Introduction to Predicate Logic 1

Examples 2

CSE 607: E-2

Title: Introduction to Predicate Logic 1

SML files: none

Objective: Practice with predicate logic proof terms.

1 Introduction

The following sections have examples based on the description of predicate logic given by Manna and Waldinger in [1]. Make sure you review the definitions of terms in Chapter 3.

Predicates are functions that yield a Boolean value – true or false when applied to their arguments. We use predicates all the time. For example $x < y$ is a predicate, i.e., it is either true or false depending on the values of $x$ and $y$.

The crucial concepts introduced in Chapter 3 are the notions of universal and existential quantification denoted by $\forall$ and $\exists$. They are understood in terms of interpretations. If a formula $\forall x. F$ is valid, then it means that the interpretation of $F$ is true for all values or interpretations of $x$. If a formula $\exists x. F$ is valid, then it means that there is at least one value of $x$ or one interpretation of $x$ under which $F$ is true.

2 Free and Bound Variables

It is crucial to understand the notions of free and bound variables. To understand them we need to define the structure of quantified formulas.

Quantified formulas have the form: $\forall x. F$ or $\exists x. F$. $\forall x$ (or $\exists x$) is the quantifier of the formula, and $F$ is the scope of the formula.

Variable $x$ in expression $E$ is bound by the innermost quantifier $\forall x$ or $\exists x$ that has $x$ within its scope. Any variable $x$ is free in $E$ if $x$ is not in the scope of any quantifier $\forall x$ or $\exists x$.

For example, let $E$ be the formula $\forall x. (P(x) \land \exists y. \forall x. Q(x, y))$. $E$ has three bound variables. Variables $x$ and $y$ in $Q(x, y)$ are bound by the quantifiers in $\exists y. \forall x. Q(x, y)$. Variable $x$ in $P(x)$ is bound by the single outermost quantifier in $\forall x. (P(x) \land \exists y. \forall x. Q(x, y))$. To see this, we can successively break apart $E$ into its components. We analyze $E$ from the “inside-out.”

1. The innermost quantified formula is: $E_1 = \forall x. Q(x, y)$. $E_1$ has bound variable $x$ and free variable $y$ in scope $Q(x, y)$. 
2. The next innermost quantified formula is: $E_2 = \exists y. E_1$. The $y$ in $\exists y$ binds the free occurrence of $y$ in $E_1$. As there are no free variables in $E_2$, it is a closed formula, i.e. there are no free variables which are open to interpretation.

3. The next innermost quantified formula is $E = \forall x. (P(x) \land E_2)$. $x$ in $\forall x$ binds the free occurrence of $x$ in $P(x)$. As $E_2$ is closed and has no free occurrences of $x$, the $x$ in $P(x)$ is distinct from the bound occurrence of $x$ in $E_2$. In fact, we could have renamed $x$ as $z$ to get $E = \forall z. (P(z) \land E_2)$ and have an equivalent formula.

3 Interpretations

Interpretations assign values to symbols. They include a domain (set of objects) and assign meanings to each constant, variable, function, and predicate symbol. Two interpretations $I$ and $J$ agree on $s$ if $I$ and $J$ make the same assignment to $s$.

If interpretations $I$ and $J$ agree on all constants, functions, predicate symbols and free variables of formula $E$, then the value of $E$ under $I$ equals the value of $E$ under $J$.

An interpretation $I$ is modified by composing it with new bindings. For example, $\langle x \leftarrow d \rangle \circ I$ denotes an interpretation which makes the same assignments as $I$ except for $x$ which is assigned the value $d$.

When $x$ and $y$ are distinct terms, $\langle x \leftarrow d_x \rangle \circ \langle y \leftarrow d_y \rangle \circ I$ is the same as $\langle y \leftarrow d_y \rangle \circ \langle x \leftarrow d_x \rangle \circ I$.

As an example, consider the value of $E$ under various interpretations as shown in Table 1.

Table 1: Interpretations of $E = x \land y$

<table>
<thead>
<tr>
<th>Term</th>
<th>$I$</th>
<th>$\langle y \leftarrow \text{true} \rangle \circ I$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x \land y$</td>
<td>$x \land y$</td>
<td>$x \land y$</td>
</tr>
<tr>
<td>$x$</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>$y$</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>$E$</td>
<td>false</td>
<td>true</td>
</tr>
</tbody>
</table>

We denote the value of $E$ under an interpretation $I$ by $I[E]$.

4 Semantics for Quantifiers

Using interpretations, we define the meaning of sentences quantified with $\forall$ and $\exists$.

$\forall$-rule: $I$ is an interpretation over domain $D$. The $I[\forall x. F] = \text{true}$ if-and-only-if for every $d \in D$, $\langle x \leftarrow d \rangle \circ I[F] = \text{true}$

Consider the following examples.

1. $\forall x. (x \lor \neg x)$
   - $D = \{\text{true}, \text{false}\}$
   - $I = \{x \leftarrow \text{false}\}$
   - $I[x \lor \neg x] = I[x]$ or $I[\neg x] = \text{false or (not false)} = \text{true}$
• $(\langle x \leftarrow \text{true} \rangle \circ \mathcal{I})[x \lor \neg x] = \text{true}$
• $\mathcal{I}[\forall x. (x \lor \neg x)] = \text{true}$

2. $\forall x. (x \land y)$
   • $D = \{\text{true}, \text{false}\}$
   • $\mathcal{I} = \{x \leftarrow \text{true}, y \leftarrow \text{true}\}$
   • $\mathcal{I}[x \land y] = \mathcal{I}[x] \land \mathcal{I}[y] = \text{true} \land \text{true} = \text{true}$
   • $(\langle x \leftarrow \text{false} \rangle \circ \mathcal{I})[x \land y] = \text{false} \land \text{true} = \text{false}$
   • $\mathcal{I}[\forall x. (x \land y)] = \text{false}$

3. $\forall x. (x \lor y)$
   • $D = \{\text{true}, \text{false}\}$
   • $\mathcal{I} = \{x \leftarrow \text{true}, y \leftarrow \text{true}\}$
   • $\mathcal{I}[x \lor y] = \text{true} \lor \text{false} = \text{true}$
   • $(\langle x \leftarrow \text{false} \rangle \circ \mathcal{I})[x \lor y] = \text{false} \lor \text{true} = \text{true}$
   • $\mathcal{I}[\forall x. (x \lor y)] = \text{true}$

$\exists$-rule: $\mathcal{I}$ is an interpretation over domain $D$. $\mathcal{I}[\exists x. \mathcal{F}] = \text{true}$ if-and-only-if there is a $d \in D$ such that $(\langle x \leftarrow d \rangle \circ \mathcal{I})[\mathcal{F}] = \text{true}$

Consider the following examples.

1. $\exists x. (x \land \neg x)$
   • $D = \{\text{true}, \text{false}\}$
   • $\mathcal{I} = \{x \leftarrow \text{true}\}$
   • $\mathcal{I}[x \land \neg x] = \text{true} \land \neg \text{true} = \text{false}$
   • $(\langle x \leftarrow \text{false} \rangle \circ \mathcal{I})[x \land \neg x] = \text{false} \land \neg \text{false} = \text{false}$
   • $\mathcal{I}[\exists x. (x \land \neg x)] = \text{false}$

2. $\exists x. (x \lor y)$
   • $D = \{\text{true}, \text{false}\}$
   • $\mathcal{I} = \{x \leftarrow \text{false}, y \leftarrow \text{false}\}$
   • $\mathcal{I}[x \lor y] = \text{false} \lor \text{false} = \text{false}$
   • $(\langle x \leftarrow \text{true} \rangle \circ \mathcal{I})[x \lor y] = \text{true} \lor \text{false} = \text{true}$
   • $\mathcal{I}[\exists x. (x \lor y)] = \text{true}$

3. $\exists x. (y \supset x)$
   • $D = \{\text{true}, \text{false}\}$
   • $\mathcal{I} = \{x \leftarrow \text{false}, y \leftarrow \text{true}\}$
\[ I[y \supset x] = true \implies false = false \]
\[ (\langle x \leftarrow true \rangle \circ I)[y \supset x] = true \implies true = true \]
\[ I[\exists x.(y \supset x)] = true \]

4. \( \exists x.(x \geq 4) \)
\[ D = \{0, 1, 2, \ldots\} \]
\[ I = \{ x \leftarrow 2 \} \]
\[ I[x \geq 4] = two \ greater \ than \ or \ equal \ to \ four = false \]
\[ (\langle x \leftarrow 4 \rangle \circ I)[x \geq 5] = four \ greater \ than \ or \ equal \ to \ four = true \]
\[ I[\exists x.(x \geq 4)] = true \]

5 \ Validity

Validity is a property of closed sentences, i.e., sentences with no free variables. A closed sentence \( F \) is valid if \( I[F] = true \) for any interpretation \( I \).

Consider the following examples.

1. \( \forall x.\exists y.(x \lor y) \)
\[ \bullet \ \text{Domain } D = \{true, false\}. \]
\[ \bullet \ \text{By } \forall\text{-rule } I[\exists y.(x \lor y)] = true \text{ must be true for all interpretations } I. \]
\[ \quad \text{Case } x \leftarrow false: \text{ by } \exists\text{-rule } (\langle x \leftarrow false \rangle \circ I)[x \lor y] \text{ must be true for some value of } y. \text{ In this case, } x \lor y \text{ under } (y \leftarrow true) \circ (x \leftarrow false) \circ I \text{ is true.} \]
\[ \quad \text{Case } x \leftarrow true: \text{ by } \exists\text{-rule } x \lor y \text{ under } (x \leftarrow true) \circ I \text{ must be true for some value of } y. \text{ In this case } x \lor y \text{ under } (y \leftarrow true) \circ (x \leftarrow true) \circ I \text{ is true. Note, we also could have used } y \leftarrow false. \]
\[ \bullet \ \neg \neg \forall x.\exists y.(x \lor y) \text{ is valid.} \]

2. \( \exists x.\forall y.(x \lor y) \)
\[ \bullet \ \text{Domain } D = \{true, false\}. \]
\[ \bullet \ \text{By } \exists\text{-rule: } I[\forall y.(x \lor y)] = true \text{ must be true for some modified interpretation } I \text{ of any arbitrary interpretation } I. \]
\[ \quad \text{Consider the interpretation } (x \leftarrow true) \circ I. \]
\[ \quad \text{By } \forall\text{-rule for all modifications } \langle y \leftarrow d \rangle \text{ of } (x \leftarrow true) \circ I, \ x \lor y \text{ must be true.} \]
\[ \quad \neg \neg (\langle y \leftarrow true \rangle \circ \langle x \leftarrow true \rangle \circ I)[x \lor y] = true. \]
\[ \bullet \ \neg \exists x.\forall y.(x \lor y) \text{ is valid.} \]

3. \( \forall x.\forall y.(x \lor y) \)
• Domain $D = \{true, false\}$.

• By $\forall$-rule for all modifications ($\langle x \leftarrow d \rangle \circ \mathcal{I} \models \forall y.(x \lor y)$ = true where $\mathcal{I}$ is any arbitrary interpretation over $D$.
  
  – Consider the interpretation $\langle x \leftarrow false \rangle \circ \mathcal{I}$.

  – By $\forall$-rule ($\langle y \leftarrow d' \rangle \circ \langle x \leftarrow false \rangle \circ \mathcal{I} \models [x \lor y] = true$.

    • Consider the interpretation ($\langle y \leftarrow false \rangle \circ \langle x \leftarrow false \rangle \circ \mathcal{I} \models [x \lor y] = false$

• $\sim \forall x.\forall y.(x \lor y)$ is not valid.

6 Closures

6.1 Universal Closures

Let $x_1, \ldots, x_n$ be a complete list of distinct free variables in order of occurrence in $\mathcal{F}$ when scanning $\mathcal{F}$ from left-to-right. $(\forall\exists).\mathcal{F}$ denotes $\forall x_1 x_2 \ldots x_n.\mathcal{F}$ which denotes $\forall x_1 . \forall x_2 . \ldots . \forall x_n.\mathcal{F}$. $\mathcal{I}[(\forall\exists).\mathcal{F}] = true$ if-and-only-if

• For any $d_1, \ldots, d_n \in D$, $\langle x_1 \leftarrow d_1 \rangle \circ \ldots \circ \langle x_n \leftarrow d_n \rangle \circ \mathcal{I}[[\mathcal{F}]] = true$ if-and-only-if

• For any interpretation $\mathcal{J}$ that agrees with $\mathcal{I}$ on the constant, function, and predicate symbols of $\mathcal{F}$, $\mathcal{F}$ is true under $\mathcal{J}$, $\mathcal{J}[[\mathcal{F}]] = true$

6.2 Existential Closures

Let $x_1, \ldots, x_n$ be a complete list of distinct free variables in order of occurrence in $\mathcal{F}$ when scanning $\mathcal{F}$ from left-to-right. $(\exists\forall).\mathcal{F}$ denotes $\exists x_1 x_2 \ldots x_n.\mathcal{F}$ which denotes $\exists x_1 . \exists x_2 . \ldots . \exists x_n.\mathcal{F}$. $(\exists\forall).\mathcal{F}$ is true under interpretation $\mathcal{I}$ if-and-only-if

• There are elements $d_1, \ldots, d_n \in D$, such that $\langle x_1 \leftarrow d_1 \rangle \circ \ldots \circ \langle x_n \leftarrow d_n \rangle \circ \mathcal{I}[[\mathcal{F}]] = true$ if-and-only-if

• There is an interpretation $\mathcal{J}$ that agrees with $\mathcal{I}$ on the constant, function, and predicate symbols of $\mathcal{F}$, such that $\mathcal{F}$ is true under $\mathcal{J}$, $\mathcal{J}[[\mathcal{F}]] = true$.

6.3 Universal Closure Property

The universal closure property states

For any sentence $\mathcal{F}$, $\{(\forall\exists).\mathcal{F}$ is valid} if-and-only-if $\mathcal{I}[[\mathcal{F}]] = true$ under every interpretation $\mathcal{I}$.

The proof is in two parts: first $(\forall\exists).\mathcal{F}$ is assumed to be valid from which we show that $\mathcal{I}[[\mathcal{F}]] = true$ for every interpretation $\mathcal{I}$, and second we assume $\mathcal{I}[[\mathcal{F}]] = true$ for every interpretation $\mathcal{I}$ and show $(\forall\exists).\mathcal{F}$ is valid.
1. Assume $(\forall \ast).F$ is valid.
   - By definition of $(\forall \ast).F$ being valid, $\mathcal{I}[(\forall \ast).F] = true$ for all $\mathcal{I}$.
   - By definition of universal closure, for all modified interpretations $\langle x_1 \leftarrow d_1 \rangle \circ \ldots \circ \langle x_n \leftarrow d_n \rangle \circ \mathcal{I}[F] = true$.
   - $\sim F$ is true for all interpretations $\mathcal{I}$, $\mathcal{I}[F] = true$.

2. Assume $\mathcal{I}[F] = true$ for all interpretations $\mathcal{I}$.
   - Consider an arbitrary interpretation, $\mathcal{I}'$.
   - Under the assumption, for all interpretations $\langle x_1 \leftarrow d_1 \rangle \circ \ldots \circ \langle x_n \leftarrow d_n \rangle \circ \mathcal{I}'[F] = true$.
   - By definition of universal closure, $(\forall \ast).F$ for $\mathcal{I}'$.
   - As $\mathcal{I}'$ is an arbitrary interpretation, $\mathcal{I}'[F] = true$.
   - $(\forall \ast).F$ is valid.

7 Valid Sentence Schemata

We can use the universal closure property proved in the previous section to prove the validity of various forms of sentences or sentence schemata. For a particular sentence form $\mathcal{E}$, we can show its validity by proving $\mathcal{I}[(\forall \ast).\mathcal{E}] = true$ for all interpretations $\mathcal{I}$.

Consider the following examples.

1. $\neg \forall x. F \equiv \exists x. \neg F$
   - By universal closure property we must show $\mathcal{I}[(\neg \forall x. F \equiv \exists x. \neg F)] = true$ for all interpretations $\mathcal{I}$.
   - Show $\neg \forall x. F$ and $\exists x. \neg F$ have the same truth value under any interpretation.
     - $\mathcal{I}'[\neg \forall x. F] = true$ under $\mathcal{I}'$ if-and-only-if $\mathcal{I}'[\forall x. \neg F] = false$ under $\mathcal{I}'$.
     - if-and-only-if there is a $d$ such that $\langle x \leftarrow d \rangle \circ \mathcal{I}'[\neg F] = false$.
     - if-and-only-if if-and-only-if $\mathcal{I}'[\exists x. \neg F] = true$.

2. $\forall x. \forall y. F \equiv \forall y. \forall x. F$
   - Show $\mathcal{I}[(\forall x. \forall y. F \equiv \forall y. \forall x. F)] = true$ for all interpretations $\mathcal{I}$ where $x$ and $y$ are distinct.
   - Consider an arbitrary interpretation $\mathcal{I}'$.
     - $\mathcal{I}'[\forall x. \forall y. F] = true$ for all $d_1 \in D$, $\langle x \leftarrow d_1 \rangle \circ \mathcal{I}'[\forall y. F] = true$.
     - if-and-only-if for all $d_1 \in D, d_2 \in D$, $\langle y \leftarrow d_2 \rangle \circ \langle x \leftarrow d_1 \rangle \circ \mathcal{I}'[F] = true$.
     - $\mathcal{I}'[\forall y. \forall x. F] = true$ if-and-only-if for all $d_2 \in D$, $\langle y \leftarrow d_2 \rangle \circ \mathcal{I}'[\forall x. F] = true$.
     - if-and-only-if for all $d_1, d_2 \in D$, $\langle x \leftarrow d_1 \rangle \circ \langle y \leftarrow d_2 \rangle \circ \mathcal{I}'[F] = true$. 

For distinct \(x\) and \(y\), \(\langle y \leftarrow d_2 \rangle \circ \langle x \leftarrow d_1 \rangle \circ \mathcal{I}' = \langle x \leftarrow d_1 \rangle \circ \langle y \leftarrow d_2 \rangle \circ \mathcal{I}'\)

- \(\forall x.\forall y.\mathcal{F} \equiv \forall y.\forall x.\mathcal{F}\).

3. \(\forall x. [\mathcal{F} \land \mathcal{G}] \equiv \forall x. \mathcal{F} \land \forall x. \mathcal{G}\)

- Show \(\mathcal{I}[\forall x. [\mathcal{F} \land \mathcal{G}]] \equiv \forall x. \mathcal{F} \land \forall x. \mathcal{G} = \text{true}\) for all interpretations \(\mathcal{I}\).

- Consider an arbitrary interpretation \(\mathcal{I}'\).

\(- \mathcal{I}'[\forall x. [\mathcal{F} \land \mathcal{G}]] = \text{true}\) under \(\mathcal{I}'\) if-and-only-if \((\langle x \leftarrow d \rangle \circ \mathcal{I}', \mathcal{F} \land \mathcal{G} = \text{true}\).

\(- \mathcal{I}'[\forall x. \mathcal{F} \land \forall y. \mathcal{G}] = \text{true}\) under \(\mathcal{I}'\) if-and-only-if under all modified interpretations \((\langle x \leftarrow d \rangle \circ \mathcal{I}'\)[\mathcal{F}] = \text{true}\) and under all modified interpretations \((\langle x \leftarrow d \rangle \circ \mathcal{I}'\)[\mathcal{G}] = \text{true}\).

\(- \mathcal{I}'[\forall x. \mathcal{F} \land \forall y. \mathcal{G}] = \text{true}\) under \(\mathcal{I}'\) if-and-only-if under all modified interpretations \((\langle x \leftarrow d \rangle \circ \mathcal{I}'\)[\mathcal{F}] = \text{true}\) and \((\langle x \leftarrow d \rangle \circ \mathcal{I}'\)[\mathcal{G}] = \text{true}\).

- \(\forall x. \mathcal{F} \land \forall x. \mathcal{G} \equiv \forall x. [\mathcal{F} \land \mathcal{G}]\).

8 Safe Substitution

Safe substitution requires the avoidance of two problems: (1) substitution into bound occurrences of a subexpression, and (2) name capture within a quantified expression.

A subexpression \(\mathcal{E}'\) in an expression \(\mathcal{E}\) is bound in \(\mathcal{E}\) if there is a variable \(x\) that is free in \(\mathcal{E}'\) but is bound in \(\mathcal{E}\) because \(\mathcal{E}'\) is within the scope of a quantifier \(\forall x\) or \(\exists x\) when it appears in \(\mathcal{E}\).

For example, \(x\) in \(p(x)\) is free. The occurrence of \(p(x)\) in \(\exists x. [r(y) \land p(x)]\) is bound because \(x\) in \(p(x)\) is within the scope \(r(y) \land p(x)\) of quantifier \(\forall x\).

To illustrate how substitution into bound occurrences creates problems, assume that \(p(x) \equiv q(x)\). We can show that \(\forall x. p(x) \not\equiv \forall x. q(x)\).

1. Let \(\mathcal{I}\) be defined over \(\{\text{true, false}\}\).

2. Let \(x \leftarrow \text{true}\), \(p(x) \leftarrow x\), and \(q(x) \leftarrow x \lor \neg x\).

3. \(p(x) \equiv q(x)\) under \(\mathcal{I}\).

4. But, \(\forall x. x \not\equiv \forall x. (x \lor \neg x)\).

To illustrate how name capture is a problem, consider the interpretation \(\mathcal{I}\) where \(x \leftarrow 1\) and \(y \leftarrow 1\). Under \(\mathcal{I}\), \(x > 0 \equiv y > 0\).

1. Consider \(\mathcal{F} = \forall x. [x \geq 0 \land y > 0]\) where \(x\) and \(y\) are interpreted to be over the natural numbers \(0, 1, \ldots\).

2. \(\mathcal{F} = \text{true}\) under \(\mathcal{I}\).

3. If we blindly substitute \(x > 0\) for \(y > 0\) in \(\mathcal{F}\) we get \(\mathcal{F}[(x > 0)/(y > 0)] = \forall x. [x \geq 0 \land x > 0]\) which is \(\text{false}\) as \(x \geq 0 \land x > 0 = \text{false}\) for \(x \leftarrow 0\).

The correct substitution renames \(x\) in \(\forall x\) to avoid name capture. Doing this we would instead get: \(\mathcal{F}[(x > 0)/(y > 0)] = \forall x'. [x' \geq 0 \land x > 0]\) which has the same value as \(\mathcal{F}\).

Safe (total) substitution of \(\mathcal{G}\) by \(\mathcal{H}\) in \(\mathcal{F}\), denoted by \(\mathcal{F}[\mathcal{H}/\mathcal{G}]\), is defined as follows:
• Replace every free occurrence of $G$ in $F$ by $H$.
  
  but

• If any free variable $x$ in $H$ is captured (falls within the scope) of a quantifier $\forall x$ or $\exists x$ in $F[G]$ as a result of the replacement, rename $x$ in the quantifier to $x'$ where $x'$ is a variable which does not already occur in $F[G]$ or in $H$.

To illustrate correct total substitution, consider $F = (\exists x. \forall y. [p(x) \land q(y)]) \supset \forall x. [p(x) \land q(y)]$. Total safe substitution of $r(x)$ for $q(y)$ in $F$ is:

• $F[r(x)/q(y)] = (\exists x. \forall y. [p(x) \land q(y)]) \supset \forall x'. [p(x') \land r(x)]$.

Safe partial substitution is denoted by $F(\langle H/G \rangle)$ and is defined as follows:

• Replace zero, one, or more free occurrence of $G$ in $F$ by $H$,
  
  but

• If any free variable $x$ in $H$ is captured (falls within the scope) of a quantifier $\forall x$ or $\exists x$ in $F[G]$ as a result of the replacement, rename $x$ in the quantifier to $x'$ where $x'$ is a variable which does not already occur in $F[G]$ or in $H$.

9 A Hardware Example

Consider the truth table of a half adder shown in Figure 1. What we want to do is “prove” informally using the semantic rules of $\forall$ and $\exists$ the correctness of the following statement.

$$\forall x. \forall y. [(BV(x) + BV(y) = 2 \times BV(carry(x, y)) + BV(sum(x, y)))] \quad (1)$$

What (1) states is the addition property of half adders. Specifically, given the appropriate interpretations for carry, sum, and $BV$, the relationship between the inputs and outputs is, the sum of the bit values of the inputs equals the 2-bit binary interpretation of the carry and sum. The specific interpretations we have in mind are shown in (2) through (4) where $\oplus$ denotes exclusive-or. (2) and (3) are the usual definitions for the sum and carry outputs of a half adder. The crucial definition is $BV$ which maps $T$ and $T$ into 1 and 0, respectively.

$$sum(x, y) \leftarrow x \oplus y \quad (2)$$

$$carry(x, y) \leftarrow x \land y \quad (3)$$

$$BV(x) \leftarrow x \rightarrow 1|0 \quad (4)$$

We “prove” (1) using the quantifier rules by showing

$$((y \leftarrow d_1) \circ (x \leftarrow d_2) \circ \mathcal{I})$$

$$[[((BV(x) + BV(y) = 2 \times BV(carry(x, y)) + BV(sum(x, y)))]]) = true$$

for all interpretations $\mathcal{I}$ where $\mathcal{I}$ is any interpretation which agrees on (2) through (4) and where $d_1$ and $d_2$ are assigned all combinations of Boolean values from $(F, F)$ to $(T, T)$. 
Figure 1: Half Adder

Table 2: Half Adder Correctness Proof

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>carry</th>
<th>sum</th>
<th>$BV(x) + BV(y) = 2 \times BV(\text{carry}(x,y)) + BV(\text{sum}(x,y))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>$0 + 0 = 2 \times 0 + 0$</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>$0 + 1 = 2 \times 0 + 1$</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>$1 + 0 = 2 \times 0 + 1$</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>$1 + 1 = 2 \times 1 + 0$</td>
</tr>
</tbody>
</table>

References