2018 年度 数理情報学 6・講義ノート [*†]

木原 貴行
名古屋大学 情報学部・情報学研究科

最終更新日: 2018 年 7 月 5 日

目次

1 **命題論理** 2
1.1 日常における命題論理 . . . 2
1.2 推論とは何か . . . 5
1.3 公理と推論規則 . . . 8
1.4 古典論理法則 . . . 12
1.5 LK の完全性定理 . . . 15
1.6 LK のカット除去定理 . . . 20

2 **計算量と論理** 22
2.1 ブール回路 . . . 22
2.2 計算量クラス NP . . . 26
2.3 一方向関数 . . . 29

3 **一階述語論理** 32
3.1 述語論理とは . . . 32
3.2 構文論 . . . 35
3.3 数学的公理と形式証明* . . . 38
3.4 意味論 . . . 41
3.5 完全性定理 . . . 42

4 **自然数論の形式体系** 49

---

* 本講義ノートは，2018 年度春期開講の名古屋大学情報文化学部 3 年生対象講義「数理情報学 6」の内容をまとめる予定のものである．

† このノートは講義期間中にリアルタイムで更新しており，現時点では未完成なので，あまり拡散しないでください．講義のページ： http://www.math.mi.i.nagoya-u.ac.jp/~kihara/teach.html

4.1 離散順序半環 49
4.2 Σ_1-完全性 52
4.3 $\mathbb{Z}$-環と開帰納法 55
4.4 超準モデルの順序型 59

5 **原始再帰関数** 61
5.1 原始再帰法 62
5.2 初等関数とグジェゴルチク階層 64
5.3 有界原始再帰と多項式時間計算* 68

1 命題論理

1.1 日常における命題論理

1.1.1 論理パズルと真理値表

この街には，「常に正しいことしか言わない正直者」か「常に嘘しか言わない嘘付き」のどちらかしか存在しない．そんな生き辛い人たちが過ごす街で，住人の A, B, C, D は次のような発言をしている．

A 「C さんは嘘つきだぞ〜」
B 「いやいや，私も C さんも正直者だ」
C 「A か B の少なくとも一方は嘘つきだと知っているが，D さんは正直者だ」
D 「信用してくれてありがとう．でも A か B の少なくとも一方は正直者だよ」

さて，このうちの誰が正直者で誰が嘘つきだろうか．この問題を記号論理学的に分析してみよう．記号 H_X によって「X さんが正直である」を意味することとする．まず，A の発言には 2 つの可能性がある：A が正直者かつ C が嘘つきである，または A が嘘つきかつ C が正直者である．これは記号的に次のように記述される．

$$(H_A \wedge \neg H_C) \vee (\neg H_A \wedge H_C). \tag{1}$$

同様にして，B, C, D の発言から，次の情報を得られる．

$$(H_B \wedge (H_B \wedge H_C)) \vee (\neg H_B \wedge \neg(H_B \wedge H_C)), \tag{2}$$
$$(H_C \wedge (\neg H_A \vee \neg H_B) \wedge H_D) \vee (\neg H_C \wedge \neg(\neg H_A \vee \neg H_B) \wedge H_D)), \tag{3}$$
$$(H_D \wedge (H_A \vee H_B)) \vee (\neg H_D \wedge \neg(H_A \vee H_B)). \tag{4}$$

A, B, C, D のうち誰が正直者で誰が嘘つきか，ということは H_A, H_B, H_C, H_D の**真理値** (*truth value*) がどうなっているかに対応する．さて，命題論理式 (1), (2), (3), (4) の真理値は全て「真」であるはずである．したがって，この嘘つきパズルを解くためには，H_A, H_B, H_C, H_D の真理値をそれぞれ真・偽のいずれにすれば，(1), (2), (3), (4) の全てを真にできるかを考えればよい．このための最も素朴な方法は，真理値表を書くことである．

H_A	H_B	H_C	H_D	(1)	(2)	(3)	(4)	H_A	H_B	H_C	H_D	(1)	(2)	(3)	(4)
真	真	真	真	偽	真	偽	真	偽	真	真	真	**真**	**真**	**真**	**真**
真	真	真	偽	偽	真	偽	偽	偽	真	真	偽	真	真	偽	偽
真	真	偽	真	真	偽	真	真	偽	真	偽	真	偽	偽	偽	真
真	真	偽	偽	真	偽	真	偽	偽	真	偽	偽	偽	偽	真	偽
真	偽	真	真	偽	真	真	真	偽	偽	真	真	真	真	真	偽
真	偽	真	偽	偽	真	偽	偽	偽	偽	真	偽	真	真	偽	真
真	偽	偽	真	真	真	偽	真	偽	偽	偽	真	偽	真	偽	偽
真	偽	偽	偽	真	真	真	偽	偽	偽	偽	偽	偽	真	真	真

実際に真理値表を書いてみると，(1), (2), (3), (4) の全てが真になるような真理値の割り当ては，$H_A =$ 偽, $H_B =$ 真, $H_C =$ 真, $H_D =$ 真しか存在しない．つまり，A が嘘つきで，B, C, D は正直者であった．

しかし，嘘つきパズルの登場人物が 4 人だと $2^4 = 16$ 通りの真理値のチェックが必要で，それなりの労力が要る．また，登場人物が増えるに伴い，真理値表のサイズは指数的に大きくなるだろう．多くの人は上記のような嘘つきパズルを解く際，真理値表の全てのマスを埋めるという手間の掛かることをせず，もう少し効率の良い推論をしていると思われる．

演習問題 1.1. 上記の嘘つきパズルを解こうと試みたとき，本当に真理値表を全て埋めようとしただろうか．自分がどのような方法で嘘つきパズルを解こうと試みたかについて論理的に説明せよ．

1.1.2 数独と充足可能性問題

世の中の様々なパズルは，命題論理の問題と考えることができる．その代表例が**数独**である．数独は 9×9 行列 $B = (b_{ij})_{i,j<9}$ の各成分 b_{ij} に 1〜9 の数字を代入するパズルである．

$$B = \left(\begin{array}{ccc|ccc|ccc} b_{00} & b_{01} & b_{02} & b_{03} & b_{04} & b_{05} & b_{06} & b_{07} & b_{08} \\ b_{10} & b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ b_{20} & b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} & b_{27} & b_{28} \\ \hline b_{30} & b_{31} & b_{32} & b_{33} & b_{34} & b_{35} & b_{36} & b_{37} & b_{38} \\ b_{40} & b_{41} & b_{42} & b_{43} & b_{44} & b_{45} & b_{46} & b_{47} & b_{48} \\ b_{50} & b_{51} & b_{52} & b_{53} & b_{54} & b_{55} & b_{56} & b_{57} & b_{58} \\ \hline b_{60} & b_{61} & b_{62} & b_{63} & b_{64} & b_{65} & b_{66} & b_{67} & b_{68} \\ b_{70} & b_{71} & b_{72} & b_{73} & b_{74} & b_{75} & b_{76} & b_{77} & b_{78} \\ b_{80} & b_{81} & b_{82} & b_{83} & b_{84} & b_{85} & b_{86} & b_{87} & b_{88} \end{array}\right)$$

この 9×9 行列 B は，3×3 サイズのブロック $B_{ab} = (b_{3a+i,3b+j})_{i,j<3}$ の 9 つの成分 $(B_{ab})_{a,b<3}$ から構成されていると考える．つまり，行列 B は以下のように表すことができる．

$$B = \begin{pmatrix} B_{00} & B_{01} & B_{02} \\ B_{10} & B_{11} & B_{12} \\ B_{20} & B_{21} & B_{22} \end{pmatrix}, \qquad B_{ab} = \begin{pmatrix} b_{3a,3b} & b_{3a,3b+1} & b_{3a,3b+2} \\ b_{3a+1,3b} & b_{3a+1,3b+1} & b_{3a+1,3b+2} \\ b_{3a+2,3b} & b_{3a+2,3b+1} & b_{3a+2,3b+2} \end{pmatrix}.$$

数字は次の条件を満たすように埋める必要がある．

$$\text{各 } b_{ij} \text{ には } 1\sim9 \text{ の数字のいずれかを代入する．} \tag{5}$$
$$B \text{ の各行に同じ数字が出現してはならない．} \tag{6}$$
$$B \text{ の各列に同じ数字が出現してはならない．} \tag{7}$$
$$B_{ab} \text{ 内に同じ数字が出現してはならない．} \tag{8}$$

このルールを記号論理学的に記述してみよう．記号として，$b_{ij;k}$ を「b_{ij} に数 k を代入した」ことを表すこととする．この記号を用いると，数独のルールは以下の命題論理式として記述できる．

$$(5)\quad \bigwedge_{i,j<9}\bigvee_{1\leqslant k\leqslant 9} b_{ij;k} \qquad (6)\quad \bigwedge_{i<9}\bigwedge_{1\leqslant k\leqslant 9}\bigwedge_{s\neq t}(\neg b_{is;k}\vee\neg b_{it;k}) \qquad (7)\quad \bigwedge_{j<9}\bigwedge_{1\leqslant k\leqslant 9}\bigwedge_{s\neq t}(\neg b_{sj;k}\vee\neg b_{tj;k})$$

$$(8)\quad \bigwedge_{a,b<3}\bigwedge_{1\leqslant k\leqslant 9}\bigwedge_{\substack{i,i',j,j'<3\\(i,j)\neq(i',j')}}(\neg b_{3a+i,3b+j;k}\vee\neg b_{3a+i',3b+j';k})$$

また，数独では最初に行列 B の幾つかの要素の数字が既に埋められている．たとえば，以下のような様子である．

$$B=\left[\begin{array}{ccc|ccc|ccc}
b_{00} & b_{01} & b_{02} & b_{03} & \mathbf{8} & b_{05} & \mathbf{3} & b_{07} & b_{08}\\
b_{10} & b_{11} & \mathbf{2} & b_{13} & \mathbf{3} & b_{15} & b_{16} & \mathbf{8} & b_{18}\\
\mathbf{7} & b_{21} & b_{22} & b_{23} & b_{24} & \mathbf{6} & b_{26} & b_{27} & b_{28}\\
\hline
b_{30} & \mathbf{4} & b_{32} & \mathbf{5} & b_{34} & b_{35} & b_{36} & b_{37} & \mathbf{2}\\
\mathbf{6} & b_{41} & b_{42} & \mathbf{3} & b_{44} & b_{45} & b_{46} & b_{47} & b_{48}\\
b_{50} & b_{51} & b_{52} & b_{53} & b_{54} & \mathbf{9} & \mathbf{4} & b_{57} & b_{58}\\
\hline
b_{60} & b_{61} & b_{62} & b_{63} & b_{64} & b_{65} & \mathbf{9} & b_{67} & \mathbf{4}\\
b_{70} & \mathbf{2} & b_{72} & b_{73} & b_{74} & \mathbf{1} & b_{76} & \mathbf{6} & b_{78}\\
\mathbf{5} & b_{81} & \mathbf{8} & b_{83} & b_{84} & b_{85} & b_{86} & b_{87} & b_{88}
\end{array}\right]$$

上の状況は，以下の論理式によって記述される．

$$\begin{aligned}&b_{04;8}\wedge b_{06;3}\wedge b_{12;2}\wedge b_{14;3}\wedge b_{17;8}\wedge b_{20;7}\wedge b_{25;6}\wedge b_{31;4}\wedge b_{33;5}\wedge b_{38;2}\wedge b_{40;6}\\&\wedge b_{43;3}\wedge b_{55;9}\wedge b_{56;4}\wedge b_{66;9}\wedge b_{68;4}\wedge b_{71;2}\wedge b_{75;1}\wedge b_{77;6}\wedge b_{80;5}\wedge b_{82;8}\end{aligned} \tag{9}$$

各 $b_{ij;k}$ を命題変数と考えよう．上によって与えられた数独の問題を解く，ということは，次の命題論理式

$$(5)\wedge(6)\wedge(7)\wedge(8)\wedge(9)$$

を真にするような命題変数 ($b_{ij;k}$) への真理値の割り当て（付値）が存在するか，という命題論理の問題に他ならない．

嘘つきパズルや数独のように，与えられた命題論理式を真にするような付値が存在するかを尋ねる問題は**充足可能性問題** (*satisfiability problem*) と呼ばれる．数独を始めとする様々なパズルだけでなく，実用的に重要な数多くの問題を充足可能性問題として表すことができる．一般の充足可能性問題を解くのは非常に難しそうであること（NP 完全）が知られているが，現実に遭遇する具体的な充足可能性問題は高速に解けることが非常に多いようである．このため，充足可能性問題はコンピュータ科学では大きなトピックの 1 つとなっており，**SAT ソルバ** (*SAT solver*) などは深く研究されている．

1.2 推論とは何か

1.2.1 命題論理式

本稿では最初に**古典命題論理** (*classical propositional logic*) というものを学ぶ．命題論理を語るには，命題とは何かということを考えなければならない．まず，命題の最も基本的な構成要素は**命題変数** (*propositional variable*) と呼ばれるものである．たとえば第 1.1.1 では「X さんは正直である」ということを H_X と書き，第 1.1.2 では「数独問題 B の i 行 j 列目に数 k を記入した」ということを $b_{ij;k}$ と書いた．これらの記号 P, H_X, $b_{ij;k}$ が命題変数の例である．命題論理式とは，命題変数と論理結合子から構成される記号列である．正確には，以下のように定義される．

定義 1.2. 命題論理式 (*propositional formula*) とは，以下のように帰納的に定義される．

1. 命題変数は命題論理式である．
2. A, B が命題論理式ならば，以下はいずれも命題論理式である．

$$A \to B, \qquad A \wedge B, \qquad A \vee B, \qquad \neg A.$$

1.2.2 推件計算

命題論理の形式証明体系として，ここでは**推件計算** (*sequent calculus*) の体系 LK を解説する．推件計算の主役は，命題論理式ではなく，命題論理式たちを集めてきた推件式と呼ばれるものである．**推件式** (*sequent*) とは，論理式の列 $(A_i)_{i<m}$ と $(B_j)_{j<n}$ に対する次の形の表現を表す．

$$A_0, \ldots, A_m \vdash B_0, \ldots, B_n. \tag{10}$$

この表現が「意図」するものは，

$A_0, \ldots, A_m$ を全て仮定すると，$B_0, \ldots, B_n$ のいずれかを導出できる．

つまり，たとえば $A, B \vdash C, D$ は「(A かつ B) ならば (C または D)」の略記だと考えておくとよい．表記上，平仮名の「かつ, または, ならば」は論理記号 $\wedge, \vee, \to$ と区別されるが，

$$\frac{(A \text{ かつ } B) \text{ ならば } C}{A \wedge B \text{ ならば } C} \qquad \frac{A \text{ ならば } (B \text{ または } C)}{A \text{ ならば } B \vee C} \qquad \frac{A \text{ ならば } B}{\text{ならば } (A \to B)}$$

のように平仮名の論理結合子は記号の論理結合子に置き換えることができる．ここで，上の記法は，上式から下式を推論したことを意味する．推件計算の記法を用いると，これは以下のように書き表せる．

$$\frac{A, B \vdash C}{A \wedge B \vdash C}\ (\wedge \text{ 左}) \qquad \frac{A \vdash B, C}{A \vdash B \vee C}\ (\vee \text{ 右}) \qquad \frac{A \vdash B}{\vdash A \to B}\ (\to \text{ 右}) \tag{11}$$

さて，なぜ単独の論理式を直接取り扱うのではなく，論理式の塊である推件などというものを扱うのか疑問に思うかもしれないが，実際に手を動かして証明図を書く段階になると推件の便利さは

身に染み付いてくる．ちなみに，(11) のうち左 2 つの推論は厳密に言えば，後に述べる ($\wedge$ 左) と ($\vee$ 右) とは少し異なるが，本稿の範囲では気にする必要はない．

後に推件計算における形式的証明の概念を導入するが，一言で言えば「命題論理式 A を証明する」ということは「推件式 $\vdash A$ が最下段に来るような証明図を記述する」ことである．ただし，実際に証明を記述する場合には，証明したい論理式を最下段に配置した後，**下式から上式へ遡ってゆく**と考えたほうがよい．つまり，目的の論理式をスタートとして，証明を逆算するのである．これについては後の節で詳述しよう．

さて，推件計算による証明を定式化するためには，公理と推論規則を導入する必要がある．しかし，いきなり大量の推論規則を羅列してしまうと初学者は怖気づいてしまうかもしれないので，順を追って少しずつ公理と推論規則を導入したい．このために，具体的な命題論理式を例に取って，その証明の流れを丁寧に解説してみよう．

1.2.3 爆発律

「矛盾からは何でも証明できる」ことの証明を例にとって，推論とは何かについて解説しよう．まず，「A を前提にすれば A は証明できる」ということは誰も疑いようなく認めるだろう．これを

$$A \vdash A$$

と書く．また，もし何か A という前提の下で B を証明できるならば，当然 B または C も証明できる．これを以下のように書く．

$$\frac{A \vdash B}{A \vdash B, C}\ (\text{弱化・右})$$

これは**弱化** ($weakening$) の右規則と呼ばれる構造規則である．

つづいて，A という前提の下で B または C を証明できるとする．このとき，さらに $\neg B$ であるという前提が追加されたとしたら，C を証明できるということが確定する．これを否定の左規則と呼び，以下のように書く．

$$\frac{A \vdash B, C}{A, \neg B \vdash C}\ (\neg\ \text{左})$$

いずれの規則も妥当であると納得してもらえるかと思う．これらを用いて，「矛盾からは何でも証明できる」つまり $A, \neg A \vdash B$ は以下のように証明できる．

$$\dfrac{\dfrac{A \vdash A}{A \vdash A, B}\ (\text{弱化・右})}{A, \neg A \vdash B}\ (\neg\ \text{左})$$

ところで推件 $A, \neg A \vdash B$ が意図するものは $(A \wedge \neg A) \to B$ であった．これを証明するには，もう少しのステップが必要である．具体的には，以下の推論を用いればよい．

$$\dfrac{\dfrac{A, \neg A \vdash B}{A \wedge \neg A \vdash B}\ (\wedge\ \text{左})}{\vdash (A \wedge \neg A) \to B}\ (\to\ \text{右})$$

1.2.4 含意記号

つづいて，$A \to B$ が $(\neg A) \vee B$ と同値であるという有名な事実を証明しよう:

$$A \to B \quad \equiv \quad (\neg A) \vee B$$

先に，同値性の一方向である $((\neg A) \vee B) \to (A \to B)$ を証明したい．このために必要な推論規則を述べよう．まず，もし何か A という前提の下で C を証明できるならば，前提をもっと増やしても C を証明できる．これを以下のように書く．

$$\frac{A \vdash C}{A, B \vdash C}\ (\text{弱化・左})$$

これは弱化の左規則と呼ばれる構造規則である．さらに，もし「B を前提にして D を証明できる」かつ「C を前提にして D を証明できる」のであれば，当然「B または C のどちらかが前提にあれば D を証明できる」と結論付けることができるであろう．この推論を次のように表す．

$$\frac{A, B \vdash D \qquad A, C \vdash D}{A, B \vee C \vdash D}\ (\vee \text{左})$$

つづいて，(11) の右端の推論規則を次のように一般化しても差し支えなさそうである．

$$\frac{A, B \vdash C}{A \vdash B \to C}\ (\to \text{右})$$

なぜなら，下式では A を前提として，$B \to C$ を示したいのだが，このために B を仮定すると，上式より C が導かれる．このように，いずれも当然の推論規則のように思うので，これらの推論規則さえ認めてしまえば，以下の証明図を得る．

$$\dfrac{\dfrac{\dfrac{\dfrac{A, \neg A \vdash B \qquad \dfrac{B \vdash B}{A, B \vdash B}\ (\text{弱化・左})}{A, \neg A \vee B \vdash B}\ (\vee \text{左})}{(\neg A) \vee B \vdash A \to B}\ (\to \text{右})}{\vdash ((\neg A) \vee B) \to (A \to B)}\ (\to \text{右})}$$

つづいて，逆方向の含意 $(A \to B) \to ((\neg A) \vee B)$ を証明しよう．まず，$\neg A$ であること，すなわち「A が否定される」ことの意味は，「A を仮定すると矛盾が導かれる」ということである．矛盾を記号 $\bot$ で書き表すこととすれば，これは次を意味する．

$$\neg A \quad \equiv \quad A \to \bot$$

したがって，次の証明図を得る．

$$\dfrac{\dfrac{\dfrac{A \vdash B}{A \vdash \bot, B}\ (\text{弱化・右})}{\vdash A \to \bot, B}\ (\to \text{右})}{\vdash \neg A, B}$$

つまり，$A \vdash B$ を仮定すれば，$\vdash \neg A, B$ を推論することができる．この推論の途中経過を省略したものを否定 $\neg$ の右規則と呼ぶ:

$$\frac{A \vdash B}{\vdash \neg A, B}\ (\neg \text{右})$$

上の証明図がなんとなく目的の式 $(A \to B) \to ((\neg A) \vee B)$ に既に近いことに気づくとは思う．人によっては，この時点でもう納得するかもしれないが，念のため証明を完成させよう．まず，B が証明できるならば，B または C も証明できるのは当然であろう:

$$\frac{A \vdash B}{A \vdash B \vee C}\ (\vee \text{右})$$

もうひとつ必要なものが，次の推論規則である．

$$\frac{\vdash A, C \qquad B \vdash C}{A \to B \vdash C}\ (\to \text{左})$$

まず，上式 $\vdash A, C$ より，A または C が成り立つ．C が成り立っているときは下式が成立するのは当然であるから，A が成り立っているとしよう．下式の前提 $A \to B$ を用いると，B が導かれる．一方，上式 $B \vdash C$ を用いれば C が導かれる．よって，この推論規則は妥当そうである．これらの推論規則を用いることにより，次の証明図を得る．

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{\vdash A, \neg A}\ (\neg \text{右})}{\vdash A, (\neg A) \vee B}\ (\vee \text{右}) \qquad \dfrac{B \vdash B}{B \vdash (\neg A) \vee B}\ (\vee \text{右})}{A \to B \vdash (\neg A) \vee B}\ (\to \text{左})}{\vdash (A \to B) \to ((\neg A) \vee B)}\ (\to \text{右})$$

1.3 公理と推論規則

推件計算の体系 LK は，公理 $A \vdash A$ と弱化のような構造に関する推論規則，各論理記号 $\to, \neg, \wedge, \vee, \neg$ に対する推論規則からなる．以下，ギリシャ文字の大文字 $\Gamma, \Delta, \Theta, \Lambda$ などによって命題論理式の列（空でもよい）を表す．第 1.2 節で述べたように，推件式とは $\Gamma \vdash \Delta$ の形の表現である．まず，構造に関する推論規則から与えよう．

定義 1.3 (構造に関する推論規則)**.** LK の構造に関する推論規則は以下によって与えられる:

$$\frac{\Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\text{弱化・左}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\ (\text{弱化・右})$$

$$\frac{A, A, \Gamma \vdash \Delta}{A, \Gamma \vdash \Delta}\ (\text{縮約・左}) \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\ (\text{縮約・右})$$

$$\frac{\Delta, A, B, \Gamma \vdash \Theta}{\Delta, B, A, \Gamma \vdash \Theta}\ (\text{交換・左}) \qquad \frac{\Gamma \vdash \Delta, A, B, \Lambda}{\Gamma \vdash \Delta, B, A, \Lambda}\ (\text{交換・右})$$

$$\frac{\Gamma \vdash \Theta, A \qquad A, \Delta \vdash \Lambda}{\Gamma, \Delta \vdash \Theta, \Lambda}\ (\text{カット})$$

これらの規則は，上から順に，**弱化** (*weakening*), **縮約** (*contraction*), **交換** (*exchanging*), **カット** (*cut*) と呼ばれる．

カットは，いわゆる**三段論法** (*modus ponens*) のようなものである．実際，Γ と Θ が空列で Λ が単独の論理式 B であるならば，カットとは，A と「A ならば B」という仮定から B を推論できることを意味する．弱化，縮約，交換規則に関しては，しばしば暗黙に用いられているものとして，証明図の中では明示しないことがある．

また，構造に関する推論規則だけでなく，各論理記号に対して左規則と右規則がある．命題論理には 5 種類の論理記号があるから，少なくとも合計 10 個の推論規則が更に加わるということになる．実用的には，具体的な証明図を作るときなどに推論規則が多いことはむしろメリットなのだが，体系自体の理論的側面を調べる際には，規則の多さはネックとなる．このため，まずは LK を少し簡易化したものを導入しよう．

前節で見たように，幾つかの公理と推論規則を仮定すると $A \to B$ は $(\neg A) \vee B$ と同値になる．したがって，

$$A \wedge B \quad \equiv \quad \neg(A \to \neg B) \qquad\qquad A \vee B \quad \equiv \quad (A \to B) \to B \tag{12}$$

が成立することを確認するのは難しくない．また，矛盾を意味する記号 $\bot$ を追加すれば，

$$\neg A \quad \equiv \quad A \to \bot \tag{13}$$

が成り立つから，全ての命題論理式は，命題変数と $\bot$ と $\to$ の組合せで記述された論理式と同値になる．そういうわけで，まずは，記号として命題変数，$\bot, \to$ しか用いない簡易的な命題論理の体系 LK$'$ を議論しよう．

定義 1.4 (公理と推論規則)**.** LK$'$ の公理は次によって与えられる:

$$A \vdash A \qquad\qquad \bot \vdash$$

論理記号 $\to$ に関する推論規則は以下によって与えられる:

$$\frac{\Gamma \vdash \Theta, A \qquad B, \Delta \vdash \Lambda}{A \to B, \Gamma, \Delta \vdash \Theta, \Lambda}\ (\to \text{左}) \qquad \frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}\ (\to \text{右})$$

ここで，定義 1.4 の 2 つめの公理は，矛盾から空列を導く推件式である．形式体系 LK$'$ とは，定

義 1.3 の構造に関する推論規則と定義 1.4 を合わせたものである．そして，記号 $\neg$, $\wedge$, $\vee$ は (12) と (13) によって定義される略記であると考える．

LK′ の**証明図** (*proof figure*) とは，始式から LK′ の推論規則を適用していく様子を図示したものである．より正確には，証明図とは，各ノードが推件式でラベル付けられた有限二分木であり，各ノードの推件式は子ノードの推件式から LK′ の推論規則の適用によって導かれるものである．証明図の木の各葉の推件式を始式と呼び，根の推件式を終式と呼ぶ．

定義 1.5. 推件式 $\Gamma \vdash \Delta$ が LK′ で**証明可能** (*provable*) とは，LK′ の公理を始式として $\Gamma \vdash \Delta$ を終式とする LK′ の証明図が存在することである．命題論理式 A が LK′ で証明可能とは，$\vdash A$ が LK′ で証明可能であることを意味する．

実は，含意記号 $\to$ に関する右規則の上式と下式はひっくり返すことができる．また，左規則についても，前件と後件中の余計な論理式を外せば，上式と下式をひっくり返すことができる．

補題 1.6. LK′ において，以下の派生規則を導くことができる．つまり，以下のそれぞれについて，公理または上式を始式とし下式を終式とするような LK′ の証明図が存在する．

$$\frac{\Gamma \vdash \Delta, A \to B}{A, \Gamma \vdash \Delta, B} \qquad \frac{A \to B, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \qquad \frac{A \to B, \Gamma \vdash \Delta}{B, \Gamma \vdash \Delta}$$

Proof. まず，含意記号 $\to$ の右規則の反転については，以下の証明図を与えられる．

$$\dfrac{\Gamma \vdash \Delta, A \to B \qquad \dfrac{A \vdash A \qquad B \vdash B}{A \to B, A \vdash B}\,(\to \text{左})}{A, \Gamma \vdash \Delta, B}\,(\text{カット})$$

つづいて，含意記号 $\to$ の左規則の反転を示す．まず，中央の式については，以下のように導出できる．

$$\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A, B}\,(\text{弱化・右})}{\vdash A, A \to B}\,(\to \text{右}) \qquad A \to B, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\,(\text{カット})$$

最後に，右の式については，以下のように導出できる．

$$\dfrac{\dfrac{\dfrac{B \vdash B}{A, B \vdash B}\,(\text{弱化・左})}{B \vdash A \to B}\,(\to \text{右}) \qquad A \to B, \Gamma \vdash \Delta}{B, \Gamma \vdash \Delta}\,(\text{カット})$$

以上より，補題は示された． □

LK′ で含意記号 $\to$ 以外の論理結合子をまともに取り扱えることを示しておく必要があるだろう．

定理 1.7. LK′ において，以下の $\neg, \vee, \wedge$ に関する規則を導くことができる．つまり，以下のそれぞれについて，公理または上式を始式とし下式を終式とするような LK′ の証明図が存在する．

$$\frac{\Gamma \vdash \Delta, A}{\neg A, \Gamma \vdash \Delta}\ (\neg \text{左}) \qquad \frac{A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg A}\ (\neg \text{右})$$

$$\frac{A, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}\ (\wedge \text{左}) \qquad \frac{B, \Gamma \vdash \Delta}{A \wedge B, \Gamma \vdash \Delta}\ (\wedge \text{左}) \qquad \frac{\Gamma \vdash \Delta, A \qquad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B}\ (\wedge \text{右})$$

$$\frac{A, \Gamma \vdash \Delta \qquad B, \Gamma \vdash \Delta}{A \vee B, \Gamma \vdash \Delta}\ (\vee \text{左}) \qquad \frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B}\ (\vee \text{右}) \qquad \frac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \vee B}\ (\vee \text{右})$$

Proof. まず，否定 $\neg$ の左規則については，以下のように導出できる．

$$\dfrac{\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\bot \vdash}{\bot \vdash \Delta}\ (\text{弱化・右})}{A \to \bot, \Gamma \vdash \Delta}\ (\to \text{左})}{\neg A, \Gamma \vdash \Delta}$$

ただし，上の証明図の作り方としては，終式に $\neg A, \Gamma \vdash \Delta$ を配置した後，下から上に向かって論理式を徐々に分解していく解体作業と見てほしい．つづいて，否定 $\neg$ の右規則については，第 1.2.4 節で見た方法と同様であるから省略する．以後，否定の規則については自由に利用していいものとしよう．たとえば，否定の規則を用いると，$\wedge$ の左規則について，以下のような証明図が記述できる．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A, \Gamma \vdash \Delta}{A, B, \Gamma \vdash \Delta}\ (\text{弱化・左})}{A, \Gamma \vdash \Delta, \neg B}\ (\neg \text{右})}{\Gamma \vdash \Delta, A \to \neg B}\ (\to \text{右})}{\neg(A \to \neg B), \Gamma \vdash \Delta}\ (\neg \text{左})}{A \wedge B, \Gamma \vdash \Delta}$$

上の証明図についても，下から上に向かって論理式を徐々に分解していく流れである．つづいて，論理積 $\wedge$ の右規則の証明図を記述する．ただし，以後は，縮約などの構造に関する推論規則については，使用が明らかな場合には，以下のように記述を省略する．

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash \Delta, A \qquad \dfrac{\Gamma \vdash \Delta, B}{\neg B, \Gamma \vdash \Delta}\ (\neg \text{左})}{A \to \neg B, \Gamma \vdash \Delta}\ (\to \text{左})}{\Gamma \vdash \Delta, \neg(A \to \neg B)}\ (\neg \text{右})}{\Gamma \vdash \Delta, A \wedge B}$$

上の証明図において，暗黙に縮約規則が使われていることに注意する．つづいて，論理和 $\vee$ の

右規則は以下のように導出できる．

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, B, A}\,(\text{弱化・右}) \qquad B \vdash B}{\dfrac{A \to B, \Gamma \vdash \Delta, B, B}{\dfrac{A \to B, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, (A \to B) \to B}\,(\to \text{右})}\,(\text{縮約・右})}\,(\to \text{左})}{\Gamma \vdash \Delta, A \vee B}$$

ここで，下から上へと流れる解体作業を行う際に，なかなか縮約の右規則の利用は見落としがちなので注意しよう．論理和 $\vee$ の左規則については読者の演習問題とする． □

演習問題 1.8. 規則 ($\vee$ 左) について，公理または上式を始式とし下式を終式とするような LK′ の証明図を記述せよ．

豆知識. 命題論理の形式体系には推件計算の体系以外にも沢山あり，代表的なものがヒルベルト式の体系と自然演繹である．多くには特有のメリットとデメリットがある．推件計算のメリットは証明図を作るのが圧倒的に容易なことである．ヒルベルト式の体系で証明を書くには超人的な能力が必要とされるが，推件計算は誰でも簡単に証明を書けるので実用的で教育的である．また，自然演繹や推件計算の証明図は視覚的に分かりやすく，どういう証明の流れになっているか一目瞭然である．

一方で，理論的には，それぞれの体系に重要性がある．ヒルベルト式は**組合せ論理** (*combinatory logic*) との対応を見ることで，その姿が非常に明瞭となる．同様に，自然演繹にもラムダ計算との対応があり，これらはいわゆる**カリー-ハワード同型対応** (*Curry-Howard correspondence*) と呼ばれるものである．推件計算の難点として，このような計算との対応が少しばかり不明瞭になるという部分を指摘できる[*1]．しかし，その一方で，推件計算は構造と論理結合子に対する推論規則が分離しているために論理自体の分析がしやすく，**部分構造論理** (*substructural logic*) の研究などでは主役として活躍している．

1.4 古典論理法則

定義 1.9. 推件計算の形式体系 LK とは，公理 $A \vdash A$ と構造に関する推論規則 (定義 1.3), および論理結合子 $\to, \neg, \wedge, \vee$ に関する推論規則 (定義 1.4 および定理 1.7) からなるものである．

注意. 定理 1.7 より，LK で証明可能な命題論理式は LK′ で証明可能である．

LK における証明に慣れ親しむためには，いくつかの論理法則の証明図を記述してみるのがよい．まずは，古典論理において，ある命題とその**対偶** (*contraposition*) が同値であることの証明を与えてみよう．

[*1] 推件計算も $\overline{\lambda}\mu\tilde{\mu}$-計算とは明確な対応があるとの情報を佐藤雅大さんから頂きました．

命題 1.10. ある命題とその対偶の同値性 $(A \to B) \leftrightarrow (\neg B \to \neg A)$ は LK で証明可能である．

Proof. ここでは $(\neg B \to \neg A) \to (A \to B)$ の証明を与えよう．

$$\dfrac{\dfrac{\dfrac{\dfrac{B \vdash B}{\vdash \neg B, B}\,(\neg\ \text{右}) \qquad \dfrac{A \vdash A}{A, \neg A \vdash}\,(\neg\ \text{左})}{A, \neg B \to \neg A \vdash B}\,(\to\ \text{左})}{\neg B \to \neg A \vdash A \to B}\,(\to\ \text{右})}{\vdash (\neg B \to \neg A) \to (A \to B)}\,(\to\ \text{右})$$

逆向きの含意については読者の演習問題とする． □

演習問題 1.11. $(\neg B \to \neg A) \to (A \to B)$ を証明せよ．

演習問題 1.12. 二重否定除去の法則 $\neg\neg A \leftrightarrow A$ を証明せよ．

他に有名な古典論理法則の代表例として，**ド・モルガンの法則** (*de Morgan's law*) がある．これは論理和 $\vee$ と論理積 $\wedge$ の双対性を述べる法則である．

$$\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B) \qquad\qquad \neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B).$$

実際に，LK でド・モルガンの法則を証明してみよう．

命題 1.13. ド・モルガンの法則 $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$ は LK で証明可能である．

Proof. まず，$\neg(A \wedge B) \to (\neg A \vee \neg B)$ の証明図は以下によって与えられる．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A \qquad B \vdash B}{A, B \vdash A \wedge B}\,(\wedge\ \text{右})}{\vdash A \wedge B, \neg A, \neg B}\,(\neg\ \text{右})}{\vdash A \wedge B, \neg A \vee \neg B}\,(\vee\ \text{右})}{\neg(A \wedge B) \vdash \neg A \vee \neg B}\,(\neg\ \text{左})}{\vdash \neg(A \wedge B) \to (\neg A \vee \neg B)}\,(\to\ \text{右})$$

つづいて，$(\neg A \vee \neg B) \to \neg(A \wedge B)$ の証明図は以下によって与えられる．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A, \neg A \vdash}\,(\neg\ \text{左}) \qquad \dfrac{B \vdash B}{B, \neg B \vdash}\,(\neg\ \text{左})}{A, B, \neg A \vee \neg B \vdash}\,(\vee\ \text{左})}{A \wedge B, \neg A \vee \neg B \vdash}\,(\wedge\ \text{左})}{\neg A \vee \neg B \vdash \neg(A \wedge B)}\,(\neg\ \text{右})}{\vdash (\neg A \vee \neg B) \to \neg(A \wedge B)}\,(\to\ \text{右})$$

□

演習問題 1.14. ド・モルガンの法則 $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$ を証明せよ.

次は，**分配律** (*distributive law*) を証明するが，形式的に証明すると意外とややこしいので，ここまででどれだけ鍛えられたかの実力試しになるだろう.

命題 1.15. 分配律 $A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$ は LK で証明可能である.

Proof. まず，$A \vee (B \wedge C) \to (A \vee B) \wedge (A \vee C)$ の証明は以下によって与えられる.

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A \vee B}\,(\vee\text{右}) \quad \dfrac{\dfrac{B \vdash B}{B \vdash A \vee B}\,(\vee\text{右})}{B \wedge C \vdash A \vee B}\,(\wedge\text{左})}{A \vee (B \wedge C) \vdash A \vee B}\,(\vee\text{左}) \quad \dfrac{\dfrac{A \vdash A}{A \vdash A \vee C}\,(\vee\text{右}) \quad \dfrac{\dfrac{C \vdash C}{C \vdash A \vee C}\,(\vee\text{右})}{B \wedge C \vdash A \vee C}\,(\wedge\text{左})}{A \vee (B \wedge C) \vdash A \vee C}\,(\vee\text{左})}{A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C)}\,(\wedge\text{右})}{\vdash A \vee (B \wedge C) \to (A \vee B) \wedge (A \vee C)}\,(\to\text{右})$$

つづいて，$(A \vee B) \wedge (A \vee C) \to A \vee (B \wedge C)$ の証明は以下によって与えられる.

$$\dfrac{\dfrac{\dfrac{\dfrac{A \vdash A}{A, A \vee C \vdash A}\,(\text{弱化})}{A, A \vee C \vdash A \vee (B \wedge C)}\,(\vee\text{右}) \quad \dfrac{\dfrac{\dfrac{A \vdash A}{B, A \vdash A}\,(\text{弱化})}{B, A \vdash A \vee (B \wedge C)}\,(\vee\text{右}) \quad \dfrac{\dfrac{\dfrac{B \vdash B}{B, C \vdash B}\,(\text{弱化}) \quad \dfrac{C \vdash C}{B, C \vdash C}\,(\text{弱化})}{B, C \vdash B \wedge C}\,(\wedge\text{右})}{B, C \vdash A \vee (B \wedge C)}\,(\vee\text{右})}{B, A \vee C \vdash A \vee (B \wedge C)}\,(\vee\text{左})}{A \vee B, A \vee C \vdash A \vee (B \wedge C)}\,(\wedge\text{左，縮約})}{(A \vee B) \wedge (A \vee C) \vdash A \vee (B \wedge C)}\,(\to\text{右})}{\vdash (A \vee B) \wedge (A \vee C) \to A \vee (B \wedge C)}$$

□

演習問題 1.16. $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$ を証明せよ.

以上の法則を用いて，LK と LK′ は同値であり，どちらを使うも自由であることを確認しよう.

系 1.17. LK と LK′ は同値である.

Proof. 先に述べたように，定理 1.7 より，LK で証明可能な命題論理式は LK′ で証明可能である. 逆に，第 1.2 節の議論から，LK において $A \to B$ と $\neg A \vee B$ の同値性を証明することができる. これを利用すると，ド・モルガンの法則と二重否定除去を用いて，$\wedge$ および $\vee$ は式 (13) のように特徴づけられることを LK で証明できる. したがって，LK′ で証明可能な命題論理式は LK で証明可能である. □

命題変数 p に対して，p または $\neg p$ の形の命題論理式を**リテラル** (*literal*) と呼ぶ. ここで，$\neg\neg p$ などはリテラルではない. L_{ij} がリテラルであるとき，$\bigwedge_i \bigvee_j L_{ij}$ の形の命題論理式を**連言標準形** (*conjunctive normal form*) と呼ぶ.

例 1.18. $(p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (q \vee r)$ は連言標準形である．$(\neg(p \to q)) \wedge (q \vee r)$ や $(\neg\neg p) \vee q$ などは連言標準形ではない．第 1.1.2 節の数独の命題論理式による表現は，連言標準形である．

定理 1.19. 任意の命題論理式は，ある連言標準形と同値である．

Proof. 命題論理式 A が与えられているとする．次の手続きで，A を連言標準形に変形する．

Step 1. まず，A に現れる含意記号 $\to$ を全て取り除く．

このために，まず，A に現れる $B \to C$ という形の論理式を見る．第 1.2.4 節より，$B \to C$ を $\neg B \vee C$ に置き換えても A と同値である．このようにして，A に現れる $\to$ を全て取り除くことができる．

Step 2. A に現れる否定記号が命題変数の直後にしか現れないようにする．

このために, A に現れる $\neg D$ の形の論理式を見る．もし D が命題変数でないとすると, $D \equiv \neg E$, $D \equiv E \wedge F$, $D \equiv E \vee F$ のいずれかの形である．

1. $D \equiv \neg E$ のときは，二重否定除去 (演習問題 1.12) より，$\neg D$ の部分を E に置き換えてよい．
2. $D \equiv E \wedge F$ のときは，ド・モルガンの法則 (命題 1.13) より，$\neg D$ の部分を $\neg E \vee \neg F$ に置き換えてよい．
3. $D \equiv E \vee F$ のときは，ド・モルガンの法則 (演習問題 1.14) より，$\neg D$ の部分を $\neg E \wedge \neg F$ に置き換えてよい．

このようにして，否定 $\neg$ が必ず $\wedge$ や $\vee$ の内側に現れるようにできる．

Step 3. 論理積 $\wedge$ を論理和 $\vee$ より外に出す．

もし $\wedge$ が $\vee$ の内側に現れていた場合，つまり $L \vee (M \wedge N)$ のような式が現れた場合，分配律 (命題 1.15) を用いて，$(L \vee M) \wedge (L \vee N)$ に置き換えることができる．以上の手続きによって，A と同値な連言標準形の論理式を得ることができる． □

1.5 LK の完全性定理

これまで，命題論理の形式体系における証明概念を取り扱ってきた．しかし，あるシステムを用いて何らかの命題を証明したとしても，そのシステムにバグがあったとしたらどうだろう．バグのあるシステムによる証明は，命題の正しさの保証になりそうもない．この感覚は，「形式体系による証明」と「命題の真偽」は一致しない可能性があることを示唆している．つまり，命題の真偽概念は，証明可能性概念と全く独立に存在している．

それでは，そもそも命題の真偽とは一体どういう意味であるか，という点について考察しよう．しばしば命題とは，真偽の定まった主張のことだと言われることがある．一方，我々の定義 1.2 では，命題論理式とはあくまで記号列であって，アプリオリに真偽が定まっているものではなかった．とはいえ，定義 1.2 の意味での命題論理式にも，自然に真偽を割り当てることができる．まず，命題論理式 A の真偽は，A に含まれる命題変数の真偽が決まって，はじめて定まる．このような命題変数への真理値割り当てのことを付値と呼ぶ．以下，Var を命題変数の集合とする．

定義 1.20. 付値 (*assignment*) とは関数 $v : \mathrm{Var} \to \{\, 真, 偽 \,\}$ である．このとき，以下のようにして，付値は帰納的に任意の命題論理式に拡張される．

$$\begin{aligned} v(\neg A) = 真 &\iff v(A) = 偽 \\ v(A \wedge B) = 真 &\iff v(A) = v(B) = 真 \\ v(A \vee B) = 真 &\iff v(A) = 真 \text{ または } v(B) = 真 \\ v(A \to B) = 真 &\iff v(A) \leqslant v(B) \end{aligned}$$

ここで，偽 $\leqslant$ 真という順序が入っているものとする．つまり，$A \to B$ が真であるということは，A が成り立つ場合には常に B も成り立つ，つまり「A よりも B の方が尤もらしい」ということである．ここでは真と偽の 2 値しかないので，以下が成立する．

$$v(A \to B) = 真 \iff v(A) \leqslant v(B) \iff v(A) = 偽 \text{ または } v(B) = 真.$$

命題論理式 A が**恒真**または**トートロジー** (*tautology*) であるとは，任意の付値 v に対して $v(A) =$ 真であることを意味する．一般に推件式 $A_0, \ldots, A_m \vdash B_0, \ldots, B_n$ が恒真であるというのは，次の命題論理式

$$\bigwedge_{i \leqslant m} A_i \to \bigvee_{j \leqslant n} B_j$$

が恒真であるということとして定義される．

あるシステムが信用に値する，すなわち証明可能なものが全て恒真である，という性質は**健全性** (*soundness*) と呼ばれる．まずは命題論理の形式体系 LK が健全であることを示そう．

> **定理 1.21** (命題論理の体系 LK の健全性定理)**.** LK は健全である．つまり，任意の推件式 $\Gamma \vdash \Delta$ に対して，$\Gamma \vdash \Delta$ が証明可能ならば $\Gamma \vdash \Delta$ は恒真である．

Proof. 系 1.17 より LK と LK′ は同値であるから，定理の証明のためには，以下を確認すればよい．

1. LK′ の公理は恒真である．
2. LK′ の各推論規則について，上式が恒真ならば下式も恒真である．

まず，公理 $A \vdash A$ の恒真性については明らかである．公理 $\bot \vdash A$ については，任意の付値 v について $v(\bot)$ は偽であるから，$v(\bot \vdash A)$ は真である．また，構造に関する推論規則について，上

式が恒真ならば下式も恒真であることは明らかであろう．よって，含意記号 $\to$ の左および右規則について (2) を示せばよい．

[$\to$ **右**] 記号の簡易化のために，$\gamma = \bigwedge \Gamma$ および $\delta = \bigvee \Delta$ とおく．含意 $\to$ の右規則（以下の左の図式）に対しては，以下の右の図式を検証すればよい．

$$\frac{A, \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \to B}\ (\to \text{右}) \qquad\qquad \frac{A \wedge \gamma \to \delta \vee B \ \text{は恒真}}{\gamma \to [\delta \vee (A \to B)] \ \text{は恒真}}$$

つまり，上式 $A \wedge \gamma \to \delta \vee B$ の恒真性を仮定して，下式 $\gamma \to [\delta \vee (A \to B)]$ の恒真性を示したい．これを示すために，v を与えられた付値とする．

- 上式の恒真性より $v(A \wedge \gamma \to \delta \vee B)$ は真である．
- $v(\gamma)$ が真であると仮定して，$v(\delta \vee (A \to B))$ が真であることを示せばよい．

$v(A)$ が真か偽かで場合分けを行う．$v(A)$ が偽の場合は，定義に従って，次のように我々は真理値の計算を行うことができる．

$$\dfrac{\dfrac{v(A) = \text{偽}}{v(A \to B) = \text{真}}}{v(\delta \vee (A \to B)) = \text{真}}$$

$v(A)$ が真の場合は，定義に従って，次のように我々は真理値の計算を行うことができる．

$$\dfrac{\dfrac{\dfrac{v(A) = \text{真} \qquad v(\gamma) = \text{真}}{v(A \wedge \gamma) = \text{真}} \qquad v(A \wedge \gamma \to \delta \vee B) = \text{真}}{v(\delta \vee B) = \text{真}}}{\dfrac{v(\delta) = \text{真}}{v(\delta \vee (A \to B)) = \text{真}} \quad \text{or} \quad \dfrac{\dfrac{v(B) = \text{真}}{v(A \to B) = \text{真}}}{v(\delta \vee (A \to B)) = \text{真}}}$$

[$\to$ **左**] 記号の簡易化のために，$\gamma = \bigwedge \Gamma$, $\delta = \bigwedge \Delta$, $\theta = \bigvee \Theta$, $\lambda = \bigvee \Lambda$ とおく．含意 $\to$ の左規則（以下の左の図式）に対しては，以下の右の図式を検証すればよい．

$$\frac{\Gamma \vdash \Theta, A \qquad B, \Delta \vdash \Lambda}{A \to B, \Gamma, \Delta \vdash \Theta, \Lambda}\ (\to \text{左}) \qquad\qquad \frac{\gamma \to \theta \vee A \ \text{は恒真} \qquad B \wedge \delta \to \lambda \ \text{は恒真}}{(A \to B) \wedge \gamma \wedge \delta \to \theta \vee \lambda \ \text{は恒真}}$$

つまり，上式 $\gamma \to \theta \vee A$ および $B \wedge \delta \to \lambda$ の恒真性を仮定して，下式 $(A \to B) \wedge \gamma \wedge \delta \to \theta \vee \lambda$ の恒真性を示したい．これを示すために，v を与えられた付値とする．

- 上式の恒真性より，$v(\gamma \to \theta \vee A) = \text{真}$，かつ $v(B \wedge \delta \to \lambda) = \text{真}$である．
- $v((A \to B) \wedge \gamma \wedge \delta) = \text{真}$であると仮定して，$v(\theta \vee \lambda) = \text{真}$であることを示す．

$v(A)$ が真か偽かで場合分けを行う．$v(A)$ が偽の場合は，定義に従って，次のように我々は真理

値の計算を行うことができる．

$$\dfrac{\dfrac{v((A \to B) \wedge \gamma \wedge \delta) = \text{真}}{v(\gamma) = \text{真}} \qquad v(\gamma \to \theta \vee A) = \text{真}}{\dfrac{v(A) = \text{偽} \qquad v(\theta \vee A) = \text{真}}{\dfrac{v(\theta) = \text{真}}{v(\theta \vee \lambda) = \text{真}}}}$$

$v(A)$ が真の場合は，定義に従って，次のように我々は真理値の計算を行うことができる．

$$\dfrac{\dfrac{v(A) = \text{真} \qquad \dfrac{v((A \to B) \wedge \gamma \wedge \delta) = \text{真}}{v(A \to B) = \text{真}}}{v(B) = \text{真}} \qquad \dfrac{v((A \to B) \wedge \gamma \wedge \delta) = \text{真}}{v(\delta) = \text{真}}}{\dfrac{v(B \wedge \delta) = \text{真} \qquad v(B \wedge \delta \to \lambda) = \text{真}}{\dfrac{v(\lambda) = \text{真}}{v(\theta \vee \lambda) = \text{真}}}}$$

以上より，定理は示された． □

ある命題論理式が恒真であるかどうかの素朴な確認方法は，全ての付値を確認する，すなわち真理値表を書き上げることである．しかし，命題変数の数に応じて，真理値表のサイズは指数的に膨れ上がるので，現実的ではない．実際，真理値表を書くよりは証明図を書いた方が楽なことはしばしばある．さて，健全性定理より，LK の証明図を書けば，恒真であることが保証されていた．ここで問題となるのは，その逆である．全ての恒真命題は，形式的に証明可能であるだろうか．このような性質を**完全性** (*completeness*) と言う．

定理 1.22 (命題論理の体系 LK の完全性定理)**.** 任意の推件式 $\Gamma \vdash \Delta$ に対して，

$$\Gamma \vdash \Delta\text{は証明可能} \iff \Gamma \vdash \Delta\text{は恒真.}$$

Proof. 主張の対偶，つまり $\Gamma \vdash \Delta$ が証明不可能ならば $\bigwedge \Gamma \to \bigvee \Delta$ を偽にするような付値が存在することを示す．Γ と Δ の中に含まれる含意記号 $\to$ の合計数に関する帰納法によって示そう．

[$\to$ **の数が** 0 **個の場合**]: この場合，Γ と Δ の要素は命題変数または $\bot$ のいずれかである．まず，

観測. $\Gamma \vdash \Delta$ が証明不可能という仮定より，Γ は $\bot$ を含まない．

なぜなら $\bot$ に関する公理と弱化・右より $\bot \vdash \Delta$ であるが，Γ が $\bot$ を含んでいたとすると，弱化・左より $\Gamma \vdash \Delta$ を推論できるからである．次に，

観測. Γ と Δ は共通の命題変数を含まない．

なぜなら，もし共通の命題変数 p を含んでいたとすると，公理より $p \vdash p$ であるが，弱化規則によって $\Gamma \vdash \Delta$ が推論できるからである．

以上 2 つの観測により，Γ の全ての命題変数を真に，Δ の全ての命題変数を偽にする付値が存在する．これは $\bigwedge\Gamma \to \bigvee\Delta$ を偽にする．

[**$\to$ の数が $(n+1)$ 個の場合**]: $\to$ の数が n の場合の完全性定理は既に示されていると仮定する．

(a) まずは Δ が $A \to B$ を含む場合，つまり $\Delta \equiv \Delta_0, A \to B, \Delta_1$ の場合を考える．このとき，$\to$ の右規則より，

$$\frac{A, \Gamma \vdash \Delta_0, \Delta_1, B}{\Gamma \vdash \Delta_0, A \to B, \Delta_1}\ (\to \text{右}) \tag{14}$$

であるが，(14) の下式は $\Gamma \vdash \Delta$ であるから，仮定より証明不可能である．したがって，(14) の上式も証明不可能である．(14) の上式に含まれる $\to$ の数は下式よりも 1 つ少ない n 個であるから，帰納的仮定より，(14) の上式を偽にする付値が存在する．つまり，A, Γ に現れる論理式を全て真に，Δ_0, Δ_1, B に現れる論理式を全て偽にする．

A	$\bigwedge\Gamma$	$\bigvee\Delta_0$	$\bigvee\Delta_1$	B	$A \to B$
真	真	偽	偽	偽	偽

特に A は真で B は偽となるから，$A \to B$ は偽となる．このとき，(14) の下式について，Γ の論理式は全て真であり，$\Delta \equiv \Delta_0, A \to B, \Delta_1$ の論理式は全て偽であるから，この付値は $\bigwedge\Gamma \to \bigvee\Delta$ を偽にする．

(b) つづいて，Γ が $A \to B$ を含む場合，つまり $\Gamma \equiv \Gamma_0, A \to B, \Gamma_1$ の場合を考える．このとき，$\to$ の左規則より，

$$\frac{\Gamma_0, \Gamma_1 \vdash \Delta, A \qquad B, \Gamma_0, \Gamma_1 \vdash \Delta}{\Gamma_0, A \to B, \Gamma_1 \vdash \Delta}\ (\to \text{左}) \tag{15}$$

であるが，(15) の下式は $\Gamma \vdash \Delta$ であるから，仮定より証明不可能である．したがって，(15) の上式の少なくとも一方は証明不可能である．(15) の上式のどちらも $\to$ の数は下式よりも 1 つ少ない n 個であることに注意する．

[**Case b1**]: (15) の左上の式が証明不可能だったと仮定すると，帰納的仮定より (15) の左上の式を偽にする付値が存在する．つまり，Γ_0, Γ_1 に現れる論理式を全て真に，Δ, A に現れる論理式を全て偽にする．

$\bigwedge\Gamma_0$	$\bigwedge\Gamma_1$	$\bigvee\Delta$	A	$A \to B$
真	真	偽	偽	真

特に A が偽であることから，$A \to B$ は真となる．このとき，(15) の下式について，$\Gamma \equiv (\Gamma_0, A \to B, \Gamma_1)$ の論理式は全て真であり，Δ の論理式は全て偽であるから，この付値は $\bigwedge\Gamma \to \bigvee\Delta$ を偽にする．

[**Case b2**]: (15) の右上の式が証明不可能だったと仮定すると，帰納的仮定より (15) の右上の式を偽にする付値が存在する．つまり，B, Γ_0, Γ_1 に現れる論理式を全て真に，Δ に現れる論理式を全て偽にする．

B	$\bigwedge\Gamma_0$	$\bigwedge\Gamma_1$	$\bigvee\Delta$	$A \to B$
真	真	真	偽	真

特に B が真であることから，$A \to B$ は真となる．このとき，(15) の下式について，$\Gamma \equiv (\Gamma_0, A \to B, \Gamma_1)$ の論理式は全て真であり，Δ の論理式は全て偽であるから，この付値は $\bigwedge\Gamma \to \bigvee\Delta$ を偽にする．

以上より，$\to$ の数が n の場合の完全性定理を仮定すれば，$\to$ の数が $(n+1)$ の場合の完全性定理を導けることが示された．したがって，数学的帰納法より，定理は示された． □

命題論理式 A が**充足可能** (*satisfiable*) とは，A を真にするような付値が存在することを意味する．これは $\neg A$ が恒真でないことと同値である．命題論理式の充足可能性を問う問題は，形式体系での証明不可能性を問う問題と深く関連している．

系 1.23 (完全性定理の系)**.** A を命題論理式とする．このとき，

$$A \text{ が充足可能である} \iff \neg A \text{ が LK で証明不可能である．}$$

Proof. A が充足可能であることと $\neg A$ が恒真でないことは同値であるから，命題論理の完全性定理 1.22 より，これは $\neg A$ は LK で証明不可能であることと同値である． □

演習問題 1.24. $(A \to B) \to (\neg A \to \neg B)$ が LK で証明不可能であることを示せ．

1.6 LK のカット除去定理

論理結合子に関する推論規則を見てみよう．上式の個々の推件式を見ると，下式の推件式よりも論理結合子の数が減っていることに気づくと思う．また，カット以外の構造に関する推論規則を見ても，下式の推件式中に現れる論理式よりも上式の推件式中に現れる論理式が複雑であるということは有り得ない．つまり，カットを用いなければ，下式から上式に遡るにつれ，各推件式の中に現れる論理式の複雑性は徐々に下がっていくのである．そして，最終的には命題変数だけからなる推件式に辿り着く．

それでは，どのような命題論理式ならば，必ずカットを使わないで証明できるだろうか．その答えはカット除去定理であり，カットを利用して証明できる式はカットを利用せずとも証明できる，というものである．したがって，もし命題論理式が恒真ならば，その命題論理式を終式に置いて，推論規則に当てはめて順に論理結合子を取り除いていくだけで，証明図を逆算できる，ということとなる．

定理 1.25 (カット除去定理)**.** $\Gamma \vdash \Delta$ を推件式とする．もし，$\Gamma \vdash \Delta$ が *LK* において証明可能ならば，*LK* における $\Gamma \vdash \Delta$ のカットなし証明図が存在する．

Proof (スケッチ). 論理式の複雑さに関する帰納法を用いて示す．論理式 A にカット規則を用いていると仮定する．

$$\dfrac{\begin{array}{cc}\vdots & \vdots \\ \mathcal{L} & \mathcal{R} \\ \vdots & \vdots \\ \Gamma \vdash \Theta, A & A^n, \Delta \vdash \Lambda\end{array}}{\Gamma, \Delta \vdash \Theta, \Lambda}\ (\text{カット})$$

ここで，帰納的に $\mathcal{L}$ と $\mathcal{R}$ の部分はカットなしの証明図であるとする．まず，$\mathcal{L}$ が公理の適用であるとすると，Θ は空であり，Γ は A または $\bot$ である．どちらにせよ，以下のようにカットなしで証明できる．

$$\dfrac{A^n, \Delta \vdash \Lambda}{A, \Delta \vdash \Lambda}\ (\text{弱化}) \qquad\qquad \dfrac{\bot \vdash}{\bot, \Delta \vdash \Lambda}\ (\text{弱化})$$

つづいて，A は $B \to C$ の形であり，$\mathcal{L}$ は含意 $\to$ の右規則，$\mathcal{R}$ は含意 $\to$ の左規則を最後に適用していると仮定しよう．このとき，

$$\dfrac{\dfrac{\begin{array}{c}\vdots \\ \mathcal{L}_0 \\ \vdots \\ B, \Gamma \vdash \Theta, C\end{array}}{\Gamma \vdash \Theta, B \to C}\ (\to \text{左}) \qquad \dfrac{\begin{array}{cc}\vdots & \vdots \\ \mathcal{R}_0 & \mathcal{R}_1 \\ \vdots & \vdots \\ (B \to C)^i, \Delta_0 \vdash B & C, (B \to C)^j, \Delta_1 \vdash \Lambda\end{array}}{B \to C, (B \to C)^{i+j}, \Delta_0, \Delta_1 \vdash \Lambda}\ (\to \text{右})}{\Gamma, \Delta_0, \Delta_1 \vdash \Theta, \Lambda}\ (\text{カット})$$

帰納的仮定より，$\mathcal{L}_0, \mathcal{R}_0, \mathcal{R}_1$ はカットを含まないと仮定できる．この証明図は次のように書き換えることができる．

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots \\ \mathcal{L} \\ \vdots \\ \Gamma \vdash \Theta, B \to C\end{array} \qquad \begin{array}{c}\vdots \\ \mathcal{R}_0 \\ \vdots \\ (B \to C)^i, \Delta_0 \vdash B\end{array}}{\Gamma, \Delta_0 \vdash \Theta, B}\ (\text{cut}) \qquad \dfrac{\begin{array}{c}\vdots \\ \mathcal{L}_0 \\ \vdots \\ B, \Gamma \vdash \Theta, C\end{array} \qquad \dfrac{\begin{array}{cc}\vdots & \vdots \\ \mathcal{L} & \mathcal{R}_1 \\ \vdots & \vdots \\ \Gamma \vdash \Theta, B \to C & C, (B \to C)^j, \Delta_1 \vdash \Lambda\end{array}}{C, \Gamma, \Delta_1 \vdash \Theta, \Lambda}\ (\text{cut})}{B, \Gamma^2, \Delta_1 \vdash \Theta^2, \Lambda}\ (\text{cut})}{\Gamma^3, \Delta_0, \Delta_1 \vdash \Theta^3, \Lambda}\ (\text{cut})}{\Gamma, \Delta_0, \Delta_1 \vdash \Theta, \Lambda}\ (\text{縮約})$$

仮定より $\mathcal{L}, \mathcal{R}, \mathcal{L}_0, \mathcal{R}_0, \mathcal{R}_1$ はカットを含まない．さらに，上の証明図におけるいずれのカット中の論理式も，元の証明図のカット中の論理式よりも複雑性が低いから，帰納法の仮定により，カットを除去できる． □

2 計算量と論理

2.1 ブール回路

2.1.1 回路計算量

本節では，命題論理と計算量理論と関わりについて述べよう．ブール回路の理論は，現実世界における電子回路の論理演算を記述する目的で導入されたが，理論的にも非常に興味深い対象である．ブール回路の概念を導入する前に，グラフ理論の用語を軽くおさらいしておこう．

定義 2.1. 有向グラフ (*directed graph*) とは，集合 V と関係 $E \subseteq V^2$ の対 $G = (V, E)$ である．

- V の各要素を**頂点** (*vertex*) といい，E の各要素を**辺** (*edge*) と言う．
- 頂点の列 $(v_0, v_1, \ldots, v_n)$ で，任意の i について $(v_i, v_i + 1) \in E$ を満たすものを**路** (*path*) と呼ぶ．
- $v_0 = v_n$ となるような長さ 1 以上の路 $(v_0, v_1, \ldots, v_n)$ を持つグラフを**巡回グラフ** (*cyclic graph*) と呼び，さもなくば**非巡回グラフ** (*acyclic graph*) と呼ぶ．
- 各頂点 $v \in V$ について，$\{u \in V : (u, v) \in E\}$ の数を v **の入次数** (*in-degree*) と呼び，$\{w \in V : (v, w) \in E\}$ の数を v **の出次数** (*out-degree*) と呼ぶ．

定義 2.2. ブール回路 (*Boolean circuit*) とは，次のような非巡回有向有限グラフである．

- 入次数 0 の頂点を入力ノード，出次数 0 の頂点を出力ノード，他の頂点をゲートと呼ぶ．
- 各ゲートには，論理結合子がラベル付けされている．
- 各入力ノードには命題変数が割り当てられている
- 出力ノードの数が n である場合，出力ノードに 1 から n までの番号が重複なく割り当てられている．

入力ノードのラベルの種類数 m, 出力ノード数 n のブール回路を関数 $C : \{0,1\}^m \to \{0,1\}^n$ と考えることができる．つまり，入力ノードに割り当てられた命題変数のリスト $p_1, \ldots p_m$ に対する付値 $v : m \to \{0,1\}$ を決めれば，i 番目の出力ノードの真理値 t_i^v が定まる．このとき，

$$C(v) = (t_1^v, \ldots t_n^v)$$

として定義する．また，ブール回路の辺の数を回路の**サイズ**と呼び，最長の路の長さを回路の**深さ**と呼ぶ．

定義 2.3. 関数 $f : \{0,1\}^* \to \{0,1\}^*$ が**回路族** $(C_n)_{n \in \mathbb{N}}$ **によって計算される**とは，任意の $x \in \{0,1\}^*$ に対して，$C_{|x|}(x) = f(x)$ を満たすことである．

さて，回路族によって計算できる関数と，現実のコンピュータで計算できる関数には如何なる関係があるかについて見ていこう．

2.1.2 ブール演算による計算の模倣

■ブール・プログラム　さて，これからコンピュータの計算を命題論理（ブール演算）によって模倣することを考えよう．模倣を明瞭にするために，ブール演算を以下のように簡易プログラミング的に表すことを考えよう．

```
x:= true; y:= false; z:= true;
p:= x ∧ y; q:= z ∨ ¬p; r:= q ∧ x; output r;
```

上のブール・プログラムは以下のような 1 つの命題論理式を表すと考える．

$$R \equiv (Q \wedge X) \equiv ((Z \vee \neg P) \wedge X) \equiv ((Z \vee \neg(X \wedge Y)) \wedge X).$$

ここで，第 1 行で $X \equiv \top$, $Y \equiv \bot$, $Z \equiv \top$ という付値が与えられているので，これを解釈すると，R の真理値は $\top$ である．つまり，上記のプログラムは `true` を出力する．

また，ブール演算プログラミングにおいて，場合分けを利用してよいとする．たとえば，

```
x:= true; y:= false; z:= true;
p:= x ∧ y; q:= z ∨ ¬p; r:= q ∧ x;
if r then (q:= p∧q; output q) else (output ¬r);
```

のようなものである．先程のように 2 行目の段階での `r` の値は `true` であるから，$Q' \equiv P \wedge Q \equiv \bot \wedge \top \equiv \bot$ となり，つまり `false` が出力される．

■チューリング機械の模倣　いま，チューリング機械 M が与えられているとしよう．この機械 M は，長さ n の任意の入力に対して高々時間 $t(n)$ で計算を停止すると仮定する．このとき，与えられた入力 x に対して，次のようなブール・プログラム $B(x)$ を作りたい．

$$M \text{ は } x \text{ を受理する} \iff B(x) \text{ は } \texttt{true} \text{ を出力する}.$$

これを実現するためには，かなり多くの命題変数を準備する必要がある．簡単のために，アルファベットは $\{0, 1\}$ であり，状態は $Q = \{0, 1, \ldots, s\}$ と並べられているとしよう．ここで，s が受理状態であると仮定する．

まず，命題変数 $(\texttt{tape[i,a]})_{-t(n) \leqslant i \leqslant t(n)}$ を準備する．これは，以下の性質を満たすように，後にうまくプログラムを記述する．

`tape[i,a] = true` $\iff$ ヘッド位置との相対位置が i のセルに書かれた文字が `a` である．

一応，注意しておくと，計算時間の上界 $t(n)$ のため，計算中にヘッドは高々 $t(n)$ セル分しか動けない．したがって，$-t(n) \leqslant i \leqslant t(n)$ だけ考えれば十分ということである．

また，命題変数 $(\texttt{state[q]})_{q \leqslant s}$ も準備する．これについては，以下の性質を満たすようにしたい．

`state[q] = true` $\iff$ 現在の状態が `q` である．

セルの文字の書き換えや状態の遷移を模倣するために，いくつかの便利なマクロを準備する．まず，tape[i]:= a を以下の略記とする．

マクロ tape[i]:= a の定義
tape[i,0]:= false; tape[i,1]:= false; tape[i,␣]:= false;
tape[i,a]:= true;

同様の発想で，tape[i]:= tape[j] のようなものも定義できる．同様にして，state:= p を以下の略記とする．

マクロ state:= p の定義
state[0]:= false; state[1]:= false; ...; state[s]:= false;
state[p]:= true;

さて，ヘッドが左右に動くと，各セルの相対位置が動くため，tape[i,a] の値をシフトする必要がある．これを実行するためのマクロ right と left を用意する．

マクロ right の定義
tape[-t(n)]:= tape[-t(n)+1]; ...; tape[-1]:= tape[0];
tape[0]:= tape[1]; ...; tape[t(n)-1]:= tape[t(n)]; tape[t(n)]:= ␣;

マクロ left の定義
tape[-t(n)]:= ␣; tape[-t(n)+1]:= tape[-t(n)]; ...; tape[0]:= tape[-1];
tape[1]:= tape[0]; ...; tape[t(n)]:= tape[t(n)-1];

そうすると，たとえば，$\delta(q,a) = (p,b,\mathrm{right})$ という遷移は，以下のブール・プログラムによって実現できる．

遷移 $\delta(q,a) = (p,b,\mathrm{right})$ の実装 I[q,a] else ...
x:= state[q]∧tape[0,a];
if x then (
state:= p; tape[0]:= b; right;
) else (...)

上のプログラムを I[q,a] else ... と略記すると，チューリング機械の計算の 1 ステップは，以下のブール・プログラム STEP で模倣できる．

以上より，入力 $x = x_1x_1 \ldots x_n$ に対するブール・プログラム $B_n(x)$ は以下によって与えられる．

ここで，ブール・プログラム $B_n(x)$ は，1 行目を除けば，入力サイズ n のみに依存することに注意する．

マクロ STEP の定義
I[0,0] else I[0,1] else I[0,␣] else I[1,0] else I[1,1] else I[1,␣] else ... I[s-1,0] else I[s-1,1] else I[s-1,␣] else output true;

ブール・プログラム $B_n(x)$

tape[1]:= x1; tape[2]:= x2; ...; tape[n]:= xn;
tape[n+1]:= ␣; tape[n+2]:= ␣; ...; tape[t(n)]:= ␣;
tape[0]:= ␣; tape[-1]:= ␣; ...; tape[-t(n)]:= ␣;
state:=0; (STEP;)$^{t(n)}$ output false;

■場合分けの除去　上記のプログラムにおいて，あまりブール演算が用いられていない．これは，多くのブール演算を場合分けに肩代わりさせているためである．しかし，場合分けは，以下のような命題論理式で表現することが可能である．

$$(P \wedge R) \vee (Q \wedge \neg R) \equiv \begin{cases} P & \text{if } R = \texttt{true}, \\ Q & \text{if } R = \texttt{false}. \end{cases}$$

よって，ブール・プログラム中のすべての `if q then I else J` の出現を $(\texttt{I} \wedge \texttt{q}) \vee (\texttt{J} \vee \neg\texttt{q})$ のような形に置き換えてやればよさそうだ．より正確には，帰納的に，I と J からは既にすべての `if-then-else` を取り除いていると仮定しよう．そうすると，

```
I ≡ x1:=d1; x2:=d2; ...; xm:=dm;
J ≡ y1:=e1; y2:=e2; ...; yn:=en;
```

のような形になっている．このとき，`if q then I else J` を以下のように書き換える．

```
x1:= (d1 ∧ q) ∨ (x1 ∧ ¬q); x2:= (d2 ∧ q) ∨ (x2 ∧ ¬q);
                    ...; xm:= (dm ∧ q) ∨ (xm ∧ ¬q);
y1:= (y1 ∧ q) ∨ (e1 ∧ ¬q); y2:= (y2 ∧ q) ∨ (e2 ∧ ¬q);
                    ...; yn:= (yn ∧ q) ∨ (en ∧ ¬q);
```

このようにして，ブール・プログラムから場合分けを除去することができる．場合分けの除去されたブール・プログラムから 1 つの命題論理式が得られることは容易に分かるであろう．以上より，計算時間の束縛されたチューリング機械を模倣する命題論理式の列 $(C_n)_{n\in\mathbb{N}}$ が構成された．

2.2 計算量クラス NP

2.2.1 探索問題と検証系

日常においてしばしば現れる問題が**探索問題** (*search problem*) である．単純に関係 $P \subseteq \{0,1\}^* \times \{0,1\}^*$ が与えられているとしよう．問題としては，入力 $x \in \{0,1\}^*$ に対して，$P(x,y)$ なる y を見つけよ，というものである．

例 2.4. 以下は探索問題の例である．

1. 与えられた命題論理式を真にするような付値を求めよ，という問題 V_{eval} は探索問題である．

$$V_{\mathrm{eval}}(A,v) \iff \text{付値 } v \text{ の下で命題論理式 } A \text{ は真である．}$$

2. 与えられた命題論理式の LK における証明図を書け，という問題 V_{proof} は探索問題である．

$$V_{\mathrm{proof}}(A,p) \iff p \text{ は推件式} \vdash A \text{ の LK における証明図である．}$$

探索問題 V_{eval} は命題論理式の充足可能性の証拠を見つけよ，V_{proof} は命題論理式の証明可能性の証拠を見つけよ，という問題である．しかし，しばしば単に充足可能か否かだけ答えよ，証明可能か否かだけ答えよ，と言ったように，証拠の提出までは求めないことがある．そのような問題を**決定問題** (*decision problem*) という．数学的には，決定問題とは $Q \subseteq \{0,1\}^*$ であり，入力 $x \in \{0,1\}^*$ に対して，$Q(x)$ が真か偽かを答えよ，というものである．

例 2.5 (決定問題の例)**.** 以下は決定問題の例である．

1. 充足可能性問題 SAT は，与えられた命題論理式が充足可能かどうかを問う．

$$\mathsf{SAT}(A) \iff \text{命題論理式 } A \text{ を真とする付値が存在する．}$$

2. 恒真性問題 TAUT は，与えられた命題論理式が恒真かどうかを問う．

$$\mathsf{TAUT}(A) \iff \text{命題論理式 } A \text{ は恒真である．}$$

探索問題から決定問題が一意に与えられるのに対して，決定問題から探索問題を一意に復元することはできない．したがって，決定問題に対応する探索問題は複数存在し得るが，それぞれを検証系と呼ぶ．

定義 2.6. 決定問題 Q の**検証系** (*verification system*) とは，次の**完全性**と**健全性**を満たす関係 $V \subseteq \{0,1\}^* \times \{0,1\}^*$ である．

1. (完全性) 真な主張には正しさの証明がある．つまり，$Q(x)$ が真ならば，$V(x,y)$ となるような y が存在する．
2. (健全性) 偽な主張を証明することはない．つまり，$Q(x)$ が偽ならば，$V(x,y)$ となるような y は存在しない．

例 2.7. V_{eval} は SAT の検証系である．同様に，V_{proof} は TAUT の検証系である．後者については，健全性定理と完全性定理の帰結である．

- 命題論理式 A が充足可能ならば，$v(A) = \top$ であるような付値 v が存在する．
- 命題論理式 A が充足可能でないならば，$\neg A$ が恒真であるから，$\vdash \neg A$ の LK-証明が存在する．

さて，検証系にもう少し強いことを要求しよう．まず，現実的計算可能性を考えれば，検証系 V が多項式時間計算可能な述語であることを要求することは妥当であろう．さらに，完全性の条件として，$Q(x)$ の証拠となる y が多項式サイズで抑えられる，つまり $|y| \leqslant p(|x|)$ であることも要求したい．このような良い検証系を持つような，行儀の良い決定問題は，NP 問題と呼ばれる．

定義 2.8. 決定問題 Q が**多項式時間検証可能**または NP であるとは，ある多項式時間計算可能述語 V と多項式 p が存在して，任意の $\bar{x}$ に対して，以下が成立することである．

$$Q(\bar{x}) \iff (\exists y)_{|y| \leqslant p(|\bar{x}|)}\, V(\bar{x}, y).$$

例 2.9. SAT は NP 問題である．なぜなら，V_{eval} は SAT の検証系であり，まず，付値 v の下での命題論理式 A の真偽性判定が多項式時間計算可能であることは容易に分かる．さらに，命題変数の数が n 個の場合，各付値 v は長さ n の真理値のリスト $v(1), \ldots, v(n)$ に過ぎないことから，多項式有界性も明らかに保証されている．

注意. TAUT が NP 問題であることは保証されていない．まず，TAUT の検証系である V_{proof} が多項式時間計算可能述語であることは間違いない．しかし，各命題論理式 A の証明可能性の証拠，すなわち LK-証明図のサイズが多項式で抑えられることが保証されていないのである．

2.2.2 NP 完全性

定義 2.10. P と Q を決定問題とし，$\mathcal{F}$ を関数族とする．このとき，P が Q に **$\mathcal{F}$-多対一還元可能** ($\mathcal{F}$-*many-one reducible*) とは，ある関数 $f \in \mathcal{F}$ が存在して，次が成立することである．

$$(\forall x \in \{0,1\}^*) \quad x \in P \iff f(x) \in Q.$$

$\mathcal{F}$ が多項式時間計算可能関数の族の場合，$\mathcal{F}$-多対一還元は**多項式時間多対一還元**または**カープ還元** (*Karp reduction*) と呼ばれる．

豆知識. $\mathcal{F}$ が計算可能関数全体の場合，$\mathcal{F}$-多対一還元は単に多対一還元と呼ばれ，エミール・ポストによって 1940 年代に導入された後，計算可能性理論においては深く研究されている．P, Q が位相空間の部分集合であり，$\mathcal{F}$ が連続関数の族の場合，$\mathcal{F}$-多対一還元は**ワッジ還元** (*Wadge reduction*) と呼ばれ，1970 年代頃から記述集合論において深く研究されている．また，探索問題についても多項式時間多対一還元可能性の類似

物があり，それは**レヴィン還元** (*Levin reduction*) として知られている．位相空間あるいは表現空間における探索問題のレヴィン還元に似た概念としては，**ヴァイラウフ還元** (*Weihrauch reduction*) が近年，逆数学などとの関連性から活発に研究されている．

定義 2.11. Γ を決定問題の族とする．このとき，決定問題 Q が Γ-**困難** (Γ-*hard*) であるとは，任意の決定問題 $P \in \Gamma$ に対して，P が Q に多項式時間多対一還元可能であることを意味する．決定問題 Q が Γ-**完全** (Γ-*complete*) とは，$Q \in \Gamma$ かつ Q が Γ-困難であることを意味する．

豆知識． NP 完全性の概念は，神託機械を用いて定義されるチューリング還元の多項式版である**クック還元** (*Cook reduction*) を用いて定義されることもある．

定理 2.12. SAT は NP 完全である．

Proof. Q を任意の NP 問題とする．このとき，ある多項式時間チューリング機械 M が存在して，

$$Q(a) \iff (\exists b)_{|b| \leqslant p(|a|)}\ [M \text{ は入力 } ab \text{ を受理する }].$$

このような機械 M と任意の入力 z に対して，次を満たすブール・プログラム $B_{|z|}(z)$ を構成できる．

$$M \text{ は入力 } z \text{ を受理する} \iff B_{|z|}(z) \text{ は } \texttt{true} \text{ を出力する}.$$

ここで，$B_{|z|}(z)$ からは既に `if-then-else` が除去されているとしてよい．構成より，$n \mapsto B_n$ は多項式時間計算可能である．また，B_n は `if-then-else` を含まないので，命題論理式だと思うことができる．より正確には，B_n を以下のような命題論理式 $\tilde{B}_n(p_1, \ldots, p_n)$ と同一視しよう．$z = z_1 z_2 \ldots z_n$ に対して，

$$B_n(z) \text{ は } \texttt{true} \text{ を出力する} \iff \tilde{B}_n(\tilde{z}_1, \ldots, \tilde{z}_n) \equiv \top$$

ここで，$z_i = 1$ のとき $\tilde{z}_i = \top$, $z_i = 0$ のとき $\tilde{z}_i = \bot$ と定義する．以上より，

$$\begin{aligned} Q(a_1 \ldots a_n) &\iff (\exists b_1 \ldots b_{p(n)})\ \tilde{B}_{n+p(n)}(\tilde{a}_1, \ldots, \tilde{a}_n, \tilde{b}_1, \ldots, \tilde{b}_{p(n)}) \equiv \top \\ &\iff \tilde{B}_{n+p(n)}(\tilde{a}_1, \ldots, \tilde{a}_n, x_1, \ldots, x_{p(n)}) \in \mathsf{SAT}. \end{aligned}$$

よって，Q は SAT に多項式時間多対一還元可能であることが示された．これは任意の NP 問題 Q について成立するので，SAT は NP 完全である． □

Γ を決定問題の族とする．このとき，coΓ によって，補問題が Γ であるような決定問題全体の族を表す．つまり，

$$Q \in \mathsf{co}\Gamma \iff \neg Q := \{x : \neg Q(x)\} \in \Gamma.$$

系 2.13.

$$\mathsf{TAUT} \text{ が NP 問題である} \iff \mathsf{NP} = \mathsf{coNP}.$$

Proof. TAUT の補問題 ¬TAUT を考える．このとき，

$$A \in \mathsf{SAT} \iff \neg A \in \neg\mathsf{TAUT}$$

であることは容易に分かる．$A \mapsto \neg A$ は多項式時間計算可能であるから，これは SAT が ¬TAUT に多項式時間多対一還元可能であることを導く．特に，¬TAUT は NP 完全であり．TAUT は coNP 完全である．したがって，

$$\mathsf{NP} \subseteq \mathsf{coNP} \iff \neg\mathsf{TAUT} \in \mathsf{coNP} \iff \mathsf{TAUT} \in \mathsf{NP} \iff \mathsf{coNP} \subseteq \mathsf{NP}.$$

以上より，目的の性質は示された． □

定義 2.14. 命題証明系 (*propositional proof system*) とは，次を満たす多項式時間チューリング機械 M である：任意の命題論理式 A に対して，

$$A \in \mathsf{TAUT} \iff (\exists p)\ M(p, A) = 1.$$

例 2.15. 推件計算の体系 LK は，上記の意味で，命題証明系と思うことができる．

命題証明系 M が与えられたとき，$\ell_M(A)$ を M における A の最も短い証明の長さとする．つまり，M が (p, A) を受理するような最小の証明 p の長さ $|p|$ である．このとき，ℓ_M は，証明系 M における恒真式の証明複雑性を捉えたものと考える．

系 2.16. 証明複雑性 ℓ_M が多項式で上から押さえられるような命題証明系 M が存在することと NP = coNP は同値である．

2.3 一方向関数

2.3.1 関数の不可逆性

さて，NP の定義を思い出すと，Q が NP であるとは次のようなものであった：ある多項式時間計算可能述語 R と多項式 p が存在して，任意の $\bar{x}$ に対して

$$Q(\bar{x}) \iff (\exists y)_{|y| \leqslant p(|\bar{x}|)}\ R(\bar{x}, y).$$

関数 f が PB-可逆 (polynomially bounded invertible) とは，ある多項式 q が存在して，次の性質を満たすことである．

$$[(\exists x)\ f(x) = y] \iff [(\exists x)_{|x| \leqslant q(|y|)}\ f(x) = y].$$

この性質は，ある多項式有界関数 g が存在して，次を満たすことと同値である．

$$[(\exists x)\ f(x) = y] \iff f \circ g(y) = y.$$

関数 f が P-可逆 (polytime computable invertible) とは，ある P-関数 g が存在して，次を満たすことと同値である．

$$[(\exists x)\ f(x) = y] \iff f \circ g(y) = y.$$

補題 2.17. 空でない集合 $A \subseteq \Sigma^*$ について，以下が成立する．

$$A \in NP \iff \text{ある } PB\text{-可逆 } P\text{-関数 } f \text{ について，} A = \mathrm{range}(f),$$

$$A \in P \iff \text{ある } P\text{-可逆 } P\text{-関数 } f \text{ について，} A = \mathrm{range}(f).$$

Proof. まず $a \in A$ を固定する．A が NP であると仮定する．このとき，ある P-述語 R と多項式 p が存在して，

$$x \in A \iff (\exists y)_{|y| \leqslant p(|x|)}\ R(x, y)$$

となる．このとき，関数 f を次によって定義する．入力 $\langle x, y\rangle$ に対して，y が $x \in A$ の証拠ならば x を並べ，そうでなかったら余計なことはせずに a を並べる．つまり，

$$f(\langle x, y\rangle) = \begin{cases} x & \text{if } |y| \leqslant p(|x|) \text{ and } R(x, y), \\ a & \text{otherwise.} \end{cases}$$

明らかに f は P-関数である．もし $f(\langle x, y\rangle) = x$ なる y が存在するなら，そのような y で $|y| \leqslant p(|x|)$ なるものが存在するので，$\langle x, y\rangle$ の長さも $|x|$ に関する多項式で抑えられる．つまり，多項式有界な g で $f \circ g(x) = x$ なるものが存在する．よって f は PB-可逆である．

逆に，A が PB-可逆 P-関数 f の値域になると仮定する．このとき，

$$y \in A \iff (\exists x)\ f(x) = y \iff (\exists x)_{|x| \leqslant q(|y|)}\ f(x) = y$$

であり，f は P-関数であるから，$f(x) = y$ は P-述語である．よって，$A \in NP$ である．

次に，A が P であると仮定すると，次の関数 ι は P-関数である．

$$\iota(x) = \begin{cases} x & \text{if } x \in A, \\ a & \text{otherwise.} \end{cases}$$

明らかに A は ι の値域であり，$y \in A$ ならば $\iota \circ \iota(y) = y$ であるから，ι は P-可逆である．

逆に，A が P-可逆 P-関数 f の値域になると仮定する．このとき，g を f の P-逆関数とすれば，

$$y \in A \iff f \circ g(y) = y$$

が成立する．右式 $f \circ g(y) = y$ は P-述語であるから，$A \in P$ であることが示された． □

命題 2.18.

$$P \neq NP \iff PB\text{-可逆だが } P\text{-可逆でない } P\text{-関数が存在する.}$$

Proof. ($\Rightarrow$) PB-可逆だが P-可逆でない P-関数が存在しないと仮定する．このとき，補題 2.17 より $P = NP$ が従う．

($\Leftarrow$) $P = NP$ を仮定する．また f を PB-可逆な P-関数とする．このとき，補題 2.17 より f の値域は NP に属している．$P = NP$ という仮定より，f の値域は P に属す．f が P-可逆であることを示すために P-関数 g を構成する．g の動作は次のようなものである．

仮定より，与えられた y が f の値域に入るかどうかの判定は P であるから，まずその判定を行う．入っていないなら $g(y) = 0$ とする．さもなくば，g は $f(x) = y$ なる x を探す．まず，x の 1 桁目を探索するために，各 $\mathtt{a} \in \Sigma$ に対して，$\mathtt{a}$ を拡張する z で $f(z) = y$ なるものが存在するかを尋ねる．どれかの $\mathtt{a}$ で解は YES となるならば，そのような $\mathtt{a}$ を x の 1 桁目とすればよい．問題は計算時間である．f は PB-可逆なので，z の捜索範囲は $q(|y|)$ で押さえられている．よって，この判定は NP であるが，$P = NP$ であるから，多項式時間で判定できる．

この手続きを繰り返す．$x \restriction n$ が構成されていると仮定する．各 $\mathtt{a} \in \Sigma$ について

$$(\exists z)_{|(x\restriction n)\mathtt{a}z| \leqslant q(|y|)}\ f(z) = y$$

かどうかを確認する．この判定は NP であるが，$P = NP$ であるから，多項式時間で判定できる．f は q によって PB-可逆であるから，そのような $\mathtt{a}$ を探す手続きを高々 $q(|y|)$ 回繰り返せば，目的の x を見つけられる．以上より f は P-可逆であることが示された． □

2.3.2 確率的チューリング機械

このような可逆操作は，暗号の世界では，おおよそ暗号解読の部分に相当する．P-可逆でない，という状況は，最悪ケースにおいては元のデータを逆算するのが困難ということである．しかし，最悪ケースにおける計算の困難性は，平均的な計算の困難性を意味しないことが多々ある．暗号理論において重要なことは，最悪ケースだけでなく，ほとんどのケースで計算が困難なことである．この概念の 1 つの定式化を与えるために，確率的な計算概念を導入する．

確率的チューリング機械は，通常のチューリング機械と違って，2 つの遷移関数 δ_0, δ_1 を持つ．計算の各ステップで，δ_0 と δ_1 は半々の確率で選ばれる．確率的チューリング機械の計算時間が T-有界であるとは，どんな入力 x と如何なる遷移の選択に対しても，$T(|x|)$ 時間で計算が停止することを意味する．

定義 2.19. 安全性 s を持つ ε-一方向関数 (*one-way function*) とは，P-関数 $f : \{0,1\}^* \to \{0,1\}^*$ であり，次の不可逆性を満たすものである．任意の $s(n)$ 時間計算可能関数 g に対して，

$$(\forall n \in \mathbb{N}) \quad \Pr_{x\in\{0,1\}^n}[f \circ g \circ f(x) = f(x)] \leqslant \varepsilon(n).$$

$s(n)$ が任意の多項式であり，任意の k について $\varepsilon(n) < n^{-k}$ となる ε に対して上式が成立するとき，f を単に一方向関数と呼ぶ.

一方向関数は，疑似乱数の概念と大きく関わっている.

定義 2.20. $\{g_n\}$ を P-関数の族で，$g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ なるものとする．このとき，(δ, s)-**疑似乱数生成器** ((δ, s)-*pseudorandom generator*) とは，任意の確率的 $s(n)$-時間計算可能関数 h に対して，有限個を除くすべての n について，

$$|\Pr_{y\in\{0,1\}^{m(n)}}[h(y) = 1] - \Pr_{x\in\{0,1\}^n}[h(g_n(x)) = 1]| \leqslant \delta(n).$$

本稿では証明を与えないが，一方向関数の存在と疑似乱数生成器の存在は同値である.

定理 2.21.

一方向関数が存在する $\iff$ 疑似乱数生成器が存在する.

疑似乱数生成器が一方向関数であることは容易に確認できるので，軽い説明を与えよう．関数列 (g_n) に対して，$g(x) = g_{|x|}(x)$ によって定義する．この g が一方向関数でなかったとすると，高い確率の入力で $g \circ G \circ g(x) = g(x)$ なる G が存在する．いま，y の長さが $m(n)$ ならば $G(y)$ の長さが n であると仮定しても一般性を失わない．このとき，$g \circ G(y) = y$ ならば $h(y) = 1$, さもなくば $h(y) = 0$ とする．n が $m(n)$ より十分小さいのであれば，$h(y) = 1$ すなわち $g \circ G(y) = y$ となる入力 y の確率は極めて低い．一方，$h(g_n(x)) = 1$ すなわち $g \circ G \circ g_n(x) = g_n(x)$ は極めて高確率で成立する．よって，(g_n) は擬似乱数生成器では有り得ない.

3 一階述語論理

3.1 述語論理とは

数学を分析するには命題論理では力不足である．数学の強みはその一般性にあり，「全ての○○は△△である」のような形式の定理は数多い．一方で，「××が存在する」という形のいわゆる存在定理も有り触れている．論理式で書くのが容易な例を挙げれば，前者として「任意の自然数は高々 4 つの平方数の和である」ということを述べるラグランジュの四平方定理，後者として「素数が無限に存在する」という主張などがあるだろう．つまり，数学における論理の主役は「任意」「全て」を表す全称量化記号 $\forall$ と「存在」を表す存在量化記号 $\exists$ である．四平方定理を論理式で記述するならば,

$$(\forall x)(\exists a, b, c, d)\ [x = a^2 + b^2 + c^2 + d^2] \tag{16}$$

であり，素数の無限性を論理式で記述するならば,

$$(\forall x)(\exists p > x)\ [p \text{ は素数である}]$$

と表される．ここで $\forall$ と $\exists$ の量化範囲は自然数を想定している．もう少し細かく見ると，「p が素数である」という主張は次のように表される．

$$p > 1 \ \wedge \ (\forall r, s)\,[p = r \cdot s \ \rightarrow \ (r = 1 \ \vee \ s = 1)]. \tag{17}$$

そういうわけで，数学と量化子 $\forall, \exists$ は切っても切り離せない．また，数学における論理式の詳細な分析を行う際には，論理記号より細部に踏み入る必要がある．たとえば，上式においては論理結合子 $\rightarrow, \neg, \wedge, \vee$ や量化子 $\forall, \exists$ のような**論理記号** (*logical symbol*) だけではなく，和 $+$, 積 $\cdot$, 順序 $<$, 数 1 のような**非論理記号** (*non-logical symbol*) が含まれている．このうち，和 $+$ と積 $\cdot$ は関数記号，順序 $<$ は関数記号，数 1 は定数記号と呼ばれる．

定数記号の例:	$0, 1$ など
関数記号の例:	$+, \cdot$ など
関係記号の例:	$<$ など

一階述語論理を扱う際には，まずどのような非論理記号を用いるかを宣言する必要がある．そのような非論理記号を集めたものを言語と呼ぶ．

定義 3.1. 言語 (*language*) とは，記号たちの集合 $\mathcal{L}$ である．ここで，$\mathcal{L}$ は 3 つの集合 $\mathcal{L} = \mathcal{L}_{\mathrm{c}} \cup \mathcal{L}_{\mathrm{f}} \cup \mathcal{L}_{\mathrm{r}}$ に分割されており，$\mathcal{L}_{\mathrm{c}}, \mathcal{L}_{\mathrm{f}}, \mathcal{L}_{\mathrm{r}}$ に属す記号をそれぞれ**定数記号** (*constant symbol*)，**関数記号** (*function symbol*)，**関係記号** (*relation symbol*) と呼ぶ．さらに，各関数記号 $f \in \mathcal{L}_{\mathrm{f}}$ と関係記号 $R \in \mathcal{L}_{\mathrm{r}}$ には**アリティ** (*arity*) と呼ばれる自然数が割り当てられている．アリティ n の関数記号を n 項関数記号，アリティ n の関係記号を n 項関係記号と呼ぶ．

例 3.2. 算術の言語として $\mathcal{L}_{\mathrm{arith}} = \{0, 1, +, \cdot, <\}$ を考える．ここで，$0, 1$ が定数記号であり，$+, \cdot$ は 2 項関数記号，$<$ は 2 項関係記号である．

例 3.3. グラフの言語として $\mathcal{L}_{\mathrm{graph}} = \{E\}$ を考える．ここで，E は 2 項関係記号であり，$E(u, v)$ によって，頂点 u, v が辺によって結ばれていることを表現する．

ところで，算術の言語において，変数記号 $x, y, z, \ldots$ と定数記号 $0, 1$ および関数記号 $+, \cdot$ を組み合わせることによって，記号操作のみによって，いくつかの多項式 (polynomial) を作り上げることができる．このような多項式の概念を一般の言語に拡張したものが項と呼ばれる概念である．

定義 3.4. 言語 $\mathcal{L}$ の**項** (*term*) とは，以下によって帰納的に定義されるものである．

1. 変数記号および定数記号は項である．
2. f が n 項関数記号であり，$t_1, \ldots, t_n$ が項ならば $f(t_1, \ldots, t_n)$ も項である．

例 3.5. 例 3.2 の算術の言語において，$x \cdot x + 1 + 1$ は項である．

例 3.6. 例 3.3 のグラフの言語における項は，変数記号と定数記号のみである．

定義 3.7. 言語 $\mathcal{L}$ の**原子論理式** (*atomic formula*) とは，n 項関係記号 R と項 $t_1, \ldots, t_n$ に対して，$R(t_1, \ldots, t_n)$ の形の式のことを指す．

たとえば，$x \cdot x + 1 + 1 > 1 + 1 + 1$ は原子論理式である．これは $x^2 + 2 > 3$ ということであるが，成立・不成立は変数 x の値などに依存するから何とも言えない．命題論理と比較するならば，気分的には，このような原子論理式 $R(t_1, \ldots, t_n)$ が，命題変数に相当する部分だと思うと分かりやすいかもしれない．もちろん，単なる命題変数という以上の情報は含んでいるのだが．とにかく，一階述語論理式の正確な定義を与えよう．

定義 3.8. 言語 $\mathcal{L}$ の**論理式** (*formula*) とは，以下によって帰納的に定義されるものである．

1. 原子論理式は論理式である．
2. A, B が論理式ならば，以下はいずれも論理式である．

$$A \to B, \qquad A \wedge B, \qquad A \vee B, \qquad \neg A.$$

3. A が論理式であり，x が変数記号ならば，以下も論理式である．

$$\exists x A, \qquad \forall x A.$$

例 3.9. n^2 を $n \cdot n$ の略記だと思うこととすれば，ラグランジュの四平方定理を表す式 (16) は例 3.2 の算術の言語 $\mathcal{L}_{\mathrm{arith}}$ の論理式である．同様に，p が素数であることを表す式 (17) は算術の言語 $\mathcal{L}_{\mathrm{arith}}$ の論理式である．

例 3.10. グラフの頂点 u から v への長さ 2 の路が存在する，という主張は，グラフの言語 $\mathcal{L}_{\mathrm{graph}}$ の以下の論理式として記述できる．

$$(\exists w)\,[E(u, w) \ \wedge \ E(w, v)].$$

定義 3.11. A が $\exists x(\ldots x \ldots)$ または $\forall x(\ldots x \ldots)$ の形の部分論理式を含むとき，その部分の変数記号 x は**束縛変数** (*bounded variable*) として出現しているという．そうでない変数記号は**自由変数** (*free variable*) として出現しているという．

例 3.12. 論理式 $(x = 0) \ \wedge \ \exists x(x \cdot x = 1 + 1)$ について，前者の変数記号 x は自由変数として出現しており，後者の変数記号 x は束縛変数として出現している．

注意. 例 3.12 のように同じ変数記号が自由変数と束縛変数として同時に現れると処理が面倒になる部分が起こる．これを回避するために，自由変数用の記号 $x, y, z, \ldots$ と束縛変数用の記号 $\dot{x}, \dot{y}, \dot{z}, \ldots$ を別々に用意しておくと都合がよい．このとき，例 3.12 の式 $(x = 0) \wedge \exists x(x \cdot x = 1+1)$ は正確には $(x = 0) \wedge \exists \dot{x}(\dot{x} \cdot \dot{x} = 1+1)$ を表しているものと考える．厳密な処理としては，論理式の定義 3.8 の 3 番目の条件について，A が論理式であり x が自由変数記号ならば，$\exists \dot{x} A[\dot{x}/x]$ と $\forall \dot{x} A[\dot{x}/x]$ も論理式である，という形に置き換える．以後は束縛変数記号のドットは明記しないが，暗にこのような処理を行っていると仮定する．

ところで数学に慣れ親しんでいる人であると，量化子の束縛範囲を明示しなかったり，関数記号の始域と終域などに言及がなかったりといったことに違和感を抱くと思う．しかし，構文論的には，束縛範囲の指定は量化子のレベルではなく，論理式のレベルで行う．量化範囲をたとえば $\mathbb{N}$ に限定したいならば，$\mathbb{N}$ の性質を具体的に論理式 $\varphi_{\mathbb{N}}$ として記述し，

$$(\forall x)\,[\varphi_{\mathbb{N}}(x) \ \to \ \ldots]$$

のようにすればよい．たとえば集合論の場合，無限公理によって ω の存在が保証されるから，$\varphi_{\mathbb{N}}(x)$ として式 $x \in \omega$ を用いればよい．一方，言語や理論などによっては $\varphi_{\mathbb{N}}$ に相当するものを必ずしも定義できるわけではない．

3.2 構文論

それでは一階述語論理の推件計算を考えよう．ここでも同様に，推件式を取り扱う．一階述語論理における推件式の「意図」を説明するために，まず $\bar{x} = x_0, \ldots x_i$ を推件式中に現れる全ての自由変数のリストとしよう．すると，推件式は以下のように記述できる．

$$A_0(\bar{x}), A_1(\bar{x}), \ldots, A_m(\bar{x}) \vdash B_0(\bar{x}), B_1(\bar{x}), \ldots, B_n(\bar{x}). \tag{18}$$

さて，命題論理の場合を思い出すと，推件式が証明可能ということは，その式に含まれる命題変数に如何なる真理値が割り当てられようとも真になる，ということと同値であった．同様に，述語論理の場合も，推件式 (18) が証明可能という場合，自由変数 $\bar{x}$ に如何なる値 $\bar{y} = y_0, \ldots, y_i$ が代入されようとも証明可能であるに違いない．

$$A_0(\bar{y}), A_1(\bar{y}), \ldots, A_m(\bar{y}) \vdash B_0(\bar{y}), B_1(\bar{y}), \ldots, B_n(\bar{y}).$$

ただし，命題論理の場合とは違って，述語論理の場合は少し注意が必要であり，$\bar{y}$ に含まれる変数記号が既に束縛されている可能性がある．束縛変数記号を代入するのはまずいので，その状況は除外しよう．つまり，正確には，上記の $\bar{y}$ には $A_0, \ldots, A_m, B_0, \ldots, B_n$ の束縛変数は含まれないということを要請していると仮定する．

このような推件式の「意図」を念頭において，一階述語論理の推論規則を導入していこう．まず，以下の推論が妥当であることは納得できると思う．

$$\frac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A(x)}\ (\exists \text{ 右}) \qquad\qquad \frac{A(t) \vdash \Delta}{\forall x A(x) \vdash \Delta}\ (\forall \text{ 左})$$

念のため詳細な説明を与えよう．存在量化 $\exists$ の右規則は，こう述べる．何らかの t によって $A(t)$ が満たされるということは，特に $\exists x A(x)$ が満たされているということである．全称量化 $\forall$ の左規則は，こう述べる．$A(t)$ を仮定して Δ を導けるならば，当然 $\forall x A(x)$ の方がより強い仮定であるから，$\forall x A(x)$ を仮定すれば Δ を導ける．

一方，全称記号 $\forall$ の右規則と存在記号 $\exists$ の左規則は少し分かりづらい．具体的に推論規則を書き下す前に，次の状況を考えよう．

$$\Gamma \vdash A(z) \qquad\qquad B(z) \vdash \Delta$$

ただし，「Γ **や** Δ **の中に** z **は現れない**」ものとする．ところで，推件式に現れる自由変数 z には，束縛変数を含まないどんな項 y を代入してもよいのだった．また，「Γ **や** Δ **の中に** z **は現れない**」という仮定より，記号 z をどんな値 y に置き換えても，Γ と Δ の部分は変化しない．

$$\Gamma \vdash A(y) \qquad\qquad B(y) \vdash \Delta \tag{19}$$

さて，ここで重要なことは，束縛変数を含まない任意の y について推件式 (19) が成立しているという点である．左の推件式については，言い換えれば，任意の元 x について $A(x)$ が成立する，つまり $\forall x A(x)$ である．非形式的にこれを式で表すとすれば，以下のようになる．

$$\frac{\Gamma \vdash A(z) \qquad z \text{ は } \Gamma \text{ の中に現れない．}}{\Gamma \vdash \forall x A(x)} \ (\forall \text{ 右})$$

つづいて，$\exists x B(x)$ を仮定してみると，ある y について $B(y)$ である．しかし，(19) は任意の y について成り立っているのだから，(19) の右の推件式より，Δ が導かれる．つまり，$\exists x B(x) \vdash \Delta$ である．非形式的にこれを式で表すと，以下のようになる．

$$\frac{B(z) \vdash \Delta \qquad z \text{ は } \Delta \text{ の中に現れない．}}{\exists x B(x) \vdash \Delta} \ (\exists \text{ 左})$$

さて，上では，$A(x)$ のように論理式 A 中に現れる自由変数を明示したが，以後は単に A と書き，自由変数は明示しない．この場合，A の変数 x の部分に y を代入する，という操作を $A(y)$ と書く代わりに，$A[y/x]$ と書く．以上の観測の下，一階述語論理の体系 LK の推論規則は次によって与えられる．

定義 3.13 (一階述語論理の体系 LK)**.**

$$\frac{A[t/x], \Gamma \vdash \Delta}{\forall x A, \Gamma \vdash \Delta} \ (\forall \text{ 左}) \qquad \frac{\Gamma \vdash \Delta, A[z/x]}{\Gamma \vdash \Delta, \forall x A} \ (\forall \text{ 右})$$

$$\frac{A[z/x], \Gamma \vdash \Delta}{\exists x A, \Gamma \vdash \Delta} \ (\exists \text{ 左}) \qquad \frac{\Gamma \vdash \Delta, A[t/x]}{\Gamma \vdash \Delta, \exists x A} \ (\exists \text{ 右})$$

ここで自由変数 z は下式には現れないものとする．このように z が渦中の論理式 A 以外の部分には現れない，という性質を**変数条件** (*eigenvariable condition*) と言う．

まず，証明の具体例として，$\forall$ と $\exists$ の双対性を示そう．

命題 3.14. $\forall x \neg A \leftrightarrow \neg \exists x A$ は LK で証明可能である．

Proof. 以下の証明図によって示される．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A[z/x] \vdash A[z/x]}{\neg A[z/x], A[z/x] \vdash} \ (\neg \text{ 左})}{A[z/x], \forall x \neg A \vdash} \ (\forall \text{ 左})}{\exists x A, \forall x \neg A \vdash} \ (\exists \text{ 左})}{\forall x \neg A \vdash \neg \exists x A} \ (\neg \text{ 右})}{\vdash \forall x \neg A \to \neg \exists x A} \ (\to \text{ 右})$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A[z/x] \vdash A[z/x]}{\vdash A[z/x], \neg A[z/x]} \ (\neg \text{ 右})}{\vdash \exists x A, \neg A[z/x]} \ (\exists \text{ 右})}{\vdash \exists x A, \forall x \neg A} \ (\forall \text{ 右})}{\neg \exists x A \vdash \forall x \neg A} \ (\neg \text{ 左})}{\vdash \neg \exists x A \to \forall x \neg A} \ (\to \text{ 右})$$

□

全称記号 $\forall$ の右規則と存在記号 $\exists$ の左規則について，上式と下式は以下のようにひっくり返すことができることを示しておくと便利である．

補題 3.15 ($\forall$ と $\exists$ の除去)**.** LK$'$ において，以下の派生規則を導くことができる．つまり，以下のそれぞれについて，公理または上式を始式とし下式を終式とするような LK$'$ の証明図が存在する．

$$\frac{\Gamma \vdash \Delta, \forall x A}{\Gamma \vdash \Delta, A[t/x]} \qquad \frac{\exists x A, \Gamma \vdash \Delta}{A[t/x], \Gamma \vdash \Delta}$$

Proof. 全称記号 $\forall$ については，以下の証明図による．

$$\dfrac{\Gamma \vdash \Delta, \forall x A \qquad \dfrac{A[t/x] \vdash A[t/x]}{\forall x A \vdash A[t/x]}\,(\forall \text{左})}{\Gamma \vdash \Delta, A[t/x]}\,(\text{カット})$$

存在記号 $\exists$ については，以下の証明図による．

$$\dfrac{\dfrac{A[t/x] \vdash A[t/x]}{A[t/x] \vdash \exists x A}\,(\exists \text{右}) \qquad \exists x A, \Gamma \vdash \Delta}{A[t/x], \Gamma \vdash \Delta}\,(\text{カット})$$

□

さて，$A \to B$ という論理式や $A \vdash B$ という形の推件式を見たとき，直感的にはこれらは縦方向の推論 $\frac{A}{B}$ と同様の意味を持っているように思える．つまり，我々は $A \to B$, $A \vdash B$, $\frac{A}{B}$ のいずれも「A ならば B」と解釈しているようである．実際にこれらは形式的に等価なのであろうか．最初の 2 つの等価性については，含意 $\to$ の右規則と補題 1.6 によって保証されるであろう．つづいて，縦向きの推論 $\frac{A}{B}$ を横向きの式 $A \vdash B$ に倒すのは容易である．つまり，規則 $\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, B}$ を仮定すれば，$A, \Lambda \vdash \Delta, B$ は以下のように容易に導ける．

$$\dfrac{\dfrac{A \vdash A}{A, \Lambda \vdash \Delta, A}\,(\text{弱化})}{A, \Lambda \vdash \Delta, B}\,(\Gamma = A, \Lambda \text{ に仮定を適用})$$

後は，横向きの式 $A \vdash B$ を縦向きの図式 $\frac{A}{B}$ として起こすだけである．これは非常に便利な性質であるから，以下のように補題として証明しよう．

補題 3.16. $S \equiv \forall \bar{x}(A_0 \wedge \cdots \wedge A_n \to B)$ とする．このとき，以下の派生規則を導くことができる．つまり，公理または上式のいずれかを始式とし下式を終式とするような LK$'$ の証明図が存在する．

$$\frac{S, \Gamma \vdash \Delta, A_0[\bar{t}/\bar{x}] \qquad \ldots \qquad S, \Gamma \vdash \Delta, A_n[\bar{t}/\bar{x}]}{S, \Gamma \vdash \Delta, B[\bar{t}/\bar{x}]}$$

Proof. $n = 1$ の場合のみ示す．以下，Γ, Δ は省略する．このとき，$A \equiv A_0 \wedge A_1$ について，

$$\dfrac{\dfrac{\dfrac{S \vdash A_0[t/x] \qquad S \vdash A_1[t/x]}{S \vdash A_0[t/x] \wedge A_1[t/x]}\,(\wedge\text{右})}{S \vdash A[t/x]}\,(A\text{の定義}) \qquad \dfrac{\dfrac{\dfrac{\forall x(A \to B) \vdash \forall x(A \to B)}{S \vdash \forall x(A \to B)}\,(S\text{の定義})}{S \vdash (A \to B)[t/x]}\,(\text{補題 3.15})}{S \vdash A[t/x] \to B[t/x]}\,(\text{補題 1.6})}{A[t/x], S \vdash B[t/x]}\,(\text{カット})$$
$$S \vdash B[t/x]$$

□

3.3 数学的公理と形式証明*

さて，ここまでで述語論理を導入したが，実際には数学的な議論はどのように形式的に表されるだろうか．数学を形式的に取り扱う場合，幾つかの付加的な公理を前提として，結論を導く操作として扱われる．付加的な公理とは，たとえば**群の公理**であるとか**体の公理**であるとか**ペアノ算術の公理**であるとか ZFC **集合論**であるとかいったものである．このような付加的な公理の集まりのことを**公理系**や**理論**と言ったりする．本稿で最初に取り上げる公理系は，上に挙げた中では，群の公理や体の公理のようなタイプのものである．

定義 3.17. $\mathcal{L}$**-理論** ($\mathcal{L}$*-theory*) とは，$\mathcal{L}$-文の集合のことを指す．

$\mathcal{L}$-理論は無限集合でもよい．たとえば，ペアノ算術などの自然数論は，和と積などに関する有限個の公理と，数学的帰納法を表す公理図式を持つ．ここで，論理式毎に数学的帰納法を公理に加える必要があるので，公理は無限個になる．

代数学の講義などで初めて群を習ったとき，群の公理からたとえば単位元の一意性や逆元の一意性などが導かれることを学んだかもしれない．これを形式的に理解すると，

$$\text{群の公理} \vdash \text{単位元の一意性} \qquad\qquad \text{群の公理} \vdash \text{逆元の一意性}$$

という推件を LK によって証明可能である，と言い換えられるに違いない．

定義 3.18. $\mathcal{L}$-理論 T において論理式 B が**証明可能** (*provable*) であるとは，ある有限個の $A_1, \ldots, A_n \in T$ が存在して，$A_1, \ldots, A_n \vdash B$ が証明可能であることを意味する．このとき，$T \vdash B$ と書く．

厳密には，「一意性」を論理式として記述するためには等号記号 $=$ が必要であり，**等号に関する公理**もこの証明のためには必要である．

定義 3.19 (同値関係)**.** $\sim$ を 2 変数関係記号とする．このとき，$\sim$ に対する**同値関係** (*equivalence relation*) の公理は以下によって与えられる．

$$
\begin{array}{ll}
\text{反射律:} & \forall x(x \sim x) \\
\text{対称律:} & \forall x, y(x \sim y \to y \sim x) \\
\text{推移律:} & \forall x, y, z[(x \sim y \wedge y \sim z) \to x \sim z]
\end{array}
$$

$\mathsf{ER}_\sim$ によって $\sim$ に対する同値関係の公理の集まりを表すものとする．補題 3.16 の帰結として，以下が派生規則として導けることに注意する．

$$
\frac{\mathsf{ER}_\sim, \Gamma \vdash \Delta, x \sim y}{\mathsf{ER}_\sim, \Gamma \vdash \Delta, y \sim x} \qquad \frac{\mathsf{ER}_\sim, \Gamma \vdash \Delta, x \sim y \qquad \mathsf{ER}_\sim, \Gamma \vdash \Delta, y \sim z}{\mathsf{ER}_\sim, \Gamma \vdash \Delta, x \sim z}
$$

定義 3.20 (合同関係)**.** $*$ を 2 変数関数記号，$\equiv$ を 2 変数関係記号とする．このとき，$\{*, \equiv\}$ に対する**合同関係** (*congruence relation*) の公理は以下によって与えられる．

$$
\begin{array}{c}
\equiv \text{に対する同値関係の公理} \\
\mathsf{E}_{*,\equiv}\colon \quad (\forall x_0, x_1, y_0, y_1)\,[(x_0 \equiv y_0 \ \wedge \ x_1 \equiv y_1) \ \to \ x_0 * x_1 \equiv y_0 * y_1]
\end{array}
$$

$\mathsf{CR}_{*,\equiv}$ によって $\{*, \equiv\}$ に対する合同関係の公理の集まりを表すものとする．上と同様に，補題 3.16 の帰結として，横向きの式 $E_{*,\equiv}$ を縦向きに起こすことにより，以下が派生規則として導ける．

$$
\frac{\mathsf{CR}_{*,\equiv}, \Gamma \vdash \Delta, x_0 \equiv y_0 \qquad \mathsf{CR}_{*,\equiv}, \Gamma \vdash \Delta, x_1 \equiv y_1}{\mathsf{CR}_{*,\equiv}, \Gamma \vdash \Delta, x_0 * x_1 \equiv y_0 * y_1}
$$

以下，$\mathsf{CR}_{*,\equiv}$ を単に CR と略記する．$\mathsf{E}_{*,\equiv}$ は $*$ による $\equiv$ の保存性しか保証していないが，実際には任意の項の適用で $\equiv$ を保存することを証明できる．つまり，与えられた項 $s(x)$ に同値な項 p, q を代入した結果 $s(p), s(q)$ は同値であることを以下のように証明する．

補題 3.21. 任意の項 s, t と束縛変数を含まない項 p, q および自由変数 x について，以下の派生規則が証明できる．

$$
\frac{\mathsf{CR}, \Gamma \vdash \Delta, s[p/x] \equiv t \qquad \mathsf{CR}, \Gamma \vdash \Delta, p \equiv q}{\mathsf{CR}, \Gamma \vdash \Delta, s[q/x] \equiv t}
$$

Proof. 項 s の構成に関する帰納法により，以下の図式を派生規則として導出できることを示す．

$$
\frac{\mathsf{CR}, \Gamma \vdash \Delta, p \equiv q}{\mathsf{CR}, \Gamma \vdash \Delta, s[p/x] \equiv s[q/x]} \tag{20}
$$

s が変数記号ならば明らかである．さもなくば，$s = s_0 * s_1$ の形である．以下，s_i^p と s_i^q を $s_i[p/x]$ と $s_i[q/x]$ の略記とする．s^p と s^q も同様である．また，記述の単純化のため，以下では Γ, Δ の部分を省略して書く．まず，帰納的仮定より次の証明図を得る．

$$
\dfrac{\dfrac{\dfrac{\mathsf{CR} \vdash p \equiv q}{\mathsf{CR} \vdash s_0^p \equiv s_0^q}\ \text{(帰納的仮定)} \qquad \dfrac{\mathsf{CR} \vdash p \equiv q}{\mathsf{CR} \vdash s_1^p \equiv s_1^q}\ \text{(帰納的仮定)}}{\mathsf{CR} \vdash s_0^p * s_1^p \equiv s_0^q * s_1^q}\ \text{(補題 3.16: } \mathsf{E}_{\equiv,*}\text{)}}{\mathsf{CR} \vdash s^p \equiv s^q} \tag{21}
$$

よって，帰納法により派生規則 (20) は示された．同様の議論により，

$$\dfrac{\dfrac{\dfrac{\mathsf{CR} \vdash p \equiv q}{\mathsf{CR} \vdash s^p \equiv s^q}\ (\text{図式 (20)})}{\mathsf{CR} \vdash s^q \equiv s^p}\ (\text{補題 3.16: 対称律}) \qquad \mathsf{CR} \vdash s^p \equiv t}{\mathsf{CR} \vdash s^q \equiv t}\ (\text{補題 3.16: 推移律})$$

□

先に述べたような簡単な代数的定理を形式的に証明してみよう．形式的に取り扱う場合，群は最初の例としては少し複雑すぎるので，もう少し単純なモノイドと呼ばれる概念をここでは扱う．

定義 3.22 (モノイド)**.** $*$ を 2 変数関数記号，e を定数記号とする．このとき，$(*, e)$ に対する**モノイド** (*monoid*) の公理は以下によって与えられる．

$$\begin{aligned} \text{結合法則:} &\quad \forall a, b, c((a * b) * c = a * (b * c)) \\ \text{単位元:} &\quad \forall a(a * e = e * a = a) \end{aligned}$$

いま，言語 $\mathcal{L} = \{e, \cdot, =\}$ を考え，次の公理からなる理論 M を考えよう．

- $(\cdot, e)$ に関するモノイドの公理
- $(\cdot, =)$ に関する合同関係の公理

例 3.23. 理論 M において，「任意の x, y, z について，もし y が x の右逆元であり，z が x の左逆元ならば，$y = z$ である」ということが証明できる．つまり，以下が LK で証明可能である．

$$\mathsf{M} \vdash \forall x, y, z\ [(x \cdot y = e\ \wedge\ z \cdot x = e)\ \rightarrow\ y = z].$$

Proof. まず，次に注意する．

$$\dfrac{\dfrac{\dfrac{\mathsf{M},\ a \cdot b = e,\ c \cdot a = e \vdash b = c}{\mathsf{M},\ a \cdot b = e \wedge c \cdot a = e \vdash b = c}\ (\text{縮約; } \wedge \text{ 左})}{\mathsf{M} \vdash (a \cdot b = e \wedge c \cdot a = e) \rightarrow b = c}\ (\rightarrow \text{右})}{\mathsf{M} \vdash \forall x, y, z\ [(x \cdot y = e\ \wedge\ z \cdot x = e)\ \rightarrow\ y = z]}\ (\forall \text{ 右})$$

したがって，上の図式の始式が LK で証明可能であることを示せばよい．つまり，$\Gamma = (a \cdot b = e, c \cdot a = e)$ とおくと，目標は $\mathsf{M}, \Gamma \vdash b = c$ を示すことである．

まず，$\forall$ 除去補題 3.15 の応用として，以下を得る．

$$\dfrac{\dfrac{\mathsf{M} \vdash e \text{ は } \cdot \text{ の単位元}}{\mathsf{M} \vdash \forall x(x = e \cdot x)}\ (\text{補題 3.15})}{\mathsf{M} \vdash b = e \cdot b} \qquad \dfrac{\dfrac{\mathsf{M} \vdash e \text{ は } \cdot \text{ の単位元}}{\mathsf{M} \vdash \forall x(x \cdot e = x)}\ (\text{補題 3.15})}{\mathsf{M} \vdash b = e \cdot b}$$

$$\dfrac{\dfrac{\mathsf{M} \vdash \cdot \text{ の結合則}}{\mathsf{M} \vdash \forall x, y, z\ (x \cdot y) \cdot z = x \cdot (y \cdot z)}\ (\text{補題 3.15})}{\mathsf{M} \vdash (c \cdot a) \cdot b = c \cdot (a \cdot b)}$$

以下が通常の単位元の一意性証明の本体となる．簡単のために $M, \Gamma \vdash$ の部分は省略して書く．以下の推論には補題 3.21 を用いていることに注意する．

$$\dfrac{\dfrac{\dfrac{\dfrac{e \text{ は } \cdot \text{ の単位元}}{b = e \cdot b} \qquad c \cdot a = e}{b = (c \cdot a) \cdot b} \qquad \dfrac{\cdot \text{ の結合則}}{(c \cdot a) \cdot b = c \cdot (a \cdot b)}}{b = c \cdot (a \cdot b)} \qquad a \cdot b = e}{b = c \cdot e} \qquad \dfrac{e \text{ は } \cdot \text{ の単位元}}{c \cdot e = c}$$
$$b = c$$

□

3.4 意味論

命題論理と同様に，述語論理における論理式に対する真理値を考えることができる．このために，命題論理における付値に相当するものを述語論理にも導入する必要があるだろう．命題変数に真理値を割り当てるものが付値であったから，原子論理式に真理値を割り当てればよいと思うかもしれない．しかし，原子論理式は単なる命題変数より細かい情報を持つから，直接，真理値を割り当てるより良い方法がある．各記号へ**意味**を与えることによって，自動的に原子論理式へ真理値は割り当てられる．各記号に意味を与えるものが，**構造**と呼ばれる概念である．

定義 3.24. 言語 $\mathcal{L}$ における**構造** (*structure*) とは，$\mathcal{U} = (U; c^{\mathcal{U}}, f^{\mathcal{U}}, R^{\mathcal{U}})_{c \in \mathcal{L}_{\mathrm{c}}, f \in \mathcal{L}_{\mathrm{f}}, R \in \mathcal{L}_{\mathrm{r}}}$ である．

1. U は空でない集合であり，これを $\mathcal{U}$ の領域と呼ぶ．
2. 各定数記号 c について，$c^{\mathcal{U}} \in U$ である
3. 各 n 変数関数記号 f について，$f^{\mathcal{U}} \colon U^n \to U$ である．
4. 各 n 変数関係記号 R について，$R^{\mathcal{U}} \subseteq U^n$ である．

例 3.25. モノイドの言語 $\mathcal{L}_{\mathrm{mono}} = \{*, e\}$ に対して，各記号を和と 0 として解釈し，$*^{\mathcal{N}} = +$, $e^{\mathcal{N}} = 0$ を考えると，$\mathcal{N} = (\mathbb{N}; +, 0) = (\mathbb{N}; *^{\mathcal{N}}, e^{\mathcal{N}})$ は $\mathcal{L}_{\mathrm{mono}}$-構造である．同様に，各記号を積と 1 として解釈し，$*^{\mathcal{N}'} = \cdot$, $e^{\mathcal{N}'} = 1$ を考えると，$\mathcal{N}' = (\mathbb{N}; \cdot, 1) = (\mathbb{N}; *^{\mathcal{N}'}, e^{\mathcal{N}'})$ も $\mathcal{L}_{\mathrm{mono}}$-構造である．

$\mathcal{L}$-構造 $\mathcal{U}$ が与えられれば，自由変数を含まない $\mathcal{L}$-項 t の $\mathcal{U}$ での解釈 $t^{\mathcal{U}}$ も帰納的に導入できる．具体的には，$t = f(t_1, \ldots, t_n)$ であり，$t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}}$ が既に与えられているならば，$t^{\mathcal{U}} = f^{\mathcal{U}}(t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}})$ で定義すればよい．もし $t_1, \ldots, t_n$ が閉項ならば，$t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}} \in U$ であるから，$(t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}}) \in R^{\mathcal{U}}$ の真偽について議論できる．つまり，構造 $\mathcal{U}$ による原子文 $R(t_1, \ldots, t_n)$ の真理値割り当ては，$(t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}}) \in R^{\mathcal{U}}$ の真偽によって行われる．命題論理の場合と同様に，原子論理式の真偽が決まれば，任意の文の真偽は定まる．

定義 3.26. $\mathcal{L}$-構造 $\mathcal{U}$ と $\mathcal{L}$-文 φ が与えられているとき，$\mathcal{U}$ で φ が真であることを表す記法 $\mathcal{U} \models \varphi$ を以下のように帰納的に定義する．

1. φ が原子文 $R(t_1, \ldots, t_n)$ ならば，

$$\mathcal{U} \models \varphi \iff R^{\mathcal{U}}(t_1^{\mathcal{U}}, \ldots, t_n^{\mathcal{U}}) \text{ が成立する．}$$

2. 論理結合子については，以下のように定義する．

$$\begin{aligned}
\mathcal{U} \models \neg\psi &\iff \mathcal{U} \models \psi \text{ でない} \\
\mathcal{U} \models \psi \wedge \theta &\iff \mathcal{U} \models \psi \text{ かつ } \mathcal{U} \models \theta \\
\mathcal{U} \models \psi \vee \theta &\iff \mathcal{U} \models \psi \text{ または } \mathcal{U} \models \theta \\
\mathcal{U} \models \psi \to \theta &\iff \mathcal{U} \models \psi \text{ ならば } \mathcal{U} \models \theta
\end{aligned}$$

3. 量化子については，以下のように定義する．

$$\begin{aligned}
\mathcal{U} \models \forall x\psi &\iff \text{任意の } a \in \mathcal{U} \text{ に対して, } \mathcal{U} \models \psi[a/x] \\
\mathcal{U} \models \exists x\psi &\iff \text{ある } a \in \mathcal{U} \text{ が存在して, } \mathcal{U} \models \psi[a/x]
\end{aligned}$$

例 3.27.

$\mathbb{N} \models (\exists x)(\forall y)\ x + y \neq 0$	$\mathbb{Z} \models (\forall x)(\exists y)\ x + y = 0$
$\mathbb{N} \models (\forall x, y)\ x \cdot y = y \cdot x$	$M_2(\mathbb{Z}) \models (\exists x, y)\ x \cdot y \neq y \cdot x$
$\mathbb{Z} \models (\exists x)\ [x \neq 0\ \wedge\ (\forall y)\ x \cdot y \neq 0]$	$\mathbb{Q} \models (\forall x)\ [x \neq 0\ \to\ (\exists y)\ x \cdot y = 0]$
$\mathbb{R} \models (\forall x, y)\ [x \cdot y = 0\ \to\ (x = 0\ \vee\ y = 0)]$	$M_2(\mathbb{Z}) \models (\exists x, y)\ [x \cdot y = 0\ \wedge\ (x \neq 0\ \wedge\ y \neq 0)]$
$\mathbb{N} \models (\exists x)(\forall y)\ x \leqslant y$	$\mathbb{Z} \models (\forall x)(\exists y)\ y < x$
$\mathbb{Z} \models (\exists x, y)\ [x < y\ \wedge\ (\forall z)\ \neg[x < z < y]]$	$\mathbb{Q} \models (\forall x, y)\ [x < y\ \to\ (\exists z)\ x < z < y]$

定義 3.28. T が理論であるとする．構造 $\mathcal{U}$ が理論 T の**モデル** (*model*) であるとは，$\mathcal{U} \neq \varnothing$ であり，任意の $\varphi \in T$ について $\mathcal{U} \models \varphi$ となることである．このとき，$\mathcal{U} \models T$ と書く．

有向グラフの公理，半順序の公理のモデルなど……

例 3.29. 群の公理のモデルのことを**群**と呼ぶ．

3.5 完全性定理

数学において，たとえば，「群の公理から逆元の一意性を導ける」ということを証明する場合，通常，群の公理から逆元の一意性の形式的な証明を書くことはあまりない．実際にはどのような証明を行うかといえば，「任意の群 G に対して，G の単位元は唯一である」ということを証明する．これは，以下の同値性が数学では暗黙に用いられているということである．

- 群の公理から A を形式的に証明できる．
- 任意の群 G について，$G \models A$ が成立する．

しかし，このような証明可能性と恒真性との同値性が本当に成り立つ，ということを数学的に証明しなければならないだろう．つまり，述語論理における健全性と完全性を証明したい．

まず，述語論理における推件式の恒真性は次によって定義される．

定義 3.30. 推件式 $\Gamma \vdash \Delta$ が**恒真**であるとは，任意の $\mathcal{L}$-構造 $\mathcal{U}$ に対して，

$$\mathcal{U} \models (\forall \bar{u}) \bigwedge \Gamma \to \bigvee \Delta.$$

ここで，$\bar{u}$ は Γ, Δ に現れる自由変数のリストである．

3.5.1 健全性定理

まずは，述語論理の推件計算が嘘は証明しないこと，つまり健全性を証明しよう．

定理 3.31 (健全性定理)**.** $\Gamma \vdash \Delta$ が証明ならば，$\Gamma \vdash \Delta$ は恒真である．

Proof. 以前と同様に，各推論規則の適用について，上式が恒真ならば下式が恒真であることを示せばよい．

まず存在量化 $\exists$ の右規則について示そう．$\bar{v}$ を出現する自由変数全てのリストとし，$\exists$ の右規則の自由変数を明示的に書くと，次のように表せる．

$$\frac{\gamma(\bar{v}) \vdash \delta(\bar{v}), A(\bar{v}, t(\bar{v}))}{\gamma(\bar{v}) \vdash \delta(\bar{v}), \exists x A(\bar{v}, x)} \ (\exists \text{ 右})$$

上式が恒真であるということは，任意の $\mathcal{L}$-構造 $\mathcal{U}$ と任意の $\bar{a} \in \mathcal{U}$ に対して，

$$\mathcal{U} \models \gamma(\bar{a}) \to \delta(\bar{a}) \vee A(\bar{a}, t(\bar{a}))$$

が成立するということである．$t(\bar{a}) \in \mathcal{U}$ であることから，明らかに以下を得る．

$$\mathcal{U} \models \gamma(\bar{a}) \to [\delta(\bar{a}) \vee \exists x A(\bar{a}, x)].$$

よって，下式の恒真性は示された．

つづいて，存在量化 $\exists$ の左規則についても，自由変数を明示すると，

$$\frac{A(\bar{v}, z), \gamma(\bar{v}) \vdash \delta(\bar{v})}{\exists x A(\bar{v}, x), \gamma(\bar{v}) \vdash \delta(\bar{v})} \ (\exists \text{ 左})$$

となる．ここで，z の変数条件より，z は $\bar{v}$ の中には含まれないと仮定できる．上式が恒真であるということは，任意の $\mathcal{L}$-構造 $\mathcal{U}$ と任意の $\bar{a}, b \in \mathcal{U}$ に対して，

$$\mathcal{U} \models [A(\bar{a}, b) \wedge \gamma(\bar{a})] \to \delta(\bar{a})$$

が成立するということである．下式が恒真であることを示すために，$\mathcal{U} \models \exists x A(\bar{a}, x)$ かつ $\mathcal{U} \models \gamma(\bar{a})$ を仮定する．このとき，非形式的な記法であるが，以下の手続きに習って $\mathcal{U} \models \delta(\bar{a})$ であることを求めることができる．

$$\dfrac{\dfrac{\mathcal{U} \models \exists x A(\bar{a}, x)}{\text{ある } c \in \mathcal{U} \text{ について，} \mathcal{U} \models A(\bar{a}, c)} \qquad \mathcal{U} \models \gamma(\bar{a})}{\mathcal{U} \models A(\bar{a}, c) \wedge \gamma(\bar{a})} \qquad \dfrac{\text{任意の } b \in \mathcal{U} \text{ に対して，} \mathcal{U} \models [A(\bar{a}, b) \wedge \gamma(\bar{a})] \to \delta(\bar{a})}{\mathcal{U} \models \delta(\bar{a})}$$

全称量化 $\forall$ については，右規則だけ確認しよう．自由変数を明示して書けば，

$$\dfrac{\gamma(\bar{v}) \vdash \delta(\bar{v}), A(\bar{v}, z)}{\gamma(\bar{v}) \vdash \delta(\bar{v}), \forall x A(\bar{v}, x)} \ (\forall \text{ 右})$$

となる．ここで，z の変数条件より，z は $\bar{v}$ の中には含まれないと仮定できる．上式が恒真ということは，任意の $\mathcal{L}$-構造 $\mathcal{U}$ と任意の $\bar{a}, b \in \mathcal{U}$ に対して，

$$\mathcal{U} \models \gamma(\bar{a}) \to (\delta(\bar{a}) \vee A(\bar{a}, b))$$

である．下式の恒真性を示すために，$\mathcal{U} \models \gamma(\bar{a})$ を仮定する．$\mathcal{U} \models \delta(\bar{a}) \vee \forall x A(\bar{a}, x)$ を示したい．$\mathcal{U} \models \delta(\bar{a})$ の場合は明らかであるから，$\mathcal{U} \not\models \delta(\bar{a})$ を仮定する．このとき，以下の手続きに習って $\mathcal{U} \models \forall x A(\bar{a}, x)$ であることを求めることができる．

$$\dfrac{\dfrac{\mathcal{U} \not\models \delta(\bar{a}) \qquad \dfrac{\mathcal{U} \models \gamma(\bar{a}) \qquad \text{任意の } b \in \mathcal{U} \text{ に対して，} \mathcal{U} \models \gamma(\bar{a}) \to \delta(\bar{a}) \vee A(\bar{a}, b)}{\text{任意の } b \in \mathcal{U} \text{ に対して，} \mathcal{U} \models \delta(\bar{a}) \vee A(\bar{a}, b)}}{\text{任意の } b \in \mathcal{U} \text{ に対して，} \mathcal{U} \models A(\bar{a}, b)}}{\mathcal{U} \models \forall x A(\bar{a}, x)}$$

□

健全性定理の応用を 1 つ述べよう．

定義 3.32. T が**矛盾**している (*inconsistent*) とは，$T \vdash \bot$ であることである．

補題 3.33. T を $\mathcal{L}$-理論とし，A の任意の論理式とする．このとき，以下が成立する．

$$T \vdash \bot \iff T \vdash A \text{ かつ } T \vdash \neg A.$$

この結論として，矛盾 $\bot$ のモデルは存在しないことが分かる．つまり任意の構造 $\mathcal{U}$ について，$\mathcal{U} \not\models \bot$ である．

系 3.34. 理論 T がモデルを持つならば，T は無矛盾である．

Proof. 対偶を示す．もし T が矛盾しているならば，ある $A_1, \ldots, A_n \in T$ について，$A_1, \ldots, A_n \vdash \bot$ である．よって，$\vdash A_1 \wedge \cdots \wedge A_n \to \bot$ である．このとき，健全性定理より，任意の構造 $\mathcal{U}$ について，$\mathcal{U} \models A_1 \wedge \cdots \wedge A_n \to \bot$ である．もし $\mathcal{U}$ が T のモデルならば，特に $\mathcal{U} \models A_1 \wedge \cdots \wedge A_n$

である．したがって，$\mathcal{U} \models \bot$ が成り立つが，先に述べたように，これは有り得ない．よって，$\mathcal{U}$ は T のモデルでは有り得ない．つまり，T はモデルを持たない． □

例 3.35. ユークリッド幾何学の公理系を E と書き，平行線公準を P と書こう．E のモデルがユークリッド幾何学であり，$(E-P)+\neg P$ のモデルとして，双曲幾何学や楕円幾何学などの非ユークリッド幾何学が知られている．このとき，系 3.34 より，理論 E と $(E-P)+\neg P$ は共に無矛盾であることが分かる．

3.5.2 完全性定理

矛盾に関する次の性質を後に用いる．

補題 3.36. $T \nvdash A$ ならば $T+\neg A$ は無矛盾である．

Proof. $T+\neg A$ が矛盾すると仮定する．つまり，ある有限列 $\Gamma \subseteq T$ について，$\Gamma, A \to \bot \vdash \bot$ を意味する．このとき，$\Gamma \vdash A$ は次のように証明できる．

$$\dfrac{\dfrac{\Gamma, A \to \bot \vdash \bot}{\Gamma \vdash (A \to \bot) \to \bot}\ (\to \text{右}) \qquad \dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash \bot, A}\ (\text{弱化})}{\vdash A \to \bot, A}\ (\to \text{右}) \qquad \bot \vdash A}{(A \to \bot) \to \bot \vdash A}\ (\to \text{左})}{\Gamma \vdash A}\ (\text{カット})$$

$\Gamma \subseteq T$ であるから，これは $T \vdash A$ を導く． □

定理 3.37 (ゲーデルの完全性定理)**.** 無矛盾な理論はモデルを持つ．

証明は後回しにして，恒真文を全て証明できる，という意味での完全性とどう対応するか説明しよう．

系 3.38. 任意の恒真な推件式は証明可能である．

Proof. 対偶を考える．$\Gamma \vdash \Delta$ が証明不可能とする．これは補題**??**より，$\Gamma \vdash \bigvee \Delta$ が証明不可能であることと同値である．$\delta \equiv \bigvee \Delta$ とする．$\Gamma \nvdash \delta$ なので，Γ を理論だと思うと，補題 3.36 より，$\Gamma + \neg\delta$ は無矛盾である．よって，ゲーデルの完全性定理 3.37 より，$\Gamma + \neg\delta$ のモデル $\mathcal{U}$ が存在する．特に $\mathcal{U} \models \bigwedge \Gamma \wedge \delta$ であるから，$\Gamma \vdash \Delta$ は恒真ではない． □

ゲーデルの完全性定理 3.37 の証明の鍵となる補題を証明しよう．

補題 3.39. T が無矛盾ならば $T+A$ または $T+\neg A$ は無矛盾である．

Proof. 対偶を示す．$T+A$ と $T+\neg A$ は共に矛盾していると仮定すると，ある有限列 $\Gamma_0 \subseteq T$ と $\Gamma_1 \subseteq T$ が存在して，$A, \Gamma_0 \vdash \bot$ かつ $\neg A, \Gamma_1 \vdash \bot$ となる．よって，T が矛盾することは以下のよ

うに証明できる．

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg A, \Gamma_1 \vdash \bot}{\neg A, \Gamma \vdash \bot}\,(\text{弱化・左})}{\Gamma \vdash \bot, \neg\neg A}\,(\neg \text{右}) \qquad \dfrac{\dfrac{A \vdash A}{\vdash A, \neg A}\,(\neg \text{右})}{\neg\neg A \vdash A}\,(\neg \text{左})}{\Gamma \vdash \bot, A}\,(\text{カット}) \qquad \dfrac{A, \Gamma_0 \vdash \bot}{A, \Gamma \vdash \bot}\,(\text{弱化・左})}{\Gamma \vdash \bot}\,(\text{カット})$$

□

補題 3.40. $T + \exists x A$ が無矛盾ならば，新しい定数記号 c について，$T + A[c/x]$ は無矛盾である．

Proof. 対偶を示す．$T + A[c/x]$ は矛盾すると仮定する．このとき，ある有限列 $\Gamma \subseteq T$ について $\Gamma, A[c/x] \vdash \bot$ である．z を $\Gamma, A[c/x] \vdash \bot$ の証明中に現れない任意の変数とする．c は新しい定数記号なので，Γ には含まれないから，$(\Gamma, A[c/x])[z/c] = \Gamma, A[z/x]$ である．つまり，$\Gamma, A[z/x] \vdash \bot$ は証明可能である．z は Γ に現れないから，変数条件を満たすので，存在量化 $\exists$ の左規則を適用可能である．つまり，$\Gamma, \exists x A \vdash \bot$ である．この証明の流れを非形式的に図示すると：

$$\dfrac{\dfrac{\dfrac{\Gamma, A[c/x] \vdash \bot \qquad z \text{ は新しい変数}}{(\Gamma, A[c/x] \vdash \bot)[z/c]} \qquad c \text{ は } \Gamma \text{ に現れない}}{\Gamma, A[z/x] \vdash \bot \qquad z \text{ は新しい変数}}}{\Gamma, \exists x A \vdash \bot}\,(\exists \text{ 右})$$

$\Gamma \subseteq T$ であるから，これは $T + \exists x A$ が矛盾することを導く． □

完全性定理の証明のために，どんな無矛盾な理論もヘンキン拡大と呼ばれる，非常に良い性質を持った理論に拡張できることを示そう．

補題 3.41 (ヘンキン拡大)**.** T を無矛盾な $\mathcal{L}$-理論とする．このとき，次のような言語 $\mathcal{L}_\infty \supseteq \mathcal{L}$ と $\mathcal{L}_\infty$-理論 $T_\infty \supseteq T$ が存在する．

1. T_∞ は無矛盾である．
2. 任意の $\mathcal{L}_\infty$-文 A について，次が成立する．

$$T_\infty \vdash \exists x A \implies T_\infty \vdash A[c/x] \text{ となる定数記号 } c \in \mathcal{L}_\infty \text{ が存在する．}$$

Proof. まず $\mathcal{L}$ における $\exists x A$ の形の各文に対して，これまでの言語に含まれていない新しい定数記号 $c_{\exists x A}$ を準備し，次の公理 $H_{\exists x A}$ を T に加えよう．

$$H_{\exists x A} \quad :\equiv \quad \exists x A \to A[c_{\exists x A}/x]$$

この形の論理式を**ヘンキン公理** (*Henkin axiom*) と呼び，$c_{\exists x A}$ を**ヘンキン定数** (*Henkin constant*) と呼ぶ．T が無矛盾ならば，ヘンキン公理 $H_{\exists x A}$ を加えても無矛盾であることを示す．もしヘンキ

ン公理を加えて矛盾するならば，T の矛盾に至る以下の証明図を得る．

$$\dfrac{\dfrac{T, \exists x A \to A[c_{\exists x A}/x] \vdash \bot}{T \vdash \exists x A, \bot}\ (\text{補題 } 1.6) \qquad \dfrac{\dfrac{T, \exists x A \to A[c_{\exists x A}/x] \vdash \bot}{T, A[c_{\exists x A}/x] \vdash \bot}\ (\text{補題 } 1.6)}{T, \exists x A \vdash \bot}\ (\text{補題 } 3.40)}{T \vdash \bot}\ (\text{カット})$$

よって，$T + H_{\exists x A}$ の無矛盾性が示された．

さて，まず $\mathcal{L}_0 = \mathcal{L}$ とし，$\mathcal{L}_0$ の存在文に対するヘンキン定数の全体を C_0, ヘンキン公理全体の集合を H_0 と書く．上の主張により，$T + H_0$ が無矛盾であることを示せる．これを繰り返し，$\mathcal{L}_n, C_n, H_n$ が既に作られていると仮定したとする．$\mathcal{L}_{n+1} = \mathcal{L}_n \cup C_n$ とし，$\mathcal{L}_n$ の存在文に対するヘンキン定数の全体を C_{n+1}, ヘンキン公理全体の集合を H_{n+1} と書く．帰納的に $T + H_n$ の無矛盾性を示せる．最後に $\mathcal{L}_\infty = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n$, $C_\infty = \bigcup_{n\in\mathbb{N}} C_n$ かつ $H_\infty = \bigcup_{n\in\mathbb{N}} H_n$ と定義する．このとき，$T + H_\infty$ を T の**ヘンキン拡大** (*Henkin extension*) と呼ぶ．主張の T_∞ はこのヘンキン拡大 $T + H_\infty$ によって与えられる．

主張. ヘンキン拡大 $T + H_\infty$ は無矛盾である．

もし $T + H_\infty$ が矛盾するならば，ある有限列 $\Gamma \subseteq T + H_\infty$ について $\Gamma \vdash \bot$ である．しかし，Γ は有限であるから，$\Gamma \subseteq T + H_n$ となる n が存在する．一方，$T + H_n$ は無矛盾であったから，Γ も無矛盾である．よって，$\Gamma \vdash \bot$ は有り得ないから，$T + H_\infty$ は無矛盾である．

主張. 任意の $\mathcal{L}_\infty$-文 A について，次が成立する．

$$T + H_\infty \vdash \exists x A \implies T \cup H_\infty \vdash A[c_{\exists x A}/x]$$

A は $\mathcal{L}_\infty$-文なので，ある m について $\mathcal{L}_m$ 文である．$T + H_\infty \vdash \exists x A$ ならば，ある有限列 $\Gamma \subseteq T + H_\infty$ について $\Gamma \vdash \exists x A$ である．Γ は有限なので，ある $n \geqslant m$ について $\Gamma \subseteq T + H_n$ であるから，特に $T + H_n \vdash \exists x A$ である．このとき，次の証明図を得る．

$$\dfrac{T + H_n \vdash \exists x A \qquad \dfrac{H_{\exists x A} \vdash \exists x A \to A[c_{\exists x A}/x]}{\exists x A, H_{\exists x A} \vdash A[c_{\exists x A}/x]}\ (\text{補題 } 1.6)}{T + H_n + H_{\exists x A} \vdash A[c_{\exists x A}/x]}\ (\text{カット})$$

この $\exists x A$ に対するヘンキン公理 $H_{\exists x A}$ は H_{m+1} に含まれるので，特に H_{n+1} にも含まれる．よって，上の証明図より $T + H_{n+1} \vdash A[c_{\exists x A}/x]$ が導かれる．特に $T + H_\infty \vdash A[c_{\exists A}/x]$ である．また，$c_{\exists x A} \in C_{n+1} \subseteq C_\infty$ であるから，これは $\mathcal{L}_\infty$ の定数記号であり，主張は示された． □

完全性定理 3.37 の証明に入る前に，本稿では言語 $\mathcal{L}$ は可算であるとしよう．言語が非可算である場合も証明のアイデアは大きくは変わらないが，初学者にとって概念的に難しい部分があるため，本稿では取り扱わない．しかし，非可算言語の理論に興味がある読者ならば，可算の場合の証明を手本にすれば，自身の手で容易に証明できるであろう．

*Proof (*言語 $\mathcal{L}$ が可算の場合の完全性定理 *3.37).* 無矛盾な理論 T が与えられたとき，補題 3.41 によってヘンキン拡大した理論 T_∞ を得る．この理論 T_∞ を無矛盾かつ完全な理論 T' に拡張する．ここで，T' が**完全** (*complete*) であるというのは，任意の $\mathcal{L}_\infty$-文 φ に対して，

$$T' \vdash \varphi \text{ または } T' \vdash \neg\varphi$$

が成立することである．この無矛盾かつ完全な理論 T' の構成には，幾分か超越的手法が必要であり，一般には，T' がどんな公理を含むかを判定するアルゴリズムは存在しない．

言語 $\mathcal{L}$ が可算ならば補題 3.41 の $\mathcal{L}_\infty$ も可算であることは容易に分かる．よって，言語の可算性より，$\mathcal{L}_\infty$ の文を $(A_n)_{n\in\mathbb{N}}$ のように具体的に並べることができる．このとき，T'_n を以下のように帰納的に定義する．

$$T'_0 = T_\infty$$
$$T'_{n+1} = \begin{cases} T'_n + A_n & \text{if } T_n + A_n \nvdash \bot \\ T'_n + \neg A_n & \text{if } T_n + A_n \vdash \bot \end{cases}$$

このとき，$T' = \bigcup_{n\in\mathbb{N}} T'_n$ によって定義する．ここで，理論 T' を定義するために理論 $T_n + A_n$ が無矛盾かどうかの場合分けが必要であるが，一般に無矛盾性判定を行うアルゴリズムは存在しないことに注意する．したがって，最終的な T' が A_n と $\neg A_n$ のどちらを公理に持っているかを知る術はない．ただし，どちらが成り立っているか分からない場合分けは数学においては日常茶飯事であり，この議論は数学の中では具体的に定義されている部類である．

主張. T' は無矛盾かつ完全である．

まず，T_∞ は無矛盾であるから，帰納的に T'_n も無矛盾であることを示せる．もし T' が矛盾するならば，T' のある有限部分が矛盾するから，ある n について T'_n が矛盾するはずであるが，これは有り得ない．よって，T' は無矛盾である．また，T' の構成により，任意の n について，$A_n \in T'$ または $\neg A_n \in T'$ が成立しているから，完全性は明らかである．

それでは，T のモデルを構成しよう．$\mathcal{U}$ の領域 U は $\mathcal{L}_\infty$ の項全体の集合とする．

$$U = \mathcal{L}_\infty \text{ の項全体}$$

このとき，各記号の解釈は以下によって与える．

1. c が定数記号ならば，$c^{\mathcal{U}} = c$.
2. f が n 変数関数記号ならば，

$$f^{\mathcal{U}}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n).$$

3. R が n 変数関係記号ならば，

$$R^{\mathcal{U}}(t_1, \ldots, t_n) \iff T' \vdash R(t_1, \ldots, t_n).$$

この $\mathcal{U} = (U; c^{\mathcal{U}}, f^{\mathcal{U}}, R^{\mathcal{U}})_{c,f,R\in\mathcal{L}_\infty}$ が T のモデルになってることを示そう．任意の $\mathcal{L}$-論理式 A について，

$$\mathcal{U} \models A \iff T' \vdash A$$

であることを論理式の複雑さに関する帰納法によって示す．

Case 1. A が原子論理式の場合は定義より自明である．

Case 2. $A \equiv B \vee C$ と仮定する．このとき，

$$\mathcal{U} \models B \vee C \iff \mathcal{U} \models B \text{ または } \mathcal{U} \models C \overset{\text{I.H.}}{\iff} T' \vdash B \text{ または } T \vdash C \iff T \vdash B \vee C.$$

最後の同値性は，T' の無矛盾完全性による．$A \equiv B \wedge C$, $A \equiv B \to C$, $A \equiv \neg B$ の場合も同様に示せる．

Case 3. $A \equiv \exists x B$ と仮定する．

$$\mathcal{U} \models \exists x B \iff \text{ある } t \in U \text{ が存在して } \mathcal{U} \models B[t/x].$$

同様に，理論 T' がヘンキン理論であることから，以下が成立する．

$$T' \vdash \exists x B \iff \text{ある } \mathcal{L}_\infty\text{-項 } t \text{ が存在して } T' \vdash B[t/x].$$

U の定義より，$t \in U$ であることと t が $\mathcal{L}_\infty$-項であることは同値であるから，帰納的仮定より，上の 2 つの式の右辺は同値である．以上より，$U \models \exists x B$ と $T' \vdash \exists x B$ であることは同値であることが示された． □

豆知識. 可算言語に対する完全性定理の証明は，T_∞ の構成が計算不可能性の領域に入るなどの点で，計算論的立場からは極めて超越的である．一方，現代数学においては，これは通常は超越的と見なされない程度の論法である．たとえば選択公理などは用いていない．実際，上の証明は算術的内包公理の体系 ACA_0 の内部でそのまま形式化できる．ここで，ACA_0 は ZF とは比べ物にならないほど弱い理論である．また，上の場合分けによる T' の構成を木構造で解釈することにより，ACA_0 よりも真に弱い体系である WKL_0 ですら，可算言語に対する完全性定理を証明できることが分かる．

演習問題 3.42. T をペアノ算術の公理系であるとすると，完全性定理 *3.37* の証明中の理論 T' はペアノ算術を含む無矛盾かつ完全な理論である．このような理論 T' の存在が，後に述べるゲーデルの不完全性定理とは矛盾していない理由を説明せよ．

4 自然数論の形式体系

4.1 離散順序半環

自然数上の演算の持つ性質を抽象化したい．自然数の代数的性質の分析を行うため，加法の単位元（乗法の零元）である 0 は自然数である $(0 \in \mathbb{N})$ と仮定する．考察する対象は，$(\mathbb{N}, +, \cdot, \leqslant)$ の構造である．たとえば，整数の加法 $(\mathbb{Z}, +)$ はアーベル群をなすが，$(\mathbb{N}, +)$ は逆元を持たないから，

そもそも群ですらない．しかし，可換モノイドではある．$(\mathbb{Z}, +, \cdot)$ や $(\mathbb{R}, +, \cdot)$ は可換環であるが，先程と同じ理由により，$(\mathbb{N}, +, \cdot)$ は環ではない．しかし，環になるためには，加法的逆元が足りないだけであって，だいぶ環に近い．こういうものは**半環** (*semiring*) と呼ばれており，$(\mathbb{N}, +, \cdot)$ は可換半環となる．順序も考慮に入れると，$(\mathbb{Z}, +, \cdot, \leqslant)$ や $(\mathbb{R}, +, \cdot, \leqslant)$ は順序環と呼ばれるものになる．もう少し細かく述べると，$(\mathbb{Z}, +, \cdot, \leqslant)$ は離散順序環であり，$(\mathbb{R}, +, \cdot, \leqslant)$ は離散でない順序環である．そうすると，$(\mathbb{N}, +, \cdot, \leqslant)$ は**離散順序半環**というものであろうことは想像に難くない．

それでは，ここまで書き連ねた内容の正確な定義を述べよう．実際には，ここでは，離散順序半環というよりは，**離散順序環の非負部** (*non-negative parts of discretely ordered rings*) と言った方が正確なものの定義を与える．

定義 4.1 (可換モノイド)**.** $*$ を 2 変数関数記号，e を定数記号とする．このとき，$(*, e)$ に対する**可換モノイド** (*commutative monoid*) の公理は以下によって与えられる．

$$\begin{aligned} \text{結合法則:} &\quad \forall a, b, c((a * b) * c = a * (b * c)) \\ \text{単位元:} &\quad \forall a(a * e = e * a = a) \\ \text{可換性:} &\quad \forall a, b(a * b = b * a) \end{aligned}$$

定義 4.2 (可換半環)**.** $+$ と $\cdot$ を 2 変数関数記号とし，0 と 1 を定数記号とする．このとき，$(+, \cdot, 0, 1)$ に対する**可換半環** (*commutative semiring*) の公理は以下によって与えられる．

$$\begin{aligned} &(+, 0) \text{ は可換モノイドの公理を満たす.} \\ &(\cdot, 1) \text{ は可換モノイドの公理を満たす.} \\ \text{分配律:} &\quad \forall x, y, z(x \cdot (y + z) = x \cdot y + x \cdot z) \\ \text{零元:} &\quad \forall x(x \cdot 0 = 0) \end{aligned}$$

定義 4.3 (全順序)**.** $\leqslant$ を 2 変数関係記号とする．このとき，$\leqslant$ に対する**全順序** (*linear order*) の公理は以下によって与えられる．

$$\begin{aligned} \text{反射律:} &\quad \forall x(x \leqslant x) \\ \text{推移律:} &\quad \forall x, y, z(x \leqslant y \wedge y \leqslant z \to x \leqslant z) \\ \text{反対称律:} &\quad \forall x, y(x \leqslant y \wedge y \leqslant x \to x = y) \\ \text{比較可能律:} &\quad \forall x, y(x \leqslant y \vee y \leqslant x) \end{aligned}$$

定義 4.4 (順序半環)**.** $+$ と $\cdot$ を 2 変数関数記号とし，0 と 1 を定数記号とする．このとき，$(+, \cdot, 0, 1)$ に対する**順序半環** (*ordered semiring*) の公理は以下によって与えられる．

$$\begin{aligned} &(+, \cdot, 0, 1) \text{ は可換半環の公理を満たす.} \\ &\leqslant \text{ は全順序の公理を満たす.} \\ \text{和の順序保存性:} &\quad \forall x, y, z(x \leqslant y \ \to \ x + z \leqslant y + z) \\ \text{非負積の順序保存性:} &\quad \forall x, y, z(0 \leqslant z \wedge x \leqslant y \ \to \ x \cdot z \leqslant y \cdot z) \end{aligned}$$

定義 4.5. $(+, \cdot, \leqslant, 0, 1)$ に対する以下の公理を考える．

$$\begin{aligned} \text{非自明性:} &\quad 0 < 1 \\ \text{離散性:} &\quad \forall x(x > 0 \ \to \ x \geqslant 1) \\ \text{非負性:} &\quad \forall x(x \geqslant 0) \\ \text{加法的逆元:} &\quad \forall x \exists y(x + y = 0) \\ \text{減法:} &\quad \forall x, y(x \leqslant y \ \to \ \exists z(x + z = y)) \end{aligned}$$

非負性を満たす順序半環を**正順序半環** (*positive ordered semiring*), 加法的逆元を持つ順序半環を**順序環** (*ordered ring*), 離散性を満たす順序環を**離散順序環** (*discretely ordered ring*) と呼ぶ.

定義 4.6. 順序半環の公理に非自明性，離散性，非負性，減法の公理を加えたものを**離散順序環の非負部**の公理と呼び，DOR^+ と書く.

つまり，公理 DOR^+ を満たす構造とは，減法の公理を満たす非自明な離散正順序半環である[*2].

例 4.7. 自然数全体のなす構造 $(\mathbb{N}, +, \cdot, \leqslant, 0, 1)$ は，DOR^+ を満たす.

離散順序環は $\mathbb{Z}$ 以外にも沢山ある．同様に，DOR^+ のモデルが $\mathbb{N}$ 以外にも沢山あることは予想できる.

例 4.8. $\mathbb{Z}[X]$ を $\mathbb{Z}$ 上の 1 変数多項式環とする，つまり，

$$\mathbb{Z}[X] = \left\{a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 : n \in \mathbb{N} \ \wedge \ a_0, \ldots, a_n \in \mathbb{Z}\right\}.$$

このとき，$\mathbb{Z}[X]$ が環をなすことはよく知られているが，この上に順序 $\preceq$ を定義することもできる．まず，各多項式 $p \in \mathbb{Z}[X]$ について，$p \succ 0$ とは，p に現れる最大次数の項の係数が非負であることとする．つまり，

$$p = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \succ 0 \iff a_n > 0.$$

一般に，多項式 $p, q \in \mathbb{Z}[X]$ に対して，

$$p \prec q \ \Leftrightarrow \ q - p \succ 0$$

によって順序を定義する．このとき，$(\mathbb{Z}[X], +, \cdot, \preceq, 0, 1)$ は非自明な離散順序環である.

例 4.9. 上で定義した順序 $\preceq$ に対して，次の集合を考える.

$$\mathbb{Z}[X]^+ = \{p \in \mathbb{Z}[X] : p \succeq 0\}.$$

このとき，$(\mathbb{Z}[X]^+, +, \cdot, \preceq, 0, 1)$ は DOR^+ を満たす.

$\mathbb{Z}[X]$ や $\mathbb{Z}[X]^+$ において，順序だけに注目すると，変数 X を無限大の数のように扱っているように思える．たとえば，$\mathbb{Z}[X]^+$ の順序型としては，始切片として標準自然数 $\mathbb{N}$ があって，その無限の彼方に，無限大元たちの住む「整数の形の島」たちが無限に並んでいるような形をしている．より正確には，以下によって定義される $[p]$ を各 p の所属する “島” のように考える.

$$[p] = \{q \in \mathbb{Z}[X]^+ : (\exists k \in \mathbb{Z})\ q = p + k\}.$$

[*2] この公理は，ペアノ算術の公理系 PA と関連付けて語られることが多く，その場合には，DOR^+ ではなく PA^- と書かれることが多い.

すると，自然数定数の所属する島 $[n]$ の無限の彼方に $\mathbb{Z}$-型の島 $[X]$ があって，その更に無限の彼方に $[2X]$, $[3X]$, といった島が無限に連なっており，といったことが見て取れるだろう．

$$[n] \prec [X] \prec [2X] \prec [3X] \prec \cdots \prec [X^2 - 2X] \prec [X^2 - X] \prec [X^2] \prec [X^2 + X] \prec \ldots$$
$$\cdots \prec [2X^2 - 6X] \prec [2X^2 + 3X] \prec [3X^2 - X] \prec \cdots \prec [X^3 - 6X^2 - 9X] \prec \ldots$$

例 4.10. 任意の非自明な離散順序環 $(R, +, \cdot, \leq, 0, 1)$ に対して，$R^+ = \{x \in R : x \geq 0\}$ と定義すると，$(R^+, +, \cdot, \leq, 0, 1)$ は DOR^+ を満たす．

豆知識. 逆に，DOR^+ の任意のモデル $\mathcal{M}$ に対して，ある非自明な離散順序環 R が存在して，$\mathcal{M}$ は R の非負部 R^+ と同型になる．これによって，DOR^+ を「離散順序環の非負部の公理」と呼ぶことは正当化されるであろう．

離散順序環の非負部の公理 DOR^+ は自然数の基本演算に関するかなりの部分を捉えるが，それでもやはり完璧には程遠い．たとえば，離散順序環の非負部の公理から「全ての元を偶数と奇数に類別できる」といったようなことを演繹することはできない．ちょうどよい《**証明不可能性の証明**》の練習問題なので，これを確認してみよう．

命題 4.11. $\mathsf{DOR}^+ \nvdash (\forall x)(\exists y)\,[2y = x \vee 2y + 1 = x]$.

Proof. DOR^+ のあるモデルが偶数でも奇数でもない元を持つことを示せばよい．実際，例 4.9 で定義した DOR^+ のモデル $\mathbb{Z}[X]^+$ には，偶数でも奇数でもない元が存在する．$q = a_n X^n + \cdots + a_0$ とすると，$2q = 2a_n X^n + \cdots + 2a_0$ であり，$2q + 1 = 2a_n X^n + \cdots + 2a_0 + 1$ である．したがって，多項式 p の次数正の項の係数が全て偶数でない限り，$p = 2q$ または $p = 2q + 1$ という形には書けないことが分かる．たとえば，X や $3X^2$ などは偶数でも奇数でもない． □

4.2 Σ_1-完全性

命題 4.11 で見たように，わりと自明そうな自然数の性質でも DOR^+ から導出できない可能性がある．しかし，実は，自然数 $\mathbb{N}$ に関する存在型の性質であれば，DOR^+ から導出できることを見ていこう．このために，自然数に関する性質の量化の複雑性による分類の概念を導入する．

言語 $\mathcal{L}_{\mathsf{arith}} = \{+, \cdot, \leqslant, 0, 1\}$ を考える．略記 $(\forall x \leqslant t)\varphi$ および $(\exists x \leqslant t)\varphi$ を以下によって定義する．

$$(\forall x \leqslant t)\varphi \iff (\forall x)\,[x \leqslant t \;\to\; \varphi],$$
$$(\exists x \leqslant t)\varphi \iff (\exists x)\,[x \leqslant t \;\wedge\; \varphi].$$

この形の量化を**有界量化** (*bounded quantification*) と呼ぶ．一方，$\forall x\varphi$ や $\exists x\varphi$ の形の量化を**非有界量化** (*unbounded quantification*) と呼ぶ．

定義 4.12. 非有界量化を用いずに構成される論理式を Δ_0 **論理式** (Δ_0-*formula*) と呼ぶ．本稿では，非有界全称量化を用いずに構成される論理式を Σ_1 **論理式** (Σ_1-*formula*) と呼ぶ．また，ある

Δ_0 論理式 θ に対して $\exists x\theta$ の形で書ける論理式を**狭義の Σ_1 論理式** (*strict Σ_1-formula*) と呼ぶ[*3]. 同様に，ある Δ_0 論理式 θ に対して $\forall x\theta$ の形で書ける論理式を Π_1 **論理式** (Π_1-*formula*) と呼ぶ.

豆知識. 広義と狭義の Σ_1 が同値であるという性質は，Σ_1-採集原理 $\mathrm{B}\Sigma_1$ と呼ばれる公理と同値である．この公理は，Σ_1-帰納法公理 $\mathsf{I}\Sigma_1$ (定義 4.24) から証明することができる.

例 4.13. 「x は素数である」ということを表す式 $\mathrm{Prime}(x)$ は Δ_0 論理式である.

$$\mathrm{Prime}(x) \equiv (\forall y \leqslant x)\ [[(\exists z \leqslant x)\ x = z \cdot y] \ \to\ (y = 1\ \vee\ y = x)].$$

例 4.14. 以下，x^3 は項 $x \cdot x \cdot x$ の略記であるとする.

- 次の式は Σ_1 論理式である.

$$(\exists a, b, c, d)\ [a, b, c \geqslant 1\ \wedge\ a^3 + b^3 + c^3 = d^3].$$

- フェルマーの最終定理の $n = 3$ のとき (オイラーの定理) を表す次の式は Π_1 論理式である.

$$(\forall a, b, c)\ [a, b \geqslant 1\ \to\ a^3 + b^3 \neq c^3].$$

豆知識. 例 4.14 の Σ_1 論理式は真である．たとえば，$a = 3$, $b = 4$, $c = 5$, $d = 6$ がこれを満たすことはプラトンにより発見された.

問題 4.15. ゴールドバッハ予想，双子素数予想はいずれも Π_1 論理式で記述されていることを示せ.

定義 4.16. $\mathcal{L}_{\mathsf{arith}}$-理論 T が **Σ_1-完全** (Σ_1-*complete*) であるとは，$\mathbb{N}$ で真な Σ_1-閉論理式は必ず T で証明可能であることを意味する．つまり，任意の Σ_1-閉論理式 φ に対して，次が成立するときを言う.

$$\mathbb{N} \models \varphi \implies T \vdash \varphi.$$

定理 4.17. 離散順序環の非負部の公理 DOR^+ は Σ_1-完全である.

証明のアイデアを述べるために，離散順序環の非負部の構造を少し見てゆこう．まず，以下の略記を使用していたことを思い出そう.

$$\underline{n} = \underbrace{1 + 1 + \cdots + 1}_{n\ \text{個}}$$

さて，順序半環 $\mathcal{M} = (M, +, \cdot, \leqslant, 0, 1)$ が与えられたとき，$\underline{n}$ は M の要素である．つまり，

$$\mathbb{N}^{\mathcal{M}} = \{\underline{n} : n \in \mathbb{N}\} \subseteq M$$

が成立している．したがって，どんな順序半環を持ってきても，その中に $\mathbb{N}$ の複製のようなものがあるようである.

[*3] 狭義の Σ_1 論理式のことを Σ_1 論理式と呼び，本稿の意味での Σ_1 論理式を $\Delta_0(\Sigma_1)$ 論理式と呼ぶ流儀もある.

定理 4.18. $\mathcal{M}$ を非自明な順序半環とする．このとき，$(+,\cdot,\leqslant,0,1)$ を保つ $\mathbb{N}$ の $\mathcal{M}$ への埋め込みが存在する．さらに，もし $\mathcal{M}$ が離散順序環の非負部であれば．そのような埋め込みの像は $\mathcal{M}$ の始切片となる．

実際，$\mathbb{Z}[X]^+$ などでは，$\underline{n}$ は本物の自然数 n であり，$\mathbb{N}^{\mathbb{Z}[X]^+} = \mathbb{N}$ である．しかし，一般には，あくまで $\mathcal{M}$ はある種の順序半環でしかないので，1 や $1+1$ や $1+1+1$ などが $\mathcal{M}$ の中のどんな要素になっているかはよく分からない．そうすると，$n \mapsto \underline{n}$ が全ての構造を保つ埋め込みになっているというのは，そんなに自明なことではない．つまり，$\mathbb{N}^{\mathcal{M}}$ での演算が，本物の自然数の演算と同じとなっているかどうか，念のため確認する必要がある．非自明な順序半環の公理を OR^+ と書く．

補題 4.19. $\ell, k \in \mathbb{N}$ とする．

1. $\mathsf{OR}^+ \vdash \underline{\ell + k} = \underline{\ell} + \underline{k}$.
2. $\mathsf{OR}^+ \vdash \underline{\ell \cdot k} = \underline{\ell} \cdot \underline{k}$.
3. $\ell < k$ ならば，$\mathsf{OR}^+ \vdash \underline{\ell} < \underline{k}$.
4. $\mathsf{DOR}^+ \vdash (\forall x)\,[x \leqslant \underline{k} \;\to\; \bigvee_{m=0}^{k}(x = \underline{m})]$.

Proof. (1) 和に関する結合法則より自明である．(2) 帰納法を用いる．$\underline{\ell \cdot k} = \underline{\ell} \cdot \underline{k}$ は証明できたと仮定する．このとき，DOR^+ より次を導出できる．

$$\underline{\ell} \cdot (\underline{k+1}) = \underline{\ell} \cdot \underline{k} + \underline{\ell} = \underline{\ell \cdot k} + \underline{\ell} = \underline{\ell \cdot k + \ell} = \underline{\ell \cdot (k+1)}.$$

これらの等号は順に，分配律，帰納的仮定, (1) の性質より導かれる．

(3) まず，DOR^+ の非自明性より $\underline{0} < \underline{1}$ であり，順序半環の性質である和の順序保存性と推移律を利用して，任意の正整数 n について，$\underline{n} > \underline{0}$ であることを示せる．それでは，$\ell < k$ なる $k, \ell \in \mathbb{N}$ が与えられているとする．このとき，$k = \ell + n$ なる正整数 n が存在する．(1) を用いて，DOR^+ から $\underline{k} = \underline{\ell} + \underline{n}$ が導出される．すると，$\underline{n} > \underline{0}$ であることと和の順序保存性から，$\underline{k} = \underline{n} + \underline{\ell} > \underline{\ell}$ を得る．

(4) DOR^+ から $y < x \;\to\; y + 1 \leqslant x$ が導けることを確認する．これについては，$y < x$ なので，減法公理より $y = x + z$ なる z が存在する．このとき $z > 0$ である．なぜなら，$z \leqslant 0$ であると仮定すると，和の順序保存性より $x = y + z \leqslant y + 0 = y$ を得るが，これは $y < x$ に矛盾する．したがって，$z > 0$ なので，離散性より $z \geqslant 1$ である．再び和の順序保存性を用いて $x = y + z \geqslant y + 1$ を得る．

さて，帰納法より，$x \leqslant \underline{k} \;\to\; \bigvee_{m=0}^{k}(x = \underline{m})$ が示されていると仮定する．上の性質より，$x \leqslant \underline{k}$ または $x \geqslant \underline{k+1}$ が示される．したがって，もし $x \leqslant \underline{k+1}$ ならば，$x \leqslant \underline{k}$ または $x = \underline{k+1}$ である．帰納的仮定より，$x \leqslant \underline{k+1}$ ならば，$\bigvee_{m=0}^{k+1}(x = \underline{m})$ を得る． □

それでは，DOR^+ の Σ_1-完全性の証明に入ろう．

Proof (定理 4.17). Σ_1-閉論理式 φ の構成に関する帰納法による．最初に，φ が論理記号を含まな

い場合を考える．まず，$a, b, c, d \in \mathbb{N}$ について，$a \leqslant b$ かつ $c \nleqslant d$ ならば $\mathsf{DOR}^+ \vdash \underline{a} \leqslant \underline{b}$ かつ $\mathsf{DOR}^+ \vdash \underline{c} \nleqslant \underline{d}$ である．これについては，補題 4.19 (3) から従う．項は和 $+$ と積 $\cdot$ から作られるので，補題 4.19 (1) と (2) を用いれば，項 s, t, u, v について，$\mathbb{N} \models s \leqslant t$ かつ $\mathbb{N} \models u \nleqslant v$ ならば $\mathsf{DOR}^+ \vdash s \leqslant t$ かつ $\mathsf{DOR}^+ \vdash u \nleqslant v$ であることが分かる．等号については，$s = t$ であることと $s \leqslant t$ かつ $t \leqslant s$ が同値であることを利用する．続いて，φ が $\psi \wedge \eta$ または $\psi \vee \eta$ の場合は，帰納法の仮定に還元できる．

続いて，有界量化の場合を考える．$\mathbb{N} \models (\forall x \leqslant t)\ \psi(x)$ を仮定する．いま，ある $n \in \mathbb{N}$ について $\mathbb{N} \models t = \underline{n}$ であるから，帰納的仮定より $\mathsf{DOR}^+ \vdash t = \underline{n}$ である．また，$\mathbb{N} \models \bigwedge_{k=0}^{n} \psi(\underline{k})$ であるが，同様に帰納的仮定より，$\mathsf{DOR}^+ \vdash \bigwedge_{k=0}^{n} \psi(\underline{k})$ である．補題 4.19 (4) より，$\mathsf{DOR}^+ \vdash (\forall x)\ [x \leqslant \underline{n} \to \bigvee_{k=0}^{n} (x = \underline{k})]$ が従う．これらを合わせて，$\mathsf{DOR}^+ \vdash (\forall x \leqslant t)\ \psi(x)$ が導かれる．有界存在量化の場合も同様にして示される．

最後に，$\mathbb{N} \models \exists x \psi(x)$ を仮定する．このとき，ある $n \in \mathbb{N}$ について $\mathbb{N} \models \psi(\underline{n})$ となる．帰納法の仮定より，$\mathsf{DOR}^+ \vdash \psi(\underline{n})$ であり，したがって，$\mathsf{DOR}^+ \vdash \exists x \psi(x)$ となる．よって，定理は示された． □

豆知識． $\mathcal{N}$ が $\mathcal{M}$ の始切片であるような部分 $\mathcal{L}_{\mathsf{arith}}$-構造であるとき，$\mathcal{M}$ を $\mathcal{N}$ の**終拡大** (*end extension*) であると言う．上の定理の証明を修正することで，$\mathcal{M}$ が $\mathcal{N}$ の終拡大ならば，$\mathcal{M}$ は $\mathcal{N}$ の Δ_0**-初等拡大** (Δ_0-*elementary extension*) である，ということを示すことができる．特に，$\mathcal{M}$ が離散順序環の非負部であるとき，$n \mapsto \underline{n}$ は $\mathbb{N}$ の $\mathcal{M}$ への Δ_0**-初等埋め込み** (Δ_0-*elementary embedding*) を与えている．

4.3 $\mathbb{Z}$-環と開帰納法

離散順序環の非負部の公理 DOR^+ は，まだ $\mathbb{N}$ とはかけ離れた構造をモデルに持つようである．もう少し $\mathbb{N}$ に近づくには，どのような公理を更に加えたらよいだろうか．まずは小学校の算数で習った割り算を思い出そう．小学校では，2 つの正整数 x, n が与えられたとき，$x \div n$ を問う問題には，「q 余り r」のように答えていた．ここで，$x \div n =$ “q 余り r” とは，$x = qn + r$ かつ $r < n$ であることを思い出そう．この小学校の割り算は，以下のユークリッド除法の原理に基づくものである．

$$\text{除法の原理 } \mathsf{Div}(\underline{n}) : \quad (\forall x)(\exists q, r)\ [x = q \cdot \underline{n} + r\ \&\ 0 \leqslant r < \underline{n}].$$

命題 4.11 で見たことは，DOR^+ のモデル $\mathbb{Z}[X]^+$ では 2 によるユークリッド除法が実行できないという点である．したがって，DOR^+ に除法の原理を加えれば，より強い体系を得ることができる．

定義 4.20. $\mathbb{Z}$**-環** ($\mathbb{Z}$-*ring*) とは，任意の正整数 n に対して除法の原理 $\mathsf{Div}(\underline{n})$ を満たす非自明な離散順序環のことを意味する．言い換えれば，$R/nR \simeq \mathbb{Z}/n\mathbb{Z}$ を満たす非自明な離散順序環である．

定義 4.21. 離散順序環の非負部の公理 DOR^+ に各正整数 n に対して除法の原理 $\mathsf{Div}(\underline{n})$ を加え

たものを $\mathbb{Z}$**-環の非負部の公理**と呼び，ZR^+ と書く．標準的な名称ではないが，ここでは，$\mathbb{Z}$-環の非負部の公理を満たすモデルを $\mathbb{N}$**-半環** ($\mathbb{N}$-*semiring*) と呼ぶ．

例 4.22. $\mathbb{Z}[X]$ は $\mathbb{Z}$-環ではない．同様に，$\mathbb{Z}[X]^+$ は $\mathbb{N}$-半環ではない．

例 4.23. $\mathbb{Q}[X]$ を $\mathbb{Q}$ 上の 1 変数多項式環とし，$\mathbb{Q}[X]_Z$ を $\mathbb{Q}[X]$ の多項式のうち次数 0 の項が整数であるもの全体の集合とする．つまり，

$$\mathbb{Q}[X]_Z = \{a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 : n \in \mathbb{N} \ \wedge \ a_0 \in \mathbb{Z} \ \wedge \ a_1, \ldots, a_n \in \mathbb{Q}\}.$$

順序を $\mathbb{Z}[X]$ と同じように定義すると，$\mathbb{Q}[X]_Z$ は $\mathbb{Z}$-環となる．除法の原理については，多項式 $p = \sum_{i=0}^n a_iX^i \in \mathbb{Q}[X]_Z$ を自然数 n で割ることを考えよう．a_0 は整数なので，ある $0 \leqslant r < n$ に対して，$qn + r$ と書ける．よって，$p = (\sum_{i=1}^n (a_i/n)X^i + q) \cdot n + r$ となる．同様にして，$\mathbb{Q}[X]_Z$ の非負部 $\mathbb{Q}[X]_Z^+$ は $\mathbb{N}$-半環となる．

証明は省略するが，除法が全域には定義されないような $\mathbb{N}$-半環も存在する．そういうわけで，$\mathbb{N}$-半環もまだ $\mathbb{N}$ とはかなり異なる性質を持ち得る．さて，ここまでやってきたように公理を少しずつ加えていって $\mathbb{N}$ に地道に近づいていくのもよいが，それでは終わりが見えず，埒が明かないので，もう少し一般的な $\mathbb{N}$ 固有とおぼしき性質に着目しよう．以後，$\{+, \cdot, \leqslant, 0, 1\}$ を算術の言語と呼び，$\mathcal{L}_{\mathsf{arith}}$ と書く．そういうわけで，$\mathbb{N}$-半環もまだ $\mathbb{N}$ とはかなり異なる性質を持ち得る．さて，ここまでやってきたように公理を少しずつ加えていって $\mathbb{N}$ に地道に近づいていくのもよいが，それでは終わりが見えず，埒が明かないので，もう少し一般的な $\mathbb{N}$ 固有とおぼしき性質に着目しよう．以後，$\{+, \cdot, \leqslant, 0, 1\}$ を算術の言語と呼び，$\mathcal{L}_{\mathsf{arith}}$ と書く．

定義 4.24 (帰納法公理)**.** Γ を $\mathcal{L}_{\mathsf{arith}}$-論理式の集合とする．公理系 $\mathsf{I}\Gamma$ とは，離散順序環の非負部の公理 DOR^+ に，以下の**数学的帰納法**の公理を各 Γ-論理式 φ 毎に加えた公理図式である．

$$\text{数学的帰納法:} \quad [\varphi(0) \ \wedge \ (\forall x)\, \varphi(x) \to \varphi(x+1)] \ \to \ (\forall x)\, \varphi(x).$$

帰納法公理における φ は x 以外の自由変数を含んでもよい[*4]．Γ の例としては，量化記号を含まない $\mathcal{L}_{\mathsf{arith}}$-論理式全体の集合 Open，量化記号は有界存在量化 $\exists x \leqslant t$ のみを認める E_1, Σ_1 論理式全体の集合 Σ_1 などがあり，IOpen, IE_1 や $\mathsf{I}\Sigma_1$ などを考える．また，**ペアノ算術** (*Peano arithmetic*) とは，$\mathcal{L}_{\mathsf{arith}}$-論理式の集合 Arith に対する公理系 IArith のことを意味する．以後，PA によって，ペアノ算術を表す．

[*4] x 以外の自由変数を許さない帰納法は，**パラメータなし帰納法** (*parameter-free induction*) と呼ばれ，対応する公理系は $\mathsf{I}\Gamma^-$ のようにマイナスを付けて表されることが多い．

命題 4.25. IOpen から全域的な除法の原理を証明できる:

$$\mathsf{IOpen} \vdash (\forall x)(\forall y > 0)(\exists q, r)\ [x = q \cdot y + r\ \wedge\ r < y].$$

特に，IOpen の任意のモデルは $\mathbb{N}$-半環であるが，逆は成り立たない．たとえば，例 *4.23* の $\mathbb{N}$-半環 $\mathbb{Q}[X]_Z^+$ は IOpen のモデルではない．

Proof. x, y を任意に固定し，$\varphi(q)$ を $q \cdot y \leqslant x$ によって定義する．このとき，$\varphi \in \mathsf{Open}$ である．まず，DOR^+ で明らかに $\varphi(0)$ かつ $\neg\varphi(x+1)$ が証明できる．したがって，Open-帰納法の対偶を用いることによって，IOpen で $\varphi(q)$ かつ $\neg\varphi(q+1)$ であるような q の存在が示される．つまり，DOR^+ における順序の比較可能性より，$qy \leqslant x$ かつ $(q+1)y > x$ である．$r = x - qy$ とおくと，$x = qy + r$ となる．$r < y$ については，$qy + r = x < (q+1)y = qy + y$ であることから分かる． □

IOpen のモデルの特徴付けとして，以下に述べる**シェファードソンの定理** (*Shepherdson's theorem*) は重要であるが，本講義のスコープを越えることと，後の節では用いないことから，証明は省略する．しかし，算術体系のモデルのイメージを鍛えるために有用であるから，シェファードソンの定理を応用した例に幾つか触れよう．

事実 4.26 (シェファードソンの定理)**.** IOpen のモデルとは，ある実閉体の整数部 Z の非負部 Z^+ に他ならない．

例 4.27. $\mathbb{R}$ 係数の**ピュイズー級数** (*Puiseux series*) たちが実閉体をなすことは知られている．したがって，シェファードソンの定理より，その整数部の非負部は IOpen のモデルであり，$\mathbb{N}$ と同型でないことも分かる．

例 4.28 (シェファードソンのモデル)**.** IOpen の可算モデルを得るためには，分数体 $\mathbb{Q}(X)$ の実閉包 $\mathrm{rcl}(\mathbb{Q}(X))$ を考えよう．これは，実代数的数を係数に持つ非負冪の有限ピュイズー級数たちのなす実閉体である．$\mathbb{R}_{\mathrm{alg}}$ を実代数的数全体を表すものとすると，$\mathrm{rcl}(\mathbb{Q}(X))$ の整数部として，以下を得る．

$$\begin{aligned} S :=& \mathrm{rcl}(\mathbb{Q}(X))_Z \\ =& \{a_n X^{\frac{n}{k}} + a_{n-1} X^{\frac{n-1}{k}} + \cdots + a_1 X^{\frac{1}{k}} + a_0 : n \in \mathbb{N},\ k \in \mathbb{N}\backslash\{0\},\ a_0 \in \mathbb{Z},\ a_i \in \mathbb{R}_{\mathrm{alg}}\}. \end{aligned}$$

S の非負部 S^+ は IOpen の可算モデルというだけではなく，計算可能モデルである．この S は**シェファードソンのモデル** (*Shepherdson's model*) と呼ばれる．

証明は省略するが，以下の事実が知られている．

命題 4.29. IOpen では，素数の無限性を証明できない．

$$\mathsf{IOpen} \nvdash (\forall x)(\exists p > x)(\forall a, b < p)\ p \neq a \cdot b.$$

形式体系	可算モデル	証明できない性質の例
離散順序環の非負部 DOR^+	$\mathbb{N}$, $\mathbb{Z}[X]^+$, $\mathbb{Q}[X]^+_Z$, S^+ など	任意の数が偶または奇
$\mathbb{Z}$-環の非負部 ZR^+	$\mathbb{N}$, $\mathbb{Q}[X]^+_Z$, S^+ など	全域的な除法の原理
開帰納法公理 IOpen	$\mathbb{N}$, S^+ など	整閉性，素数の無限性
Δ_0-帰納法公理 $\mathsf{I}\Delta_0$	$\mathbb{N}$ など	指数関数の全域性
Σ_1-帰納法公理 $\mathsf{I}\Sigma_1$	$\mathbb{N}$ など	アッカーマン関数の全域性
ペアノ算術 PA	$\mathbb{N}$ など	パリス・ハーリントンの定理

表 1　$\mathbb{N}$ をモデルとする形式体系の階層

実際，シェファードソンのモデル S^+ において，素数の無限性を表す上式は偽となる．しかし，上式は，S^+ の中で素数が有界であることを示すものであるが，各素数 $p \in \mathbb{N}$ は S^+ でも素数であるから，外から見れば，S^+ は素数を無限個持つことに注意する．

$$S^+ \models \neg(\forall x)(\exists p > x) \text{ “}p \text{ は素数である”}.$$
$$(\forall x \in \mathbb{N})\ S^+ \models (\exists p > \underline{x}) \text{ “}p \text{ は素数である”}.$$

命題 4.30. IOpen では，フェルマーの最終定理を証明できない．実際，$n = 3$ の場合すら証明できない．

$$\mathsf{IOpen} \nvdash (\forall x, y, z > 0)\ [x^3 + y^3 \neq z^3].$$

Proof. シェファードソンのモデルの非負部 S^+ でフェルマーの最終定理の $n = 3$ の場合を証明できないことを示す．具体的に $x^3 + y^3 = z^3$ を満たす $x, y, z \in S^+$ を取ってこよう．これについては，$X, \sqrt[3]{2}X \in S^+$ であり，$X^3 + X^3 = (\sqrt[3]{2}X)^3$ であることから従う． □

IOpen のモデルの代数的性質に関して，もう一つ例を挙げておく．

例 4.31. シェファードソンのモデル S は**整閉** (*integrally closed*) ではない．

Proof. たとえば，$X, \sqrt{2}X \in S$ であるから，$\sqrt{2} = \sqrt{2}X/X$ は S で有理数であるが，これは S の分数体における S 係数モニック多項式 $x^2 - 2 = 0$ の根であり，つまり S 上整である．しかし，明らかに $\sqrt{2} \notin S$ であるから，S が整閉でないことが分かる． □

例 4.31 とは対照的に，有界存在量化帰納法 $\mathsf{I}\mathbf{E}_1$ のモデルは必ず整閉整域の非負部になることが知られている．したがって，S^+ は $\mathsf{I}\mathbf{E}_1$ のモデルではない．しかし，$\mathsf{I}\mathbf{E}_1$ くらいまで強い体系になると，これまでのように容易くモデルを構成する，ということができなくなる．実は，$\mathsf{I}\mathbf{E}_1$ には**テネンバウムの定理** (*Tennenbaum's theorem*) というものが成り立ってしまい，$\mathsf{I}\mathbf{E}_1$ の計算可能な超準モデルは存在しないのである．

以上のようにして，自然数をモデルとするような形式体系の階層が作られていく．その概要を表 1 にまとめた．

豆知識. ここで挙げた体系以外でも，$\mathbb{Z}$-環や IOpen の周辺のようなテネンバウムの定理の呪縛を受けない弱い体系では，たとえばベズー整域や GCD 整域といったような代数的な性質と絡み合ったモデル理論的研究が行われている．また，$\mathsf{I}\Delta_0$ 周辺は，**限定算術** (*bounded arithmetic*) と呼ばれる，算術体系と**計算量理論** (*computational complexity theory*) を結び付ける理論と関わりがある．$\mathsf{I}\Sigma_1$ と PA の中間の帰納法の階層構造は，証明論や計算可能性理論などの分野で深く研究されており，前者ではたとえば**可証全域関数** (*provably total function*) であるとか，後者では算術の超準モデル上の計算論と**認容順序数** (*admissible ordinal*) 上の計算論の類似であるとかいったものである．PA より強い体系は二階算術などといったものと絡むことが多いが，その分析は証明論における不朽のテーマであり，数多の深遠な研究がなされている．

さて，これまでに，不足な公理を次々に追加していくことにより IOpen のような公理系を作り上げてきたが，未だ証明不可能な自然数の性質は無数に残る．$\mathsf{I}\Sigma_1$ くらいになると幾分か状況はよくなって，自然数について成り立つ閉論理式で，通常の数学的活動で取り扱うようなもののかなりの部分は証明できるといっても過言ではないだろう．しかし，たとえ $\mathsf{I}\Sigma_1$ や PA のような公理系といえど，まだ自然数を完全には捉えきれていないであろうことは容易に想像が付く．たとえば，有限ラムゼーの定理を技巧的に複雑化した主張である**パリス・ハーリントンの定理** (*Paris-Harrington theorem*) というものは，$\mathbb{N}$ で成立することが十分強い体系の下で証明できるが，PA では証明できない．実際，幾ら DOR^+ に公理を加えていったとしても，それが無矛盾であり，何を公理に加えたかを有限的なアルゴリズムによって判定できる限り，自然数に関する真な式を全て証明するということは決してできない．これについては，第**??**節で詳述する．

4.4 超準モデルの順序型

ここまでで，$\mathbb{N}$ の持つ様々な性質を公理化し，その公理を満たすが，$\mathbb{N}$ と非同型となるようなモデルを取り扱ってきた．それでは，そのような $\mathbb{N}$ と非同型なモデルについて，何か共有する性質はあるだろうか．離散順序環の非負部のことを思い出すと，$\mathbb{Z}[X]^+$ では，$\mathbb{N}$ の形の島の無限の彼方に，$\mathbb{Z}$ の形の島が $\mathbb{N}$ の形に並んだ列島 $\mathbb{Z}\cdot\mathbb{N}$ があり，その更に無限の彼方には $\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{N}$ がある，さらに無限の彼方には $\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{Z}\cdot\mathbb{N}$ があって，... といったようなことが見て取れる．それでは，他のモデルは，一体どのような形状をしているだろうか．

定理 4.32. 非自明な離散順序環の非負部の順序型は，最大元を持たない全順序 J が存在して，$\mathbb{N}+\mathbb{Z}\cdot J$ の形となる．$\mathbb{N}$-半環の順序型は，最大・最小元を持たない稠密全順序 Q が存在して，$\mathbb{N}+\mathbb{Z}\cdot Q$ の形となる．

特に，$\mathbb{N}$ と非同型な可算 $\mathbb{N}$-半環の順序型は $\mathbb{N}+\mathbb{Z}\cdot\mathbb{Q}$ である．

Proof. $\mathcal{M}$ を非自明な離散順序環の非負部とする．$\mathcal{M}$ が $\mathbb{N}$ と同型ならば, $\mathbb{N}+\mathbb{Z}\cdot\varnothing$ である．$\mathcal{M}$ が $\mathbb{N}$ と非同型であると仮定する．定理 4.18 より，$\mathbb{N}$ の $\mathcal{M}$ への埋め込み像 $\mathbb{N}^{\mathcal{M}}=\{\underline{n}:n\in\mathbb{N}\}$ は $\mathcal{M}$ の始切片だった．簡単のために, $\mathbb{N}^{\mathcal{M}}$ を $\mathbb{N}$ と略記する．以前と同様に, $\mathcal{M}$ の元を標準整数差によって同値分類する．つまり, 各 $x\in\mathcal{M}$ に対して, 島 $[x]=\{y\in\mathcal{M}:(\exists n\in\mathbb{N})\ x+\underline{n}=y\ \vee\ y+\underline{n}=x\}$

を考える．また，$[x] < [y]$ によって，任意の $x' \in [x]$ と $y' \in [y]$ について，$x' < y'$ となることを意味する．超準元 $a \in \mathcal{M}\backslash\mathbb{N}$ を取ると，そこから任意の標準自然数 $n \in \mathbb{N}$ に対して，$a+n$ と $a-n$ が存在するので，$[a]$ の順序型は $\mathbb{Z}$ と等しい．また，$a \in \mathcal{M}\backslash\mathbb{N}$ ならば $[a] < [2a]$ なので，最上位の島が存在しないことは容易に分かる．したがって，最大元を持たないある全順序 J に対して，$\mathcal{M}$ の順序型は $\mathbb{N} + \mathbb{Z} \cdot J$ となっている．

続いて，$\mathcal{M}$ が $\mathbb{N}$-半環であると仮定する．標準自然数たちが住む $\mathbb{N}$ の島が最下位に位置するが，その次の島は存在しない．なぜなら，$\mathbb{N}$-半環であれば，任意の超準元 $a \in \mathcal{M}\backslash\mathbb{N}$ に対し，$a = 2b$ または $a = 2b+1$ なる b が存在する．このとき，$\mathbb{N} < [b] < [a]$ は容易に分かる．

稠密性を示すために，$[a] < [b]$ なる $a, b \in \mathcal{M}\backslash\mathbb{N}$ を取る．$\mathcal{M}$ は $\mathbb{N}$-半環であるから，$a+b = 2c$ または $a+b = 2c+1$ となるような $c \in \mathcal{M}$ が存在する．このとき，$[a] < [c] < [b]$ であることが確認できる．よって，島たちは稠密に存在する．

以上より，どんな $\mathbb{N}$-半環も，ある最大及び最小元を持たない稠密全順序 Q に対して，$\mathbb{N} + \mathbb{Z} \cdot Q$ の順序型を持つ．また，$\mathcal{M}$ が可算の場合，$Q \neq \varnothing$ ならば，そのような全順序の性質の $\aleph_0$-範疇性から，Q は有理数の順序 $\mathbb{Q}$ と同型になる．よって，$\mathbb{N}$ と非同型などんな可算 $\mathbb{N}$-半環も，その順序型は $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$ であることが分かった． □

注意． 2 つの構造が同型ならば，初等同値である．したがって，$\mathbb{N}$ では偽となる閉論理式（たとえば，素数の有限性など）を 1 つでも満たす $\mathbb{N}$-半環 R は，$\mathbb{N}$ と初等非同値になるので，非同型になる．したがって，定理 4.32 より，そのような $\mathbb{N}$-半環 R の順序型は，最大・最小元を持たない稠密全順序 Q に対して，必ず $\mathbb{N} + \mathbb{Z} \cdot Q$ という形になっている．具体的には，例 4.23 の $\mathbb{N}$-半環 $\mathbb{Q}[X]^+_Z$ や例 4.28 の IOpen のモデル S^+ は $\mathbb{N}$ と初等非同値で可算であるから，その順序型は $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$ である．

しかし，最大・最小元を持たない稠密全順序ならどんなものでも良いかというと，そういうわけではない．

命題 4.33. IOpen のモデルで，順序型が $\mathbb{N} + \mathbb{Z} \cdot \mathbb{R}$ であるようなものは存在しない．

この主張を証明するためには少し準備が必要である．$\mathcal{M}$ を離散順序環の非負部とする．このとき，$I \subseteq \mathcal{M}$ が $\mathcal{M}$ の**カット** (*cut*) であるとは，$a \in I$ かつ $b < a$ ならば $b \in I$ であり，$a \in I$ ならば $a+1 \in I$ であるもののことである．

補題 4.34 (溢れ出し)**.** $\mathcal{M} \models \mathsf{I}\Gamma$ かつ $I \neq \mathcal{M}$ を $\mathcal{M}$ のカットとする．$\varphi(x)$ を Γ-論理式とする．もし，任意の $a \in I$ で，$M \models \varphi(a)$ が成立しているならば，ある $c \in \mathcal{M}\backslash I$ で，$M \models \varphi(c)$ が成立する．

Proof. 結論が偽であると仮定する．このとき，$\varphi(x) \Leftrightarrow x \in I$ であり，I はカットなので，$0 \in I$ かつ $\forall x\,(x \in I \Rightarrow x+1 \in I)$ である．つまり，

$$\varphi(0) \ \wedge \ \forall x\,(\varphi(x) \ \rightarrow \ \varphi(x+1))$$

ここで $\varphi(x)$ は Γ-論理式なので，$M \models \mathsf{I}\Gamma$ を用いて $\forall x\varphi(x)$ を得る．これは $I = M$ を意味し，仮定に矛盾する． □

Proof (**定理** 4.33). M を IOpen のモデルで，順序型が $\mathbb{N}+\mathbb{Z}\cdot\mathbb{R}$ だったとする．このとき，適当に超準元 $a \in M\backslash\mathbb{N}$ を取る．各 $b \in M$ について，$a\cdot b$ は，ある $x_b \in \mathbb{R}$ について，x_b 番目の $\mathbb{Z}$-島におり，$b < c \in M$ ならば $x_b < x_c$ である．数列 $(x_n)_{n\in\mathbb{N}}$ を考えると，任意の $n \in N$ と $b \in M\backslash\mathbb{N}$ について $x_n < x_b$ が成立するので，$(x_n)_{n\in\mathbb{N}}$ は有界な実数列である．$\mathbb{R}$ の完備性より，上限 $x = \sup_n x_n$ が存在する．x 番目の $\mathbb{Z}$-島の元 $b \in M$ を取る．$\varphi(n) \equiv a\underline{n} < b$ の溢れ出しによって，ある超準元 $c \in M\backslash\mathbb{N}$ が存在して，任意の $n \in \mathbb{N}$ について $a\cdot n < a\cdot(c-1) < a\cdot c < b$ となるが，これは b の性質に矛盾する． □

5 原始再帰関数

自然数の足し算および掛け算のような基本的な演算から，**原始再帰法** (*primitive recursion*)[*5]と呼ばれる操作によって，様々な自然数上の関数を構成できることを本節では見ていこう．

このアイデアを説明するために，人類が「新しい演算」を創造していく過程をシミュレートしよう[*6]．まず，自然数 x が与えられたとき，「x の次」である数が何であるかを知っているとしよう．すると，「x の次の次」や「x の次の次の次」などを考えることができる．しかし，いくつも「の次」という文字を書くのは億劫なので，x の y 個次の数を $x+y$ と書くことにしよう．こうして，人類は，「足す」という演算を生み出した．

$$x + y = x \text{ の } \underbrace{\text{次の次の次} \ldots \text{の次の次}}_{y \text{ 個}}$$

このように「足す」という演算を知った人類は，$x+x+x$ や $x+x+x+x+x$ のように x を何度も足す，という演算が有用であることに次第に気づき始める．これを簡潔に表すために，人類は「掛ける」という演算を次のように定義した．

$$x \cdot y = \underbrace{x + x + \cdots + x + x}_{y \text{ 個}}$$

そして，「掛ける」という演算を知った人類は，$x\cdot x\cdot x$ のように x を何度も掛ける，という演算の有用性に気づく．そして「累乗」という演算を次のように定義した．

$$x^y = \underbrace{x \cdot x \cdot \cdots \cdot x \cdot x}_{y \text{ 個}}$$

[*5] Primitive recursion は伝統的には，原始再帰でなく**原始帰納**と訳されることがある．しかし，本講義ではそこまで辿り着かないが，再帰理論やその周辺の理論では， inductive と recursive が全く別概念として登場し，たとえば，「recursive ではないが inductive であるような集合が存在する」「Π^1_1-transfinite induction は Π^1_1-transfinite recursion を導かない」というような定理が成立する．したがって，inductive と recursive には異なる訳語を割り当てる必要があるが，ここでは inductive を**帰納**と訳し，recursive を**再帰**と訳す流儀を採用する．

[*6] 本稿の記述は現実の数学史に沿っているとは限らない．

すると，自然に x^{x^x} や $x^{x^{x^x}}$ のようなものを考える人も現れる．上方向にたくさん添字が付くのは見づらいので，x^y のことを今後は $x \uparrow y$ と書くこととしよう．たとえば，x^{x^x} は $x \uparrow (x \uparrow x)$ であり，$x^{x^{x^x}}$ は $x \uparrow (x \uparrow (x \uparrow x))$ である．また，以下，括弧は省略し，これらの演算は右から順に適用するものとする．さて，累乗でも飽き足らない一部の人類は，「テトレーション」という演算を編み出した．

$$x \uparrow\uparrow y = \underbrace{x \uparrow x \uparrow \ldots \uparrow x \uparrow x}_{y \text{ 個}}$$

飽くなき人類は，更なる演算「ペンテーション」を定義する．

$$x \uparrow\uparrow\uparrow y = \underbrace{x \uparrow\uparrow x \uparrow\uparrow \ldots \uparrow\uparrow x \uparrow\uparrow x}_{y \text{ 個}}$$

より一般に，クヌースの矢印記法というものは以下によって定義される．

$$x \uparrow^{n+1} y = \underbrace{x \uparrow^n x \uparrow^n \ldots \uparrow^n x \uparrow^n x}_{y \text{ 個}}$$

更なる高みを目指す人類の一部は，矢印記法を越えて続く演算を生み出している[*7]が，キリがないので，本講義で触れるのはここまでとしよう．

このような再帰的な関数構成を数学的に抽象化したものが，原始再帰法と呼ばれる概念である．

5.1 原始再帰法

さて，ここまで，何かの演算 $x \diamond y$ を元に，人類が新たな演算 $x \star y$ を創造する過程を見てきた．これらの過程が共有するものとは何であろうか．それは以下の性質である．

$$x \star y = \underbrace{x \diamond x \diamond \cdots \diamond x \diamond x}_{y \text{ 個}}$$

実際に，この値 $x \star y$ を計算する場合には，$x \star 2 = x \diamond x$ を求め，$x \star 3 = x \diamond x \diamond x = x \diamond (x \star 2)$ を求め，$x \star 4 = x \diamond x \diamond x \diamond x = x \diamond (x \star 3)$ を求め，$\ldots$ という手続きを行うこととなるだろう．たとえば，掛け算以降の演算の定義を少し書き直せば，次のようにして定義されていることがわかる．

$$\begin{cases} x \star 1 = x, \\ x \star (y+1) = x \diamond (x \star y). \end{cases}$$

上の定義では曖昧であるが，$x \star 0$ の場合も定義しておくのが自然である．たとえば，$x \cdot 0 = 0$ であるし，$x \uparrow 0 = x^0 = 1$ である．

[*7] たとえば，コンウェイのチェーン記法と呼ばれるものがある．

$$x \to y \to z = x \uparrow^z y.$$

チェーンはより長く伸びてゆき，更なる演算が定義される．しかし，ここまでゆくと，既に原始再帰の枠組みを越えてしまう．たとえば，$x \mapsto x \uparrow^x x$ の増大速度は原始再帰でない関数として有名な**アッカーマン関数** (*Ackermann function*) のそれとおおよそ同程度である．

演習問題 5.1. 以下のようにして，$x \uparrow^{n+1} y$ を定義する．

$$\begin{cases} x \uparrow^{n+1} 0 = 1, \\ x \uparrow^{n+1} (y+1) = x \uparrow^{n} (x \uparrow^{n+1} y). \end{cases}$$

このとき，$x \uparrow^{n+1} 1 = x$ であることを示せ．

さて，ここまでは演算の形式で書いてきたが，これらを関数として見直すこととする．つまり，今までのことを，関数 $h(x,y) = x \diamond y$ から新たな関数 $f(x,y) = x \star y$ を創造する過程を考えてきたものとしよう．また，$g(x) = x \star 0$ は与えられているものとする．これまでの内容を言い直せば，g と h からの新たな関数 f は以下のように生み出された．

$$\begin{cases} f(x,0) = g(x), \\ f(x,y+1) = h(x, f(x,y)). \end{cases}$$

それでは，原始再帰法の厳密な定義に入ろう．上では，f は 2 変数関数であったが，より多変数であってよい．

定義 5.2 (原始再帰法)**.** 関数 $g : \mathbb{N}^n \to \mathbb{N}$ と $h : \mathbb{N}^{n+2} \to \mathbb{N}$ が与えられているとする．さらに，$f : \mathbb{N}^{n+1} \to \mathbb{N}$ が，次のように定義されるとしよう: 任意の $\bar{x} \in \mathbb{N}^n$ と $y \in \mathbb{N}$ について，

$$\begin{cases} f(\bar{x},0) = g(\bar{x}), \\ f(\bar{x},y+1) = h(\bar{x}, y, f(\bar{x},y)). \end{cases}$$

このとき，f は g と h から**原始再帰法** (*primitive recursion*) によって定義されるという．

それでは，原始再帰関数の概念を導入しよう．

定義 5.3 (原始再帰関数)**.** 以下のように，**原始再帰関数** (*primitive recursive function*) を帰納的に定義する．

1. 以下によって定義される後続関数 $\mathsf{succ} : \mathbb{N} \to \mathbb{N}$, 零関数 $\mathsf{zero}^n : \mathbb{N}^n \to \mathbb{N}$ および射影関数 $\mathsf{proj}_i^n : \mathbb{N}^n \to \mathbb{N}$ は原始再帰関数である．

$$\mathsf{succ}(x) = x+1, \quad \mathsf{zero}^n(x_1, \ldots, x_n) = 0, \quad \mathsf{proj}_i^n(x_1, \ldots, x_n) = x_i.$$

2. 原始再帰関数たちの合成は原始再帰関数である．つまり，$h : \mathbb{N}^m \to \mathbb{N}$ と $g_1, \ldots, g_m : \mathbb{N}^n \to \mathbb{N}$ が原始再帰的ならば，以下のように定義される関数 $f : \mathbb{N}^n \to \mathbb{N}$ もまた原始再帰的である．

$$f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x})).$$

3. 原始再帰関数 g, h から原始再帰法によって定義される関数は原始再帰的である．

以後，後続関数，零関数，射影関数のことを**初期関数** (*initial function*) と呼ぶ．つまり，原始再帰関数全体の族とは，初期関数を含み合成と原始再帰法で閉じた最小の関数族として与えられる．

例 5.4. 和 $(x,y) \mapsto x+y$, 積 $(x,y) \mapsto x \cdot y$, 冪乗 $(x,y) \mapsto x^y$, 第 n 矢印演算 $(x,y) \mapsto x \uparrow^n y$ はいずれも原始再帰的関数である．

例 5.5. ここでは自然数上の関数を考えるので，引き算は一般には定義されないが，部分的引き算 $x \dot{-} y = \max\{0, x-y\}$ を考えることはできる．これが原始再帰的であることを示そう．まず，「入力が正の数であれば，値を 1 減らす」という演算 pred が原始再帰的であることを確認する．これは，$g = \mathsf{zero}^0$ と $h = \mathsf{proj}_1^2$ から原始再帰法によって定義される関数を考えればよい．

$$\begin{cases} \mathsf{pred}(0) = \mathsf{zero}^0 = 0, \\ \mathsf{pred}(y+1) = \mathsf{proj}_1^2(y, \mathsf{pred}(y)) = y. \end{cases}$$

このとき，部分的引き算 $f(x,y) = x \dot{-} y = \max\{0, x-y\}$ は，$g = \mathsf{proj}_1^1$ と $h = \mathsf{pred} \circ \mathsf{proj}_3^3$ から原始再帰法によって定義される．

$$\begin{cases} x \dot{-} 0 = \mathsf{proj}_1^1(x) = x, \\ x \dot{-} (y+1) = \mathsf{pred}(\mathsf{proj}_3^3(x, y, x \dot{-} y) = \mathsf{pred}(x \dot{-} y). \end{cases}$$

例 5.6. 典型的な原始再帰関数として，総和と総乗がある．

$$f_0(\bar{x}, y) = \sum_{i=0}^{y-1} p(\bar{x}, i), \qquad f_1(\bar{x}, y) = \prod_{i=0}^{y-1} p(\bar{x}, i).$$

ここで，$p : \mathbb{N}^{n+1} \to \mathbb{N}$ は与えられた原始再帰関数とする．このとき，f_0 は $g_0 = \mathsf{zero}^n$ と $h_0(\bar{x}, y, z) = z + p(\bar{x}, y)$ から原始再帰法によって定義される．

$$\begin{cases} f_0(\bar{x}, 0) = \mathsf{zero}^n(\bar{x}) = 0, \\ f_0(\bar{x}, y+1) = f_0(\bar{x}, y) + p(\bar{x}, y). \end{cases}$$

同様に，f_1 は $g_1 = \mathsf{succ} \circ \mathsf{zero}^n$ と $h_1(\bar{x}, y, z) = z \cdot p(\bar{x}, y)$ から原始再帰法によって定義される．

$$\begin{cases} f_1(\bar{x}, 0) = \mathsf{succ}(\mathsf{zero}^n(\bar{x})) = 1, \\ f_1(\bar{x}, y+1) = f_0(\bar{x}, y) \cdot p(\bar{x}, y). \end{cases}$$

さて，新しい原始再帰関数を作るために，場合分けを自由に使用してよいことを示しておくと便利である．

しかし，実に世の中の色々なものが原始再帰的である．証明図の原始再帰性

証明図 D が推件式 $\Gamma \vdash \Delta$ の証明である，ということ．「c が理論」

5.2 初等関数とグジェゴルチク階層

原始再帰関数に類似の構成をされるものとして初等関数がある．初等関数の族とは，初期関数と加法，部分的減法を含み，合成と総和，総乗で閉じている最小の関数族である．より正確には，以下のように定義される．

定義 5.7. 以下のように，**初等関数** (*elementary function*) を帰納的に定義する．

1. 初期関数，加法 $x+y$, 部分的減法 $x \dot{-} y$ は初等関数である．
2. 初等関数たちの合成は初等関数である．
3. 初等関数から総和, 総乗によって定義される関数は初等関数である．つまり, $p : \mathbb{N}^{n+1} \to \mathbb{N}$ が初等関数ならば，以下のように定義される関数 $f, g : \mathbb{N}^{n+1} \to \mathbb{N}$ もまた初等関数である．

$$f(\bar{x}, y) = \sum_{i=0}^{y-1} p(\bar{x}, i) \qquad\qquad g(\bar{x}, y) = \prod_{i=0}^{y-1} p(\bar{x}, i).$$

例 5.8. 任意の $n \in \mathbb{N}$ について，関数 $f(x) = x \uparrow\uparrow n$ は初等関数である．なぜなら，総乗を用いれば，指数関数 x^y が初等関数であることは明らかで，$x \uparrow\uparrow n$ は指数関数の n 回合成として表されるためである．

また，例 5.6 より，任意の初等関数は原始再帰的である．一方，$f(x) = x \uparrow\uparrow x$ は初等関数ではない．よって，初等関数でないような原始再帰的関数が存在する:

$$\text{初等関数全体の族} \subsetneq \text{原始再帰的関数全体の族}.$$

例 5.9. 割り算，素数判定，etc. 初等関数によって様々なコーディングを定義できる．

初等関数と原始再帰関数の関連性を理解するための良い方法が,

定義 5.10 (有界原始再帰法)**.** 関数 $g : \mathbb{N}^n \to \mathbb{N}$, $h : \mathbb{N}^{n+2} \to \mathbb{N}$ および $t : \mathbb{N}^{n+1} \to \mathbb{N}$ が与えられているとする．さらに，$f : \mathbb{N}^{n+1} \to \mathbb{N}$ が，次のように定義されるとしよう: 任意の $\bar{x} \in \mathbb{N}^n$ と $y \in \mathbb{N}$ について,

$$\begin{cases} f(\bar{x}, 0) = g(\bar{x}), \\ f(\bar{x}, y+1) = h(\bar{x}, y, f(\bar{x}, y)), \\ f(\bar{x}, y) \leqslant t(\bar{x}, y) \end{cases}$$

このとき，f は g, h, t から**有界原始再帰法** (*bounded primitive recursion*) によって定義されるという．

初等関数は，有界原始再帰法によって特徴づけることができる．

定理 5.11. 初等関数全体の族は，以下を満たす最小の関数族と正確に一致する．

- 初期関数と指数関数 x^y を含む．
- 合成と有界原始再帰法で閉じている．

Proof. 初等関数全体の族が有界原始再帰法で閉じていることを示す．f が初等関数 g, h, t から有界原始再帰法で定義されていると仮定する．まず

$$\begin{aligned} m = \langle f(\bar{x}, 0), \ldots, f(\bar{x}, y)\rangle \iff & lh(m) = y + 1 \ \wedge \ (m)_0 = g(\bar{x}) \\ & \wedge \ (\forall i < y)\ (m)_{i+1} = h(\bar{x}, i, (m)_i) \end{aligned} \tag{22}$$

であり，例 5.9 で見たように，(22) の右式の真偽判定は初等関数によって行うことができる．また，$f(\bar{x}, y) \leqslant t(\bar{x}, y)$ であるから，$t^+(\bar{x}, y) = \sum_{i \leqslant y} t(\bar{x}, i)$ とすると $f(\bar{x}, i) \leqslant t^+(\bar{x}, y)$ である．よって，$q(\bar{x}, y) = (p_y^{t^+(\bar{x}, y)})^{y+1}$ とすれば $\langle f(\bar{x}, 0), \ldots, f(\bar{x}, y)\rangle \leqslant q(\bar{x}, y)$ であることが分かる．いま，q は明らかに初等関数である．

以上より，$f(\bar{x}, y)$ は (22) の条件を満たす $m \leqslant q(\bar{x}, y)$ について $(m)_y$ として得られる．より正確には，

$$h(\bar{x}, y, m) = 1 \iff h(\bar{x}, y, m) \neq 0 \iff m \text{ は (22) の条件を満たす}$$

と h を定義すると，h は初等関数であり，

$$f(\bar{x}, y) = \sum_{m \leqslant q(\bar{x}, y)} h(\bar{x}, m) \cdot (m)_y$$

が成立する．よって，f は初等関数である．

逆方向については，総和と総乗が有界原始再帰法によって定義できることを示せばよい．例 5.6 において総和と総乗が原始再帰法によって定義できることを示したので，これらの有界性をみればよい．これについては，

$$\begin{aligned} \sum_{z \leqslant y} p(\bar{x}, z) &\leqslant (y + 1) \cdot \max_{z \leqslant y} p(\bar{x}, z), \\ \prod_{z \leqslant y} p(\bar{x}, z) &\leqslant (\max_{z \leqslant y} p(\bar{x}, z))^{y+1} \end{aligned}$$

であるから，$q(\bar{x}, y) = \max_{z \leqslant y} p(\bar{x}, z)$ が有界原始再帰法によって構成できることを示せばよい．場合分け関数

$$\texttt{[if } z \texttt{ is zero then } x \texttt{ else } y\texttt{]} = \begin{cases} x & \text{if } z = 0, \\ y & \text{if } z \neq 0. \end{cases}$$

は $x + y$ で有界であるから，有界原始再帰法によって定義できる．$\{p(\bar{z})\}_{z \leqslant y}$ の中から最大値を達成する z を探索する関数 p^* を次の原始再帰法によって定義する．

$$\begin{aligned} p^*(\bar{x}, 0) &= 0, \\ p^*(\bar{x}, z + 1) &= \begin{cases} p^*(\bar{x}, z) & \text{if } p(\bar{x}, z + 1) \leqslant p(\bar{x}, p^*(\bar{x}, z)) \\ z + 1 & \text{otherwise.} \end{cases} \\ &= \texttt{[if } p(\bar{x}, z + 1 \dot{-} p(\bar{x}, p^*(\bar{x}, z)) \texttt{ is zero then } p^*(\bar{x}, z) \texttt{ else } z + 1\texttt{]}. \end{aligned}$$

明らかに $p^*(\bar{x}, z) \leqslant z$ であるから，有界原始再帰法によって p^* を構成できる．このとき，明らかに $\max_{z \leqslant y} p(\bar{x}, z) = p(\bar{x}, p^*(\bar{x}, y))$ であるから，定理は示された． □

有界原始再帰で初等関数を構成できることを示した．原始再帰関数にどのようなものがあるかを理解するために，原始再帰関数を構成に必要な原始再帰法の利用回数によって分類し，その各レベルがどのような関数を含むかを分析しよう．具体的には，次の関数族を考える．

$$\mathcal{PR}_n = \text{初等関数を始点とし，高々 } n \text{ 回の原始再帰法の適用で構成できる関数族.}$$

より正確には，以下のように定義する．

定義 5.12. 各 $n \in \mathbb{N}$ について，原始再帰関数の族 $\mathcal{PR}_n$ を以下のように帰納的に定義する．

1. $\mathcal{PR}_0$ を初等関数全体の族とする．
2. $\mathcal{PR}_{n+1}$ を $\mathcal{PR}_n$ から任意回の合成と高々 1 回の原始再帰法の適用で構成できる関数全体の族とする．

例 5.13. 演習問題 5.1 で定義を与えたクヌースの矢印表記 $\uparrow^n$ について，定義より $\uparrow^1$ は初等関数である．よって，$\uparrow^{n+1}$ は $\mathcal{PR}_n$ に属す．一方，$\uparrow^{n+2}$ は $\mathcal{PR}_n$ に属さないことが知られている．

以後，$\mathcal{PR}_n$ に属す関数を，**階数 n の原始再帰関数**と呼ぶこととする．$\mathcal{PR}_n$ の性質を調べるために，次のような初等関数の相対化を考えよう．

定義 5.14. 関数 $g : \mathbb{N} \to \mathbb{N}$ が与えられているとする．このとき，以下のように，**g-初等関数** (g-*elementary function*) を帰納的に定義する．

1. 初期関数，加法 $x + y$, 部分的減法 $x \dot{-} y$, および g は g-初等関数である．
2. g-初等関数たちの合成は g-初等関数である．
3. g-初等関数から総和，総乗によって定義される関数は g-初等関数である．

g-初等関数全体の族を $\mathcal{E}(g)$ と書こう．ここで主に取り扱うものは $\mathcal{E}(\uparrow^n)$ である．この階層は，**グジェゴルチク階層** (*Grzegorczyk hierarchy*) と呼ばれる．まず，グジェゴルチク階層が巨大関数の階層を与えることを示そう．以下，$\uparrow^n (x)$ によって $x \uparrow^n x$ を表す．関数 $f, g : \mathbb{N} \to \mathbb{N}$ について，g が f を**支配** (*dominate*) するとは，次が成立することである．

$$(\exists d \in \mathbb{N})(\forall x \geqslant d)\ f(x) \leqslant g(x).$$

補題 5.15. $n \geqslant 1$ とする．任意の関数 $f \in \mathcal{E}(\uparrow^n)$ について，$\uparrow^n$ のある定数 c 回合成 $(\uparrow^n)^{(c)}$ が f を支配する．

Proof. 総和と総乗について示せばよい． □

定理 5.16. 任意の $n \in \mathbb{N}$ について，$\mathcal{PR}_n = \mathcal{E}(\uparrow^{n+1})$ が成立する．つまり，

階数 n の原始再帰関数 $= (\uparrow^{n+1})$-初等関数.

Proof. まず，$\uparrow^{n+1} \in \mathcal{PR}_n$ であるから，$\mathcal{E}(\uparrow^{n+1}) \subseteq \mathcal{PR}_n$ であることは明らかである．逆向きの包含関係を帰納法により証明する．$\mathcal{PR}_n = \mathcal{E}(\uparrow^{n+1})$ は既に示されていると仮定する．$\mathcal{PR}_{n+1} = \mathcal{E}(\uparrow^{n+2})$ を示すためには，$\mathcal{E}(\uparrow^{n+1})$ の関数から 1 回の原始再帰法の適用で定義できる関数が $\mathcal{E}(\uparrow^{n+2})$ に属すことを示せばよい．$g, h \in \mathcal{E}(\uparrow^{n+1})$ から原始再帰法によって f が構成されていると仮定する．f の構成過程をコードする関数 t を次によって定義する．

$$t(\langle \bar{x}, n, z \rangle) = \langle \bar{x}, n+1, h(\bar{x}, n, z) \rangle.$$

このとき，

$$t^{(y)}(\langle \bar{x}, 0, g(\bar{x}) \rangle) = \langle \bar{x}, y, f(\bar{x}, y) \rangle.$$

が成立するから，$(x, y) \mapsto t^{(y)}(x)$ から合成を用いて f を定義できる．これより，関数 $(x, y) \mapsto t^{(y)}(x)$ が $\mathcal{E}(\uparrow^{n+2})$ に属すことを示せばよい．定理 5.11 と同様にして，$\mathcal{E}(\uparrow^{n+2})$ が有界原始再帰法で閉じていることは示せるので，ある $s \in \mathcal{E}(\uparrow^{n+2})$ が存在して，$t^{(y)}(x) \leqslant s(x, y)$ であることを示せば十分である．補題 5.15 より，ある定数 c が存在して，十分大きな x について，$t(x) \leqslant (\uparrow^{n+1})^{(c)}(x)$ が成立する．よって，十分大きな x, y について，

$$t^{(y)}(x) \leqslant (\uparrow^{n+1})^{(c+y)}(x) \leqslant \uparrow^{n+2} (x + y).$$

よって，$t^{(y)}(x)$ は $\mathcal{E}(\uparrow^{n+2})$ の関数で抑えられることが示された．以上より，$\mathcal{PR}_{n+1} = \mathcal{E}(\uparrow^{n+2})$ が結論付けられる． □

5.3 有界原始再帰と多項式時間計算*

定義 5.10 の有界原始再帰法は，初等関数を特徴づける．

定義 5.17 (語上の有界原始再帰法)**.** 関数 $g : (\Sigma^*)^n \to \Sigma^*$ と各 $\mathtt{a} \in \Sigma$ について $h_{\mathtt{a}} : (\Sigma^*)^{n+2} \to \Sigma^*$ および $t : (\Sigma^*)^{n+1} \to \Sigma^*$ が与えられているとする．さらに，$f : (\Sigma^*)^{n+1} \to \Sigma^*$ が，次のように定義されるとしよう: 任意の $\bar{x} \in (\Sigma^*)^n$ と $y \in \Sigma^*$ について，

$$\begin{cases} f(\bar{x}, \sqcup) = g(\bar{x}), \\ f(\bar{x}, y\mathtt{a}) = h_{\mathtt{a}}(\bar{x}, y, f(\bar{x}, y)), \\ |f(\bar{x}, y)| \leqslant |t(\bar{x}, y)| \end{cases}$$

このとき，f は g, h, t から**語上の有界原始再帰法** (*bounded primitive recursion on notations*) によって定義されるという．

1964 年，Cobham は，実はこの概念によって多項式時間計算可能性を特徴づけることができる．多項式時間計算可能性の詳細については後に述べるが，.

定理 5.18 (Cobham の定理)**.** 多項式時間計算可能関数全体の族は，以下を満たす最小の関数族と正確に一致する．

- 初期関数と関数 $(x, y) \mapsto x^{|y|}$ を含む．
- 合成と語上の有界原始再帰法で閉じている．

原始再帰関数をプログラミング言語と考えよう．関数 $g : (\Sigma^*)^n \to \Sigma^*$ と $h_{\mathtt{a}} : (\Sigma^*)^{n+2} \to \Sigma^*$ および多項式 p, q が与えられているとする．$f_* : (\Sigma^*)^n \times \mathbb{N} \to \Sigma^*$ が，次のように定義されるとしよう: 任意の $\bar{x} \in (\Sigma^*)^n$ と $y \in \mathbb{N}$ について，

$$\begin{cases} f_*(\bar{x}, 0) = g(\bar{x}), \\ f_*(\bar{x}, y+1) = h(\bar{x}, y, f_*(\bar{x}, y)), \\ |f_*(\bar{x}, y)| \leqslant q(|\bar{x}|) \text{ for all } y \leqslant p(|\bar{x}|). \end{cases}$$

さらに，$f : (\Sigma^*)^n \to \Sigma^*$ は次のように定義されるとする．

$$f(\bar{x}) = f_*(\bar{x}, p(|\bar{x}|)).$$

このとき，f は g, h, p, q から**多項式有界原始再帰法** (*polynomially bounded primitive recursion*) によって定義されるという．

補題 5.19. 多項式時間計算可能関数全体の族は，以下を満たす最小の関数族と正確に一致する．

- 初期関数と関数 $x \mapsto x\mathtt{a}$ および $x \mapsto x^-$ を含む．
- 合成と多項式有界原始再帰法で閉じている．

Proof. $\mathcal{B}$ を主張内の最小の関数族とする．まず，$\mathcal{B}$ に含まれる任意の関数が多項式時間計算可能関数であることを示す．g, h が多項式時間計算可能であり，p, q が多項式であるとする．f が g, h, p, q から多項式有界原始再帰法で定義されていると仮定する．このとき，$f(|\bar{x}|)$ を計算するためには，まず $g(|\bar{x}|)$ から開始して，h を $p(|\bar{x}|)$ 回適用すればよい．ここで，$f(|\bar{x}|)$ を計算するのに必要な h の入力の長さは高々 $q(|\bar{x}|)$ であるから，$|\bar{x}|$ に対する多項式時間でその値を計算できる．

逆を示すには，多項式時間 p で関数を計算するチューリング機械 M の計算状況を $\mathcal{B}$ でシミュレートする必要がある．ここでは証明のスケッチを与える．まず，次を考える．

$$g(\bar{x}) = \text{入力 } \bar{x} \text{ に対する } M \text{ の計算の初期状況のコード}$$
$$h(\bar{x}, y, z) = z \text{ でコードされる計算状況の次ステップの計算状況}$$

このコーディングは，通常のように多項式有界原始再帰で行うことができる．f_* は g と h から原始再帰によって定義されるものとする．M は多項式時間チューリング機械であるから，計算状況のコード長は $|\bar{x}|$ に関する多項式で抑えられる．また，計算は高々 $p(|\bar{x}|)$ 時間で停止するから，停止時点での計算状況は $f(\bar{x}) = f_*(\bar{x}, p(|\bar{x}|))$ を見ればよい．よって，$f \in \mathcal{B}$ であり，f から M の出力の復元も $\mathcal{B}$ によって容易に行うことができる． □

*Proof (*定理 *5.18).* $\mathcal{C}$ を定理 5.18 の主張における最小の関数族とする．まず，$\mathcal{C}$ に含まれる任意の関数が多項式時間計算可能関数であることを示す．このためには，多項式時間計算可能性が語上の有界原始再帰で閉じていることを示せばよい．g, h, t が多項式時間計算可能であるとする．$f(\bar{x}, y)$ を求めるためには，$|y|$ 回の計算を行えばよい．さらに，t は多項式時間計算可能であるから，$|t(\bar{x}, y)|$ は $|\bar{x}|$ と $|y|$ に関する多項式で抑えられる．つまり，f は多項式時間有界原始再帰から定義されるので，補題 5.19 より多項式時間計算可能であることが従う．

つづいて, $\mathcal{C}$ が多項式有界原始再帰で閉じていることを示す．まず, p が多項式ならば $\bar{x} \mapsto 0^{p(|\bar{x}|)}$ が $\mathcal{C}$ に属すことは容易に確認できる．f が g と h から多項式有界原始再帰によって定義されていると仮定する．このとき，

$$
\begin{aligned}
v(\bar{x}, \sqcup) &= g(\bar{x}), \\
v(\bar{x}, y\mathsf{a}) &= \begin{cases} h(\bar{x}, y, v(\bar{x}, y)), & \text{if } |y| \leqslant p(|\bar{x}|), \\ 0, & \text{otherwise} \end{cases}
\end{aligned}
$$

として定義する．このとき

$$
|v(\bar{x}, y)| = |f_*(\bar{x}, |y| - 1)| \leqslant q(|\bar{x}|)
$$

であるから，語上の有界原始再帰の条件を満たす．また，多項式場合分け関数は $\mathcal{C}$ に属すから，v は $\mathcal{C}$ に属す．よって，一方，$f(\bar{x}) = f_*(\bar{x}, p(|\bar{x}|)) = v(\bar{x}, 0^{p(|\bar{x}|)})$ であるから，合成によって f が $\mathcal{C}$ に属すことが示された． □