From Propositional Logic to Set Theory

Lucas Salim

June 3, 2022

The Question.

Given any truth table in any dimensions, can we find a systematic way of coming up with the propositional sentence that produces the table's output? For instance, consider the following truth table: Just use:

$$https://en.wikipedia.org/wiki/Karnaugh\_map$$

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 sentence is responsible for such output? To start, let us define some useful terms. 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 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 change T to ones and F to zeros, then it is easy to see that $R_n = \mathbb{Z}_2^n$ and $T_n = \mathbb{Z}_2^{2^n}$. For example, the table with output $TFFT \in T_2$ becomes $(1, 0, 0, 1) \in \mathbb{Z}_2^4$. Moreover, the set $\mathscr{P}(X)$ (for any set X), if equipped with the operation of symmetric difference, becomes a group. This operation is defined as follows: if A and B are sets, then the symmetric difference $A \triangle B$ is

$$A \triangle B := A \cup B - A \cap B.$$

Hence, we should now see 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 sentence, but also we would explictly present such algorithm (i.e., the isomorphism between the groups), proving the existence of an answer to our problem. If we have any truth table $TTFTFFFT = (1, 1, 0, 1, 0, 0, 0, 1) \in \mathbb{Z}_2^8$, (this case $n = 3$), then the isomorphism $\phi : \mathbb{Z}_2^8 \longrightarrow \mathscr{P}(\mathscr{P}(P_3))$ will send us to a unique set $S \in \mathscr{P}(\mathscr{P}(P_3))$, which is itself, a set of sets containing our propositional variables p_1, p_2, p_3. This will uniquely correspond to a logical sentence (to understand which sentence exactly is one of the tasks we ought to solve). 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,

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

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

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

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

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

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. □

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., already labeled), so we don't have to worry about it. But how could we possibly label the elements of the set $\mathscr{P}(P_n)$? Easy, we know that our set of rows comes with a predefined order, and because $R_n = \mathbb{Z}_2^n \cong \mathscr{P}(P_n)$, we can make the isomorphism preserve such order. For example (for two dimensions), some people like starting the rows with Trues, while others prefer starting them with Falses:

p_1	p_2
T	T
T	F
F	T
F	F

$$\Rightarrow R_2 = \{(1,1),(1,0),(0,1),(0,0)\} \cong \{\{p_1,p_2\},\{p_1\},\{p_2\},\emptyset\}$$

p_1	p_2
F	F
F	T
T	F
T	T

$$\Rightarrow R_2 = \{(0,0),(0,1),(1,0),(1,1)\} \cong \{\emptyset,\{p_2\},\{p_1\},\{p_1,p_2\}\}$$

In any case, we can always make our isomorphism preserve such order. That is, 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 $S \in \mathscr{P}(P_n)$, then by the rule of our isomorphism, $\varphi(S)$ has 1 in position i if and only if $x_i \in S$. If $b \in \mathbb{Z}_2^n$, we can define set $\mathrm{pos}(b)$ 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 $\mathrm{pos}(b) = \{1,4,6,7\}$. 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

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

Now we have all the necessary tools to answer our question.

The Answer (in set notation).

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

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 sentence is responsible for such output?

Say $b \in \mathbb{Z}_2^{2^n}$ is such output. Then, $\phi : \mathbb{Z}_2^{2^n} \to \mathscr{P}(\mathscr{P}(P_n))$ maps b to a set S by the following rule:

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

Consider $\varphi' : \mathscr{P}(P_n) \to \mathbb{Z}_2^n$ (and similarly, $\phi' : \mathbb{Z}_2^n \to \mathscr{P}(P_n)$). Since x_i is the *ith* element in $\mathscr{P}(P_n)$, we have that $\varphi'(x_i) = r_i \in \mathbb{Z}_2^n$ (the *ith* element in $\mathbb{Z}_2^n$). Moreover, x_i contains p_j if and only if r_i has 1 in position j. Namely, $x_i = \phi'(r_i) = \{p_j : j \in \text{pos}(r_i)\}$. It follows that

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

and we are done.

An example.

Consider 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,

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

From set notation to propositional logic.

The actual logical sentence for such table is

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

Can you think of a way of translating set $\{\{p_1, p_2, p_3\}, \{p_1\}, \{p_2, p_3\}, \{p_3\}\}$ *to sentence* $(p_1 \land p_2 \land p_3) \lor (p_1 \land \neg p_2 \land \neg p_3) \lor (\neg p_1 \land p_2 \land p_3) \lor (\neg p_1 \land \neg p_2 \land p_3)$?

Notice that we have four chunks of $(p_1 \land p_2 \land p_3)$ all connected through logical disjunction, and some of these chunks contain negated variables. The rule of such translation is rather simple: the i^{th} element of 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 (not considering the output column, obviously). 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 negate 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.

From propositional logic to set theory.

Our perspective allows us to write any logical sentence in terms of sets. The only insight we used was one from abstract algebra: the concept of an isomorphism between groups. Here is what we've done: we provided a new notation (in terms of sets) for the definition of logical operators, and showed that such notation is consistent with the usual notation from classical logic. Now, in regards to our initial question; one can easily solve it with techniques from boolean algebra, or simple direct reasoning from logic. But all we had to do was put on our set theoretical lenses and realize that even logical sentences are, in a way, disguised sets (or even better; sets of sets).

p_1	p_2	$p_1 \wedge p_2$
T	T	T
T	F	F
F	T	F
F	F	F

The *AND* operator is translated to $\{\{p_1, p_2\}\}$, because $b = (1, 0, 0, 0)$, and $\mathrm{pos}(b) = \{1\}$, so

$$\begin{aligned}\phi(b) &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \mathrm{pos}(b)\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \{1\}\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_1)\}\} = \{\{p_j : j \in \{1, 2\}\}\}\\ &= \{\{p_1, p_2\}\}.\end{aligned}$$

p_1	p_2	$p_1 \vee p_2$
T	T	T
T	F	T
F	T	T
F	F	F

The *OR* operator is translated to $\{\{p_1, p_2\}, \{p_1\}, \{p_2\}\}$, because $b = (1, 1, 1, 0)$, and $\mathrm{pos}(b) = \{1, 2, 3\}$, so

$$\begin{aligned}\phi(b) &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \mathrm{pos}(b)\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \{1, 2, 3\}\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_1)\}, \{p_j : j \in \mathrm{pos}(r_2)\}, \{p_j : j \in \mathrm{pos}(r_3)\}\}\\ &= \{\{p_j : j \in \{1, 2\}\}, \{p_j : j \in \{1\}\}, \{p_j : j \in \{2\}\}\}\\ &= \{\{p_1, p_2\}, \{p_1\}, \{p_2\}\}.\end{aligned}$$

p_1	p_2	$p_1 \oplus p_2$
T	T	F
T	F	T
F	T	T
F	F	F

The *XOR* operator is translated to $\{\{p_1\}, \{p_2\}\}$, because $b = (0, 1, 1, 0)$, and $\mathrm{pos}(b) = \{2, 3\}$, so

$$\begin{aligned}\phi(b) &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \mathrm{pos}(b)\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \{2, 3\}\}\\ &= \{\{p_j : j \in \mathrm{pos}(r_2)\}, \{p_j : j \in \mathrm{pos}(r_3)\}\}\\ &= \{\{p_j : j \in \{1\}\}, \{p_j : j \in \{2\}\}\}\\ &= \{\{p_1\}, \{p_2\}\}.\end{aligned}$$

Enough of sets.

If we were to investigate our question directly from the perspective of propositional logic, our argument would be basically what is here (link). And this is what the solution would look like (say, for instance in 3 dimensions):

$$\bigvee_{i\in \mathrm{pos}(b)} \left(\bigwedge_{j=1}^{3} m_{ij} p_j \right), \text{ where } (m_{ij}) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & \neg \\ 1 & \neg & 1 \\ 1 & \neg & \neg \\ \neg & 1 & 1 \\ \neg & 1 & \neg \\ \neg & \neg & 1 \\ \neg & \neg & \neg \end{pmatrix}.$$

The matrix (m_{ij}) is precisely the rows of the truth table, but instead of T, we write 1, and instead of F, we write $\neg$ (so that $1p_j = p_j$ and $\neg p_j = \neg p_j$).

Not enough of sets.

Just notice the similarity of the answer above with

$$\{\{p_j : j \in \mathrm{pos}(r_i)\} : i \in \mathrm{pos}(b)\} = \bigcup_{i\in \mathrm{pos}(b)} \{\{p_j : j \in \mathrm{pos}(r_i)\}\}$$

$$= \bigcup_{i\in \mathrm{pos}(b)} \left\{ \bigcup_{j\in \mathrm{pos}(r_i)} \{p_j\} \right\}$$

$$= \bigcup_{i\in \mathrm{pos}(b)} \left\{ \left(\bigcap_{j\in \mathrm{pos}(r_i)} \{p_j\}^c \right)^c \right\}$$

$$= \bigcup_{i\in \mathrm{pos}(b)} \left\{ \left(\bigcap_{j\in \mathrm{pos}(r_i)^c} \{p_j\} \right)^c \right\}$$

The only difference is that by taking the complement we are not including the negated variables inside our sets.