ゴール：

鳩の巣原理の証明は
「長い」ものしかないという結果の紹介
(Haken, 1985)

定義（リテラル・節・CNF）

- 原子論理式 p またはその否定 $\neg p$ をリテラルと呼ぶ.
- リテラルの有限集合 $\{L_1, \dots, L_n\}$ を節と呼び論理式 $L_1 \vee L_2 \vee \cdots \vee L_n$ と同一視する.

特に0個のリテラルから成る節 $\{\}$ を $\perp$ で表す.

- 節の有限集合 $\{C_1, \dots, C_n\}$ をCNFと呼び論理式 $C_1 \wedge \cdots \wedge C_n$ と同一視する.

例：CNF $\{\{\neg p, r\}, \{p, q\}, \{r\}\}$ は論理式 $(\neg p \vee r) \wedge (p \vee q) \wedge r$ と対応.

命題：任意の古典命題論理の論理式に対し
それと論理的に等価なCNFが存在する.

例：・ $p \to q \equiv \neg p \lor q$

・ $(p \to q) \to p \equiv \neg(\neg p \lor q) \lor p$

$$\equiv (p \land \neg q) \lor p$$

$$\equiv (p \lor p) \land (\neg q \lor p)$$

$$\equiv p \land (\neg q \lor p)$$

定義（導出計算）Φ をCNFとする.

節 C の Φ からの長さ n の導出とは
節の列 $C_1, C_2, \cdots, C_n = C$ であり
各 $k \in \{1, \cdots, n\}$ について

- C_k は Φ に現れる節であるか、もしくは
- ある $i, j < k$ が存在して以下をみたすもの:

$$\begin{cases} C_i = \boxed{A} \lor \boxed{p} \lor \boxed{B} \\ C_j = \boxed{D} \lor \boxed{\lnot p} \lor \boxed{E} \end{cases} \quad C_k = \boxed{A} \lor \boxed{B} \lor \boxed{C} \lor \boxed{E}$$

とかける.

例:

CNF $(p \vee q) \wedge \neg p \wedge (\neg q \vee p)$ から

空節⊥の長さ6の導出:

① $p \vee q$

② $\neg p$

③ q (①と②から)

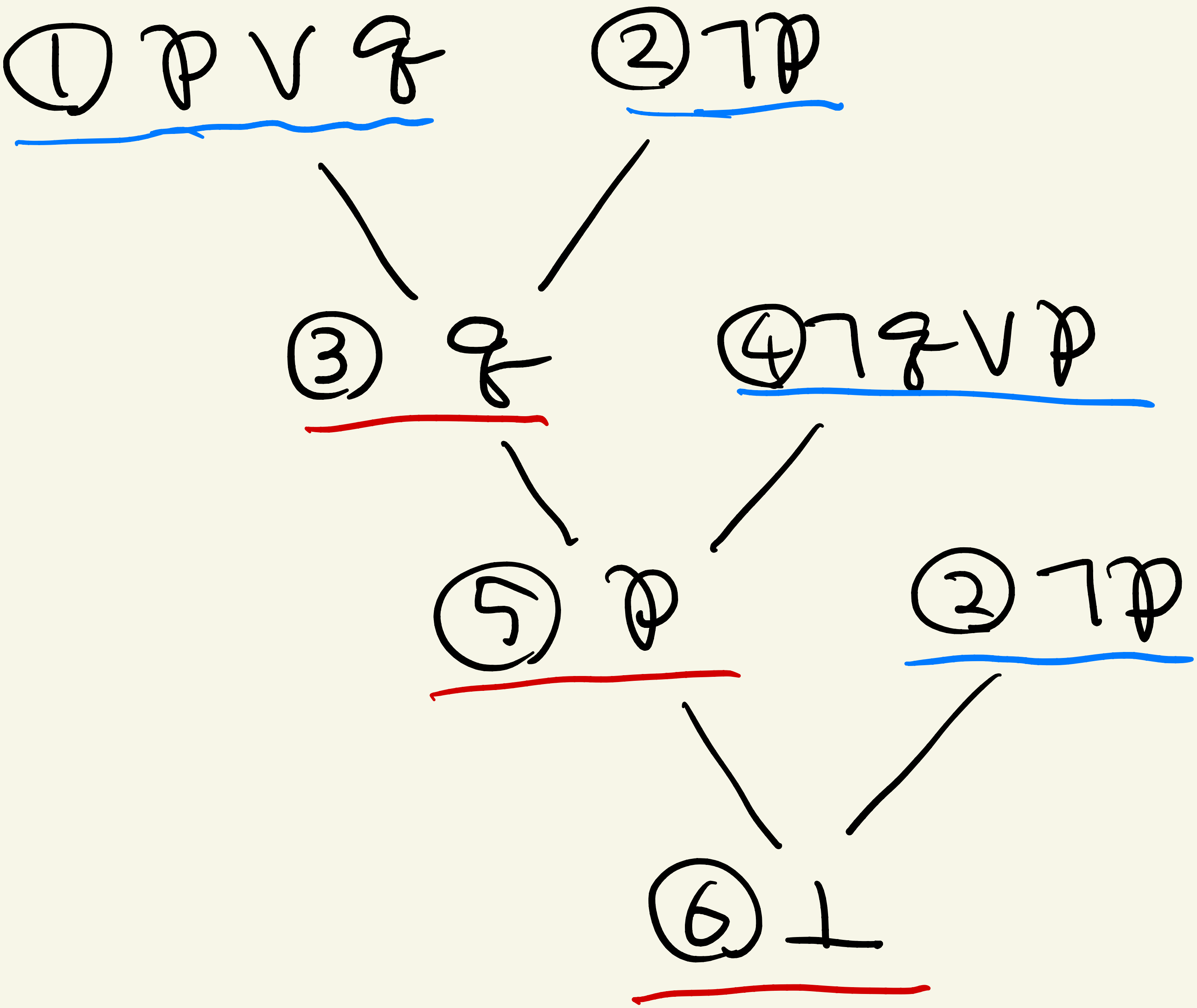
④ $\neg q \vee p$

⑤ p (③と④から)

⑥ $\perp$ (②と⑤から)

記法：導出は木として表す：

例：



命題: CNF φ から $\perp$ への導出が存在するとき、φ は充足不能である.

命題: 古典命題論理の論理式 φ について以下は同値:

- φ は恒真
- $\neg\varphi$ が充足不能.

例: $(p \vee q) \wedge \neg p \wedge (\neg q \vee p)$ は充足不能.

定義：$n\in\mathbb{N}$に対し

n穴 $n+1$羽 の鳩の巣原理のCNFは

原子論理式 $p^1_1, p^1_2, \dots, p^1_n$

$p^2_1, p^2_2, \dots, p^2_n,$

$\dots$

$p^{n+1}_1, p^{n+1}_2, \dots, p^{n+1}_n$ に対して

以下の節を∧で結んだもので、PHP_nで表す.

- $p^i_1 \vee p^i_2 \vee \dots \vee p^i_n \quad (i=1,\dots,n+1)$
- $\neg p^i_k \vee \neg p^j_k \quad \left(\begin{array}{l} i,j\in\{1,\dots,n+1\} \\ k\in\{1,\dots,n\} \\ i\neq j \end{array} \right.$

例： PHP$_1$（1穴2羽のとき）

$$p_1^1 \wedge p_1^2 \wedge (\neg p_1^1 \vee \neg p_1^2)$$

コメント：

- p_1^1：「鳩1が穴1に入っている」
- p_1^2：「鳩2が穴1に入っている」
- $\neg p_1^1 \vee \neg p_1^2$：「鳩1と2が穴1に同時に入っていることはない」

$$\neg p_1^1 \vee \neg p_1^2 \equiv \neg(p_1^1 \wedge p_1^2)$$

例：$\neg PHP_1$ は

$$\neg(p_1^1 \wedge p_1^2 \wedge (\neg p_1^1 \vee \neg p_1^2))$$

$$\equiv \neg p_1^1 \vee \neg p_1^2 \vee (p_1^1 \wedge p_1^2)$$

$$\equiv (p_1^1 \wedge p_1^2) \to (p_1^1 \wedge p_1^2).$$

これは恒真で

「ふつう」の鳩の巣原理と対応．

<u>例</u>: PHP_1から$\bot$への導出:

$$\dfrac{\dfrac{p_1^1 \qquad \neg p_1^1 \vee \neg p_1^2}{\neg p_1^2} \qquad p_1^2}{\bot}$$

例：PHP_2（2穴3羽のとき）は

以下の9つの節を∧で結んだもの；

① $p_1^1 \lor p_2^1$

② $p_1^2 \lor p_2^2$

③ $p_1^3 \lor p_2^3$

④ $\neg p_{\underline{1}}^1 \lor \neg p_{\underline{1}}^2$

⑤ $\neg p_{\underline{1}}^1 \lor \neg p_{\underline{1}}^3$

⑥ $\neg p_{\underline{1}}^2 \lor \neg p_{\underline{1}}^3$

⑦ $\neg p_{\underline{2}}^1 \lor \neg p_{\underline{2}}^2$

⑧ $\neg p_{\underline{2}}^1 \lor \neg p_{\underline{2}}^3$

⑨ $\neg p_{\underline{2}}^2 \lor \neg p_{\underline{2}}^3$

例：$\neg PHP_2$（2穴3羽のとき）は

以下の9つの節を$\vee$で結んだもの；

① $\neg(p_1^1 \vee p_2^1)$　④ $p_1^1 \wedge p_1^2$　⑦ $p_2^1 \wedge p_2^2$

② $\neg(p_1^2 \vee p_2^2)$　⑤ $p_1^1 \wedge p_1^3$　⑧ $p_2^1 \wedge p_2^3$

③ $\neg(p_1^3 \vee p_2^3)$　⑥ $p_1^2 \wedge p_1^3$　⑨ $p_2^2 \wedge p_2^3$

すなわち

$$((p_1^1 \vee p_2^1) \wedge (p_1^2 \vee p_2^2) \wedge (p_1^3 \vee p_2^3))$$

$$\longrightarrow (④ \vee ⑤ \vee ⑥ \vee ⑦ \vee ⑧ \vee ⑨).$$

命題: 各 $n \in \mathbb{N}$ について PHP_n は充足不能。

例: PHP_2 から $\bot$ への導出があることを見る。

まず $p^1_\bullet = a_\bullet$, $p^2_\bullet = b_\bullet$, $p^3_\bullet = c_\bullet$ と約束。

(穴は1と2, 鳩は a, b, c がいると読む。)

すると PHP_2 は以下の節の $\wedge$ になる:

① $a_1 \vee a_2$　④ $\neg a_1 \vee \neg b_1$　⑦ $\neg a_2 \vee \neg b_2$

② $b_1 \vee b_2$　⑤ $\neg a_1 \vee \neg c_1$　⑧ $\neg a_2 \vee \neg c_2$

③ $c_1 \vee c_2$　⑥ $\neg b_1 \vee \neg c_1$　⑨ $\neg b_2 \vee \neg c_2$

例(つづき):

① $a_1 \vee a_2$ ⑦ $\neg a_2 \vee \neg b_2$ ② $b_1 \vee b_2$ ⑥ $\neg b_1 \vee \neg c_1$

⑩ $a_1 \vee \neg b_2$ ⑪ $b_2 \vee \neg c_1$

⑫ $a_1 \vee \neg c_1$ ⑤ $\neg a_1 \vee \neg c_1$

⑬ $\neg c_1$ ③ $c_1 \vee c_2$

⑭ c_2

⋮

① $a_1 \lor a_2$ ⑧ $\neg a_2 \lor \neg c_2$

⑮ $a_1 \lor \neg c_2$ ⑭ c_2

⑯ a_1

② $b_1 \lor b_2$ ④ $\neg a_1 \lor \neg b_1$

⑰ $\neg a_1 \lor b_2$

⑱ b_2

⑨ $\neg b_2 \lor \neg c_2$

⑲ $\neg c_2$ ⑭ c_2

⑳ $\perp$

PHP_2は長さ20の$\perp$への導出をもつ。

定理 (Haken, 1985):

ある定数 c が存在して、

任意の PHP_n から ⊥ への導出の長さ L について

$$L \geq c \cdot 2^n$$ が成立。

コメント: 雑な導出計算の証明器をつくったら PHP_3 ですでに解けなかった。

PHP_2 の長さ 21 の導出は発見できた。

まとめ：鳩の巣原理の証明は長い。

与太話：P ≠ NP予想との関連？
（限定算術？）

参考資料：Massimo Lauriaの講義資料

https://massimolauria.net/courses/2015.ProofComplexity/