QUÈ HEM FET FINS ARA?

El darrer que hem treballat són els següents mètodes estàndard de demostració: prova d'una disjunció, disjunció a l'antecedent, prova per casos, demostració d'una equivalència, demostració de la unicitat i exemples de cadascun.

CLASSE D'AVUI 19/10/2020

Tema d'inducció.

2.-INDUCCIÓ

2.1 Inducció simple

Molt sovint ens trobarem que hem de demostrar una propietat per a tots els nombres naturals (o per tots els naturals a partir d'un fixat). Moltes afirmacions en informàtica són dependents d'un n pertanyent a $\mathbb{N}$ i per tant diuen coses de l'estil $\forall n \geq 1\ P(n)$ a on, per exemple, la propietat $P(n)$ es refereix al que triga un cert programa en funció del número d'entrades, o el número de bytes d'emmagatzematge de memòria que requereix l'execució d'un programa en funció de la llargada n de l'entrada, etc. Comencem amb un exemple estrictament matemàtic.

EX.: Demostreu que $1 + 3 + 5 + 7 + \ldots + (2n + 1) = (n + 1)^2$ per a tot natural $n \geq 0$.

Observem que aquesta propietat diu que la suma dels primers nombres senars sempre dona un quadrat i a més diu quin quadraat és. Mirem aquestes sumes:

- per $n = 0$: $1 = 1 = (0 + 1)^2$
- per $n = 1$: $1 + 3 = 4 = (1 + 1)^2$
- per $n = 2$: $1 + 3 + 5 = 9 = (2 + 1)^2$
- per $n = 3$: $1 + 3 + 5 + 7 = 16 = (3 + 1)^2$
- $\ldots$

Serà cert sempre? Com es demostra amb els mètodes estudiats?

Aquests tipus de sumes se sol escriure amb el símbol de sumatori $\sum$ (utilitza la lletra "S" majúscula grega):

$$1 + 3 + 5 + 7 + \ldots + (2n + 1) = \sum_{i=0}^{n} 2i + 1$$

Per demostrar que aquestes afirmacions són certes es poden intentar els mètodes que hem estudiat fins ara però per aquest tipus de demostracions tenim un mètode específic: el mètode d'inducció. El mètode de demostració per inducció simple es basa en el principi següent:

$$\forall n \geq n_0\ P(n) \equiv P(n_0) \wedge \forall n > n_0 (P(n-1) \to P(n))$$

i serveix per demostrar que una propietat $P(n)$ és certa $\forall n \geq n_0$ natural. Usualment el que hem de demostrar és que $P(n)$ és certa $\forall n \in \mathbb{N}$ o sigui $P(n)$ és certa $\forall n \geq 0$ natural. La manera de demostrar és en dos passos:

CAS BASE $P(n_0)$

CAS INDUCTIU Sigui $n > n_0$ i volem demostrar que $P(n-1) \Rightarrow P(n)$.

Per tant es redueix a fer una comprovació en el cas base i en el pas inductiu suposes la hipòtesi d'inducció (HI) $P(n-1)$ i a partir d'aquesta demostres $P(n)$.

Fixem-nos que la idea que hi ha al darrera del mètode d'inducció és (suposeu que $n_0 = 1$):

- tenim provat que $P(1)$ és cert i que $P(n-1) \Rightarrow P(n)$, per tant en particular per $n = 2$ obtenim $P(1) \Rightarrow P(2)$ i com que $P(1)$ és cert obtenim que també ho és $P(2)$
- per ara tenim que $P(1)$, $P(2)$ són certs i del cas inductiu obtenim per $n = 3$ que $P(2) \Rightarrow P(3)$ i com que $P(2)$ és cert obtenim que també ho és $P(3)$
- ara tenim que $P(1)$, $P(2)$, $P(3)$ són certs i del cas inductiu obtenim per $n = 4$ que $P(3) \Rightarrow P(4)$ i com que $P(3)$ és cert obtenim que també ho és $P(4)$
- ...

Aleshores obtenim que tots els casos són certs amb un mecanisme com el de les fitxes del dòmino que cauen d'uan en una (https://www.youtube.com/watch?v=bUI295oyeIc). És com un esquema d'implicacions

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow P(4) \Rightarrow \ldots$$

en el qual partim de que $P(1)$ és cert i fa que per modus ponens la certesa vagi afirmant-se pels següents.

EX.: (continuació) Demostreu que $1 + 3 + 5 + 7 + \ldots + (2n + 1) = (n + 1)^2$ per a tot natural $n \geq 0$.

CAS BASE: L'afirmació és certa per $n = 0$ ja que per una banda a la igualtat que hem de justificar tenim 1 i per l'altra bana tenim $(0 + 1)^2$, resultats idèntics, per tant queda justificat el cas base.

CAS INDUCTIU: Sigui $n > 0$ i volem demostrar que $P(n-1) \Rightarrow P(n)$. Per tant hem de suposar que és cert el cas $n - 1$:

$1 + 3 + 5 + 7 + \ldots + (2(n-1) + 1) = (n - 1 + 1)^2$ (hipòtesi d'inducció, HI)

i vull demostrar que es cert el cas n:

$1 + 3 + 5 + 7 + \ldots + (2n + 1) =^{?????} (n + 1)^2$

En efecte, calculo els dos costats de la igualtat:

- $1 + 3 + 5 + 7 + \ldots + (2n + 1) = 1 + 3 + 5 + 7 + \ldots + (2n - 1) + (2n + 1) =$
  $= (n - 1 + 1)^2 + (2n + 1) = n^2 + 2n + 1$
- $(n + 1)^2 = (n + 1)^2$

com que son iguals hem justificat que és cert el cas n a partir de la suposició de que el cas $n - 1$ és cert.

EX.: (1) Demostreu que $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ per a tot $n \geq 0$.

En primer lloc el significat del sumatori és $\sum_{i=0}^{n} i = 0+1+2+3+4+\ldots+n$. La formalització del que ens demanen demostrar és $\forall n \in \mathbb{N}\left(\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\right)$. Per fer la demostració d'aquesta fórmula per inducció seguim l'esquema estàndard:

CAS BASE Cal veure que l'afirmació és certa per $n = 0$: calculo el costat esquerra de la igualtat $\sum_{i=0}^{0} i = 0$ i calculo el costat dret de la igualtat $\frac{0(0+1)}{2} = 0$ i per tant és cert que dona el mateix.

CAS INDUCTIU Sigui $n > 0$ i volem demostrar que el cas $n-1$ implica el cas n, és a dir, que si sabem que és cert:

$0+1+2+3+4+\ldots+(n-1) = \frac{(n-1)(n-1+1)}{2}$ (HI)

llavors serà cert:

$0+1+2+3+4+\ldots+n =^{?????} \frac{n(n+1)}{2}$

En efecte:

- $0+1+2+3+4+\ldots+n = 0+1+2+3+4+\ldots+(n-1) \; + \; n =$
  $= \frac{(n-1)(n-1+1)}{2} + n = \frac{(n-1)n}{2} + n = \frac{n^2-n+2n}{2} = \frac{n^2+n}{2}$
- $\frac{n(n+1)}{2} = \frac{n^2+n}{2}$

com que ens ha donat el mateix resultat, tenim demostrat el cas n.

EX.: És cert que $991n^2+1$ no és mai un quadrat? (per a tot $n \geq 1$)

Experimentem una mica a veure si és cert o no en els primers nombres naturals:

$991+1 = 992 = 2^5 31$

$991 \cdot 2^2 + 1 = 3965 = 5 \times 13 \times 61$

$991 \cdot 3^2 + 1 = 8920 = 2^3 5 \times 223$

$991 \cdot 4^2 + 1 = 15\,857 = 101 \times 157$

$991 \cdot 5^2 + 1 = 24\,776 = 2^3 19 \times 163$

$991 \cdot 6^2 + 1 = 35\,677 = 35\,677$

Sembla que és cert que mai dona un quadrat perquè els exponents a la descomposició factorial no són parells. Serà veritat o fals???

És fals: el primer nombre natural pel qual falla és $n = 12055735790331359447442538767$ (29 xifres) ja que

$991 \cdot (12055735790331359447442538767)^2 + 1 =$

$= 144\,032\,698\,557\,259\,999\,607\,886\,110\,560\,755\,362\,973\,171\,476\,419\,973\,199\,366\,400 =$

$= 2^8 5^2 31^2 1093^2 100\,271^2 140\,527^2 1516\,049^2 6554\,059^2$

per tant és un quadrat. Sense calculadora programable ni ordinador mai podríem arribar a veure que és falsa l'afirmació (ni en anys de calculadora, ni res).

EX.: (2) Demostreu que $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ per a $n \geq 1$.

En primer lloc la propietat sense utilitzar el sumatori diu

$\frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \frac{1}{4\cdot5} + \ldots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$ per a tot $n \geq 1$.

Per fer la demostració d'aquesta fórmula per inducció seguim l'esquema estàndard:

PAS BASE Per $n = 1$ el canto esquerra de la igualtat és $\frac{1}{1\cdot2} = \frac{1}{2}$ i el cantó dret és $\frac{1}{1+1} = \frac{1}{2}$ llavors és cert que són iguals.

PAS INDUCTIU Sigui $n > 1$ i volem demostrar que si suposem cert

$\frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \frac{1}{4\cdot5} + \ldots + \frac{1}{(n-1)\cdot(n-1+1)} = \frac{n-1}{n-1+1}$ (HI)

aleshores seríem capaços de demostrar que és cert

$\frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \frac{1}{4\cdot5} + \ldots + \frac{1}{n\cdot(n+1)} =^{?????} \frac{n}{n+1}$

En efecte:

$$\frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \frac{1}{4\cdot5} + \ldots + \frac{1}{n\cdot(n+1)} = \frac{1}{1\cdot2} + \frac{1}{2\cdot3} + \frac{1}{3\cdot4} + \frac{1}{4\cdot5} + \ldots + \frac{1}{(n-1)\cdot(n-1+1)} + \frac{1}{n\cdot(n+1)} =$$
$$= \frac{n-1}{n-1+1} + \frac{1}{n\cdot(n+1)} = \frac{n-1}{n} + \frac{1}{n\cdot(n+1)} = \frac{(n+1)(n-1)+1}{n\cdot(n+1)} = \frac{n^2}{n\cdot(n+1)} = \frac{n}{n+1}$$

Just el que volíem demostrar (el cas n a partir de suposar cert el cas $n-1$).

EX.: (3) Demostreu que $\sum_{i=1}^{n} \frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$ per a tot $n \geq 1$.

En primer lloc la propietat sense utilitzar el sumatori diu

$\frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \frac{1}{13\cdot17} + \ldots + \frac{1}{(4n-3)(4n+1)} = \frac{n}{4n+1}$ per a tot $n \geq 1$.

Per fer la demostració d'aquesta fórmula per inducció seguim l'esquema estàndard:

PAS BASE Per $n = 1$ el canto esquerra de la igualtat és $\frac{1}{1\cdot5} = \frac{1}{5}$ i el cantó dret és $\frac{1}{4+1} = \frac{1}{5}$ llavors és cert que són iguals.

PAS INDUCTIU Sigui $n > 1$ i volem demostrar que si suposem cert

$\frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \frac{1}{13\cdot17} + \ldots + \frac{1}{(4(n-1)-3)(4(n-1)+1)} = \frac{n-1}{4(n-1)+1}$ (HI)

aleshores seríem capaços de demostrar que és cert

$\frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \frac{1}{13\cdot17} + \ldots + \frac{1}{(4n-3)(4n+1)} =^{???} \frac{n}{4n+1}$

En efecte:

- $\frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \frac{1}{13\cdot17} + \ldots + \frac{1}{(4n-3)(4n+1)} =$
  $= \frac{1}{1\cdot5} + \frac{1}{5\cdot9} + \frac{1}{9\cdot13} + \frac{1}{13\cdot17} + \ldots + \frac{1}{(4(n-1)-3)(4(n-1)+1)} + \frac{1}{(4n-3)(4n+1)} = \frac{n-1}{4(n-1)+1} + \frac{1}{(4n-3)(4n+1)} =$
  $= \frac{n-1}{4n-3} + \frac{1}{(4n-3)(4n+1)} = \frac{(n-1)(4n+1)+1}{(4n-3)(4n+1)} = \frac{4n^2-3n}{(4n-3)(4n+1)} = \frac{n(4n-3)}{(4n-3)(4n+1)}$
- $\frac{n}{4n+1} = \frac{n(4n-3)}{(4n-3)(4n+1)}$

iguals tal com volíem demostrar.

EX.: (4) Demostreu que $\prod_{k=2}^{n}\left(1-\frac{1}{k}\right) = \frac{1}{n}$ per a tot $n \geq 2$.

Ens demanen demostrar que:

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\ldots\left(1-\frac{1}{n}\right) = \frac{1}{n}$$

CAS $n = 2$ Calculem el costat esquerra de la igualtat i dona $1-\frac{1}{2} = \frac{1}{2}$ i el cantó dret dona $\frac{1}{2}$ per tant son iguals i així queda justificat el cas base.

CAS $n-1$ **IMPLICA EL CAS** n Sigui un $n > 2$ i suposant que és cert

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\ldots\left(1-\frac{1}{n-1}\right) = \frac{1}{n-1} \text{ (HI)}$$

volem demostrar que és cert:

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\ldots\left(1-\frac{1}{n}\right) =^{???} \frac{1}{n}$$

En efecte:

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\ldots\left(1-\frac{1}{n}\right) =$$
$$= \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\ldots\left(1-\frac{1}{n-1}\right)\ \left(1-\frac{1}{n}\right) =$$
$$= \frac{1}{n-1}\left(1-\frac{1}{n}\right) = \frac{1}{n-1}\left(\frac{n-1}{n}\right) = \frac{1}{n}$$

per tant queda demostrat el cas n a partir del cas $n-1$.

EX.: (5) Demostreu que $3^n < (n+2)!$ per a tot $n \geq 0$.
Aquest exemple ja és diferent perquè involucra demostrar desigualtats.

CAS $n = 0$ Calculem el costat esquerra de la desigualtat i dona $3^0 = 1$ i el cantó dret dona $(0+2)! = 2! = 2$ per tant queda justificat el cas base perquè $1 < 2$.

CAS $n-1$ **IMPLICA EL CAS** n Sigui un $n > 0$ i suposem que és cert $3^{n-1} < (n-1+2)!$ (HI) i vull deduir d'aquí que és cert $3^n <^{???} (n+2)!$. En efecte calculem els dos cantons per separat (i utilitzem la HI):

- $3^n = 3^{n-1}3^1 < (n-1+2)!3^1 = (n+1)!3$
- $(n+2)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot \ldots \cdot n \cdot (n+1) \cdot (n+2) = (n+1)!(n+2)$

Com que $n > 0$, és a dir, $n \geq 1$ tenim que $3 \leq n+2$ llavors tindrem que $3^n < (n+1)!3 \leq (n+1)!(n+2) = (n+2)!$ i per tant $3^n < (n+2)!$.

EX.: (6) Demostreu que $\sum_{i=2}^{n}\frac{1}{i^2} < \frac{n-1}{n}$ per a tot $n \geq 2$.

$$\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+\ldots+\frac{1}{n^2} < \frac{n-1}{n}$$

CAS $n = 2$ Calculo cantó esquerra de la desigualtat $\frac{1}{2^2} = \frac{1}{4}$ i el cantó dret $\frac{2-1}{2} = \frac{1}{2}$, per tant el cas $n = 2$ és cert perquè $\frac{1}{4} < \frac{1}{2}$.

CAS $n - 1$ **IMPLICA EL CAS** n Sigui $n > 2$ i volem demostrar que a partir de

$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \ldots + \frac{1}{(n-1)^2} < \frac{n-2}{n-1}$ (HI)

es pot deduir que

$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \ldots + \frac{1}{n^2} <^{???} \frac{n-1}{n}$

En efecte: calculem cada cantó de la desigualtat i obtenim utilitzant la hipòtesi d'inducció

- $\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \ldots + \frac{1}{n^2} = \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \ldots + \frac{1}{(n-1)^2} + \frac{1}{n^2} < \frac{n-2}{n-1} + \frac{1}{n^2} =$
  $= \frac{n^3-2n^2+n-1}{n^2(n-1)}$
- $\frac{n-1}{n}$

Si veig que $\frac{n^3-2n^2+n-1}{n^2(n-1)} \leq \frac{n-1}{n}$ ja estarà demostrat tot. Per demostrar aquesta desigualtat faig la resta:

$\frac{n^3-2n^2+n-1}{n^2(n-1)} - \frac{n-1}{n} = -\frac{1}{n^2(n-1)} \leq 0$

i així queda demostrat que el cas $n - 1$ implica el cas n.

EX.: (7) Demostreu que $6^{2n+1} - 6$ és múltiple de 210 per a tot $n \geq 0$.

CAS $n = 0$ Mirem si per $n = 0$ ens dona un múltiple de 210:
$6^{0+1} - 6 = 6 - 6 = 0 = 0 \cdot 210$ per tant és cert.

CAS $n - 1$ **IMPLICA EL CAS** n Sigui un $n > 0$ i suposem que $6^{2(n-1)+1} - 6 = 210k$ i ara volem demostrar que també passa $6^{2n+1} - 6$ és múltiple de 210. Per això volem calcular $6^{2n+1} - 6 = ???$. Per HI: $6^{2n-1} - 6 = 210k$, o sigui $6^{2n-1} = 6 + 210k$ i llavors:

$6^{2n+1} - 6 = 6^{2n-1+2} - 6 = 6^{2n-1}6^2 - 6 = (6 + 210k)6^2 - 6 =$

$= 6^2 210k + 6^3 - 6 = 6^2 210k + 210 = 210(6^2k + 1)$

per tant és múltiple de 210 tal com havíem de demostrar.

De vegades en el cas base s'han de veure més d'un cas i cal fer un raonament de l'estil:

PAS BASE $P(n_0), P(n_0 + 1), P(n_0 + 2), \ldots, P(n_0 + r)$,

PAS INDUCTIU Sigui $n > n_0 + r$ i volem demostrar que $P(n - 1) \Rightarrow P(n)$.

Veiem en aquest exemple perquè es necessita mirar més d'un cas base:

EX.: Demostreu que $5^n < 27n!$ per a tot $n \geq 0$.

3.-CONJUNTS I RELACIONS

3.1 Conjunts

Tenim conjunts i elements entre els quals podem dir si un element pertany a un conjunt o si no hi pertany. Per A un conjunt i x un element escriurem $x \in A$ per dir que x pertany al conjunt A i escriurem $x \notin A$ per dir que x no pertany al conjunt A. Els conjunts els pensem com un sac en el qual estan dins els elements (no tenen un ordre determinat ni poden estar repetits).

Els conjunts els podem donar:

- per una llista dels seus elements entre claus (es diu que donem el conjunt *per extensió*): $A = \{a_1, a_2, a_3, \ldots, a_n\}$ (conjunt format pels elements $a_1, a_2, a_3, \ldots, a_n$; es poden posar en l'ordre que es vulgui i no n'hi poden haver repetits). Tindrem que $x \in A \Leftrightarrow x = a_1$ o $x = a_2$ o $x = a_3$ o $\ldots$ o $x = a_n$. Per exemple $A = \{0, 2, 4, 6\}$ és el conjunt format pels elements $0, 2, 4, 6$.
- també els podem donar dient una propietat que els defineixin (es diu que donem el conjunt *per comprensió*): $A = \{x | P(x)\}$ (conjunt format pels elements x que tenen la propietat $P(x)$ i es llegeix que és el conjut dels x tals que satisfan la propietat $P(x)$; la barra vertical de vegades se substitueix per ":" o per "$t.q.$"). Tindrem que $x \in A \Leftrightarrow P(x)$. Per exemple $A = \{x | x \text{ natural parell menor o igual que } 6\}$ que també se sol escriure com a $A = \{x \in \mathbb{N} | x \text{ parell menor o igual que } 6\}$. En general escriurem $A = \{x \in B | P(x)\}$ per designar el conjunt format pels elements de B que verifiquen la propietat $P(x)$.

Direm que dos conjunts són iguals quan tenen els mateixos elements (*principi d'extensionalitat*): $A = B \Leftrightarrow \forall x (x \in A \Leftrightarrow x \in B)$. Tenim un conjunt molt especial que està definit per no tenir cap element: el conjunt buit $\varnothing = \{\} = \{x | x \neq x\}$. Tenim una relació entre conjunts que és la següent:

DEF.: Direm per dos conjunts A, B que A està inclòs dins B (i ho escriurem així: $A \subseteq B$) quan:

$A \subseteq B \Leftrightarrow \forall x (x \in A \Rightarrow x \in B)$

Es diu també que A és un subconjunt de B (o que és una part de B).

EX.: Siguin $A = \{a, b\}$, $B = \{a, b, c\}$, $C = \{a\}$. Raoneu si són certes les afirmacions següents:

1. $a \in A$ certa perquè a està a la llista amb la quel està definit A
2. $c \in A$ falsa
3. $A \subseteq B$ certa perquè ...
4. $B \subseteq A$ falsa perquè c$\in$ $B però c \notin A$
5. $A \subseteq C$ falsa perquè b$\in$ $A però b \notin C$
6. $A \subseteq \{a, b, \{a\}\}$ certa
7. $\{a\} \in \{a, b, \{a\}\}$ certa

8. $\{b\} \in \{a, b, \{a\}\}$ falsa

S'observa que pel principi d'extensionalitat podem afirmar que:
PROP.: Siguin A, B conjunts. Aleshores $A = B \Leftrightarrow A \subseteq B, B \subseteq A$.
DEM.: OK.

Tenim també aquestes propietats bàsiques:
PROP.: Siguin A, B, C conjunts. Aleshores

1. $\varnothing \subseteq A$
2. $A \subseteq A$
3. $A \subseteq B$ i $B \subseteq C$ implica $A \subseteq C$