

# Involution from Commutative Symmetry

by Sven Nilsen, 2020

*In this paper I prove that commutative symmetry implies involution of the symmetry operator.*

A binary operator `f` is commutative symmetric if there exists a unary operator `g` such that:

$$\forall a, b \{ f(a, b) = g(f(b, a)) \} \quad \wedge \quad \exists f \Leftrightarrow \forall g$$

Here, `g` is called the “symmetry operator”.

When `g`  $\Leftrightarrow$  id, the binary operator `f` is commutative.

When `g`  $\Leftrightarrow$  neg, the binary operator `f` is anti-commutative.

Commutative symmetry unifies the properties of commutative and anti-commutative operators.

From commutative symmetry, one can prove the following:

$$\forall a, b \{ f(a, b) = g(f(b, a)) \} \quad = \quad \forall a, b \{ g(f(a, b)) = f(b, a) \}$$

In path semantical notation:

$$f \Leftrightarrow f[\text{swap} \rightarrow g] \quad \Leftrightarrow \quad f[\text{id} \times \text{id} \rightarrow g] \Leftrightarrow f[\text{swap} \rightarrow \text{id}]$$

Proof:

$$\begin{aligned} \because \quad & \forall a, b \{ g(f(a, b)) = f(b, a) \} \\ \because \quad & \forall a, b \{ f(b, a) = g(f(a, b)) \} && \text{using } `(x = y) = (y = x)` \\ \because \quad & \forall b, a \{ f(a, b) = g(f(b, a)) \} && \text{replacing } `a \Rightarrow b` \text{ and } `b \Rightarrow a` \\ \because \quad & \forall a, b \{ f(a, b) = g(f(b, a)) \} && \text{using } ` \forall x, y \{ \dots \} = \forall y, x \{ \dots \} ` \end{aligned}$$

Now, one can use this to prove that the symmetry operator `g` is an involution:

$$g^2 \Leftrightarrow \text{id}$$

Proof:

$$\begin{aligned} \because \quad & g(g(f(a, b))) \\ \because \quad & g(f(b, a)) && \text{using } ` \forall a, b \{ g(f(a, b)) = f(b, a) \} ` \\ \because \quad & f(a, b) && \text{using } ` \forall a, b \{ f(a, b) = g(f(b, a)) \} ` \end{aligned}$$

Strictly said, this only proves `g · g{∃f}  $\Leftrightarrow$  id{∃f}`.

However, since `∃f  $\Leftrightarrow$  ∃g, g · g{∃f}  $\Leftrightarrow$  g · g{∃g}  $\Leftrightarrow$  g · g  $\Leftrightarrow$  g<sup>2</sup> and `id{∃f}  $\Leftrightarrow$  id{∃g}`.

Under this condition, `g<sup>2</sup>  $\Leftrightarrow$  id{∃g}` which can be simplified to `g<sup>2</sup>  $\Leftrightarrow$  id`.

Q.E.D.