Lean 4: Set Theory Game*の解説

木原 貴行
名古屋大学 情報学部・情報学研究科

最終更新日: 2024 年 2 月 13 日

§1. この講義資料の目的

論理学における自然演繹は本来は**動的**なものであるが，文書に書かれた自然演繹の証明図はどうしても**静的**なものとなってしまい，それをもって自然演繹を本当の意味で理解するのは困難である．自然演繹をどうにかして動的に理解する必要があるが，このためには実際に自然演繹を利用したシステムを触ってみるのが良い．そのようなシステムの例として証明支援系があるが，ちょうどよいことに，証明支援系 Lean のブラウザ上のチュートリアルが公開されており，しかもそれが自然演繹を学ぶためにちょうど良い内容であった．Lean のようなインタラクティブなシステムの長所は，自然演繹が「仮定」と「ゴール」を変形していく動的なものであることを実際に手を動かして理解できることであり，さらに学習者にとっては，常に自分の推論が正しいか否かについて即時に確認できるというのが良い点である．

とはいえ，Lean を利用した自然演繹の学習は，自然演繹だけでなく Lean の命令も覚える必要があるという点でかなりハードルが高い．本資料は，実際に Lean の命令と自然演繹がどう対応しているかを丁寧に解説し，Lean を利用した自然演繹の学習のハードルを下げることを試みるためのものである．

注意. 本稿は Lean の学習教材ではないので，Lean については解説を行わない．Lean については，非常に詳細な公式マニュアルがあり，その日本語の翻訳もあるので，そちらを読むことを推奨する．“Lean 4: Set Theory Game” のプレイのためには，Lean の予備知識は一切必要としない．本稿はあくまで，“Lean 4: Set Theory Game” の各解答が自然演繹による推論とどう対応しているかの説明を与えるためのものである．

* `https://adam.math.hhu.de/#/g/djvelleman/stg4`

目次

§ 2. 命題論理

2.1. 基本命令

我々の目的は「式 $H_1, H_2, \ldots, H_n$ を仮定して，式 G を導け」という形式の問題に対して証明を与えることである．この種の主張は，論理学ではしばしば以下のような記法で表される．

$$H_1, H_2, \ldots, H_n \vdash G$$

$H_1, H_2, \ldots, H_n$ のことを前件，G のことを後件と言ったりするが，つまりは**仮定**と**結論**である．仮定は我々が自由に使える手札であり, 結論は我々の目指すゴールである．式 $H_1, H_2, \ldots, H_n \vdash G$ は「手札 $H_1, H_2, \ldots, H_n$ を上手く活用して，ゴール G を目指せ」ということを意味する．何らかの主張の証明は，式変形などを経由して，徐々に構成されていく．実を言えば，この証明の構成という活動を「手札」と「ゴール」の変遷と理解することができる．つまり，何かを証明する途中過程では，我々には常にその時点での「仮定（手札）」と「結論（ゴール）」がある．

実際には，証明中に仮定（手札）をどのように使うなどを指示するために，各仮定 H_i にはラベル $\mathtt{h}_i$ が付けられている．これを $\mathtt{h}_i\colon H_i$ のように記述する．

$$\mathtt{h}_1\colon H_1,\ \mathtt{h}_2\colon H_2, \ldots, \mathtt{h}_n\colon H_n \vdash G$$

自然演繹の文脈では，この状況を縦向きに記述する．

$$\begin{array}{c} \mathtt{h}_i\colon H_i \\ \vdots \\ \mathtt{Goal}\colon G \end{array}$$

ゴールは下部に配置され，仮定は上部に配置しておくことが多い．証明が実際にどのように進むかを各推論規則について見ていこう．

■含意 → の推論規則: ゴールが $A \to B$ の形であるとき，もちろん我々は ($\to$Intro) を用いて「仮定 A を取得」し「ゴールを B へと変更」する．

$$\mathtt{Goal}\colon\ A \to B \qquad \rightsquigarrow \qquad \cfrac{\begin{array}{c}[\mathtt{h}\colon A]^1 \\ \vdots \\ \mathtt{Goal}\colon\ B\end{array}}{\cancel{\mathtt{Goal}}\colon\ A \to B}\ (\to\mathtt{Intro})^1$$

この推論を行う命令が `intro h` である．ここで，`h` は仮定 A の名前であり，別の変数に変えても良い．

次に我々が既に仮定 $A \to B$ を所持している場合について考える．この場合，推論としては「上から下へ」と「下から上へ」との 2 パターンがある．前者については，仮定として $A \to B$ だけではなく A も所持していた場合であり．仮定 $A \to B$ と A を用いて B を導出できることはすぐに分かるはずだ．

$$\cfrac{\mathtt{h}_1\colon A \to B \qquad \mathtt{h}_2\colon A}{\mathtt{h}_3 := \mathtt{h}_1\mathtt{h}_2\colon B}\ (\to\mathtt{Elim})$$

この推論を行う命令が $\mathtt{have}\ \mathtt{h}_3 \mathrel{\mathtt{:=}} \mathtt{h}_1\ \mathtt{h}_2$ である．つまり，手持ちの仮定 $\mathtt{h}_1\colon A \to B$ と仮定 $\mathtt{h}_2\colon A$ に（$\to$Elim）を適用して，新たな仮定 $\mathtt{h}_3\colon B$ を取得せよ，という指示をしている．

最後の推論パターンは，仮定として $A \to B$ があり，現在のゴールが B の場合である．この場合，ゴールを達成するためには，A を示せば十分であると推論できる．つまり，「ゴールが B から A へと変更」される．

$$\begin{array}{c}[\mathtt{h}\colon A \to B]\\ \vdots \\ \mathtt{Goal}\colon\ B\end{array} \quad \rightsquigarrow \quad \dfrac{[\mathtt{h}\colon A \to B] \qquad \mathtt{Goal}\colon\ A}{\cancel{\mathtt{Goal}}\colon B}\ (\to\mathtt{Elim})$$

この推論を行う命令が，$\mathtt{apply}\ \mathtt{h}$ である．手持ちの仮定 $\mathtt{h}\colon A \to B$ を用いて，ゴールを B から A へと変更せよ，という指示だ．どちらかと言えば，こちらの方が由緒正しい（$\to$Elim）の使い方である．

■連言 $\wedge$ の推論規則: 仮定 $A \wedge B$ を所持している場合，ここから A と B の両方を推論できる．

$$\dfrac{\mathtt{h}_1\colon A \wedge B}{\mathtt{h}_1\mathtt{.left}\colon A}\ (\wedge\mathtt{Elim}) \qquad\qquad \dfrac{\mathtt{h}_1\colon A \wedge B}{\mathtt{h}_1\mathtt{.right}\colon B}\ (\wedge\mathtt{Elim})$$

つまり，仮定 $\mathtt{h}_1\colon A \wedge B$ から新たな仮定 $\mathtt{h}_1\mathtt{.left}\colon A$ と $\mathtt{h}_1\mathtt{.right}\colon A$ を取得できる．新たな仮定の取得には，以前と同様に $\mathtt{have}$ を用いる．つまり，上記の推論を行う命令は $\mathtt{have}\ \mathtt{h}_2 \mathrel{\mathtt{:=}} \mathtt{h}_1\mathtt{.left}$ および $\mathtt{have}\ \mathtt{h}_3 \mathrel{\mathtt{:=}} \mathtt{h}_1\mathtt{.right}$ によって記述できる．

次に $A \wedge B$ を結論付けたい場合にも，推論としては「上から下へ」と「下から上へ」の 2 パターンがある．前者については，既に仮定 A と仮定 B を所持しているならば，そこから新たな仮定 $A \wedge B$ を取得することができる．

$$\dfrac{\mathtt{h}_1\colon A \qquad \mathtt{h}_2\colon B}{\mathtt{And.intro}\ \mathtt{h}_1\ \mathtt{h}_2\colon A \wedge B}\ (\wedge\mathtt{Intro})$$

つまり，仮定 $\mathtt{h}_1\colon A$ と $\mathtt{h}_2\colon B$ から新たな仮定 $\mathtt{And.intro}\ \mathtt{h}_1\ \mathtt{h}_2\colon A \wedge B$ を取得できる．新たな仮定の取得には，以前と同様に $\mathtt{have}$ を用いる．

最後のパターンは，現在のゴールが $A \wedge B$ の場合である．ゴール $A \wedge B$ を証明するためには，A と B の両方を証明すればよいので，「A を証明する」および「B を証明する」という 2 つのゴールに分岐する．

$$\mathtt{Goal}\colon\ A \wedge B \quad \rightsquigarrow \quad \dfrac{\mathtt{Goal}_1\colon\ A \qquad \mathtt{Goal}_2\colon\ B}{\cancel{\mathtt{Goal}}\colon\ A \wedge B}\ (\wedge\mathtt{Intro})$$

この推論を行う命令が $\mathtt{apply}\ \mathtt{And.intro}$ である．

■選言 $\vee$ の推論規則: 仮定 A か B のいずれかを所持している場合，ここから $A \vee B$ を推論できる．

$$\dfrac{\mathtt{h}\colon A}{\mathtt{Or.inl}\ \mathtt{h}\colon A \vee B}\ (\vee\mathtt{Intro}) \qquad\qquad \dfrac{\mathtt{h}\colon B}{\mathtt{Or.inr}\ \mathtt{h}\colon A \vee B}\ (\vee\mathtt{Intro})$$

新たな仮定の取得には，以前と同様に `have` を用いる．仮定 $A \lor B$ を所持している場合には，条件分岐を行うことができる．この場合，「ゴール G は変化せず」に「A を仮定してゴール G を導く」「B を仮定してゴール G を導く」という 2 つのパスに分岐する．

$$\begin{array}{c}[\mathtt{h}_1 : A \lor B]\\ \vdots \\ \mathtt{Goal}:\ G\end{array} \quad \rightsquigarrow \quad \dfrac{[\mathtt{h}_1 : A \lor B] \qquad \begin{array}{c}[\mathtt{h}_2 : A]^1\\ \vdots \\ \mathtt{Goal}:\ G\end{array} \qquad \begin{array}{c}[\mathtt{h}_3 : B]^1\\ \vdots \\ \mathtt{Goal}:\ G\end{array}}{\cancel{\mathtt{Goal}}:\ G}\ (\lor\mathtt{Elim})^1$$

この推論を行う命令が，`cases'` $\mathtt{h}_1$ `with` $\mathtt{h}_2$ $\mathtt{h}_3$ である．これは，仮定 $\mathtt{h}_1 : A \lor B$ を使用して，仮定 $\mathtt{h}_2 : A$ と仮定 $\mathtt{h}_3 : B$ の場合の条件分岐を行うことを指示する．

2.2. Subset world

2.2.1 Level 1/6: The exact tactic

$x \in A \vdash x \in A$ を証明せよ．既に手札 $\mathtt{h}: P$ を得ているとき，これがゴール P の証拠だと Lean に伝えなければならない．それを行う命令が `exact h` である．これによって，手札 `h` がゴールをそのまま示していると Lean に伝えることができる．

2.2.2 Level 2/6: A subset hypothesis

$A \subseteq B,\ x \in A \vdash x \in B$ を証明せよ．包含関係の定義を思い出すと，以下のようになっている．

$$A \subseteq B \iff \forall x\,[x \in A \to x \in B]$$

Lean はこの定義の書き換えを自動的に処理してくれるので，実際には，仮定 $\mathtt{h}_1 : A \subseteq B$ がそのまま上式右辺の括弧の内側を表しているものとみなすことができる．

$$\dfrac{\begin{array}{c}\mathtt{h}_1 : A \subseteq B\\ \vdots \\ \mathtt{h}_1 : x \in A \to x \in B\end{array} \qquad \mathtt{h}_2 : x \in A}{\mathtt{h}_1\ \mathtt{h}_2 : x \in B}\ (\to\mathtt{Elim})$$

この推論を行う手続きの例を 3 つ挙げておこう．

- `have` $\mathtt{h}_3$ `:=` $\mathtt{h}_1$ $\mathtt{h}_2$`;` `exact` $\mathtt{h}_3$
  手札 $\mathtt{h}_1$ と $\mathtt{h}_2$ を合わせて $x \in B$ を導けるので，これを $\mathtt{h}_3$ と名付け，解として提示する．
- `apply` $\mathtt{h}_1$`;` `exact` $\mathtt{h}_2$
  手札 $\mathtt{h}_1$ を用いれば，ゴール $x \in B$ を $x \in A$ へと移行できる．この新たなゴールは $\mathtt{h}_2$ そのものだ．
- `exact` $\mathtt{h}_1$ $\mathtt{h}_2$
  上記の証明図を見れば分かるように，$\mathtt{h}_1$ $\mathtt{h}_2$ がゴール $x \in B$ を指し示す．

2.2.3 Level 3/6: The have tactic

$A \subseteq B,\ B \subseteq C,\ x \in A \vdash x \in C$ を証明せよ．包含関係の取り扱いは上記と同様である．

$$\dfrac{\begin{array}{c}\mathtt{h}_2 : B \subseteq C \\ \vdots \\ \mathtt{h}_2 : x \in B \to x \in C\end{array} \qquad \dfrac{\begin{array}{c}\mathtt{h}_1 : A \subseteq B \\ \vdots \\ \mathtt{h}_1 : x \in A \to x \in B\end{array} \qquad \mathtt{h}_3 : x \in A}{\mathtt{h}_1\ \mathtt{h}_3 : x \in B}\ (\to\mathtt{Elim})}{\mathtt{h}_2\ (\mathtt{h}_1\ \mathtt{h}_3) : x \in C}\ (\to\mathtt{Elim})$$

この推論を行う手続きの例を 2 つ挙げておこう．

- `have h4 := h1 h3;  have h5 := h2 h4;  exact h5`
  手札 $\mathtt{h}_1, \mathtt{h}_3$ から新たな手札 $\mathtt{h}_4 : x \in B$ を得る．手札 $\mathtt{h}_2, \mathtt{h}_4$ から手札 $\mathtt{h}_5 : x \in C$ を得る．この手札 $\mathtt{h}_5$ がゴール $x \in C$ を示す．
- `apply h2;  apply h1;  exact h3`
  手札 $\mathtt{h}_2$ を用いて，ゴールを $x \in C$ から $x \in B$ に変える．手札 $\mathtt{h}_1$ を用いて，ゴールを $x \in B$ から $x \in A$ に変える．手札 $\mathtt{h}_3$ がゴールを示す．

2.2.4 Level 4/6: Implication

$A \subseteq B,\ x \in B \to x \in C \vdash x \in A \to x \in C$ を証明せよ．ゴールが含意の形なので，まずはゴールの式を仮定 $x \in A$ と結論 $x \in C$ に分解するのが妥当であろう．この推論を行うものが，`intro` 命令であった．この命令を実行すると，ゴール $x \in A \to x \in C$ が $x \in C$ へと移行し，手札 $x \in A$ を得る．

$$\dfrac{\dfrac{\begin{array}{c}\mathtt{h}_2 : B \subseteq C \\ \vdots \\ \mathtt{h}_2 : x \in B \to x \in C\end{array} \qquad \dfrac{\begin{array}{c}\mathtt{h}_1 : A \subseteq B \\ \vdots \\ \mathtt{h}_1 : x \in A \to x \in B\end{array} \qquad [\mathtt{h}_3 : x \in A]^1}{\mathtt{h}_1\ \mathtt{h}_3 : x \in B}\ (\to\mathtt{Elim})}{\mathtt{h}_2\ (\mathtt{h}_1\ \mathtt{h}_3) : x \in C}\ (\to\mathtt{Elim})}{\mathtt{Goal:}\ x \in A \to x \in C}\ (\to\mathtt{Intro})^1$$

この推論を行う手続きの例を 2 つ挙げておこう．

- `intro h3;  have h4 := h1 h3;  have h5 := h2 h4;  exact h5`
  まず含意式を仮定 $\mathtt{h}_3$ とゴールに分解する．手札 $\mathtt{h}_1, \mathtt{h}_3$ から新たな手札 $\mathtt{h}_4 : x \in B$ を得る．手札 $\mathtt{h}_2, \mathtt{h}_4$ から新たな手札 $\mathtt{h}_5 : x \in C$ を得る．この手札 $\mathtt{h}_5$ がゴールを示す．
- `intro h3;  apply h2;  apply h1;  exact h3`
  まず含意式を仮定 $\mathtt{h}_3$ とゴールに分解する．手札 $\mathtt{h}_2$ を用いて，ゴールを $x \in C$ から $x \in B$ に変える．手札 $\mathtt{h}_1$ を用いて，ゴールを $x \in B$ から $x \in A$ に変える．手札 $\mathtt{h}_3$ がゴールを示す．

2.2.5 Level 5/6: Subset is reflexive

$\vdash A \subseteq A$ を証明せよ．これは，集合の「元を取る」という操作に関する練習問題である．重要なので何度でも書くが，集合の包含関係の定義は以下である．

$$A \subseteq B \iff \forall x\,[x \in A \to x \in B]$$

つまり，形式的に包含関係を証明するためには，「任意に元 x を取る」という議論を行わなければならない．これを行う命令の名称も `intro` である．たとえば，`intro x` という記述によって，元 `x` を取るよう指示できる．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}_1 : x \in A]^1$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\texttt{Goal}:\ x \in A$}
\RightLabel{$(\to\texttt{Intro})^1$}
\UnaryInfC{$\cancel{\texttt{Goal}}:\ x \in A \to x \in A$}
\RightLabel{$(\forall\texttt{Intro})$}
\UnaryInfC{$\cancel{\texttt{Goal}}:\ \forall z\,(z \in A \to z \in A)$}
\doubleLine
\UnaryInfC{$A \subseteq A$}
\end{prooftree}
$$

この推論を表す手続きは，たとえば以下である．

- `intro x;` `intro` $\mathtt{h}_1$`;` `exact` $\mathtt{h}_1$
  任意に x を取り，仮定 $\mathtt{h}_1 : x \in A$ とゴール $x \in A$ に分解する．手札 $\mathtt{h}_1$ が既にゴールを示している．

推論は下から上へとゴールを順に書き換えていく形で行われていることに注意しよう．

2.2.6 Level 6/6: Subset is transitive

$A \subseteq B,\ B \subseteq C \vdash A \subseteq C$ を証明せよ．ここまでの議論の組合せである．

$$
\begin{prooftree}
\AxiomC{$\mathtt{h}_2 : B \subseteq C$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{h}_2 : x \in B \to x \in C$}
\AxiomC{$\mathtt{h}_1 : A \subseteq B$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{h}_1 : x \in A \to x \in B$}
\AxiomC{$[\mathtt{h}_3 : x \in A]^1$}
\BinaryInfC{$\mathtt{h}_1\ \mathtt{h}_3 : x \in B$}
\BinaryInfC{$\texttt{Goal}:\ \mathtt{h}_2\ (\mathtt{h}_1\ \mathtt{h}_3) : x \in C$}
\RightLabel{$(\to\texttt{Intro})^1$}
\UnaryInfC{$\cancel{\texttt{Goal}}:\ x \in A \to x \in C$}
\RightLabel{$(\forall\texttt{Intro})$}
\UnaryInfC{$\cancel{\texttt{Goal}}:\ \forall z\,(z \in A \to z \in C)$}
\doubleLine
\UnaryInfC{$A \subseteq C$}
\end{prooftree}
$$

この推論を表す手続きは，たとえば以下である．

- `intro x;` `intro` $\mathtt{h}_3$`;` `have` $\mathtt{h}_4$ `:=` $\mathtt{h}_1$ $\mathtt{h}_3$`;` `exact` $\mathtt{h}_2$ $\mathtt{h}_4$
  任意に x を取り，仮定 $\mathtt{h}_3 : x \in A$ とゴール $x \in C$ に分解する．手札 $\mathtt{h}_1, \mathtt{h}_3$ から新たな手札 $\mathtt{h}_4 : x \in B$ を得る．手札 $\mathtt{h}_2, \mathtt{h}_4$ を合わせるとゴールを得る．

2.3. Complement world

2.3.1 Level 1/5: Proof by contradiction

$x \in A, x \notin B \vdash A \nsubseteq B$ を証明せよ．背理法命令 `by_contra` を用いるように指示されるはずである．$\neg P$ を示すためには，P を仮定して矛盾 $\bot$ を導けばよい．これによって，ゴールは $\neg P$ から $\bot$ に変化し，新たな手札 P を得る．たとえば，ゴール $A \nsubseteq B$ において，命令 `by_contra` $\mathtt{h_3}$ を実行すると，ゴールが $A \nsubseteq B$ から $\bot$ へと移行し，手札 $\mathtt{h_3}: A \subseteq B$ を得る．

$$\dfrac{\dfrac{\mathtt{h_2}: x \notin B \qquad \dfrac{\begin{matrix}[\mathtt{h_3}: A \subseteq B]^1 \\ \vdots \\ \mathtt{h_3}: x \in A \to x \in B\end{matrix} \qquad \mathtt{h_1}: x \in A}{x \in B}\,(\to\mathtt{Elim})}{\mathtt{Goal}:\ \bot}\,(\to\mathtt{Elim})}{\cancel{\mathtt{Goal}}:\ A \nsubseteq B}\,(\to\mathtt{Intro})^1$$

この推論を表す手続きは，たとえば以下である．

- `by_contra` $\mathtt{h_3}$; `have` $\mathtt{h_4}$:= $\mathtt{h_3}$ $\mathtt{h_1}$; `exact` $\mathtt{h_2}$ $\mathtt{h_4}$
  背理法を用いると宣言し，$\mathtt{h_3}: A \subseteq B$ を仮定し，矛盾をゴールに設定する．手札 $\mathtt{h_3}, \mathtt{h_1}$ から新たな手札 $\mathtt{h_4}: x \in B$ を得る．手札 $\mathtt{h_2}, \mathtt{h_4}$ を合わせるとゴールを得る．

しかし，標準的な論理学においては，否定文 $\neg P$ はそもそも $P \to \bot$ の略記として導入される．したがって，実はこの証明には背理法は不要であり，含意に関する推論をしているとしても差し支えない．たとえば，$A \nsubseteq B$ はそもそも $(A \subseteq B) \to \bot$ の略記でしかないのであるから，これを証明するためには，$A \subseteq B$ を仮定して $\bot$ を導けばよい．つまり，ここで用いているものは，背理法ではなく，$(\to\mathtt{Intro})$ である．実際，以下のプログラムも正常に実行されるはずである．

- `intro` $\mathtt{h_3}$; `have` $\mathtt{h_4}$:= $\mathtt{h_3}$ $\mathtt{h_1}$; `exact` $\mathtt{h_2}$ $\mathtt{h_4}$

2.3.2 Level 2/5: Definition of complement

$\vdash x \in A^{\mathsf{c}} \leftrightarrow x \notin A$ を証明せよ．これは補集合の定義から従う．示したい主張が $X = X$ や $p \leftrightarrow p$ のようなトートロジーであることを Lean に伝える命令があり，それが `rfl` である．

2.3.3 Level 3/5: Complement subsets from subsets

$A \subseteq B \vdash B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ を証明せよ．証明はこれまでの議論の組合せであるが，それを Lean に伝えるためには，定義の書き換えという操作が必要である．定義の書き換えは，`rewrite` または `rw` と

いう命令によって行われる．ここでは，補集合の定義 `comp_def` に対する定義の書き換えを行う．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h_2} : x \in B^{\mathsf{c}}]^1$}
\doubleLine
\RightLabel{\texttt{(rw)}}
\UnaryInfC{$\mathtt{h_2} : x \notin B$}
\AxiomC{$\mathtt{h_1} : A \subseteq B$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{h_1} : x \in A \to x \in B$}
\AxiomC{$[\mathtt{h_3} : x \in A]^2$}
\BinaryInfC{$x \in B$}
\BinaryInfC{$\texttt{Goal:}\ \bot$}
\RightLabel{$\texttt{(by\_contra h3)}^2$}
\UnaryInfC{$x \notin A$}
\doubleLine
\RightLabel{\texttt{(rw)}}
\UnaryInfC{$x \in A^{\mathsf{c}}$}
\RightLabel{$\texttt{(intro h2)}^1$}
\UnaryInfC{$x \in B^{\mathsf{c}} \to x \in A^{\mathsf{c}}$}
\RightLabel{\texttt{(intro x)}}
\UnaryInfC{$\forall z (z \in B^{\mathsf{c}} \to z \in A^{\mathsf{c}})$}
\doubleLine
\UnaryInfC{$B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$}
\end{prooftree}
$$

最終ゴール以外は省略したが，実際にはゴールは最下部から徐々に上へと持ち上がっている．この推論を表す手続きの例を 2 ステップに分解して記述しておく．

01. `intro x;  intro h₂;  rw [comp_def];  by_contra h₃;`
   任意に x を取り，含意式は仮定 $\mathtt{h_2}$ とゴール $x \in A^{\mathsf{c}}$ に分解する．このゴールは定義に従って $x \notin A$ と書き換える．$\mathtt{h_3} : x \in A$ を仮定して，ゴールを矛盾を導くことと設定する．
02. `rw [comp_def] at h₂;  have h₄ := h₁ h₃;  exact h₂ h₄`
   仮定 $\mathtt{h_2} : x \in B^{\mathsf{c}}$ を定義に従って $x \notin B$ と書き換える．次に，手札 $\mathtt{h_1}, \mathtt{h_3}$ を合わせて，手札 $\mathtt{h_4} : x \in B$ を得る．手札 $\mathtt{h_2}, \mathtt{h_4}$ を合わせると，矛盾が導かれるので，これはゴールを示すと指摘する．

ここで，先程と同様に，`by_contra` は `intro` に置き換えてもよい．

2.3.4 Level 4/5: Complement of a complement

$\vdash (A^{\mathsf{c}})^{\mathsf{c}} = A$ を証明せよ．ここが背理法を真に必要とする最初の命題である．集合の等式は，以下によって定義される．

$$
\begin{aligned}
A = B \iff& A \subseteq B \text{ and } B \subseteq A \\
\iff& \forall x\ (x \in A \leftrightarrow x \in B)
\end{aligned}
$$

この証明に用いるものは，背理法命令 `by_contra` である．これは，P を証明するためには「P が偽であると仮定して矛盾を導けばよい」と推論するものである．つまり，ゴールが $\bot$ へと変更され，手札 $\neg P$ を得る．

$$
\begin{prooftree}
\AxiomC{$\neg P$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\bot$}
\RightLabel{\texttt{(by\_contra)}}
\UnaryInfC{P}
\end{prooftree}
\qquad\qquad
\begin{prooftree}
\AxiomC{$\neg P$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\bot$}
\RightLabel{$(\to$\texttt{Intro}$)$}
\UnaryInfC{$(\neg P) \to \bot$}
\doubleLine
\UnaryInfC{$\neg\neg P$}
\RightLabel{$(\neg\neg$\texttt{Elim}$)$}
\UnaryInfC{P}
\end{prooftree}
$$

右図のように，論理学的には，これは (→`Intro`) と二重否定除去 $\neg\neg P \to P$ の組合せである．以上のアイデアの下で，目的の式の証明は以下のように行われる．

$$
\begin{prooftree}
\AxiomC{$[\mathrm{h}_1 : x \in A^{\mathrm{cc}}]^1$}
\RightLabel{\texttt{(rw)}}
\doubleLine
\UnaryInfC{$x \notin A^{\mathrm{c}}$}
\AxiomC{$[\mathrm{h}_2 : x \notin A]^2$}
\RightLabel{\texttt{(rw)}}
\doubleLine
\UnaryInfC{$x \in A^{\mathrm{c}}$}
\BinaryInfC{$\perp$}
\RightLabel{\texttt{(by\_contra h2)}^{2}}
\UnaryInfC{$x \in A$}
\RightLabel{\texttt{(intro h1)}^{1}}
\UnaryInfC{$x \in A^{\mathrm{cc}} \to x \in A$}
\RightLabel{\texttt{(intro x)}}
\UnaryInfC{$\forall z(z \in A^{\mathrm{cc}} \to z \in A)$}
\doubleLine
\UnaryInfC{$A^{\mathrm{cc}} \subseteq A$}
\AxiomC{$[\mathrm{h}_4 : x \in A^{\mathrm{c}}]^4$}
\RightLabel{\texttt{(rw)}}
\doubleLine
\UnaryInfC{$x \notin A$}
\AxiomC{$[\mathrm{h}_3 : x \in A]^3$}
\BinaryInfC{$\perp$}
\RightLabel{\texttt{(intro h4)}^{4}}
\UnaryInfC{$x \in A^{\mathrm{cc}}$}
\RightLabel{\texttt{(intro h3)}^{3}}
\UnaryInfC{$x \in A \to x \in A^{\mathrm{cc}}$}
\RightLabel{\texttt{(intro x)}}
\UnaryInfC{$\forall z(z \in A \to z \in A^{\mathrm{cc}})$}
\doubleLine
\UnaryInfC{$A \subseteq A^{\mathrm{cc}}$}
\RightLabel{\texttt{(sub\_antisymm)}}
\BinaryInfC{$A^{\mathrm{cc}} = A$}
\end{prooftree}
$$

ここで，$x \leqslant y$ かつ $y \leqslant x$ ならば $x = y$ である，という性質は反対称律 (anti-symmetric law) と呼ばれる．包含関係に対する反対称律は，$A \subseteq B$ かつ $B \subseteq A$ ならば $A = B$ であるという主張であり，これは `sub_antisymm` によって与えられる．命令 `sub_antisymm` を適用すると，ゴールが $A = B$ が 2 つのゴール $A \subseteq B$ と $B \subseteq A$ に分岐する．実際には，`apply sub_antisymm` という命令を記述すればよい．推論ステップが長いので，何ステップかに分けて手続きを記述しよう．

01. `apply sub_antisymm;`
    反対称律より，ゴール $A^{\mathrm{cc}} = A$ を 2 つのゴール $A^{\mathrm{cc}} \subseteq A$ と $A \subseteq A^{\mathrm{cc}}$ に分岐させる．
02. `intro x;` `intro` h_1; `by_contra` h_2;
    まずは前者のゴールを達成することを目指し，任意に x を取る．ゴールの含意式を仮定 h_1 とゴール $x \in A$ に分解する．背理法を用いると宣言して，$\mathrm{h}_2 : x \notin A$ を仮定し，矛盾をゴールに設定する．
03. `rw [comp_def] at` h_1; `apply` h_1; `rw [comp_def];` `exact` h_2;
    仮定 $\mathrm{h}_1 : x \in A^{\mathrm{cc}}$ を定義に従って $x \notin A^{\mathrm{c}}$ に書き換える．手札 $\mathrm{h}_1 : x \notin A^{\mathrm{c}}$ を用いて，ゴールを $\perp$ から $x \in A^{\mathrm{c}}$ へと移行する．ゴール $x \in A^{\mathrm{c}}$ を定義に従って $x \notin A$ に書き換える．手札 h_2 がこのゴールを示している．
04. `intro x;` `intro` h_3; `intro` h_4; `rw [comp_def] at` h_4; `exact` h_4 h_3
    第 2 のゴールを達成することを目指し，任意に x を取る．ゴールの含意式を仮定 h_3 とゴール $x \in A^{\mathrm{cc}}$ に分解する．このゴールを仮定 $\mathrm{h}_4 : x \in A^{\mathrm{c}}$ とゴール $\perp$ に分解する．手札 $\mathrm{h}_4 : x \in A^{\mathrm{c}}$ を定義に従って $x \notin A$ に書き換える．手札 $\mathrm{h}_4, \mathrm{h}_3$ は矛盾しているので，ゴール $\perp$ を得る．

もちろん，このコマンド列だけを見ても意味が分かりづらいと思うが，実際には，それぞれのコマンドを入力する毎に，現在の手札とゴールが表示されているはずである．その時点での手札とゴールを確認しながらであれば，このコマンド列の意味するものは明瞭である．

2.3.5 Level 5/5: Complement subsets equivalence

$\vdash A \subseteq B \leftrightarrow B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ を証明せよ．ここでのポイントは，既に証明した主張は用いてよいという点である．既に第 2.3.3 節で，$A \subseteq B \vdash B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ を証明しているので，これに `comp_sub_of_sub` という名前を付けておく．また，第 2.3.4 節では，$A^{\mathsf{cc}} = A$ を証明しているので，この等式には `comp_comp` という名前を付けておく．このように，既に証明した命題を利用すれば，目的の式は容易に証明できる．

$$\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 \colon A \subseteq B]}{B^{\mathsf{c}} \subseteq A^{\mathsf{c}}}\,\texttt{(comp\_sub\_of\_sub)}}{A \subseteq B \to B^{\mathsf{c}} \subseteq A^{\mathsf{c}}}\,\texttt{(intro h1)} \qquad \dfrac{\dfrac{\dfrac{[\mathtt{h}_2 \colon B^{\mathsf{c}} \subseteq A^{\mathsf{c}}]}{A^{\mathsf{cc}} \subseteq B^{\mathsf{cc}}}\,\texttt{(comp\_sub\_of\_sub)}}{A \subseteq B}\,\texttt{(rw [comp\_comp])}}{B^{\mathsf{c}} \subseteq A^{\mathsf{c}} \to A \subseteq B}\,\texttt{(intro h2)}}{A \subseteq B \leftrightarrow B^{\mathsf{c}} \subseteq A^{\mathsf{c}}}\,\texttt{(Iff.intro)}$$

$P \leftrightarrow Q$ を証明するためには $P \to Q$ と $Q \to P$ を証明すればよい．この推論を行うのが `Iff.intro` であり，これはゴール $P \leftrightarrow Q$ を 2 つのゴール $P \to Q$ と $Q \to P$ に分岐させる．実際には $P \leftrightarrow Q$ とは $(P \to Q) \wedge (Q \to P)$ の略記であるから，`And.intro` を用いても全く同じ動作が行われる．推論ステップが長いので，何ステップかに分けて手続きを記述しよう．

01. `apply Iff.intro;`
    ゴールの両向き矢印 $\leftrightarrow$ を 2 つのゴール $\to$ と $\leftarrow$ に分岐させる．
02. `intro h₁;  exact comp_sub_of_sub h₁;`
    第 1 のゴールを仮定 $\mathtt{h}_1 \colon A \subseteq B$ とゴール $B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ に分解する．既証明の定理 $A \subseteq B \vdash B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ に $\mathtt{h}_1$ を適用して，ゴールを得る．
03. `intro h₂;  have h₃ := comp_sub_of_sub h₂;`
    第 2 のゴールを仮定 $\mathtt{h}_2 \colon B^{\mathsf{c}} \subseteq A^{\mathsf{c}}$ とゴールに分解する．既証明の定理 $B^{\mathsf{c}} \subseteq A^{\mathsf{c}} \vdash A^{\mathsf{cc}} \subseteq B^{\mathsf{cc}}$ に $\mathtt{h}_2$ を適用して，新たな手札 $\mathtt{h}_3$ を得る．
04. `rw [comp_def] at h₃;  rw [comp_def] at h₃;  exact h₃`
    手札 $\mathtt{h}_3 \colon A^{\mathsf{cc}} \subseteq B^{\mathsf{cc}}$ に対して，まず A^{cc} を A に書き換え，次に B^{cc} を B に書き換える．この書き換わった手札 $\mathtt{h}_3 \colon A \subseteq B$ はゴールを示している．

2.4. Intersection World

2.4.1 Level 1/8: And

$x \in A \wedge x \in B \vdash x \in A$ を証明せよ．これについては，基本命令の所で紹介した方法による．

$$\dfrac{\mathtt{h} \colon x \in A \wedge x \in B}{\mathtt{h.left} \colon x \in A}\,\texttt{(}\wedge\texttt{Elim)}$$

つまり，これを証明する命令は `exact h.left` である．

2.4.2 Level 2 / 8 : Element of an intersection

$x \in A \cap B \vdash x \in B$ を証明せよ．これは $A \cap B$ の定義 `inter_def` の書き換えを経由すれば明らかである．

$$
\begin{prooftree}
\AxiomC{$\mathtt{h}\colon x \in A \cap B$}
\doubleLine
\RightLabel{(rw)}
\UnaryInfC{$\mathtt{h}\colon x \in A \wedge x \in B$}
\RightLabel{($\wedge$Elim)}
\UnaryInfC{$\mathtt{h.right}\colon x \in B$}
\end{prooftree}
$$

つまり，`rw [inter_def] at h` と打ち込めば，$x \in A \cap B$ の定義 $x \in A \wedge x \in B$ が復元される．実際には，このステップを明示的に記述しなくとも，Lean は自動的にこのステップを補完してくれる．つまり，命令 `exact h.right` によって証明が与えられる．

2.4.3 Level 3/8: Intersection is a subset

$\vdash A \cap B \subseteq A$ を証明せよ．ここまでのアイデアの組合せである．

$$
\begin{prooftree}
\AxiomC{$\mathtt{h}\colon x \in A \cap B$}
\doubleLine
\UnaryInfC{$\mathtt{h}\colon x \in A \wedge x \in B$}
\RightLabel{($\wedge$Elim)}
\UnaryInfC{$\mathtt{h.left}\colon x \in A$}
\RightLabel{(intro h)}
\UnaryInfC{$x \in A \cap B \to x \in A$}
\RightLabel{(intro x)}
\UnaryInfC{$\forall z (z \in A \cap B \to z \in A)$}
\doubleLine
\UnaryInfC{$A \cap B \subseteq A$}
\end{prooftree}
$$

つまり，`intro x;`　`intro h;`　`exact h.left` である．

2.4.4 Level 4/8: Proving a conjunction

$x \in A,\ x \in B \vdash x \in A \cap B$ を証明せよ．これについては，基本命令の所で紹介した方法による．

$$
\begin{prooftree}
\AxiomC{$\mathtt{h}_1\colon x \in A$}
\AxiomC{$\mathtt{h}_2\colon x \in B$}
\RightLabel{($\wedge$Intro)}
\BinaryInfC{$\mathtt{And.intro}\ \mathtt{h}_1\ \mathtt{h}_2\colon x \in A \wedge x \in B$}
\doubleLine
\UnaryInfC{$x \in A \cap B$}
\end{prooftree}
$$

つまり，`exact And.intro h₁ h₂` である．

2.4.5 Level 5/8: Subset of an intersection

$A \subseteq B,\ A \subseteq C \vdash A \subseteq B \cap C$ を証明せよ．現在の手札とゴールを見ながら進めていけば，特に詰まる点は無いはずだ．

$$
\begin{prooftree}
\AxiomC{$\mathtt{h}_1\colon A \subseteq B$}
\doubleLine
\UnaryInfC{$x \in A \to x \in B$}
\AxiomC{$\mathtt{h}_3\colon x \in A$}
\BinaryInfC{$x \in B$}
\AxiomC{$\mathtt{h}_2\colon A \subseteq C$}
\doubleLine
\UnaryInfC{$x \in A \to x \in C$}
\AxiomC{$\mathtt{h}_3\colon x \in A$}
\BinaryInfC{$x \in C$}
\RightLabel{(And.intro)}
\BinaryInfC{$x \in B \wedge x \in C$}
\doubleLine
\UnaryInfC{$x \in B \cap C$}
\RightLabel{(intro h3)}
\UnaryInfC{$x \in A \to x \in B \cap C$}
\RightLabel{(intro x)}
\UnaryInfC{$\forall z (z \in A \to z \in B \cap C)$}
\doubleLine
\UnaryInfC{$A \subseteq B \cap C$}
\end{prooftree}
$$

この証明を与える手続きは，以下のように記述できる．

01. intro x; intro $\mathtt{h}_3$; apply And.intro;

最初の 2 つのコマンドで，ゴールが $A \subseteq B \cap C$ から $x \in B \cap C$ へと移行する．その後，And.intro の適用で，ゴールが $x \in B$ と $x \in C$ へと分岐する．

02. exact $\mathtt{h}_1$ $\mathtt{h}_3$; exact $\mathtt{h}_2$ $\mathtt{h}_3$;

第 1 ゴールの解は $\mathtt{h}_1$ $\mathtt{h}_3$ で，第 2 ゴールの解は $\mathtt{h}_2$ $\mathtt{h}_3$ であるとすぐに分かる．

2.4.6 Level 6/8: Intersection subset of swap

$\vdash A \cap B \subseteq B \cap A$ を証明せよ．これもここまでのアイデアの組合せである．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}\colon x \in A \cap B]$}
\doubleLine
\UnaryInfC{$\mathtt{h}\colon x \in A \wedge x \in B$}
\UnaryInfC{$\mathtt{h.right}\colon x \in B$}
\AxiomC{$[\mathtt{h}\colon x \in A \cap B]$}
\doubleLine
\UnaryInfC{$\mathtt{h}\colon x \in A \wedge x \in B$}
\UnaryInfC{$\mathtt{h.left}\colon x \in A$}
\RightLabel{(And.intro)}
\BinaryInfC{$x \in B \wedge x \in A$}
\doubleLine
\UnaryInfC{$x \in B \cap A$}
\RightLabel{(intro h)}
\UnaryInfC{$x \in A \cap B \to x \in B \cap A$}
\RightLabel{(intro x)}
\UnaryInfC{$\forall z (z \in A \cap B \to z \in B \cap A)$}
\doubleLine
\UnaryInfC{$A \cap B \subseteq B \cap A$}
\end{prooftree}
$$

- intro x; intro h; apply And.intro; exact h.right; exact h.left

2.4.7 Level 7/8: Intersection is commutative

$\vdash A \cap B = B \cap A$ を証明せよ．既に証明した定理は，いつでも用いることができる．第 2.4.6 節で証明した定理 $A \cap B \subseteq B \cap A$ を inter_sub_swap A B として参照する．

- apply sub_antisymm; exact inter_sub_swap A B; exact inter_sub_swap B A

2.4.8 Level 8/8: Intersection is associative

$\vdash (A \cap B) \cap C = A \cap (B \cap C)$ を証明せよ．集合の等号を示すためには，両方向の包含関係を示せばよい．反対称律 sub_antisymm を用いてもよいが，$P = Q$ の定義 $\forall x (x \in P \leftrightarrow x \in Q)$ に従って，任意の x を取る，という動作から行う ext というコマンドもある．

$$
\begin{prooftree}
\AxiomC{$x \in P \to x \in Q$}
\AxiomC{$x \in Q \to x \in P$}
\RightLabel{(Iff.intro)}
\BinaryInfC{$x \in P \leftrightarrow x \in Q$}
\RightLabel{(ext x)}
\UnaryInfC{$\forall z (z \in P \leftrightarrow z \in Q)$}
\doubleLine
\UnaryInfC{$P = Q$}
\end{prooftree}
$$

したがって，目的の証明を行う最初の 2 ステップは以下のように与えることができるだろう．

- ext x; apply Iff.intro

これでゴールは 2 つに分岐するので，各ゴール毎に以下のように証明を与える．

$$
\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : x \in (A \cap B) \cap C]}{\mathtt{h}_2 := \mathtt{h}_1.\mathtt{left} : x \in A \cap B}}{\mathtt{h}_2.\mathtt{left} : x \in A} \qquad \dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : x \in (A \cap B) \cap C]}{\mathtt{h}_3 := \mathtt{h}_1.\mathtt{left} : x \in A \cap B}}{\mathtt{h}_3.\mathtt{right} : x \in B} \qquad \dfrac{[\mathtt{h}_1 : x \in (A \cap B) \cap C]}{\mathtt{h}_1.\mathtt{right} : x \in C}}{x \in B \cap C}\ (\mathtt{And.intro})}{x \in A \cap (B \cap C)}\ (\mathtt{And.intro})}{x \in (A \cap B) \cap C \to x \in A \cap (B \cap C)}\ (\mathtt{intro\ h1})
$$

この部分を表す手続きは以下である．

- `intro h₁; apply And.intro; have h₂ := h₁.left; exact h₂.left;`
  `apply And.intro; have h₃ := h₁.left; exact h₃.right; exact h₁.right`

次のゴールも以下のように証明できる．

$$
\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_4 : x \in A \cap (B \cap C)]}{\mathtt{h}_4.\mathtt{left} : x \in A} \qquad \dfrac{\dfrac{[\mathtt{h}_4 : x \in A \cap (B \cap C)]}{\mathtt{h}_5 := \mathtt{h}_4.\mathtt{right} : x \in B \cap C}}{\mathtt{h}_5.\mathtt{left} : x \in B}}{x \in A \cap B}\ (\mathtt{And.intro}) \qquad \dfrac{\dfrac{[\mathtt{h}_4 : x \in A \cap (B \cap C)]}{\mathtt{h}_6 := \mathtt{h}_4.\mathtt{right} : x \in B \cap C}}{\mathtt{h}_6.\mathtt{right} : x \in C}}{x \in (A \cap B) \cap C}\ (\mathtt{And.intro})}{x \in A \cap (B \cap C) \to x \in (A \cap B) \cap C}\ (\mathtt{intro\ h4})
$$

この部分を表す手続きは以下である．

- `intro h₄; apply And.intro; apply And.intro; exact h₄.left;`
  `have h₅ := h₄.right; exact h₅.left; have h₆ := h₄.right; exact h₆.right`

ちなみに `h` の添字については，各コマンドが証明図のどの部分を表しているかを明瞭にするために，それぞれ別のものを用いているが，ここまですべての `h` の添字を異なるものに変える必要はない．

2.5. Union World

2.5.1 Level 1/6: Or

$x \in A \vdash x \in A \lor x \in B$ を証明せよ．これは基本命令を使えるようになるための練習問題である．

$$
\dfrac{\mathtt{h} : x \in A}{\mathtt{Or.inl\ h} : x \in A \lor x \in B}\ (\lor\mathtt{Intro})
$$

つまり，これを証明するための手続きは `exact Or.inl h` である．

2.5.2 Level 2/6: Subset of a union

$\vdash B \subseteq A \cup B$ を証明せよ．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}\colon x \in B]$}
\doubleLine
\UnaryInfC{$\mathtt{Or.inr}\ \mathtt{h}\colon x \in A \lor x \in B$}
\doubleLine
\UnaryInfC{$x \in A \cup B$}
\RightLabel{$\mathtt{(intro\ h)}$}
\UnaryInfC{$x \in B \to x \in A \cup B$}
\RightLabel{$\mathtt{(intro\ x)}$}
\UnaryInfC{$\forall z (z \in B \to z \in A \cup B)$}
\doubleLine
\UnaryInfC{$B \subseteq A \cup B$}
\end{prooftree}
$$

- `intro x;  intro h;  exact Or.inr h`

2.5.3 Level 3/6: Proof by cases

$A \subseteq C,\ B \subseteq C \vdash A \cup B \subseteq C$ を証明せよ．条件分岐に関する問題である．この証明図は丁寧に記述しよう．まずはいつも通りのプロセスから始まる．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}_3\colon x \in A \cup B]$}
\doubleLine
\UnaryInfC{$\mathtt{h}_3\colon x \in A \lor x \in B$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\RightLabel{$\mathtt{(intro\ h3)}$}
\UnaryInfC{$\cancel{\mathtt{Goal}}\colon\ x \in A \cup B \to x \in C$}
\RightLabel{$\mathtt{(intro\ x)}$}
\UnaryInfC{$\cancel{\mathtt{Goal}}\colon\ \forall z (z \in A \cup B \to z \in C)$}
\doubleLine
\UnaryInfC{$A \cup B \subseteq C$}
\end{prooftree}
$$

手札 $\mathtt{h}_3$ を使用すると，$x \in A$ の場合と $x \in B$ の場合の条件分岐が行われる．前者に $\mathtt{h}_4$，後者に $\mathtt{h}_5$ という名前を付ける場合には，この操作を行うコマンドは `cases'` $\mathtt{h}_3$ `with` $\mathtt{h}_4$ $\mathtt{h}_5$ である．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}_3\colon x \in A \cup B]$}
\doubleLine
\UnaryInfC{$\mathtt{h}_3\colon x \in A \lor x \in B$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\end{prooftree}
\quad \rightsquigarrow \quad
\begin{prooftree}
\AxiomC{$[\mathtt{h}_3\colon x \in A \cup B]$}
\doubleLine
\UnaryInfC{$\mathtt{h}_3\colon x \in A \lor x \in B$}
\AxiomC{$[\mathtt{h}_4\colon x \in A]$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\AxiomC{$[\mathtt{h}_5\colon x \in B]$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\RightLabel{$\mathtt{(\lor Elim)}$}
\TrinaryInfC{$\cancel{\mathtt{Goal}}\colon\ x \in C$}
\end{prooftree}
$$

各条件分岐において，ゴールは以下のように達成できる．

$$
\begin{prooftree}
\AxiomC{$[\mathtt{h}_1\colon A \subseteq C]$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{h}_1\colon x \in A \to x \in C$}
\AxiomC{$[\mathtt{h}_4\colon x \in A]$}
\BinaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\end{prooftree}
\qquad
\begin{prooftree}
\AxiomC{$[\mathtt{h}_2\colon B \subseteq C]$}
\noLine
\UnaryInfC{$\vdots$}
\noLine
\UnaryInfC{$\mathtt{h}_2\colon x \in B \to x \in C$}
\AxiomC{$[\mathtt{h}_5\colon x \in B]$}
\BinaryInfC{$\mathtt{Goal}\colon\ x \in C$}
\end{prooftree}
$$

以上をまとめると，目的の主張は以下によって証明される．

- `intro x;  intro h₃;  cases' h₃ with h₄ h₅;  exact h₁ h₄;  exact h₂ h₅`

2.5.4 Level 4/6: Union subset of swap

$\vdash A \cup B \subseteq B \cup A$ を証明せよ．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : x \in A \cup B]}{\mathtt{h}_1 : x \in A \lor x \in B} \qquad \dfrac{[\mathtt{h}_2 : x \in A]}{\mathtt{Or.inr}\ \mathtt{h}_2 : x \in B \cup A} \qquad \dfrac{[\mathtt{h}_3 : x \in B]}{\mathtt{Or.inl}\ \mathtt{h}_3 : x \in B \cup A}}{x \in B \cup A}\ \texttt{(cases' h1 with h2 h3)}}{x \in A \cup B \to x \in B \cup A}\ \texttt{(intro h1)}}{\forall z (z \in A \cup B \to z \in B \cup A)}\ \texttt{(intro x)}}{A \cup B \subseteq B \cup A}
$$

- `intro x;` `intro h₁;` `cases' h₁ with h₂ h₃;` `exact Or.inr h₂;` `exact Or.inl h₃`

2.5.5 Level 5/6: Union is commutative

$\vdash A \cup B = B \cup A$ を証明せよ．第 2.5.4 で証明した定理は，`union_sub_swap` という名前を付けておくことにする．

$$
\dfrac{\dfrac{}{A \cup B \subseteq B \cup A}\ \texttt{(union\_sub\_swap)} \qquad \dfrac{}{B \cup A \subseteq A \cup B}\ \texttt{(union\_sub\_swap)}}{A \cup B = B \cup A}\ \texttt{(sub\_anti\_symm)}
$$

- `apply sub_antisymm;` `exact union_sub_swap A B;` `exact union_sub_swap B A`

2.5.6 Level 6/6: Union is associative

$\vdash (A \cup B) \cup C = A \cup (B \cup C)$ を証明せよ．アイデアはここまでの議論の単純な組合せであるが，証明が長いので，少しずつ証明していこう．

$$
\dfrac{\dfrac{\overset{\texttt{Goal}_1}{x \in (A \cup B) \cup C \to x \in A \cup (B \cup C)} \qquad \overset{\texttt{Goal}_2}{x \in A \cup (B \cup C) \to x \in (A \cup B) \cup C}}{\cancel{\texttt{Goal}_1} : x \in (A \cup B) \cup C \leftrightarrow x \in A \cup (B \cup C)}\ \texttt{(Iff.intro)}}{\cancel{\texttt{Goal}_1} : (A \cup B) \cup C = A \cup (B \cup C)}\ \texttt{(ext x)}
$$

- `ext x;` `apply Iff.intro;`

ゴールが 2 つに分岐したので，まずは左のゴール $\texttt{Goal}_1$ を目指そう．

$$
\dfrac{\dfrac{[\mathtt{h}_1 : x \in (A \cup B) \cup C] \qquad \begin{matrix}[\mathtt{h}_2 : x \in A \cup B] \\ \vdots \\ \texttt{Goal}_1 : x \in A \cup (B \cup C)\end{matrix} \qquad \begin{matrix}[\mathtt{h}_3 : x \in C] \\ \vdots \\ \texttt{Goal}_1 : x \in A \cup (B \cup C)\end{matrix}}{\cancel{\texttt{Goal}_1} : x \in A \cup (B \cup C)}\ \texttt{(cases')}}{\cancel{\texttt{Goal}_1} : x \in (A \cup B) \cup C \to x \in A \cup (B \cup C)}\ \texttt{(intro h1)}
$$

- `intro h₁;` `cases' h₁ with h₂ h₃;`

手札 $x \in (A \cup B) \cup C$ を消費して条件分岐が行われた．$x \in A \cup B$ の場合と $x \in C$ の場合でそれぞれゴールに到達すればよい．まずは $x \in A \cup B$ の場合を考えよう．

$$\dfrac{[\mathtt{h}_2 : x \in A \cup B] \qquad \dfrac{[\mathtt{h}_4 : x \in A]}{\mathtt{Goal}_1 : x \in A \cup (B \cup C)}\,(\mathtt{Or.inl}) \qquad \dfrac{\dfrac{[\mathtt{h}_5 : x \in B]}{\mathtt{Goal}_1 : x \in B \cup C}\,(\mathtt{Or.inl})}{\cancel{\mathtt{Goal}_1} : x \in A \cup (B \cup C)}\,(\mathtt{Or.inr})}{\cancel{\mathtt{Goal}_1} : x \in A \cup (B \cup C)}\,(\mathtt{cases'})$$

- cases' $\mathtt{h}_2$ with $\mathtt{h}_4$ $\mathtt{h}_5$; exact Or.inl $\mathtt{h}_4$; apply Or.inr; exact Or.inl $\mathtt{h}_5$;
  手札 $x \in A \cup B$ を消費して，$x \in A$ の場合と $x \in B$ の場合に分岐した．$x \in A$ の場合には，直ちにゴールに到達できる．$x \in B$ の場合には，まず Or.inr を適用してゴールを変更した．このゴールは，手札 $x \in B$ から直ちに到達できる．

次に，条件分岐の $x \in C$ の場合について考えよう．この場合は簡単である．

$$\dfrac{\dfrac{[\mathtt{h}_3 : x \in C]}{\mathtt{Goal}_1 : B \cup C}\,(\mathtt{Or.inr})}{\cancel{\mathtt{Goal}_1} : A \cup (B \cup C)}\,(\mathtt{Or.inr})$$

- apply Or.inr; exact Or.inr $\mathtt{h}_3$;

右のゴール $\mathtt{Goal}_2$ の達成方法も同様であるので，省略する．

§ 3. 述語論理

3.1. 基本命令

■全称量化 ∀ の推論規則: 全称量化の除去規則は，$\forall z A(x)$ から，どんな x に対しても $A(x)$ を導けるというものである．つまり，我々は手札に $\forall z A(z)$ を所持しているとき，どんな x に対しても，$A(x)$ を新たな手札として得ることができる．手札 $\forall z A(z)$ のラベルが h ならば，h x が手札 $A(x)$ を指し示す．

$$\dfrac{\mathtt{h} : \forall z A(z)}{\mathtt{h\,x} : A(x)}\,(\forall\mathtt{Elim})$$

つまり，手札 $A(x)$ を得るためには，たとえば have $\mathtt{h}_2$:= h x と打ち込めばよい．

次に，全称量化の導入規則である．ゴールが $\forall z A(z)$ であるとき，我々は，どんな x が与えられたとしても $A(x)$ を証明できなければならない．つまりは，「x が与えられた」という状況の変化があり，「ゴールは $A(x)$ へと変更」とされる．

$$\mathtt{Goal}:\ \forall z A(z) \qquad \rightsquigarrow \qquad \dfrac{\mathtt{Goal}:\ A(x)}{\cancel{\mathtt{Goal}}:\ \forall z A(z)}\,(\forall\mathtt{Intro})$$

この動作を行うコマンドは intro x である．一応，注意点を述べるとすれば，通常の数学においても Lean においても，実際のところ，1 つの x を取った上で，$A(x)$ の証明が進んでいく．これで $\forall z A(z)$ の証明として成立している理由としては，我々はどんな x を取ったとしても成り立つ証明を記述するためである．したがって，この記号 x はどんな別の記号と置き換えても証明が成立する必要があり，他の自由変数と記号の衝突をしてはならない．

つまり，intro x で用いる x は，他の自由変数と異なるものでなければない．とはいえ，もし x が既に用いられていたとすると，Lean は自動的にそれを $x^{\dagger}$ などの別の記号に変換してくれるはずだ．また，$\forall x A(x)$ に対して intro x を用いるなどの束縛変数との記号の衝突は問題ない．

■存在量化の推論規則: 仮定 $A(t)$ から $\exists x A(x)$ を推論できる．この推論を行うためのコマンドは Exists.intro であるが，このためには，手札 $A(t)$ のラベル h だけではなく，手札 $A(t)$ のどの変数記号に対して存在量化の導入を行うのかの情報も必要である．今回の場合は，それは t である．

$$\dfrac{\texttt{h}\colon A(t)}{\texttt{Exists.intro t h}\colon \exists x A(x)}\ (\exists\texttt{Intro})$$

実際には，このコマンドはいつものように have や apply と組み合わせる．たとえば，apply Exists.intro t と打ち込めば，ゴールを $\exists x A(x)$ から $A(t)$ へと変更できる．

$$\texttt{Goal}\colon\ \exists x A(x) \qquad \rightsquigarrow \qquad \dfrac{\texttt{Goal}\colon\ A(t)}{\cancel{\texttt{Goal}}\colon\ \exists x A(x)}\ (\exists\texttt{Intro})$$

次に，$\exists x A(x)$ を仮定として得ていたとしよう．これは $A(x)$ となる x が存在すると主張しているのだから，実際にそのような x を得ることができるはずだ．この存在の証拠を実際に得るためのコマンドが obtain である．より正確には，手札 $\texttt{h}\colon \exists x A(x)$ を使用して，その存在の証拠 w について，新たな手札 $\texttt{h}_2\colon A(w)$ を得るコマンドは，obtain <w, h₂> := h である．新たな手札を得るだけなので，ゴールの変更は行われない．

$$\begin{array}{c}\texttt{h}\colon \exists x A(x)\\ \vdots\\ \texttt{Goal}\colon\ B\end{array} \qquad \rightsquigarrow \qquad \dfrac{\texttt{h}\colon \exists x A(x) \qquad \begin{array}{c}[\texttt{h}_2\colon A(w)]\\ \vdots\\ \texttt{Goal}\colon\ B\end{array}}{\cancel{\texttt{Goal}}\colon\ B}\ (\exists\texttt{Elim})$$

ここでも注意点であるが，我々が得た存在の証拠 w の可能性は色々とあり得るが，この証拠 w が（$A(w)$ を満たす限りは）どんなものであったとしても通用する証明を記述しなければならない．したがって，この記号 w はどんな別の記号と置き換えても証明が成立する必要があり，他の自由変数と記号の衝突をしてはならない．

3.2. Family Intersection World

3.2.1 Level 1/6: Family intersection is subset

$A \in F \vdash \bigcap F \subseteq A$ を証明せよ．定義に立ち返ると，この記号 $\bigcap$ は，全称量化のようなものである．

$$x \in \bigcap F \iff \forall S \in F.\ x \in S \iff \forall S\ (S \in F \to x \in S)$$

この記号は慣れるまでは少し分かりにくいと思うが，つまり，$\bigcap\{S_i : i \in I\}$ が $\bigcap_{i \in I} S_i$ に対応する．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_2 : x \in \bigcap F]}{\mathtt{h}_2 : \forall S \in F.\ x \in S}}{\mathtt{h}_2 : \forall S (S \in F \to x \in S)}}{\mathtt{h}_2\ \mathtt{A} : A \in F \to x \in A}\,(\forall\mathtt{Elim}) \qquad [\mathtt{h}_1 : A \in F]}{x \in A}}{x \in \bigcap F \to x \in A}\,(\mathtt{intro\ h2})}{\bigcap F \subseteq A}\,(\mathtt{intro\ x})
$$

- `intro x;` `intro` $\mathtt{h}_2$`;` `have` $\mathtt{h}_3$ `:=` $\mathtt{h}_2$ `A;` `exact` $\mathtt{h}_3$ $\mathtt{h}_1$

3.2.2 Level 2/6: Intersection of larger family is smaller

$F \subseteq G \vdash \bigcap G \subseteq \bigcap F$ を証明せよ．数学の証明の際に最も基本的かつ重要なアイデアは「定義に戻って考える」ことである．$\bigcap$ の定義には `fam_inter_def` というラベルが付けられている．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_2 : x \in \bigcap G]}{\mathtt{h}_2 : \forall Z \in G. x \in Z}\,(\mathtt{rw})}{\mathtt{h}_2 : \forall Z (Z \in G \to x \in Z)}}{\mathtt{h}_2\ \mathtt{S} : S \in G \to x \in S} \qquad \dfrac{\begin{array}{c}[\mathtt{h}_1 : F \subseteq G] \\ \vdots \\ \mathtt{h}_1 : S \in F \to S \in G\end{array} \qquad [\mathtt{h}_3 : S \in F]}{\mathtt{h}_1\ \mathtt{h}_3 : S \in G}}{\mathtt{Goal} : x \in S}}{S \in F \to x \in S}\,(\mathtt{intro\ h3})}{\forall Z (Z \in F \to x \in Z)}\,(\mathtt{intro\ S})}{\forall Z \in F. x \in Z}}{x \in \bigcap F}\,(\mathtt{rw})}{x \in \bigcap G \to x \in \bigcap F}\,(\mathtt{intro\ h2})}{\bigcap G \subseteq \bigcap F}\,(\mathtt{intro\ x})
$$

- `intro x;` `intro` $\mathtt{h}_2$`;` `rw [fam_inter_def];` `rw [fam_inter_def] at` $\mathtt{h}_2$`;`
  ゴールを $x \in \bigcap F$ まで変更した後，$\bigcap$ の定義に従ってゴールを書き換えた．ついでに手札 $\mathtt{h}_2$ も $\bigcap$ の定義に従って書き換えておいた．
- `intro S;` `intro` $\mathtt{h}_3$`;` `have` $\mathtt{h}_4$ `:=` $\mathtt{h}_1$ $\mathtt{h}_3$`;` `have` $\mathtt{h}_5$ `:=` $\mathtt{h}_2$ `S;` `exact` $\mathtt{h}_2$ $\mathtt{h}_4$
  ゴールを $x \in S$ まで変更した後，既にある手札を組合せて，ゴールに到達した．

3.2.3 Level 3/6: Intersection of a pair

$\vdash A \cap B = \bigcap\{A, B\}$ を証明せよ．ここで，対の定義には pair_def というラベルが付けられている．等号の証明は，これまでと同様，両方向の含意の証明に持ち込む．つまり，以下のように 2 つのゴールへと分岐する．

$$\dfrac{\dfrac{\texttt{Goal}_1 : x \in A \cap B \to x \in \bigcap\{A, B\} \qquad \texttt{Goal}_2 : x \in \bigcap\{A, B\} \to x \in A \cap B}{x \in A \cap B \leftrightarrow x \in \bigcap\{A, B\}}\;(\texttt{Iff.intro})}{A \cap B = \bigcap\{A, B\}}\;(\texttt{ext x})$$

- `ext x;  apply Iff.intro;`

第 2 のゴールは以下のように達成される．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_2 : S \in \{A, B\}]}{\mathtt{h}_2 : S = A \lor S = B}\;(\texttt{rw}) \quad \dfrac{[\mathtt{h}_3 : S = A] \quad \dfrac{[\mathtt{h}_1 : x \in A \cap B]}{x \in A}}{x \in S}\;(\texttt{rw}) \quad \dfrac{[\mathtt{h}_4 : S = B] \quad \dfrac{[\mathtt{h}_1 : x \in A \cap B]}{x \in B}}{x \in S}\;(\texttt{rw})}{x \in S}}{S \in \{A, B\} \to x \in S}\;(\texttt{intro h2})}{\forall Z \in \{A, B\}.\ x \in S}\;(\texttt{intro S})}{x \in \bigcap\{A, B\}}\;(\texttt{rw})}{x \in A \cap B \to x \in \bigcap\{A, B\}}\;(\texttt{intro h1})$$

- `intro h₁;  rw [fam_inter_def];  intro S;  intro h₂;  rw [pair_def] at h₂;`
  $\bigcap$ の定義の書き換えを経由しながら，まずはゴールを $x \in S$ に変更し，途中で得た手札 $\mathtt{h}_2$ の定義に従った書き換えも行った．
- `cases' h₂ with h₃ h₄;  have h₅ := h₁.left;  rw [<-h₃] at h₅;  exact h₅;`
  $S = A$ の場合と $S = B$ の場合で分岐する．前者の場合，$\mathtt{h}_5 : x \in A$ を得た後，$\mathtt{h}_3 : S = A$ を用いて $x \in S$ を得たい．しかし，`rw [h₃]` は「S に A を代入する」と解釈されてしまう．我々が行いたいことは，「A に S を代入する」ことであり，これは `rw [<-h₃]` によって成し遂げられる．
- `have h₆ := h₁.right;  rw [<-h₄] at h₆;  exact h₆;`
  $S = B$ の場合も同様に，$\mathtt{h}_6 : x \in B$ を得た後，$\mathtt{h}_4 : S = B$ を用いてゴール $x \in S$ を得られる．

第 2 のゴールは，更に次のように分岐する．

$$\dfrac{\dfrac{\texttt{Goal}_{2.1} : x \in A \qquad \texttt{Goal}_{2.2} : x \in B}{\cancel{\texttt{Goal}_2} : x \in A \cap B}\;(\texttt{And.intro})}{\cancel{\texttt{Goal}_2} : x \in \bigcap\{A, B\} \to x \in A \cap B}\;(\texttt{intro h7})$$

- `intro h₇;  apply And.intro;`

まず，$\text{Goal}_{2.1}$ は以下のように達成できる．

$$\dfrac{\dfrac{\dfrac{[\texttt{h}_7 : x \in \bigcap\{A, B\}]}{\texttt{h}_7 : \forall S \in \{A, B\}.\, x \in S}\;(\texttt{rw})}{\texttt{h}_7\ \texttt{A} : A \in \{A, B\} \to x \in A} \qquad \dfrac{\dfrac{\texttt{rfl} : A = A}{A = A \lor A = B}\;(\texttt{Or.inl})}{\texttt{Goal} : A \in \{A, B\}}\;(\texttt{rw})}{\cancel{\texttt{Goal}} : x \in A}\;(\texttt{apply})$$

- `rw [fam_inter_def] at` $\texttt{h}_7$`;  have` $\texttt{h}_8$ `:=` $\texttt{h}_7$ `A;  apply` $\texttt{h}_8$`;`
  手札 $\texttt{h}_7$ を $\bigcap$ の定義に従って書き換え，A を代入したものを用いると，ゴールが $x \in A$ から $A \in \{A, B\}$ へと変化する．
- `rw [pair_def];  apply Or.inl;  rfl;`
  対の定義に従って，ゴールを書き換えると，その左部は自明な式 $A = A$ である．このとき，`rfl` によって，これが自明な式であることを Lean に伝える．

同様の方法で，$\text{Goal}_{2.2}$ も達成できる．

$$\dfrac{\dfrac{\dfrac{[\texttt{h}_7 : x \in \bigcap\{A, B\}]}{\texttt{h}_7 : \forall S \in \{A, B\}.\, x \in S}\;(\texttt{rw})}{\texttt{h}_7\ \texttt{B} : B \in \{A, B\} \to x \in B} \qquad \dfrac{\dfrac{\texttt{rfl} : B = B}{B = A \lor B = B}\;(\texttt{Or.inr})}{\texttt{Goal} : B \in \{A, B\}}\;(\texttt{rw})}{\cancel{\texttt{Goal}} : x \in B}\;(\texttt{apply})$$

- `rw [fam_inter_def] at` $\texttt{h}_7$`;  have` $\texttt{h}_9$ `:=` $\texttt{h}_7$ `B;  apply` $\texttt{h}_9$`;`
  `rw [pair_def];  apply Or.inr;  rfl;`

3.2.4 Level 4/6: Intersection of a union of families

$\vdash (\bigcap F) \cap (\bigcap G) \to x \in \bigcap(F \cup G)$ を証明せよ．初見では一見非自明な主張であるが，定義に従って推論を進めていけば，特に難しい点は無いはずだ．まずは，特に頭を使わないで良い段階まででゴールを変形していく．

$$\dfrac{\dfrac{\dfrac{\dfrac{\texttt{Goal}_{1.1} : x \in \bigcap F \qquad \texttt{Goal}_{1.2} : x \in \bigcap G}{\cancel{\texttt{Goal}_1} : x \in (\bigcap F) \cap (\bigcap G)}\;(\texttt{And.intro})}{\cancel{\texttt{Goal}_1} : x \in \bigcap(F \cup G) \to x \in (\bigcap F) \cap (\bigcap G)}\;(\texttt{intro h1}) \qquad \texttt{Goal}_2 : x \in (\bigcap F) \cap (\bigcap G) \to x \in \bigcap(F \cup G)}{\cancel{\texttt{Goal}} : x \in \bigcap(F \cup G) \leftrightarrow x \in (\bigcap F) \cap (\bigcap G)}\;(\texttt{Iff.intro})}{\cancel{\texttt{Goal}} : \bigcap(F \cup G) = (\bigcap F) \cap (\bigcap G)}\;(\texttt{ext x})$$

- `ext x;  apply Iff.intro;  intro` $\texttt{h}_1$`;  apply And.intro;`
  まず，等式の証明を両方向の含意への証明へと分岐させる．左のゴール $\texttt{Goal}_1$ を達成するために，仮定と結論を分解した後，連言文を示すためにゴールを $\texttt{Goal}_{1.1}$ と $\texttt{Goal}_{1.2}$ へと分岐させる．

まず，$\mathtt{Goal}_{1.1}$ は以下のように達成できる．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : x \in \bigcap(F \cup G)]}{\mathtt{h}_1 : \forall Z \in F \cup G.\ x \in Z}\ (\mathtt{rw})}{\mathtt{h}_1\,\mathtt{S} : S \in F \cup G \to x \in S} \qquad \dfrac{[\mathtt{h}_2 : S \in F]}{S \in F \cup G}\ (\mathtt{Or.inl})}{x \in S}}{S \in F \to x \in S}\ (\mathtt{intro\ h2})}{\forall Z \in F.\ x \in Z}\ (\mathtt{intro\ S})}{x \in \bigcap F}\ (\mathtt{rw})
$$

- rw [fam_inter_def]; rw [fam_inter_def] at $\mathtt{h}_1$; intro S; intro $\mathtt{h}_2$;
  $\bigcap$ を定義に従って書き換えつつ，ゴールを $x \in S$ まで変更する．
- apply $\mathtt{h}_1$ S; exact Or.inl $\mathtt{h}_2$;
  $\mathtt{h}_1\,\mathtt{S}$ が指し示す式は，ゴール $x \in S$ を $S \in F \cup G$ へと変更する．手札 $\mathtt{h}_2$ がゴールの左部になっている．

次の $\mathtt{Goal}_{1,2}$ の達成方法も全く同様である．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : x \in \bigcap(F \cup G)]}{\mathtt{h}_1 : \forall Z \in F \cup G.\ x \in Z}\ (\mathtt{rw})}{\mathtt{h}_1\,\mathtt{S} : S \in F \cup G \to x \in S} \qquad \dfrac{[\mathtt{h}_3 : S \in G]}{S \in F \cup G}\ (\mathtt{Or.inr})}{x \in S}}{S \in G \to x \in S}\ (\mathtt{intro\ h3})}{\forall Z \in G.\ x \in Z}\ (\mathtt{intro\ S})}{x \in \bigcap G}\ (\mathtt{rw})
$$

- rw [fam_inter_def]; rw [fam_inter_def] at $\mathtt{h}_1$; intro S; intro $\mathtt{h}_3$;
  apply $\mathtt{h}_1$ S; exact Or.inr $\mathtt{h}_3$;

次に，$\mathtt{Goal}_2$ の達成を目指そう．

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_5 : S \in F \cup G] \qquad \begin{matrix}[\mathtt{h}_6 : S \in F]\\ \vdots \\ x \in S\end{matrix} \qquad \begin{matrix}[\mathtt{h}_7 : S \in G]\\ \vdots \\ x \in S\end{matrix}}{x \in S}\ (\mathtt{cases'})}{S \in F \cup G \to x \in S}\ (\mathtt{intro\ h5})}{\forall Z \in F \cup G.\ x \in Z}\ (\mathtt{intro\ S})}{x \in \bigcap(F \cup G)}\ (\mathtt{rw})}{x \in (\bigcap F) \cap (\bigcap G) \to x \in \bigcap(F \cup G)}\ (\mathtt{intro\ h4})
$$

- intro $\mathtt{h}_4$; rw [fam_inter_def]; intro S; intro $\mathtt{h}_5$; cases' $\mathtt{h}_5$ with $\mathtt{h}_6$ $\mathtt{h}_7$;
  ゴールを $x \in S$ まで持ち上げ，手札 $\mathtt{h}_5$ を用いて条件分岐を行う．

$S \in F$ の場合には，以下の推論を行う．

$$\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h_4} : x \in (\bigcap F) \cap (\bigcap G)]}{\mathtt{h_4.left} : x \in \bigcap F}}{\mathtt{h_4.left} : \forall Z \in F.\ x \in Z}\ \texttt{(rw)}}{\mathtt{h_4.left\ S} : S \in F \to x \in S}\ \texttt{(intro S)} \qquad [\mathtt{h_6} : S \in F]}{x \in S}$$

- $\mathtt{have\ h_8 := h_4.left;\ \ rw\ [fam\_inter\_def]\ at\ h_8;\ \ apply\ h_8\ S;\ \ exact\ h_6;}$

$S \in G$ の場合にも全く同様である．

3.2.5 Level 5/6: Subset of an intersection

$\vdash A \subseteq \bigcap F \leftrightarrow \forall B \in F.\ A \subseteq B$ を証明せよ．もちろん，初手は `apply Iff.intro` を用いて，ゴールを両方向の含意へと分岐させる．まず，順方向であるが，特に証明に困難な点は無いであろう．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}[\mathtt{h_1} : A \subseteq \bigcap F] \\ \hline\hline \mathtt{h_1} : x \in A \to x \in \bigcap F\end{array} \qquad [\mathtt{h_3} : x \in A]}{\mathtt{h_1\ h_3} : x \in \bigcap F}}{\mathtt{h_1\ h_3} : \forall S \in F.\ x \in S}\ \texttt{(rw)}}{\mathtt{h_1\ h_3\ B} : B \in F \to x \in B} \qquad [\mathtt{h_2} : B \in F]}{x \in B}}{x \in A \to x \in B}\ \texttt{(intro h3)}}{A \subseteq B}\ \texttt{(intro x)}}{B \in F \to A \subseteq B}\ \texttt{(intro h2)}}{\forall B \in F.\ A \subseteq B}\ \texttt{(intro B)}}{A \subseteq \bigcap F \to \forall B \in F.\ A \subseteq B}\ \texttt{(intro h1)}$$

- $\mathtt{intro\ h_1;\ \ intro\ B;\ \ intro\ h_2;\ \ intro\ x;\ \ intro\ h_3;}$
  まずは何も考えずにゴールを可能な限り書き換え，$x \in B$ まで変更する．
- $\mathtt{have\ h_4 := h_1\ h_3;\ \ rw\ [fam\_inter\_def]\ at\ h_4;\ \ apply\ h_4\ B;\ \ exact\ h_2}$

次に，逆方向の証明である．こちらも特別なアイデアは必要としない．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\dfrac{\dfrac{[\mathtt{h_5} : \forall B \in F.\ A \subseteq B]}{\mathtt{h_5\ S} : S \in F \to A \subseteq S} \qquad [\mathtt{h_7} : S \in F]}{\mathtt{h_5\ S\ h_7} : A \subseteq S} \\ \hline\hline x \in A \to x \in S\end{array} \qquad [\mathtt{h_6} : x \in A]}{x \in S}}{S \in F \to x \in S}\ \texttt{(intro h7)}}{\forall Z \in F.\ x \in Z}\ \texttt{(intro S)}}{x \in \bigcap F}\ \texttt{(rw)}}{x \in A \to x \in \bigcap F}\ \texttt{(intro h6)}}{A \subseteq \bigcap F}\ \texttt{(intro x)}}{\forall B \in F.\ A \subseteq B \to A \subseteq \bigcap F}\ \texttt{(intro h5)}$$

- intro h_5; intro x; intro h_6; rw [fam_inter_def]; intro S; intro h_7;
  まずは愚直にゴールを可能な限り書き換え，$x \in S$ まで変更する．
- have h_8 := h_5 S h_7; apply h_8; exact h_6

3.2.6 Level 6/6: Intersection of a family of unions

$\forall S \in F.\ A \cup S \in G \vdash G \subseteq A \cup \bigcap F$ を証明せよ．ここまでの問題と比較すると，難易度が跳ね上がる．まず，ぱっと見でこれが正しい主張なのかどうかあまり明らかではないし，証明には排中律 $P \vee \neg P$ を用いることが要求されている．排中律 $P \vee \neg P$ を利用するためのコマンドは，by_cases である．by_cases h: P と打ち込むことによって，議論は P の場合と $\neg P$ の場合への場合分けが行われる．

$$\texttt{Goal}:\ Q \quad \rightsquigarrow \quad \frac{P \vee \neg P \qquad \begin{array}{c}[\texttt{h}\colon P]\\ \vdots \\ \texttt{Goal}:\ Q\end{array} \qquad \begin{array}{c}[\texttt{h}\colon \neg P]\\ \vdots \\ \texttt{Goal}:\ Q\end{array}}{\cancel{\texttt{Goal}}:\ Q}\ (\texttt{by\_cases})$$

ともあれ，実際に手を動かしてみないことは始まらない．

$$\cfrac{\cfrac{x \in A \vee x \notin A \qquad \cfrac{[\mathtt{h_2}\colon x \in A]}{x \in A \cup \bigcap F}\ (\texttt{Or.inl}) \qquad \begin{array}{c}[\mathtt{h_2}\colon x \notin A]\\ \vdots \\ x \in A \cup \bigcap F\end{array}}{\cfrac{x \in A \cup \bigcap F}{x \in \bigcap G \to x \in A \cup \bigcap F}\ (\texttt{intro h1})}\ (\texttt{by\_cases})}{\bigcap G \subseteq A \cup \bigcap F}\ (\texttt{intro x})$$

- intro x; intro h_1; by_cases h_2: x∈A; exact Or.inl h_2;
  ゴールを可能な限り変形した後，排中律を用いて，$x \in A$ の場合と $x \notin A$ の場合に分岐する．前者の場合には，手札 $x \in A$ がそのままゴールの左部である．

少し難しいのは，$x \notin A$ の場合である．一旦，愚直にゴールを変形していこう．

$$\cfrac{\cfrac{\cfrac{\cfrac{x \in S}{S \in F \to x \in S}\ (\texttt{intro h3})}{\forall Z \in F.\ x \in Z}\ (\texttt{intro S})}{x \in \bigcap F}\ (\texttt{rw})}{x \in A \cup \bigcap F}\ (\texttt{Or.inr})$$

- apply Or.inr; rw [fam_inter_def]; intro S; intro h_3;

ゴールを変形し尽くしたら，手札を変形して新たな有用な手札を得られないかを探るのがよい．

$$\cfrac{\cfrac{\cfrac{[\mathtt{h_1}\colon x \in \bigcap G]}{\mathtt{h_1}\colon \forall Z \in G.\ x \in Z}\ (\texttt{rw})}{\mathtt{h_4} := \mathtt{h_1}\ (\mathtt{A} \cup \mathtt{S})\colon A \cup S \in G \to x \in A \cup S} \qquad \cfrac{\cfrac{[\mathtt{h}\colon \forall S \in F.\ A \cup S \in G]}{\mathtt{h}\,\mathtt{S}\colon S \in F \to A \cup S \in G} \qquad [\mathtt{h_3}\colon S \in F]}{\mathtt{h_5} := \mathtt{h}\,\mathtt{S}\,\mathtt{h_3}\colon A \cup S \in G}}{\mathtt{h_6} := \mathtt{h_4}\,\mathtt{h_5}\colon x \in A \cup S}$$

- `rw [fam_inter_def] at h1;`　`have h4 := h1 (A∪S);`　`have h5 := h S h3;`
  `have h6 := h4 h5;`

新たに得た手札を利用すれば，ゴールは達成できそうである．

$$\dfrac{[\mathtt{h}_6 : x \in A \cup S] \qquad \dfrac{\dfrac{[\mathtt{h}_2 : x \notin A] \qquad [\mathtt{h}_7 : x \in A]}{\bot}}{x \in S}\ (\texttt{by\_contra}) \qquad [\mathtt{h}_8 : x \in S]}{x \in S}\ (\texttt{cases'})$$

- `cases' h6 with h7 h8;`　`by_contra h9;`　`exact h2 h7;`　`exact h8`
  まず，$x \in A$ と $x \in S$ の場合に分岐する．前者の場合には，背理法を用いて，矛盾 $\bot$ をゴールに変更する．この分岐においては我々は $x \notin A$ と $x \in A$ の両方を仮定しているから，明らかに矛盾が導かれる．後者の場合は，仮定がそのままゴールである．

3.3. Family Union World

3.3.1 Level 1/7: Proving existential statements

$\vdash \exists S.\, S \subseteq A$ を証明せよ．これは以下のように証明できることは容易に分かる．

$$\dfrac{A \subseteq A}{\exists S.\, S \subseteq A}\ (\texttt{Exists.intro})$$

ここで，$A \subseteq A$ は既に第 2.2.5 節で証明しており，この定理には `sub_ref` というラベルが付けられている．したがって，上記の証明は以下のコマンドによって記述できる．

- `apply Exists.intro A;`　`exact sub_ref`

3.3.2 Level 2/7: Subset of family union

$A \in F \vdash A \subseteq \bigcup F$ を証明せよ．これは $\bigcup F$ の定義に立ち返る必要がある．

$$x \in \bigcup F \iff \exists S \in F.\, x \in S \iff \exists S.\, (S \in F \wedge x \in S)$$

愚直にゴールを変形していけば，自ずと証明に辿り着けるだろう．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\mathtt{h}_1 : A \in F] \qquad [\mathtt{h}_2 : x \in A]}{A \in F \wedge x \in A}\ (\texttt{And.intro})}{\exists S.\, (S \in F \wedge x \in S)}\ (\texttt{Exists.intro A})}{\dfrac{\exists S \in F.\, x \in S}{x \in \bigcup F}\ (\texttt{rw})}}{x \in A \to x \in \bigcup F}\ (\texttt{intro h2})}{\forall x\, (x \in A \to x \in \bigcup F)}\ (\texttt{intro x})}{A \subseteq \bigcup F}$$

- `intro x;`　`intro h2;`　`rw [fam_union_def];`
  `apply Exists.intro A;`　`exact And.intro h1 h2`

3.3.3 Level 3/7: Union of larger family is larger

$F \subseteq G \vdash \bigcup F \subseteq \bigcup G$ を証明せよ．まずは無心にゴールを変形していこう．

$$
\cfrac{\cfrac{\cfrac{\exists S \in G.\ x \in S}{x \in \bigcup G}\ \texttt{(rw)}}{x \in \bigcup F \to x \in \bigcup G}\ \texttt{(intro h2)}}{\bigcup F \subseteq \bigcup G}\ \texttt{(intro x)}
$$

- $\texttt{intro x;}\quad \texttt{intro h}_2\texttt{;}\quad \texttt{rw [fam\_union\_def];}$

この時点の手札は $F \subseteq G$ と $x \in \bigcup F$ である．後者の手札は $\exists S \in F.\ x \in S$ を意味するから，この手札を使用して存在の証拠を得るのが良いだろう．この操作でゴールの変更は無い．

$$
\begin{array}{c}
\cfrac{[\texttt{h}_2 : \exists x \in \bigcup F]}{\texttt{h}_2 : \exists S \in F.\ x \in S}\ \texttt{(rw)} \\
\vdots \\
\texttt{Goal}:\ \exists S \in G.\ x \in S
\end{array}
\quad \rightsquigarrow \quad
\cfrac{\cfrac{[\texttt{h}_2 : \exists x \in \bigcup F]}{\texttt{h}_2 : \exists S \in F.\ x \in S}\ \texttt{(rw)} \qquad \begin{array}{c}[\texttt{hB}: B \in F \land x \in B] \\ \vdots \\ \texttt{Goal}:\ \exists S \in G.\ x \in S\end{array}}{\cancel{\texttt{Goal}}:\ \exists S \in G.\ x \in S}\ \texttt{(obtain)}
$$

- $\texttt{rw [fam\_union\_def] at h}_2\texttt{;}\ \texttt{obtain <B,hB> := h}_2\texttt{;}$

残るは，手札を組み合わせるだけである．

$$
\cfrac{\cfrac{\cfrac{[\texttt{h}_1 : F \subseteq G] \qquad \cfrac{[\texttt{hB}: x \in B \land B \in F]}{\texttt{hB.right}: B \in F}}{B \in G} \qquad \cfrac{[\texttt{hB}: x \in B \land B \in F]}{\texttt{hB.left}: x \in B}}{B \in G \land x \in B}\ \texttt{(And.intro)}}{\exists S \in G.\ x \in S}\ \texttt{(Exists.intro)}
$$

- $\texttt{have h}_2 \texttt{ := h}_1 \texttt{ hB.right;}\quad \texttt{have h}_3 \texttt{ := And.intro h}_2 \texttt{ hB.left;}$
  $\texttt{exact Exists.intro B h}_3$