シークエント体系に基づく証明の構成

2011SE089　伊藤　遼
指導教員：佐々木克巳

1　はじめに

3 年次の「情報システム数理演習」でシークエントを用いた形式体系について学び，形式体系の証明図の理解により実際の証明を理解することができることに興味を持った．

本研究の目的は，シークエントを用いた形式体系の証明図と実際の証明を比較することによって，実際の証明を理解することである．具体的には，自然数・実数・関数の性質を対象として，形式体系の証明図と実際の証明をシークエントの変化で表した図式とを考察する．

卒業論文では，8 つの問題に対して，上の考察を行った．本稿ではそのうちの 2 つの問題に対する考察の結果を示す．

以下の 2 節で用いる記号と推論規則を説明し．3 節で考察を行う．

2　シークエント体系

この節では，佐々木 [2] に従い，シークエント体系 SNK を導入する．本研究では，この体系の対象とする領域を実数全体の集合 $\mathbb{R}$ とし，項及び論理式は，以下の言語を用いてふつうの方法で定義する．

- 対象変数：$a, b, c, \cdots, x, y, z$
- 論理記号：$\bot$(矛盾), $\wedge$ (かつ), $\vee$ (または), $\supset$ (ならば),$\neg$(否定), $\forall$(すべての), $\exists$(ある)
- 対象定数：$1, 0, \sqrt{3}, -1, \pi$ など，実数を表すふつうの記号を対象定数としても用いる．
- 関数記号：$+, -, \cdot, /, \sin, \cos$ など，実数の演算を表すふつうの記号を関数記号としても用いる．
- 述語記号:等号 $(=)$，不等号 $(<, \leq, >, \geq)$ をふつうに用いる．さらに表 1 の記号も用いる．問題に応じて追加することもある．

表 1　述語記号

記号	記号の意味
$x \in \mathbb{N}$	x は正の整数である
$x \in \mathbb{Z}$	x は整数である
$x \in \mathbb{Q}$	x は有理数である
$\mathbf{prime}(x)$	x は素数である

シークエントは，

$$\Gamma \ \rightarrow P$$

の形の表現である．Γ をシークエントの左辺，P を右辺という．

SNK 証明図は，次の SNK 公理と SNK 推論規則から [1] の方法で定義する．

SNK 公理:

$$\{P\} \rightarrow P$$
$$\{\} \rightarrow t = t$$

ただし，述語の性質により，明らかなものは適宜，公理に追加することがある．

SNK 推論規則:

$$\frac{\{P, Q\} \cup \Gamma \rightarrow R}{\{P \wedge Q\} \cup \Gamma \rightarrow R}(\wedge左) \qquad \frac{\Gamma \ \rightarrow P \quad \Gamma \ \rightarrow Q}{\Gamma \ \rightarrow P \wedge Q}(\wedge右)$$

$$\frac{\{P\} \cup \Gamma \ \rightarrow R \quad \{Q\} \cup \Gamma \ \rightarrow R}{\{P \vee Q\} \cup \Gamma \ \rightarrow R}(\vee左) \qquad \frac{\Gamma \ \rightarrow P_i}{\Gamma \ \rightarrow P_1 \vee P_2}(\vee右)(i = 1, 2)$$

$$\frac{\Gamma \ \rightarrow P}{\{\neg P\} \cup \Gamma \ \rightarrow \bot}(\neg左) \qquad \frac{\{P\} \cup \Gamma \ \rightarrow \bot}{\Gamma \ \rightarrow \neg P}(\neg右)$$

$$\frac{\{P(t)\} \cup \Gamma \ \rightarrow Q}{\{\forall x P(x)\} \cup \Gamma \ \rightarrow Q}(\forall \text{ 左}) \qquad \frac{\Gamma \ \rightarrow P(z)}{\Gamma \ \rightarrow \forall x P(x)}(\forall \text{ 右})$$

$$\frac{\{P(z)\} \cup \Gamma \ \rightarrow Q}{\{\exists x P(x)\} \cup \Gamma \ \rightarrow Q}(\exists \text{ 左}) \qquad \frac{\Gamma \ \rightarrow P(t)}{\Gamma \ \rightarrow \exists x P(x)}(\exists \text{ 右})$$

$$\frac{\Gamma \ \rightarrow Q}{\{P\} \cup \Gamma \ \rightarrow Q}(w \text{ 左}) \qquad \frac{\{\neg P\} \cup \Gamma \ \rightarrow \bot}{\Gamma \ \rightarrow P}(RAA)$$

$$\frac{\Gamma \ \rightarrow Q \quad \{Q\} \cup \Gamma \ \rightarrow P}{\Gamma \ \rightarrow P}(cut) \qquad \frac{\{s = t\} \cup \Gamma[t/x] \rightarrow P[t/x]}{\{s = t\} \cup \Gamma[s/x] \rightarrow P[s/x]}(\text{代入})$$

$$\frac{\{\neg P \vee \neg Q\} \cup \Gamma \ \rightarrow R}{\{\neg(P \wedge Q)\} \cup \Gamma \ \rightarrow R}(dM) \qquad \frac{\{\forall x P(x)\} \cup \Gamma \ \rightarrow R}{\{\neg \exists x P(x)\} \cup \Gamma \ \rightarrow R}(dM)$$

$$\frac{\{P_2\} \cup \Gamma \rightarrow Q}{\{P_1\} \cup \Gamma \rightarrow Q}(Def) \qquad \frac{\Gamma \rightarrow P_2}{\Gamma \rightarrow P_1}(Def)$$

$$\frac{\Gamma[t/x] \rightarrow P[t/x]}{\Gamma[s/x] \rightarrow P[s/x]}(\text{変形})$$

ただし，(∀ 右)，(∃ 左) における z は，下式 (下のシークエント) に自由に出現しない変数であり，(∀ 左)，(∃ 右) における t は，任意の項である．(代入) における s, t は任意の項で，$P[s/x]$ は，P の x に s を代入したものであり，$\Gamma\ [s/x] = \{P[s/x] | P \in \Gamma\}$ である．(変形) における s, t は任意の項で，t と s がふつうの式変形できる関係にある，とする．(Def) における P_1, P_2 は論理式であり，対象としている理論において，文 P_1 が文 P_2 により定義されている，とする．

3　証明の考察

この節では，[1] から抽出した 2 つの問題に対して，
(1) 問題の記号表現
(2)(1) から直接作成した証明図

(3)[1] に記述されている証明
(4)(3) の証明をシークエントの変化で表現した図式
(5) 考察
の 5 つを示す．ただし，(2) において，(w 左) は適宜省略する．また，$\Gamma \to Q$ が公理として認められているとき，

$$\frac{\Gamma\ \to Q \quad \{Q\} \cup \Gamma\ \to P}{\Gamma\ \to P}(cut)$$

を

$$\frac{\{Q\} \cup \Gamma\ \to P}{\Gamma\ \to P}(cut)$$

と表す．

問題 1．n が 2 以上の整数で，2 の n 乗から 1 引いた数が素数ならば，n も素数である．
※この問題では，記号表現と証明図において，用いる変数はすべて整数と約束する．
(1) 記号表現: $\{n \geq 2 \wedge \mathbf{prime}(2^n - 1)\} \to \mathbf{prime}(n)$
(2) 証明図 ($\exists i(i \neq 1 \wedge i \neq 2^n - 1 \wedge i \mid 2^n - 1)$ を B，$\exists k(k \neq 1 \wedge k \neq n \wedge k \mid n)$ を C，$2^k - 1$ を s，$2^{k(h-1)} + \cdots + (2^k) + 1$ を t とする．)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{k = n\} \to k = n}{\{2^k = 2^n\} \to k = n}\,(\text{変形})}{\{2^k - 1 = 2^n - 1\} \to k = n}\,(\text{変形})}{\{k \neq n, 2^k - 1 = 2^n - 1\} \to \bot}\,(\neg\text{左})}{\{k \neq n\} \to 2^k - 1 \neq 2^n - 1}\,(\neg\text{右}) \quad \dfrac{\dfrac{\{n = kh\} \to 2^n - 1 = 2^{kh} - 1}{\{n = kh\} \to 2^n - 1 = ts}\,(\text{変形})}{\{n = kh\} \to \exists g(2^n - 1 = gs)}\,(\exists\ \text{右})}{\{k \neq 1, k \neq n, n = kh\} \to s \neq 1 \wedge s \neq 2^n - 1 \wedge \exists g(2^n - 1 = gs)}\,(\wedge\text{右})(*1)}{\{k \neq 1, k \neq n, n = kh\} \to B}\,(\exists\ \text{左})}{\{k \neq 1, k \neq n, \exists h(n = kh)\} \to B}\,(\exists\ \text{左}, \wedge\ \text{左}\times\ 2)}{\{n \geq 2, 2^n - 1 > 1, C\} \to B}\,(\neg\text{左}, \neg\text{右})}{\{n \geq 2, 2^n - 1 > 1, \neg B\} \to \neg C}\,(Def, \wedge\ \text{右})(*2)}{\{n \geq 2, 2^n - 1 > 1, \neg B\} \to \mathbf{prime}(n)}\,(Def, \wedge\ \text{左})}{\{n \geq 2 \mathbf{prime}(2^n - 1)\} \to \mathbf{prime}(n)}\,(\wedge\text{左})$$

(∗1)(∧右) の左の上式の証明図は省略する．
(∗2) (∧右) に対して，左の上式の証明図は省略する．
(3) 実際の証明:$2^n - 1$ が素数である場合に n が素数であることを証明するために背理法を利用する．$2^n - 1$ が素数であり，n が素数でないと仮定する．$n = xy(x \geq 2, y \geq 2)$ とおくと，$2^{xy} - 1 = (2^x - 1)\{(2^x)^{y-1} + (2^x)^{y-2} + \cdots + (2^y) + 1\}$ である．$x \geq 2, y \geq 2$ より，$2^x - 1 \geq 3$ かつ，$(2^x)^{y-1} + (2^x)^{y-2} + \cdots + (2^x) + 1 \geq (y-1)2^x + 1 \geq 5$ となる．これは $2^n - 1$ が素数であることに反する．よって n は素数である．
(4) 実際の証明に対する図式:($2^{xy-1} = (2^x - 1)\{(2^x)^{y-1} + \cdots + (2^y) + 1\}$ を D とする)

$$\dfrac{\dfrac{\dfrac{\dfrac{\{D,\ 2^x - 1 \geq 3, (2^x)^{y-1} + \cdots + 1 \geq (y-1)2^x + 1 \geq 5, \mathbf{prime}(2^n - 1)\} \to \bot}{\{D,\ 2^x - 1 \geq 3, n \geq 2, \mathbf{prime}(2^n - 1), x \geq 2, y \geq 2, n = xy\} \to \bot}\,(\text{変形})}{\{D,\ n \geq 2, \mathbf{prime}(2^n - 1), x \geq 2, y \geq 2, n = xy\} \to \bot}\,(cut)}{\{n \geq 2, \mathbf{prime}(2^n - 1), x \geq 2, y \geq 2, n = xy\} \to \bot}\,(\exists\ \text{左}, \wedge\ \text{左})}{\{n \geq 2, \mathbf{prime}(2^n - 1), \exists x \exists y(x \geq 2 \wedge y \geq 2 \wedge n = xy)\} \to \bot}\,(Def,\ dM)$$

(5) 考察: (4) は背理法を使って安全に証明しているが，$(2^x)^{y-1} + \cdots + (2^y) + 1 \geq (y-1)2^x + 1 \geq 5$ に対する式の変形が難しい．一方 (2) では，この変形は必要ないので，(2) の方が分かりやすいと考える．

問題 2．s と t が有理数で $t \neq 0$ ならば，s/t も有理数である．
(1) 記号表現: $\{s \in \mathbb{Q} \wedge t \in \mathbb{Q} \wedge t \neq 0\} \to s/t \in \mathbb{Q}$
(2) 証明図:(“$m \in \mathbb{N}$, $n \in \mathbb{Z}$, $s = n/m$, $g \in \mathbb{N}$, $h \in \mathbb{Z}$, $t = h/g$” を A とする．)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{s = n/m, t = h/g, t \neq 0, h > 0\} \to ng/mh = ng/(mh)}{\{s = n/m.\ t = h/g, t \neq 0, h > 0\} \to s/t = ng/(mh)}\,(\text{代入})}{\{A, t \neq 0, h > 0\} \to mh \in \mathbb{N} \wedge ng \in \mathbb{Z} \wedge s/t = ng/(mh)}\,(\wedge\text{右})(*1)}{\{A, t \neq 0, h > 0\} \to \exists e \exists f(e \in \mathbb{N} \wedge f \in \mathbb{Z} \wedge s/t = f/e)}\,(\exists\ \text{右})}{\{A, t \neq 0, h > 0 \vee h = 0 \vee h < 0\} \to \exists e \exists f(e \in \mathbb{N} \wedge f \in \mathbb{Z} \wedge s/t = f/e)}\,(\vee\text{左}\times\ 2)(*2)}{\{A, t \neq 0\} \to \exists e \exists f(e \in \mathbb{N} \wedge f \in \mathbb{Z} \wedge s/t = f/e)}\,(cut)}{\{A, t \neq 0\} \to s/t \in \mathbb{Q}}\,(Def)}{\{m \in \mathbb{N}, n \in \mathbb{Z}, s = n/m, t \in \mathbb{Q}, t \neq 0\} \to s/t \in \mathbb{Q}}\,(Def, \exists\ \text{左}, \wedge\text{左})}{\{m \in \mathbb{N} \wedge n \in \mathbb{Z} \wedge s = n/m, t \in \mathbb{Q}, t \neq 0\} \to s/t \in \mathbb{Q}}\,(\wedge\text{左})}{\{\exists m \exists n(m \in \mathbb{N} \wedge n \in \mathbb{Z} \wedge s = n/m), t \in \mathbb{Q}, t \neq 0\} \to s/t \in \mathbb{Q}}\,(\exists\ \text{左})}{\{s \in \mathbb{Q}, t \in \mathbb{Q}, t \neq 0\} \to s/t \in \mathbb{Q}}\,(Def)}{\{s \in \mathbb{Q} \wedge t \in \mathbb{Q} \wedge t \neq 0\} \to s/t \in \mathbb{Q}}\,(\wedge\text{左}\times\ 2)$$

(∗1)2 つの (∧右) に対して，左の上式の証明図は省略する．
(∗2)2 つの (∨左) に対して，右の上式の証明図は省略する．
(3) 実際の証明:s，t は有理数なので，$b \neq 0$, $d \neq 0$, $s = a/b$，$t = c/d$ となる整数 a, b, c, d が存在する．このとき，$t \neq 0$ なので $c \neq 0$ である．$p = ad$, $q = bc$ とおくと，これらは整数で $q \neq 0$．これに対して $s/t = (a/b)/(c/d) = ad/bc = p/q$ となり，s/t は有理数である．
(4) 実際の証明に対する図式: (“$p = ad, q = bc, q \neq 0$” を B とする)
※以下の証明図について，整数に関する記述は反映していない．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{B, b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0, s/t = p/q\} \to s/t \in \mathbb{Q}}{\{B, b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0, s/t = (ad)/(bc)\} \to s/t \in \mathbb{Q}}\,(\text{代入})}{\{B, b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0, s/t = (a/b)/(c/d)\} \to s/t \in \mathbb{Q}}\,(\text{変形})}{\{B, b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0\} \to s/t \in \mathbb{Q}}\,(cut)}{\{p = ad, q = bc, b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0\} \to s/t \in \mathbb{Q}}\,()}{\{\exists(p = ad), \exists(q = bc), b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0\} \to s/t \in \mathbb{Q}}\,(\exists\ \text{左})}{\{b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0, c \neq 0\} \to s/t \in \mathbb{Q}}\,(cut)}{\{b \neq 0, d \neq 0, s = a/b, t = c/d, t \neq 0\} \to s/t \in \mathbb{Q}}\,()}{\{b \neq 0 \wedge d \neq 0 \wedge s = a/b \wedge t = c/d, t \neq 0\} \to s/t \in \mathbb{Q}}\,(\wedge\text{左})}{\{\exists a \exists b \exists c \exists d(b \neq 0 \wedge d \neq 0 \wedge s = a/b \wedge t = c/d), t \neq 0\} \to s/t \in \mathbb{Q}}\,(\exists\ \text{左})}{\{s \in \mathbb{Q}, t \in \mathbb{Q}, t \neq 0\} \to s/t \in \mathbb{Q}}\,(Def)}{\{s \in \mathbb{Q} \wedge t \in \mathbb{Q} \wedge t \neq 0\} \to s/t \in \mathbb{Q}}\,(\wedge\text{左}\times 2)$$

(5) 考察: (2) では，s，t に自然数と整数を代入しているが，(4) では，s，t に分数の形を代入しており，その形からは，s/t が有理数であるかはわからないので，(2) のほうがわかりやすいと考える．

参考文献

[1] ダニエル・ソロー :「証明の読み方・考え方 -数学的思考過程への手引き-」，共立出版，(1985)，東京．
[2] 佐々木克巳 :『シークエント体系の証明図から実証明を作る方法』，アカデミア　情報理工学編　第 11 巻　南山大学，pp. 34-55，2011．