Program Verification & Testing; Review of Propositional Logic

CS 536: Science of Programming, Fall 2019

A. Why

- Course guidelines are important.
- Active learning is the style we'll be using in the class.
- Understanding what Science of Programming is is important.
- Reviewing/overviewing logic is necessary because we'll be using it in the course.

B. Outcomes

At the end of this lecture, you should

- Know how the course will be structured and graded.
- Have practiced some of the techniques we'll be using in class.
- Know what Science of Programming is about and how it differs from and is related to program testing.
- Understand what a propositional formula is, how to write them, how to tell whether one is a tautology or contradiction using truth tables, and see a basic set of logical rules for transforming propositions.

C. Introduction and Welcome

- The course webpages for Fall 2019 are at http://cs.iit.edu/~cs536/
- There you'll find schedules of lectures, coursework, and tests. Also included is information on how the final grade is calculated and the disability and academic honesty policies, etc. You're responsible for this info even if you don't read it.
- Be sure to study how tests work (**closed notes**) and how a higher score on the Final Exam can supersede earlier lower scores on Exams 1 and 2.
- We'll use Piazza for group discussions. (If you haven't gotten an invitation to join Piazza, let me know.)
- We'll use myIIT → Blackboard for submitting homework and viewing grades.

D. Course Prerequisite: Basic Logic

- The course prerequisite formally is CS 401. In reality, what you need is some background in boolean logic (propositions and predicates) and some comfort in syntactic operations and formal languages.
- For a very rough assessment of your preparedness for this course, study the following questions: If you get all 5 correct, you have more than enough background for this course;. If you get 3 correct, you're probably okay but will need to brush up. If you get none correct, I recommend you drop this course as soon as possible.
  1. Are 2+2 and 4 syntactically equal and why?
  2. If AND higher precedence than OR and OR is left associative, how do you parenthesize V AND W OR X OR Y?

3. If φ and ψ are propositions then what are the contrapositive, converse, and inverse of the implication $\varphi \rightarrow \psi$ and how are they related?
4. How do you pronounce $(\neg \forall x \in \mathbb{Z} \,.\, \exists y \in \mathbb{Z} \,.\, y^2 < x)$ in English, and is it true?
5. What's the difference between saying that a predicate φ is true vs saying that you have a (mechanically checkable) proof of φ?*

- We'll quickly review basic logic in class. If you want other references to study, try
  - Chapter 13 of Discrete Structures (4th edition) by Satinder Bal Gupta and C.P. Gandhi © 2015, ISBN 9789380386355 (free for students, via myIIT → library e-resources > B > Books 24x7 > Search ...)
  - Discrete Structures, Logic, and Computability, (2nd ed), by James L. Hein, © 2002, Jones and Bartlett, ISBN 9780763718435 (free for students, via myIIT → library e-resources library e-resources > B > Books 24x7 > Search...) Note this author uses non-CS precedences and associativities.

E. Active Learning

- Education research shows that students learn better when they are active participants in class, compared to passive listeners of lectures.
- This active kind of learning includes obvious things like answering questions in class, but it also includes in-class activities and quick feedback to the instructor.
- You'll need to put more effort into class, but you'll learn more/better/faster.

F. So What Is Science of Programming Anyway?

- Science of Programming is about **program verification**.
- Program verification aims to get reliable programs by proving properties about programs.
  - Harder to do this by writing programs and then proving them correct.
  - In practice, it's better to reason about programs as we write them.
- Distinguish program verification from program testing.
  - In testing, we run a program and verify that it behaves correctly.

G. Neither Reasoning or Testing is Completely Sufficient

- We need both testing and reasoning; neither is always better than the other. Reasoning about a program can generalize an infinite set of test cases, but testing gives us a reality check to show that our reasoning is sound. Good testing uses reasoning to identify a good set of test cases. E.g.,, say our specification is "If $z \geq c$ before the program, then $z > c$ after it", where the program is just "add `x` to `z`, but only if `x` is nonnegative."
- In C, we can write `/* z >= c */ if (x >= 0) z = z+x; else ++z; /* z > c */`
- To figure out which test cases are good, we reason about how the statements and properties interact.

---

* Answers: (1) No, because operator expressions aren't constants. (2) ((V AND W) OR X) OR Y. (3) Contra-positive: $\neg\psi \rightarrow \neg\varphi$; Converse: $\psi \rightarrow \varphi$; Inverse: $\neg\varphi \rightarrow \neg\psi$? An implication and its contrapositive are semantically equivalent, as are the converse and inverse, but an implication and its converse are not. (4) "It's not the case that for every integer x, there exists an integer y such that y squared is less than x." It's true (try x = 0). (5) "φ is true" is a semantic claim; "… is a proof of p" is a syntactic claim.

- E.g., take `x ≥ 0` (and its negation `x < 0`) and break up ≥ into separate > and = cases (`x > 0`, `x = 0`), to get `x < 0`, `x = 0`, and `x > 0` as the general set of cases. If we think `x = -1` and 1 are good enough generalizations of `x < 0` and `x > 0`, then we're done: Our test cases are `x = -1`, `x = 0`, `x = 1`.
- If we decide we want to be more thorough and treat `x = -1` and `x < -1` as different cases (and `x > 1` similarly), we can turn them into `x = -2` and `x = 2`, and end up with five test cases, `x = -2`, `x = -1`, `x = 0`, `x = 1`, `x = 2`.
- Of course, if we keep breaking edge cases off of the < and > tests, we could get `x = -3` and `x = 3`, then `x = -4` and `x = 4`, and so on to infinity. A big part of testing is figuring when to stop doing all this.

H. Type-Checking as a Kind of Program Verification

- **Static** (i.e., compile-time) **type-checking** is an example of program verification: We analyze a program textually to reason about how it uses types, to check for type-correctness.
- The reasoning is symbolic / textual because we aren't actually running the program, so a type-checker is a mechanical theorem prover for judgements of the form "this variable or expression has type …" and "This operation is type-correct."
  - E.g., if variables `x` and `y` are of type integer, then `x+1` and `x/y` are integers, so `x+1 = x/y` is type-correct, etc. (Note `x/y` might still cause a runtime error, but it's wouldn't be a type error.)
- A **strong type-checker** produces proofs that provide complete evidence for type safety. A **weak type-checker** produces proofs that provide only partial evidence for type safety.
  - E.g., type-checkers for Haskell or Standard ML are very strong; they guarantee type safety. (Note: You might still get runtime errors, but not for type-incorrect operations.)
  - However, type-checkers for C are weak; they have to assume you know what you're doing when you cast pointers.

I. Reasoning About One State of Memory vs Many States of Memory

- In testing, we have a finite number of specific values we use for our variables. We can verify that our program works with those specific values.
- In program verification we aim to say that our programs work in all possible cases. Typically, we have an infinite number of cases[†]. (Actually, it's a finite number, since memory is finite, but who wants to deal with, e.g., 2^{32} separate individual tests for an integer variable `x`?)
- In program verification, we use **predicates** like `x > 0` to stand for a possibly infinite number of values. (A predicate is a syntactic object that has a truth value once you plug in specific values for its variables.)
- Using predicates, we can talk about an infinite number of possible execution paths simultaneously. Instead of actually executing a program, we simulate its execution symbolically, using rules of logic to manipulate our predicates. "If `x > 0`, then after adding 1 to `x`, we have `x > 1`" stands for an infinite number of execution paths.

[†] Actually, it's probably a finite number of cases but still so many that "infinity" is a decent generalization.

- **That's what program verification is**: Instead of actually executing a program on one set of inputs to get one set of outputs, we simulate execution on sets of states using reasoning on predicates. We describe a set of input states using a logical predicate and reason about the possible output states using rules of logic plus rules for program execution.
- So to do program verification we need predicates to describe sets of memory states, rules of logic to reason about predicates, plus rules for how our programs execute (i.e., how they take and modify memory states).

J. Logic Review/Overview, Part 1: Propositional Logic

- If you weren't a CS major as an undergrad and haven't seen propositional and predicate logic before, you should study up on it (see **Course Prerequisites: Basic Logic** on page 2.)
- **Propositional logic** is logic over **proposition variables**, which are just variables that can have the values true or false. In propositional logic we study the logical connectives and (∧), or (∨), not (¬), implication (→), and biconditional (↔) operating over variables that have true or false as their values. In computer science terms, propositional logic is the logic used for boolean expressions: True and false are boolean constants, and the connectives are boolean operators (in C, ∧, ∨, ¬, and ↔ are written `&&`, `||`, `!`, and ==).
- **Notation**: Typically we'll use p, q, … for preposition variables and T, F for true and false. We'll use φ, ψ, … for propositions.

Terminology

- φ ∧ ψ is the **conjunction** or **logical and** of φ and ψ. φ and ψ are **conjuncts** of φ ∧ ψ.
- φ ∨ ψ is the **disjunction** or **logical or** of φ and ψ. φ and ψ are **disjuncts** of φ ∨ ψ.
- φ → ψ is the **implication** or **conditional** of φ and ψ. φ is the **antecedent** or **hypothesis** and ψ is the **consequent** or **conclusion**.

Other Ways to Phrase Implications

- Other phrasings of φ → ψ*:* "**if** φ **then** ψ"; "φ is **sufficient for** ψ"; "φ **only if** ψ"
- Other phrasings of ψ → φ*:* φ ← ψ , "φ is **necessary for** ψ"; "φ **if** ψ"; "**if** ψ **then** φ", "ψ **only if** φ".

Biconditional

- φ ↔ ψ is the **equivalence** or **biconditional** of φ and ψ; they are both true or both false. φ is the **antecedent** or **hypothesis** and ψ is the **consequent** or **conclusion**.
- Note ↔ is not the same as "equivalence" in the sense that "φ is equivalent to ψ, which is equivalent to χ, so φ is equivalent to χ". For two items, φ ↔ ψ is true exactly when φ and ψ are both true or both false, so e.g., F ↔ F evaluates to T. But for three items, ↔ doesn't behave as you might expect: Since F ↔ F evaluates to T, we can substitute it for the first T in T ↔ T and get that (F ↔ F) ↔ T evaluates to T.
- The kind of equivalence where "φ is equivalent to ψ, and ψ is equivalent to χ, so φ is equivalent to χ" is called "logical equivalence" and it's related to ↔ but not exactly the same. We'll look at it in a bit.

Precedences and Associativities for Propositional Operators

- **Precedences**: For the precedences of propositional operators, let's use ¬, ∧, ∨, →, ↔ (going from strong to weak). E.g., $((((\neg p) \wedge q) \vee r) \rightarrow s) \leftrightarrow t$ means $\neg p \wedge q \vee r \rightarrow s \leftrightarrow t$. E.g., we'll take $p \rightarrow q \leftrightarrow p \vee \neg q$ to mean

$(p \to q) \leftrightarrow (p \vee \neg q)$. This is pretty standard except sometimes people take $\to$ and $\leftrightarrow$ as having the same precedence.

- **Associativity**: $\wedge$ and $\vee$ are associative, so $((p \wedge q) \wedge r) \equiv (p \wedge (q \wedge r))$. Let's make these operators left associative, so the full parenthesization of $p \wedge q \wedge r$ will be $((p \wedge q) \wedge r)$.
- Implication is not associative; we'll take it to be right associative.
  - To see non-associativity, compare ((F → T) → F) and (F → (T → F)).
  - Right associativity tells us that φ → ψ → χ means (φ → (ψ → χ)).
- For the biconditional (↔), we'll use right associativity: φ ↔ ψ ↔ χ means (φ ↔ (ψ ↔ χ)).
  - Note φ ↔ ψ evaluates to T if φ and ψ evaluate to the same value, T or F.
  - On the other hand, φ ↔ ψ ↔ χ means (φ ↔ (ψ ↔ χ)), which leads to possibly-puzzling properties like T ↔ T↔ T means (T ↔ (F ↔ F)), which evaluates to true.

Semantic Equality

- **Semantic equality** is equality of meanings or results. This is usually what we mean when we write "=": $2+2 = 4$, $a+b = b+a$
- For propositions, we'll use ⇔ to indicate semantic equality. (This is the "logical equivalence" we'll discuss in a bit.)
  - Example: You can distribute ∨ over ∧: $(p \wedge q) \vee r \Leftrightarrow (p \vee r) \wedge (q \vee r)$
- For propositions, where we have only the values T and F (and only boolean variables), semantic equality can be mechanically determined (though for propositions, it can take time exponential in the number of basic variables).
- Later, with predicates, semantic equality can be impractical or even impossible to determine, so we usually fall back on a property that's easier to determine, namely, syntactic equality.

Syntactic Equality

- **Syntactic equality** (written ≡) means equality as structured text: Two expressions or propositions are syntactically equal if they are textually identical — with one exception: We'll ignore redundant parentheses. E.g., `(1*2)+3` ≡ `1*2+3`. We'll use ≢ for syntactic inequality. E.g., `2+2` ≢ `4`.
- We'll consider three kinds of redundancy for parentheses:
  - **Precedence**: $(p \wedge q) \vee r \equiv p \wedge q \vee r$ because "∧" has higher precedence than "∨".
  - **Left or Right Associativity**: $a - b - c \equiv (a - b) - c$ because "–" is left associative. Similarly, $p \to q \to r \equiv p \to (q \to r)$ because "→" is right associative.
  - **Associative Operators**: For an associative operator, all parenthesizations will be syntactically equal. E.g., $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$. But $(a - b) - c \not\equiv a - (b - c)$ because "–" is not associative.
  - We are not going to take commutativity of operators into account, so $p \wedge q \not\equiv q \wedge p$. Of course, they evaluate to the same truth value, so we can see that syntactically unequal items can stand for the same value. (Leaving out commutativity makes "≡" easier to calculate. Without commutativity, the *non-parenthesis symbols* of two ≡ items have to appear in the same order. E.g., no parenthesizations of 1+3+2 and 1+2+3 make them ≡.

- What about operator pairs like * and / or + and – where the members of the pair have equal precedence and one of the pair (but not both) are associative. In particular, do we want (x * (y / z)) ≡ ((x * y) / z) or (x + (y – z)) ≡ ((x + y) – z)? It turns out we'll take each pair to be ≢, but the justification has to do with how syntactic and semantic equality are related, so we'll put off the explanation for a bit.

Syntactic Equality Versus Semantic Equality

- **Why Use Syntactic Equality?** We often want to know whether two items are semantically equal, but depending on the kind of item, semantic equality can be hard or even impossible to calculate. Syntactic equality is easy to calculate, and if we define ≡ carefully, then we can guarantee that if two items are ≡, then they're semantically =. In other words, we use syntactic equality to be a rough approximation of semantic equality — "rough' because two items can be ≢ but =.
- **Syntactic Equality Implies Semantic Equality**: Keeping this property in mind makes it easy to see why we can ignore redundant parentheses when determining ≡ because preserving = is what makes parentheses redundant. E.g., 1+2*3 ≡ (1+(2*3)), so they stand for the same value. Since "≡ implies =" is true, the contrapositive "≠ implies ≢" is also true. E.g., 2+2 ≠ 5, so 2+2 ≢ 5.
- **Semantic Equality Does Not Imply Syntactic Equality**: A separate question from "≡ implies =" is the converse: Does = imply ≡? It's easy to find examples where two expressions are = but not ≢. E.g., 2 + 2 ≢ 4. Similarly, $a + 0 \neq a$ and $p \wedge q \not\equiv q \wedge p$.
- **Back to mixing * and / (or + and –)**: Now let's go back to the question of "Should (x * (y / z)) ≡ or ≢ ((x * y) / z)?" On integers, the two expressions are not = because of truncation: (2 * (2 / 4)) = 2 * 0 = 0 but (2 * 2) / 4 = 4 / 4 = 1. On the other hand, on infinite precision reals, the two expressions are =. So the question of = or ≠ depends on the types of x, y, and z. Having to take the types of x, y, and z into consideration for determining ≡ or ≢ would make things more complicated, so it seems better to take our pair of expressions to be ≢. More generally, we can say that if we have two operators that have the same precedence and are both associative, then it's okay to treat them as being associative.

Parenthesizations

- The **minimal parenthesization** of a syntactic item is the one with the fewest parentheses that preserves ≡. (I.e., it is still ≡ to the original.)
- For associative operators, let's omit parentheses inside sequences like $p \wedge q \wedge r$. We may still need them around the whole proposition, as in $p_1 \wedge (q_1 \vee q_2 \vee q_3)$
- The **full parenthesization** of an item is the one that preserves ≡ and also includes parentheses around each operator expression (i.e., (*op p*) for a unary operator or (*p op q*) for a binary operator).
  - We'll omit parentheses around constants, variables, and already-parenthesized expressions; we don't want to be writing things like (((1) + (((2) * (3))))).
  - Let's also agree that the parentheses around the whole propositions are optional. So the full parenthesization of 1 + 2 * 3 is (1 + (2 * 3)) or 1 + (2 * 3).
  - For associative operators like + and *, let's write using left associativity, just to avoid having multiple correct results. So we'll take (((1 + 2) + 3) + 4) to be the full parenthesization of 1 + 2 + 3 + 4.

- Note: If you include the outermost parentheses, then a fully parenthesized item has the same number of pairs of parentheses as it has number of operators. E.g., (1 + (2 * 3)) has two pairs of parentheses: one for the + and one for the *.

K. Semantics of Propositional Logic

- The typical semantics for propositional logic uses truth tables as below.

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

p	$\neg p$
F	T
T	F

- Implication sometimes bothers people ("Why does F → T ?")
  - Basically, $p \rightarrow q$ means "p is less true than or equal to q".
  - If you treat true, false, and → as being like 1, 0, and ≤, then F → T is like 0 ≤ 1.

States and Satisfaction

- Here's one way to talk about the truth of a proposition. First, we'll look at states — a state represents one truth table row of possible values for a set of proposition variables. Then we'll look at satisfaction, the notion that a proposition is true in that particular truth table row.
- **Definition**: A (**well-formed**) **state** σ is a set of pairs (a.k.a. bindings) of a proposition letter and a truth value where there's only one binding for any given variable. If a set of bindings σ has more than one binding for some variable, we'll say it's **ill-formed** as a state.
- **Examples**: Examples of states are $\{p = \text{T}\}$ (has one binding), $\{p = \text{F}, q = \text{T}\}$ and $\{q = \text{T}, p = \text{F}\}$ (two ways to write the same state), and the empty state ∅ (the empty set of bindings). On the other hand, $\{p = \text{T}, p = \text{F}\}$ is ill-formed, since it has two bindings for p.
  - **Note**: It's important for the bindings to involve only proposition letters, not more complicated propositions. E.g., $\{p \vee q = \text{F}\}$ is not well-formed.
- **Definition**: A proposition is **satisfied** in (or by) a state if it evaluates to true in that state. E.g., $p \vee \neg q$ is satisfied in $\{p = \text{T}, q = \text{F}\}$. The proposition is **not satisfied** (or **unsatisfied**) in a state if it evaluates to false in that state.
- **Notation**: If σ is a state and φ is a proposition, then σ ⊨ φ means that σ satisfies φ and σ ⊭ φ means σ does not satisfy φ. (The ⊨ symbol is a "double turnstile", if you haven't run across it before.)
- **Examples**: $\{p = \text{T}\} \models p$, $\{p = \text{F}\} \models \neg p$, and $\{p = \text{T}, q = \text{F}\} \models p \vee \neg q$. For nonsatisfaction, $\{p = \text{T}\} \not\models \neg p$, $\{p = \text{F}\} \not\models p$, and $\{p = \text{T}, q = \text{F}\} \models p \wedge \neg q$. A less-obvious case is ∅ ⊨ T ∧ (F → T). Here, the state is empty, but that's okay because the proposition doesn't contain any variables, just the constants T and F.
- **Note**: For satisfaction purposes, it's okay for a state to have unused bindings (bindings of variables that don't appear in the proposition). So if σ and τ are two states with σ ⊆ τ, then if σ ⊨ φ, then τ ⊨ φ. Since every state extends the empty set and ∅ ⊨ T ∧ (F → T), then this proposition is satisfied in every state.

- Though extra bindings are okay, not having enough bindings makes for a somewhat unsettled situation. For example, we can't say $\varnothing \vDash p \wedge q$ because we can't evaluate $p \wedge q$ in $\varnothing$ and get true. But we also can't say $\varnothing \nvDash p \wedge q$, since we can't evaluate $p \wedge q$ and get false. Does this prevent us from making statements like $\varphi \vee \neg\varphi$ is satisfied by every state"?
- **Definition**: A state is **proper** for a proposition φ if it includes bindings for (at least) all the variables of φ. If σ is **improper** (i.e., not proper) for φ, then we can't even evaluate φ in σ, so we can't evaluate φ and get true or to false, so we can't say $\sigma \vDash \varphi$ and we can't say $\sigma \nvDash \varphi$. Since $\sigma \vDash$ or $\nvDash \varphi$ only makes sense if σ is proper, when we make statements like "φ is satisfied in all σ"), we'll quietly assume that we're talking about only the σ that are proper for φ. So we can say "$\sigma \vDash p \vee \neg p$ for all σ" even though $p \vee \neg p$ certainly isn't satisfied in $\varnothing$ or in $\{q = \mathrm{T}\}$, for of the infinitely many examples.
- To sum up, for any arbitrary set of bindings σ and a proposition φ, we can have four situations
  - σ is ill-formed (not a state at all)
  - σ is (well-formed but) improper for φ
  - $\sigma \vDash \varphi$ and $\sigma \nvDash \neg\varphi$
  - $\sigma \nvDash \varphi$ and $\sigma \vDash \neg\varphi$
- And again, when we look at "all states for φ," we mean only the well-formed proper states. We can now make statements like "if it is not the case that $\sigma \vDash \varphi$, then $\sigma \nvDash \varphi$" because we're ignoring the ill-formed and the improper σ.

Validity, Tautologies, and Logical Equivalence

- Now that we have the notion of a proposition being true in a given truth table row, we can go further and talk about a proposition being true in every truth table row.
- **Definition**: φ is **valid** (notation: $\vDash \varphi$) if $\sigma \vDash \varphi$ for every σ. φ is **invalid** (not valid), written $\nvDash \varphi$, if this is not the case. (Remember, we're talking only about well-formed proper states here, so $\nvDash \varphi$ is equivalent to "for some σ, $\sigma \nvDash \varphi$.")
- **Examples**: $\vDash \mathrm{T}$, $\vDash \neg\mathrm{F}$ (the two simplest examples), $\vDash \varphi \vee \neg\varphi$, $\vDash (\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$.
- If $\nvDash \varphi$, then it is not the case that $\sigma \vDash \varphi$ for every σ; this is equivalent to saying for some σ, $\sigma \nvDash \varphi$. Since (by assumption) σ is proper, $\sigma \nvDash \varphi$ is equivalent to $\sigma \vDash \neg\varphi$.
- One way to categorize propositions is through their validity.
- **Definition**: φ is a **tautology** if $\vDash \varphi$, a **contradiction** if $\vDash \neg\varphi$, and a **contingency** if $\nvDash \varphi$ and $\nvDash \neg\varphi$ (simultaneously). Another way to say this is that a tautology has a truth table column of all true; a contradiction has a column of all false, and a contingency has a mix of true and false (at least one row T and at least one row F).
- Some properties:
  - If φ is a tautology, then $\neg\varphi$ is a contradiction and vice versa.
  - If φ is a contingency, then so is $\neg\varphi$ and vice versa.
  - If φ is not a tautology, then it is a contingency or a contradiction.
  - If φ is not a contradiction, then it is a contingency or a tautology.

- If φ is not a contingency, then it is a tautology or a contradiction.

<---------- ended M 2019-08-19

- **Definition**: Two propositions φ and ψ are **logically equivalent** (written φ ⇔ ψ) if ⊨ φ ↔ ψ. Note since ⊨ T ↔ T and F ↔ F (and ⊨ ¬(T ↔ F) and ⊨ ¬(F ↔ T)), φ and ψ are logically equivalent if they have matching columns in their truth tables.
- **Notation**: "⇔" is often pronounced "if and only if", so φ ⇔ ψ is also often written as "φ iff ψ".
- It's easy to show that ⇔ is **transitive**: If $\varphi_1 \Leftrightarrow \varphi_2$ and $\varphi_2 \Leftrightarrow \varphi_3$, then $\varphi_1 \Leftrightarrow \varphi_3$. So ⇔ is the notion of equivalence used when we write a sequence of step-by-step transitions like $p \to q \Leftrightarrow \neg p \vee q \Leftrightarrow q \vee \neg p \leftrightarrow \neg\neg q \vee \neg p \Leftrightarrow \neg q \to p$.
- ⇔ on propositions is like = on arithmetic expressions: If φ ⇔ ψ, then in any semantic context, we can always substitute one for the other. The context has to be semantic because ⇔ has to do with the … ⊨ … relationships between states and propositions
- Though they are similar, it's important to keep the difference between ⇔ and ↔ straight in your head.
  - ↔ is a symbol that can actually appear in a boolean expression. (In C, ↔ is written ==.) I.e., ↔ is a syntactic operator. On the other hand, ⇔ doesn't appear in propositions because it indicates semantic equality.
  - ⇔ is transitive and ↔ is not transitive. Consider (F ↔ F ↔ T), which means (F ↔ (F ↔ T)), since ↔ is right associative. Semantically, (F ↔ (F ↔ T)) ⇔ (F ↔ F) ⇔ T
  - Second, iterated ⇔ means all the propositions are logically equivalent to each other. E.g., (T ∨ T) ⇔ (T ∨ F) ⇔ T. (For an analogy, remember how in algebra we might write "$(x+1)^2 + 3 = (x^2 + 2x + 1) + 3 = x^2 + 2x + 4$"? Here, "=" is being used on numbers the same way we use ⇔ on propositions.
  - So $p \Leftrightarrow q \Leftrightarrow r \Leftrightarrow s$ means ($p \Leftrightarrow q$ and $q \Leftrightarrow r$ and $r \Leftrightarrow s$; i.e., all four are true or all four are false.
  - Compare this to F ↔ F ↔ T ↔ T, which ≡ (F ↔ (F ↔ (T ↔ T))), which evaluates to true.

Relations Between Implications

- The **contrapositive** of φ → ψ is ¬ψ → ¬φ; its **converse** is ψ → φ; its **inverse** is ¬φ → ¬ψ. An implication is ⇔ to its contrapositive; similarly, the converse of an implication is ⇔ to its inverse: (φ → ψ) ⇔ (¬ψ → ¬φ) and (ψ → φ) ⇔ (¬φ → ¬ψ)

More Equivalences

- **Definition of implication**: φ → ψ ⇔ ¬φ ∨ ψ.
- **Negation of implication**: ¬(φ → ψ) ⇔ φ ∧ ¬ψ.
  - Note ¬(φ → ψ) and (¬φ → ¬ψ) are different: ¬(φ → ψ) ⇔ (φ ∧ ¬ψ) but (¬φ → ¬ψ) ⇔ (φ ∨ ¬ψ)
- **"Definition of biconditional**: (φ ↔ ψ) ⇔ (φ → ψ) ∧ (ψ → φ)
- **Exclusive or** of φ and ψ: One of φ and ψ is true but not the other. Turns out to be the opposite of the biconditional:
  - (φ ∧ ¬ψ) ∨ (¬φ ∧ ψ) ⇔ ¬(φ ↔ ψ)
- The usual "inclusive" or allows one or both of φ and ψ to be true:
  - (φ ∨ ψ) ⇔ (¬φ ∧ ψ) ∨ (φ ∧ ¬ψ) ∨ (φ ∧ ψ)

Program Verification; Review of Propositional Logic

CS 536: Science of Programming, Fall 2019

A. Why?

- Reviewing/overviewing logic is necessary because we'll be using it in the course.
- Learning how homeworks and tests work and how the final grade is calculated may save you heartache at the end of the semester.

B. Outcomes

At the end of this activity you should be able to

- Define program verification is and characterize type-checking as a form of it.
- Read and write basic propositional formulas.
- Develop truth tables for propositional formulas.
- Do some simple logical manipulations on propositional formulas.

C. Propositional Logic Questions

Get together in groups of, say, five and agree on someone to be the speaker. As a group, discuss the questions below; write out your group's results.

D. Program Verification and Propositional Logic

1. What is program verification? How is it done?
2. How is type-checking a form of program verification?
3. What is propositional logic? What are propositional connectives?
4. Given values for p and q, what are the values of $p \wedge q$, $p \vee q$, etc?
5. Translate each of the following to either $\varphi \rightarrow \psi$ or $\psi \rightarrow \varphi$:
   a. if φ then ψ
   b. φ is sufficient for ψ
   c. φ only if ψ
   d. φ is necessary for ψ
   e. φ if ψ
   f. if ψ then φ
6. What are the converse, contrapositive, and inverse of $\varphi \rightarrow \psi$? How are they related?
7. What is syntactic equality and how is it denoted?
8. What is semantic equality? How do we indicate semantic equality of two arithmetic expressions? Two propositions?
9. How are syntactic and semantic equality related?
10. How do parentheses affect syntactic equality for us?
11. How do precedence and associativity rules relate to syntactic equality and to the notions of minimal and full parenthesization?

12. What are the minimal and full parenthesizations of
    a. $(x + y * (z / x) * x) - (y / z)$
    b. $(\neg(p \wedge ((\neg q) \rightarrow r)) \vee (s \wedge (t \wedge v))) \rightarrow x$
    c. $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$
    d. $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$
13. What are the precedence and associativity rules we are using for +, -, *, /, %, ≤, =, (etc.), ∧, ∨, →, ↔, and ¬ ?
14. For propositions, what are the definitions of tautology, contradiction, and contingency?
15. Consider the six statements "φ is a *X*" and "¬ φ is a *X*" where *X* ranges over "tautology", "contradiction", and "contingency". How are these statements related?
16. Repeat the previous problem on the six statements "φ is not a *X*" and "φ is a *X*".
17. Which of $\varphi \rightarrow \psi \rightarrow \chi$, $\varphi \rightarrow (\psi \rightarrow \chi)$, and $(\varphi \rightarrow \psi) \rightarrow \chi$ are ≡ ?
18. Write out truth tables for the following. Are any of these semantically equivalent? (I.e., do they have the same truth table rows?)
    a. $p \leftrightarrow (q \leftrightarrow r)$
    b. $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$
    c. $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$
19. Which of $\{p = \mathrm{T}, q = \mathrm{T}\}$, $\{p \wedge q = \mathrm{T}\}$, $\{q = \mathrm{F}\}$, $\{\ \}$, and $\{r = \mathrm{T}, r = \mathrm{F}\}$ are well-formed? Of the ones that are well-formed, which ones are proper for $(\mathrm{T} \rightarrow \mathrm{F})$, $(p \wedge \neg\neg p)$, and $((p \vee q \vee \neg p) \leftrightarrow q)$?
20. List all the states σ such that $\sigma \vDash p \leftrightarrow (q \leftrightarrow r)$.
21. Are there any σ such that $\sigma \vDash \mathrm{T} \rightarrow \mathrm{F}$? Does this tell us that $\varnothing \vDash \mathrm{T} \rightarrow \mathrm{F}$?
22. Define $\varphi \nLeftrightarrow \psi$ to mean that φ and ψ are logically inequivalent (i.e., not ⇔).
    a. Define $\varphi \nLeftrightarrow \psi$ using ⊨
    b. Is $\nLeftrightarrow$ transitive? I.e., if $p \nLeftrightarrow q \nLeftrightarrow r$ (an abbreviation for $p \nLeftrightarrow q$ and $q \nLeftrightarrow r$), then $p \nLeftrightarrow r$? Provide a counterexample if the answer is no; give an informal proof if the answer is yes.

E. Course Organization Questions

Read the home page information and answer these questions.

1. What (if anything) happens if your
    a. Final Exam score > Exam 1 score?
    b. Exam 1 score > Final Exam score?
    c. Final Exam score > Exam 2 score?
    d. Exam 2 score > Exam 1 score ?
2. Say you take a test on a day you're not feeling very well. You get the graded test back and realize the score is lower than you wanted. Can you retake the test?
3. Can you hand in a homework late? How late? Do you lose points?
4. Say you turn in your homework but upload the wrong pdf file. What happens?
5. How is the end-of-semester score calculated?
6. How is the final grade calculated?

7. What, if anything, happens to your final grade if, at the end of the semester,
   a. Adding 2 points to your Final Exam score will get you to the next letter grade?
   b. Adding 5 points to your Final Exam?
   c. Adding 2 points to your end-of-semester score?
8. Which of the following are allowed?
   a. Turning in a homework you missed a month ago
   b. Redoing a homework assignment
   c. Doing an extra homework assignment
   d. Point out a grading error on a test

CS 536: Solution to Activity 1 (Program Verification & Testing; Review of Propositional Logic)

1. Program verification aims to get reliable programs by mechanically reasoning about them. We name sets of values or states using predicates and simulate program execution on them, using rules of logic plus rules describing program execution.
2. Type-checking uses types to denote sets of values (e.g., values of type int); it uses mechanical type-checking rules to show how values manipulated (e.g., plus takes two ints and yields an int).
3. Propositional logic is logic over proposition variables (i.e., Boolean variables). The connectives ¬, ∧, ∨, →, and ↔ are standard functions on boolean values.
4. See the table in the lecture notes. Be especially knowledgeable about $p \rightarrow q$.
5. (a), (b), and (c) mean φ → ψ; (d), (e), and (f) mean ψ → φ.
6. φ → ψ is equivalent to its contrapositive ¬ψ → ¬φ. Its converse ψ → φ and inverse ¬φ → ¬ψ are equivalent to each other. In general, an implication is not equivalent to its converse.
7. Syntactic equality is equality as structured text. It is denoted by ≡
8. Semantic equality is equality of meaning. To denote it, we write φ ⇔ ψ for logical propositions and $e_1 = e_2$ for other expressions.
9. Syntactic equality implies semantic equality (but not vice versa).
10. Redundant parentheses are ignored. E.g., 1 + 2 * 3 ≡ (1 + (2 * 3)).
11. Precedence, left/right associativity, and associative operator rules tell us which parentheses are necessary and which are redundant. The minimal parenthesization of an item uses no redundant parentheses; the full parenthesization puts parentheses around each operation. They are both ≡ to the original syntactic item.
12. (Minimal and full parenthesizations)

    12a. $(x + y * (z/x) * x) - (y/z)$
    Minimal: $x + y * (z/x) * x - y/z$ Full[‡]: $((x + ((y * (z/x)) * x)) - (y/z))$

    12b. $(\neg(p \wedge (\neg q \rightarrow r)) \vee (s \wedge (t \wedge v))) \rightarrow x$
    Minimal: $\neg(p \wedge (\neg q \rightarrow r)) \vee s \wedge t \wedge v \rightarrow x$ Full: $((\neg(p \wedge ((\neg q) \rightarrow r)) \vee ((s \wedge t) \wedge v)) \rightarrow x)$

    12c. $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$ is already minimal Full: $((p \leftrightarrow q) \wedge (q \leftrightarrow r))$

    12d. $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$
    Minimal: $p \wedge q \wedge r \vee \neg p \wedge \neg q \wedge \neg r$ Full: $(((p \wedge q) \wedge r) \vee ((((\neg p) \wedge (\neg q)) \wedge (\neg r)))$
13. From low to high: ↔, →, ∨, ∧, ≤ and = and etc. (a tie), + and –,* and / and %, unary – and ¬.
14. A tautology is true for all possible combinations of truth values for its variables. A contradiction is false for all possible combinations. A contingency is true for at least one combination and is false for at least one combination.
15. (φ is a tautology) and (¬φ is a contradiction) are equivalent; so are (φ is a contingency) and (¬φ is a contingency)
16. (φ is not a tautology) is equivalent to (φ is a contradiction or φ is a contingency).
    (φ is not a contradiction(is equivalent to (φ is a tautology or φ is a contingency).

[‡] I'm showing the outermost parentheses; remember that they're optional.

(φ is not a contingency) is equivalent to (φ is a tautology or φ is a contradiction).

(Every proposition falls into exactly one of the three categories, so if it's not some particular one of the three, it must be one of the other two.)

17. $\varphi \to \psi \to \chi \equiv \varphi \to (\psi \to \chi)$.

18. The table is below. The only pair of semantically equivalent propositions are $(p \leftrightarrow q) \wedge (q \leftrightarrow r)$ and $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$.

Note $((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \leftrightarrow ((p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r))$ is a tautology
and $\neg((p \leftrightarrow q) \wedge (q \leftrightarrow r)) \leftrightarrow ((p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r))$ is a contradiction.

p	q	r	$p \leftrightarrow (q \leftrightarrow r)$	$(p \leftrightarrow q) \wedge (q \leftrightarrow r)$	$p \wedge q \wedge r \vee \neg p \wedge \neg q \wedge \neg r$
F	F	F	F	T	T
F	F	T	T	F	F
F	T	F	T	F	F
F	T	T	F	F	F
T	F	F	T	F	F
T	F	T	F	F	F
T	T	F	F	F	F
T	T	T	T	T	T

20. The σ such that $\sigma \vDash p \leftrightarrow (q \leftrightarrow r)$ are $\{p = \text{T}, q = \text{T}, r = \text{T}\}$, $\{p = \text{T}, q = \text{F}, r = \text{F}\}$, $\{p = \text{F}, q = \text{T}, r = \text{F}\}$, and $\{p = \text{F}, q = \text{F}, r = \text{T}\}$.

21. There are no σ such that $\sigma \vDash \text{T} \to \text{F}$. This is different from claiming $\varnothing \vDash \text{T} \to \text{F}$, which means "we don't need the values of any proposition letters to know that T → F is true". One could write "$\sigma \vDash \text{T} \to \text{F}$ if and only if $\sigma \in \varnothing$", but that's just a symbolic way of saying that there aren't any σ that work.

22. a. Since $\varphi \Leftrightarrow \psi$ means $\vDash \varphi \leftrightarrow \psi$, $\varphi \not\Leftrightarrow \psi$ means $\nvDash \varphi \leftrightarrow \psi$, which means that for some σ, we have $\sigma \nvDash \varphi \leftrightarrow \psi$. One way to expand out this last statement is that $\sigma \vDash (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi)$.

b. $\not\Leftrightarrow$ is not transitive. A simple example is (T $\not\Leftrightarrow$ F and F $\not\Leftrightarrow$ T does not imply T $\not\Leftrightarrow$ T).

Course Organization Questions

1 – 8. Study the home page and its syllabus information.

