Automata Theory
CS411 & CS675 2015F-01
Set Theory & Proof Techniques

David Galles

Department of Computer Science
University of San Francisco
01-0: Syllabus

- Office Hours
- Course Text
- Prerequisites
- Test Dates & Testing Policies
  - Check dates now!
- Grading Policies
01-1: How to Succeed

• Come to class. Pay attention. Ask questions.
How to Succeed

• Come to class. Pay attention. Ask questions.
  • A question as vague as “I don’t get it” is perfectly acceptable.
  • If you’re confused, at least 2 other people are, too.
How to Succeed

• Come to class. Pay attention. Ask questions.
  • A question as vague as “I don’t get it” is perfectly acceptable.
  • If you’re confused, at least 2 other people are, too.

• Come by my office
  • I am very available to students.
How to Succeed

- Come to class. Pay attention. Ask questions.
  - A question as vague as “I don’t get it” is perfectly acceptable.
  - If you’re confused, at least 2 other people are, too.
- Come by my office
  - I am very available to students.
- Start the homework assignments early
  - Homework in this class requires “thinking time”
01-5: How to Succeed

• Come to class. Pay attention. Ask questions.
  • A question as vague as “I don’t get it” is perfectly acceptable.
  • If you’re confused, at least 2 other people are, too.

• Come by my office
  • I am very available to students.

• Start the homework assignments early
  • Homework in this class requires “thinking time”

• Read the textbook.
  • Ask Questions! The textbook can be hard to follow – reading a dense, technical work is a “learning outcome” for this class
01-6: Class Goals

• Prove that there are some problems that cannot be solved

• Show that there are some problems that (are believed to) require an exponential amount of time to solve (NP-Complete)
  • Examine some strategies for dealing with these problems

• Along the way, learn how to model computation mathematically, and pick up some useful formalisms & techniques
  • DFA, regular expressions, CFGs, etc.
Most (but perhaps not all) of the following material is review from discrete mathematics.

I will go fairly fast, assuming it is review.

• Ask me to slow down if you have any questions!
A set is an unordered collection of objects

\[ S = \{a, b, c\} \]

\[ a, b, c \text{ are elements or members of the set } S \]
Sets – Definition

- A set is an unordered collection of objects
- \( S = \{a, b, c\} \)
  - \( a, b, c \) are elements or members of the set \( S \)
- Elements in a set need have no relation to each other
  - \( S_1 = \{1, 2, 3\} \)
  - \( S_2 = \{ \text{red, farmhouse, } \pi, -32 \} \)
01-10: Sets – Definition

- Sets can contain other sets as elements
  - $S_1 = \{3, \{3, 4\}, \{4, \{5, 6\}\}\}$
  - $S_2 = \{\{1, 2\}, \{\{4\}\}\}$
- Sets do not contain duplicates
  - NotASet = $\{4, 2, 4, 5\}$
01-11: Sets – Cardinality

• **Cardinality** of a set is the number of elements in the set
  
  • $|\{a, b, c\}| = 3$
  
  • $|\{\{a, b\}, c\}| = ?$
01-12: **Sets – Cardinality**

- **Cardinality** of a set is the number of elements in the set
  - $|\{a, b, c\}| = 3$
  - $|\{\{a, b\}, c\}| = 2$ (\{a, b\} and c)
01-13: Sets – Empty, Singleton

- **Empty Set:** \{\} or \emptyset, |\{\}| = |\emptyset| = 0
- **Singleton set** – set with one element
  - \{1\}
  - \{4\}
  - {} ?
  - {{}} ?
  - {{1}} ?
  - {{3, 1, 2}} ?
• Empty Set: $\{\}$ or $\emptyset$, $|\{\}| = |\emptyset| = 0$

• Singleton set – set with one element
  - $\{1\}$ Singleton
  - $\{4\}$ Singleton
  - $\{\}$ Not a Singleton (empty)
  - $\{\{}\}$ Singleton
  - $\{\{3, 1, 2\}\}$ Singleton
Set membership: \( x \in S \)
- \( 3 \in \{1, 3, 5\} \)
- \( a \not\in \{b, c, d\} \)
- \( 3 \in \{1, \{2, 3\}\} \) ?
- \( \{} \in \{1, 2, 3\} \) ?
- \( \{} \in \{1, \{}, 4\} \) ?
Set membership: $x \in S$

- $3 \in \{1, 3, 5\}$
- $a \notin \{b, c, d\}$
- $3 \notin \{1, \{2, 3\}\}$
- $\emptyset \notin \{1, 2, 3\}$
- $\emptyset \in \{1, \emptyset, 4\}$
Sets – Describing

- Referring to sets
  - List all members
    - \{3, 4, 5\}, \{0, 1, 2, 3, \ldots\}
  - \(S = \{x : x \text{ has a certain property}\}\)
  - \(S = \{x \mid x \text{ has a certain property}\}\)
  - \(S = \{x : x \in \mathbb{N} \land x < 10\}\)
    - \(\mathbb{N}\) is the set of natural numbers \{0, 1, 2, \ldots\}
  - \(S = \{x : x \text{ is prime}\}\)
  - \(A \cup B = \{x : x \in A \lor x \in B\}\)
  - \(A \cap B = \{x : x \in A \land x \in B\}\)
  - \(A - B = \{x : x \in A \land x \notin B\}\)
More Union & Intersection

- \( A \) and \( B \) are disjoint if \( A \cap B = \{\} \)
- \( S \) is a collection of sets (set of sets)
  \[ \bigcup S = \{ x : x \in A \text{ for some } A \in S \} \]
  \[ \bigcup \{\{1, 2\}, \{2, 3\}\} = \{1, 2, 3\} \]
  \[ \bigcap S = \{ x : x \in A \text{ for all } A \in S \} \]
  \[ \bigcap \{\{1, 2\}, \{2, 3\}\} = \{2\} \]
Subsets & Supersets

- \( A \) is a subset of \( B \), \( A \subseteq B \) if:
  - \( \forall x, x \in A \implies x \in B \)
  - \( \forall (x \in A), x \in B \)

- \( A \) is a proper subset of \( B \), \( A \subset B \) if:
  - \( A \subseteq B \land (\exists x, x \in B \land x \notin A) \)

- \{\} is a subset of any set (including itself)
- \{\} is the only set that does not have a proper subset
01-20: Sets – Power Set

- Power set: Set of all subsets
  
  \[ 2^S = \{ x : x \subseteq S \} \]
  
  - \[ 2^{\{a,b\}} = ? \]
  
  - \[ 2^{\{\}} = ? \]

- \[ |2^S| = ? \]
Power set: Set of all subsets

$2^S = \{x : x \subseteq S\}$

- $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $2^\emptyset = \{\emptyset\}$

$|2^S| = 2^{|S|}$
Π is a partition of $S$ if:

- $\Pi \subseteq 2^S$
- $\emptyset \notin \Pi$
- $\forall (X, Y \in \Pi), X \neq Y \implies X \cap Y = \emptyset$
- $\bigcup \Pi = S$

{{a, c}, {b, d, e}, {f}} is a partition of {a,b,c,d,e,f}

{{a, b, c, d, e, f}} is a partition of {a,b,c,d,e,f}

{{a, b, c}, {d, e, f}} is a partition of {a,b,c,d,e,f}
In other words, a partition of a set $S$ is just a division of the elements of $S$ into 1 or more groups.

- All the partitions of the set $\{a, b, c\}$?
In other words, a partition of a set $S$ is just a division of the elements of $S$ into 1 or more groups.

- All the partitions of the set \{a, b, c\}?
  - \{\{a, b, c\}\}, \{\{a, b\}, \{c\}\}, \{\{a, c\}, \{b\}\}, \{\{a\}, \{b, c\}\}, \{\{a\}, \{b\}, \{c\}\}
01-25: Ordered Pair

- \((x, y)\) is an ordered pair
- Order matters – \((x, y) \neq (y, x)\) if \(x \neq y\)
  - hence ordered
- \(x\) and \(y\) are the components of the ordered pair \((x, y)\)
$A \times B = \{(x, y) : x \in A \land y \in B\}$

- $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
- $\{1, 2\} \times \{1, 2\} = ?$
- $2\{a\} \times \{b\} = ?$
- $2\{a\} \times 2\{b\} = ?$
01-27: Cartesian Product

\[ A \times B = \{(x, y) : x \in A \land y \in B\} \]

- \[ \{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\} \]
- \[ \{1, 2\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2)\} \]
- \[ 2^\{\{a\}\} \times \{b\} = \{\{(a, b)\}, \{\}\}\} \]
- \[ 2^\{\{a\}\} \times 2^\{\{b\}\} = \{(\{a\}, \{b\}), (\{a\}, \{\}), (\{\}, \{b\}), (\{\}, \{\})\}\]
Which of the following is true:

- $\forall (A, B) \quad A \times B = B \times A$
- $\forall (A, B) \quad A \times B \neq B \times A$
- None of the above
Which of the following is true:

- \( \forall (A, B) \ A \times B = B \times A \)
  - If and only if \( A = B \)
- \( \forall (A, B) \ A \times B \neq B \times A \)
  - If and only if \( A \neq B \)
Why “Cartesian”? 
- Think “Cartesian Coordinates” (standard coordinate system)
- \( \mathbb{R} \times \mathbb{R} \) is the real plane
  - Set of all points \((x, y)\) where \(x, y \in \mathbb{R}\)
  - \(\mathbb{R}\) is the set of real numbers (think “floats” if you’re CS)
Can take the Cartesian product of $\geq 2$ sets.

$A \times B \times C = \{(x, y, z) : x \in A, y \in B, z \in C\}$

$\{a\} \times \{b, c\} \times \{d\} = \{(a, b, d), (a, c, d)\}$

(Technically, $A \times B \times C = (A \times B) \times C$)

$\{a\} \times \{b, c\} \times \{d\} = \{((a, b), d), ((a, c), d)\}$

Often drop the extra parentheses for readability
01-32: Relations

- A relation $R$ is a set of ordered pairs.
- For example, the relation $<$ over the Natural Numbers is the set:

\[
\{(0,1), (0,2), (0,3), ... \\
(1,2), (1,3), (1,4), ... \\
(2,3), (2,4), (2,5), ...
\}
\]
Often, relations are over the same set
  that is, a subset of $A \times A$ for some set $A$
Not all relations are over the same set, however
  Relation describing prices of computer components
  \{(Hard dive, $55), (WAP, $49), (2G DDR, $44), \ldots\}
A function is a special kind of relation (all functions are relations, but not all relations are functions)

A relation $R \subseteq A \times B$ is a function if:
- For each $a \in A$, there is exactly one ordered pair in $R$ with the first component $a$
01-35: Functions

- A function $f$ that is a subset of $A \times B$ is written: $f : A \rightarrow B$
  - $(a, b) \in f$ is written $f(a) = b$
  - $A$ is the domain of the function
  - if $A' \subseteq A$, $f(A') = \{b : a \in A' \land f(a) = b\}$ is the image of $A'$
  - The range of a function is the image of its domain
A function $f : A \mapsto B$ is:

- **one-to-one** if no two elements in $A$ match to the same element in $B$
- **onto** Each element in $B$ is mapped to by at least one element in $A$
- **a bijection** if it is both one-to-one and onto

The inverse of a binary relation $R \subset A \times B$ is denoted $R^{-1}$, and defined to be $\{(b, a) : (a, b) \in R\}$

- A function only has an inverse if ...
A function $f : A \mapsto B$ is:

- **one-to-one** if no two elements in $A$ match to the same element in $B$
- **onto** Each element in $B$ is mapped to by at least one element in $A$
- **a bijection** if it is both one-to-one and onto

The inverse of a binary relation $R \subset A \times B$ is denoted $R^{-1}$, and defined to be $\{(b, a) : (a, b) \in R\}$

- A function only has an inverse if it is a bijection
What if we want to take the inverse of a function that is not a bijection – what can we do?

- Want to preserve full information about the original function
- Resulting inverse must be an actual function
What if we want to take the inverse of a function that is not a bijection – what can we do?

- Want to preserve full information about the original function
- Resulting inverse must be an actual function
- How can we have an element map to 0, 1, or more elements, and still have a function? *HINT: If we modified the range* ...
What if we want to take the inverse of a function that is not a bijection – what can we do?

- Want to preserve full information about the original function
- Resulting inverse must be an actual function

\[ f : A \mapsto B \quad f^{-1} : B \mapsto 2^A \]

(example on chalkboard)
• $Q$ and $R$ are two relations
• The composition of $Q$ and $R$, $Q \circ R$ is:
  \[ \{(a, b) : (a, c) \in Q, (c, b) \in R \text{ for some } c\} \]

$Q = \{(a, c), (b, d), (c, a)\}$
$R = \{(a, c), (b, c), (c, a)\}$

$Q \circ R = \{(a, a), (c, c)\}$

$Q \circ Q \, ? \quad (Q \circ R) \circ Q \, ?$
01-42: Relation Graph

- Each element is a node in the graph
- If \((a, b) \in R\), then there is an edge from \(a\) to \(b\) in the graph

\[
R = \{(a, b), (a, c), (c, a), (b, b), (b, d)\}
\]

\[
\begin{array}{ccc}
a & \xrightarrow{\quad} & c \\
& \downarrow & \\
b & \xrightarrow{\quad} & d
\end{array}
\]
A relation \( R \subseteq A \times A \) is reflexive if:

1. \( (a, a) \in R \) for each \( a \in A \)
2. \( \forall (a \in A), (a, a) \in R \)
3. Each node has a self loop
A relation $R \subseteq A \times A$ is symmetric if

- $(a, b) \in R$ whenever $(b, a) \in R$
- $(a, b) \in R \implies (b, a) \in R$
- Every edge goes “both ways”
A relation \( R \subseteq A \times A \) is antisymmetric if

- whenever \((a, b) \in R\), \(a, b\) are distinct \((b, a) \notin R\)
- \((a, b) \in R \land a \neq b \implies (b, a) \notin R\)
- No edge goes “both ways”

Can a relation be neither symmetric nor antisymmetric?
A relation $R \subseteq A \times A$ is antisymmetric if
- whenever $(a, b) \in R$, $a$, $b$ are distinct $(b, a) \not\in R$
- $(a, b) \in R \land a \neq b \implies (b, a) \not\in R$
- No edge goes “both ways”

Can a relation be both symmetric and antisymmetric?

Antisymmetric  Not Antisymmetric
A relation $R \subseteq A \times A$ is transitive if

- whenever $(a, b) \in R$, and $(b, c) \in R$, $(a, c) \in R$
- $(a, b) \in R \land (b, c) \in R \implies (a, c) \in R$
- Every path of length 2 has a direct edge
A set $A \subseteq B$ is closed under a relation $R \subseteq ((B \times B) \times B)$ if:

- $a_1, a_2 \in A \land ((a_1, a_2), c) \in R \implies c \in A$
- That is, if $a_1$ and $a_2$ are both in $A$, and $((a_1, a_2), c)$ is in the relation, then $c$ is also in $A$

- $\mathbb{N}$ is closed under addition
- $\mathbb{N}$ is not closed under subtraction or division
Relations are also sets (of ordered pairs)

We can talk about a relation $R$ being closed over another relation $R'$

Each element of $R'$ is an ordered triple of ordered pairs!
01-50: Closure

• Relations are also sets (of ordered pairs)
• We can talk about a relation $R$ being closed over another relation $R'$
  • Each element of $R'$ is an ordered triple of ordered pairs!
• Example:
  • $R \subseteq A \times A$
  • $R' = \{(((a, b), (b, c)), (a, c)) : a, b, c \in A\}$
  • If $R$ is closed under $R'$, then . . .
01-51: Closure

- Relations are also sets (of ordered pairs)
- We can talk about a relation $R$ being closed over another relation $R'$
  - Each element of $R'$ is an ordered triple of ordered pairs!
- Example:
  - $R \subseteq A \times A$
  - $R' = \{(((a, b), (b, c)), (a, c)) : a, b, c \in A\}$
  - If $R$ is closed under $R'$, then $R$ is transitive!
01-52: **Closure**

- **Reflexive closure** of a relation $R \subseteq A \times A$ is the smallest possible superset of $R$ which is reflexive
  - Add self-loop to every node in relation
  - Add $(a,a)$ to $R$ for every $a \in A$

- **Transitive Closure** of a relation $R \subseteq A \times A$ is the smallest possible superset of $R$ which is transitive
  - Add direct link for every path of length 2.
  - $\forall (a, b, c \in A) \text{ if } (a, b) \in R \wedge (b, c) \in R \text{ add } (a, c) \text{ to } R.$

(examples on board)
Equivalence Relation
- Symmetric, Transitive, Reflexive

Examples:
- Equality (=)
- $A$ is the set of English words, $(w_1, w_2) \in R$ if $w_1$ and $w_2$ start with the same letter

(example graphs)
Equivalence Relation
  • Symmetric, Transitive, Reflexive
Separates set into equivalence classes (all words that start with a, for example)
If $a \in A$, then $[a]$ represents equivalence class that contains $a$. 
Relation Types

- Partial Order
  - Antisymmetric, Transitive, Reflexive
- Examples:
  - $\leq$ for integers
    - $A$ is the set of integers, $(a, b) \in R$ if $a \leq b$
  - Ancestor
    - $R \subseteq A \times A = \{(x, y) : x$ is an ancestor of $y,$
or $x = y\}$

(example graphs)
Total Order

- $R \subseteq A \times A$ is a total order if:
  - $R$ is a partial order
  - For all $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$

- Is $\leq$ a total order?
- Is Ancestor a total order?

(example graphs)
How can we tell if two sets $A$ and $B$ have the same cardinality?
How can we tell if two sets $A$ and $B$ have the same cardinality?

- Calculate $|A|$ and $|B|$, make sure numbers are the same.
- Match each element in $A$ to an element in $B$.
  - Create a bijection $f : A \mapsto B$ (or $f : B \mapsto A$).
What about infinite sets? Are they all equinumerous (that is, have the same cardinality)?

A set is countable infinite (or just countable) if it is equinumerous with \( \mathbb{N} \).
A set is countable infinite (or just countable) if it is equinumerous with $\mathbb{N}$.

- Even elements of $\mathbb{N}$?
A set is countable infinite (or just countable) if it is equinumerous with $\mathbb{N}$.
- Even elements of $\mathbb{N}$?
- $f(x) = 2x$
A set is countable infinite (or just countable) if it is equinumerous with $\mathbb{N}$.

- Integers ($\mathbb{Z}$)?
A set is countable infinite (or just countable) if it is equinumerous with $\mathbb{N}$.

- Integers ($\mathbb{Z}$)?
- $f(x) = \left\lfloor \frac{x}{2} \right\rfloor \times (-1)^x$
A set is countable infinite (or just countable) if it is equinumerous with $\mathbb{N}$.

Union of 3 (disjoint) countable sets $A$, $B$, $C$?
A set is countable infinite (or just countable) if it is equinumerous with \( \mathbb{N} \).

- Union of 3 (disjoint) countable sets \( A, B, C \)?

\[
\begin{align*}
    a_0 & \quad a_1 & \quad a_2 & \quad a_3 & \quad a_4 & \quad \ldots \\
    b_0 & \quad b_1 & \quad b_2 & \quad b_3 & \quad b_4 & \quad \ldots \\
    c_0 & \quad c_1 & \quad c_2 & \quad c_3 & \quad c_4 & \quad \ldots
\end{align*}
\]

- \( f(x) = \begin{cases} 
    a \frac{x}{3} & \text{if } x \mod 3 = 0 \\
    b \frac{x-1}{3} & \text{if } x \mod 3 = 1 \\
    c \frac{x-2}{3} & \text{if } x \mod 3 = 2
\end{cases} \)
A set is **countable infinite** (or just **countable**) if it is equinumerous with $\mathbb{N}$.

- $\mathbb{N} \times \mathbb{N} = \{(0,0), (0,1), (0,2), (0,3), (0,4), \ldots \}$
- $\ldots$
- $\{(4,0), (4,1), (4,2), (4,3), (4,4), \ldots \}$
- $\ldots$
- $\ldots$
A set is countable infinite (or just countable) if it is equinumerous with \( \mathbb{N} \).

\[ \mathbb{N} \times \mathbb{N} ? \]

\[
\begin{array}{ccccccc}
(0,0) & (0,1) & (0,2) & (0,3) & (0,4) & \ldots \\
(1,0) & (1,1) & (1,2) & (1,3) & (1,4) & \ldots \\
(2,0) & (2,1) & (2,2) & (2,3) & (2,4) & \ldots \\
(3,0) & (3,1) & (3,2) & (3,3) & (3,4) & \ldots \\
(4,0) & (4,1) & (4,2) & (4,3) & (4,4) & \ldots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
\end{array}
\]

\[ f((x, y)) = \frac{(x+y)(x+y+1)}{2} + x \]
A set is **countable infinite** (or just **countable**) if it is equinumerous with $\mathbb{N}$.

- Real numbers between 0 and 1 (exclusive)?
Proof by contradiction

Assume that \( R \) between 0 and 1 (exclusive) is countable

- (that is, assume that there is some bijection from \( \mathbb{N} \) to \( R \) between 0 and 1)

Show that this leads to a contradiction

- Find some element of \( R \) between 0 and 1 that is not mapped to by any element in \( \mathbb{N} \)
01-70: **Uncountable** $\mathbb{R}$

- Assume that there is some bijection from $\mathbb{N}$ to $\mathbb{R}$ between 0 and 1

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.3412315569...</td>
</tr>
<tr>
<td>1</td>
<td>0.0123506541...</td>
</tr>
<tr>
<td>2</td>
<td>0.1143216751...</td>
</tr>
<tr>
<td>3</td>
<td>0.2839143215...</td>
</tr>
<tr>
<td>4</td>
<td>0.2311459412...</td>
</tr>
<tr>
<td>5</td>
<td>0.8381441234...</td>
</tr>
<tr>
<td>6</td>
<td>0.7415296413...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Assume that there is some bijection from $\mathbb{N}$ to $\mathbb{R}$ between 0 and 1

Consider: 0.425055...
01-72: **Proof Techniques**

- Three basic proof techniques used in this class
  - Induction
  - Diagonalization
  - Pigeonhole Principle
Induction

Can create exact postage for any amount $\geq 0.08$ using only 3 cent and 5 cent stamps
**Induction**

Can create exact postage for any amount $\geq$ $0.08$ using only 3 cent and 5 cent stamps

- **Base case**

  Can create postage for 0.08 using one 5-cent and one 3-cent stamp
Can create exact postage for any amount $\geq 0.08$ using only 3 cent and 5 cent stamps

- Inductive case
  - To show: if we can create exact postage for $x$ using only 3-cent and 5-cent stamps, we can create exact postage for $x + 0.01$ using 3-cent and 5-cent stamps
- Two cases:
  - Exact postage for $x$ uses at least one 5-cent stamp
  - Exact postage for $x$ uses no 5-cent stamps
To show: if we can create exact postage for $x using only 3-cent and 5-cent stamps, we can create exact postage for $x + $0.01 using 3-cent and 5-cent stamps

- Exact postage for $x uses at least one 5-cent stamp
  - Replace a 5-cent stamp with two 3-cent stamps to get $x + $0.01

- Exact postage for $x uses no 5-cent stamps
  - Replace three 3-cent stamps with two 5-cent stamps to get $ + $0.01
Pigeonhole Principle

- $A, B$ are finite sets, with $|A| > |B|$, then there is no one-to-one function from $A$ to $B$

- If you have $n$ pigeonholes, and $> n$ pigeons, and every pigeon is in a pigeonhole, there must be at least one hole with $> 1$ pigeon.
01-78: Pigeonhole Principle

• Show that in a relation $R$ over a set $A$, if there is a path from $a_i$ to $a_j$ in $R$, then there is a path from $a$ to $b$ whose length is at most $|A|$.
Proof by Contradiction

- Assume that there exists some shortest path from $a_i$ to $a_j$ of length $>|A|$.
- By pigeonhole principle, some element must repeat:
  - $\{a_i, \ldots, a_k, \ldots, a_k \ldots a_j\}$
- We can create a shorter path by removing elements between $a_k$'s.
- We’ve just found a shorter path from $a_i$ to $a_j$ — a contradiction.