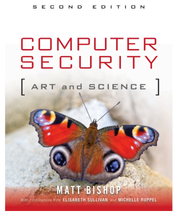
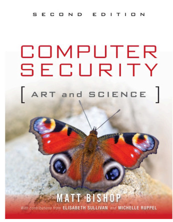


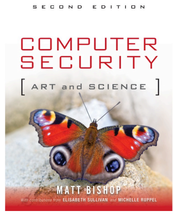
Symbolic Logic

Appendix E



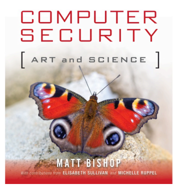
Outline

- Propositional logic
  - Mathematical induction
- Predicate logic
- Temporal logic systems
  - CTL



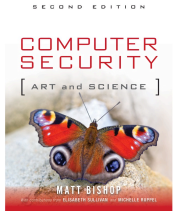
Propositional Logic

- *Proposition* is an atomic, declarative sentence that can be shown to be true or false but not both
  - "There was not a cloud in the sky today"
- Represent as *p* or *q*, usually with subscripts
- Connectives:
  - ¬, or *negation* (not) [highest precedence]
  - ∨, or *disjunction* (and) [this and conjunction have the same precedence]
  - ∧, or *conjunction* (or) [this and disjunction have the same precedence]
  - →, or *implication* (if … then …) [lowest precedence]
  - (,) group operands and operators in the usual way



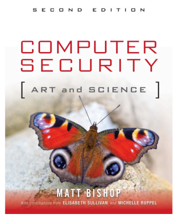
Terms

- *Natural deduction*, a means of reasoning about propositions
- *Proof rules*, rules letting infer formulas from other formulas
- *Premises*, formulas we know or assume to be true to reach a conclusion (formula) we want to establish
- *Contradiction*, a formula that is always false; denoted by $\bot$ (*bottom*)
- *Tautology*, a formula that is always true; denoted by $\top$ (*top*)



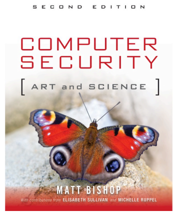
Examples

- $p \wedge \neg p = \bot$
  - A contradiction, as *p* and ¬*p* cannot both be true
- $p \vee \neg p = \top$
  - A tautology, as either p or ¬*p* will be true



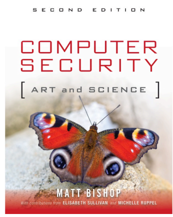
Rules of Natural Deduction

1. If p and q are true, so is $p \land q$ (*conjunction introduction* rule)
2. If $p \land q$ is true, so is p and so is q (*conjunction elimination* rule)
3. If p is true, so is $p \lor q$; if q is true, so is $p \lor q$ (*disjunction introduction* rule)
4. If $p \lor q$ is true, and we want to conclude Q, we assume p and conclude Q; then we assume q and conclude Q. Given $p \lor q$ and these two proofs, we can infer Q (*disjunction elimination* rule)



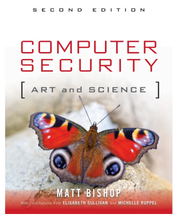
Rules of Natural Deduction

5. Assume p is true temporarily and based on this assumption prove q. Then we can conclude $p \rightarrow q$ (*implication introduction*)
6. If we can conclude p and $p \rightarrow q$, then we can conclude q. (*modus ponens;* also *implication elimination*)
7. If we assume p and conclude $\perp$, then we infer $\neg p$ (*negation introduction*)
8. If we assume p and $\neg p$, then we conclude $\perp$ (*negation elimination*)



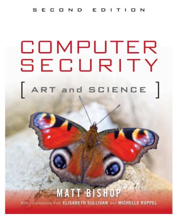
Rules of Natural Deduction

9. If we assume ⊥, then we can prove any *p*. (*bottom elimination*)
10. If we have concluded *p*, then we can also conclude ¬¬*p* (*double negation introduction*)
11. If we have concluded ¬¬*p*, then we can also conclude *p* (*double negation elimination*)



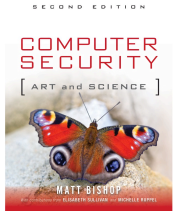
Derived Rules

- If we have concluded $\neg q$ and $p \rightarrow q$, we can also conclude $\neg p$ (*modus tollens*)
- Assume $\neg q$ is true. Suppose we assume p and we can then prove $p \rightarrow q$. Then q holds. But this is impossible, so our assumption (that p is true) must be false (*reductio ad absurdum* or *proof by contradiction*)
  - See the implication elimination rule above



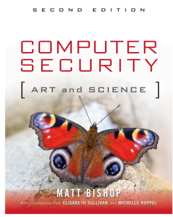
Well-Formed Formulas

- A *word* is a set of symbols using symbols for propositions, connectors, parentheses
- Only some (*well-formed formulas* or *WFF*s) are meaningful; these are defined inductively
  - A propositional atom is a WFF
  - Negation of a WFF is a WFF
  - Conjunction of WFFs is a WFF
  - Disjunction of WFFs is a WFF
  - Implication between two WFFs is a WFF



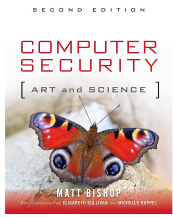
Truth Tables

p	q	p ∧ q	p ∨ q	p → q	¬p
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	T
F	F	F	F	T	T



Equivalence of Formulas: Definitions

- *Sequent* is a set of formulas $\phi_1, \ldots \phi_n$ and a conclusion ψ; denoted $\phi_1, \ldots \phi_n \vdash \psi$
- Sequent is *valid* if a proof of it can be found
- ϕ and ψ are *provably equivalent* if and only if both $\phi \vdash \psi$ and $\psi \vdash \phi$ hold
- Two formulas are *semantically equivalent* if they have the same truth table values. If ψ evaluates to true whenever $\phi_1, \ldots \phi_n$ evaluate to true, this is denoted $\phi_1, \ldots \phi_n \vDash \psi$



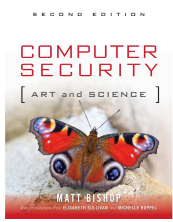
Soundness and Completeness Theorems

Soundness Theorem: Let $\phi_1, \ldots \phi_n$ and ψ be propositional logic formulas. If $\phi_1, \ldots \phi_n \vdash \psi$, then $\phi_1, \ldots \phi_n \vDash \psi$.

- If, given a set of premises, there is a proof of a conclusion, then the premises and conclusion are semantically equivalent

Completeness Theorem: Let $\phi_1, \ldots \phi_n$ and ψ be propositional logic formulas. If $\phi_1, \ldots \phi_n \vDash \psi$, then $\phi_1, \ldots \phi_n \vdash \psi$.

- If a set of premises and a conclusion are semantically equivalent, then there is a natural deduction proof for the sequent.



Mathematical Induction

We want to prove a property *M*(*n*) holds for all natural numbers n

We proceed as follows:

- BASIS: prove that *M*(1) holds
- INDUCTION HYPOTHESIS: assert that *M*(*n*) holds for n = 1, . . ., *k*
- INDUCTION STEP: prove that if *M*(*k*) holds, then *M*(*k*+1) holds

Then *M*(*n*) is true for all natural numbers n.

Example

- Prove the sum of the first *n* natural numbers is $\frac{n(n+1)}{2}$.

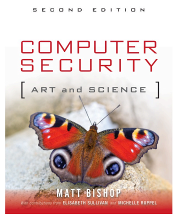
BASIS: M(1) = $\frac{1(1+1)}{2} = \frac{1(2)}{2} = \frac{2}{2}$ = 1, which is clearly true

INDUCTION HYPOTHESIS: For $n = 1, . . ., k$, $M(k)$ is true

INDUCTION STEP: Consider $M(k+1) = 1 + . . . + k + (k+1)$

$1 + . . . + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$ induction hypothesis

(*continued on next slide*)



Example (con’t)

$$1 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)$$ induction hypothesis

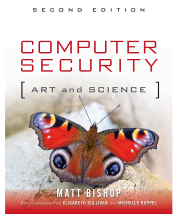
$$= \frac{k^2}{2} + \frac{k}{2} + \frac{2k}{2} + \frac{2}{2}$$ expanding terms

$$= \frac{k^2+3k+2}{2}$$ combining terms

$$= \frac{(k+1)(k+2)}{2}$$ factoring the numerator

$$= \frac{(k+1)[(k+1)+1]}{2}$$ combining terms

which is $M(k+1)$, completing the proof



Predicate Logic

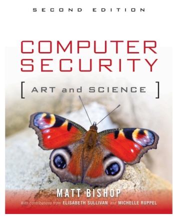
- Logic using predicates and quantifiers
- Predicates describe something; quantifiers say what the description applies to
- Quantifiers
  - There exists an x: $\exists x$
  - For all x: $\forall x$
  - Can combine with ¬ for negation
- Variables
  - *Bound* if quantified with either ∃ or ∀
  - *Unbound* or *free* if not bound

Examples

- Define:
  - $F(x)$: x is a file
  - $D(y)$: y is a directory
  - $C(x, y)$: directory y contains file x
- Then:

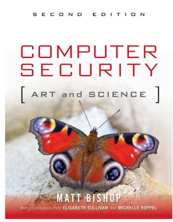
$$\forall\, x F(x) \text{ -> } (\exists\, y\, (D(y) \wedge C(x, y)))$$

says that "every file is contained in a directory"



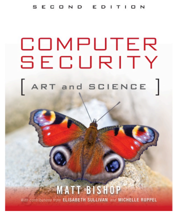
Formula in Predicate Logic

- If p is a predicate of n arguments ($1 \leq n$) and the arguments are terms $t_1, \ldots, t_n$ defined over the set of functions, then $p(t_1, \ldots, t_n)$ is a formula
- If ϕ is a formula, then $\neg\phi$ is also a formula
- If ϕ and φ are formulas, then $\phi \land \varphi$, $\phi \lor \varphi$, and $\phi \rightarrow \varphi$ are also formulas
- If ϕ is a formula and x a variable, then $\forall x\phi$ and $\exists x\phi$ are also formulas



Rules for Natural Deduction in Predicate Logic

- *Equality*: A term t is equal to itself
- *Substitution*: If $t_1 = t_2$ and x is a free variable in $\phi(x)$, then $f(t_1) = f(t_2)$
- *Universal quantifier elimination*: If you have $\forall x\ \phi(x)$, then you can replace the x in $\phi(x)$ by any term t that is free in $\phi(x)$
- *Universal quantifier introduction*: If you can prove some formula $\phi(x)$ with x a free variable, then you can derive $\forall x\ \phi(x)$



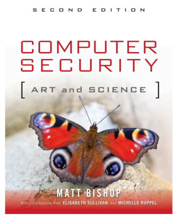
Temporal Logic Systems

Introduce notion of time into logic system

- *Linear time logic systems*: events are sequential
- *Branching time logic systems*: events are concurrent ("alternative universes")

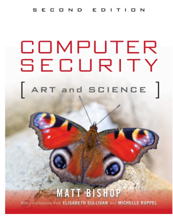
Systems view time as:

- *continuous* flow of events
- *discrete* events



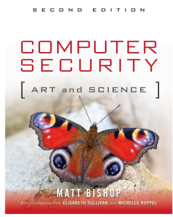
Example: Control Tree Logic (CTL)

- Begin with propositional logic
- Add temporal connectives; each uses 2 symbols
  - First symbol: “A”, along all paths; “E”: along at least one path
  - Second symbol: ”X”, the next state; “F”, some next state; “G”, all future states; “U”, until some future state
- Precedence rules (high to low)
  - ¬, AG, EG, AF, EF, AX, EX
  - ∧, ∨
  - →
  - AU, EU



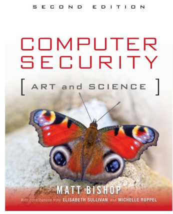
Well-Formed Formulas in CTL

- ⊤ (top), ⊥ (bottom) are formulas
- All atomic descriptions are formulas
- If ϕ and φ are formulas, then $\phi \wedge \varphi$, $\phi \vee \varphi$, $\phi \rightarrow \varphi$, $\neg\phi$, AXϕ, EXϕ, A[ϕUφ], E[ϕUφ], AGϕ, EGϕ, AFϕ, and EFϕ are also formulas



Semantics of CTL

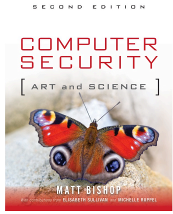
- A *model* is $M = (S, \Rightarrow, L)$, where S is a set of states, $\Rightarrow$ is the transition operator on S such that $\forall s \in S\ (\exists s \in S\ [s \Rightarrow s'])$, L is a labeling function, and $L : S \rightarrow \mathcal{P}(atoms)$
    - $\mathcal{P}(atoms)$ power set of the defined atoms
- Let $M = (S, \Rightarrow, L)$ be a model for CTL. Given any $s \in S$, if a CTL formula ϕ holds in state s, we write this as $M,s \vDash \phi$, and say that state s of model M satisfies formula ϕ.
    - $M,s \nvDash \phi$ means state s in model M does not satisfy ϕ



Rules of CTL

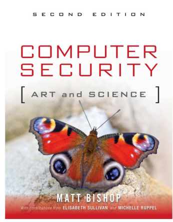
M model, *s*, s_1, . . . states of *M*, *p* atomic proposition of *M*, ϕ, ϕ_1, ϕ_2 CTL formulas

- $\forall s \in S$ [$M, s \vDash \top$]
  - Tautologies hold in all states of M
- $\forall s \in S$ [$M, s \nvDash \bot$]
  - Tautologies hold in all states of M
- $M, s \vDash p$ if and only if $p \in L(s)$
  - *P* holds in state *s* of *M* whenever *p* is in the set of atoms that hold in state *s*; conversely, if *p* not in that set, then *p* does not hold in state *s*



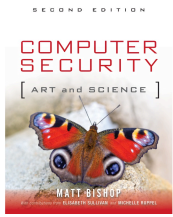
Rules of CTL

- If $M, s \nvDash \phi$, then $M, s \vDash \neg\phi$
  - If a state does not satisfy a formula in the model then it satisfies the negation of the formula
- $M, s \vDash \phi_1 \wedge \phi_2$ if and only if $M, s \vDash \phi_1$ and $M, s \vDash \phi_2$
- $M, s \vDash \phi_1 \vee \phi_2$ if and only if $M, s \vDash \phi_1$ or $M, s \vDash \phi_2$
  - A state in M satisfies the {and, or} of two formulas if and only if it satisfies {both formulas, either formula} on the right
- $M, s \vDash \phi_1 \rightarrow \phi_2$ if and only if $M, s \nvDash \phi_1$ or $M, s \vDash \phi_2$
  - A state in M satisfies the implication of two formulas if and only if it satisfies the second formula, or neither formula



Rules of CTL

- $M, s \vDash AX\phi$ if and only if $\forall s_1$ such that $s \rightarrow s_1$ then $M, s_1 \vDash \phi$
- $M, s \vDash EX\phi$ if and only if $\exists s_1$ such that $s \rightarrow s_1$ then $M, s_1 \vDash \phi$
  - A state satisfies a formula in some next state if and only if {every, at least one} state implied by the original state also satisfies the formula
- $M, s \vDash AG\phi$ if and only if, for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$, where $s = s_1$ and $\forall s_i$ on the path, $[M, s_i \vDash \phi]$
  - A state satisfies a formula in some next state if and only if every state implied by the original state also satisfies the formula
- $M, s \vDash EG\phi$ if and only if there exists a path $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$, where $s = s_1$ and $\forall s_i$ on the path, $[M, s_i \vDash \phi]$
  - A path with all states satisfying a formula exists if and only if every state on the path beginning at the original state satisfies the formula



Rules of CTL

- $M, s \vDash AF\phi$ if and only if for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$, where $s = s_1$ and $\exists s_i\ [M, s_i \vDash \phi]$
  - On all paths, there will be a state satisfying the formula if and only if every path of transitions beginning at the original state contains at least one state that satisfies the formula
- $M, s \vDash EF\phi$ if and only for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$, where $s = s_1$ and $\exists s_i$ on the path $[M, s_i \vDash \phi]$
  - There is a path with one state satisfying the formula if and only if a state on a path of transitions beginning at the original state satisfies the formula

Rules of CTL

- $M, s \vDash A[\phi \mathrm{U} \phi]$ if and only if for all paths $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots,$

$$\exists i\, [i \geq 0 \wedge s_i \vDash \phi_2 \text{ and } [\forall j\, [0 \leq j < i \rightarrow s_j \vDash \phi_1]]$$

  - On all paths, there will be a state satisfying the formula if and only if every path of transitions beginning at the original state has a state satisfying the second formula and all previous states in that path satisfy the first formula
- $M, s \vDash E[\phi \mathrm{U} \phi]$ if and only if for some path $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots,$

$$\exists i\, [i \geq 0 \wedge s_i \vDash \phi_2 \text{ and } [\forall j\, [0 \leq j < i \rightarrow s_j \vDash \phi_1]]$$

  - There is a path on which there is a state satisfying the formula if and only if every path of transitions beginning at the original state has a state satisfying the second formula and all previous states in that path satisfy the first formula