Chapter 1
Math backgrounds

We always start with sets. ☺

A *set* is a collection of objects. The objects collected in a set are called its *elements* or *members.* If a is a member of A, we write "$a \in A$", namely, a belongs to A.

A set is called *finite* (respectively, *infinite,*) if it contains finite (respectively, infinite) number of elements. If a set is finite, it can be described by listing all of its members, e.g., $\{7, 21, 57\}$. (Can it really? ☺) Otherwise, we have to use a property to specify its members, e.g., $\{x : x \text{ is even}\}$ for all the even numbers.

$\mathcal{N}$, the set of all the *natural numbers,* and $\mathcal{Z}$, the set of all the *integers,* is defined as $\{1, 2, 3, \ldots\}$ and $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$, respectively.

Operations and relations

An *operation* applied to sets brings back a set, but a *relation* just says it is *true* or *false.*

Let A, B be two sets,

$$\begin{aligned} \textit{Union } A \cup B &= \{x : x \in A \vee x \in B\} \\ \textit{Intersection } A \cap B &= \{x : x \in A \wedge x \in B\} \\ \textit{Complement } A - B &= \{x : x \in A \wedge x \notin B\} \\ \textit{Subset } A \subseteq B &\equiv \forall x, x \in A \Rightarrow x \in B. \end{aligned}$$

An example should be helpful. ☺

Let A be $\{1, 2\}$, and B be $\{2, 3\}$, we have that

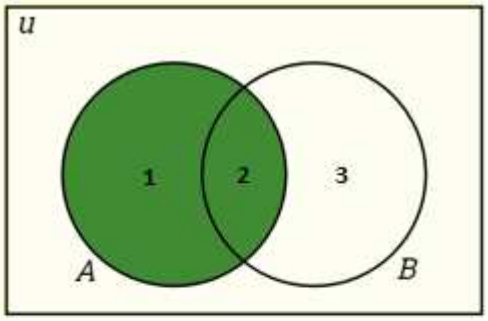
$A \cup B = \{1, 2, 3\} = B \cup A$,
$A \cap B = \{2\} = B \cap A$,
$A - B = \{1\}$, but $B - A = \{3\}$, and
$A \not\subseteq B$.

Clearly, both Union and Intersection are *commutative,* e.g., $A \cup B = B \cup A$; but Complement is not: $A - B \neq B - A$ ☹.

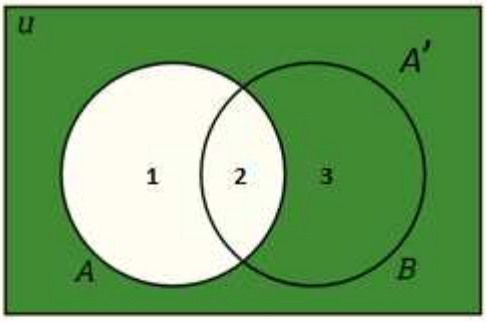
Homework: Exercise 0.1-0.3.

I want to see...

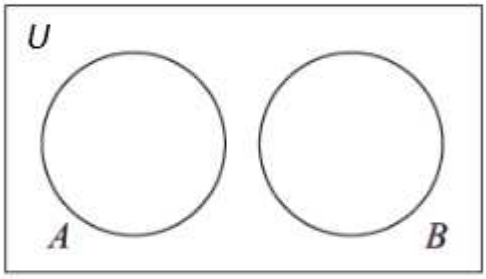
Set Operations and Venn Diagrams



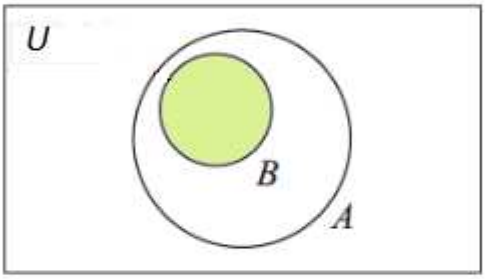
Set A



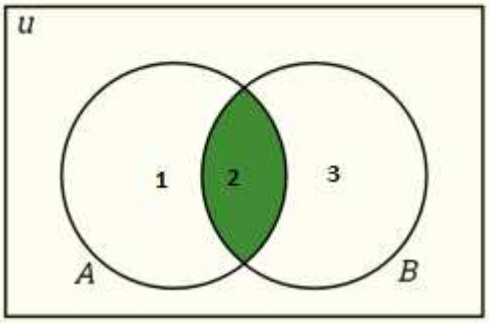
A' the complement of A



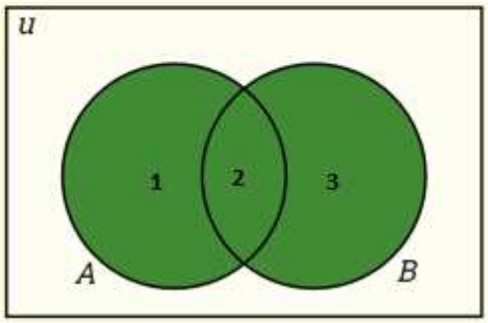
A and B are disjoint sets



B is proper subset of A $\quad B \subset A$



Both A and B
A intersect B $\quad A \cap B$



Either A or B
A union B $\quad A \cup B$

Sequences and tuples

A *sequence* of objects is a list of these objects *in some order.* For example, $(7, 21, 57)$ represents the sequence $7, 21, 57$; while $\{7, 21, 57\}$ is just a collection.

Question: What is the difference between a set and a sequence?

Answer: Order. ☺

A finite sequence with k elements is usually called a $k-$*tuple.* Particularly, a 2-tuple is called a *pair,* and a 3-tuple a *triplet.*

For example, $(7, 21, 57)$ is a 3-tuple, or a triplet, while $(7, 21)$ is a pair.

Cartesian product

It is yet another set operation. Let A, B be two sets, the *Cartesian product* of A and B is defined as follows:

$$A \times B \ = \ \{(a, b) | a \in A \wedge b \in B\}$$

We dealt with *it* in *CS 3600 Database* a lot, where it is used to get stuff from multiple tables, or relations.

For example, if $A = \{1, 2\}$ and $B = \{x, y, z\}$, then

$$A \times B \ = \ \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}.$$

This operation is easily extended (?) to $k(\geq 3)$ sets as it is associative, e.g.,

$$A \times B \times C = (A \times B) \times C.$$

Questions: What is $A \times B \times \{a, b, c\}$?

Notice that $|A \times B \times C| = |A| \times |B| \times |C|$.

Homework: Exercise 0.4-0.5.

Functions and relations

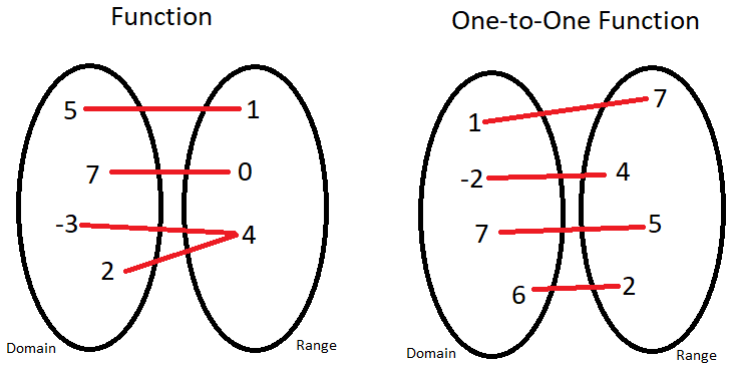
Just like a *Java* method or a *Python* function, a *function* takes in one or more input(s) and sends out an output, e.g., $f(a) = b$.

A function is a special *mapping* in the sense that the following always holds: for all x, y,

$$x = y \Rightarrow f(x) = f(y).$$

Let f be a function, the collections of its possible inputs, and outputs, are called its *domain,* and *range,* respectively.

$$f : D \rightarrow R.$$



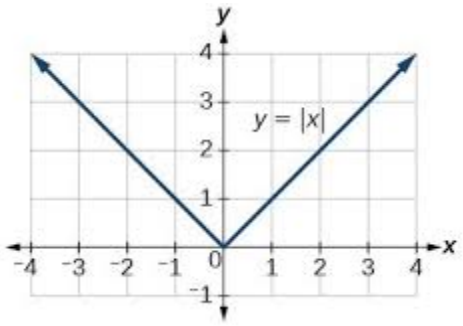
Function specification

A function is often analytically represented via an expression. For example, the absolute value function, $f(x) = |x|$, can be represented as follows:

$$\begin{aligned} |x| : \mathcal{Z} &\rightarrow \mathcal{Z}, \\ |x| &= \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{otherwise.} \end{cases} \end{aligned}$$

Such an expression immediately leads to a procedure (algorithm) to compute $abs(x)$ for any x.

Graphically speaking, it can be represented as follows:



Another way

Another way to describe a function is to use a table. For example,

$$\begin{aligned} f : \{0,1,2,3,4\} &\rightarrow \{0,1,2,3,4\}, \\ \forall n, 0 \leq n \leq 4, f(n) &= (n+1) \,\%\, 5. \end{aligned}$$

The following table describes f :

n	$f(n)$
0	1
1	2
2	3
3	4
4	0

When the domain of f is $A_1 \times \cdots \times A_k$, the input to f is a $k-$tuple $(a_1, \ldots, a_k)$ and is called an *argument* to f. When $k = 1, 2$, f is called a *unary* or a *binary* function, respectively.

Question: Why do we love, and hate, functions in Computer Science? ☺

Homework: Exercise 0.6.

A special function

A *predicate* is a function whose range is {T(rue), F(alse)}. For example, $even$ is a predicate such that $even(x) = T$ if and only if x is an even number.

A *predicate* whose domain is a set of $k-$tuples is called a *relation.* In an expression involved with a binary relation, the latter is usually written as an infix notation, aRb, which means that $aRb = T$. In general, $R(a_1, \ldots, a_n)$ means that the latter is true.

Let R be a binary relation whose domain is D, it might have the following properties:

R is *reflexive* if and only if for all $x \in D, xRx$.

R is *symmetric* iff for all $x, y \in D, xRy \Leftrightarrow yRx$.

R is *transitive* iff for all $x, y, z \in D$, xRy and $yRz \Rightarrow xRz$.

Examples

The equality "$=$" is reflexive, symmetric and transitive.

The inequality "$\leq$" is reflexive, transitive, but *not symmetric.*

We first notice the following fact.

$$A \to B \equiv \neg A \vee B.$$

For example, "If $(\to)$ *I have five bucks* (A), *I will buy you lunch* (B)."

A	B	$\neg A$	$\neg A \vee B$	$A \to B$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Question: Why is '$\leq$' not symmetric?

"$\leq$" is not symmetric.

1. Show that $\forall x \forall y \ [x \leq y \Rightarrow y \leq x]$ is false.

Since $(x \leq y) \Rightarrow (y \leq x) \equiv \neg(x \leq y) \vee (y \leq x)$, we have that

$$\forall x \forall y \ [x \leq y \Rightarrow y \leq x] \equiv \forall x \forall y \, [\neg(x \leq y) \vee y \leq x]$$
$$\equiv \forall x \forall y \, [(x > y) \vee (y \leq x)] \, .$$

The last expression says that '$\leq$' is symmetric iff, for all x, y, either $x > y$ or $x \geq y$.

Question: *Is it true?*

We just need to find some x, y such that $x < y$ to show that *it* is false.

For example, $x = 3$, and $y = 4$. Then, neither $x > y$ nor $y \leq x$ $(\equiv x \geq y)$ holds.

Thus, $3 \leq 4$, but it is not true the other way around. *As a result, '$\leq$' is not symmetric.*

2. Show its opposite is true, i.e.,

$$\begin{aligned}
&\neg\left[\forall x \forall y \; x \leq y \Rightarrow y \leq x\right] \\
&\equiv \exists x \exists y \neg\left[x \leq y \Rightarrow y \leq x\right] \\
&\equiv \exists x \exists y \neg\left[\neg(x \leq y) \vee y \leq x\right] \\
&\equiv \exists x \exists y\left[(x \leq y) \wedge (y > x)\right].
\end{aligned}$$

We now only need to find a pair (x, y) such that $x < y$, which will make the above predicate true. Clearly, (3, 4) will do.

The strict inequality "$<$" is neither reflexive nor symmetric, but transitive.

The "Knowing" relation is reflexive, but neither symmetric nor transitive. For example, You definitely know President Biden ☺, but I doubt he knows you ☹. And if I know Bob, and Bob definitely knows his own parents, but I don't usually know Bob's parents. ☹

By the same token, "friendship" is also reflexive, symmetric, but not transitive: Amy is a friend of Bob, who is a friend of Charlie. Is Amy necessarily a friend of Charlie? ☺

Equivalent relations

A relation is *equivalent* iff it is reflexive, symmetric, and transitive. As we just went through, "=" is equivalent, but friendship is not.

Question: Let $R_1 = \{(a, a), (b, b), (c, c), (b, c)\}$. Is it equivalent?

It is both reflexive and transitive, but not symmetric: $(b, c) \in R$, but $(c, b) \notin R$. Thus, it is not equivalent.

On the other hand, let $R_2 = \{(p_1, p_2) : p_1$ and p_2 share the same birthday.$\}$. Then, it is equivalent.

Moreover, R_2 can be used to partition all the people on the earth to 366 (for this leap year of 2024) *equivalent classes,* where all the people in each such class share the same birthday.

Another example

Question: Let "$\equiv_7$" be a relation with $\mathcal{N}$ as its domain such that for all $i, j \in \mathcal{N}$, $i \equiv_7 j$ iff $i - j$ is a multiple of 7. Is it equivalent?

1) $\equiv_7$ is reflexive, because $0 (= i - i)$ is a multiple of 7. Indeed, 0 is a multiple of anything.

2) $\equiv_7$ is symmetric, because if $i - j = 7q$ for some q, then $j - i = 7(-q)$.

3) $\equiv_7$ is transitive, because if $i - j = 7q_1$ and $j - k = 7q_2$, then $i - k = (i - j) + (j - k) = 7(q_1 + q_2)$.

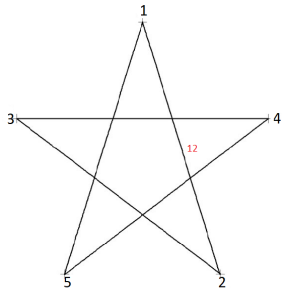
Thus, by definition, "$\equiv_7$" is indeed equivalent. So is "objects of same color".

Clearly, they also lead to respective equivalent classes.

Homework: Exercise 0.7.

Graphs again...

As we discussed in *CS 3221 Algorithm Analysis*, a *graph*, $G(V, E)$, is a set of vertices (nodes) V with edge (links), E, connecting some of these vertices. Here is an example:



The above graph can be represented as

$$\begin{aligned} G &= (V, E) \\ &= (\{1,2,3,4,5\}, \{(1,2),(1,5),(2,3),(3,4),(4,5)\}). \end{aligned}$$

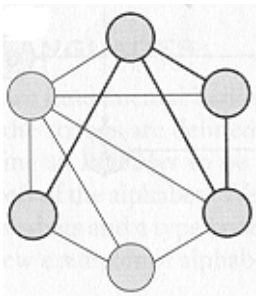
Graphs can also be *labeled,* if we want to attach more information, such as distance, with the edges. For example, in the above

$$\omega(1,2) = 12.$$

We have seen plenty of graph related applications in the algorithm course. ☺

Several related notions

A graph G is a *subgraph of* H if the vertices of G is a subset of that of H and the edges of G are edges of H for the corresponding vertices. The following shows a (darker) subgraph.



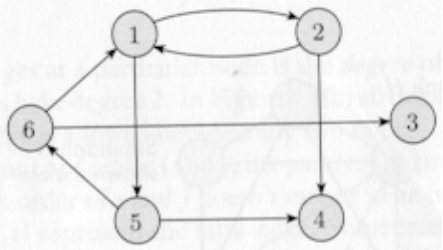
A *path* in a graph is a sequence of vertices connected by edges, which is a *cycle* if it starts and ends at the same vertex. A path is *simple* if no vertex repeats. A graph is *connected* if there is a path between every two vertices of this graph.

A graph is a *tree* if it is connected and contains no cycles. We also have intuitive notions of *leaves* and *root.* A *forest* is a group of trees.

Homework: Exercise 0.8-0.9.

Directed graphs

An edge in a *directed graphs* is not a set, but a pair. Here is a directed graph.



The one-way street maps of many big cities such as Boston provide another category of examples.

A path in which all the arrows point in the same direction is called a *directed path.* A directed graph is *strongly connected* if a directed path connects every two vertices.

Directed graphs are often used to describe binary relations. Let R be such a relation whose domain is $D \times D$, a labeled graph $G = (D, E)$ represents R, where $(x, y) \in E$ iff xRy.

Strings and languages

As mentioned earlier, we use *languages* to describe the ability of computers.

A language is based on its alphabet, e.g., English has 'a' through 'z' as its alphabet.

In general, an *alphabet* is a finite set, generally denoted as Σ or Γ. For example,

$$\begin{aligned} \Sigma_1 &= \{0, 1\} \\ \Sigma_2 &= \{0, 1, x, y, z\}. \end{aligned}$$

A *String* over an alphabet is a finite sequence of elements of that alphabet, e.g., "010001" is a string over Σ_1. "String" is an English string.

If w is a string over Σ, the *length* of w, written as $|w|$, is the number of symbols that it contains.

Particularly, the string of length 0, denoted as ϵ, is called the *empty string,* often represented as 'ϵ'.

String operation

If a string w has length n, it can be written as $w = w_1 \cdots w_n$. Then, its reverse is defined as $w^R = w_n \cdots w_1$.

A string, z, is a *substring* of w if z appears consecutively within w. For example, "is" is a substring of "This".

Let $x = x_1 \cdots x_m$ and $y = y_1 \cdots y_n$ be two strings, then the *concatenation* of x and y, written as xy, $x \circ y$, or $x + y$ in *Java,* is the string $x_1 \cdots x_m \circ y_1 \cdots y_n$. Thus, $(ab) \circ cd = abcd$.

Obviously, for any string w, $w \circ \epsilon = \epsilon \circ w = w$.

A *language* over Σ is a set of strings over Σ.

The *lexicographic ordering* of strings is the same as the familiar dictionary ordering, except that *shorter ones always precede the longer ones.* For example, $abc \prec acb$, but $bc \prec abc$.

Definition, theorem and proof

Definitions describe the objects and notions that we use. It could be either simple or complicated, but it must be *precise.* ☺

After definitions are given, we usually make some mathematical statements about the properties some objects might or might not have. A *proof* is a logic argument that a statement is true. It should be not only convincing, but correct *beyond any doubt.* ☹

A *theorem* is a mathematical statement proven true. Sometimes, we prove a theorem only because it is needed in the proof of another statement. Such statements are called *lemmas.* Also, a theorem might lead us to conclude that other statements are true, as well, which are called the *corollaries* of the theorem.

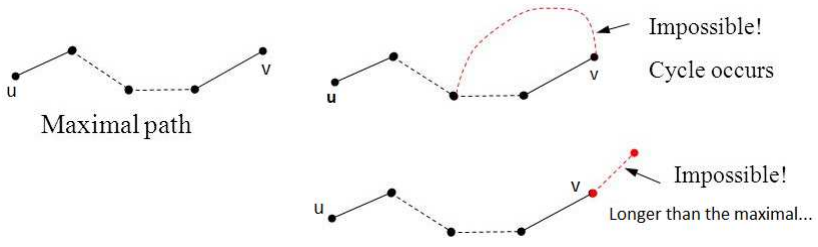
Remember this stuff? ☺

Definition: A graph is a *tree* if it is connected and contains no cycles.

Lemma 1: Any finite tree with at least two vertices has at least two leaves.

Proof: Since a tree is connected, there is a path between any two vertices. Take a longest path among all these paths.

Let v be one of the two end points.

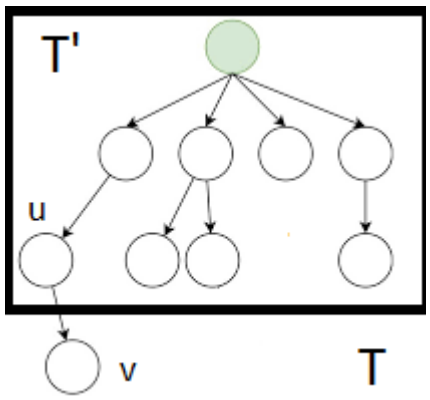


The same argument goes through with u, thus, both u and v are leaves. □

Theorem 1: Let T be a finite tree containing n vertices. Then it has $n-1$ edges.

Proof: By construction and induction. When a tree holds just one vertex, it has 0 edge.

Assume this holds for a tree with n vertices. Let T be a tree with n+1 vertices. By Lemma 1, let v be a leaf of T, adjacent to u.



Let T' be a tree after removing v and the edge (u, v). Then, T' has n vertices, thus, by the inductive assumption, it has $n-1$ edges

Thus, T has n edges, including (u, v).

We are done. □

Definition: A forest is a collection of trees.

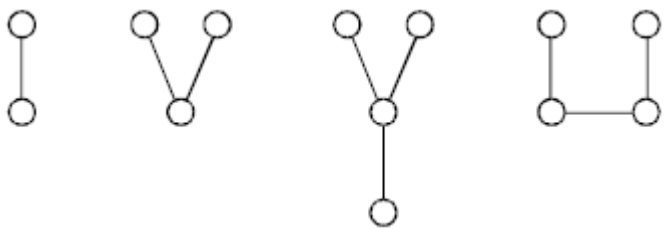
Corollary 1: A forest with $n > 1$ nodes and $k > 1$ trees contains exactly $n - k$ edges.

Proof: Let $T_i, i \in [1, k]$, contain n_i nodes. By Theorem 1, we have that e_i, the nodes of T_i, equals to $n_i - 1$. Hence,

$$e = (n_1 - 1) + (n_2 - 1) + \cdots (n_k - 1) = n - k.$$

This ends the proof. □

For example, the following forest of four trees contains 13 vertices, so it must contain nine edges. ☺



Looking for proofs

The only way to determine the truth of a mathematical statement is to give *it* a mathematical proof, which is usually challenging. ☹

Question: What to do? ☺

1) Make sure you know what you are doing.

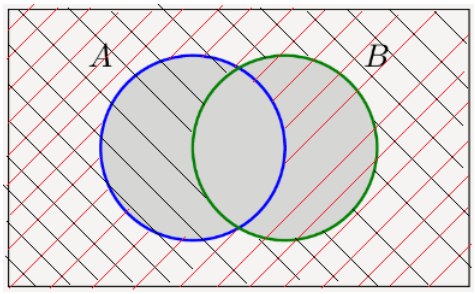
For example, we often have to show that "P iff Q" where both P and Q are statements. It can be put into two parts. The first is "P only if Q", which means "if P, then Q". The other is "P, if Q". We clearly have to show both parts hold.

Another type is to show $A = B$, where both A and B are sets, i.e., they contains the same stuff.

Based on the definition of sets, we must prove that $A \subseteq B$ and $B \subseteq A$, i.e., both A and B hold exactly the same stuff.

An example

Theorem 0.10: For any two sets A and B, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.



Proof: We have to prove both $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Assume that $x \in \overline{A \cup B}$. By definition, $x \notin A \cup B$. Hence, $x \notin A$ and $x \notin B$, i.e., $x \in \overline{A}$ and $x \in \overline{B}$. Thus, $x \in \overline{A} \cap \overline{B}$. This proves that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

To show the other direction, let $x \in \overline{A} \cap \overline{B}$. By definition, $x \in \overline{A}$ and $x \in \overline{B}$. Then, $x \notin A$ and $x \notin B$, which means $x \notin A \cup B$. Hence, $x \in \overline{A \cup B}$. $\square$

2) Try to get an intuitive, gut, feeling about why the statement *should* be true.

Besides a picture ☺, *it is always a good idea to start with some small and/or simple examples.* We will hit the jackpot if we find a *counterexample* which shows that the statement is actually false. We have nothing else to do.

For example, given the statement that, *for all* n, e_n *is a prime number, where* e_n *is defined as follows:*

$$\begin{aligned} e_1 &= 2, \\ e_n &= e_1 e_2 \cdots e_{n-1} + 1. \end{aligned}$$

Before giving a general argument, we test it out first with $n = 1, 2, 3, \ldots$ it turns out that the statement is false for $n = 5$, since

$$e_5 = 1807 = 13 \times 139.$$

We are done... It is not true. ☺

If we are not lucky,...

,... you will have a much better understanding of the statement.

For example, given the statement that, *for every graph G, the sum of the degrees of all the vertices is an even number.*

Begin with graphs with one, two or three edges, we gradually recognize that every edge increases this sum by 2. This process might lead to a proof on the next page.

3) When convinced a proof has been found, it must be written up properly so that other people can read it, verify it and accept it.

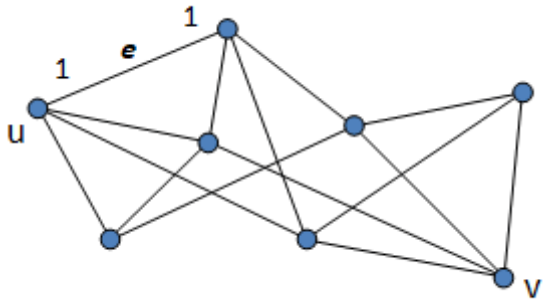
It is not just for yourself, but for the community as a whole.

You have to use a word processor to type up the homeworks....

An example

Theorem 0.11: For every graph $G(V, E)$, the sum of the degrees of all the vertices is an even number.

Proof: Every edge, e.g., e, connects two nodes, thus, contributes a one to the degree of these two nodes, i.e., a two to the sum of degrees of all the nodes.



Hence, since G contains $|E|$ edges, the sum of all the degrees is $2|E|$, an even number. $\square$

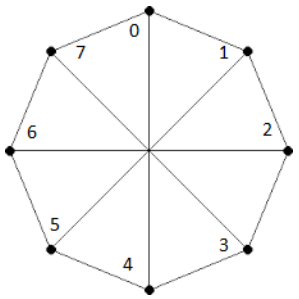
Type of proofs

1. Proof by Construction: This technique is used to show the *existence of objects* that satisfy certain properties.

Theorem 0.12: For each even number of $n \geq 4$, there exists a 3-regular graph with n vertices.

Proof: Let n be such a number and we construct $G(V, E)$ with n nodes as follows: $V = \{0, 1, \ldots, n-1\}$ and $E = \{(i, i+1) | i \in [0, n-2]\} \cup \{(n-1, 0)\} \cup \{(i, i + \frac{n}{2}) | i \in [0, \frac{n}{2} - 1]\}$. □

Here is a 3-regular graph with $n = 8$.



Question: Why n has to be even?

2. Proof by Contradiction: Given a true statement, A, to show that a statement, B, is true, we assume that it is false first, i.e., $\neg B$, and then show that this assumption leads to, e.g., $\neg A$, to get a *contradiction.* Hence, the assumption, $\neg B$, must be false, i.e., the original statement B must be true.

Logically speaking, starting with a formula as given on Page 10,

$$\neg B \to \neg A \equiv B \vee \neg A \equiv \neg A \vee B \equiv A \to B.$$

A	B	$\neg B$	$\neg A$	$A \to B$	$\neg B \to \neg A$
0	0	1	1	1	1
0	1	0	1	1	1
1	0	1	0	0	0
1	1	0	0	1	1

Hence, if both A and $\neg B \to \neg A$ are true, i.e., both A and $A \to B$ are true, so is B by *Modus Ponens.* (Cf. Course page)

This is the gist of proof by contradiction.

An example

Question: How do you know I don't have five bucks in my pocket ($\neg A$)?

Answer: We would assume otherwise, A, i.e., I do have five bucks in my picket, and see what happens.

On Page 10, we saw the sentence: "If ($\rightarrow$) *I have five bucks* (A)*, I will buy you lunch* (B)."

Therefore, we must conclude that "I will buy you lunch (B)." Unfortunately, this won't happen, at least not today. ☹ Thus, the above conclusion (B) contradicts with the fact of $\neg B$.

As a result, our assumption of A must be false, i.e., the original statement $\neg A$ must be true: I don't have five bucks in my pocket. ☺

Let's get serious...

We once showed the following in *Algorithm Analysis*:

Theorem 0.14: $\sqrt{2}$ is irrational.

Question: Is it true for any number n? No. $\sqrt{4}$ $(= 2)$ is certainly rational.

Question: Is it true for all the prime numbers? Yes, and 2 is the smallest prime number.

Question: How to prove the above statement, as there are infinite number of prime numbers (Cf. Course page)?

Lemma 2: Every integer greater than 1 is either a prime number itself or can be represented as a unique product of prime numbers.

For example, $15 = 3 \times 5$.

Lemma 3: Let p be a prime number, and r a natural number. If p divides r^2, it also divides r.

Proof: By Lemma 2, let $p_1 p_2 \cdots p_k$ be the unique prime factorization of r, then $p_1^2 p_2^2 \cdots p_k^2$ is the unique prime factorization of r^2.

Since p divides r^2, for some $i \in [1, k], p_i = p$, thus, p also divides r. □

Notice that $16 = 8 \times 2$. Thus, 8, not prime, divides 16 ($= 4^2$), but 8 does not divide 4. ☹

Theorem 2: Let p be any prime number, $\sqrt{p}$ is irrational (“B”, Cf. Page 30).

Proof: Just assume that, for some integers m and n,

$$\sqrt{p} = \frac{m}{n}.(\text{“}\neg B\text{”})$$

W.l.o.g, m and n don't have any common divisor greater than 1. Particularly, they can't be both divided by p (“A”).

Simple arithmetical manipulation leads to that $m^2 = pn^2$. Thus, p divides m^2. By Lemma 3, p also divides m. Let $m = p \times k$, for some k.

We have $m^2 = pn^2 = p^2k^2$, i.e., $n^2 = pk^2$. Thus, p also divides n^2, and n by Lemma 3. Thus, p divides both m and n ("$\neg A$"), which is a contradiction.

Thus, the "$\neg B$" part must be false, and "B" must be true, i.e., $\sqrt{p}$ is irrational for any prime number p. □

In particular, Theorem 0.14 turns into a corollary of Theorem 2.

Notice that 6 is not prime, but $\sqrt{6}$ is also irrational. Thus, this condition of p being prime is *sufficient,* but not *necessary.*

We often have alternative proofs of the same result, just have multiple choices for lunch. ☺

Another proof

Theorem 2: Let p be any prime number, $\sqrt{p}$ is irrational.

Proof: Just assume the opposite, then for some m, n, $\sqrt{p} = m/n$, i.e., $m^2 = pn^2$. ("$\neg B$")

Clearly, p is a prime factor of m^2. Since m^2 is a square, any prime factor of m^2, including p, must occur even times in its prime factorization. ("A")

For example, let $m = 18 = 2 \times 3^2$, then $m^2 = 2^2 \times 3^4$, where 2 occurs twice, and 3 occurs four times.

Now, if p is not a prime factor of n, it occurs exactly once in the prime factorization of m^2.

If it occurs once in the prime factorization of n, e.g., $n = p \times n_1$, then $m^2 = p^3 \times n_1^2$, i.e., p would occur three times in that of m^2.

If p occurs twice in the prime factorization of n, e.g., $n = p^2 \times n_1$, then $m^2 = p^5 \times n_1^2$, i.e., p would occur five times in the prime factorization of m^2.

...

In general, this prime number p, of m^2, must occur odd number of times in the prime factorization of m^2. ("$\neg A$") This contradicts the fact that any prime factor of m^2 must occur even number of times there ("A").

Hence, $\sqrt{p}$ is not rational ("B"). $\square$

3: Proof by cases: We sometimes have to deal with different cases, sort of like the `Switch` statement of *Java*.

```
switch(expression) {
  case x:
    // code block
    break;
  case y:
    // code block
    break;
  default:
    // code block
}
```

Question: What is $1 + 2 + \cdots + 100$?

Answer: We looked at *it* in *CS 3221*, which equals 5,050.

Question: How about $1 + 2 + \cdots + n$?

Play with *it*

Here is another way to do $1+2+\cdots+100$:

$$\begin{aligned} & 1+2+\cdots+100 \\ = \; & [(1+99)+(2+98)+\cdots(49+51)+\mathbf{50}]+100 \\ = \; & 49\times 100+150 \\ = \; & 4900+150 \\ = \; & 5050. \end{aligned}$$

Notice that, when $n = 100$, we have an additional 50. ☹

On the other hand,

$$\begin{aligned} & 1+2+\cdots 100+101 \\ = \; & [(1+100)+(2+99)+\cdots(50+51)]+101 \\ = \; & 50*101+101 \\ = \; & 5151. \end{aligned}$$

We now don't have this additional term, when $n = 101$. ☺

Thus, when we follow this approach to derive the sum of $S(n) = 1+2+\cdots+n$, we have to go through two cases, depending on if n is even or odd.

A proof

Theorem 3: $1 + 2 + \cdots + n = n(n+1)/2$.

Proof: We proceed with two cases:

Case 1: When n is even...

$$\begin{aligned} S(n) &= 1 + 2 + \cdots + (n-1) + n \\ &= [1 + 2 + \cdots n - 1] + n \\ &= \{[1 + (n-1)] + [2 + (n-2)] + \cdots \\ &\quad + \left[\left(\frac{n}{2} - 1\right) + \left(\frac{n}{2} + 1\right)\right]\} + \frac{n}{2} + n \\ &= \left(\frac{n}{2} - 1\right) n + \frac{n}{2} + n = \frac{1}{2} n(n+1). \end{aligned}$$

Case 2: When n is odd...

$$\begin{aligned} S(n) &= 1 + 2 + \cdots + (n-1) + n \\ &= [1 + 2 + \cdots n - 1] + n \\ &= \{[1 + (n-1)] + [2 + (n-2)] + \cdots \\ &\quad + \left[\left(\frac{n-1}{2}\right) + \left(\frac{n+1}{2}\right)\right]\} + n \\ &= \left(\frac{n-1}{2}\right) n + n = \frac{1}{2} n(n+1). \end{aligned}$$

Question: Are you sure? ☺

Play with a few values of n...

4. Proof by Induction: This technique can be used to show that all elements of an infinite set have a specified property. We usually apply it to $\mathcal{N}$, to show that every natural number has a property $\mathcal{P}$.

Every inductive proof to show that $\forall i \geq n_0, \mathcal{P}(i)$ consists of the following two steps: 1) $\mathcal{P}(n_0)$. and 2) $\forall i, \mathcal{P}(i) \Rightarrow \mathcal{P}(i+1)$.

Step 1 is referred to as the *base case* and step 2 is the *inductive case.* Finally, the left-hand-side in step 2 is called the *inductive hypothesis.*

Below is the pattern in which an inductive proof is written:

Basis: Show that $\mathcal{P}(n_0)$ is true.
Inductive step: For each $i \geq n_0$, assume that $\mathcal{P}(i)$ is true and use this assumption to prove that $\mathcal{P}(i+1)$ is true. . . .

Example

Problem 0.11(a): for all $n \geq 1$,

$$\Sigma_{i=1}^{n} i \;=\; \frac{n(n+1)}{2}.$$

Proof: Basis: Show that the equation is true when $n = 1$.

$$\Sigma_{i=1}^{1} i = 1 = \frac{1 \times 2}{2}.$$

For each $n \geq 1$, assume that the equation holds, and prove it also holds for $n + 1$.

$$\begin{aligned}
\Sigma_{i=1}^{n+1} i &= \Sigma_{i=1}^{n} i + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) = (n+1)\left[\frac{n}{2} + 1\right] \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

Thus, the equation holds for all $n \geq 1$. □

Homework: Problem 0.10, 0.11, and 0.12. Read through the proof of Theorem 0.25.

The pigeonhole principle

Question: How to put ten pigeons in nine holes?

Answer: we have to put at least two pigeons into at least one hole. ☹

In general, *if we put n items into m boxes, and if $n > m$, then at least one box must have at least two items.*

An example

Question: You have seven pairs of socks in you drawer, one of each color of the rainbow. How many socks do you have to draw out in order to have at least one pair?

After grabbing seven socks, at worst, you have got one sock of each color. Thus, after grabbing one more sock, it has to match up with one of the previous socks. Thus, you need to grab eight socks to guarantee a pair.

By the pigeon-hole principle, on the other hand, there are seven boxes (different colors), if you throw in eight objects (socks), two of them must fall into the same box, sharing the same color. ☺

Question: Same question, but seven pairs of gloves?

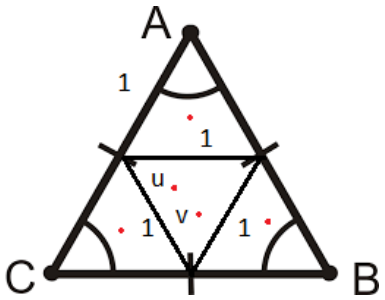
Answer: This time, 14 boxes, thus 15 will do.

Another example

Definition: Let u, v be two vertices in a graph, their distance, denoted by $d(u, v)$, is the length of a shortest path in between.

Theorem 4: Given five points inside an equilateral triangle of side length 2. The distance of at east two of them is at most 1.

Proof: Connect the midpoints of the sides of this equilateral triangle, A, to construct four equilateral triangles of side length 1.



By the Pigeonhole Principle, at least two of these five points, u, v, must be located in one of these four triangles, and $d(u, v) \leq 1$.

Homework: Problem 0.13