# Logic Synthesis & Verification, Fall 2024

**National Taiwan University**

## Problem Set 1

Due on 2024/10/06 23:59 on NTU Cool.

## 1 [Characteristic Function]

| current state | input | next state | output | value |
|---|---|---|---|---|
| 0 0 | 0 | 0 0 | 0 | 0 |
| 0 0 | 0 | 0 0 | 1 | 0 |
| 0 0 | 0 | 0 1 | 0 | 0 |
| 0 0 | 0 | 0 1 | 1 | 0 |
| 0 0 | 0 | 1 0 | 0 | 0 |
| 0 0 | 0 | 1 0 | 1 | 0 |
| 0 0 | 0 | 1 1 | 0 | 1 |
| 0 0 | 0 | 1 1 | 1 | 0 |
| 0 0 | 1 | 0 0 | 0 | 0 |
| 0 0 | 1 | 0 0 | 1 | 0 |
| 0 0 | 1 | 0 1 | 0 | 0 |
| 0 0 | 1 | 0 1 | 1 | 0 |
| 0 0 | 1 | 1 0 | 0 | 1 |
| 0 0 | 1 | 1 0 | 1 | 0 |
| 0 0 | 1 | 1 1 | 0 | 0 |
| 0 0 | 1 | 1 1 | 1 | 0 |
| 0 1 | 0 | 0 0 | 0 | 0 |
| 0 1 | 0 | 0 0 | 1 | 0 |
| 0 1 | 0 | 0 1 | 0 | 0 |
| 0 1 | 0 | 0 1 | 1 | 1 |
| 0 1 | 0 | 1 0 | 0 | 0 |
| 0 1 | 0 | 1 0 | 1 | 0 |
| 0 1 | 0 | 1 1 | 0 | 0 |
| 0 1 | 0 | 1 1 | 1 | 0 |
| 0 1 | 1 | 0 0 | 0 | 0 |
| 0 1 | 1 | 0 0 | 1 | 1 |
| 0 1 | 1 | 0 1 | 0 | 0 |
| 0 1 | 1 | 0 1 | 1 | 0 |
| 0 1 | 1 | 1 0 | 0 | 0 |
| 0 1 | 1 | 1 0 | 1 | 0 |
| 0 1 | 1 | 1 1 | 0 | 0 |
| 0 1 | 1 | 1 1 | 1 | 0 |

| current state | input | next state | output | value |
|---|---|---|---|---|
| 1 0 | 0 | 0 0 | 0 | 0 |
| 1 0 | 0 | 0 0 | 1 | 0 |
| 1 0 | 0 | 0 1 | 0 | 0 |
| 1 0 | 0 | 0 1 | 1 | 0 |
| 1 0 | 0 | 1 0 | 0 | 0 |
| 1 0 | 0 | 1 0 | 1 | 0 |
| 1 0 | 0 | 1 1 | 0 | 0 |
| 1 0 | 0 | 1 1 | 1 | 1 |
| 1 0 | 1 | 0 0 | 0 | 0 |
| 1 0 | 1 | 0 0 | 1 | 0 |
| 1 0 | 1 | 0 1 | 0 | 1 |
| 1 0 | 1 | 0 1 | 1 | 0 |
| 1 0 | 1 | 1 0 | 0 | 0 |
| 1 0 | 1 | 1 0 | 1 | 0 |
| 1 0 | 1 | 1 1 | 0 | 0 |
| 1 0 | 1 | 1 1 | 1 | 0 |
| 1 1 | 0 | 0 0 | 0 | 0 |
| 1 1 | 0 | 0 0 | 1 | 0 |
| 1 1 | 0 | 0 1 | 0 | 0 |
| 1 1 | 0 | 0 1 | 1 | 0 |
| 1 1 | 0 | 1 0 | 0 | 1 |
| 1 1 | 0 | 1 0 | 1 | 0 |
| 1 1 | 0 | 1 1 | 0 | 0 |
| 1 1 | 0 | 1 1 | 1 | 0 |
| 1 1 | 1 | 0 0 | 0 | 0 |
| 1 1 | 1 | 0 0 | 1 | 0 |
| 1 1 | 1 | 0 1 | 0 | 0 |
| 1 1 | 1 | 0 1 | 1 | 1 |
| 1 1 | 1 | 1 0 | 0 | 0 |
| 1 1 | 1 | 1 0 | 1 | 0 |
| 1 1 | 1 | 1 1 | 0 | 0 |
| 1 1 | 1 | 1 1 | 1 | 0 |

## 2 [Boolean Algebra Definition]

No, $(\{0,1\}, \oplus, \cdot, 0, 1)$ doesn't form a Boolean algebra because it does not satisfy the postulate of distributive. For example, $a = 1, b = 1, c = 0$, $a \oplus (b \cdot c) = 1$, but $(a \oplus b) \cdot (a \oplus c) = 0$.

## 3 [Uniqueness of Complement]

We prove it by contradiction. If $a'$ is not unique, we can find two different elements $a'_1, a'_2 \in \mathbb{B}$, $a'_1 \neq a'_2$ that are both complements of $a$. By the definition of complements, we have

$$\begin{aligned} a + a_0' &= \underline{1} \\ a \ \cdot \ a_0' &= \underline{0} \\ a + a_1' &= \underline{1} \\ a \ \cdot \ a_1' &= \underline{0} \end{aligned}$$

Therefore,

$$\begin{aligned} a_0' &= \underline{1} \cdot a_0' && \text{(Identities)} \\ &= (a + a_1') \cdot a_0' && \text{(Complements)} \\ &= a_0' \cdot (a + a_1') && \text{(Commutative)} \\ &= (a_0' \cdot a) + (a_0' \cdot a_1') && \text{(Distributive)} \\ &= (a \cdot a_0') + (a_0' \cdot a_1') && \text{(Commutative)} \\ &= \underline{0} + (a_0' \cdot a_1') && \text{(Complements)} \\ &= \underline{0} + (a_1' \cdot a_0') && \text{(Commutative)} \\ &= (a \cdot a_1') + (a_1' \cdot a_0') && \text{(Complements)} \\ &= (a_1' \cdot a) + (a_1' \cdot a_0') && \text{(Commutative)} \\ &= a_1' \cdot (a + a_0') && \text{(Distributive)} \\ &= (a + a_0') \cdot a_1' && \text{(Commutative)} \\ &= \underline{1} \cdot a_1' && \text{(Complements)} \\ &= a_1' && \text{(Identities).} \end{aligned}$$

This result violates $a_0' \neq a_1'$. Therefore, the assumption that $a'$ is not unique is incorrect, so $a'$ must be unique.

## 4 [Properties of Boolean Algebra]

(a)

$$\begin{aligned} a + a' \cdot b &= (a + a') \cdot (a + b) && \text{(Distributive)} \\ &= \underline{1} \cdot (a + b) && \text{(Complements)} \\ &= a + b && \text{(Identities)} \end{aligned}$$

(b) To show that $(a + b)' = (a' \cdot b')$.
First, assuming that $(a' \cdot b')$ is complement of $(a + b)$. Second, showing that $(a+b)+(a' \cdot b') = \underline{1}$ and $(a+b) \cdot (a' \cdot b') = \underline{0}$ by the definition of the complement. Before we get into the proof, there are some rules we need to prove first.

– Associative rule $a + (b + c) = (a + b) + c$

$$\begin{aligned} a + (b + c) &= \underline{1} \cdot (a + (b + c)) && \text{(Identities)} \\ &= (c + c') \cdot (a + (b + c)) && \text{(Complements)} \end{aligned}$$

$$
\begin{aligned}
&= (c \cdot (a + (b + c))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + (c \cdot (b + c))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + (c \cdot (c + b))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + ((c \cdot c) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + (((\underline{0}) + (c \cdot c)) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= ((c \cdot a) + (((c \cdot c') + (c \cdot c)) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= ((c \cdot a) + ((c + (c' \cdot c)) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + ((c + (c \cdot c')) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + ((c + \underline{0}) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= ((c \cdot a) + ((\underline{0} + c) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + ((c) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= ((c \cdot a) + ((\underline{1} \cdot c) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= ((c \cdot a) + ((c \cdot \underline{1}) + (c \cdot b))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + (c \cdot (\underline{1} + b))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + (c \cdot ((\underline{1}) \cdot (\underline{1} + b)))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= ((c \cdot a) + (c \cdot ((b + b') \cdot (\underline{1} + b)))) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= ((c \cdot a) + (c \cdot ((b + b') \cdot (b + \underline{1})))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + (c \cdot (b + (b' \cdot \underline{1})))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= ((c \cdot a) + (c \cdot (b + (\underline{1} \cdot b')))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= ((c \cdot a) + (c \cdot (b + b'))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= ((c \cdot a) + (c \cdot \underline{1})) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= (c \cdot (a + \underline{1})) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= (c \cdot ((\underline{1}) \cdot (a + \underline{1}))) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= (c \cdot ((a + a') \cdot (a + \underline{1}))) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= (c \cdot (a + (a' \cdot \underline{1}))) + (c' \cdot (a + (b + c))) && \text{(Distributive)} \\
&= (c \cdot (a + (\underline{1} \cdot a'))) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= (c \cdot (a + a')) + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= (c \cdot \underline{1}) + (c' \cdot (a + (b + c))) && \text{(Complements)} \\
&= (\underline{1} \cdot c) + (c' \cdot (a + (b + c))) && \text{(Commutative)} \\
&= c + (c' \cdot (a + (b + c))) && \text{(Identities)} \\
&= c + ((c' \cdot a) + (c' \cdot (b + c))) && \text{(Distributive)} \\
&= c + ((c' \cdot a) + ((c' \cdot b) + (c' \cdot c))) && \text{(Distributive)} \\
&= c + ((c' \cdot a) + ((c' \cdot b) + (c \cdot c'))) && \text{(Commutative)} \\
&= c + ((c' \cdot a) + ((c' \cdot b) + \underline{0})) && \text{(Complements)} \\
&= c + ((c' \cdot a) + (\underline{0} + (c' \cdot b))) && \text{(Commutative)} \\
&= c + ((c' \cdot a) + (c' \cdot b)) && \text{(Identities)}
\end{aligned}
$$

$$
\begin{aligned}
&= c + (c' \cdot (a+b)) && \text{(Distributive)}\\
&= (c + c') \cdot (c + (a+b)) && \text{(Distributive)}\\
&= \underline{1} \cdot (c + (a+b)) && \text{(Complements)}\\
&= c + (a+b) && \text{(Identities)}\\
&= (a+b) + c && \text{(Commutative)}
\end{aligned}
$$

– Associative rule $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$$
\begin{aligned}
a \cdot (b \cdot c) &= \underline{0} + (a \cdot (b \cdot c)) && \text{(Identities)}\\
&= (c \cdot c') + (a \cdot (b \cdot c)) && \text{(Complements)}\\
&= (c + (a \cdot (b \cdot c))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Distributive)}\\
&= ((c + a) \cdot (c + (b \cdot c))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Distributive)}\\
&= ((c + a) \cdot ((\underline{1} \cdot c) + (b \cdot c))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= ((c + a) \cdot ((c \cdot \underline{1}) + (b \cdot c))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= ((c + a) \cdot ((c \cdot \underline{1}) + (c \cdot b))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= ((c + a) \cdot (c \cdot (\underline{1} + b))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Distributive)}\\
&= ((c + a) \cdot (c \cdot ((\underline{1}) \cdot (\underline{1} + b)))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= ((c + a) \cdot (c \cdot ((b + b') \cdot (\underline{1} + b)))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Complements)}\\
&= ((c + a) \cdot (c \cdot ((b + b') \cdot (b + \underline{1})))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= ((c + a) \cdot (c \cdot (b + (b' \cdot \underline{1})))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Distributive)}\\
&= ((c + a) \cdot (c \cdot (b + (\underline{1} \cdot b')))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= ((c + a) \cdot (c \cdot (b + b'))) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= ((c + a) \cdot (c \cdot \underline{1})) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Complements)}\\
&= ((c + a) \cdot (\underline{1} \cdot c)) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= ((c + a) \cdot (c)) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= ((c + a) \cdot (\underline{0} + c)) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= ((c + a) \cdot (c + \underline{0})) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= (c + (a \cdot \underline{0})) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Distributive)}\\
&= (c + (\underline{0} \cdot a)) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= (c + \underline{0}) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= (\underline{0} + c) \cdot (c' + (a \cdot (b \cdot c))) && \text{(Commutative)}\\
&= c \cdot (c' + (a \cdot (b \cdot c))) && \text{(Identities)}\\
&= c \cdot ((c' + a) \cdot (c' + (b \cdot c))) && \text{(Distributive)}\\
&= c \cdot ((c' + a) \cdot ((c' + b) \cdot (c' + c))) && \text{(Distributive)}\\
&= c \cdot ((c' + a) \cdot ((c' + b) \cdot (c + c'))) && \text{(Commutative)}\\
&= c \cdot ((c' + a) \cdot ((c' + b) \cdot (\underline{1}))) && \text{(Complements)}\\
&= c \cdot ((c' + a) \cdot ((\underline{1}) \cdot (c' + b))) && \text{(Commutative)}\\
&= c \cdot ((c' + a) \cdot (c' + b)) && \text{(Identities)}
\end{aligned}
$$

$$
\begin{aligned}
&= c \cdot (c' + (a \cdot b)) && \text{(Distributive)}\\
&= (c \cdot c') + (c \cdot (a \cdot b)) && \text{(Distributive)}\\
&= (\underline{0}) + (c \cdot (a \cdot b)) && \text{(Complements)}\\
&= c \cdot (a \cdot b) && \text{(Identities)}\\
&= (a \cdot b) \cdot c && \text{(Commutative)}
\end{aligned}
$$

1.

$$
\begin{aligned}
(a+b) + (a' \cdot b') &= ((a+b)+a') \cdot ((a+b)+b') && \text{(Distributive)}\\
&= ((b+a)+a') \cdot ((a+b)+b') && \text{(Commutative)}\\
&= (b+(a+a')) \cdot ((a+b)+b') && \text{(Associative)}\\
&= (b+\underline{1}) \cdot ((a+b)+b') && \text{(Complements)}\\
&= (\underline{1} \cdot (b+\underline{1})) \cdot ((a+b)+b') && \text{(Identities)}\\
&= ((b+b') \cdot (b+\underline{1})) \cdot ((a+b)+b') && \text{(Complements)}\\
&= (b+(b' \cdot \underline{1})) \cdot ((a+b)+b') && \text{(Distributive)}\\
&= (b+(\underline{1} \cdot b')) \cdot ((a+b)+b') && \text{(Commutative)}\\
&= (b+b') \cdot ((a+b)+b') && \text{(Identities)}\\
&= \underline{1} \cdot ((a+b)+b') && \text{(Complements)}\\
&= ((a+b)+b') && \text{(Identities)}\\
&= (a+(b+b')) && \text{(Associative)}\\
&= (a+\underline{1}) && \text{(Complements)}\\
&= \underline{1} \cdot (a+\underline{1}) && \text{(Identities)}\\
&= (a+a') \cdot (a+\underline{1}) && \text{(Complements)}\\
&= a+(a' \cdot \underline{1}) && \text{(Distributive)}\\
&= a+(\underline{1} \cdot a') && \text{(Commutative)}\\
&= a+a' && \text{(Identities)}\\
&= \underline{1} && \text{(Complements)}
\end{aligned}
$$

2.

$$
\begin{aligned}
(a+b) \cdot (a' \cdot b') &= (a' \cdot b') \cdot (a+b) && \text{(Commutative)}\\
&= ((a' \cdot b') \cdot a) + ((a' \cdot b') \cdot b) && \text{(Distributive)}\\
&= ((b' \cdot a') \cdot a) + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= (b' \cdot (a' \cdot a)) + ((a' \cdot b') \cdot b) && \text{(Associative)}\\
&= ((a \cdot a') \cdot b') + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= (\underline{0} \cdot b') + ((a' \cdot b') \cdot b) && \text{(Complements)}\\
&= (\underline{0} + (\underline{0} \cdot b')) + ((a' \cdot b') \cdot b) && \text{(Identities)}\\
&= ((b+b') + (\underline{0} \cdot b')) + ((a' \cdot b') \cdot b) && \text{(Complements)}
\end{aligned}
$$

$$
\begin{aligned}
&= ((b' + b) + (\underline{0} \cdot b')) + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= ((b' + b) + (b' \cdot \underline{0})) + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= (b' \cdot (b + \underline{0})) + ((a' \cdot b') \cdot b) && \text{(Distributive)}\\
&= (b' \cdot (\underline{0} + b)) + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= (b' \cdot b) + ((a' \cdot b') \cdot b) && \text{(Identities)}\\
&= (b \cdot b') + ((a' \cdot b') \cdot b) && \text{(Commutative)}\\
&= \underline{0} + ((a' \cdot b') \cdot b) && \text{(Complements)}\\
&= (a' \cdot b') \cdot b && \text{(Identities)}\\
&= a' \cdot (b' \cdot b) && \text{(Associative)}\\
&= a' \cdot (b \cdot b') && \text{(Commutative)}\\
&= a' \cdot \underline{0} && \text{(Complements)}\\
&= \underline{0} + (a' \cdot \underline{0}) && \text{(Identities)}\\
&= (a + a') + (a' \cdot \underline{0}) && \text{(Complements)}\\
&= (a' + a) + (a' \cdot \underline{0}) && \text{(Commutative)}\\
&= a' \cdot (a + \underline{0}) && \text{(Distributive)}\\
&= a' \cdot (\underline{0} + a) && \text{(Commutative)}\\
&= a' \cdot a && \text{(Identities)}\\
&= a \cdot a' && \text{(Commutative)}\\
&= \underline{0} && \text{(Complements)}
\end{aligned}
$$

$\rightarrow$ Complete the proof.

(c)

$$
\begin{aligned}
&(a + b) \cdot (a' + c) \cdot (b + c)\\
&= (a + b) \cdot (a' + c) \cdot (\underline{0} + (b + c)) && \text{(Identities)}\\
&= (a + b) \cdot (a' + c) \cdot ((a \cdot a') + (b + c)) && \text{(Complements)}\\
&= (a + b) \cdot (a' + c) \cdot ((b + c) + (a \cdot a')) && \text{(Commutative)}\\
&= (a + b) \cdot (a' + c) \cdot (((b + c) + a) \cdot ((b + c) + a')) && \text{(Distributive)}\\
&= (a + b) \cdot ((a' + c) \cdot ((b + c) + a)) \cdot ((b + c) + a') && \text{(Associative)}\\
&= (a + b) \cdot (((b + c) + a) \cdot (a' + c)) \cdot ((b + c) + a') && \text{(Commutative)}\\
&= ((a + b) \cdot ((b + c) + a)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Associative)}\\
&= ((a + b) \cdot ((c + b) + a)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Commutative)}\\
&= ((a + b) \cdot (c + (b + a))) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Associative)}\\
&= ((a + b) \cdot (c + (a + b))) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Commutative)}\\
&= ((a + b) \cdot ((a + b) + c)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Commutative)}\\
&= (((a + b) \cdot (a + b)) + ((a + b) \cdot c)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Distributive)}\\
&= (((\underline{0}) + ((a + b) \cdot (a + b))) + ((a + b) \cdot c)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Identities)}\\
&= ((((a + b) \cdot (a + b)') + ((a + b) \cdot (a + b))) + ((a + b) \cdot c)) \cdot (a' + c) \cdot ((b + c) + a') && \text{(Complements)}
\end{aligned}
$$

$$
\begin{aligned}
&= (((a+b)\cdot((a+b)'+(a+b))) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Distributive)}\\
&= (((a+b)\cdot((a+b)+(a+b)')) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= (((a+b)\cdot(\underline{1})) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Complements)}\\
&= (((\underline{1})\cdot(a+b)) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= ((a+b) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Identities)}\\
&= ((\underline{1}\cdot(a+b)) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Identities)}\\
&= (((a+b)\cdot\underline{1}) + ((a+b)\cdot c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= ((a+b)\cdot(\underline{1}+c))\cdot(a'+c)\cdot((b+c)+a') && \text{(Distributive)}\\
&= ((a+b)\cdot((\underline{1})\cdot(\underline{1}+c)))\cdot(a'+c)\cdot((b+c)+a') && \text{(Identities)}\\
&= ((a+b)\cdot((c+c')\cdot(\underline{1}+c)))\cdot(a'+c)\cdot((b+c)+a') && \text{(Complements)}\\
&= ((a+b)\cdot((c+c')\cdot(c+\underline{1})))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= ((a+b)\cdot(c+(c'\cdot\underline{1})))\cdot(a'+c)\cdot((b+c)+a') && \text{(Distributive)}\\
&= ((a+b)\cdot(c+(\underline{1}\cdot c')))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= ((a+b)\cdot(c+(c')))\cdot(a'+c)\cdot((b+c)+a') && \text{(Identities)}\\
&= ((a+b)\cdot(\underline{1}))\cdot(a'+c)\cdot((b+c)+a') && \text{(Complements)}\\
&= ((\underline{1})\cdot(a+b))\cdot(a'+c)\cdot((b+c)+a') && \text{(Commutative)}\\
&= (a+b)\cdot(a'+c)\cdot((b+c)+a') && \text{(Identities)}\\
&= (a+b)\cdot(a'+c)\cdot(b+(c+a')) && \text{(Associative)}\\
&= (a+b)\cdot(a'+c)\cdot((c+a')+b) && \text{(Commutative)}\\
&= (a+b)\cdot(a'+c)\cdot((a'+c)+b) && \text{(Commutative)}\\
&= (a+b)\cdot(((a'+c)\cdot(a'+c)) + ((a'+c)\cdot b)) && \text{(Distributive)}\\
&= (a+b)\cdot(((\underline{0}) + ((a'+c)\cdot(a'+c))) + ((a'+c)\cdot b)) && \text{(Identities)}\\
&= (a+b)\cdot((((a'+c)\cdot(a'+c)') + ((a'+c)\cdot(a'+c))) + ((a'+c)\cdot b)) && \text{(Complements)}\\
&= (a+b)\cdot(((a'+c)\cdot((a'+c)'+(a'+c))) + ((a'+c)\cdot b)) && \text{(Distributive)}\\
&= (a+b)\cdot(((a'+c)\cdot((a'+c)+(a'+c)')) + ((a'+c)\cdot b)) && \text{(Commutative)}\\
&= (a+b)\cdot(((a'+c)\cdot(\underline{1})) + ((a'+c)\cdot b)) && \text{(Complements)}\\
&= (a+b)\cdot(((\underline{1})\cdot(a'+c)) + ((a'+c)\cdot b)) && \text{(Commutative)}\\
&= (a+b)\cdot(((a'+c) + ((a'+c)\cdot b)) && \text{(Identities)}\\
&= (a+b)\cdot((((\underline{1})\cdot(a'+c)) + ((a'+c)\cdot b)) && \text{(Identities)}\\
&= (a+b)\cdot((((a'+c)\cdot(\underline{1})) + ((a'+c)\cdot b)) && \text{(Commutative)}\\
&= (a+b)\cdot((a'+c)\cdot(\underline{1}+b)) && \text{(Distributive)}\\
&= (a+b)\cdot((a'+c)\cdot((\underline{1})\cdot(\underline{1}+b))) && \text{(Identities)}\\
&= (a+b)\cdot((a'+c)\cdot((b+b')\cdot(\underline{1}+b))) && \text{(Complements)}\\
&= (a+b)\cdot((a'+c)\cdot((b+b')\cdot(b+\underline{1}))) && \text{(Commutative)}\\
&= (a+b)\cdot((a'+c)\cdot(b+(b'\cdot\underline{1}))) && \text{(Distributive)}\\
&= (a+b)\cdot((a'+c)\cdot(b+(\underline{1}\cdot b'))) && \text{(Commutative)}
\end{aligned}
$$

$$
\begin{aligned}
&= (a+b)\cdot((a'+c)\cdot(b+\cdot b')) && \text{(Identities)}\\
&= (a+b)\cdot((a'+c)\cdot(\underline{1})) && \text{(Complements)}\\
&= (a+b)\cdot((\underline{1})\cdot(a'+c)) && \text{(Commutative)}\\
&= (a+b)\cdot(a'+c) && \text{(Identities)}
\end{aligned}
$$

## 5 [Boole's Expansion Theorem]

(a)

$$
\begin{aligned}
u\cdot f(u,v,w) &= u\cdot(u\cdot f(1,v,w)+u'\cdot f(0,v,w)) && \text{(Boole's Expansion)}\\
&= u\cdot(u\cdot f(1,v,w))+u\cdot(u'\cdot f(0,v,w)) && \text{(Distributive)}\\
&= u\cdot(u\cdot f(1,v,w))+(u\cdot u')\cdot f(0,v,w) && \text{(Associative)}\\
&= u\cdot(u\cdot f(1,v,w))+(\underline{0})\cdot f(0,v,w) && \text{(Complements)}\\
&= u\cdot(u\cdot f(1,v,w))+\underline{0} && \text{(Identities)}\\
&= \underline{0}+u\cdot(u\cdot f(1,v,w)) && \text{(Commutative)}\\
&= u\cdot(u\cdot f(1,v,w)) && \text{(Identities)}\\
&= (u\cdot u)\cdot f(1,v,w) && \text{(Associative)}\\
&= ((\underline{0})+(u\cdot u))\cdot f(1,v,w) && \text{(Identities)}\\
&= ((u\cdot u')+(u\cdot u))\cdot f(1,v,w) && \text{(Complements)}\\
&= (u\cdot(u'+u))\cdot f(1,v,w) && \text{(Distributive)}\\
&= (u\cdot(u+u'))\cdot f(1,v,w) && \text{(Commutative)}\\
&= (u\cdot\underline{1})\cdot f(1,v,w) && \text{(Complements)}\\
&= (\underline{1}\cdot u)\cdot f(1,v,w) && \text{(Commutative)}\\
&= u\cdot f(1,v,w) && \text{(Identities)}
\end{aligned}
$$

(b)

$$
\begin{aligned}
u' + f(u,v,w) &= u' + (u \cdot f(1,v,w) + u' \cdot f(0,v,w)) && \text{(Boole's Expansion)}\\
&= u' + (u' \cdot f(0,v,w) + u \cdot f(1,v,w)) && \text{(Commutative)}\\
&= (u' + u' \cdot f(0,v,w)) + u \cdot f(1,v,w) && \text{(Associative)}\\
&= (\underline{1} \cdot u' + u' \cdot f(0,v,w)) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= (u' \cdot \underline{1} + u' \cdot f(0,v,w)) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' \cdot (\underline{1} + f(0,v,w))) + u \cdot f(1,v,w) && \text{(Distributive)}\\
&= (u' \cdot ((\underline{1}) \cdot (\underline{1} + f(0,v,w)))) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= (u' \cdot ((f(0,v,w) + f'(0,v,w)) \cdot (\underline{1} + f(0,v,w)))) + u \cdot f(1,v,w) && \text{(Complements)}\\
&= (u' \cdot ((f(0,v,w) + f'(0,v,w)) \cdot (f(0,v,w) + \underline{1}))) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' \cdot (f(0,v,w) + (f'(0,v,w) \cdot \underline{1}))) + u \cdot f(1,v,w) && \text{(Distributive)}\\
&= (u' \cdot (f(0,v,w) + (\underline{1} \cdot f'(0,v,w)))) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' \cdot (f(0,v,w) + f'(0,v,w))) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= (u' \cdot (\underline{1})) + u \cdot f(1,v,w) && \text{(Complements)}\\
&= (u' \cdot (f(1,v,w) + f'(1,v,w))) + u \cdot f(1,v,w) && \text{(Complements)}\\
&= (u' \cdot (f(1,v,w) + (\underline{1} \cdot f'(1,v,w)))) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= (u' \cdot (f(1,v,w) + (f'(1,v,w) \cdot \underline{1}))) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' \cdot ((f(1,v,w) + f'(1,v,w)) \cdot (f(1,v,w) + \underline{1}))) + u \cdot f(1,v,w) && \text{(Distributive)}\\
&= (u' \cdot ((f(1,v,w) + f'(1,v,w)) \cdot (\underline{1} + f(1,v,w)))) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' \cdot ((\underline{1}) \cdot (\underline{1} + f(1,v,w)))) + u \cdot f(1,v,w) && \text{(Complements)}\\
&= (u' \cdot (\underline{1} + f(1,v,w))) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= (u' \cdot \underline{1} + u' \cdot f(1,v,w)) + u \cdot f(1,v,w) && \text{(Distributive)}\\
&= (\underline{1} \cdot u' + u' \cdot f(1,v,w)) + u \cdot f(1,v,w) && \text{(Commutative)}\\
&= (u' + u' \cdot f(1,v,w)) + u \cdot f(1,v,w) && \text{(Identities)}\\
&= u' + (u' \cdot f(1,v,w) + u \cdot f(1,v,w)) && \text{(Associative)}\\
&= u' + (f(1,v,w) \cdot u' + u \cdot f(1,v,w)) && \text{(Commutative)}\\
&= u' + (f(1,v,w) \cdot u' + f(1,v,w) \cdot u) && \text{(Commutative)}\\
&= u' + (f(1,v,w) \cdot (u' + u)) && \text{(Distributive)}\\
&= u' + (f(1,v,w) \cdot (\underline{1})) && \text{(Complements)}\\
&= u' + ((\underline{1}) \cdot f(1,v,w)) && \text{(Commutative)}\\
&= u' + f(1,v,w) && \text{(Identities)}
\end{aligned}
$$

## 6 Boolean Functions

(a)

$$\begin{aligned}
g(h(x)) &= (h(x)=0)g(0) + (h(x)=1)g(1) \\
&= h(x)'g(0) + h(x)g(1) \\
f(0) &= h(0)'g(0) + h(0)g(1) \\
f(1) &= h(1)'g(0) + h(1)g(1)
\end{aligned}$$

(b)

$$\begin{aligned}
g(g'(x)) &= (g'(x)=0)g(0) + (g'(x)=1)g(1) \\
&= g(x)g(0) + g'(x)g(1) \\
f(0) &= g(0)g(0) + g'(0)g(1) \\
&= g(0) + g'(0)g(1) \\
f(1) &= g(1)g(0) + g'(1)g(1) \\
&= g(1)g(0)
\end{aligned}$$

## 7 Boolean Algebra Application

(a)

$$D_0 = 1,\ D_1 = 1,\ D_2 = 0,\ D_3 = 0,\ D_4 = 1,\ D_5 = 0,\ D_6 = 1,\ D_7 = 1$$

(b)
- The new Boolean algebra is the five tuple $(\mathbb{B}, +, \cdot, \underline{0}, \underline{1})$ where $\mathbb{B}$ is the set of all possible Boolean functions of variable $x$, i.e. $\{0, 1, x, x'\}$. The rest are the same as the in the original Boolean algebra.
- The possible values of variables $y$ and $z$ are $0, 1, x, x'$. By the minterm canonical form theorem, the Boolean function $g(y, z)$ is uniquely determined by $g(0, 0), g(0, 1), g(1, 0)$, and $g(1, 1)$.
- $g(y, z)$ is equivalent to $f(x, y, z)$ if $g(y, z)$ is also viewed as a Boolean function over variable $x, y, z$.

$$D'_0 = 1,\ D'_1 = x',\ D'_2 = x,\ D'_3 = x$$

(c) The new Boolean algebra is the five tuple $(\mathbb{B}, +, \cdot, \underline{0}, \underline{1})$ where $\mathbb{B}$ is the set of all possible Boolean functions of variable $x, y$, i.e. $\{0, 1, x, x'\}$. The rest are the same as the in the original Boolean algebra.

$$D''_0 = x + y',\ D''_1 = xy + x'y'$$