

情報科学基礎論

推論と論理

山本 章博

京都大学 情報学研究科

<http://www.i.kyoto-u.ac.jp/~akihiro>



数理論理学



情報科学における論理

- 論理回路
- 計算の原理
- 定理自動証明
- ハードウェア・ソフトウェアの正当性
- データベースの正当性

- 推論

与えられた(観測可能な)前提から、明示的に表示されていない結論を導出



数理論理学

- 命題や論証の正しさを数学的手法で明らかにする

もともとは

- 論理学：思考の法則を研究する学問
 - 思考：人間の知的活動
- 数理論理学：論理を数学的手法で研究
 - 思考の法則を数学的手法で研究
 - 人間の知的活動を対象とした数学



数学的対象としての命題

- 命題：正しいか否かに関心がある文
 - 文：ある言語中の語と語彙の並び
 - 命題が正しいかどうかを知る，こととは区別する

例：“二等辺三角形の底角は等しい”

“29は3で割り切れる”

“新薬〇〇はがんに効く”

- “命題”を対象とした数学を構成する
 - “4は偶数である”
 - “4は偶数である”は正しい命題である



意味論と証明論

命題の“正しさ”の形式化に対する二つの立場

- 意味論(semantics)

命題の“正しさ”を数学的な“値”を用いて表現

- Booleは0, 1で表現 → Boole代数

- 証明論(syntax)

命題の“正しさ”を数学的な証明を用いて表現

- 前提となる命題から結論となる命題を“正しく”導く規則を用いる



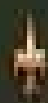
Click to **LOOK INSIDE!**



An Investigation of The Laws of Thought



George Boole





論理式

- 数学的対象として扱えるように，命題を記述するための形式言語(人工言語)を設計する
 - 命題のどのような性質に着目するかに依存して，さまざまなものが設計されている.

命題論理，述語論理，様相論理，...

- 数学で用いられる形式言語の例：多項式

$$x^2 y + x (y^3 + z)$$

- 多項式は数の計算方法とその結果を表現する句(文)
- “多項式の計算”は，多項式という文の扱い方

➡ 命題を数学的に扱うための文：論理式



意味論と証明論

命題の“正しさ”の形式化に対する二つの立場

- 意味論(semantics)

命題の正しさを代数的構造で表現

1, 0 (真偽値)だけを用いる空間

- 1 は 真, 0 は 偽 を表す.
- 真偽値間の演算は真理値表により定義

- 証明論(syntax)

演繹的な推論を命題の操作として形式化

正しい命題を導く捜査を規則で表現



命題論理



命題論理とは

- 最小単位として, 肯定の単文を用いる言語を設計する
 - p : “29は3で割り切れる”
 - “二等辺三角形の底角は等しい”
 - ➡ “三角形ABCが二等辺三角形である”
ならば“三角形ABCの底角は等しい”



命題論理とは

- 語彙として, 否定文をつくる副詞, 単文をつなぐ接続詞を用意する.
 - p : “29は3で割り切れる”
 $\neg p$: “29は3で割り切れない”
 - q : “三角形ABCが二等辺三角形である”
 r : “三角形ABCの底角は等しい”
 $q \rightarrow r$: “三角形ABCが二等辺三角形である”
ならば“三角形ABCの底角は等しい”
 - s : “6は3で割り切れる”
 t : “6は2で割り切れる”
 $s \wedge t$: “6は3で割り切れる”かつ“6は2で割り切れる”



命題論理(2)

接続詞

自然言語

... かつ ... (and)

... または ... (or)

... ならば ... (If..., then...)

... かつそのときに限り

(...if and only if ...)

... でない

命題論理

$\wedge$ $\&$

$\vee$

$\rightarrow$ $\supset$

$\leftrightarrow$ $\equiv$

$\neg$



命題論理に用いる言語

Definition アルファベット

- 命題記号 : $p, q, r, \dots, p_1, p_2, \dots$
- 命題定数 : $\square(\perp), \blacksquare(T)$
- 論理結合子 : $\wedge, \vee, \rightarrow, \leftarrow, \leftrightarrow,$
- 補助記号 : $()$

Definition 命題論理に用いる言語は, 下のように帰納的に定義される論理式からなる:

- 命題記号と命題定数は論理式である
- φ と ζ が論理式であれば,
 $(\varphi \wedge \zeta), (\varphi \vee \zeta), (\varphi \rightarrow \zeta), (\varphi \leftarrow \zeta), (\varphi \leftrightarrow \zeta), (\neg \varphi)$
はすべて論理式である.

Note ここで定義される言語は文脈自由言語である, すなわち, ある文脈自由文法によって構成される.



証明論



数理論理学

- 命題や論証の正しさを数学的手法で明らかにする

もともとは

- 論理学：思考の法則を研究する学問
 - 思考：人間の知的活動
- 数理論理学：論理を数学的手法で研究
 - 思考の法則を数学的手法で研究
 - 人間の知的活動を対象とした数学



辞書では

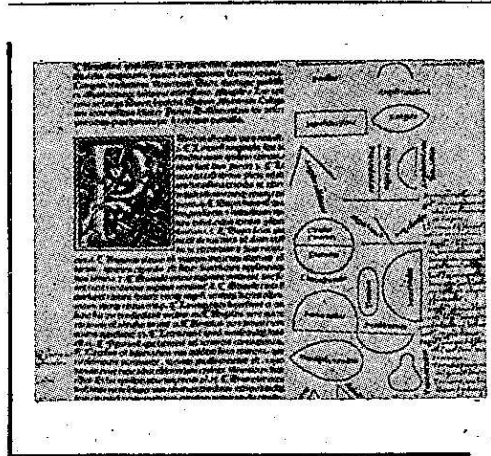
広辞苑(第五版)

- 【演繹】(deduction)推論の一種。前提を認めるならば、結論もまた必然的に認めざるをえないもの。数学における証明はその典型。

Concise Oxford Dictionary

- Deduction: . the inferring of particular instances from a general law

第2章



図形と論証

ユークリッドの「原論」

数学Iでも学んだように、数学では、種々の命題を取り扱い、証明によって、その真偽を明らかにしながら、正しい命題を次々に積み重ねて、1つの体系に組み立てていく。

ここでは、その方法を、平面上の図形を研究する幾何学を例にとって、くわしく考えていこう。

■ 公 理

一般に、ある命題Xが正しいと判断するには、大きく分けて、2つの方法がある。

その1つは、命題Xに関する具体例をいくつか調べて、どの例についても、命題Xの成り立つことから、その命題Xが正しいと結論する方法である。

たとえば、命題

「正三角形の3つの内角は、すべて、 60° である」 …………… ①

が正しいことを示すのに、いくつかの正三角形の内角を測って、どの場合にも、3つの内角がすべて 60° であるから、①は正しいと結論する方法である。この方法は、帰納的方法と呼ばれ、自然科学・社会科学の分野など広く一般に用いられる。

他の1つは、すでに正しいことが認められている他の命題A, B, C, ……………などを根拠にして、命題Xが正しいことを、論理的に導く方法である。

たとえば、上の命題①は、中学校で学んだように、次の2つの命題
「三角形において、2つの辺が等しいならば、

それらの辺に対する角は等しい」 …………… ②

「三角形の3つの内角の和は 180° である」 …………… ③

から導かれる。

この方法を、**演えき的方法**と呼び、この方法において、命題が正しいことを論理的に導く過程が**証明**である。

ある命題Xが、帰納的方法によって正しいと判断されたとしても、それが、あらゆる可能な場合について検討されたものでない限り、命題Xが厳密に正しいと結論することは、立証の方法としては、不完全である。

これに対して、演えき的方法によって、命題Xの正しいことが証明されたときは、その証明の根拠となった命題が正しいものである限り、命題Xも、また、厳密に正しい。

数学における正しい命題は、例外なく成り立つことが必要であるから、その正しいことは、演えき的に示されたものでなければならない。

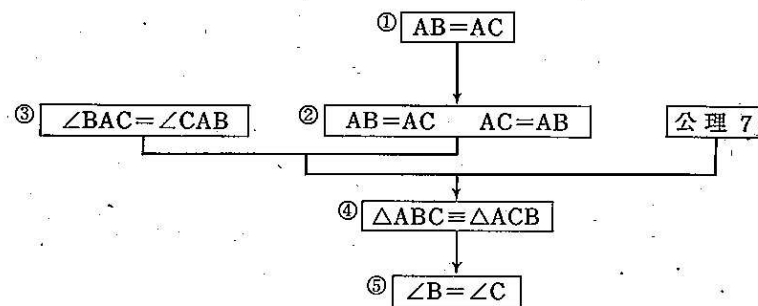
公理

演えき的に、ある新しい命題を証明するには、他の正しい命題を根拠にとる必要がある。ところが、この根拠にとった命題の正しいことを証明するには、また、他の正しい命題を根拠にとる必要がある。しかし、このようにして、次々に根拠をたどっていくとすると、いつまでたっても、証明は完了しない。また、実際には、より基本的な根拠を求めることが、しだいに、むずかしくなってくる。

そこで、あらかじめ正しいことが明らかだと思われる基本的な命題を、いくつか定めておいて、その正しいことは証明なしで認めることとし、これらの基本的な命題を用いて証明される命題は、すべて正しいとする。このとき、これらの基本命題を**公理**という。

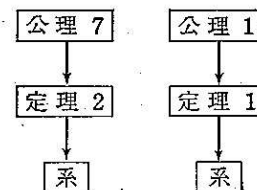
また、定理2の証明の内容を分析し、図に表わすと、下の図のようになる。

この図からわかるように、この証明では、仮設 $AB=AC$ と公理7を用いて、結論 $\angle B=\angle C$ を導いている。



一般に、命題 $p \rightarrow q$ …… ④ が正しいことを証明するには、公理・定理など、すでに正しいことが認められている命題と、④の仮設 p を用いて、結論 q を導けばよい。

また、上の図から明らかなように、定理2の証明の根拠となっている命題は、公理7であることがわかる。同様にして、62ページの定理1は、公理1を根拠としている。



また、定理1では

仮設： l と m が異なる

結論： l, m は2点以上を共有しない

であるが、その証明では、結論の否定から矛盾を導き、結論の正しいことを示している。

数学Iでも学んだように、このような証明法を 背理法 という。



演繹における命題, 証明

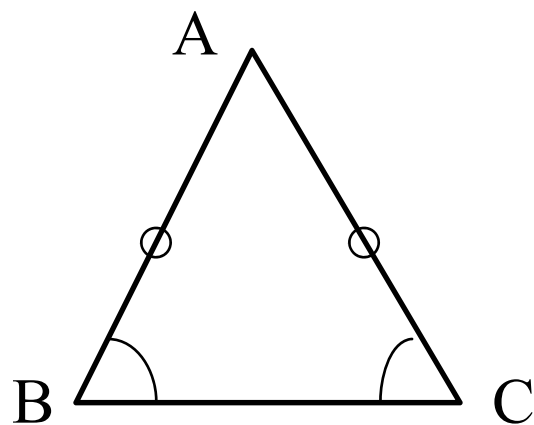
- 命題: 正しさを考察対象とする文
 - 数学では, その意義や用途に応じて, 定理, 補題, 命題, 公理, などと呼ばれる
- 証明: 命題から命題を次々と導く連鎖

証明の例

考察の対象: ユークリッド幾何

定理 三角形ABCが二等辺ならば底角は等しい

$$AB = AC \rightarrow \angle ABC = \angle ACB$$



人手による“証明”

■ 前提: $AB=AC$ (1)

(1)から $AC=AB$ (2)

一方

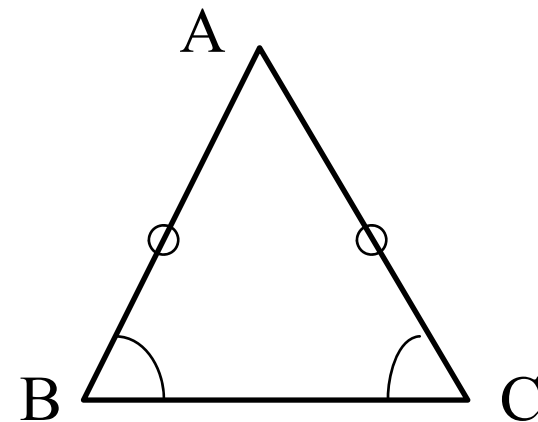
$$\angle BAC \equiv \angle CAB \quad (3)$$

(1), (2), (3)に三角形の合同条件を適用して

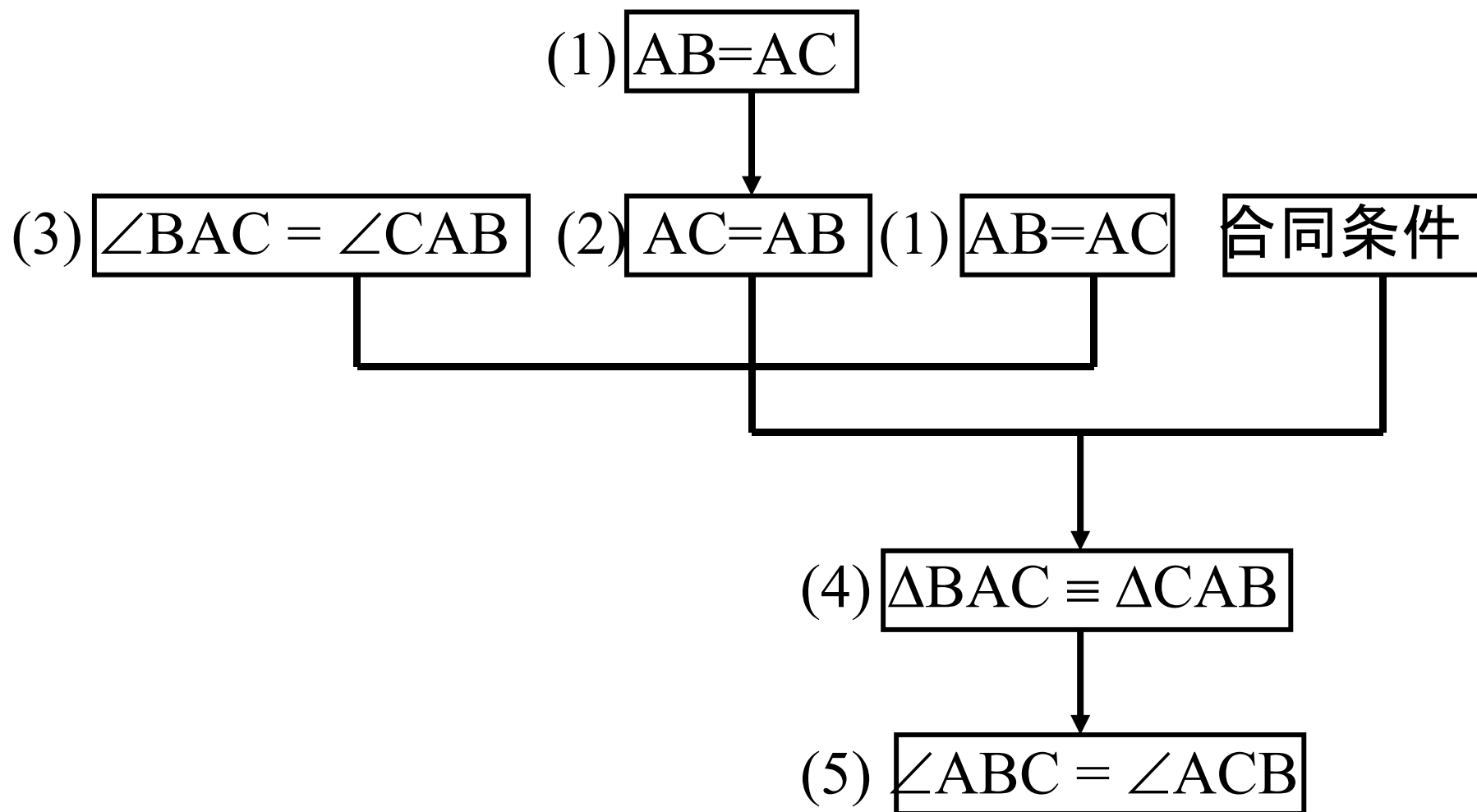
$$\triangle BAC = \triangle CAB \quad (4)$$

したがって

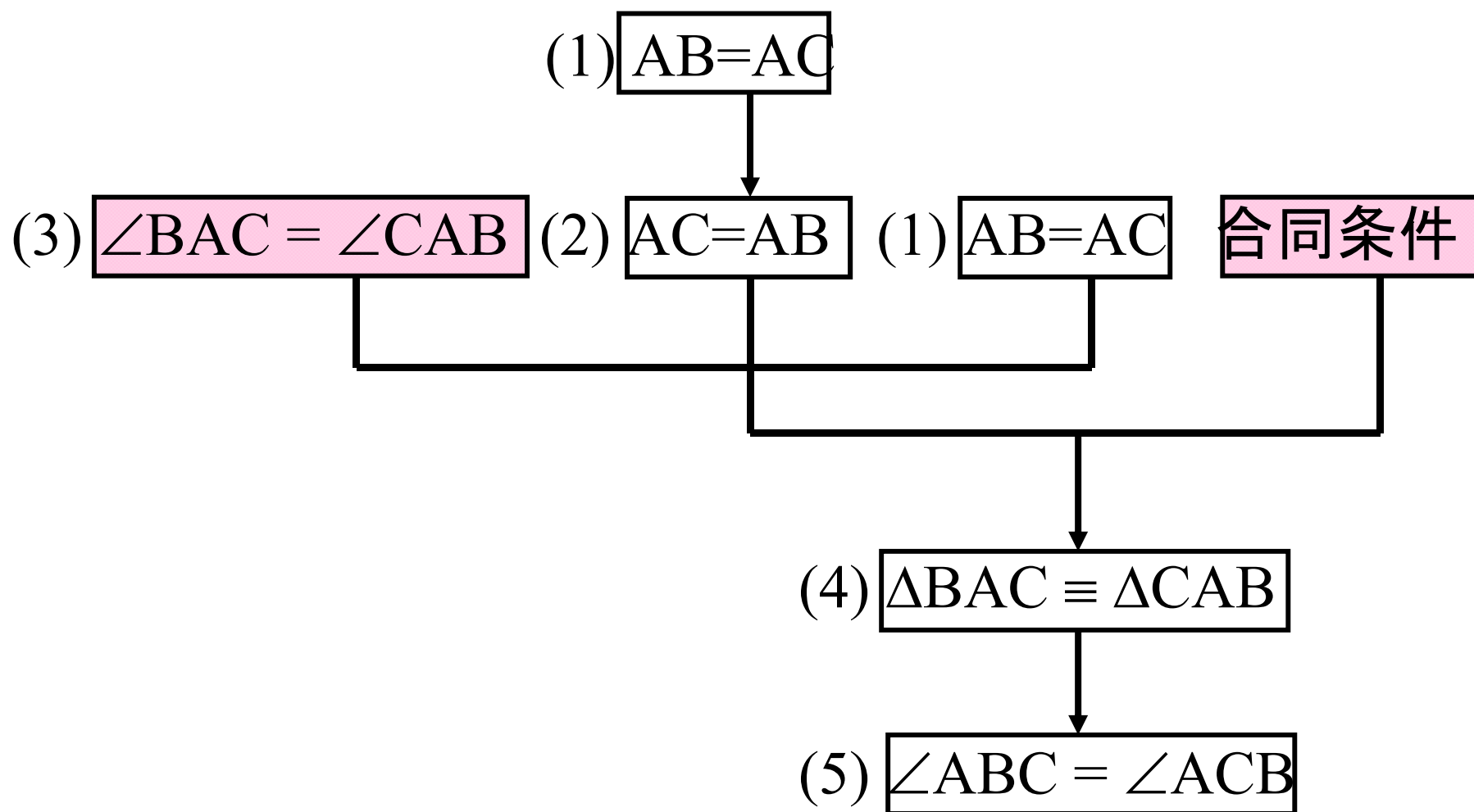
$$\angle ABC = \angle ACB \quad (5)$$



証明の構造

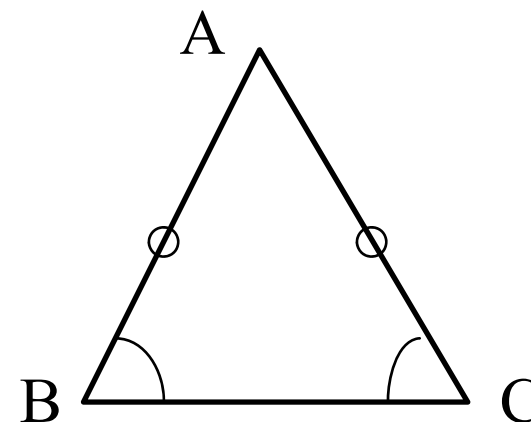


証明の構造



明示的には用いていない命題

- $AB=AC$ (1) $\rightarrow AC=AB$ (2)
- $\angle BAC = \angle CAB$ (3)
- 三角形の合同条件
 - 二辺とその挟角が等しい三角形は合同
- $\triangle BAC \equiv \triangle CAB$ (4) $\rightarrow \angle ABC = \angle ACB$ (5)
 - 合同な三角形の角が等しい





公理

- 公理: 証明なしで正しさを認める命題

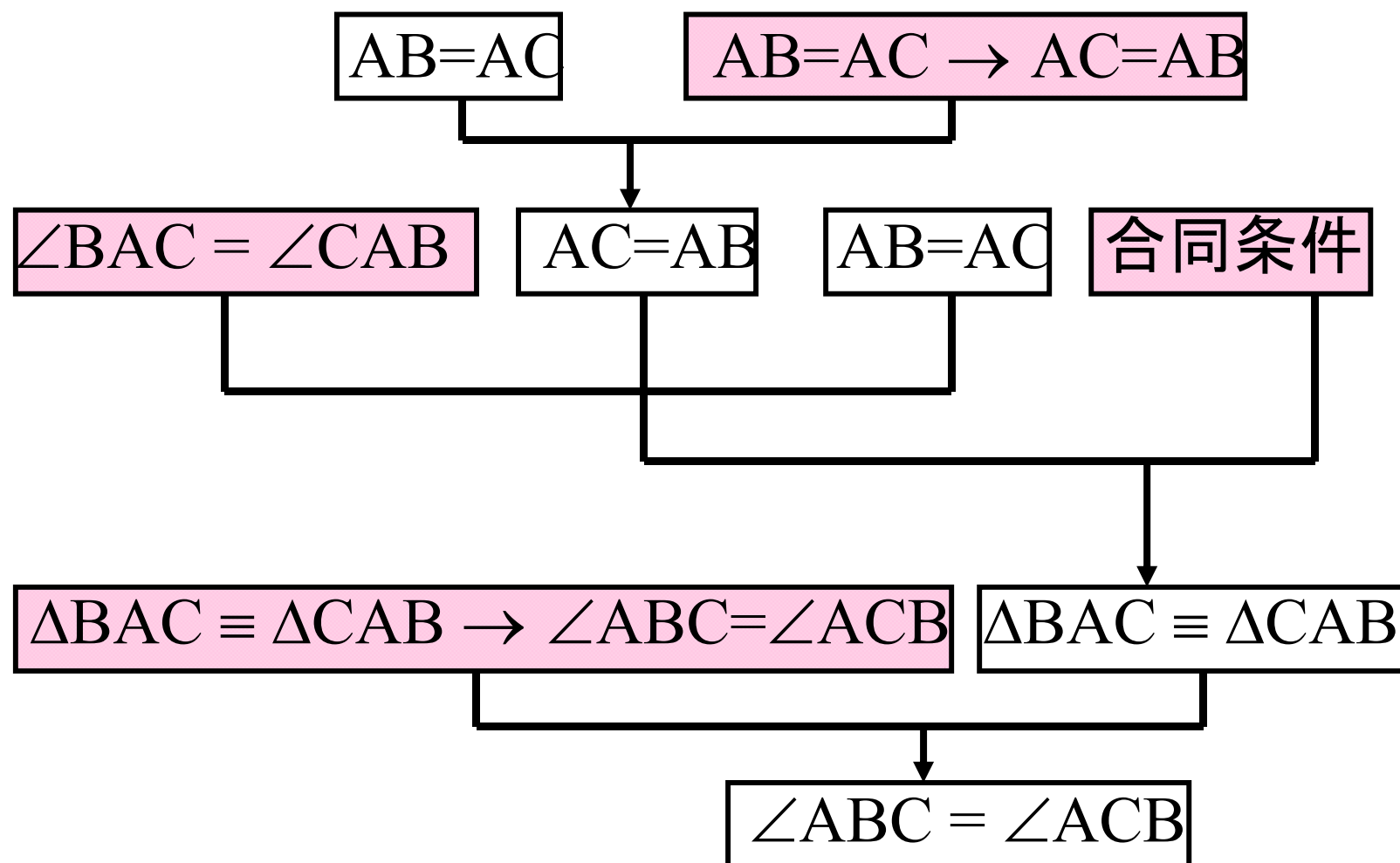
証明の始点

- 証明: 命題から命題を次々と導く連鎖 $\Rightarrow$ 始点が必要
- 公理の設定が考察対象領域を決めてしまう.

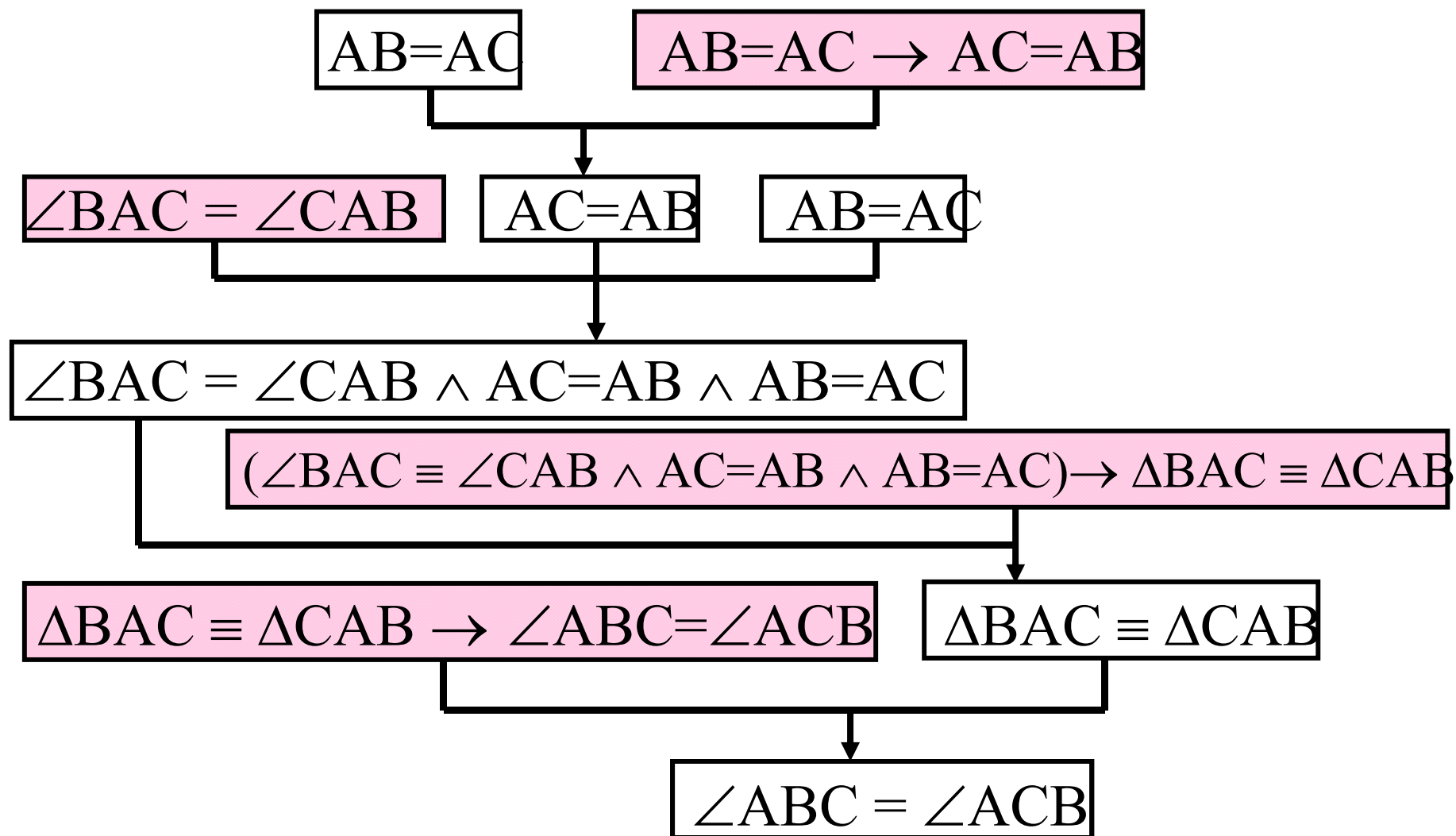
例 前出の証明で用いる公理

- 等号の対称性: $AB=AC \rightarrow AC=AB$
- 角の対称性: $\angle BAC=\angle CAB$
- 合同: $AB=EF \wedge AC=EG \wedge \angle BAC=\angle FEG \rightarrow$
 $\Delta ABC \equiv \Delta EFG$
- 合同な三角形の角が等しい:
 $\Delta BAC \equiv \Delta CAB \rightarrow \angle ABC = \angle ACB$

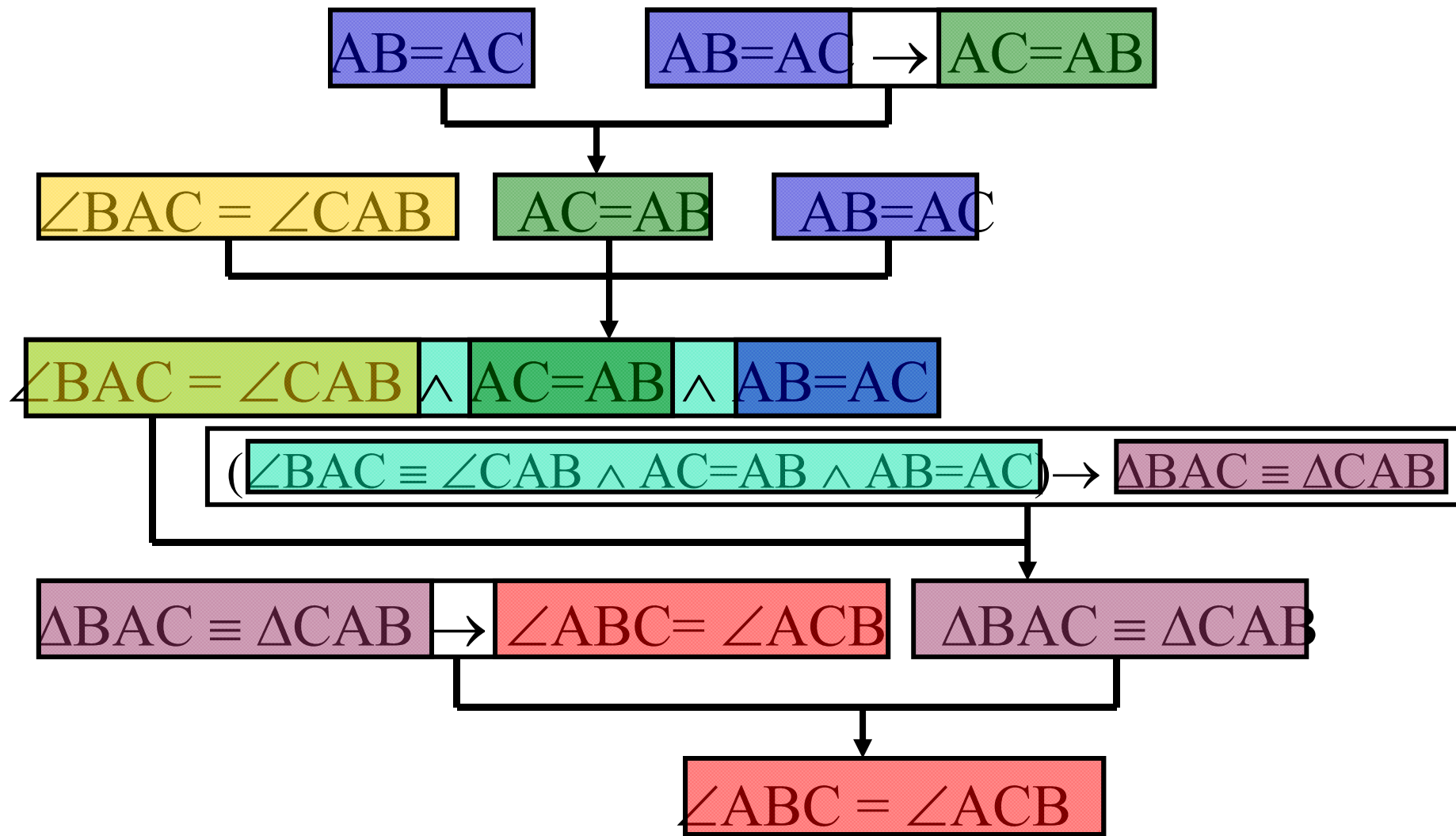
証明の構造



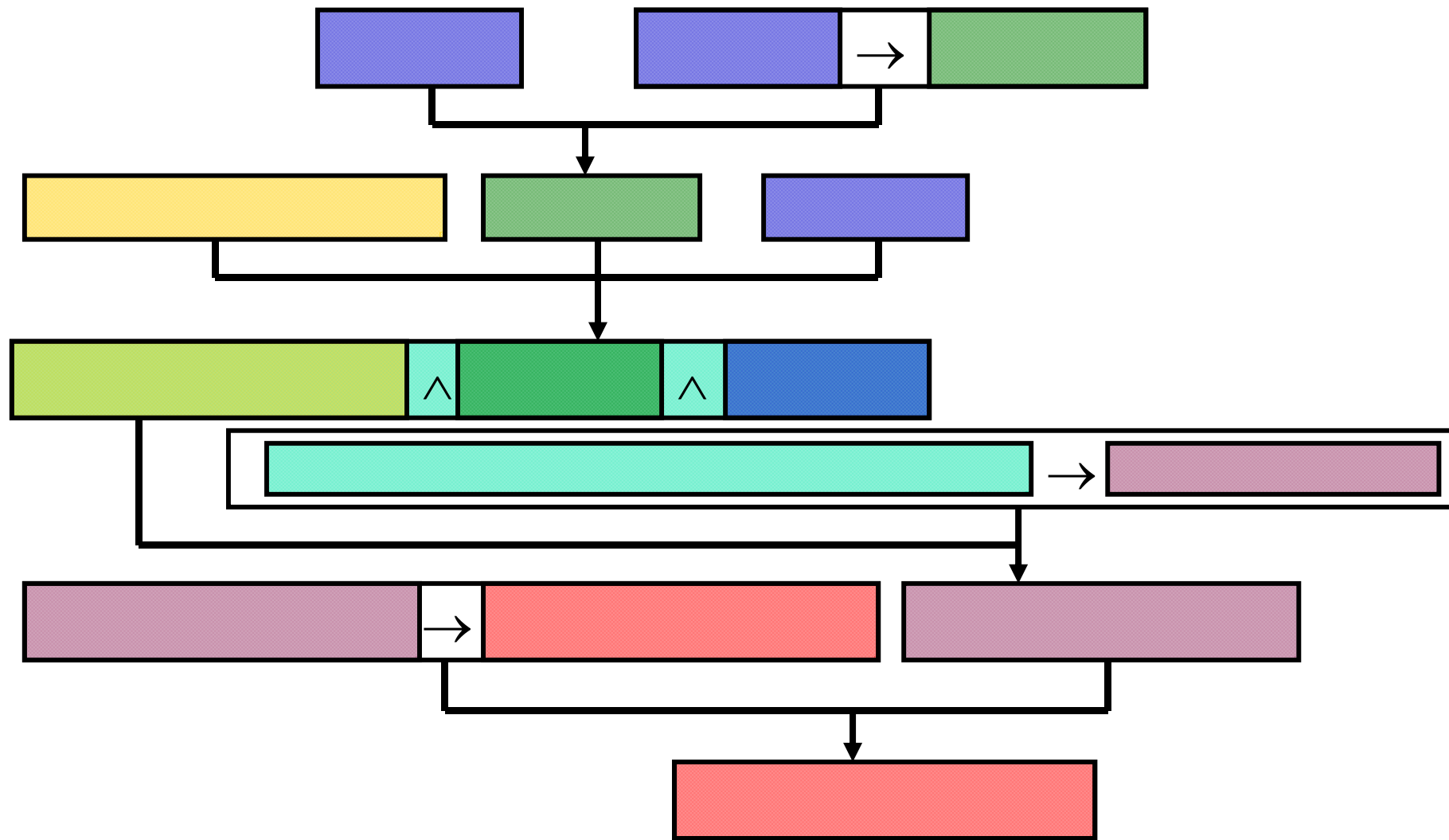
証明の構造(2)



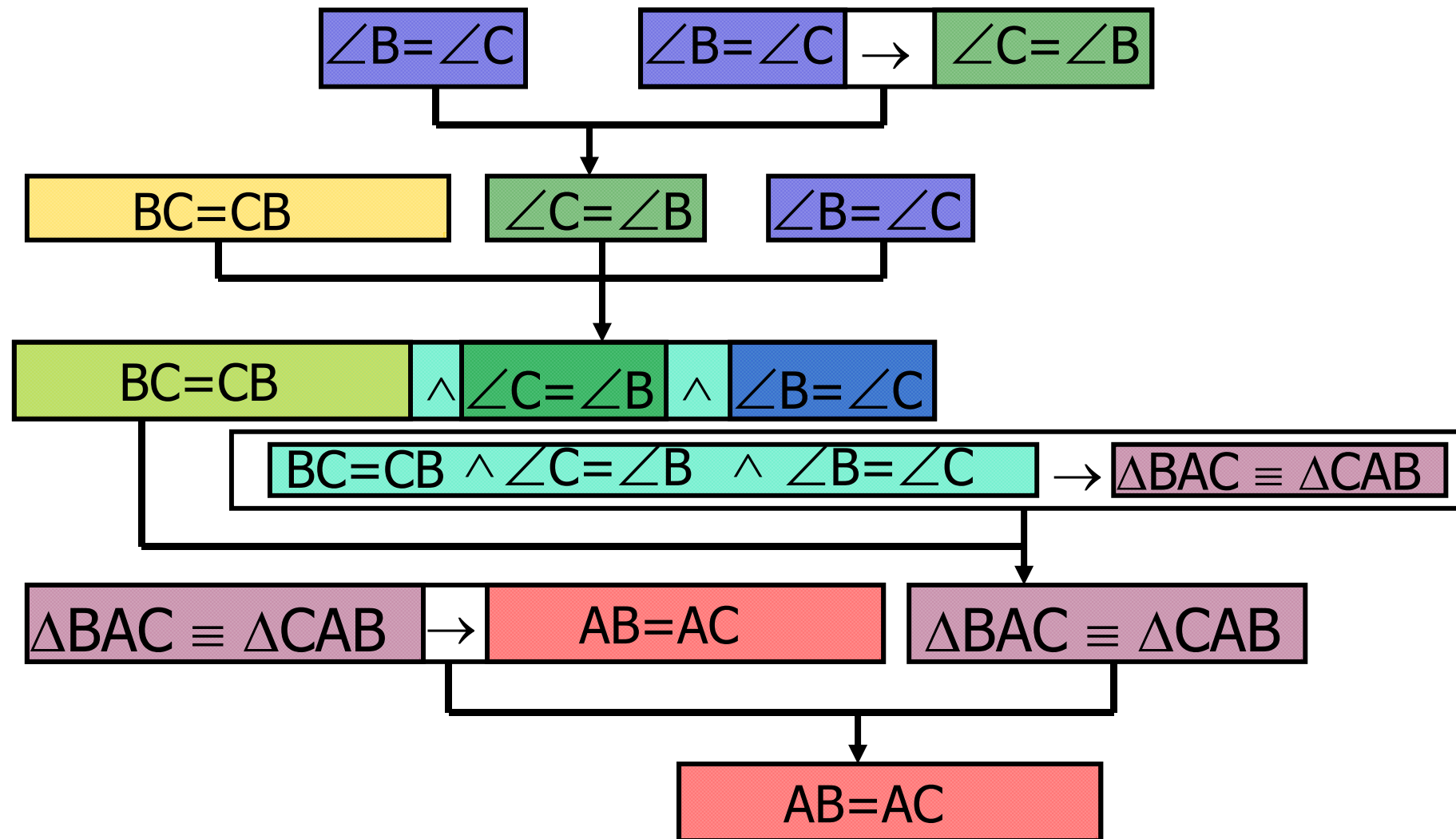
命題の構造と証明(1)



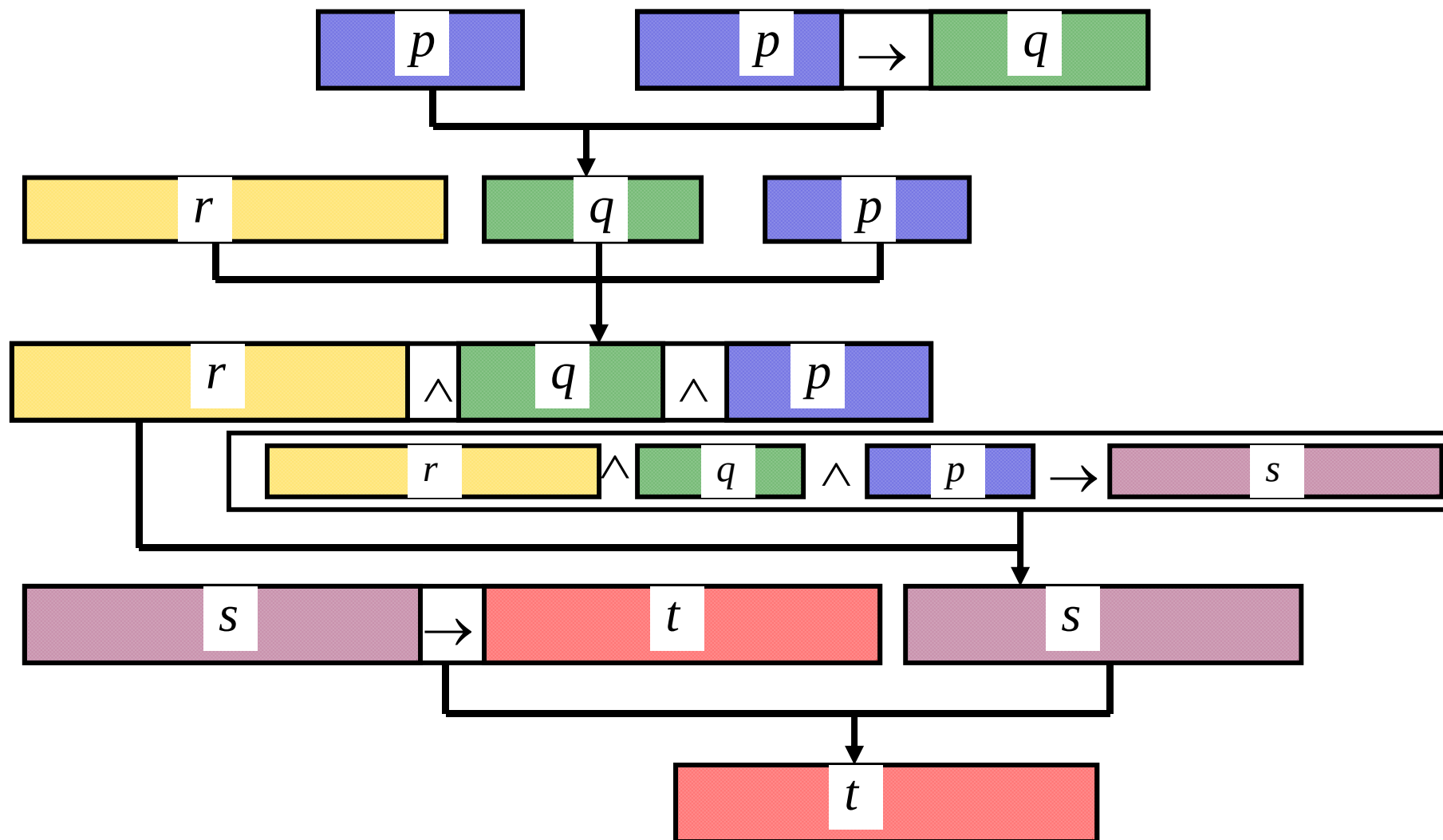
命題の構造と証明(1)



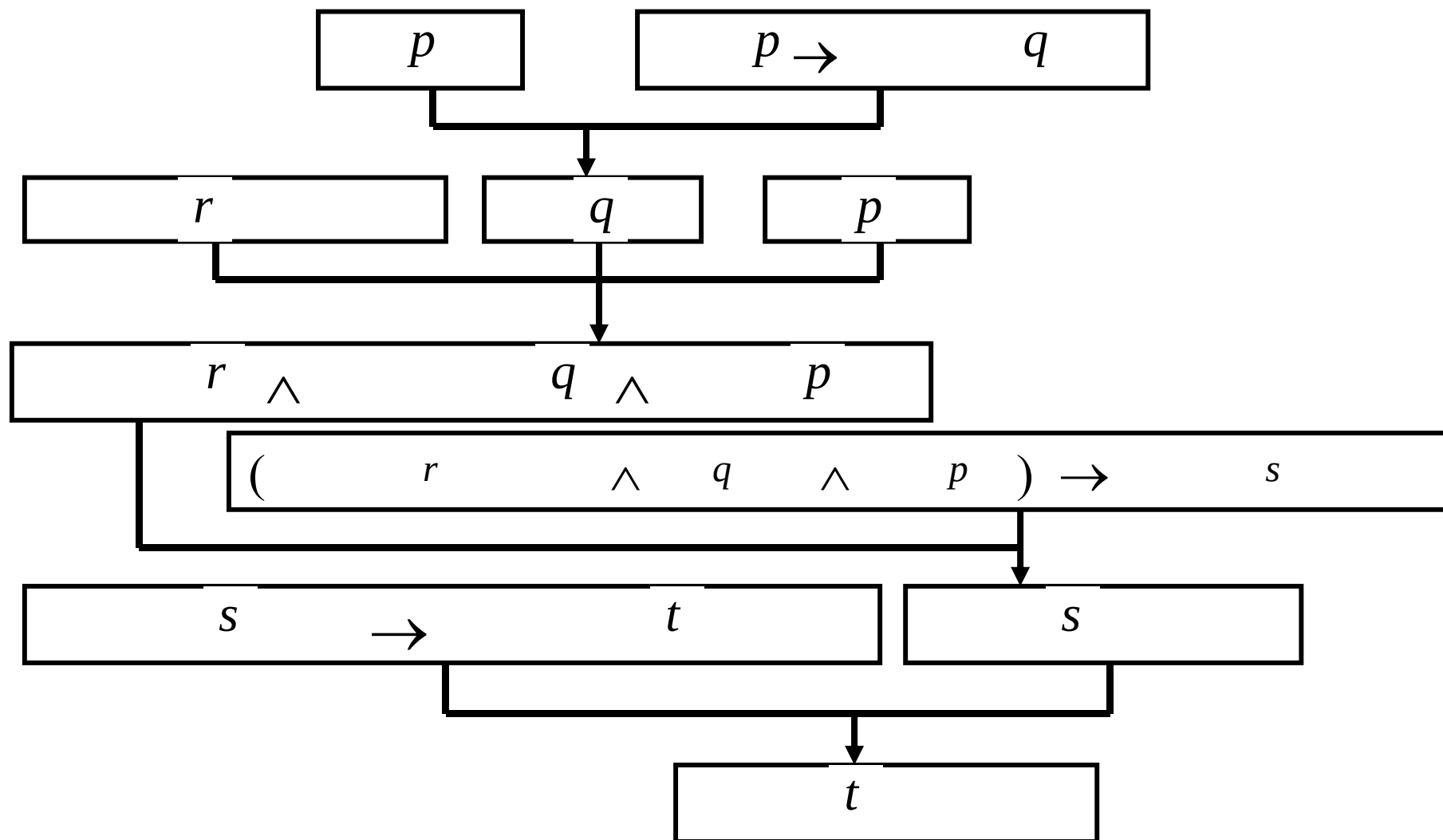
命題の構造と証明(2)



命題の構造と証明(3)

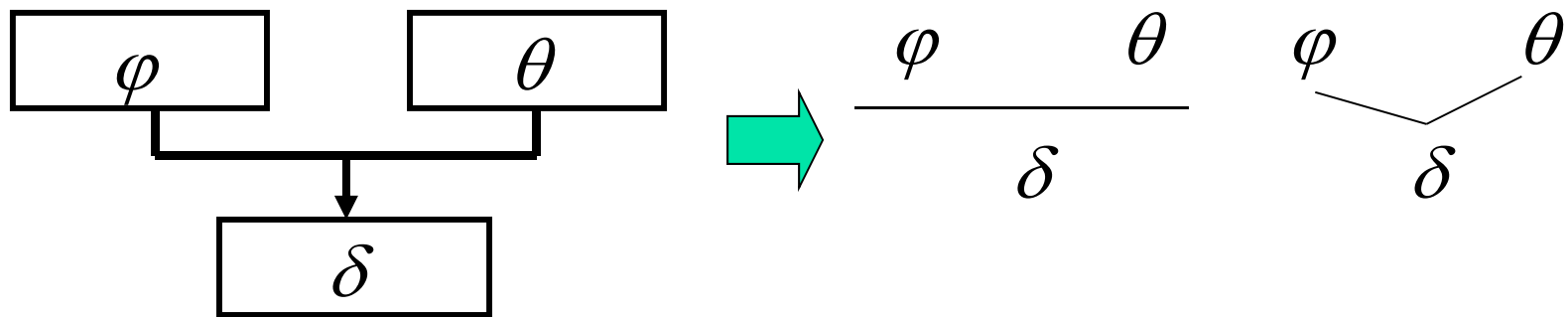


命題の構造と証明(3)



命題の構造と証明(4)

- 証明は命題中に用いられている論理結合子
 $\rightarrow$ (ならば) $\wedge$ (かつ)
の用法に従って構成されている.
- 用法と構成の関係は, 命題が何を表している
かには依存しない.
- 表記法





推論規則(1)

- 推論規則: 命題から命題を導くための規則
 - 命題中の論理結合子の用法で定まる
- 命題 φ と $\varphi \rightarrow \zeta$ から ζ を導く
 - “ φ と $\varphi \rightarrow \zeta$ が成り立つので, ζ も成り立つ”

$$\frac{\varphi \quad \varphi \rightarrow \zeta}{\zeta}$$



推論規則(2)

- 命題 φ と ζ から $\varphi \wedge \zeta$ を導く

“ φ と ζ が成り立つので, $\varphi \wedge \zeta$ も成り立つ”

$$\frac{\varphi \qquad \zeta}{\varphi \wedge \zeta}$$

- 命題 $\varphi_1, \varphi_2, \dots, \varphi_n$ から $\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n$ を導く

$$\frac{\varphi_1 \quad \varphi_2 \quad \dots \quad \varphi_n}{\varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_n}$$

推論規則(2)

$$\frac{\varphi \quad \zeta}{\varphi \wedge \zeta}$$

$$\frac{\varphi \wedge \zeta}{\varphi} \quad \frac{\varphi \wedge \zeta}{\zeta}$$

$$\frac{\varphi}{\varphi \vee \zeta} \quad \frac{\zeta}{\varphi \vee \zeta}$$

$$\frac{\varphi \vee \zeta \quad \begin{array}{c} [\varphi] \\ \dots \\ \theta \end{array} \quad \begin{array}{c} [\zeta] \\ \dots \\ \theta \end{array}}{\theta}$$

$$\frac{\begin{array}{c} [\varphi] \\ \dots \\ \zeta \end{array}}{\varphi \rightarrow \zeta}$$

$$\frac{\varphi \quad \varphi \rightarrow \zeta}{\zeta}$$

推論規則(3)

$$\frac{\begin{array}{c} [\varphi] \\ \dots \\ \perp \end{array}}{\neg \varphi}$$

$$\frac{\varphi \quad \neg \varphi}{\perp}$$

$$\frac{\begin{array}{cc} [\varphi] & [\zeta] \\ \dots & \dots \\ \zeta & \varphi \end{array}}{\varphi \leftrightarrow \zeta}$$

$$\frac{\varphi \quad \varphi \leftrightarrow \zeta}{\zeta}$$

$$\frac{\zeta \quad \varphi \leftrightarrow \zeta}{\varphi}$$

$$\frac{\perp}{\varphi}$$

$$\varphi \vee \neg \varphi$$



命題の構造と証明(3')

$$\frac{\frac{\frac{r}{s \rightarrow t} \quad \frac{\frac{p \quad p \rightarrow q}{q} \quad p}{r \wedge q \wedge p} \quad (r \wedge q \wedge p) \rightarrow s}{s}}{t}$$

証明を構成する手続き

- 証明したい論理式 $\zeta \rightarrow \theta$ と公理を表す論理式 $\varphi_1, \varphi_2, \dots, \varphi_n$ が与えられたとき, $\zeta, \varphi_1, \varphi_2, \dots, \varphi_n$ から θ に至る証明を構成する手続き

例 $\zeta \rightarrow \theta = p \rightarrow t,$

$\varphi_1 = p \rightarrow q, \varphi_2 = r, \varphi_3 = (r \wedge q \wedge p) \rightarrow s, \varphi_4 = s \rightarrow t$

$$\begin{array}{c}
 \begin{array}{c}
 \begin{array}{c}
 r \\
 \hline
 r
 \end{array}
 \quad
 \begin{array}{c}
 \begin{array}{c}
 p \quad p \rightarrow q \\
 \hline
 q
 \end{array}
 \quad
 p \\
 \hline
 r \wedge q \wedge p
 \end{array}
 \quad
 (r \wedge q \wedge p) \rightarrow s \\
 \hline
 \begin{array}{c}
 s \rightarrow t \quad s \\
 \hline
 t
 \end{array}
 \end{array}
 \end{array}$$



命題の構成方法

$$s \rightarrow t$$

$$t$$



命題の構成方法

$$\frac{s \rightarrow t \quad s}{t}$$



命題の構成方法

$$\frac{s \rightarrow t}{t} \quad \frac{(r \wedge q \wedge p) \rightarrow s}{s}$$



命題の構成方法

$$\frac{s \rightarrow t \quad \frac{r \wedge q \wedge p \quad (r \wedge q \wedge p) \rightarrow s}{s}}{t}$$



命題の構成方法

$$\frac{\frac{\frac{r}{\hline} \quad (r \wedge q \wedge p) \rightarrow s}{r \wedge q \wedge p} \quad s \rightarrow t}{s} \quad t$$



命題の構成方法

$$\frac{\frac{\frac{r}{s \rightarrow t} \quad q}{r \wedge q \wedge p} \quad (r \wedge q \wedge p) \rightarrow s}{s} t$$



命題の構成方法

$$\frac{\frac{\frac{r}{\quad} \quad \frac{q}{\quad} \quad \frac{p}{\quad}}{r \wedge q \wedge p} \quad (r \wedge q \wedge p) \rightarrow s}{\frac{s \rightarrow t \quad s}{t}} t$$



命題の構成方法

$$\frac{\frac{\frac{r}{s \rightarrow t} \quad \frac{\frac{p \rightarrow q}{q} \quad p}{r \wedge q \wedge p}}{(r \wedge q \wedge p) \rightarrow s} \quad s}{t}$$



命題の構成方法

$$\frac{\frac{\frac{r}{s \rightarrow t} \quad \frac{\frac{p \quad p \rightarrow q}{q} \quad p}{r \wedge q \wedge p} \quad (r \wedge q \wedge p) \rightarrow s}{s}}{t}$$

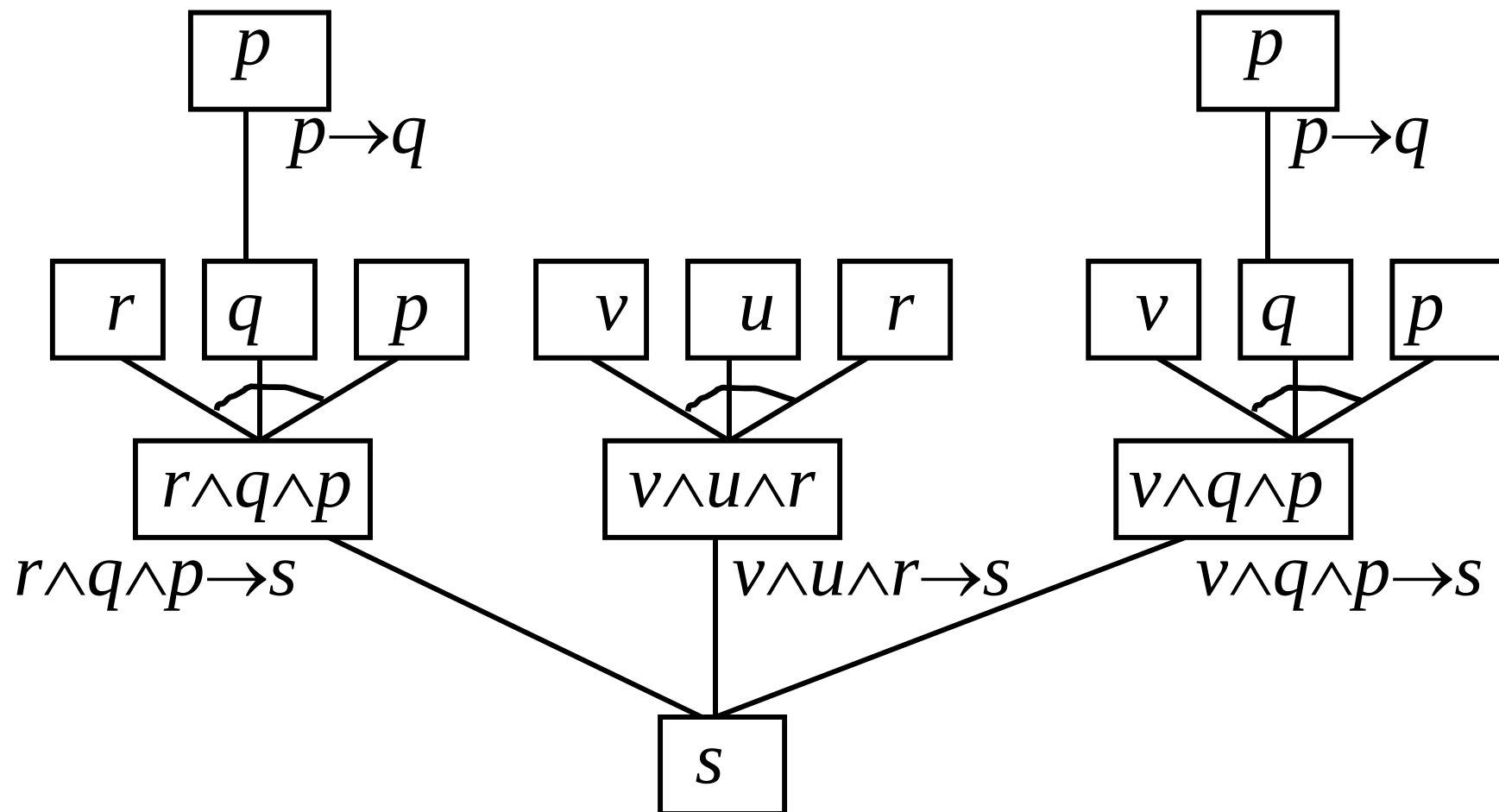


証明と探索(1)

- ある命題を証明するために適用可能な公理や命題は複数あり得る.
- 選択した公理や命題によっては証明が構成できないことがある.
 - s: $\triangle BAC = \triangle CAB$ を結論とする命題は複数ある
$$\angle B = \angle C \wedge AC = AB \wedge AB = AC \rightarrow \triangle BAC = \triangle CAB$$
$$BC = CB \wedge \angle C = \angle B \wedge \angle B = \angle C \rightarrow \triangle BAC = \triangle CAB$$
$$BC = CB \wedge AC = AB \wedge AB = AC \rightarrow \triangle BAC = \triangle CAB$$
$$\dots$$
- 証明は全ての可能性を試すような“探索”によって見つける.

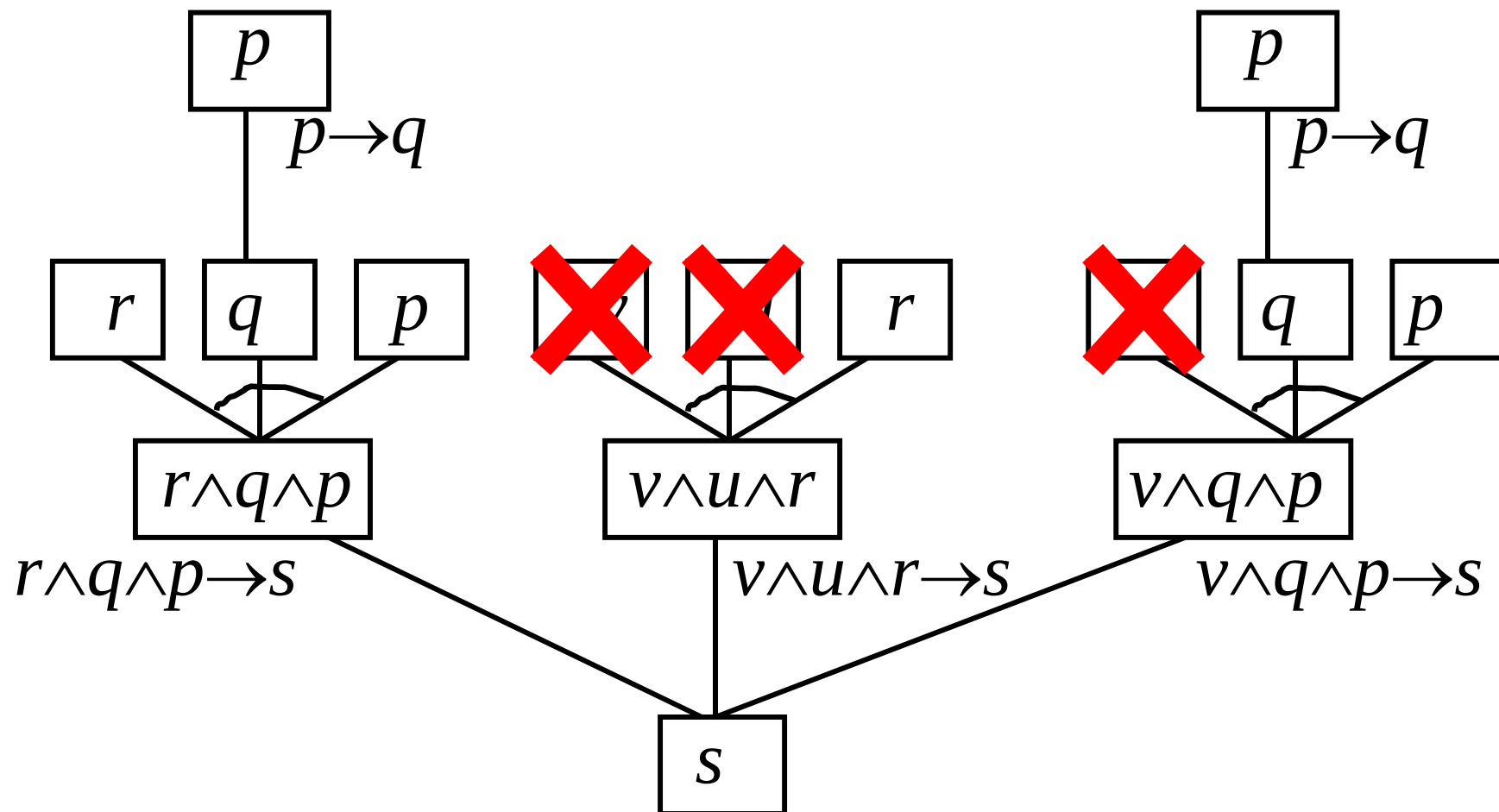
証明と探索(2)

■ AND-OR木



証明と探索(2)

■ AND-OR木





矛盾を導く証明(1)

$$\frac{\frac{p \quad p \rightarrow q}{q} \quad \frac{r \quad r \rightarrow \neg q}{\neg q}}{\perp}$$



矛盾を導く証明(2)

$$\frac{\frac{[p] \quad p \rightarrow q}{q} \quad \frac{r \quad r \rightarrow \neg q}{\neg q}}{\perp} \\ \hline \neg p$$



意味論: BOOLE代数



Boole代数(論理演算)

- 命題論理における論理式の“正しさ”の値の定式化
- 2種類の値 1, 0 (真偽値)だけを用いる空間
1 は 真, 0 は 偽 を表す.
- 真偽値間の演算は真理値表により定義
 - 真偽値の和, 積は, 代数的には体の構造を持つ
つまり, 自然数や実数の和, 積と非常に似た性質を持つ

論理演算

- 一般に, n 変数の論理演算は $2^{(2^n)}$ 種類しかない

→ 真理値表で表現

x	$f(x)$
0	
1	

x	y	$f(x, y)$
0	0	
0	1	
1	0	
1	1	



代表的な論理演算

論理積

x	y	xy
0	0	0
0	1	0
1	0	0
1	1	1

論理和

x	y	$x + y$
0	0	0
0	1	1
1	0	1
1	1	1

否定

x	$\overline{y}$
0	1
1	0



単項(1引数)論理演算

- 単項(1引数)論理演算は 2^2 種類

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	0	1	1
1	0	1	0	1



否定 $\bar{x}$

2項(2引数)論理演算

■ 2項(2引数)論理演算は 2^4 種類

x	y	f_1															f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

論理積 $x y$

論理和 $x + y$

同値 $x \Leftrightarrow y$

含意 $x \Rightarrow y$



否定, 論理和, 論理積の性質

交換律 $x + y = y + x$

$$x y = y x$$

結合律 $(x + y) + z = x + (y + z)$

$$(x y) z = x (y z)$$

分配律 $(x + y) z = x z + y z$

$$x y + z = (x + z)(y + z)$$

冪等律 $x + x = x$

$$x x = x$$

零元 $x + 0 = x$

$$x \cdot 0 = 0$$

単位元 $x \cdot 1 = x$

$$x + 1 = 1$$

補元 $x + \bar{x} = 1$

$$x \bar{x} = 0$$

$$\bar{\bar{1}} = 0, \quad \bar{\bar{0}} = 1$$

二重否定 $\bar{\bar{x}} = x$

ド・モルガン律 $\overline{x + y} = \bar{x} \bar{y}, \quad \overline{x y} = \bar{x} + \bar{y}$



含意, 同値

x	y	$x \Rightarrow y$
0	0	1
0	1	1
1	0	0
1	1	1

x	y	$\bar{x}$	$\bar{x} + y$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

x	y	$x \Leftrightarrow y$
0	0	1
0	1	0
1	0	0
1	1	1

x	y	$x \Rightarrow y$	$y \Rightarrow x$	$(x \Rightarrow y) (y \Rightarrow x)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1



論理式の解釈(1)

- 解釈 I : 命題記号全体の集合 Π から $\{0, 1\}$ への関数
 - 命題記号に真偽値を“割り当てる”
 - $\{0, 1\}^n$ 内の1点
- 解釈 I のもとでの論理式の解釈

1. 論理定数の解釈値

$$I(\Box) = 0, I(\blacksquare) = 1$$

2. 論理演算子

$$I(\varphi \wedge \zeta) = I(\varphi) \cdot I(\zeta)$$

$$I(\varphi \vee \zeta) = I(\varphi) + I(\zeta)$$

$$I(\varphi \rightarrow \zeta) = I(\varphi) \Rightarrow I(\zeta)$$

$$I(\neg \varphi) = \overline{I(\varphi)}$$



論理式の解釈(2)

例 解釈 I :

$$I(r) = 1, I(s) = 0, I(t) = 0, I(u) = 1, I(v) = 1$$

$$I(((r \wedge s) \wedge (t \wedge u)) \rightarrow v)$$

$$= I((r \wedge s) \wedge (t \wedge u)) \Rightarrow I(v)$$

$$= (I(r \wedge s) \cdot I(t \wedge u)) \Rightarrow I(v)$$

$$= ((I(r) \cdot I(s)) \cdot (I(t) \cdot I(u))) \Rightarrow I(v)$$

$$= ((1 \cdot 0) \cdot (0 \cdot 1)) \Rightarrow 1$$

$$= (0 \cdot 0) \Rightarrow 1$$

$$= 0 \Rightarrow 1 = 1$$



論理的帰結

- ζ が $\varphi_1, \dots, \varphi_n$ の論理的帰結:

$I(\varphi_1) = \dots = I(\varphi_n) = 1$ であるどのような解釈 I に対しても $I(\zeta) = 1$

$$\varphi_1, \dots, \varphi_n \models \zeta$$

例 $\varphi_1 = r, \varphi_2 = t, \varphi_3 = (s \wedge u)$

$$\varphi_4 = ((r \wedge s) \wedge (t \wedge u)) \rightarrow v$$

$$\zeta = v$$

The Logic Piano[Jevons 1869]

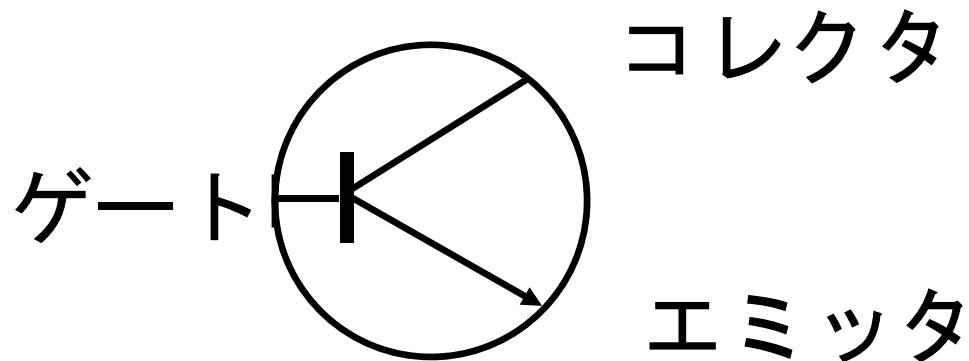




論理回路による実現

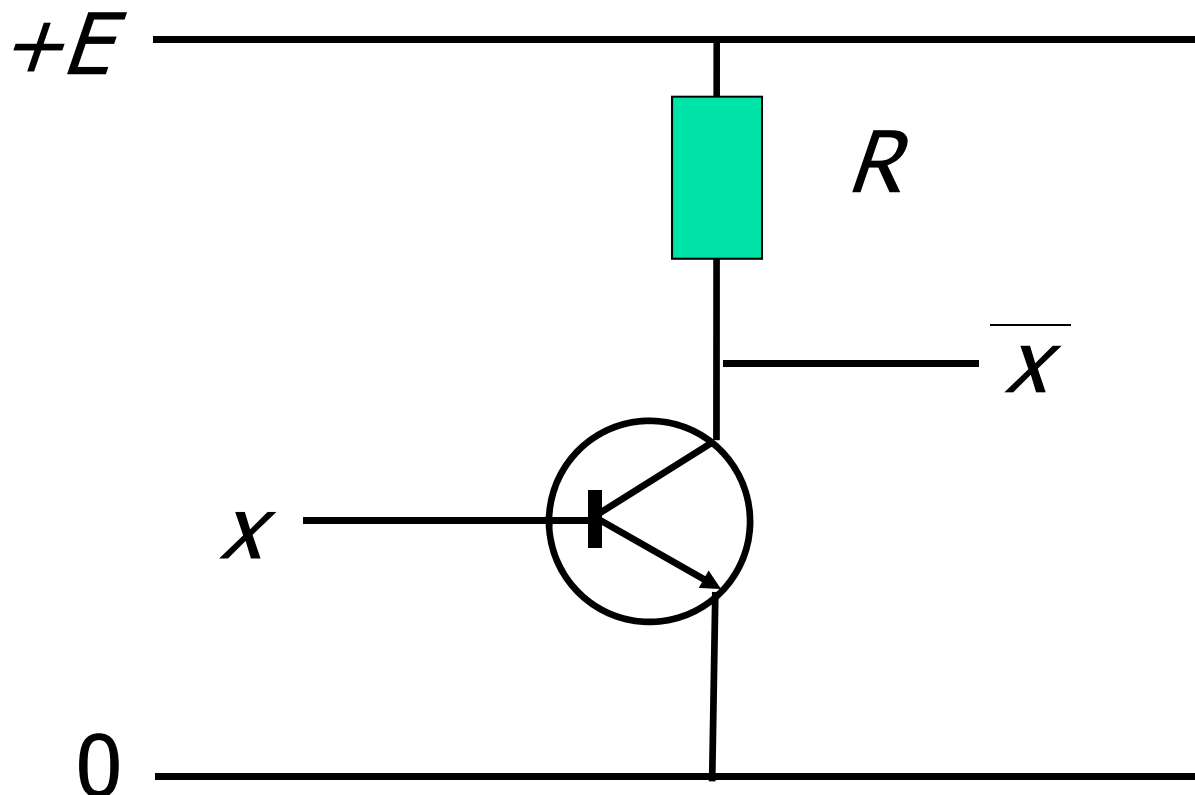
NPNトランジスタ

- ゲートに(エミッタに対して)正の電圧がかけられるときに限り
コレクタからエミッタ方向への抵抗が0になる

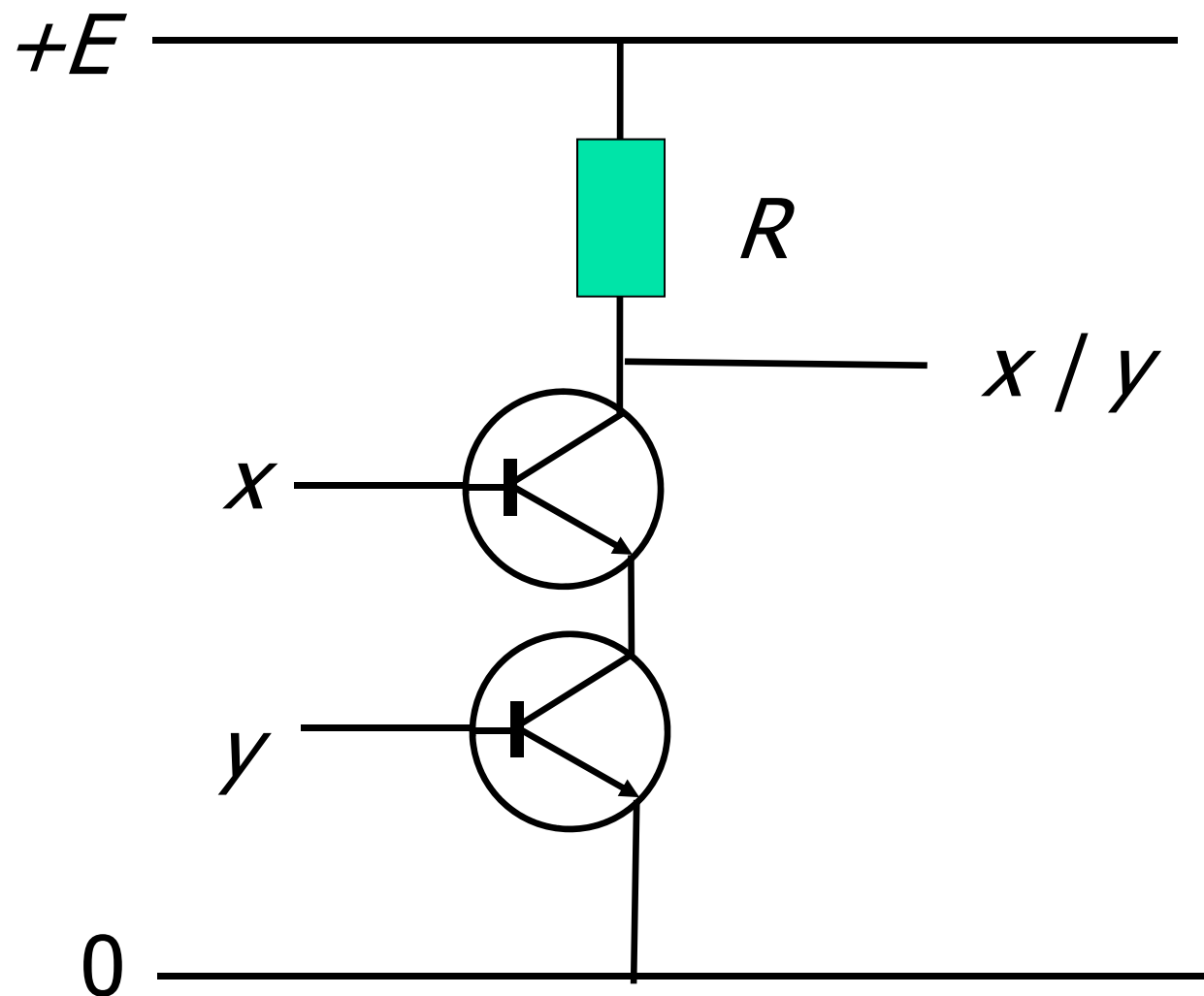


NOT回路

- x の電位が $+E$ (1と解釈) $\rightarrow y$ の電位は0
- x の電位が0 (0と解釈) $\rightarrow y$ の電位は $+E$



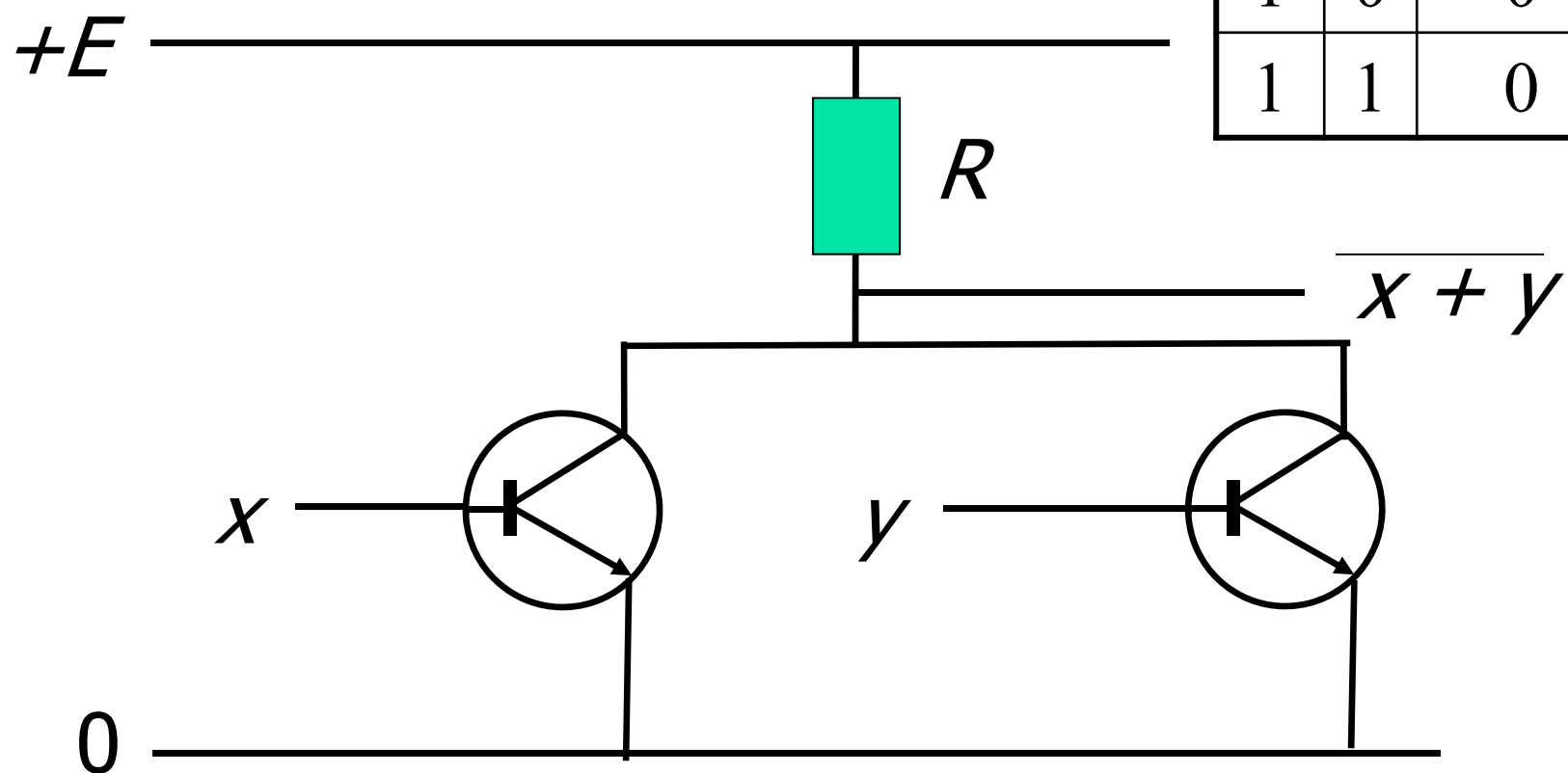
NAND回路



x	y	$x \mid y$
0	0	1
0	1	1
1	0	1
1	1	0

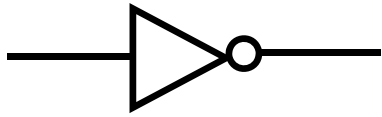
NOR回路

x	y	$\overline{x + y}$
0	0	1
0	1	0
1	0	0
1	1	0

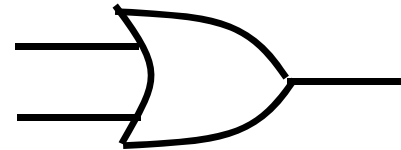


代表的演算

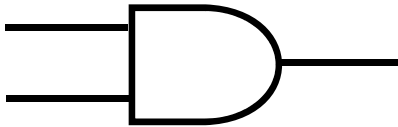
■ NOT



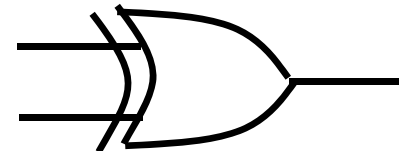
OR



■ AND

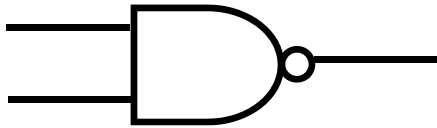


EOR

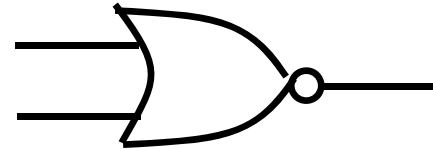


否定との組合せ

- NAND

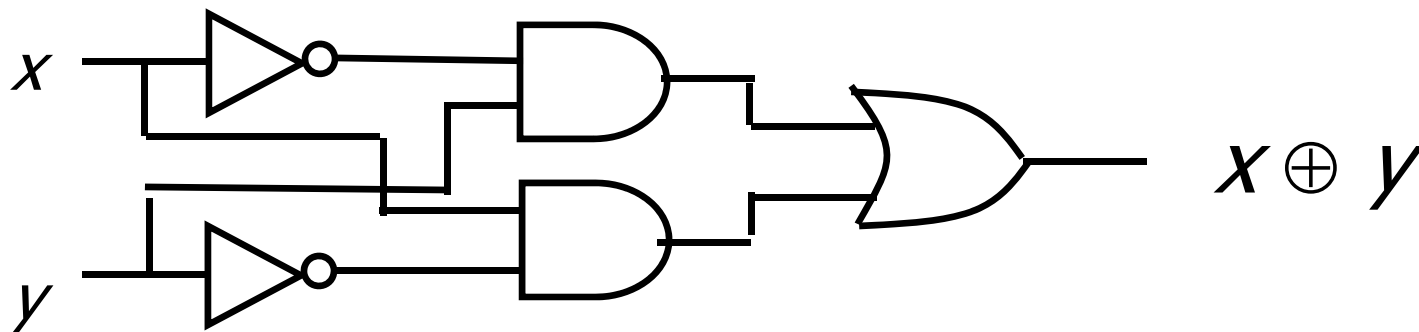
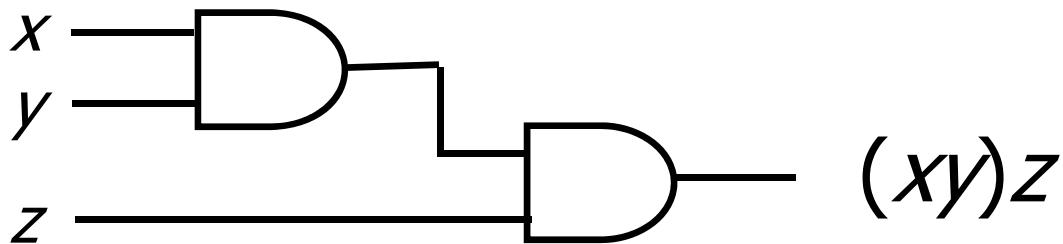


NOR

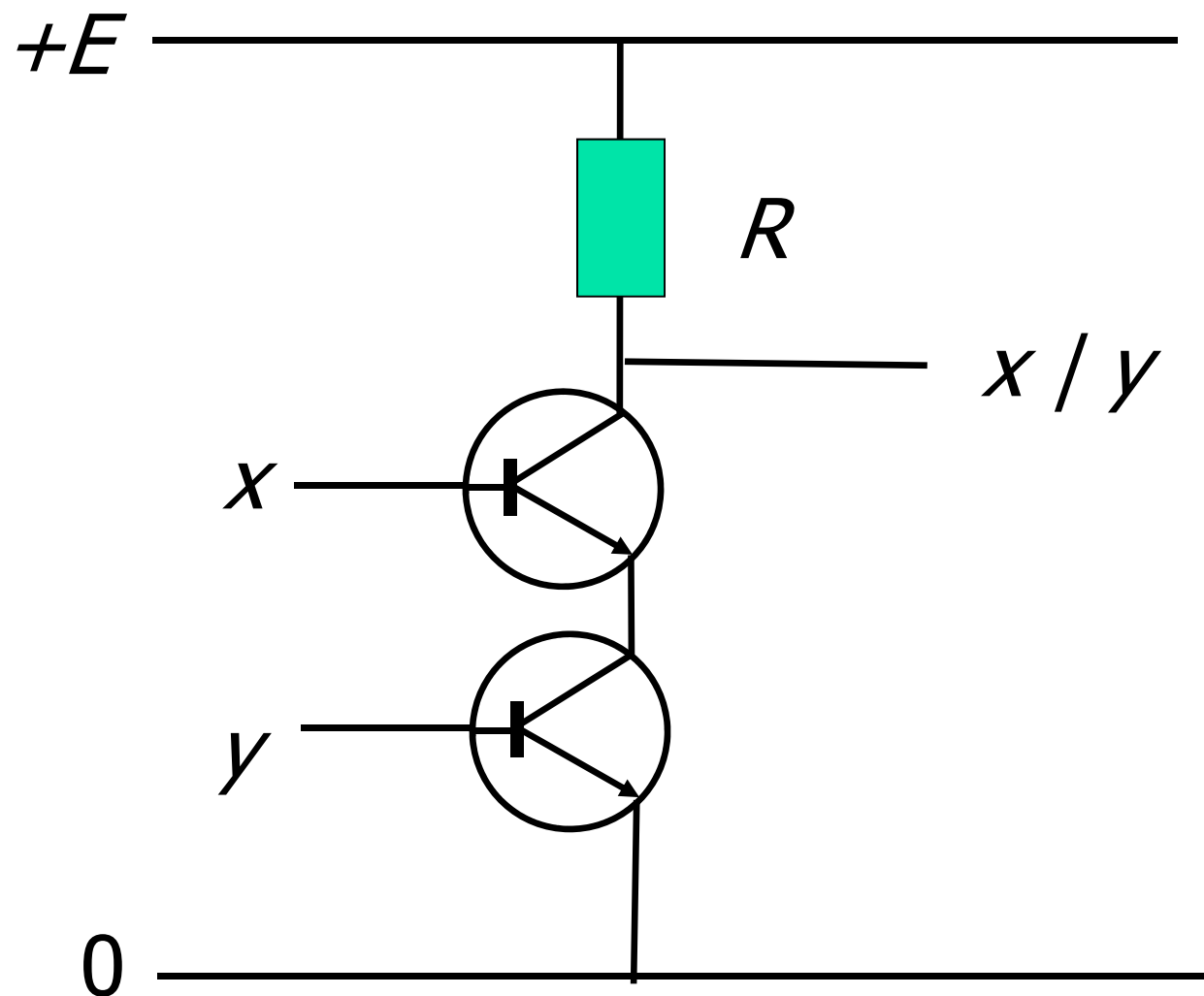


組合せ論理回路

- 0, 1(電圧高低)の伝播を表現した回路



NAND回路



x	y	x / y
0	0	1
0	1	1
1	0	1
1	1	0

NAND演算の性質

x	y	$x y$
0	0	1
0	1	1
1	0	1
1	1	0

- $x | x = \bar{x}$
- $x y = \overline{x | y}$
 $= (x | y) | (x | y)$
- $x + y = \overline{x | y}$
 $= (x | x) | (y | y)$
- 全てのブール関数は
NAND 演算の組合せで
表すことができる.



2進法の加法

- 1桁の整数同士の加法

→ 結果を2桁に揃えておく

$$0 + 0 = 00 \quad 0 + 1 = 01$$

$$1 + 0 = 01 \quad 1 + 1 = 10$$

- n桁の整数同士の加法

$$\begin{array}{r} 111 \\ 1101 \\ + 1011 \\ \hline 11000 \end{array}$$

← 繰上がり

1桁加法の真理値表

- 2進法で1桁の整数同士の加法

数としての加法

x	y	
0	0	00
0	1	01
1	0	01
1	1	10



2の位

x	y	u
0	0	0
0	1	0
1	0	0
1	1	1

1の位

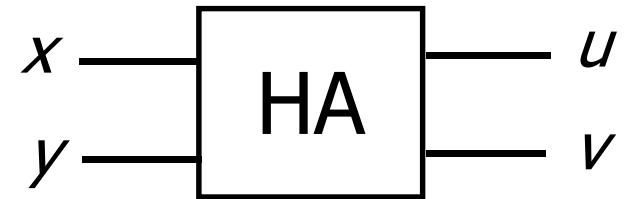
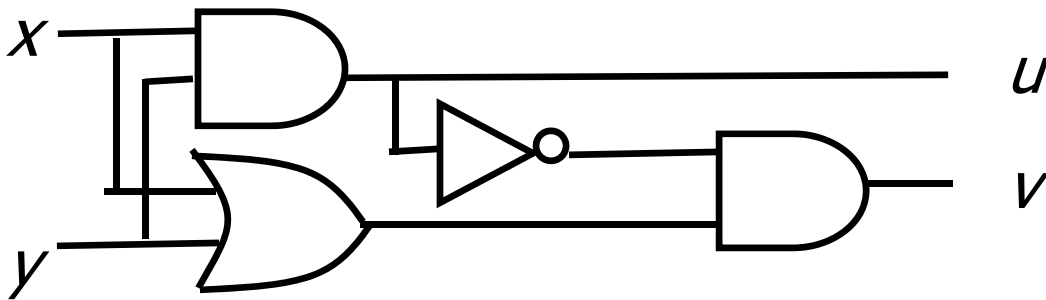
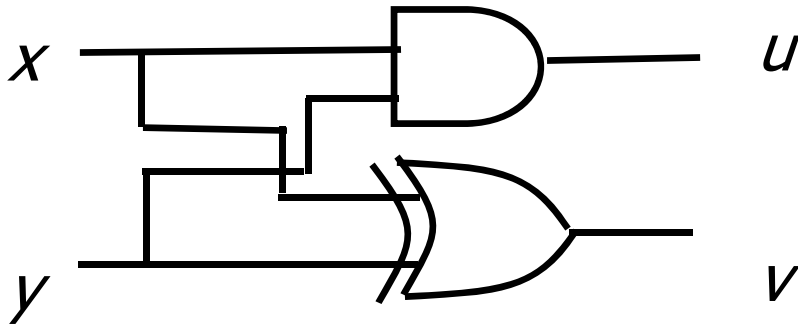
x	y	v
0	0	0
0	1	1
1	0	1
1	1	0

ブール演算とみれば

$$u = x y$$

$$v = x \oplus y$$

半加算器(Half Adder)





繰上りを扱う加法の真理値表

■ c : 下の桁からの繰上り

c	x	y	数としての和
0	0	0	00
0	0	1	01
0	1	0	01
0	1	1	10
1	0	0	01
1	0	1	10
1	1	0	10
1	1	1	11



繰上りを扱う加法の真理値表

■ c : 下の桁からの繰上り

c	x	y	u 和の2の位	v 和の1の位
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

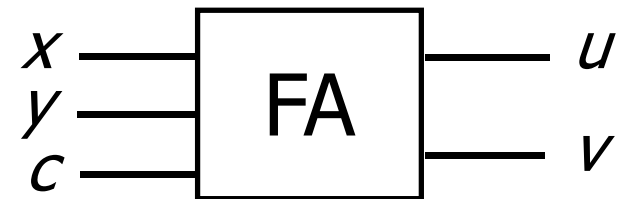
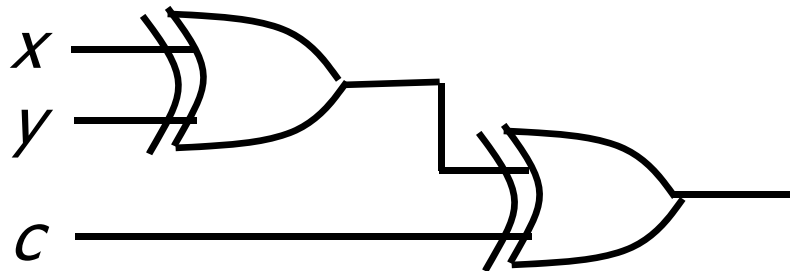
全加算器(Full Adder)

- 2の位 : 多数決関数

$$u = xy + yc + cx$$

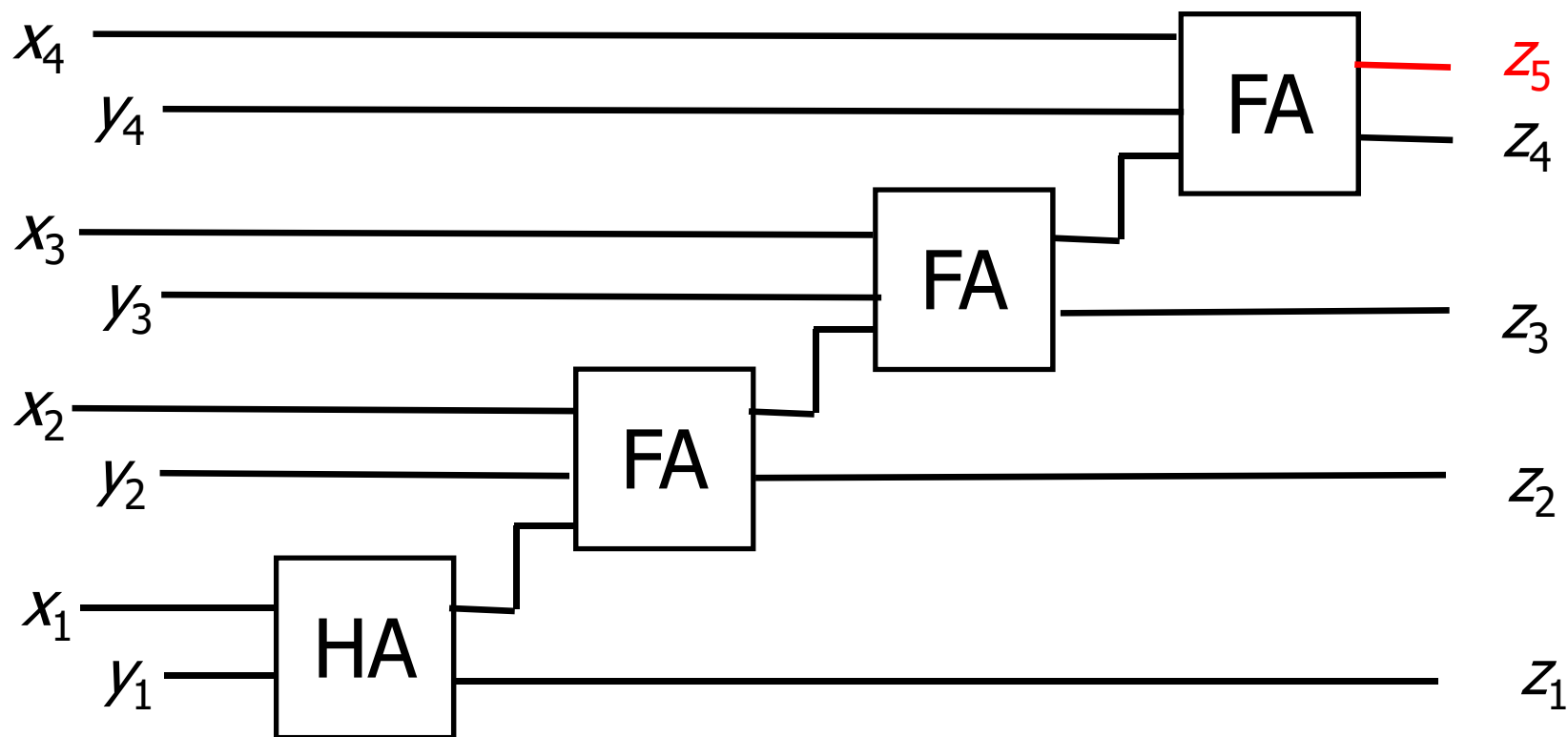
- 1の位 : 3入力EOR

$$v = c \oplus x \oplus y$$



n 桁同士の2進加算

$$x_n x_{n-1} \dots x_2 x_1 + y_n y_{n-1} \dots y_2 y_1 = z_{n+1} z_n z_{n-1} \dots z_2 z_1$$





完全性定理

- ζ が $\varphi_1, \dots, \varphi_n$ の論理的帰結である

$\Leftrightarrow$

$\varphi_1, \dots, \varphi_n$ を前提とし, ζ を結論とする証明図を構成することができる



命題論理から述語論理へ



一般性を持つ命題(1)

これまでの証明で用いた公理は一般性をもつ

- 等号の対称性: $AB=AC \rightarrow AC=AB$
- 角の対称性: $\angle BAC=\angle CAB$
- 合同: $(AB=EF \wedge AC=EG \wedge \angle BAC=\angle FEG) \rightarrow$
 $\Delta ABC=\Delta EFG$
- 合同な三角形の角が等しい:
 $\Delta BAC \equiv \Delta CAB \rightarrow \angle ABC=\angle ACB$



一般性を持つ命題(2)

これまでの証明で用いた公理は一般性をもつ

- 等号の対称性: $x y = z u \rightarrow z u = x y$
- 角の対称性: $\angle x y z = \angle z y x$
- 合同: $(x y = u v \wedge x z = u w \wedge \angle y x z = \angle v u w) \rightarrow$
 $\Delta x y z = \Delta u v w$
- 合同な三角形の角が等しい:
 $\Delta y x z = \Delta v u w \rightarrow \angle x y z = \angle u v w$



一般性を持つ命題(2)

これまでの証明で用いた公理は一般性をもつ

- 等号の対称性: $\forall x \forall y \forall z \forall u. xy = zu \rightarrow zu = xy$
- 角の対称性: $\forall x \forall y \forall z. \angle x y z = \angle z y x$
- 合同: $\forall x \forall y \forall z \forall u \forall v \forall w.$

$$(xy = uv \wedge xz = uw \wedge \angle yxz = \angle vuw) \rightarrow \\ \Delta xyz = \Delta uvw$$

- 合同な三角形の角が等しい:

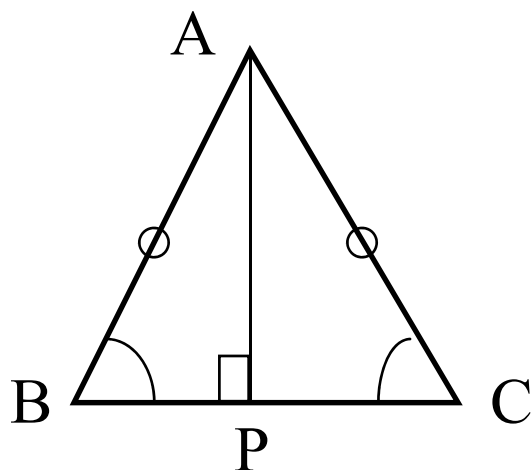
$$\forall x \forall y \forall z \forall u \forall v \forall w. \Delta yxz = \Delta vuw \rightarrow \angle xyz = \angle uvw$$

記号論理(1)

- 記号論理：(数学的)推論の定式化

例 三角形ABCが二等辺ならば底角は等しい

$$\angle B = \angle C \leftarrow AB = AC$$





記号論理(2)

- 命題論理

命題文の内部構造に言及しない

- 述語論理

命題文の主述関係を扱う

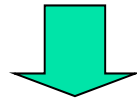
全称と存在を扱う

$$\boxed{\angle B = \angle C} \leftarrow \boxed{A B = A C}$$

命題論理

- 命題を文単位で形式化記号化

$$\boxed{\Delta x y z \equiv \Delta u v w} \leftarrow \boxed{x y = u v} \wedge \boxed{x z = u w} \\ \wedge \boxed{\angle z = 90} \wedge \boxed{\angle w = 90}$$



$$p \leftarrow q \wedge r \wedge s \wedge t$$

- 命題の正しさを真偽値 (0, 1) でモデル化 (古典論理) すると電気回路に応用可能

述語論理

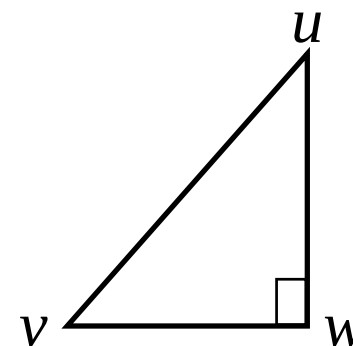
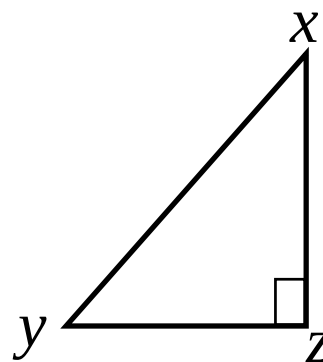
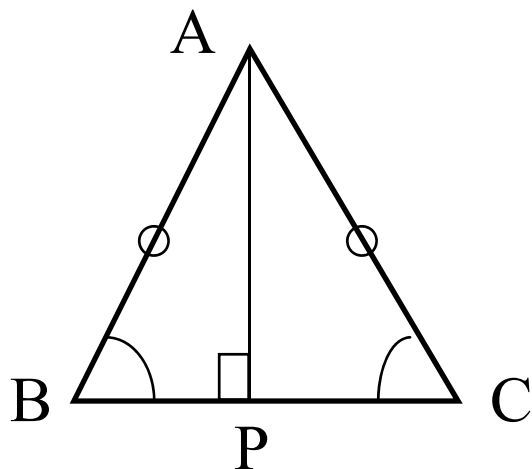
- 命題内の対象と述語に注目して形式化・記号化

$$\angle B = \angle C \leftarrow AB = AC$$

$$\forall x \forall y \forall z \forall u \forall v \forall w ($$

$$\triangle xyz \equiv \triangle uvw \leftarrow xy = uv \wedge xz = uw$$

$$\wedge \angle z = 90 \wedge \angle w = 90)$$





全称記号に対する推論規則

$$\frac{\forall x_1 \forall x_2 \dots \forall x_n. \varphi}{\varphi [x_1 = t_1, x_2 = t_2, \dots, x_n = t_n]} \quad t_i \text{ は具体的な対象}$$

例

$$\frac{\forall x \forall y \forall z \forall u. xy = zu \rightarrow zu = xy}{AB = AC \rightarrow AC = AB}$$

$$\frac{\forall x \forall y \forall z. \angle x y z = \angle z y x}{\angle BAC = \angle CAB}$$



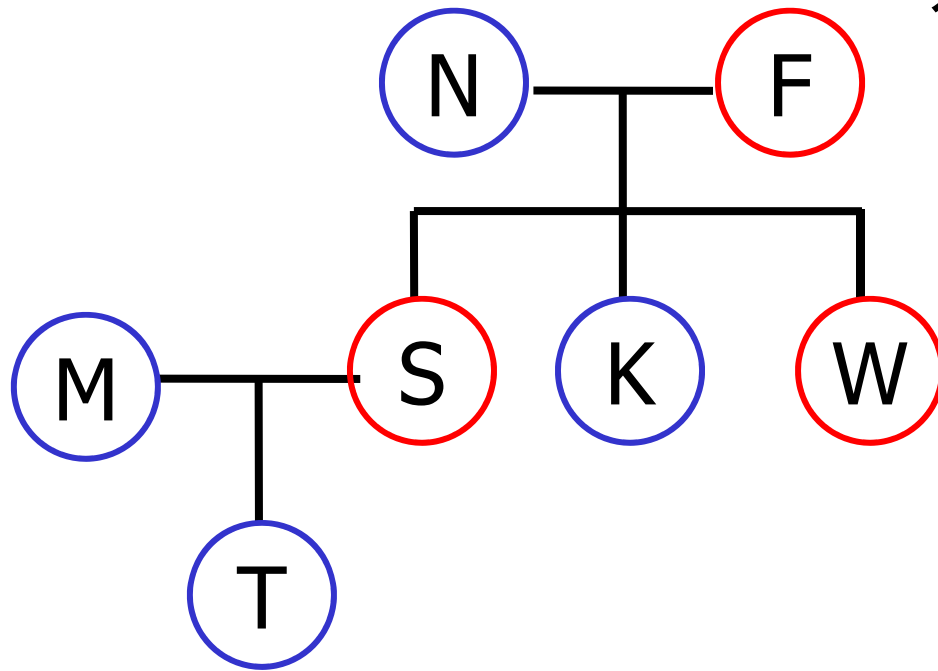
注意

- 命題の一般性の構造は，命題が表現する内容に依存する.

例 $\forall x \forall y \forall z. \angle x y z = \angle z y x$
 $\forall x \forall y. x z = z x$

- 数理論理学では
命題論理: 一般性を扱わない
述語論理: 一般性を扱う

数学以外の例



親子関係を表す記号を導入

$x >_f y$: x は y の父親

$x >_m y$: x は y の母親

$x >_p y$: x は y の親

$x >_{gf} y$: x は y の祖父

$x >_{gm} y$: x は y の祖母

$\text{male}(x)$: x は男性

$\text{female}(x)$: x は女性



親子関係の“公理”

$$\forall x \forall y. x >_p y \wedge \text{male}(x) \rightarrow x >_f y$$

$$\forall x \forall y. x >_p y \wedge \text{female}(x) \rightarrow x >_m y$$

$$\forall x \forall y \forall z. x >_f y \wedge y >_p z \rightarrow x >_{gf} z$$

$$\forall x \forall y \forall z. x >_m y \wedge y >_p z \rightarrow x >_{gm} z$$

$$N >_p S$$

$$F >_p S$$

$$S >_p T$$

$$M >_p T$$

$$\text{male}(N)$$

$$\text{female}(F)$$



親子関係の“証明”

$$\begin{array}{c}
 \frac{N >_p S \quad \text{male}(N)}{\quad} \\
 \frac{N >_p S \wedge \text{male}(N) \rightarrow N >_f S \quad N >_p S \wedge \text{male}(N)}{\quad} \\
 \frac{N >_f S \quad S >_p T}{\quad} \\
 \frac{N >_f S \wedge S >_p T \rightarrow N >_{gf} T \quad N >_f S \wedge S >_p T}{\quad} \\
 N >_{gf} T
 \end{array}$$



親子関係の“証明”(2)

$$\frac{N >_f S \wedge S >_p T \rightarrow N >_{gf} T \qquad N >_f S \wedge S >_p T}{N >_{gf} T}$$



親子関係の“証明”(3)

$$x >_f y \wedge y >_p z \rightarrow x >_{gf} z$$

$$N >_{gf} T$$



親子関係の“証明”(4)

$$\frac{N >_f y \wedge y >_p T \rightarrow N >_{gf} T \quad N >_f y \wedge y >_p T}{N >_{gf} T}$$



親子関係の“証明”(5)

$$\frac{\frac{N >_f S \quad S >_p T}{N >_f S \wedge S >_p T} \rightarrow N >_{gf} T \quad N >_f S \wedge S >_p T}{N >_{gf} T}$$

親子関係の“証明”(6)

$$\begin{array}{c}
 \frac{N >_p S \quad \text{male}(N)}{N >_p S \wedge \text{male}(N)} \\
 \frac{N >_p S \wedge \text{male}(N) \rightarrow N >_f S \quad N >_p S \wedge \text{male}(N)}{N >_f S} \\
 \frac{N >_f S \quad S >_p T}{N >_f S \wedge S >_p T} \\
 \frac{N >_f S \wedge S >_p T \rightarrow N >_{gf} T \quad N >_f S \wedge S >_p T}{N >_{gf} T}
 \end{array}$$

親子関係の“証明”(7)

$$\begin{array}{c}
 \frac{N >_p S \quad \text{male}(N)}{N >_p S \wedge \text{male}(N)} \\
 \frac{N >_p S \wedge \text{male}(N) \rightarrow N >_f S \quad N >_p S \wedge \text{male}(N)}{N >_f S} \\
 \frac{N >_f S \quad S >_p T}{N >_f S \wedge S >_p T} \\
 \frac{N >_f S \wedge S >_p T \rightarrow N >_{gf} T \quad N >_f S \wedge S >_p T}{N >_{gf} T}
 \end{array}$$



数学における記法(習慣)の排除

$$\angle B = \angle C \quad AB = AC \quad \triangle xyz \equiv \triangle uvw$$

- 表記されない記号を明示する

- 前置き記法(prefix notation)で表す

$$= (\angle(B), \angle(C)) \quad = (d(A, B), d(A, C))$$

$$\equiv (\triangle(x, y, z), \triangle(u, v, w))$$

- (この講義では)アルファベット・数字などのISO文字の列を用いることにする

$$= (agl(B), agl(C)) \quad = (d(A, B), d(A, C))$$

$$\text{equiv}(\text{tri}(x, y, z), \text{tri}(u, v, w))$$



対象と関数による表現

命題の主語や目的語などに用いられる対象の表現方法

- “対象”自身に名前を付ける

例 $A, B, C, \dots$

- 対象に“関数”を適用する

例 $\text{agl}(A), \text{agl}(B), \dots$

(厳密には $\text{agl}(A, B, C), \dots$)

$d(A, B), d(A, C), \dots$

$\text{tri}(A, B, C), \dots$

命題の主述の記号化(1)

- 用意する記号(幾何の場合)

対象を表す記号(対象(定数)記号): $A, B, \dots$

関数を表す記号(関数記号): $agl, d, tri, \dots$

対象の属性や対象間の

関係を表す記号(述語記号): $equiv, =, \dots$

- 対象の表現: 基礎項(ground term)

$A, agl(A), d(A, C), tri(A, B, C), \dots$

- 対象間の関係の表現: 基礎原子論理式(ground atomic formula, ground atom)

$= (agl(B), agl(C)), = (d(A, B), d(A, C)), \dots$

$equiv (tri(A, B, C), tri(u, v, w)), \dots$



命題論理の論理式

- 命題定数: $\perp$ ($\square$), $\top$ ($\blacksquare$)
- 命題変数: $p, q, r, \dots$
- 論理演算子: $\neg$ (でない), $\wedge$ (かつ), $\vee$ (または),
 $\rightarrow$ (ならば), $\leftrightarrow$ (同値),
 - この講義では $\rightarrow$ よりも $\leftarrow$ を使うことが多い

以上の構成要素を用いて, 数式と同じ要領で式を構成する. (括弧は適宜省略)

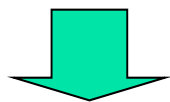
例

$$\neg p \vee q$$
$$((r \wedge s) \wedge (t \wedge u)) \rightarrow v$$



命題論理式と意味

- 論理式は，命題を記号化したもの
- 命題論理では，命題中の個々の文の構造までは考慮しない



- 文はそれがどのような内容を表していようと
“正しい”か“正しくないか”のいずれかである
- 命題の正しさは，命題中の個々の文の正しさと，
接続詞の使い方決まる。

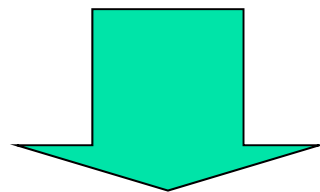
一般性を表す命題の記号化(1)

- 一般に成立する命題

幾何において“一般に $AB = BA$ が成立する”
という場合, 特定の点 A, B を指していない

$$\begin{aligned} &= (d(A, B), d(B, A)) \wedge = (d(A, C), d(C, A)) \wedge \dots \\ &\wedge = (d(B, A), d(A, B)) \wedge \dots \end{aligned}$$

- 数式の Π に相当



- “任意の点 x, y に対して $xy = yx$ が成立する”

$$\forall x \forall y (= (d(x, y), d(y, x)))$$



命題の主述の記号化(2)

$$\forall x \forall y \forall z \forall u \forall v \forall w (\\ = (\text{agl}(x), \text{agl}(u)) \leftarrow \\ \text{equiv}(\text{tri}(x, y, z), \text{tri}(u, v, w)))$$

$$0, s(0), s(s(0)), +(s(0), s(s(0))), \dots$$

- 対象間の関係の表現: 基礎原子論理式 (ground atomic formula, ground atom)

$$\text{even}(s(s(0))), =(+(s(0), s(s(0))), s(s(s(0))))), \dots$$



一般性を表す命題の記号化(3)

- $\forall x \forall y (= (+ (x, y), + (y, x)))$
- $\forall x (= (+ (0, x), x))$
- $\forall x (= (+ (x, s(0)), s(x)))$
- $\forall x \forall y (= (+ (x, s(y)), s(+ (x, y))))$
- $\forall x \forall y \forall z (= (+ (s(x), y), s(z)) \leftarrow (+ (x, y), z))$
- $\forall x (\text{even}(s(s(x))) \leftarrow \text{even}(x)) \wedge \text{even}(0))$

述語論理の論理式と意味(2)

$$\forall x \forall y \forall z \forall u \forall v \forall w (\\ \triangle x y z \equiv \triangle u v w \leftarrow x y = u v \wedge x z = u w \\ \wedge \angle z = 90 \wedge \angle w = 90)$$

$$\forall x \forall y \forall z \forall u \forall v \forall w (\\ \text{equiv}(\text{tri}(x, y, z), \text{tri}(u, v, w))) \leftarrow \\ = (d(x, y), d(u, v)) \wedge = (d(x, z), d(u, w)) \\ \wedge = (\text{agl}(z), 90) \wedge = (\text{agl}(w), 90))$$

$$\forall x (\text{even}(s(s(x))) \leftarrow \text{even}(x)) \wedge \text{even}(0))$$



基礎原子論理式(1)

- 基礎項 t や基礎項の組 $(t_1, t_2, \dots, t_n)$ が S に属していることを表すための式 : $p(t), q(t_1, t_2, \dots, t_n)$

基礎原子論理式(ground atomic formula)

p, q : 述語記号

例 $S_{\text{even}} = \{ t \mid t \text{ は偶数を表す項} \}$

even : 述語記号

$\text{even}(0) \in S_{\text{even}}, \quad \text{even}(s(s(0))) \in S_{\text{even}},$

$\text{even}(s(0)) \notin S_{\text{even}}, \quad \text{even}(s(s(s(0)))) \notin S_{\text{even}},$

...



基礎原子論理式(2)

例 $S_{\text{mod}} = \{ (t, s, u) \mid t \text{ (が表す自然数)を} s \text{ で割ったときの余りが } u \}$

mod : 述語記号

$\text{mod}(0, s(s(0)), 0) \in S_{\text{mod}},$

$\text{mod}(s(0), s(s(0)), s(0)) \in S_{\text{mod}},$

$\text{mod}(s(s(s(0))), s(s(s(0))), 0) \in S_{\text{mod}},$

$\text{mod}(s(0), s(s(0)), 0) \notin S_{\text{mod}}, \quad \dots$

- 基礎原子論理式全体の集合をHerbrand baseとよぶ.



量子子のない論理式(1)

- 基礎原子論理式から論理結合子

$\neg$ $\wedge$ $\vee$ $\rightarrow$ $\leftarrow$ $\leftrightarrow$

を用いて構成される式

$\neg \text{even}(s(0))$

$\text{even}(s(s(0))) \leftrightarrow \text{mod}(s(s(0)), s(s(0)), 0)$

$\text{even}(s(s(0))) \vee \neg \text{even}(0)$

$\text{even}(s(s(s(s(0))))) \leftarrow \text{even}(s(s(0)))$

- Cf. $(-4) \times (6+5)$



量子子のない論理式(2)

- 項は以下のように再帰的に定義される:

(1) 論理定数 $\Box(\perp)$, $\blacksquare(T)$ は論理式である.

(2) 基礎原子論理式は論理式である.

(3) φ, ζ を論理式とするとき

$$\neg \varphi$$

$$\varphi \wedge \zeta \quad \varphi \vee \zeta \quad \varphi \rightarrow \zeta \quad \varphi \leftarrow \zeta \quad \varphi \leftrightarrow \zeta$$

(4) (1), (2) を有限回適用して得られる式だけが論理式である.



述語論理の論理式

- 命題定数: $\perp$ (□), $\top$ (■)
 - 原子論理式: 定数(対象)記号: $0, A, B, \dots$
関数記号: $s, d, \dots$
述語記号: $even, mod, \dots$
変数(対象変数): $x, y, z, \dots$
 - 論理演算子: $\neg$ (でない), $\wedge$ (かつ), $\vee$ (または),
 $\rightarrow$ (ならば), $\leftrightarrow$ (同値)
量化子: $\forall$ (全ての), $\exists$ (ある)
- 以上の構成要素を用いて, 数式と同じ要領で式を構成する. (括弧は適宜省略)

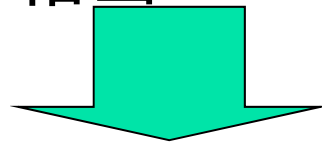
一般性を表す命題の記号化(1)

- 一般に成立する命題

“一般に 自然数 x は 0 以上である”
という場合, 特定の数 $0, 1, 2, \dots$ を指していない

$$\text{geq}(0, 0) \wedge \text{geq}(s(0), 0) \wedge \text{geq}(s(s(0)), 0) \wedge \text{geq}(s(s(s(0))), 0) \wedge \dots$$

- 数式の $\Pi_{n=1}^{\infty}$ に相当



- “任意の数 x に対して 0 に x を加えた結果は x である”

$$\forall x \text{geq}(x, 0)$$



一般性を表す命題の記号化(2)

例

$$\forall x \text{ geq } (x, 0)$$

$$\forall x \forall y (\text{geq}(s(x), s(y)) \leftarrow \text{geq}(x, y))$$

$$\forall x (\text{even}(s(s(x))) \leftarrow \text{even}(x))$$

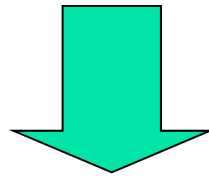
$$\forall x \text{ plus } (0, x, x)$$

$$\forall x \forall y \forall z \text{ plus } (y, x, z) \leftarrow \text{plus } (x, y, z)$$

$$\forall x \forall y \forall z \text{ plus}(s(x), y, s(z)) \leftarrow \text{plus}(x, y, z)$$

一般性の否定

- “任意の x に対して $\varphi[x]$ が成立する”
の否定は反例の存在.



“ $\varphi[x]$ が成立しない x が存在する”

- 直感的には $\vee$ が (一般には) 無限個連なった式
- 数式の $\Sigma_{n=1}^{\infty}$ に相当

例 $\exists x \exists y \text{ geq}(x, y)$
 $\exists x \text{ even}(s(s(x)))$
 $\forall x \forall y \exists z \text{ plus}(x, y, z)$

推論規則(2)

$$\frac{\varphi \quad \zeta}{\varphi \wedge \zeta}$$

$$\frac{\varphi \wedge \zeta}{\varphi} \quad \frac{\varphi \wedge \zeta}{\zeta}$$

$$\frac{\varphi}{\varphi \vee \zeta} \quad \frac{\zeta}{\varphi \vee \zeta}$$

$$\frac{\varphi \vee \zeta \quad \begin{array}{c} [\varphi] \quad [\zeta] \\ \dots \\ \theta \quad \theta \end{array}}{\theta}$$

$$\frac{\begin{array}{c} [\varphi] \\ \dots \\ \zeta \end{array}}{\varphi \rightarrow \zeta}$$

$$\frac{\varphi \quad \varphi \rightarrow \zeta}{\zeta}$$

推論規則(3)

$$\frac{\begin{array}{c} [\varphi] \\ \dots \\ \perp \end{array}}{\neg\varphi}$$

$$\frac{\varphi \quad \neg\varphi}{\perp}$$

$$\frac{\begin{array}{cc} [\varphi] & [\zeta] \\ \dots & \dots \\ \zeta & \varphi \end{array}}{\varphi \leftrightarrow \zeta}$$

$$\frac{\varphi \quad \varphi \leftrightarrow \zeta}{\zeta}$$

$$\frac{\zeta \quad \varphi \leftrightarrow \zeta}{\varphi}$$

$$\frac{\perp}{\varphi}$$

$$\varphi \vee \neg\varphi$$



推論規則(4)

$$\frac{\varphi[a]}{\forall x \varphi[x]}$$

a は変数で, $\varphi[a]$ の上
にある仮定に自由に出
現してはならない

$$\frac{\varphi[t]}{\exists x \varphi[x]}$$

t は項

$$\frac{\forall x \varphi[x]}{\varphi[t]}$$

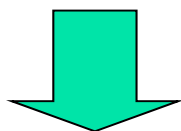
t は項

$$\frac{\begin{array}{c} [\varphi[a]] \\ \dots \\ \exists x \varphi[x] \end{array} \quad \theta}{\theta}$$

a は変数で, θ の上にある
仮定と θ に自由に出現して
はならない

述語論理の論理式と意味(1)

- 論理式は, 命題を記号化したもの
- 述語論理では, 命題中の主述を表現



- 論理式中で用いられる記号が何を表現しているかは, 表現する人が決める
- 命題の正しさは,
 - 命題中の個々の記号が何を表しているのか
 - 接続詞の使い方
 - 一般性の表現で決まる.



量化子のない論理式の解釈

- 解釈 I : Herbrand base B から $\{0, 1\}$ への関数
 - 基礎原子論理式に真偽値を“代入”する
 - $\{0, 1\}^n$ 内の1点
- 解釈 I のもとでの論理式の解釈

1. 命題定数の解釈値

$$I(\square) = 0, I(\blacksquare) = 1$$

2. 論理演算子

$$I(\varphi \wedge \zeta) = I(\varphi) \cdot I(\zeta)$$

$$I(\varphi \vee \zeta) = I(\varphi) + I(\zeta)$$

$$I(\varphi \rightarrow \zeta) = I(\varphi) \Rightarrow I(\zeta)$$

$$I(\neg \varphi) = \overline{I(\varphi)}$$

述語論理の論理式の解釈(1)

■ 基礎原子論式の解釈 I

D : 考察対象全体からなる集合(領域)

I_C : 対象(定数)記号を D 中の対象に写す写像

I_F : 関数記号を D^n から D への関数へ写す写像

I_P : 述語記号を D^n から $\{0,1\}$ への関数へ写す写像

例 $\text{geq}(s(s(0)), s(0))$

D : 自然数の集合 $\mathbb{N}$

$I_C(0)$: 自然数の 0

$I_F(s)$: 次の自然数

$I_P(\text{geq})$: 自然数の順序関係 $\geq$

述語論理の論理式の解釈(2)

- 命題定数, 論理演算子の解釈は量子化子の
ない場合と論理と同じ
- $I(\forall x(\varphi[x]))$:
 x に D 中の任意の対象 c を“代入”したときに,
 常に $I(\varphi[c]) = 1$ であれば $I(\forall x(\varphi[x])) = 1$
 そうでなければ $I(\forall x(\varphi[x])) = 0$
- $I(\exists x(\varphi[x]))$:
 D 中の対象 c で, x に c を“代入”したときに,
 $I(\varphi[c]) = 1$ なるものがあれば $I(\exists x(\varphi[x])) = 1$
 そうでなければ $I(\exists x(\varphi[x])) = 0$

述語論理の論理式の解釈(3)

例 $\forall x \text{ geq}(s(x), x)$
 $\forall x \forall y \text{ geq}(s(x), y)$

D : 自然数の集合 $\mathbb{N}$

$I_C(0)$: 自然数の 0

$I_F(s)$: 次の自然数

$I_P(\text{geq})$: 自然数の順序関係 $\geq$

- 任意の自然数 m を x に代入して $I(\text{geq}(m', m)) = 1$

$$I(\forall x \text{ geq}(s(x), x)) = 1$$

- 自然数 2, 4 を x, y に代入して $I(\text{geq}(3, 4)) = 0$

$$I(\forall x \forall y \text{ geq}(s(x), y)) = 0$$

述語論理の論理式の解釈(4)

- 記号の解釈は一般にいくつでも種類与えられる

例 $\forall x \text{ geq}(s(x), x)$

解釈1 D : 自然数の集合 N

$I_C(0)$: 自然数の 0

$I_F(s)$: 次の自然数

$I_P(\text{geq})$: 自然数の順序関係 $\geq$

解釈1' $I_P(\text{geq}) :=$

解釈2 D : 平面 π

$I_C(0)$: 原点

$I_F(s)$: 原点と対称点

$I_P(\text{geq})$: 一直線上にある

論理的帰結(1)

- ζ が $\varphi_1, \dots, \varphi_n$ の論理的帰結:

$I(\varphi_1) = \dots = I(\varphi_n) = 1$ であるどのような解釈 I に対しても $I(\zeta) = 1$

$$\varphi_1, \dots, \varphi_n \models \zeta$$

例

$$\forall x \text{ geq}(s(x), x) \models \text{geq}(s(s(0)), s(0))$$



形式的手法

- 形式的: 数学的な表現と分析
 - 形式言語, 形式的証明
- ソフトウェア工学における形式的手法:
ソフトウェア(プログラム)の性質を数学的な表現と分析によって明らかにする
数学的な表現方法としては数理論理の体系を用いる
 - 形式的仕様記述
 - プログラムの正しさの形式的証明



表現方法として用いる論理

- 一階述語論理：プログラムの実行前後に満たすべき条件を表現
 - Hoare論理
- 等号論理：データ構造の満たすべき条件を表現
 - OBJ
- 時相論理: 並行システムの動作が満たすべき条件を表現



Hoare論理(Floyd-Hoare論理)

- プログラムP

Pの実行前に仮定する条件 : A

Pの実行後に成立すべき条件 : B

$\{A\} P \{B\}$: “Aが成立しているとき, Pを実行して**停止すれば**, Bが成立している” (部分正当性)

$\langle A \rangle P \langle B \rangle$: “Aが成立しているとき, Pを実行すると**必ず停止して**, Bが成立している” (完全正当性)

- A, Bを表明(assertion), Aを前条件(precondition), Bを後条件(postcondition) AとBの組を仕様とよぶ



仕様の例(1)

- 表明は日本語と数学記法, プログラムはCの一部としておく.

$\{N \geq 1\}$

$i = 1;$

$f = 1;$

$\text{while}(i \leq N)$

$\{f = f * i;$

$i = i + 1;\}$

$\{f = N!\}$



仕様の例(2)

$\{x=a \text{ かつ } y=b\}$

$t = x;$

$x = y;$

$y = t;$

$\{x=b \text{ かつ } y=a\}$



数理論理学の応用: ソフトウェアの検証



Hoare論理の公理と推論規則(1)

- 厳密には表明は一階述語論理の論理式を用いる

- 代入文の公理

$$\{A[x:=e]\} \ x=e \ \{A\}$$

- 逐次実行

$$\frac{\{A\}P\{B\} \quad \{B\}Q\{C\}}{\{A\}P;Q\{C\}}$$

Hoare論理の公理と推論規則(2)

- 条件

$$\frac{\{A \wedge B\} P \{C\} \quad \{A \wedge \neg B\} Q \{C\}}{\{A\} \text{ if } B \text{ P else } Q \{C\}}$$

- whileループ

$$\frac{\{A \wedge B\} P \{A\}}{\{A\} \text{ while}(B) P \{A \wedge \neg B\}} \quad A: \text{ループ不変式}$$

- 帰結の規則

$$\frac{A \Rightarrow A' \quad \{A'\} P \{B'\} \quad B' \Rightarrow B}{\{A\} P \{B\}}$$

Hoare論理による証明(例1)

$$\begin{array}{c}
 \{y=b \wedge x=a\} \\
 x=a \wedge y=b \qquad t=x; \\
 \Rightarrow y=b \wedge x=a \qquad \{y=b \wedge t=a\} \\
 \hline
 \{x=a \wedge y=b\} \qquad \{y=b \wedge t=a\} \\
 t=x; \qquad x=y; \\
 \{y=b \wedge t=a\} \qquad \{x=b \wedge t=a\} \\
 \hline
 \{x=a \wedge y=b\} \qquad \{x=b \wedge t=a\} \\
 t=x; x=y; \qquad y=t; \\
 \{x=b \wedge t=a\} \qquad \{x=b \wedge y=a\} \\
 \hline
 \{x=a \wedge y=b\} \quad t=x; x=y; y=t; \{x=b \wedge y=a\}
 \end{array}$$

Hoare論理による証明(例2-1)

$$\{1 \leq i+1 \leq N+1 \wedge f * i = i!\}$$

$$1 \leq i+1 \leq N+1 \wedge f = (i-1)! \wedge i \leq N \qquad f = f * i;$$

$$\Rightarrow 1 \leq i+1 \leq N+1 \wedge f * i = i! \quad \{1 \leq i+1 \leq N+1 \wedge f = i!\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i \leq N\} \qquad \{1 \leq i+1 \leq N+1 \wedge f = i!\}$$

$$f = f * i; \qquad i = i + 1;$$

$$\{1 \leq i+1 \leq N+1 \wedge f = i!\} \qquad \{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i \leq N\}$$

$$f = f * i; i = i + 1;$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i > N \quad \text{while}(i \leq N) \{f = f * i; i = i + 1;\}$$

$$\Rightarrow f = N! \qquad \{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i > N\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\text{while}(i \leq N) \{f = f * i; i = i + 1;\}$$

$$\{f = N!\}$$



Hoare論理による証明の(例2-2)

$$\{1 \leq i \leq N+1 \wedge i = (i-1)!\}$$

$N \geq 0 \Rightarrow$

$i=1;$

$$1 \leq i \leq N+1 \wedge i = (i-1)!$$

$$\{1 \leq i \leq N+1 \wedge i = (i-1)!\}$$

$$\{N \geq 0\}$$

$i=1;$

$$\{1 \leq i \leq N+1 \wedge i = (i-1)!\}$$

$$\{1 \leq i \leq N+1 \wedge i = (i-1)!\}$$

$f=1;$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\{N \geq 0\}$$

$i=1; f=1;$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

(1-1)

$$\{N \geq 0\}$$

$i=1; f=1; \text{while}(i \leq N) \{f = f*i; i=i+1;\}$

$$\{f=N!\}$$



部分正当性と完全正当性

- 部分正当性では

$\{N \geq 1\}$

`while(1==1)`

`x=1;`

$\{f=N!\}$

- 部分正当性 + 停止性 = 完全正当性



停止性

- Halting Problemなので一般には非可解
- 整礎集合を用いる
 - 整礎集合:無限の減少列が存在しない半順序集合
例: 通常の大小関係での自然数全体は整礎集合
- whileループ

$$\frac{\langle A \wedge B \wedge \text{bound}=k \rangle P \langle B \wedge \text{bound} < k \rangle}{\langle A \rangle \text{while}(B) P \langle A \wedge \neg B \rangle}$$

Hoare論理による証明(例2-3)

$$\{1 \leq i+1 \leq N+1 \wedge f * i = i!\}$$

$$1 \leq i+1 \leq N+1 \wedge f = (i-1)! \wedge i \leq N \quad f = f * i;$$

$$\Rightarrow 1 \leq i+1 \leq N+1 \wedge f * i = i! \quad \{1 \leq i+1 \leq N+1 \wedge f = i!\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i \leq N\} \quad \{1 \leq i+1 \leq N+1 \wedge f = i! \}$$

$$f = f * i; \quad i = i + 1;$$

$$\{1 \leq i+1 \leq N+1 \wedge f = i!\} \quad \{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i \leq N \wedge \textcolor{red}{N-i = N-I}\}$$

$$f = f * i; i = i + 1;$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge \textcolor{red}{N-i = N-(I+1) < N-I}\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i > N \quad \text{while}(i \leq N) \{f = f * i; i = i + 1;\}$$

$$\Rightarrow f = N! \quad \{1 \leq i \leq N+1 \wedge f = (i-1)! \wedge i > N\}$$

$$\{1 \leq i \leq N+1 \wedge f = (i-1)!\}$$

$$\text{while}(i \leq N) \{f = f * i; i = i + 1;\}$$

$$\{f = N!\}$$



Hoare論理の位置付け(1)

- 表明は厳密には
- 一階述語論理を用いた形式的仕様記述方法を確立 → 表現言語として
- 一階述語論理の自動証明システムを用いれば、仕様の検証の部分的自動化も可能
→ 検証のメカニズムとして
- ループ普遍式を見つけることが困難
- 以後の研究は、表現言語か検証メカニズムのいずれかに焦点を当てる



形式的仕様記述言語

- 表明を記述するための形式言語

VDM [IBM Wien研究所]

Z [Oxford Programming research group]

B [Abrail 96]

- Hoare論理のような検証はあまり意識していない
- 表明を記述するために特化した一階述語論理の論理式の記法と考えられる
- 仕様を形式言語を用いて記述するので、仕様記述の誤りを防ぐ効果がある(実例もある)