Logic and Proof

Lecture 2

Discrete Mathematical Structures

At the Last Class …

- Part I: Sets, Sequences and Structures
  - Sets: fundamental model in mathematics
  - Sequences: elements and order
  - Structures: sets with operations
- Part II: Some Useful Tools
  - Division, prime and algorithm
  - Matrices and operations on them

Logic and Proof

- Part I: Propositional and Predicate Logic
  - Logical operations and truth tables
  - Quantifiers
  - Logic statements
- Part II: Methods of Proof
  - Rules of inference
  - Indirect method of proof
  - Proof by contradiction
  - Disproving by counterexamples

Logic about Award

- Smith, Brown, Jones, Robinson will be granted awards for Math, English, French and Logic, respectively, with each award for one person.
- They guessed which-for-which as following:
  - Smith: Robinson will win the award for Logic.
  - Brown: Jones will win the award for English.
  - Jones: Smith will not win the award for Math.
  - Robinson: Brown will win the award for French.
- It turned out that only winner of Math and Logic Awards made the correct guesses.
- Problem: Can you tell who win what exactly?

Looking for the solution

- Describe the problem as clearly as possible.
  - For example, we use P(x) denoting a person x win the award P.
- List all related useful information (rules)
  - For example
    - If x win P, others cannot win the same award.
    - If x didn't win any three of the four award, then he must win the fourth.
    - If x make the wrong guess, then the negation of the guess must be true.
    - ……
- THE approach: guess + reasoning
  - but guess what?

Possible reasoning

- Smith: Robinson will win the award for Logic.
- Brown: Jones will win the award for English.
- Jones: Smith will not win the award for Math.
- Robinson: Brown will win the award for French

If we guess BJ, that is “Brown and Jones win the awards for Math and logic”, then, what brown said is true :Jones wins the award for English.” **Contradiction!**

If we guess RS, that is: “Robinson and Smith win the awards of Math and Logic”, then, what Robinson say is true: Brown wins the award for French. So, Jones wins the award for English.

So, what Brown said is true, but Brown is not the winner of award of

If we guess JR: that is “Jones and Robinson win the awards for Math and Logic”. Then we know that **Brown wins the award for French, and Smith wins the award for English.**

So what Smith said about Robinson is false, that means **Robinson wins the award for Math. And the award for Logic goes to Jones.** Done!

- Smith: Robinson will win the award for Logic.
- Brown: Jones will win the award for English.
- Jones: Smith will not win the award for Math.
- Robinson: Brown will win the award for French

- **Are there any rules in reasoning, unrelated to the concrete contents?**
- **How can we describe these rules, and how can we make use of them effectively?**

Proposition

- Proposition (statement)
  - A declarative sentence that is either true or false, but not both.
- Examples
  - 1+1=2
  - John is a student.
  - Today is Tuesday.

More Examples of Proposition

- Do you speak English?
  - This is a question, not a statement.
- 3-x=5
  - x is a variable, so the truth value of this sentence is open.
- Let’s go!
  - It is not a statement, but a command.
- The 4-color guess is true.
  - We believe that it is true or false, but not both even before it was solved.
- He is a good man.
  - What’s the meaning of “good man”

Propositional Variable

- A propositional variable assumes a value from the set {*True, False*}
- A propositional variable is often denoted as *p*, *q*, *r*, etc.
- A statement can be represented by a propositional variable, e.g.
  - *p*: Today is Tuesday.
  - *q*: 2+2=4

Logical Connectives

- A simple declarative sentence can be represented by an ***atom*** proposition.
- More than one atom propositions can be combined into a compound statement.
- The combination is achieved using “connectives”. Usually, the connective roughly corresponds some conjunctive in the natural language.
- The connective is defined exactly using “***truth table***”.

Negation

~*p*: it is not the case that *p*

p	~*p*
T	F
F	T

Truth table for ~

All possible value of *p*

Conjunction

"p and q" is denoted as $p \wedge q$

$p \wedge q = true$ iff both p and q

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

All possible value of <p,q>

Disjunction

"p or q" is denoted as $p \vee q$, *but not exactly*

$p \vee q$=false iff both $\sim p$ and $\sim q$

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

All possible value of <p,q>

Exclusive Disjunction

"exclusive" means "exactly one is true"

p	q	$\alpha(p,q)$
T	T	F
T	F	T
F	T	T
F	F	F

$$(p \wedge {\sim}q) \vee ({\sim}p \wedge q)$$

Predicate

- If *x* is an integer, "x is larger than 2" is not a proposition, and its truth value depends on the value of x.
- It can be denoted as *P*(*x*), a propositional function.
  - The domain of *P* is the set of all integer, and
  - The range of *P* is {*true*, *false*}
- A propositional function is called a ***predicate*(谓词）**.

Universal Quantification

- Given the domain, “for all x, *P*(x)” is a statement, that is the sentence is either true or false, but not both.
- If *P*(*x*) is a predicate, $\forall x P(x)$ means “for all *x*, *P*(*x*), and $\forall$ is called ***universal quantifier（全称量词）***.
- If x is real number, $\forall x P(x)$ is true if *P*(*x*) represents “-(-x)=x”

Existential Quantification

- Given the domain, "There is some x, P(x)" is a statement, that is the sentence is either true or false, but not both.
- If $P(x)$ is a predicate, $\exists x P(x)$ means "there is some x, $P(x)$, and $\exists$ is called ***existential quantifier*（存在量词）**.
- If a,b are real constants, $a<b$, in the domain of real number, $\exists x P(x)$ is true if $P(x)$ means "$a<x<b$"

Negation of Quantifications

Domain of real number is assumed

- Negation of universal quantification
  - For all x, the square of x is positive
  - There exists some x, the square of x is not positive.
- Negation of existential quantification
  - There exists some x, 5x=x.
  - For all x, 5x is not equal to x.

Negation of Quantifications

- $\sim\forall x P(x)$ is equivalent to $\exists x(\sim P(x))$
- $\sim\exists x P(x)$ is equivalent to $\forall x(\sim P(x))$

Multiple Quantifiers

Considering the set of real numbers

- $\forall x \forall y P(x,y)$ and $\forall y \forall x P(x,y)$ have the same truth values.
  - They are both true if $P(x,y)$ means x+y=y+x.
- $\exists x \exists y P(x,y)$ and $\exists y \exists x P(x,y)$ have the same truth values.
  - They are both true if $P(x,y)$ means x=y+1.
- $\forall x \exists y P(x,y)$ and $\exists y \forall x P(x,y)$?
  - If $P(x,y)$ means "y>x" then $\forall x \exists y P(x,y)$ is true, but $\exists y \forall x P(x,y)$ is false.

Implication

$\sim$p v q

"if p then q" can be denoted as $p \Rightarrow q$

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

However, "$\Rightarrow$" **doesn't** exactly mean "if…then…":

$p \Rightarrow q$ is true has nothing to do with the connection between p and q in common sense.

In fact, a false hypothesis implies **any** conclusion.

Equivalence

Logically equivalent

$p \Leftrightarrow q$ means p and q **always** have the same truth value

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$$

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Examples of Quantification

- All people know China.
  - $P(x)$: x is a person; $Q(x)$: x knows China.
  - $\forall x(P(x) \Rightarrow Q(x))$
- Some people know Guatemala.
  - $P(x)$: x is a person; $Q(x)$: x knows Guatemala.
  - $\exists x(P(x) \wedge Q(x))$

1. $\sim(\forall x(P(x) \Rightarrow \sim Q(x)))$
2. $\exists x(\sim(P(x) => \sim Q(x)))$
3. $\exists x(P(x) \wedge Q(x))$

nnectives!

Statement about Prime Number

- For all positive integer n, there is a prime number between *n* and 2*n* (Tschebyscheff's theorem):

$$\forall n(N(n)\Rightarrow\exists x(N(x)\wedge(x\geq n) \wedge (x\leq 2n) \wedge$$

$$\forall y(y|x\Rightarrow(y=1\vee y=x))))$$

where: $N(x)$: x is a positive integer

$y|x$: y divides x

Exercise: "There is no largest prime number."

Contrapositive

p	q	$p \Rightarrow q$	$\sim q$	$\sim p$	$\sim q \Rightarrow \sim p$	$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$
T	T	T	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

$p \Leftrightarrow q$ if and only if $p \equiv q$

Tautology, Contradiction and Contingency

- $(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$ is a tautology
- $p \wedge \sim p$ is a contradiction
- $(p \Rightarrow q) \wedge (p \vee q)$:
  - this logical expression is true when:

    (p,q) = (*true*,*true*) or (*false*,*true*)
  - and is false when:

    (p,q) = (*true*,*false*) or (*false*,*false*)
  - So, this is a contingency, i.e. neither tautology nor contradiction.

Properties of Logical Operations

Commutative Properties

1. $p \vee q \equiv q \vee p$ 2. $p \wedge q \equiv q \wedge p$

Associative Properties

3. $p \vee (q \vee r) \equiv (p \vee q) \vee r$ 4. $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$

Distributive Properties

5. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ 6. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Idempotent Properties

7. $p \vee p \equiv p$ 8. $q \wedge q \equiv q$

Properties of Negation

9. $\sim(\sim p) \equiv p$

10. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ 11. $\sim(p \wedge q) \equiv \sim p \vee \sim q$ De Morgan’s laws

Substitution of Connectives

1. $(p \Rightarrow q) \equiv ((\sim p) \vee q)$
2. $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$
3. $\sim(p \Rightarrow q) \equiv (p \wedge \sim q)$
4. $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (q \Rightarrow p))$
5. $\sim(p \Leftrightarrow q) \equiv ((p \wedge \sim q) \vee (q \wedge \sim p))$

Proof of (3) not using truth table:

$\sim(p \Rightarrow q) = \sim(\sim p \vee q)$ formula 1

$= \sim\sim p \wedge \sim q$ De Morgan's

$= p \wedge \sim q$ Double Negation

Inference by Logical Equivalence

We know that Bill, Jim and Sam are from Boston, Chicago and Detroit, respectively. Each of following sentence is half right and half wrong:

Bill is from Boston(p_1), and Jim is from Chicago(p_2).

Sam is from Boston(p_3), and Bill is from Chicago(p_4).

Jim is from Boston(p_5), and Bill is from Detroit(p_6).

Tell the truth about their home town.

We have:

$$((p_1 \wedge \sim p_2) \vee (\sim p_1 \wedge p_2)) \wedge ((p_3 \wedge \sim p_4) \vee (\sim p_3 \wedge p_4)) \wedge ((p_5 \wedge \sim p_6) \vee (\sim p_5 \wedge p_6))$$

Equivalently

$$(p_1 \vee p_2) \wedge (\sim p_1 \vee \sim p_2) \wedge (p_3 \vee p_4) \wedge (\sim p_3 \vee \sim p_4) \wedge (p_5 \vee p_6) \wedge (\sim p_5 \vee \sim p_6)$$

Inference by Logical Equivalence (cont.)

We know that Bill, Jim and Sam are from Boston, Chicago and Detroit, respectively. Each of following sentence is half right and half wrong:

Bill is from Boston(p_1), and Jim is from Chicago(p_2).

Sam is from Boston(p_3), and Bill is from Chicago(p_4).

Jim is from Boston(p_5), and Bill is from Detroit(p_6).

Tell the truth about their home town.

- p_1， p_3， p_5有且只有一个成立

  $(p_1 \vee p_3 \vee p_5) \wedge (\sim p_1 \vee \sim p_3) \wedge (\sim p_1 \vee \sim p_5) \wedge (\sim p_3 \vee \sim p_5)$
- p_2， p_4不能同时成立: $(\sim p_2 \vee \sim p_4)$
- p_1， p_4， p_6有且只有一个成立

  $(p_1 \vee p_4 \vee p_6) \wedge (\sim p_1 \vee \sim p_4) \wedge (\sim p_1 \vee \sim p_6) \wedge (\sim p_4 \vee \sim p_6)$
- p_2， p_5不能同时成立

  $(\sim p_2 \vee \sim p_5)$

Inference by Logical Equivalence (cont.)

We have:

$$(p_1 \vee p_2) \wedge (\sim p_1 \vee \sim p_2) \wedge (p_3 \vee p_4) \wedge (\sim p_3 \vee \sim p_4) \wedge (p_5 \vee p_6) \wedge (\sim p_5 \vee \sim p_6)$$
$$\wedge (p_1 \vee p_3 \vee p_5) \wedge (\sim p_1 \vee \sim p_3) \wedge (\sim p_1 \vee \sim p_5) \wedge (\sim p_3 \vee \sim p_5) \wedge (\sim p_2 \vee \sim p_4)$$
$$\wedge (p_1 \vee p_4 \vee p_6) \wedge (\sim p_1 \vee \sim p_4) \wedge (\sim p_1 \vee \sim p_6) \wedge (\sim p_4 \vee \sim p_6) \wedge (\sim p_2 \vee \sim p_5)$$

which logically equivalent to：

$$(\sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4 \wedge \sim p_5 \wedge p_6)$$

So, Jim is from Chicago, Sam is from Boston, and Bill is from Detroit.

Bill is from Boston(p_1), and Jim is from Chicago(p_2).
Sam is from Boston(p_3), and Bill is from Chicago(p_4).
Jim is from Boston(p_5), and Bill is from Detroit(p_6).

Properties of Quantifications

1. $\sim(\forall x P(x)) \equiv \exists x \sim P(x)$
2. $\sim(\exists x P(x)) \equiv \forall x(\sim P(x))$
3. $\exists x(P(x) \Rightarrow Q(x)) \equiv \forall x P(x) \Rightarrow \exists x Q(x)$
4. $\exists x P(x) \Rightarrow \forall x Q(x) \equiv \forall x(P(x) \Rightarrow Q(x))$
5. $\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$
6. $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$

For quantifications, truth table is invalid, so some axioms are needed for strict proof.

Logical Inference

- Premises: $A_1, A_2, \ldots, A_k$
- Conclusion: B
- Valid inference: For any assignment of values of the variables in all A_i's and B, if the conjunction of all A_i's is true, then B must be true.
- That is, the inference is valid if and only if

$$(A_1 \wedge A_2 \wedge \ldots \wedge A_k) \Rightarrow B$$

is a tautology.

Modus Ponens

- We have: $(p \wedge (p \Rightarrow q)) \Rightarrow q$, so, the rule:

$$p,\ p \Rightarrow q \rightarrow q$$

- A classic inference, dating back to ancient Greece:

$P(x)$: x is a man; $Q(x)$: x will die;

Socrates is a Man: $P(s)$

Every man will die: $\forall x(P(x) \Rightarrow Q(x))$

Conclusion: Socrates will die: $Q(s)$

Proof

- The proof for $A_1, A_2, \ldots, A_k \rightarrow B$ is a sequence of statements, in which, each statement is one of the following: (the last one should be *B*)
  - a tautology, or
  - any one of $A_1, A_2, \ldots, A_k$, or
  - a new statement obtained by applying logical equivalences on any prior statement
  - a new statement obtained by applying modus ponens on one or more prior statements

Some Important Tautologies

Propositional Tautologies

1. $(p \wedge q) \Rightarrow p$
2. $(p \wedge q) \Rightarrow q$
3. $p \Rightarrow (p \vee q)$
4. $q \Rightarrow (p \vee q)$
5. $\sim p \Rightarrow (p \Rightarrow q)$
6. $\sim (p \Rightarrow q) \Rightarrow p$
7. $(p \wedge (p \Rightarrow q)) \Rightarrow q$
8. $(\sim p \wedge (p \vee q)) \Rightarrow q$
9. $(\sim q \wedge (p \Rightarrow q)) \Rightarrow \sim p$
10. $((p \Rightarrow q) \wedge (p \Rightarrow q)) \Rightarrow (p \Rightarrow q)$

Predicate Tautologies

11. $(\forall x P(x) \vee \forall x Q(x)) \Rightarrow \forall x (P(x) \vee Q(x))$
12. $\exists x (P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$

Rules of Inference

- Tautology and rule of inference
  - For each tautology with implication

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$$

    we get a rule of inference:

$$p_1,\ p_2, \ldots, p_n \rightarrow q$$

  - p_i's are hypotheses or premises, and q is called the conclusion.

$p_1,\ p_2 \rightarrow p_1 \wedge p_2$

（1）	$p_1 \Rightarrow (p_2 \Rightarrow p_1 \wedge p_2)$	Tautologies
（2）	$(p_2 \Rightarrow p_1 \wedge p_2)$	（1） and premise
（3）	$(p_1 \wedge p_2)$	（2） and premise

Proof of Implication

- If $p_1, p_2, \ldots p_n \rightarrow q$, then:
  - $p_1 \Rightarrow (p_2 \Rightarrow (\ldots \Rightarrow (p_n \Rightarrow q)..)$ is tautology.
  - $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$ is tautology.
- Example: prove $((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$

Partly or wholly substituted using logically equivalent expressions

1. $(p \Rightarrow q) \wedge (\sim q)$	Premise
2. $p \Rightarrow q$	Th.4(a)
3. $\sim q$	Th.4(b)
4. $\sim p \vee q$	Th.2(a), 2
5. $q \vee \sim p$	Th.1(1), 4
6. $\sim\sim q \vee \sim p$	Th.1(9), 5
7. $\sim q \Rightarrow \sim p$	Th.2(a), 6
8. $\sim p$ (conclusion)	Th.4(g), 3, 7 (modus ponens)

Basic Rules about Quantification

- US: $\forall x P(x) \rightarrow P(x)$
- UG: $P(x) \rightarrow \forall x P(x)$
- ES: $\exists x P(x) \rightarrow P(c)$
- EG: $P(c) \rightarrow \exists x P(x)$

$$\forall x(\sim P(x) \Rightarrow Q(x)) \Rightarrow (\forall x(\sim Q(x)) \Rightarrow \exists x P(x))$$

1. $\forall x(\sim P(x) \Rightarrow Q(x))$	Premise
2. $\forall x(\sim Q(x))$	Premise
3. $\sim P(x) \Rightarrow Q(x)$	US, 1
4. $\sim Q(x)$	US, 2
5. $\sim\sim P(x)$	Th.4(i), 4,3
6. $P(x)$	Double negation, 5
7. $\exists x P(x)$	

Somebody don’t want to walk

Premises:

1. Those who like walking don’t want to take bus.
2. Everyone either likes taking bus or likes riding bike.
3. Someone don’t want to ride bike.

Conclusion:

There are someone who don’t want to walk.

Premises: 1. $\forall x(W(x) \Rightarrow \sim B(x))$

2. $\forall x(B(x) \vee K(x))$

3. $\exists x(\sim K(x))$

Conclusion: $\exists x(\sim W(x))$

W(x): x likes walking

B(x): x likes taking bus

K(x): x likes riding bike

Somebody don't want to walk(cont.)

1. $\forall x(W(x) \Rightarrow \sim B(x))$	Premise
2. $\forall x(B(x) \vee K(x))$	Premise
3. $\exists x(\sim K(x))$	Premise
4. $\sim K(c)$	ES, 3
5. $W(c) \Rightarrow \sim B(c)$	US, 1
6. $B(c) \vee K(c)$	US, 2
7. $\sim\sim B(c) \vee K(c)$	Double negation, 6
8. $\sim B(c) \Rightarrow K(c)$	Th.2(a), 7
9. $\sim\sim B(c)$	Th.4(i), 4,8
10. $\sim W(c)$	Th.4(i), 9,5
11. $\exists x(\sim W(x))$	EG, 10

What's Wrong?

Somebody proves the expression:

$$\exists x A(x) \wedge \exists x B(x) \Rightarrow \exists x (A(x) \wedge B(x))$$

as follows:

1. $\exists x A(x) \wedge \exists x B(x)$	Premise
2. $\exists x A(x)$	Th.2(a), 1
3. $\exists x B(x)$	Th.2(b), 1
4. $A(c)$	ES, 2
5. $B(c)$	ES, 3
6. $A(c) \wedge B(c)$	Def. $\wedge$
7. $\exists x (A(x) \wedge B(x))$	EG, 6

Indirect Proof – Using Contraposition

- Prove that if n^2 is odd, then n is odd.
- Proof
  - Let p: n^2 is odd, and q: n is odd.
  - What is to be proved is: $p \Rightarrow q$.
  - Easy to see that:
    - Dealing with square (n to n^2) is easier than dealing with square root (n^2 to n)
  - So, we prove "if n is even, then n^2 is even", which is "$\sim q \Rightarrow \sim p$" and is equivalent to $p \Rightarrow q$

Proof by Contradiction

- The tautology:

$$(p \Rightarrow q) \Leftrightarrow ((p \wedge \sim q \Rightarrow \text{false})$$

- The method:
  - Goal: $p_1, p_2, ..., p_n \rightarrow q$
  - Extra hypothesis: $\sim q$
  - Process: $p_1, p_2, ..., p_n , \sim q \rightarrow$ an absurdity
  - Conclusion: there must be at least one false in $\{p_1, p_2, ..., p_n , \sim q\}$, that must be $\sim q$, so, q is true.

Proof by Contradiction: an Example

- There is no rational number whose square is 2.
- Proof:
  - Extra hypothesis: $(p/q)^2=2$, and p,q are integers which have no common factors except for 1.
  - Then, $p^2=2q^2 \rightarrow p^2$ is even $\rightarrow p$ is even $\rightarrow p^2$ is multiple of 4 $\rightarrow q^2$ is even $\rightarrow q$ is even $\rightarrow$ p,q have 2 as common factor $\rightarrow$ ***contradiction***

Dealing with Disjunction

Prove: n^2=m^2 if and only if m=n or m= -n, where m,n are integers.

Proof:

Let: p: n^2=m^2 , q: m=n, and r: m= -n.

Then, what is to be proved is: $p \Leftrightarrow (q \vee r)$

$\leftarrow$ (premise is a disjunction)

$(q \vee r) \Rightarrow p$ is true when both $q \Rightarrow p$ and $r \Rightarrow p$.

$q \Rightarrow p$: $m=n \rightarrow n^2=m^2$,

$r \Rightarrow p$: $m= -n \rightarrow n^2=m^2$,

Dealing with Disjunction (cont.)

$\rightarrow$ (conclusion is a disjunction)

$p \Rightarrow (q \vee r) \equiv p \Rightarrow (\sim q \Rightarrow r)$, which can be proved by

$$p, \mathbf{\sim q} \rightarrow r$$

that is: $n^2 = m^2,\ m \neq n \rightarrow m = -n$

Proof:

$n^2 = m^2 \rightarrow n^2 - m^2 = 0 \rightarrow (n+m)(n-m) = 0$

since $m \neq n$, we have $n-m \neq 0$, so, $n+m=0$

So, $m = -n$

Negating a Statement Using Counterexample

- Prove or disprove:

$$\exists x(A(x) \wedge B(x)) \Leftrightarrow \exists x A(x) \wedge \exists x B(x)$$

- Assume that:
  - The domain is the set of all natural number
  - $A(x)$: x is odd
  - $B(x)$: x is even
- Then, $\exists x A(x) \wedge \exists x B(x)$ = *True*, and $\exists x(A(x) \wedge B(x))$ = *False*. So, the above equivalence is disproved.

Loop Invariant

Computing the square of A(A is a positive integer):

FUNCTION SQ(A)

1. $C \leftarrow 0$
2. $D \leftarrow 0$
3. **WHILE** ($D \neq A$)
   a. $C \leftarrow C + A$
   b. $D \leftarrow D + 1$
4. **RETURN**(C)

END OF FUNCTION SQ

This is a loop, the body of which(statements a and b) will be executed repeatedly until D=A

C and D assume new values at the beginning of each new cycle of the loop. Let the value of C,D be C_n and D_n just after the nth cycle, with initial values of C_0 and D_0. Then the relation $\boldsymbol{C_n = A \times D_n}$ will be invariate all the time.

Correctness of Function SQ

Computing the square of A(A is a positive integer):

FUNCTION SQ(A)

1. $C \leftarrow 0$
2. $D \leftarrow 0$
3. **WHILE** ($D \neq A$)
   - a. $C \leftarrow$
   - b. $D \leftarrow$
4. **RETURN**

END OF FUN

Terminatio D

will es

It is easy to prove that the loop will terminat after exactly *A* cycles, which means that *D*=*A* at the end, so *C*=*A*² for any positive input *A*.

the exucution procedure, $_{n-1}+A$ and $D_n=D_{n-1}+1$, but $C_{n-1}=A\times D_{n-1}$ by induction hypothesis. So $C_n=(A\times D_{n-1})+A=A\times(D_{n-1}+1)=A\times D_n$

Exact Cover Problem

- definition of exact cover of a set:
  - Given a set A and a finite number of A: $A_1, A_2, \ldots A_k$, a exact cover of A with respect to the A_i's is a set $S \subseteq \{A_1, A_2, \ldots A_k\}$, satisfying:
    - Any two sets in S are disjoint, and
    - $\cup S = A$
  - Mathematically, we call S a partition of A.
- An example: $A=\{a,b,c,d,e,f,g,h,i,j\}$; $A_1=\{a,c,d\}$, $A_2=\{a,b,e,f\}$, $A_3=\{b,f,g\}$, $A_4=\{d,h,i\}$, $A_5=\{a,h,j\}$, $A_6=\{e,h\}$, $A_7=\{c,i,j\}$, $A_8=\{i,j\}$
  - The exact cover is $\{A_1, A_3, A_6, A_8\}$

Representation Using Matrix

Let $|A|=n$, and there are m subsets for A_i's, we can represent the input of exact cover problem as a $m \times n$ matrix, with each row for a A_i .

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Solution:

Find a collection of rows of M: r_1, $r_2, \ldots r_k$, satisfying:

$r_i \wedge r_j = \mathbf{0}$ for $1 \le i,j \le k$, and

$r_1 \vee r_2 \vee \ldots \vee r_k = \mathbf{1}$

where $\mathbf{0}=[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$

$\mathbf{1}=[1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$

and, $\wedge$ is boolean product, $\vee$ is boolean sum

Algorithm X for Exact Cover

- input: matrix A
- Initialization: label the rows of A;
- $M=A$; $L=\{\}$;
- (1) If there is a column of 0's in M, return "No solution"
- (2) Otherwise:
  - Choose the column c with the fewest 1's;
  - Choose a row r with a 1 in column c, $L=L\cup\{r\}$;
  - Eliminate any row r_i having the property: $r \wedge r_i \neq \mathbf{0}$;
  - Eliminate all columns in which r has a 1;
  - Eliminate row r;
  - If No row and column left, then output L, otherwise repeat (1) and (2) on resulted M;

Solving Soduku by Covering

- Describe the problem in suitable form
  - 9 constraints for cells
  - 9 constraints for columns
  - 9 constraints for rows
- Construct the matrix of covering
  - 27 columns for constraints
  - 27 rows for “moves”

Why can the algorithm X solve the 3×3 pseudo-Soduku using the matrix constructed as above?

Logic about Award(Revisited)

- Smith, Brown, Jones, Robinson will be granted awards for Math, English, French and Logic, respectively, with each award for one person.
- They guessed which-for-which as following:
  - Smith: Robinson will win the award for Logic.
  - Brown: Jones will win the award for English.
  - Jones: Smith will not win the award for Math.
  - Robinson: Brown will win the award for French.
- It turned out that only winner of Math and Logic Awards made the correct guesses.
- Problem: Can you tell who win what exactly?

Logic, English, Math, French
Smith, Brown, Jones, Robinson
编码方式：课程名(人名)表示人获得课程奖励

公式化（1）

- With each award for one person.
- 每门课有且只有一人获奖
  - $(L(S) \wedge !L(B) \wedge !L(J) \wedge !L(R)) \vee (!L(S) \wedge L(B) \wedge !L(J) \wedge !L(R)) \vee (!L(S) \wedge !L(B) \wedge L(J) \wedge !L(R)) \vee (!L(S) \wedge !L(B) \wedge !L(J) \wedge L(R))$
  - $(E(S) \wedge !E(B) \wedge !E(J) \wedge !E(R)) \vee (!E(S) \wedge E(B) \wedge !E(J) \wedge !E(R)) \vee (!E(S) \wedge !E(B) \wedge E(J) \wedge !E(R)) \vee (!E(S) \wedge !E(B) \wedge !E(J) \wedge E(R))$
  - $(M(S) \wedge !M(B) \wedge !M(J) \wedge !M(R)) \vee (!M(S) \wedge M(B) \wedge !M(J) \wedge !M(R)) \vee (!M(S) \wedge !M(B) \wedge M(J) \wedge !M(R)) \vee (!M(S) \wedge !M(B) \wedge !M(J) \wedge M(R))$
  - $(F(S) \wedge !F(B) \wedge !F(J) \wedge !F(R)) \vee (!F(S) \wedge F(B) \wedge !F(J) \wedge !F(R)) \vee (!F(S) \wedge !F(B) \wedge F(J) \wedge !F(R)) \vee (!F(S) \wedge !F(B) \wedge !F(J) \wedge F(R))$
- 每个人至少获得一项奖励（这个有点多余）
  - $(L(S) \vee E(S) \vee M(S) \vee F(S)) \wedge (L(B) \vee E(B) \vee M(B) \vee F(B)) \wedge (L(J) \vee E(J) \vee M(J) \vee F(J)) \wedge (L(R) \vee E(R) \vee M(R) \vee F(R))$

公式化（2）

Smith: Robinson will win the award for Logic.	L(R)
Brown: Jones will win the award for English.	E(J)
Jones: Smith will not win the award for Math.	M(S)
Robinson: Brown will win the award for French.	F(B)

- Only winner of Math and Logic Awards made the correct guesses.
- 如果X获得了数学或者逻辑奖励，则X的猜测是正确的
  - M(S) => L(R)，M(B) => E(J)，M(J) => !M(S)，M(R)=>F(B)
  - L(S) => L(R)，L(B) => E(J)，L(J) => !M(S)，L(R)=>F(B)
- 如果X没有获得数学或逻辑奖励，则X的猜测不成立
  - !M(S) & !L(S) => !L(R)，!M(B) & !L(B) => !E(J)，
  - !M(J) & !L(J) => !M(S)，!M(R) & ! L(R) => !F(B)

Home Assignments

- To be checked
  - pp.55- 12, 15-16, 18, 28, 30, 32, 35
  - pp.60- 6-7, 12-16, 24, 27-35
  - pp.67- 8, 12, 18, 20, 22-24, 30
  - pp.73- 20, 22, 26, 28, 30, 34, 36
  - pp.78 20-25