Hardware & Embedded Security

Part 2

Academic Year: 2024-2025

Prof Daniele Rossi


Via G. Caruso 16, room B-1-03


daniele.rossi1@unipi.it


050 221 7611

1

Course Content – Prof. D. Rossi

- **Security issues and threat modelling for hardware supply chain** (Prof. Saponara)
- **Basics on CMOS VLSI technology and testing**
- **Counterfeiting of electronics**
  - Different types of counterfeits (Prof. Saponara)
  - Testing for counterfeit detection
  - Recycled and Remarked ICs → Design for Anticounterfeit
- **Hardware Trojans** (characteristics and detection techniques)
- **Physical(ly) Unclonable Functions (PUFs) and True Random Number Generators (TRNGs)**
  - Scope, operating principle, architectures, security issues
- **Hardware-level attack** (attacks and protection techniques)
  - Side Channel Attacks, Power Attacks, Fault-Injection Attacks

2

Study Material & Reading List

- **Lecture notes**
- Additional material provided by the lecturer (scientific articles, book chapters, dissertations, etc.)
- Mark (Mohammad) Tehranipoor, Ujjwal Guin, Domenic Forte, **Counterfeit Integrated Circuits - Detection and Avoidance**, Springer International Publishing, 2015
- Mohammad Tehranipoor, Hassan Salmani, Xuehui Zhang, **Integrated Circuit Authentication - Hardware Trojans and Counterfeit Detection**, Springer International Publishing, 2014
- Basel Halak, **Physically Unclonable Functions - From Basic Design Principles to Advanced Hardware Security Applications**, Springer International Publishing, 2018

3

Office Hours

- Students can make an appointment for a meeting by emailing daniele.rossi1@unipi.it
- Students can contact me either via email or on the MS Teams chat
- We can carry out either f-2-f meetings or joint sessions in our MS Teams virtual classroom

4

Brief Outline

- Counterfeit detection
  - Recalling some basics on CMOS VLSI technology
    - Logic gates
    - Propagation delay
    - Power consumption
  - Aging effects in electronic devices
  - Process variations

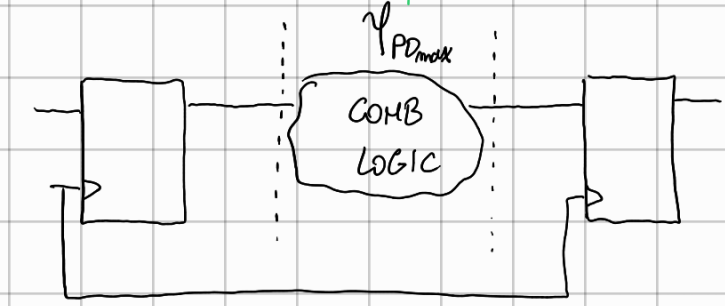
5

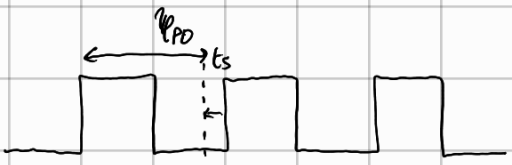
Detection of Counterfeit ICs

Lecture 1 - DR

6

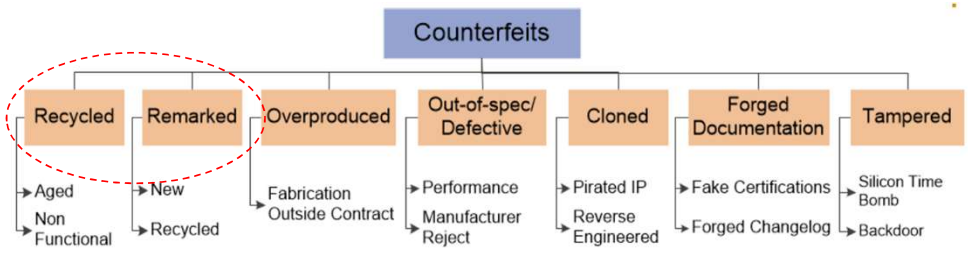
↳ consider the worst case of the prop. delay





When a component ages, the time it takes to perform tasks increases. So t_{PD} is going to be longer. So if the t_{PD} is so long that the setup time constraint is no longer satisfied, a performance degradation becomes a reliability issue. Imagine this as a piece in your car.

Counterfeit Types



- More than 80% of the counterfeit components are recycled
- Most of the recycled parts are at the end of life → damaged considerably due to usage and aging

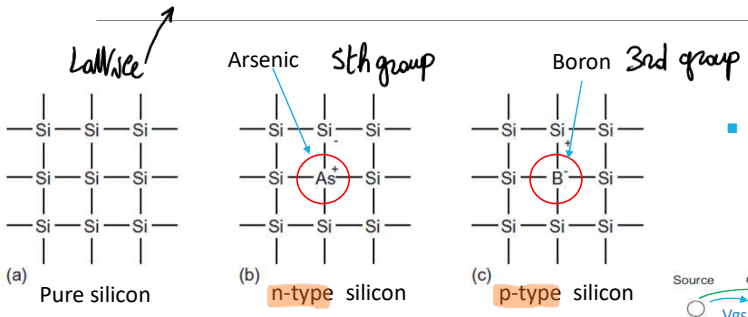
7

Basics on CMOS VLSI

8

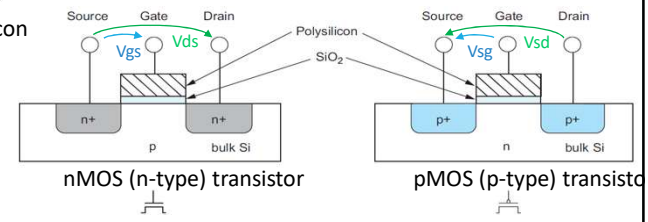
Silicon: 4th group in periodic table

From Silicon to Devices



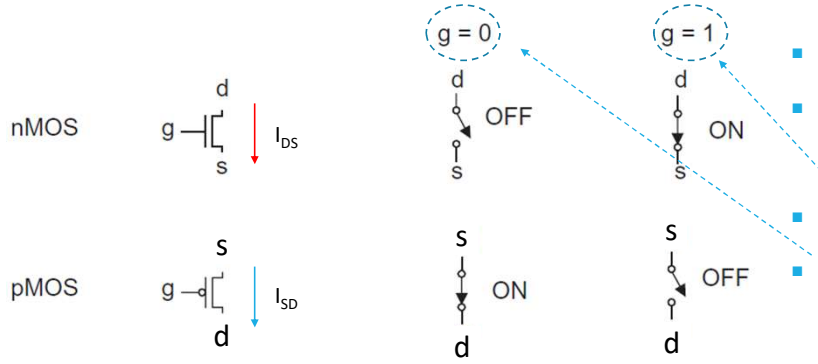
- MOS transistors: stack of Metal-Oxide-Semiconductor

- Silicon (Si), a semiconductor, forms the basic starting material for most integrated circuits



9

MOS Transistors: Switch-level models



- Supply (positive) voltage: V_{DD}
- Ground (low) voltage: V_{SS} (0 V)

- V_{DD} represents a **logic 1**
- V_{SS} (ground, 0 V) represents a **logic 0**

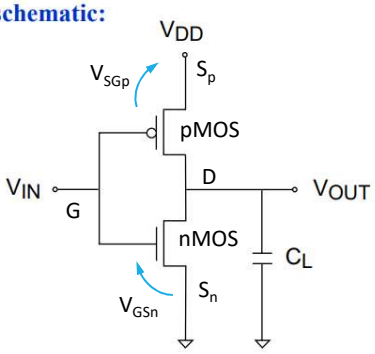
11

Complementary MOS (CMOS) Logic

$V_{Tn} > 0$
$V_{Tp} < 0$

- Complementary MOS inverter

Circuit schematic:



Basic Operation:

- $V_{IN} = 0 \Rightarrow V_{OUT} = V_{DD}$
  - $V_{GSn} = 0 \ (< V_{Tn}) \Rightarrow$ **NMOS OFF**
  - $V_{SGp} = V_{DD} \ (> -V_{Tp}) \Rightarrow$ **PMOS ON**
- $V_{IN} = V_{DD} \Rightarrow V_{OUT} = 0$
  - $V_{GSn} = V_{DD} \ (> V_{Tn}) \Rightarrow$ **NMOS ON**
  - $V_{SGp} = 0 \ (< -V_{Tp}) \Rightarrow$ **PMOS OFF**

tech parameter

$$I_D \equiv \frac{k_n}{2}\left(\frac{W}{L}\right)_n (V_{GS} - V_{Tn})^2 \text{ for } V_{DS} > V_{GS} - V_{Tn}$$

$$I_D \equiv k_n\left(\frac{W}{L}\right)_n \left[(V_{GS} - V_{Tn})V_{DS} - V_{DS}^2/2\right] \text{ for } V_{DS} \le V_{GS} - V_{Tn}$$

- Ideally: no power consumption while idle in any logic state

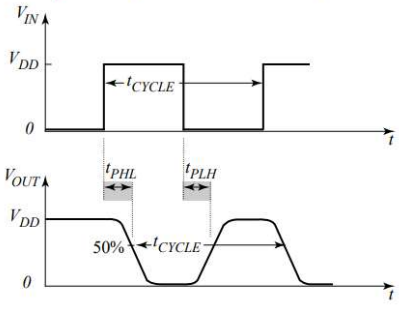
12

$V_{IN}=1$, switch closed, discharges V_{out}. V_{out} is in shortcircuit with ground so 0V.
$V_{IN}=0$, switch p closed, V_{out} is in short circuit with the supply voltage.
We have C_L to represent the load of all the gates connected together. ①

Propagation Delay in a CMOS Inverter (I)

- Inverter propagation delay: delay time between input and output signals; figure of merit of logic speed

Estimation of t_p: use square-wave at input So assume to change input instantaneously.

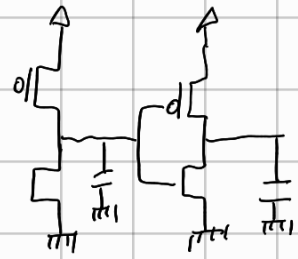


Average propagation delay:

$$t_p = \frac{1}{2}(t_{PHL} + t_{PLH})$$

13

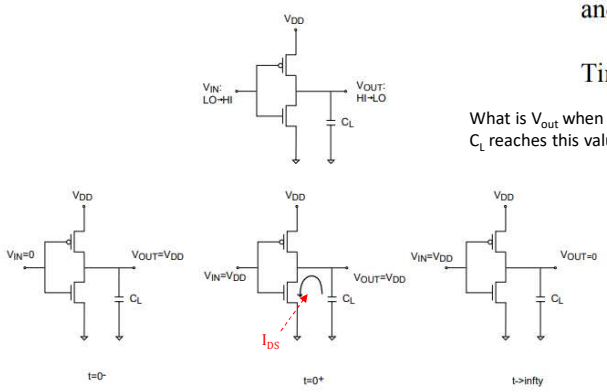
① This is what we call parasitic capacitance. Because of other gates, plus you have a connection to other gates, so a connection to a gate (metal), oxide and semiconductor. So those are part of the parasitic capacitance effect.



How long does it take to charge/discharge? It depends on the I_D drain current. Which depends on the size of the MOS, on the V_{GS} (so depends on the power supply), but you also have a threshold voltage for the conduction of current. In a first approximation, V_T can be seen as constant. This depends on the technology, which is recognised by the name of tech + the size of your components you can produce. For CMOS we are producing them in the size of 1mm. For 3mm tech, $V_{Tn} \approx 0.3/0.4$ V. But this parameter increases with aging. So I_D decreases in the equation. So if current is decreased, the time it takes to charge or discharge parasitic capacitances increases over time.

Propagation Delay in CMOS Inverter (II)

Propagation delay high-to-low



During early phases of discharge, NMOS is saturated and PMOS is cut-off.

Time to discharge ***half*** of charge stored in C_L:.

What is V_{out} when the charge in C_L reaches this value?

$$t_{pHL} \approx \frac{\frac{1}{2}\text{charge on } C_L \ @t=0^-}{\text{NMOS discharge current}}$$

This relation comes from:

$$I_C = C_L \frac{dV_c}{dt}$$

I_C = discharge current I_{DS}
$V_C = V_{out}$

14

Propagation Delay in CMOS Inverter (III)

Propagation delay high-to-low (cont'd)

Charge in C_L at t=0⁻:

$$Q_L(t=0^-) = C_L V_{DD}$$

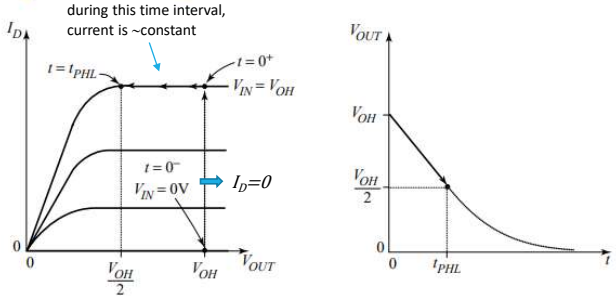
Discharge Current (NMOS in saturation):

$$I_{Dn} = \frac{W_n}{2L_n}\mu_n C_{ox}(V_{DD} - V_{Tn})^2$$

Then:

$$t_{PHL} \approx \frac{C_L V_{DD}}{\frac{W_n}{L_n}\mu_n C_{ox}(V_{DD} - V_{Tn})^2}$$

Graphical Interpretation



$k_n = \mu_n C_{ox}$

15

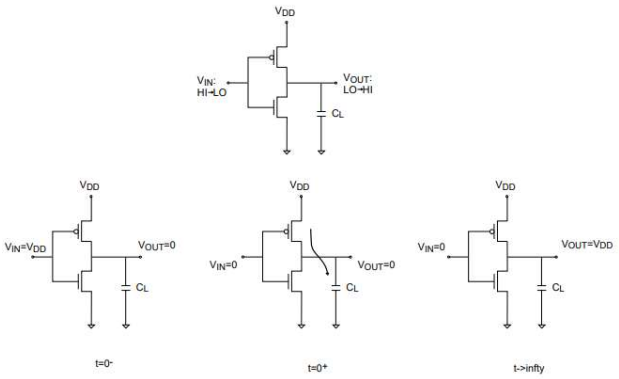
If the current decreases or takes longer to charge/discharge

REMEMBER: if current decreases over time, macroscopic effect is increase in prop. delay.

HIGH TO LOW deals with NMOS

Propagation Delay in CMOS Inverter (IV)

Propagation delay low-to-high



During early phases of discharge, PMOS is saturated and NMOS is cut-off.

Time to charge to ***half*** of final charge on C_L:.

$$t_{PLH} \approx \frac{\frac{1}{2}\text{charge on } C_L \ @t=\infty}{\text{PMOS charge current}}$$

16

Propagation Delay in CMOS Inverter (V)

Propagation delay low-to-high (cont'd)

Charge in C_L at $t=\infty$:

$$Q_L(t=\infty) = C_L V_{DD}$$

Charge Current (PMOS in saturation):

$$-I_{Dp} = \frac{W_p}{2L_p}\mu_p C_{ox}\left(V_{DD}+V_{Tp}\right)^2 \qquad V_{Tp} < 0$$

Then:

$$t_{PLH} \approx \frac{C_L V_{DD}}{\frac{W_p}{L_p}\mu_p C_{ox}\left(V_{DD}+V_{Tp}\right)^2}$$

$k_p = \mu_p C_{ox}$

Key dependencies of propagation delay:

- $V_{DD} \uparrow \Rightarrow t_p \downarrow$
  - Reason: $V_{DD} \uparrow \Rightarrow Q(C_L) \uparrow$, but I_D goes as square$\uparrow$
  - Trade-off: $V_{DD} \uparrow \Rightarrow$ more power consumed.
- $L \downarrow \Rightarrow t_p \downarrow$
  - Reason: $L \downarrow \Rightarrow I_D \uparrow$
  - Trade-off: manufacturing cost!

- Ideally, $V_{Tn,p}$ is constant (depends on technology, so it is not a design parameter)
- We will see that this is not true, and that $V_{Tn,p} \uparrow$ over lifetime → t_p increases

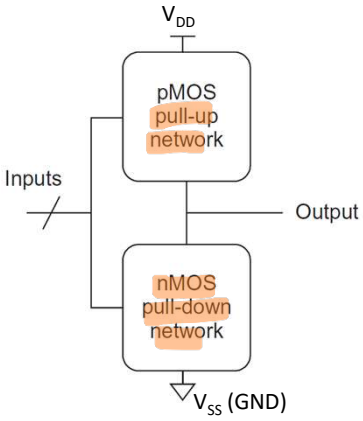
17

LOW TO HIGH deals with PMOS

V_{Tp} is negative. Low to high is defined in the same way. So V_{Tp} decreases, current decreases, so prop. delay increases.

Generalization of a logic gate

CMOS Logic Gates (I)

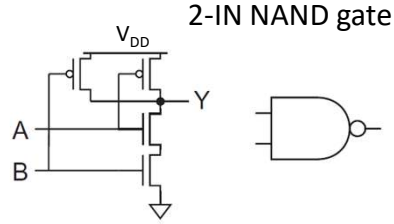


- In general, a static CMOS gate has an
  - nMOS pull-down network to connect the output to 0 (GND) and
  - pMOS pull-up network to connect the output to 1 (VDD)
- The networks are arranged such that one is ON and the other OFF for any input pattern.

18

CMOS Logic Gates (III)

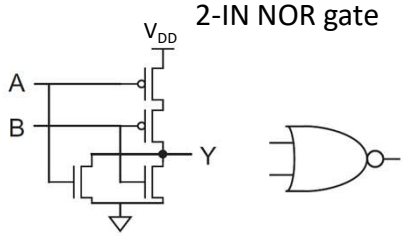
2-IN NAND gate



NAND gate truth table

A	B	Pull-Down Network	Pull-Up Network	Y
0	0	OFF	ON	1
0	1	OFF	ON	1
1	0	OFF	ON	1
1	1	ON	OFF	0

2-IN NOR gate



NOR gate truth table

A	B	Y
0	0	1
0	1	0
1	0	0
1	1	0

20

When functioning, either the pull up or pull down network is on. So in a steady state, there is no conductive connection from supply and ground. Power consumption is ideally 0.

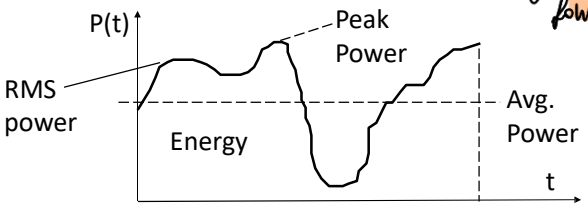
Power Consumption in CMOS circuits

- Power consumption
  - **Dynamic** power consumption
  - **Short-circuit** power consumption
  - **Static** power consumption

Consumed during switching

→ We have during the switching of the input. Since input doesn't go from 0 to 1 instantaneously so you have current flowing

↳ Nowadays even in a steady state we have small currents flowing through the devices: ①

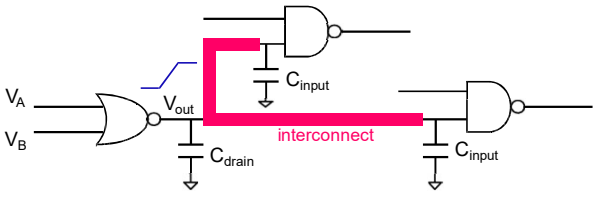


- **Average power**: related to overall power consumption
- **Peak power**: related to reliability
- **RMS power**: related to cycle-by-cycle power
- **Energy** = power x time

21 ① We have sub threshold current ($V_{GS} < V_t$)

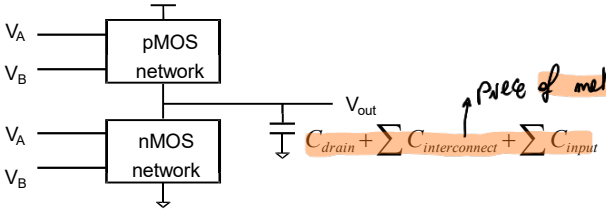
We want to understand whether our system includes only what it needs or we have something that consumes more (HW trojans!)

Dynamic Power Consumption



- Power consumed to process information (main part of switching power)
  → power consumed by each logic gate to charge its output capacitance

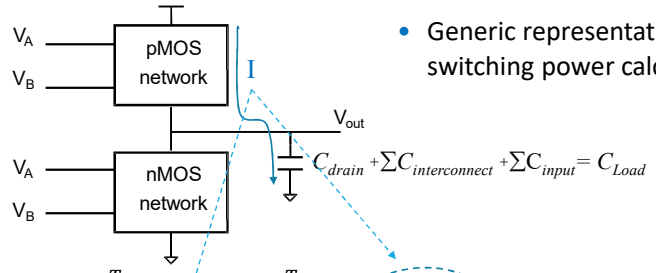
- Generic representation of a CMOS logic gate for dynamic power calculation



piece of metal for connection: contributing to the total capacitance

22 Average power = $V_{DD} I_D$. When we operate, we need to charge and discharge capacitors. NOTE that the higher the capacitance, the higher the charge you need to put in there to have voltage.

Dynamic Power Consumption



- Generic representation of a CMOS logic gate for switching power calculation

$$P_{dyn-} = \frac{1}{T}\int_0^T V_{DD}\, I dt = \frac{1}{T}\int_0^T V_{DD}\, C_{Load}\frac{dV_{out}}{dt} dt = \frac{C_{Load}V_{DD}}{T}\int_0^{V_{DD}} dV_{out} = \frac{1}{T}C_{Load}V_{DD}^2$$

Dynamic power consumption per switching cycle T

$$P_{dyn} = \frac{1}{T}C_{Load}V_{DD}^2 = C_{Load}\,V_{DD}^2\, f$$

T (or f) : switching period (frequency) of the output node voltage

23

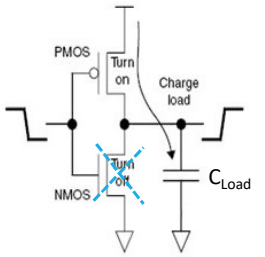
Recall: I_c ↓ $\frac{I_c}{T}$ ↑ V_c for a capacitor: $I_c = C \cdot \frac{dV_c}{dt}$

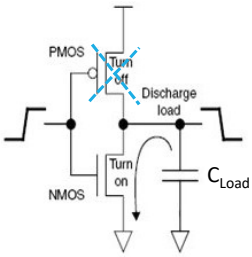
Recall what the dyn power depends on: $P_{dyn} = C_{load} V_{DD}^2 f$

Why V_{DD}^2? P depends on V_{DD} and I, that depends on V. Then of course it depends on load. (1)

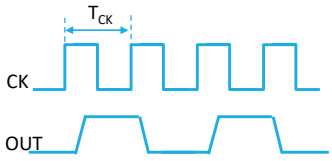
f is as the switching frequency of the output (imagine a gate that never switches).

Dynamic Power: Example





Dynamic (switching) power

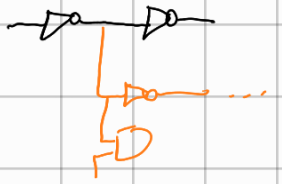


Energy provided by the supply to charge C_{Load} : $E_{dyn} = C_{Load}\, V_{dd}^2$

Energy provided by the supply to discharge C_{Load} : $E_{dyn} = 0$

24

Imagine your circuit is this:



Then your supplier includes this circuit and you don't know. In this case you could recognise that something is wrong because you have an increased parasitic capacitance. If it is higher enough, you might be able to detect this difference.

① In the worst case for power consumption, the switching frequency can be half of the actual clock frequency. This is the case we switch every edge of the clock.

- Note that we consume power when our voltage is providing power. This only happens during the charge of the capacitor. So not all switches produce power consumption. That's why in the expression for $P_{dyn-average} = \alpha_{0\to1} C_{LOAD} V_{DD}^2 f_{CK}$, where $\alpha_{0\to1}$ is a number that explains how many switches from 0 to 1 we have.

Dynamic Power Consumption

- The average dynamic power consumption can be expressed as

$$P_{dyn-a} = \frac{1}{T} C_{Load} V_{DD}^2 = C_{Load} V_{DD}^2 f$$

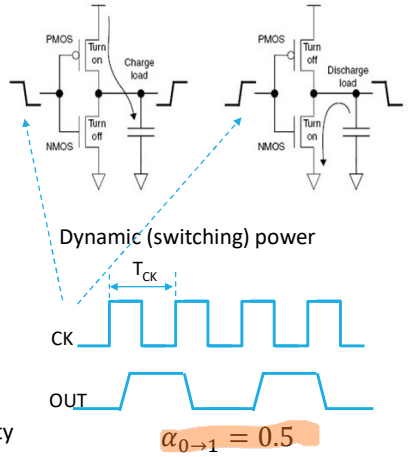
$T(f)$: switching period (frequency) of the output node voltage

- The node transition rate is usually slower than the clock rate. To better represent this behavior, a node *transition factor* (aka *switching activity*) is introduced

$$P_{dyn-a} = \alpha_{0\to1} C_{Load} V_{DD}^2 f_{ck} \quad \text{with } 0 \le \alpha_{0\to1} \le 1$$

Switching activity

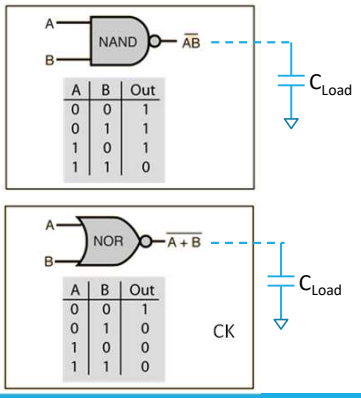
- **Dynamic power is data (workload) dependent**



25

Dynamic Power: Exercise

Dynamic power = $\alpha_{0\to1} C_{Load} V_{dd}^2 f_{ck}$



- All input patterns are equally likely
- Input patterns are applied at the clock frequency f_{CK}

1. What is the value of the switching activity?
2. What is the expression of the dynamic power?

- Same hypotheses and questions as above

$$Pr[Out_1 = 1 \mid Out_0 = 0] = \frac{Pr[Out_1 = 1, Out_0 = 0]}{Pr[Out_0 = 0]} = \frac{1}{8}\ ?$$

=

26

Let's see transition table; show all the possible transitions we go through

NAND

AB_i \ AB_{i+1}	00	01	10	11
00	1	1	1	1→0
01	1	1	1	1→0
10	1	1	1	1→0
11	0→1	0→1	0→1	0

So, $\alpha_{0\to1} = 3/16$

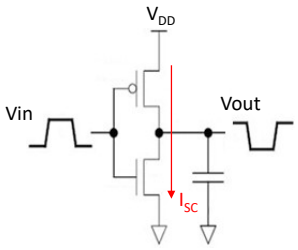
↳ average prob. to have a 0→1 transition

NOR

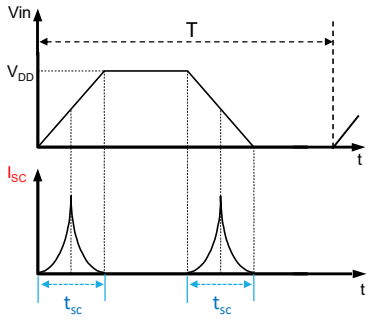
AB_i \ AB_{i+1}	00	01	10	11
00	1	1→0	1→0	1→0
01	0→1	0	0	0
10	0→1	0	0	0
11	0→1	0	0	0

$\alpha_{0\to1} = 3/16$

Short-Circuit Power Consumption



I_{SC} : short-circuit current



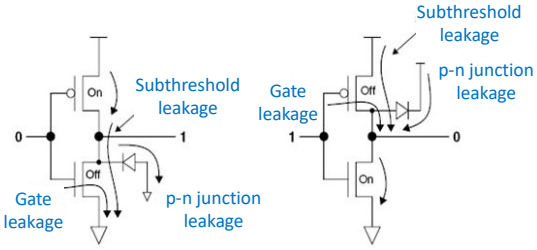
- Short circuit power is usually **neglected**

- When the input switches from 0 →1 and 1 → 0, a conductive path between VDD and ground temporarily establishes for a duration equal to t_{sc}
  ⇒ I_{SC} : short-circuit current ⇒ short circuit power $P_{SC}(t) = I_{SC}(t)V_{DD}$

27

27

Static Power Consumption



- Ideally, in CMOS logic, static power consumption is 0
- However, MOS transistors are not ideal switch
  - Leakage current I_{leak} flowing through OFF transistors
  - Static power = $V_{dd}\, I_{leak}$

28

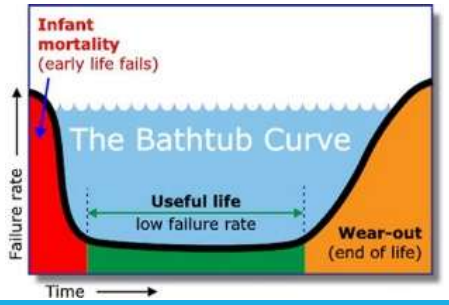
28

Any questions so far?

31

Recycled Components & Aging Phenomena

- **More than 80%** of the counterfeit components are **recycled**
- Most of the recycled parts are at the end of life → damaged considerably due to usage and **aging**



32