Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Examen

9 de diciembre de 2020
Profesores: Gabriel Diéguez - Fernando Suárez

Instrucciones

- La duración del examen es de 3 horas.
- Se podrán realizar preguntas solamente durante los módulos del examen, de 8:30 a 11:30 hrs., por el foro de Canvas correspondiente.
- Debe entregar una solución escrita a mano, ya sea en papel o tablet, antes de las 23:59 horas del día del examen. En el caso de hacerlo en papel, debe preocuparse que la copia digital sea legible. Se recomienda el uso de algún software de escaneo como CamScanner o la app de Google Drive.
- Responda cada pregunta en archivo separados: `numalumno-P1.pdf`, `numalumno-P2.pdf`, `numalumno-P3.pdf` y `numalumno-P4.pdf`
- Ponga su nombre y sección en cada archivo.
- En caso de hacer el examen fuera del horario, se recomienda tomar el tiempo (3 horas) y entregarlo justo después de concluido el tiempo.
- Durante la evaluación puede hacer uso de sus apuntes o slides del curso.
- Esta es una evaluación estrictamente individual y, por lo tanto, no puede compartir información con sus compañeros o usar material fuera de sus apuntes o slides del curso. En caso de hacerlo, el examen no reflejará su progreso en el curso, viéndose perjudicada su formación personal y profesional.
- **Al comienzo de cada pregunta debe escribir la siguiente oración y firmarla:** *"Doy mi palabra que la siguiente solución de la pregunta X fue desarrollada y escrita individualmente por mi persona según el código de honor de la Universidad."*

  En caso de no escribir la oración o no firmarla, su solución no será evaluada.
- Entregue al menos una hoja por pregunta.
  - Si entrega la pregunta **completamente en blanco**, tiene nota mínima 1.5 en vez de 1.0 en la pregunta entregada.

Pregunta 1 [Inducción y Lógica de predicados]

a) Demuestre que $\sum_{i=0}^{n} 2F_{3i+3} = F_{3n+5} - 1$, donde F_n corresponde al n-ésimo término de la sucesión de Fibonacci.

b) Sea $S(\cdot,\cdot), P(\cdot,\cdot)$ predicados binarios. Considere el siguiente conjunto de fórmulas en lógica de predicados:

$$\Sigma = \{\forall x \exists y (S(x,y)), \forall x \forall y (S(x,y) \rightarrow P(y,x))\}$$

y la fórmula $\varphi = \forall x \exists y (P(y,x))$.

Demuestre usando resolución que $\Sigma \models \varphi$.

Solución

a) Demostraremos la propiedad utilizando el principio de inducción simple.

BI: Si $n = 0$ tenemos que

$$\begin{aligned}
\sum_{i=0}^{n} 2F_{3i+3} &= 2F_{3\cdot 0+3} \\
&= 2F_3 \\
&= 2(F_2 + F_1) \\
&= 2(F_1 + F_0 + F_1) \\
&= 2(1 + 0 + 1) \\
&= 4 \\
&= 5 - 1 \\
&= F_5 - 1 \\
&= F_{3n+5} - 1
\end{aligned}$$

HI: Suponemos que $\sum_{i=0}^{n} 2F_{3i+3} = F_{3n+5} - 1$ para algún $n \in \mathbb{N}$.

TI: Mostraremos que $\sum_{i=0}^{n+1} 2F_{3i+3} = F_{3(n+1)+5} - 1$

$$\begin{aligned}
\sum_{i=0}^{n+1} 2F_{3i+3} &= \sum_{i=0}^{n} 2F_{3i+3} + 2F_{3n+6} \\
&\overset{\textbf{HI}}{=} (F_{3n+5} - 1) + 2F_{3n+6} \\
&= (F_{3n+6} + (F_{3n+5} + F_{3n+6})) - 1 \\
&= (F_{3n+6} + F_{3n+7}) - 1 \\
&= F_{3n+8} - 1 \\
&= F_{3(n+1)+5} - 1
\end{aligned}$$

Por principio de inducción simple, concluímos que la propiedad de cumple para todo natural n.

b) En primer lugar debemos convertir Σ a cláusulas:

$$\begin{aligned}
\Sigma &= \{\forall x \exists y (S(x,y)), \forall x \forall y (S(x,y) \to P(y,x))\} \\
&\equiv \{\forall x \exists y (S(x,y)), \forall x \forall y (\neg S(x,y) \lor P(y,x))\}
\end{aligned}$$

Luego, definimos Σ' como $\Sigma \cup \{\neg\varphi\}$:

$$\begin{aligned}
\Sigma' &= \{\forall x \exists y (S(x,y)), \forall x \forall y (\neg S(x,y) \lor P(y,x)), \neg \forall x \exists y (P(y,x))\} \\
&\equiv \{\forall x \exists y (S(x,y)), \forall x \forall y (\neg S(x,y) \lor P(y,x)), \exists x \forall y (\neg P(y,x))\}
\end{aligned}$$

Y ahora aplicamos resolución:

(1)	$\exists x \forall y (\neg P(y,x))$	$\in \Sigma'$
(2)	$\forall y (\neg P(y,a))$ para algún a	especificación existencial de (1)
(3)	$\forall x \exists y (S(x,y))$	$\in \Sigma'$
(4)	$\exists y (S(a,y))$	especificación universal de (3)
(5)	$S(a,b)$ para algún b	especificación existencial de (4)
(6)	$\neg P(b,a)$	especificación universal de (2)
(7)	$\forall x \forall y (\neg S(x,y) \lor P(y,x))$	$\in \Sigma'$
(8)	$\forall y (\neg S(a,y) \lor P(y,a))$	especificación universal de (7)
(9)	$\neg S(a,b) \lor P(b,a)$	especificación universal de (8)
(10)	$P(b,a)$	resolución de $(5), (9)$
(11)	$\square$	resolución de $(6), (10)$

Concluimos entonces que $\Sigma \cup \{\neg\varphi\} \vdash \square$, y por lo tanto $\Sigma \models \varphi$.

Pauta (6 pts.)

a)
- Base de inducción: 0,5 ptos
- Hipótesis de inducción: 0,5 ptos
- Tesis de inducción: 2 ptos

b)
- Plantear Σ': 1 pto
- Aplicar resolución correctamente: 2 ptos

Puntajes intermedios y soluciones alternativas a criterio del corrector.

Pregunta 2 [Relaciones y Funciones]

Sean A y B conjuntos y $(B, \preceq)$ un orden parcial. Considere el siguiente conjunto:

$$\phi(A, B) = \{f \mid f : A \to B\}$$

Además definimos la relación binaria $\preceq_\phi$ sobre $\phi(A, B)$ como:

$$f \preceq_\phi g \text{ si y solo si } f(a) \preceq g(a) \quad \forall a \in A$$

Demuestre que $(\phi(A, B), \preceq_\phi)$ es un orden parcial.

Solución

- <u>Refleja</u>:
  Como $\preceq$ es refleja, sabemos que:

$$f(a) \preceq f(a) \quad \forall a \in A \Rightarrow f \preceq_\phi f$$

- <u>Antisimétrica</u>:
  Suponemos que $f \preceq_\phi g$ y $g \preceq_\phi f$

$$\Rightarrow \forall a \in A(f(a) \preceq g(a)) \land \forall a \in A(g(a) \preceq f(a))$$
$$\Rightarrow \forall a \in A(f(a) \preceq g(a) \land g(a) \preceq f(a))$$

  Como $\preceq$ es antisimétrica:

$$\Rightarrow \forall a \in A(f(a) = g(a))$$
$$\Rightarrow f = g$$

- Transitiva:

  Suponemos que $f \preceq_\phi g$ y $g \preceq_\phi h$

$$\begin{aligned}\Rightarrow \forall a \in A(f(a) \preceq g(a)) \wedge \forall a \in A(g(a) \preceq h(a))\\ \Rightarrow \forall a \in A(f(a) \preceq g(a) \wedge g(a) \preceq h(a))\end{aligned}$$

  Como $\preceq$ es transitiva:

$$\begin{aligned}\Rightarrow \forall a \in A(f(a) \preceq h(a))\\ \Rightarrow f \preceq_\phi h\end{aligned}$$

Concluimos que $(\phi(A, B), \preceq_\phi)$ es un orden parcial.

Pauta (6 pts.)

- Refleja: 1 pto
- Antisimétrica: 2 ptos
- Transitiva: 3 ptos

Puntajes intermedios y soluciones alternativas a criterio del corrector.

Pregunta 3 [Teoría de números][1]

a) **(2 pts)** Encuentre el menor número tal que su resto al dividirlo por 5, 7, 9 y 11 es 1, 2, 3 y 4 respectivamente.

b) **(4 pts)** Demuestre que para cada número primo $p \geq 6$ se cumple que $p^2 - 1$ o $p^2 + 1$ es múltiplo de 10.

Solución

a) Debemos encontrar el menor x que cumpla con el siguiente sistema:

$$\begin{aligned}x &\equiv 1 \pmod 5\\ x &\equiv 2 \pmod 7\\ x &\equiv 3 \pmod 9\\ x &\equiv 4 \pmod{11}\end{aligned}$$

[1] Es válido encontrar algunos resultados, como inversos, por inspección (es decir, probando números), pero en tal caso debe explicitarlo y comprobarlo en su desarrollo.

Como los módulos son todos números primos, son coprimos entre sí, y entonces podemos aplicar el teorema chino del resto. Sean:

$$m = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$$
$$M_1 = \frac{m}{5} = 693, \quad M_2 = \frac{m}{7} = 495, \quad M_3 = \frac{m}{9} = 385, \quad M_4 = \frac{m}{11} = 315$$

Buscamos los inversos de los M_i por inspección:

- $M_1^{-1 \bmod 5} = 2$ pues $693 \cdot 2 = 1386$, y es claro que $1386 \bmod 5 = 1$.
- $M_2^{-1 \bmod 7} = 3$ pues $495 \cdot 3 = 1485$, y $7 \cdot 212 = 1484$, por lo que $1485 \bmod 7 = 1$.
- $M_3^{-1 \bmod 9} = 4$ pues $385 \cdot 4 = 1540$, y $9 \cdot 171 = 1539$, por lo que $1540 \bmod 9 = 1$.
- $M_4^{-1 \bmod 11} = 8$ pues $315 \cdot 8 = 2520$, y $11 \cdot 229 = 2519$, por lo que $2520 \bmod 11 = 1$.

Entonces, la solución será tal que

$$\begin{aligned} x &\equiv 1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 3 \cdot 315 \cdot 8 \pmod{3465} \\ &\equiv 19056 \pmod{3465} \end{aligned}$$

El número más pequeño que cumple con esto es $19056 \bmod 3465 = 1731$ (es fácil ver que $3465 \cdot 5 = 17325$ y que $19056 - 17325 = 1731$). Por lo tanto, la respuesta es 1731, y el teorema chino del resto garantiza que es el menor, dado que la solución es única hasta 3465.

Opcionalmente podemos comprobar que efectivamente satisface el sistema:

- Claramente $1731 \equiv 1 \pmod{5}$.
- $1731 \bmod 7 = 2$ pues $7 \cdot 247 = 1729$.
- $1731 \bmod 9 = 3$ pues $9 \cdot 192 = 1728$.
- $1731 \bmod 11 = 4$ pues $11 \cdot 157 = 1727$.

b) Como p es primo y $p \geq 6$, p es impar, y por lo tanto p^2 es también impar. Luego tenemos que $2|p^2 - 1$ y $2|p^2 + 1$.

También tenemos que $5 \not| p$, y entonces se debe cumplir que $p \equiv 1, 2, 3 \text{ o } 4 \pmod{5}$. Además tenemos que:

$$\begin{aligned} p \equiv 1 \pmod{5} &\Rightarrow p^2 \equiv 1^2 \pmod{5} \Rightarrow p^2 \equiv 1 \pmod{5} \\ p \equiv 2 \pmod{5} &\Rightarrow p^2 \equiv 2^2 \pmod{5} \Rightarrow p^2 \equiv -1 \pmod{5} \\ p \equiv 3 \pmod{5} &\Rightarrow p^2 \equiv 3^2 \pmod{5} \Rightarrow p^2 \equiv -1 \pmod{5} \\ p \equiv 4 \pmod{5} &\Rightarrow p^2 \equiv 4^2 \pmod{5} \Rightarrow p^2 \equiv 1 \pmod{5} \end{aligned}$$

Como tenemos que $p^2 \equiv 1 \pmod{5}$, se cumple que $5|p^2 - 1$ o $5|p^2 + 1$.

Concluimos que $10|p^2 - 1$ o $10|p^2 + 1$.

Pauta (6 pts.)

a)
- Plantear el sistema: 0,25 ptos
- Resolver el sistema: 1,5 ptos
- Encontrar y justificar el menor: 0,25 ptos
- **IMPORTANTE:** tal como dice en el título, esta es una pregunta de teoría de números, por lo que la respuesta debe contener el desarrollo necesario para llegar al resultado final. Se considerará incorrecto el solo plantear la respuesta y comprobar que cumple con las congruencias. Esto también se respondió durante los módulos del examen en el foro de Canvas.

b)
- Mostrar que ambos son divisibles por 2: 2 ptos
- Mostrar que al menos uno es divisible por 5: 2 ptos

Puntajes intermedios y soluciones alternativas a criterio del corrector.

Pregunta 4 [Complejidad, Grafos y Lógica proposicional]

Decimos que un grafo es COVID-k si es que tiene un clique y un conjunto independiente de tamaño k. Considere el siguiente problema:

$$\textsc{Covid-3} = \{G = (V, E) \mid G \text{ tiene un clique y un conjunto independiente de tamaño } 3\}$$

Demuestre que $\textsc{Covid-3} \propto \text{SAT}$[2].

Solución

Sea $G = (V, E)$ con $|V| = n$. Buscamos construir una fórmula $\varphi \in L(P)$ en tiempo polinomial tal que

$$G \text{ es COVID-3 si y sólo si } \varphi \text{ es satisfacible}$$

Definimos el siguiente conjunto P de variables proposicionales:

$$P = \{\ p_{ij} \mid \text{existe una arista entre } i \text{ y } j\ \}$$

Considere las siguientes fórmulas:

- **Fórmula 1**: Existe un clique de tamaño 3 en el grafo:

$$\varphi_1 = \bigvee_{\substack{(i,j,k)\in\{1,\ldots,n\}^3 \\ i\neq j\neq k}} p_{ij} \wedge p_{jk} \wedge p_{ki}$$

[2]SAT corresponde al problema de determinar si una fórmula en $L(P)$ es satisfacible.

- **Fórmula 2**: Existe un conjunto independiente de tamaño 3 en el grafo:

$$\varphi_2 = \bigvee_{\substack{(i,j,k)\in\{1,\ldots,n\}^3 \\ i\neq j\neq k}} \neg p_{ij} \wedge \neg p_{jk} \wedge \neg p_{ki}$$

- **Fórmula 3**: Toda arista del grafo está representada en el modelo:

$$\varphi_3 = \bigwedge_{(i,j)\in E} p_{ij}$$

- **Fórmula 4**: Toda arista que no está en el grafo tampoco debe estar en el modelo:

$$\varphi_4 = \bigwedge_{(i,j)\notin E} \neg p_{ij}$$

Finalmente, podemos considerar

$$\varphi = \varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4$$

Ahora mostraremos que

$$G \text{ es COVID-3 si y sólo si } \varphi \text{ es satisfacible}$$

($\Rightarrow$) Suponemos que G tiene un clique $k = \{1,2,3\}$ y un conjunto independiente $c = \{4,5,6\}$, ambos[3] de tamaño 3. Por un lado, consideremos una valuación $\sigma : P \to \{0,1\}$ tal que $\sigma(p_{12}) = \sigma(p_{23}) = \sigma(p_{31}) = 1$ y que $\sigma(p_{45}) = \sigma(p_{56}) = \sigma(p_{64}) = 0$. Por otro lado, por las reglas 3 y 4, φ debe ser tal que cumpla $(p_{12} \wedge p_{23} \wedge p_{31})$ y $(\neg p_{45} \wedge \neg p_{56} \wedge \neg p_{64})$, las cuales son satisfacibles por σ. Además, el hecho de que satisfaga estas expresiones, implica que debe satisfacer a φ_1 y φ_2 respectivamente. Concluimos que

$$\sigma(\varphi) = \sigma(\varphi_1 \wedge \varphi_2 \wedge \varphi_3 \wedge \varphi_4) = 1$$

y por ende φ es satisfacible.

($\Leftarrow$) Suponemos que φ es satisfacible, por lo tanto existe una valuación $\sigma : P \to \{0,1\}$ tal que $\sigma(\varphi) = 1$. Por lo tanto, σ debe ser tal que $\sigma(\varphi_1) = \sigma(\varphi_2) = 1$. Sin pérdida de generalidad, de lo anterior podemos asumir que $\sigma(p_{12}) = \sigma(p_{23}) = \sigma(p_{31}) = 1$ y que $\sigma(p_{45}) = \sigma(p_{56}) = \sigma(p_{64}) = 0$. Además, como $\sigma(\varphi_3) = \sigma(\varphi_4) = 1$, se tiene que $(1,2), (2,3), (3,4) \in E$ y $(4,5), (5,6), (6,4) \notin E$. Por lo tanto, en G tenemos un clique $k = \{1,2,3\}$ y un conjunto independiente $c = \{4,5,6\}$.

[3] Sin pérdida de generalidad podemos tomar estos vértices, con otros también funciona.

Pauta (6 pts.)

- 1 pto por definir P.
- 1 pto por φ_1.
- 1 pto por φ_2.
- 1 pto por φ_3 y φ_4.
- 1 pto por ($\Rightarrow$).
- 1 pto por ($\Leftarrow$).

Puntajes intermedios y soluciones alternativas a criterio del corrector.