A Formal Verification of Reversible Primitive Permutations

Giacomo Maletto

Introduction

Conventions

1. The definition

1.1 The original definition

Formalizing definitions can be quite a challenge on its own. Here is the original definition of Reversible Primitive Permutations (ORPP for short):

Definition 1.1.1 (Original Reversible Primitive Permutations)**.**
By definition, $\mathsf{ORPP} = \bigcup_{k\in\mathbb{N}} \mathsf{ORPP}^k$ is the smallest class of functions $\mathbb{N}^k \to \mathbb{N}$ such that

- The *identity* Id,

  $x \;\boxed{\mathsf{Id}}\; x$

- The *sign-change* Ne,

  $x \;\boxed{\mathsf{Ne}}\; -x$

- The *successor* Su,

  $x \;\boxed{\mathsf{Su}}\; x+1$

- The *predecessor* Pr,

  $x \;\boxed{\mathsf{Pr}}\; x-1$

- $\begin{matrix} x \\ y \end{matrix} \;\boxed{\mathsf{Sw}}\; \begin{matrix} y \\ x \end{matrix}$

- $\begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \;\boxed{f \fatsemi g}\; \begin{matrix} y_1 \\ \vdots \\ y_n \end{matrix} = \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \;\boxed{f}\;\boxed{g}\; \begin{matrix} y_1 \\ \vdots \\ y_n \end{matrix}$

- $\begin{matrix} x_1 \\ \vdots \\ x_n \\ y_1 \\ \vdots \\ y_m \end{matrix} \;\boxed{f \| g}\; \begin{matrix} w_1 \\ \vdots \\ w_n \\ z_1 \\ \vdots \\ z_m \end{matrix} = \begin{matrix} x_1 \\ \vdots \\ x_n \\ y_1 \\ \vdots \\ y_m \end{matrix} \;\begin{matrix}\boxed{f} \\ \boxed{g}\end{matrix}\; \begin{matrix} w_1 \\ \vdots \\ w_n \\ z_1 \\ \vdots \\ z_m \end{matrix}$

- $\begin{matrix} x_1 \\ \vdots \\ x_n \\ x \end{matrix}$ $\boxed{\mathsf{It}[f]}$ $\begin{matrix} y_1 \\ \vdots \\ y_n \\ x \end{matrix} = \begin{matrix} x_1 \\ \vdots \\ x_n \\ x \end{matrix} \overbrace{\boxed{f} \cdots \boxed{f}}^{|x| \text{ times}} \begin{matrix} y_1 \\ \vdots \\ y_n \\ x \end{matrix}$
- $\begin{matrix} x_1 \\ \vdots \\ x_n \\ x \end{matrix}$ $\boxed{\mathsf{If}[f, g, h]}$ $\left.\begin{matrix} y_1 \\ \vdots \\ y_n \\ x \end{matrix}\right\} = \begin{cases} f\left[x_1, \cdots, x_n\right] & \text{if } x > 0 \\ g\left[x_1, \cdots, x_n\right] & \text{if } x = 0 \\ h\left[x_1, \cdots, x_n\right] & \text{if } x < 0 \end{cases}$