Digital Logic Systems

Recitation 1: Sets and Functions, Induction and Recursion

Guy Even Moti Medina

School of Electrical Engineering Tel-Aviv Univ.

March 3, 2019

Digital Logic and its place in electronics

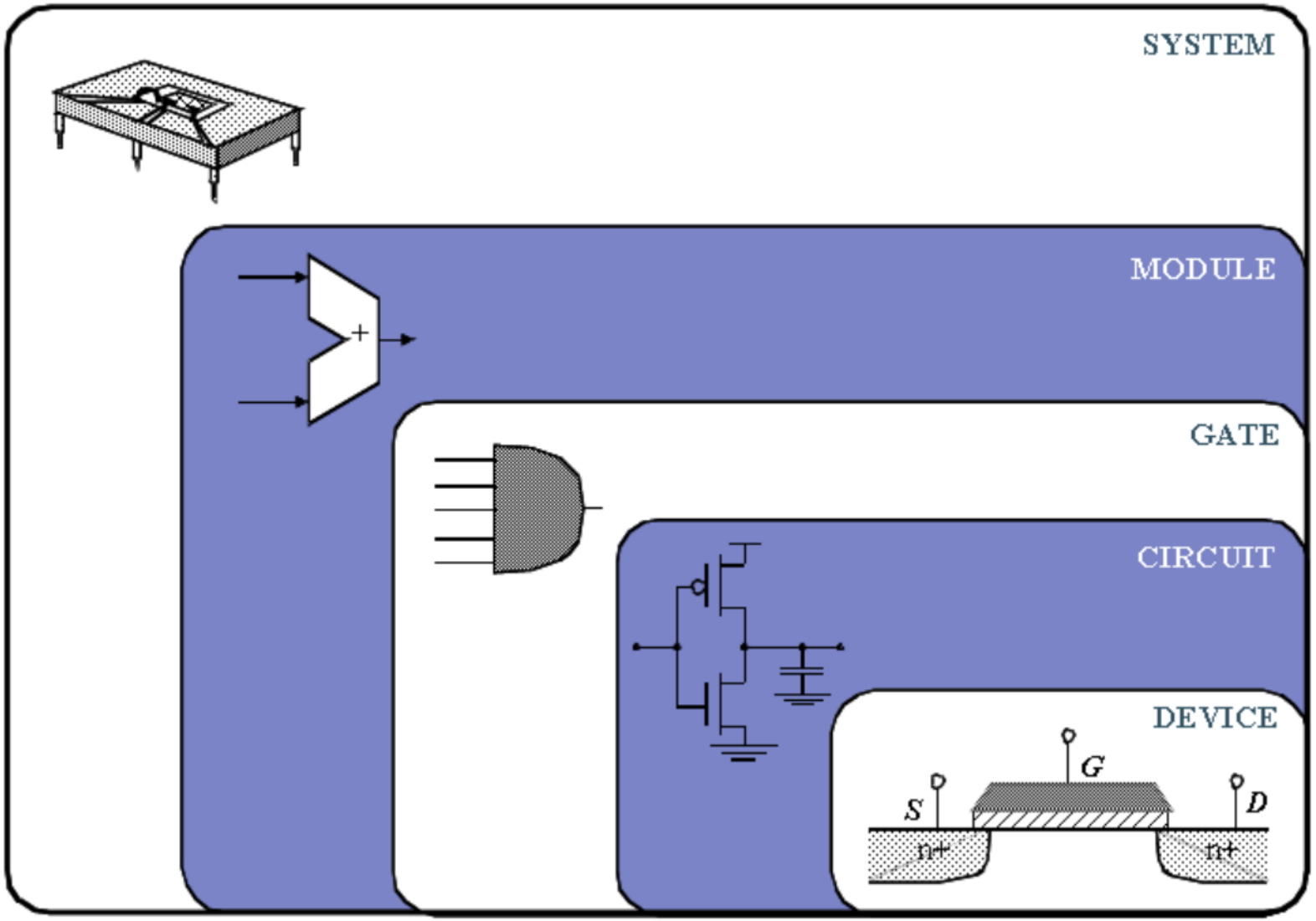

Figure: A hierarchy of design levels in modern electronics

Sets

- Let $A \triangleq \{1, 2, 4, 8\}$ and $B \triangleq \{\text{pencil}, \text{pen}, \text{eraser}\}$.
- Examples of equal sets:
  (i) Order and repetitions do not affect the set, e.g., $\{1, 1, 1\} = \{1\}$ and $\{1, 2\} = \{2, 1\}$.
  (ii) $\{2, 4, 8, 1, 1, 2\} = A$,
  (iii) $\{1, 2, 44, 8\} \neq A$,
  (iv) $A \neq B$.
- The empty set is denoted by $\varnothing$. The set $\{\varnothing\}$ contains a single element which is the empty set. Therefore, $\varnothing \neq \{\varnothing\}$.

Sets can be disjoint

- If $A \cap B = \varnothing$, then we say that A and B are *disjoint*.
- if $A_1 \cap \cdots \cap A_k = \varnothing$ then we say $A_1, \ldots, A_k$ are disjoint .
- if for every $i \neq j$, the sets A_i and A_j are disjoint, we say that the sets $A_1, \ldots, A_k$ are *pairwise-disjoint*

Example

Consider the three sets $\{1,2\}$, $\{2,3\}$ and $\{1,3\}$. Their intersection is empty, therefore, they are disjoint. However, the intersection of every pair of sets is nonempty, therefore, they are not pairwise disjoint.

- When $A \cap B = \varnothing$, we denote their union by $A \cup B$:
  1. $|A \cup B| = |A| + |B|$,
- When it is unknown whether A and B are disjoint, we denote their union by $A \cup B$:
  1. $|A \cup B| \leq |A| + |B|$

Sets equality

Lemma

For every sets A and B,

$$A \setminus B = A \cap \bar{B} .$$

Proof.

To prove this we show containment in both directions:

(i) We prove that $A \setminus B \subseteq A \cap \bar{B}$. Let $x \in A \setminus B$. By the definition of subtraction of sets, this means that $x \in A$ and $x \notin B$. By the definition of complement, $x \in \bar{B}$. By the definition of intersection, $x \in A \cap \bar{B}$, as required.

(ii) We prove that $A \cap \bar{B} \subseteq A \setminus B$. Let $x \in A \cap \bar{B}$. By the definition of intersection of sets, this means that $x \in A$ and $x \in \bar{B}$. By the definition of complement, $x \in \bar{B}$ implies that $x \notin B$. By the definition of subtraction, $x \in A \setminus B$, as required.

Boolean Functions

- The *parity* function $p : \{0,1\}^n \to \{0,1\}$ is defined as follows.

$$p(b_1, \ldots, b_n) \triangleq \begin{cases} 1 & \text{if } \sum_{i=1}^n b_i \text{ is odd} \\ 0 & \text{if } \sum_{i=1}^n b_i \text{ is even.} \end{cases}$$

  For example: (i) $p(0,1,0,1,0) = 0$, (ii) $p(0,1,1,1,0) = 1$, (iii) for $n = 2$, the parity function is identical to the XOR function.

- The *majority* function $m : \{0,1\}^n \to \{0,1\}$ is defined as follows.

$$m(b_1, \ldots, b_n) = 1 \quad \text{if and only if} \quad \sum_{i=1}^n b_i > \frac{n}{2}.$$

  For example: (i) $m(0,1,0,1,0) = 0$, (ii) $m(0,1,1,1,0) = 1$, (iii) for $n = 2$, the majority function is identical to the AND function.

Boolean Functions: Truth Tables

Remember

If you have the truth-tables of the functions $f, g : \{0,1\}^n \to \{0,1\}$ and these truth tables are exactly identical, then $g = f$

Definition

- The implication operator $\rightarrow(x,y)$ is defined by

$$x \rightarrow y \Leftrightarrow \bar{x} \vee y \,.$$

- The equivalence operator $\leftrightarrow(x,y)$ is defined by

$$x \leftrightarrow y \Leftrightarrow \neg(x \oplus y) \,.$$

Truth tables:

x	y	$\rightarrow(x,y)$
0	0	1
1	0	0
0	1	1
1	1	1

x	y	$\leftrightarrow(x,y)$
0	0	1
1	0	0
0	1	0
1	1	1

Commutative and Associative Binary Operations

The subtraction operation $- : \mathbb{R}^2 \to \mathbb{R}$ is neither associative nor commutative.
For example:

- $0 - (0 - 1) = 1$ but $(0 - 0) - 1 = -1$, and
- $1 - 2 = -1$ but $2 - 1 = 1$.

Proving or Refuting Claims

Remember

- proving a claim: prove it for every example possible
- refuting a claim: provide a single counter example

Two variants of proof by induction

Theorem (Induction)

Let $P \subseteq \mathbb{N}$. Assume that (i) $0 \in P$ and (ii) for every $n \in \mathbb{N}$, $n \in P$ implies that $(n+1) \in P$. Then, $P = \mathbb{N}$.

We remark, that sometimes the induction hypothesis is that $i \in P$, for every $i \leq n$. This form of induction is often called *complete induction*, as formulated in the following theorem.

Theorem (Complete Induction)

Let $P \subseteq \mathbb{N}$. Assume that (i) $0 \in P$ and (ii) for every $n \in \mathbb{N}$, $\{0, \ldots, n\} \subseteq P$ implies that $(n+1) \in P$. Then, $P = \mathbb{N}$.

Proof by Induction

How to approach induction:

1. Understand the claim you are proving.
2. Determine the n on which the induction is to be performed.
3. Declare "induction/complete induction on n"
4. Induction basis: prove that $0 \in P$.
5. Induction hypothesis: assume that $n \in P$.
6. Induction step: prove that if the induction hypothesis holds, then $n+1 \in P$. (if you haven't used the hypothesis here, you probably have a mistake)

Induction on sets Example 1

Lemma (1)

For finite sets A and B (regardless of their disjointness)

$$|A \times B| = |A| \cdot |B|$$

Proof by induction on $|A| = n \in \mathbb{N}$.

- **Basis:** $n = 0 \rightarrow |A| = 0 \rightarrow A = \varnothing$. Hence $|A \times B| = |\varnothing \times B| = |\varnothing| = 0$ and also $|A| \cdot |B| = |\varnothing| \cdot |B| = 0$
- **Hypothesis:**For $|A| = n$: $|A \times B| = n \cdot |B|$
- **Step:** Must prove for $|A| = n + 1$: $|A \times B| = (n+1) \cdot |B|$. Define $A' = A \backslash \{a_0\}$ where $a_0 \in A$.
  - Clearly $|A'| = n$ and $|\{a_0\}| = 1$
  - $A \times B = A' \times B \biguplus \{(a_0, b) | b \in B\}$
  - $|A \times B| = |A' \times B| + |\{(a_0, b) | b \in B\}| \underbrace{=}_{hypo.} n \cdot |B| + 1 \cdot |B| = (n+1) \cdot |B|$

Induction on sets Example 2

Lemma (2)

For finite set A

$$|A^n| = |A|^n$$

Proof by induction on $n \in \mathbb{N}^+$.

- **Basis:** Is trivial: $n = 1 \rightarrow A^1 = A$ and $|A|^1 = |A|$
- **Hypothesis:** For $n > 1$: $|A^n| = |A|^n$
- **Step:** Must prove for $n+1$: $|A^{n+1}| = |A|^{n+1}$.

$$|A^{n+1}| \underbrace{=}_{\text{cartesian}} |A^n \times A| \underbrace{=}_{\text{lemma 1}} |A^n| \cdot |A| \underbrace{=}_{\textit{hypo.}} |A|^n \cdot |A| \underbrace{=}_{\text{power rule}} |A|^{n+1}$$

□

Pólya's proof that "all horses have the same color".
We obviously know that there are two horses with different colors, as depicted in the following figure.

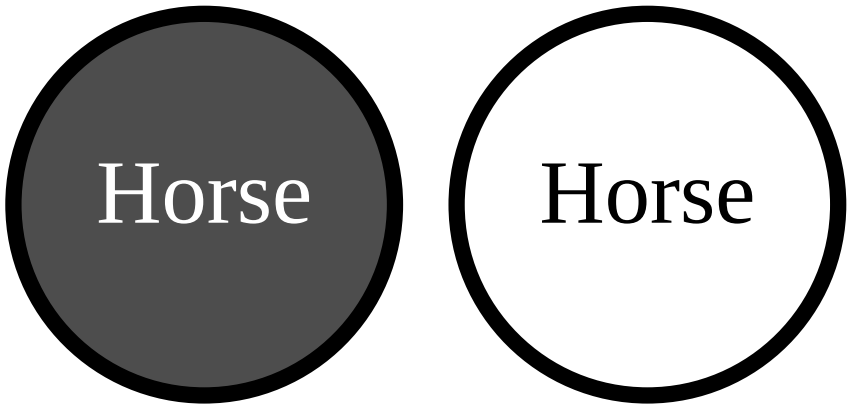

Figure: A counter example to the claim that all the (spherical) horses are the same color. To prove that a claim is not correct all we need is to supply a counter example.

- The "proof" is by induction on the number of horses, denoted by n.
- Thus, we wish to prove that in every set of n horses, all the horses have the same color.
- The induction basis, for $n = 1$, is trivial since in a set consisting of a single horse there is only one color.
- The induction hypothesis simply states that in every set of n horses, all horses have the same color.

Induction (cont.)

- The induction step. We need to prove that if the claim holds for n, then it also holds for $n+1$.
  1. Number the horses, i.e., $\{1,\ldots,n+1\}$.
  2. Consider two subsets of horses $A \triangleq \{1,\ldots,n\}$ and $B \triangleq \{2,\ldots,n+1\}$.
  3. By the induction hypothesis the horses in set A have the same color and the horses in set B also have the same color.
  4. Since $2 \in A \cap B \Rightarrow$ the horses in $A \cup B$ have the same color.
- We have "proved" the induction step, and the "theorem" follows.

Induction (cont.)

What is wrong with this proof?

- Note that, in the induction step, $A \cap B \neq \emptyset$ only if $n \geq 3$.
- However, the induction basis was proved only for $n = 1 \Rightarrow$ we did not prove the induction step for a set of 2 horses.
- A correct proof would have to extend the basis to $n = 2$, an impossible task.
- The take home advice is to make sure that the induction basis is proved for all the cases. In particular, never skip the induction basis even if you think that the claim is "easy" for small values of n.

Lemma

$|P(A)| = 2^{|A|}$, *for every finite set* A.

Proof.

1. We define a function $f : P(A) \to \{0,1\}^{|A|}$ as follows. Assume that without loss of generality $A = \{a_0, a_1, ..., a_{|A|-1}\}$ and $f(s) = v_s$. The vector v_s is formed according to the following rule: $v_s[i] = 1$ if $a_i \in s$ and $v_s[i] = 0$ if $a_i \notin s$.
2. We show that f is **one-to-one** and **onto**.(requires proof)
3. From combinational considerations: $|\{0,1\}^{|A|}| = 2^{|A|}$
4. From (2) and (3) it follows that $|P(A)| = |\{0,1\}^{|A|}| = 2^{|A|}$

Recursion: the factorial function

Definition

The tower of Hanoi function $t : \mathbb{N} \to \mathbb{N}$ is defined recursively by:

(i) Base case: $t(0) = 0$.

(ii) Reduction rule: $t(n+1) = 2t(n) + 1$.

Claim

$t(n) = 2^n - 1$.

Proof.

By induction on n. □

Contraposition

Problem

Prove that $x^2 + 6x + 5$ is even $\rightarrow$ x is odd.

Proof.

By contraposition:

- Assume that x is even.
- Therefore x^2 is even, $6x$ is even, 5 is odd.
- Summing up all of the above leads to an odd sum.