Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC1253 — Matemáticas Discretas — 1' 2016

TAREA 4

Publicación: Viernes 22 de Abril.
Entrega: **Viernes 29 de Abril hasta las 10:15 horas**.

Indicaciones

- Debe entregar una solución para cada pregunta (sin importar si esta en blanco).
- Cada solución debe estar escrita en LaTeX. No se aceptarán tareas escritas a mano ni en otro sistema de composición de texto.
- Responda cada pregunta en una hoja separada y ponga su nombre en cada hoja de respuesta.
- Si usa más de una hoja para una misma pregunta corchetelas.
- Junte las respuestas a preguntas distintas usando un clip (no un corchete).
- Debe entregar una copia escrita durante la ayudantía asignada y una copia digital por el buzón del curso, ambas antes de la fecha/hora de entrega.
- **Se penalizará con 1 punto en la nota final de la tarea por cada regla que no se cumpla.**
- La tarea es individual.

Pregunta 1

Sea A un conjunto finito. Una relación $R \subseteq A \times A$ se dice que es un *rectangulo* si existen conjuntos $B, C \subseteq A$ tal que $R = B \times C$.

1. Demuestre que R es un rectangulo si, y solo si, para todo $a_1, b_1, a_2, b_2 \in A$ se cumple que:

$$\text{si } (a_1, b_1) \in R \text{ y } (a_2, b_2) \in R, \text{ entonces } (a_1, b_2) \in R.$$

2. Un rectangulo R se dice *simple* si $R = B \times B$ para algún $B \subseteq A$. Demuestre que si R es una relación de equivalencia, entonces para algún $n \in \mathbb{N}$ existen rectangulos simples $R_1, \ldots, R_n \subseteq A \times A$ tal que:

$$R = \bigcup_{i=1}^{n} R_i$$

¿es la otra dirección cierta? Demuestrelo o de un contra-ejemplo.

Pregunta 2

Para esta pregunta fije un $n \in \mathbb{N}$. Para el alfabeto de bits $\{0,1\}$ se define $\{0,1\}^n$ como el conjunto de todas las palabras de bits de largo n y $\{0,1\}^+$ como el conjunto de todas las palabras de bits de largo mayor o igual a 1. El largo de una palabra $u \in \{0,1\}^+$ la denotaremos como $|u|$. Para una letra $a \in \{0,1\}$ denotaremos como a^i la palabra que tiene la letra a repetida i-veces, o sea, $a^i = \underbrace{aa\ldots a}_{i\text{-veces}}$.

Considere una función $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Se dice que un par de funciones (g_L, g_B) con:

$$g_L : \{0,1\}^n \to \{0,1\}^+ \quad \text{y} \quad g_B : \{0,1\}^+ \times \{0,1\}^n \to \{0,1\}$$

es un *protocolo* para f si se cumple que $f(u,v) = g_B(g_L(u), v)$ para todo $u, v \in \{0,1\}^n$. Denotaremos por $\mathcal{P}(f)$ el conjunto de todos los protocolos para f.

La interpretación de g_L y g_B es la siguiente. Suponga que Lisa y Bart desean calcular la función $f(u,v)$ pero Lisa tiene la palabra u y Bart tiene la palabra v (obviamente Lisa no conoce la palabra v ni Bart la palabra u). Para calcular $f(u,v)$, Lisa convierte su palabra u en $u' = g_L(u)$ (u' puede tener cualquier largo mayor o igual a 1) y le envía u' a Bart, el cual puede calcular la función $f(u,v)$ calculando $g_B(u', v)$.

Un posible protocolo para cualquier función f es considerar las funciones $g_L(u) = u$ y $g_B(u,v) = f(u,v)$. En este caso, Lisa le esta "enviando" toda la palabra u a Bart. La pregunta interesante es pensar cuando Lisa puede enviarle menos de n bits a Bart para calcular la función f en el peor caso. Por ejemplo, considere la función $f^{\mathbf{ones}}$ tal que $f^{\mathbf{ones}}(u,v) = 1$ si $u = v = 1^n$ y $f^{\mathbf{ones}}(u,v) = 0$ en otro caso (en otras palabras, $f^{\mathbf{ones}}(u,v) = 1$ si ambas palabras contienen solo 1's al mismo tiempo). En este caso, un posible protocolo para que Lisa y Bart calculen la función $f^{\mathbf{ones}}$ son las funciones $(g_L^{\mathbf{ones}}, g_B^{\mathbf{ones}})$ tal que:

- $g_L^{\mathbf{ones}}(u) = 1$ si $u = 1^n$ y $g_L^{\mathbf{ones}}(u) = 0$ en otro caso.
- $g_B^{\mathbf{ones}}(u,v) = 1$ si $u = 1, v = 1^n$ y $g_B^{\mathbf{ones}}(u,v) = 0$ en otro caso.

Notese que en este caso Lisa solo le tiene que enviar un solo bit a Bart (en el peor caso) para calcular la función $f^{\mathbf{ones}}$ en vez de enviarle toda su palabra.

La discusión anterior motiva la definición de *complejidad* $\mathcal{C}(f)$ de una función f como:

$$\mathcal{C}(f) \;:=\; \min_{(g_L, g_B) \in \mathcal{P}(f)} \left\{ \max_{u \in \{0,1\}^n} |g_L(u)| \right\}$$

En otras palabras, la complejidad $\mathcal{C}(f)$ es la máxima cantidad de bits que necesita enviar Lisa a Bart en el mejor protocolo para f. Note que la complejidad $\mathcal{C}(f)$ siempre satisface que $1 \leq \mathcal{C}(f) \leq n$. Por ejemplo, en el caso de $f^{\mathbf{ones}}$ tenemos que $\mathcal{C}(f^{\mathbf{ones}}) = 1$.

1. Para una palabra $w \in \{0,1\}^n$, suponga que $w = a_1 \ldots a_n$ con $a_i \in \{0,1\}$ para todo $i \leq n$. Definimos $w^{\downarrow}$ como la menor posición $i \leq n$ tal que $a_i = 1$ y $a_j = 0$ para todo $j < i$. Por ejemplo, $(0001010)^{\downarrow} = 4$ ya que el cuarto bit de la palabra 0001010 es el primer bit igual a 1. Si $w = 0^n$, entonces definimos $w^{\downarrow} = n + 1$.

   Considere la función $f^{\downarrow} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ tal que:

   $$f^{\downarrow}(u,v) = 1 \quad \text{si, y solo si,} \quad u^{\downarrow} \leq v^{\downarrow}$$

   Demuestre que $\mathcal{C}(f^{\downarrow}) \leq \log_2(n+1) + 1$. (Hint: recuerda la codificación de números binarios)

2. Considere la función $f^{=} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ tal que:

   $$f^{=}(u,v) = 1 \quad \text{si, y solo si,} \quad u = v$$

   Demuestre que $\mathcal{C}(f^{=}) \geq n$. En otras palabras, el mejor protocolo para la función $f^{=}$ es que Lisa le envíe toda su palabra a Bart.

Evaluación y puntajes de la tarea

Cada **item** de cada pregunta se evaluará con un puntaje de:

- 0 (respuesta incorrecta),
- 3 (con errores menores),
- 4 (correcta).

Todas las preguntas tienen la misma ponderación en la nota final.