Chapter 3
Logical Operations

In this chapter, we define and analyze the four basic logical operations: the unary "not", or complement, and the binary "and", "inclusive or" and "exclusive or". These are commonly known as *bit-wise* operations, as each one may be computed by performing a certain operation on each bit of its argument (in the unary case) or each pair of corresponding bits of its arguments (for binary operations). For example, the logical "and" x & y of two bit vectors may be specified in a bit-wise manner as the bit vector z such that for all $k \in \mathbb{N}$, $z[k] = 1$ iff $x[k] = y[k] = 1$.

In the context of our formalization, however, the logical operations are more naturally defined as arithmetic functions: the complement is constructed as an arithmetic difference and the binary operations are defined by recursive formulas, which facilitate inductive proofs of their relevant properties. Among these are the bit-wise characterizations, as represented by Lemmas 3.7 and 3.20.

3.1 Binary Operations

Following standard RTL syntax, we denote "and", "inclusive or" and "exclusive or" with the infix symbols &, |, and ^, respectively.

Definition 3.1 For all $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,

$$\text{(a)}\ \ x \ \&\ y = \begin{cases} 0 & \text{if } x = 0 \text{ or } y = 0 \\ x & \text{if } x = y \\ 2 \cdot (\lfloor x/2 \rfloor \ \&\ \lfloor y/2 \rfloor) + (x \bmod 2) \ \&\ (y \bmod 2) & \text{otherwise,} \end{cases}$$

$$\text{(b)}\ \ x \mid y = \begin{cases} y & \text{if } x = 0 \text{ or } x = y \\ x & \text{if } y = 0 \\ 2 \cdot (\lfloor x/2 \rfloor \mid \lfloor y/2 \rfloor) + (x \bmod 2) \mid (y \bmod 2) & \text{otherwise;} \end{cases}$$

D. M. Russinoff, *Formal Verification of Floating-Point Hardware Design*,
https://doi.org/10.1007/978-3-319-95513-1_3

$$\text{(c)}\ \ x \mathbin{\hat{}} y = \begin{cases} y & \text{if } x = 0 \\ x & \text{if } y = 0 \\ 0 & \text{if } x = y \\ 2 \cdot (\lfloor x/2 \rfloor \mathbin{\hat{}} \lfloor y/2 \rfloor) + (x \bmod 2) \mathbin{\hat{}} (y \bmod 2) & \text{otherwise.} \end{cases}$$

It is not obvious that these are admissible recursive definitions, i.e., that each of them is satisfied by a unique function. To establish this, it suffices to demonstrate the existence of a *measure* function $\mu : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ that strictly decreases on each recursive call. Thus, we define

$$\mu(x, y) = \begin{cases} 0 & \text{if } x = y \\ |xy| & \text{if } x \neq y. \end{cases}$$

For the admissibility of each of the three definitions, we must show that μ satisfies the following two inequalities, corresponding to the two recursive calls, under the restrictions $x \neq 0$, $y \neq 0$, and $x \neq y$:

(1) $\mu(\lfloor x/2 \rfloor, \lfloor y/2 \rfloor) < \mu(x, y)$.
(2) $\mu(x \bmod 2, y \bmod 2) < \mu(x, y)$..

Since the restrictions imply that at least one of x and y is neither 0 nor -1, (1) follows from Lemma 1.3. To establish (2), note that either $x \bmod 2 = 0$, $y \bmod 2 = 0$, or $x \bmod 2 = 1 = y \bmod 2$. In any case,

$$\mu(x \bmod 2, y \bmod 2) = 0 < |xy| = \mu(x, y).$$

The proof of the following is a typical inductive argument based on the recursion of Definition 3.1 (a).

Lemma 3.1 *If $x \in \mathbb{N}$ and $y \in \mathbb{Z}$, then $0 \leq x \mathbin{\&} y \leq x$.*

Proof We may assume that $x \neq 0$, $y \neq 0$, and $x \neq y$. Thus,

$$x \mathbin{\&} y = 2(\lfloor x/2 \rfloor \mathbin{\&} \lfloor y/2 \rfloor) + x \bmod 2 \mathbin{\&} y \bmod 2$$

and by induction,

$$0 \leq x \mathbin{\&} y \leq 2\lfloor x/2 \rfloor + x \bmod 2 = x.$$

□

Corollary 3.2 *If x is an n-bit vector and $y \in \mathbb{Z}$, then $x \mathbin{\&} y$ is an n-bit vector.*

Proof By Lemma 3.1, $0 \leq x \mathbin{\&} y \leq x < 2^n$ □

Lemma 3.3 *If x and y and n-bit vectors, then so are $x \mid y$ and $x \mathbin{\hat{}} y$.*

Proof The same argument applies to both operations. The claim is trivial if $n = 0$, $x = 0$, $y = 0$, or $x = y$. In all other cases, $\lfloor x/2 \rfloor$ and $\lfloor y/2 \rfloor$ are $(n-1)$-bit vectors

and by induction, so is, for example, $\lfloor x/2 \rfloor \mid \lfloor y/2 \rfloor$. Thus,

$$x \mid y = 2(\lfloor x/2 \rfloor \mid \lfloor y/2 \rfloor) + (x \bmod 2) \mid (y \bmod 2) \leq 2 \cdot (2^{n-1} - 1) + 1 < 2^n.$$

□

Lemma 3.4 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $n \in \mathbb{N}$,*

(a) $(x \,\&\, y) \bmod 2^n = (x \bmod 2^n) \,\&\, (y \bmod 2^n)$;
(b) $(x \mid y) \bmod 2^n = (x \bmod 2^n) \mid (y \bmod 2^n)$;
(c) $(x \,\hat{}\, y) \bmod 2^n = (x \bmod 2^n) \,\hat{}\, (y \bmod 2^n)$.

Proof We present the proof for (a); (b) and (c) are similar.

We may assume that $n > 0$, $x \neq 0$, $y \neq 0$, and $x \neq y$. By Definition 3.1 (a) and Lemma 1.22,

$$\begin{aligned}
&(x \,\&\, y) \bmod 2^n \\
&= (2 \cdot (\lfloor x/2 \rfloor \,\&\, \lfloor y/2 \rfloor) + (x \bmod 2) \,\&\, (y \bmod 2)) \bmod 2^n \\
&= \big((2 \cdot (\lfloor x/2 \rfloor \,\&\, \lfloor y/2 \rfloor)) \bmod 2^n + (x \bmod 2) \,\&\, (y \bmod 2)\big) \bmod 2^n.
\end{aligned}$$

By induction and Lemmas 1.18, 2.3, and 2.13, the first addend may be written as

$$\begin{aligned}
(2 \cdot (\lfloor x/2 \rfloor \,\&\, \lfloor y/2 \rfloor)) \bmod 2^n &= 2 \cdot \Big((\lfloor x/2 \rfloor \,\&\, \lfloor y/2 \rfloor) \bmod 2^{n-1}\Big) \\
&= 2 \cdot \Big((\lfloor x/2 \rfloor \bmod 2^{n-1}) \,\&\, (\lfloor y/2 \rfloor \bmod 2^{n-1})\Big) \\
&= 2 \cdot (\lfloor x/2 \rfloor [n-2:0] \,\&\, \lfloor y/2 \rfloor [n-2:0]) \\
&= 2 \cdot (\lfloor x[n-1:0]/2 \rfloor \,\&\, \lfloor y[n-1:0]/2 \rfloor),
\end{aligned}$$

and by Lemmas 2.22 and 2.31, the second addend is

$$\begin{aligned}
(x \bmod 2) \,\&\, (y \bmod 2) &= x[0] \,\&\, y[0] = x[n-1:0][0] \,\&\, y[n-1:0][0] \\
&= (x[n-1:0] \bmod 2) \,\&\, (y[n-1:0] \bmod 2).
\end{aligned}$$

Thus, by Definition 3.1 (a) and Lemmas 3.2 and 2.3,

$$\begin{aligned}
(x \,\&\, y) \bmod 2^n &= (x[n-1:0] \,\&\, y[n-1:0]) \bmod 2^n \\
&= x[n-1:0] \,\&\, y[n-1:0] \\
&= (x \bmod 2^n) \,\&\, (y \bmod 2^n).
\end{aligned}$$

□

Lemma 3.5 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $n \in \mathbb{N}$,*

(a) $\lfloor (x \,\&\, y)/2^n \rfloor = \lfloor x/2^n \rfloor \,\&\, \lfloor y/2^n \rfloor$;
(b) $\lfloor (x \mid y)/2^n \rfloor = \lfloor x/2^n \rfloor \mid \lfloor y/2^n \rfloor$;
(c) $\lfloor (x \,\hat{}\, y)/2^n \rfloor = \lfloor x/2^n \rfloor \,\hat{}\, \lfloor y/2^n \rfloor$.

Proof We present the proof for (a); (b) and (c) are similar.

We may assume that $n > 0$, $x \neq 0$, $y \neq 0$, and $x \neq y$. By Lemma 1.2, induction, and Definition 3.1 (a),

$$\begin{aligned}
\lfloor (x \,\&\, y)/2^n \rfloor &= \left\lfloor \lfloor (x \,\&\, y)/2^{n-1} \rfloor /2 \right\rfloor \\
&= \left\lfloor (\lfloor x/2^{n-1} \rfloor \,\&\, \lfloor y/2^{n-1} \rfloor)/2 \right\rfloor \\
&= \left\lfloor \lfloor x/2^{n-1} \rfloor /2 \rfloor \,\&\, \lfloor x/2^{n-1} \rfloor /2 \rfloor \right\rfloor \\
&= \left\lfloor x/2^n \rfloor \,\&\, \lfloor y/2^n \right\rfloor .
\end{aligned}$$

□

All three binary logical operators commute with the bit slice operator:

Lemma 3.6 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $i \in \mathbb{N}$, and $j \in \mathbb{N}$,*

(a) $(x \,\&\, y)[i : j] = x[i : j] \,\&\, y[i : j]$;
(b) $(x \mid y)[i : j] = x[i : j] \mid y[i : j]$;
(c) $(x \,\hat{}\, y)[i : j] = x[i : j] \,\hat{}\, y[i : j]$.

Proof We present the proof for (a); (b) and (c) are similar.

We may assume that $n > 0$, $x \neq 0$, $y \neq 0$, and $x \neq y$. By Definition 2.2 and Lemmas 3.4 and 3.5,

$$\begin{aligned}
(x \,\&\, y)[i : j] &= \left\lfloor ((x \,\&\, y) \bmod 2^{i+1})/2^j \right\rfloor \\
&= \left\lfloor ((x \bmod 2^{i+1}) \,\&\, (y \bmod 2^{i+1}))/2^j \right\rfloor \\
&= \lfloor (x \bmod 2^{i+1})/2^j \rfloor \,\&\, \lfloor (y \bmod 2^{i+1})/2^j \rfloor \\
&= x[i : j] \,\&\, y[i : j].
\end{aligned}$$

□

Corollary 3.7 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $k \in \mathbb{N}$,*

(a) $(x \,\&\, y)[n] = x[n] \,\&\, y[n]$;
(b) $(x \mid y)[n] = x[n] \mid y[n]$;
(c) $(x \,\hat{}\, y)[n] = x[n] \,\hat{}\, y[n]$.

Lemma 3.8 *For all $x_1 \in \mathbb{Z}$, $y_1 \in \mathbb{Z}$, $x_2 \in \mathbb{Z}$, $y_2 \in \mathbb{Z}$, $m \in \mathbb{N}$, and $n \in \mathbb{N}$,*

(a) $\{m'x_1, n'y_1\} \mathbin{\&} \{m'x_2, n'y_2\} = \{m'(x_1 \mathbin{\&} x_2), n'(y_1 \mathbin{\&} y_2)\}$;
(b) $\{m'x_1, n'y_1\} \mid \{m'x_2, n'y_2\} = \{m'(x_1 \mid x_2), n'(y_1 \mid y_2)\}$;
(c) $\{m'x_1, n'y_1\} \mathbin{\hat{}} \{m'x_2, n'y_2\} = \{m'(x_1 \mathbin{\hat{}} x_2), n'(y_1 \mathbin{\hat{}} y_2)\}$.

Proof We present the proof for (a); (b) and (c) are similar.

Let $C = \{m'x_1, n'y_1\} \mathbin{\&} \{m'x_2, n'y_2\}$. By Lemmas 3.4 and 2.48,

$$\begin{aligned} & C \bmod 2^n \\ &= \{x_1[m{-}1:0], y_1[n{-}1:0]\}[n{-}1:0] \mathbin{\&} \{x_2[m{-}1:0], y_2[n{-}1:0]\}[n{-}1:0] \\ &= y_1[n{-}1:0] \mathbin{\&} y_2[n{-}1:0]. \end{aligned}$$

By Lemma 3.5,

$$\lfloor C/2^n \rfloor = \lfloor \{x_1[m{-}1:0], y_1[n{-}1:0]\}/2^n \rfloor \mathbin{\&} \lfloor \{x_2[m{-}1:0], y_2[n{-}1:0]\}/2^n \rfloor,$$

where, by Definition 2.3 and the properties of the floor,

$$\begin{aligned} \lfloor \{x_i[m{-}1:0], y_i[n{-}1:0]\}/2^n \rfloor &= \lfloor (2^n x_i[m{-}1:0] + y_i[n{-}1:0])/2^n \rfloor \\ &= x_i[m{-}1:0] + \lfloor y_i[n{-}1:0]/2^n \rfloor \\ &= x_i[m{-}1:0]. \end{aligned}$$

Thus,

$$\lfloor C/2^n \rfloor = x_1[m{-}1:0] \mathbin{\&} x_2[m{-}1:0].$$

Finally, by Definitions 1.3 and 2.3,

$$\begin{aligned} C &= \lfloor C/2^n \rfloor 2^n + (C \bmod 2^n)) \\ &= 2^n (x_1[m{-}1:0] \mathbin{\&} x_2[m{-}1:0]) + y_1[m{-}1:0] \mathbin{\&} y_2[m{-}1:0]) \\ &= \{x_1[m{-}1:0] \mathbin{\&} x_2[m{-}1:0], y_1[n{-}1:0] \mathbin{\&} y_2[n{-}1:0]\}. \end{aligned}$$

□

Lemma 3.9 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $n \in \mathbb{N}$,*

(a) $2^n(x \mathbin{\&} y) = 2^n x \mathbin{\&} 2^n y$;
(b) $2^n(x \mid y) = 2^n x \mid 2^n y$;
(c) $2^n(x \mathbin{\hat{}} y) = 2^n x \mathbin{\hat{}} 2^n y$.

Proof We present the proof for (a); (b) and (c) are similar.

We may assume that $n > 0$, $x \neq 0$, $y \neq 0$, and $x \neq y$. By induction and Definition 3.1 (a),

$$\begin{aligned}
2^n(x \mathbin{\&} y) &= 2\left(2^{n-1}(x \mathbin{\&} y)\right) \\
&= 2\left(2^{n-1}x \mathbin{\&} 2^{n-1}y\right) \\
&= 2\left(\lfloor 2^n x/2\rfloor \mathbin{\&} \lfloor 2^n x/2\rfloor\right) + (2^n x \bmod 2) \mathbin{\&} (2^n y \bmod 2) \\
&= 2^n x \mathbin{\&} 2^n y.
\end{aligned}$$

□

Lemma 3.10 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $n \in \mathbb{N}$,*

(a) $2^n x \mathbin{\&} y = 2^n(x \mathbin{\&} \lfloor y/2^n\rfloor)$;
(b) $2^n x \mid y = 2^n(x \mid \lfloor y/2^n\rfloor) + y \bmod 2^n$;
(c) $2^n x \mathbin{\hat{}} y = 2^n(x \mathbin{\hat{}} \lfloor y/2^n\rfloor) + y \bmod 2^n$.

Proof

(a) The claim is trivial if $x = 0$, $y = 0$, or $y = 2^n x$; otherwise, by Definition 3.1 (a), induction, and Lemma 1.2,

$$\begin{aligned}
2^n x \mathbin{\&} y &= 2\left(\lfloor 2^n x/2\rfloor \mathbin{\&} \lfloor y/2\rfloor\right) + (2^n x \bmod 2) \mathbin{\&} (y \bmod 2) \\
&= 2(2^{n-1}x \mathbin{\&} \lfloor y/2\rfloor) + 0 \\
&= 2\left(2^{n-1}(x \mathbin{\&} \left\lfloor \lfloor y/2\rfloor/2^{n-1} \right\rfloor)\right) \\
&= 2^n(x \mathbin{\&} \lfloor y/2^n\rfloor).
\end{aligned}$$

(b) Similarly,

$$\begin{aligned}
2^n x \mid y &= 2\left(\lfloor 2^n x/2\rfloor \mid \lfloor y/2\rfloor\right) + (2^n x \bmod 2) \mid (y \bmod 2) \\
&= 2(2^{n-1}x \mid \lfloor y/2\rfloor) + y \bmod 2 \\
&= 2\left(2^{n-1}\left(x \mid \left\lfloor \lfloor y/2\rfloor/2^{n-1} \right\rfloor\right) + \lfloor y/2\rfloor \bmod 2^{n-1}\right) + y \bmod 2 \\
&= 2^n(x \mid \lfloor y/2^n\rfloor) + 2(\lfloor y/2\rfloor \bmod 2^{n-1}) + y \bmod 2,
\end{aligned}$$

where, by Lemmas 2.3 and 2.12,

$$\begin{aligned}
2(\lfloor y/2\rfloor \bmod 2^{n-1}) + y \bmod 2 &= 2\lfloor y/2\rfloor[n-2:0] + y[0] \\
&= 2y[n-1:1] + y[0] \\
&= y[n-1:0] \\
&= y \bmod 2^n.
\end{aligned}$$

The proof of (c) is similar to that of (b). □

Corollary 3.11 *Let $x \in \mathbb{Z}$ and let y be an n-bit vector, where $n \in \mathbb{N}$. Then*

$$2^n x \mid y = 2^n x + y.$$

Proof By Lemmas 3.10 and 1.11 and Definition 3.1 (b),

$$2^n x \mid y = 2^n (x \mid \lfloor y/2^n \rfloor) + y \bmod 2^n = 2^n (x \mid 0) + y = 2^n x + y.$$

□

Lemma 3.12 *For all $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, $2^n \mid x = \begin{cases} x & \text{if } x[n] = 1 \\ x + 2^n & \text{if } x[n] = 0. \end{cases}$*

Proof By Definition 2.2 and Lemmas 3.4, 3.8, and 2.32,

$$\begin{aligned}
(2^n \mid x) \bmod 2^{n+1} &= (2^n \mid x)[n:0] \\
&= (2^n)[n:0] \mid x[n:0] \\
&= \{1'1, 0'(n-1)\} \mid \{x[n], x[n-1:0]\} \\
&= \{1'1, x[n-1:0]\} \\
&= \begin{cases} x[n:0] & \text{if } x[n] = 1 \\ x[n:0] + 2^n & \text{if } x[n] = 0 \end{cases} \\
&= \begin{cases} x \bmod 2^{n+1} & \text{if } x[n] = 1 \\ x \bmod 2^{n+1} + 2^n & \text{if } x[n] = 0. \end{cases}
\end{aligned}$$

By Lemma 3.5,

$$\lfloor (2^n \mid x)/2^{n+1} \rfloor = 0 \mid \lfloor x/2^{n+1} \rfloor = \lfloor x/2^{n+1} \rfloor.$$

The lemma follows from Definition 1.3. □

The logical "and" operator may be used to extract a bit slice:

Lemma 3.13 *Let $x \in \mathbb{Z}$, $n \in \mathbb{N}$, and $k \in \mathbb{N}$. If $k < n$, then*

$$x \mathbin{\&} (2^n - 2^k) = 2^k x[n-1:k].$$

Proof The proof is by induction on n. If $n = 1$, then $k = 0$ and

$$x \mathbin{\&} (2^n - 2^k) = x \mathbin{\&} 1 = 2(\lfloor x/2 \rfloor \mathbin{\&} 0) + (x \bmod 2) \mathbin{\&} 1 = 0 + x[0] = x[n-1:k].$$

If $n > 1$ and $k = 0$, then by induction and Lemmas 2.12 and 2.32,

$$\begin{aligned} x \mathbin{\&} (2^n - 2^k) &= x \mathbin{\&} (2^n - 1) \\ &= 2(\lfloor x/2 \rfloor \mathbin{\&} \lfloor (2^n - 1)/2 \rfloor) + (x \bmod 2) \mathbin{\&} ((2^n - 1) \bmod 2) \\ &= 2(\lfloor x/2 \rfloor \mathbin{\&} (2^{n-1} - 1)) + (x \bmod 2) \mathbin{\&} 1 \\ &= 2\lfloor x/2 \rfloor [n-2:0] + x[0] \\ &= 2x[n-1:1] + x[0] \\ &= x[n-1:0]. \end{aligned}$$

In the remaining case, $n > k > 1$ and

$$\begin{aligned} x \mathbin{\&} (2^n - 2^k) &= 2(\lfloor x/2 \rfloor \mathbin{\&} \lfloor (2^n - 1)/2 \rfloor) + (x \bmod 2) \mathbin{\&} ((2^n - 2^k) \bmod 2) \\ &= 2(\lfloor x/2 \rfloor \mathbin{\&} (2^{n-1} - 2^{k-1})) + (x \bmod 2) \mathbin{\&} 0 \\ &= 2\lfloor x/2 \rfloor [n-2:k-1] \\ &= x[n-1:k]. \end{aligned}$$

□

Corollary 3.14 *For all $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, $x \mathbin{\&} 2^n = 2^n x[n]$.*

Proof By Lemma 3.13,

$$x \mathbin{\&} 2^n = x \mathbin{\&} (2^{n+1} - 2^n) = x[n:n] = x[n].$$

□

3.2 Complement

We have a simple arithmetic definition of the logical complement.

Definition 3.2 For all $x \in \mathbb{Z}$, $\sim x = -x - 1$.

Lemma 3.15 *For all $x \in \mathbb{Z}$, $\sim(\sim x) = x$.*

Proof By Definition 3.2, $\sim(\sim x) = -(-x - 1) - 1 = x$. □

Lemma 3.16 *If $x \in \mathbb{Z}$ and $k \in \mathbb{N}$, then $\sim(2^k x) = 2^k(\sim x) + 2^k - 1$.*

Proof By Definition 3.2,

$$2^k(\sim x) + 2^k - 1 = 2^k(-x - 1) + 2^k - 1 = -2^k x - 1 = \sim(2^k x).$$

□

Lemma 3.17 *If $x \in \mathbb{Z}$, $n \in \mathbb{N}$, and $n > 0$, then $\sim\lfloor x/n \rfloor = \lfloor \sim x/n \rfloor$.*

Proof By Definition 3.2 and Lemma 1.5,

$$\lfloor (\sim x)/n \rfloor = \left\lfloor \frac{-x-1}{n} \right\rfloor = \left\lfloor -\frac{x+1}{n} \right\rfloor = -\left\lfloor \frac{x}{n} \right\rfloor - 1 = \sim\lfloor x/n \rfloor.$$

□

Lemma 3.18 *If $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, then*

$$\sim x \bmod 2^n = 2^n - (x \bmod 2^n) - 1.$$

Proof First note that by Lemmas 1.10 and 1.11,

$$0 \le 2^n - (x \bmod 2^n) - 1 < 2^n.$$

Therefore, by Lemmas 1.15, 1.23, and 1.11,

$$\begin{aligned} \sim x \bmod 2^n &= (-x-1) \bmod 2^n \\ &= (2^n - (x \bmod 2^n) - 1) \bmod 2^n \\ &= 2^n - (x \bmod 2^n) - 1. \end{aligned}$$

□

Notation For the purpose of resolving ambiguous expressions, the complement has higher precedence than the bit slice operator, e.g., $\sim x[i:j] = (\sim x)[i:j]$.

Lemma 3.19 *If $x \in \mathbb{Z}$, $i \in \mathbb{N}$, $j \in \mathbb{N}$, and $j \le i$, then*

$$\sim x[i:j] = 2^{i+1-j} - x[i:j] - 1.$$

Proof By Definitions 3.2 and 2.2 and Lemmas 3.18, 1.1, and 1.5,

$$\begin{aligned} \sim x[i:j] &= \left\lfloor (\sim x \bmod 2^{i+1})/2^j \right\rfloor \\ &= \left\lfloor \frac{2^{i+1} - (x \bmod 2^{i+1}) - 1}{2^j} \right\rfloor \\ &= \frac{2^{i+1}}{2^j} + \left\lfloor -\frac{(x \bmod 2^{i+1}) + 1}{2^j} \right\rfloor \\ &= 2^{i+1-j} - \left\lfloor \frac{x \bmod 2^{i+1}}{2^j} \right\rfloor - 1 \\ &= 2^{i+1-j} - x[i:j] - 1. \end{aligned}$$

□

The usual bit-wise characterization of the complement is a special case of Lemma 3.19:

Corollary 3.20 *If $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, then $\sim x[n] \neq x[n]$.*

Proof By Lemma 3.19, $\sim x[n] = 2^{n+1-n} - x[n] - 1 = 1 - x[n]$. □

The remaining results of this section are properties of complements of bit slices that have proved useful in manipulating expressions derived from RTL designs.

Lemma 3.21 *Let $x \in \mathbb{Z}$, $i \in \mathbb{N}$, $j \in \mathbb{N}$, $k \in \mathbb{N}$, and $\ell \in \mathbb{N}$. If $\ell \leq k \leq i - j$, then*

$$\sim(x[i : j])[k : \ell] = \sim x[k + j : \ell + j].$$

Proof By Lemmas 3.19 and 2.19,

$$\begin{aligned} \sim(x[i : j])[k : \ell] &= 2^{k+1-\ell} - x[i : j][k : \ell] - 1 \\ &= 2^{(k+j)+1-(\ell+j)} - x[k + j : \ell + j] - 1 \\ &= \sim x[k + j : \ell + j]. \end{aligned}$$

□

Lemma 3.22 *If $x \in \mathbb{Z}$ and y in an n-bit vector, where $n \in \mathbb{N}$, then*

$$\sim(x[n-1 : 0])\ \&\ y = \sim x[n-1 : 0]\ \&\ y.$$

Proof By Lemma 3.21, $\sim(x[n-1 : 0])[n-1 : 0] = \sim x[n-1 : 0]$, and hence by Lemmas 3.2, 2.4, and 3.6

$$\begin{aligned} \sim(x[n-1 : 0])\ \&\ y &= (\sim(x[n-1 : 0])\ \&\ y)\,[n-1 : 0] \\ &= \sim(x[n-1 : 0])[n-1 : 0]\ \&\ y[n-1 : 0] \\ &= \sim x[n-1 : 0]\ \&\ y. \end{aligned}$$

□

Lemma 3.23 *Let $x \in \mathbb{Z}$, $i \in \mathbb{N}$, $j \in \mathbb{N}$, $k \in \mathbb{N}$, and $\ell \in \mathbb{N}$. If $\ell \leq k \leq i - j$, then*

$$\sim(\sim x[i : j])[k : \ell] = x[k + j : \ell + j].$$

Proof By Lemmas 3.19, 2.19, and 3.15,

$$\begin{aligned} \sim(\sim x[i : j])[k : \ell] &= 2^{k+1-\ell} - \sim x[i : j][k : \ell] - 1 \\ &= 2^{(k+j)+1-(\ell+j)} - \sim x[k + j : \ell + j] - 1 \\ &= \sim(\sim x)[k + j : \ell + j] \\ &= x[k + j : \ell + j]. \end{aligned}$$

□

3.3 Algebraic Properties

We conclude this chapter with a set of identities pertaining to special cases and compositions of logical operations.

The first two lemmas are immediate consequences of the definitions.

Lemma 3.24 *For all $x \in \mathbb{Z}$,*

(a) $x \,\&\, 0 = 0$;
(b) $x \mid 0 = x$;
(c) $x \,\hat{}\, 0 = x$.

Lemma 3.25 *For all $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,*

(a) $x \,\&\, x = x$;
(b) $x \mid x = x$;
(c) $x \,\hat{}\, x = 0$.

All of the remaining results of this section may be derived in a straightforward manner from Lemmas 3.20, 3.7, and 2.40.

Lemma 3.26 *For all $x \in \mathbb{Z}$,*

(a) $x \,\&\, -1 = x$;
(b) $x \mid -1 = -1$;
(c) $x \,\hat{}\, -1 = {\sim}x$.

Lemma 3.27 *For all $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$,*

(a) $x \mid y = 0 \Leftrightarrow x = y = 0$;
(b) $x \,\hat{}\, y = 0 \Leftrightarrow x = y$.

Proof Suppose $x \mid y = 0$. By Lemma 3.7, for all $k \in \mathbb{N}$

$$x[k] \mid y[k] = (x \mid y)[k] = 0[k] = 0,$$

and it is readily seen by exhaustive computation that this implies $x[k] = y[k] = 0$. It follows from Lemma 2.40 that $x = y = 0$. A similar argument applies to (b). □

The proofs of the remaining lemmas are sufficiently similar to that of Lemma 3.27 that they may be safely omitted.

Lemma 3.28 *For all $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, and $n \in \mathbb{Z}$,*

(a) $x \,\&\, y = y \,\&\, x$;
(b) $x \mid y = y \mid x$;
(c) $x \,\hat{}\, y = y \,\hat{}\, x$.

Lemma 3.29 *For all $x \in \mathbb{N}$, $y \in \mathbb{N}$, and $z \in \mathbb{N}$,*

(a) $(x \,\&\, y) \,\&\, z = x \,\&\, (y \,\&\, z)$;
(b) $(x \mid y) \mid z = x \mid (y \mid z)$;
(c) $(x \,\hat{}\, y) \,\hat{}\, z = x \,\hat{}\, (y \,\hat{}\, z)$.

Lemma 3.30 *For all $x \in \mathbb{N}$, $y \in \mathbb{N}$, and $z \in \mathbb{N}$,*

(a) $(x \mid y) \,\&\, z = (x \mid y) \,\&\, (x \mid z)$;
(b) $x \,\&\, (y \mid z) = x \,\&\, y \mid x \,\&\, z$;
(c) $x \,\&\, y \mid x \,\&\, z \mid y \,\&\, z = x \,\&\, y \mid (x \mathbin{\hat{}} y) \,\&\, z$.

Lemma 3.31 *For all $x \in \mathbb{N}$ and $y \in \mathbb{N}$,*

(a) $x \mathbin{\hat{}} y = x \,\&\, {\sim}y \mid y \,\&\, {\sim}x$;
(b) ${\sim}(x \mathbin{\hat{}} y) = ({\sim}x) \mathbin{\hat{}} y$.