## 4-phase reshufflings with 2 ports

#### September 15, 2015

This document lists 2 port, 4-phase HSE reshufflings and their implementations in PRS. By symmetry, some reshufflings are redundant. Specifically,  $[x_i \wedge y_i]$  is the same as  $[y_i \wedge x_i]$ , and  $x_o \uparrow, y_o \uparrow$  is the same as  $y_o \uparrow, x_o \uparrow$ . In addition, when the ports are both active or both passive, their names are interchangeable, which makes other reshufflings redundant. Redundant reshufflings are not included. Some implementations require a state variable. We use u as our state variable.

# 1 Active X, Active Y

This combination has 30 orderings.

```
0) x_o \uparrow; [x_i]; x_o \downarrow; [\neg x_i]; y_o \uparrow; [y_i]; y_o \downarrow; [\neg y_i]
          x_o \uparrow; [x_i]; x_o \downarrow, y_o \uparrow; [\neg x_i \land y_i]; y_o \downarrow; [\neg y_i]
    2) x_o \uparrow; [x_i]; x_o \downarrow, y_o \uparrow; [y_i]; y_o \downarrow; [\neg x_i \land \neg y_i]
    3) x_o \uparrow; [x_i]; x_o \downarrow; y_o \uparrow; [\neg x_i \land y_i]; y_o \downarrow; [\neg y_i]
    4) x_o \uparrow; [x_i]; x_o \downarrow; y_o \uparrow; [y_i]; y_o \downarrow; [\neg x_i \land \neg y_i]
    5) x_o \uparrow; [x_i]; y_o \uparrow; x_o \downarrow; [\neg x_i \land y_i]; y_o \downarrow; [\neg y_i]
    6) x_o \uparrow; [x_i]; y_o \uparrow; x_o \downarrow; [y_i]; y_o \downarrow; [\neg x_i \land \neg y_i]
    7) x_o \uparrow; [x_i]; y_o \uparrow; [y_i]; x_o \downarrow; [\neg x_i]; y_o \downarrow; [\neg y_i]
   8) x_o \uparrow; [x_i]; y_o \uparrow; [y_i]; x_o \downarrow, y_o \downarrow; [\neg x_i \land \neg y_i]
    9) x_o \uparrow; [x_i]; y_o \uparrow; [y_i]; x_o \downarrow; y_o \downarrow; [\neg x_i \land \neg y_i]
10) x_o \uparrow; [x_i]; y_o \uparrow; [y_i]; y_o \downarrow; x_o \downarrow; [\neg x_i \land \neg y_i]
11) x_o \uparrow; [x_i]; y_o \uparrow; [y_i]; y_o \downarrow; [\neg y_i]; x_o \downarrow; [\neg x_i]
12) x_o \uparrow, y_o \uparrow; [x_i]; x_o \downarrow; [\neg x_i \land y_i]; y_o \downarrow; [\neg y_i]
13) x_o \uparrow, y_o \uparrow; [x_i]; x_o \downarrow; [y_i]; y_o \downarrow; [\neg x_i \land \neg y_i]
14) x_o \uparrow, y_o \uparrow; [x_i \land y_i]; x_o \downarrow; [\neg x_i]; y_o \downarrow; [\neg y_i]
15) x_o \uparrow, y_o \uparrow; [x_i \land y_i]; x_o \downarrow, y_o \downarrow; [\neg x_i \land \neg y_i]
16) x_o \uparrow, y_o \uparrow; [x_i \land y_i]; x_o \downarrow; y_o \downarrow; [\neg x_i \land \neg y_i]
17) x_o \uparrow, y_o \uparrow; [x_i \land y_i]; y_o \downarrow; x_o \downarrow; [\neg x_i \land \neg y_i]
18) x_o \uparrow, y_o \uparrow; [x_i \land y_i]; y_o \downarrow; [\neg y_i]; x_o \downarrow; [\neg x_i]
19) x_o \uparrow, y_o \uparrow; [y_i]; y_o \downarrow; [x_i]; x_o \downarrow; [\neg x_i \land \neg y_i]
20) x_o \uparrow, y_o \uparrow; [y_i]; y_o \downarrow; [x_i \land \neg y_i]; x_o \downarrow; [\neg x_i]
21) x_o \uparrow; y_o \uparrow; [x_i]; x_o \downarrow; [\neg x_i \land y_i]; y_o \downarrow; [\neg y_i]
22) x_o \uparrow; y_o \uparrow; [x_i]; x_o \downarrow; [y_i]; y_o \downarrow; [\neg x_i \land \neg y_i]
23) x_o \uparrow; y_o \uparrow; [x_i \land y_i]; x_o \downarrow; [\neg x_i]; y_o \downarrow; [\neg y_i]
24) x_o \uparrow ; y_o \uparrow ; [x_i \land y_i] ; x_o \downarrow , y_o \downarrow ; [\neg x_i \land \neg y_i]
25) x_o \uparrow; y_o \uparrow; [x_i \land y_i]; x_o \downarrow; y_o \downarrow; [\neg x_i \land \neg y_i]
26) x_o \uparrow; y_o \uparrow; [x_i \land y_i]; y_o \downarrow; x_o \downarrow; [\neg x_i \land \neg y_i]
27) x_o \uparrow; y_o \uparrow; [x_i \land y_i]; y_o \downarrow; [\neg y_i]; x_o \downarrow; [\neg x_i]
28) x_o \uparrow; y_o \uparrow; [y_i]; y_o \downarrow; [x_i]; x_o \downarrow; [\neg x_i \land \neg y_i]
29) x_o \uparrow; y_o \uparrow; [y_i]; y_o \downarrow; [x_i \land \neg y_i]; x_o \downarrow; [\neg x_i]
```

$$\begin{array}{cccc}
\neg y_i \to x_o \uparrow & & x_o \to y_o \uparrow \\
y_o \to x_o \downarrow & & \neg x_i \to y_o \downarrow
\end{array}$$

$$\begin{array}{ccc} u & \to & x_o \uparrow & & \neg x_i \land \neg y_i & \to & u \uparrow \\ \neg u & \to & x_o \downarrow & & x_i \land y_i & \to & u \downarrow \end{array}$$

$$\begin{array}{ccc} u & \to & y_o \uparrow \\ \neg u & \to & y_o \downarrow \end{array}$$

### 2 Passive X, Passive Y

This combination has 28 orderings.

- 1)  $[x_i]; x_o \uparrow; [\neg x_i]; x_o \downarrow; [y_i]; y_o \uparrow; [\neg y_i]; y_o \downarrow$
- 2)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; x_o \downarrow, y_o \uparrow; [\neg y_i]; y_o \downarrow$
- 3)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; x_o \downarrow; y_o \uparrow; [\neg y_i]; y_o \downarrow$
- 4)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; y_o \uparrow; x_o \downarrow; [\neg y_i]; y_o \downarrow$
- 5)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; y_o \uparrow; [\neg y_i]; x_o \downarrow, y_o \downarrow$
- 6)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; y_o \uparrow; [\neg y_i]; x_o \downarrow; y_o \downarrow$
- 7)  $[x_i]; x_o \uparrow; [\neg x_i \land y_i]; y_o \uparrow; [\neg y_i]; y_o \downarrow; x_o \downarrow$
- 8)  $[x_i]; x_o \uparrow; [y_i]; y_o \uparrow; [\neg x_i]; x_o \downarrow; [\neg y_i]; y_o \downarrow$
- 9)  $[x_i]; x_o \uparrow; [y_i]; y_o \uparrow; [\neg x_i \land \neg y_i]; x_o \downarrow, y_o \downarrow$
- 10)  $[x_i]; x_o \uparrow; [y_i]; y_o \uparrow; [\neg x_i \land \neg y_i]; x_o \downarrow; y_o \downarrow$
- 11)  $[x_i]; x_o \uparrow; [y_i]; y_o \uparrow; [\neg x_i \land \neg y_i]; y_o \downarrow; x_o \downarrow$
- 12)  $[x_i]; x_o \uparrow; [y_i]; y_o \uparrow; [\neg y_i]; y_o \downarrow; [\neg x_i]; x_o \downarrow$
- 13)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; x_o \downarrow, y_o \uparrow; [\neg y_i]; y_o \downarrow$
- 14)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; x_o \downarrow; y_o \uparrow; [\neg y_i]; y_o \downarrow$
- 15)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; y_o \uparrow; x_o \downarrow; [\neg y_i]; y_o \downarrow$
- 16)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; y_o \uparrow; [\neg y_i]; x_o \downarrow, y_o \downarrow$
- 17)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; y_o \uparrow; [\neg y_i]; x_o \downarrow; y_o \downarrow$
- 18)  $[x_i \wedge y_i]; x_o \uparrow; [\neg x_i]; y_o \uparrow; [\neg y_i]; y_o \downarrow; x_o \downarrow$
- 19)  $[x_i \wedge y_i]; x_o \uparrow, y_o \uparrow; [\neg x_i]; x_o \downarrow; [\neg y_i]; y_o \downarrow$
- 20)  $[x_i \land y_i]$ ,  $x_0 \uparrow$ ,  $y_0 \uparrow$ ,  $[\neg x_i \land \neg y_i]$ ,  $x_0 \downarrow$ ,  $y_0 \downarrow$
- 21)  $[x_i \land y_i]; x_o \uparrow, y_o \uparrow; [\neg x_i \land \neg y_i]; x_o \downarrow; y_o \downarrow$
- 22)  $[x_i \wedge y_i]; x_o \uparrow, y_o \uparrow; [\neg x_i \wedge \neg y_i]; y_o \downarrow; x_o \downarrow$
- 23)  $[x_i \wedge y_i]; x_o \uparrow, y_o \uparrow; [\neg y_i]; y_o \downarrow; [\neg x_i]; x_o \downarrow$
- 24)  $[x_i \land y_i], x_o \uparrow; y_o \uparrow; [\neg x_i], y_o \downarrow; [\neg y_i], y_o \downarrow$
- 25)  $[x_i \wedge y_i]; x_o \uparrow; y_o \uparrow; [\neg x_i \wedge \neg y_i]; x_o \downarrow, y_o \downarrow$
- 26)  $[x_i \wedge y_i]; x_o \uparrow; y_o \uparrow; [\neg x_i \wedge \neg y_i]; x_o \downarrow; y_o \downarrow$
- 27)  $[x_i \wedge y_i]; x_o \uparrow; y_o \uparrow; [\neg x_i \wedge \neg y_i]; y_o \downarrow; x_o \downarrow$
- 28)  $[x_i \wedge y_i]; x_o \uparrow; y_o \uparrow; [\neg y_i]; y_o \downarrow; [\neg x_i]; x_o \downarrow$

8

$$x_i \wedge \neg y_o \rightarrow x_o \uparrow$$
  $y_i \wedge x_o \rightarrow y_o \uparrow$   $\neg x_i \wedge y_o \rightarrow x_o \downarrow$   $\neg y_i \wedge \neg x_o \rightarrow y_o \downarrow$ 

$$\begin{array}{cccc}
\neg u \to y_o \uparrow & & x_i \wedge y_i \to u \downarrow \\
u \to y_o \downarrow & & \neg x_i \wedge \neg y_i \to u \uparrow \\
\neg u \to x_o \uparrow & & \\
u \to x_o \downarrow
\end{array}$$

#### **3** Active A, Passive P

This combination has 60 orderings.

```
1) a_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i \land p_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow
   2) a_o \uparrow; [a_i]; a_o \downarrow; [p_i]; p_o \uparrow; [\neg a_i \land \neg p_i]; p_o \downarrow
   3) a_o \uparrow; [a_i]; a_o \downarrow; [p_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
   4) a_o \uparrow; [a_i \land p_i]; a_o \downarrow; [\neg a_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow
   5) a_o \uparrow; [a_i \land p_i]; a_o \downarrow, p_o \uparrow; [\neg a_i \land \neg p_i]; p_o \downarrow
   6) a_o \uparrow; [a_i \land p_i]; a_o \downarrow, p_o \uparrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
   7)
          a_o \uparrow; [a_i \land p_i]; a_o \downarrow; p_o \uparrow; [\neg a_i \land \neg p_i]; p_o \downarrow
   8) a_o \uparrow; [a_i \land p_i]; a_o \downarrow; p_o \uparrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
   9) a_o \uparrow; [a_i \land p_i]; p_o \uparrow; a_o \downarrow; [\neg a_i \land \neg p_i]; p_o \downarrow
10) a_o \uparrow; [a_i \land p_i]; p_o \uparrow; a_o \downarrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
11)
          a_o\uparrow; [a_i \land p_i]; p_o\uparrow; [\neg p_i]; a_o\downarrow; [\neg a_i]; p_o\downarrow
          a_o \uparrow; [a_i \land p_i]; p_o \uparrow; [\neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
12)
13) a_o \uparrow; [a_i \land p_i]; p_o \uparrow; [\neg p_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
          a_o\uparrow; [a_i \land p_i]; p_o\uparrow; [\neg p_i]; p_o\downarrow; a_o\downarrow; [\neg a_i]
14)
          a_o\uparrow; [p_i]; p_o\uparrow; [a_i]; a_o\downarrow; [\neg a_i \land \neg p_i]; p_o\downarrow
15)
16)
          a_o\uparrow; [p_i]; p_o\uparrow; [a_i]; a_o\downarrow; [\neg p_i]; p_o\downarrow; [\neg a_i]
17)
          a_o \uparrow; [p_i]; p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
          a_o \uparrow; [p_i]; p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
18)
          a_o\uparrow; [p_i]; p_o\uparrow; [a_i \land \neg p_i]; a_o\downarrow; p_o\downarrow; [\neg a_i]
19)
         a_o \uparrow; [p_i]; p_o \uparrow; [a_i \land \neg p_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
21) a_o \uparrow; [p_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow; [a_i]; a_o \downarrow; [\neg a_i]
22)
           [p_i]; a_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow
23) [p_i]; a_o \uparrow; [a_i]; a_o \downarrow, p_o \uparrow; [\neg a_i \land \neg p_i]; p_o \downarrow
24) [p_i]; a_o \uparrow; [a_i]; a_o \downarrow, p_o \uparrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
25) [p_i]; a_o \uparrow; [a_i]; a_o \downarrow; p_o \uparrow; [\neg a_i \land \neg p_i]; p_o \downarrow
26)
          [p_i]; a_o \uparrow; [a_i]; a_o \downarrow; p_o \uparrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
        [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; a_o \downarrow; [\neg a_i \land \neg p_i]; p_o \downarrow
27)
28) [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; a_o \downarrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
29) [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; [\neg p_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
30) [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; [\neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
\neg a_i \wedge \neg p_o \wedge u \rightarrow a_o \uparrow
                                                                   p_o \rightarrow u \uparrow
a_i \wedge \neg u
                                                                    a_i \rightarrow u \downarrow
                          \rightarrow a_o \downarrow
```

```
31) [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; [\neg p_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
32) [p_i]; a_o \uparrow; [a_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
33) [p_i]; a_o \uparrow, p_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i \land \neg p_i]; p_o \downarrow
34) [p_i]; a_o \uparrow, p_o \uparrow; [a_i]; a_o \downarrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
35) [p_i]; a_o \uparrow, p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
36) [p_i]; a_o \uparrow, p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
37) [p_i]; a_o \uparrow, p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
38) [p_i]; a_o \uparrow, p_o \uparrow; [a_i \land \neg p_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
39) [p_i]; a_o \uparrow, p_o \uparrow; [\neg p_i]; p_o \downarrow; [a_i]; a_o \downarrow; [\neg a_i]
40) [p_i]; a_o \uparrow; p_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i \land \neg p_i]; p_o \downarrow
41) [p_i]; a_o \uparrow; p_o \uparrow; [a_i]; a_o \downarrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
42) [p_i]; a_o \uparrow; p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
43) [p_i]; a_o \uparrow; p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
44) [p_i]; a_o \uparrow; p_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
45) [p_i]; a_o \uparrow; p_o \uparrow; [a_i \land \neg p_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
46) [p_i]; a_o\uparrow; p_o\uparrow; [\neg p_i]; p_o\downarrow; [a_i]; a_o\downarrow; [\neg a_i]
47) [p_i]; p_o \uparrow; a_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i \land \neg p_i]; p_o \downarrow
48) [p_i]; p_o \uparrow; a_o \uparrow; [a_i]; a_o \downarrow; [\neg p_i]; p_o \downarrow; [\neg a_i]
49) [p_i]; p_o \uparrow; a_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
50) [p_i]; p_o \uparrow; a_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
51) [p_i]; p_o \uparrow; a_o \uparrow; [a_i \land \neg p_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
52) [p_i]; p_o \uparrow; a_o \uparrow; [a_i \land \neg p_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
53) [p_i]; p_o \uparrow; a_o \uparrow; [\neg p_i]; p_o \downarrow; [a_i]; a_o \downarrow; [\neg a_i]
54) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i]; p_o \downarrow
55) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow; [a_i]; a_o \downarrow, p_o \downarrow; [\neg a_i]
56) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow; [a_i]; a_o \downarrow; p_o \downarrow; [\neg a_i]
57) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow; [a_i]; p_o \downarrow; a_o \downarrow; [\neg a_i]
58) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow, p_o \downarrow; [a_i]; a_o \downarrow; [\neg a_i]
59) [p_i]; p_o \uparrow; [\neg p_i]; a_o \uparrow; p_o \downarrow; [a_i]; a_o \downarrow; [\neg a_i]
60) [p_i]; p_o \uparrow; [\neg p_i]; p_o \downarrow; a_o \uparrow; [a_i]; a_o \downarrow; [\neg a_i]
```

1

$$\neg a_i \wedge \neg p_o \wedge u \to a_o \uparrow \qquad p_o \to u \uparrow 
a_i \wedge \neg u \to a_o \downarrow \qquad a_i \to u \downarrow 
\neg a_i \wedge p_i \wedge \neg u \to p_o \uparrow 
\neg p_i \wedge u \to p_o \downarrow$$

9

$$\begin{array}{cccc}
 \neg p_o \to a_o \uparrow & & a_i \wedge p_i & \to p_o \uparrow \\
 p_o \to a_o \downarrow & & \neg a_i \wedge \neg p_i \to p_o \downarrow
 \end{array}$$

$$\begin{array}{ccc} p_i & \rightarrow & a_o \uparrow & & a_i & \rightarrow & p_o \uparrow \\ \neg p_i & \rightarrow & a_o \downarrow & & \neg a_i & \rightarrow & p_o \downarrow \end{array}$$

$$\begin{array}{ccc} u & \to & a_o \uparrow & & & \neg a_i \wedge p_i & \to & u \uparrow \\ \neg u & \to & a_o \downarrow & & & a_i \wedge \neg p_i & \to & u \downarrow \end{array}$$

$$\begin{array}{ccc} u & \to & p_o \uparrow \\ u & \to & p_o \downarrow \end{array}$$