シークエントを用いた証明分析

—背理法を用いた証明を中心として—

2013SE247 山口 実
指導教員：佐々木 克巳

1 はじめに

本研究の目的は，実際の証明を，シークエントの変化で表現し(結果としてできる図を証明図という)，その本質を理解することである．とくに，背理法を用いた証明を扱う．[2]によれば，背理法を用いて示す命題は次の性質を持っていることが多い．

(i) 証明すべき命題が否定的な命題である．
(ii) 証明すべき命題を否定の形に言い換えることができる．
(iii) 証明すべき命題に「少なくとも 1 つ」が含まれている．

本研究では，これらの性質をもついくつかの命題の，背理法を用いた証明を証明図で表現した．さらに(iii)の 4 つの命題は，場合分けによる証明も証明図で表現し，背理法を用いた証明と比較した．

本稿では，2 節でシークエントと証明図を導入し，3 節では，上の(iii)の性質をもつ命題を対象に，背理法を用いた証明と場合分けの証明を証明図で表現し，両者を比較する．

2 シークエントと証明図

この節では，[1]に従って，シークエントを導入し，さらに，そのシークエントの変化により証明を表現した証明図を導入する．

文$P, P_1, \cdots, P_n$に対して，表現

$$P_1, \cdots, P_n \to P \qquad \text{(S1)}$$

をシークエントという．“$P_1, \cdots, P_n$”をこのシークエントの左辺，Pを右辺という．左辺における各P_iの順番と重複は考えないものとする．例えば

$$P, P, Q \to R$$
$$P, Q \to R$$
$$Q, P \to R$$

はどれも同じシークエントと考える．シークエント(S1)において，各P_iは使える性質，Pは導きたい性質を表す．

証明は推論を繰り返して構成される．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，文Pから文Qを導く推論は，前に示したシークエントの解釈から，

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

のいずれかのシークエントの変化で表現できる．また，背理法の推論は

$$\begin{array}{c} \neg P, R_1, \cdots, R_n \to \bot \\ \Downarrow \\ R_1, \cdots, R_n \to P \end{array}$$

というシークエントの変化で表現できる．ただし，⊥は矛盾を表す．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

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

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．文Pから文Qを導く推論は，2 つの推論規則，

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

のいずれかで表現できる．

ある推論規則$\dfrac{S_2}{S_1}$ (I)の下式S_1が，別の推論規則$\dfrac{S_3 \quad S_4}{S}$ (J)の上式S_3と等しいとき，次のように(J)に(I)を積み上げることができる．

$$\dfrac{\dfrac{S_2}{S_1}\text{(I)} \quad S_4}{S}\text{(J)}$$

この図は，(I)に対応する推論と(J)に対応する推論を続けて行う操作を表している．同様に考えると，証明は，推論規則を上のように積み上げた図式で表現できることになる．推論規則を上のように積み上げてできる図式を証明図という．

証明図を簡潔に表現するために，証明図の各推論規則において，上式の左辺では下式左辺の部分列を“↑”で表してもよいとし，上式右辺と下式右辺が一致する場合，上式右辺を“↓”で表してもよいとする．

3 背理法と場合分け

この節では，「少なくとも 1 つ」を含む命題を対象に，背理法を用いた証明と場合分けの証明を証明図で表現し，両者を比較する．以後，∧, ∨, ¬をそれぞれ，「かつ」，「または」，「でない」を表す記号として用いる．

本研究で対象とする「少なくとも 1 つ」を含む命題とは，

$$P_1 \vee \cdots \vee P_n$$

の形の命題である．本研究では，この命題に対する次の 2 つの形の証明を比較することになる．

(Ⅰ)背理法を用いた証明

$$\dfrac{\dfrac{\dfrac{\vdots}{\neg P_1, \cdots, \neg P_n, \Gamma \to \bot}\mathcal{F}}{\neg(P_1 \vee \cdots \vee P_n), \Gamma \to \bot}}{\Gamma \to P_1 \vee \cdots \vee P_n}\text{(背理法)}$$

ただし, Γは文の列である.

(Ⅱ)場合分けを用いた証明

$$\dfrac{\left.\dfrac{\vdots}{Q_1,\Sigma\to\downarrow}\right\}\mathcal{F}_1 \quad \cdots \quad \left.\dfrac{\vdots}{Q_m,\Sigma\to\downarrow}\right\}\mathcal{F}_m}{\left.\dfrac{\dfrac{Q_1\vee\cdots\vee Q_m,\Sigma\to P_1\vee\cdots\vee P_n}{\vdots}}{\Gamma\to P_1\vee\cdots\vee P_n}\right\}\mathcal{F}_0}\text{(場合分け)}$$

ただし, Γ, Σは文の列である. $Q_1\vee\cdots\vee Q_m$は, ${Q'}_1\vee{R'}_1,\cdots,{Q'}_k\vee{R'}_k$の形になることもあり, その場合の各$Q_i$は, $({Q'}_1\vee{R'}_1)\wedge\cdots\wedge({Q'}_k\vee{R'}_k)$と$Q_1\vee\cdots\vee Q_m$が同値になるように選ばれる.

(Ⅰ), (Ⅱ)を比較した結果として, 少なくとも本研究で扱った 5 つの例では次の性質が成り立つと分かった.

性質 4.1. (Ⅰ)の$\mathcal{F}$と同等な推論が, (Ⅱ)の$\mathcal{F}_0$か, $\mathcal{F}_0$と$\mathcal{F}_1$の組か, …, $\mathcal{F}_0$と$\mathcal{F}_m$の組かのどれかに含まれ, 後者の組$(\mathcal{F}_0,\mathcal{F}_i)$に含まれるときは, $\mathcal{F}_i$で背理法が用いられている.

本研究では, $\mathcal{F}$と同等な推論が$\mathcal{F}_0$に含まれる例を 2 つ挙げ, $\mathcal{F}$が$(\mathcal{F}_0,\mathcal{F}_m)$に含まれる例を 3 つ挙げた. 後者の 3 つでは, $\mathcal{F}_m$で背理法が用いられていることも確認した. 本稿では前者の例のうちの 1 つを示す.

例 3.1.

対象とする命題. 正の整数a,b,c,dが等式$a^2+b^2+c^2=d^2$を満たすとする. a,b,cのなかに, 3 の倍数がちょうど 2 つで, 2 の倍数もちょうど 2 つならば, a,b,cのうち少なくとも 1 つは 6 の倍数である.

証明図Ⅰ(背理法を用いた証明).

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\uparrow,\neg(2|a)\vee\neg(3|a),\neg(2|b)\vee\neg(3|b),\neg(2|c)\vee\neg(3|c)\to\downarrow}\text{(F1) (F2) (F3) (F4) (F5) (F6)}}{\uparrow,\neg(2|a\wedge3|a),\neg(2|b\wedge3|b),\neg(2|c\wedge3|c)\to\downarrow}}{\uparrow,\neg(6|a),\neg(6|b),\neg(6|c)\to\downarrow}}{\uparrow,\neg(6|a\vee6|b\vee6|c)\to\bot}}{\#\,2(a,b,c)=2,\#\,3(a,b,c)=2\to6|a\vee6|b\vee6|c}$$

ただし, $\#\,k(x_1,\cdots,x_n)$は, $i=1,\cdots,n$のうち$k|x_i$を満たすiの個数である. $l|m$は「lはmの約数である」を表す. また, (F1), (F2)は次の通りである.

(F1)

$$\dfrac{\uparrow,\#\,2(a,b,c)\le1\to\downarrow}{\uparrow,\neg(2|a),\neg(2|b)\to\downarrow}$$

(F2)

$$\dfrac{\dfrac{\uparrow,\#\,2(a,b,c)\le1\to\downarrow}{\uparrow,\neg(2|a),\neg(2|c)\to\downarrow}}{\uparrow,\neg(2|a),\neg(3|b),\neg(2|c)\to\downarrow}$$

(F3)～(F6)も同様なので, その一番下のシークエントのみを示す.

(F3) $\uparrow,\neg(2|a),\neg(3|b),\neg(3|c)\to\downarrow$

(F4) $\uparrow,\neg(3|a),\neg(2|b),\neg(2|c)\to\downarrow$

(F5) $\uparrow,\neg(3|a),\neg(2|b),\neg(3|c)\to\downarrow$

(F6) $\uparrow,\neg(3|a),\neg(3|b)\to\downarrow$

証明図Ⅱ(場合分けの証明). 図 1 に示す. ただし,

$$D2=(2|a\wedge2|b\wedge\neg(2|c))\vee(2|a\wedge\neg(2|b)\wedge2|c)\vee(\neg(2|a)\wedge2|b\wedge2|c)$$

$$D3=(3|a\wedge3|b\wedge\neg(3|c))\vee(3|a\wedge\neg(3|b)\wedge3|c)\vee(\neg(3|a)\wedge3|b\wedge3|c)$$

であり, (F7)は次の通りである.

(F7)

$$\dfrac{2|a,3|a\to\downarrow}{(2|a\wedge2|b\wedge\neg(2|c))\wedge(3|a\wedge3|b\wedge\neg(3|c))\to\downarrow}$$

(F8)～(F15)も同様なので, その一番下のシークエントのみを示す.

(F8) $(2|a\wedge\neg(2|b)\wedge2|c)\wedge(3|a\wedge3|b\wedge\neg(3|c))\to\downarrow$

(F9) $(\neg(2|a)\wedge2|b\wedge2|c)\wedge(3|a\wedge3|b\wedge\neg(3|c))\to\downarrow$

(F10) $(2|a\wedge2|b\wedge\neg(2|c))\wedge(3|a\wedge\neg(3|b)\wedge3|c)\to\downarrow$

(F11) $(2|a\wedge\neg(2|b)\wedge2|c)\wedge(3|a\wedge\neg(3|b)\wedge3|c)\to\downarrow$

(F12) $(\neg(2|a)\wedge2|b\wedge2|c)\wedge(3|a\wedge\neg(3|b)\wedge3|c)\to\downarrow$

(F13) $(2|a\wedge2|b\wedge\neg(2|c))\wedge(\neg(3|a)\wedge3|b\wedge3|c)\to\downarrow$

(F14) $(2|a\wedge\neg(2|b)\wedge2|c)\wedge(\neg(3|a)\wedge3|b\wedge3|c)\to\downarrow$

(F15) $(\neg(2|a)\wedge2|b\wedge2|c)\wedge(\neg(3|a)\wedge3|b\wedge3|c)\to\downarrow$

考察. 証明図Ⅰの(F1)～(F6)はあわせて「a,b,cのどれも 6 の倍数でない」場合を対象としている. 一方, 証明図Ⅱの(F7)～(F15)はあわせて「a,b,cのどれかが 6 の倍数である」場合を対象としている. つまり, 証明図Ⅱの(場合分け)までに, 証明図Ⅰの(F1)～(F6)は起こらないこと((F1)～(F6)は矛盾が導かれること)を示していることになる. 言い換えれば, 証明図Ⅱの(場合分け)までに, 証明図Ⅰの下 2 行を除く部分が含まれていることになる. この意味で性質 4.1 が確認できる.

$2|a,2|b,2|c,3|a,3|b,3|c$のそれぞれが成り立つかどうかで$2^6=64$とおりの場合がある. この 64 とおりの場合で上のことを具体的に述べる. 証明図Ⅰは 27 個の場合が矛盾することを示している. 証明図Ⅱは 9 個の場合, つまり$\mathcal{F}$の部分で$2^6\to9$への絞り込みをしている. 証明図Ⅰの 27 個の場合は2^6-9個の場合に含まれており, その絞り込みが$\mathcal{F}$の推論を含むといえる.

参考文献

[1] 佐々木克巳：『2015 年度数理論理学講義資料』, 南山大学, 2015.

[2] 堀場康行：『南山大学院　数理情報研究科　修士論文　推論を適切に選択するための数理的手法』, 南山大学, 2013.

$$\dfrac{\#\,2(a,b,c)=2\to D2 \qquad \dfrac{\#\,3(a,b,c)=2\to D3 \qquad \dfrac{\text{(F7) (F8) (F9) (F10) (F11) (F12) (F13) (F14) (F15)}}{D2,D3\to\downarrow}\text{(場合分け)}}{D2,\#\,3(a,b,c)=2\to\downarrow}}{\#\,2(a,b,c)=2,\#\,3(a,b,c)=2\to6|a\vee6|b\vee6|c}$$

図 1　例 3.1 の証明図Ⅱ(場合分けの証明)