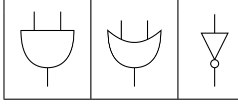
Dave Tompkins's Awesome CPSC 121 Handout. Version 7 (2013.01.22)

and	or	not
$\wedge$	$\vee$	$\sim$
		$\neg$



p	q	$p \wedge q$	$p \vee q$	$\sim p$	$p \oplus q$
T	T	T	T	F	F
T	F	F	T	F	T
F	T	F	T	T	T
F	F	F	F	T	F

Logical Equivalence ($\equiv$) Laws: *(and accepted [SHORT] name)*

Commutative: [COM]	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative: [ASS]	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive: [DIST]	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity: [I]	$p \wedge T \equiv p$	$p \vee F \equiv p$
Negation: [NEG]	$p \vee (\sim p) \equiv T$	$p \wedge (\sim p) \equiv F$
Double Negation: [DNEG]	$\sim(\sim p) \equiv p$	
Idempotent: [ID]	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound: [UB]	$p \vee T \equiv T$	$p \wedge F \equiv F$
De Morgan's: [DM]	$\sim(p \wedge q) \equiv (\sim p) \vee (\sim q)$	$\sim(p \vee q) \equiv (\sim p) \wedge (\sim q)$
Absorption: [ABS]	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negations of T and F: [NTF]	$\sim T \equiv F$	$\sim F \equiv T$

Prove $P \equiv Q$:	LHS	$\equiv P$	
		$\equiv$ ...	(Equivalence Law)
		$\equiv Q$	(Equivalence Law)
		$\equiv$ RHS	
		$\therefore\ P \equiv Q$	

Implication: [IMP]

$p \rightarrow q \equiv \sim p \vee q$	if p then q	p implies q	p is sufficient for q	q is necessary for p

contrapositive: $\sim q \rightarrow \sim p \equiv p \rightarrow q$	*converse:* $q \rightarrow p \not\equiv p \rightarrow q$	*inverse:* $\sim p \rightarrow \sim q \not\equiv p \rightarrow q$

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \equiv \sim(p \oplus q)$	p if and only if q	p is sufficient and necessary for q

Exclusive Or [XOR]:

$p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$	$p \oplus q \equiv (p \wedge \sim q) \vee (\sim p \wedge q)$

Multiplexer [MUX]:

s is a when c is false, b when c is true	$s \equiv (a \wedge \sim c) \vee (b \wedge c)$

Powers of 2:

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}
1	2	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,768	65,536

Binary Representation:

x_3	x_2	x_1	x_0	HEX	unsigned	signed
0	0	0	0	0	0	0
0	0	0	1	1	1	1
0	0	1	0	2	2	2
0	0	1	1	3	3	3
0	1	0	0	4	4	4
0	1	0	1	5	5	5
0	1	1	0	6	6	6
0	1	1	1	7	7	7

x_3	x_2	x_1	x_0	HEX	unsigned	signed
1	0	0	0	8	8	-8
1	0	0	1	9	9	-7
1	0	1	0	A	10	-6
1	0	1	1	B	11	-5
1	1	0	0	C	12	-4
1	1	0	1	D	13	-3
1	1	1	0	E	14	-2
1	1	1	1	F	15	-1

Arguments:

Premises:	w x y	The argument is *valid* iff: $[w \land x \land y] \to z$ is a *tautology*
Conclusion:	$\therefore\ z$	

Rules of Inference:

Modus Ponens: [M.PON]	$p \to q$ p $\therefore\ q$	Modus Tollens: [M.TOL]	$p \to q$ $\sim q$ $\therefore \sim p$
Generalization: [GEN]	p $\therefore\ p \lor q$	Specialization: [SPEC]	$p \land q$ $\therefore\ p$
Conjunction: [CONJ]	p q $\therefore\ p \land q$	Elimination: [ELIM]	$p \lor q$ $\sim q$ $\therefore\ p$
Transitivity: [TRANS]	$p \to q$ $q \to r$ $\therefore\ p \to r$	Proof by cases: [CASE]	$p \to r$ $q \to r$ $\therefore\ (p \lor q) \to r$
Resolution: [RES]	$p \lor q$ $\sim p \lor r$ $\therefore\ (q \lor r)$		

Alternate Implication ($\to$) Forms:

Generalization: [GEN$\to$]	p $\therefore \sim p \to q$	p $\therefore\ q \to p$	Resolution: [RES$\to$]	$p \to q$ $\sim p \to r$ $\therefore\ (q \lor r)$

Domains:

$\mathbb{Z}$	Integers	$\{\ldots, -1, 0, 1, +2, \ldots\}$	$\mathbb{N}_0$	Natural Numbers	$\{0, 1, 2, \ldots\}$
$\mathbb{Q}$	Rational Numbers	$\{\ldots, \frac{-1}{3}, 0, \frac{1}{2}, 1, \ldots\}$	$\mathbb{Z}^+$	Positive Integers	$\{x \in \mathbb{Z} \mid x > 0\}$
$\mathbb{R}$	Real Numbers	$\{\ldots, \frac{-1}{2}, 0, \sqrt{2}, \pi, \ldots\}$	$\overline{\mathbb{Q}}$	Irrational	$\{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$

Quantifiers:

$\forall x \in \mathbb{U}, P(x)$	$P(x)$ is true for *all* (every) x in $\mathbb{U}$	$\sim \forall x \in D, P(x) \equiv \exists x \in D, \sim P(x)$
$\exists x \in \mathbb{U}, P(x)$	$P(x)$ is true for *at least one* x in $\mathbb{U}$	$\sim \exists x \in D, P(x) \equiv \forall x \in D, \sim P(x)$

Equivalent Domain Representation:

$D = \{x \in \mathbb{U} \mid P(x)\}$
$\forall x \in D, Q(x) \equiv \forall x \in \mathbb{U}, P(x) \to Q(x)$ $\exists x \in D, Q(x) \equiv \exists x \in \mathbb{U}, P(x) \land Q(x)$

Handy Predicates:

Even(x) $\Leftrightarrow \exists k \in \mathbb{Z}, x = 2k$	$x \in \mathbb{Q} \Leftrightarrow \exists a, b \in \mathbb{Z}, (x = \frac{a}{b}) \land (b \neq 0)$
Odd(x) $\Leftrightarrow \exists k \in \mathbb{Z}, x = 2k + 1$	Prime(x) $\Leftrightarrow \forall k, m \in \mathbb{Z}, (x = km) \to [(m = x) \lor (m = 1)]$

Divisibility:

$a \mid b \ \Leftrightarrow\ a$ divides b	b is divisible by a	b is a multiple of a	$b/a \in \mathbb{Z}$ (or $a = b = 0$)	$\exists k \in \mathbb{Z}, b = ak$

Proof Methods:

Universal Modus Ponens:	$\forall x, P(x) \to Q(x)$ $P(a)$ ——— $\therefore\ Q(a)$	Universal Modus Tollens:	$\forall x, P(x) \to Q(x)$ $\sim Q(a)$ ——— $\therefore \sim P(a)$
Direct Proof (Existential):	$a \in D$ $P(a)$ ——— $\therefore\ \exists x \in D, P(x)$	Direct Proof (Counterexample):	$a \in D$ $\sim P(a)$ ——— $\therefore \sim(\forall x \in D, P(x))$
Direct Proof (Exhaustive):	$D = \{a, b, c\}$ $P(a)$ $P(b)$ $P(c)$ ——— $\therefore\ \forall x \in D, P(x)$	Direct Proof (Generalization):	$P(x)$ for arbitrary $x \in D$ ——— $\therefore\ \forall x \in D, P(x)$
		Direct Proof (by cases):	$D = \{x \mid (x \in E) \vee (x \in F)\}$ $\forall x \in E, P(x)$ $\forall x \in F, P(x)$ ——— $\therefore\ \forall x \in D, P(x)$
Indirect Proof (Contradiction):	assume $\sim P(x)$ ——— $\therefore\ a$ $\therefore \sim a$ ——— $\therefore\ P(x)$	Indirect Proof (Contraposition):	$\forall x \in D, \sim Q(x) \to \sim P(x)$ ——— $\therefore\ \forall x \in D, P(x) \to Q(x)$
Induction:	$P(1)$ $P(k) \to P(k+1)$ ——— $\therefore\ \forall n \in \mathbb{Z}^+, P(n)$	Strong Induction:	$P(1)$ $P(1) \wedge \ldots \wedge P(k) \to P(k+1)$ ——— $\therefore\ \forall n \in \mathbb{Z}^+, P(n)$

Sets:

$A \subseteq B \Leftrightarrow \forall x \in \mathbb{U}, (x \in A) \to (x \in B)$	$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
$A \cup B = \{x \in \mathbb{U} \mid (x \in A) \vee (x \in B)\}$	$A \cap B = \{x \in \mathbb{U} \mid (x \in A) \wedge (x \in B)\}$
$A - B = \{x \in \mathbb{U} \mid (x \in A) \wedge (x \notin B)\}$	$A^C = \{x \in \mathbb{U} \mid (x \notin A)\}$
$\mathcal{P}(A) = \{X \in \mathbb{U} \mid X \subseteq A\}$	$A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}$

Functions:

$f : X \to Y$	X is the domain of f	Y is the co-domain of f
	range of $f = \{y \in Y \mid \exists x \in X, f(x) = y\}$	

f is one-to-one (injective)	$\Leftrightarrow \forall x_1, x_2 \in X, (f(x_1) = f(x_2)) \to (x_1 = x_2)$
f is onto (surjective)	$\Leftrightarrow \forall y \in Y, \exists x \in X, f(x) = y$
f is a one-to-one correspondence (bijection)	$\Leftrightarrow (f$ is one-to-one$) \wedge (f$ is onto$)$

Regular Expressions:

.	Matches any character
[xy]	Matches one character from those listed
[x-z]	Matches one character from the range of characters listed
[ˆxy]	Matches one character from those not listed
|	Matches one element from those separated by pipes
*	Matches the previous element 0 or more times
+	Matches the previous element 1 or more times
?	Matches the previous element 0 or 1 time
$\{m, n\}$	matches the preceding element from m to n times
\s	matches a whitespace character
\d	matches a digit, same as [0-9]
\w	matches an alphanumeric character, including "_"