#|

|#

EVENT: Start with the library "mlp" using the compiled version.

```
; bcdSbi.bm: = bcdS, but with integer bits instead of booleans on the wires.
;   LESSONS:
;    - the quality of the proofs is not degraded, we usually get the same
;      case splits, except sometime with one or two more cases.
;    - the timing is degraded by 50% on average, with a range of 20% to 300%
; So in general we should stick (or start) with a boolean model of 0 and 1,
; but if for some crucial reason we have to go numerical, it's no major
; disaster.
;

;;; CIRCUIT in SUGARED form:
```

```
#|
(setq sysd '(sy-BCDSBI (x)
(Y01 S bnot x)
(Y02 S bnot x)
(Y03 S bnot YR3)
(Y04 S bnot YR1)
(Y05 S bnot YR2)
(Y06 S bnot YR3)
(Y07 S bnot YR1)
(Y08 S bnot YR3)
(Y11 S band3 Y01 YR1 YR3)
(Y12 S band3 Y02 YR2 Y03)
(Y13 S band3 Y04 Y05 Y06)
(Y14 S band3 x Y07 Y08)
(Y15 S band3 x YR1 YR3)
(Y21 S bor Y11 Y12)
(Y22 S bor Y13 Y14)
(Y23 S bor YR2 Y15)
(YR1 R 0 Y21)
(YR2 R 0 Y22)
(YR3 R 0 Y23)
(Y31 S bnot YR1)
(Y32 S bnot YR2)
(Y41 S band4 x Y31 Y32 YR3)
(Yout S bnot Y41)
))

(setq bcdSbi '( |#
; this load entered by hand, because needed in the SPEC
; comb_band.bm: Binary And combinational element
; U7-DONE
```

DEFINITION:
band $(u,\ v)$
$=$ **if** $(u = 0) \lor (v = 0)$ **then** 0
else 1 **endif**

```
; Everything below generated by: (bmcomb 'band '() '(x y))
```

DEFINITION:
s-band $(x,\ y)$
$=$ **if** empty (x) **then** E
else a (s-band (p (x), p (y)), band (l (x), l (y))) **endif**

```
;; A2-Begin-S-BAND
```

THEOREM: a2-empty-s-band
$\text{empty}\,(\text{s-band}\,(x,\ y)) = \text{empty}\,(x)$

THEOREM: a2-e-s-band
$(\text{s-band}\,(x,\ y) = \text{E}) = \text{empty}\,(x)$

THEOREM: a2-lp-s-band
$\text{len}\,(\text{s-band}\,(x,\ y)) = \text{len}\,(x)$

THEOREM: a2-lpe-s-band
$\text{eqlen}\,(\text{s-band}\,(x,\ y),\ x)$

THEOREM: a2-ic-s-band
$(\text{len}\,(x) = \text{len}\,(y))$
$\rightarrow \quad (\text{s-band}\,(\text{i}\,(c\_x,\ x),\ \text{i}\,(c\_y,\ y)) = \text{i}\,(\text{band}\,(c\_x,\ c\_y),\ \text{s-band}\,(x,\ y)))$

THEOREM: a2-lc-s-band
$(\neg\ \text{empty}\,(x)) \rightarrow (\text{l}\,(\text{s-band}\,(x,\ y)) = \text{band}\,(\text{l}\,(x),\ \text{l}\,(y)))$

THEOREM: a2-pc-s-band
$\text{p}\,(\text{s-band}\,(x,\ y)) = \text{s-band}\,(\text{p}\,(x),\ \text{p}\,(y))$

THEOREM: a2-hc-s-band
$((\neg\ \text{empty}\,(x)) \wedge (\text{len}\,(x) = \text{len}\,(y)))$
$\rightarrow \quad (\text{h}\,(\text{s-band}\,(x,\ y)) = \text{band}\,(\text{h}\,(x),\ \text{h}\,(y)))$

THEOREM: a2-bc-s-band
$(\text{len}\,(x) = \text{len}\,(y)) \rightarrow (\text{b}\,(\text{s-band}\,(x,\ y)) = \text{s-band}\,(\text{b}\,(x),\ \text{b}\,(y)))$

THEOREM: a2-bnc-s-band
$(\text{len}\,(x) = \text{len}\,(y)) \rightarrow (\text{bn}\,(n,\ \text{s-band}\,(x,\ y)) = \text{s-band}\,(\text{bn}\,(n,\ x),\ \text{bn}\,(n,\ y)))$

```
;; A2-End-S-BAND

; eof:comb_band.bm


; BM DEFINITIONS and A2 LEMMAS, generated by BMSYSD:
; comb_band3.bm: Binary And3 combinational element
; U7-DONE
```

DEFINITION:
band3 ($u1$, $u2$, $u3$)
= **if** ($u1$ = 0) ∨ ($u2$ = 0) ∨ ($u3$ = 0) **then** 0
else 1 **endif**

```
; Everything below generated by: (bmcomb 'band3 '() '(x1 x2 x3))
```

DEFINITION:
s-band3 ($x1$, $x2$, $x3$)
= **if** empty ($x1$) **then** E
else a (s-band3 (p ($x1$), p ($x2$), p ($x3$)), band3 (l ($x1$), l ($x2$), l ($x3$))) **endif**

```
;; A2-Begin-S-BAND3
```

THEOREM: a2-empty-s-band3
empty (s-band3 ($x1$, $x2$, $x3$)) = empty ($x1$)

THEOREM: a2-e-s-band3
(s-band3 ($x1$, $x2$, $x3$) = E) = empty ($x1$)

THEOREM: a2-lp-s-band3
len (s-band3 ($x1$, $x2$, $x3$)) = len ($x1$)

THEOREM: a2-lpe-s-band3
eqlen (s-band3 ($x1$, $x2$, $x3$), $x1$)

THEOREM: a2-ic-s-band3
((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$)))
→ (s-band3 (i (c_x1, $x1$), i (c_x2, $x2$), i (c_x3, $x3$))
= i (band3 (c_x1, c_x2, c_x3), s-band3 ($x1$, $x2$, $x3$)))

THEOREM: a2-lc-s-band3
(¬ empty ($x1$)) → (l (s-band3 ($x1$, $x2$, $x3$)) = band3 (l ($x1$), l ($x2$), l ($x3$)))

THEOREM: a2-pc-s-band3
p (s-band3 ($x1$, $x2$, $x3$)) = s-band3 (p ($x1$), p ($x2$), p ($x3$))

THEOREM: a2-hc-s-band3
((¬ empty ($x1$)) ∧ ((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$))))
→ (h (s-band3 ($x1$, $x2$, $x3$)) = band3 (h ($x1$), h ($x2$), h ($x3$)))

THEOREM: a2-bc-s-band3
((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$)))
→ (b (s-band3 ($x1$, $x2$, $x3$)) = s-band3 (b ($x1$), b ($x2$), b ($x3$)))

THEOREM: a2-bnc-s-band3
$((\mathrm{len}(x1) = \mathrm{len}(x2)) \wedge (\mathrm{len}(x2) = \mathrm{len}(x3)))$
$\rightarrow \quad (\mathrm{bn}(n, \text{s-band3}(x1, x2, x3)) = \text{s-band3}(\mathrm{bn}(n, x1), \mathrm{bn}(n, x2), \mathrm{bn}(n, x3)))$

```
;; A2-End-S-BAND3

; eof:comb_band3.bm

; comb_bor.bm: Binary Or combinational element
; U7-DONE
```

DEFINITION:
$\mathrm{bor}(u, v)$
$= \quad$ **if** $(u = 0) \wedge (v = 0)$ **then** 0
else 1 **endif**

```
; Everything below generated by: (bmcomb 'bor '() '(x y))
```

DEFINITION:
$\text{s-bor}(x, y)$
$= \quad$ **if** $\mathrm{empty}(x)$ **then** E
else $\mathrm{a}(\text{s-bor}(\mathrm{p}(x), \mathrm{p}(y)), \mathrm{bor}(\mathrm{l}(x), \mathrm{l}(y)))$ **endif**

```
;; A2-Begin-S-BOR
```

THEOREM: a2-empty-s-bor
$\mathrm{empty}(\text{s-bor}(x, y)) = \mathrm{empty}(x)$

THEOREM: a2-e-s-bor
$(\text{s-bor}(x, y) = \mathrm{E}) = \mathrm{empty}(x)$

THEOREM: a2-lp-s-bor
$\mathrm{len}(\text{s-bor}(x, y)) = \mathrm{len}(x)$

THEOREM: a2-lpe-s-bor
$\mathrm{eqlen}(\text{s-bor}(x, y), x)$

THEOREM: a2-ic-s-bor
$(\mathrm{len}(x) = \mathrm{len}(y))$
$\rightarrow \quad (\text{s-bor}(\mathrm{i}(c\_x, x), \mathrm{i}(c\_y, y)) = \mathrm{i}(\mathrm{bor}(c\_x, c\_y), \text{s-bor}(x, y)))$

THEOREM: a2-lc-s-bor
$(\neg\, \mathrm{empty}(x)) \rightarrow (\mathrm{l}(\text{s-bor}(x, y)) = \mathrm{bor}(\mathrm{l}(x), \mathrm{l}(y)))$

THEOREM: a2-pc-s-bor
$p(\text{s-bor}(x, y)) = \text{s-bor}(p(x), p(y))$

THEOREM: a2-hc-s-bor
$((\neg\, \text{empty}(x)) \wedge (\text{len}(x) = \text{len}(y)))$
$\rightarrow \quad (h(\text{s-bor}(x, y)) = \text{bor}(h(x), h(y)))$

THEOREM: a2-bc-s-bor
$(\text{len}(x) = \text{len}(y)) \rightarrow (b(\text{s-bor}(x, y)) = \text{s-bor}(b(x), b(y)))$

THEOREM: a2-bnc-s-bor
$(\text{len}(x) = \text{len}(y)) \rightarrow (\text{bn}(n, \text{s-bor}(x, y)) = \text{s-bor}(\text{bn}(n, x), \text{bn}(n, y)))$

```
;; A2-End-S-BOR

; eof:comb_bor.bm

; comb_band4.bm: Binary And4 combinational element
; U7-DONE
```

DEFINITION:
$\text{band4}(u1, u2, u3, u4)$
$=$ **if** $(u1 = 0) \vee (u2 = 0) \vee (u3 = 0) \vee (u4 = 0)$ **then** 0
else 1 **endif**

```
; Everything below generated by: (bmcomb 'band4 '() '(x1 x2 x3 x4))
```

DEFINITION:
$\text{s-band4}(x1, x2, x3, x4)$
$=$ **if** $\text{empty}(x1)$ **then** E
else $a(\text{s-band4}(p(x1), p(x2), p(x3), p(x4)),$
$\text{band4}(l(x1), l(x2), l(x3), l(x4)))$ **endif**

```
;; A2-Begin-S-BAND4
```

THEOREM: a2-empty-s-band4
$\text{empty}(\text{s-band4}(x1, x2, x3, x4)) = \text{empty}(x1)$

THEOREM: a2-e-s-band4
$(\text{s-band4}(x1, x2, x3, x4) = \text{E}) = \text{empty}(x1)$

THEOREM: a2-lp-s-band4
$\text{len}(\text{s-band4}(x1, x2, x3, x4)) = \text{len}(x1)$

THEOREM: a2-lpe-s-band4
eqlen (s-band4 ($x1$, $x2$, $x3$, $x4$), $x1$)

THEOREM: a2-ic-s-band4
((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$)) ∧ (len ($x3$) = len ($x4$)))
→ (s-band4 (i (c_x1, $x1$), i (c_x2, $x2$), i (c_x3, $x3$), i (c_x4, $x4$))
= i (band4 (c_x1, c_x2, c_x3, c_x4), s-band4 ($x1$, $x2$, $x3$, $x4$)))

THEOREM: a2-lc-s-band4
(¬ empty ($x1$))
→ (l (s-band4 ($x1$, $x2$, $x3$, $x4$)) = band4 (l ($x1$), l ($x2$), l ($x3$), l ($x4$)))

THEOREM: a2-pc-s-band4
p (s-band4 ($x1$, $x2$, $x3$, $x4$)) = s-band4 (p ($x1$), p ($x2$), p ($x3$), p ($x4$))

THEOREM: a2-hc-s-band4
((¬ empty ($x1$))
∧ ((len ($x1$) = len ($x2$))
∧ (len ($x2$) = len ($x3$))
∧ (len ($x3$) = len ($x4$))))
→ (h (s-band4 ($x1$, $x2$, $x3$, $x4$)) = band4 (h ($x1$), h ($x2$), h ($x3$), h ($x4$)))

THEOREM: a2-bc-s-band4
((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$)) ∧ (len ($x3$) = len ($x4$)))
→ (b (s-band4 ($x1$, $x2$, $x3$, $x4$)) = s-band4 (b ($x1$), b ($x2$), b ($x3$), b ($x4$)))

THEOREM: a2-bnc-s-band4
((len ($x1$) = len ($x2$)) ∧ (len ($x2$) = len ($x3$)) ∧ (len ($x3$) = len ($x4$)))
→ (bn (n, s-band4 ($x1$, $x2$, $x3$, $x4$))
= s-band4 (bn (n, $x1$), bn (n, $x2$), bn (n, $x3$), bn (n, $x4$)))

```
;; A2-End-S-BAND4

; eof:comb_band4.bm

; comb_bnot.bm: Binary Not combinational element
; U7-DONE
```

DEFINITION:
bnot (u)
= **if** $u = 0$ **then** 1
else 0 **endif**

```
; Everything below generated by: (bmcomb 'bnot '() '(x))
```

DEFINITION:
s-bnot (x)
$=$ **if** empty (x) **then** E
else a (s-bnot (p (x)), bnot (l (x))) **endif**

```
;; A2-Begin-S-BNOT
```

THEOREM: a2-empty-s-bnot
empty (s-bnot (x)) $=$ empty (x)

THEOREM: a2-e-s-bnot
(s-bnot (x) $=$ E) $=$ empty (x)

THEOREM: a2-lp-s-bnot
len (s-bnot (x)) $=$ len (x)

THEOREM: a2-lpe-s-bnot
eqlen (s-bnot (x), x)

THEOREM: a2-ic-s-bnot
s-bnot (i (c_x, x)) $=$ i (bnot (c_x), s-bnot (x))

THEOREM: a2-lc-s-bnot
($\neg$ empty (x)) $\rightarrow$ (l (s-bnot (x)) $=$ bnot (l (x)))

THEOREM: a2-pc-s-bnot
p (s-bnot (x)) $=$ s-bnot (p (x))

THEOREM: a2-hc-s-bnot
($\neg$ empty (x)) $\rightarrow$ (h (s-bnot (x)) $=$ bnot (h (x)))

THEOREM: a2-bc-s-bnot
b (s-bnot (x)) $=$ s-bnot (b (x))

THEOREM: a2-bnc-s-bnot
bn (n, s-bnot (x)) $=$ s-bnot (bn (n, x))

```
;; A2-End-S-BNOT

; eof:comb_bnot.bm
```

DEFINITION:
topor-sy-bcdsbi (ln)

```
=   if ln = 'y01 then 1
    elseif ln = 'y02 then 1
    elseif ln = 'y03 then 1
    elseif ln = 'y04 then 1
    elseif ln = 'y05 then 1
    elseif ln = 'y06 then 1
    elseif ln = 'y07 then 1
    elseif ln = 'y08 then 1
    elseif ln = 'y11 then 2
    elseif ln = 'y12 then 2
    elseif ln = 'y13 then 2
    elseif ln = 'y14 then 2
    elseif ln = 'y15 then 1
    elseif ln = 'y21 then 3
    elseif ln = 'y22 then 3
    elseif ln = 'y23 then 2
    elseif ln = 'yr1 then 0
    elseif ln = 'yr2 then 0
    elseif ln = 'yr3 then 0
    elseif ln = 'y31 then 1
    elseif ln = 'y32 then 1
    elseif ln = 'y41 then 2
    elseif ln = 'yout then 3
    else 0 endif
```

DEFINITION:
sy-bcdsbi (ln, x)

```
=   if ln = 'y01 then s-bnot (x)
    elseif ln = 'y02 then s-bnot (x)
    elseif ln = 'y03 then s-bnot (sy-bcdsbi ('yr3, x))
    elseif ln = 'y04 then s-bnot (sy-bcdsbi ('yr1, x))
    elseif ln = 'y05 then s-bnot (sy-bcdsbi ('yr2, x))
    elseif ln = 'y06 then s-bnot (sy-bcdsbi ('yr3, x))
    elseif ln = 'y07 then s-bnot (sy-bcdsbi ('yr1, x))
    elseif ln = 'y08 then s-bnot (sy-bcdsbi ('yr3, x))
    elseif ln = 'y11
    then s-band3 (sy-bcdsbi ('y01, x),
                  sy-bcdsbi ('yr1, x),
                  sy-bcdsbi ('yr3, x))
    elseif ln = 'y12
    then s-band3 (sy-bcdsbi ('y02, x),
                  sy-bcdsbi ('yr2, x),
```

```
                        sy-bcdsbi ('y03, x))
    elseif ln = 'y13
    then s-band3 (sy-bcdsbi ('y04, x),
                  sy-bcdsbi ('y05, x),
                  sy-bcdsbi ('y06, x))
    elseif ln = 'y14
    then s-band3 (x, sy-bcdsbi ('y07, x), sy-bcdsbi ('y08, x))
    elseif ln = 'y15
    then s-band3 (x, sy-bcdsbi ('yr1, x), sy-bcdsbi ('yr3, x))
    elseif ln = 'y21
    then s-bor (sy-bcdsbi ('y11, x), sy-bcdsbi ('y12, x))
    elseif ln = 'y22
    then s-bor (sy-bcdsbi ('y13, x), sy-bcdsbi ('y14, x))
    elseif ln = 'y23
    then s-bor (sy-bcdsbi ('yr2, x), sy-bcdsbi ('y15, x))
    elseif ln = 'yr1
    then if empty (x) then E
         else i (0, sy-bcdsbi ('y21, p (x))) endif
    elseif ln = 'yr2
    then if empty (x) then E
         else i (0, sy-bcdsbi ('y22, p (x))) endif
    elseif ln = 'yr3
    then if empty (x) then E
         else i (0, sy-bcdsbi ('y23, p (x))) endif
    elseif ln = 'y31 then s-bnot (sy-bcdsbi ('yr1, x))
    elseif ln = 'y32 then s-bnot (sy-bcdsbi ('yr2, x))
    elseif ln = 'y41
    then s-band4 (x,
                  sy-bcdsbi ('y31, x),
                  sy-bcdsbi ('y32, x),
                  sy-bcdsbi ('yr3, x))
    elseif ln = 'yout then s-bnot (sy-bcdsbi ('y41, x))
    else sfix (x) endif
```

```
;; A2-Begin-SY-BCDSBI
```

THEOREM: a2-empty-sy-bcdsbi
empty (sy-bcdsbi (ln, x)) = empty (x)

THEOREM: a2-e-sy-bcdsbi
(sy-bcdsbi (ln, x) = E) = empty (x)

THEOREM: a2-lp-sy-bcdsbi
len (sy-bcdsbi (ln, x)) = len (x)

THEOREM: a2-lpe-sy-bcdsbi
eqlen (sy-bcdsbi (ln, x), x)

THEOREM: a2-pc-sy-bcdsbi
p (sy-bcdsbi (ln, x)) = sy-bcdsbi (ln, p (x))

```
;; A2-End-SY-BCDSBI

;;; Circuit CORRECTNESS /Paillet:

; BCD-bits defines a correct binary coded decimal, b0 is most-significant.
```

DEFINITION:
bcd-bits ($b0$, $b1$, $b2$, $b3$) = (($b0$ = 0) ∨ (($b1$ = 0) ∧ ($b2$ = 0)))

```
; CORRECTNESS:

;;; WHAT PAILLET ACTUALLY PROVES:
```

DEFINITION:
```
sy-b2i (ln, x)
=   if ln = 'yr1
    then if empty (x)  then E
         else i (0,
                 s-bor (s-band3 (s-bnot (p (x)),
                                 sy-b2i ('yr1, p (x)),
                                 sy-b2i ('yr3, p (x))),
                        s-band3 (s-bnot (p (x)),
                                 sy-b2i ('yr2, p (x)),
                                 s-bnot (sy-b2i ('yr3, p (x)))))) endif
    elseif ln = 'yr2
    then if empty (x)  then E
         else i (0,
                 s-bor (s-band3 (s-bnot (sy-b2i ('yr1, p (x))),
                                 s-bnot (sy-b2i ('yr2, p (x))),
                                 s-bnot (sy-b2i ('yr3, p (x)))),
                        s-band3 (p (x),
                                 s-bnot (sy-b2i ('yr1, p (x))),
                                 s-bnot (sy-b2i ('yr3, p (x)))))) endif
    elseif ln = 'yr3
    then if empty (x)  then E
         else i (0,
                 s-bor (sy-b2i ('yr2, p (x)),
                        s-band3 (p (x),
```

sy-b2i ('yr1, p (x)),
sy-b2i ('yr3, p (x))))) **endif**
else sfix (x) **endif**

```
; B2 is just a GENERALIZED sysd, and our A2 lemmas should still be true:
; The following were generated by:
; (vp (bma2sysd-aux 'sy-b2i 'sy-b2i '(x) '(band3 bor band4 bnot)))
; with A2-PC preemptively disabled.

;; A2-Begin-SY-B2I
```

THEOREM: a2-empty-sy-b2i
empty (sy-b2i (ln, x)) = empty (x)

THEOREM: a2-e-sy-b2i
(sy-b2i (ln, x) = E) = empty (x)

THEOREM: a2-lp-sy-b2i
len (sy-b2i (ln, x)) = len (x)

THEOREM: a2-lpe-sy-b2i
eqlen (sy-b2i (ln, x), x)

```
;(PROVE-LEMMA A2-PC-SY-B2I (REWRITE)
;    (EQUAL (P (SY-B2I LN X)) (SY-B2I LN (P X)))
;    ((DISABLE S-BAND3 S-BOR S-BAND4 S-BNOT A2-IC-S-BAND3 A2-IC-S-BOR
;              A2-IC-S-BAND4 A2-IC-S-BNOT)))

;; A2-End-SY-B2I

; BCDS-is-B2i is the essence of this simplification.
```

THEOREM: bcdsbi-is-b2i
(sy-bcdsbi ('yr1, x) = sy-b2i ('yr1, x))
$\land$ (sy-bcdsbi ('yr2, x) = sy-b2i ('yr2, x))
$\land$ (sy-bcdsbi ('yr3, x) = sy-b2i ('yr3, x))

```
; at this point we should never need SY-BCDSBI anymore:
```

EVENT: Disable sy-bcdsbi.

```
; and also he does the expansion for Yout once and for all:
; Note: A-POSTERIORI analysis indicates that this lemma is not really useful
; to BM, which is usual, since it's just a non-recursive rewrite, and we might
; as well give the expand hint at the right place.
```

THEOREM: bcdsbi-eq-yout

$$
\begin{aligned}
&\text{sy-bcdsbi}(\texttt{'yout}, x)\\
=\ &\text{s-bnot}(\text{s-band4}(x,\\
&\qquad\qquad \text{s-bnot}(\text{sy-b2i}(\texttt{'yr1}, x)),\\
&\qquad\qquad \text{s-bnot}(\text{sy-b2i}(\texttt{'yr2}, x)),\\
&\qquad\qquad \text{sy-b2i}(\texttt{'yr3}, x)))
\end{aligned}
$$

```
;; SECOND, he proves things about his DEROULEMENTS:
; note: all thms below are "one-shot", i.e. disabled and enabled explicitely
; NOTE: at this point we express everything in terms of B2; obviously
;       with BCDSBI-IS-B2i we can carry everything over.  This follows Paillet.
```

THEOREM: bcdsbi-paillet-1

$$
\begin{aligned}
&(\text{len}(x) = \texttt{1})\\
\rightarrow\ &((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x)) = \texttt{0})\\
&\ \wedge\ (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x)) = \texttt{0})\\
&\ \wedge\ (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x)) = \texttt{0}))
\end{aligned}
$$

EVENT: Disable bcdsbi-paillet-1.

THEOREM: bcdsbi-paillet-1out

$$(\text{len}(x) = \texttt{1}) \rightarrow (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x)) = \texttt{1})$$

EVENT: Disable bcdsbi-paillet-1out.

THEOREM: bcdsbi-paillet-2

$$
\begin{aligned}
&(\text{len}(x) = \texttt{2})\\
\rightarrow\ &((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x)) = \texttt{0})\\
&\ \wedge\ (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x)) = \texttt{1})\\
&\ \wedge\ (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x)) = \texttt{0}))
\end{aligned}
$$

EVENT: Disable bcdsbi-paillet-2.

THEOREM: bcdsbi-paillet-2out

$$(\text{len}(x) = \texttt{2}) \rightarrow (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x)) = \texttt{1})$$

EVENT: Disable bcdsbi-paillet-2out.

```
; Note that the "bitp" hyp is not explicit in Paillet...
```

THEOREM: bcdsbi-paillet-3

$((\text{len}(x) = \texttt{3}) \wedge \text{s-bitp}(x))$
$\rightarrow \quad ((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x)) = \text{bnot}(\text{l}(\text{p}(x))))$
$\quad\quad \wedge \quad (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x)) = \text{l}(\text{p}(x)))$
$\quad\quad \wedge \quad (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x)) = \texttt{1}))$

EVENT: Disable bcdsbi-paillet-3.

THEOREM: bcdsbi-paillet-3out
$((\text{len}(x) = \texttt{3}) \wedge \text{s-bitp}(x)) \rightarrow (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x)) = \texttt{1})$

EVENT: Disable bcdsbi-paillet-3out.

THEOREM: bcdsbi-paillet-4
$((\text{len}(x) = \texttt{4}) \wedge \text{s-bitp}(x))$
$\rightarrow \quad ((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x)) = \text{band}(\text{bnot}(\text{l}(\text{p}(x))), \text{bnot}(\text{l}(\text{p}(\text{p}(x))))))$
$\quad\quad \wedge \quad (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x)) = \texttt{0})$
$\quad\quad \wedge \quad (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x))$
$\quad\quad\quad\quad = \quad \text{bor}(\text{l}(\text{p}(\text{p}(x))), \text{band}(\text{l}(\text{p}(x)), \text{bnot}(\text{l}(\text{p}(\text{p}(x))))))))$

EVENT: Disable bcdsbi-paillet-4.

```
; and his conclusion:
```

THEOREM: bcdsbi-paillet-4out
$((\text{len}(x) = \texttt{4}) \wedge \text{s-bitp}(x))$
$\rightarrow \quad (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x))$
$\quad\quad = \quad \text{bor}(\text{bnot}(\text{l}(x)), \text{band}(\text{bnot}(\text{l}(\text{p}(x))), \text{bnot}(\text{l}(\text{p}(\text{p}(x)))))))$

EVENT: Disable bcdsbi-paillet-4out.

```
; from which he leaves to the reader the real conclusion:
```

THEOREM: bcdsbi-paillet-4out-correct
$((\text{len}(x) = \texttt{4}) \wedge \text{s-bitp}(x))$
$\rightarrow \quad (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x))$
$\quad\quad = \quad \text{bobi}(\text{bcd-bits}(\text{l}(x), \text{l}(\text{p}(x)), \text{l}(\text{p}(\text{p}(x))), \text{l}(\text{p}(\text{p}(\text{p}(x)))))))$

EVENT: Disable bcdsbi-paillet-4out-correct.

```
; and the last "re-initialization" condition:
```

THEOREM: bcdsbi-paillet-5
$((\text{len}(x) = \texttt{5}) \land \text{s-bitp}(x))$
$\rightarrow ((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x)) = \texttt{0})$
$\land (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x)) = \texttt{0})$
$\land (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x)) = \texttt{0}))$

EVENT: Disable bcdsbi-paillet-5.

```
;;; WHAT I CAN PROVE! :
```

THEOREM: bcdsbi-paillet-r-correct
$((\neg \text{empty}(x)) \land \text{s-bitp}(x))$
$\rightarrow ((\text{l}(\text{sy-b2i}(\texttt{'yr1}, x))$
$= \textbf{if } (\text{len}(x) \textbf{ mod } 4) = \texttt{1} \textbf{ then } \texttt{0}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{2} \textbf{ then } \texttt{0}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{3} \textbf{ then } \text{bnot}(\text{l}(\text{p}(x)))$
$\textbf{else } \text{band}(\text{bnot}(\text{l}(\text{p}(x))), \text{bnot}(\text{l}(\text{p}(\text{p}(x))))) \textbf{ endif})$
$\land (\text{l}(\text{sy-b2i}(\texttt{'yr2}, x))$
$= \textbf{if } (\text{len}(x) \textbf{ mod } 4) = \texttt{1} \textbf{ then } \texttt{0}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{2} \textbf{ then } \texttt{1}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{3} \textbf{ then } \text{l}(\text{p}(x))$
$\textbf{else } \texttt{0} \textbf{ endif})$
$\land (\text{l}(\text{sy-b2i}(\texttt{'yr3}, x))$
$= \textbf{if } (\text{len}(x) \textbf{ mod } 4) = \texttt{1} \textbf{ then } \texttt{0}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{2} \textbf{ then } \texttt{0}$
$\textbf{elseif } (\text{len}(x) \textbf{ mod } 4) = \texttt{3} \textbf{ then } \texttt{1}$
$\textbf{else } \text{bor}(\text{l}(\text{p}(\text{p}(x))),$
$\text{band}(\text{l}(\text{p}(x)), \text{bnot}(\text{l}(\text{p}(\text{p}(x)))))) \textbf{ endif}))$

```
; and finally, the true, general correctness of Paillet#5 :
```

THEOREM: bcdsbi-paillet-yout-correct
$((\neg \text{empty}(x)) \land \text{s-bitp}(x))$
$\rightarrow (\text{l}(\text{sy-bcdsbi}(\texttt{'yout}, x))$
$= \textbf{if } (\text{len}(x) \textbf{ mod } 4) = \texttt{0}$
$\textbf{then } \text{bobi}(\text{bcd-bits}(\text{l}(x), \text{l}(\text{p}(x)), \text{l}(\text{p}(\text{p}(x))), \text{l}(\text{p}(\text{p}(\text{p}(x))))))$
$\textbf{else } \texttt{1} \textbf{ endif})$

```
; eof: bcdsbi.bm
;))
```

Index

a, 2, 4–6, 8
a2-bc-s-band, 3
a2-bc-s-band3, 4
a2-bc-s-band4, 7
a2-bc-s-bnot, 8
a2-bc-s-bor, 6
a2-bnc-s-band, 3
a2-bnc-s-band3, 5
a2-bnc-s-band4, 7
a2-bnc-s-bnot, 8
a2-bnc-s-bor, 6
a2-e-s-band, 3
a2-e-s-band3, 4
a2-e-s-band4, 6
a2-e-s-bnot, 8
a2-e-s-bor, 5
a2-e-sy-b2i, 12
a2-e-sy-bcdsbi, 10
a2-empty-s-band, 3
a2-empty-s-band3, 4
a2-empty-s-band4, 6
a2-empty-s-bnot, 8
a2-empty-s-bor, 5
a2-empty-sy-b2i, 12
a2-empty-sy-bcdsbi, 10
a2-hc-s-band, 3
a2-hc-s-band3, 4
a2-hc-s-band4, 7
a2-hc-s-bnot, 8
a2-hc-s-bor, 6
a2-ic-s-band, 3
a2-ic-s-band3, 4
a2-ic-s-band4, 7
a2-ic-s-bnot, 8
a2-ic-s-bor, 5
a2-lc-s-band, 3
a2-lc-s-band3, 4
a2-lc-s-band4, 7
a2-lc-s-bnot, 8
a2-lc-s-bor, 5
a2-lp-s-band, 3
a2-lp-s-band3, 4
a2-lp-s-band4, 6
a2-lp-s-bnot, 8
a2-lp-s-bor, 5
a2-lp-sy-b2i, 12
a2-lp-sy-bcdsbi, 10
a2-lpe-s-band, 3
a2-lpe-s-band3, 4
a2-lpe-s-band4, 7
a2-lpe-s-bnot, 8
a2-lpe-s-bor, 5
a2-lpe-sy-b2i, 12
a2-lpe-sy-bcdsbi, 11
a2-pc-s-band, 3
a2-pc-s-band3, 4
a2-pc-s-band4, 7
a2-pc-s-bnot, 8
a2-pc-s-bor, 6
a2-pc-sy-bcdsbi, 11

b, 3, 4, 6–8
band, 2, 3, 14, 15
band3, 4
band4, 6, 7
bcd-bits, 11, 14, 15
bcdsbi-eq-yout, 13
bcdsbi-is-b2i, 12
bcdsbi-paillet-1, 13
bcdsbi-paillet-1out, 13
bcdsbi-paillet-2, 13
bcdsbi-paillet-2out, 13
bcdsbi-paillet-3, 14
bcdsbi-paillet-3out, 14
bcdsbi-paillet-4, 14
bcdsbi-paillet-4out, 14
bcdsbi-paillet-4out-correct, 14
bcdsbi-paillet-5, 15
bcdsbi-paillet-r-correct, 15
bcdsbi-paillet-yout-correct, 15
bn, 3, 5–8
bnot, 7, 8, 14, 15

bobi, 14, 15
bor, 5, 6, 14, 15

e, 2–6, 8, 10–12
empty, 2–8, 10–12, 15
eqlen, 3–5, 7, 8, 11, 12

h, 3, 4, 6–8

i, 3–5, 7, 8, 10–12

l, 2–8, 13–15
len, 3–8, 10, 12–15

p, 2–8, 10–12, 14, 15

s-band, 2, 3
s-band3, 4, 5, 9–12
s-band4, 6, 7, 10, 13
s-bitp, 14, 15
s-bnot, 8–11, 13
s-bor, 5, 6, 10–12
sfix, 10, 12
sy-b2i, 11–15
sy-bcdsbi, 9–15

topor-sy-bcdsbi, 9