An Application of Auxiliary Variables

John C. Reynolds - March 17, 2011

An ad hoc proof of the list reversal program:

$$
\begin{array}{l}
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\} \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ (\mathbf{emp} \wedge \mathbf{nil} = \mathbf{nil})\} \\
\mathsf{j} := \mathbf{nil}\ ; \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ (\mathbf{emp} \wedge \mathsf{j} = \mathbf{nil})\} \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ \mathsf{list}\ \epsilon\ \mathsf{j}\} \\
\Rightarrow \{\exists \alpha, \beta.\ (\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\} \\
\quad \mathbf{while}\ \mathsf{i} \neq \mathbf{nil}\ \mathbf{do} \\
\quad\quad \big(\{\exists \alpha, \beta.\ (\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha \neq \epsilon\} \\
\quad\quad \Rightarrow \{\exists \mathsf{a}, \alpha, \beta.\ (\mathsf{list}\ (\mathsf{a} \cdot \alpha)\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathsf{a} \cdot \alpha)^\dagger \cdot \beta\} \\
\quad\quad\quad \{\exists \mathsf{a}, \alpha, \beta, \mathsf{k}.\ (\mathsf{i} \mapsto \mathsf{a}, \mathsf{k}\ *\ \mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathsf{a} \cdot \alpha)^\dagger \cdot \beta\} \\
\quad\quad\quad \mathsf{k} := [\mathsf{i} + 1]\ ; \\
\quad\quad\quad \{\exists \mathsf{a}, \alpha, \beta.\ (\mathsf{i} \mapsto \mathsf{a}, \mathsf{k}\ *\ \mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathsf{a} \cdot \alpha)^\dagger \cdot \beta\} \\
\quad\quad\quad [\mathsf{i} + 1] := \mathsf{j}\ ; \\
\quad\quad\quad \{\exists \mathsf{a}, \alpha, \beta.\ (\mathsf{i} \mapsto \mathsf{a}, \mathsf{j}\ *\ \mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathsf{a} \cdot \alpha)^\dagger \cdot \beta\} \\
\quad\quad\quad \{\exists \mathsf{a}, \alpha, \beta.\ (\mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ (\mathsf{a} \cdot \beta)\ \mathsf{i}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \mathsf{a} \cdot \beta\} \\
\quad\quad \Rightarrow \{\exists \alpha, \beta.\ (\mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{i}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\} \\
\quad\quad\quad \mathsf{j} := \mathsf{i}\ ;\ \mathsf{i} := \mathsf{k} \\
\quad\quad\quad \{\exists \alpha, \beta.\ (\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\big) \\
\{\exists \alpha, \beta.\ \mathsf{list}\ \beta\ \mathsf{j} \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha = \epsilon\} \\
\{\mathsf{list}\ \alpha_0^\dagger\ \mathsf{j}\}
\end{array}
$$

Note the change of existential witnesses.

A Derivation — the abstract program:

$$
\begin{array}{l}
\{\mathbf{true}\} \\
\{\alpha_0^\dagger = \alpha_0^\dagger \cdot \epsilon\} \\
\alpha := \alpha_0 \,;\, \beta := \epsilon \,; \\
\{\alpha_0^\dagger = \alpha^\dagger \cdot \beta\} \\
\mathbf{while}\ \alpha \neq \epsilon\ \mathbf{do} \\
\quad \big(\{\alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha \neq \epsilon\} \\
\quad\ \{\alpha_0^\dagger = (\mathbf{f}\,\alpha \cdot \mathbf{r}\,\alpha)^\dagger \cdot \beta\} \\
\quad\ \{\alpha_0^\dagger = (\mathbf{r}\,\alpha)^\dagger \cdot (\mathbf{f}\,\alpha) \cdot \beta\} \\
\quad\ \beta := (\mathbf{f}\,\alpha) \cdot \beta \,; \\
\quad\ \{\alpha_0^\dagger = (\mathbf{r}\,\alpha)^\dagger \cdot \beta\} \\
\quad\ \alpha := \mathbf{r}\,\alpha \,; \\
\quad\ \{\alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\big) \\
\{\alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha = \epsilon\} \\
\{\beta = \alpha_0^\dagger\}
\end{array}
$$

where $\mathbf{f}(a \cdot \alpha) = a$ and $\mathbf{r}(a \cdot \alpha) = \alpha$.

Adding the concrete representation: $\mathsf{list}\,\alpha\,\mathsf{i} \;*\; \mathsf{list}\,\beta\,\mathsf{j}$

$\{\mathsf{list}\,\alpha_0\,\mathsf{i}\}$
$\{\mathsf{list}\,\alpha_0\,\mathsf{i} \;*\; (\mathbf{emp} \wedge \mathbf{nil} = \mathbf{nil})\}$
$\boxed{\mathsf{j} := \mathbf{nil}}\,;$
$\{\mathsf{list}\,\alpha_0\,\mathsf{i} \;*\; (\mathbf{emp} \wedge \mathsf{j} = \mathbf{nil})\}$
$\{\mathsf{list}\,\alpha_0\,\mathsf{i} \;*\; \mathsf{list}\,\epsilon\,\mathsf{j}\}$
$\{(\mathsf{list}\,\alpha_0\,\mathsf{i} \;*\; \mathsf{list}\,\epsilon\,\mathsf{j}) \wedge \alpha_0^\dagger = \alpha_0^\dagger{\cdot}\epsilon\}$
$\alpha := \alpha_0\,;\, \beta := \epsilon\,;$
$\{(\mathsf{list}\,\alpha\,\mathsf{i} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta\}$
while $\alpha \neq \epsilon$ **do**
$\big($
$\{(\mathsf{list}\,\alpha\,\mathsf{i} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \wedge \alpha \neq \epsilon\}$
$\{(\mathsf{list}\,(\mathbf{f}\,\alpha{\cdot}\mathbf{r}\,\alpha)\,\mathsf{i} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\,\alpha{\cdot}\mathbf{r}\,\alpha)^\dagger{\cdot}\beta\}$
$\{\exists \mathsf{k}.\ (\mathsf{i} \mapsto \mathbf{f}\,\alpha, \mathsf{k} \;*\; \mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\,\alpha{\cdot}\mathbf{r}\,\alpha)^\dagger{\cdot}\beta\}$
$\boxed{\mathsf{k} := [\mathsf{i}+1]}\,;$
$\{(\mathsf{i} \mapsto \mathbf{f}\,\alpha, \mathsf{k} \;*\; \mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\,\alpha{\cdot}\mathbf{r}\,\alpha)^\dagger{\cdot}\beta\}$
$\boxed{[\mathsf{i}+1] := \mathsf{j}}\,;$
$\{(\mathsf{i} \mapsto \mathbf{f}\,\alpha, \mathsf{j} \;*\; \mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\,\alpha{\cdot}\mathbf{r}\,\alpha)^\dagger{\cdot}\beta\}$
$\{(\mathsf{i} \mapsto \mathbf{f}\,\alpha, \mathsf{j} \;*\; \mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{r}\,\alpha)^\dagger{\cdot}(\mathbf{f}\,\alpha){\cdot}\beta\}$
$\{(\mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,(\mathbf{f}\,\alpha){\cdot}\beta\,\mathsf{i}) \wedge \alpha_0^\dagger = (\mathbf{r}\,\alpha)^\dagger{\cdot}(\mathbf{f}\,\alpha){\cdot}\beta\}$
$\beta := (\mathbf{f}\,\alpha){\cdot}\beta\,;$
$\{(\mathsf{list}\,(\mathbf{r}\,\alpha)\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{i}) \wedge \alpha_0^\dagger = (\mathbf{r}\,\alpha)^\dagger{\cdot}\beta\}$
$\alpha := \mathbf{r}\,\alpha\,;$
$\{(\mathsf{list}\,\alpha\,\mathsf{k} \;*\; \mathsf{list}\,\beta\,\mathsf{i}) \wedge \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta\}$
$\boxed{\mathsf{j} := \mathsf{i}\,;\, \mathsf{i} := \mathsf{k}}$
$\{(\mathsf{list}\,\alpha\,\mathsf{i} \;*\; \mathsf{list}\,\beta\,\mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta\}\big)$
$\{\mathsf{list}\,\beta\,\mathsf{j} \wedge \alpha_0^\dagger = \alpha^\dagger{\cdot}\beta \wedge \alpha = \epsilon\}$
$\{\mathsf{list}\,\alpha_0^\dagger\,\mathsf{j}\}$

Making the while-test concrete:

$$
\begin{array}{l}
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\} \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ (\mathbf{emp} \wedge \mathbf{nil} = \mathbf{nil})\} \\
\mathsf{j} := \mathbf{nil}\ ; \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ (\mathbf{emp} \wedge \mathsf{j} = \mathbf{nil})\} \\
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ \mathsf{list}\ \epsilon\ \mathsf{j}\} \\
\{(\mathsf{list}\ \alpha_0\ \mathsf{i}\ *\ \mathsf{list}\ \epsilon\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha_0^\dagger \cdot \epsilon\} \\
\alpha := \alpha_0\ ;\ \beta := \epsilon\ ; \\
\{(\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\} \\
\mathbf{while}\ \boxed{\mathsf{i} \neq \mathbf{nil}}\ \mathbf{do} \\
\quad \big(\{(\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha \neq \epsilon\} \\
\quad \{(\mathsf{list}\ (\mathbf{f}\ \alpha \cdot \mathbf{r}\ \alpha)\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\ \alpha \cdot \mathbf{r}\ \alpha)^\dagger \cdot \beta\} \\
\quad \{\exists \mathsf{k}.\ (\mathsf{i} \mapsto \mathbf{f}\ \alpha, \mathsf{k}\ *\ \mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\ \alpha \cdot \mathbf{r}\ \alpha)^\dagger \cdot \beta\} \\
\quad \mathsf{k} := [\mathsf{i} + 1]\ ; \\
\quad \{(\mathsf{i} \mapsto \mathbf{f}\ \alpha, \mathsf{k}\ *\ \mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\ \alpha \cdot \mathbf{r}\ \alpha)^\dagger \cdot \beta\} \\
\quad [\mathsf{i} + 1] := \mathsf{j}\ ; \\
\quad \{(\mathsf{i} \mapsto \mathbf{f}\ \alpha, \mathsf{j}\ *\ \mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{f}\ \alpha \cdot \mathbf{r}\ \alpha)^\dagger \cdot \beta\} \\
\quad \{(\mathsf{i} \mapsto \mathbf{f}\ \alpha, \mathsf{j}\ *\ \mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = (\mathbf{r}\ \alpha)^\dagger \cdot (\mathbf{f}\ \alpha) \cdot \beta\} \\
\quad \{(\mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ (\mathbf{f}\ \alpha) \cdot \beta\ \mathsf{i}) \wedge \alpha_0^\dagger = (\mathbf{r}\ \alpha)^\dagger \cdot (\mathbf{f}\ \alpha) \cdot \beta\} \\
\quad \beta := (\mathbf{f}\ \alpha) \cdot \beta\ ; \\
\quad \{(\mathsf{list}\ (\mathbf{r}\ \alpha)\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{i}) \wedge \alpha_0^\dagger = (\mathbf{r}\ \alpha)^\dagger \cdot \beta\} \\
\quad \alpha := \mathbf{r}\ \alpha\ ; \\
\quad \{(\mathsf{list}\ \alpha\ \mathsf{k}\ *\ \mathsf{list}\ \beta\ \mathsf{i}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\} \\
\quad \mathsf{j} := \mathsf{i}\ ;\ \mathsf{i} := \mathsf{k} \\
\quad \{(\mathsf{list}\ \alpha\ \mathsf{i}\ *\ \mathsf{list}\ \beta\ \mathsf{j}) \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta\}\big) \\
\{\mathsf{list}\ \beta\ \mathsf{j} \wedge \alpha_0^\dagger = \alpha^\dagger \cdot \beta \wedge \alpha = \epsilon\} \\
\{\mathsf{list}\ \alpha_0^\dagger\ \mathsf{j}\}
\end{array}
$$

Eliminating assignments to the auxiliary variables α and β:

$$
\begin{array}{l}
\{\mathsf{list}\ \alpha_0\ \mathsf{i}\} \\
\mathsf{j} := \mathbf{nil}\ ; \\
\boxed{\alpha := \alpha_0\ ;\ \beta := \epsilon}\ ; \\
\mathbf{while}\ \mathsf{i} \neq \mathbf{nil}\ \mathbf{do} \\
\quad \big(\mathsf{k} := [\mathsf{i}+1]\ ; \\
\quad\ [\mathsf{i}+1] := \mathsf{j}\ ; \\
\quad\ \boxed{\beta := (\mathbf{f}\ \alpha)\cdot\beta}\ ; \\
\quad\ \boxed{\alpha := \mathbf{r}\ \alpha}\ ; \\
\quad\ \mathsf{j} := \mathsf{i}\ ;\ \mathsf{i} := \mathsf{k} \big) \\
\{\mathsf{list}\ \alpha_0^{\dagger}\ \mathsf{j}\}
\end{array}
$$