo. En caso contrario, vuelve al paso 1.

Ejemplo Pruebas Interactivas: Problema QR

Demostración.

La prueba es **completa**:

Instancia (x, N) *Verdadera* $\Rightarrow x$ es residuo cuadrático, existe raíz.

P computacionalmente todopoderoso \Rightarrow puede calcular w raíz de x o xu , residuos cuadráticos.

V acepta la prueba de P .



Ejemplo Pruebas Interactivas: Problema QR

Demostración.

La prueba es **robusta**:

Instancia *Falsa*, x no residuo cuadrático. P^* intenta adivinar el reto $b \in_R \{0, 1\}$.

- Si $b = 0$, sigue el protocolo, elige $u \in_R \mathbb{Z}_N^{Q+}$.
- Si $b = 1$, elige $u \equiv x^{-1}a^2 \pmod N$, con $a \in_R \mathbb{Z}_N$. Responde con $w = a$. V comprobará $w^2 \equiv a^2 \stackrel{?}{=} x \cdot x^{-1}a^2 \equiv a^2 \pmod N$.

Si P^* falla al adivinar, o no existirá raíz de xu , o $w^2 \not\equiv u \pmod N$.

Probabilidad de acertar el reto b : $\frac{1}{2}$.

Probabilidad de pasar la prueba: $2^{-t(n)}$.



Pruebas de Conocimiento Cero

Definición (Propiedad de conocimiento cero)

Un sistema de prueba interactiva (completo y robusto), para un problema de decisión Q , es de *conocimiento cero* si el ensamble $Vista_{P,V}(q, h)$ es idéntico al ensamble generado por un Simulador $S_{V^*}(q, h)$, para cualquier instancia Verdadera $q \in Q$ y cualquier historial h .

Pruebas de Conocimiento Cero

Definición (Ensamble)

Llamamos ensamble probabilístico (*ensemble* en inglés) a una familia de variables aleatorias $\{X_i\}_{i \in I}$, con I numerable.

$$\text{Vista}_{P, V^*}(q, h) = (q, h, A_1, B_1, C_1, \dots, A_{t(n)}, B_{t(n)}, C_{t(n)}).$$

Definición (Simulador)

Un Simulador $S_{V^*}(q, h)$ es un algoritmo probabilístico de tiempo polinomial, que utiliza toda la información que V^* tiene disponible, para generar una transcripción de una prueba interactiva, para una instancia q del problema Q , sin necesidad de interactuar con P .

Si V no sigue el protocolo, elegirá los retos en base a un algoritmo $F(\cdot)$ en base a toda la información disponible.

Pruebas de Conocimiento Cero: Problema QR

Teorema

La prueba interactiva del problema QR es de conocimiento cero.

Demostración

Variables aleatorias

U_i El residuo cuadrático aleatorio enviado por P en el primer mensaje, $u \in_R \mathbb{Z}_N^{Q+}$.

B_i El reto aleatorio generado por V, $b \in_R \{0, 1\}$.

W_i La *prueba* de P, $w \in_R \Omega_u$ o bien $w \in_R \Omega_{xu}$.

$$\text{Vista}_{P,V^*}(x, N, h) = (x, N, h, U_1, B_1, W_1, \dots, U_{t(n)}, B_{t(n)}, W_{t(n)})$$

Probabilidad en la Vista

$$P(U_i = u, B_i = b, W_i = w) =$$

$$P(U_i = u) \cdot P(B_i = b \mid V_{i-1} = v, U_i = u, h) \cdot P(W_i = w \mid U_i = u, B_i = b)$$

Sea $\alpha = |\mathbb{Z}_N^{Q+}|$, entonces $P(U_i = u) = \frac{1}{\alpha}$.

Denotamos $P(B_i = b \mid U_i = u) = p_b$, dependerá de F .

Por último, sea $\beta = |\Omega_u| = |\Omega_{xu}|$. u fijo por construcción.

Entonces:

$$P(W_i = w \mid U_i = u, B_i = 0) = 1/\beta, \quad \forall w \in \Omega_u$$

$$P(W_i = w \mid U_i = u, B_i = 1) = 1/\beta, \quad \forall w \in \Omega_{xu}$$

En total nos queda, $P(U_i = u, B_i = b, W_i = w) = \frac{p_b}{\alpha\beta}$.

Simulador Instancia (x, N) *Verdadera* del problema QR.

Ejecución: Generadas las primeras i rondas. Repetir para $i + 1 \leq t(n)$:

1. Elegir $b_{i+1} \in_R \{0, 1\}$
2. Elegir $w_{i+1} \in_R \mathbb{Z}_N^*$
3. **Si** $b_{i+1} = 0$, **entonces** calcular $u_{i+1} \equiv w_{i+1}^2 \bmod N$
Si no, $u_{i+1} \equiv w_{i+1}^2 \cdot x^{-1} \bmod N$
4. **Si** $b_{i+1} = F(x, N, h, v_i, u_{i+1})$, **entonces** añadir la tupla $(u_{i+1}, b_{i+1}, w_{i+1})$ a la transcripción. **Si no,** volver al paso 1.
5. $i = i + 1$

Probabilidad del Simulador

$$P(U_i = u, B_i = b, W_i = w) = \\ P(W_i = w) \cdot P(B_i = b \mid U_i = u) \cdot P(U_i = u \mid W_i = w, B_i = b)$$

Sabemos que $|\mathbb{Z}_N^*| = \alpha \cdot \beta$, por lo que $P(W_i = w) = \frac{1}{\alpha\beta}$.

$$\begin{aligned} P(U_i = u) &= \sum_{w \in \Omega_u} P(U_i = u, W_i = w, B_i = 0) + \sum_{w \in \Omega_{xu}} P(U_i = u, W_i = w, B_i = 1) = \\ &= \sum_{w \in \Omega_u} P(W_i = w)P(B_i = 0) + \sum_{w \in \Omega_{xu}} P(W_i = w)P(B_i = 1) = \\ &= \beta \cdot \frac{1}{\alpha\beta} \cdot (P(B_i = 0) + P(B_i = 1)) = \frac{1}{\alpha} \end{aligned}$$

$\Rightarrow U_i$ misma distribución que U_i de la *Vista* \Rightarrow

$$P(B_i = b = F(\cdot) \mid U_i = u) = p_b.$$

$P(U_i = u \mid W_i = w, B_i = b) = 1$ por construcción de u .

$$P(U_i = u, B_i = b, W_i = w) = \frac{p_b}{\alpha\beta}.$$

↑ **Perfectas** Igualdad de los ensambles.

Estadísticas Igualdad asintótica de los ensambles.

Verificador Honesto Igualdad, suponiendo que V sigue el protocolo.

Computacionales Indistinguibilidad computacional de los ensambles. Los **esquemas de compromiso** son una herramienta fundamental.

Aplicaciones

Heurística de Fiat-Shamir: Firma digital

Problema: Sincronizar a P y V.

Sustituir reto de V por un valor difícil de predecir: función hash.

→ **Firma digital**

P calcula : el *testigo* u ,
 el *reto* $h = \text{hash}(u|m)$,
 y la *respuesta* $w = \xi(u, h)$.

$P \rightarrow V$: **firma del mensaje** m : (h, w)

V verifica : $h = \text{hash}(\vartheta(h, w) | m)$.

Protocolos de identificación: Fiat-Shamir

Configuración de la identidad:

1. La entidad de confianza selecciona y publica $N = pq$, con p y q primos y secretos.
2. Cada usuario P genera un secreto $s \in \mathbb{Z}_N^*$, coprimo con N (si no, se podría obtener la factorización de N y perder la seguridad del protocolo). Calcula $v \equiv s^2 \bmod N$ y lo envía a la entidad de confianza como su clave pública.

Protocolo: Repetir t rondas:

1. P escoge aleatoriamente $r \in_R \mathbb{Z}_N^*$, el *compromiso*.
2. $P \rightarrow V$: $u \equiv r^2 \bmod N$, el *testigo*.
3. $V \rightarrow P$: $b \in_R \{0, 1\}$, el *reto*.
4. $P \rightarrow V$: $w \equiv r \cdot s^b \bmod N$, la *respuesta*.
5. V verifica si $w^2 \equiv u \cdot v^b \bmod N$.

- **Firma distribuida de la credencial:** las pruebas de conocimiento cero aseguran que se sigue el algoritmo.
- **Muestra selectiva de atributos:** prueba de conocimiento cero sobre la posesión de una firma válida, sin revelarla.

Pruebas de Conocimiento Cero y sus Aplicaciones

José Luis Cánovas Sánchez

Tutores:

Antonio José Pallarés Ruiz

Leandro Marín Muñoz

13 de julio de 2017

Universidad de Murcia

Facultad de Matemáticas

Residuos Cuadráticos: Símbolo de Jacobi

Propiedades del Símbolo de Jacobi.

Sean $a, b \in \mathbb{Z}$ y sean m, n enteros positivos impares:

1. Si $a \equiv b \pmod{n}$ entonces $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
2. $\left(\frac{a^2}{n}\right) = 1$.
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$.
4. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
5. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.
6. $\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4} \left(\frac{n}{m}\right)$ *Ley de Reciprocidad Cuadrática.*

Residuos Cuadráticos: Símbolo de Jacobi

Podemos calcular el Símbolo de Jacobi $\left(\frac{a}{b}\right)$ en tiempo polinomial **sin conocer la factorización de b** :

1. En caso de que a sea mayor que b , reducirlo módulo b ,
 $a := a \bmod b$.
2. Si a es 0, devolver 0.
3. Si a es 1, devolver 1.
4. Dividir a por 2 para ponerlo en la forma $a = 2^e a'$ con a' impar. Si e es par o $b \equiv \pm 1 \bmod 8$ poner $s := 1$, en caso contrario poner $s := -1$.
5. Finalmente si $a' \equiv 3 \bmod 4$ y $b \equiv 3 \bmod 4$ devolver $-s \text{Jacobi}(b, a')$ y en caso contrario devolver $s \text{Jacobi}(b, a')$.

Definición

Denominamos clase de problemas **IP** (Interactivos en tiempo Polinomial) al conjunto de problemas de decisión para los que existe un sistema de prueba interactivo.

Pruebas Interactivas

Teorema

$\text{NP} \subset \text{IP}$.

Demostración.

Sea Q un problema **NP**. Definimos el siguiente protocolo:

1. P resuelve la instancia del problema gracias a su capacidad de cómputo ilimitada y genera el certificado para V .
2. V recibe y verifica el certificado en tiempo polinomial. Si es válido, V acepta como *Verdadera* la instancia. Si no, rechaza la prueba.

