Theory of Computation
CS3102 – Spring 2014
A tale of computers, math, problem solving, life, love and tragic death

Nathan Brunelle
Department of
Computer Science
University of Virginia

www.cs.virginia.edu/~njb2b/theory
Binary Relations

• Mondays 7pm-10pm
  • Olsson 005
• Course reddit
  • www.reddit.com/r/cs3102
• New TA: Saba Eskandarian
  • Office Hours: Tues/Thurs 3:30pm-4:30pm
  • Thornton Stacks
Binary Relations

• A relation between sets $S$ and $T$ is a subset of $S \times T$
  • consider the relation “x has eaten y for dinner”
  • $P = \{\text{all people}\}$, $F = \{\text{all food}\}$
  • To say “Nathan has eaten ice cream for dinner”
    • $(\text{Nathan}, \text{ice cream})$
    • Nathan ~ ice cream
  • Without loss of generality we can assume $S = T$
    • Why?
    • If $S \neq T$ the let $A = S \cup T$
Binary Relations

• Without loss of generality we can assume $S = T$
• If $S \neq T$ the let $A = S \cup T$
Binary Relations - Properties

• A relation \( \sim \) is reflexive if:
  • \( \forall x \in A \ x \sim x \)

• Is symmetric if:
  • \( \forall x, y \in A \ x \sim y \Rightarrow y \sim x \)

• Is transitive if:
  • \( \forall x, y, z \in A \ x \sim y \land y \sim z \Rightarrow x \sim z \)

• Is called an equivalence relation if:
  • It’s reflexive, symmetric, and transitive
Binary Relations

1. Can a relation be reflexive and symmetric but not transitive?
   - Yes! Consider the relation “Has eaten a meal with”

2. Can a relation be reflexive and transitive but not symmetric?
   - Yes! Consider the relation “Is the boss of”

3. Can a relation be symmetric and transitive but not reflexive?
   - Tricky....
Binary Relations

Can a relation be symmetric and transitive but not reflexive?

Incorrect proof:

Consider some relation \( \sim \) which is symmetric and transitive. Consider now a pair of elements \( x, y \). Since \( x \sim y \) and the relation is symmetric we know that \( y \sim x \). Since the relation is transitive we may therefore conclude that \( x \sim x \).

Why is this incorrect?
Binary Relations

Can a relation be symmetric and transitive but not reflexive?

Incorrect proof:

Consider some relation \( \sim \) which is symmetric and transitive. Consider now a pair of elements \( x, y \). Since \( x \sim y \) and the relation is symmetric we know that \( y \sim x \). Since the relation is transitive we may therefore conclude that \( x \sim x \).

This shows: if \( \sim \) is symmetric and transitive and each term participates in at least 1 relation then \( \sim \) is reflexive.

Consider the relation “voted for the same candidate as”
Binary Relations

• \(x, y\) both vote for George Washington
• So, “\(x\) voted for the same candidate as \(y\)”
• If “\(y\) voted for the same candidate as \(z\)” then \(z\) voted for George Washington, so “\(x\) voted for the same candidate as \(z\)”
• Thus this is both symmetric and transitive.
• What if \(w\) didn’t vote?
• \(w\) does not participate in any relation, so “\(w\) voted for the same candidate as \(w\)” is not a valid relation, i.e., \((w, w)\) is not valid
Binary Relations - Closure

- Add in those terms which give the relation a certain property
  - Consider \( R=\{(1, 2), (1,1), (3, 2), (2, 4)\} \)
  - Reflexive closure: \( r(R) \)
    \[ \{(1, 2), (1,1), (3, 2), (2, 4), (2, 2), (3, 3), (4, 4)\} \]
  - Symmetric closure: \( s(R) \)
    \[ \{(1, 2), (1,1), (3, 2), (2, 4), (2, 1), (2, 3), (4, 2)\} \]
  - Transitive closure: \( t(R) \)
    \[ \{(1, 2), (1,1), (3, 2), (2, 4), (1,4), (3,4)\} \]
Binary Relations - Closure

- Exercise:
  - Consider the relation $R = \{(x, x + 1) | x \in \mathbb{Z}\}$
  - Find the transitive closure of $R$, $t(R)$
    - $<$
  - Find the reflexive transitive closure of $R$, $r(t(R))$
    - $\leq$
  - Find the symmetric transitive closure of $R$, $s(t(R))$
    - $\neq$
Example Equivalence Relation

- Show that $\mathbb{Z}_m = \{ (x, y) \in \mathbb{Z}^2 | x \equiv y \mod m \}$ is an equiv. relation
- Helpful: $x \equiv y \mod m \iff m|(x - y)$
  - Reflexive: $x \equiv x \mod m$
    
    Proof: $m|(x - x)$ since $m|0$
  - Symmetric: $x \equiv y \mod m \Rightarrow y \equiv x \mod m$
    
    Proof: $m|(x - y) \Rightarrow \exists k \ s.t. \ km = (x - y)$
    
    $\Rightarrow (-k)m = (y - x) \Rightarrow m|(y - x)$
  - Transitive: $x \equiv y \mod m \land y \equiv z \mod m \Rightarrow x \equiv z \mod m$
    
    Proof: $m|(x - y) \land m|(y - z) \Rightarrow$
    
    $\exists j, k \in \mathbb{Z} \ s.t. \ x - y = jm \land y - z = km \Rightarrow$
    
    $(x - y) + (y - z) = (j + k)m \Rightarrow m|(x - z)$
Equivalence Classes

- Let R be an equivalence relation over set A
- \([a]_R = \{s \in A \mid (a, s) \in R\}\)
- \(a\) is the representative of \([a]_R\)
- Any term in \([a]_R\) can be the representative
- Give some terms in \([3]_5 = \{x \in \mathbb{Z} \mid 3 \equiv x \, \text{mod} \, 5\}\)
  - 3, 8, 13, -2, -7
Problem: Prove that there are an infinity of primes.

Extra Credit: Find a short, induction-free proof.
Assume FSORC that there is a largest prime $p$.
Now consider $N = p! + 1$, since $N > p$ we know $N$ must be composite. This means there is some prime $q$ which divides $N$.
However $q$ cannot be any number less than $p$ since $1 \equiv N \mod q$ for any such $q$. This contradicts the assumption that there was a largest prime.
**Problem**: True or false: there arbitrary long blocks of consecutive composite integers.

**Extra Credit**: find a short, induction-free proof.

Consider the value $k + n!$ if $k < n$ then we know that this value is composite. Why?

$$n! = n \cdot (n - 1) \cdot \ldots \cdot k \cdot \ldots \cdot 2 \cdot 1$$

Thus

$$k + n! = k \cdot \left(\frac{n!}{k} + 1\right)$$

This means that for any value $n$ all integers in the interval $[n!, n - 1 + n!]$ form a block of $n$ consecutive composite integers