1 Program Correctness: Template

Given an array b of type **integer** $\to$ **boolean** and a non-negative length n. The following program computes the numerical representation of a bitvector.

$i \coloneqq 0;$
$x \coloneqq 0;$
while $i < n$ **do**
  $x \coloneqq 2 \cdot x;$
  if $b[i]$ **then**
    $x \coloneqq x + 1$
  fi;
  $i \coloneqq i + 1$
od

Let S be above program. Prove the following partial correctness formula:

$$\{n \geq 0\}\ S\ \{x = \sum_{i=0}^{n-1} 2^{n-1-i} \cdot (b[i]\ ?\ 1 : 0)\}$$

Here is a proof outline in proof system PW:

$\{n \geq 0\}$
$i \coloneqq 0;$
$x \coloneqq 0;$
$\{\mathbf{inv} : i \leq n \wedge x = \sum_{j=0}^{i-1} 2^{i-1-j} \cdot (b[j]\ ?\ 1 : 0)\}$
while $i < n$ **do**
  $\{i < n \wedge x = \sum_{j=0}^{i-1} 2^{i-1-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  $\{i < n \wedge 2 \cdot x = 2 \cdot \sum_{j=0}^{i-1} 2^{i-1-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  $\{i < n \wedge 2 \cdot x = \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  $x \coloneqq 2 \cdot x;$
  $\{i < n \wedge x = \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  if $b[i]$ **then**
    $\{i < n \wedge x = \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0) \wedge b[i]\}$
    $\{i < n \wedge x + 1 = (b[i]\ ?\ 1 : 0) + \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
    $x \coloneqq x + 1$
    $\{i < n \wedge x = (b[i]\ ?\ 1 : 0) + \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  else
    $\{i < n \wedge x = \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0) \wedge \neg b[i]\}$
    $\{i < n \wedge x = (b[i]\ ?\ 1 : 0) + \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
    skip
    $\{i < n \wedge x = (b[i]\ ?\ 1 : 0) + \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  fi;
  $\{i < n \wedge x = (b[i]\ ?\ 1 : 0) + \sum_{j=0}^{i-1} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  $\{i < n \wedge x = \sum_{j=0}^{i} 2^{i-j} \cdot (b[j]\ ?\ 1 : 0)\}$
  $i \coloneqq i + 1$
  $\{i \leq n \wedge x = \sum_{j=0}^{i-1} 2^{i-1-j} \cdot (b[j]\ ?\ 1 : 0)\}$
od
$\{i = n \wedge x = \sum_{j=0}^{i-1} 2^{i-1-j} \cdot (b[j]\ ?\ 1 : 0)\}$
$\{x = \sum_{i=0}^{n-1} 2^{n-1-i} \cdot (b[i]\ ?\ 1 : 0)\}$