Deduction

• Not in book

Show something is equivalent to a different problem

Prove that regular languages are closed under complementation

Let \( L \) be any regular language

So there exists a DFA that recognizes \( L \)

So there exists a string in the alphabet of \( \Sigma \)

So there exists a DFA that recognizes \( L \)

From a set of facts, deduce something that must be true

Closure Properties of Regular Languages

• Induction
• Construction
• Contradiction
• Deduction
Overview

• Deduction
• Construction
• Contradiction
• Induction
• Closure Properties of Regular Languages

How Much Detail?

• How is current line derived?
  - You can label each line and show what is used in deriving new lines
  - You don't have to be super detailed
    - Or spell out what happens if $n = 0$, then there are no $w_i$
    - If obvious, or just use the previous line, don't need to number them
    - You can label each line and show what is used in deriving new lines
    - How is current line derived?
Regular Languages Closed under Complementation

Let \( L \) be any regular language
Sufficient to show that \( \overline{L} \) is regular
Sufficient to show there exists a DFA that recognizes \( \overline{L} \)

Since \( L \) is regular, there exists a DFA that recognizes it. Call it \( M \)

Let \( M = (Q, \Sigma, \delta, q_0, F) \)

Construct DFA \( M' = (Q, \Sigma, \delta, q_0, F') \)
where \( F' = Q - F \)

Claim: \( L(M') = \overline{L} \)

Let \( w \in L \)
So \( M \) accepts \( w \)
Let \( q \) be the state that \( M \) is in at the end of processing \( w \)
So \( q \in F \).

So when \( M' \) processes \( w \), at the end of processing \( w \), it will also be in \( q \).
Let \( q' \in F' \), \( q' \neq q \)

Since \( q \) is in \( F \), \( q' \) is not in \( F' \), \( M' \) does not accept \( w \)
So \( w \not\in L(M') \)

Similarly, if \( w \in L(M') \)
then \( w \not\in L \)
So \( L(M') = \overline{L} \)
Overview

- Deduction
- Construction ⇒ Contradiction
- Induction
- Closure Properties of Regular Languages

How Much Detail?

- How much detail is needed?
  - Need to convince me that you know how to do the proof
  - Should be clear what you need to prove (and why)

- Do you need to show construction does as is intended?
  - Sometimes you can handwave
  - Should be clear when you need to prove (and why)

- How much detail is needed?
  - Notice the word ‘let’, as in ‘let x be’...
  - Sometimes you can handwave

So \( I = \langle M' \rangle I \) and if \( m \in I \) then \( I \not\in L \) and if \( m \not\in I \) then \( I \in L \). Could add:

Is the last line obvious enough?

- Notice the word ‘let’, as in ‘let x be’...
- Sometimes you can handwave

- Do you need to show construction does as is intended?
  - Sometimes you can handwave
  - Should be clear when you need to prove (and why)
Let $A = \{a^i b^i \mid i \geq 0\}$. Assume $A$ is regular. So there exists DFA $M$ such that $L(M) = A$.

Let $n$ be the number of states that $M$ has.

Let $s = a^n b^{n+1}$. Obviously $s \in L(M)$.

Let $r_0, \ldots, r_{2n+2}$ be the state sequence for accepting $s$.

Now consider the state sequence from $r_0$ to $r_n$ in which each $r_k$ on input $a$ transitions to $r_{k+1}$ for $k \leq n$ (i.e., $\delta(r_k, a) = r_{k+1}$).

Since $M$ just has $n$ states, there must be at least one duplicate to reach $r_{n+1}$ for $r_k$ in which each $r_k$ on input $a$ transitions.

Let $r_i$ and $r_{i+j}$ be duplicate states, with $j > 0$, so $r_i = r_{i+j}$.

Since $M$ can transition from $r_{i+j}$ to $r_{i+j+1}$ on $a$,

$r_i$ can transition to $r_{i+j+1}$ on $a$, since they are the same state.

So, we can cut out the intervening $j$ states and still have an accepting state sequence.

So, $r_0, \ldots, r_i, r_i+j+1, \ldots, r_{2n+2}$ is a valid state sequence and accepts $a^{n+j} b^{n+1}$. So $A$ is not regular.

Proof by Contradiction

• If you have to prove $X$ assume that $X$ is false, and show that you get a contradiction.

• Sometimes this is easier than trying to directly prove $X$. If you have to prove $X$,
Induction

• Prove that all Xs have a certain property where all Xs can be categorized in terms of some property $P$ based on the natural numbers, such as
  - number of states in a DFA
  - number of nodes in a graph
  - number of edges in a graph
  - some variable that is restricted to the natural numbers

• Break problem into a base case and an induction step
  - Base case: prove that $P(1)$ is true
  - Induction step: prove that if $P(i)$ is true for $i \geq 1$, then so is $P(i+1)$

• After proven both parts, you know that $P(i)$ must be true for $i \geq 1$.

• Prove that all Xs have a certain property where all Xs can be categorized in terms of some property $P$ based on the natural numbers.
Prove that \( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \) for \( n \geq 1 \).

Proof by Induction:

Base case: prove for \( n = 1 \)

\[ \text{LHS} = \sum_{i=1}^{n} i = 1 \]

\[ \text{RHS} = \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1 \]

Since LHS = RHS, true for base case

\( \ast \)

Continued

• Many variations of this:
  - Starting at a number other than 1
  - Needing to prove two base cases \( P(1) \) and \( P(2) \)
  - Needing to assume \( P(j) \) is true for all \( j \leq i \) in order to prove \( P(i+1) \)

- Stating at a number other than 1

(\( \star \))
Overview:

- Deduction
- Construction
- Contradiction
- Induction

⇒ Closure Properties of Regular Languages

---

Continued:

\[ \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \]

\[ \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2} \]

Since LHS = RHS, true for \( n + 1 \).

Induction Step: Assume it is true for \( n \), prove it is true for \( n + 1 \).
Proof Idea (continued)

Approach 1:
- We could have $M_1$ first simulate $M_1$ and then simulate $M_2$
- This won't work because in simulating $M_1$, we will have used up the input with $w$, and we won't be able to get it back

Approach 2:
- Simulate both $M_1$ and $M_2$ at the same time!
- Have the states of $M$ be the product of states of $M_1$ and $M_2$
- Have the transition function for $M$ on $w$ transition to the new state depending on what $M_1$ and $M_2$ would have individually done
- Have accepting states of $M$ be any state with an accepting state from $M_1$ or from $M_2$

Closed under Union

Definition of Union:
$$A \cup B = \{ x | x \in A \text{ or } x \in B \}$$
• What are the states of $M$ (draw them in a 3x2 array)?

• What are the transitions of $M$?
  - Take each state, like $a$, and each input, like 0, and ask:
    - Where does $M^1$ transition to from $a$ on 0? 
    - Where does $M^1$ transition to from $a$ on 0? 

Example Continued

Example

Let $\Sigma = \{0, 1\}$

Let $A^1$ be strings in which the number of 0's is divisible by 3
- Draw a state diagram for $M^1$ with 3 states: $a$, $b$, $c$
  - Draw the 3 states horizontally

Let $A^2$ be strings that have an even number of 1's
- Draw the 2 states vertically
  - Draw a state diagram for $M^1$ with 2 states: $d$, $e$

Let $A^3$ be strings that have an even number of $\{0, 1\}
- Draw the 3 states horizontally

Let $A^4$ be strings in which the number of 0's is divisible by 3
- Draw a state diagram for $M^1$ with 3 states: $a$, $b$, $c$
Other Operations

- Are regular languages closed under Intersection?
  \[ A \cap B = \{ x \mid x \in A \text{ and } x \in B \} \]

- Complementation?
  \[ A = \{ x \mid x \notin A \} \]

- Concatenation?
  \[ A \circ B = \{ xy \mid x \in A \text{ and } y \in B \} \]

- Star?
  \[ A^* = \{ x_1 x_2 \ldots x_k \mid k \geq 0 \text{ and each } x_i \in A \} \]

Formal Proof

Let \( M_1 \) recognize \( A_1 \) where
\[ M_1 = (Q_1, \Sigma, \delta_1, q_1, F_1) \]

Let \( M_2 \) recognize \( A_2 \) where
\[ M_2 = (Q_2, \Sigma, \delta_2, q_2, F_2) \]

Construct \( M \) to recognize \( A_1 \cup A_2 \) where \( M = (Q, \Sigma, \delta, q_0, F) \)

\( \delta \): Construct to recognize \( A_1 \cup A_2 \) where
\[ \delta' \]

\( q_0 \): Construct to recognize \( A_1 \cup A_2 \) where

\( F \): Construct to recognize \( A_1 \cup A_2 \) where

- Construct to recognize \( A_1 \cup A_2 \) where

- Construct to recognize \( A_1 \cup A_2 \) where

- Construct to recognize \( A_1 \cup A_2 \) where