Presentació

Teoria de la Computació

FIB

Antoni Lozano

Q1 2024–2025

Presentació

1. Qüestions pràctiques
2. Perspectiva
3. Prerequisits

Presentació

TC, grup 12

- Classes:
  - dj 10:00–12:00 (problemes), A5202
  - dv 8:00–10:00 (laboratori), A5S111
- Professor: Antoni Lozano
- C/E: antoni@cs.upc.edu
- Despatx: 233, edifici Ω

Informació del curs

- Pàgina web: `https://www.cs.upc.edu/~alvarez/tc2.html`
  Calendari de laboratoris, mètode docent, material (llibres i vídeos), llistes d'exercicis.
- RACSO: `https://racso.cs.upc.edu`
  Jutge del curs.
- Racó: avisos i lliurament d'exercicis.

Material docent

Llibres:

- Els de TC enllaçats en la pàgina (Cases-Màrquez i Serna *et al*)
- M. Sipser. *Introduction to the Theory of Computation* (3a edició, disponible en línia). Ens hi referirem com [S].

Vídeos:

- Els del curs enllaçats en la pàgina
- Els del curs de M. Sipser a **ocw.mit.edu** (2020)

Metodologia

- Teoria:
  - introduccions de cada tema a classe
    (de problemes o lab.)
  - autoaprenentatge
    (referències a l'inici dels fulls de problemes)
- Problemes: presentació d'exercicis a pissarra (els dijous)
- Laboratori: treball amb el jutge RACSO (els divendres)

Exàmens

- Parcial 1
  - Data: 6 de novembre de 2024
  - Temes 1–3
  - Metodologia: RACSO
- Parcial 2
  - Data: 9 de gener de 2025
  - Temes 4–7
  - Metodologia: RACSO i part escrita
- Final
  - Data: 16 de gener de 2025
  - Temes 1–7
  - Metodologia: examen escrit

Avaluació

P = nota de pissarra (entre 0 i 2)
L = nota de laboratori (entre 0 i 8), mitjana de 2 parcials
$C = P + L$ = nota de l'avaluació continuada
F = nota de l'examen final (entre 0 i 10)

Nota final de curs:

- Sense presentar-se al final: C
- Presentant-se al final: $\max(F, \frac{F+C}{2})$

Presentació

L'assignatura és una introducció a dues de les àrees centrals de la teoria de la computació (TC):

- La teoria d'autòmats
- La teoria de la calculabilitat

La pregunta que les uneix és:

Quines són les capacitats i limitacions fonamentals dels ordinadors?

Una tercera àrea de la TC, la teoria de la complexitat, serà present durant el curs encara que no tingui un tema específic.

L'assignatura és una introducció a dues de les àrees centrals de la teoria de la computació (TC):

- La teoria d'autòmats
- La teoria de la calculabilitat

La pregunta que les uneix és:

Quines són les capacitats i limitacions fonamentals dels ordinadors?

Una tercera àrea de la TC, la teoria de la complexitat, serà present durant el curs encara que no tingui un tema específic.

L'assignatura és una introducció a dues de les àrees centrals de la teoria de la computació (TC):

- La teoria d'autòmats
- La teoria de la calculabilitat

La pregunta que les uneix és:

Quines són les capacitats i limitacions fonamentals dels ordinadors?

Una tercera àrea de la TC, la teoria de la complexitat, serà present durant el curs encara que no tingui un tema específic.

Teoria de la calculabilitat

Neix en la dècada de 1930 quan matemàtics com K. Gödel, A. Turing o A. Church descobreixen que hi ha problemes que no es poden resoldre amb ordinadors. Exemples:

- Decidir si una afirmació matemàtica és certa o falsa
- Decidir si un programa s'atura o no

La teoria de la calculabilitat classifica els problemes com a decidibles o indecidibles. Amb els conceptes que introdueix, cap als anys 1960s neix la teoria de la complexitat, que refina la classificació dels problemes decidibles segons la seva dificultat.

Teoria de la calculabilitat

Neix en la dècada de 1930 quan matemàtics com K. Gödel, A. Turing o A. Church descobreixen que hi ha problemes que no es poden resoldre amb ordinadors. Exemples:

- Decidir si una afirmació matemàtica és certa o falsa
- Decidir si un programa s'atura o no

La teoria de la calculabilitat classifica els problemes com a decidibles o indecidibles. Amb els conceptes que introdueix, cap als anys 1960s neix la teoria de la complexitat, que refina la classificació dels problemes decidibles segons la seva dificultat.

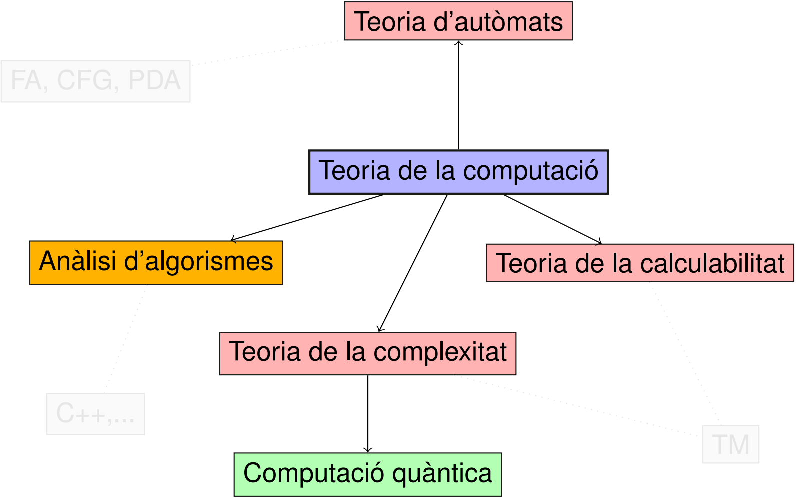
Teoria d'autòmats

Tracta les definicions i propietats dels models abstractes de càlcul que s'utilitzen en diverses àrees de la informàtica.

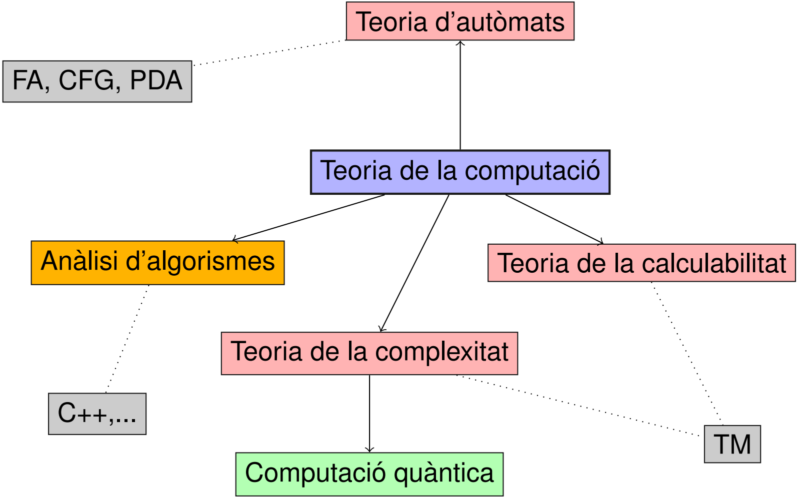
Els que estudiarem a TC són:

- Els autòmats finits (FA)
- Els autòmats amb pila (PDA)
- Les gramàtiques incontextuals (CFG)
- La màquina de Turing (TM)

Teoria de la computació i models de càlcul



Teoria de la computació i models de càlcul



Temari

1. Teoria de llenguatges
2. Autòmats finits
3. Gramàtiques incontextuals
4. Expressions regulars
5. - No regularitat
   - Autòmats amb pila i jerarquia de Chomsky
6. Màquines de Turing i decidibilitat
7. Problemes indecidibles i reduccions
8. Problemes naturals indecidibles

Presentació

Capacitats prèvies

Segons la guia docent:

1. Capacitat d'expressar en fórmules lògiques els enunciats descrits en llenguatge natural; també capacitat de manipular aquestes fórmules
2. Coneixements d'àlgebra i combinatòria
3. Coneixements d'algorísmia; en particular, saber avaluar la complexitat temporal d'un algorisme

1. Formalització

Exemple: enunciats sobre primalitat

Siguin $n, m \in \mathbb{N}$.

- m divideix n (en símbols, $m \mid n$):

$$\exists p \in \mathbb{N} \;\; mp = n$$

- n és primer:

$$n > 1 \land \neg(\exists m \in \mathbb{N} \;\; m > 1 \;\land\; m < n \;\land\; m \mid n)$$

- Conjunt dels primers:

$$\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ és primer}\}$$

- n és potència d'un primer:

$$\exists p \in P \, \exists e \in \mathbb{N} \;\; n = p^e$$

1. Formalització

Exemple: enunciats sobre primalitat

Siguin $n, m \in \mathbb{N}$.

- m divideix n (en símbols, $m \mid n$):

$$\exists p \in \mathbb{N} \;\; mp = n$$

- n és primer:

$$n > 1 \wedge \neg(\exists m \in \mathbb{N} \;\; m > 1 \;\wedge\; m < n \;\wedge\; m \mid n)$$

- Conjunt dels primers:

$$\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ és primer}\}$$

- n és potència d'un primer:

$$\exists p \in P \, \exists e \in \mathbb{N} \;\; n = p^e$$

1. Formalització

Exemple: enunciats sobre primalitat

Siguin $n, m \in \mathbb{N}$.

- m divideix n (en símbols, $m \mid n$):

$$\exists p \in \mathbb{N} \;\; mp = n$$

- n és primer:

$$n > 1 \land \neg(\exists m \in \mathbb{N} \;\; m > 1 \;\land\; m < n \;\land\; m \mid n)$$

- Conjunt dels primers:

$$\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ és primer}\}$$

- n és potència d'un primer:

$$\exists p \in P \; \exists e \in \mathbb{N} \;\; n = p^e$$

1. Formalització

Exemple: enunciats sobre primalitat

Siguin $n, m \in \mathbb{N}$.

- m divideix n (en símbols, $m \mid n$):

$$\exists p \in \mathbb{N} \;\; mp = n$$

- n és primer:

$$n > 1 \wedge \neg(\exists m \in \mathbb{N} \;\; m > 1 \;\wedge\; m < n \;\wedge\; m \mid n)$$

- Conjunt dels primers:

$$\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ és primer}\}$$

- n és potència d'un primer:

$$\exists p \in P \, \exists e \in \mathbb{N} \;\; n = p^e$$

1. Formalització

Exemple: enunciats sobre primalitat

Siguin $n, m \in \mathbb{N}$.

- m divideix n (en símbols, $m \mid n$):

$$\exists p \in \mathbb{N} \;\; mp = n$$

- n és primer:

$$n > 1 \wedge \neg(\exists m \in \mathbb{N} \;\; m > 1 \;\wedge\; m < n \;\wedge\; m \mid n)$$

- Conjunt dels primers:

$$\mathbb{P} = \{n \in \mathbb{N} \mid n \text{ és primer}\}$$

- n és potència d'un primer:

$$\exists p \in P \; \exists e \in \mathbb{N} \;\; n = p^e$$

2. Àlgebra i combinatòria

- Conceptes: conjunts, tuples, funcions, grafs
- Metodologia: definició $\rightarrow$ teorema $\rightarrow$ demostració

(referència: capítol 0 [S])

2. Àlgebra i combinatòria

- Conceptes: conjunts, tuples, funcions, grafs
- Metodologia: definició $\rightarrow$ teorema $\rightarrow$ demostració

(referència: capítol 0 [S])

Metodologia: definicions

Com definir que un conjunt A té cardinalitat més petita o igual que B?

1. Definint la cardinalitat d'un conjunt i comparant les d'A i B
2. Comparant els conjunts mitjançant funcions

Metodologia: definicions

Com definir que un conjunt A té cardinalitat més petita o igual que B?

1. Definint la cardinalitat d'un conjunt i comparant les d'A i B
2. Comparant els conjunts mitjançant funcions

Definició

Diem que A té *cardinalitat més petita o igual* que B, i escrivim $A \preceq B$, si existeix una injecció $A \mapsto B$.

Exemples

- $\{1, 2\} \preceq \mathbb{N}$ (via la identitat)
- $\mathbb{P} \preceq \mathbb{N}$ (via la identitat)
- $\mathbb{N} \preceq \mathbb{R}$ (via la identitat)

Metodologia: definicions

Com definir que un conjunt A té cardinalitat més petita o igual que B?

1. Definint la cardinalitat d'un conjunt i comparant les d'A i B
2. Comparant els conjunts mitjançant funcions

Definició

Diem que A té la *mateixa cardinalitat* que B, i escrivim $A \sim B$, si existeix una bijecció $A \mapsto B$.

Exemples

- $\{1, 2, 3\} \sim \{a, b, c\}$ (via $f(1) = a, f(2) = b, f(3) = c$)
- $\mathbb{P} \sim \mathbb{N}$ (via $g(p) = i$, o p és l'i-èsim primer)
- $\mathbb{N} \sim \{ n^2 \mid n \in \mathbb{N}\}$ (via $h(n) = n^2$)

Metodologia: definicions

Com definir que un conjunt A té cardinalitat més petita o igual que B?

1. Definint la cardinalitat d'un conjunt i comparant les d'A i B
2. Comparant els conjunts mitjançant funcions

Definició

Diem que A té *cardinalitat més petita* que B, i escrivim $A \prec B$, si $A \preceq B$ però $A \not\sim B$.

Exemple

- $\{1, 2, 3\} \prec \mathbb{N}$

Ja hem vist que $\{1, 2, 3\} \preceq \mathbb{N}$. D'altra banda, si $\{1, 2, 3\} \sim \mathbb{N}$, existiria una bijecció $f : \{1, 2, 3\} \to \mathbb{N}$. Com que $A = \{1, 2, 3, 4\} \subseteq \mathbb{N}$, cada element d'$A$ hauria de tenir una antiimatge diferent en $\{1, 2, 3\}$. Contradicció.

Metodologia: definicions

Definició

El conjunt de parts d'un conjunt A es defineix com

$$\mathcal{P}(A) = \{ B \mid B \subseteq A \}.$$

Exemples

- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$
- $\mathcal{P}(\{1,2\}) = \{ \emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $\mathcal{P}(\{1,2,3\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Metodologia: definicions

Definició

El conjunt de parts d'un conjunt A es defineix com

$$\mathcal{P}(A) = \{ B \mid B \subseteq A \}.$$

Exemples

- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$
- $\mathcal{P}(\{1,2\}) = \{ \emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $\mathcal{P}(\{1,2,3\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Metodologia: teoremes

Observació

Per a tot conjunt A,

1. $|\mathcal{P}(A)| = 2^{|A|}$ si A és finit
2. $A \preceq \mathcal{P}(A)$ (via $f(x) = \{x\}$, on $x \in A$)

Teorema de Cantor

Per a tot conjunt A, $A \prec \mathcal{P}(A)$.
(per reducció a l'absurd + diagonalització)

Veure:

- $\mathbb{N} \sim \mathbb{Q}$ (exemple 4.15 [S])
- $\mathbb{N} \prec \mathbb{R}$ (teorema 4.17 [S])

Metodologia: teoremes

Observació

Per a tot conjunt A,

1. $|\mathcal{P}(A)| = 2^{|A|}$ si A és finit
2. $A \preceq \mathcal{P}(A)$ (via $f(x) = \{x\}$, on $x \in A$)

Teorema de Cantor

Per a tot conjunt A, $A \prec \mathcal{P}(A)$.
(per reducció a l'absurd + diagonalització)

Veure:

- $\mathbb{N} \sim \mathbb{Q}$ (exemple 4.15 [S])
- $\mathbb{N} \prec \mathbb{R}$ (teorema 4.17 [S])

Metodologia: teoremes

Observació

Per a tot conjunt A,

1. $|\mathcal{P}(A)| = 2^{|A|}$ si A és finit
2. $A \preceq \mathcal{P}(A)$ (via $f(x) = \{x\}$, on $x \in A$)

Teorema de Cantor

Per a tot conjunt A, $A \prec \mathcal{P}(A)$.
(per reducció a l'absurd $+$ diagonalització)

Veure:

- $\mathbb{N} \sim \mathbb{Q}$ (exemple 4.15 [S])
- $\mathbb{N} \prec \mathbb{R}$ (teorema 4.17 [S])

Metodologia: demostracions

Mètodes de demostració:

- Per construcció*
- Per contradicció*
- Per casos
- Per inducció*
- Pel principi de les caselles
- Per diagonalització+

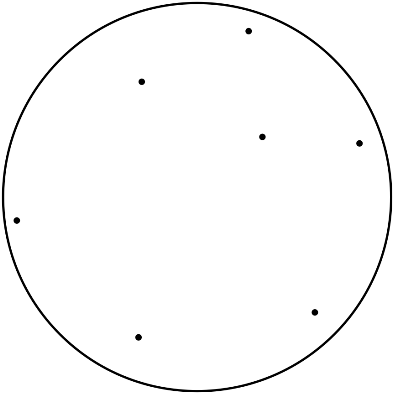
*: secció 0.4 [S]
+: teorema 4.17 [S]

Metodologia: demostracions

Principi de les caselles.

Exemple 1

Si hi ha 7 punts en un cercle de radi unitat, n'hi haurà 2 a distància ≤ 1.

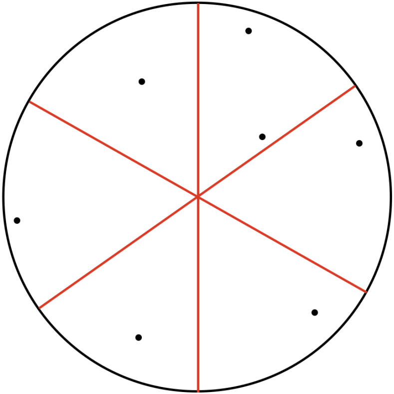


Metodologia: demostracions

Principi de les caselles.

Exemple 1

Si hi ha 7 punts en un cercle de radi unitat, n'hi haurà 2 a distància ≤ 1.

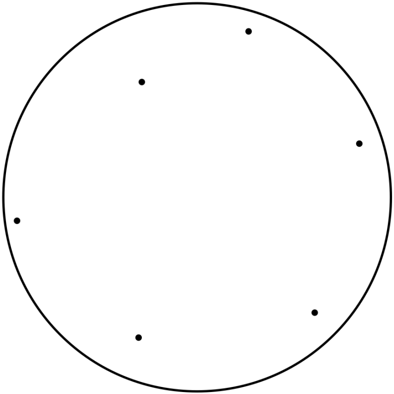


Metodologia: demostracions

Casos + principi de les caselles.

Exemple 2

Si hi ha 6 punts en un cercle de radi unitat, n'hi haurà 2 a distància ≤ 1.

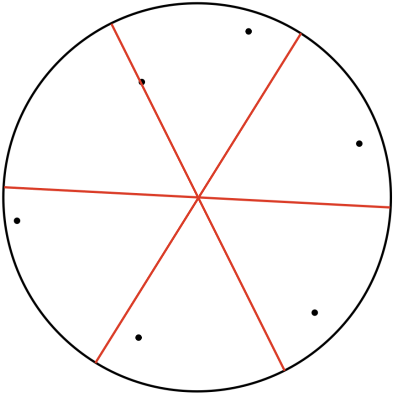


Metodologia: demostracions

Casos + principi de les caselles.

Exemple 2

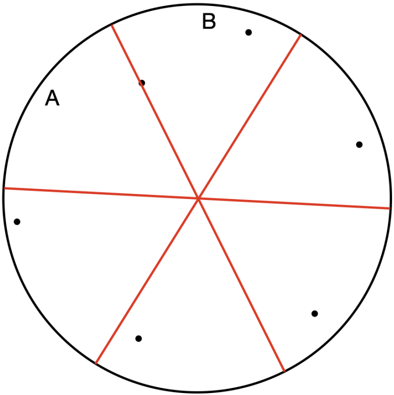
Si hi ha 6 punts en un cercle de radi unitat, n'hi haurà 2 a distància ≤ 1.



Metodologia: demostracions

Casos:

1. *A* o *B* contenen més punts $\rightarrow$ solució en *A* o *B*
2. ni *A* ni *B* contenen més punts



Metodologia: demostracions

Casos:

1. A o B contenen més punts
2. ni A ni B contenen més punts $\rightarrow$ p. caselles: 5 punts / 4 regions