Mathematics for CS

30 September 2019 17:05

https://warwick.ac.uk/fac/sci/dcs/teaching/material/cs130/

Rosen, Discrete Maths and its Applications
Ross and Wright, Discrete Mathematics
Truss, Discrete Mathematics for Computer Science

Read about proof – Bloch, Proofs and Fundamentals: A First Course in Abstract Mathematics

CS130 Maths for CS 1 – Discrete Maths
CS131 Maths for CS 2 – Continuous Structures

- Logic
- Sets
- Relations
- Functions
- Induction
- Graphs
- Probability

Discrete Maths
Study of discrete structures, e.g. integer numbers, finite or countable sets, finite or countable relations
Less concerned with continuous structures, e.g. real numbers, continuous functions, limits, derivatives
Discrete maths is intimately related to computation and therefore computer science

Four sets of assessed exercises. Thursday week 2, 4, 6, 8, to be submitted noon of week 3,5,7,9

Graphs

28 November 2019 22:30

A graph is an abstraction of a network
Connections between nodes represent relations
A graph is a subset of the cartesian product

Bipartite graphs (a case of a k-partite graph where k = 2) is a graph in which two sets of vertices (nodes) that are disjoint such that no two vertices within the same set are adjacent

Bipartite graphs are equivalent to two-color graphs. All acyclic graphs are bipartite. A cyclic graph can be bipartite iff all its cycles are of even length

A graph is **complete** when there is an edge between all nodes

A walk is a sequence of nodes with an edge between adjacent nodes

A walk that ends up at the same vertice is a closed walk

A walk that ends up away from its initial vertice is an open walk

A trail is a walk where all edges are traversed at most once.

If two nodes are connected by a walk then they are in a relation

A tour is a walk from a node to itself (a closed walk)

1 element in a graph is still a tour

Introduction to Proof

02 October 2019 10:13

Infinite sets do have a size, beyond natural numbers
Infinite sets can have different sizes
There exists no set of all sets, and this can be proved

Proof

Natural science is based on evidence, mathematics is based on proof.
Proofs need precise and concise language.
The grammar of this language is logic.

All eagles can fly
Therefore for all x, eagle(x) -> canfly(x)

Some pigs are not eagles
Therefore for some y, pig(y) ^ ¬canfly(y)

By (1) ¬canfly(y) => ¬eagle(x) - if it can't fly, its not an eagle

Some statements are axiomatic and do not need definition

Proving that Neven is an infinite set
Proof by contradiction
Start by assuming that a number exists, b, that is the sum of the set, then disprove that it exists

Neven = {2,4,6,8...}
There is a number b such that size(Neven) = b
A = {2,4,6,8 … , 2b, }
B = {2,4,6,8,… , 2b, 2b + 2}
B contains a set of numbers greater than b, therefore the statement is contradicted.

Logic

02 October 2019 10:45

True and False are the basic elements of logic, similar to how numbers are the basic elements of arithmetic

Statements can only be true or false, not both
e.g. "five is less than ten" == value(5<10) = T

Value("blue") = undefined

Like arithmetic operators, logical operators exist. <=> means equivalent too

Logical operation	Logical symbol	Macro
There is	$\exists$	(isE)
There is exactly	$\exists!$	(isE!)
if, then	$\supset$	ifthen
inclus. or	$\vee$	vr*
exclus. or xor	$\oplus$	vr**
and	$\wedge$	a*d
logical. equiv.	$\equiv$	lgeq
material. equiv.	$\Leftrightarrow$	mteq
Because	$\because$	b/c*
For all	$\forall$	fral*
proport. to	$\propto$	prpto*
intersection	$\cap$	nxn
union	$\cup$	uni*
tilde	$\sim$	tld*
asymptot. equal	$\approx$	aeql*
is true	$\models$	isT*
is not true	$\not\models$	isnT*
necessarily	$\Box$	ncsry
element of	$\in$	lmnt
inferred from	$\vdash$	infr*

Implication

Think of the implication symbol as merely another operator, to avoid confusion.
IF A THEN B: A → B
True if A

A	B	A→B
F	F	T
F	T	T
T	F	F
T	T	T

If second row was not as it is, the following could happen;
1+2=4 => 3 = 4 => 3.0 = 4.0 => 0 = 0

Implication can be hidden in many sentences

- A implies B
- B is necessary for A
- A is sufficient for B
- A is stronger than B
- A leads to B
- B follows from A
- B is implied by A
- B is weaker than A
- A if B
- P only if Q
- Q provided that P
- Assuming P, then Q
- Q given that P

Equivalence (Biconditional)

The statement that, intuitively, is true if P and Q are both true or both false, and is false otherwise.
We read P ↔ Q as "P if and only if Q."
The phrase "if and only if" is often abbreviated as "iff."
↔ is true if A and B agree e.g. TT or FF. TF or FT results in false.

It is common to say "P is necessary and sufficient for Q."

2 equal sides ↔ 2 equal angles
Proof:
Let a triangle have 2 equal sides
We now assume this statement to be true
→ … some logical reasoning => therefore 2 equal angles

An example of a biconditional statement is "I will go for a walk if and only if Fred will join me." This statement has the form P ↔ Q, where P = "I will go for a walk," and Q = "Fred will join me." The truth of this statement does not say that I will go for a walk, or that Fred will join me. It says that either Fred will join me and I will go for a walk, or that neither of these things will happen. In other words, it could not be the case that Fred joins me and yet I do not go for a walk, and it also could not be the case that I go for a walk, and yet Fred has not joined me.

A **tautology** is a statement that is always true by logical necessity, regardless of whether the component statements are true or false, and regardless of what we happen to observe in the real world.
A **contradiction** is a statement that is always false by logical necessity.

Relations Between Statements

23 October 2019 23:02

Relations between statements are not formal statements in themselves, but are “meta-statements" that we make about statements.
An example of a meta-statement is the observation that:

- “if the statement ‘Ethel is tall and Agnes is short’ is true, then the statement ‘Ethel is tall’ is true.”
- “the statement "Katie has brown hair or Mel has red hair’ being true is equivalent to the statement ‘Mel has red hair or Katie has brown hair’ being true.”
- Yes this is true

Implication

The intuitive idea of logical implication is that **statement P implies statement Q if necessarily Q is true whenever P is true**.
In other words, it can never be the case that P is true and Q is false. **Necessity is the key here**, because one statement implying another should **not simply be a matter of coincidentally appropriate truth values**

¬(P → Q) implies P ∨ Q

We abbreviate the English expression “P implies Q” with the notation “P ⇒ Q.”

- It is important to note the difference between the notations “P ⇒ Q” and “P → Q.”
- The notation “P → Q” is a statement; it is a compound statement built up out of the statements P and Q.
- The notation “P ⇒ Q” is a meta-statement, which is simply a shorthand way of writing the English expression “P implies Q,” and it means that P → Q is not just true in some particular instances, but is a tautology.

Equivalence

Logical implication is not always reversible. Some logical implications, however, are reversible. Such implications are very convenient, and they convey the idea of logical equivalence.

It is important to note the difference between the notations “P ⇔ Q” and “P ↔ Q.”
The latter is a statement, whereas the former is a meta-statement, which is simply a shorthand way of writing the English expression “P is equivalent to Q.”

Laws

1. P∧(Q∨R) ⇔ (P∧Q)∨(P∧R) (Distributive Law)
2. P → Q ⇔ ¬P∨Q
3. P → Q ⇔ ¬Q → ¬P (Contrapositive)
4. P ↔ Q ⇔ (P → Q)∧(Q → P)
5. ¬(P∧Q) ⇔ ¬P∨ ¬Q (De Morgan’s Law)
6. ¬(P∨Q) ⇔ ¬P∧ ¬Q (De Morgan’s Law)

A reformulation of the biconditional in terms of conditionals

For example, the statement “I will play the flute today if and only if I listen to the radio” is equivalent to the statement

“if I play the flute today I will listen to the radio, and if I listen to the radio I will play the flute today.”

The equivalence of law 4, $P \leftrightarrow Q$ and $(P \rightarrow Q) \wedge (Q \rightarrow P)$ says that to prove a statement of the form $P \leftrightarrow Q$, it is sufficient to prove $(P \rightarrow Q) \wedge (Q \rightarrow P)$; it therefore suffices to prove each of $(P \rightarrow Q)$ and $(Q \rightarrow P)$

Contrapositive

Given a conditional statement of the form $P \rightarrow Q$, we call $\neg Q \rightarrow \neg P$ the contrapositive of the original statement
“if I eat too much I will feel sick” is “if I do not feel sick I did not eat too much.”

Arguments

An argument is a collection of statements that are broken up into premises and a conclusion.
An argument is VALID if the conclusion NECESSARILY follows from the premises.

Proof

08 October 2019 22:15

Proof By Contradiction

In logic and mathematics **proof by contradiction** is a form of proof that establishes the truth or validity of a proposition by showing that assuming the proposition to be false leads to a contradiction. Proof by contradiction is also known as **indirect proof**, **proof by assuming the opposite**, and ***reductio ad impossibile***.

- Start with a statement
- Follow it through logically until a contradiction occurs
- Back propagate the false until you get to the false statement (assuming that the logical steps taken are all correct then the false statement will be the initial precondition set out in the beginning of the proof)

This doesn't work when you arrive to a true statement.
e.g. if your initial assumption is incorrect, you can imply correct logic and the result will be true, but back-propagating doesn't reveal this falsehood, for example:

1. assume 1=2
2. 0.1 = 0.2
3. 0=0 is true
4. Therefore 1=2

The logic is correct but the precondition undermines the validity of the proof

e.g. root 2 is irrational

Direct Proof

In direct proof, the conclusion is established by logically combining the axioms, definitions and earlier theorems.

E.g. the sum of two even integers is always even

Consider two even integers x and y
They are even, so x = 2a, y = 2b
X + y = 2a + 2b = 2(a + b)
X + y therefore has a factor of 2
By definition, anything with a factor of two is even

This proof uses the definition of integers, the integer properties of closure under addition and multiplication, and distributivity.

Working on Proof

10 October 2019 10:25

The implies symbol can be ambiguous depending on how you evaluate it
(F => T) => F evaluates to F
F => (T => F) evaluates to T

When proving ,=>, you must it through the proof
Alternatively, prove both => and <=

Logical Priorities
NOT, (AND. OR), (=>, <=>)

Laws of Boolean logic (hold for all A, B, C):

$\neg\neg A \iff A$	*double negation*
$A \wedge A \iff A$	$\wedge$ *idempotent*
$A \vee A \iff A$	$\vee$ *idempotent*
$A \wedge B \iff B \wedge A$	$\wedge$ *commutative*
$A \vee B \iff B \vee A$	$\vee$ *commutative*
$(A \wedge B) \wedge C \iff A \wedge (B \wedge C)$	$\wedge$ *associative*
$(A \vee B) \vee C \iff A \vee (B \vee C)$	$\vee$ *associative*
$A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$	$\wedge$ *distributes over* $\vee$
$A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$	$\vee$ *distributes over* $\wedge$

Compare $a \cdot (b + c) = a \cdot b + a \cdot c$, but $a + b \cdot c \neq (a + b) \cdot (a + c)$

Logical Operators

14 October 2019 15:10

Material Conditional →

The material conditional, (also know as material implication, consequence) is a logical connective that is symbolized by the forward arrow.

The material conditional is used to form statements of the form:
p → q (called a conditional statement)
This translates to "if p then q"

Unlike the construction in English "if … then …" the material conditional statement does not conventionally specify a causal relationship between p and q, e.g. "p is the cause and q is the consequence from it". This is not generally a valid interpretation.

It generally just means, that "if p is true, then q is also true", such that the only time when this is false is when p is true and q is false.

Logical Consequence

A fundamental concept in logic, which describes the relationship between statements that hold true when one statement logically follows from one or more statements.

A valid logical argument is one in which the conclusion is entailed by the premises, because the conclusion is the consequence of the premises.

Predicates

15 October 2019 12:37

A predicate is a sentence with variables, which becomes true or false when values are substituted in

Let $P(x)$ be a predicate

$\{x \mid P(x)\}$: the set of *all* x, such that $P(x)$ is true

Range often made explicit: $\{x \in S \mid P(x)\}$

In particular: $\{x \in S \mid T\} = S \quad \{x \in S \mid F\} = \emptyset$

For each variables, its values are taken from a particular set (the variables range)

We always assume the predicate has > 1 variables (else it would be a sentence) and the predicate has a range that is nonempty (always)

X < Y (x,y in N)

Quantifiers
Existential (FOR SOME x, P(x)):
Universal (FOR ALL x, P(x));

If P(X) is the predicate (sentence with variables)
Then ∀x:p(x) denotes p(x1) AND p(x2) AND p(x3) etc
∃x:p(x) denotes p(x1) OR p(x2) OR p(x3) etc...

Existential quantification ∃

- "There exists an element x in the domain such that p(x) (is true)"
- Denote that as $\exists x \quad p(x)$ where $\exists$ is the existential quantifier
- In English, "for some", "for at least one", or "there is"
- Read as "There is an x such that p(x)", "There is at least one x such that p(x)", or "For some x, p(x)"

12

∀x:T <=> T
∀x:F <=> F
∃x:T <=> T
∃x:F <=> F

$(\forall x : T) \iff T \qquad (\forall x : F) \iff F$
$(\exists x : T) \iff T \qquad (\exists x : F) \iff F$

Assuming Q does not contain free x:

$\forall x : (P(x) \wedge Q) \iff (\forall x : P(x)) \wedge Q$
$\exists x : (P(x) \wedge Q) \iff (\exists x : P(x)) \wedge Q$

These hold also for $\ldots \vee Q$

De Morgan's laws for predicates:

$\neg\forall x : P(x) \iff \exists x : \neg P(x)$
$\neg\exists x : P(x) \iff \forall x : \neg P(x)$

Quantifiers — handle with care!

$\forall x : (P(x) \wedge Q(x)) \iff (\forall x : P(x)) \wedge (\forall x : Q(x))$
$\exists x : (P(x) \vee Q(x)) \iff (\exists x : P(x)) \vee (\exists x : Q(x))$

But:

$\forall x : (P(x) \vee Q(x)) \not\iff (\forall x : P(x)) \vee (\forall x : Q(x))$ (why?)

However, "$\Longleftarrow$" holds

$\exists x : (P(x) \wedge Q(x)) \not\iff (\exists x : P(x)) \wedge (\exists x : Q(x))$ (why?)

However, "$\Longrightarrow$" holds

Examples for $P(x)$ and $Q(x)$?

Set Operations

25 October 2019 16:43

There are a number of ways to make new sets out of old, somewhat analogous to combining numbers via addition and multiplication

The union of A and B, denoted A∪B, is the set defined by **A∪B = {x | x ∈ A or x ∈ B}**

The intersection of A and B, denoted A∩B, is the set defined by **A∩B = {x | x ∈ A and x ∈ B}**

Laws

- A∪B = B∪A and A∩B = B∩A (Commutative Laws)
- (A∪B)∪C = A∪(B∪C) and (A∩B)∩C = A∩(B∩C) (Associative Laws)
- **A∩(B∪C) = (A∩B)∪(A∩C) and A∪(B∩C) = (A∪B)∩(A∪C)** (Distributive Laws)
- A∪ ∅ = A and A∩ ∅ = ∅ (Identity Laws)
- A∪A = A and A∩A = A (Idempotent Laws)
- A∪(A∩B) = A and A∩(A∪B) = A (Absorption Laws)

Proof for (A ∪ B) ∪C = A ∪ (B ∪C)

We will show that (A ∪ B) ∪C = A ∪ (B ∪C)
As usual, the equality of the two sets under consideration is demonstrated by showing that each is a subset of the other

Let x ∈ (A∪B)∪C
Then x ∈ A∪B or x ∈ C
First, suppose that x ∈ A∪B
Then x ∈ A or x ∈ B
If x ∈ A then x ∈ A∪(B∪C) by Part (2) of this theorem, and if x ∈ B
Then x ∈ B ∪C, and hence x ∈ A ∪ (B ∪C)
Second, suppose that x ∈ C
It follows from Part (2) of this theorem that x ∈ B∪C, and hence x ∈ A∪(B∪C)

Putting the two cases together, we deduce that (A∪B)∪C ⊆ A∪(B∪C).

The proof that A ∪ (B ∪C) ⊆ (A ∪ B) ∪C is similar to the above proof, simply changing the roles of A and C, and we omit the details

Once proved both ways, it follows that the two sides of the equation are equal.

Proof that A∩(B∪C) = (A∩B)∪(A∩C)

We prove A∩(B∪C) = (A∩B)∪(A∩C)
the other equation can be proved similarly

Let x ∈ A∩(B∪C)
Then x ∈ A and x ∈ B∪C
Hence x ∈ B or x ∈ C
If x ∈ B we deduce that x ∈ A ∩ B, and if x ∈ C we deduce that x ∈ A ∩C
In either case, we use Part (2) of this theorem to see that x ∈ (A ∩ B) ∪ (A ∩C)
Therefore A∩(B∪C) ⊆ (A∩B)∪(A∩C)

Now let y ∈ (A∩B)∪(A∩C)
Then y ∈ A∩B or y ∈ A∩C
First, suppose that y ∈ A∩B
Then y ∈ A and y ∈ B
Hence y ∈ B∪C by Part (2) of the theorem, and therefore y ∈ A∩(B∪C)
Second, suppose that y ∈ A∩C

A similar argument to the previous case shows that y ∈ A ∩ (B ∪C); we omit the details
Combining the two cases we deduce that (A∩B)∪(A∩C) ⊆ A∩(B∪C)
We conclude that A∩(B∪C) = (A∩B)∪(A∩C).

Proof Of De Morgans Laws

$$\begin{aligned}\overline{A \cap B} = S \setminus (A \cap B) = \\ \{x \mid (x \in S) \wedge \neg(x \in A \cap B)\} = \\ \{x \mid (x \in S) \wedge \neg((x \in A) \wedge (x \in B))\} = \\ \{x \mid (x \in S) \wedge (\neg(x \in A) \vee \neg(x \in B))\} = \\ \{x \mid ((x \in S) \wedge \neg(x \in A)) \vee ((x \in S) \wedge \neg(x \in B))\} = \\ \{x \mid (x \in S \setminus A) \vee (x \in S \setminus B)\} = \\ \{x \mid (x \in \bar{A}) \vee (x \in \bar{B})\} = \bar{A} \cup \bar{B} \quad \square\end{aligned}$$

Cartesian Product

Let A and B be sets
The product (also called the Cartesian product) of A and B, denoted A×B, is the set
A×B = {(a,b) | a ∈ A and b ∈ B}
where (a,b) denotes an ordered pair.

Example
Let A = {a,b, c} and B = {1,2}
Then **A×B = {(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)}**

Laws

- If A ⊆ B and C ⊆ D, then A×C ⊆ B×D
- A×(B∪C) = (A×B)∪(A×C) and (B∪C)×A = (B×A)∪(C×A) (Distributive Laws)
- A×(B∩C) = (A×B)∩(A×C) and (B∩C)×A = (B×A)∩(C×A) (Distributive Laws)
- A× ∅ = ∅ and ∅×A = ∅
- (A∩B)×(C∩D) = (A×C)∩(B×D).

Proof that A × (B∩C) = (A × B)∩(A ×C)

As usual, we will show that the sets on the two sides of the equation are subsets of each other
First, we show that (A × B)∩(A×C) ⊆ A×(B∩C)
This part of the proof proceeds in the standard way
Let y ∈ (A×B)∩(A×C)
It would not be correct at this point to say that y equals some ordered pair (p,q), because (A×B)∩(A×C) does not have the form X ×Y for some sets X and Y
We can say, however, that y ∈ A×B and y ∈ A×C. Using the former we deduce that y = (a,b) for some a ∈ A and b ∈ B

Because $y \in A \times C$, we then have $(a,b) \in A \times C$
It follows that $b \in C$
Hence $b \in B \cap C$
Therefore $y = (a,b) \in A \times (B \cap C)$
We deduce that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$
Next, we show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$
In this part of the proof we take a slightly different approach than the one we have been using so far (though the standard method would work here too)
By Lemma 3.2.4 (1) we know that $A \subseteq A$. Using the first sentence in Theorem 3.3.3 (1) we know that $B \cap C \subseteq B$ and $B \cap C \subseteq C$
By Part (1) of this theorem we deduce that $A \times (B \cap C) \subseteq A \times B$ and $A \times (B \cap C) \subseteq A \times C$
It now follows that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$
We conclude that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Observe that A×B is not the same as B×A, unless A and B happen to be equal

Quantification

25 October 2019 10:29

We often encounter expressions which we wish to prove, that are not precise, because they do not state the possible values of X under consideration.

X * X > 8, for all real numbers X > 2

"For all real numbers X > 2" is an example of a quantifier

"There exists a real number X such that X * X > 9" is another example of a quantifier

The type of logic that uses quantifiers is called **Predicate** logic

Bound and Unbound Variables

“for all positive real numbers x, the inequality x+y > 0 holds.”

Here, X is called a bound variable because we cannot chose which values of X we want to consider
Y is called a free variable, because its possible values are not limited

Because Y is a free variable, it is often useful to write Q(y) instead of just Q. to show Y is free.

Quantifiers

Universal

Let P(x) be an expression with free variable (a predicate)
Let U denote a collection of possible values of x

$(\forall x \text{ in } U)P(x)$, which is true if P(x) is true for all possible values of x in U
(For all X in U, P(X)) - Statement is true if all values of X in U fulfil the requirements of the predicate

“if x is in U, then P(x) is true.”
The truth of the statement “if x is in U, then P(x) is true” does not say anything about what happens if X is in U.
That is, if the statement is true, then it tells us only about P(x) when x is in U

It might or might not be true that P(x) is true for some x values not included in U, but this statement does not tell us that

Ways of writing this statement in English:

- For all values of x in U, the statement P(x) is true
- For each x in U, the statement P(x) is true
- The statement P(x) is true for all x in U
- All values of x in U satisfy the P(x).

Let S(n) = “n is a perfect square greater than 1,”
C(n) = “n is a composite number” (a composite number is an integer that is not a prime number)
where the collection of possible values of n is the integers
$(\forall n)[S(n) \rightarrow C(n)]$

“for all integers n, if n is a perfect square greater than 1, then n is a composite number”
This statement is true

Empty U

For the sake of completeness, we need to allow the case where the collection U has nothing in it. In that case, the statement (∀x in U)P(x) is always true, no matter what P(x) is
The statement “(∀x in U)P(x)” is equivalent to the statement “if x is in U, then P(x) is true.” When the collection U has nothing in it, then the statement “x is in U” is false, and hence the conditional statement “if x is in U, then P(x) is true” is true.

Existential

- There exists some x in U such that P(x) holds
- There is x in U such that P(x) holds
- There exists at least one x in U such that P(x) holds
- For some value of x in U, the condition P(x) holds
- It is the case that P(x) is true for some x in U

An existential quantifier applied to P(x) is the statement, denoted (∃x in U)P(x), which is true if P(x) is true for at least one value of x in U.

If the collection U is understood from the context, then we will write (∃x)P(x).

Observe that if the collection U has nothing in it, then the statement (∃x)P(x) is false.

It is important to note that the phrase “at least one value of x in U” means one or more, possibly many, or even all x in U.
In particular, **if (∀x in U)P(x) is true, then (∃x in U)P(x) is true**, except in the special case that U has nothing in it.

Let E(m) = “m is an even number”
let M(m) = “m is a prime number,” where the collection of possible values of m is the integers.
The statement “some integers are even and prime” can be expressed symbolically by first rephrasing it as “there exists x such that x is even and x is prime,”
(∃x) [E(x) ∧ M(x)]
(this statement is true, because 2 is both even and prime).

We can form statements with more than one quantifier, as long as **different quantifiers involve different variables**
The order of the quantifiers matters

Laws

¬[(∀x in U)P(x)] ⇔ (∃x in U)(¬P(x))

If the original statement was "all pigs have wings" then the negation of that statement would be "Some pigs do not have wings" which is achieved by switching out the quantifier and negating the function.
E.g. if P(x) = "X has wings" then ¬P(x) = "it is not that case that X has wings"

¬[(∃x in U)P(x)] ⇔ (∀x in U)(¬P(x))

If the original statement was "Some people like chocolate" then the negation of that statement

would be "All people do not like chocolate" which would be achieved by switching the existential quantifier to universal and negating the predicate.
The statement would then read "For all x, it is not the case that x likes chocolate"

Sets

17 October 2019 10:39

The empty set is a member of all sets. This can pre proved with the following:

Set A is *a subset* of set B, if all elements of A are also elements of B (but not necessarily the other way round)

$A \subseteq B \iff \forall x : x \in A \Rightarrow x \in B$

Proof by contradiction that the empty set is a subset of all sets

Suppose that $\emptyset \not\subseteq A$. Then there exists some $x \in \emptyset$ such that $x \notin A$. This statement cannot be true, however, because there is no x such that $x \in \emptyset$. We have therefore reached a contradiction, and hence the desired result is true.

Proof by contradiction that only one empty set exists

Assume that there are 2 sets, E1 and E2 that are different
E1 is a member of E2 (we know that the empty set is a member of all sets)
E2 is a member of E1
Therefore E2 is equivalent to E1
Contradiction

The axioms of set theory

Proving set A is equivalent to set B

Let $a \in A$. . . .
(argumentation) . . .
Then $a \in B$
Therefore $A \subseteq B$

Next, Let $b \in B$. . . .
(argumentation)
. . Then $b \in A$
Hence $B \subseteq A$

We conclude that A = B.

Powersets

Let A be a set. The power set of A is the denoted by P(A) and is the set defined by **$P(A) = \{X \mid X \subseteq A\}$**

Because $\emptyset \subseteq \emptyset$, then $P(\emptyset) = \{\emptyset\}$. In particular, we see that $P(\emptyset) \neq \emptyset$

Let A = {a, b, c} P(A) = {∅,{a},{b},{c},{a,b},{a,c},{b,c},{a,b,c}}.

If A is a finite set with n elements, then P(A) is a finite set with 2n elements

We see that this formula holds even when n = 0 (2 to the power 0 = 1)

If S is infinite then P(S) is infinite

Properties of the Powerset

- $P(A \cap B) = P(A) \cap P(B)$
- In general, $P(A \cup B) \neq P(A) \cup P(B)$ (why?)
  However, $\supseteq$ holds
- In general, $P(A \setminus B) \neq P(A) \setminus P(B)$ (why?)
  Neither $\subseteq$ nor $\supseteq$ holds

Partitions and Equivalence

06 November 2019 11:49

Partitions

The relation induced by the partition of a set satisfies all 3 properties – reflexivity, symmetry and transitivity. The induced relation is therefore an equivalence relation

Theorem. Set A is *partitioned* by relation $R_\sim$ into a *disjoint union* of equivalence classes

In other words, the equivalence classes of $R_\sim$ are

- pairwise disjoint
- cover the whole A

If A finite, $A/R_\sim$ finite

If A has n elements, and if every $[a]_\sim$ has m elements, then $m \mid n$, and $A/R_\sim$ has n/m elements (hence the "/" notation)

If A infinite, $A/R_\sim$ can be finite or infinite

Equivalence Relation

A relation that is reflexive, symmetric and transitive. Examples of equivalence relationships are abundant:

- A and B are born in the same year
- A and B are born on the same day
- A is in the same family as B
- A and B are parallel lines in a plane
- A and B both have congruence modulo n

~ is the symbol for equivalence

For any element a ∈ A, the equivalence class of a, denoted **[a]~**, is the set of all elements in A related to a

congruence modulo

Let $n \in \mathbb{N} \setminus \{0\}$

$R_{\equiv_n} : \mathbb{Z} \leftrightarrow \mathbb{Z} \qquad a \equiv_n b \iff n \mid (a - b)$

$R_{\equiv_n}$ is called *congruence modulo n*

$R_{\equiv_{12}}$: the "clock arithmetic"

Proving Equivalence Relations

- Prove that the relation is reflexive by showing that the relation holds for x when it is applied to itself
- Prove that the relation is symmetric by showing that the result of A relation B is the same as the result of B relation A
- Prove the relation is transitive by showing that the relation between A and B, and B and C, implies a relation between A and A.

Equivalence Classes

The importance of equivalence classes is that every element within the equivalence relation only belongs to one equivalence class.

Therefore the equivalence classes are **pairwise disjoint** and the **union of all equivalence classes is the whole set A.**

The equivalence classes therefore represent a partition of the set A.

Let $R_\sim : A \leftrightarrow A$ be an equivalence relation Let $a \in A$

The *equivalence class of a* is the set of all elements related to a

$[a]_\sim = \{x \in A \mid x \sim a\}$

By reflexivity, $a \in [a]_\sim$

For example, an equivalence relation may be 'A shares the same birth month as B'
The equivalence classes for this would therefore be the months; there would be a class for Jan, Feb etc

Quotient Sets

The quotient set is the set of all equivalence classes.

The set of all equivalence classes of $R_\sim$ is *the quotient set of A with respect to* $R_\sim$

$A/R_\sim = \{[a]_\sim \mid a \in A\}$

A / R_ signifies the quotient set of A (the set of all equivalence classes)

Example: $R_{\equiv_5} : \mathbb{Z} \leftrightarrow \mathbb{Z}$ $a \equiv_5 b \iff 5 \mid (a - b)$

$[0]_{\equiv_5} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$
$[1]_{\equiv_5} = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$[2]_{\equiv_5} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$
$[3]_{\equiv_5} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$
$[4]_{\equiv_5} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

$[m]_{\equiv_5} = \{m + 5k \mid k \in \mathbb{Z}\}$ for all $m \in \mathbb{Z}$

The equivalence classes of $R_{\equiv_n}$ are called *residue classes modulo n*

Partial and Fully Ordered

06 November 2019 11:40

Relation $R_{\preceq} : A \leftrightarrow A$ is called *a partial order*, if it is

- reflexive
- *anti*symmetric
- transitive

In this case, set A is called *partially ordered*

Relation $R_{\preceq} : A \leftrightarrow A$ is called *a total order*, if

- it is a partial order
- for all $a, b \in A$, either $a \preceq b$ or $b \preceq a$

In this case, set A is called *totally ordered*

Note that a total order remains technically partial!

Example of a partial order

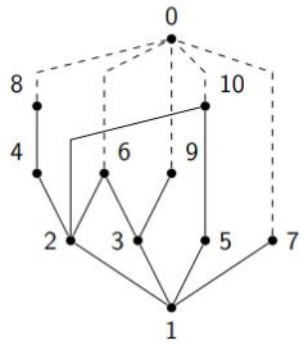
A partial order exists when a relation is reflexive, antisymmetric (no two different elements precede each other) and transitive.

Note that because a relation can be antisymmetric and symmetric at the same time, a relation can therefore be both equivalent and partially or totally ordered simultaneously.

Example:

$R_{|} : \mathbb{N} \leftrightarrow \mathbb{N} \qquad x \mid y \iff \exists k : k \cdot x = y$

A partial order, but not a total order



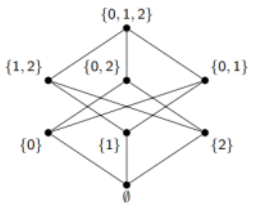
For partial orders (need not be total) we can define the following:

Example:

$R_{\subseteq} : \mathcal{P}(S) \leftrightarrow \mathcal{P}(S)$

A partial order, but not a total order (unless S is empty or a singleton)

$S = \{0, 1, 2\}$



Least Upper Bound

Greatest Upper Bound

Let $R_{\preceq} : A \leftrightarrow A$ be a partial order (need not be total)

Let $a, b \in A$

$c \in A$ is *the least upper bound of* a, b, if

- $(a \preceq c) \wedge (b \preceq c)$

Example:

$R_{\trianglelefteq} : People \leftrightarrow People \qquad x \trianglelefteq y \iff x$ is a descendant of y

$\text{lub}(x, y) = $ closest common ancestor(x, y)

$\text{glb}(x, y) = $ closest common descendant(x, y)

Either may not exist, e.g. if x, y are not relatives, or if there is no single closest ancestor/descendant

$c \in A$ is *the least upper bound of* a, b, if

- $(a \preceq c) \wedge (b \preceq c)$
- for all $x \in A$, $(a \preceq x) \wedge (b \preceq x) \Rightarrow (c \preceq x)$

$d \in A$ is *the greatest lower bound of* a, b, if

- $(d \preceq a) \wedge (d \preceq b)$
- for all $x \in A$, $(x \preceq a) \wedge (x \preceq b) \Rightarrow (x \preceq d)$

$c = \text{lub}(a, b)$ $\quad$ $d = \text{glb}(a, b)$ $\quad$ (either may not exist)

$\text{glb}(x, y) = \text{closest common descendant}(x, y)$

Either may not exist, e.g. if x, y are not relatives, or if there is no single closest ancestor/descendant

Will exist e.g. for two grandparents sharing one grandchild, or two half-cousins sharing one (but not two) grandparent

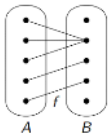
Biologists often look for closest common ancestors between *species*

Functions

13 November 2019 15:27

A function from set A to set B is a relation Rf : A <-> B
Where for every a in A, there is a unique b in B such that afb

$\forall a \in A : \exists! b \in B : afb$



F maps A into B – A is the domain and B is the codomain

We write f(a) = b or f : a -> b for afb and say

- f maps a to b
- (b is the image of a)
- (a is the pre-image of b)

Identity function $\mathrm{id}_A : A \to A \qquad \mathrm{id}_A = \{(a, a) \mid a \in A\} = R_{=_A}$
$f : \mathbb{N} \to \mathbb{N} \qquad f = \{(m, n) \in \mathbb{N}^2 \mid m^2 = n\} =$
$\{(0, 0), (1, 1), (2, 4), (3, 9), (4, 16), \ldots\}$

Composite Functions

Let $R_p : A \leftrightarrow B \quad R_q : B \leftrightarrow C$

Prove: if R_p, R_q are functions, then the composition $R_{p \circ q}$ is a function

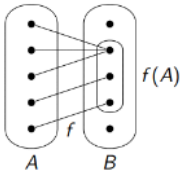
$f : A \to B \quad g : B \to C$
$\forall a \in A : (f \circ g)(a) = g(f(a))$

Inverse Functions

Let $R_p : A \leftrightarrow B$
Even if R_p is a function, its inverse $R_{p^{-1}}$ may not be a function
Examples:
$f : \mathbb{Z} \to \mathbb{Z} \qquad f(n) = n + 1$
$f^{-1} : \mathbb{Z} \to \mathbb{Z} \qquad f^{-1}(n) = n - 1$
$g : \mathbb{N} \to \mathbb{N} \qquad g(n) = n + 1$
$R_{g^{-1}}$ is not a function

Function Range

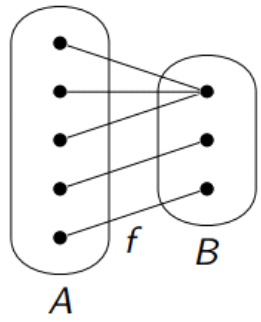
The range of a function is the set of of all elements in the co-domain B that have a preimage in domain A, so the range below would be those 3 dots in the middle of B.



Surjective Functions

A function f is called surjective if its range f(A) is the whole co-domain B

$$f : A \twoheadrightarrow B \iff f(A) = B \iff \forall b \in B : \exists a \in A : f(a) = b$$

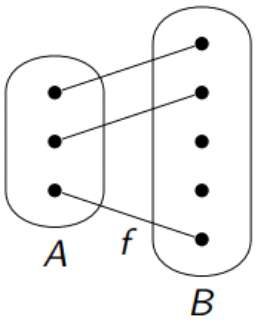


We also say that f maps A onto B

Injective Functions

A function f is called injective if it maps every element of A onto a different element of B

$$f : A \rightarrowtail B \iff \forall x, y : (f(x) = f(y)) \Rightarrow (x = y)$$



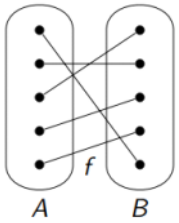
Proving Injectivity
For all x different to y f(x) does not equal f(y)
Pick an element and show that the result of the function is different to the result of f(y)

Bijective Functions

A function f is called bijective if it is both surjective and injective simultaneously

$$f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B \iff (f : A \twoheadrightarrow B) \wedge (f : A \rightarrowtail B) \iff \forall b \in B : \exists! a \in A : f(a) = b$$

We also say f is a *one-to-one correspondence between A and B*



For any set A, a bijective $f : A \rightarrowtail\!\!\!\!\twoheadrightarrow A$ is called *a permutation*
For any set A, a permutation $g : A \rightarrowtail\!\!\!\!\twoheadrightarrow A$ with $g^{-1} = g$ is called *an involution*

Proof that if f is a bijective function then the inverse function is also bijective:

Proof.

f bijective $\implies \forall b \in B : \exists! a \in A : afb \implies$
$\forall b \in B : \exists! a \in A : b(f^{-1})a \implies f^{-1}$ a function

f a function $\implies \forall a \in A : \exists! b \in B : afb \implies$
$\forall a \in A : \exists! b \in B : b(f^{-1})a \implies f^{-1}$ bijective

If f is bijective then for every b that is an element of B, there exists one a that is an element of A such that f(a) = b.
Therefore, for all b, there exists one a such that the inverse function f-1(b) = a
Because for every b there exists an a, the inverse is a function.

If f is a function, then we know for every a there is a b such that f(a) = b
Therefore, for every a, there exists a b such that the inverse function f-1(b) =a

So for every a, there exists a b such that f-1(a) = b
And for every b, there exists a b such that f-1(a) = b
So the function maps 1 b onto 1 a, and is therefore bijective

As such, if a function has an inverse that is also a function then both are bijective.

Equinumerous

Two sets are equinumerous if there is a bijection between A and B

$$A \cong B \iff \exists f : A \rightarrowtail\!\!\!\!\!\rightarrow B$$

Countability

We call a set countable if it is equinumerous with the set of all natural numbers N. This set can be put in one-to-one correspondence with N.

E.g. we can write an algorithm that would reach any and all values of the set given enough time

- Contrary to the intuition, a "part" (i.e. a proper subset) of an infinite set can be of the same "size" as the whole.
- In fact, it can be proved that every subset of a countable set is either finite or countable.
- In other words, the cardinality of N is the "smallest" among infinite cardinalities.
- As a consequence, for any equivalence relation on a countable set, the quotient set (i.e. the set of all equivalence classes) is either finite or countable.
- This can be shown by selecting an arbitrary representative from every equivalence class.
- The function that maps every equivalence class to its representative is a bijection, therefore the quotient set is equinumerous with a subset of the initial set.
- Since the initial set is countable, its quotient set must be finite or countable. It turns out that not only subsets, but also certain supersets of N may be countable.

Cantor's Theorem

Do uncountable sets exist at all? The answer to this question is given by Cantor's theorem: no set can be equinumerous with its own powerset.

Proof. The proof method is called Cantor's *diagonal argument*, and is reminiscent of Russell's paradox.

To prove the statement by contradiction, suppose that for some set A, there exists a bijective function $f : A \rightarrowtail\!\!\!\!\!\rightarrow \mathcal{P}(A)$, which puts elements of A in one-to-one correspondence with subsets of A. Consider the set of all elements of A that are *not* in their corresponding subsets: $D = \{a \in A \mid a \notin f(a)\}$. Since D is a subset of A, it must, like all other subsets, have a corresponding element d, such that $f(d) = D$.

Consider the statement $d \in D$. Suppose this statement is true. Then d is an element of the set D of all elements that are not in their corresponding subsets. But the corresponding subset of d is set D itself, therefore, by the definition of D, we have $d \notin D$. Hence, the statement $d \in D$ cannot be true.

Suppose the statement $d \in D$ is false. Then d is not an element of the corresponding set D. We have a special set for such elements, which happens to be D itself! Therefore, by the definition of D, we have $d \in D$. Hence, the statement $d \in D$ cannot be false.

By the laws of logic, $d \in D$ must be true or false. As we have shown above, both cases lead to a contradiction. Therefore, our initial assumption must be false, and the bijective function f cannot exist. □

In other words:
Suppose a function exists that maps the elements of A into a one-to-one correspondence with the powerset of A
Consider the set of all elements of A that are not in their corresponding subsets D

D is a subset of A and so an element d such that f(d) = D
If d is in D is true: D is an element of the set D for all elements that are not in their corresponding subsets. But the corresponding subset is D itself, so d is not in D. But the statement was d is in D. So there is a contradiction
If d is in D is false: Then d is not an element of the correesponding. So d belongs to the set of elements that are not in their corresponding sets: D. Therefore by defintion of D, we have d is in D. So the statement d is in D cannot be false. Thus we have another contradiction
Logic says d in D must be true or false but we have reached a contradiction in both cases
So the bijcetive function f cannot exist and it is impossible to map A to the powerset of A.

N^2 is countable. N^3 is countable. Any finite cartesian product is countable.

$$\mathbb{N}^3 = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \cong \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$$

However an infinite Cartesian product of countable sets need not be countable

Proof that Real numbers between 0-1 are uncountable

Proof: Suppose that 0, 1 is countable. It is clearly not finite so we are assuming that it is countably infinite.
Then there exists a bijection from N to 0, 1. In other words we can create an infinite list which contains every real number between 0 and 1.
We can therefore write a list of all of the numbers in decimal notation :

$$\begin{array}{ll} 1 & 0.023424242090590394349 34\ldots \\ 2 & 0.324342934294294924392 42\ldots \\ 3 & 0.500000000000000000000 0\ldots \\ 4 & 0.203423049209402940294 90\ldots \\ \vdots & \vdots \end{array}$$

Let X the number we are going to create. For all n in N, let the nth decimal spot of X be NOT equal to the nth decimal place of the nth number in the list.
In other words, move diagonally through the list and change each digit by an arbitrary amount – append this new digit to the list. What is that the nth digit is not equal to the nth digit of the nth number.

By construction we have created a number that does not exist on our list and as such we have reached a contradiction – 0, 1 is uncountable.

Relations

29 October 2019 12:14

A relation between sets A and B is a subset of A x B (the cartesian product of A and B)

$$R_{\mathrm{p}} : A \leftrightarrow B \iff R_{\mathrm{p}} \subseteq A \times B$$

A relation corresponds to a predicate with two free variables

$$\text{Example: } P(x, y) = x \leq y \quad x, y \in \mathbb{N}$$

Some Relations

$$\textit{Equality relation } R_{=_A} : A \leftrightarrow A \qquad R_{=_A} = \{(a, a) \mid a \in A\}$$

X q y = x is a child of y
X t y = x keeps y as a pet

Composed Relationships

The *composition* of p and q: $R_{\mathrm{p} \circ \mathrm{q}} : A \leftrightarrow C$

$$\forall (a, c) \in A \times C : a(\mathrm{p} \circ \mathrm{q})c \Leftrightarrow \left(\exists b \in B : (a\,\mathrm{p}\,b) \wedge (b\,\mathrm{q}\,c)\right)$$

Let $R_{\mathrm{q}} : \textit{People} \leftrightarrow \textit{People}$ $\quad x\,\mathrm{q}\,y \iff x$ is a child of y

Let $R_{\mathrm{t}} : \textit{People} \leftrightarrow \textit{Animals}$ $\quad x\,\mathrm{t}\,y \iff x$ keeps y as a pet

$R_{\mathrm{q} \circ \mathrm{t}} : \textit{People} \leftrightarrow \textit{Animals}$ $\quad x(\mathrm{q} \circ \mathrm{t})z \iff$
x has a parent who keeps z as a pet

I have a relation with pet food when I have a relation with my pet that is in a relation with the pet food

Reflexive Relations

When all elements of the set have a relation with themselves

Relation $R_\mathsf{p} : A \leftrightarrow A$ is *reflexive*, if $\forall a \in A : a \mathsf{p} a$

Examples: $R_=$ A^2 $R_\leq$ $R_|$

R_p reflexive iff $R_= \subseteq R_\mathsf{p}$

Symmetric Relations

Relation $R_\mathsf{p} : A \leftrightarrow A$ is *symmetric*, if $\forall a, b \in A : a \mathsf{p} b \Rightarrow b \mathsf{p} a$

Examples: $R_=$ A^2 $\emptyset$

$R_* : \mathbb{N} \leftrightarrow \mathbb{N}$ $x * y \Leftrightarrow (x + y = 10)$

R_p symmetric iff $R_{\mathsf{p}^{-1}} = R_\mathsf{p}$

Antisymmetric Relations

Relation $R_\mathsf{p} : A \leftrightarrow A$ is *antisymmetric*, if $\forall a, b \in A : (a \mathsf{p} b \wedge b \mathsf{p} a) \Rightarrow a = b$

Examples: $R_=$ $\emptyset$ $R_\leq$ $R_<$

R_p antisymmetric iff $R_\mathsf{p} \cap R_{\mathsf{p}^{-1}} \subseteq R_=$

Note that a relation can be both symmetric and antisymmetric (e.g. $R_=$)

Transitive Relations

Relation $R_\mathsf{p} : A \leftrightarrow A$ is *transitive*, if $\forall a, b, c \in A : (a \mathsf{p} b \wedge b \mathsf{p} c) \Rightarrow a \mathsf{p} c$

Examples: $R_=$ A^2 $\emptyset$ $R_\leq$ $R_<$

R_p transitive iff $R_{\mathsf{p} \circ \mathsf{p}} \subseteq R_\mathsf{p}$

Quotient Set
A set of sets,

Induction

19 November 2019 12:32

If n = k we can deduce k + 1

Proof by induction is similar to ordinary proof, but we employ a trick where we prove a statement for n = 1 and then assume it is true for n = k and show it is true for n = k + 1.

E.g. if we are proving that the sum of integers can be written as sum = n(n+1)/2
Assume n = k holds: 1 + 2 + 3 + … + k = k(k+1)/2 (Induction Hypothesis)
Show n = k + 1 holds: 1 + 2 + 3 + … + k + (k + 1) = (k + 1)((k + 1) + 1) / 2

Useful examples

http://comet.lehman.cuny.edu/sormani/teaching/induction.html

$\frac{k(k+1)}{2} + k + 1$ By the induction hypothesis

(k(k+1) + 2(k+1))/2 by 2/2 = 1 and distribution of division over the addition

(k+2)(k+1)/2 by distribution of multiplication over addition
(k+1)(k+2)/2 by commutativity

QED

Benoulli's Inequality

$$(1+x)^r \geq 1 + rx,$$

Proceed by induction:
We prove the inequality for r in {0, 1}
From validity for some r we deduce validity for r+2

For r = 0
(1 + x)^0 > 1 + 0x is equivalent to 1 >= 1 which is true as required

For r = 1 we have (1 + x)^1 = (1 + x) >= (1 + x) which is true

Now suppose the statement is true for r = k

$$(1+x)^k \geq 1 + kx.$$

$$\begin{aligned}(1+x)^{k+2} &= (1+x)^k(1+x)^2 \\ &\geq (1+kx)\left(1+2x+x^2\right) && \text{by hypothesis and } (1+x)^2 \geq 0 \\ &= 1+2x+x^2 + kx + 2kx^2 + kx^3 \\ &= 1+(k+2)x + kx^2(x+2) + x^2 \\ &\geq 1+(k+2)x\end{aligned}$$

The modified induction we conclude that the statement is true for every non-negative integer r.

QED

Defining Objects

We can use induction to define objects. You cant define all N without induction because we don't know all N.
Induction can create a self-referential definition of the natural numbers.

So we start with 0
If the number is a natural number, the next number is a natural number too.

For a queue:
The empty set is a queue
A queue with a person behind is a queue
Every queue can then be defined

Structure of an Inductive Definition
Induction base: initial objects
Inductive step: ways to make new objects
Completeness (often implicit): no other objects allowed)

So given a predicate P(x), we need to prove for all x in the set that p(x), where S is inductively defined

Strong Induction

Strong induction is a variant of induction, in which we assume that the statement holds for all values preceding k. This provides us with more information to use when trying to prove the statement.

When we use induction we start with the base step and use it to imply the next step.
Once we have used this to show that p(1), p(2), p(3) etc holds, we can use those steps as a group to prove the rest

Prove: every n in N greater than 1 is divisible by a prime
Induction base 2 | 2 prime
Inductive step: suppose 2, 3, 4, 5, … n –1 are divisible by a prime
We need to prove that n is divisible by a prime

Case 1 n is prime: n | n

Case 2: n is not prime so n = m x k where m, n > 1

If n is not prime then it is composed of a prime k and a number m. We can say that m is p x l