FEBBRAIO 2017 d

$\{p = M, M \geq 0, b > 0\}$

```
q := 0;
WHILE b ≤ p DO
    q := q+1
    p := p-b
ENDWHILE
```

A, C, W, P

$\{M - qb = p, p < b\}$

RICERCA DELL'INVARIANTE

q	0	1	2	3	4
p	M	M-3	M-(2·3)	M-(3·3)	M-(4·3)
b	3	3	3	3	3

$p = M - qb$

$? \{p = M - qb \wedge b \leq p\} C \{p = M - qb\}$

$\vdash_{AIS} \{p - b = M - (q-1)b\} C \{inv\}$

$p - b = M - qb - b$

$\vdash \{p = M - qb\} C \{inv\}$

$p - b = M - pb \wedge b \leq p \rightarrow p = M - qb$

$\vdash_{IMPL} \{p = M - qb \wedge b \leq p\} C \{p = M - qb\}$

inv. = dimostrata

$\vdash_{ITER} \{inv\}\ W\ \{inv \wedge b > p\}$

$\vdash_{ASS} \{p = M \wedge b \leq p\}\ A\ \{inv\}$

CORRETTEZZA PARZIALE DIMOSTRATA

SCELGO $p \geq 0$ COME INVARIANTE E p COME VARIANTE

$? \{p \geq 0 \wedge b \leq p \wedge p = E_0\} \subset \{p \geq 0 \wedge p < E_0\}$

$\vdash_{ASS} \{p - b \geq 0 \wedge p - b < E_0\} \subset \{$ $\}$

$p \geq 0 \wedge b \leq p \wedge p = E_0 \rightarrow p - b \geq 0 \wedge p - b < E_0$

$\vdash_{IMPL} \{p \geq 0 \wedge b \leq p \wedge p = E_0\} \subset \{p \geq 0 \wedge p < E_0\}$

CORR. TOT. DIMOSTRATA

FEBBRAIO 2017 6

$\{p \geq 0, q > 0\}$

$b = 0$ (A)
$r = p$
WHILE $q \leq r$ DO (W)
  $r = r - q$ (C)
  $b = b + 1$
ENDWHILE (P)

$\{p = bq + r, r < q\}$

r	p	p-q	p-2q	p-3q
b	0	1	2	3
p	10	10	10	10
q	3	3	3	3

$r = p - bq$

$p = bq + r$

? $\{p = bq + r \wedge q \leq r\} \subset \{p = bq + r\}$

$\xleftarrow{ASS} \{p = (b+1)q + r - q\} \subset \{p = bq + r\}$

$p = bq + r \wedge q \leq r \rightarrow p = bq + r$

$\xleftarrow{IMPL} \{p = bq + r \wedge q \leq r\} \subset \{INV\}$

INVARIANTE DIMOSTRATA

$\vdash \{p = bq + r\}\ W\ \{p = bq + r \wedge q > r\}$

$? \{p \geq 0, q > 0\}\ A\ \{p = bq + r\}$

$\vdash^{AS} \{p = q + p\}$

BOH

CORRETTEZZA TOTALE

INVARIANTE $r \geq 0$ VARIANTE r

$? \{r \geq 0 \wedge q \leq r \wedge r = E_0\}\ C\ \{r \geq 0 \wedge r < E_0\}$

$\vdash^{AS} \{r - q \geq 0 \wedge r - q < E_0\}\ C\ \{\ \ldots\ \}$

$\{\sim\} \rightarrow \{\sim\}$

$\vdash^{IND} \ldots$

TOTALE DIMOSTRATA

SETTEMBRE 2016

$\{M>0,\ u>0\}$

$y = M$
$x = u$
WHILE $(x>0)$ DO
$y = y \cdot 2$
$x = x - 1$
ENDWHILE

$\{y = M 2^u\}$

x	4	3	2	1	0
y	3	$3\cdot 2$	$3\cdot 2^2$	$3\cdot 2^3$	$3\cdot 2^4$
u	4	4	4	4	4
M	3	3	3	3	3

INV $y = M 2^{(u-x)}$

? $\{y = M 2^{(u-x)} \wedge x>0\}$ C $\{y = M 2^u\}$

ASS $\{2y = M 2^{u-x-1}\}$

SETTEMBRE 2021

```
x:=1; h:=1        A
WHILE h<N DO
   x:= 2*x+1;     C
   h:=h+1         WP
ENDWHILE
```

$?\{N>0\}\ P\ \{x=2^N-1\}$

x	1	3	7	15	31
h	1	2	3	4	5
N	S	S	S	S	S

inv. $x=2^h-1 \wedge h\leq N$

$?\{x=2^h-1 \wedge h\leq N \wedge h<N\} \subset \{x=2^h-1 \wedge h\leq N\}$

$\overset{\text{ASS SEQ.}}{\{2x+1=2^{h+1}-1 \wedge h+1\leq N\}} \subset \{inv\}$

$2x = 2^h\cdot 2-2 \wedge h<N$

$x=2^h-1 \wedge h<N$

$\vdash \{x=2^h-1 \wedge h<N\} \subset \{inv\}$

$x=2^h-1 \wedge h\leq N \wedge h<N \rightarrow x=2^h-1 \wedge h<N$

$\overset{\text{IMPL.}}{\{x=2^h-1 \wedge h\leq N \wedge h<N\}} \subset \{inv\}$

INVARIANTE DIMOSTRATA

$\vdash^{\text{TERM.}} \{inv\} \; W \; \{x = 2^h - 1 \wedge h \leq N \wedge h \geq N\}$

$\vdash \{inv\} \; W \; \{x = 2^h - 1 \wedge h = N\}$

$\vdash \{inv\} \; W \; \{x = 2^N - 1\}$

POSTCONDIZIONE DIMOSTRATA

$\vdash^{\text{ASS}} \{1 = 2^1 - 1 \wedge 1 < N\} \; C \; \{inv\}$

$N > 0 \rightarrow N > 1$

$\vdash^{\text{IMPL. SEQ.}} \{N > 0\} \; P \; \{x = 2^N - 1\}$

CORRETTEZZA PARZIALE DIMOSTRATA

VARIANTE: $N - h$ NUOVA INVARIANTE: $N > 0 \wedge N - h \geq 0$

$? \{N > 0 \wedge h < N \wedge N - h = E_0 \wedge N - h \geq 0\} \; C \; \{N > 0 \wedge N - h < E_0 \wedge N - h \geq 0\}$

$\vdash^{\text{ASS}} \{N > 0 \wedge N - (h+1) < E_0 \wedge N - (h+1) \geq 0\} \; C \; \{\dots ?\}$

$N > 0 \wedge h < N \wedge N - h \geq 0 \wedge N - h = E_0 \rightarrow N > 0 \wedge N > h \wedge N - h - 1 < E_0$

$\vdash^{\text{IMPL}} \{N > 0 \wedge h < N \wedge N > h \geq 0 \wedge N - h = E_0\} \; C \; \{\dots\}$

CORRETTEZZA TOTALE DIMOSTRATA

Luglio 2016

$\{k \geq 0\}$

$x := a; n := 0;$ A

while $(n < k)$ do

$x := a + b \cdot x;$ C

$n := n + 1$ P

end while

$\{x = a \sum_{i=0}^{k} b^i\}$

a	2	2	2	2	2
x	2	8	26	80	242
n	0	1	2	3	4
b	3	3	3	3	3
k	4	4	4	4	4

inv: $x = a \sum_{i=0}^{n} b^i \wedge n \leq k$

$? \vdash \{x = a \sum_{i=0}^{n} b^i \wedge n \leq k \wedge n < k\}\ C\ \{inv\}$

[ASS] $\vdash \{a + b \cdot x = a \sum_{i=0}^{n+1} b^i \wedge n+1 \leq k\}\ C\ \{inv\}$

$\rightarrow$

[IMPL] $\vdash \{x = a \sum_{i=0}^{n} b^i \wedge n \leq k \wedge n < k\}\ C\ \{inv\}$

INV dimostrata

[ITER] $\vdash \{inv\}\ W\ \{x = a \sum_{i=0}^{n} b^i \wedge n \leq k \wedge n \geq k\}$

$\vdash \{inv\}\ W\ \{x = a \sum_{i=0}^{k} b^i\}$

$\vdash^{ASS} \{ a = a \sum_{i=0}^{0} b^i \wedge 0 \leq k \} A \{ inv \}$

$\vdash \{ a = a \wedge k \geq 0 \} A \{ inv \}$

$\vdash^{SEQ} \{ k \geq 0 \} P \{ x = a \sum_{i=0}^{k} b^i \}$

CORRETTEZZA PARZIALE DIMOSTRATA

VARIANTE: $k - n$ INVARIANTE $k - n \geq 0$

$k - n \geq 0 \rightarrow k - n \geq 0$ ✓

$? \{ k - n \geq 0 \wedge n < k \wedge k - n = E_0 \} C \{ inv \wedge k - n < E_0 \}$

$\vdash^{ASS} \{ k - (n+1) \geq 0 \wedge k - (n+1) < E_0 \} C \{ \quad \}$

$\vdash \{ k - n > 0 \wedge k - n - 1 < E_0 \} C \{ \quad \}$

$k - n \geq 0 \wedge n < k \wedge k - n = E_0 \rightarrow$

$\vdash^{IMPL} \{ k - n \geq 0 \wedge n < k \wedge k - n = E_0 \} C \{ \quad \}$

CORRETTEZZA TOTALE DIMOSTRATA

SETTEMBRE 2022

```
z = N; x = M        A
WHILE z > 0 DO
    x = 2 · x       C   W   P
    z = z - 1
ENDWHILE
```

$? \{N \geq 0\} P \{x = 2^N \cdot M\}$

x	3	6	12	24	48
z	4	3	2	1	0
N	4	4	4	4	4
M	3	3	3	3	3

INV: $x = 2^{N-z} \cdot M \wedge z \geq 0$

$? \{x = 2^{N-z} \cdot M \wedge z \geq 0 \wedge z > 0\} C \{INV\}$

ASS SEQ $\{x = 2^{N-(z-1)} \cdot M \wedge z - 1 \geq 0 \wedge z - 1 > 0\} C \{INV\}$

$\vdash \{x = 2^{N-z} \cdot M \wedge z \geq 1 \wedge z > 1\} C \{INV\}$

$x = 2^{N-z} \cdot M \wedge z \geq 0 \wedge z > 0 \rightarrow x = 2^{N-z} \cdot M \wedge z \geq 1 \wedge z > 1$

IMPL $\vdash \{x = 2^{N-z} \cdot M \wedge z \geq 0 \wedge z > 0\} C \{INV\}$

INVARIANTE DIMOSTRATA

ITM $\vdash \{x = 2^{N-z} \cdot M \wedge z \geq 0\} W \{x = 2^{N-z} \cdot M \wedge z \geq 0 \wedge z \leq 0\}$

$\rightarrow z = 0$

$\vdash \{INV\} W \{x = 2^N \cdot M\}$

UGUALE ALLA POST CONDIZIONE OBIETTIVO

$\vdash_{ASS} \{M = 2^{N-N} \cdot M \wedge N \geq 0\}\ A\ \{inv\}$

$\vdash_{SEQ} \{N \geq 0\}\ P\ \{x = 2^N \cdot M\}$

CORRETTEZZA PARZIALE DIMOSTRATA

VARIANTE z INVARIANTE $z \geq 0$

$?\ \{z \geq 0 \wedge z > 0 \wedge z = E_0\}\ C\ \{z \geq 0 \wedge z < E_0\}$

$\vdash_{ASS} \{z - 1 \geq 0 \wedge z - 1 < E_0\}$

$z \geq 0 \wedge z > 0 \wedge z E_0 \rightarrow z > 0 \wedge z - 1 < E_0$

$\vdash_{IMPL} \{z \geq 0 \wedge z > 0 \wedge z E_0\}\ C\ \{z \geq 0 \wedge z < E_0\}$

CORRETTEZZA TOTALE DIMOSTRATA

MARZO 2016

$\{ y = k \wedge k > 0 \}$

$z = 0;\ x = 0;$ A

WHILE $(y > 0)$ DO

$x = 2 \cdot z + x + 1$ B

$z = z + 1$ C

$y = y - 1$ D

ENDWHILE W

P

$\{ x = k^2 \}$

X	0	1	4	9
Y	3	2	1	0
z	0	1	2	3
k	3	3	3	3

INV: $x = z^2 \wedge z = k - y \wedge y \geq 0$

$? \{ x = z^2 \wedge z = k - y \wedge y \geq 0 \wedge y > 0 \} C \{ INV \}$

ASS SEQ $\{ x = (z+1)^2 \wedge z + 1 = k - (y-1) \wedge y - 1 \geq 0 \} D \{ \}$

ASS SEQ $\{ 2 \cdot z + x + 1 = (z+1)^2 \wedge z + 1 = k - y + 1 \wedge y - 1 \geq 0 \} (\{ INV \}$

$2z + x + 1 = z^2 + 2z + 1$ $\qquad$ $y > 0$

$\vdash \{ x = z^2 \wedge z = k - y \wedge y > 0 \} C \{ INV \}$

$x = z^2 \wedge z = k - y \wedge y \geq 0 \wedge y > 0 \rightarrow \ldots$

IMPL $\{ x = z^2 \wedge z = k - y \wedge y \geq 0 \wedge y > 0 \} C \{ INV \}$

INVARIANTE DIMOSTRATA

ITER $\{ INV \} W \{ x = z^2 \wedge z = k - y \wedge y \geq 0 \wedge y \leq 0 \}$

$z = k \quad \leftarrow \quad y = 0$

$\vdash \{ INV \} W \{ x = k^2 \}$

UGUALE ALLA POSTCONDIZIONE OBIETTIVO

$$\frac{\text{ASS}}{\text{SEQ}} \quad \{0=0^2 \wedge 0=k-y \wedge y>0\}\ A\ \{inv\}$$

$$\vdash \{k=y \wedge y>0\}\ A\ \{inv\}$$

$$y=k \wedge k>0 \rightarrow k=y \wedge y>0$$

$$\frac{\text{IMPL}}{\text{SEQ}} \quad \{y=k \wedge k>0\}\ P\ \{x=k^2\}$$

CORRETTEZZA PARZIALE DIMOSTRATA

inv $y \geq 0$ VAR y inv $\rightarrow y \geq 0$

$$? \{y \geq 0 \wedge y>0 \wedge y=E_0\} C \{y \geq 0 \wedge y<E_0\}$$

$$\frac{\text{ASS}}{} \{y-1 \geq 0 \wedge y-1<E_0\} C \{ \quad \downarrow \quad \}$$

$$y \geq 0 \wedge y>0 \wedge y=E_0 \rightarrow y>0 \wedge y-1<E_0$$

$$\frac{\text{IMPL}}{} \{y \geq 0 \wedge y>0 \wedge y=E_0\} C \{y \geq 0 \wedge y<E_0\}$$

CORRETTEZZA TOTALE DIMOSTRATA

$\{M>0\}$

$s:=1 \quad i:=0$ A

WHILE $i<M$ DO W

$s:=5\cdot s$ C

$i:=i+1$

ENDWHILE P

$\{s=5^M\}$

s	1	5	25	125
i	0	1	2	3
M	3	3	3	3

INVARIANTE:

$s=5^i \wedge i \leq M$

$\{s=5^i \wedge i<M\}\ C\ \{s=5^i\}$

$\vdash_{\text{ASS SEQ}} \{s\cdot 5 = 5^{i+1}\}\ C\ \{inv\}$

$\vdash \{s=5^i\}\ C\ \{inv\}$

INVARIANTE DIMOSTRATA

$\vdash_{\text{ITER}} \{inv\}\ W\ \{s=5^i \wedge i \leq M \wedge i \geq M\}$

$\vdash \{inv\}\ W\ \{s=5^M\}$

POST CONDIZIONE OBIETTIVO DIMOSTRATA

$\vdash_{\text{ASS}} \{1=5^0 \wedge 0 \leq M\}\ A\ \{inv\}$

$M>0 \rightarrow M \geq 0$

$\vdash_{\substack{\text{INAL}\\ \text{SEQ}}} \{M>0\}\ P\ \{s=5^M\}$

CORRETTEZZA PARZIALE DIMOSTRATA

$E : M_{-i}$ $I : M_{-i} \geq 0$

$? \{ M_{-1} \geq 0 \wedge i < M \wedge M_{-i} = E_0 \} \subset \{ i \in \mathbb{N} \wedge E < E_0 \}$

$\overset{\text{INV}}{\vdash} \{ M_{-i-1} \geq 0 \wedge M_{-i-1} < E_0 \} \subset \{ \quad * \}$

$M_{-1} \geq 0 \wedge i < M \wedge M_{-i} = E_0 \rightarrow M_{-i} > 0 \wedge M_{-i-1} < E_0$

$\overset{\text{impl}}{\vdash} \{ M_{-1} \geq 0 \wedge i < M \wedge M_{-i} = E_0 \} \subset \{ i \in \mathbb{N} \wedge E < E_0 \}$