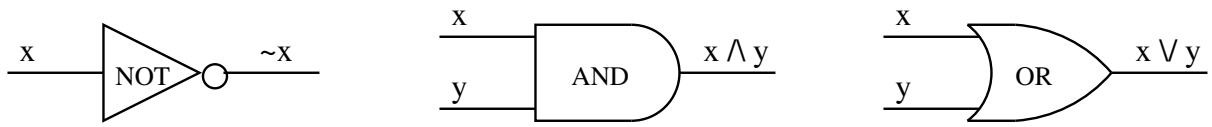


Figure 1: Types of gates in a digital circuit.

CS2742 midterm test 2 study sheet

Boolean circuits:

- *Boolean circuits* is a generalization of Boolean formulas in which we allow to reuse a part of a formula rather than writing it twice. To make a transition write Boolean formulas as trees and reuse parts that are repeating. The connectives become *circuit gates*.

  It is possible to have more than 2 inputs into an AND or OR circuit, but not a NOT circuit.

  It is possible to construct arithmetic circuits (e.g., for doing addition on numbers) by using a Boolean circuit to compute each bit of the answer separately.

Predicate logic:

- A *predicate* is like a propositional variable, but with *free variables*, and can be true or false depending on the value of these free variables. A *domain* of a predicate is a set from which the free variables can take their values (e.g., the domain of $Even(n)$ can be integers).

- *Quantifiers* For a predicate $P(x)$, a quantified statement "for all" ("every", "all") $\forall x P(x)$ is true iff $P(x)$ is true for every value of x from the domain (also called universe); here, $\forall$ is called a *universal quantifier*. A statement "exists" ("some", "a") $\exists x P(x)$ is true whenever $P(x)$ is true for at least one element x in the universe; $\exists$ is an existential quantifier. The word "any" means sometimes $\exists$ and sometimes $\forall$. A domain (universe) of a quantifier, sometimes written as $\exists x \in D$ and $\forall x \in D$ is the set of values from which the possible choices for x are made. If the domain of a quantifier is empty, then if the quantifier is universal then the formula is true, and if quantifier is existential, false. A *scope* of a quantifier is a part of the formula (akin to a piece of code) on which the variable under that quantifier can be used (after the quantifier symbol/inside the parentheses/until there is another quantifier over a variable with the same name). A variable is *bound* if it is under a some quantifier symbol, otherwise it is free.

- *First-order formula* A predicate is a first-order formula (possibly with free variables). A $\wedge, \vee, \neg$ of first-order formulas is a first-order formula. If a formula $A(x)$ has a free variable (that is, a variable x that occurs in some predicates but does not occur under quantifiers such as $\forall x$ or $\exists x$), then $\forall x\ A(x)$ and $\exists x\ A(x)$ are also first-order formulas.

- *Negating quantifiers.* Remember that $\neg \forall x P(x) \iff \exists x \neg P(x)$ and $\neg \exists x P(x) \iff \forall x \neg P(x)$.

- *Database queries* A *query* in a relational database is often represented as a first-order formula, where predicates correspond to the relations occurring in database (that is, a predicate is true on a tuple of values of variables if the corresponding relation contains that tuple). A query "returns" a set of values that satisfy the formula describing the query; a Boolean query, with no free variables, returns true or false. For example, a relation $StudentInfo(x, y)$ in a university database contains, say, all

pairs x, y such that x is a student's name and y is the student number of student with the name x. A corresponding predicate $StudentInfo(x, y)$ will be true on all pairs x, y that are in the database. A query $\exists x StudentInfo(x, y)$ returns all valid student numbers. A query $\exists x \exists y StudentInfo(x, y)$, saying that there is at least one registered student, returns true if there is some student who is registered and false otherwise.

- *Reasoning in predicate logic* The *rule of universal instantiation* says that if some property is true of everything in the domain, then it is true for any particular object in the domain. A combination of this rule with modus ponens such as what is used in the "all men are mortal, Socrates is a man $\therefore$ Socrates is mortal" is called universal modus ponens.

- *Normal forms* In a first-order formula, it is possible to rename variables under quantifiers so that they all have different names. Then, after pushing negations into the formulas under the quantifiers, the quantifier symbols can be moved to the front of a formula (making their scope the whole formula).

- *Formulas with finite domains* If the domain of a formula is finite, it is possible to check its truth value using Resolution method. For that, the formula is converted into a propositional formula (*grounding*) by changing each $\forall x$ quantifier with a $\wedge$ of the formula on all possible values of x; an $\exists$ quantifier becomes a $\vee$. Then terms of the form $P(value)$ (e.g., $Even(5)$) are treated as propositional variables, and resolution can be used as in the propositional case.

- *Limitations of first-order logic* There are concepts that are not expressible by first-order formulas, for example, transitivity ("is there a flight from A to B with arbitrary many legs?" cannot be a database query described by a first-order formula).

- *Resolution for predicate logic* Given a first-order formula with only universal quantifiers (and with different named variables under different quantifiers), the resolution rule $(C \vee P(\bar{X})) \vee (D \vee \neg P(\bar{X}))$ can be applied to obtain $(C \vee D)$ as before. Note, though, that not only the predicate on which resolution is done is the same in both clauses (e.g., you cannot resolve $P()$ with $\neg Q()$), but also the parameters X have to be the same in both cases. The goal of the resolution procedure is, just like in the propositional case, to derive an empty clause(i.e., by resolving a clause containing just a variable with a clause containing just its negation.)

- *Skolemization* When starting with a first-order formula with both universal and existential quantifiers, convert it into a formula with only universal ones by, for every existentially quantified variable, replacing its every occurrence by a function of preceding universally quantified variables (different for different variables); for example, $\forall x \exists y \forall z \forall u \exists v A(x, y, z, u, v)$ becomes $\forall x \forall z \forall u A(x, f(x), z, u, g(x, z, u))$, where f and g are distinct new function symbols.

- *Unification* is a procedure allowing to match parameters in different occurrences of a predicate (to make them the same so that the resolution rule can be applied). A variable can be substituted by anything other than a function of the same variable (i.e., a constant, a term, or another variable); a substitution should replace all occurrences of a variable whether directly in predicates or inside a term. For example, $Q(x, f(x), 5)$ and $\neg Q(3, y, z)$ can be unified via substitutions $x/3$, then $y/f(3)$ then $z/5$, giving $(3, f(3), 5)$ as parameters to both occurrences. This substitution is called the unifier. Usually, the most general unifier is sought: that is, if some substitution can be avoided, then don't do it.

Set Theory

- A *set* is a well-defined collection of objects, called elements of a set. An object x belongs to set A is denoted $x \in A$ (said "x in A" or "x is a member of A"). Usually for every set we consider a bigger "universe" from which its elements come (for example, for a set of even numbers, the universe can be all natural numbers). A set is often constructed using *set-builder notation*: $A = \{x\ inU|P(x)\}$ where U is a universe , and $P(x)$ is a predicate statement; this is read as "x in U such that $P(x)$" and denotes all elements in the universe for which $P(x)$ holds. Alternatively, for a small set, one can list its elements in curly brackets (e.g., $A = \{1, 2, 3, 4\}$.)

- A set A is a *subset* of set B, denoted$A \subseteq B$, if $\forall x(x \in A \to x \in B)$. It is a *proper* subset if $\exists x \in B$ such that $x \notin A$. Otherwise, if $\forall x(x \in A \leftrightarrow x \in B)$ two sets are equal.

- Special sets are: *empty set* $\emptyset$, defined as $\forall x(x \notin \emptyset)$. Universal set U: all potential elements under consideration at given moment. A *power set* for a given set A, denoted 2^A is the set of all subsets of A. If A has n elements, then 2^A has 2^n elements (since for every element there are two choices, either it is in, or not). A power set is always larger than the original set, even in the infinite case (use diagonalization to prove that).

- Basic set operations are a *complement* $\bar{A}$, denoting all elements in the universe that are *not* in A, then *union* $A \cup B = \{x|x \in A \text{ or } x \in B\}$, and *intersection* $A \cap B = \{x|x \in A \text{ and } x \in B\}$ and *set difference* $A - B = \{x|x \in A \text{ and } x \notin B\}$. Lastly, the Cartesian product of two sets $A \times B = \{(a, b)|a \in A \text{ and } b \in B\}$.

- To prove that $A \subseteq B$, show that if you take an arbitrary element of A then it is always an element of B. To prove that two sets are equal, show both $A \subseteq B$ and $B \subseteq A$. You can also use set-theoretic identities.

- A *cardinality* of a set is the number of elements in it. Two sets have the same cardinality if there is a bijection between them. If the cardinality of a set is the same as the cardinality of $\mathbb{N}$, the set is called *countable*. If it is greater, then *uncountable*.

- **Boolean algebra**: A set B with three operations $+, \cdot$ and $\bar{}$, and special elements 0 and 1 such that $0 \neq 1$, and axioms of identity, complement, associativity and distributivity. Logic is a boolean algebra with F being 0, T being 1, and $\bar{}, +, \cdot$ being $\neg, \vee, \wedge$,respectively. Set theory is a boolean algebra with $\emptyset$ for 0, U for 1, and $\bar{}, \cup, \cap$ for $\bar{}, +, \cdot$. Boolean algebra is sound and complete: anything true is provable (completeness) and anything provable is true (soundness).

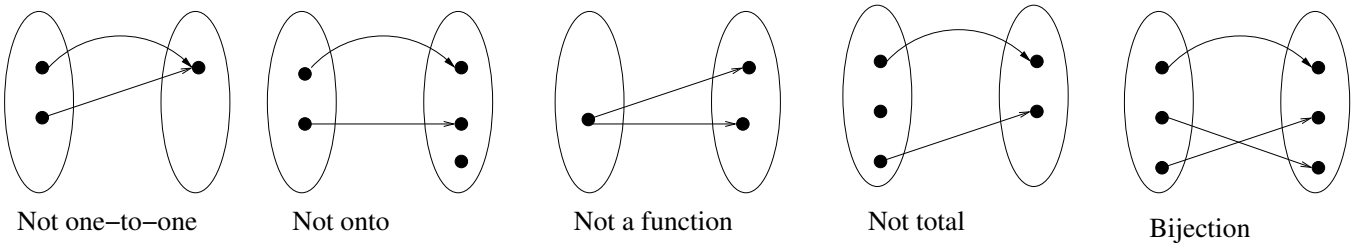
  To see that it is sound, use the fact that the axioms are true in the language of first-order logic or set theory, and the rules of inference are $x = x$, $x = y \to y = x$ and $x = y \wedge y = z \to y = z$, which preserve soundness. For completeness, show that every formula in Boolean algebra can be simplified and then extended to its "normal form" DNF obtained from its truth table.

Relations and Functions

1. A **function** f: $A \to B$ is a special type of relation $R \subseteq A \times B$ such that for any $x \in A, y, z \in B$, if $f(x) = y$ and $f(x) = z$ then $y = z$. If $A = A_1 \times \ldots \times A_k$, we say that the function is k-ary. In words, a $k+1$-ary relation is a k-ary function if for any possible value of the first k variables there is at most one value of the last variable. We also say "f is a mapping from A to B" for a function f, and call $f(x) = y$ "f maps x to y".
   - A function is *total* if there is a value $f(x) \in B$ for every x; otherwise the function is *partial*. For example, $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ is a total function, but $f(x) = \frac{1}{x}$ is partial, because it is not defined when $x = 0$.

Table 1: **Laws of boolean algebras, logic and sets**

Name	**Logic law**	**Set theory law**	**Boolean algebra law**
Double Negation	$\neg\neg p \iff p$	$\overline{\overline{A}} = A$	$\overline{\overline{x}} = x$
DeMorgan's laws	$\neg(p \vee q) \iff (\neg p \wedge \neg q)$ $\neg(p \wedge q) \iff (\neg p \vee \neg q)$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\overline{x + y} = \overline{x} \cdot \overline{y}$ $\overline{x \cdot y} = \overline{x} + \overline{y}$
Associativity	$(p \vee q) \vee r \iff p \vee (q \vee r)$ $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	$(x + y) + z = x + (y + z)$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
Commutativity	$p \vee q \iff q \vee p$ $p \wedge q \iff q \wedge p$	$A \cup B = B \cup A$ $A \cap B = B \cap A$	$x + y = y + x$ $x \cdot y = y \cdot x$
Distributivity	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ $x + (y \cdot z) = (x + y) \cdot (x + z)$
Idempotence	$(p \vee p) \iff p \iff (p \wedge p)$	$A \cup A = A = A \cap A$	$x + x = x = x \cdot x$
Identity	$p \vee F \iff p \iff p \wedge T$	$A \cup \emptyset = A = A \cap U$	$x + 0 = x = x \cdot 1$
Inverse	$p \vee \neg p \iff T$ $p \wedge \neg p \iff F$	$A \cup \bar{A} = U$ $A \cap \bar{A} = \emptyset$	$x + \bar{x} = 1$ $x \cdot \bar{x} = 0$
Domination	$p \vee T \iff T$ $p \wedge F \iff F$	$A \cup U = U$ $A \cap \emptyset = \emptyset$	$x + 1 = 1$ $x \cdot 0 = 0$



- If a function is $f\colon A \to B$, then A is called the *domain* of the function, and B a *codomain*. The set of $\{y \in B \mid \exists x \in A, f(x) = y\}$ is called the *range* of f. For $f(x) = y$, y is called the *image* of x and x a *preimage* of y.
- A *composition* of $f\colon A \to B$ and $g\colon B \to C$ is a function $g \circ f\colon A \to C$ such that if $f(x) = y$ and $g(y) = z$, then $(g \circ f)(x) = g(f(x)) = z$.
- A function $g\colon B \to A$ is an *inverse* of f (denoted f^{-1}) if $(g \circ f)(x) = x$ for all $x \in A$.
- A total function f is *one-to-one* if for every $y \in B$, there is at most one $x \in A$ such that $f(x) = y$. For example, the function $f(x) = x^2$ is not one-to-one when $f\colon \mathbb{Z} \to \mathbb{N}$ (because both $-x$ and x are mapped to the same x^2), but is one-to-one when $f\colon \mathbb{N} \to \mathbb{N}$.
- A total function $f\colon A \to B$ is *onto* if the range of f is all of B, that is, for every element in B there is some element in A that maps to it. For example, $f(x) = 2x$ is onto when $f\colon \mathbb{N} \to Even$, where $Even$ is the set of all even numbers, but not onto $\mathbb{N}$.
- A total function that is both one-to-one and onto is called a *bijection*.
- A function $f(x) = x$ is called the *identity* function. It has the property that $f^{-1}(x) = f(x)$. A function $f(x) = c$ for some fixed constant c (e.g., $f(x) = 3$) is called a *constant* function.

Foundations of mathematics

- *Zermelo-Fraenkel set theory* The foundations of mathematics, that is, the axioms from which all the mathematics is derived are several axioms about sets called Zermelo-Fraenkel set theory (together with the axiom of choice abbreviated as ZFC). For example, numbers can be defined from sets as follows: 0 is $\emptyset$. 1 is $\{\emptyset\}$. 2 is $\{\emptyset, \{\emptyset\}\}$ and in general n is $n-1 \cup \{n-1\}$. ZFC is carefully constructed to explicitly disallow *Russell's paradox* "if a barber shaves everybody who does not shave himself, who shaves the barber?" (in set theoretic terms, if X is a set of sets A such as $A \notin A$, is $X \in X$?) This kind of reasoning is used to prove that *halting problem* of checking whether a given piece of code contains an infinite loop is not solvable (an alternative way to prove this is diagonalization).

- A *theory* is a set of statements, or, in a different view, a set of axioms from which a set of statements can be proven. Here, *axioms* are statements that are assumed in the theory (for example, $\forall x, y \;\; x+y = y+x$).

- A *model* of a theory is a description of a possible world, that is, a set of objects and interpretations of functions and relations, in which axioms are true. There can be several models for the same theory. For example, Euclidean geometry has as a model the geometry on a plane. Without the 5th postulate about parallel lines, there are other possible models such as geometry on a sphere (where parallel lines intersect).

- A theory is called *complete* if it contains (proves) every true (in every model) statement about the objects that can be described in its language (e.g., sets or natural numbers) and *sound* if every statement provable from the axioms is indeed true.