Q4.22 (★★) (Exercise 3.8 of [2].) The set $\{\wedge, \neg\}$ is *functionally complete*: using these two we can "encode" any logical connective. Give formulas that use only these connectives and are equivalent to the following formulas.

$$A \supset B, \quad A \vee B$$

$A \supset B \leftrightarrow \neg(A \wedge \neg B)$ を示す

$$\dfrac{}{A \Rightarrow A}\ (\text{INIT}) \qquad \dfrac{}{B \Rightarrow B}\ (\text{INIT})$$

$$\dfrac{B \Rightarrow B}{\neg B, B \Rightarrow}\ (\neg\text{-L}) \qquad \dfrac{\neg B, B \Rightarrow}{B, \neg B \Rightarrow}\ (\text{EXCHANGE-L})$$

$$\dfrac{A \Rightarrow A \qquad B, \neg B \Rightarrow}{A \supset B, A, \neg B \Rightarrow}\ (\supset\text{-L})$$

$$\dfrac{A \supset B, A, \neg B \Rightarrow}{\neg B, A \supset B, A \Rightarrow}\ (\text{EXCHANGE-L})$$

$$\dfrac{\neg B, A \supset B, A \Rightarrow}{A \wedge \neg B, A \supset B, A \Rightarrow}\ (\wedge\text{-L2})$$

$$\dfrac{A \wedge \neg B, A \supset B, A \Rightarrow}{A, A \wedge \neg B, A \supset B \Rightarrow}\ (\text{EXCHANGE-L})$$

$$\dfrac{A, A \wedge \neg B, A \supset B \Rightarrow}{A \wedge \neg B, A \wedge \neg B, A \supset B \Rightarrow}\ (\wedge\text{-L1})$$

$$\dfrac{A \wedge \neg B, A \wedge \neg B, A \supset B \Rightarrow}{A \wedge \neg B, A \supset B \Rightarrow}\ (\text{CONTRACTION-L})$$

$$\dfrac{A \wedge \neg B, A \supset B \Rightarrow}{A \supset B \Rightarrow \neg(A \wedge \neg B)}\ (\neg\text{-R})$$

$$\dfrac{A \supset B \Rightarrow \neg(A \wedge \neg B)}{\Rightarrow (A \supset B) \supset \neg(A \wedge \neg B)}\ (\supset\text{-R})$$

$$\dfrac{}{A \Rightarrow A}\ (\text{INIT}) \qquad \dfrac{A \Rightarrow A}{A \Rightarrow A, B}\ (\text{WEAKNING-R}) \qquad \dfrac{A \Rightarrow A, B}{\Rightarrow A, A \supset B}\ (\supset\text{-R}) \qquad \dfrac{\Rightarrow A, A \supset B}{\Rightarrow A \supset B, A}\ (\text{EXCHANGE-R})$$

$$\dfrac{}{B \Rightarrow B}\ (\text{INIT}) \qquad \dfrac{B \Rightarrow B}{A, B \Rightarrow B}\ (\text{WEAKNING-L}) \qquad \dfrac{A, B \Rightarrow B}{B, A \Rightarrow B}\ (\text{EXCHANGE-L})$$

$$\dfrac{B, A \Rightarrow B}{A \Rightarrow B, \neg B}\ (\neg\text{-R}) \qquad \dfrac{A \Rightarrow B, \neg B}{A \Rightarrow \neg B, B}\ (\text{EXCHANGE-R}) \qquad \dfrac{A \Rightarrow \neg B, B}{\Rightarrow \neg B, A \supset B}\ (\supset\text{-R}) \qquad \dfrac{\Rightarrow \neg B, A \supset B}{\Rightarrow A \supset B, \neg B}\ (\text{EXCHANGE-R})$$

$$\dfrac{\Rightarrow A \supset B, A \qquad \Rightarrow A \supset B, \neg B}{\Rightarrow A \supset B, A \wedge \neg B}\ (\wedge\text{-R})$$

$$\dfrac{\Rightarrow A \supset B, A \wedge \neg B}{\neg(A \wedge \neg B) \Rightarrow A \supset B}\ (\neg\text{-L})$$

$$\dfrac{\neg(A \wedge \neg B) \Rightarrow A \supset B}{\Rightarrow (\neg(A \wedge \neg B)) \supset (A \supset B)}\ (\supset\text{-R})$$

$$\dfrac{\Rightarrow (A \supset B) \supset \neg(A \wedge \neg B) \qquad \Rightarrow (\neg(A \wedge \neg B)) \supset (A \supset B)}{\Rightarrow ((A \supset B) \supset \neg(A \wedge \neg B)) \wedge (\neg(A \wedge \neg B) \supset (A \supset B))}\ (\wedge\text{-R})$$

上の証明図より、$\vdash (A \supset B) \leftrightarrow \neg(A \wedge \neg B)$ だから、$A \supset B$ は $\neg(A \wedge \neg B)$ と同値.

この表現は $\neg$ と $\wedge$ の 2つの結合子しか用いていない

続いて、$A \vee B \Longleftrightarrow \neg(\neg A \wedge \neg B)$を示す

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(INIT)}
\UnaryInfC{$A \Rightarrow A$}
\RightLabel{($\neg$-L)}
\UnaryInfC{$\neg A, A \Rightarrow$}
\RightLabel{($\wedge$-L1)}
\UnaryInfC{$\neg A \wedge \neg B, A \Rightarrow$}
\RightLabel{(EXCHANGE-L)}
\UnaryInfC{$A, \neg A \wedge \neg B \Rightarrow$}
\AxiomC{}
\RightLabel{(INIT)}
\UnaryInfC{$B \Rightarrow B$}
\RightLabel{($\neg$-L)}
\UnaryInfC{$\neg B, B \Rightarrow$}
\RightLabel{($\wedge$-L2)}
\UnaryInfC{$\neg A \wedge \neg B, B \Rightarrow$}
\RightLabel{(EXCHANGE-L)}
\UnaryInfC{$B, \neg A \wedge \neg B \Rightarrow$}
\RightLabel{($\vee$-L)}
\BinaryInfC{$A \vee B, \neg A \wedge \neg B \Rightarrow$}
\RightLabel{(EXCHANGE-L)}
\UnaryInfC{$\neg A \wedge \neg B, A \vee B \Rightarrow$}
\RightLabel{($\neg$-R)}
\UnaryInfC{$A \vee B \Rightarrow \neg(\neg A \wedge \neg B)$}
\RightLabel{($\supset$-R)}
\UnaryInfC{$\Rightarrow (A \vee B) \supset \neg(\neg A \wedge \neg B)$}
\AxiomC{}
\RightLabel{(INIT)}
\UnaryInfC{$A \Rightarrow A$}
\RightLabel{($\neg$-R)}
\UnaryInfC{$\Rightarrow A, \neg A$}
\RightLabel{(WEAKNING-R)}
\UnaryInfC{$\Rightarrow A, \neg A, B$}
\RightLabel{(EXCHANGE-R)}
\UnaryInfC{$\Rightarrow A, B, \neg A$}
\AxiomC{}
\RightLabel{(INIT)}
\UnaryInfC{$B \Rightarrow B$}
\RightLabel{($\neg$-R)}
\UnaryInfC{$\Rightarrow B, \neg B$}
\RightLabel{(WEAKNING-R)}
\UnaryInfC{$\Rightarrow B, \neg B, A$}
\RightLabel{(EXCHANGE-R)}
\UnaryInfC{$\Rightarrow A, B, \neg B$}
\RightLabel{($\wedge$-R)}
\BinaryInfC{$\Rightarrow A, B, \neg A \wedge \neg B$}
\RightLabel{(EXCHANGE-R)}
\UnaryInfC{$\Rightarrow A, \neg A \wedge \neg B, B$}
\RightLabel{($\vee$-R2)}
\UnaryInfC{$\Rightarrow A, \neg A \wedge \neg B, A \vee B$}
\RightLabel{(EXCHANGE-R)}
\UnaryInfC{$\Rightarrow \neg A \wedge \neg B, A \vee B, A$}
\RightLabel{($\vee$-R1)}
\UnaryInfC{$\Rightarrow \neg A \wedge \neg B, A \vee B, A \vee B$}
\RightLabel{(CONTRACTION-R)}
\UnaryInfC{$\Rightarrow \neg A \wedge \neg B, A \vee B$}
\RightLabel{(EXCHANGE-R)}
\UnaryInfC{$\Rightarrow A \vee B, \neg A \wedge \neg B$}
\RightLabel{($\neg$-L)}
\UnaryInfC{$\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$}
\RightLabel{($\supset$-R)}
\UnaryInfC{$\Rightarrow \neg(\neg A \wedge \neg B) \supset (A \vee B)$}
\RightLabel{($\wedge$-R)}
\BinaryInfC{$\Rightarrow ((A \vee B) \supset \neg(\neg A \wedge \neg B)) \wedge (\neg(\neg A \wedge \neg B) \supset (A \vee B))$}
\end{prooftree}
$$

上の証明図より、$\vdash (A \vee B) \longleftrightarrow \neg(\neg A \wedge \neg B)$ だから $A \vee B$は $\neg(\neg A \wedge \neg B)$と同値.

この表現は $\neg$と$\wedge$の2つの結合子しか用いていない。

What about other subsets of $\{\wedge, \vee, \neg, \supset\}$?

任意の論理結合をencodeできる$\{\wedge, \vee, \neg, \supset\}$の部分集合は以下の7つのみである.

$\{\wedge, \neg\}$, $\{\vee, \neg\}$, $\{\neg, \supset\}$, $\{\wedge, \vee, \neg\}$, $\{\wedge, \neg, \supset\}$, $\{\vee, \neg, \supset\}$, $\{\wedge, \vee, \neg, \supset\}$

これらは$\{\wedge, \neg\}$, $\{\vee, \neg\}$, $\{\neg, \supset\}$のいずれかを部分集合に持つので、これらが任意の論理結合をencodeできるのを示すには、$\{\wedge, \neg\}$, $\{\vee, \neg\}$, $\{\neg, \supset\}$がそれぞれ任意の論理結合をencodeできるのを示せばよい。

$\{\wedge, \neg\}$については上に示した通り。

(i) $\{\vee, \neg\}$に関する証明

$A \wedge B \longleftrightarrow \neg(\neg A \vee \neg B)$を示す.

$$A \Rightarrow A \quad (\mathrm{INIT})$$
$$\neg A, A \Rightarrow \quad (\neg\text{-}L)$$
$$A, \neg A \Rightarrow \quad (\mathrm{Exchange}\text{-}L)$$
$$A\wedge B, \neg A \Rightarrow \quad (\wedge\text{-}L_1)$$
$$\neg A, A\wedge B \Rightarrow \quad (\mathrm{Exchange}\text{-}L)$$

$$B \Rightarrow B \quad (\mathrm{INIT})$$
$$\neg B, B \Rightarrow \quad (\neg\text{-}L)$$
$$B, \neg B \Rightarrow \quad (\mathrm{Exchange}\text{-}L)$$
$$A\wedge B, \neg B \Rightarrow \quad (\wedge\text{-}L_2)$$
$$\neg B, A\wedge B \Rightarrow \quad (\mathrm{Exchange}\text{-}L)$$

$$\neg A \vee \neg B, A\wedge B \Rightarrow \quad (\vee\text{-}L)$$
$$A\wedge B \Rightarrow \neg(\neg A\vee\neg B) \quad (\neg\text{-}R)$$
$$\Rightarrow (A\wedge B) \supset \neg(\neg A\vee\neg B) \quad (\supset\text{-}R)$$

$$A \Rightarrow A \quad (\mathrm{INIT})$$
$$\Rightarrow \neg A, A \quad (\neg\text{-}R)$$
$$\Rightarrow A, \neg A \quad (\mathrm{Exchange}\text{-}R)$$
$$\Rightarrow A, \neg A\vee\neg B \quad (\vee\text{-}R_1)$$
$$\Rightarrow \neg A\vee\neg B, A \quad (\mathrm{Exchange}\text{-}R)$$

$$B \Rightarrow B \quad (\mathrm{INIT})$$
$$\Rightarrow \neg B, B \quad (\neg\text{-}R)$$
$$\Rightarrow B, \neg B \quad (\mathrm{Exchange}\text{-}R)$$
$$\Rightarrow B, \neg A\vee\neg B \quad (\vee\text{-}R_2)$$
$$\Rightarrow \neg A\vee\neg B, B \quad (\mathrm{Exchange}\text{-}R)$$

$$\Rightarrow \neg A \vee \neg B, A\wedge B \quad (\wedge\text{-}R)$$
$$\Rightarrow A\wedge B, \neg A\vee\neg B \quad (\mathrm{Exchange}\text{-}R)$$
$$\neg(\neg A\vee\neg B) \Rightarrow A\wedge B \quad (\neg\text{-}L)$$
$$\Rightarrow (\neg(\neg A\vee\neg B)) \supset A\wedge B \quad (\supset\text{-}R)$$

$$\Rightarrow ((A\wedge B) \supset \neg(\neg A\vee\neg B)) \wedge (\neg(\neg A\vee\neg B) \supset A\wedge B) \quad (\wedge\text{-}R)$$

上の証明図より $\vdash (A\wedge B) \leftrightarrow \neg(\neg A\vee\neg B)$　$\therefore (A\wedge B) \leftrightarrow \neg(\neg A\vee\neg B)$

すると、$(A\supset B) \leftrightarrow \neg(A\wedge\neg B)$ より、$(A\supset B) \leftrightarrow \neg(\neg(\neg A\vee\neg\neg B))$

以上より、$A\wedge B$, $A\supset B$ は $\vee$ と $\neg$ のみを用いた同値な式で表せるので、$\{\vee, \neg\}$ は任意の論理式をencodeできる。

(ii) $\{\neg, \supset\}$ に関する証明

$A\vee B \leftrightarrow \neg A \supset B$ を示す

$$A \Rightarrow A \quad (\mathrm{INIT})$$
$$\Rightarrow A, \neg A \quad (\neg\text{-}R)$$

$$B \Rightarrow B \quad (\mathrm{INIT})$$

$$\neg A \supset B \Rightarrow A, B$$
$$\neg A\supset B \Rightarrow A, A\vee B \quad (\vee\text{-}R_2)$$
$$\neg A\supset B \Rightarrow A\vee B, A \quad (\mathrm{Exchange}\text{-}R)$$
$$\neg A\supset B \Rightarrow A\vee B, A\vee B \quad (\vee\text{-}R_1)$$
$$\neg A\supset B \Rightarrow A\vee B \quad (\mathrm{Contraction}\text{-}R)$$
$$\Rightarrow (\neg A\supset B) \supset (A\vee B) \quad (\supset\text{-}R)$$

$$A \Rightarrow A \quad (\mathrm{INIT})$$
$$A \Rightarrow A, B \quad (\mathrm{Weakening}\text{-}R)$$
$$A \Rightarrow B, A \quad (\mathrm{Exchange}\text{-}R)$$
$$\neg A, A \Rightarrow B \quad (\neg\text{-}L)$$
$$A, \neg A \Rightarrow B \quad (\mathrm{Exchange}\text{-}R)$$

$$B \Rightarrow B \quad (\mathrm{INIT})$$
$$\neg A, B \Rightarrow B \quad (\mathrm{Weakening}\text{-}L)$$
$$B, \neg A \Rightarrow B \quad (\mathrm{Exchange}\text{-}L)$$

$$A\vee B, \neg A \Rightarrow B \quad (\vee\text{-}L)$$
$$\neg A, A\vee B \Rightarrow B \quad (\mathrm{Exchange}\text{-}L)$$
$$A\vee B \Rightarrow \neg A \supset B \quad (\supset\text{-}R)$$
$$\Rightarrow (A\vee B) \supset (\neg A\supset B) \quad (\supset\text{-}R)$$

$$\Rightarrow ((\neg A\supset B) \supset (A\vee B)) \wedge ((A\vee B) \supset (\neg A\supset B)) \quad (\wedge\text{-}R)$$

上の証明図より、$\vdash (\neg A\supset B) \leftrightarrow (A\vee B)$　$\therefore (A\vee B) \leftrightarrow \neg A\supset B$

すると、$A\wedge B \leftrightarrow \neg(\neg A\vee\neg B)$ より、$A\wedge B \leftrightarrow \neg(\neg\neg A\supset\neg B)$

以上より、$A \land B$, $A \lor B$ は $\supset$ と $\neg$ のみを用いた同値な式で表せるので、$\{\neg, \supset\}$ は任意の論理式を encode できる。

以上より、$\{\land, \neg\}$, $\{\lor, \neg\}$, $\{\neg, \supset\}$, $\{\land, \lor, \neg\}$, $\{\land, \neg, \supset\}$, $\{\lor, \neg, \supset\}$, $\{\land, \lor, \neg, \supset\}$ は任意の論理結合を encode できる。

次に、$\{\land, \lor, \neg, \supset\}$ の他の部分集合が任意の論理結合を encode できるわけではないのを示す。

ここで、$\{\land, \lor, \neg, \supset\}$ の他の部分集合は $\{\neg\}$ か $\{\land, \lor, \supset\}$ のいずれかの部分集合であるから、$\{\land, \lor, \supset\}$ と $\{\neg\}$ が任意の論理結合を encode できるわけではないのを示せばよい。

まず、任意の同値な論理式は任意の付値で同じ値をとるのを示す

$\vdash A \leftrightarrow B$ とすると、$\vdash (A \supset B) \land (B \supset A)$

よって任意の付値で $[\![(A \supset B) \land (B \supset A)]\!] = tt$ となる。…①

ここで、$[\![A]\!]$, $[\![B]\!]$ と $[\![(A \supset B) \land (B \supset A)]\!]$ との対応は以下の通り

		$[\![B]\!]$	
		tt	ff
$[\![A]\!]$	tt	tt	ff
	ff	ff	tt

よって①より任意の付値 J で $[\![A]\!] = [\![B]\!]$ である。 つまり、任意の同値な論理式は任意の付値で同じ値をとる。…②

$\{\land, \lor, \supset\}$ と $\{\neg\}$ に対し、それのみを用いた同値な論理式が構成できないような論理式が存在するのを示せばよい。

(i) $\{\land, \lor, \supset\}$ について

任意の $A \in PVar$ に対し $[\![A]\!] = tt$ となる付値 J を考える。

$A, B \in PFml$ に対し、$[\![A]\!] = [\![B]\!] = tt$ のとき、

$[\![A \land B]\!] = [\![A \lor B]\!] = [\![A \supset B]\!] = tt$

よって論理式に含まれる論理結合子の数について帰納的に、$\{\land, \lor, \supset\}$ のみを用いた任意の論理式 A に対し

$[\![A]\!] = tt$ となる。

$B \in PVar$ として、$[\![\neg B]\!] = ff$

よってこの付値の下で $\neg B$ の付値は $\{\land, \lor, \supset\}$ のみを用いた任意の論理式 A の付値と違う値をとる。

よって②より、$\neg B$ は $\{\land, \lor, \supset\}$ のみを用いた任意の論理式 A と同値でない。 よって示された。

(ii) $\{\neg\}$ について

相異なる $A, B \in PVar$ に対し、$\{\neg\}$ のみを用いた論理式 C について、$A \land B \leftrightarrow C$ とする。

論理結合子 $\neg$ は常に1つの論理式にのみ作用するから、C に含まれる命題変数は1つで、これを D とする。

$[\![A]\!] = [\![B]\!] = tt$ とする付値 J について、$[\![A \land B]\!] = tt$ で ②より $[\![C]\!] = tt$ このとき $[\![D]\!] = d$ とする。

A, B は相異なるから A, B の少なくとも一方は D と異なる。対称性より、一般性を保ったまま $B \neq D$ とできる。

$[\![A]\!] = tt$, $[\![B]\!] = ff$, $[\![D]\!] = d$ とする付値 J' をとることができ、この下で

$[\![A \wedge B]\!] = ff$, $[\![C]\!] = tt$ $\therefore [\![A \wedge B]\!] \neq [\![C]\!]$

しかし, $A \wedge B \leftrightarrow C$ と ② より $[\![A \wedge B]\!] = [\![C]\!]$ だから, 矛盾

よって $A \wedge B$ に対し, $\{\neg\}$ のみを用いた同値な論理式は構成できない。 よって示された。

以上より, $\{\wedge, \vee, \neg\}$ と $\{\neg\}$ に対し, それのみ用いた同値な論理式が構成できないような論理式が存在する。

$\therefore$ $\{\wedge, \vee, \neg\}$, $\{\neg\}$ の任意の部分集合に対し, 任意の論理式を encode することはできない。

以上より, 任意の論理結合を encode できる $\{\wedge, \vee, \neg, \neg\}$ の部分集合は以下の7つのみである.

$\{\wedge, \neg\}$, $\{\vee, \neg\}$, $\{\neg, \neg\}$, $\{\wedge, \vee, \neg\}$, $\{\wedge, \neg, \neg\}$, $\{\vee, \neg, \neg\}$, $\{\wedge, \vee, \neg, \neg\}$