

Decision problems

ian.mcloughlin@gmit.ie

Example: PRIMES

$$\text{PRIMES} = \{i : j \nmid i \ \forall j < i ; 1 < i, j \in \mathbb{N}\}$$

PRIMES is a subset of the natural numbers.

Decision problem: map f from \mathbb{N} to $\{0, 1\}$.

Indicates whether $i \in \text{PRIMES}$ ($f(i) = 1$) or not ($f(i) = 0$).

Stipulate the elements of PRIMES are written in binary, e.g. 7 is 111.

Then PRIMES is a language over $\{0, 1\}$.

Decision problem

$$f : S \rightarrow T \text{ where } |T| = 2$$

A decision problem is a map to a set with two elements. Usually $T = \{0, 1\}$ and S is a language over $\{0, 1\}$.

Example

$$f : \{0, 1\}^* \rightarrow \{0, 1\}$$

$$f(s) = 0 \Leftrightarrow |s| \equiv_2 0$$

Another example

$$f : \{0, 1\}^* \rightarrow \{0, 1\}$$

$$f(s) = 0 \Leftrightarrow wt(s) \equiv_2 0$$

Set: collection of objects

- Denoted by capital letters: A, B, X
- Objects in a set are called elements.
- Elements are denoted by lower case letters: a, b, x
- Curly braces around elements: $A = \{a_0, a_1, a_2\}$

Examples

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

$$B = \{p \mid p \text{ is a prime number}\}$$

No order and no count

A set doesn't maintain an order of its elements:

$$\begin{aligned}\{1, 2, 3\} &= \{1, 3, 2\} = \{2, 1, 3\} = \{2, 3, 1\} \\ &= \{3, 1, 2\} = \{3, 2, 1\}\end{aligned}$$

An object is either in the set or not:

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

Sets containing sets

Subsets

A is a subset of B if all the elements of A are in B .

$$A = \{1, 2, 3, 4\} \quad B = \{2, 3\} \quad B \subset A$$

Powersets

Some sets contain other sets as elements. The powerset of a set is the set containing all subsets of it:

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

$$\mathcal{P}(A) = \{\{\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Note A contains 3 elements and $\mathcal{P}(A)$ contains $2^3 = 8$.

Famous sets

\mathbb{N} – the natural numbers $\{1, 2, 3, \dots\}$.

\mathbb{N}_0 – the natural numbers with zero $\{0, 1, 2, 3, \dots\}$.

\mathbb{Z} – the integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

\mathbb{Q} – the rational numbers $\{\frac{m}{n} \mid m, n \in \mathbb{Z}\}$.

\mathbb{R} – the **real numbers**.

\mathbb{C} – the complex numbers $\{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$.

Tuples: finite list of elements taken from sets

$$t = (2, 1, 1) \quad t \in \mathbb{N} \times \mathbb{N} \times \mathbb{N} \quad |t| = 3$$

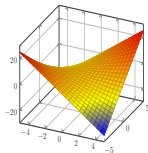
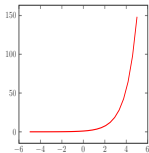
- Round brackets denote tuples, and t is a 3-tuple or a triple.
- Tuples have order, and can repeat elements.
- Sometimes we omit the brackets and commas: $t = 211$.
- $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is sometimes shortened to \mathbb{N}^3 .
- The first \mathbb{N} means the first element comes from \mathbb{N} .
- The second \mathbb{N} means the second element comes from \mathbb{N} , etc.
- Note that there is a single empty tuple: $()$.

Cartesian products of sets

$$A = \{1, 2, 3\} \quad B = \{x, y\}$$

$$A \times B = \{(1, x), (2, x), (3, x), (1, y), (2, y), (3, y)\}$$

- $A \times B$ is called the cartesian product of A and B – the set of tuples with first element from A and second from B .
- $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the usual 2D plane where we draw plots.
- Can extend to any length of tuple: \mathbb{R}^3 is the 3D plane.



Maps

Definition of map

A map from a set A to a set B is a subset M of $A \times B$ where each element of A appears as the first element of a tuple in M exactly once.

$$A = \{a, b, c\} \quad B = \{x, y, z\}$$

Maps

- $\{(a, x), (b, x), (c, x)\}$
- $\{(a, x), (b, y), (c, z)\}$

Not maps

- $\{(a, x), (a, y), (b, x), (c, x)\}$
- $\{(a, x), (b, y)\}$

Languages

Alphabet: finite set of symbols, denoted Σ .

String: tuple w over Σ .

Star: all strings over Σ , denoted Σ^* .

Language: subset L of Σ^* .

Length: of a string, denoted $|w|$.

Deciding PRIMES

Is there an algorithm that decides if an arbitrary natural number is a prime number?

Yes — there are many algorithms such as trial division.

```
for i in range(2, n):  
    if n % i == 0:  
        return False  
return True
```

Agrawal, Kayal and Saxena 2002 showed that PRIMES is in P.

An undecidable language

- Encode all Turing machines as strings over $\{0, 1\}$.
- Consider the subset of Turing machines that don't ever get stuck in an infinite loop irrespective of the input.
- This set is undecidable.

SAT

Example propositional formula: $(A \vee B) \wedge (\neg A \vee \neg C)$.

Variables: A, B, C, \dots – boolean.

Operations: AND (\wedge), OR (\vee), NOT (\neg).

Brackets: $()$.

A formula is satisfiable if there is any values for the variables that makes the formula True.

Boolean Satisfiability Problem (SAT): $\{w : w \text{ is satisfiable}\}$.

Turing machines recap

For a given input a Turing machine does one of three things:

Accepts the input string by finishing in the accept state in a finite number of steps.

Rejects the input string by finishing in the reject/fail state in a finite number of steps.

Continues indefinitely in some sort of infinite loop.

Remember there are a finite number of states and tape symbols.

Deciders

$$f : \Sigma^* \rightarrow \{q_f, q_a\}$$

Decider: a Turing machine that always finishes in a finite number of steps.

Decides: decides the language it accepts.

Decidable: a language is called decidable if any Turing machine decides it.

Important question: are all languages decidable?