Simplifying compound proposition and Logical equation

Oh Jung Uk

Abstract

If $B(P)$ is the truth value of proposition P then connectives could be translated to arithmetic operation in the congruent expression of 2 as described below.

$$B(\sim p) \equiv 1 + B(p)(\ mod\ 2\ ), B(p \wedge q) \equiv B(p)B(q)(\ mod\ 2\ )$$

$$B(p \vee q) \equiv B(p) + B(q) + B(p)B(q)(\ mod\ 2\ )$$

$$B(p \longrightarrow q) \equiv 1 + B(p) + B(p)B(q)(\ mod\ 2\ )$$

$$B(p \leftrightarrow q) \equiv 1 + B(p) + B(q)(mod\ 2)$$

By using this, logical laws could be proved, compound proposition could be simplified, and logical equation could be solved.

1. Introduction

We know by or using logical laws, and the use of such karnaughmap in order to simplify the compound proposition. We think the method of using local laws has inconvenience that we need to memorize several logical laws and directions of a connectives, and the method of using karnaughmap has inconvenience of processing of multivariate. For eliminating the inconvenience, we study how to simplify the compound proposition by changing logical connectives to the arithmetic operators of congruent expression. We prove again several logical laws by using this method for helpful. We think that this method will be used to “simplifying of logical circuit”.

We know that the method is not exist how to get the truth value easily if we know the truth value of a certain compound poroposition but the truth value of a certain proposition that make up the compound proposition is not known. If x is a certain proposition that the truth value is not known, we define logical equation as a compound proposition including x. And we study how to get the truth value of x. We don’t study in this paper, but we think this method, making use of the matrix, to study value of “n variables 1st order equation” would be also meaning.

2. Simplifying compound proposition

Definition 1. Let us define $B(P)$ as a number of truth value of the compound proposition P. That is,if P is true then $B(P) = 1$, if P is false then $B(P) = 0$.

Theorem 1. Expression of connectives in the congruent expression of 2

For arbitrary simple proposition p, q, connectives could be expressed to arithmetic operators by using the congruent expression of 2 as described below.

$$B(\sim p) \equiv 1 + B(p)(\ mod\ 2\ )$$
$$B(p \wedge q) \equiv B(p)B(q)(\ mod\ 2\ )$$
$$B(p \vee q) \equiv B(p) + B(q) + B(p)B(q)(\ mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 1 + B(p) + B(p)B(q)(\ mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 1 + B(p) + B(q)(mod\ 2)$$
$$\text{But, } B\left(\sim {}^{\exists x}p(x)\right) \equiv 1 + B\left({}^{\forall x}p(x)\right)\ (\ mod\ 2\ ), B\left(\sim {}^{\forall x}p(x)\right) \equiv 1 + B\left({}^{\exists x}p(x)\right)\ (\ mod\ 2\ )$$

Proof 1. Let us define p, q as arbitray simple proposition.

If p is false, q is false, that is, $B(p) = 0, B(q) = 0$ then

$$B(p) \equiv 0\ (\ mod\ 2\ ), \qquad B(\sim p) \equiv 1 \equiv 1 + 0 \equiv 1 + B(p)\ (\ mod\ 2\ )$$
$$B(p \wedge q) \equiv 0 \equiv 0 \times 0 \equiv B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \vee q) \equiv 0 \equiv 0 + 0 + 0 \times 0 \equiv B(p) + B(q) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 1 \equiv 1 + 0 + 0 \times 0 \equiv 1 + B(p) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 1 \equiv 1 + 0 + 0 \equiv 1 + B(p) + B(q)\ (mod\ 2)$$

If p is false, q is true, that is, $B(p) = 0, B(q) = 1$ then

$$B(p \wedge q) \equiv 0 \equiv 0 \times 1 \equiv B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \vee q) \equiv 1 \equiv 0 + 1 + 0 \times 1 \equiv B(p) + B(q) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 1 \equiv 1 + 0 + 0 \times 1 \equiv 1 + B(p) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 0 \equiv 1 + 0 + 1 \equiv 1 + B(p) + B(q)\ (mod\ 2)$$

If p is true, q is false, that is, $B(p) = 1, B(q) = 0$ then

$$B(p) \equiv 1\ (\ mod\ 2\ ), \qquad B(\sim p) \equiv 0 \equiv 1 + 1 \equiv 1 + B(p)\ (\ mod\ 2\ )$$
$$B(p \wedge q) \equiv 0 \equiv 1 \times 0 \equiv B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \vee q) \equiv 1 \equiv 1 + 0 + 1 \times 0 \equiv B(p) + B(q) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 0 \equiv 1 + 1 + 1 \times 0 \equiv 1 + B(p) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 0 \equiv 1 + 1 + 0 \equiv 1 + B(p) + B(q)\ (mod\ 2)$$

If p is true, q is true, that is, $B(p) = 1, B(q) = 1$ then

$$B(p \wedge q) \equiv 1 \equiv 1 \times 1 \equiv B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \vee q) \equiv 1 \equiv 1 + 1 + 1 \times 1 \equiv B(p) + B(q) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 1 \equiv 1 + 1 + 1 \times 1 \equiv 1 + B(p) + B(p)B(q)\ (\ mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 1 \equiv 1 + 1 + 1 \equiv 1 + B(p) + B(q)\ (mod\ 2)$$

Therefore, for connectives $\sim,\wedge,\vee,\longrightarrow,\leftrightarrow$, following formula is satisfied.

$$B(\sim p) \equiv 1 + B(p)\ (mod\ 2\ )$$
$$B(p \wedge q) \equiv B(p)B(q)\ (mod\ 2\ )$$
$$B(p \vee q) \equiv B(p) + B(q) + B(p)B(q)\ (mod\ 2\ )$$
$$B(p \longrightarrow q) \equiv 1 + B(p) + B(p)B(q)\ (mod\ 2\ )$$
$$B(p \leftrightarrow q) \equiv 1 + B(p) + B(q)\ (mod\ 2)$$

But, the logical law of $\sim$ for quantifier $\exists, \forall$ is maintained. [1]

That is,

$$B(\sim^{\exists x} p(x)) \equiv 1 + B\left(^{\forall x} p(x)\right)\ (mod\ 2\ )$$
$$B\left(\sim^{\forall x} p(x)\right) \equiv 1 + B\left(^{\exists x} p(x)\right)\ (mod\ 2\ ) \blacksquare$$

Definition 2. If an arbitray proposition P does not have connectives then we could simply express $B(P)$ to P in the congruent expression of 2 according to theorem 1. But, if P has connectives then we could not omit $B(\ )$.

For example, if P does not have connectives then we could express as $B(P) \equiv P \equiv s(mod\ 2)$,

otherwise $P \wedge Q$ then we could not express as $P \wedge Q \equiv s(mod\ 2)$

but we could express as $B(P \wedge Q) \equiv s(mod\ 2)$,

where, s means a number of truth value of the proposition P.

Theorem 2. Characteristics of $B(P)$ in the congruent expression of 2

For arbitray natural number n, proposition P, simple proposition p, the following equation is satisfied.

$$2nB(P) \equiv 0\ (mod\ 2\ ), 2np \equiv 0\ (mod\ 2\ )$$
$$(2n+1)B(P) \equiv B(P)\ (mod\ 2\ ), (2n+1)p \equiv p\ (mod\ 2\ )$$
$$\{B(P)\}^n \equiv B(P)\ (mod\ 2\ ), p^n \equiv p\ (mod\ 2\ )$$
$$-B(P) \equiv B(P)\ (mod\ 2\ ), -p \equiv p\ (mod\ 2\ )$$

Proof 2. Let us define n as arbitray natural number, P as proposition, p as simple proposition which does not have connectives.

$2nB(P) \equiv 2 \times nB(P) \equiv 0 \times nB(P) \equiv 0(\ mod\ 2\ )$ and

$(2n+1)B(P) \equiv 2nB(P) + B(P) \equiv 0 + B(P) \equiv B(P)(\ mod\ 2\ )$.

When $B(P) \equiv 1(\ mod\ 2\ )$, $\{B(P)\}^n \equiv \{1\}^n \equiv 1 \equiv B(P)\ (mod\ 2\ )$

When $B(P) \equiv 0(\ mod\ 2\ )$, $\{B(P)\}^n \equiv \{0\}^n \equiv 0 \equiv B(P)\ (mod\ 2\ )$

So, $\{B(P)\}^n \equiv B(P)\ (mod\ 2\ )$.

Because, $-B(P) \equiv -1 \times B(P)\ (mod\ 2\ )$ and $-1 \equiv 1-2 \equiv 1-0 \equiv 1\ (mod\ 2\ )$, so,

$-1 \times B(P) \equiv 1 \times B(P) \equiv B(P)\ (mod\ 2\ )$.

The above contents could be simply expressed for p as described below according to definition 2.

$2np \equiv 0\ (mod\ 2\ ), (2n+1)p \equiv p\ (mod\ 2\ ), p^n \equiv p\ (mod\ 2\ ), -p \equiv p\ (mod\ 2\ ) \blacksquare$

Theorem 3. Proving logical laws

We could prove logical laws as like Contrapositive Law, De Morgan's Law by using theorem 1,theorem 2, the congruent expression of 2.

Proof 3. Let us define p, q as arbitrary simple proposition.

According to theorem 1,theorem 2,definition 2,

When Contrapositive Law $p \longrightarrow q \equiv \sim q \longrightarrow \sim p$,

$B(p \longrightarrow q) \equiv 1 + p + pq \ (mod\ 2)$,

$B(\sim q \longrightarrow \sim p) \equiv 1 + B(\sim q) + B(\sim q)B(\sim p) \equiv 1 + (1 + q) + (1 + q)(1 + p)$

$\equiv 1 + (1 + q) + (1 + p + q + qp) \equiv 3 + 2q + p + qp \equiv 1 + p + qp \ \ (mod\ 2)$

Therefore, $B(p \longrightarrow q)$ and $B(\sim q \longrightarrow \sim p)$ is same, so, $p \longrightarrow q \equiv \sim q \longrightarrow \sim p$.

When De Morgan's Law $\sim(p \wedge q) \equiv \sim p \vee \sim q$

$B\big(\sim(p \wedge q)\big) \equiv 1 + B(p \wedge q) \equiv 1 + pq \ (mod\ 2)$

$B(\sim p \vee \sim q) \equiv B(\sim p) + B(\sim q) + B(\sim p)B(\sim q) \equiv (1 + p) + (1 + q) + (1 + p)(1 + q)$

$\equiv 1 + p + 1 + q + 1 + q + p + pq \equiv 3 + 2p + 2q + pq \ \equiv 1 + pq (mod\ 2)$

Therefore, $B\big(\sim(p \wedge q)\big)$ and $B(\sim p \vee \sim q)$ is same,so, $\sim(p \wedge q) \equiv \sim p \vee \sim q$.

When De Morgan's Law $\sim(p \vee q) \equiv \sim p \wedge \sim q$

$B\big(\sim(p \vee q)\big) \equiv 1 + B(p \vee q) \equiv 1 + p + q + pq \ (mod\ 2)$

$B(\sim p \wedge \sim q) \equiv B(\sim p)B(\sim q) \equiv (1 + p)(1 + q) \equiv 1 + q + p + pq \ (mod\ 2)$

Therefore, $B\big(\sim(p \vee q)\big)$ and $B(\sim p \wedge \sim q)$ is same,so, $\sim(p \vee q) \equiv \sim p \wedge \sim q$.

We omit to prove extra logical laws.

■

Theorem 4. Simplifying compound proposition

We could simplify compound proposition by using theorem1,theorem2 and the congruent expression of 2.

Proof 4. Let us define P as compound proposition and p, q as simple proposition.

According to theorem1,theorem2

When $P \equiv \sim p \longrightarrow (\sim p \vee q) \wedge q$,

$$B(\sim p \longrightarrow (\sim p \vee q) \wedge q) \equiv 1 + B(\sim p) + B(\sim p)B\big((\sim p \vee q) \wedge q\big)$$
$$\equiv 1 + (1 + p) + (1 + p)\big(B(\sim p \vee q)B(q)\big)$$
$$\equiv 1 + (1 + p) + (1 + p)\{B(\sim p) + B(q) + B(\sim p)B(q)\}B(q)$$
$$\equiv 1 + (1 + p) + (1 + p)\{(1 + p) + q + (1 + p)q\}q$$
$$\equiv 1 + (1 + p) + (1 + p)\{2 + p + q + pq\}q$$
$$\equiv 1 + (1 + p) + (1 + p)\{2q + pq + q^2 + p^2q\}$$
$$\equiv 1 + (1 + p) + (1 + p)\{pq + q + pq\} \equiv 1 + (1 + p) + (1 + p)\{2pq + q\}$$
$$\equiv 1 + (1 + p) + (1 + p)\{q\} \equiv 1 + (1 + p) + (q + pq) \equiv 2 + p + q + pq$$
$$\equiv p + q + pq \ (mod\ 2)$$

Because $p + q + pq \equiv B(p \vee q)\ (mod\ 2)$

$P \equiv \sim p \longrightarrow (\sim p \vee q) \wedge q \equiv p \vee q$ could be simplified to $p \vee q$.

When $P \equiv (p \vee q) \leftrightarrow ((p \wedge q) \vee \sim q)$, according to theorem1,theorem2

$$B\Big((p \vee q) \leftrightarrow \big((p \wedge q) \vee \sim q\big)\Big) \equiv 1 + B(p \vee q) + B((p \wedge q) \vee \sim q))$$
$$\equiv 1 + B(p \vee q) + \big(B(p \wedge q) + B(\sim q) + B(p \wedge q)B(\sim q)\big)$$
$$\equiv 1 + (p + q + pq) + \big((pq) + (1 + q) + (pq)(1 + q)\big)$$
$$\equiv 1 + (p + q + pq) + \big((pq) + (1 + q) + (pq + pq^2)\big)$$
$$\equiv 1 + (p + q + pq) + \big((pq) + (1 + q) + (pq + pq)\big)$$
$$\equiv 1 + (p + q + pq) + \big((pq) + (1 + q) + (2pq)\big)$$
$$\equiv 1 + (p + q + pq) + (pq) + (1 + q) \equiv 2 + p + 2q + 2pq \equiv p\ (mod\ 2)$$

Therefore, $P \equiv (p \vee q) \leftrightarrow ((p \wedge q) \vee \sim q)$ could be simplified to p.

We omit to prove extra cases ■

3. Logical equation

Definition 3. Let us define "Logical equation" as the equation included proposition x which has unknown truth value and let us define "value of x" as a number of the truth value. And, let us define "n variables logical equation" as that the logical equation has n proposition unknown truth value.
For reference, we do not express "n variables 1st order equation", because all of "n variables m'th order equation" is "n variables 1st order equation" by $\{B(P)\}^n \equiv B(P)\ (mod\ 2)$ according to theorem 2.

Theorem 5. 1 varible logical equation

For proposition p, q, r which is known the truth value, proposition x which is unknown the truth value, and "value of x" of "1 varible logical equation" $px + q \equiv r\ (mod\ 2)$ is as described below
When $p \equiv 0, q + r \equiv 0\ (mod\ 2),\ x \equiv 0,1\ (mod\ 2)$, that is, it does not care of x
When $p \equiv 0, q + r \equiv 1\ (mod\ 2)$, value of x is not exist
When $p \equiv 1\ (mod\ 2),\ x \equiv q + r\ (mod\ 2)$

Proof 5. Let us define p, q, r as the proposition known the truth value,
and let us define x as the proposition unknown the truth value
and let us define $px + q \equiv r\ (mod\ 2)$ as "1 varibles logical equation".
$px \equiv q + r\ (mod\ 2)$ and $px \equiv B(p \wedge x)\ (mod\ 2)$,so,
When $p \equiv 0, q + r \equiv 0\ (mod\ 2)$, logical equation is satisfied that the truth value of x does not care
When $p \equiv 0, q + r \equiv 1\ (mod\ 2)$, logical equation is not satisfied that x has any truth value.
When $p \equiv 1\ (mod\ 2)$, $px + q \equiv r\ (mod\ 2)$ is $x + q \equiv r\ (mod\ 2)$, so, value of x is
$x \equiv q + r\ (mod\ 2)$.

If we explain the above contents with example $B(x \vee p) \equiv q\ (mod\ 2)$ then
$B(x \vee p) \equiv x + p + xp \equiv (1 + p)x + p \equiv q\ (mod\ 2)$, so,
$1 + p \equiv 0, p + q \equiv 0\ (mod\ 2)$, that is, when $p \equiv 1, q \equiv p \equiv 1\ (mod\ 2),\ x \equiv 0,1\ (mod\ 2)$
$1 + p \equiv 0, p + q \equiv 1\ (mod\ 2)$, that is, when $p \equiv 1, q \equiv p + 1 \equiv 0\ (mod\ 2)$, value of x is not exist
$1 + p \equiv 1\ (mod\ 2)$,that is, when $p \equiv 0\ (mod\ 2),\ x \equiv p + q\ \equiv q(mod\ 2)$.
■

Theorem 6. 2 variables logical equation

For p_1, p_2, q_1, q_2 which is known the truth value, x, y which is unknown the truth value, and if we define "2 varibles logical equation" as described below then

$$\left\{ \begin{array}{l} x + p_1 y \equiv q_1 \ (mod\ 2) \\ x + p_2 y \equiv q_2 \ (mod\ 2) \end{array} \right\}$$

"value of x, y" is as described below.

When $p_1 \equiv p_2 \ (mod\ 2), q_1 \equiv q_2 \ (mod\ 2)$, $y \equiv 0,1 \ (mod\ 2)$, that is, it does not care of y

When $p_1 \equiv p_2 \ (mod\ 2), q_1 \equiv q_2 + 1 \ (mod\ 2)$, value of x, y is not exist

When $p_1 \equiv p_2 + 1 \ (mod\ 2)$,

$$y \equiv q_1 + q_2 \ (mod\ 2), x \equiv p_1 q_1 + p_1 q_2 + q_1 \equiv p_2 q_1 + p_2 q_2 + q_2 \ (mod\ 2)$$

Proof 6. Let us define p_1, p_2, q_1, q_2 as the proposition known the truth value, and let us define x, y as the proposition unknown the truth value and let us define "2 varibles logical equation" as described below.

$$\left\{ \begin{array}{l} x + p_1 y \equiv q_1 \ (mod\ 2) \text{ ---------- (6.1)} \\ x + p_2 y \equiv q_2 \ (mod\ 2) \text{ ---------- (6.2)} \end{array} \right\}$$

If we (6.1)-(6.2) then $x + p_1 y - (x + p_2 y) \equiv q_1 - q_2 (mod\ 2)$, and if we arrange then $(p_1 + p_2) y \equiv q_1 + q_2 (mod\ 2)$,so,according to theorem 5,

when $p_1 + p_2 \equiv 0, q_1 + q_2 \equiv 0 \ (mod\ 2)$,that is, when $p_1 \equiv p_2 \ (mod\ 2), q_1 \equiv q_2 \ (mod\ 2)$, $y \equiv 0,1 \ (mod\ 2)$, that is, it does not care of y

when $y \equiv 0 \ (mod\ 2)$ in (6.1) $x \equiv q_1 \ (mod\ 2)$ and $q_1 \equiv q_2 \ (mod\ 2)$,so, $x \equiv q_1 \equiv q_2 \ (mod\ 2)$

when $y \equiv 1 \ (mod\ 2)$ in (6.1) $x \equiv p_1 + q_1 \ (mod\ 2)$ and $p_1 \equiv p_2, q_1 \equiv q_2 \ (mod\ 2)$,so, $x \equiv p_1 + q_1 \equiv p_2 + q_2 (mod\ 2)$

when $p_1 + p_2 \equiv 0, q_1 + q_2 \equiv 1 \ (mod\ 2)$,that is,when $p_1 \equiv p_2 \ (mod\ 2), q_1 \equiv q_2 + 1 \ (mod\ 2)$, value of y is not exist.Therefore, value of x is not exist,too.

when $p_1 + p_2 \equiv 1 \ (mod\ 2)$,that is, when $p_1 \equiv p_2 + 1 \ (mod\ 2)$, $y \equiv q_1 + q_2 \ (mod\ 2)$,so, if we apply this to (6.1) then $x + p_1 q_1 + p_1 q_2 \equiv q_1 \ (mod\ 2)$,so $x \equiv p_1 q_1 + p_1 q_2 + q_1 \ (mod\ 2)$ and because $p_1 \equiv p_2 + 1 \ (mod\ 2)$

$$x \equiv (p_2 + 1) q_1 + (p_2 + 1) q_2 + q_1 \equiv (p_2 q_1 + q_1) + (p_2 q_2 + q_2) + q_1$$
$$\equiv p_2 q_1 + p_2 q_2 + q_2 \ (mod\ 2)$$

■

References

[1] You-Feng Lin, Shwu-Yeng T.Lin, translated by Lee Hung Chun, *Set Theory*, Kyung Moon(2010), pp49

(This is Korean book. I translate, sorry . Original book is

You-Feng Lin, Shwu-Yeng T.Lin, 이흥천 옮김, *집합론*, 경문사(2010))

Oh Jung Uk, South Korea (I am not in any institutions of mathematics)

E-mail address: ojumath@gmail.com