Proofs:
Contrapositive/Cases/Contradiction
$s(T \circ R)p$: student s takes
a subject taught by professor p.
$s(T \circ R)p \leftrightarrow \exists j \in J. s\ R\ j \wedge j\ T\ p$.
$s(T \circ R)p$: student s takes
a subject taught by professor p.

10.11 Summary of Relational Properties

A relation $R : A \to A$ is the same as a digraph with vertices A.

Reflexivity R is *reflexive* when

$$\forall x \in A.\ x\ R\ x.$$

Every vertex in R has a self-loop.

Irreflexivity R is *irreflexive* when

$$\text{NOT}[\exists x \in A.\ x\ R\ x].$$

There are no self-loops in R.

Symmetry R is *symmetric* when

$$\forall x, y \in A.\ x\ R\ y \text{ IMPLIES } y\ R\ x.$$

If there is an edge from x to y in R, then there is an edge back from y to x as well.

Asymmetry R is *asymmetric* when

$$\forall x, y \in A.\ x\ R\ y \text{ IMPLIES NOT}(y\ R\ x).$$

There is at most one directed edge between any two vertices in R, and there are no self-loops.

asymmetric means not reflexive

Antisymmetry R is *antisymmetric* when

$$\forall x \neq y \in A.\ x\ R\ y \text{ IMPLIES NOT}(y\ R\ x).$$

Equivalently,

$$\forall x, y \in A.\ (x\ R\ y \text{ AND } y\ R\ x) \text{ IMPLIES } x = y.$$

There is at most one directed edge between any two distinct vertices, but there may be self-loops.

Transitivity R is *transitive* when

$$\forall x, y, z \in A.\ (x\ R\ y \text{ AND } y\ R\ z) \text{ IMPLIES } x\ R\ z.$$

If there is a positive length path from u to v, then there is an edge from u to v.

Linear R is *linear* when

$$\forall x \neq y \in A.\ (x\ R\ y \text{ OR } y\ R\ x)$$

Given any two vertices in R, there is an edge in one direction or the other between them.

Strict Partial Order R is a *strict partial order* iff R is transitive and irreflexive iff R is transitive and asymmetric iff it is the positive length walk relation of a DAG.

Weak Partial Order R is a *weak partial order* iff R is transitive and anti-symmetric and reflexive iff R is the walk relation of a DAG.

Equivalence Relation R is an *equivalence relation* iff R is reflexive, symmetric and transitive iff R equals the *in-the-same-block*-relation for some partition of domain(R).

The empty relation is strict partial order.
The identity relation is weak partial order and equivalence order in int.
Empty relation is a unique binary relation that is symmetric and asymmetric.

Definition 10.9.1. The product $R_1 \times R_2$ of relations R_1 and R_2 is defined to be the relation with

$$\begin{aligned} \text{domain}(R_1 \times R_2) &::= \text{domain}(R_1) \times \text{domain}(R_2), \\ \text{codomain}(R_1 \times R_2) &::= \text{codomain}(R_1) \times \text{codomain}(R_2), \\ (a_1, a_2)\,(R_1 \times R_2)\,(b_1, b_2) &\quad \text{iff} \quad [a_1\ R_1\ b_1 \text{ and } a_2\ R_2\ b_2]. \end{aligned}$$

It follows directly from the definitions that products preserve the properties of transitivity, reflexivity, irreflexivity, and antisymmetry (see Problem 10.52). If R_1 and R_2 both have one of these properties, then so does $R_1 \times R_2$. This implies that if R_1 and R_2 are both partial orders, then so is $R_1 \times R_2$.

[11] Linear orders are often called "total" orders, but this terminology conflicts with the definition of "total relation," and it regularly confuses students.
Being a linear order is a much stronger condition than being a partial order that is a total relation. For example, any weak partial order is a total relation but generally won't be linear.

Definition 4.4.2. A binary relation R is:

- a *function* when it has the [≤ 1 arrow **out**] property.
- *surjective* when it has the [≥ 1 arrows **in**] property. That is, every point in the right-hand, codomain column has at least one arrow pointing to it.
- *total* when it has the [≥ 1 arrows **out**] property.
- *injective* when it has the [≤ 1 arrow **in**] property.
- *bijective* when it has both the [$= 1$ arrow **out**] and the [$= 1$ arrow **in**] property.

(A)symmetry

A relation R on set A is
- *symmetric* if $a\ R\ b \to b\ R\ a$.
- *antisymmetric* if $u\ R\ v \to \neg(v\ R\ u)$ for $u \neq v$.
- *asymmetric* if $u\ R\ v \to \neg(v\ R\ u)$.

- A nonempty relation cannot be both symmetric and asymmetric.
- An asymmetric relation is always antisymmetric.

However, a relation can be
- both symmetric and asymmetric (Problem 10.32)
- both symmetric and antisymmetric ($=$ on $\mathbb{R}$)
- neither symmetric nor asymmetric, e.g., $\leq$ and "preys on";
- symmetric but not antisymmetric, e.g., $\pmod n$
- antisymmetric but not symmetric, e.g., $\leq$ on $\mathbb{R}$.
- neither symmetric nor antisymmetric, e.g., "is a multiplier of" on $\mathbb{Z}$ (why?).

See more on wikipedia.

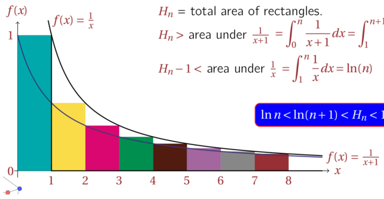
$$1 + r + r^2 + \cdots + r^n = \frac{r^{(n+1)} - 1}{r - 1} \text{ for } r \neq 1.$$

Proof (By induction on n).
- The induction hypothesis, $P(n)$, is $1 + r + r^2 + \cdots + r^n = \frac{r^{(n+1)}-1}{r-1}$, for $r \neq 1$
- In the base case, $1 + r + \cdots + r^0 = 1 = \frac{r^{(0+1)}-1}{r-1}$.
- Inductive step: Assume $P(n)$, where $n \geq 0$ and prove $P(n+1)$, i.e.,

$$1 + r + r^2 + \cdots + r^{n+1} = \frac{r^{((n+1)+1)} - 1}{r - 1}, \text{ for } r \neq 1$$

- From induction hypothesis $P(n)$ we have $1 + r + r^2 + \cdots + r^n = \frac{r^{(n+1)}-1}{r-1}$.
- Adding r^{n+1} to both sides we obtain
$(1 + r + r^2 + \cdots + r^n) + r^{n+1} = \frac{r^{(n+1)}-1}{r-1} + r^{n+1} = \frac{r^{(n+1)}-1+r^{n+1}(r-1)}{r-1} = \frac{r^{((n+1)+1)}-1}{r-1}$.
- This proves $P(n+1)$ and completes the proof by induction.

$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ (nth harmonic number)



H_n = total area of rectangles.
$H_n >$ area under $\frac{1}{x+1} = \int_0^n \frac{1}{x+1} dx = \int_1^{n+1} \frac{1}{x} dx = \ln(n+1)$.
$H_n - 1 <$ area under $\frac{1}{x} = \int_1^n \frac{1}{x} dx = \ln(n) \quad \to \quad H_n > 1 + \ln(n)$.

$\ln n < \ln(n+1) < H_n < 1 + \ln n$

We've seen $\ln n < H_n < 1 + \ln n$. They are very very close in a sense.

Def: $f(n) \sim g(n)$ if $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1$ (f is *asymptotic equal* to g).

Since $\ln n < H_n < 1 + \ln n$, we can write $H_n = \ln n + \epsilon$, where $0 < \epsilon < 1$. Hence

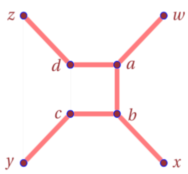
$$\lim_{n \to \infty} \frac{H_n}{\ln n} = \lim_{n \to \infty} \frac{\ln n + \epsilon}{\ln n} = 1.$$

Example: $(n^2 + n) \sim n^2$

$$\lim_{n \to \infty} \frac{n^2 + n}{n^2} = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right) = 1.$$

$\sim$ is symmetric, transitive, hence an equivalence relation.

Great if you can prove it by calculus;

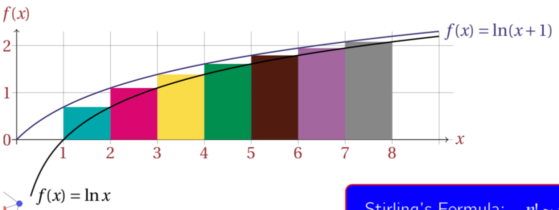


0	1	2	3	4	5	6	7
z	d	a	b	c	y	x	w
$\perp$	z	d	a	b	c	b	a

We need to keep track the "discovery" relation.

Another approach:
- Find an arbitrary vertex as root.
- If it is incident to an unselected edge then
  - If the other endpoint of this edge is not visited, visit it and repeat.
  - Else, remove this edge.
- If all edges incident to the current vertex are selected or removed then mark it "finished."
- All vertices "finished," and we end with a rooted tree.

- $\sum_{i=1}^{n} i$ is easy, but how about $\prod_{i=1}^{n} i$? Can we have a closed form for $n!$?
- $n! = \exp\left(\sum_{i=1}^{n} \ln i\right)$ because $\ln(n!) = \ln(1\cdot 2\cdot\cdots\cdot n) = \ln 1 + \ln 2 + \cdots + \ln n = \sum_{i=1}^{n} \ln i$.
- We can use the integral method to bound $\ln(n!)$, hence $n!$.



Stirling's Formula: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

Def: $f(n) = o(g(n))$ if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. ($f$ is *asymptotic smaller* than g)

For example, $n^2 = o(n^2 \ln n)$
and $n^2 = o(n^3)$.

Lemma: $o(\cdot)$ is a strict partial order.

Def: $f(n) = O(g(n))$ if $\limsup_{n\to\infty} \frac{f(n)}{g(n)} < \infty$. (Asymptotic Order of Growth)

For example, $3n^2 = O(n^2)$. §14.7.2

Lemma: $O(\cdot)$ is a partial order.

Def: $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$. (Same Order of Growth)

Lemma: $\Theta(\cdot)$ is an equivalence relation.

ymptotics: Intuitive summary

$f \sim g$ — f and g are nearly equal.
$f = o(g)$ — f much less than g.
$f = O(g)$ — f roughly $\leq g$.
$f = \Theta(g)$ — f roughly equal g.
$x^a = o(x^b)$ for $a < b$: $\frac{x^a}{x^b} = \frac{1}{x^{b-a}}$.

Lemma: $\ln x = o(x^\epsilon)$ for $\epsilon > 0$.

Proof: $\frac{1}{y} \leq y$ for $y \geq 1$, so $\int_1^z \frac{1}{y} dy \leq \int_1^z y dy$, i.e., $\ln z \leq \frac{z^2}{2}$ for $z \geq 1$.
Letting $z = \sqrt{x^\delta}$, we get $\ln z = \frac{\delta \ln x}{2} \leq \frac{z^2}{2} = \frac{x^\delta}{2}$ for $x \geq 1$.
Hence $\ln x \leq \frac{x^\delta}{\delta} = o(x^\epsilon)$ for $\delta < \epsilon$.

Corollary: $(\log_b x)^a = o(x^\epsilon)$ for all $b > 1, \epsilon >$

Lemma: $x^c = o(a^x)$ for all $a > 1, c > 0$.

Can be argued by L'Hopital's Rule or McLaurin S
(see any Calculus text).

An informal argument: $c \cdot \ln x = o(x + \ln a)$, and take exponentiation.

Logarithmic smaller than polynomial smaller than exponential.

Lemma: If $f = o(g)$ or $f \sim g$, then $f = O(g)$.
Proof: $\lim = 0 \vee \lim = 1 \to \lim < \infty$.

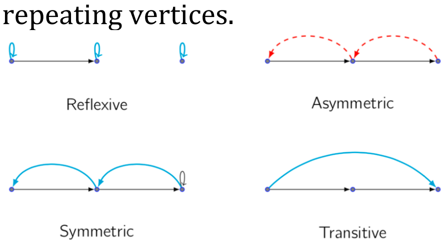
Lemma: If $f = o(g)$, then $g \neq O(f)$.
Proof: $\lim \frac{f}{g} = 0 \to \lim \frac{g}{f} = \infty$.

- G^* is walk relation of G, defined as
  uG^*v if and only if $\exists$ walk from u to v (u is connected to v).
- $G^{\leq} = G \cup Id_V$. (Id_V: edges from a vertex to itself, called *self-loops*).
- $G^{\leq}$ has a length-n walk if and only if G has a length-$\leq n$ walk.
- If G has n vertices, then the length of any path $< n$, and

$$G^* = (G^{\leq})^{n-1}.$$

$\exists$ a length-p path from u to v implies $\exists$ a length-q walk from u to v in G^* for $q > p$
(Just keep looping $q - p$ times on u.)

A cycle is a closed walk of length > 2 without repeating vertices.



Cyan arcs must exist (implied by the black arcs).
Red dashed arcs cannot exist (forbidden by the black arcs).

G_1 is *isomorphic* to G_2 if
$\exists$ bijection $f: V_1 \to V_2$ with $uv \in E_1 \longleftrightarrow f(u)f(v) \in E_2$.

We can use the Inclusion-Exclusion on 2 sets several times to prove it.

$$\begin{aligned}
|A\cup B\cup C| &= |A| + |B\cup C| - |A\cap(B\cup C)| \\
&= |A| + \left(|B| + |C| - |B\cap C|\right) - |(A\cap B)\cup(A\cap C)| \\
&= |A| + |B| + |C| - |B\cap C| - \left(|A\cap B| + |A\cap C| - |(A\cap B)\cap(A\cap C)|\right) \\
&= |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C|.
\end{aligned}$$

More generally,
on n sets $A_1, A_2, \ldots, A_n$,

$$|A_1 \cup A_2 \cup \cdots A_n| = \sum_{\emptyset \neq S \subseteq \{1,2,\ldots,n\}} (-1)^{|S|+1} \left|\bigcap_{i\in S} A_i\right|.$$

Try $n = 2$ and $n = 3$.

By induction on n.
Also see Problem 15.59.

All of the following hold for finite sets, but fail for infinite sets.

- If $A \subset B$ then $|A| < |B|$.
- A set has more elements than any of its proper subsets.
- In a finite set of numbers, there is a maximum and a minimum.
- $\exists$ a surjective function $f: A \to B$ and $\exists$ a surjective function $g: B \to A$, imply both f and g are bijections.

irref	$R \cap \mathrm{Id}_D = \emptyset$	ref	$\forall a. a\ R\ a$
sym	$R \subseteq R^{-1}$	irref	$\forall a. \neg(a\ R\ a)$
sym	$R = R^{-1}$	tran	$\forall a.\forall b.\forall c.(a\ R\ b \wedge b\ R\ c) \to a\ R\ c$
ref	$\mathrm{Id}_D \subseteq R$	comp	$\forall a.\forall b. a \neq b \to (a\ R\ b \vee b\ R\ a)$
tran	$R \circ R \subseteq R$	sym	$\forall a.\forall b. a\ R\ b \to b\ R\ a$
ints. none	$R \subseteq R \circ R$	asym	$\forall a.\forall b. a\ R\ b \to \neg(b\ R\ a)$
asym	$R \cap R^{-1} = \emptyset$	sym	$\forall a.\forall b. a\ R\ b \longleftrightarrow b\ R\ a$
anti	$R \cap R^{-1} \subseteq \mathrm{Id}_D$	anti	$\forall a.\forall b.(a \neq b \wedge a\ R\ b) \to \neg(b\ R\ a)$
ref & comp	$\overline{R} \subseteq R^{-1}$	comp & anti	$\forall a.\forall b. a = b \vee [a\ R\ b \longleftrightarrow \neg(b\ R\ a)]$
comp & anti	$\overline{R} - \mathrm{Id}_D = R^{-1} - \mathrm{Id}_D$	tran	$\forall a.\forall c.[\exists b. a\ R\ b \wedge b\ R\ c] \to a\ R\ c$

Given any total function $f: A \to B$,
we can define an equivalence relation $\equiv_f$ on A

$$a \equiv_f a' \longleftrightarrow f(a) = f(a').$$

Theorem:
Relation R on set A is an equivalence relation if and only if
R is $\equiv_f$ for some total function $f: A \to B$.

(Weak) password conditions:

- characters are digits and letters
- between 6 and 8 characters long
- starts with a letter
- case sensitive

Let $L = \{a, b, \ldots, z, A, B, \ldots, Z\}$
and $D = \{0, 1, 2, \ldots, 9\}$.

Using the product rule and the sum rule.

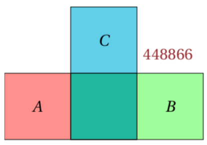
All length-n words starting with a letter can be written as $P_n = L \times (L \cup D)^{n-1}$. Hence

$$\begin{aligned}
|P_n| &= |L \times (L\cup D)^{n-1}| \\
&= |L| \cdot |(L\cup D)|^{n-1} \\
&= |L| \cdot (|L| + |D|)^{n-1} \\
&= 52 \cdot (52 + 10)^{n-1}.
\end{aligned}$$

All passwords comprises length-6, length-7, and length-8 passwords, Hence

$$\begin{aligned}
|P| &= |P_6 \cup P_7 \cup P_8| \\
&= 52 \cdot (62^5 + 62^6 + 62^7) \\
&\approx 1.8 \cdot 10^{14}.
\end{aligned}$$

- A: 6-digits numbers containing 3, 6.
- B: 6-digits numbers containing 3, 0.
- C: 6-digits numbers containing 6, 0.



$A \cap B \subset C \to A \cap B = A \cap B \cap C$;
$B \cap C = A \cap B \cap C$;
$A \cap C = A \cap B \cap C$.

- N_3: 6-digits numbers containing 3.
- N_6: 6-digits numbers containing 6.
- N_0: 6-digits numbers containing 0.
- $|N_3| = |N_6| = |N_0| = 10^6 - 9^6 = 468559$.
- $|N_3 \cup N_6| = |N_6 \cup N_0| = |N_3 \cup N_0| = 10^6 - 8^6 = 737856$.
- $|N_3 \cup N_6 \cup N_0| = 10^6 - 7^6 = 882351$.

$A = N_3 \cap N_6$.
$|A| = |N_3 \cap N_6| = |N_3| + |N_6| - |N_3 \cup N_6| = 199262$.

$|A \cap B \cap C| = |N_3 \cap N_6 \cap N_0| = |N_3 \cup N_6 \cup N_0|$
$-|N_3| - |N_6| - |N_0| + |N_3 \cap N_6| + |N_3 \cap N_0| + |N_6 \cap N_0|$
$= 74460$.

$$|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C| = |A| + |B| + |C| - 2|A\cap B\cap C|.$$

H is a *subgraph* of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

A subgraph H is a *spanning subgraph* if $V(H) = V(G)$.

A *spanning tree* of G is a spanning subgraph of G that is a tree.