Two’s Complement

Borderite

March 3, 2026

Two’s Complement Encoding and Decoding

Let $\mathbb{Z} \equiv (\mathbb{Z}, +, -)$ denote the integer field with usual arithmetic addition and subtraction. Let W be a natural number no smller than two, which will be fixed throughout this note. Write

$$\mathcal{N}_W \equiv \{x \in \mathbb{Z} :\, 0 \leq x < 2^W - 1\}.$$

We primarily treat each $x \in \mathcal{N}_W$ as an unsigned integer and identify it with its W-bit binary representation.

An important unary operator on $\mathcal{N}_W$ is the bitwise NOT operator. It flips each position in the binary representation of a given unsigned number. Because the bitwidth of the resulting number is W, the bitwise NOT operator maps each member of $\mathcal{N}_W$ to a member of $\mathcal{N}_W$. Also, we see that the sum of $x \in \mathcal{N}_W$ and its bitwise NOT $\neg x$ is represented by the W-bit binary representation all of whose positions are set, i.e.,

$$x + \neg x = 2^W - 1$$

or equivalently,

$$\neg x = 2^W - 1 - x.$$

Based on this fact, we define a function $\texttt{NOT}_W : \mathcal{N}_W \to \mathcal{N}_W$ by

$$\texttt{NOT}_W(x) \equiv 2^W - 1 - x.$$

A function whose inverse is the function itself is called an *involution*.

Proposition 1. *The function* $\mathtt{NOT}_W$ *is a involution; hence, it is a bijection.*

Proof. The function $\mathtt{NOT}_W$ is involution, because for each $x \in \mathcal{N}_W$,

$$\mathtt{NOT}_W(\mathtt{NOT}_W(x)) = 2^W - 1 - (2^W - 1 - x) = x.$$

□

Besides unsigned integers, we need to deal with signed integers. Because the compouters only deal with binary data, each signed integer needs to converted to the binary data containing information on both its signs and magnitude. If the data width is W bits, one bit is consumed by the information on the sign. We can naturally cover signed integers that can be expressed in $W - 1$ bits.

A widely used method for the encoding of signed numbers is the two's complement method. Write

$$\mathcal{Z}_W \equiv \{z \in \mathbb{Z} : -2^{W-1} \leq z \leq 2^{W-1} - 1\}.$$

and define the function $\mathtt{TCE}_W : \mathcal{Z}_W \to \mathcal{N}_W$ defined by

$$\mathtt{TCE}_W(z) \equiv z \bmod 2^W.$$

Proposition 2. *(a) For each nonnegative* $z \in \mathcal{Z}_W$*, it holds that*

$$\mathtt{TCE}_(z) = z.$$

The function $\mathtt{TCE}_W$ *is a bijection from* $\{z \in \mathcal{Z}_W : z \geq 0\}$ *to* $\{y \in \mathcal{N}_W : y \leq 2^{W-1} - 1\}$.

(b) For each negative $z \in \mathcal{Z}_W$*, it holds that*

$$\mathtt{TCE}_(z) = 2^W + z.$$

The function $\mathtt{TCE}_W$ *is a bijection from* $\{z \in \mathcal{Z}_W : z < 0\}$ *to* $\{y \in \mathcal{N}_W : y \geq 2^{W-1}\}$.

(c) The function $\mathtt{TCE}_W$ *is bijection.*

Proof. For each nennegative $z \in \mathcal{Z}_W$, we have that $0 \leq z \leq 2^{W-1} - 1 < 2^W$, so that

$$\mathtt{TCE}_W(z) = z \bmod 2^W = z.$$

It follows that $\mathtt{TCE}_W$ is a bijection from $\{z \in \mathcal{Z}_W : z \geq 0\}$ to

$$\begin{aligned}\mathtt{TCE}_W(\{z \in \mathcal{Z}_W : z \geq 0\}) &= \{y \in \mathcal{N}_W : \mathtt{TCE}_W(0) \leq y \leq \mathtt{TCE}_W(2^{W-1} - 1)\} \\ &= \{y \in \mathcal{N}_W : 0 \leq y \leq 2^{W-1} - 1\}.\end{aligned}$$

This verifies (a).

For each negative $z \in \mathcal{Z}_W$, we have that $-2^W < -2^{W-1} \leq z < 0$, so that

$$\mathtt{TCE}_W(z) = z \bmod 2^W = 2^W + z$$

It follows that $\mathtt{TCE}_W$ is a bijection from $\{z \in \mathcal{Z}_W : z < 0\}$ to

$$\begin{aligned}
&\mathtt{TCE}_W(\{z \in \mathcal{Z}_W : z \leq -1\}) = \{y \in \mathcal{N}_W : \mathtt{TCE}_W(-2^{W-1}) \leq y \leq \mathtt{TCE}_W(-1)\} \\
&\quad = \{y \in \mathcal{N}_W : 2^{W-1} \leq y \leq 2^W - 1\}.
\end{aligned}$$

Claim (b) therefore follows.

Given claims (a) and (b), $\mathtt{TCE}_W$ is an injection on $\mathcal{Z}_W$. It is also a surjection, because

$$\mathtt{TCE}_W(\mathcal{Z}_W) = \mathtt{TCE}_W(\{z \in \mathcal{Z}_W : z \geq 0\}) \cup \mathtt{TCE}_W(\{z \in \mathcal{Z}_W : z \leq -1\}) = \mathcal{N}_W.$$

Thus, Claim (c) holds. □

As Proposition 2 shows, $\mathtt{TCE}_W$ maps nonnegative integers in $\mathcal{Z}_W$ to the same values in the lower half of $\mathcal{N}_W$, while it maps negative integers in $\mathcal{Z}_W$ to the upper half of $\mathcal{N}_W$. For a negative integer $z \in \mathcal{Z}_W$, we have that

$$\begin{aligned}
\mathtt{TCE}_W(z) &= 2^W + z = (2^W - 1) + (-z) + 1 \\
&= \mathtt{NOT}_W(-z) + 1 = \mathtt{NOT}_W(|z|) + 1
\end{aligned}$$

In this view, $\mathtt{TCE}_W$ maps each negative $z \in \mathcal{Z}_W$ to the two's complement of the magnitude of z. So, we can take $\mathtt{TCE}_W$ as an encoder using the two's complement method.

In addition to the encoding method for signed integers, we also need a decoding method. Define $\mathtt{TCD}_W : \mathcal{N}_W \to \mathcal{Z}_W$ by

$$\mathtt{TCD}_W(y) \equiv ((2^{W-1} + y) \bmod 2^W) - 2^{W-1}.$$

Then:

Proposition 3. *The function* $\mathtt{TCD}_W$ *is the inverse function of* $\mathtt{TCE}_W$*.*

Proof. For each $z \in \mathcal{Z}_W$, we have that

$$\begin{aligned}
&\mathtt{TCD}_W(\mathtt{TCE}_W(z)) = \mathtt{TCD}_W(z \bmod 2^W) \\
&\quad = ((2^{W-1} + (z \bmod 2^W)) \bmod 2^W) - 2^{W-1} \\
&\quad = ((2^{W-1} + z) \bmod 2^W) - 2^{W-1}
\end{aligned}$$

Because $0 \leq 2^{W-1} + z \leq 2^W - 1$, the right-hand side of this equality is equal to

$$2^{W-1} + z - 2^{W-1} = z.$$

The result therefore follows. □

Bitwise Shift Operations

We sometimes need to take bitwise shift operations on an integer of a particular bitwidth. Define $\mathtt{SHL}_W : \mathcal{N}_W \times \{0, 1, \ldots, W\} \to \mathcal{N}_W$, $\mathtt{SHR}_W : \mathcal{N}_W \times \{0, 1, \ldots, W\} \to \mathcal{N}_W$, $\mathtt{SAL}_W : \mathcal{N}_W \times \{0, 1, \ldots, W\} \to \mathcal{N}_W$, and $\mathtt{SAR}_W : \mathcal{N}_W \times \{0, 1, \ldots, W\} \to \mathcal{N}_W$ by

$$\mathtt{SHL}_W(x, k) = (2^k x) \bmod 2^W$$

$$\mathtt{SHR}_W(x, k) = \lfloor x/2^k \rfloor,$$

$$\mathtt{SAL}_W(x, k) = \mathtt{SHL}_W(x, k),$$

and

$$\mathtt{SAR}_W(x, k) = \lfloor x/2^{W-1} \rfloor (2^W - 2^{W-k}) + \mathtt{SHR}_W(x, k),$$

respectively. The values of $\mathtt{SHL}_W(x, k)$ and $\mathtt{SHR}_W(x, k)$ are obtained by logical left and right shifts of the W-bit unsigned integer x by k, respectively. On the other hand, the values of $\mathtt{SAL}_W(x, k)$ and $\mathtt{SAR}_W(x, k)$ are obtained by arthmetic left and right shifts of x by k. While $\mathtt{SHL}_W$ and $\mathtt{SAL}_W$ work exactly in the same say, $\mathtt{SHR}_W$ fills the vacant bit positions created by the shift by zeros, while $\mathtt{SAR}_W$ fills the vancant bit positions by the most significant bit of x ($\lfloor x/2^{W-1} \rfloor$).

The bitwise shift operations with signed integers encoded by the two's complement method requires some care.

Example 1. Suppose that a 8-bit signed integer z is equal to $5 = \mathtt{0b0000101}$. Then $y \equiv \mathtt{TCE}_8(x)$ is also $\mathtt{0b0000101}$. If we take the logical left shift of y by a single bit position and decode the result, we get

$$\begin{aligned}
\mathtt{TCD}_8(\mathtt{SHL}_8(y, 1)) &= \mathtt{TCD}_8(\mathtt{0b00001010}) = \mathtt{0b0001010} = 2x \\
\mathtt{TCD}_8(\mathtt{SHL}_8(y, 3)) &= \mathtt{TCD}_8(\mathtt{0b00101000}) = \mathtt{0b0101000} = 2^3 x \\
\mathtt{TCD}_8(\mathtt{SHL}_8(y, 5)) &= \mathtt{TCD}_8(\mathtt{0b10100000}) = -\mathtt{0b01100000} = -48 \neq 2^5 x
\end{aligned}$$

Example 2. Suppose that a 8-bit signed integer z is equal to $-5 = -\mathtt{0b00000101}$. Then $y \equiv \mathtt{TCE}_8(x)$ is $\mathtt{0b11111011}$. If we take the logical right shifts of y and decode the results, then we get

$$\mathtt{TCD}_8(\mathtt{SHR}_8(y, 1)) = \mathtt{TCD}_8(\mathtt{0b01111101}) = \mathtt{0b01111101} = 253,$$

whose sign is different from that of x. If we instead take the arithmetic right shifts, we do not see this phenomenon.

Proposition 4. *Let z be an integer in $\mathcal{Z}_W$ and k an integer such that $0 \leq k \leq W - 1$. Then*

$$\mathtt{TCD}_W(\mathtt{SAR}_W(\mathtt{TCE}_W(z), k)) = \lfloor z/2^k \rfloor.$$

Remark. The arithmetic right shift rounds down the quotient (not round it toward zero).

Proof. Suppose that $z \geq 0$. Then we have

$$\begin{aligned}&\texttt{SAR}_W(\texttt{TCE}_W(z), k) = \texttt{SAR}_W(z, k)\\&= \lfloor z/2^{W-1} \rfloor (2^W - 2^{W-k}) + \lfloor z/2^k \rfloor = \lfloor z/2^k \rfloor,\end{aligned}$$

where the last equality holds because $0 \leq z \leq 2^{W-1} - 1$. The claim follows by Propositions 2(a) and 3.

Now, suppose instead that $z < 0$. Then it holds that

$$\begin{aligned}&\texttt{SAR}_W(\texttt{TCE}_W(z), k) = \texttt{SAR}_W(2^W + z, k)\\&= \lfloor (2^W + z)/2^{W-1} \rfloor (2^W - 2^{W-k}) + \lfloor (2^W + z)/2^k \rfloor.\end{aligned}$$

Because $2^{W-1} \leq 2^W + z \leq 2^W - 1$, the first term on the right-hand side is equal to $1 \cdot (2^W - 2^{W-k}) = (2^W - 2^{W-k})$, it follows that

$$\begin{aligned}&\texttt{SAR}_W(\texttt{TCE}_W(z), k) = (2^W - 2^{W-k}) + \lfloor 2^{W-k} + (z/2^k)) \rfloor\\&= (2^W - 2^{W-k}) + 2^{W-k} + \lfloor z/2^k \rfloor\\&= 2^W + \lfloor z/2^k \rfloor.\end{aligned}$$

Because $\lfloor z/2^k \rfloor \leq -1$, the claim follows by Propositions 2(b) and 3. □

Addition and Subtraction

The computers have instructions for arithmetic operations. Define functions $\texttt{ADD}_W : \mathcal{N}_W \to \mathcal{N}_W$ and $\texttt{SUB}_W : \mathcal{N}_W \to \mathcal{N}_W$ by

$$\texttt{ADD}_W(x, y) \equiv (x + y) \bmod 2^W$$

and

$$\texttt{SUB}_W(x, y) \equiv (x - y) \bmod 2^W,$$

respectively, which perform the addition and subtraction operations on unsigned integers. If $x + y \geq 2^W$, then the addition instruction causes an overflow. When $x - y < 0$, the subtraction instruction again cuases an overflow. The modularization by 2^W in these definitions ensure that the result from the functions stay within $\mathcal{N}_W$ even when an overflow occurs.

An overflow occurs in subtracting y from x occurs if and only if $x < y$. This condition is easy to check. For the addition operation:

Proposition 5. *Let x and y be integers in $\mathcal{N}_W$. Then:*

(a) If $x + y \geq 2^W$, then if $\texttt{ADD}_W(x, y) \leq \min(x, y) - 1$.

(b) If $\texttt{ADD}_W(x, y) \leq x - 1$ or $\texttt{ADD}_W(x, y) \leq y - 1$, then $x + y \geq 2^W$.

Proof. Without loss of generality, assume that $x \leq y$. If $x + y \geq 2^W$, we have that $2^W \leq x + y \leq 2^W - 2$, so that

$$\begin{aligned} \mathtt{ADD}_W(x, y) &= (x + y) \bmod 2^W = x + y - 2^W \\ &\leq x + (2^W - 1) - 2^W = x - 1. \end{aligned}$$

Claim (a) therefore follows.

To prove claim (b), we verify its contraposition. Suppose that $x + y \leq 2^W - 1$. Then we have that

$$\mathtt{ADD}_W(x, y) = (x + y) \bmod 2^W = x + y \geq y \geq x,$$

so that $\mathtt{ADD}_W(x, y) \geq x$ and $\mathtt{ADD}_W(x, y) \geq y$. The result therefore follows. □

Given a signed integer encoded by the two's complement method, we sometimes need to find the encoded value of the signed integer with an opposite sign. The $\mathtt{NEG}_W : \mathcal{N}_W \to \mathcal{N}_W$ defined by

$$\mathtt{NEG}_W(x) \equiv (2^W - x) \bmod 2^W$$

does such task.

Proposition 6. *For each $z \in \mathcal{Z}_W \backslash \{-2^{W-1}\}$, it holds that*

$$\mathtt{NEG}_W(\mathtt{TCE}_W(z)) = \mathtt{TCE}_W(-z).$$

Remark. The function $\mathtt{NEG}_W$ has two fixed points, 0 and 2^{W-1}, which are the encoded values of the signed integers, 0 and -2^{W-1}. Though it might look strange that $negfw$ maps the encoded value of -2^{W-1} to itself, this feature is still useful if the value obtained by $\mathtt{NEG}_W$ is used as a unsigned integer, because $-(-2^{W-1}) = 2^{W-1}$.

Proof. Pick $z \in \mathcal{Z}_W \backslash \{-2^{W-1}\}$ arbitrarily. Then

$$\begin{aligned} \mathtt{NEG}_W(\mathtt{TCE}_W(z)) &= \mathtt{NEG}_W(z \bmod 2^W) \\ &= (2^W - (z \bmod 2^W)) \bmod 2^W \\ &= (2^W - z) \bmod 2^W = -z \bmod 2^W = \mathtt{TCE}_W(-z) \end{aligned}$$ □

The subtraction instruction can be created by combining the addition and the $\mathtt{NEG}_W$ instructions, because:

Proposition 7. *For each $(x, y) \in \mathcal{N}_W^2$, $\mathtt{SUB}_W(x, y) = \mathtt{ADD}_W(x, \mathtt{NEG}_W(y))$.*

Proof.

$$\begin{aligned} \mathtt{SUB}_W(x, y) &= (x - y) \bmod 2^W = (x + 2^W - y) \bmod 2^W \\ &= (x + ((2^W - y) \bmod 2^W)) \bmod 2^W \\ &= (x + \mathtt{NEG}_W(y)) \bmod 2^W = \mathtt{ADD}_W(x, \mathtt{NEG}_W(y)). \end{aligned}$$ □

An interesting feature of the two's complement method is that the unsigned addition of the signed integers encoded by it delivers the correct result in the encoded form, as long as an overflow does not occur.

Proposition 8. *Let x and y be integers in $\mathcal{Z}_W$.*

(a) If $-2^{W-1} \leq x + y \leq 2^{W-1} - 1$, then

$$\mathtt{TCD}_W(\mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = x + y.$$

(b) If $x + y \geq 2^{W-1}$, then

$$\mathtt{TCD}_W(\mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = (x + y) - 2^W \leq -2.$$

(c) If $x + y \leq -2^{W-1} - 1$, then

$$\mathtt{TCD}_W(\mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = 2^W + (x + y) \geq 0.$$

Remarks.

(a) If one of x and y is nonnegative and the other is negative, then the condition of Proposition 8(a) is satisfied, so that $x + y$ is correctly calculated by $\mathtt{TCD}_W(\mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)))$.

(b) The condition of proposition 8(b) can occur only when both x and y are positive. The result indicates that the overflow in the addition in such a case results in a negative value.

(c) The condition of proposition 8(c) can occur only when both x and y are negative. The result indicates that the overflow in the addition in such a case results in a nonnegative value.

Proof. By the definitions of $\mathtt{TCE}_W$ and $\mathtt{ADD}_W$, we have that

$$\begin{aligned} \mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)) &= ((x \bmod 2^W) + (y \bmod 2^W)) \bmod 2^W \\ &= (x + y) \bmod 2^W. \end{aligned} \tag{1}$$

Under the hypothesis of claim (a), the right-hand side of this equality is equal to $\mathtt{TCE}_W(x + y)$. Claim (a) follows by Proposition 3.

Under the hypothesis of claim (b), it holds that $x + y - 2^W \in \mathcal{Z}_W$, so that

$$\begin{aligned} \mathtt{TCE}_W(x + y - 2^W) &= (x + y - 2^W) \bmod 2^W \\ &= (x + y) \bmod 2^W = \mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)), \end{aligned}$$

where the last equality holds by (1). Claim (b) follows by Proposition 3.

Under the hytpothesis of claim (c), it holds that $2^W + (x+y) \in \mathcal{Z}_W$, so that

$$\begin{aligned} \mathtt{TCE}_W(2^W + (x+y)) &= (2^W + (x+y)) \bmod 2^W \\ &= (x+y) \bmod 2^W = \mathtt{ADD}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)). \end{aligned}$$

Claim (c) follows by Proposition 3. □

The two's complement encoding also works with the unsigned subtraction.

Proposition 9. *Let x and y be integers in $\mathcal{Z}_W$.*

(a) If $-2^{W-1} \le x - y \le 2^{W-1} - 1$, then

$$\mathtt{TCD}_W(\mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = x - y.$$

(b) If $x - y \ge 2^{W-1}$, then

$$\mathtt{TCD}_W(\mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = (x-y) - 2^W \le -1.$$

(c) If $x - y \le -2^{W-1} - 1$, then

$$\mathtt{TCD}_W(\mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y))) = (x-y) + 2^W \ge 1.$$

Remarks.

(a) If x and y are both nonnegative or both negative, then the condition of Proposition 9(a) is satisfied, so that $x - y$ is correctly calculated by $\mathtt{TCD}_W(\mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)))$.

(b) The condition of proposition 9(b) can occur only when $x \ge 0$ and $y \le 0$. The result indicates that the overflow in the subtraction in such a case results in a negative value.

(c) The condition of proposition 9(c) can occur only when $x \le -2$ and $y \ge 1$. The result indicates that the overflow in the subtraction in such a case results in a positive value.

Proof. By the definitions of $\mathtt{TCE}_W$ and $\mathtt{SUB}_W$, we have that

$$\begin{aligned} \mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)) &= ((x \bmod 2^W) - (y \bmod 2^W)) \bmod 2^W \\ &= (x-y) \bmod 2^W. \end{aligned} \tag{2}$$

Under the hypothesis of claim (a), the right-hand side of this equality is equal to $\mathtt{TCE}_W(x-y)$. Claim (a) follows by Proposition 3.

Under the hypothesis of claim (b), it holds that $x - y - 2^W \in \mathcal{Z}_W$, so that

$$\begin{aligned}\mathtt{TCE}_W(x-y-2^W) &= (x-y-2^W) \bmod 2^W \\ &= (x-y) \bmod 2^W \\ &= \mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)),\end{aligned}$$

where the last equality holds by (2). Claim (b) follows by Proposition 3.

Under the hytpothesis of claim (c), it holds that $2^W + (x - y) \in \mathcal{Z}_W$, so that

$$\begin{aligned}&\mathtt{TCE}_W(2^W + (x-y)) = (2^W + (x-y)) \bmod 2^W \\ &\quad = (x-y) \bmod 2^W = \mathtt{SUB}_W(\mathtt{TCE}_W(x), \mathtt{TCE}_W(y)).\end{aligned}$$

Claim (c) follows by Proposition 3. □

Multiplication

We now consideer another arithmetic operation, multiplication. When we take a pair of unsigned W-bit integers, the binary representation of their product can be as long as $2W$ bits. To eliminate or reduce the chance of overflows, we can perform multiplication using a longer bitwidth than the input integers. Let V be a natural number no less than W, and define $\mathtt{MUL}_V : \mathcal{N}_V^2 \to \mathcal{N}_V$ by

$$\mathtt{MUL}_V(x, y) = (xy) \bmod 2^V.$$

Complete avoidance of overflows in unsigned multiplication requires that $V \geq 2W$. But some CPU multiplication instructions are designed for $V = W$.

Addition and subtraction combined with the two's complement encoding work well for signed addition and subtraction. Because multiplication can be viewed as repeated additions or subtractions, it is not surprising to see the same kind of properties for the multiplication operation. But the multiplication operation is subtly different from addition and subtraction because the bitwidth, W, of values of which we want to take the product can be smaller than the bitwidth, V, of the values the multiplication operator handles. The two's complement of a signed integer depends on the bitwidth to work with.

Example 3. It holds that $\mathtt{TCE}_8(-1) = \mathtt{0xff} = \mathtt{0x00ff}$ while $\mathtt{TCE}_{16}(-1) = \mathtt{0xffff}$.

Let x be an W-bit unsigned integer with the most significant bit x_{W-1}. A V-bit unsigned integer each of whose most significant $V - W$ bits is x_{W-1} and the remining bits are x is called the *sign expansion* of z. Note that z_{W-1} is 1 if and only if $z \geq 2^{W-1}$. Define a function $\mathtt{SX}_{W,V} : \mathcal{N}_W \to \mathcal{N}_V$ by

$$\mathtt{SX}_{W,V}(x) \equiv \lfloor x/2^{W-1} \rfloor (2^V - 2^W) + x.$$

Proposition 10. *For each $z \in \mathcal{Z}_W$, it holds that*

$$\mathtt{TCE}_V(z) = \mathtt{SX}_{W,V}(\mathtt{TCE}_W(z)).$$

Proof. Suppose that $z \geq 0$. Then it follows from Proposition 6 that $\mathtt{TCE}_V(z) = z$ and that $\mathtt{SX}_{W,V}(\mathtt{TCE}_W(z)) = z$, as $z \leq 2^{W-1}$. Thus, the equality in question holds. Suppose instead that $z < 0$. Then we have that $\mathtt{TCE}_V(z) = 2^V + z$. Because $2^{W-1} \leq 2^W + z <= 2^W - 1$, we also have that

$$\begin{aligned}
&\mathtt{SX}_{W,V}(\mathtt{TCE}_W(z)) = \mathtt{SX}_{W,V}(2^W + z) = \lfloor (2^W + z)/2^{W-1} \rfloor (2^V - 2^W) + (2^W + z) \\
&\quad = (2^V - 2^W) + (2^W + z) = 2^V + z.
\end{aligned}$$

The equality in question again holds. □

The unsigned addition and subtraction combinaed with the two's complement encoding work well in signed addition and subtraction. We try the same strategy in multiplication.

Proposition 11. *Let x and y be integers in $\mathcal{Z}_W$. If $-2^{V-1} \leq xy \leq 2^{V-1} - 1$, then*

$$\mathtt{TCD}_V(\mathtt{MUL}_V(\mathtt{TCE}_V(x), \mathtt{TCE}_V(y))) = xy.$$

Remark. As Proposition 10 shows, applying $\mathtt{TCE}_V$ appering in this proposition is the same as applying $\mathtt{TCE}_W$ and then apply $\mathtt{SX}_{W,V}$.

Proof. In general, we have that

$$\begin{aligned}
&\mathtt{MUL}_V(\mathtt{TCE}_V(x), \mathtt{TCE}_V(y)) = \mathtt{MUL}_V((x \bmod 2^V), (y \bmod 2^V)) \\
&\quad = ((x \bmod 2^V) \cdot (y \bmod 2^V)) \bmod 2^V = (xy) \bmod 2^V \\
&\quad = \mathtt{TCE}_V(xy).
\end{aligned}$$

The result follows by Proposition 3. □

Division

Define a function $\mathtt{DIV}_{V,W} : \mathcal{N}_V \times \mathcal{N}_W \to \mathcal{N}_W \times \mathcal{N}_W \times \{0, 1\}$

$$\mathtt{DIV}_{V,W}(x, y) \equiv (q, r, f),$$

where

$$f \equiv \begin{cases} 0 & \text{if } y \geq 1 \text{ and } 2^W y > x, \\ 1 & \text{otherwise,} \end{cases}$$

$$q \equiv \begin{cases} \lfloor x/y \rfloor & \text{if } f = 0, \\ 0 & \text{otherwise,} \end{cases}$$

$$r \equiv \begin{cases} x - qy & \text{if } f = 0, \\ 0 & \text{otherwise.} \end{cases}$$

This function calculates the quotient q and remaindere r in division of the first parameter by the second parameter, when the division is possible, i.e., the divisor is nonzero and the quotient fits in the W-bit unsigned integer range. The third return value f of the function is binary and equal to zero if and only if the division is possible. The values of q and r are meaningless when $f = 1$.

When $W = V$, the quotient is always in $\mathcal{N}_W$, provided that the divisor is not zero. In such case, f becomes 1 if and only if the divisor is zero. We below devise signed division of a $\mathcal{Z}_V$-valued dividend by a $\mathcal{Z}_W$-valued divisor using $\mathtt{DIV}_{V,V}$.

Let x and y be integers such that $y \neq 0$. Also, let q^* and r^* be the quotient and the remainder in the division of $|x|$ by $|y|$. Then the quotient q and the remainder r in the division of x by y (rounded toward zero) can be written as

$$q = \operatorname{sgn}(x) \operatorname{sgn}(y) \lfloor |x|/|y| \rfloor = \operatorname{sgn}(x) \operatorname{sgn}(y) q^* \tag{3}$$

and

$$\begin{aligned} r = x - qy &= \operatorname{sgn}(x)|x| - q \operatorname{sgn}(y)|y| \\ &= \operatorname{sgn}(x)|x| - (\operatorname{sgn}(x) \operatorname{sgn}(y) q^*) \operatorname{sgn}(y)|y| \\ &= \operatorname{sgn}(x)(|x| - q^*|y|) = \operatorname{sgn}(x) r^*. \end{aligned} \tag{4}$$

Given (3) and (4), we can perform signed division operation through unsigned division of the absolute value of the dividend by the absolute value of the divisor. Define $\mathtt{ABS}_W : \mathcal{N}_W \to \mathcal{N}_W$ by

$$\mathtt{ABS}_W(x) \equiv \begin{cases} x & \text{if } x_{W-1} = 0 \\ \mathtt{NEG}_W(x) & \text{otherwise,} \end{cases}$$

where x_{W-1} is the most significant bit of x, which is one if and only if $\mathtt{TCD}_W(x) < 0$.

Proposition 12. *For each $z \in \mathcal{Z}_W$, it holds that*

$$\mathtt{ABS}_W(\mathtt{TCE}_W(z)) = |z|.$$

Remark. When $z \neq -2^{W-1}$, it also holds that $\mathtt{TCD}_W(\mathtt{ABS}_W(\mathtt{TCE}_W(z))) = |z|$. When $z = -2^{W-1}$, we have that $\mathtt{ABS}_W(\mathtt{TCE}_W(z)) = 2^{W-1}$. If we apply $\mathtt{TCD}_W$ to this value, we get -2^{W-1}, not 2^{W-1}. See the remark to Proposition 6.

Proof. If $z \geq 0$, then the most significant bit of $\mathtt{TCE}_V(z)$ is zero, the result clearly holds. If $z < 0$, on the other hand, the most significant bit of $\mathtt{TCE}_V(z)$ is one. We have that

$$\mathtt{ABS}_W(\mathtt{TCE}_W(z)) = \mathtt{NEG}_W(\mathtt{TCE}_W(z)) = \mathtt{TCE}_W(-z) = -z.$$

where the second equality holds by Proposition 6. The result therefore follows. □

Define $\mathtt{IDIV}_{V,W} : \mathcal{Z}_V \times \mathcal{Z}_W \to \mathcal{Z}_W \times \mathcal{Z}_W \times \{0,1\}$ by

$$\mathtt{IDIV}_{V,W}(x,y) = (q,r,f),$$

where

$$q \equiv \begin{cases} 0 & \text{if } f = 1, \\ q^* & \text{if } \lfloor \mathtt{TCE}_V(x)/2^{V-1} \rfloor = \lfloor \mathtt{TCE}_W(y)/2^{W-1} \rfloor, \\ 2^W - q^* & \text{otherwise,} \end{cases}$$

$$r \equiv \begin{cases} 0 & \text{if } f = 1, \\ r^* & \text{if } \lfloor \mathtt{TCE}_V(x)/2^{V-1} \rfloor = 0, \\ 2^W - r^* & \text{otherwise,} \end{cases}$$

$$f \equiv \begin{cases} 1 & \text{if } f^* = 1, \\ 1 & \text{if } \lfloor \mathtt{TCE}_V(x)/2^{V-1} \rfloor = \lfloor \mathtt{TCE}_W(y)/2^{W-1} \rfloor \text{ and } q^* \geq 2^{W-1} \\ 1 & \text{if } \lfloor \mathtt{TCE}_V(x)/2^{V-1} \rfloor \neq \lfloor \mathtt{TCE}_W(y)/2^{W-1} \rfloor \text{ and } q^* \geq 2^{W-1} + 1 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$(q^*, r^*, f^*) = \mathtt{DIV}_{V,V}(\mathtt{ABS}_V(\mathtt{TCE}_V(x)), \mathtt{ABS}_V(\mathtt{TCE}_V(y))).$$

Proposition 13. *Suppose that x is an arbitrary integer in $\mathcal{Z}_V$, and that y is an arbitrary integer in $\mathcal{Z}_W$. Let $q \in \mathcal{Z}_W$, $r \in \mathcal{Z}_W$, and $f \in \{0,1\}$ be given by $(q,r,f) = \mathtt{IDIV}_{V,W}(x,y)$. If $y \neq 0$ and*

$$-2^{W-1} \leq \operatorname{sgn}(x)\operatorname{sgn}(y)\lfloor |x|/|y| \rfloor \leq 2^{W-1} - 1, \tag{5}$$

it holds that $\mathtt{TCD}_W(q) = \operatorname{sgn}(x)\operatorname{sgn}(y)\lfloor |x|/|y| \rfloor$, $\mathtt{TCD}_W(r) = x - qy$, and $f = 0$; otherwise, $q = r = 0$ and $f = 1$.

Proof. If $y = 0$, then it holds that $f^* = 1$, so that $q = r = 0$ and $f = 1$, as claimed by the proposition.

Suppose that $y \neq 0$. Then (5) is equivalent to $f = 0$. We can think of four possibilities about the values of x and y: (a) $x >= 0$ and $y > 0$; (b) $x >= 0$ and $y < 0$; (c) $x < 0$ and $y > 0$; and (d) $x < 0$ and $y < 0$. When (5) is satisfied, it is tedious but easy to verify that the claim holds in each of these four cases. If (5) instead is violated, it clearly holds that $f = 1$, the claim again holds. $\square$