Suppose we want to prove that some property $P$ holds for a recursively defined function $f : A \rightarrow A$. We can prove $P(f)$ by fixed-point induction via the following three steps:

1. Define a non-recursive functional $F : (A \rightarrow A) \rightarrow (A \rightarrow A)$ whose least fixed point is $f$.

2. **Base Case:** Prove that property $P$ holds for the function whose preimage is empty. That is, prove that $P(\bot_{A \rightarrow A})$ holds.

3. **Inductive Case:** Assume as the inductive hypothesis that $P$ holds for some arbitrary function $g$, and prove that this implies that $P$ holds for function $F(g)$. That is, prove $P(g) \Rightarrow P(F(g))$.

Here is an example of such a proof:

**Exercise 1.** Consider the following recursive definition of the factorial function $f : \mathbb{N}_0 \rightarrow \mathbb{N}_0$.

$$f(x) = (x=0 \rightarrow 1 \mid x>0 \rightarrow xf(x-1))$$

Prove that for all $x \in \mathbb{Z}$, $f(x)$ is either undefined or $f(x) = x!$. (It also turns out that $f(x)$ is defined for all $x \geq 0$, but we won’t prove that here.)

**Proof.** The property $P$ to be proved can be formally expressed as $P(g) \equiv \forall x \in g^\rightarrow . g(x) = x!$. We wish to prove $P(f)$. Define functional $F : (\mathbb{N}_0 \rightarrow \mathbb{N}_0) \rightarrow (\mathbb{N}_0 \rightarrow \mathbb{N}_0)$ as follows:

$$F(g) = \lambda x . (x=0 \rightarrow 1 \mid x>0 \rightarrow xg(x-1))$$

Observe that $fix(F) = f$. Thus, to prove $P(f)$ it suffices to prove $P(fix(F))$ by fixed-point induction.

**Base Case:** $P(\bot_{\mathbb{N}_0 \rightarrow \mathbb{N}_0})$ holds vacuously. That is, $P(\bot_{\mathbb{N}_0 \rightarrow \mathbb{N}_0})$ requires us to prove something about all members of $\bot_{\mathbb{N}_0 \rightarrow \mathbb{N}_0}^\rightarrow$, but $\bot_{\mathbb{N}_0 \rightarrow \mathbb{N}_0}^\rightarrow$ has no members, so there is nothing to prove.

**Inductive Case:** Assume that $P(g)$ holds for some arbitrary function $g$. That is, assume that $\forall x \in g^\rightarrow . g(x) = x!$. We will prove that $P(F(g))$ holds. That is, we will prove that $\forall x \in F(g)^\rightarrow . F(g)(x) = x!$. Let an arbitrary $x \in F(g)^\rightarrow$ be given. Looking at the definition of $F$, there are two cases to consider:

**Case 1:** Suppose $x = 0$. Then by definition of $F$, $F(g)(x) = 1 = x!$.

**Case 2:** Suppose $x > 0$. Then by definition of $F$, $F(g)(x) = xg(x-1)$. By inductive hypothesis, $g(x-1) = (x-1)!$. Hence, $F(g)(x) = x(x-1)! = x!$. 

$\square$
The same general technique can be used to prove a property $P$ of the denotation of a while loop. First, define a non-recursive functional $\Gamma$ whose least fixed point is $C[\text{while } b \text{ do } c]$.

$$\Gamma(f) = \{ (\sigma, (f \circ C[c])(\sigma)) \mid (\sigma, T) \in B[b] \} \cup \{ (\sigma, \sigma) \mid (\sigma, F) \in B[b] \}$$

We can now prove that $P$ holds for $\text{fix}(\Gamma)$ using fixed-point induction. The induction has two steps:

1. As the base case of the induction, prove $P(\bot_{\Sigma \rightarrow \Sigma})$.

2. Assume as the inductive hypothesis that $P(f)$ holds, and prove that $P(\Gamma(f))$ holds.

To prove a property $P$ by induction it is often easier to prove a stronger property $P'$ that implies $P$. The stronger $P'$ yields a stronger inductive hypothesis. Here is an example:

**Exercise 2.** Define $c$ to be the SIMPL program $\text{while } 2 \leq x \text{ do } (y := y \cdot x; x := x - 1)$. Define property $P$ by $P(f) \equiv \forall (\sigma, \sigma') \in f$, if $\sigma(x) \geq 1$ and $\sigma(y) = 1$ then $\sigma'(y) = \sigma(x)$. Prove $P(C[c])$.

**Proof.** We will instead prove a different property $P'(C[c])$, where $P'$ is defined as follows:

$$P'(f) \equiv \forall (\sigma, \sigma') \in f$, if $\sigma(x) \geq 1$ then $\sigma'(y) = \sigma(y) \cdot \sigma(x)!$$

Notice that $P'(f)$ implies $P(f)$. That is, since we know by assumption that $\sigma(y) = 1$, $P'(f)$ implies that $\sigma'(y) = \sigma(y) \cdot \sigma(x)! = \sigma(x)!$. Thus, proving $P'(C[c])$ suffices to prove the theorem.

We begin by defining a functional $\Gamma$ whose least fixed point is $C[c]$:

$$\Gamma(f) = \{ (\sigma, (f \circ C[c])(\sigma)) \mid (\sigma, T) \in B[2 \leq x] \} \cup \{ (\sigma, \sigma) \mid (\sigma, F) \in B[2 \leq x] \}$$

$$= \{ (\sigma, f(\sigma[x \mapsto \sigma(y)\sigma(x)]\sigma(x) \mapsto \sigma(x) - 1])) \mid \sigma \in \Sigma, 2 \leq \sigma(x) \} \cup \{ (\sigma, \sigma) \mid \sigma \in \Sigma, 2 > \sigma(x) \}$$

We shall prove by fixed-point induction that property $P'(\text{fix}(\Gamma))$ holds.

**Base Case:** Property $P'(\bot)$ holds vacuously.

**Inductive Case:** Assume as the inductive hypothesis that property $P'(f)$ holds. That is, assume that for all $(\sigma_0, \sigma'_0) \in f$, if $\sigma_0(x) \geq 1$ then $\sigma'_0(y) = \sigma_0(y) \cdot \sigma_0(x)!$. We wish to prove that property $P'(\Gamma(f))$ holds.

Let $(\sigma, \sigma') \in \Gamma(f)$ be given and assume that $\sigma(x) \geq 1$. We must prove that $\sigma'(y) = \sigma(y) \cdot \sigma(x)!$.

**Case 1:** Assume that $2 \leq \sigma(x)$. From the definition of $\Gamma$ we conclude that $\sigma' = f(\sigma_2)$ where $\sigma_2 = [\sigma[y \mapsto \sigma(y)\sigma(x)]\sigma(x) \mapsto \sigma(x) - 1]$. Writing $\sigma' = f(\sigma_2)$ is the same as writing $(\sigma_2, \sigma') \in f$. Therefore, we intend to apply the inductive hypothesis with $\sigma_0 = \sigma_2$ and $\sigma'_0 = \sigma'$. To do so, we must first prove that $\sigma_2(x) \geq 1$. From the definition of $\sigma_2$ we infer that $\sigma_2(x) = \sigma(x) - 1$. Since $2 \leq \sigma(x)$ by assumption, it follows that $\sigma_2(x) \geq 1$. By inductive hypothesis, $\sigma'(y) = \sigma_2(y) \cdot \sigma_2(x)! = (\sigma(y)\sigma(x)) \cdot (\sigma(x) - 1)! = \sigma(y) \cdot \sigma(x)!$.

**Case 2:** Assume that $2 > \sigma(x)$. From the definition of $\Gamma$ we conclude that $\sigma' = \sigma$, so $\sigma'(y) = \sigma(y)$. Since we have supposed both that $\sigma(x) \geq 1$ and that $2 > \sigma(x)$, it follows that $\sigma(x) = 1$. Hence, $\sigma'(y) = \sigma(y) = \sigma(y) \cdot \sigma(x)!$.

We have therefore proved by fixed-point induction that property $P'(\text{fix}(\Gamma))$ holds. Since $\text{fix}(\Gamma) = C[c]$, it follows that $P'(C[c])$ holds. Since property $P'$ implies the theorem, this proves the theorem.