Constrained Normal Path Proofs

by Sven Nilsen, 2020

A constrained normal path proof is a quantified existential path equation over a constrained normal path such that every path returns `true` for all inputs:

$$\forall x \{ f\{g_i(x)\}[unit \to g_n(x)] \Leftarrow\Rightarrow \backslash true \}$$

$$f : T \to U$$
$$g_{in} : (T \to bool) \times U \to bool$$

The form of the constrained normal path follows from these two requirements:

- It is constrained
- It returns `true` for all inputs

It is always possible to reduce this problem to:

$$\forall x, t \{ \forall i \{ g_i(x)(t) \} \Rightarrow g_n(x)(f(t)) \}$$

Here, `=>` means material implication.

By constraining the path, it is necessary to check for the input domain. If it passes, then the path output must be checked to be `true`. However, if it fails to pass the input domain, then the output is irrelevant.

This corresponds to pre- and postconditions of computer programming.

Here is an example:

$$\forall x, y \{ add\{(> x), (> y)\}[unit \to (> x + y)] \Leftarrow\Rightarrow \backslash true \}$$

$$add : nat \times nat \to nat$$

Reducing:

$$\forall x, y, ta, tb : nat \{ ta > x \land tb > y \Rightarrow ta + tb > x + y \}$$

Test case:

$$add\{(> 2), (> 3)[unit \to (> 5)]$$
$$\forall ta, tb : nat \{ ta > 2 \land tb > 3 \Rightarrow ta + tb > 5 \}$$

$0 > 2 \land 1 > 3 \Rightarrow 1 > 5$	true
$1 > 2 \land 5 > 3 \Rightarrow 6 > 5$	true
$3 > 2 \land 3 > 3 \Rightarrow 6 > 5$	true
$3 > 2 \land 4 > 3 \Rightarrow 7 > 5$	true

The most constrained normal path proof is obtained using the higher order constrained existential path:

$\forall\ x\ \{\ \exists f\{g_i(x)\} => g_n(x)\ \}$

$\forall\ x\ \{\ \exists f\{g_i(x)\} : U \rightarrow bool\ \}$
$g_n : U \rightarrow bool$

For example, by applying this to the same problem:

$\exists add\{(> x), (> y)\} => (> x + y)$
$(> x + y + 1) => (> x + y)$
$(> 1) => (> 0)$ removing `x` and `y` on both sides of implication
true

The post-condition `(> x + y + 1)` is stronger than `(> x + y)`.

This means that the following is a tautology in path semantics:

$\forall\ x\ \{\ f\{g_i(x)\}[unit \rightarrow \exists f\{g_i(x)\}] <=> \backslash true\ \}$

The tautology has a structure such that it puts maximum constraints
for any parameterized pre- and postconditions of the function.