162 (cube) Write a program that cubes using only addition, subtraction, and test for zero.

After trying the question, scroll down to the solution.

§ Let n be a natural constant, and let x be a natural variable. Then

$$x'=n^3 \ \Leftarrow\ x{:=}\ n.\ x'=x\times n.\ x'=x\times n$$

Proof:

$x{:=}\ n.\ x'=x\times n.\ x'=x\times n$ — definition of sequential composition

$=\ x{:=}\ n.\ \exists x''\cdot\ x''=x\times n \wedge x'=x''\times n$ — one-point

$=\ x{:=}\ n.\ x'=x\times n\times n$ — substitution law

$=\ x'=n\times n\times n$ — arithmetic

$=\ x'=n^3$

Now we have only one specification to refine, namely $x'=x\times n$, and it's a multiplication, which is easier than cubing. We'll have to use repeated addition, so we have to start x at 0 , and then keep adding n . How many times do we add n ? We add it x times, but that's x before we initialized it to 0 . So we have to save the value of x before we initialize it to 0 , and we introduce natural variable y for that.

$$x'=x\times n \ \Leftarrow\ y{:=}\ x.\ x{:=}\ 0.\ x' = x + y\times n$$

The last part $x' = x + y\times n$ says the final value x' is the sum so far, that's x , plus y more values of n .

Proof:

$y{:=}\ x.\ x{:=}\ 0.\ x' = x + y\times n$ — substitution law

$=\ y{:=}\ x.\ x' = 0 + y\times n$ — simplify, then substitution law

$=\ x' = x\times n$

Now the last refinement is straightforward.

$$x' = x + y\times n \ \Leftarrow\ \textbf{if } y{=}0 \textbf{ then } ok \textbf{ else } x{:=}\ x{+}n.\ y{:=}\ y{-}1.\ x' = x + y\times n \textbf{ fi}$$

Proof:

$\textbf{if } y{=}0 \textbf{ then } ok \textbf{ else } x{:=}\ x{+}n.\ y{:=}\ y{-}1.\ x' = x + y\times n \textbf{ fi}$ — expand ok , substitution twice

$=\ \textbf{if } y{=}0 \textbf{ then } x'=x \wedge y'=y \textbf{ else } x' = x + n + (y{-}1)\times n \textbf{ fi}$ — context, simplify

$=\ \textbf{if } y{=}0 \textbf{ then } x' = x + y\times n \wedge y'=y \textbf{ else } x' = x + y\times n \textbf{ fi}$ — monotonicity

$\Rightarrow\ \textbf{if } y{=}0 \textbf{ then } x' = x + y\times n \textbf{ else } x' = x + y\times n \textbf{ fi}$ — case idempotent

$=\ x' = x + y\times n$

Adding recursive time, we need to put $t{:=}\ t{+}1$ just before the recursive call. Since t goes up 1 just when y goes down 1 , we see that the time must be y . So that last refinement becomes

$$x' = x + y\times n \wedge t'=t{+}y \ \Leftarrow$$
$$\textbf{if } y{=}0 \textbf{ then } ok \textbf{ else } x{:=}\ x{+}n.\ y{:=}\ y{-}1.\ t{:=}\ t{+}1.\ x' = x + y\times n \wedge t'=t{+}y \textbf{ fi}$$

We recalculate the refinement of $x'=x\times n$ with timing, and we find

$y{:=}\ x.\ x{:=}\ 0.\ x' = x + y\times n \wedge t'=t{+}y$

$=\ x'=x\times n \wedge t'=t{+}x$

We recalculate the refinement of $x'=n^3$ with timing, and we find

$x{:=}\ n.\ x'=x\times n \wedge t'=t{+}x.\ x'=x\times n \wedge t'=t{+}x$

$=\ x'=n^3 \wedge t'=t{+}n^2{+}n$

We have calculated the timing for the solution to be $n^2{+}n$, which wasn't obvious.

Here's a linear solution in which n is a natural variable. We can try to find n^3 in terms of $(n{-}1)^3$. We find

$$n^3 \ =\ (n{-}1)^3 + 3\times n^2 - 3\times n + 1$$

The problem is the occurrence of n^2 . But maybe we can find it the same way, in terms of $(n{-}1)^2$ using the identity

$$n^2 \ =\ (n{-}1)^2 + 2\times n - 1$$

So we need a variable x for the cubes and a variable y for the squares.

$x'=n^3 \Leftarrow x'=n^3 \land y'=n^2$
$x'=n^3 \land y'=n^2 \Leftarrow$
if $n=0$ **then** $x:= 0.\ y:= 0$ **else** $n:= n-1.\ x'=n^3 \land y'=n^2$.

We cannot complete that refinement due to a little problem: in order to get the new values of x and y, we need not only the values of x and y just produced by the recursive call, but also the original value of n, which was not saved. So we revise.

$x'=n^3 \Leftarrow x'=n^3 \land y'=n^2 \land n'=n$
$x'=n^3 \land y'=n^2 \land n'=n \Leftarrow$
if $n=0$ **then** $x:= 0.\ y:= 0$
else $n:= n-1.\ x'=n^3 \land y'=n^2 \land n'=n.\ n:= n+1.$
$y:= y + n + n - 1.\ x:= x + y + y + y - n - n - n + 1$ **fi**

After we decrease n, the recursive call promises to leave it alone, and then we increase it back to its original value, which fulfills the promise. With recursive time,

$x'=n^3 \land t'=t+n \Leftarrow x'=n^3 \land y'=n^2 \land n'=n \land t'=t+n$
$x'=n^3 \land y'=n^2 \land n'=n \land t'=t+n \Leftarrow$
if $n=0$ **then** $x:= 0.\ y:= 0$
else $n:= n-1.\ t:= t+1.\ x'=n^3 \land y'=n^2 \land n'=n \land t'=t+n.\ n:= n+1.$
$y:= y + n + n - 1.\ x:= x + y + y + y - n - n - n + 1$ **fi**

The proof is easier if we express the specifications in program form:

$x:= n^3.\ t:= t+n \Leftarrow x:= n^3.\ y:= n^2.\ t:= t+n$
$x:= n^3.\ y:= n^2.\ t:= t+n \Leftarrow$
if $n=0$ **then** $x:= 0.\ y:= 0$
else $n:= n-1.\ t:= t+1.\ x:= n^3.\ y:= n^2.\ t:= t+n.\ n:= n+1.$
$y:= y + n + n - 1.\ x:= x + y + y + y - n - n - n + 1$ **fi**

Now we can use the substitution law more.

Here's another linear solution. It is similar to the previous solution, calculating n^3 from $(n-1)^3$. The recursion in the previous solution requires a stack implementation; the recursion in this solution does not require a stack implementation. This solution uses a backward-looking specification. Let n be a natural constant, and let x be a natural variable. The result we want is

$R = x'=n^3 \land t'=t+n$

We want that result by a sequence of additions to x. Let k be a natural variable that counts up from 0 to n. Define

$Q = x=k^3 \Rightarrow x'=n^3 \land t' = t+n-k$

to say that, in the middle of the computation, we have already computed $x=k^3$, and we need to finish computing $x'=n^3$ in time $n-k$. Then

$R \Leftarrow k:= 0.\ x:= 0.\ Q$
$Q \Leftarrow$ **if** $k=n$ **then** ok **else** $x:= x+y.\ k:= k+1.\ t:= t+1.\ Q$ **fi**

where y is a value yet to be determined. The proof of the R refinement is two uses of the substitution law. The proof of the Q refinement is two cases. The first case $k=n$ is easy. The other case $k<n$ is

$Q \Leftarrow k<n \land (x:= x+y.\ k:= k+1.\ t:= t+1.\ Q)$ expand second Q

$= Q \Leftarrow k<n \land (x:= x+y.\ k:= k+1.\ t:= t+1.\ x=k^3 \Rightarrow x'=n^3 \land t' = t+n-k)$
substitution 3 times

$= Q \Leftarrow k<n \land (x+y=(k+1)^3 \Rightarrow x'=n^3 \land t' = t+1+n-(k+1))$ simplify

$= Q \Leftarrow k<n \land (x+y = k^3 + 3\times k^2 + 3\times k + 1 \Rightarrow x'=n^3 \land t' = t+n-k)$
mirror and expand Q

$= k<n \land (x+y = k^3 + 3\times k^2 + 3\times k + 1 \Rightarrow x'=n^3 \land t' = t+n-k)$
$\Rightarrow (x=k^3 \Rightarrow x'=n^3 \land t' = t+n-k)$
If we somehow had $y = 3\times k^2 + 3\times k + 1$, then by specialization

$= \top$

So we see what y has to be. Let's just give it to ourselves by modifying Q .

$$Q \;=\; x{=}k^3 \;\land\; y = 3{\times}k^2 + 3{\times}k + 1 \;\;\Rightarrow\;\; x'{=}n^3 \;\land\; t' = t{+}n{-}k$$

Now we need to modify our refinements to initialize and update natural variable y .

$$R \;\Leftarrow\; k{:=}\,0.\;\; x{:=}\,0.\;\; y{:=}\,1.\;\; Q$$

$$Q \;\Leftarrow\; \textbf{if } k{=}n \textbf{ then } ok \textbf{ else } x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; k{:=}\,k{+}1.\;\; t{:=}\,t{+}1.\;\; Q \textbf{ fi}$$

where z is a value yet to be determined. The proof of the R refinement is three uses of the substitution law. The proof of the Q refinement is two cases. The first case $k{=}n$ is easy. The other case $k{<}n$ is

$$\begin{aligned}
& Q \;\Leftarrow\; k{<}n \;\land\; (x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; k{:=}\,k{+}1.\;\; t{:=}\,t{+}1.\;\; Q) && \text{expand second } Q\\
= \;& Q \;\Leftarrow\; k{<}n \;\land\; (x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; k{:=}\,k{+}1.\;\; t{:=}\,t{+}1.\\
& \qquad x{=}k^3 \;\land\; y = 3{\times}k^2 + 3{\times}k + 1 \;\;\Rightarrow\;\; x'{=}n^3 \;\land\; t' = t{+}n{-}k)\\
& && \text{substitution 4 times}\\
= \;& Q \;\Leftarrow\; k{<}n \;\land\; (\quad x{+}y{=}(k{+}1)^3 \;\land\; y{+}z = 3{\times}(k{+}1)^2 + 3{\times}(k{+}1) + 1\\
& \qquad \Rightarrow\; x'{=}n^3 \;\land\; t' = t{+}1{+}n{-}(k{+}1)) && \text{simplify}\\
= \;& Q \;\Leftarrow\; k{<}n \;\land\; (\quad x{+}y = k^3 + 3{\times}k^2 + 3{\times}k + 1 \;\land\; y{+}z = 3{\times}k^2 + 9{\times}k + 7\\
& \qquad \Rightarrow\; x'{=}n^3 \;\land\; t' = t{+}n{-}k) && \text{mirror and expand } Q\\
= \;& \quad k{<}n \land (x{+}y = k^3 + 3{\times}k^2 + 3{\times}k + 1 \land y{+}z = 3{\times}k^2 + 9{\times}k + 7 \Rightarrow x'{=}n^3 \land t' = t{+}n{-}k)\\
& \Rightarrow\; (x{=}k^3 \;\land\; y = 3{\times}k^2 + 3{\times}k + 1 \;\;\Rightarrow\;\; x'{=}n^3 \;\land\; t' = t{+}n{-}k)\\
& && \text{If we somehow had } z = 6{\times}k + 6 \text{ , then by specialization}\\
= \;& \top
\end{aligned}$$

So we see what z has to be. Let's just give it to ourselves by modifying Q .

$$Q \;=\; x{=}k^3 \;\land\; y = 3{\times}k^2 + 3{\times}k + 1 \;\land\; z = 6{\times}k + 6 \;\;\Rightarrow\;\; x'{=}n^3 \;\land\; t' = t{+}n{-}k$$

Now we need to modify our refinements to initialize and update natural variable z .

$$R \;\Leftarrow\; k{:=}\,n.\;\; x{:=}\,0.\;\; y{:=}\,1.\;\; z{:=}\,6.\;\; Q$$

$$Q \;\Leftarrow\; \textbf{if } k{=}0 \textbf{ then } ok \textbf{ else } x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; z{:=}\,z{+}w.\;\; k{:=}\,k{-}1.\;\; t{:=}\,t{+}1.\;\; Q \textbf{ fi}$$

where w is a value yet to be determined. The second case $k{<}n$ of the Q refinement is

$$\begin{aligned}
& Q \;\Leftarrow\; k{<}n \;\land\; (x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; z{:=}\,z{+}w.\;\; k{:=}\,k{+}1.\;\; t{:=}\,t{+}1.\;\; Q) && \text{expand second } Q\\
& && \text{and use substitution 5 times and simplify}\\
= \;& Q \;\Leftarrow\; k{<}n \land (x{+}y = k^3 + 3{\times}k^2 + 3{\times}k + 1 \land y{+}z = 3{\times}k^2 + 9{\times}k + 7 \;\land\; z{+}w = 6{\times}k + 12\\
& \qquad \Rightarrow\; x'{=}n^3 \;\land\; t' = t{+}n{-}k) && \text{mirror and expand } Q\\
= \;& \quad k{<}n \land (\quad x{+}y = k^3 + 3{\times}k^2 + 3{\times}k + 1 \land y{+}z = 3{\times}k^2 + 9{\times}k + 7 \;\land\; z{+}w = 6{\times}k + 12\\
& \qquad \Rightarrow\; x'{=}n^3 \land t' = t{+}n{-}k)\\
& \Rightarrow\; (x{=}k^3 \;\land\; y = 3{\times}k^2 + 3{\times}k + 1 \;\land\; z = 6{\times}k + 6 \;\;\Rightarrow\;\; x'{=}n^3 \;\land\; t' = t{+}n{-}k)\\
& && \text{If } w = 6 \text{ , then by specialization}\\
= \;& \top
\end{aligned}$$

So we see that w has to be 6 . The solution is

$$R \;\Leftarrow\; k{:=}\,n.\;\; x{:=}\,0.\;\; y{:=}\,1.\;\; z{:=}\,6.\;\; Q$$

$$Q \;\Leftarrow\; \textbf{if } k{=}0 \textbf{ then } ok \textbf{ else } x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; z{:=}\,z{+}6.\;\; k{:=}\,k{-}1.\;\; t{:=}\,t{+}1.\;\; Q \textbf{ fi}$$

The solution is simple and efficient, and we couldn't have found it without using the theory.

Here's the same linear solution using a forward-looking Q , but the recursion requires a stack. Let

$$Q \;=\; x'{=}n^3 \;\land\; y' = 3{\times}n^2 + 3{\times}n + 1 \;\land\; z' = 6{\times}n + 6 \;\land\; t'{=}t{+}n$$

Then

$$x'{=}n^3 \land t'{=}t{+}n \;\Leftarrow\; Q$$

$$\begin{aligned}
Q \;\Leftarrow\; & \textbf{if } n{=}0 \textbf{ then } x{:=}\,0.\;\; y{:=}\,1.\;\; z{:=}\,6\\
& \textbf{else } n{:=}\,n{-}1.\;\; t{:=}\,t{+}1.\;\; Q.\;\; x{:=}\,x{+}y.\;\; y{:=}\,y{+}z.\;\; z{:=}\,z{+}6 \textbf{ fi}
\end{aligned}$$

Now here's the same solution using the invariant **for**-loop rule in Subsection 5.2.3. We haven't got many operations to work with. We can try to accumulate a sum, as follows.

$$x'=n^3 \;\Leftarrow\; x:=0.\;\; \textbf{for } k:=0;..n \textbf{ do } x:=x+?\textbf{ od}$$

where the question mark means we don't know what goes here yet. We define invariant

$$A\,k \;=\; x=k^3$$

Then

$$x'=n^3 \;\Leftarrow\; x:=0.\;\; A\,0 \Rightarrow A'n$$

is easily proven. Now, for free,

$$A\,0 \Rightarrow A'n \;\Leftarrow\; \textbf{for } k:=0;..n \textbf{ do } k\colon 0,..n \wedge A\,k \;\Rightarrow\; A'(k+1) \textbf{ od}$$

and what remains is to refine $k\colon 0,..n \wedge A\,k \;\Rightarrow\; A'(k+1)$.

$$\begin{array}{ll} & k\colon 0,..n \wedge A\,k \;\Rightarrow\; A'(k+1) \qquad \text{drop } k\colon 0,..n \text{ and expand } A\,k \text{ and } A'(k+1) \\ \Leftarrow & x=k^3 \;\Rightarrow\; x'=(k+1)^3 \\ = & x=k^3 \;\Rightarrow\; x' = k^3 + 3\times k^2 + 3\times k + 1 \qquad \text{context} \\ = & x=k^3 \;\Rightarrow\; x' = x + 3\times k^2 + 3\times k + 1 \\ \Leftarrow & x:= x + 3\times k^2 + 3\times k + 1 \end{array}$$

Unfortunately, we don't have squaring or multiplication. So let's just say $x:= x+y$ and strengthen the invariant $A\,k$ to

$$A\,k \;=\; x=k^3 \;\wedge\; y \;=\; 3\times k^2 + 3\times k + 1$$

Now we must revise the initialization

$$x'=n^3 \;\Leftarrow\; x:=0.\;\; y:=1.\;\; A\,0 \Rightarrow A'n$$

and recalculate the loop body

$$\begin{array}{ll} & k\colon 0,..n \;\wedge\; A\,k \;\Rightarrow\; A'(k+1) \qquad \text{drop } k\colon 0,..n \text{ and expand } A\,k \text{ and } A'(k+1) \\ \Leftarrow & x=k^3 \;\wedge\; y = 3\times k^2 + 3\times k + 1 \;\Rightarrow\; x'=(k+1)^3 \;\wedge\; y' = 3\times(k+1)^2 + 3\times(k+1) + 1 \\ \Leftarrow & x' = x+y \;\wedge\; y' = y + 6\times k + 6 \\ = & x:= x+y.\;\; y:= y+k+k+k+k+k+k+6 \end{array}$$

and we're done, but it's a little inelegant to add up $6\;k$ so let's say $y:= y+z$ and strengthen $A\,k$ again to

$$A\,k \;=\; x=k^3 \;\wedge\; y = 3\times k^2 + 3\times k + 1 \;\wedge\; z = 6\times k + 6$$

Now we must revise the initialization

$$x'=n^3 \;\Leftarrow\; x:=0.\;\; y:=1.\;\; z:=6.\;\; A\,0 \Rightarrow A'n$$

and recalculate the loop body

$$\begin{array}{ll} & k\colon 0,..n \;\wedge\; A\,k \;\Rightarrow\; A'(k+1) \\ \Leftarrow & \quad x=k^3 \;\wedge\; y = 3\times k^2 + 3\times k + 1 \;\wedge\; z = 6\times k + 6 \\ & \Rightarrow\; x'=(k+1)^3 \;\wedge\; y' = 3\times(k+1)^2 + 3\times(k+1) + 1 \;\wedge\; z' = 6\times(k+1) + 6 \\ \Leftarrow & x' = x+y \;\wedge\; y' = y + 6\times k + 6 \;\wedge\; z' = z+6 \\ = & x:= x+y.\;\; y:= y+z.\;\; z:= z+6 \end{array}$$

and we're done again. Altogether,

$$x'=n^3 \;\Leftarrow\; x:=0.\;\; y:=1.\;\; z:=6.\;\; \textbf{for } k:=0;..n \textbf{ do } x:=x+y.\;\; y:=y+z.\;\; z:=z+6 \textbf{ od}$$