TALLER 4.
VERIFICACIÓ FORMAL DE PROGRAMES.

2. Sigui E= {∃i: 0≤i<n:(b[0..n-1]≤b[i])∧(b[i]>b[0..i-1])} Calcula:

   a) $((E)^b_c)^n_w$ b) $((E)^b_c)^i_k$

   a) E = {∃i: 0≤i<n:(b[0..n-1] ≤b[i]) ∧ (b[i] >b[0..i-1])} =
      = {∃i: 0≤i<n:(c[0..n-1] ≤c[i]) ∧ (c[i] >c[0..i-1])} =
      = {∃i: 0≤i<w:(b[0..w-1] ≤b[i]) ∧ (b[i] >b[0..i-1])}

   b) E = {∃i: 0≤i<n:(b[0..n-1] ≤b[i]) ∧ (b[i] >b[0..i-1])} =
      = {∃i: 0≤i<n:(c[0..n-1] ≤c[i]) ∧ (c[i] >c[0..i-1])} =
      no se puede sustituir 'i' porque es una variable ligada

3. Sigui E= {(x<y) ∧ a ∧ (y≤z) ∨ (x ≤ y)}. Calcula:

   a) $(((E)^x_y)^y_4)^z_6$ b) $E^{x,y,z}_{y,4,6}$

   a) E = {(y<y)∧a∧(y≤z)∨(y≤y)} = {(4<4)∧a∧(4≤z)∨(4≤4)} = {(4<4)∧a∧(4≤6)∨(4≤4)} = {F∨(4≤4)} = {4≤4} = T

   b) E = {(y<4)∧a∧(4≤6)∨(y≤4)} = {(y<4)∧a∧T∨(y≤4)} = {(y<4)∧a∨(y≤4)}

5. Demostra la llei de distributivitat de disjunció per un programa no determinista: wp(S, Q) ∨ wp(S, R) => wp(S, Q∨R)

   - Demostración:
     Si tenemos un dados de seis caras, no se puede asegurar que número saldrá en el dado, es decir:

        wp(lanzar, seis) = F y wp(lanzar, cinco) = F … wp(lanzar, uno) = F
        Pero sí que está garantizado que saldrá alguna cara del dado
        wp(lanzar,seis∨...∨uno) = T
        Por lo que
        wp(anzar, seis)∨...∨wp(anzar, uno) => wp(lanzar,seis∨...∨uno)

     P € LHS => p € RHS P € LHS => Q => R => Q ∧ R Q v R v (Q ∧ R) = Q v R

6. Demostra que si un programa S és determinista, llavors:
    $wp(S, Q) \vee wp(S, R) = wp(S, Q \vee R)$

- En wp(S,Q), sabemos que el programa empieza por S y da como resultado seguro Q, en wp(S, R) tenemos que empieza por S y da como resultado R, por lo que podemos extraer que el programa siempre va a empezar por S, y por el enunciado sabemos que debe acabar en Q o en R sí o sí, es decir, el resultado del programa puede ser tanto Q como R, $wp(S,Q \vee R)$. Demostración con ejemplo:
    $wp(S, Q) \vee wp(S, R) = wp(S, Q \vee R)$
    Wp(sortir el sol, si)= T , wp(sortir el sol, No) = F
    Hi ha garantia de que demà sortirà el sol
    S=sortir el sol
    Q=si
    R=no
    Wp(sortir el sol,si)V wp(sortir el sol, no) = wp(sortir el sol, si V no)

7. Demostra la llei de monotonicitat emprant sols la llei de distributivitat de conjunció:
    Si Q => R, llavors wp(S, Q) => wp(S, R)

- Sabemos que si Q implica R, significa que el resultado Q implicará a R entonces wp(S, Q) => wp(S, R). Demostración:
    Si Q->R, llavors wp(S, Q) -> wp(S, R)
    Consideram la part esquerra com a s (LHS):
    Q->R, llavors Q -> R per tant es True
    Consideram la part de la dreta com a s
    Consideram la part de la dreta com a s (RHS):
    Q->R, llavors Q -> R per tant es true

8. Demostra a partir de la llei de distributivitat de conjunció que:
    $wp(S, R) \wedge wp(S, \neg R) = F$

- Sabemos que por una parte S tiene que dar R como resultado, y por la otra parte dice lo contrario, que no debe dar R. Por lo que: $wp(S, R) \wedge wp(S, \neg R) = wp(S, R \wedge \neg R) = wp(S,F) = F$, ya que, por la ley de contradicción $R \wedge \neg R = F$. Demostración:
    $wp(S, R) \wedge wp(S, \neg R) = F$
    $wp(S, R \wedge \neg R) = wp(S,R) \wedge wp(S, \neg R)$
    $wp(S, R \wedge \neg R) = F$
    Consideram la part de la esquerra com a s:
    $R \wedge \neg R = F$ se cumple la condición de contradicción.

10. És correcta la següent especificació?. $\{Q: x<3 \wedge y=0\}$ x:=6; y:=x+1 $\{R: x>3 \wedge y>x\}$ Demostra formalment la resposta.

- Primero se calcula wp(S,R):
    $wp(S,R) = wp(S1;S2,R) = wp(x=6; y = x+1, x>3 \wedge y>x) =$
    $= wp(x = 6, wp(y = x +1, x>3 \wedge y>x)) =$
    $= wp(x = 6, (x>3 \wedge y>x)^{y}_{x+1}) =$
    $= wp(x = 6, (x>3 \wedge x+1>x)) =$

$= (x>3 \wedge x+1>x)^x_6 = 6>3 \wedge 6+1>6 = T \wedge T = T$

- Segundo [Q=> wp(S,R)]=T
  Q => wp(S1;S2,R)
  [Q => T] = T
  [Q => T] = ¬Q v T = T

11.Calcula wp(x:=K; y:=M, {R: x > y}), on K i M són dues constants.

wp(S1;S2,R) = wp(x=K, wp(y=M, x>y)) =
$= wp(x=K,(x>y)^y_M) =$
= wp(x=K, (x>M)) =
$= wp(x=K, (x>M)^x_K) = K>M$

12.Demostra formalment que les dues especificacions següents són correctes:
a. {T} x:=X; y:=Y; x:=y {R: x=y}

- Es T, ya que el resultado del problema x=y es verdadera, y en el programa se asigna x:=y, por lo que x e y valen lo mismo.

b. {x > y} x:=X; y:=Y; x:=y {R: x=y} on X, Y són dues constants.

- Será T, siempre y cuando x sea > que y, ya que luego se cumplirá la asignación de x:=y.

13.És vàlida la següent especificació: {F} S {R} ? Cóm interpretes el resultat?

14.Sigui S: x:=y. Demostra que {y=Y} S {x=Y} és una especificació vàlida, és a dir, és una tautologia.

15.Calcula $wp(t:=x; x:=y; y:=t, x=X \wedge y=Y)$.

$wp(S1;S2;S3,R) = wp(t:=x; x:=y; y:=t, x=X \wedge y=Y) =$
$= wp(t:=x; x:=y, wp(y:=t, x=X \wedge y=Y)) =$
$= wp(t:=x; x:=y, (x=X \wedge y=Y)^y_t) =$
$= wp(t:=x; x:=y,(x=X \wedge t=Y)) =$
$= wp(t:=x, wp(x:=y,(x=X \wedge t=Y))) =$
$= wp(t:=x,(x=X \wedge t=Y)^x_y) =$
$= wp(t:=x, y=X \wedge t=Y) = (y=X \wedge t=Y)^t_x = (y=X \wedge x=Y)$

16.A en Joan li donen una quantitat de doblers X, deriva formalment emprant el wp quína quantitat de doblers hem de donar a na Lluisa per què tengui les tres quartes parts de doblers que li han donat a en Joan.

S1: Joan = X
S2: Lluisa = Y

{R: Lluisa = ¾ Joan}

wp(S1;S2,R) = wp(S1;wp(S2,R)) =
= wp(Joan = x; wp(Lluisa = y, Lluisa = ¾ Joan)) =
= wp(Joan = x; $(\text{Lluisa} = ¾\ \text{Joan})^{\text{Lluisa}}_{y}$) =
= wp(Joan = x, y = ¾ Joan) =
= $(y = ¾\ \text{Joan})^{\text{Joan}}_{x}$
y = ¾* X

17.En Joan té inicialment una certa quantitat de doblers i na Lluisa en té la meitat que en Joan. Si posteriorment a en Joan li donen una determinada quantitat de doblers, deriva formalment la quantitat de doblers que hauran de donar a na Lluisa per què finalment tengui les tres quartes parts dels doblers que té en Joan.

S1: Joan = x + α
S2: Lluisa = x/2 + β
{R: Lluisa = ¾ Joan}
wp(S1;S2,R) = wp(S1; wp(S2,R)) =
= wp(Joan = x + α; wp(Lluisa= x/2 + β, Lluisa = ¾ Joan)) =
= wp(Joan = x + α; $(\text{Lluisa} = ¾\ \text{Joan})^{\text{Lluisa}}_{x/2+\beta}$) =
= wp(Joan = x + α, x/2 + β= ¾ Joan) =
= $(x/2 + \beta = ¾\ \text{Joan})^{\text{Joan}}_{x+\alpha}$=
= x/2 + β= ¾ * (x + α)
β = ¼ *x + ¾ * α

21.Demostra pas a pas que la següent definició referent a la comanda composta: wp(S1;S2, R) = wp(S1, wp(S2,R)) satisfà les lleis del miracle exclòs i la distributivitat de conjunció.
wp(S1;S2, R) =

22.Construeix un programa, S, que calculi el major de dos nombres naturals x, y, i guardi el resultat en una variable z, i fes un esquema de demostració del mateix.

{Q} S {R}

	{x=X, y=Y}
if x≥y then	{x=X; y=Y ∧ x≥y}
z:=x	{z=X; y=Y ∧ x≥y}
else	{x=X; y=Y ∧ y≥x}
z:=y	{x=X; z=Y ∧ y≥x}

{R: z = max(x,y)}

23.Verifica formalment el programa de la qüestió anterior.
wp(S1;S2,R) = wp(x=X; y=Y, z = max(x,y)) =

24.Calcula i simplifica al màxim: wp(S, x≤y), on S:
if x>y → x, y:=y, x
x≤y → skip
fi

$wp(if, R) = BB \wedge [(B1 \rightarrow wp(S1,R)) \wedge (B2 \rightarrow wp(S2,R))] =$

$= [(x>y) \vee (x \le y)] \wedge [((x>y) \rightarrow wp(x, y:=y, x, y \ge x)) \wedge ((x \le y) \rightarrow wp(skip, y \ge x))] =$

$= T \wedge [((x>y) \rightarrow (y \ge x)) \wedge ((x \le y) \rightarrow (y \ge x))] = T \wedge T \wedge T = T$

26.Demostra formalment, pas a pas, la validesa de la següent especificació:

```
{a, b>0}
if (a≥b) ∧ (b=1) → z:=a;
  (a<b) ∧ (a=1) → z:=b;
  (a≥b) ∧ (b≠1) → z:=a*b;
  (a<b) ∧ (a≠1) → z:=a*b;
fi
{R: z=a*b}
```

$wp(IF,R)=BB \wedge [(B1 \rightarrow wp(S1,R)) \wedge (B2 \rightarrow wp(S2,R)) \wedge (B3 \rightarrow wp(S3,R)) \wedge (B4 \rightarrow wp(S4,R))]=$

$= [a \ge b \vee a<b] \wedge [\{(a \ge b \wedge b=1) \rightarrow wp(z:=a, z=a*b)\} \wedge \{(a<b \wedge a=1) \rightarrow wp(z:=b, z=a*b)\} \wedge$

$\wedge \{(a \ge b \wedge b \ne 1) \rightarrow wp(z:=a*b, z=a*b)\} \wedge \{(a<b \wedge a \ne 1) \rightarrow wp(z:=a*b, z=a*b)\}] =$

$= T \wedge [\{(a \ge b \wedge b=1) \rightarrow (z=a*b)^z_a\} \wedge \{(a<b \wedge a=1) \rightarrow (z=a*b)^z_b\} \wedge \{(a \ge b \wedge b \ne 1) \rightarrow (z=a*b)^z_{a*b}\} \wedge$

$\wedge \{(a<b \wedge a \ne 1) \rightarrow (z=a*b)^z_{a*b}\}] =$

$= T \wedge [\{(a \ge b \wedge b=1) \rightarrow (a=a*b)\} \wedge \{(a<b \wedge a=1) \rightarrow (b=a*b)\} \wedge \{(a \ge b \wedge b \ne 1) \rightarrow (a*b=a*b)\} \wedge$

$\wedge \{(a<b \wedge a \ne 1) \rightarrow (a*b=a*b)\}] =$

$= T \wedge [(a=a*1) \wedge (b=1*b) \wedge (a*b=a*b) \wedge (a*b=a*b)] = T \wedge T \wedge T \wedge T \wedge T = T$

27.Calcula wp(IF, R) del següent programa:

```
if x≥0 → z:=x
  x<0 → z:=-x
fi
{R: z=abs(x)}
```

$wp(IF,R) = BB \wedge [(B1 \rightarrow wp(S1,R)) \wedge (B2 \rightarrow wp(S2,R))] =$

$= [(x \ge 0) \vee (x<0)] \wedge [(x \ge 0 \rightarrow wp(z:=x, z=abs(x))) \wedge (x<0 \rightarrow wp(z:=-x, z=abs(x)))] =$

$= T \wedge [(x \ge 0 \rightarrow (z=abs(x))^z_x) \wedge (x<0 \rightarrow (z=abs(x))^z_{-x})] =$

$= [(x \ge 0 \rightarrow x=abs(x)) \wedge (x<0 \rightarrow -x=abs(x))] = T \wedge T = T$