- Norman Nnabhan
- Jonas Schneider
- Cyril Fahlenbock

#1

$$\dfrac{\dfrac{}{\Gamma \vdash (\mathrm{p} \Rightarrow [s_1]\, e) \wedge (\neg \mathrm{p} \Rightarrow [s_2]\, e)}}{\Gamma \vdash [\mathrm{ifpthen} s_1 \mathrm{else} s_2 \mathrm{end}]\, e}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, P(X), x \in S \vdash Q(x,a)}}{\Gamma, P(X), x \in S \vdash [y.=a]\, Q(x,y)}\,(\text{SubstitutionEquality})}{\Gamma, x \in S \vdash P(x) \Rightarrow [y.=a]\, Q(x,y)}\,(\text{R=>})}{\Gamma \vdash [x.\in S]\,(P(x) \Rightarrow [y.=a]\, Q(x,y))}\,(\text{SubstitutionAssignIn}) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \neg P(x), x \in S \vdash Q(x,b)}}{\Gamma, \neg P(x), x \in S \vdash [y.=b]\, Q(x,y)}\,(\text{SubstitutionEquality})}{\Gamma, x \in S \vdash \neg P(x) \Rightarrow [y.=b]\, Q(x,y)}\,(\text{R=>})}{\Gamma \vdash [x.\in S]\,(\neg P(x) \Rightarrow [y.=b]\, Q(x,y))}\,(\text{SubstitutionAssignIn})}{\Gamma \vdash [x.\in S]\,[\mathrm{if} P(x)\, then \mathrm{y}.=\mathrm{a} else \mathrm{y}.=\mathrm{b} end]\, Q(x,y)}\,(\text{SubstitutionIf})$$

#2

Some lemmas to start with:

$$\dfrac{\dfrac{}{\Gamma \vdash \forall i.\forall j. i \leqslant j \Rightarrow f(i) \leqslant f(j)}\,(\text{Hyp})}{\Gamma \vdash \forall i.\forall j. f(j) > f(i) \Rightarrow j > i}\,(\text{Flip})$$

$$\dfrac{}{v \in f[p..q] \vdash \exists z. z \in p..q \wedge f(z) = v}\,(\text{Triv})$$

Now we can link p/q and r via z

Feasability

$$\dfrac{}{b \geqslant a \vdash a..b \neq \{\}}\,(\text{Triv})$$

$$\dfrac{\dfrac{\dfrac{}{r > p \vdash r+1 \geqslant p}\,(\text{Triv})}{z \geqslant p, r > z \vdash r+1 \geqslant p}\,(\text{Simpl}) \quad \dfrac{}{\text{Sorted}, f(r) > f(z) \vdash r > z}\,(\text{Lemma})}{\text{Sorted}, f(r) < v, v \in f[p..q], \exists z.(z \in p..q \wedge v = f(z)) \vdash r+1 \geqslant q}\,(\text{Skolemize})$$

.

$$\dfrac{\dfrac{\dfrac{}{p < r \vdash p \leqslant r - 1}\,(\text{Triv})}{z \geqslant p, r > z \vdash p \leqslant r - 1}\,(\text{Simpl}) \qquad \dfrac{}{\text{Sorted}, f\,(r) > f\,(z) \vdash z < r}\,(\text{Lemma})}{\text{Sorted}, f\,(r) \geqslant v, f\,(r) \neq v, v \in f\,[p..p]\,, \exists z.\,(z \in p..q \wedge v = f\,(z)) \vdash p \leqslant r - 1}\,(\text{Skolemize})$$

Variant.

$p - q$

Nat.

$$ First show that the loop guard implies `p < q` in the loop:

$$\dfrac{\dfrac{}{p < q \vdash p < q}\,(\text{Hyp}) \qquad \dfrac{\dfrac{}{f\,(r) \neq f\,(r) \vdash \bot}\,(\text{LEM})}{p = q, r = p, v = f\,(p)\,, f\,(r) \neq v \vdash p < q}\,(\text{Simpl}) \qquad \dfrac{}{p > q, r \in p..q \vdash \bot}\,(\text{LEM})}{r \in p..q, v \in f\,[p..q]\,, f\,(r) \neq v \vdash p < q}\,(\text{By Case})$$

.

$$\dfrac{\dfrac{}{\Gamma \vdash p \leqslant q}\,(\text{Lemma})}{\Gamma \vdash q - p \geqslant 0}\,(\text{Simpl})$$

Progress.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{r \geqslant p \vdash r + 1 > p}\,(\text{Triv})}{r \geqslant p \vdash -(r + 1) < -p}\,(\text{Simpl})}{r \geqslant p \vdash q - (r + 1) < q - p}\,(\text{Simpl})}{r \in p..q \vdash [p. = r + 1]\, q - p < q - p}\,(\text{Eql})$$

$$\dfrac{\dfrac{\dfrac{}{r \leqslant q \vdash r < q + 1}\,(\text{Triv})}{r \leqslant q \vdash r - 1 - p < q - p}\,(\text{Simpl})}{r \in p..q \vdash [q. = r - 1]\, q - p < q - p}\,(\text{Eql})$$

3.

Proof `(0+n-1)/2 in 0..n-1`

$$\dfrac{\dfrac{}{n > 0 \vdash \frac{n-1}{2} \leqslant n-1}\,(\text{Triv}) \qquad \dfrac{}{n > 0 \vdash \frac{n-1}{2} \geqslant 0}\,(\text{Triv})}{n > 0 \vdash \frac{0+n-1}{2} \in 0..n-1}\,(\text{Split})$$

Proof `(r + 1 + q)/2 in r+1..q`

$$\dfrac{\dfrac{\dfrac{}{\vdash q \geqslant r+1}\,(\text{Proof in Lemma})}{\vdash r+1+q \geqslant (r+1)\cdot 2}\,(\text{Simpl}) \qquad \dfrac{\dfrac{}{\vdash r+1 \leqslant q}\,(\text{Proof in Lemma})}{\vdash r+1+q \leqslant q \cdot 2}\,(\text{Simpl})}{\vdash \frac{r+1+q}{2} \in r+1..q}\,(\text{Split Range})$$

Proof `q >= r+1` during loop We use already know that `p < q` in the loop body.

$$\dfrac{\dfrac{\dfrac{}{r+1 < q \vdash r+1 < q}\,(\text{Triv})}{r+1 < q \vdash r+1+q < 2q}\,(\text{Simpl}) \qquad \dfrac{}{p < q, p = r+1 \vdash r+1 < q}\,(\text{Helper Lemma})}{p < q, p = r+1 \vdash \frac{r+1+q}{2} < q}\,(\text{Simpl})$$

Proof `(p + r - 1 )/2 in p..r-1`

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash r-1 \geqslant p}\,(\text{Proof in Lemma})}{\vdash p+r-1 \geqslant 2p}\,(\text{Simpl})}{\vdash \frac{p+r-1}{2} \geqslant p}\,(\text{Simpl}) \qquad \dfrac{\dfrac{\dfrac{}{\vdash p \leqslant r-1}\,(\text{Proof in Lemma})}{\vdash (p+r-1) \leqslant 2r-2}\,(\text{Simpl})}{\vdash \frac{p+r-1}{2} \leqslant r-1}\,(\text{Simpl})}{\vdash \frac{p+r-1}{2} \in p..r-1}\,(\text{Split Range})$$

Proof `p <= r-1` during loop

$$\dfrac{\dfrac{\dfrac{}{p < r-1 \vdash p < r-1}\,(\text{Triv})}{p < r-1 \vdash (p+r-1) < 2r-2}\,(\text{Simpl}) \qquad \dfrac{}{q = r-1, p < q \vdash p < r-1}\,(\text{Helper Lemma})}{q = r-1, p < q \vdash \frac{p+r-1}{2} < r-1}\,(\text{Simpl})$$

```c
int p;
int q;
int r;
#define n 10
const int f[10] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10};

int binsearch() {
    p = 0;
    q = n - 1;
    r = (0 + n - 1)/2;
    while (f[r] != v) {
        if f(r) < v {
            p = r + 1;
            r = (r + 1 + q)/2;
        } else {
            q = r - 1;
            r = (p + r - 1)/2
        }
    }
    return 0;
}
```