Abstract

This document specifies models of the theories of SMT-LIB in the Z notation.
0.1 Contents

0.1 Contents ................................................................. 2
0.2 References ............................................................ 3
0.3 Changes History ....................................................... 3
0.4 Distribution ............................................................ 3

1 INTRODUCTION

2 THE SMT-LIB THEORIES

2.1 Core ................................................................. 5
2.2 Integer Numbers .................................................... 7
2.3 Reals ............................................................... 8
2.4 Reals_Ints .......................................................... 8
2.5 ArraysEx ........................................................... 9
2.6 FixedSizeBitVectors ............................................. 9

3 THE SMT-LIB LOGICS

3.1 Bit Vector Extensions ............................................. 13

4 INDEX

4 INDEX ................................................................. 19
0.2 References


0.3 Changes History

2016/04/16 Initial draft.

2016/05/13 First commit to the ProofPower contrib repository.

0.4 Distribution

Rob Arthan Lemma 1
Colin O’Halloran D-RisQ
ProofPower Repo https://github.com/RobArthan/pp-contrib
1 INTRODUCTION

This document gives a model written in the Z notation of each of the theories defined by the SMT-LIB standard version 2.5 [4, 2, 1]. This model was developed by Lemma 1 primarily to assist D-RisQ in reasoning about programming language datatypes that are modelled in Z and mapped into SMT-LIB to check assertions using an SMT solver. The model is made freely available to the Formal Methods community and comments are invited.

See [3] for an overview of SMT-LIB and its aims. See [6] for details of the Z notation, but note that the specification in this document makes use of features introduced in the ISO Z standard [5], specifically, it uses schemas with empty declaration parts to represent booleans as first-order values.

This document has been prepared using the document preparation tools supplied with ProofPower. It includes the ML commands required to type-check the Z and load it into a ProofPower database. Some small experimental proofs have been carried out and are included in the source of this document, but are omitted from the typeset document.

Please note this is work in progress.

2 THE SMT-LIB THEORIES

First we give the ML commands that set up the theory hierarchy for the SMT-LIB theories. Theory names comprise the SMT-LIB theory name prefixed with ZS_. The Core theory uses the Z Library up to and including the material on sequences. Sequences are used to represent functions that take two or more arguments.

The remaining theories depend on the Core theory and (in the case of Reals_Ints other SMT-LIB theories). The ML coommands to set up the theories are given in the following table.
<table>
<thead>
<tr>
<th>Theory</th>
<th>ML set-up commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core</td>
<td><code>open_theory&quot;z_library&quot;; new_theory&quot;ZS_Core&quot;;</code></td>
</tr>
<tr>
<td>Integer Numbers</td>
<td><code>open_theory&quot;ZS_Core&quot;; new_theory&quot;ZS_Ints&quot;; new_parent&quot;ZS_numbers&quot;;</code></td>
</tr>
<tr>
<td>Real Numbers</td>
<td><code>open_theory&quot;ZS_Core&quot;; new_theory&quot;ZS_Reals&quot;; new_parent&quot;ZS_reals&quot;;</code></td>
</tr>
<tr>
<td>Real and Integer Numbers</td>
<td><code>open_theory&quot;ZS_Core&quot;; new_theory&quot;ZS_Reals_Ints&quot;; new_parent&quot;ZS_Reals&quot;; new_parent&quot;ZS_Ints&quot;;</code></td>
</tr>
<tr>
<td>Arrays</td>
<td><code>open_theory&quot;ZS_Core&quot;; new_theory&quot;ZS_ArraysEx&quot;;</code></td>
</tr>
<tr>
<td>Bit Vectors</td>
<td><code>open_theory&quot;ZS_Core&quot;; new_theory&quot;ZS_FixedSizeBitVectors&quot;;</code></td>
</tr>
</tbody>
</table>

2.1 Core

SML

```
open_theory"ZS_Core";
```

Standard Z is a form of first-order typed set theory. While the ProofPower system that we use to type-check and reason about Z actually supports a higher-order extension of Z, we prefer to stay within Standard Z in this specification. We will use what turns out to be a very convenient way of representing truth values as first-order objects following an idea of Sam Valentine. This uses a special case of the labelled record types provided in Z and referred to as schema types. The elements of schema types are called bindings. Z provides a convenient notation for denoting arbitrary subsets of schema types. For example, `[x, y : Z | x < y]` denotes the set of all bindings `(x == a, y == b)` where `a < b`. In this notation, the declarations to the right of the vertical bar are called the signature. As a special case, `[true]` denotes the total set of the schema type over the empty signature, which has just one element. The power set of this type then has two elements, which we use to represent the two truth values.
Lemma 1 Ltd. SMT-LIB in Z

\[
\begin{align*}
\text{Bool} &= \mathbb{P} \{ \text{true} \} \\
\text{True} &= \{ \text{true} \} \\
\text{False} &= \{ \text{false} \}
\end{align*}
\]

\(Z\) has built-in operators (referred to collectively as the schema calculus) that combine sets of bindings by combining the defining properties of the sets with logical connectives. This gives us a direct representation of the propositional connectives on our chosen representation of truth values.

\[
\begin{align*}
\text{Not} &: \text{Bool} \to \text{Bool}; \\
\text{And}, \text{Or}, \text{Xor}, \text{Implies} &: \text{Bool} \to \text{Bool} \to \text{Bool}
\end{align*}
\]

\[
\begin{align*}
\forall p : \text{Bool} &\bullet \text{Not } p = (\neg_s p); \\
\forall p, q : \text{Bool} &\bullet \text{And } p \ q = (p \land_s q); \\
\forall p, q : \text{Bool} &\bullet \text{Or } p \ q = (p \lor_s q); \\
\forall p, q : \text{Bool} &\bullet \text{Xor } p \ q = (\neg_s (p \leftrightarrow_s q)); \\
\forall p, q : \text{Bool} &\bullet \text{Implies } p \ q = (p \Rightarrow_s q)
\end{align*}
\]

It is now very straightforward to define the chainable equality and pairwise distinct predicates:

\[
\begin{align*}
\text{Equal, Distinct} &: \text{seq } A \to \text{Bool}
\end{align*}
\]

\[
\begin{align*}
\forall s : \text{seq } A &\bullet \text{Equal } s = [\forall i, j : \text{dom } s \bullet s i = s j]; \\
\forall s : \text{seq } A &\bullet \text{Distinct } s = [\forall i, j : \text{dom } s \bullet s i = s j \iff i = j]
\end{align*}
\]

We define if-then-else by pattern-matching:

\[
\begin{align*}
\text{ITE} &: \text{Bool} \to A \to A \to A
\end{align*}
\]

\[
\begin{align*}
\forall x, y : A &\bullet \text{ITE } \text{True } x \ y = x; \\
\forall x, y : A &\bullet \text{ITE } \text{False } x \ y = y
\end{align*}
\]
2.2 Integer Numbers

The integers from the Z toolkit provide the representation for the theory of Integers.

SML

```sml
open theory "ZS_Ints";
```

Z

```z
| Int == Z
```

Note that (unlike Lisp) addition and multiplication are binary operators not operators on lists. Division and modulus are defined the same way in the ProofPower Z toolkit as they are in SMT-LIB, but Standard Z offers a different definition

Z

```z
| INeg, IAbs : Int → Int;
| ISub, IAdd, IMul, IDiv, IMod : Int → Int → Int
```

```z
∀x : Int • INeg x = ~x;
∀x : Int • IAbs x = abs x;
∀x, y : Int • ISub x y = x − y;
∀x, y : Int • IAdd x y = x + y;
∀x, y : Int • IMul x y = x * y;
∀x, y : Int | ¬ y = 0 • 0 ≤ IMod x y < abs y;
∀x, y : Int | ¬ y = 0 • x = (IDiv x y) * y + IMod x y
```

Z

```z
| ILE, ILT, IGE, IGT : seq Int → Bool
```

```z
∀s : seq Int • ILE s = \[ ∀i, j : dom s • i < j ⇒ s i ≤ s j \];
∀s : seq Int • ILT s = \[ ∀i, j : dom s • i < j ⇒ s i < s j \];
∀s : seq Int • IGE s = \[ ∀i, j : dom s • i < j ⇒ s i ≥ s j \];
∀s : seq Int • IGT s = \[ ∀i, j : dom s • i < j ⇒ s i > s j \]
```

Z

```z
| Divisible : N₁ → Int → Bool
```

```z
∀n, i : Int • Divisible n i = \[ ∃q : Int • i = q * n \]
```
2.3 Reals

The ProofPower-Z library defines the real numbers as a separate type with the operators distinguished from those for the integers by a subscript.

SML

| open theory "ZS_Reals"; |

$\text{Real} == \mathbb{R}$

$\text{RNeg} : \text{Real} \to \text{Real}$;
$\text{RSub, RAdd, RMul, RDiv} : \text{Real} \to \text{Real} \to \text{Real}$

$\forall x : \text{Real} \bullet \text{RNeg} x = \sim_R x;$
$\forall x, y : \text{Real} \bullet \text{RSub} x y = x -_R y;$
$\forall x, y : \text{Real} \bullet \text{RAdd} x y = x +_R y;$
$\forall x, y : \text{Real} \bullet \text{RMul} x y = x *_R y;$
$\forall x, y : \text{Real} \bullet \text{RDiv} x y = x /_R y$

$\text{RLE, RLT, RGE, RGT} : \text{seq Real} \to \text{Bool}$

$\forall s : \text{seq Real} \bullet \text{RLE} s = [\forall i, j : \text{dom} s \bullet i < j \Rightarrow s \ i \leq_R s \ j];$
$\forall s : \text{seq Real} \bullet \text{RLT} s = [\forall i, j : \text{dom} s \bullet i < j \Rightarrow s \ i \ <_R s \ j];$
$\forall s : \text{seq Real} \bullet \text{RGE} s = [\forall i, j : \text{dom} s \bullet i < j \Rightarrow s \ i \geq_R s \ j];$
$\forall s : \text{seq Real} \bullet \text{RGT} s = [\forall i, j : \text{dom} s \bullet i < j \Rightarrow s \ i \ >_R s \ j]$

2.4 Reals_Ints

SML

| open theory"ZS_Reals_Ints"; |

$\text{ToReal} : \text{Int} \to \text{Real}$

$\text{ToReal} = \text{real}$
Lemma 1 Ltd. SMT-LIB in Z

\[ \textbf{ToInt} : \text{Real} \rightarrow \text{Int} \]

\[ \forall x : \text{Real} \bullet \text{let } i = \text{real } (\text{ToInt } x) \bullet i \leq_R x <_R i +_R 1.0 \]

\[ \textbf{IsInt} : \text{Real} \rightarrow \text{Bool} \]

\[ \forall x : \text{Real} \bullet \text{IsInt } x = [ \mid x \in \text{ran } \text{ToReal} ] \]

2.5 ArraysEx

\texttt{open theory "ZS\_ArraysEx";}

\[ \textbf{Array}[X, Y] = X \to Y \]

\[ \begin{align*}
\textbf{Select} & : \text{Array}[X, Y] \to X \to Y; \\
\textbf{Store} & : \text{Array}[X, Y] \to X \to Y \to \text{Array}[X, Y]
\end{align*} \]

\[ \forall a : \text{Array}[X, Y]; x : X \bullet \text{Select } a x = a x; \]
\[ \forall a : \text{Array}[X, Y]; x : X; y : Y \bullet \text{Store } a x y = a \oplus \{x \mapsto y\} \]

2.6 FixedSizeBitVectors

\texttt{open theory "ZS\_FixedSizeBitVectors";}

We represent SMTLIB bit vectors as (non-empty) sequences of bits:

\[ \textbf{Bit} = \{0, 1\} \]

The bit vectors of lengths 1, 2, \ldots partition the set of all non-empty bit strings:
\begin{align*}
\text{BitString} &= \text{seq}_1 \text{Bit} \\
\text{BitVec} : \mathbb{N}_1 \to \mathbb{P} \text{BitString} \\
\forall m : \mathbb{N}_1 \bullet \text{BitVec } m = \{ b : \text{BitString} \mid \#b = m \}
\end{align*}

Note that in SMTLIB, the length of a bit vector is always statically known. So SMTLIB can and does impose static restrictions that we will have to model in $\mathbb{Z}$ by treating $\text{BitVec}$ like a dependent subtype constructor.

We need some auxiliary functions to assist in defining the sequence operations. We need the function that converts a bit string into the natural number it represents (in binary, most-significant bit at the left):

\begin{align*}
\text{BV2Nat} : \text{BitString} \to \mathbb{N} \\
\forall x : \text{Bit} \bullet \text{BV2Nat } \langle x \rangle = x; \\
\forall x : \text{Bit}; b : \text{BitString} \bullet \text{BV2Nat } (b \upharpoonright \langle x \rangle) = 2^x \text{BV2Nat } b + x
\end{align*}

To define the conversion from natural numbers to bit vectors, we need natural number powers of integers. This may be defined already in later versions of ProofPower. The following ML defends against that:

\begin{verbatim}
val _ = ⌜Z(^)\^1 handle Fail _ => ( diag_line "Please ignore the above error message.";

fun 80 rightassoc _ ^ _

_ ^ _ : Z \times N \to Z

\forall i : Z\bullet i \^ 0 = 1; \\
\forall i : Z; j : N\bullet i \^ (j + 1) = i \ast i \^ j
\end{verbatim}
Now we can define the conversion from natural numbers to bit vectors of a given length. Note that the restriction $\text{BitVec } m \triangleleft \text{BV2Nat}$ is a bijection between $\text{BitVec } m$ and $0..2^m - 1$ for any $m$.

$$\forall m : \mathbb{N}_1; n : \mathbb{N}\cdot \text{Nat2BV } m \cdot n = (((\text{BitVec } m \triangleleft \text{BV2Nat})^\sim) \cdot (n \mod 2^m)$$

We need the logical operations on bits:

$$\forall x : \text{Bit}\cdot \text{BitNot } x = 1 - x;$$
$$\forall x, y : \text{Bit}\cdot \text{BitAnd } x \cdot y = x \cdot y;$$
$$\forall x, y : \text{Bit}\cdot \text{BitOr } x \cdot y = x + y - x \cdot y$$

We define the binary bitwise logical operations on operands of mixed length to give a result that has the same length as the shorter operand. Mixed length operands are statically disallowed allowed in SMTLIB.
Lemma 1 Ltd.  SMT-LIB in Z  12

\[ \text{BVNot} : \text{BitString} \to \text{BitString}; \]
\[ \text{BVAnd, BVOr} : \text{BitString} \to \text{BitString} \to \text{BitString} \]

\[
\forall s : \text{BitString}.
\quad \text{dom}(\text{BVNot } s) = \text{dom } s
\wedge (\forall i : \text{dom } s \bullet \text{BVNot } s \ i = \text{BitNot}(s \ i));
\]

\[
\forall s, t : \text{BitString}.
\quad \text{dom}(\text{BVAnd } s \ t) = \text{dom } s \cap \text{dom } t
\wedge (\forall i : \text{dom } s \cap \text{dom } t \bullet \text{BVAnd } s \ t \ i = \text{BitAnd } (s \ i) (t \ i));
\]

\[
\forall s, t : \text{BitString}.
\quad \text{dom}(\text{BVOr } s \ t) = \text{dom } s \cap \text{dom } t
\wedge (\forall i : \text{dom } s \cap \text{dom } t \bullet \text{BVOr } s \ t \ i = \text{BitOr } (s \ i) (t \ i))
\]

For the binary arithmetic operations on operands of mixed length we take the result to have the same length as the longer operand. Again, SMTLIB disallows mixed length operands statically. The treatment of zero divisors is just inherited from the Z toolkit.

\[ \text{BVNeg} : \text{BitString} \to \text{BitString}; \]
\[ \text{BVAdd, BMul, BVDiv, BURem} : \text{BitString} \to \text{BitString} \to \text{BitString} \]

\[
\forall s : \text{BitString}.
\quad \text{let } m = \#s \bullet \text{BVNeg } s = \text{Nat2BV } m (2^m - \text{BV2Nat } s);
\]

\[
\forall s, t : \text{BitString}.
\quad \text{let } m = \max\{\#s, \#t\} \bullet \text{BVAdd } s \ t = \text{Nat2BV } m (\text{BV2Nat } s + \text{BV2Nat } t);
\]

\[
\forall s, t : \text{BitString}.
\quad \text{let } m = \max\{\#s, \#t\} \bullet \text{BVMul } s \ t = \text{Nat2BV } m (\text{BV2Nat } s \ast \text{BV2Nat } t);
\]

\[
\forall s, t : \text{BitString}.
\quad \text{let } m = \max\{\#s, \#t\} \bullet \text{BVDiv } s \ t = \text{Nat2BV } m (\text{BV2Nat } s \div \text{BV2Nat } t);
\]

\[
\forall s, t : \text{BitString}.
\quad \text{let } m = \max\{\#s, \#t\} \bullet \text{BURem } s \ t = \text{Nat2BV } m (\text{BV2Nat } s \mod \text{BV2Nat } t)
\]

For the shift operations on operands of mixed length we take the result to have the same length as the first operand. Again, SMTLIB disallows mixed length operands statically.
Lemma 1 Ltd. SMT-LIB in Z

$\text{BVShl, BVLshr : BitString} \rightarrow \text{BitString} \rightarrow \text{BitString}$

$\forall s, t : \text{BitString} \bullet \text{let } m == \#s \bullet$

$\text{BVShl } s \ t = \text{Nat2BV } m \ (\text{BV2Nat } s \ast \ 2^{\text{BV2Nat } t})$

$\forall s, t : \text{BitString} \bullet \text{let } m == \#s \bullet$

$\text{BVShr } s \ t = \text{Nat2BV } m \ (\text{BV2Nat } s \ 	ext{div} \ 2^{\text{BV2Nat } t})$

Finally we have the arithmetic comparison operator:

$\text{BVULT : BitString} \rightarrow \text{BitString} \rightarrow \text{Bool}$

$\forall s, t : \text{BitString} \bullet \text{BVULT } s \ t = \left[\right] \text{BV2Nat } s \ < \text{BV2Nat } t \left]\right.$

3 THE SMT-LIB LOGICS

In this section, we give Z models that support the restrictions and extensions to the various theories that are defined in the SMT-LIB logics.

The ML commands to set up the theories for the logics are given in the following table.

<table>
<thead>
<tr>
<th>Theory</th>
<th>ML set-up commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit Vector Logics</td>
<td>open theory&quot;ZS_FixedSizeBitVectors&quot;; new theory&quot;ZS_BV_Extensions&quot;;</td>
</tr>
</tbody>
</table>

3.1 Bit Vector Extensions

Note that the family of new constants (\_ bvX n) for numerals X and n introduced in the BV logic is implemented by the constant Nat2BV that is already defined in our model of the fixed length bit vector theory.

The four additional bitwise logical operations are defined in terms of basic ones just as in the SMT-LIB definition.
Lemma 1 Ltd. SMT-LIB in Z

14

\[ \text{BV Nand, BV Nor, BV Xor, BV Xnor : BitString} \to \text{BitString} \to \text{BitString} \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Nand } s \ t = \text{BV Not} (\text{BV And } s \ t) ; \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Nor } s \ t = \text{BV Not} (\text{BV Or } s \ t) ; \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Xor } s \ t = \text{BV Or} (\text{BV And } s \ (\text{BV Not } t)) \ (\text{BV And} \ (\text{BV Not } s) \ t) ; \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Xnor } s \ t = \text{BV Or} (\text{BV And } s \ t) \ (\text{BV And} \ (\text{BV Not } s) \ (\text{BV Not } t)) \]

We define the comparison operator in terms of equality rather than recursively. This extends the operation to operands of non-equal length so as to return \( \#b0 \).

\[ \text{BV Comp : BitString} \to \text{BitString} \to \text{BitVec 1} \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Comp } s \ t = \text{if } s = t \text{ then } (1) \text{ else } (0) \]

Subtraction is defined in terms of addition and 2s complement negation just as in the SMT-LIB definition.

\[ \text{BV Sub : BitString} \to \text{BitString} \to \text{BitString} \]

\[ \forall s, t : \text{BitString} \bullet \text{BV Sub } s \ t = \text{BV Add } s \ (\text{BV Neg } t) \]

The definitions of the other signed arithmetic operators are a little clearer in Z if we extract the sign bit using sequence indexing rather than \textit{Extract} and if we use \textit{Z if-then-else} rather than \textit{ITE}.

The SMT-LIB \texttt{sdiv} operator is 2s-complement signed division truncating towards 0. It is defined by cases on the signs of the operands using negation and unsigned division. The definition is equivalent to the following:

\[ s \texttt{sdiv } t = \text{sgn} (s) \cdot \text{sgn} (t) \cdot (\text{abs} (s) \texttt{udiv abs } t) \]

In \( m\)-bit 2s-complement arithmetic, \( s \texttt{sdiv } t \) gives the correct signed result except \((i)\) when \( t = 0 \), in which case the result is unspecified, and \((ii)\) when \( s = -2^{m-1} \) and \( t = -1 \), in which case the result is \(-2^{m-1} \) (i.e., the absolute value is correct, but the sign is wrong).
Lemma 1 Ltd. SMT-LIB in Z

$\textbf{BV Sdiv} : \text{BitString} \rightarrow \text{BitString} \rightarrow \text{BitString}$

$\forall s, t : \text{BitString} \bullet \text{BV Sdiv } s \ t =$

(let $\text{msb}_s == s 1; \text{msb}_t == t 1$ •

if $\text{msb}_s = 0 \land \text{msb}_t = 0$

then $\text{BVUdiv } s \ t$

else if $\text{msb}_s = 1 \land \text{msb}_t = 0$

then $\text{BVNeg } (\text{BVUdiv } (\text{BVNeg } s) \ t)$

else if $\text{msb}_s = 0 \land \text{msb}_t = 1$

then $\text{BVNeg } (\text{BVUdiv } s (\text{BVNeg } t))$

else $\text{BVUdiv } (\text{BVNeg } s) (\text{BVNeg } t)$)

The SMT-LIB $\textbf{srem}$ operator is signed remainder with sign following the dividend. The definition is equivalent to the following:

$s \textbf{srem } t = \text{sgn}(s) \cdot (\text{abs}(s) \textbf{urem } \text{abs}(t))$.

If $T = 0$ this is undefined, otherwise when $t$ is an $m$-bit 2s-complement number, $0 \leq \text{abs}(s) \textbf{urem } \text{abs}(t) < \text{abs}(t) \leq 2^{m-1}$, hence the multiplication by $\text{sgn}(s)$ will not overflow in $m$-bit arithmetic.

The operators $\textbf{sdiv}$ and $\textbf{srem}$ satisfy the following identities:

$\text{abs}(s \textbf{srem } t) \leq \text{abs}(t)$ provided $t \neq 0$

$s = (s \textbf{sdiv } t) \ast t + s \textbf{srem } t$ provided $t \neq 0$ and $(s, t) \neq (-2^{m-1}, -1)$.

$\textbf{BV Srem} : \text{BitString} \rightarrow \text{BitString} \rightarrow \text{BitString}$

$\forall s, t : \text{BitString} \bullet \text{BV Srem } s \ t =$

(let $\text{msb}_s == s 1; \text{msb}_t == t 1$ •

if $\text{msb}_s = 0 \land \text{msb}_t = 0$

then $\text{BVUrem } s \ t$

else if $\text{msb}_s = 1 \land \text{msb}_t = 0$

then $\text{BVNeg } (\text{BVUrem } (\text{BVNeg } s) \ t)$

else if $\text{msb}_s = 0 \land \text{msb}_t = 1$

then $\text{BVUrem } s (\text{BVNeg } t)$

else $\text{BVNeg } (\text{BVUrem } (\text{BVNeg } s) (\text{BVNeg } t))$)
The SMT-LIB \texttt{smod} operator is signed remainder with sign following the divisor. The definition is equivalent to the following:

\[ s \texttt{smod} t = s - \lfloor s / t \rfloor \cdot t. \]

This is defined by cases in such a way as to give the correct result in 2s-complement arithmetic except when \( t = 0 \), in which case the result is undefined.

\[ \texttt{BV Smod} : \texttt{BitString} \to \texttt{BitString} \to \texttt{BitString} \]

\[
\forall s, t : \texttt{BitString} \bullet \texttt{BV Smod} s t = \\
(\text{let } \texttt{msb}_s == s 1; \texttt{msb}_t == t 1 \bullet \\
\text{let } \texttt{abs}_s == \text{if } \texttt{msb}_s = 0 \text{ then } s \text{ else } \texttt{BV Neg} s; \\
\texttt{abs}_t == \text{if } \texttt{msb}_t = 0 \text{ then } t \text{ else } \texttt{BV Neg} t \bullet \\
\text{let } u == \texttt{BV Urem} \texttt{abs}_s \texttt{abs}_t \bullet \\
\text{if } u = \texttt{Nat2BV (#s) 0} \text{ then } u \\
\text{else if } \texttt{msb}_s = 0 \land \texttt{msb}_t = 0 \text{ then } u \\
\text{else if } \texttt{msb}_s = 1 \land \texttt{msb}_t = 0 \text{ then } \texttt{BV Add} (\texttt{BV Neg} u) t \\
\text{else if } \texttt{msb}_s = 0 \land \texttt{msb}_t = 1 \text{ then } \texttt{BV Add} u t \\
\text{else } \texttt{BV Neg} u)
\]

Unsigned less-than is already defined in the fixed size bit vector theory. The bit vector extensions add the three unsigned comparison operators.

\[ \texttt{BVULE, BVUGT, BVUGE} : \texttt{BitString} \to \texttt{BitString} \to \texttt{Bool} \]

\[
\forall s, t : \texttt{BitString} \bullet \texttt{BVULE} s t = [\text{BV2Nat } s \leq \text{BV2Nat } t]; \\
\forall s, t : \texttt{BitString} \bullet \texttt{BVULE} s t = [\text{BV2Nat } s > \text{BV2Nat } t]; \\
\forall s, t : \texttt{BitString} \bullet \texttt{BVULE} s t = [\text{BV2Nat } s \geq \text{BV2Nat } t]
\]

The BV logic extensions give the four signed comparison operators.
Lemma 1 Ltd. SMT-LIB in Z

\[ \text{BVSLT, BVSL, BVSGT, BVSGE: BitString} \to \text{BitString} \to \text{Bool} \]

\[ \forall s, t : \text{BitString}\bullet \text{BVSLT}\ s\ t = [\]
\[ s \ 1 = 1 \land t \ 1 = 0 \]
\[ \lor \ s \ 1 = t \ 1 \land \text{BV2Nat}\ s < \text{BV2Nat}\ t]; \]
\[ \forall s, t : \text{BitString}\bullet \text{BVSLT}\ s\ t = [\]
\[ s \ 1 = 1 \land t \ 1 = 0 \]
\[ \lor \ s \ 1 = t \ 1 \land \text{BV2Nat}\ s \leq \text{BV2Nat}\ t]; \]
\[ \forall s, t : \text{BitString}\bullet \text{BVSGT}\ s\ t = \text{BVSLT}\ t\ s; \]
\[ \forall s, t : \text{BitString}\bullet \text{BVSGE}\ s\ t = \text{BVSL}\ t\ s \]

The SMT-LIB operator \texttt{ashr} is an arithmetic right shift, i.e., it shifts in copies of the sign-bit from the left. (Note that left shifts are the same for signed and unsigned arithmetic.)

\[ \text{BV Ashr : BitString} \to \text{BitString} \to \text{BitString} \]

\[ \forall s, t : \text{BitString}\bullet \text{BV Ashr}\ s\ t = [\]
\[ \text{if } s \ 1 = 0 \text{ then BVLshr}\ s\ t\ \text{else BVNot}\ (BVLshr\ (BVNot\ s)\ t) \]

The repeat operator replicates a bit vector a specified number of times. We define this using indexing rather than recursion.

\[ \text{BV Repeat : N} \to \text{BitString} \to \text{BitString} \]

\[ \forall j : \text{N}; t : \text{BitString}\bullet \]
\[ \#(\text{BV Repeat}\ j\ t) = j \ast \#t \]
\[ \lor \ (\forall i : 1..j \ast \#t\bullet \text{BV Repeat}\ j\ t\ i = t\ ((i - 1) \mod j) + 1) \]

The zero extension operator pads a bit vector on the left with a specified number of zeroes.

\[ \text{BV ZeroExtend : N} \to \text{BitString} \to \text{BitString} \]

\[ \forall i : \text{N}; t : \text{BitString}\bullet \text{BV ZeroExtend}\ i\ t = ((1..i) \times \{0\}) \uparrow t \]
Lemma 1 Ltd. SMT-LIB in Z

\[ \forall i : \mathbb{N};\ t : \text{BitString} \]
\[ BV\text{RotateLeft} \ i \ t = (((i + 1) \ldots \#t) \uparrow t) \leftarrow ((1 \ldots i) \downarrow t); \]
\[ \forall i : \mathbb{N};\ t : \text{BitString} \]
\[ BV\text{RotateRight} \ i \ t = (((\#t - i + 1) \ldots \#t) \uparrow t) \leftarrow ((1 \ldots (\#t - i)) \downarrow t) \]
4 INDEX

And .......................... 6  IAbs ............................. 7
BitAnd ......................... 11  IAdd .............................. 7
BitNot .......................... 11  IDiv ............................. 7
BitOr .......................... 11  IGE .............................. 7
BitVec ......................... 10  IGT ............................. 7
Bool ............................ 6  ILE .............................. 7
BV2Nat ......................... 10  ILT ............................. 7
BVAdd .......................... 12  IMod ............................. 7
BVAnd .......................... 12  Implies ......................... 6
BVAshr .......................... 17  Int ............................. 7
BVComp ......................... 14  Int2BV ......................... 11
BVLShr .......................... 13  IsInt ........................... 9
BVMul .......................... 12  IsNat ........................... 9
BVNot .......................... 14  ISub ............................. 7
BVRepeat ........................ 17  ITE ............................ 6
BVRotateLeft ................... 18  RAdd ............................ 8
BVRotateRight .................. 18  RDiv ............................ 8
BVSDiv .......................... 15  Real ............................ 8
BVSGE .......................... 17  RGE ............................. 8
BVSGT .......................... 17  RGT ............................. 8
BVSGT .......................... 17  RLE ............................. 8
BVShl .......................... 13  RLT ............................. 8
BVSLT .......................... 17  RMul ............................ 8
BVSSlt .......................... 17  RNeg ............................ 8
BVSmod .......................... 16  RSub ............................ 8
BVStrem .......................... 15  Select ........................... 9
BVSub .......................... 14  Store ............................ 9
BVUDiv .......................... 12  ToInt ........................... 9
BVUGE .......................... 16  ToReal ........................... 8
BVUGT .......................... 16  True ............................ 6
BVULE .......................... 16  Xor ............................ 6
BVULT .......................... 13  ^ .............................. 10
BVUrem .......................... 12  ~ .............................. 7
BVXor .......................... 14  IT E ............................ 6
BVXnor .......................... 14  IMul .............................. 8
BVZeroExtend .................... 17  IMod .............................. 8
Concat ........................... 11  INeg ............................. 7
Distinct ........................ 6  IMul .............................. 8
Divisible ....................... 7  IMod .............................. 8
Equal ........................... 6  IReLU ............................ 7
Extract .......................... 11  IReU ............................ 7
False ............................ 6  IRem ............................. 7