

情報論理学

松田 一孝

今日の話

- ❖ 講義情報
- ❖ 数理論理学とは？
- ❖ どうして数理論理学を学ぶのか？

講義の進め方

- ❖ (来週から) 板書+配布プリント
 - プリントは講義ページから入手可
 - プリントには練習問題も
- ❖ 成績評価
 - 主に試験 (2回) による
 - ◆1回はレポートにするかも
 - レポートを課した場合はそれも評価
 - 出席点はない

教科書・参考書

❖教科書

- なし

❖参考書

- シラバス参照

その講義情報

❖ 講義ページ

<http://www2.sf.ecei.tohoku.ac.jp/~kztk/teaching/2016/logic/>

❖ 質問等

- 講義中に直接質問（オススメ）
- メールで質問 or 訪問予約

kztk@ecei.tohoku.ac.jp

重要なお知らせ

- ❖ 7/19は期末試験
 - 範囲, 方式は追って通知
- ❖ 7/26は答案の返却と問題の解説
 - 点数に関する異議申立はこの日以降受けつけない
- ❖ 再試験は行わない

数理論理学って？

論理学って

❖ 「推論の方法やその正しさ」

についての学問

◦例：アリストテレスの3段論法

ソクラテスは人である

全ての人は定命である

よって

ソクラテスは定命である

数理論理学

- ❖ 数学としての論理学
 - 数学基礎論の一つ
 - ◆ 「数学」の数学
- ❖ 19, 20世紀に大きく発展
 - Hilbertのプログラム
 - 素朴集合論の破綻
 - ◆ Russelの逆説, Cantorの逆説,
Burali-Fortiの逆説

例：アリストテレスの3段論法

ソクラテスは人である

全ての人は定命である

よって

ソクラテスは定命である

例：アリストテレスの3段論法

仙台市は政令指定都市である

全ての政令指定都市は人口50万以上である

よって

仙台市は人口50万以上である

「論理的」ではない推論

仙台市は政令指定都市である
全ての政令指定都市は人口50万以上である
よって

仙台市は人口100万以上である

「論理的」ではある推論

仙台市は政令指定都市である

全ての政令指定都市は人口100万以上である

よって

仙台市は人口100万以上である

「論理的」な推論の形式

cは□□である

□□であるものは全て△△である

よって

cは△△である

記号を変数に

c は P である

P である x は全て Q である

よって

c は Q である

二文目をいいかえ

c は P である

全ての x について x が P であるならば x は Q である

よって

c は Q である

論理記号を利用

cはPである

かつ

$P(c) \wedge$

$(\forall x. P(x) \Rightarrow Q(x))$

すべてのxについて

\Rightarrow

ならば

$Q(c)$

cはPである

cf. 全てのxについてxがPであるならばxはQである

よって

cはQである

「論理的」な推論とは？

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow P(s)$$

意味論（モデル論）：**妥当性**

任意のc, P, Qの解釈に対し正しい

構文論（証明論）：**証明可能性**

妥当な証明規則によって証明できる

妥当な式

❖ 全ての解釈において真となる式

◦ 変数/定数をどう具体的に割り当てるか

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow P(c)$$

解釈1

ソクラテスは人である
全ての人は定命である

よって

ソクラテスは定命である

解釈2

仙台市は政令指定都市である
全ての政令指定都市は人口50万以上である

よって

仙台市は人口50万以上である

証明可能な式

❖ 特定の推論規則によって導出できる式

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow Q(c)$$

$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x))$ を仮定.

仮定より, $\forall x. P(x) \Rightarrow Q(x)$ が言える.

よって, $P(c) \Rightarrow Q(c)$.

また, 仮定より $P(c)$. よって $Q(c)$.

従って $P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow Q(c)$.

証明可能な式

❖ 特定の推論規則によって導出できる式

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow Q(c)$$

$$\Gamma \vdash P(c) \wedge (\forall x. P(x) \Rightarrow Q(x))$$

$$\Gamma \vdash \forall x. P(x) \Rightarrow Q(x)$$

$$\Gamma \vdash P(c) \wedge (\forall x. P(x) \Rightarrow Q(x))$$

$$\Gamma \vdash P(c) \Rightarrow Q(c)$$

$$\Gamma \vdash P(c)$$

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \vdash Q(c)$$

$$\vdash P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow Q(c)$$

ただし, $\Gamma = P(c) \wedge (\forall x. P(x) \Rightarrow Q(x))$

健全性と完全性

❖ 健全性

- 証明可能な式は妥当
 - ◆ 例：一階述語論理は健全

❖ 完全性

- 妥当な式は証明可能
 - ◆ 例：一階述語論理は完全 (1930)
 - Gödelの完全性定理

本講義で扱う論理

❖ 命題論理

$$P \wedge (P \Rightarrow Q) \Rightarrow Q$$

❖ 一階述語論理

◦ 量化子 (\forall , \exists) 含む

$$P(c) \wedge (\forall x. P(x) \Rightarrow Q(x)) \Rightarrow Q(c)$$

講義の流れ

❖ 前半：命題論理

○ モデル論

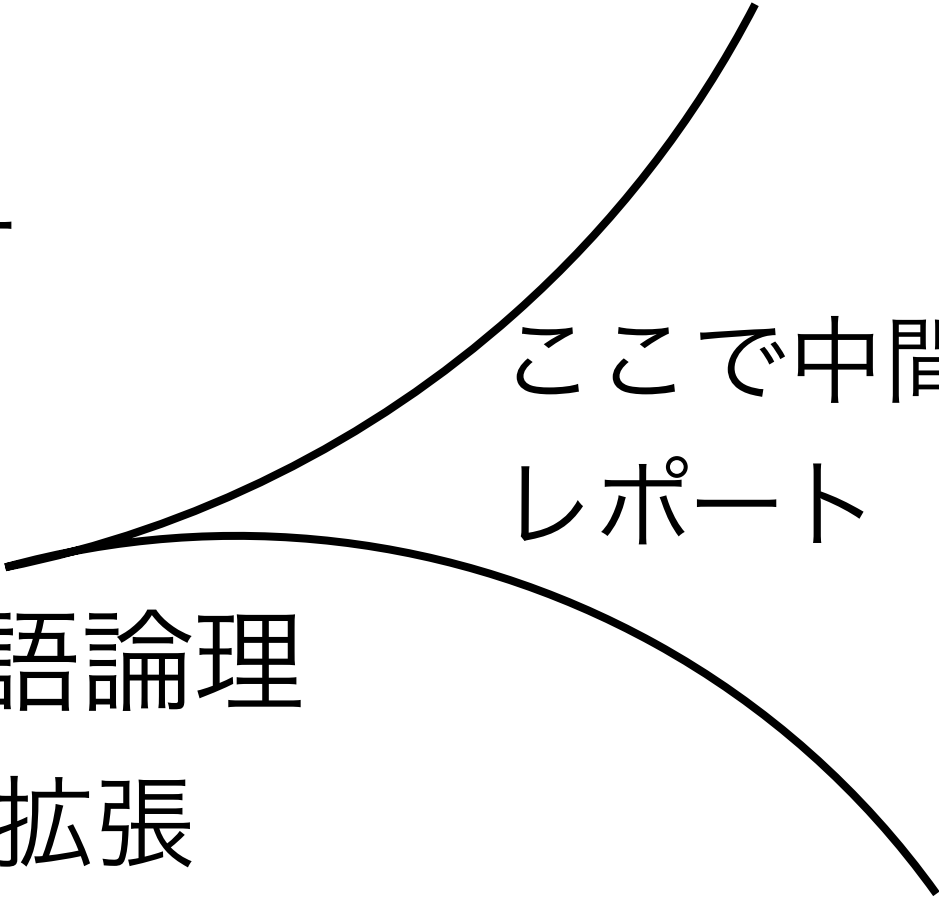
◆ トートロジー

○ 証明論

◆ 自然演繹

❖ 後半：一階述語論理

○ 前半の議論を拡張



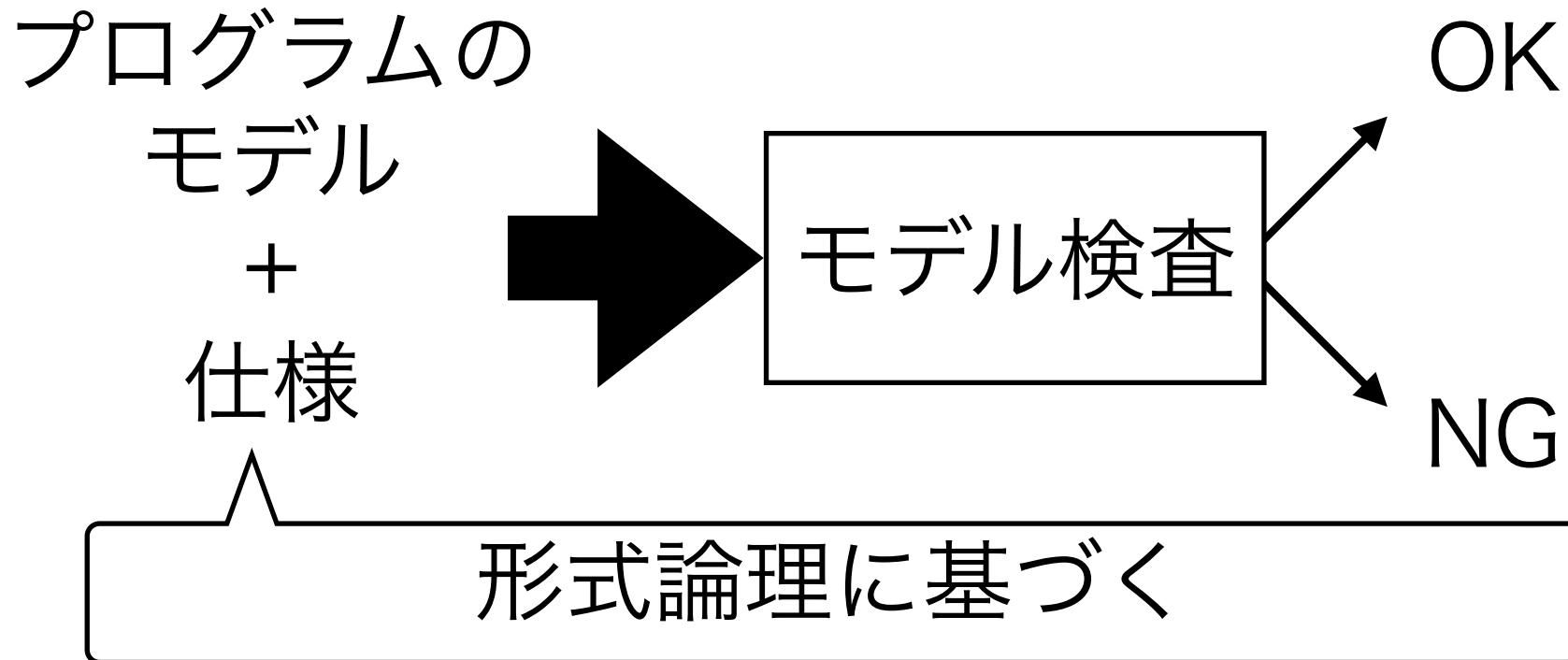
ここで中間試験か
レポート

Q. なぜ数理論理学を学ぶの？

Q. なぜ数理論理学を学ぶの？

A1. 理論・実用上有用だから

(ソフトウェア) モデル検査



Windows Driver Development Kitで利用

Microsoft Research

[Our research](#)

[Engage with us](#)

[Careers](#)

[About us](#)



[All](#)

[Downloads](#)

[Events](#)

[Groups](#)

[News](#)

[People](#)

[Projects](#)

[Publications](#)

[Videos](#)

SLAM

SLAM is a project for checking that software satisfies critical behavioral properties of the interfaces it uses and to aid software engineers in designing interfaces and software that ensure reliable and correct functioning. Static Driver Verifier is a tool in the Windows Driver Development Kit that uses the SLAM verification engine.

What's New?

- **Yogi** is now available to plug into the Static Driver Verifier Research Platform. To install SDVRP and Yogi, see this [README](#).
- **The Summer (2011) of SLAM saw** two awards and a retrospective article in CACM:
 - **Most Influential PLDI Paper award** for [Automatic Predicate Abstraction of C Programs](#), Thomas Ball, Rupak Majumdar, Todd D. Millstein, Sriram K. Rajamani, [PLDI 2001](#). The first conference paper from the SLAM project.
 - **CAV 2011 Award**. Citation: "The 2011 CAV Award is given to Thomas Ball and Sriram Rajamani, both at Microsoft Research, for their contributions to software model checking, specifically the development of the SLAM/SDV software model checker that successfully demonstrated computer-aided verification techniques on real programs."
 - **A Decade of Software Model Checking with SLAM**, T. Ball, V. Levin, S. K. Rajamani, [Communications of the ACM, Vol. 54. No. 7, 2011, Pages 68-76](#)

"Things like even software verification, this has been the Holy Grail of computer science for many decades but now in some very key areas, for example, driver verification we're building tools that can do actual proof about the software and how it works in order to guarantee the reliability." **Bill Gates, April 18, 2002.**

[Keynote address at WinHec 2002](#)



SLAM
`if= node-> i ++ vis procs. end() + node; }`

形式論理に基づく仕様記述

❖ Felicaの成功例

○ ソニーの非接触ICカード技術

特集
フォーマル
メソッドの
新潮流
3

Part II: 産業界への応用

携帯電話組込み用モバイル
FeliCa ICチップ開発における
形式仕様記述手法の適用

栗田太郎 ● フェリカネットワークス(株) 開発部 2課

筆者らは、携帯電話組込み用モバイル FeliCa IC チップファームウェアの開発に、形式仕様記述手法を適用し、手法導入の目的である、(1) 厳密な仕様の記述、(2) 仕様の段階的な記述と検証を中心とした開発スキームの構築、フレームワークの検討と導入、(3) 記述精度の向上とテストによる品質の確保、(4) 仕様で活用した徹底的なテスト、(5) コミュニケーションの活性化、を達成し、開発の成果を上げると同時に、手法適用の効果を確認した。

「情報処理」Vol.49, No.5, 2008

定理証明支援系

- ❖ 証明をプログラミング
- ❖ 証明の正しさを型検査のように確認可

- ❖ Coq, Isabelle/HOL, Agda, ...

奇数位数定理

「奇数位数の群は可解である」

- ❖ FeitとThomsonが1963に証明
 - が、200ページ以上
 - ◆ 証明の正しさを確認するのは大変
- ❖ Gonthierらが2005にCoqで形式化
 - 約15万行のCoqコード
 - ◆ 証明の正しさは機械的に確認

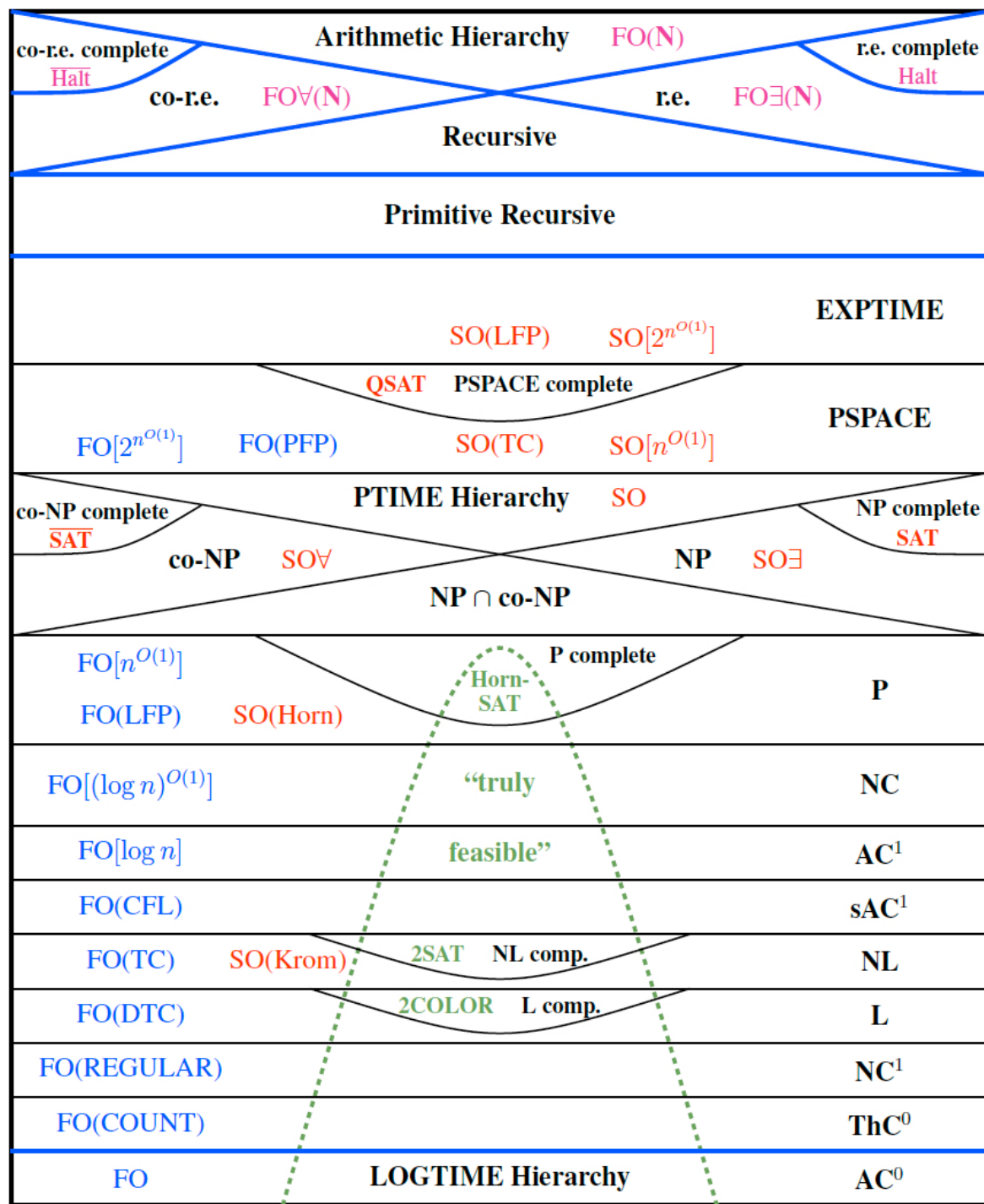
MLと命題論理

- ❖ (直観主義) 命題論理であれば,
(S)MLを使って証明できる
 - 関数抽象と関数適用のみを使って
以下の型を持つ式を定義してみよう
 - ◆ $'a \rightarrow 'a$
 - ◆ $'a \rightarrow ('a \rightarrow 'b) \rightarrow 'b$
 - ◆ $('a \rightarrow 'b \rightarrow 'c) \rightarrow ('a \rightarrow 'b) \rightarrow 'a \rightarrow 'c$

記述計算量

❖ 問題の記述に必要な形式論理と計算量の関係

❖ 有限モデル理論の一分野

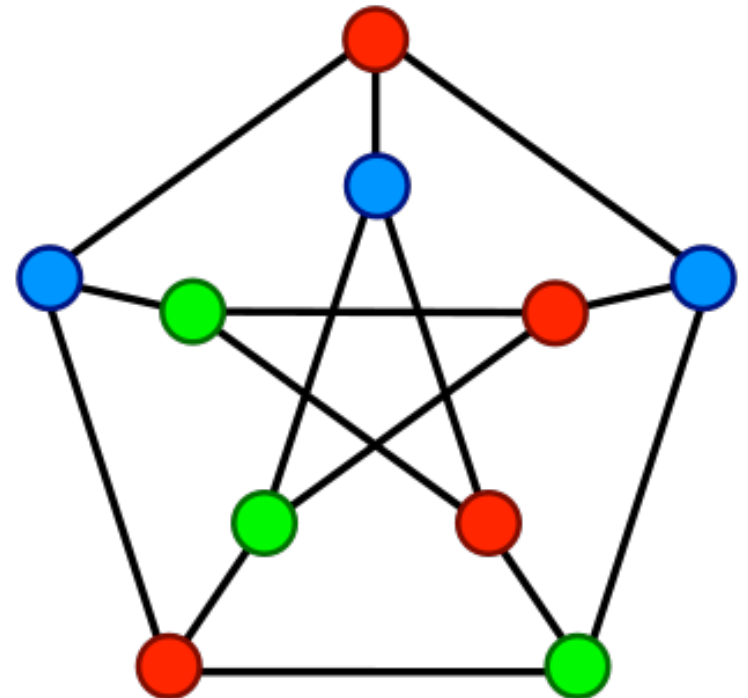


図はNeil Immermanのwebsiteより

例：グラフ彩色

❖ 無向グラフの頂点に「色」を割り当て
◦ ただし，隣接する頂点は異なる色

❖ k 色彩色可能性は
一般にNP完全
◦ $k = 1, 2$ だとP
◦ 平面で $k > 3$ だとP



「3色彩可能」の論理式

$\exists R. \exists G. \exists B.$

$(\forall v. (R(v) \vee G(v) \vee B(v)) \wedge$

$\neg(R(v) \wedge B(v)) \wedge$

$\neg(R(v) \wedge G(v)) \wedge$

$\neg(B(v) \wedge R(v))))$

$\wedge (\forall v. \forall u. E(v, u) \Rightarrow$

$\neg (R(v) \wedge R(u)) \wedge$

$\neg (G(v) \wedge G(u)) \wedge$

$\neg (B(v) \wedge B(u)))$

SO \exists の式

\Rightarrow 3色彩可能性はNP

SAT：充足可能性問題

- ❖ 与えられた命題論理式を真にする解釈が存在するか判定
 - 一般にはNP完全
 - 多くの問題に対しては高速に解ける
 - ◆ minisat等のSATソルバ

$P \wedge Q$ 充足可能 ($P=Q=真$)

$P \wedge \neg P$ 充足不能

Q. なぜ数理論理学を学ぶの？

A2. それ自体楽しい

論理パズル

❖ 論理学に基づくパズル

- たいていは命題論理に基づく
- ファンも多く多数の書籍が出版
 - ◆ Amazon.co.jpで「論理パズル」で検索すると987件ヒット
- 公務員試験とかでも出題されるらしい

正直者と嘘吐きのパズル

AとBは正直者か嘘吐きである。

A 「Bは嘘吐きです」

B 「Aとは同じタイプの人間です」

AとBはそれぞれどちらか？

- 正直者：いつでも本当のことを言う
- 嘘吐き：いつでも嘘を言う

AとBは正直者か嘘吐きである.

A 「Bは嘘吐きです」

B 「Aとは同じタイプの人間です」

AとBはそれぞれどちらか？

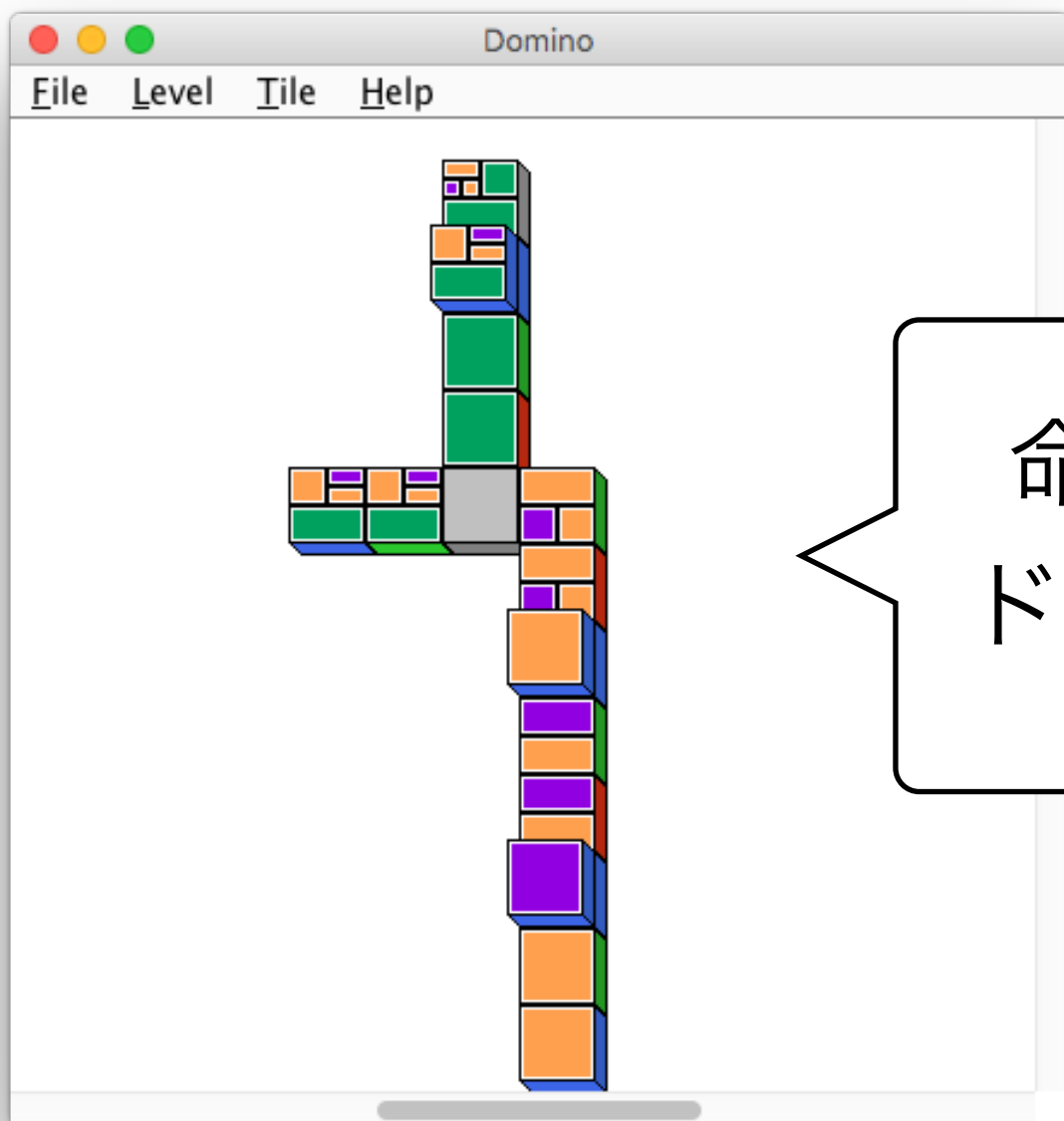
❖ T_A : Aが正直者, T_B : Bが正直者とする

❖ AがPと主張する: $T_A \Leftrightarrow P$

T_A	T_B	$T_A \Leftrightarrow \neg T_B$	$T_B \Leftrightarrow (T_A \wedge T_B) \vee (\neg T_A \wedge \neg T_B)$
真	真	偽	真
真	偽	真	真
偽	真	真	偽
偽	偽	偽	偽

ドミノゲーム

<https://sourceforge.net/projects/nddomino/>



命題論理の証明を
ドミノゲームで表現

