From Propositional Logic to Set Theory

Lucas Salim

August 22, 2022

Abstract

We consider the isomorphism between the groups $\mathbb{Z}_2^n$ and $\mathscr{P}(X)$, for any set X with cardinality n. We investigate how this can be useful to see propositional logic through the lenses of set theory (and vice-versa), and prove some interesting consequences that connect both fields.

Part 1. How to mathematically write logic?

Given any truth table in any dimensions, can we find a systematic way of coming up with the formula that produces the table's output? In general terms, one can imagine a truth table like the one bellow.

p_1	p_2	...	p_n	$f(p_1, p_2, ..., p_n)$
T	T	...	T	F
T	T	...	F	T
T	T	...	T	F
...	...	...	...	...
F	F	...	T	T
F	F	...	F	T

We let R_n be the set of all rows in n dimensions (i.e., a truth table without any output) and T_n the set of all possible tables in n dimensions (i.e., all possible distinct outputs for a truth table). First, notice that $|R_n| = 2^n$. This is because we need to form distinct n-tuples $(v_1, v_2, v_3, ..., v_n)$, where each $v_i = T$ or $v_i = F$. Moreover, notice that $|T_n| = 2^{|R_n|}$. This is because for each row there are two possibilities (T or F). Therefore, $|R_n| = 2^n$ and $|T_n| = 2^{2^n}$. If we define a set P_n that contains our n propositional variables (i.e., $P_n = \{p_1, p_2, p_3, ..., p_n\}$), then, interestingly enough, we have that

$$|R_n| = |\mathscr{P}(P_n)| \text{ and } |T_n| = |\mathscr{P}(\mathscr{P}(P_n))|,$$

where $\mathscr{P}(A)$ is the *power set* of A (the set of all subsets of set A). If we now represent T as ones and F as zeros, then it is easy to see that $R_n = \mathbb{Z}_2^n$ and $T_n = \mathbb{Z}_2^{2^n}$. Cardinality wise, the sets and power sets match perfectly, but there is more to this connection than just a bijection between sets. A hidden structure reveals itself when one considers the sets as groups: $\mathbb{Z}_2^k, k \in \mathbb{N}$ with addition mod 2, and $\mathscr{P}(X)$, for any set X, with the symmetric difference operation. By seeing the sets as groups, if we show that $T_n = \mathbb{Z}_2^{2^n} \cong \mathscr{P}(\mathscr{P}(P_n))$, then we can correspond each sequence of Trues and Falses on the output column (of a truth table with n dimensions) to a set containing sets that contain our propositional variables. Not only we would show that there exists a systematic way to find such propositional formula (to understand which formula exactly is one of the tasks we ought to solve - in fact, we hope there is a way to get such formula from a set), but also we would explictly present such algorithm (i.e., the isomorphism between the groups), proving the existence of an answer to our problem. Notice that to show $\mathbb{Z}_2^{2^n} \cong \mathscr{P}(\mathscr{P}(P_n))$, it suffices to show that for any finite set X, with $|X| = n$, one has $\mathbb{Z}_2^n \cong \mathscr{P}(X)$.

Proposition 1. *Let X be any finite set with $|X| = n$, and let the operation $\triangle$ be the symmetric difference between two sets: $A \triangle B := A \cup B - A \cap B$. Then*

$$(\mathscr{P}(X), \triangle) \cong (\mathbb{Z}_2^n, +).$$

Proof. We can label the elements of X so that $X = \{x_1, x_2, ..., x_n\}$. Moreover, let $\text{index}(x_i) := \text{i}$, and $\text{index}(Y) := \{\text{index}(x_i) : x_i \in Y\}$, for set Y with labeled elements. For example, if $S = \{x_4, x_7, x_8\}$, then $\text{index}(S) = \{4, 7, 8\}$. Define the function $\varphi : \mathscr{P}(X) \longrightarrow \mathbb{Z}_2^n$ as $\varphi : S \mapsto b$, where b has 1's in positions $i \in \text{index}(S)$ and has size n. For example, if $S = \{x_1, x_3, x_4\}$, then $\varphi(S) = b = (1, 0, 1, 1)$, for $n = 4$ (we count the positions from left to right). We see that $\varphi(S)$ has 1 in position i if and only if $x_i \in S$. This can be used to check injectivity: suppose $S, S' \in \mathscr{P}(X)$, and $\varphi(S) = \varphi(S') = b$. On the one hand, b has 1 in position i if and only if $x_i \in S$. On the other hand, b has 1 in position i if and only if $x_i \in S'$. Namely,

$$x_i \in S \iff b \text{ has 1 in position } i \iff x_i \in S'$$

$$x_i \in S \iff x_i \in S'$$
$$\therefore S = S',$$

showing that φ is injective. Because $|\text{domain}(\varphi)| = |\text{codomain}(\varphi)|$, injectivity implies surjectivity, and hence, φ is surjective. To show that φ is a homomorphism, notice that $\varphi(S) + \varphi(S')$ has 1 in position i if and only if $\varphi(S)$ has 1 in position i or $\varphi(S')$ has 1 in position i, but not both having 1 in position i (this is because in the mod2 universe, $1 + 1 = 0$). It follows that

$$\varphi(S) + \varphi(S') \text{ has 1 in position } i \iff (x_i \in S \vee x_i \in S') \wedge \neg(x_i \in S \wedge x_i \in S')$$

$$\begin{aligned}
&\iff (x_i \in S \cup S') \wedge \neg(x_i \in S \cap S') \\
&\iff (x_i \in S \cup S') \wedge (x_i \in (S \cap S')^c) \\
&\iff x_i \in (S \cup S') \cap (S \cap S')^c \\
&\iff x_i \in (S \cup S') - (S \cap S') \\
&\iff x_i \in S \triangle S' \\
&\iff \varphi(S \triangle S') \text{ has 1 in position } i.
\end{aligned}$$

Say $b, b' \in \mathbb{Z}_2^n$. It is easy to see that if b has 1 in position i if and only if b' has 1 in position i, then $b = b'$. Therefore,

$$\varphi(S \triangle S') = \varphi(S) + \varphi(S'),$$

concluding our proof for the homomorphism (and hence, isomorphism) of φ. $\square$

It follows that $R_n = \mathbb{Z}_2^n \cong \mathscr{P}(P_n)$ and $T_n = \mathbb{Z}_2^{2^n} \cong \mathscr{P}(\mathscr{P}(P_n))$. Notice that the proof requires us to label the elements of the set we are taking the power set from. The set $P_n = \{p_1, p_2, ..., p_n\}$ is already "in order" (i.e., its elements are already labeled), so we don't have to worry about it. But to label the elements of the set $\mathscr{P}(P_n)$, we use the fact that our set of rows comes with a predefined order. That is, because $R_n = \mathbb{Z}_2^n \cong \mathscr{P}(P_n)$, we can make the isomorphism preserve such order: if $b_i \in \mathbb{Z}_2^n$ is the ith element in the group, then $\varphi^{-1}(b_i)$ would be the ith element in $\mathscr{P}(P_n)$ and vice-versa (if $S_i \in \mathscr{P}(P_n)$ is the ith element in $\mathscr{P}(P_n)$, then $\varphi(S_i)$ is the ith element in $\mathbb{Z}_2^n$). Lastly, recall that if $S \in \mathscr{P}(X)$, then by the rule of our isomorphism, $\varphi(S)$ has 1 in position i if and only if $x_i \in S$. So if $b \in \mathbb{Z}_2^n$, we can define set $\text{pos}(b)$ to be the set containing the positions of 1's in b (counting from left to right). For example, if $b = (1,0,0,1,0,1,1,0) \in \mathbb{Z}_2^3$, then $\text{pos}(b) = \{1,4,6,7\}$. Then the inverse isomorphism can be state as follows: $\phi : \mathbb{Z}_2^n \to \mathscr{P}(X)$, so that if $b \in \mathbb{Z}_2^n$, then

$$\phi(b) = \varphi^{-1}(b) = \{x_i \in X : i \in \text{pos}(b)\}.$$

Remark. It is not very hard to prove that this is in fact the inverse isomorphism when we realized that $\text{pos}(b)$ is precisely $\text{index}(S)$.

Consider, again, the truth table with some unknown logical formula $f(p_1, ..., p_n)$:

p_1	p_2	...	p_n	$f(p_1, p_2, ..., p_n)$
T	T	...	T	F
T	T	...	F	T
T	T	...	T	F
...	...	...	...	...
F	F	...	T	T
F	F	...	F	T

What propositional formula is responsible for such output? Say $b \in \mathbb{Z}_2^{2^n}$ is such output. Say $\phi' : \mathbb{Z}_2^{2^n} \to \mathscr{P}(\mathscr{P}(P_n))$ maps b to a set S by the following rule:

$$\phi'(b) = S = \{x_i \in \mathscr{P}(P_n) : i \in \text{pos}(b)\},$$

(this is our inverse isomorphism). Because $\mathscr{P}(P_n) \cong \mathbb{Z}_2^n$, we can see x_i (the ith element in $\mathscr{P}(P_n)$) as the image of the isomorphism $\phi : \mathbb{Z}_2^n \to \mathscr{P}(P_n)$ applied to r_i (the ith element in $\mathbb{Z}_2^n$). Namely, $\phi(r_i) = x_i$, and the rule is that x_i contains p_j if and only if r_i has 1 in position j. In other words, $x_i = \phi(r_i) = \{p_j : j \in \text{pos}(r_i)\}$. It follows that

$$\begin{aligned}\phi'(b) &= \{x_i \in \mathscr{P}(P_n) : i \in \text{pos}(b)\}\\ &= \{\phi(r_i) : i \in \text{pos}(b)\}\\ &= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\}.\end{aligned}$$

Example 0.1. Suppose we have the following table:

p_1	p_2	p_3	?
T	T	T	T
T	T	F	F
T	F	T	F
T	F	F	T
F	T	T	T
F	T	F	F
F	F	T	T
F	F	F	F

Then $b = (1, 0, 0, 1, 1, 0, 1, 0)$, and $\text{pos}(b) = \{1, 4, 5, 7\}$. Therefore,

$$\begin{aligned}
\phi'(b) &= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \{1, 4, 5, 7\}\} \\
&= \{\{p_j : j \in \text{pos}(r_1)\}, \{p_j : j \in \text{pos}(r_4)\}, \{p_j : j \in \text{pos}(r_5)\}, \\
&\qquad\qquad\qquad\qquad\qquad\qquad \{p_j : j \in \text{pos}(r_7)\}\} \\
&= \{\{p_1, p_2, p_3\}, \{p_1\}, \{p_2, p_3\}, \{p_3\}\}.
\end{aligned}$$

Take a moment to think about the meaning of such answer. Here we have a set of sets containing the propositional variables p_1, p_2, p_3. And this was uniquely associated (due to our isomorphism) to a truth table output. What is the meaning of this? It means that this set can be understood as the set theoretic version of the well formed formula (in terms of p_1, p_2, p_3 and the usual logical operators $\neg, \vee, \wedge, ...$) that has such output. It also means that one could even "define" the logical formula using set notation itself: the process of coming up with the syntax of a logical formula is basically the same as organizing the symbols inside sets. There is, however, one thing left to resolve: we know that the set above is uniquely associated with a logical formula. But which formula exactly?

Part 2. How to logically read mathematics?

The actual wff responsible for the table above is

$$((p_1 \land \neg p_2) \lor p_3) \land (\neg p_1 \lor p_2 \lor \neg p_3).$$

It is not obvious at all how we could go from the set version to this propositional logic version of the formula. But if we write our answer in a more methodical way (using only the *minterms*) we get a longer, but better looking formula for our purposes:

$$(p_1 \land p_2 \land p_3) \lor (p_1 \land \neg p_2 \land \neg p_3) \lor (\neg p_1 \land p_2 \land p_3) \lor (\neg p_1 \land \neg p_2 \land p_3).$$

Problem 1. *Can one think of a way of translating set*

$$\{\{p_1, p_2, p_3\}, \{p_1\}, \{p_2, p_3\}, \{p_3\}\}$$

to formula

$$(p_1 \land p_2 \land p_3) \lor (p_1 \land \neg p_2 \land \neg p_3) \lor (\neg p_1 \land p_2 \land p_3) \lor (\neg p_1 \land \neg p_2 \land p_3)?$$

Notice that we have four chunks of $(p_1 \land p_2 \land p_3)$ all connected through logical disjunction ($\lor$), and some of these chunks contain negated variables (these chunks are defined to be the *minterms* in boolean algebra). The rule of such translation is rather simple: the i^{th} element of set S contains the non-negated variables for the i^{th} chunk $(p_1 \land p_2 \land p_3)$. Here is why: consider the solution $\phi'(b) = \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\}$. By looking at r_i, we are taking the ith element from $\mathbb{Z}_2^n$, which represents the ith row of our truth table. We are only considering the cases when $i \in \text{pos}(b)$; that is, when the ith row outputs a $True$. In order for the ith row to output a $True$, the ith chunk $(p_1 \land p_2 \land ... \land p_n)$ must have negated variables for $False$ variables. In other words, it must non-negate the $True$ variables. This is precisely what we say by $\{p_j : j \in \text{pos}(r_i)\}$: "include only the variables that are true in the ith row". Since each chunk outputs $True$ on a specific row, by combining all chunks with logical disjunction we will have $True$ on those specific rows, which was our initial task. This perspective allows us to write any logical formula purely in set notation.

Example 0.2. Say we are working in two dimensions, then the formula $(p_1 \wedge p_2) \vee (\neg p_1 \wedge \neg p_2)$ would be associated to set $\{\{p_1, p_2\}, \emptyset\}$. To see more of this in action, let us write some common logical formulas (in two dimensions) in terms of our set notation (we use $\cong$ to associate a formula to its set).

p_1	p_2	$p_1 \cong \{\{p_1, p_2\}, \{p_1\}\}$	$p_2 \cong \{\{p_1, p_2\}, \{p_2\}\}$	$\mathbf{T} \cong \mathscr{P}(P_2)$
T	T	T	T	T
T	F	T	F	T
F	T	F	T	T
F	F	F	F	T

p_1	p_2	$\neg p_1 \cong \{\{p_2\}, \emptyset\}$	$\neg p_2 \cong \{\{p_1\}, \emptyset\}$	$p_1 \wedge p_2 \cong \{\{p_1, p_2\}\}$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	F

p_1	p_2	$p_1 \vee p_2 \cong \{\{p_1, p_2\}, \{p_1\}, \{p_2\}\}$	$p_1 \oplus p_2 \cong \{\{p_1\}, \{p_2\}\}$
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

p_1	p_2	$p_1 \Leftrightarrow p_2 \cong \{\{p_1, p_2\}, \emptyset\}$	$p_1 \Rightarrow p_2 \cong \{\{p_1, p_2\}, \{p_2\}, \emptyset\}$
T	T	T	T
T	F	F	F
F	T	F	T
F	F	T	T

Here is something worth noting: if two formulas are combined through some logical operator, then their respective sets are also combined through the set theoretic version of such operator! For example, consider joining the formulas $(p_1 \vee p_2)$ and $(\neg p_2)$ through logical conjunction (these formulas are associated with $\{\{p_1, p_2\}, \{p_1\}, \{p_2\}\}$ and $\{\{p_1\}, \emptyset\}$ respectively). We get

$$(p_1 \vee p_2) \wedge (\neg p_2) \equiv \neg(p_1 \Rightarrow p_2) \cong \{\{p_1\}\},$$

which matches precisely our intuition on the notion of *intersection*:

$$\{\{p_1, p_2\}, \{p_1\}, \{p_2\}\} \cap \{\{p_1\}, \emptyset\} = \{\{p_1\}\}$$

This also works when taking the negation of a formula, and the *complement* of the set, and when taking the disjunction of two formulas and the *union* of two sets.

Part 3. Formalization

We will use ϕ' to specifically denote our isomorphism from $\mathbb{Z}_2^{2^n}$ to $\mathscr{P}(X)$, where $|X| = 2^n$. Recall:

$$\phi' : b \mapsto \{x_i \in X : i \in \text{pos}(b)\}.$$

Definition 0.1. Let L_n be a set containing logical formulas that use n propositional variables. Define function $f : L_n \to \mathbb{Z}_2^{2^n}$ that returns the truth table output for some wff in L_n. Let ψ be a logical formula in L_n (we are now considering the formula itself to be a variable; hence, the symbol ψ). Let S be an element of $\mathscr{P}(X)$, where X is any set with cardinality 2^n. We say ψ is **associated** with set S (or similarly, S is associated with ψ) if

$$\phi'(f(\psi)) = S \text{ or } f(\psi) = \varphi(S),$$

where ϕ' is the isomorphism between $\mathbb{Z}_2^{2^n}$ and $\mathscr{P}(X)$ and $\varphi = \phi'^{-1}$. We write $\psi \cong S$.

Remark 1. If we let $X = \mathscr{P}(P_n)$, we get the association seen in Part 1, where we realized that the process of writing a logical formula is "isomorphically" the same as organizing our variables inside sets. Now we consider any set X (that has cardinality 2^n), so that we can write the following theorem.

Theorem 1. *Any logical formula can be associated to some (finite) set and any (finite) set can be associated to some logical formula.*

Proof. Let ψ be any logical formula (say $\psi \in L_n$). We then apply the isomorphism $\phi' : \mathbb{Z}_2^{2^n} \longrightarrow \mathscr{P}(\mathscr{P}(P_n))$ to $f(\psi)$.

$$\phi'(f(\psi)) = \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(f(\psi))\},$$

where p_j denotes the jth propositional variable used in ψ. So it is trivial to see that $\psi \cong \phi'(f(\psi))$. For sets, we let $X_1, ..., X_m$ ($m \in \mathbb{N}$) be a collection of finite sets and define

$$U = \bigcup_{i=1}^{m+1} X_i,$$

where X_{m+1} is any set that allows U to have cardinality 2^n for some integer n (in fact, this will be the dimension of our propositional variables). Choose an order for this new constructed set: $U = \{u_1, u_2, u_3, ..., u_{2^n}\}$, then we can apply our group isomorphism φ with domain $\mathscr{P}(U)$ so that $\varphi(X_i) \in \mathbb{Z}_2^{2^n}$. Namely, $\varphi : \mathscr{P}(U) \longrightarrow \mathbb{Z}_2^{2^n}$ as $\varphi : X_i \mapsto b$, where b has 1's in positions $j \in \text{index}(X_i)$ (recall the definition of the index of a set: $\text{index}(S) = \{\text{index}(s_j) \ : \ s_j \in S\} = \{j \ : \ s_j \in S\}$) and has size 2^n. It follows that if $\varphi(X_i) = b_i \in \mathbb{Z}_2^{2^n}$, then there exists some formula $\psi_i \in L_n$ such that $f(\psi_i) = b_i$ (in fact, that are lots of formulas, but we only need to choose one). Hence, X_i is associated with ψ_i :

$$\varphi(X_i) = f(\psi_i).$$

□

Proposition 2. *If ψ and σ are logical formulas associated with sets X and Y respectively, then the following are true:*

- *$\neg\psi$ is associated with X^c*
- *$\psi \vee \sigma$ is associated with $X \cup Y$.*
- *$\psi \wedge \sigma$ is associated with $X \cap Y$.*

Proof. Let $b \in \mathbb{Z}_2^{2^n}$, for some $n \in \mathbb{N}$ be the truth table output of ψ (i.e., $f(\psi) = b$). Then, since X is associated with ψ, $X = \phi'(b) = \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\}$. Similarly, let $b' = f(\neg\psi)$. Then, by definition, the set associated with this formula is

$$\begin{aligned}
\phi'(b') &= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b')\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \notin \text{pos}(b)\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\}^c = X^c.
\end{aligned}$$

To see that $\psi \vee \sigma$ is associated with $X \cup Y$, we say, again, that b is the output of ψ and d the output of σ. Also, suppose the wff $\psi \vee \sigma$ has output s.

$$\begin{aligned}
\phi'(s) &= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(s)\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b) \vee i \in \text{pos}(d)\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b) \cup \text{pos}(d)\} \\
&= \{\{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(b)\} \cup \{p_j : j \in \text{pos}(r_i)\} : i \in \text{pos}(d)\} \\
&= X \cup Y
\end{aligned}$$

The proof is the same for $X \cap Y$ if we change $\vee$ to $\wedge$ and $\cup$ to $\cap$. □

Proposition 3. *If we have a compound propositional formula ψ that uses variables $\sigma_1, \sigma_1, ..., \sigma_1$ (which can also be other formulas), each associated with sets $X_1, X_2, ..., X_k$ (respectively), then ψ will be associated to the compound set theoretic expression created by exchanging each ϕ_i for X_i, and each $\neg(\cdot)$ for $(\cdot)^c, \wedge$ for $\cap$, and $\vee$ for $\cup$. We may refer to this set theoretic expression as the **set theoretic version** of formula ψ.*

Proof. We will use strong induction on the operation count m for formula ψ_m (notice that in this proof we are labeling the indices of the formula to denote its operation count). For the base case, we have $m = 1$ (just one operation), so it follows from Proposition 2. Now we assume it is true for all the cases $m = 1, m = 2, ..., m = r$, and we want to show it is true for the case $m = r + 1$. So suppose we have ψ_{r+1} (i.e., the formula has operation count of $r + 1$). Since there exists an order by which we do our operations, consider the last operation on ψ_{r+1}; if this operation is unary, then it must be the negation operation, and so our ψ_{r+1} can be written as $\neg\psi_r$ (i.e., the negation of some other formula that has operation count of r). By the inductive hypothesis, ψ_r is associated to set Y by the rule describe in Proposition 3. And by Proposition 2, ψ_{r+1} is associated to Y^c. Now suppose that $\psi_{r+1} = \neg\psi_r$ is composed by some variables σ's that are associated with sets X's. The act of exchanging each σ for its X, each $\neg$ for $\cdot^c$, $\vee$ for $\cup$, and $\wedge$ for $\cap$ (the rule in Proposition 3) gives us Y^c, which is precisely the set that ψ_{r+1} is associated with. If the last operation is binary (assume it is $\vee$), then ψ_{r+1} can be written as $\psi_l \vee \psi_p$, where $l, p \leq r$ (in fact, $l + p = r$), which means we can apply the inductive hypothesis to see that $\psi_l \cong Y_0$ and $\psi_p \cong Y_1$, where Y_0, and Y_1 were created by the rule in Proposition 3. Again, assuming $\psi_{r+1} = \psi_l \vee \psi_p$ is composed by some variables σ's that are associated with sets X's, the act of exchanging each σ for its X, each $\neg$ for $\cdot^c$, $\vee$ for $\cup$, and $\wedge$ for $\cap$ (again, this is the rule in Proposition 3) gives us $Y_0 \cup Y_1$. But by Proposition 2, this is precisely the set associated with ψ_{r+1}. If the operation is $\wedge$, the same reasoning still applies, and so we are done. $\square$

Example 0.3. Suppose $\phi_i \cong X_i, i \in \mathbb{N}$. Then

$$(\phi_1 \vee \neg\phi_4) \wedge \neg(\phi_2 \vee \phi_3) \cong (X_1 \cup X_4^c) \cap (X_2 \cup X_3)^c.$$

Definition 0.2. Suppose $\psi, \sigma \in L_n$. We say ψ and σ are **equivalent** if $f(\psi) = f(\sigma)$. If that is the case, we define $\Phi := \psi \Leftrightarrow \sigma$ and call such formula (Φ) a **law**. We usually write $\psi \equiv \sigma$.

Example 0.4. Here is a law in the world of propositional logic: $p \vee p \equiv p$.

Definition 0.3. Let us extend the definition a law to the world of sets. For that, we say two set theoretic expressions are equivalent if they refer to the same set. We then say that the law is the entire expression (involving the equality symbol). Notice this tells us something about the syntax of our writing (a law shows that we can express the same set in two different ways).

Example 0.5. Here is a law in the world of sets: $A \cup A = A$.

Theorem 2. *Two formulas in propositional logic are equivalent if and only if their set theoretic versions are equivalent.*

Proof. If ψ and σ are logical formulas associated with sets X and Y respectively, then

$$\psi \equiv \sigma \Longleftrightarrow X = Y,$$

because $\psi \equiv \sigma \Leftrightarrow f(\psi) = f(\sigma) \Leftrightarrow \phi'(f(\psi)) = \phi'(f(\sigma)) \Leftrightarrow X = Y$. By Proposition 3, we can get X by exchanging each variable in ψ by its associated set, and the logical operators for set ones; the same with Y. So X is the set theoretic version of ψ and Y is that of σ. That is, we can say the left hand side and the right hand side "take the same form" with respect to their syntax. $\square$

Example 0.6. Consider DeMorgan's Law: $\neg(p_1 \wedge p_2) \equiv \neg p_1 \vee \neg p_2 \quad p_1, p_2 \in P_2$. If we associate p_1 and p_2 to X_1 and X_2 respectively, then we have that

$$\neg(p_1 \wedge p_2) \equiv \neg p_1 \vee \neg p_2 \Longleftrightarrow (X_1 \cap X_2)^c = X_1^c \cup X_2^c.$$

Corollary 1. *We prove some law in propositional logic if and only if we prove the same law in set theory.*

Example 0.7. Say we want to prove DeMorgan's Law for sets. Suppose we know DeMorgan's Law to be true for propositional logic. Then here is what we can do. Let A, B be sets. By Theorem 1 we can associate them to some well formed formulas that contain the same number of propositional variables (say $A \cong \alpha, B \cong \beta$). Then since we know DeMorgan's Law to be true for propositional logic we have that

$$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta,$$

but by Theorem 2 we see that

$$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta \Longleftrightarrow (A \cap B)^c = A^c \cup B^c.$$

$$\therefore (A \cap B)^c = A^c \cup B^c,$$

and we have proved DeMorgan's Law for sets, as simple as that!

In the next page we can see a table with some equivalences in propositional logic (PL) and set theory.

Associations: $p \cong A, q \cong B, r \cong C$		
Equivalence in PL	Equivalence in Set Theory	Name
$p \land \mathbf{T} \equiv p$	$A \cap U = A$	Identity Laws
$p \lor \mathbf{F} \equiv p$	$A \cup \emptyset = A$	
$p \lor \mathbf{T} \equiv \mathbf{T}$	$A \cup U = U$	Domination Laws
$p \land \mathbf{F} \equiv \mathbf{F}$	$A \cap \emptyset = \emptyset$	
$p \lor p \equiv p$	$A \cup A = A$	Idempotent Laws
$p \land p \equiv p$	$A \cap A = A$	
$\neg(\neg p) \equiv p$	$(A^c)^c = A$	Double Negation Law
$p \lor q \equiv q \lor p$	$A \cup B = B \cup A$	Commutative Laws
$p \land q \equiv q \equiv p$	$A \cap B = B \cap A$	
$(p \lor q) \lor r \equiv p \lor (q \lor r)$	$A \cup B \cup C = A \cup B \cup C$	Associative Laws
$(p \land q) \land r \equiv p \land (q \land r)$	$(A \cap B) \cap C = A \cap (B \cap C)$	
$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
$\neg(p \land q) \equiv \neg p \lor \neg q$	$(A \cap B)^c = A^c \cup B^c$	De Morgan's Laws
$\neg(p \lor q) \equiv \neg p \land \neg q$	$(A \cup B)^c = A^c \cap B^c$	
$p \lor (p \land q) \equiv p$	$A \cup (A \cap B) = A$	Absorption Laws
$p \land (p \lor q) \equiv p$	$A \cap (A \cup B) = A$	
$p \lor \neg p \equiv \mathbf{T}$	$A \cup A^c = U$	Negation Laws
$p \land \neg p \equiv \mathbf{F}$	$A \cap A^c = \emptyset$	