"In mathematics you don't understand things. You just get used to them."
- John von Neumann

My alternate form:

"In mathematics it takes time for ideas and examples to sink in."

Course website:

Material: Standard 1- term into to CS Theory. The main point is that certain "problems":

1) are provably "unsolvable"
   e.g., the hatting problem is undecidable

2) may seem approachable, but no one knows how to solve them in polynomial time; if you could do so, then

   (1) \( P = NP \)  (2) You win \( 10^6 \) USD
   (minus applicable taxes)

   e.g.: SAT, 3SAT, 3COLOR, PARTITION, ...

We follow textbook [Sip] + handouts
Discussion! please post to piazza page.

If this fails, please email

To: jf@cs.ubc.ca

Subject: CPSC 421

or

Subject: CPSC 501

Grading:

421: \((10\%) \max(h, m, f) + (35\%) \max(m, f) + (55\%) f\) ,

\(h = \text{homework}, \ m = \text{midterm}, \ f = \text{final}\)

501: \((80\%) (\frac{421 \text{ grade}}{\text{grade}}) + (20\%) (\text{Presentation} + \text{Report})\)
Individual Homework: You must write up your own solution.

Group Homework: You can make a group submission, groups ≤ 4 people.

You will pass (50%) the course if on the final exam you can

1. Write a 100% correct DFA algorithm.
2. "..." Turing machine "..."

100% correct ⇒ you also explain how these algorithms work.
1st 2 weeks:

Uncomputability in CPSC 421/501

- Alphabets, strings, power set, languages, ...
- Cantor's Theorem constructs a "problem" for which there is no "algorithm"
- Proof of Cantor's theorem related to many "paradoxes"
- Halting problem is undecidable
- Use Python algorithms for now, later we use Turing machines
Terminology & Notation: \( \mathbb{R}, \mathbb{Z}, \mathbb{N} \)

\{ Alphabet, string, language, power set \( \Sigma, \Sigma^k, \Sigma^*, \text{Power}(\Sigma^*), \Sigma\text{ ASCII}, \Sigma\text{ digits} \}

PRIMES, PALINDROME, DIV-BY-3, ---

"Problem" = "Decision Problem" = "Language"

"Algorithms" expressed in Python

(or in C, in Javascript, in APL, as Turing machines, etc.)
\[ \mathbb{R} = \text{real numbers} \quad \mathbb{R} \]

\[ \mathbb{N} = \text{natural numbers} \quad \mathbb{N} \]

\[ \mathbb{Z} = \{ 1, 2, 3, \ldots \} \]

\[ \mathbb{Z}_{\geq 0} = \{ 0, 1, 2, \ldots \} \]

\[ \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \]

"Zahlen"

Alphabet: finite, non-empty set, often use \( \Sigma \)

\[ \Sigma_{\text{ASCII}} = 256 \text{ ASCII characters} \]
Often

\[ \Sigma = \{ a \} \]

or \[ \{ a, b \} \]

or \[ \Sigma \_{\text{Digits}} = \{ 0, 1, \ldots, 9 \} \]

Elements of an alphabet are symbols (letters)

\[ \Sigma^k = \Sigma \times \ldots \times \Sigma \]

\[ k \text{ copies} \]

\[ \Sigma = \{ a, b \}, \Sigma^2 \]
\[ \Sigma^2 = \{ (a,a), (a,b), (b,a), (b,b) \} \]

also:
\[ \{ aa, ab, ba, bb \} \]

aa is really \((a,a) \in \Sigma^2\)

\[ \Sigma^k \] strings of length \(k\)

\[ \Sigma^3 = \{ (a,a,a), (a,a,b), \ldots, (b,b,b) \} \]

= \{ aaa, eab, \ldots, bbb \}
$$\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma^k$$

E.g. \(\Sigma = \{a\}\)

$$\Sigma^* = \{a\}^*$$

\(= \{\varepsilon, a, aa, aaa, \ldots\}\)
\[\Sigma^2 \leftrightarrow \{\text{meps } \{1,2\} \rightarrow \Sigma\}\]

\[\Sigma^0 \leftrightarrow \{\text{meps } \emptyset \rightarrow \Sigma\}\]

\[\Sigma^0 = \{\varepsilon\} \text{ where } \varepsilon \text{ is the "empty string"}

\{a, b\}^*  

= \{\varepsilon, a, b, aa, ab, ba, bb, aaa, acb, \ldots, bbb, aaaa, \ldots \}
\[ \Sigma^5 \times \Sigma^7 \cong \Sigma^{12} \]

concatenation

\[ \Sigma^3 \times \Sigma^2 = \Sigma^5 \]

say \( \Sigma = \{a, b\} \)

\[
\begin{align*}
\text{abc} & \quad \text{b}b \\
\text{ababb} & \quad \text{ababb}
\end{align*}
\]

\[ \Sigma^0 \times \Sigma^2 = \Sigma^2 \]

\[
\begin{align*}
\Sigma & \quad \text{aa} \\
\Sigma & \quad \text{aaa} \\
= & \quad \text{aa}
\end{align*}
\]
\[ \Sigma^* = \text{set of strings over } \Sigma \]  

If \( S \) is a set, we use \( \text{Power}(S) \) to denote the set of all subsets of \( S \).

\[
S = \{1, 2\}
\]

\[
\text{Power}\{1, 2\} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}
\]
\[ \text{Power}(\{1,2,3\}) \]

\[ = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \} \]

\[ |\text{Power}(S)| = 2^{15} \]

if \( S \) is finite
Cantor's Theorem: If $S$ is a set, and function $f: S \rightarrow \text{Power}(S)$, then the image of $f$ is not all of $\text{Power}(S)$, specifically

$$T = \{ s \mid s \notin f(s) \}$$

is not in the image of $f$, i.e., there is no $t \in S$ s.t. $f(t) = T$. 
e.g. 

\[ f \]

1 \( \mapsto \) \{1, 2\}  

2 \( \mapsto \) \{1, 2, 3\}  

3 \( \mapsto \) \{1, 2\}  

1 \in f(1) = \{1, 2\}  

2 \in f(2) = \{1, 2, 3\}  

3 \notin f(3) = \{1, 2\}  

\[ T = \{ s \mid s \notin f(s) \} = \{3\} \]