- Norman Nnabhan
- Jonas Schneider
- Cyril Fahlenbock

$n > 0$ $f \in 0..n-1 \mapsto \mathbb{N}$

$g \in 0..n-1 \mapsto \mathbb{N}$ $\forall k.k \in 0..n-1 \Rightarrow g\left(k\right) = f\left(n-1-k\right)$

Ini

$$\dfrac{\dfrac{\dfrac{}{k \in \{\} \vdash g\left(k\right) = g\left(n-k-1\right)}\,(\mathrm{Bot})}{k \in 0..-1 \vdash g\left(k\right) = g\left(n-k-1\right)}\,(\mathrm{Simpl})}{\vdash [i. = 0]\,[g. = f]\,\forall k.k \in 0..i-1 \Rightarrow g\left(k\right) = f\left(n-k-1\right)}\,(\mathrm{Eql})$$

.

$$\dfrac{\dfrac{}{k \in i..j \vdash g\left(k\right) = g\left(k\right)}\,(\mathrm{Hyp})}{\vdash [g. = f]\,\forall k.k \in i..j \Rightarrow g\left(k\right) = f\left(k\right)}\,(\mathrm{Eql})$$

.

$$\dfrac{\dfrac{\dfrac{}{k \in \{\} \vdash f\left(k\right) = f\left(n-k-1\right)}\,(\mathrm{Bot})}{k \in n..n-1 \vdash f\left(k\right) = f\left(n-k-1\right)}\,(\mathrm{Simpl})}{[j. = n-1]\,[g. = f]\,\forall k.k \in j+1..n-1 \Rightarrow g\left(k\right) = f\left(n-k-1\right)}\,(\mathrm{Eql})$$

.

Inv

Let

$h = \left(\{i, j\} \mathbin{\lhd\!\!\!-} \mathrm{g}\right) \cup \{i \mapsto g\left(j\right), j \mapsto g\left(i\right)\}$

This means

$$\dfrac{}{k \in dom\left(g\right), k \notin \{i, j\} \vdash h\left(k\right) = g\left(k\right)}$$

Three cases:

For `0..i` Split on

$k \in 0..i \vdash k \in 0..i-1 \lor k = i$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash f\left(j\right) = f\left(j\right)}\,\text{(EqlRefl)}}{\Gamma, f\left(j\right) = g\left(j\right), i + j = n - 1 \vdash g\left(j\right) = f\left(n - i - 1\right)}\,\text{(Eql)} \qquad \dfrac{}{\vdash j \in i..j}\,\text{(Triv)}}{\Gamma, \forall a.a \in i..j \Rightarrow f\left(a\right) = g\left(a\right) \vdash \left(\left\{i \mapsto g\left(j\right)\right\}\right)\left(i\right) = f\left(n - i - 1\right)}\,\text{(ImplL)}}{\Gamma \vdash h\left(i\right) = f\left(n - i - 1\right)}\,\text{(Definition h)}}{\Gamma, k = i \vdash h\left(k\right) = f\left(n - k - 1\right)}\,\text{(Eql)} \qquad \dfrac{\dfrac{}{\Gamma, k \in 0..i - 1 \vdash g\left(k\right) = f\left(n - k - 1\right)}\,\text{(Hyp)}}{\Gamma, k \in 0..i - 1, k \notin \left\{i, j\right\} \vdash h\left(k\right) = f\left(n - k - 1\right)}\,\text{(Lemma)}}{\dfrac{\Gamma, k \in 0..i - 1 \cup \left\{i\right\} \vdash h\left(k\right) = f\left(n - k - 1\right)}{\dfrac{\Gamma \vdash \forall k.k \in 0..i + 1 - 1 \Rightarrow h\left(k\right) = f\left(n - k - 1\right)}{\Gamma \vdash \left[g. = h\right]\left[i. = i + 1\right]\left[j. = j - 1\right]\forall k.k \in 0..i - 1 \Rightarrow g\left(k\right) = f\left(n - k - 1\right)}\,\text{(Eql)}}\,\text{(ImplR)}}\,\text{(OrL)}
$$

.

For `i+1..j-1` narrow `i..j` invariant

$$
\dfrac{\dfrac{\dfrac{}{\Gamma, g\left(k'\right) = f\left(k'\right) \vdash g\left(k'\right) = f\left(k'\right)}\,\text{(Hyp)} \qquad \dfrac{}{k' \in i + 1..j - 1 \vdash k' \in i..j}\,\text{(Triv)}}{\Gamma, \forall k \in i..j \Rightarrow g\left(k\right) = f\left(k\right), k' \in i + 1..j - 1 \vdash g\left(k'\right) = f\left(k'\right)}\,\text{(ImplL)}}{\Gamma, \forall k \in i..j \Rightarrow g\left(k\right) = f\left(k\right) \vdash \forall k \in i + 1..j - 1 \Rightarrow h\left(k\right) = f\left(k\right)}\,\text{(ImplR)}
$$

.

And `j-1..n-1` is equivalent to 0..i-1

$$
\dfrac{\dfrac{\dfrac{}{\Gamma, g\left(i\right) = f\left(i\right) \vdash g\left(i\right) = f\left(i\right)}\,\text{(Hyp)} \qquad \dfrac{}{\Gamma \vdash i \in i..j}\,\text{(Triv)}}{\Gamma, \forall k.k \in i..j \Rightarrow g\left(k\right) = f\left(k\right) \vdash g\left(i\right) = f\left(i\right)}\,\text{(ImplL)} \qquad \dfrac{\dfrac{}{\Gamma, k \in j + 1..n - 1 \vdash g\left(k\right) = f\left(n - k - 1\right)}\,\text{(Hyp)}}{\Gamma, k \in j + 1..n - 1, k \notin \left\{i, j\right\} \vdash h\left(k\right) = f\left(n - k - 1\right)}\,\text{(Lemma)}}{\dfrac{\Gamma, k = j \vee k \in j + 1..n - 1 \vdash h\left(k\right) = f\left(n - k - 1\right)}{\dfrac{\Gamma, k \in j - 1 + 1..n - 1 \vdash h\left(k\right) = f\left(n - k - 1\right)}{\dfrac{\Gamma \vdash \forall k.k \in j - 1 + 1..n - 1 \Rightarrow h\left(k\right) = f\left(n - k - 1\right)}{\Gamma \vdash \left[g. = h\right]\left[i. = i + 1\right]\left[j. = j - 1\right]\forall k.k \in j + 1..n - 1 \Rightarrow g\left(k\right) = f\left(n - k - 1\right)}\,\text{(Eql)}}\,\text{(ImplR)}}\,\text{(SplitRange)}}\,\text{(OrL)}
$$

Post

To combine the three invariants they need to have the same shape. So we need to prove that i and j meet in the middle

$\Gamma, i \geqslant j, g\left(k\right) = f\left(k\right) \vdash g\left(k\right) = f\left(n - k - 1\right)$

To do so combine i >= j and i <= j

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash f(i) = f(i)}\ (\text{EqlRefl})}{\Gamma, i+i = n-1, g(i) = f(i) \vdash g(i) = f(n-i-1)}\ (\text{Eql}) \quad \dfrac{}{\vdash i \in i..i}\ (\text{Triv})}{\Gamma, \forall k.k \in i..i \Rightarrow g(k) = f(k) \vdash g(i) = f(n-i-1)}\ (\text{ImplL})}{\Gamma, i = j, s \in i..j \vdash g(s) = f(n-s-1)}\ (\text{Eql})}{\Gamma, i \geqslant j, i \leqslant j \vdash \forall k.k \in i..j \Rightarrow g(k) = f(n-k-1)}\ (\text{ImplR})$$

The other two parts are already in the right shape

$$\dfrac{}{\Gamma, \forall k.k \in 0..i-1 \Rightarrow g(k) = f(n-k-1) \vdash \forall k.k \in 0..i-1 \Rightarrow g(k) = f(n-k-1)}\ (\text{Hyp})$$

$$\dfrac{}{\Gamma, \forall k.k \in j+1..n-1 \Rightarrow g(k) = f(n-k-1) \vdash \forall k.k \in j+1..n-1 \Rightarrow g(k) = f(n-k-1)}\ (\text{Hyp})$$

Merge them to prove the Post condition:

$$\dfrac{}{\Gamma, \forall k.k \in (0..i-1 \cup i..j \cup j+1..n-1) \Rightarrow g(k) = f(n-k-1) \vdash \forall k.k \in (0..i-1 \cup i..j \cup j+1..n-1) \Rightarrow g(k) = f(n-k-1)}\ (\text{Hyp})$$

Nat:

$j + 1 - i$

$$\dfrac{\dfrac{}{i \leqslant j+1 \vdash j+1 \geqslant i}\ (\text{Hyp})}{i \leqslant j+1 \vdash j+1-i \geqslant 0}\ (\text{Simpl})$$

Progress:

$$\dfrac{\dfrac{\dfrac{}{\vdash 0 < 2}\ (\text{Triv})}{\vdash j-1+1-(i+1) < j+1-i}\ (\text{Simpl})}{\vdash [i. = i+1]\,[j. = j-1]\, j+1-i < j+1-i}\ (\text{Simpl})$$

```c
int f[10] = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11};
int i;
int j;
#define n 10

int reverse() {
```

```
    i = 0;
    j = n - 1;
    while (i < j) {
        temp = f[i];
        f[i] = f[j]
        f[j] = temp;
        i = i + 1;
        j = j - 1;
    }
    return 0;
}
```