QUÈ HEM FET FINS ARA?

El darrer que hem treballat són els següents mètodes estàndard de demostració: prova per reducció a l'absurd (1) i exemples, i prova per reducció a l'absurd (2) i exemples.

CLASSE D'AVUI 15/10/2020

Seguim amb els darrers mètodes de demostració.

Prova d'una disjunció

Volem provar $A \vee B$ i per això fem $\neg A \Rightarrow \ldots \Rightarrow B$. Es basa en: $q \vee r \equiv \neg q \rightarrow r$. Intuïtivament vol dir que distingim dos casos: com que hem de provar que és cert $A \vee B$ ens fixem que poden passar dues coses, o bé A és cert o bé A és fals; si A és cert llavors tindrem demostrat $A \vee B$; si $\neg A$ és cert llavors haurem de demostrar $A \vee B$ suposant $\neg A$, o sigui haurem de suposar $\neg A$ i demostrar B.

També val quan hi ha més termes a la disjunció utilitzant l'equivalència: $p_1 \vee p_2 \vee \ldots \vee p_n \equiv (\neg p_1 \wedge \neg p_2 \wedge \ldots \wedge \neg p_{n-1}) \rightarrow p_n$. En aquest cas volem provar $B_1 \vee B_2 \vee \ldots \vee B_n$ i llavors fem $(\neg B_1 \wedge \neg B_2 \wedge \ldots \wedge \neg B_{n-1}) \Rightarrow \ldots \Rightarrow B_n$.

EX.: (38) En el conjunt dels nombres enters demostreu que n és senar o n^2 és múltiple de 4.

Formalitzem: $\forall n \in \mathbb{Z}\left(n \text{ és senar o } n^2 \text{ és múltiple de } 4\right)$. Sigui n qualsevol enter i vull demostrar que n és senar o n^2 és múltiple de 4 . Suposem que n és parell i demostrem que n^2 és múltiple de 4. En efecte: si n és parell, llavors existeix un k enter tal que $n = 2k \Rightarrow n^2 = (2k)^2 = 4k^2 \Rightarrow n^2$ és múltiple de 4. Tal com volíem demostrar.

En aquest exemple també podríem haver-lo plantejat suposant que n^2 no és múltiple de 4 i a continuació deduir que n és parell. Però aquesta opció és molt més complexa de treballar. En primer lloc perquè dir que "n^2 no és múltiple de 4 " és el mateix que dir que el resultat de la divisió n^2 per 4 no és exacte i això es formalitza d'aquesta manera: existeixen $q, r \in \mathbb{Z}$ tals que $n^2 = 4q + r$, $0 < |r| < 4$ (algorisme de la divisió entera). A continuació tindríem que r podria ser $r = 1, 2, 3$ i s'haurien d'analitzar els tres casos...

EX.: (39) En el conjunt dels nombres reals demostreu que $a \leq \frac{a+b}{2}$ o $b \leq \frac{a+b}{2}$.

Formalitzem l'afirmació: $\forall a \in \mathbb{R} \forall b \in \mathbb{R}\left(a \leq \frac{a+b}{2} \text{ o } b \leq \frac{a+b}{2}\right)$.

Siguin dos nombres reals qualssevol. Suposem que $a > \frac{a+b}{2}$ i vull demostrar que $b \leq \frac{a+b}{2}$. Una de les maneres més simples de justificar una desigualtat és la següent: cal demostrar que

$b - \frac{a+b}{2} \leq 0$

Com que sé que $a > \frac{a+b}{2} \Rightarrow 2a > a + b \Rightarrow a > b$. Ara la resta valdrà:

$b - \frac{a+b}{2} = \frac{b-a}{2} < 0$
per tant ja està justificat.

EX.: (40) En el conjunt dels nombres reals demostreu que $a \leq \frac{a+b+c}{3}$ o $b \leq \frac{a+b+c}{3}$ o $c \leq \frac{a+b+c}{3}$.

Formalitzem l'afirmació: $\forall a, b, c \in \mathbb{R}\left(a \leq \frac{a+b+c}{3} \text{ o } b \leq \frac{a+b+c}{3} \text{ o } c \leq \frac{a+b+c}{3}\right)$. Siguin tres nombres reals qualssevol. Suposem que $a > \frac{a+b+c}{3}$, que $b > \frac{a+b+c}{3}$ i vull demostrar que $c \leq \frac{a+b+c}{3}$. Fem com a l'exemple anterior, és a dir, cal demostrar que
$c - \frac{a+b+c}{3} \leq 0$.

Com que sé que $a > \frac{a+b+c}{3} \Rightarrow 3a > a+b+c \Rightarrow 2a > b+c$. I també $b > \frac{a+b+c}{3} \Rightarrow 3b > a+b+c \Rightarrow 2b > a+c$. ARa podria mirar en aquestes dues desigualtats a quines conclusions arribo d'una mateixa lletra. Fem-ho per exemple amb la c. Aïllant la c en les dues desigualtats puc treure com a conclusió que $c < 2a - b$ i que $c < 2b - a$. Ara la resta que volíem calcular podem transformar-la en dues expressions utilitzant les dues desigualtats obtingudes:

$$c - \frac{a+b+c}{3} = \frac{2c-a-b}{3} < \frac{2(2a-b)-a-b}{3} = \frac{4a-2b-a-b}{3} = a - b$$
$$c - \frac{a+b+c}{3} = \frac{2c-a-b}{3} < \frac{2(2b-a)-a-b}{3} = \frac{4b-2a-a-b}{3} = b - a$$

per tant ja està justificat que és menor o igual que 0 perquè $a - b$ o $b - a$ és negatiu ($b - a = -(a-b)$) i aleshores $c - \frac{a+b+c}{3} < 0$ com volíem demostrar.

Aquest exemple és més simple si raoneu de la manera següent: quan dieu que suposem que $a > \frac{a+b+c}{3}$, que $b > \frac{a+b+c}{3}$ i vull demostrar que $c \leq \frac{a+b+c}{3}$, es pot procedir per reducció a l'absurd suposant que $c > \frac{a+b+c}{3}$ i arribant a contradicció, cosa molt fàcil perquè:

$$\left.\begin{array}{l} a > \frac{a+b+c}{3} \\ b > \frac{a+b+c}{3} \\ c > \frac{a+b+c}{3} \end{array}\right\} \Rightarrow a+b+c > \frac{a+b+c}{3} + \frac{a+b+c}{3} + \frac{a+b+c}{3} \Rightarrow a+b+c > a+b+c$$

conclusió errònia. Fixeu-vos que en el fons el que estaríeu fent és el mètode de reducció a l'absurd (1).

Disjunció al conseqüent

Volem provar $A \Rightarrow B \vee C$ i fem $A, \neg B \Rightarrow \ldots \Rightarrow C$. Es basa en: $p \to (q \vee r) \equiv (p \wedge \neg q \to r)$. Es pot entendre intuïtivament com l'anterior mètode (distinció de casos). També val quan hi ha més termes a la disjunció utilitzant l'equivalència: $p \to (q_1 \vee q_2 \vee \ldots \vee q_n) \equiv (p \wedge \neg q_1 \wedge \neg q_2 \wedge \ldots \wedge \neg q_{n-1}) \to q_n$. En aquest cas volem provar $A \to B_1 \vee B_2 \vee \ldots \vee B_n$ i llavors fem $A \wedge \neg B_1 \wedge \neg B_2 \wedge \ldots \wedge \neg B_{n-1} \Rightarrow \ldots \Rightarrow B_n$.

EX.: (47) Demostreu que per x, y reals, si $x + y \leq 2$ llavors $x \leq 1$ o $y \leq 1$.

En primer lloc formalitzem l'afirmació: $\forall x, y \in \mathbb{R}\left(x + y \leq 2 \Rightarrow x \leq 1 \text{ o } y \leq 1\right)$. Siguin x, y reals. Ara volem demostrar que $x + y \leq 2 \Rightarrow x \leq 1$ o $y \leq 1$ per la qual cosa suposo que $x+y \leq 2$, $x > 1$ i vull justificar que $y \leq 1$. Utilitzem les dues desigualtats:

$x+y \leq 2$ i $1 < x \Rightarrow 1+y < x+y \leq 2 \Rightarrow 1+y < 2 \Rightarrow y < 1 \Rightarrow y \leq 1$

tal com es volia demostrar.

EX.: (48) Demostreu que per a,b,c enters, si $a+5 = c-b$ llavors a és senar o b és senar o c és senar.

La formalització seria $\forall a,b,c \in \mathbb{Z}\big(a+5 = c-b \Rightarrow a$ és senar o b és senar o c és senar$\big)$. Siguin $a,b,c \in \mathbb{Z}$ qualssevol. Com que hem de demostrar que si $a+5 = c-b$ aleshores a és senar o b és senar o c és senar, llavors suposarem que $a+5 = c-b$, que a és parell i que b és parell i demostrarem que c és senar. Escrivim cada cosa:

$$\left.\begin{array}{r} a+5 = c-b \\ a = 2k \text{ per cert enter } k \\ b = 2k' \text{ per cert enter } k' \end{array}\right\} \Rightarrow 2k+5 = c-2k' \Rightarrow c = 2k+5+2k' = 2(k+k'+2)+1$$

per tant c és senar com s'havia de provar.

Disjunció a l'antecedent:

En aquest cas es vol demostrar que $(B \vee C) \Rightarrow A$. És equivalent a fer una prova per casos (distingim segons B o C i provem A) . Es basa en l'equivalència:$(q \vee r) \to p \equiv (q \to p) \wedge (r \to p)$. Aleshores si volem demostrar $(B \vee C) \Rightarrow A$ fem:

$B \Rightarrow \ldots \Rightarrow A$
$C \Rightarrow \ldots \Rightarrow A$

També val amb més casos: quan es vol demostrar $(B_1 \vee B_2 \vee \ldots \vee B_n) \Rightarrow A$ farem:

$B_1 \Rightarrow \ldots \Rightarrow A$
$B_2 \Rightarrow \ldots \Rightarrow A$
$\ldots$
$B_n \Rightarrow \ldots \Rightarrow A$

EX.: (60) Demostreu que si n és enter llavors si el residu de n al dividir per 4 és 1 o 3, el residu de n^2 és 1.

Fem la formalització: $\forall n \in \mathbb{Z}\big($residu de n al dividir per 4 és 1 o $3 \Rightarrow$ residu de n^2 al dividir per 4 és $1\big)$. Sigui n enter qualsevol. Volem demostrar que si el residu de n al dividir per 4 és 1 o 3 $\Rightarrow$residu de n^2 al dividir per 4 és 1. Mirarem dos casos:

- residu de n al dividir per 4 és 1 $\Rightarrow$residu al dividir per 4 de n^2 és 1: és molt fàcil ja que

  $n = 4q+1$(per cert enter q)$\Rightarrow n^2 = (4q+1)^2 = (4q+1)^2 = 16q^2+8q+1 = 4(4q^2+2q)+1$

per tant el residu al dividir per 4 és 1.

- residu de n al dividir per 4 és 3 $\Rightarrow$residu al dividir per 4 de n^2 és 1: és molt fàcil també perquè

  $n = 4q+3 \Rightarrow n^2 = (4q+3)^2 = 16q^2+24q+9 = 4(4q^2+6q+2)+1$

  com es volia demostrar.

Prova per casos

Aquest tipus de prova es basa en la tautologia:
$(p_1 \vee p_2 \vee\ldots\vee p_n) \to (p \leftrightarrow (p_1 \to p) \wedge (p_2 \to p) \wedge\ldots\wedge(p_n \to p))$. Volem demostrar A, i distingim els casos $A_1, A_2, \ldots, A_n$ sempre que $A_1 \vee A_2 \vee\ldots\vee A_n = cert$ és a dir que podem suposar que o passa A_1 o passa A_2 o ... o passa A_n (això es diu que cal que els diferents casos exhaureixin totes les possibilitats). A la pràctica fem:

Cas 1: $A_1 \Rightarrow\ldots\Rightarrow A$

…

Cas n: $A_n \Rightarrow\ldots\Rightarrow A$

EX.: (64) Demostreu que si n és enter llavors n^2+n és parell (2 casos).
La formalització seria $\forall n \in \mathbb{Z}\left(n^2+n \text{ és parell}\right)$. Sigui $n \in \mathbb{Z}$ qualsevol. Per

demostrar l'afirmació (n^2+n és parell) distingirem els dos casos A_1 =ser parell, A_2 =ser senar. Fem les distincions:

- Cas 1: $n = 2k \Rightarrow n^2+n = (2k)^2+2k = 4k^2+2k = 2(2k^2+k)$ parell tal com s'havia de demostrar.
- Cas 2: $n = 2k+1 \Rightarrow n^2+n = (2k+1)^2+2k+1 =$
  $4k^2+6k+2 = 2(2k^2+3k+1)$ parell tal com s'havia de justificar.

Demostració d'una equivalència

Per demostrar una equivalència utilitzarem que: $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$. Llavors per demostrar $A \Leftrightarrow B$ s'han de fer dues demostracions:

$A \Rightarrow B$

$B \Rightarrow A$

Quan s'ha de demostrar l'equivalència de 3 o més afirmacions $A_1 \Leftrightarrow A_2 \Leftrightarrow\ldots\Leftrightarrow A_n$ farem una justificació molt similar en forma de cercle (i poden reordenar les afirmacions com ens convingui):

$A_1 \Rightarrow A_2$

$A_2 \Rightarrow A_3$

$\ldots$

$A_{n-1} \Rightarrow A_n$

$A_n \Rightarrow A_1$

Aquest fet es basa en l'equivalència:
$(p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge\ldots\wedge(p_{n-1} \leftrightarrow p_n) \equiv (p_1 \to p_2) \wedge (p_2 \to p_3) \wedge\ldots\wedge(p_{n-1} \to p_n) \wedge (p_n$

EX.: (81) Demostreu que si n és enter aleshores n és senar si i només si $n^2 + 3$ és parell.

Tenim la formalització: $\forall n \in \mathbb{Z}\big(n$ és senar sii només si $n^2 + 3$ és parell$\big)$

- $\Rightarrow$: suposem que n és senar i vull demostrar que $n^2 + 3$ és parell; en efecte:
  $n = 2k + 1 \Rightarrow n^2 + 3 = (2k + 1)^2 + 3 = 4k^2 + 4k + 4 = 2(2k^2 + 2k + 2)$
  com es volia demostrar.
- $\Leftarrow$: suposem que $n^2 + 3$ és parell i vull demostrar que n és senar; fem-ho per contrarecíproc que sembla més fàcil: suposem que n és parell i vull demostrar que $n^2 + 3$ és senar, cosa molt fàcil perquè
  $n = 2k \Rightarrow n^2 + 3 = (2k)^2 + 3 = 4k^2 + 3 = 2(2k^2 + 1) + 1$
  com es volia provar.

EX.: (82) Demostreu que si n, m són enters llavors són equivalents:

$a)$ $5n + 3m$ és senar

$b)$ $n - 3m$ és senar

$c)$ n i m tenen diferent paritat

La formalització és idèntica als anteriors exemples. Siguin n, m enters. Fem cadascuna de les demostracions:

- $a) \Rightarrow b)$: en aquest cas suposem que $5n + 3m$ és senar i volem deduir que $n - 3m$ és senar; per tant sabem que per un enter k:
  $5n + 3m = 2k + 1 \Rightarrow n - 3m = 5n + 3m - 4n - 6m = 2k + 1 - 4n - 6m = 2(k - 2n - 3m$
  nombre que és senar;
- $b) \Rightarrow c)$: en aquest cas suposem que $n - 3m$ és senar i volem deduir que n i m tenen diferent paritat; per veure que n i m tenen diferent paritat només caldrà veure que la resta ens dona senar; per tant sabem que per un enter k:
  $n - 3m = 2k + 1 \Rightarrow n - m = n - 3m + 2m = 2k + 1 + 2m = 2(k + m) + 1$
  nombre que és senar;
- $c) \Rightarrow a)$: en aquest cas suposem que n i m tenen diferent paritat i volem deduir que $5n + 3m$ és senar; per tant sabem que per un enter k:
  $n - m = 2k + 1 \Rightarrow 5n + 3m = n - m + 4n + 4m = 2k + 1 + 4n + 4m = 2(k + 2n + 2m) +$
  nombre que també és senar;

Demostració de la unicitat

Quan diem que "si hi ha un x que satisfà $P(x)$ aquest és únic" volem dir que hi ha com a molt un x satisfent $P(x)$. Dit d'una altra manera no hi ha dos x diferents que satisfacin $P(x)$. Aquesta darrera manera de veure-ho es pot expressar així: $\neg\exists x \exists y(x \neq y \wedge P(x) \wedge P(y))$, fórmula que és equivalent a $\forall x, y(P(x) \wedge P(y) \rightarrow x = y)$. Per tant per demostrar una unicitat caldrà:

$P(x), P(y) \Rightarrow \ldots \Rightarrow x = y$

EX.: (97) En una operació $(A, *)$ associativa el neutre, en cas d'existir, és únic.

Suposem que tenim una operació en A que és associativa (per a tot $\in A$, $a * (b * c) = (a * b) * c$) i que tenim un element neutre $n \in A$ (és a dir: per a tot $a \in A$, $a * n = n * a = a$). Ara suposem que tenim un altre element neutre $n \in A$, és a dir que per a tot $a \in A$, $a * n' = n' * a = a$. Observem que:

$$\left.\begin{array}{r} \text{per a tot } a \in A,\ a * n = n * a = a \\ \text{per a tot } a \in A,\ a * n' = n' * a = a \end{array}\right\} \Rightarrow \left.\begin{array}{c} n' * n = n * n' = n' \\ n * n' = n' * n = n \end{array}\right\} \Rightarrow n = n'.$$