circom

nano

April 27, 2025

Contents

```
theory IsZero
  imports Main
begin
```

Proof that the IsZero template is correct, assuming the signals are values of some arbitrary field

```
definition is-zero :: 'a::field ⇒ 'a::field where
  is-zero in-sig ≡ if in-sig = 0 then 1 else 0
```

First we show that, if the constraints are satisfied, then the output signal is correct.

```
lemma l1:
  fixes in-sig inv-sig out-sig :: 'a::field
  defines out-sig ≡ (−in-sig)∗inv-sig + 1
  assumes in-sig∗out-sig = 0
  shows out-sig = is-zero in-sig
    — note that inv-sig is left unconstrained
  by (metis add-0 assms(1,2) is-zero-def mult-eq-0-iff mult-minus-left)
```

Next we show that the expression assigned to the inv signal satisfies the constraints

```
lemma l2:
  fixes in-sig inv-sig out-sig :: 'a::field
  defines inv-sig ≡ (if in-sig ≠ 0 then (1/in-sig) else 0)
  and out-sig ≡ (−in-sig)∗inv-sig + 1
shows in-sig∗out-sig = 0
  by (simp add: inv-sig-def out-sig-def)

end
```