Computer Science 130
Discrete Structures
Fall 2011 Lecture Notes

Alex Vondrak

December 2, 2011

1 Formal Logic

1.1 Boolean Logic

A statement (or proposition) is a sentence which is either true or false. They can be represented abstractly using variables. E.g.,

Baseballs are round	. . . is true
Baseballs are square	. . . is false
The sky is blue	. . . is true
The Earth is the center of the universe	. . . is false

We can form statements from other statements using Boolean (or propositional) operators:

- Conjunction (“and”)
- Disjunction (“or”)
- Negation (“not”)
- Implication (“if. . . then. . . ”)
- Equivalence (“if and only if”)

Conjunction (“and”)

conjuncts

A	B	$A \wedge B$
F	F	F
F	T	F
T	F	F
T	T	T

truth table

E.g.,

Baseballs are round and the sky is blue . . . is true

Disjunction ("or")

disjuncts

A	B	$A \lor B$
F	F	F
F	T	T
T	F	T
T	T	T

truth table

E.g.,

Baseballs are square or baseballs are round ...is true

Negation ("not")

A	A'
F	T
T	F

truth table

E.g.,

The Earth is not the center of the universe ...is true

Note: negation is a unary operator, whereas the other propositional operator we consider are binary operators.

Implication ("if...then...")

antecedent consequent

A	B	$A \to B$
F	F	T
F	T	T
T	F	F
T	T	T

truth table

$A \to B$ can be stated many ways in English:

- "If A, then B"
- "A implies B"
- "A only if B"
- "B if A"
- "A is a sufficient condition for B"
- "B is a necessary condition for A"

Equivalence ("if and only if")

A	B	$A \leftrightarrow B$
F	F	T
F	T	F
T	F	F
T	T	T

truth table

A (propositional) well-formed formula (WFF) is

1. A statement variable (e.g., $A, B, C, \ldots$)

or 2. An expression with the form

$$\begin{aligned} &(f_1 \wedge f_2) \\ \text{or } &(f_1 \vee f_2) \\ \text{or } &(f') \\ \text{or } &(f_1 \rightarrow f_2) \\ \text{or } &(f_1 \leftrightarrow f_2) \end{aligned}$$

where f, f_1, f_2 are WFFs.

E.g.,

- A
- $(A \rightarrow B)$
- $(((A') \vee B) \leftrightarrow (A \rightarrow B))$

The value of a variable must be assigned. The value of a compound WFF is determined by applying the Boolean operator to the values of its component WFFs.

Matching parentheses may be omitted, in which case the order of several operations within the same parentheses is determined by precedence:

high precedence (apply first)

Boolean Operator Precedence
Negation ($'$)
Conjunction ($\wedge$)
Disjunction ($\vee$)
Implication ($\rightarrow$)
Equivalence ($\leftrightarrow$)

low precedence (apply last)

Operators of equal precedence are applied left-to-right (i.e., they are left associative).

E.g.,

$$\begin{aligned} A \vee B' &\text{ has the same value as } (A \vee (B')) \\ A \rightarrow B \vee C &\text{ has the same value as } (A \rightarrow (B \vee C)) \\ A \wedge B \vee C \rightarrow D' &\text{ has the same value as } \Big(((A \wedge B) \vee C) \rightarrow (D')\Big) \end{aligned}$$

A truth table evaluates a WFF for every possible truth assignment of values to its variables.

E.g.,

A	B	$A \rightarrow B$	$A' \vee B$	$(A \rightarrow B) \leftrightarrow (A' \vee B)$
F	F	T	T	T
F	T	T	T	T
T	F	F	F	T
T	T	T	T	T

A	B	$(A \vee B)'$	$A' \wedge B'$	$(A \vee B)' \leftrightarrow A' \wedge B'$
F	F	T	T	T
F	T	F	F	T
T	F	F	F	T
T	T	F	F	T

A WFF is a tautology if its value is true for every truth assignment.

A WFF is a contradiction if its value is false for every truth assignment.

E.g.,

$$\begin{aligned} (A \rightarrow B) \leftrightarrow (A' \vee B) &\text{ is a tautology} \\ (A \vee B)' \leftrightarrow A' \wedge B' &\text{ is a tautology} \\ A \wedge A' &\text{ is a contradiction} \end{aligned}$$

WFFs P and Q are equivalent, denoted $P \Leftrightarrow Q$, if $P \leftrightarrow Q$ is a tautology.

Common Equivalences

	Equivalence	Dual
1.	$A \lor B \Leftrightarrow B \lor A$	$A \land B \Leftrightarrow B \land A$
2.	$(A \lor B) \lor C \Leftrightarrow A \lor (B \lor C)$	$(A \land B) \land C \Leftrightarrow A \land (B \land C)$
3.	$A \lor (B \land C) \Leftrightarrow (A \lor B) \land (A \lor C)$	$A \land (B \lor C) \Leftrightarrow (A \land B) \lor (A \land C)$
4.	$A \lor \mathtt{F} \Leftrightarrow A$	$A \land \mathtt{T} \Leftrightarrow A$
5.	$A \lor A' \Leftrightarrow \mathtt{T}$	$A \land A' \Leftrightarrow \mathtt{F}$
6.	$(A \lor B)' \Leftrightarrow A' \land B'$	$(A \land B)' \Leftrightarrow A' \lor B'$
7.	$A \lor A \Leftrightarrow A$	$A \land A \Leftrightarrow A$
8.	$A \to B \Leftrightarrow A' \lor B$	
9.	$A \to B \Leftrightarrow B' \to A'$	
10.	$A \to (B \to C) \Leftrightarrow (A \land B) \to C$	

The dual of a WFF having operators $\land$, $\lor$, $'$ is obtained by interchanging $\land/\lor$ and $\mathtt{T}/\mathtt{F}$. In general, the duals of equivalent WFFs are equivalent.

These equivalences are named properties:

1.	Commutativity	comm
2.	Associativity	ass
3.	Distributivity	dist
4.	Identity	
5.	Complement	
6.	De Morgan's Law	deMorgan
7.	Idempotence	idem
8.	Implication Rewriting	imp
9.	Contraposition	contr
10.	Conditional Proof, a.k.a. Exportation	exp

1.2 Propositional Logic

One way to show a propositional WFF is a tautology is by using a truth table. However, the size of a truth table grows exponentially, and they don't reflect any actual reasoning.

Another method is to make a proof using deduction in a proof system.

Proof System

An axiom is a WFF which is true and is accepted without proof.

An inference rule is a method for deducing a WFF from other WFFs.

A proof is a sequence of WFFs in which each WFF is an axiom or is deduced from preceding WFFs by an inference rule.

A theorem is the last WFF in a proof.

A system of natural deduction consists of as many intuitively valid inference rules as possible, to reflect the way we “naturally” reason. Such rules include:

Modus Ponens: Q can be deduced from P, $\mathsf{P} \to \mathsf{Q}$. mp

Modus Tollens: P' can be deduced from Q', $\mathsf{P} \to \mathsf{Q}$. mt

Hypothetical Syllogism: $\mathsf{P} \to \mathsf{R}$ can be deduced from $\mathsf{P} \to \mathsf{Q}$, $\mathsf{Q} \to \mathsf{R}$. hs

Dilemma: $\mathsf{Q} \vee \mathsf{S}$ can be deduced from $\mathsf{P} \to \mathsf{Q}$, $\mathsf{R} \to \mathsf{S}$, $\mathsf{P} \vee \mathsf{R}$. dil

Conjunction: $\mathsf{P} \wedge \mathsf{Q}$ can be deduced from P, Q. conj

Simplification: P can be deduced from $\mathsf{P} \wedge \mathsf{Q}$. simp

Q can be deduced from $\mathsf{P} \wedge \mathsf{Q}$.

Addition: $\mathsf{P} \vee \mathsf{Q}$ can be deduced from P. add

$\mathsf{P} \vee \mathsf{Q}$ can be deduced from Q.

Disjunctive Syllogism: Q can be deduced from $\mathsf{P} \vee \mathsf{Q}$, P'. ds

P can be deduced from $\mathsf{P} \vee \mathsf{Q}$, Q'.

Further rules may apply that aren’t strictly inference rules. Inference rules deduce a *new* conclusion from existing WFFs. However, rewrite rules are equivalences that let you rewrite the series of symbols that make up some WFF. E.g.,

Double Negation: $(\mathsf{P}')'$ is the same as P. dn

Material Equivalence: $\mathsf{A} \leftrightarrow \mathsf{B}$ is the same as $(\mathsf{A} \to \mathsf{B}) \wedge (\mathsf{B} \to \mathsf{A})$. equiv

Etc.: Any other known equivalence (e.g., from the list on page 5).

In contrast to natural proof systems, axiomatic proof systems are minimalist: they aim to have a small number of axioms and inference rules from which we then build up proofs of more intuitive notions. That is, we take as little for granted as we can. By considering as few things “intuitively true” as possible, it makes us more certain that resulting proofs are correct, since they rely on fewer assumptions.

We will use the following axiomatic proof system, called propositional logic:

Axioms:

1. $P \to (Q \to P)$
2. $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
3. $(Q' \to P') \to (P \to Q)$ contr

Inference Rule: Q can be deduced from P, $P \to Q$. mp

Example Proof of theorem $A \to A$

1. $(\overbrace{A}^{P} \to (\overbrace{(A \to A)}^{Q} \to \overbrace{A}^{R})) \to$
   $((\underbrace{A}_{P} \to \underbrace{(A \to A)}_{Q}) \to (\underbrace{A}_{P} \to \underbrace{A}_{R}))$ Axiom 2
2. $\overbrace{A}^{P} \to (\overbrace{(A \to A)}^{Q} \to \overbrace{A}^{P})$ Axiom 1
3. $(A \to (A \to A)) \to (A \to A)$ 1, 2, mp
4. $A \to (A \to A)$ Axiom 1
5. $A \to A$ 3, 4, mp

A proof system is sound if every theorem which can be proved is a tautology.

A proof system is complete if every tautology is a theorem which can be proved.

Propositional logic is sound and complete, although showing that is beyond the scope of this course.

Generalized Methods of Deduction

- To prove $P_1 \wedge P_2 \wedge \ldots \wedge P_n \to Q$, write P_1, P_2, …, P_n in your proof as hypotheses, then deduce Q as a conclusion.
- To prove $P_1 \wedge P_2 \wedge \ldots \wedge P_n \to (R \to S)$, write P_1, P_2, …, P_n, R in your proof as hypotheses, then deduce S as a conclusion.
- $P_1 \wedge P_2 \wedge \ldots \wedge P_n$ can be deduced from P_1, P_2, …, P_n. conj
- P with R subsituted for S can be deduced from P, $R \leftrightarrow S$

Example Prove $(P' \to Q') \wedge (P \to S) \to (Q \to S)$

1.	$P' \to Q'$	hyp
2.	$P \to S$	hyp
3.	Q	hyp
4.	$(P' \to Q') \to (Q \to P)$	Axiom 3
5.	$Q \to P$	1, 4, mp
6.	P	3, 5, mp
7.	S	2, 6, mp

Example Prove $(I \to H) \wedge (F \vee H') \wedge I \to F$

1.	$I \to H$	hyp
2.	$F \vee H'$	hyp
3.	I	hyp
4.	H	1, 3, mp
5.	$H' \vee F$	2, comm
6.	$H \to F$	5, imp
7.	F	4, 6, mp

Known tautologies can be used without proof

1.3, 1.4 Predicate Logic

A predicate well-formed formula (predicate WFF) is

1. $P(x_1, x_2, \ldots, x_n)$, where $x_1, x_2, \ldots, x_n$ are constants or variables and P is a predicate

or 2.

$$\begin{aligned} &(f_1 \wedge f_2) \\ \text{or } &(f_1 \vee f_2) \\ \text{or } &(f') \\ \text{or } &(f_1 \to f_2) \\ \text{or } &(f_1 \leftrightarrow f_2) \end{aligned}$$

where f, f_1, f_2 are WFFs.

or 3. A quantified formula—i.e., either

$$(\forall x)[f] \qquad \text{(universal quantifier (i.e., “For \textit{A}ll”))}$$
$$\text{or } (\exists x)[f] \qquad \text{(existential quantifier (i.e., “There \textit{E}xists”))}$$

where x is a variable and f is a predicate WFF.

E.g.,

- $P(x)$
- $(\forall x)[P(x)]$
- $(\exists x)[P(x)]$
- $(\forall x)\big[(\exists y)[P(x) \land Q(x, y)]\big]$
- $(\exists x)\big[(\forall y)[P(x, y) \to Q(x) \lor Q(y)']\big]$

Matching parentheses “( )” and brackets “[ ]” may be omitted, in which case the order of operations is determined by precedence and associativity as in propositional WFFs (see page 3).

An interpretation consists of

1. a domain of interpretation—a set of objects from which constants and variables are assigned,
2. an assignment of a property of the objects in the domain of interpretation to each predicate,
3. an assignment of an object in the domain of interpretation to each constant.

The value of a predicate WFF f in an interpretation depends on the form of f:

1. If $f = P(x_1, x_2, \ldots, x_n)$, the value is the result of the property assigned to P applied to the objects assigned to $x_1, x_2, \ldots, x_n$.
2. If f is formed using a Boolean operator, the value is the result of the Boolean operator applied to the values of its operands.
3. If $f = (\forall x)[f_1]$, the value is

$$\begin{cases} \text{true} & \text{if every assignment of an object in the domain of} \\ & \text{interpretation to } x \text{ causes the value of } f_1 \text{ to} \\ & \text{be true} \\ \text{false} & \text{otherwise} \end{cases}$$

4. If $f = (\exists x)[f_1]$, the value is

$$\begin{cases} \text{true} & \text{if some assignment of an object in the domain of} \\ & \text{interpretation to } x \text{ causes the value of } f_1 \text{ to} \\ & \text{be true} \\ \text{false} & \text{otherwise} \end{cases}$$

Example Consider the following interpretation:

- The domain of interpretation is the set of all integers
- $A(x)$ is "$x > 0$"
- $B(x, y)$ is "$x > y$"
- $C(x)$ is "$x \leq 0$"
- $\ldots, -2, -1, 0, 1, 2, \ldots$ are the usual constants

Evaluate the following:

$(\exists x)[A(x)]$ . . . true

$(\forall x)[A(x)]$ . . . false

$(\forall x)[A(x) \wedge C(x)]$ . . . false

$(\exists x)[A(x)] \wedge (\exists x)[C(x)]$ . . . true

$(\exists x)[A(x) \wedge C(x)]$ . . . false

$(\exists x)\big[A(x) \wedge (\forall y)[B(x, y) \rightarrow C(y)]\big]$ . . . true

$(\forall x)\big[A(x) \wedge (\forall y)[B(x, y) \rightarrow C(y)]\big]$ . . . false

Example Consider the following interpretation:

- The domain of interpretation is the set of all people
- $I(x)$ is "x is intelligent"
- $M(x)$ is "x likes music"
- $S(x)$ is "x is a student"

Rewrite the following as a predicate WFF:

- All students are intelligent

$$(\forall x)[S(x) \rightarrow I(x)]$$

- Some intelligent students like music

$$(\exists x)[I(x) \wedge S(x) \wedge M(x)]$$

- Everyone who likes music is a stupid student

$$(\forall x)[M(x) \rightarrow I(x)' \wedge S(x)]$$

$$(\forall x)[\,\overbrace{\ f_1\ }^{\text{scope of variable } x}\,]$$

$$(\exists x)[\ f_1\ ]$$

A variable in a predicate WFF is bound if

1. It occurs immediately after a quantifier (i.e., it is a quantified variable).

or 2. It is within the scope of a quantified WFF whose quantified variable is the same as it (i.e., it is bound to a quantified variable).

Otherwise, a variable is free. E.g.,

$$(\forall \underset{\star}{a})\big[(\exists \underset{\star}{b})[P(\underset{\star}{a}, \underset{\star}{b})] \land Q(\underset{\star}{a}, \underset{\star\star}{b})\big] \qquad (\star = \text{bound}, \star\star = \text{free})$$

A predicate WFF with free variables cannot be evaluated without assigning objects to its free variables.

Predicate WFFs without free variables are called sentences, and can always be evaluated (although the value may vary from one interpretation to the next).

A sentence is valid if it is true in all interpretations. E.g., the following are valid:

- $(\forall x)[P(x) \land Q(x)] \leftrightarrow (\forall x)[P(x)] \land (\forall x)[Q(x)]$
- $\big((\forall x)[f]\big)' \leftrightarrow (\exists x)[f']$
- $\big((\exists x)[f]\big)' \leftrightarrow (\forall x)[f']$
- $(\forall x)[P(x)] \to (\exists x)[P(x)]$

Is $(\forall x)[P(x) \lor Q(x)] \to (\forall x)[P(x)] \lor (\forall x)[Q(x)]$ valid?

We will use the following proof system, called predicate logic:

Axioms:

With arbitrary predicate WFFs P, Q, R and arbitrary predicate WFFs $\mathsf{P}(x)$, $\mathsf{Q}(x)$ in which x is free…

1. $\mathsf{P} \to (\mathsf{Q} \to \mathsf{P})$
2. $(\mathsf{P} \to (\mathsf{Q} \to \mathsf{R})) \to ((\mathsf{P} \to \mathsf{Q}) \to (\mathsf{P} \to \mathsf{R}))$
3. $(\mathsf{Q}' \to \mathsf{P}') \to (\mathsf{P} \to \mathsf{Q})$ contr
4. $(\forall x)[\mathsf{P}(x) \to \mathsf{Q}(x)] \to \big((\forall x)[\mathsf{P}(x)] \to (\forall x)[\mathsf{Q}(x)]\big)$
5. Universal Instantiation ui

   $(\forall x)[\mathsf{P}(x)] \to \mathsf{P}(x)$ (where x is a variable)

   $(\forall x)[\mathsf{P}(x)] \to \mathsf{P}(a)$ (where a is a constant)

6. Existential Instantiation ei

   $$(\exists x)[\mathsf{P}(x)] \to \mathsf{P}(t)$$

   where t is a constant not previously appearing in the proof
7. Existential Generalization eg

   $$\mathsf{P}(x) \to (\exists x)[\mathsf{P}(x)]$$
   $$\mathsf{P}(a) \to (\exists x)[\mathsf{P}(x)]$$

   where a is a constant and x doesn't appear in $\mathsf{P}(a)$
8. $\big((\exists x)[\mathsf{P}(x)]\big)' \leftrightarrow (\forall x)[\mathsf{P}(x)']$ deMorgan

Inference Rules:

1. Modus Ponens: Q can be deduced from P, $\mathsf{P} \to \mathsf{Q}$. mp
2. Universal Generalization: $(\forall x)\mathsf{Q}$ can be deduced from Q as long as… ug

   (a) Q has not been deduced from a hypothesis in which x is a free variable,

   and (b) Q has not been deduced using Axiom 6 from $(\exists y)[\mathsf{Q}(y)]$ in which x is a free variable.

Example Prove $(\forall x)[\mathsf{P}(x) \wedge \mathsf{Q}(x)] \to (\forall x)[\mathsf{P}(x)] \wedge (\forall x)[\mathsf{Q}(x)]$

1. $(\forall x)[\mathsf{P}(x) \wedge \mathsf{Q}(x)]$ hyp
2. $\mathsf{P}(x) \wedge \mathsf{Q}(x)$ 1, ui, mp
3. $\mathsf{P}(x)$ 2, simp
4. $\mathsf{Q}(x)$ 2, simp
5. $(\forall x)[\mathsf{P}(x)]$ 3, ug
6. $(\forall x)[\mathsf{Q}(x)]$ 4, ug
7. $(\forall x)[\mathsf{P}(x)] \wedge (\forall x)[\mathsf{Q}(x)]$ 5, 6, conj

Example Prove $(\forall x)[P(x) \vee Q(x)] \rightarrow (\exists x)[P(x)] \vee (\forall x)[Q(x)]$

1. $(\forall x)[P(x) \vee Q(x)]$	hyp
2. $P(x) \vee Q(x)$	1, ui, mp
3. $P(x)' \rightarrow Q(x)$	2, imp
4. $(\forall x)[P(x)' \rightarrow Q(x)]$	3, ug
5. $(\forall x)[P(x)'] \rightarrow (\forall x)[Q(x)]$	4, axiom 4, mp
6. $((\exists x)[P(x)])' \rightarrow (\forall x)[Q(x)]$	5, deMorgan
7. $(\exists x)[P(x)] \vee (\forall x)[Q(x)]$	6, imp

1.5 Logic Programming

A Horn clause is a WFF of the form

$$P_1 \wedge P_2 \wedge \ldots \wedge P_n \rightarrow Q$$

A logic program is a sequence of Horn clauses which are viewed as hypotheses.

A query asks whether a WFF can be deduced from a logic program. A query is answered by a method called resolution, which essentially seeks to prove that the WFF is a theorem by using modus ponens.

Prolog (programming with logic) is the most popular logic programming language, particularly in artificial intelligence applications.

This area is deeply studied in CS 352 & CS 420.

1.6 Proof of Correctness

Program verification is the process of ensuring that a computer program is correct (i.e., it behaves according to its specification).

Proofs of correctness use formal logic proofs to verify a program. Specifically, for each line P of the program, we write the Hoare triple

$$\{Q\}\ P\ \{R\}$$

where Q is the precondition and R is the postcondition, which are assertions of what holds true (respectively) before and after P.

This topic may appear in your CS 480 class (or in graduate-level courses).

2 Proofs, Recursion, and Analysis of Algorithms

2.1 Proof Techniques

In Chapter 1 we studied formal logic—arguments devoid of meaning, but true by the form of their symbols. In practice, we want to prove facts about particular subjects using the same techniques, but in *informal* ways.

Disproof by Counterexample

To prove: $(\forall x)[P(x)]$ is not true, i.e., $\big((\forall x)[P(x)]\big)'$

Show that: $(\exists x)[P(x)']$

Example Disprove that all animals living in the ocean are fish.

Proof. For example, whales live in the ocean and are not fish. □

Example Disprove that all input to a computer is provided by the keyboard.

Proof. For example, mice provide input to a computer. □

Direct Proof

To prove: $P(x)$

Show that: $P(x)$ is true by generalized methods of deduction

Example Show that every integer divisible by 6 is divisible by 3.

Proof. Let x be an integer divisible by 6. There is an integer y s.t. $x = 6 \cdot y$. Therefore, $x = 3 \cdot (2 \cdot y)$, and x is divisible by 3.

□

Proof by Contraposition

To prove: $P(x) \to Q(x)$

Show that: $Q(x)' \to P(x)'$

Example Show that every integer divisible by 6 is divisible by 3.

Proof. We show that every integer not divisible by 3 is not divisible by 6.

Let x be an integer not divisible by 3. $x \neq 3 \cdot y$, for any integer y.

Therefore $x \neq 3 \cdot (2 \cdot z)$ for any integer z.

Thus $x \neq 6 \cdot z$ for any integer z.

So x is not divisible by 6. □

Example Prove that if the square of an integer is odd, the integer is odd.

Proof. Let x be an even integer. So, $x = 2y$ for some integer y. Therefore $x^2 = (2y)^2 = 2^2y^2 = 2(2y^2)$, and x^2 is itself even. □

Proof by Contradiction

To prove: $P(x)$

Show that: $P(x)' \rightarrow \mathtt{F}$, i.e., $P(x)'$ is a contradiction.

Example Prove if $x + x = x$, then $x = 0$.

Proof. To the contrary, suppose $x + x = x$ and $x \neq 0$.

Subtracting x from both sides of $x + x = x$ implies that $x = 0$.

$\therefore x \neq 0$ and $x = 0$, a contradiction. □

Example Prove that $\sqrt{2}$ is irrational.

Proof. To the contrary, suppose $\sqrt{2}$ is rational.

Then there are integers p and $q \neq 0$ s.t. $\sqrt{2} = p/q$, and p & q have no common factors.

$$\begin{aligned}(\sqrt{2})^2 &= (p/q)^2 \\ 2 &= p^2/q^2 \\ p^2 &= 2q^2\end{aligned}$$

So, p^2 is even. Since p^2 is even, p must also be even. That is, $\exists y, p = 2y$.

$$\begin{aligned}p^2 &= 2q^2 \\ (2y)^2 &= 2q^2 \\ 2^2y^2 &= 2q^2 \\ q^2 &= 2y^2\end{aligned}$$

So q^2 is even, and therefore q is even.

$$\begin{aligned}\therefore\ \sqrt{2} = p/q &\rightarrow p \text{ and } q \text{ are both even} \\ &\rightarrow p \text{ and } q \text{ have the common factor } 2\text{, a contradiction}\end{aligned}$$

□

2.2 Induction

Proof by Weak Induction

To prove: $(\forall n)[n \geq 1 \rightarrow P(n)]$

Show that:

$$\overbrace{P(1)}^{\text{basis}} \quad \wedge \quad \overbrace{(\forall k)[\underbrace{P(k)}_{\text{I.H.}^*} \rightarrow P(k+1)]}^{\text{inductive step}}$$

* = Inductive Hypothesis

Example Prove for $n \geq 1$, $\sum_{i=1}^{n}(2i-1) = n^2$.

Proof. (By weak induction on n)

Basis ($n = 1$): $\sum_{i=1}^{1}(2i-1) = 2 \cdot 1 - 1 = 2 - 1 = 1^2$

Inductive Step:

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \sum_{i=1}^{k}(2i-1) + 2(k+1) - 1 \\ &= k^2 + 2(k+1) - 1 && \text{(by I.H.)} \\ &= k^2 + 2k + 1 \\ &= (k+1)^2\end{aligned}$$

□

Example Prove for $n \geq 0$, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Proof. (By weak induction on n)

Basis ($n = 0$): $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$

Inductive Step:

$$\begin{aligned}\sum_{i=0}^{k+1} 2^i &= \sum_{i=0}^{k} 2^i + 2^{k+1} \\ &= 2^{k+1} - 1 + 2^{k+1} && \text{(by I.H.)} \\ &= 2(2^{k+1}) - 1 \\ &= 2^{(k+1)+1} - 1\end{aligned}$$

□

Example Prove for $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Proof. (By weak induction on n)

Basis ($n = 1$): $2^{2\cdot 1} - 1 = 4 - 1 = 3$ is divisible by 3.

Inductive Step:

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^2 2^{2k} - 1 \\ &= 2^2(2^{2k} - 1) + 3 \\ &= 4(3m) + 3 && \text{(by I.H.)} \\ &= 3(4m + 1) && \text{(is divisible by 3)} \end{aligned}$$

□

Proof by Strong Induction

To prove: $(\forall n)[n \geq 1 \to P(n)]$

Show that:

$$\overbrace{P(1)}^{\text{basis}} \quad \wedge \quad \overbrace{\Big(\forall k\Big)\Big[\underbrace{(\forall r)[1 \leq r \leq k \to P(r)]}_{\text{I.H.}} \to P(k+1)\Big]}^{\text{inductive step}}$$

Example Prove that every postage ≥ 8¢ can be formed with 3¢ and 5¢ stamps.

Proof. (By strong induction on the cost.)
Let $P(n) =$"postage of n¢ can be formed using only 3¢ and 5¢ stamps".

Basis ($n = 8$): $5\text{¢} + 3\text{¢} = 8\text{¢}$

Basis ($n = 9$): $3\text{¢} + 3\text{¢} + 3\text{¢} = 9\text{¢}$

Basis ($n = 10$): $5\text{¢} + 5\text{¢} = 10\text{¢}$

Inductive Step ($n \geq 11$):

Assume as our I.H. that $P(r)$ is true for $8 \leq r \leq k$.

Consider $k + 1 \geq 11$. By the I.H., $P\big((k+1) - 3\big)$ is true, as $(k+1) - 3 = k - 2 \geq 8$. Then, to the stamps used for the $\big((k+1) - 3\big)$¢ postage, add a 3¢ stamp, thus giving us the total postage of $(k+1)$¢—proving $P(k+1)$ is true.

□

2.4 Recursive Definitions

A recursive (inductive) definition defines an entity in terms of itself; technically, in simpler versions of itself. There are two parts:

Basic Case (Basis)

The most primitive case(s) of the entity are defined without self-reference.

Recursive Case (Inductive Case)

New cases of the entity are defined in terms of simpler cases of the entity.

A sequence S is an ordered (potentially infinite) list of objects. $\mathsf{S}(n)$ denotes the n^{th} object in the sequence.

Example

$$\begin{aligned} \mathsf{S}(1) &= 2 && \text{(basic case)} \\ \mathsf{S}(n) &= 2 \cdot \mathsf{S}(n-1) \quad \text{for } n \geq 2 && \text{(recursive case)} \end{aligned}$$

The "expanded" sequence S is $2, 4, 8, 16, 32, \ldots$

Example

$$\begin{aligned} \mathsf{T}(1) &= 1 && \text{(basic case)} \\ \mathsf{T}(n) &= \mathsf{T}(n-1) + 3 \quad \text{for } n \geq 2 && \text{(recursive case)} \end{aligned}$$

The "expanded" sequence T is $1, 4, 7, 10, 13, \ldots$

Example The Fibonacci sequence F is defined by

$$\begin{aligned} \mathsf{F}(1) &= 1 && \text{(basic case)} \\ \mathsf{F}(2) &= 1 && \text{(basic case)} \\ \mathsf{F}(n) &= \mathsf{F}(n-2) + \mathsf{F}(n-1) \quad \text{for } n > 2 && \text{(recursive case)} \end{aligned}$$

The "expanded" Fibonacci sequence is $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

Proofs of properties about recursively defined entities are typically inductive.

Example Prove $F(n+4) = 3F(n+2) - F(n)$ for $n \geq 1$.

Proof. (By strong induction on n)

Basis ($n = 1$): $F(5) = 5 = 3 \cdot 2 - 1 = 3F(3) - F(1)$

Basis ($n = 2$): $F(6) = 8 = 3 \cdot 3 - 1 = 3F(4) - F(2)$

Inductive Step:

$$\begin{aligned}
F((k+1)+4) &= F(k+5) \\
&= F(k+3) + F(k+4) && \text{(by defn. } F\text{)} \\
&= \big(3F(k+1) - F(k-1)\big) + \big(3F(k+2) - F(k)\big) && \text{(by I.H.)} \\
&= 3\big(F(k+1) + F(k+2)\big) - \big(F(k-1) + F(k)\big) \\
&= 3F(k+3) - F(k+1) && \text{(by defn. } F\text{)} \\
&= 3F((k+1)+2) - F(k+1)
\end{aligned}$$

□

A set is an *un*ordered collection of objects in which no object appears twice in the collection. They, too, may be defined recursively.

Example Earlier, we defined the set of all propositional WFFs recursively:

1. A variable (e.g., $A, B, C, \ldots$) is a WFF (basic case)
2. A WFF may be an expression with the form (recursive case)

$$\begin{aligned}
&(f_1 \wedge f_2) \\
\text{or } &(f_1 \vee f_2) \\
\text{or } &(f') \\
\text{or } &(f_1 \rightarrow f_2) \\
\text{or } &(f_1 \leftrightarrow f_2)
\end{aligned}$$

   where f, f_1, f_2 are WFFs.

Example The set of ancestors of Alex Vondrak is recursively defined:

1. Alex Vondrak's parents are ancestors. (basic case)
2. Parents of ancestors are themselves ancestors. (recursive case)

Really, we could recursively define pretty much anything.

Example Multiplication can be defined recursively:

1. $m \cdot 1 = m$ (basic case)
2. $m \cdot n = m \cdot (n-1) + m$ for $n \geq 2$ (recursive case)

For instance,

$$\begin{aligned} 3 \cdot 4 &= 3 \cdot 3 + 3 \\ &= (3 \cdot 2 + 3) + 3 \\ &= \big((3 \cdot 1 + 3) + 3\big) + 3 \\ &= \big((3 + 3) + 3\big) + 3 \\ &= 12 \end{aligned}$$

Example Exponentiation can be defined recursively:

1. $a^0 = 1$ (basic case)
2. $a^n = (a^{n-1}) \cdot a$ (recursive case)

For instance,

$$\begin{aligned} 2^4 &= 2^3 \cdot 2 \\ &= 2^2 \cdot 2 \cdot 2 \\ &= 2^1 \cdot 2 \cdot 2 \cdot 2 \\ &= 2^0 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 16 \end{aligned}$$

An algorithm is a step-by-step process for solving a problem. A recursive algorithm is an algorithm that uses recursion.

Example The binary search algorithm is a fast way to search through a sorted sequence, S, for a particular member, x.

At any particular step of the algorithm, we're narrowing the search to somewhere between $S(i)$ and $S(j)$ (initially 1 and n). For each specific i and j, represent the midpoint between them with $m = \lfloor (i+j)/2 \rfloor$.

Basic Cases:

1. If $i > j$, then x is not in S.
2. If $S(m) = x$, then x is in S.

Recursive Cases:

1. If $S(m) > x$, then search between $S(i)$ and $S(m-1)$
2. If $S(m) < x$, then search between $S(m+1)$ and $S(j)$

3 Sets, Combinatorics, Probability, and Number Theory

3.1 Sets

A set is an unordered collection of objects in which no object appears twice.

Notation

$a \in A$	(object a is a member (or element) of set A)
$a \notin A$	(object a is not a member of set A)

$A = B$	$\Leftrightarrow$	$(\forall x)[x \in A \leftrightarrow x \in B]$	(equal)
$A \subseteq B$	$\Leftrightarrow$	$(\forall x)[x \in A \rightarrow x \in B]$	(subset)
$A \supseteq B$	$\Leftrightarrow$	$(\forall x)[x \in B \rightarrow x \in A]$	(superset)
$A \subset B$	$\Leftrightarrow$	$A \subseteq B \wedge A \neq B$	(proper subset)
$A \supset B$	$\Leftrightarrow$	$A \supseteq B \wedge A \neq B$	(proper superset)

Sets can be defined by enumerating its elements.

Example

$\{0, 1\}$	represents a set of two elements (0 and 1, in no particular order)
{red, blue, green}	represents a set of three elements (colors)
$\{1, 2, 3, \ldots\}$	represents an infinite set (of natural numbers)

Sets can also be defined using a characterizing property in set-builder notation.

$$\underset{\underset{\text{set}}{\uparrow}}{\{}\quad \overset{\overset{\text{expression}}{\downarrow}}{x} \quad \underset{\underset{\text{“such that”}}{\uparrow}}{\mid} \quad \overset{\overset{\text{characterizing property}}{\downarrow}}{P(x)} \quad \underset{\underset{\text{set}}{\uparrow}}{\}}$$

Example

$$\{x \mid x \text{ is a positive integer}\}$$
$$\{x \mid x \text{ is an integer} \wedge 3 < x \leq 7\}$$

Well-known sets:

$$\begin{aligned}
\mathbb{N} &= \{x \mid x \text{ is a natural number}\} \\
&= \{0, 1, 2, \ldots\} \qquad \text{(sometimes without } 0\text{)} \\
\\
\mathbb{Z} &= \{x \mid x \text{ is an integer}\} \\
&= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\
\\
\mathbb{Q} &= \{x \mid x \text{ is a rational number}\} \\
\\
\mathbb{R} &= \{x \mid x \text{ is a real number}\} \\
\\
\mathbb{C} &= \{x \mid x \text{ is a complex number}\}
\end{aligned}$$

The empty set, { }, is the set with no elements. Often, it is denoted $\varnothing$.

The powerset of a set S, denoted $\wp(S)$, is the set of all subsets of S.

Example Let $S = \{1, 2, 3\}$.

$$\wp(S) = \Big\{ \quad \varnothing, \quad \underbrace{\{1\}, \quad \{2\}, \quad \{3\}}_{\text{singletons}}, \quad \underbrace{\{1,2\}, \quad \{1,3\}, \quad \{2,3\}}_{\text{doubletons}}, \quad \{1,2,3\} \quad \Big\}$$

The cardinality of a set S, denoted $\|S\|$, is the numbers of elements in S.

Example

$$\begin{aligned}
\|\{1, 2, 3\}\| &= 3 \\
\|\varnothing\| &= 0 \\
\|\{1, 3\}\| &= 2 \\
\|\{\text{red}, \text{green}, \text{blue}\}\| &= 3
\end{aligned}$$

Operations on sets

$$\begin{aligned}
A \cup B &= \{x \mid x \in A \vee x \in B\} && \text{(union)} \\
A \cap B &= \{x \mid x \in A \wedge x \in B\} && \text{(intersection)} \\
A - B &= \{x \mid x \in A \wedge x \notin B\} && \text{(difference)} \\
A \times B &= \{(x, y) \mid x \in A \wedge y \in B\} && \text{(cross product)}
\end{aligned}$$

Two sets A, B are disjoint if $A \cap B = \varnothing$

Example Suppose $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Let $A = \{1, 3, 5, 7, 9\}$.
Let $B = \{2, 4, 6, 8, 10\}$.
Let $C = \{6, 1, 7, 3, 9\}$.
The following are true:

$$\begin{aligned} A \cup C &= \{1, 3, 5, 6, 7, 9\} \\ A \cap C &= \{1, 3, 7, 9\} \\ B \cup C &= U - \{5\} \\ B \cap C &= \{6\} \\ A \cap B &= \varnothing && \text{(A and B are disjoint)} \\ A \cup B &= U \end{aligned}$$

Set Identities

1. Commutativity

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

2. Associativity

$$(A \cup B) \cup C = A \cup (B \cup C)$$
$$(A \cap B) \cap C = A \cap (B \cap C)$$

3. Distributivity

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

4. Identity

$$A \cup \varnothing = A$$
$$A \cap U = A$$

5. Complement

$$A \cup A' = U$$
$$A \cap A' = \varnothing$$

where $A' = U - A$ and U is the universal set.

Example Prove that $A = B \leftrightarrow (A \subseteq B) \wedge (A \supseteq B)$.

Proof.

$$\begin{aligned}
& A = B \\
\leftrightarrow\quad & (\forall x)[x \in A \leftrightarrow x \in B] && \text{(by defn =)} \\
\leftrightarrow\quad & (\forall x)[x \in A \rightarrow x \in B \wedge x \in B \rightarrow x \in A] && \text{(by defn } \leftrightarrow\text{)} \\
\leftrightarrow\quad & (\forall x)[x \in A \rightarrow x \in B] \wedge (\forall x)[x \in B \rightarrow x \in A] && \text{(see page 12)} \\
\leftrightarrow\quad & (A \subseteq B) \wedge (A \supseteq B) && \text{(by defn } \subseteq, \supseteq\text{)}
\end{aligned}$$

□

Example Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof.

($\subseteq$) Consider an arbitrary member $x \in A \cup (B \cap C)$.

$$\begin{aligned}
x \in A \cup (B \cap C) & \rightarrow x \in A \vee x \in (B \cap C) && \text{(by defn } \cup\text{)} \\
& \rightarrow x \in A \vee (x \in B \wedge x \in C) && \text{(by defn } \cap\text{)} \\
& \rightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) && \text{(dist } \vee \text{ over } \wedge\text{)} \\
& \rightarrow x \in (A \cup B) \wedge x \in (A \cup C) && \text{(by defn } \cup\text{)} \\
& \rightarrow x \in (A \cup B) \cap (A \cup C) && \text{(by defn } \cap\text{)}
\end{aligned}$$

($\supseteq$) Symmetric.

□

Example Prove that $(A \subseteq B) \wedge (B \subseteq C) \rightarrow (A \subseteq C)$.

Proof. Suppose that $A \subseteq B$ and $B \subseteq C$ are both true. Keep in mind what this means:

$$\begin{aligned}
A \subseteq B \leftrightarrow (\forall x)[x \in A \rightarrow x \in B] && \text{(by defn)} \\
B \subseteq C \leftrightarrow (\forall x)[x \in B \rightarrow x \in C] && \text{(by defn)}
\end{aligned}$$

We want to show that $(A \subseteq C)$. I.e., that $(\forall x)[x \in A \rightarrow x \in C]$ must be true. Thus, fix any x (technically by universal instantiation) and assume $x \in A$. We show that $x \in C$ must be true.

Since $x \in A$ and $A \subseteq B$, $x \in B$ must be true. Since $x \in B$ and $B \subseteq C$, we know that $x \in C$ must be true, as required. □

4 Relations, Functions, and Matrices

4.1 Relations

An n-tuple is an ordered sequence of n objects. n-tuples are written by listing the n objects within parentheses separated by commas.

Example

2-tuples (a.k.a., ordered pairs):

- $(5,\ 3)$
- (apple, red)
- (Vondrak, Alex)

3-tuples (a.k.a., ordered triples):

- $(3,\ 6,\ -4)$
- (apple, red, green)
- (Olmos, Edward, James)

Let $S_1, S_2, \ldots, S_n$ be sets.

The n-ary product of $S_1, S_2, \ldots, S_n$, denoted

$$S_1 \times S_2 \times \ldots \times S_n$$

is defined by

$$S_1 \times S_2 \times \ldots \times S_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in S_1 \wedge x_2 \in S_2 \wedge \ldots \wedge x_n \in S_n\}$$

(Note that at $n = 2$, this is the same as the cross product.)

Example Let $X = \{1, 2\}$. Let $Y = \{3, 4\}$. Let $Z = \{5, 6\}$.

$$X \times Y = \{(1,3), (1,4), (2,3), (2,4)\}$$
$$X \times Y \times Z = \{(1,3,5), (1,3,6), (1,4,5), (1,4,6), (2,3,5), (2,3,6), (2,4,5), (2,4,6)\}$$

An n-ary relation is a subset of $S_1 \times S_2 \times \ldots \times S_n$.

n	Relation Type
1	unary or property
2	binary
3	ternary
4	quaternary

Example Let H = the set of humans (living or dead). $\textsc{parent} \subseteq H \times H$ is defined by

$$\textsc{parent} = \{(h_1, h_2) \mid h_1 \text{ is a parent of } h_2\}$$

Example Let F = the set of all foods, C = the set of all colors. $\textsc{Food\_Color} \subseteq F \times C$ is defined by

$$\textsc{Food\_Color} = \{(f, c) \mid f \text{ occurs in color } c\}$$

Example "$\leq$" $\subseteq \mathbb{N} \times \mathbb{N}$ is defined by

$$\text{“}\leq\text{”} = \{(x, y) \mid x \leq y\}$$

Properties of Binary Relations

Let R be a binary relation on set S (i.e., $R \subseteq S \times S$).
R is reflexive if $(\forall x \in S)[(x, x) \in R]$.
R is symmetric if $(\forall x, y \in S)[(x, y) \in R \rightarrow (y, x) \in R]$.
R is transitive if $(\forall x, y, z \in S)[(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R]$.
R is antisymmetric if $(\forall x, y \in S)[(x, y) \in R \wedge (y, x) \in R \rightarrow x = y]$.
R is 1-1 if $(\forall x_1, x_2, y \in S)[(x_1, y) \in R \wedge (x_2, y) \in R \rightarrow x_1 = x_2]$.
R is onto if $(\forall y \in S)(\exists x \in S)[(x, y) \in R]$.

R is an equivalence relation if R is reflexive, symmetric, and transitive.

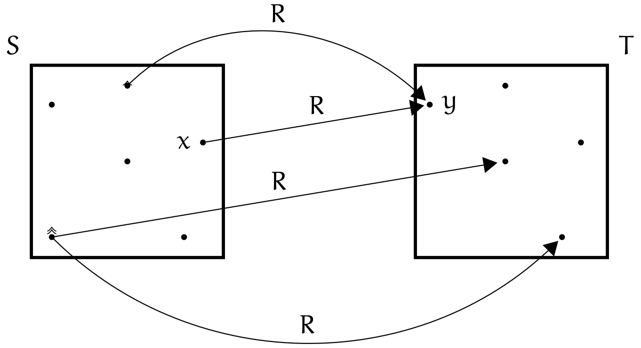
R is a partial ordering if R is reflexive, transitive, and anti-symmetric.

R is a total ordering if R is a partial ordering and $\underbrace{(\forall x, y \in S)[(x, y) \in R \vee (y, x) \in R]}_{\text{all elements are comparable}}$

The inverse (or reversal) of R, denoted R^{-1}, is defined by

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

Binary relations can be illustrates using Venn diagrams; e.g., $(x, y) \in R \subseteq S \times T$:



4.4 Functions

$f \subseteq S \times T$ is a function if f^{-1} is 1-1 and onto.

Note: $(x, y) \in f$ can be denoted $f(x) = y$.

Note: $f \subseteq S \times T$ can be denoted $f\colon S \to T$. S is called the domain and T is called the codomain.

The range of $f\colon S \to T$ is $\{f(x) \mid x \in S\}$.

3 Sets, Combinatorics, Probability, ...

3.1 Sets

Countable and Uncountable Sets

Let S and T be sets.

S and T are equipollent ($\|S\| = \|T\|$) if

$$(\exists f\colon S \to T)[f \text{ is 1-1} \wedge f \text{ is onto}]$$

S is denumerable if $\mathbb{N}$ and S are equipollent.

S is countable if

$$S \text{ is finite} \vee S \text{ is denumerable}$$

Theorem. *$\mathbb{Z}$ is countable.*

Proof. Let $f\colon \mathbb{N} \to \mathbb{Z}$ be defined by

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\[2ex] -\left\lceil \dfrac{n}{2} \right\rceil & \text{if } n \text{ is odd} \end{cases}$$

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
5	-3
6	3
$\vdots$	$\vdots$

f is 1-1 & onto $\qquad \therefore\ \mathbb{Z}$ is denumerable and thus countable □

Theorem. $S = \{x \mid x \in \mathbb{R} \land 0 \le x < 1\}$ *is uncountable.*

Proof by Contradiction. To the contrary, suppose S is countable. For S to be countable, it must be denumerable (since S is clearly infinite).

Thus, $(\exists f \colon \mathbb{N} \to S)[f \text{ is 1-1} \land f \text{ is onto}]$. So, we're assuming it's possible to write out the range of f in some order:

$$\begin{array}{llllll}
f(0) & = .d_{0,1} & d_{0,2} & d_{0,3} & d_{0,4} & \cdots \\
f(1) & = .d_{1,1} & d_{1,2} & d_{1,3} & d_{1,4} & \cdots \\
f(2) & = .d_{2,1} & d_{2,2} & d_{2,3} & d_{2,4} & \cdots \\
f(3) & = .d_{3,1} & d_{3,2} & d_{3,3} & d_{3,4} & \cdots \\
f(4) & = .d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & \ddots \\
\vdots & & & \vdots & &
\end{array}$$

Since f is onto, $(\forall y \in S)(\exists n \in \mathbb{N})[y = f(n)]$.

Since f is 1-1, there are no repeated numbers above—each "row" of digits is unique.

Consider constructing the following decimal number by diagonalization:

$$\begin{array}{llllll}
f(0) & = .\boxed{d_{0,1}} & d_{0,2} & d_{0,3} & d_{0,4} & \cdots \\
f(1) & = .d_{1,1} & \boxed{d_{1,2}} & d_{1,3} & d_{1,4} & \cdots \\
f(2) & = .d_{2,1} & d_{2,2} & \boxed{d_{2,3}} & d_{2,4} & \cdots \\
f(3) & = .d_{3,1} & d_{3,2} & d_{3,3} & \boxed{d_{3,4}} & \cdots \\
f(4) & = .d_{4,1} & d_{4,2} & d_{4,3} & d_{4,4} & \boxed{\ddots} \\
\vdots & & & \vdots & &
\end{array}$$

$y = 0.9999\ldots - 0.d_{0,1}d_{1,2}d_{2,3}d_{3,4}\ldots$ is guaranteed to not be listed above:

- Its first digit is $9 - d_{0,1}$, which is going to be different from $f(0)$'s first digit (which is $d_{0,1}$).
- Its second digit is $9 - d_{1,2}$, which is going to be different from $f(1)$'s second digit (which is $d_{1,2}$).
- Its third digit is $9 - d_{2,3}$, which is going to be different from $f(2)$'s third digit (which is $d_{2,3}$).
- And so on.

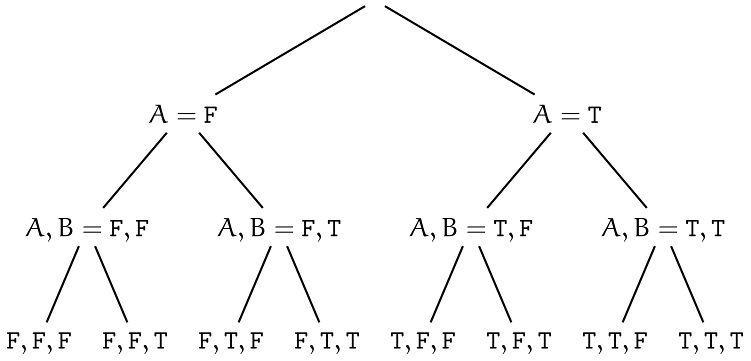
Since $0 \le y < 1$, $y \in S$.

However, $(\nexists n \in \mathbb{N})[y = f(n)]$, a contradiction. □

3.2 Counting

Combinatorics is the mathematics of counting—how many items are in a set? In how many ways can something occur? Etc.

Example How many rows are in a truth table with three variables (A, B, C)?



The multiplication principle states that if there are n_1 possible outcomes for event 1 and n_2 possible outcomes for event 2, there are $n_1 \cdot n_2$ possible outcomes for the sequence of the two events ("event 1 and event 2").

Example

Q: How many 3-bit binary numbers are there?

A: $\overbrace{2}^{\text{\# choices for 1st bit}} \times \overbrace{2}^{\text{\# choices for 2nd}} \times \overbrace{2}^{\text{\# choices for 3rd}} = 2^3 = 8$

Example

Q: How many outfits (shirts & pants) are possible if you have 3 shirts and 5 pairs of pants?

A: $3 \cdot 5 = 15$

The addition principle states that if the *disjoint* events A and B have n_1 and n_2 possible outcomes (respectively), then the event "A or B" has a total of $n_1 + n_2$ possible outcomes.

Example

Q: A dealer sells 23 different cars and 14 different trucks. How many selections does a customer have?

A: $23 + 14 = 37$

Example

Q: Someone has 7 blouses, 5 skirts, and 9 dresses. How many outfits are possible?

A: An outfit consists of either a blouse & a skirt *or* just a dress. The number of outfits consisting of a blouse & a skirt is $7 \cdot 5 = 35$. The number of outfits consisting of just a dress is 9. Thus, there are $35 + 9 = 44$ possible outfits.

3.3 Principle of Inclusion and Exclusion; Pigeonhole Principle

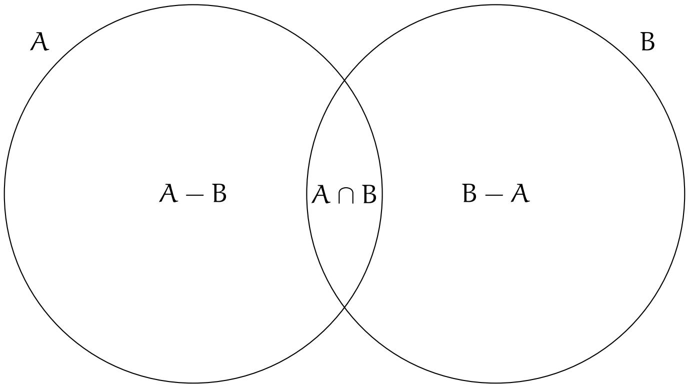
Principle of Inclusion and Exclusion

Given the finite sets A and B,

$$\|A \cup B\| = \|A\| + \|B\| - \|A \cap B\|$$

Proof. First, notice that if X and Y are any two disjoint sets, then $\|X \uplus Y\| = \|X\| + \|Y\|$ by the addition princple (where $\uplus$ is "disjoint union"). Also, it's clear that for any sets X and Y (disjoint or otherwise), $\|X - Y\| = \|X\| - \|X \cap Y\|$.

Further, if A and B are any subsets of a universal set U, then $A - B$, $B - A$, and $A \cap B$ are mutually disjoint sets.



Note that $A \cup B = (A - B) \uplus (A \cap B) \uplus (B - A)$. Then,

$$\begin{aligned}
\|(A \cup B)\| &= \|(A - B) \uplus (A \cap B) \uplus (B - A)\| \\
&= \|A - B\| + \|A \cap B\| + \|B - A\| && \text{(addition principle)} \\
&= \|A\| - \|A \cap B\| + \|A \cap B\| + \|B\| - \|B \cap A\| \\
&= \|A\| - \|A \cap B\| + \|A \cap B\| + \|B\| - \|A \cap B\| && \text{(commutativity)} \\
&= \|A\| + \|B\| - \|A \cap B\|
\end{aligned}$$

Intuitively, $\|A\|+\|B\|$ "double counts" the elements of $\|A\cap B\|$, so we subtract off the error—we *include* the number of elements in A and the number of elements in B, but we *exclude* the element of $A \cap B$ to avoid counting them twice. □

Example

Q: A total of 35 voters cast their votes (support/oppose) for two different referendums. 14 voters supported referendum A and 26 supported referendum B. How many voters supported both referendums A and B? How many supported only referendum A? How many supported only referendum B?

A: We're given the following information

$$\begin{aligned} \|A \cup B\| &= 35 \\ \|A\| &= 14 \\ \|B\| &= 26 \end{aligned}$$

We're asked for $\|A \cap B\|$, $\|A - B\|$, and $\|B - A\|$. We can use the principle of inclusion and exclusion to answer the first one:

$$\begin{aligned} \|A \cup B\| &= \|A\| + \|B\| - \|A \cap B\| \\ 35 &= 14 + 26 - \|A \cap B\| \\ -5 &= -\|A \cap B\| \\ \|A \cap B\| &= 5 \end{aligned}$$

The others can be solved with this new piece of data:

$$\begin{aligned} \|A - B\| &= \|A\| - \|A \cap B\| = 14 - 5 = 9 \\ \|B - A\| &= \|B\| - \|B \cap A\| = 26 - 5 = 21 \end{aligned}$$

Pigeonhole Principle

Imagine a series of cubbyholes in which we stuff pigeons (which I guess we raise and domesticate for our own odd amusement). Suppose there are k such pigeonholes. If we try to cram any more than k pigeons into the pigeonholes, at least one hole will contain more than 1 pigeon—no matter how hard we try.

Example

Q: A disorderly person doesn't roll their socks into pairs. They just have a drawer full of random socks—either white or black. How many socks must they pull blindly from the drawer to guarantee that they will have a matched pair?

A: Here, the pigeonholes = sock colors (either white or black), and the pigeons = socks.

- If we grab one sock, we don't have a pair.
- If we grab two socks, they might be mismatched.
- If we grab three socks, then we've overstuffed the pigeonholes: we'll have at least one duplicate color, and thus a matched pair.

Example

Q: How many people must be in a room to guarantee that two people have last names that begin with the same letter?

A: Here, the pigeonholes = letters (26 possibilities in English), and the pigeons = people. So, if there are 27 people, the pigeonhole principle guarantees that there will be at least one pigeonhole (letter) with two pigeons (two people).

3.4 Permutations and Combinations

A permutation is an ordered arrangement of objects.

The number of permutations of r distinct objects chosen from n distinct objects is denoted $P(n, r)$ (oftentimes ${}_nP_r$).

Theorem. $P(n, r) = \dfrac{n!}{(n-r)!}$

Proof. Consider selecting the r distinct objects one-by-one from the n distinct objects. Since the n objects are themselves distinct, note that there will be *no repeats* in our choices for each of the r items.

Then, by the multiplication principle, the total number of permutations possible is

$$\underbrace{n}_{\#\text{ choices for 1st item}} \times \underbrace{(n-1)}_{\#\text{ choices for 2nd item}} \times \underbrace{(n-2)}_{\#\text{ choices for 3rd item}} \times \cdots \times \underbrace{(n-(r-1))}_{\#\text{ choices for } r\text{th item}}$$

By definition of factorial, $n! = n \times (n-1) \times (n-2) \times (n-3) \times \cdots \times 3 \times 2 \times 1$. Thus,

$$\begin{aligned}
\frac{n!}{(n-r)!} &= \frac{n \times (n-1) \times \cdots \times (n-(r-1)) \times (n-r) \times (n-r-1) \times \cdots \times 3 \times 2 \times 1}{(n-r)(n-r-1)(n-r-2)\cdots \times 3 \times 2 \times 1} \\
&= \frac{n \times (n-1) \times \cdots \times (n-(r-1)) \times \cancel{(n-r)} \times \cancel{(n-r-1)} \times \cdots \times \cancel{3} \times \cancel{2} \times \cancel{1}}{\cancel{(n-r)}\cancel{(n-r-1)}\cancel{(n-r-2)}\cdots \times \cancel{3} \times \cancel{2} \times \cancel{1}} \\
&= n \times (n-1) \times \cdots \times (n-(r-1))
\end{aligned}$$

□

Example

Q: How many possible 7-digit phone numbers are there without any repeated digits?

A: $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 = 604,800$. That is,

$$\begin{aligned} P(10,7) &= \frac{10!}{(10-7)!} \\ &= \frac{10!}{3!} \\ &= \frac{10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}{3 \times 2 \times 1} \\ &= 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \\ &= 604,800 \end{aligned}$$

Sometimes we want to select r objects from a set of n, but we don't care how they are arranged. This is the number of combinations of r distinct objects chosen from n distinct objects, and is denoted by any of

$$C(n,r) \qquad {}_nC_r \qquad C^n_r \qquad \binom{n}{r}$$

Theorem. $C(n,r) = \dfrac{P(n,r)}{r!}$

Proof. Select r distinct *unordered* objects from a set of n distinct objects. There are $C(n,r)$ ways to do this. Now, take each of the r objects and place them in some order:

$$\underbrace{\text{item 1}}_{r \text{ choices}}, \quad \underbrace{\text{item 2}}_{r-1 \text{ choices}}, \quad \underbrace{\text{item 3}}_{r-2 \text{ choices}}, \ldots, \underbrace{\text{item } r}_{1 \text{ choice}}$$

By the multiplication principle, there are $r \times (r-1) \times (r-2) \times \cdots \times 3 \times 2 \times 1 = r!$ ways to select an ordering of the combination. So there are $C(n,r) \cdot r!$ ways to select any ordered subset of r distinct objects from n distinct objects.

That is, $C(n,r) \cdot r! = P(n,r)$, so $C(n,r) = \dfrac{P(n,r)}{r!}$. □

Example

Q: How many 5-card poker hands can be dealt from a 52-card deck?

A: Here, order doesn't matter (just that we have certain cards in hand). So, we're interested in the number of combinations:

$$\begin{aligned} C(52,5) &= \frac{P(52,5)}{5!} \\ &= \frac{\frac{52!}{(52-5)!}}{5!} \\ &= \frac{52!}{47! \cdot 5!} \\ &= 2,598,960 \end{aligned}$$