シークエントによる証明の理解と表現
―クリプキ・モデルの性質を利用して―

2013SE132 名倉隆浩
指導教員：佐々木克巳

1 はじめに

本研究の目的は，証明をシークエントの変化としてとらえることで，その証明の理解を深め，その変化を意識した証明を与えることである．対象とした証明は，小野［1］にあるクリプキ・モデルに関連する性質の証明である. 結果として，小野［1］の証明で省略されている道筋を理解でき，その道筋を読み取りやすい証明を与えることができた. 本稿では，2 節でシークエントと証明図を，3 節で論理式とクリプキ・モデルを導入する．4 節では，卒業研究で扱った証明のうちの 1 つに対して実践した結果を示す．

2 シークエントと証明図

この節では，佐々木 [2] に従い, シークエントを導入し，その変化の過程を表す図式（証明図）で証明を表現できることを述べる．

2.1 シークエント

$n+1$ 個の述語 $P, P_1, \cdots, P_n$に対し表現

$$P_1, \cdots, P_n \to P$$

をシークエントという．$(n = 0, 1, 2, \cdots)$.” $P_1 \cdots, P_n$” をこのシークエントの左辺，R を右辺という．$(n = 0$ のとき，左辺は空列 を表す).シークエントの左辺における各文の順番と重複は考えないものとする たとえば，次の 3 つのシークエント

$$P_1, P_2 \to P \qquad P_1, P_2, P_1 \to P \qquad P_2, P_1 \to P$$

はすべて同じとみなす. シークエントの意味は，「左辺に現れる述語から右辺の述語が導かれる」である. 証明の各段階においては，左辺が「使える性質の列」，右辺は「導きたい性質」となる. 必要に応じて限定子（すべて，存在）を含む述語を次のように表す.

すべての x が P をみたす : $\underline{\forall} xP$
P を満たす x が存在する : $\underline{\exists} xP$

2.2 証明図

証明は推論を繰り返し構成される．故に，証明における各推論をシークエントの変化で表現できれば，証明もシークエントの変化で表現できる．たとえば，述語 P から述語 Q を導く推論は，前節で示したシークエントの解釈から

$$\begin{array}{ccc} Q, R_1, \cdots, R_n \to R & & R_1, \cdots, R_n \to P \\ \downarrow & \text{または} & \downarrow \\ P, R_1, \cdots, R_n \to R & & R_1, \cdots, R_n \to Q \end{array}$$

のいずれかで表現できる．以後, n 個のシークエント $S_1 \cdots S_n$からシークエント S への変化を

$$\frac{S_1 \quad \cdots \quad S_n}{S}$$

と表現し，これを推論規則という．各 S_iをこの推論規則の上式，S を下式という.述語 P から述語 Q を導く推論は, 推論規則

$$\frac{Q, R_1, \cdots, R_n \to R}{P, R_1, \cdots, R_n \to R} \text{または} \frac{R_1, \cdots, R_n \to P}{R_1, \cdots R_n \to Q}$$

で表現することができる．

2 つの推論規則$\dfrac{S_2}{S_1}, \dfrac{S_4}{S_3}$の下式 S_1, S_3が別の推理規則 $\dfrac{S_5 \quad S_6}{S}$の上式 S_5, S_6とそれぞれ等しいとき

$$\frac{\dfrac{S_2}{S_1} \qquad \dfrac{S_4}{S_3}}{S}$$

のように上に積み上げることができる．このように推論規則を上のように積み上げていき，すでに正しいと認められたシークエントに到達した図式を証明図という．

3 論理式とクリプキ・モデルの導入

この節では，［1］にしたがい，論理式とクリプキ・モデルを導入する．

3.1 論理式

論理式を定義するのに必要な記号は次の 6 種類である．
(1) 論理結合子　$\wedge, \vee, \supset, \neg$
(2) 量化記号　$\forall, \exists$
(3) 対象変数　$x, y, x, \cdots$
(4) 対象定数　$c, d, \cdots$
(5) 述語記号　$P, Q, \cdots$
(6) 補助記号　$(,), ,$(コンマ)
論理式は次のように定義する．

定義 3.1
(1)P が n 変数の述語記号，$t_1, \cdots, t_n$ が項 (対象変数または対象定数) ならば，$P(t_1, \cdots, t_n)$ は論理式である
(2)A, B がともに論理式ならば，$(A \wedge B), (A \vee B), (A \supset B), (\neg A)$ はいずれも論理式である．
(3)A が論理式で，x が対象変数ならば，$(\forall xA), (\exists xA)$ はともに論理式である．

3.2 クリプキ・モデル

クリプキ・モデルを導入するために，まずクリプキ・フレームを導入する．

定義 3.2　次の条件をみたす三つ組 $(M, \leq, U)$ をクリプキ・フレームという．

(1)$(M,\leq)$ は順序集合
(2)U は，M から空でないある集合 W のベキ集合への写像で次の (2.1)，(2.2) をみたす．
(2.1) 任意の $a \in M$ に対し，$U(a) \neq \varnothing$
(2.2) 任意の $a,b \in M$ に対し，$a \leq b$ ならば $U(a) \subseteq U(b)$

定義 3.3　U の各要素 u に対し$\underline{u}$という対象定数を導入する.また,$\underline{u}$を u の名前とよぶ.

定義 3.4
(1) 与えられたフレーム $(M,\leq,U)$ で言語 l に属するそれぞれの m 変数の述語記号 P の解釈 I を次のように定める．M の各要素 a に対し $I(a)$ が定義され,

$$a \leq b \text{ ならば } P^{I(a)} \subseteq P^{I(b)}$$

(2)I がフレーム $(M,\leq,U)$ 上の解釈のとき，四つ組 $(M,\leq,U,I)$ をクリプキ・モデルという．このモデルに対して,
関係 $\models$ を次のように定義する．
(3.1) $a \models P(\underline{u}_1,\cdots,\underline{u}_m) \Leftrightarrow (u_1,\cdots,u_m) \in P^{I(a)}$
(3.2) $a \models A \wedge B \Leftrightarrow a \models A$ かつ $a \models B$
(3.3) $a \models A \vee B \Leftrightarrow a \models A$ または $a \models B$
(3.4) $a \models A \supset B \Leftrightarrow a \leq b$ となるすべての b に対し $b \not\models A$ または $b \models B$
(3.5) $a \models \neg A \Leftrightarrow a \leq b$ となるすべての b に対し $b \not\models A$
(3.6) $a \models \forall xA \Leftrightarrow a \leq b$ となるすべての b および $U(b)$ の任意の要素 u に対し $b \models A[\underline{u}/x]$
(3.7) $a \models \exists xA \Leftrightarrow U(a)$ のある要素 u に対し $a \models A[\underline{u}/x]$
ここで，$A[c/x]$ は，A における x のすべての自由な出現（$\forall$ と $\exists$ にともなって現れない出現）を a で置き換えて得られる論理式である．たとえば，$(P(x) \wedge \forall xQ(x))[a/x]$ は $P(a) \wedge \forall xQ(x)$ である．また，$\models$ は，I に対して一意に定まるので，$(M,\leq,U,\models)$ のこともクリプキ・モデルという．

4 証明の考察

この節では，特定の論理式のクリプキ・モデルにおける真偽に対して，2 節で示したシークエントの変化を意識した証明を与える. 結果として［1］で省略されている筋道が理解でき，この筋道を読み取りやすい証明を与えることができた.

性質 4.1　クリプキ・モデル $(M,\leq,U,\models)$ を次のように定める.
・$M = \{1,2,3\cdots\}$,
・$\leq$ は自然数の大小関係,
・$m \in M$ に対し $U(m) = \{u_1,u_2,u_3,\cdots,u_m\}$,
・$m \models P(\underline{u}) \Leftrightarrow u \in \{u_1,u_2,\cdots,u_{m-1}\}$,
とする．このとき, $1 \not\models \forall x\neg\neg P(x) \supset \neg\neg\forall xP(x)$ である.
証明図：図 1 に示す.
証明：

$1 \not\models \forall x\neg\neg P(x) \supset \neg\neg\forall xP(x)$ を示すために,(i)$1 \models \forall x\neg\neg P(x)$ と(ii)$1 \not\models \neg\neg\forall xP(x)$ を証明する.
(i)$1 \models \forall x\neg\neg P(x)$，すなわち,$\underline{\forall}k\underline{\forall}u(1 \leq k$ かつ $u \in U(k)$ ならば, $k \models \neg\neg P(\underline{u}))$ を示す. そのために, $1 \leq k$ を満たす任意の k と，$U(k)$ の要素である u_j を任意にとる．$u_j \in U(k)$ より $j \leq k$ である．次に，$k \models \neg\neg P(\underline{u_j})$，すなわち,$\underline{\forall}l(k \leq l$ ならば $l \not\models \neg P(\underline{u_j}))$ を示すために $k \leq l$ となる任意の l をとる．$l \not\models \neg P(\underline{u_j})$ すなわち, $l \leq m$ となるある m で $m \models P(\underline{u_j})$ を示せばよい. m として $l+1$ を代入する．すると,$j \leq k \leq l$ より $j \leq k \leq l+1$ である．さらに, $l+1 \models P(\underline{u_j})$ でもある.
(ii)$1 \not\models \neg\neg\forall xP(x)$,すなわち,$\underline{\exists}k(1 \leq k$ かつ $k \models \neg\forall xP(x))$ を示す．$k = 1$ のとき,$1 \leq k$ かつ $k \models \neg\forall xP(x)$ に代入すると$\underline{\exists}k(1 \leq 1$ かつ $1 \models \neg\forall xP(x))$ となる.すなわち,$1 \leq 1$ かつ $1 \models \neg\forall xP(x)$ を示せばよい．次に，$1 \models \neg\forall xP(x)$ を示すために，$1 \leq k$ を満たす任意の k をとる.$k \not\models \forall xP(x)$，すなわち，$\underline{\exists}l\underline{\exists}u(k \leq l$ かつ $u \in U(l)$ かつ $l \not\models P(\underline{u}))$ を示せばよい. 実際，$k \leq k$ かつ $u_k \in U(k)$ かつ $k \not\models P(\underline{u_k})$ であるから,$l = k, u = u_k$ とすればよい.

$$\dfrac{P_1 \qquad P_2}{\to 1 \not\models \forall x\neg\neg P(x) \supset \neg\neg\forall xP(x)}$$

P_1:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{l+1 \models P(\underline{u_j})}}{\to l \leq l+1 \quad j \leq k \leq l < l+1 \to l+1 \models P(\underline{u_j})}}{j \leq k, k \leq l \to l < l+1 \text{ かつ } l+1 \models (\underline{u_j})}}{j \leq k, k \leq l \to \underline{\exists}m(l \leq m \text{ かつ } m \models P(\underline{u_j}))}}{j \leq k, k \leq l \to l \not\models \neg P(\underline{u_j})}}{j \leq k \to \underline{\forall}l(k \leq l \text{ ならば } l \not\models \neg P(\underline{u_j}))}}{j \leq k \to k \models \neg\neg P(\underline{u_j})}}{1 \leq k, u_j \in U(k) \to k \models \neg\neg P(\underline{u_j})}}{\to \underline{\forall}k\underline{\exists}u(1 \leq k \text{ かつ } u \in U(k) \text{ ならば, } k \models \neg\neg P(\underline{u_j}))}}{\to 1 \models \forall x\neg\neg P(x)}$$

P_2:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{1 \leq k \to k \leq k \text{ かつ } u_k \in U(k) \text{ かつ } k \not\models P(\underline{u_k})}}{1 \leq k \to \underline{\exists}l\underline{\exists}u(k \leq l \text{ かつ } u \in U(l) \text{ かつ } l \not\models P(\underline{u}))}}{1 \leq k \to k \not\models \forall xP(x)}}{\to \underline{\forall}k(1 \leq k \text{ ならば } k \not\models \forall xP(x))} \qquad \to 1 \leq 1 \qquad \to 1 \models \neg\forall xP(x)}{\to \underline{\exists}k(1 \leq k \text{ かつ } k \models \neg\forall xP(x))}}{1 \not\models \neg\neg\forall xP(x)}$$

図 1：性質 4.1 の証明図

参考文献

[1] 小野寛晰：『情報科学における論理』. 日本評論社，東京，1994
[2] 佐々木克巳：『シークエントのよる証明の構想と図式化』, 教職センター紀要，南山大学教職センター，2017, pp.47–50