ソフトウェア情報学部 2025 年度入学前勉強会
コンピュータと一緒に考える：証明支援系体験

高橋 優太

青森大学 ソフトウェア情報学部

2025 年 3 月 24 日

目標・やり方

本勉強会の目標

コンピュータによる処理に触れてみよう

- 入学後，学ぶことの一つは…

  コンピュータを用いてプログラムを書く・実行する
- 入学前に先取りして触れてみよう

目標・やり方

本勉強会の目標

コンピュータによる処理に触れてみよう

- 入学後，学ぶことの一つは…

  コンピュータを用いてプログラムを書く・実行する
- 入学前に先取りして触れてみよう

本勉強会のやり方

題材として論理学を用いてみる

- 数学 I の「集合と命題」で実は触れている
  ↪ プログラミングに関する前提知識が必要ない
- 現代の論理学はコンピュータ・サイエンスと密接にかかわる
- 私の専門だから☺

集合とは

- ものの集まりで，しかもそれに属するかどうかきっちり境界線を引ける集まりのことを集合 (set) と呼ぶことにする
  - もの x が集合 A に属することを $x \in A$ と書き，反対に x が A に属さないことを $x \notin A$ と書く

集合とは

- ものの集まりで，しかもそれに属するかどうかきっちり境界線を引ける集まりのことを集合 (set) と呼ぶことにする
  - もの x が集合 A に属することを $x \in A$ と書き，反対に x が A に属さないことを $x \notin A$ と書く
- 例えば，-1 よりも大きいが 5 よりは小さい整数の集まりは集合であって，以下のように表せる：

$$\{0, 1, 2, 3, 4\}$$

集合とは

- ものの集まりで，しかもそれに属するかどうかきっちり境界線を引ける集まりのことを集合 (set) と呼ぶことにする
  - もの x が集合 A に属することを $x \in A$ と書き，反対に x が A に属さないことを $x \notin A$ と書く
- 例えば，-1 よりも大きいが 5 よりは小さい整数の集まりは集合であって，以下のように表せる：

$$\{0, 1, 2, 3, 4\} \qquad 3 \in \{0, 1, 2, 3, 4\} \qquad 5 \notin \{0, 1, 2, 3, 4\}$$

集合とは

- ものの集まりで，しかもそれに属するかどうかきっちり境界線を引ける集まりのことを集合 (set) と呼ぶことにする
  - もの x が集合 A に属することを $x \in A$ と書き，反対に x が A に属さないことを $x \notin A$ と書く
- 例えば，-1 よりも大きいが 5 よりは小さい整数の集まりは集合であって，以下のように表せる：

$$\{0, 1, 2, 3, 4\} \qquad 3 \in \{0, 1, 2, 3, 4\} \qquad 5 \notin \{0, 1, 2, 3, 4\}$$

- 一方で，おいしい食べ物を集めても集合にはならない（$\because$ 食べ物がおいしいかどうかにはきっちりした境界線を引けない）

集合とは

- ものの集まりで，しかもそれに属するかどうかきっちり境界線を引ける集まりのことを集合 (set) と呼ぶことにする
  - もの x が集合 A に属することを $x \in A$ と書き，反対に x が A に属さないことを $x \notin A$ と書く
- 例えば，-1 よりも大きいが 5 よりは小さい整数の集まりは集合であって，以下のように表せる：

$$\{0, 1, 2, 3, 4\} \qquad 3 \in \{0, 1, 2, 3, 4\} \qquad 5 \notin \{0, 1, 2, 3, 4\}$$

- 一方で，おいしい食べ物を集めても集合にはならない（$\because$ 食べ物がおいしいかどうかにはきっちりした境界線を引けない）
- 無限個の要素をもつ集まりも，境界線が引けているならば集合
  - 例えば，整数の集合 $\mathbb{Z}$ など

集合とは

- 要素を列挙することで集合を表すことができる
  - 列挙する順番は関係なく，同じ要素が列挙されたらそれらは同じ集合

$$\{0, 1, 2, 3\} = \{3, 1, 0, 2\}$$

集合とは

- 要素を列挙することで集合を表すことができる
  - 列挙する順番は関係なく，同じ要素が列挙されたらそれらは同じ集合

$$\{0, 1, 2, 3\} = \{3, 1, 0, 2\}$$

- 条件を指定することで集合を表すこともできる：例えば，

$$\{x \mid x \text{ は } 2 \text{ の倍数となる数である } \}$$

というようにして，2 の倍数となる数 x すべてを集めてできる集合（すなわち偶数の集合）を表せる

集合とは

- 要素を列挙することで集合を表すことができる
  - 列挙する順番は関係なく，同じ要素が列挙されたらそれらは同じ集合

$$\{0, 1, 2, 3\} = \{3, 1, 0, 2\}$$

- 条件を指定することで集合を表すこともできる：例えば，

$$\{x \mid x \text{ は } 2 \text{ の倍数となる数である } \}$$

  というようにして，2 の倍数となる数 x すべてを集めてできる集合（すなわち偶数の集合）を表せる
- ひとつも要素をもたない集まりも集合であり，空集合と呼び $\emptyset$ と表す
  - こんなふうにして空集合を表すこともできる：

$$\{x \mid x \text{ は } 2 \text{ の倍数となるような奇数である } \}$$

集合とは

- 要素を列挙することで集合を表すことができる
  - 列挙する順番は関係なく，同じ要素が列挙されたらそれらは同じ集合

$$\{0, 1, 2, 3\} = \{3, 1, 0, 2\}$$

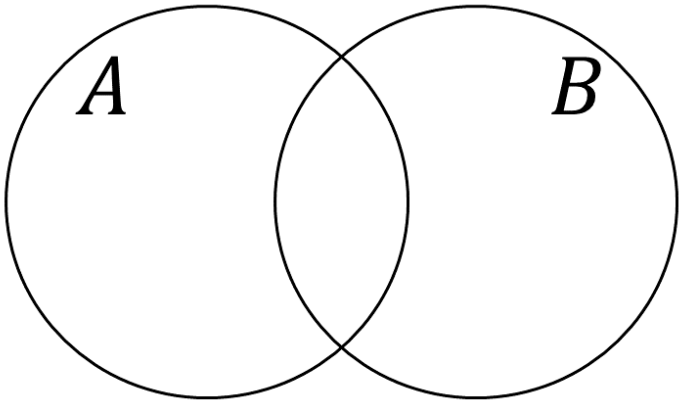
- 条件を指定することで集合を表すこともできる：例えば，

$$\{x \mid x \text{ は } 2 \text{ の倍数となる数である } \}$$

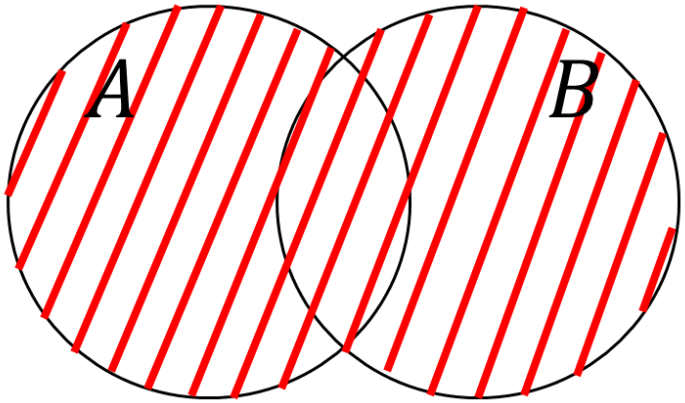
  というようにして，2 の倍数となる数 x すべてを集めてできる集合（すなわち偶数の集合）を表せる
- ひとつも要素をもたない集まりも集合であり，空集合と呼び $\emptyset$ と表す
  - こんなふうにして空集合を表すこともできる：

$$\{x \mid x \text{ は } 2 \text{ の倍数となるような奇数である } \} = \emptyset$$

和集合



和集合

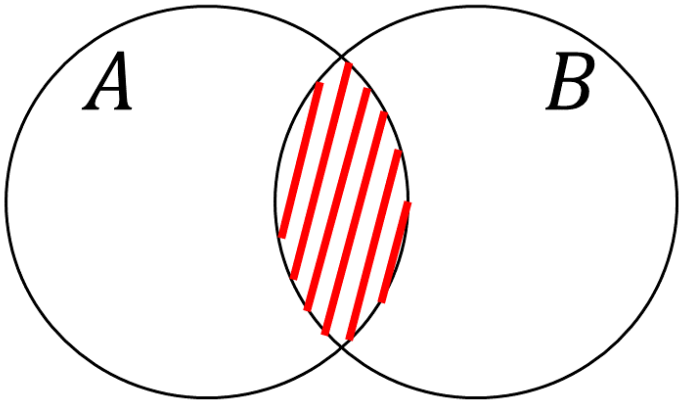


- 集合 A の要素と集合 B の要素を集めてできる集合のことを A と B の和集合と呼び，

$$A \cup B$$

と表す（つまり $A \cup B = \{x \mid x \in A \text{ または } x \in B\}$）

共通部分



- 集合 A にも集合 B にも属する要素を集めてできる集合のことを A と B の共通部分と呼び，

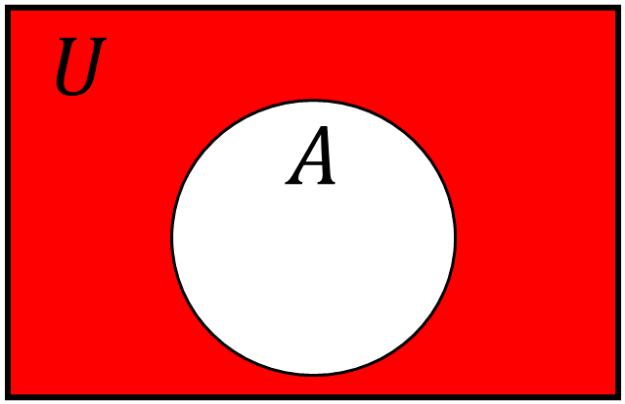
$$A \cap B$$

と表す（つまり $A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$）

補集合

- 考察する対象すべてを集めた集合を全体集合と呼び U と表す

補集合



- 考察する対象すべてを集めた集合を全体集合と呼び U と表す
- 集合 A の要素ではないものを集めてできる集合のことを A の補集合と呼び，

$$\overline{A}$$

と表す（つまり $\overline{A} = \{x \in U \mid x \notin A\}$）

命題とは

- 正しいのかそれとも正しくないのかがはっきり決まっている式や文のことを命題 (proposition) と呼ぶ
  - ある命題 A が正しいことを A は真であるといい，反対にある命題 A は正しくないことを A は偽であるという

命題とは

- 正しいのかそれとも正しくないのかがはっきり決まっている式や文のことを命題 (proposition) と呼ぶ
  - ある命題 A が正しいことを A は真であるといい，反対にある命題 A は正しくないことを A は偽であるという
- 以下はどれも命題である：
  1. $71 > 38$
  2. 2025 年 3 月 24 日時点での青森県庁所在地は青森市である．
  3. 2025 年 3 月 24 日時点での青森県庁所在地は弘前市である．

命題とは

- 正しいのかそれとも正しくないのかがはっきり決まっている式や文のことを命題 (proposition) と呼ぶ
  - ある命題 A が正しいことを A は真であるといい，反対にある命題 A は正しくないことを A は偽であるという
- 以下はどれも命題である：
  1. $71 > 38$
  2. 2025 年 3 月 24 日時点での青森県庁所在地は青森市である．
  3. 2025 年 3 月 24 日時点での青森県庁所在地は弘前市である．
- 以下はどちらも命題ではない：
  1. $x > 38$
  2. ホヤはおいしい．

命題とは

- 正しいのかそれとも正しくないのかがはっきり決まっている式や文のことを命題 (proposition) と呼ぶ
  - ある命題 A が正しいことを A は真であるといい，反対にある命題 A は正しくないことを A は偽であるという
- 以下はどれも命題である：
  1. $71 > 38$
  2. 2025 年 3 月 24 日時点での青森県庁所在地は青森市である．
  3. 2025 年 3 月 24 日時点での青森県庁所在地は弘前市である．
- 以下はどちらも命題ではない：
  1. $x > 38$
  2. ホヤはおいしい．
- 微妙なケース：
  1. 弘前は県庁所在地である．
  2. 現在の日本の大統領は青森出身である．

集合から論理を取り出す：論理和

- 集合 A と集合 B の和集合 $A \cup B$ とは

$$A \cup B = \{x \mid x \in A \text{ または } x \in B\}$$

というものであったから，次がいえる：

$$x \in A \cup B \Longleftrightarrow x \in A \text{ または } x \in B$$

「または」は論理和や選言と呼ばれ，論理的関係を表す接続詞である論理結合子のひとつ（論理結合子は命題をつなぐ言葉）

集合から論理を取り出す：論理和

- 集合 A と集合 B の和集合 $A \cup B$ とは

$$A \cup B = \{x \mid x \in A \text{ または } x \in B\}$$

というものであったから，次がいえる：

$$x \in A \cup B \iff x \in A \text{ または } x \in B$$

「または」は論理和や選言と呼ばれ，論理的関係を表す接続詞である論理結合子のひとつ（論理結合子は命題をつなぐ言葉）

- 今度は A, B を命題として「A または B」を $A \vee B$ と表すと，
  - $A \vee B$ が真である $\iff$ A と B の少なくとも一方が真である

集合から論理を取り出す：論理和

- 集合 A と集合 B の和集合 $A \cup B$ とは

$$A \cup B = \{x \mid x \in A \text{ または } x \in B\}$$

というものであったから，次がいえる：

$$x \in A \cup B \Longleftrightarrow x \in A \text{ または } x \in B$$

「または」は論理和や選言と呼ばれ，論理的関係を表す接続詞である論理結合子のひとつ（論理結合子は命題をつなぐ言葉）

- 今度は A, B を命題として「A または B」を $A \vee B$ と表すと，
  - $A \vee B$ が真である $\Longleftrightarrow$ A と B の少なくとも一方が真である
- 例：青森市は現在晴れているか，または弘前市は現在晴れている．

  青森市は現在晴れている $\vee$ 弘前市は現在晴れている

集合から論理を取り出す：論理積

- 集合 A と集合 B の共通部分 $A \cap B$ とは

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$

であったから，次がいえる：

$$x \in A \cap B \iff x \in A \text{ かつ } x \in B$$

「かつ」は論理積や連言と呼ばれる論理結合子

集合から論理を取り出す：論理積

- 集合 A と集合 B の共通部分 $A \cap B$ とは

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$

であったから，次がいえる：

$$x \in A \cap B \iff x \in A \text{ かつ } x \in B$$

「かつ」は論理積や連言と呼ばれる論理結合子

- 命題 A, B について「A かつ B」を $A \wedge B$ と表すと，
  - $A \wedge B$ が真である $\iff$ A と B の両方が真である

集合から論理を取り出す：論理積

- 集合 A と集合 B の共通部分 $A \cap B$ とは

$$A \cap B = \{x \mid x \in A \text{ かつ } x \in B\}$$

であったから，次がいえる：

$$x \in A \cap B \iff x \in A \text{ かつ } x \in B$$

「かつ」は論理積や連言と呼ばれる論理結合子

- 命題 A, B について「A かつ B」を $A \wedge B$ と表すと，
  - $A \wedge B$ が真である $\iff$ A と B の両方が真である
- 例：青森市は現在晴れており，かつ弘前市は現在晴れている．

  青森市は現在晴れている $\wedge$ 弘前市は現在晴れている

集合から論理を取り出す：否定

- 集合 A の補集合 $\overline{A}$ とは

$$\overline{A} = \{x \in U \mid x \notin A\}$$

であったから，次がいえる：

$$x \in \overline{A} \Longleftrightarrow x \in U \text{ かつ } x \notin A \Longleftrightarrow x \in U \text{ かつ（} x \in A \text{ でない）}$$

「でない」は否定と呼ばれる論理結合子

集合から論理を取り出す：否定

- 集合 A の補集合 $\overline{A}$ とは

$$\overline{A} = \{x \in U \mid x \notin A\}$$

であったから，次がいえる：

$$x \in \overline{A} \Longleftrightarrow x \in U \text{ かつ } x \notin A \Longleftrightarrow x \in U \text{ かつ（} x \in A \text{ でない）}$$

「でない」は否定と呼ばれる論理結合子

- 命題 A について「A でない」を $\neg A$ と表すと．
  - $\neg A$ が真である $\Longleftrightarrow$ A が偽である

集合から論理を取り出す：否定

- 集合 A の補集合 $\overline{A}$ とは

$$\overline{A} = \{x \in U \mid x \notin A\}$$

であったから，次がいえる：

$$x \in \overline{A} \Longleftrightarrow x \in U \text{ かつ } x \notin A \Longleftrightarrow x \in U \text{ かつ（} x \in A \text{ でない）}$$

「でない」は否定と呼ばれる論理結合子

- 命題 A について「A でない」を $\neg A$ と表すと．
  - $\neg A$ が真である $\Longleftrightarrow$ A が偽である
- 例：弘前は現在の青森県庁所在地ではない．

$$\neg(\text{弘前は現在の青森県庁所在地である})$$

論理パズル

問題 1

次の 3 つの証言が正しいとすると犯人が分かる．誰だろうか？

1. 太郎が犯人であるか，または次郎が犯人である．
2. 次郎が犯人であるならば花子も犯人である．
3. 花子は犯人でない．

論理パズル

問題 1

次の 3 つの証言が正しいとすると犯人が分かる．誰だろうか？

1. 太郎が犯人であるか，または次郎が犯人である．
2. 次郎が犯人であるならば花子も犯人である．
3. 花子は犯人でない．

- 「ならば」に対応する論理結合子は $\rightarrow$

問題 1（記号化バージョン）

次の 3 つの証言が正しいとすると犯人が分かる．誰だろうか？

1. 太郎は犯人である $\vee$ 次郎は犯人である
2. 次郎は犯人である $\rightarrow$ 花子は犯人である
3. $\neg$(花子は犯人である)

論理パズル

問題 2

証言の集まりが整合的であるのは，その集まりから矛盾が導かれない（つまり，ある命題 A とその否定 $\neg A$ がともに導かれることがない）ときである．次の 3 つの証言は整合的だろうか？

1. 次郎が犯人であり，太郎は犯人でない．
2. 次郎と花子が共犯であることはない．
3. 花子が犯人でないならば太郎が犯人である．

論理パズル

問題 2

証言の集まりが整合的であるのは，その集まりから矛盾が導かれない（つまり，ある命題 A とその否定 $\neg A$ がともに導かれることがない）ときである．次の 3 つの証言は整合的だろうか？

1. 次郎が犯人であり，太郎は犯人でない．
2. 次郎と花子が共犯であることはない．
3. 花子が犯人でないならば太郎が犯人である．

問題 2（記号化バージョン）

次の 3 つの証言は整合的だろうか？

1. 次郎は犯人である $\wedge\neg$(太郎は犯人である)
2. $\neg$(次郎は犯人である $\wedge$ 花子は犯人である)
3. $\neg$(花子は犯人である)$\rightarrow$ 太郎は犯人である

証明支援系

- 証明支援系 (proof assistant)：
  コンピュータの中で証明を書くためのツール
  - 複雑なあまり人間の手では正しさがチェックできないような証明を検証できる
  - プログラムが意図通りに動くことを厳密に検証したいときにも用いられる
  - 証明支援系を使って論理パズルを解いてみよう

[1] https://coq.inria.fr/
[2] https://rocq-prover.org/

証明支援系

- 証明支援系 (proof assistant)：
  コンピュータの中で証明を書くためのツール
  - 複雑なあまり人間の手では正しさがチェックできないような証明を検証できる
  - プログラムが意図通りに動くことを厳密に検証したいときにも用いられる
  - 証明支援系を使って論理パズルを解いてみよう
- Coq: もっとも有名な証明支援系の中の一つ [1]
  - さいきん Rocq に改名した [2]

[1] https://coq.inria.fr/
[2] https://rocq-prover.org/

証明支援系

- 証明支援系 (proof assistant)：
  コンピュータの中で証明を書くためのツール
  - 複雑なあまり人間の手では正しさがチェックできないような証明を検証できる
  - プログラムが意図通りに動くことを厳密に検証したいときにも用いられる
  - 証明支援系を使って論理パズルを解いてみよう
- Coq: もっとも有名な証明支援系の中の一つ [1]
  - さいきん Rocq に改名した [2]
- Coq を web ブラウザ上で動かせる：jsCoq
  - Emilio Jesús Gallego Arias, Benoît Pin, and Pierre Jouvelot. jsCoq: Towards Hybrid Theorem Proving Interfaces. In: Serge Autexier and Pedro Quaresma (eds.), *Proceedings of the 12th Workshop on User Interfaces for Theorem Provers, UITP 2016, Coimbra, Portugal, 2nd July 2016*, 15–27. 2017.
  - Emilio Jesús Gallego Arias, Shachar Itzhaky, and Benoît Pin. *jsCoq – Use Coq in Your Browser*. Retrieved 24 March, 2025, from `https://coq.vercel.app/`

[1] `https://coq.inria.fr/`
[2] `https://rocq-prover.org/`

Coq を体験

1. PC で参加している人は
   - Zoom チャットで共有した URL をクリック，あるいは
   - 配布スライド `pre2025slides.pdf`（いまみなさんが見ているのと同じスライド）を開いて以下の URL をクリックしても OK

     `https://coq.vercel.app/scratchpad.html`

     左半分が白紙で，右上に次のアイコンがあるページに行くはず

     
2. 配布資料 `pre2025code.txt` の中身すべてをコピーして白紙の部分にペースト
3. 今回は以下のアイコンだけで OK

    : コードを 1 つのブロックだけ読ませる

    : コードを 1 つのブロックだけ戻す

    : カーソルの箇所まで進む/戻る

Coqを体験

今回のまとめ

- 論理学を題材にコンピュータによる処理に触れた
  - 入学後はまず，Python などメジャーな言語をゼロから学ぼう
- プログラムを書く際の文法は厳密
  - 少しの打ち間違いでもコンピュータはエラーを返す
  - コンピュータとの付き合い方にも慣れていこう
- でも，情報系だけでなく他にも関心を広げよう！