1. Arithmetic modulo 2.

Let

$$\mathbf{b} = \{0, 1\}.$$

(The **b** stands for *bits*.)

We define the binary operations $+$ and $*$ on **b** by the following tables:

a	b	$a+b$
0	0	0
0	1	1
1	0	1
1	1	0

a	b	$a*b$
0	0	0
0	1	0
1	0	0
1	1	1

We note that **b** is **field** with respect to these operations. One frequently writes

$$ab \quad \text{instead of} \quad a*b.$$

We define the unary operation $\sim$ on **b** by the following table.

a	$\sim a$
1	0
0	1

Note that $\sim$ is the additive inverse in the field **b**.

We define the binary operations $\vee$ and $\wedge$ on **b** by the following tables:

a	b	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

Note that $\wedge$ equals $*$.

We define the binary operations $\rightarrow$ and $\leftrightarrow$ on **b** by the following tables:

a	b	$a \rightarrow b$
0	0	1
0	1	1
1	0	0
1	1	1

a	b	$a \leftrightarrow b$
0	0	1
0	1	0
1	0	0
1	1	1

Check that the following hold for $a, b \in \mathbf{b}$:

$$\begin{aligned} a \vee b &= ab + a + b; \\ a \wedge b &= ab; \\ \sim a &= a + 1; \\ a \rightarrow b &= ab + a + 1; \\ a \leftrightarrow b &= a + b + 1; \end{aligned}$$

and that

$$a * b = \sim (\sim a \vee \sim b)$$
$$a + b = \sim ((\sim a \vee b) \vee (\sim\sim b \vee a)).$$

2. Truth functions.

Let X be a set disjoint from the set

$$\mathbf{P}$$

consisting of the symbols

$$\mathbf{expr} \quad \sim \quad \vee \quad \wedge \quad \rightarrow \quad \leftrightarrow$$

Proposition 2.1. Suppose $A \in \mathbf{p}(X)$ and B results by replacing each occurence of a member of X in A by a member of $\mathbf{p}(X)$. Then $B \in \mathbf{p}(X)$.

Proof. Just grow the tree parsing A. □

Theorem 2.1. There is one and only way to assign to each $A \in \mathbf{p}(X)$ a function

$$\mathbf{t}_A : 2^X \to \{0, 1\}$$

in such a way that

$$\mathbf{t}_{(x)}(T) = \begin{cases} 1 & x \in T, \\ 0 & x \notin T; \end{cases}$$

whenever $x \in X$ and $T \subset X$ and

$$\begin{aligned} \mathbf{t}_{\sim\ A} &= \sim \mathbf{t}_A; \\ \mathbf{t}_{(\ A\ \vee\ B\ )} &= \mathbf{t}_A \vee \mathbf{t}_B; \\ \mathbf{t}_{(\ A\ \wedge\ B\ )} &= \mathbf{t}_A \wedge \mathbf{t}_B; \\ \mathbf{t}_{(\ A\ \rightarrow\ B\ )} &= \mathbf{t}_A \rightarrow \mathbf{t}_B; \\ \mathbf{t}_{(\ A\ \leftrightarrow\ B\ )} &= \mathbf{t}_A \leftrightarrow \mathbf{t}_B. \end{aligned} \tag{1}$$

whenever $A, B \in \mathbf{p}(X)$.

Proof. This is a straightforward consequence of the uniqueness of the parse tree for any $A \in \mathbf{p}(X)$ and our formulae for arithmetic modulo 2. □

Definition 2.1. We say $A \in \mathbf{p}(X)$ is a **tautology** if $\mathbf{t}_A(\mathcal{A}) = 1$ for all $\mathcal{A} \subset X$.

Definition 2.2. Suppose $\Gamma \subset \mathbf{p}(X)$ and $B \in \mathbf{p}(X)$ We write

$$\Gamma \models B$$

and say B **is a tautological consequence of** Γ if whenever $T \subset X$

$$\mathbf{t}_A(T) = 1 \text{ for all } A \in \Gamma \;\Rightarrow\; \mathbf{t}_B(T) = 1.$$

Example 2.1. Suppose $A, B \in \mathbf{p}(X)$. Then

$$\{A, (A \rightarrow B)\} \models B.$$

Indeed, suppose $T \subset X$, $\mathbf{t}_A(T) = 1$ and $\mathbf{t}_{(A \rightarrow B)}(T) = 1$.

To see this, consider the table

A	B	$(A \to B)$
0	0	1
0	1	0
1	0	0
1	1	1

Here is another way:

$$1 = \mathbf{t}_A(T)\mathbf{t}_{(A\to B)}(T) = \mathbf{t}_A(T)(\mathbf{t}_A(T)\mathbf{t}_B(T) + \mathbf{t}_A(T) + 1) = \mathbf{t}_B(T) + 1 + 1 = \mathbf{t}_B(T).$$