Data Types

Monday, January 4, 2021 4:03 PM

n-tuple: ordered sequence of elements with n elements

Equal means corresponding elements are equal

set: unordered collection of elements

Equal mean agreement on membership of all elements

a set with no elements is the empty set $\emptyset$

String: ordered finite sequence of elements each from a speified set

Equal means length and corresponding elements are equal.

a string with length of 0 is the empty string λ

Sets

Wednesday, January 6, 2021 4:14 PM

$\{-1, 1\}$ $\{0, 0\}$ $\{-1, 0, 1\}$ $\mathbb{Z}$

$\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$ $\emptyset$ $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x > 0\}$

roster method: $\{ , , , , , \}$

set builder: $\mathbb{K} = \{ \_\_\_\_ \mid \text{property} \}$ or $\mathbb{N}$ $\mathbb{Z}$ $\emptyset$

empty set in roster method: $\{\}$

"|" = such that, ":" is also used.

setwise concatenation:

"$\circ$" $S \circ G$ concatenates G to the end of S.

cartesian multiplication of sets:

$\{0, 1, -1\} \times \{A \;\; B \;\; C\}$ is a set that includes:

$(0, A)$		$(A, 0)$
$(-1\ B)$	but not	$(B, -1)$
$(0, C)$		$(C, 0)$

etc.

String Concatenation

Wednesday, January 6, 2021 4:33 PM

$$\underbrace{(\text{String } S) \circ (\text{String } b) \Rightarrow S \circ b}_{\text{string concatenation}}$$

Recursive Set Definition

Wednesday, January 6, 2021 4:28 PM

The set S is defined by:

Basis step: Specify finitely many elements of S

Recursive step: Give a rule for creating a new element of S from known values existing in S

The set of RNA strands S is defined is defined by:

basis step:

$A \in S$, $C \in S$, $U \in S$, $G \in S$

recursive step: If $s \in S$ and $b \in B$ then $sb \in S$

The set of linked lists of natural numbers L is defined by:

Basis step $[\,] \in L$

If $l \in L$ and $n \in \mathbb{N}$, then $(n, l) \in L$

Functions

Monday, January 4, 2021 4:38 PM

Definition:

$f(x) = x + 4$ $\quad\quad$ $d((x_1, x_2, x_3), (y_1, y_2, y_3))$

Application:

$f(7)$ $\quad\quad$ $d(P_1, P_2)$

$f(z)$ $\quad\quad$ $d((1, 0, -1), (-1, -1, 1))$

Properties:

1. Domain set of inputs
2. Codomain set of (possible) outputs
3. Rule assigning each element of the domain to exactly one element in the codomain

Notation:

f: domain $\longrightarrow$ codomain

Bases and Conversion

Monday, January 11, 2021 4:15 PM

Representing Bases

$(128)_{10}$

$(CAF)_{16}$

in memory: $(1011)_{2,4}$ ← width

etc.

Converting Bases.

Given an input n in base b_1

1) Use definition of base expansion to express input as decimal

2) Use some algorithm to convert decimal to base b_2

the width of the expansion must follow $n < b^w$

$a_0 = n \bmod b \qquad q = n \operatorname{div} 2$

$a_1 = q \bmod b \qquad q = q \operatorname{div} 2 \ldots$

so $\quad base(n, b) = base(n \operatorname{div} 2, b) \circ n \bmod b$

Fractional Numbers in Different Bases

Monday, January 11, 2021 4:25 PM

Fractional Numbers In Bases

$$(\underset{2^3}{\_}\ \underset{2^2}{\_}\ \underset{2^1}{\_}\ \underset{2^0}{\_}\ .\ \underset{2^{-1}}{\_}\ \underset{2^{-2}}{\_}\ \underset{2^{-3}}{\_}\ \underset{2^{-4}}{\_}\ \ldots\ \underset{2^{-n}}{\_})$$

radix point

thus

$$a_n b^n + a_{n-1} b^{n-1} \ldots a_1 b^1 + a_0 b^0 + a_{-1} b^{-1} + a_{-2} b^{-2} \ldots + a_m b^m$$

is a close approximation of x.

Representing Signed Integers

Wednesday, January 13, 2021 4:39 PM

Signed Representation

1st bit represents + (0) or − (1)

$[(0,1)\ a_1\ a_2 \ldots a_n]_{s,w}$

2's complement

1st bit represents + (0) or − (1). Remaining bits are modified according to the rule:

If the number is negative, flip each bit from 0 <-> 1. Add 1 to the remaining.

$$[\underbrace{1}_{(-)}\ \underbrace{01011}]_{s,6}$$

$$\downarrow$$

01011

flip = 10100

$$\begin{array}{r} 10100 \\ +\quad\ 1 \\ \hline 10101 \end{array}$$

2's complement: $[1\ 10101]_{2c,6}$

Logic Circuits

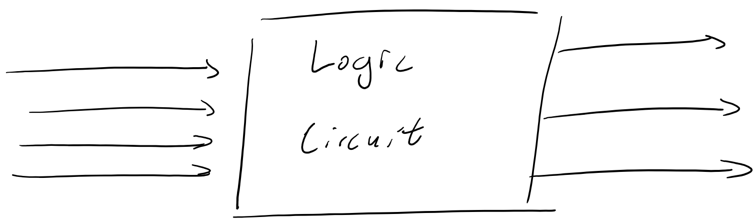
Friday, January 15, 2021 4:04 PM

Inputs

coefficients in fixed width binary

Outputs

coefficients in fixed width binary



Logic Gates

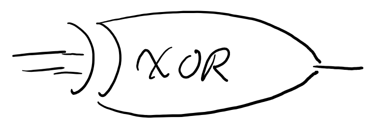
Friday, January 15, 2021 4:05 PM

AND

Input		Output
1	1	1
1	0	0
0	1	0
0	0	0

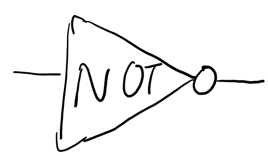
XOR

Input		Output
1	1	0
1	0	1
0	1	1
0	0	1



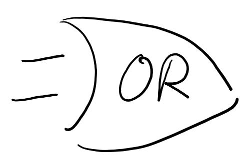
Not

Input	Output
1	0
0	1



OR

Input		Output
1	1	1
0	1	1
1	0	1

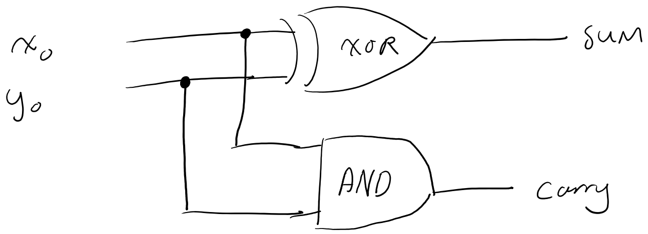


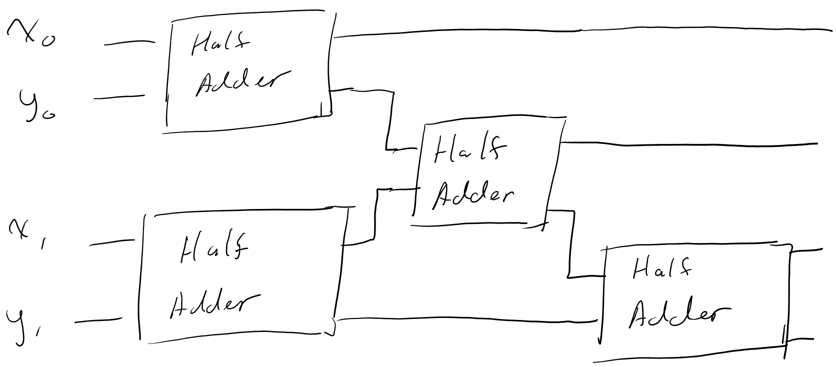
10 1

00 0

Half Adder & Full Adders

Friday, January 15, 2021 4:42 PM





$Z_0 = x_0 \oplus y_0$

$Z_1 = (x_1 \oplus y_1) \oplus [(x_1 \oplus y_1) \oplus (x_1 \wedge y_1)]$

$Z_2 =$

Overflow

Propositional Statements

Wednesday, January 20, 2021 3:54 PM

Definitions

Proposition: Declarative sentence that is T or F

Propositional variable: variables that represent propositions

Compound proposition: new propositions formed from existing propositions using logical operators

Truth table: table showing relationships between inputs and outputs

Operators

p and q $p \wedge q$

p xor q $p \oplus q$

p or q $p \vee q$

not p $\neg p$

Tautology and Contradiction

Wednesday, January 20, 2021 4:21 PM

Tautology

Compound propositions that evaluates to true for all setting of truth values to its propositional variables; abreviated T.

Contradiction

Compound propositions that evaluates to false for all settings of truth values to its propositional variables; abreviated F.

Consistent

A collection of compound propositions is consistent if there is an assignment of truth values to the propositional variables that makes each of the compound propositions true.

Logical Equivalence

Wednesday, January 20, 2021 4:25 PM

Def

Two compound propositions are logically equivalent if their truth tables are the same. All inputs map to the same outputs.

Notation

proposition is equivalent to proposition

use $\equiv$ symbol

Examples

Commutativity	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Associativity	$(p \vee q) \vee r = p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Absorbtion	$p \vee T = T$ $p \vee F = p$	$p \wedge T = T$ $p \wedge F = F$
DeMorgan	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$

DNF, CNF

Wednesday, January 20, 2021 4:40 PM

DNF: Disjunctive normal form: OR of ANDs

an OR of ANDs of variables and their negations

Selects inputs that outputs T

CNF: Conjunctive normal form: AND of ORs:

an AND of ORs of variables and their negations

Selects inputs that output F

Conditional and Biconditional Statements

Friday, January 22, 2021 4:04 PM

Conditional

The <u>hypothesis</u> of $p \to q$ is p } same

The <u>antecedent</u> of $p \to q$ is p

The <u>conclusion</u> of $p \to q$ is q } same

The <u>consequent</u> of $p \to q$ is q

The <u>converse</u> of $p \to q$ is $q \to p$

The <u>inverse</u> of $p \to q$ is $\neg p \to \neg p$

The <u>contrapositive</u> of $p \to q$ is $\neg q \to \neg p$

Input		Output
p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

"If p then q"

"p guarantees q"

$$p \to q \not\equiv q \to p \qquad p \to q \not\equiv \neg p \to \neg q \qquad p \to q \equiv \neg q \to \neg p$$

Biconditional

$$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$$
$$\equiv \neg(p \oplus q)$$
$$\equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$

Input		Output
p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

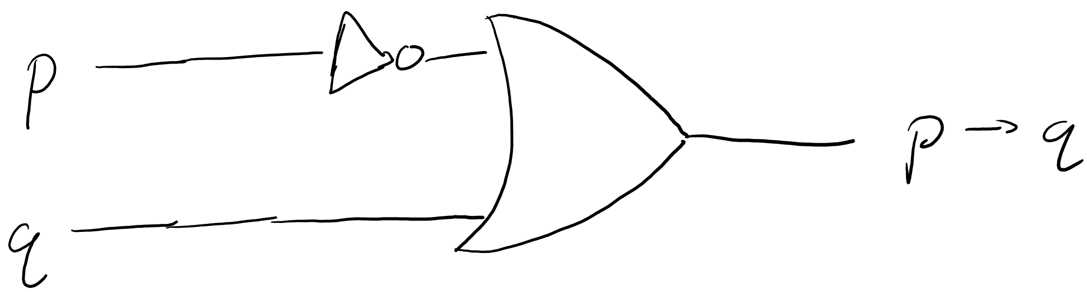
"p iff q"

"p if and only if q"

Conditional as Boolean

Friday, January 22, 2021 4:46 PM

$p \rightarrow q$ as a circuit:



as a statement:

$$p \rightarrow q \equiv \neg p \vee q$$

Predicates

Wednesday, January 27, 2021 4:08 PM

A predicate is a function from a given domain to $\{T, F\}$
It can be applied, or evaluated at, an element of the domain

Predicates as tables
It can be specified by its input-output definition table.

Predicates as functions
It can be specified by specifying the rule.
ie. $P(x)$ is T if $[x]_{2c,3} > 0$
To disprove a description, one counter example is required.

Predicates as truth sets
Specified by its truth set, which are the elements of the domain at which the predicate evaluates to T

Universal and Existential Qualifications

Wednesday, January 27, 2021 4:20 PM

We can makes claims about a set by saying which or how many of its elements satisfy a property. These claims are called quantified statements and use predicates

The universal qualification of $P(x)$ is the statement "$P(x)$ for all vallues of x in the domain" and is written $\forall x P(x)$

The existential qualification of $P(x)$ is the statement "There exists an element x such that $P(x)$" and is written $\exists x P(x)$

Counterexamples and Witnesses

Wednesday, January 27, 2021 4:24 PM

Counterexample: An element for which $P(x)$ is false

Witness : An element for which $P(x)$ is true

Quantifier DeMorgan

Wednesday, January 27, 2021 4:29 PM

Quantifier version of DeMorgan's Laws

$$\neg \forall x\, P(x) \equiv \exists x\, (\neg P(x)) \qquad \neg E x\, Q(x) \equiv \forall x\, (\neg Q(x))$$

not all elements made $P(x)$ true, therefore there was at least one element that made $P(x)$ false

not one element made $P(x)$ true, therefore all elements made $P(x)$ false.

Proof Strategies

Friday, February 5, 2021 4:04 PM

To prove $\forall x\, P(x)$ is true, use exhaustion or universal generalization

To prove $\forall x\, P(x)$ is false, use a counter example

To prove $\exists x\, P(x)$ is true, use a witness

To prove $\exists x\, P(x)$ is false, use demorgan's law to rewrite statement and prove using universal generalizations.

Cartesian Products

Friday, January 29, 2021 4:09 PM

Let A and B be sets. The Cartesian Product of A and B, denoted $A \times B$ is the set of all ordered pairs (a,b) where $a \in A$ and $b \in B$. Hence:

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

Common Sets

Monday, February 1, 2021 4:13 PM

$\mathbb{N}$	The set of all natural numbers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	The set of integers	$\{\ldots, -2, 1, 0, 1, 2, \ldots\}$
$\mathbb{Z}^+$	The set of positive integers	$\{1, 2, 3 \ldots\}$
$\mathbb{Z}^{\neq 0}$	The set of nonzero integers	$\{\ldots, -2, -1, 1, 2, \ldots\}$

Set Notation

Friday, February 5, 2021 4:08 PM

A set is an unordered collection of elements

Set equality: $A = B$ means $\forall x (x \in A \leftrightarrow x \in B)$

Subset: $A \subseteq B$ means $\forall x (x \in A \rightarrow x \in B)$

Proper subset: $A \subsetneq B$ means $(A \subseteq B) \wedge (A \neq B$

Set Operations

Friday, February 5, 2021 4:35 PM

Cartesian Product: $A \times B = \{ (a, b) \mid a \in A \wedge b \in B \}$

Union: $A \cup B = \{ x \mid x \in A \vee x \in B \}$

Intersection: $A \cap B = \{ x \mid x \in A \wedge x \in B \}$

Difference: A

Types of Induction

Friday, February 12, 2021 4:02 PM

__Structural Induction__: Used to prove universal statements with recursively defined sets

__Mathematical Induction__: Used to prove universal statements with the domain $\mathbb{N}$.

Terminology

Friday, February 12, 2021 4:08 PM

Invariant: A property that is true about our algorithm no matter what

Theorem: Statement that can be shown to be true

Lemma: A step we use to prove the theorem.

Structural Induction Principles

Monday, February 8, 2021 4:02 PM

To prove a universal qualification over a recursively defined set: Use Structural Induction.

Basis Step: Show that the statement holds for elements specified in the basis step of the definition

Recursive Step: Show that the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

Mathematical Induction

Friday, February 12, 2021 4:04 PM

To prove a universal quantification over the set of all integers greater than or equal to some base b:

<u>Basis step</u>: Show the statement holds for b.

<u>Recursive step</u>: Consider an arbitrary integer $n > b$, assume (as the <u>induction hypothesis</u>) that the property holds true for n, prove that the property hold true for $n+1$.

Logically: Basis Step $Q(0)$

Recursive Step $\forall n \in \mathbb{N} \, (Q(n) \rightarrow Q(n+1))$

Strong Induction

Wednesday, February 17, 2021 4:44 PM

To prove a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed non negative integer j and then:

Basis step: Show the statement holds for $b, b+1 \ldots b+j$.

Recursive step: Consider an arbitrary integer $n \geq b+j$, assume as the <u>strong induction hypothesis</u> that the property holds for each of $b, b+1 \ldots n$ and use this and other facts to prove that the property holds for $n+1$.

Proof by Contradiction

Friday, February 19, 2021 4:04 PM

To prove that a statement p is true, pick anothe statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

Informally: The statement p can't be false because it creates a contradiction, therefore it must be true.

Sizes of Sets

Monday, February 22, 2021 4:05 PM

Key idea: use functions (with special properties) to relate the sizes of sets.

One-to-on, Onto, Bijection

Monday, February 22, 2021 4:12 PM

Def Let D and C be non empty sets. A function $f: D \to C$ is an assignment of one element of C to each element of D

Def A function $f: D \to C$ is one-to-one means for every a, b in the domain if $f(a) = f(b)$ then $a = b$

$$\forall a, b \in D \ (f(a) = f(b) \to a = b)$$

Def A function $f: D \to C$ is onto means for every b in the codomain and some a in the domain such that $f(a) = f(b)$.

$$\forall b \in C \ \exists a \in D \ (f(a) = f(b))$$

Def A function $f: D \to C$ is a bijection means it is one-to-one and onto. The inverse of a bijection $f: D \to C$ is the function $g: D \to C$ such that $g(b) = a$ iff $f(a) = b$

Cardinality

Monday, February 22, 2021 4:29 PM

<u>Def</u> For sets A, B we say that the cardinality of A is no bigger than the cardinality of B, we write $|A| \leq |B|$, to mean there is a one-to-one function with domain A and codomain B.

<u>Def</u> For sets A, B we say that the cardinality of A is no smaller than the cardinality of B, we write $|A| \geq |B|$, to mean there is an onto function with domain A and codomain B.

<u>Def</u> For sets A, B we say that the cardinality of A is equal to the cardinality of B, we write $|A| = |B|$, to mean there is a bijection with domain A and codomain B.

Properties of Cardinality

Monday, February 22, 2021 4:41 PM

$\forall A\ (|A| = |A|)$

$\forall A\ \forall B\ (|A| = |B| \rightarrow |B| = |A|)$

$\forall A\ \forall B\ \forall C\ |A| = |B| \wedge |B| = |C| \rightarrow |A| = |C|)$

Edge Case: for $\emptyset$, $|\emptyset| = 0$, $|\emptyset| \leq |x|$ for all sets x

Cantor-Schroder-Bernstein Theorem

Monday, February 22, 2021 4:42 PM

To prove $|A| = |B|$ we can do the following:

- there exists a bijection $f : A \to B$
- there exists a bijection $f : B \to A$
- there exists 2 functions $f_1 : A \to B$, $f_2 : B \to A$ that are both one-to-one
- there exists 2 functions $f_1 : A \to B$, $f_2 : B \to A$ that are both onto.

Countable Sets

Wednesday, February 24, 2021 4:05 PM

Finite Sets: Sets who's cardinality can be counted by a natural number.

Countably Infinite: A set A is contably infinite means it has the same size of $\mathbb{N}$

Example : $\mathbb{N}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$, $\mathbb{Z}$

RNA Strand, Linked List

<u>Countable Sets</u>: A set is countable if it is finite or countably infinite

Uncountable Sets

Friday, February 26, 2021 4:05 PM

The powerset operation takes an input set and outputs a larger set. What happens when we do $P(\mathbb{N})$?

Uncountable: means it is uncountable, there does not exist a bijection from $\mathbb{N}$ to the set.

Example: $P(\mathbb{N})$, $\mathbb{R}$

Proof: There is no witness that proves $|P(\mathbb{N})| = |\mathbb{N}|$

Binary Relation

Monday, March 1, 2021 4:07 PM

Def A binary relation from A to B is a subset of $A \times B$

Modulus as Binary Relation, Congruence

Monday, March 1, 2021 4:13 PM

Def Let $R_{(\text{mod } n)}$ be the set of all pairs of integers (a, b) such that $(a \bmod n = b \bmod n)$

We say that a is congruent to b mod n means $(a,b) \in R_{(\text{mod } n)}$. A common way to write this is

$a \equiv b \pmod{n}$

Properties of Relations

Monday, March 1, 2021 4:14 PM

__Def__ A relation R on a set A is called __reflexive__ if:
$(a,a) \in R$ for all $a \in A$

__Def__ A relation R on a set A is called __symetric__ if:
whenever $(a,b) \in R$ then $(b,a) \in R$ for all $a,b \in A$

__Def__ A relation R on a set A is called __transitive__ if:
$(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$ for all $a,b,c \in A$

__Def__ A relation is an __equivalence relation__ if it is reflexive, symetric, transitive.

__Def__ An __equivalence class__ of an element $a \in A$ for an equivalence relation R on the set A is the set $\{ s \in A \mid (a,s) \in R \}$ and is written $[a]_R$

__Def__ A relation R on sets A, B is called __antisymetric__ if $\forall a \in A \ \forall b \in B \ ((a,b) \in R \land (b,a) \in R \rightarrow a = b)$

Graphical Representation

Monday, March 1, 2021 4:38 PM

For relation R on a set A then we can represent this relation as a <u>graph</u>

Nodes: elements of A

Edges: directed edge from a to b when $(a,b) \in R$

Partial Orders, Hasse Diagram

Friday, March 5, 2021 4:42 PM

Def A relation is a partial ordering if it is reflexive, antisymetric, transitive.

Def A Hasse diagram on a partial ordering is the graph whose nodes are elements of the domain and such that the edges are undirected, and omits self loops and loops guaranteed by transitivity.

Partitions

Wednesday, March 3, 2021 4:23 PM

<u>Def</u> A <u>partition</u> of a set A is a set of non-empty, disjoint subsets $A_1 \dots A_n$ such that $A_1 \cup \dots \cup A_n = A$

<u>Example</u> We can partition the set of integers using equivalence of classes $R_{(\text{mod } 4)}$:

If $[n]_R = [n]_{R(\text{mod } 4)}$

$\mathbb{Z} = [0]_R \cup [1]_R \cup [2]_R \cup [3]_R$

Relation that is Symmetric and Anti-symmetric

Wednesday, March 10, 2021 4:51 PM

Claim: There is a relation that is both symmetric and antisymmetric.

For example, $A = \{1, 2, 3\}$ $R = \{(1,1), (2,2), (3,3)\}$